P3NK-2652-02Z0

IPアクセスルータ

Si-R シリーズ

Web設定事例集 V33

FUJITSU

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2007年 7月初版
2007年11月第2版

目次

本書の構成と使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

また、CD-ROM の中の README ファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

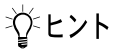
本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内　容
第 1 章　導入例	この章では、本装置の代表的な接続形態を紹介します。
第 2 章　活用例	この章では、本装置の便利な機能の活用方法について説明します。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。



本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて　本装置をご使用になる際に、注意していただきたいことを説明しています。

操作手順で説明しているもののほかに、補足情報を説明しています。

操作方法など関連事項を説明している箇所を示します。

本装置の機能を使用する際に、対象となる機種名を示します。

製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。

製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

本書における商標の表記について

Microsoft、Windows、Windows NT、Windows Server および Windows Vista は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

Adobe および Reader は、Adobe Systems Incorporated（アドビシステムズ社）の米国ならびに他の国における商標または登録商標です。

UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows® XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® Millennium Edition operating system	Windows® Me
Microsoft® Windows® 98 operating system	Windows® 98
Microsoft® Windows® 95 operating system	Windows® 95
Microsoft® Windows® 2000 Server Network operating system	Windows® 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT® 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Server® 2003, Standard Edition	Windows Server® 2003
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003, Web Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista®
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
Si-R 効率化運用ツール使用手引書	Si-R 効率化運用ツールを使用する方法を説明しています。
Si-R180　ご利用にあたって	Si-R180 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R180B　ご利用にあたって	Si-R180B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R220B　ご利用にあたって	Si-R220B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R220C　ご利用にあたって	Si-R220C の設置方法やソフトウェアのインストール方法を説明しています。
Si-R240　ご利用にあたって	Si-R240 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R240B　ご利用にあたって	Si-R240B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R260B　ご利用にあたって	Si-R260B の設置方法やソフトウェアのインストール方法を説明しています。
Si-R370　ご利用にあたって	Si-R370 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R570　ご利用にあたって	Si-R570 の設置方法やソフトウェアのインストール方法を説明しています。
Si-R シリーズ　機能説明書	本装置の便利な機能について説明しています。
Si-R シリーズ　トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
Si-R シリーズ　メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
Si-R シリーズ　仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
Si-R シリーズ　コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Si-R シリーズ　コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
Si-R シリーズ　コマンドリファレンス -構成定義編-	構成定義コマンドの項目やパラメタの詳細な情報を説明しています。
Si-R シリーズ　コマンドリファレンス -運用管理編-	運用管理コマンド、その他のコマンドの項目やパラメタの詳細な情報を説明しています。
Si-R シリーズ　Web ユーザーズガイド	Web 画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Si-R シリーズ　Web 設定事例集（本書）	Web 画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Si-R シリーズ　Web リファレンス	Web 画面の項目の詳細な情報を説明しています。

第1章　導入例

この章では、本装置の代表的な接続形態を紹介します。

1.1 「かんたん設定メニュー」で設定する

適用機種 ***Si-R180,180B,220B,220C***

［設定］タブをクリックすると、［かんたん設定メニュー］ボタンと［詳細設定メニュー］ボタンの 2 つが表示されます。
通常のご利用では、「かんたん設定メニュー」で十分に設定することができます。「かんたん設定メニュー」で設定したあとに、その他の必要な設定に関しては、「詳細設定メニュー」で設定を追加する方法をお勧めします。
「かんたん設定」は、LAN0 および LAN1 インタフェースの構成定義を行います。

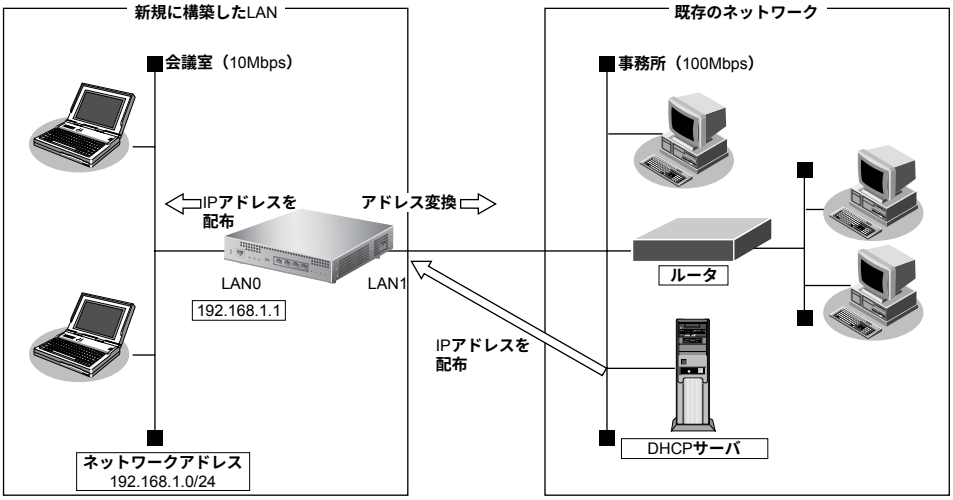
1.1.1 プライベート LAN を構築する

適用機種 ***Si-R180,180B,220B,220C***

プライベート LAN 側では、マルチ NAT 機能を利用しているので、割り当てられた 1 つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスできます。また、DHCP サーバ機能が動作しているため、パソコンの IP アドレスの管理が必要ないので簡単に LAN を構築できます。ここでは、以下の条件で一時的に会議室に LAN を構築し、事務所のネットワークと接続する場合を例に説明します。

本装置の IP アドレスを変更しない場合

本装置がご購入時の状態の場合、「かんたん設定」では以下の省略値が表示されます。［設定終了］ボタンをクリックして、設定を有効にすると通信することができます。
Si-R180、180B は、本装置の電源を投入するだけで通信することができます。ただし、インタフェースは、以下の図とは逆になります（LAN0 → LAN1、LAN1 → LAN0）。Si-R180、180B では、スイッチポート（SW1 ～ 4）が有効になります。



● 設定条件

［事務所側］

- 転送レートは自動認識
- IP アドレスは DHCP サーバから自動的に取得する

[会議室側]

- 転送レートは自動認識
- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

[その他の条件]

- パスワードを設定する
  パスワード　：himitu

参照 Si-R シリーズ　Web ユーザーズガイド「1.4 パスワード情報を設定する」（P.12）

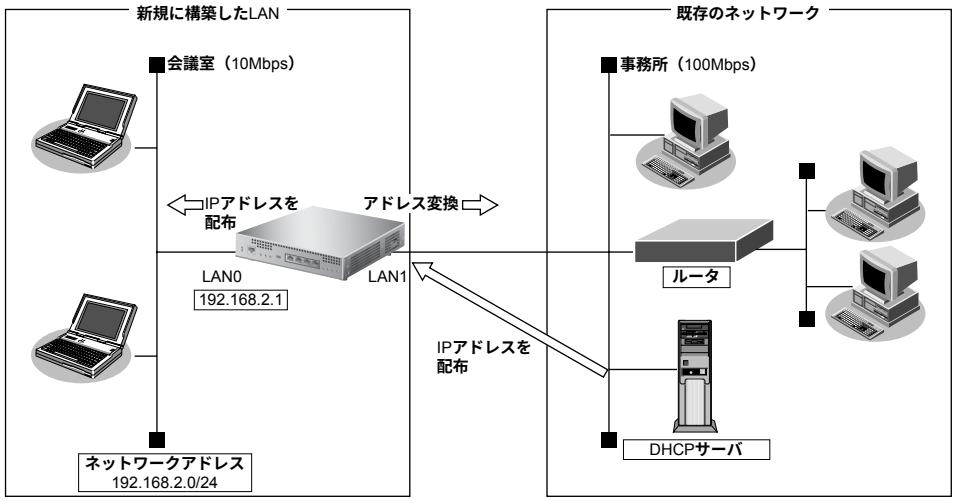
こんな事に気をつけて

- **パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。**
- **「プライベート LAN 構築」で DHCP サーバを使用すると設定した場合は、DHCP サーバが広報する情報（デフォルトルータ、DNS サーバ、ドメイン名）には、DHCP サーバが動作するインタフェース側のネットワーク構成に応じた情報を設定してください。**

本装置の IP アドレスを変更する場合

「プライベート LAN 構築」では、プライベート LAN 側のネットワークアドレスを変更することができます。

以下に、プライベート LAN 側（LAN0 側）のネットワークアドレスを 192.168.2.0/24 に変更する設定方法を説明します。



こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

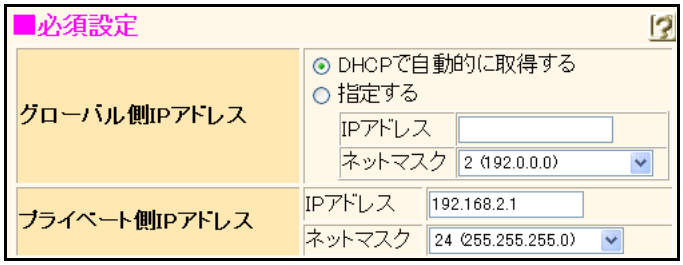
1.　かんたん設定メニューで LAN 間接続の「プライベート LAN 構築」をクリックします。

「プライベート LAN 構築かんたん設定」ページが表示されます。

この例では、グローバル LAN 側（LAN1 側）は DHCP サーバから情報を自動的に取得するので、プライベート LAN 側（LAN0 側）の設定を変更します。

2.　「必須設定」で以下の項目を指定します。

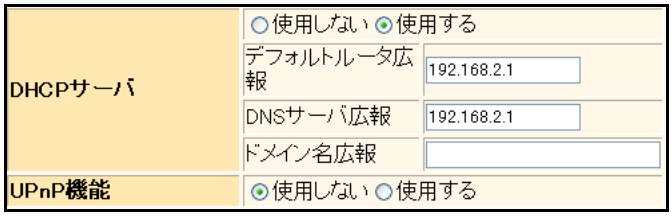
- グローバル側 IP アドレス　→ DHCP で自動的に取得する
- プライベート側 IP アドレス
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）



3.　「オプション設定」で以下の項目を指定します。

- DHCP サーバ　→使用する
  デフォルトルータ広報　→ 192.168.2.1
  DNS サーバ広報　→ 192.168.2.1
- UPnP 機能　→ UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

参照 「2.17 VoIP NAT トラバーサル機能を使う」（P.730）



4.　設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に通信できる状態になります。

こんな事に気をつけて

- **本装置の IP アドレスを変更した場合、以下に示す 2 つの操作が必要です。**
  - **本装置に接続しているパソコンの IP アドレスも変わります。再度、DHCP サーバから割り当ててもらう必要があります。**
  - **再起動後に本装置にアクセスするためには、URL で指定する IP アドレスに変更後の IP アドレスを指定する必要があります。**
- **本装置に接続するネットワーク上のパソコンは、IP アドレスを自動的に取得する設定にしてください。IP アドレスを固定的に設定していると、本装置が配布する IP アドレスと重なり、矛盾が生じる場合があります。なお、常時同じ IP アドレスを取得する場合は、設定の「ホストデータベース情報」に IP アドレスと MAC アドレスを設定してください。**
- **ご購入時は、LAN0 ポートからだけ設定できます。Si-R180、180B は LAN1 ポートから設定してください。**
- **グローバル側インタフェースを LAN0 側に変更した場合、LAN1 ポートからだけ設定できるように変更されます。**

ヒント

◆ 省略値について

プライベート LAN 構築かんたん設定に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目		適用される省略値	かんたん設定での設定変更
グローバル側	IP アドレス	DHCP クライアント機能により自動的に取得する	○
	ネットマスク	DHCP クライアント機能により自動的に取得する	○
	セカンダリ IP アドレス	なし	×
	デフォルトルータ	DHCP クライアント機能により自動的に取得する	○
	DNS サーバアドレス	DHCP クライアント機能により自動的に取得する	○
	DHCP サーバ機能	使用しない	×
	NAT 機能	マルチ NAT を使用する ・アドレス個数：1 個 ・アドレス割り当てタイマ：5 分	×
	RIP 機能 ・RIP 送信 ・RIP 受信	 ルーティングプロトコルを使用しない RIP-V1 を使用する	×
	インタフェース	Si-R180、180B：LAN0、Si-R180、180B 以外：LAN1	○（※）
	転送レート	自動認識	○
プライベート側	IP アドレス	192.168.1.1	○
	ネットマスク	24（255.255.255.0）	○
	セカンダリ IP アドレス	なし	×
	DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数	使用する 本装置のプライベート LAN 側の IP アドレス、ネットマスクから求めたネットワークアドレス＋ 2 253	○ × ×
	デフォルトルータ広報	192.168.1.1	○
	DNS サーバ広報	192.168.1.1	○
	ドメイン名広報	なし	○
	RIP 機能 ・RIP 送信 ・RIP 受信	 RIP-V1 を使用する RIP-V1 を使用する	×
	転送レート	自動認識	○
IPv6 経路		使用しない	×
ブリッジ		使用しない	×
UPnP 機能		使用しない	○

※）Si-R180、180B は変更できません。

1.1.2　セグメント接続／分割する

適用機種　*Si-R180,180B,220B,220C*

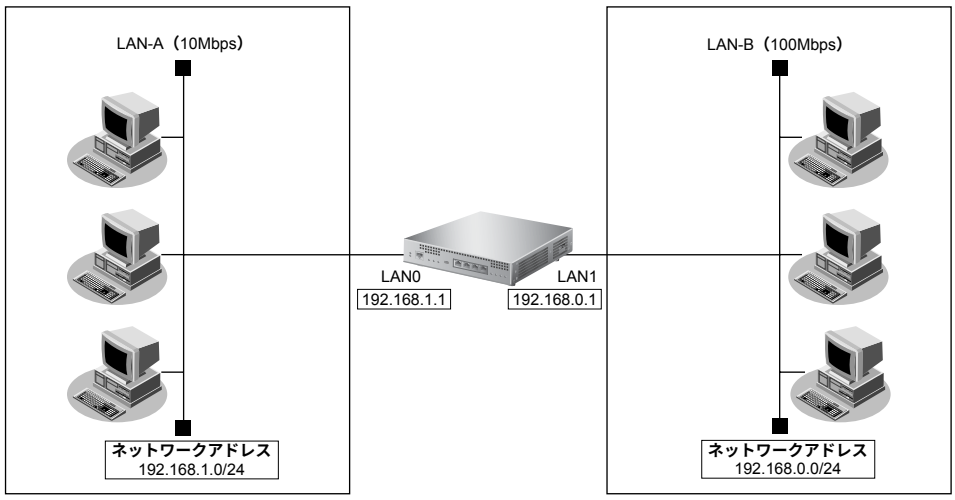
ネットワークへの接続台数が増加したり、同じネットワーク上に大量データを送受信するホストがあると、トラフィックが増加し、通信性能が劣化する場合があります。このような場合、ネットワークを分割することで、トラフィックを分散することができます。本装置は、2 つのネットワークインタフェースを持っているので、簡単にネットワークを接続したり分割したりすることができます。

ここでは、以下の条件で LAN-A と LAN-B をネットワーク間接続する場合を例に説明します。

本装置の IP アドレスを変更しない場合

本装置がご購入時の状態の場合、「かんたん設定」では以下の省略値が表示されます。［設定終了］ボタンをクリックして、設定を有効にすると通信することができます。

Si-R180、180B は、本装置の電源を投入するだけで通信することができます。ただし、インタフェースは、以下の図とは逆になります（LAN0→LAN1、LAN1→LAN0）。Si-R180、180B では、スイッチポートが有効になります。



● 設定条件

［LAN-A 側］

- 転送レートは自動認識
- IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

［LAN-B 側］

- 転送レートは自動認識
- IP アドレス　：192.168.0.1
- ネットワークアドレス/ネットマスク　：192.168.0.0/24

［その他の条件］

- パスワードを設定する
  パスワード　：himitu

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.4 パスワード情報を設定する」（P.12）

こんな事に気をつけて

パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。

1.　かんたん設定メニューで LAN 間接続の「セグメント接続／分割」をクリックします。

「セグメント接続／分割かんたん設定」ページが表示されます。

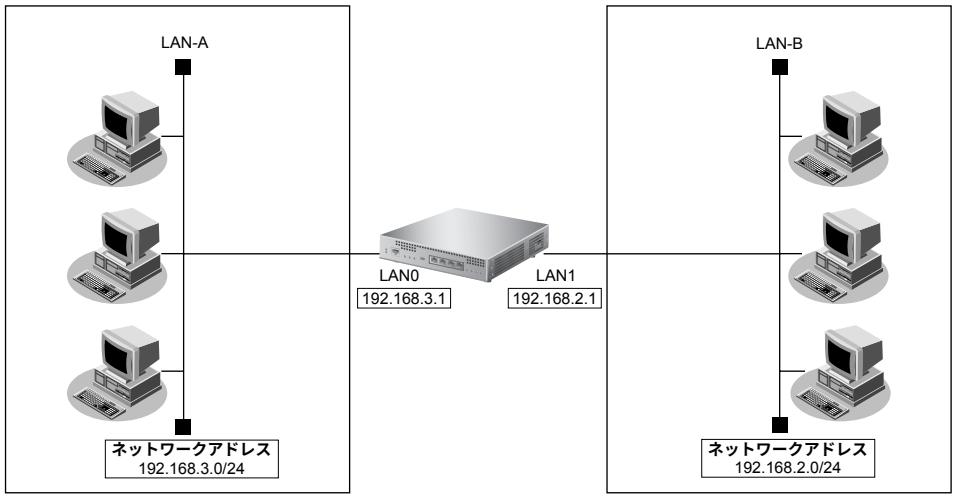
2.　［設定終了］ボタンをクリックします。

再起動後に通信できる状態となります。

本装置の IP アドレスを変更する場合

既存のネットワークどうしを接続／分割する場合は、それぞれのネットワーク環境に合わせた設定が必要です。「セグメント接続／分割」では、それぞれのネットワークのアドレスを設定できます。

以下に、LAN0 側のネットワークアドレスが 192.168.3.0/24、LAN1 側のネットワークアドレスが 192.168.2.0/24 を接続する設定方法を説明します。



こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

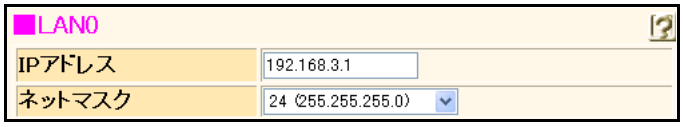
- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

1.　かんたん設定メニューで LAN 間接続の「セグメント接続／分割」をクリックします。

「セグメント接続／分割かんたん設定」ページが表示されます。

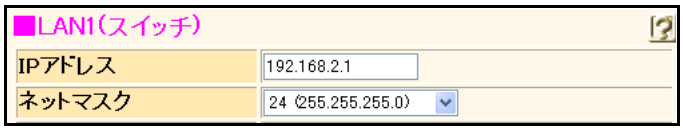
2.　「LAN0」で以下の項目を指定します。

- IP アドレス　→ 192.168.3.1
- ネットマスク　→ 24（255.255.255.0）



3.　「LAN1」で以下の項目を指定します。

- IP アドレス　→ 192.168.2.1
- ネットマスク　→ 24（255.255.255.0）



Si-R180、180B では、表示が上記の画面とは異なります。

4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に通信できる状態になります。

こんな事に気をつけて

本装置の IP アドレスを変更した場合、以下に示す 2 つの操作が必要です。

- **本装置に接続しているパソコンの IP アドレスも合わせて変更する必要があります。**
- **再起動後に本装置にアクセスするためには、URL で指定する IP アドレスに変更後の IP アドレスを指定する必要があります。**

ヒント

◆ 省略値について

セグメント接続／分割かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目		適用される省略値	かんたん設定での設定変更
LAN0	IP アドレス	192.168.1.1	○
	ネットマスク	24（255.255.255.0）	○
	セカンダリ IP アドレス	なし	×
	DHCP サーバ機能	使用しない	×
	NAT 機能	使用しない	×
	RIP 機能 ・RIP 送信 ・RIP 受信	 RIP-V1 を使用する RIP-V1 を使用する	×
	転送レート	自動認識	○
LAN1	IP アドレス	192.168.0.1	○
	ネットマスク	24（255.255.255.0）	○
	セカンダリ IP アドレス	なし	×
	DHCP サーバ機能	使用しない	×
	NAT 機能	使用しない	×
	RIP 機能 ・RIP 送信 ・RIP 受信	 RIP-V1 を使用する RIP-V1 を使用する	×
	転送レート	自動認識	○

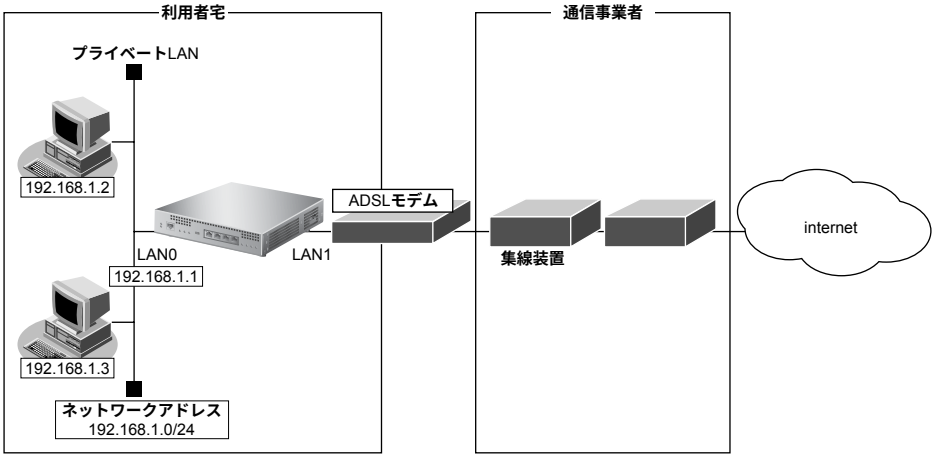
1.1.3　PPPoE 接続する

適用機種　***Si-R180,180B,220B,220C***

本装置は、通信事業者が提供する ADSL 回線で、PPPoE プロトコルを利用したインターネット接続サービスをプライベート LAN 上の複数のパソコンから利用できます。

PPPoE プロトコルは、ダイヤルアップ接続で使用する PPP プロトコルを Ethernet 上で使用するものです。

PPPoE 接続を使ってフレッツ・ADSL などのサービスを利用できます。具体的には、本装置の PPPoE で使用するインタフェースと ADSL モデムを接続し、プライベート LAN 上のパソコンからインターネット接続サービスを利用します。Si-R180、180B では、スイッチポートが有効になります。



● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

[その他の条件]

- パスワードを設定する
  パスワード　：himitu

この例の場合、本装置がご購入時の状態の場合、まず、かんたん設定でインターネットへの「PPPoE 接続」をクリックし、「PPPoE かんたん設定」画面でユーザ認証 ID とユーザ認証パスワードを入力します。次に、［設定終了］ボタンをクリックすると、通信できます（Si-R180、180B では購入時の状態の場合、インタフェースは、上の図とは逆になります（LAN0→LAN1、LAN1→LAN0）。）。

以下に、PPPoE 接続の設定方法を説明します。ただし、パスワードだけは、基本設定で設定する必要があります。

参照　Si-R シリーズ　Web ユーザーズガイド「1.4 パスワード情報を設定する」（P.12）

こんな事に気をつけて

- **パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。**
- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

☛ 参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

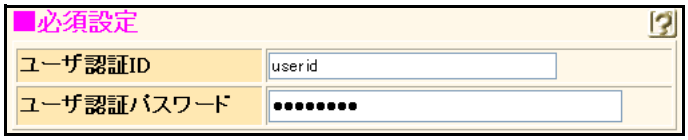
- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

1.　かんたん設定メニューでインターネットへの「PPPoE 接続」をクリックします。

「PPPoE かんたん設定」ページが表示されます。

2.　「必須設定」で以下の項目を指定します。

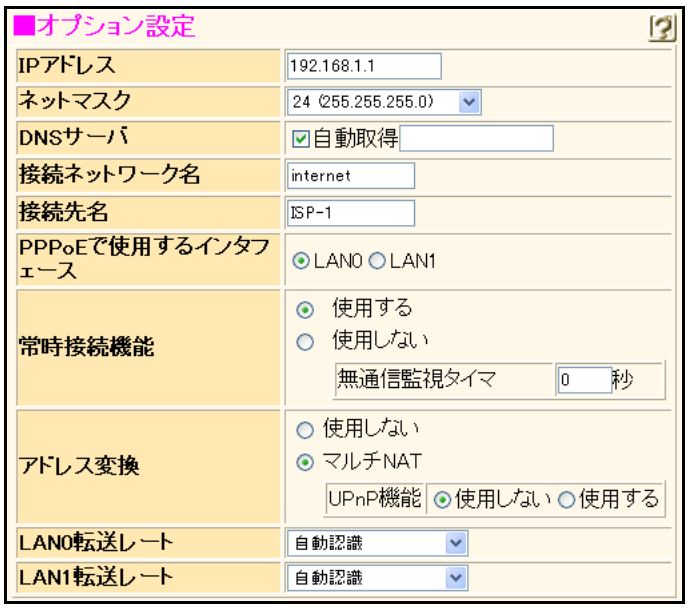
- ユーザ認証 ID　→ userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→ userpass（プロバイダから提示された内容）



3.　必要に応じて、「オプション設定」で以下の項目を指定します。

- IP アドレス　→ 192.168.1.1
- ネットマスク　→ 24（255.255.255.0）
- DNS サーバ　→ DNS サーバの IP アドレスが公開されていない場合、または DNS サーバアドレスの自動取得機能を利用する場合は“自動取得”をチェックします。ただし、自動取得はプロバイダが DNS 自動取得に対応している場合だけ使用できます。
- 接続ネットワーク名　→ internet（接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- 接続先名　→ ISP-1（プロバイダの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- PPPoE で使用するインタフェース　→ PPPoE で使用するインタフェースを選択します。Si-R180、180B では、LAN0（基本ポート 0）固定となります。
- 常時接続機能　→常時接続を行う場合は、“使用する”を選択します。
- アドレス変換　→ 1 つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスする場合は、“マルチ NAT”を選択します。

  UPnP 機能　→アドレス変換で“マルチ NAT”を選択した場合だけ設定します。UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合に“使用する”を選択します。
- LAN0 ／ 1 転送レート　→ポートの転送レートを選択します。“自動認識”を選択した場合、ネゴシエーションにより速度と全二重／半二重を自動決定します。Si-R180、180B では、LAN1（スイッチ）転送レートで選択した値は、スイッチポートで有効になります。



Si-R180、180B では、表示が上記の画面とは異なります。

4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

- フレッツ・ADSL とは、NTT が提供するサービスです。定額料金でインターネットが使えます。フレッツ・ADSL を使用する場合は、NTT との契約とフレッツ・ADSL に対応しているプロバイダとの契約が必要です。
  また、ユーザ認証 ID は「xxx@xxx.ne.jp」や「xxx@xxx.com」などの形式を使用しています。詳しくは、契約しているプロバイダに確認してください。
- プライベート LAN 上のパソコンに通信事業者が配布した PPPoE 接続ソフト（フレッツ・ADSL の場合フレッツ接続ツール）をインストールする必要はありません。
- ADSL 回線でのインターネット接続では、PPPoE だけでなく、DHCP や固定で IP アドレスを割り当てるものもあります。その場合は、「1.1.4 CATV インターネットに接続する」（P.23）を参照してください。また、通信事業者の指示に従ってください。
- 通信事業者によってはルータを用いた接続形態を認めていない事業者もあります。通信事業者の指示に従ってください。
- ご購入時は、LAN0 ポートからだけ設定できます。Si-R180、180B は LAN1 ポートから設定してください。
- 本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。
- 本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。
- PPPoE で使用するインタフェースを LAN0 側に変更した場合、LAN1 側の 10/100BASE-TX ポートからだけ設定できるように変更されます。

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	かんたん設定での設定変更
プライベート側 IP アドレス	192.168.1.1	○
ネットマスク	24（255.255.255.0）	○
DNS サーバアドレス	なし（自動取得）	○
自動接続	する	×
常時接続	使用する	○
無通信監視	しない	○
接続ネットワーク名	internet	○
接続先名	ISP-1	○
DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数 ・DNS サーバの IP アドレス	使用する 本装置のプライベート側 IP アドレス、ネットマスクから求めたネットワークアドレス +2 253 「自動取得（※ 1）」指定時は、本装置のプライベート側 IP アドレス	×
アドレス変換	マルチ NAT を使用 アドレス割り当てタイマ：5 分	○
UPnP 機能	使用しない	○
RIP 機能 ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（PPPoE 側） ・RIP 受信（PPPoE 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN 側 ・PPPoE 側	 なし デフォルトルートを設定する（メトリック値：1）	×
LAN0 転送レート	自動認識	○
LAN1 転送レート	自動認識	○
インタフェース	Si-R180、180B：LAN0、Si-R180、180B 以外：LAN1	○（※ 2）
ヘッダ圧縮	VJ-Compression：使用しない	×
MTU サイズ	1454	×
MSS 書き換え	使用する（1414 バイト）	×

※ 1）DNS サーバの IP アドレスを「自動取得」にした場合は、ProxyDNS 情報が以下のように設定されます。

「順引き情報一覧」

- 優先順位　：1
- ドメイン　：＊
  タイプ　：すべて
  送信元 IP アドレス／マスク　：any
- 動作　：接続先の DNS サーバへ問い合わせる
- ネットワーク名　：internet

「逆引き情報一覧」

- 優先順位　：1
- ネットワークアドレス　：any
- 動作　：接続先の DNS サーバへ問い合わせる
- ネットワーク名　：internet

※ 2）Si-R180、180B は変更できません。

1.1.4　CATV インターネットに接続する

適用機種　***Si-R180,180B,220B,220C***

CATV インターネット接続とは、CATV 事業者が提供するインターネット接続サービスです。CATV インターネット接続には、ケーブルモデム接続とダイヤルアップ接続の 2 つの接続形態があります。ケーブルモデム接続は、ケーブルテレビ網を利用したもので、CATV 事業者が提供するケーブルモデムに接続する形態です。ダイヤルアップ接続とは、CATV 電話サービスを利用したもので、パソコンにモデムを接続する形態です。本装置を使用して CATV インターネット接続する場合は、「ケーブルモデム接続」の形態となり、CATV 事業者との契約が必要です。接続にあたっては、CATV 事業者の指示に従ってください。

ヒント

◆ ケーブルモデムとは？

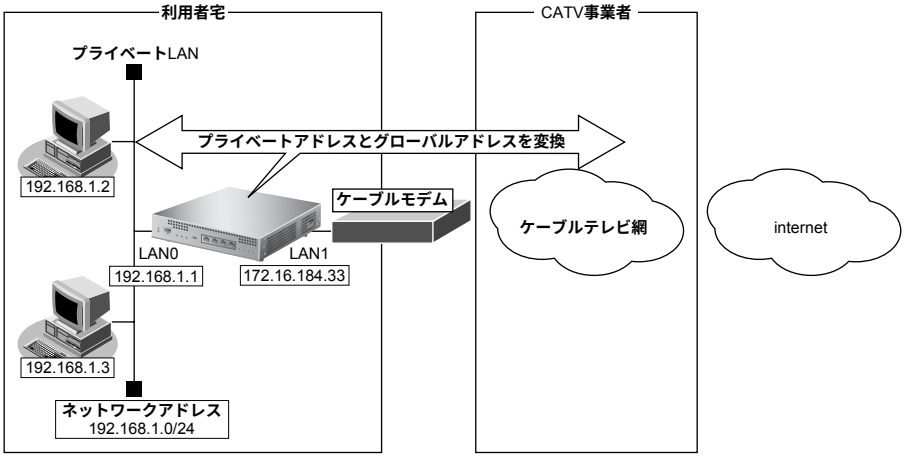
ケーブルテレビ網に接続するための専用モデムで、CATV インターネット接続サービスに必要な機器です。パソコン（LAN ボード）とは LAN ケーブルで接続します。通常、CATV サービス加入時に CATV 事業者より貸し出され、宅内工事の際に設置されます。

本装置を使った CATV インターネット接続は、CATV 事業者が提供するインターネット接続サービスをプライベート LAN 上の複数のパソコンから利用するための接続形態です。本装置と CATV 事業者が提供するケーブルモデムを接続することで、プライベート LAN 上のパソコンからインターネット接続サービスを利用できます。

本装置のアドレス変換機能が CATV 事業者側のネットワークと利用者側のプライベート LAN との間で動作し、プライベート LAN 側の IP アドレスを外部から隠すため、セキュリティが確保できます。

CATV インターネット接続は「プライベート LAN 構築かんたん設定」で設定します。

ただし、Si-R180、180B のインタフェースは、以下の図とは逆になります（LAN0 → LAN1、LAN1 → LAN0）。



● 設定条件

[CATV 事業者側]

- LAN1 ポートを使用する
- IP アドレス　：172.16.184.33
- ネットワークアドレス/ネットマスク　：172.16.184.0/24
- デフォルトルータ　：172.16.184.100
- DNS サーバ　：192.10.10.10

[プライベート LAN 側]

- IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- DHCP サーバ機能を使用する

こんな事に気をつけて

- **契約した CATV 事業者によって設定方法が異なります。実際の設定は、CATV 事業者の指示に従ってください。**
- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

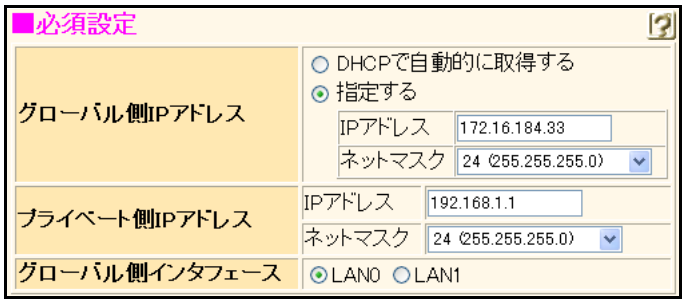
- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

1.　かんたん設定メニューで LAN 間接続の「プライベート LAN 構築」をクリックします。

「プライベート LAN 構築かんたん設定」ページが表示されます。

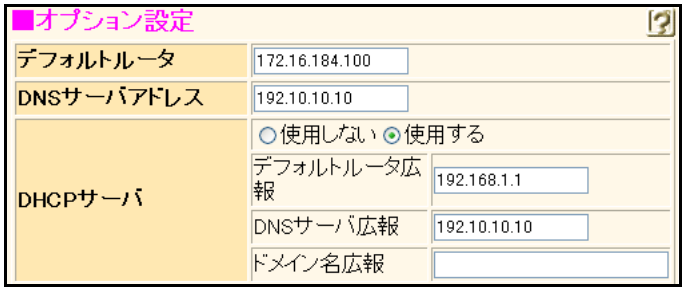
2.　「必須設定」で以下の項目を指定します。

- グローバル側 IP アドレス　→指定する
  IP アドレス　→172.16.184.33
  ネットマスク　→24（255.255.255.0）
- プライベート側 IP アドレス
  IP アドレス　→192.168.1.1
  ネットマスク　→24（255.255.255.0）
- グローバル側インタフェース　→LAN0



3.　「オプション設定」で以下の項目を指定します。

- デフォルトルータ　→172.16.184.100
- DNS サーバアドレス　→192.10.10.10
- DHCP サーバ　→使用する
  デフォルトルータ広報　→192.168.1.1
  DNS サーバ広報　→192.10.10.10



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

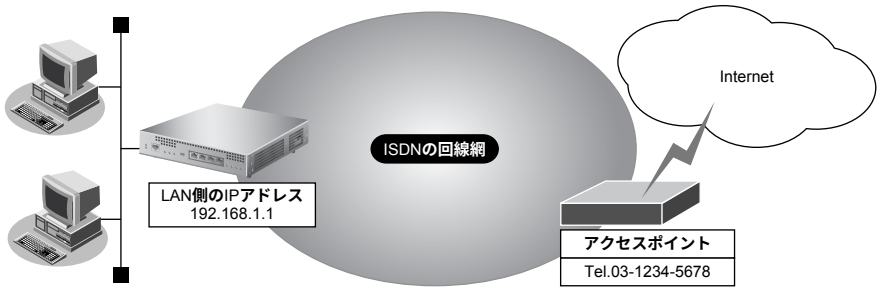
1.1.5　インターネットへ ISDN 接続する

適用機種　***Si-R220B,220C***

インターネットへ ISDN 接続するときは、「かんたん設定」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- 本装置の IP アドレスと LAN 側のネットマスクの変更
- DNS サーバの設定
- 同一プロバイダのアクセスポイントを複数指定（マルチダイヤル）
- ISDN 回線を自動切断するまでの時間の変更（無通信監視タイマ）
- 回線の切断タイミングの調整（課金単位時間）
- 接続ネットワーク名と接続先名の設定
- データの転送速度を早くする（MP-Multilink PPP）
- むだな通信料金の抑止（かんたんフィルタ）

ここでは、以下の条件でインターネットへ ISDN 接続する場合を例に説明します。



● 設定条件

- 端末型ダイヤルアップ接続を行う
- 新規に LAN を構築する
- 接続先の電話番号　：03-1234-5678
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。**
- **本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。**

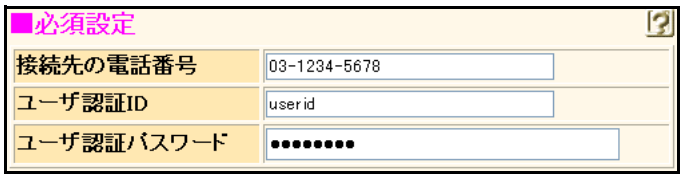
1.　かんたん設定メニューでインターネットへの「ISDN 接続」をクリックします。

「インターネットへ ISDN 接続かんたん設定」ページが表示されます。

補足 かんたんメニューは、本装置のトップページで画面上部の「トップ」アイコンをクリックして表示させることができます。

2.　「必須設定」で以下の項目を指定します。

- 接続先の電話番号　→ 03-1234-5678（プロバイダから提示された内容）
- ユーザ認証 ID　→ userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→ userpass（プロバイダから提示された内容）



3.　必要に応じて、「オプション設定」で以下の項目を指定します。

- IP アドレス　→ 192.168.1.1
- ネットマスク　→ 24（255.255.255.0）
- DNS サーバ　→ DNS サーバの IP アドレスが公開されていない場合、または DNS サーバアドレスの自動取得機能を利用する場合は“自動取得”をチェックします。ただし、自動取得はプロバイダが DNS 自動取得に対応している場合だけ使用できます。
- 接続先の電話番号 2　→ プロバイダのほかのアクセスポイントの電話番号 2
- 接続先の電話番号 3　→ プロバイダのほかのアクセスポイントの電話番号 3

補足 「接続先の電話番号 2」、「接続先の電話番号 3」は、マルチダイヤル機能を利用する場合に設定します。

- 常時接続機能　→ 初期値は“使用しない”。
- 無通信監視タイマ　→ 初期値は 60 秒。必要に応じて変更します（0 ～ 3600 秒）。

補足 0 を指定した場合、回線の自動切断は行いません。

- 課金単位時間　→ 初期値は 0 秒。必要に応じて変更します（0 ～ 3600 秒）。

補足 接続先までの課金単位に合わせて指定します。なお、0 を設定した場合、課金単位の調整は行いません。たとえば、接続先までの電話料金が 3 分 10 円の場合、180 秒をお勧めします。

- 接続ネットワーク名　→ internet（接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- 接続先名　→ ISP-1（プロバイダの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。）
- アドレス変換　→ 1 つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスする場合は、“マルチ NAT”を選択します。

  UPnP 機能　→ アドレス変換で“マルチ NAT”を選択した場合だけ設定します。UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合に“使用する”を選択します。

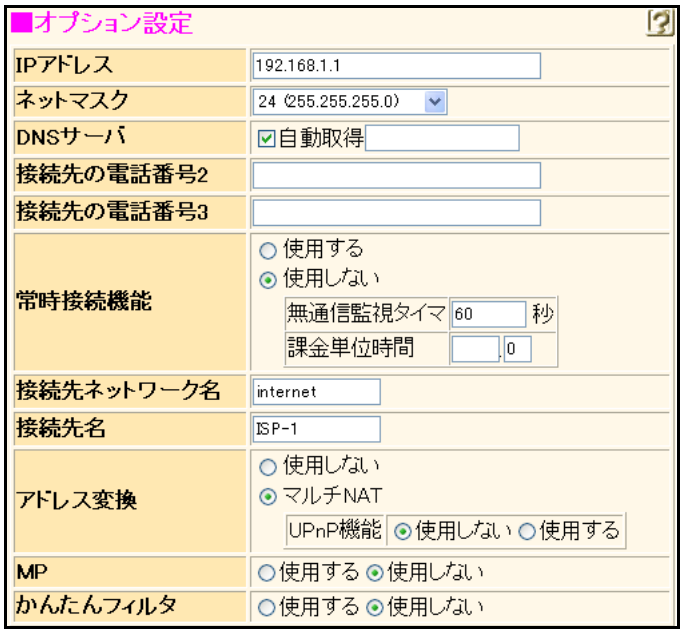
- MP　→初期値は“使用しない”。プロバイダが MP をサポートしていて、MP を使用する場合は“使用する”を選択します。通信量が多くなった場合に自動的に MP を使用します。

こんな事に気をつけて

接続先のプロバイダが MP に対応していない場合は、MP では通信できません。

- かんたんフィルタ　→初期値は“使用しない”。

補足 Windows® 環境でネットワークを構成している場合は、むだな課金が発生する場合があるため、「かんたんフィルタ」で“使用する”を選択することをお勧めします。



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

⚠注意

本装置は、10BASE-T ポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、または LAN の利用条件によって、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

1.　WWW ブラウザで URL「http://www.fujitsu.com」を入力します。

インターネットに接続できた場合は、弊社のページが表示されます。

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
すべてのデータ通信の着信	許可しない	×
常時接続機能	使用しない	○
無通信監視タイマ	60 秒	○
課金単位時間	なし	○
接続ネットワーク名	internet	○
接続先名	ISP-1	○
接続先のサブアドレス	なし	×
DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数 ・DNS サーバの IP アドレス	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋2 64 「自動取得（※ 1）」指定時は、本装置の IP アドレス	×
アドレス変換	マルチ NAT を使用 アドレス割り当てタイマ：5 分	○
UPnP 機能	使用しない	○
MP 機能（※ 2）	使用しない	○
かんたんフィルタ（※ 3）	使用する	○
RIP 機能 ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN 側 ・WAN 側	 なし デフォルトルートを設定する（メトリック値：1）	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression：使用する IP ヘッダ圧縮：使用しない	×
IPv6 経路	使用しない	×
ブリッジ	使用しない	×
課金制御	上限　3,000 円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

※ 1）DNS サーバの IP アドレスを「自動取得」にした場合は、ProxyDNS 情報が以下のように設定されます。

「順引き情報一覧」

- 優先順位　：1
- ドメイン　：＊
  タイプ　：すべて
  送信元 IP アドレス／マスク　：any
- 動作　：接続先の DNS サーバへ問い合わせる
- ネットワーク名　：internet

「逆引き情報一覧」

- 優先順位　：1
- ネットワークアドレス　：any
- 動作　：接続先の DNS サーバへ問い合わせる
- ネットワーク名　：internet

※ 2）MP 機能を「使用する（自動）」にした場合は、以下のように設定されます。

- トラフィックによる増減　：する
- 回線増加条件　：回線使用率（90%）、猶予時間（10 秒）
- 回線削除条件　：回線使用率（40%）、猶予時間（60 秒）

※ 3）かんたんフィルタを「使用する」にした場合は、以下のように設定されます。

- トラフィックによる増減　：する
- Windows® 95 ／ 98 ／ Me ／ 2000、Windows NT® で Microsoft Network を使用する場合に、NetBIOS over TCP が使用する TCP および UDP のサービスポート 137 から 139 を遮断するフィルタを設定します。
- ping（ICMP echo）や syslog、time、SNTP で使用するプロトコルを抑止するフィルタを設定します。なお、回線が接続状態の場合はそれぞれのパケットを通過させます。
- Windows® 2000 から本装置を経由してインターネットへ接続する場合、Windows® 2000 が送信する予期しない DNS パケットによって自動発信してしまう場合があります。この問題を回避するために、ProxyDNS 情報に問い合わせタイプが SOA（6）、SRV（33）の DNS パケットを破棄するフィルタ、およびホストデータベース情報に IP アドレス「127.0.0.1」でホスト名「localhost」の情報を設定します。

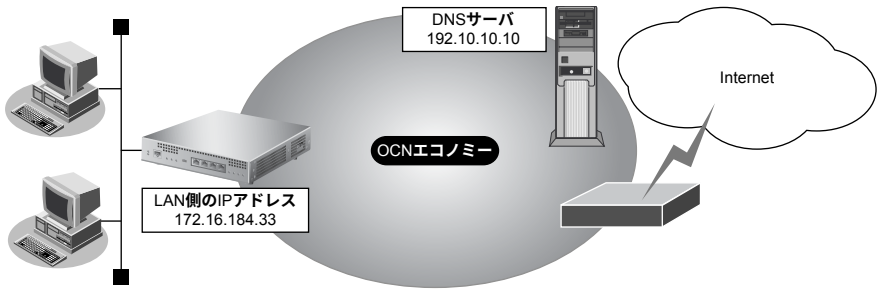
1.1.6　インターネットへ専用線接続する

適用機種　*Si-R220B,220C*

インターネットへ専用線接続するときは、「かんたん設定」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- 接続ネットワーク名称の設定
- 契約時に指示されたドメイン名の設定
- アドレス変換の設定

ここでは、以下の条件でOCNエコノミーを利用する場合を例に説明します。



● 設定条件

- OCN エコノミー専用線（128Kbps）を使用する
- 新規に LAN を構築する
- OCN 側の DNS サーバを使用　：192.10.10.10
- OCN より提示されたドメイン名　：domain.ocn.ne.jp
- 接続するパソコンの台数は OCN より割り当てられた IP アドレスよりも少ない
- 割り当て IP アドレス
  ネットワークアドレス　：172.16.184.32/29
  本装置の IP アドレス　：172.16.184.33
  ホストアドレス　：172.16.184.34 ～ 172.16.184.38
  ブロードキャストアドレス　：172.16.184.39

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  ☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

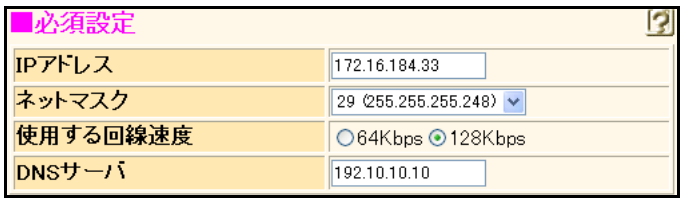
- **本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。**
- **本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。**
- **本装置の IP アドレスにネットワークアドレス、またはブロードキャストアドレスを指定しないでください。**

1.　かんたん設定メニューでインターネットへの「専用線接続」をクリックします。

「インターネットへ専用線接続かんたん設定」ページが表示されます。

2.　「必須設定」で以下の項目を指定します。

- IP アドレス　→ 172.16.184.33（割り当てられたホストアドレスの先頭）
- ネットマスク　→ 29（255.255.255.248）
- 使用する回線速度　→ 128Kbps
- DNS サーバ　→ 192.10.10.10（OCN から提示された IP アドレス）

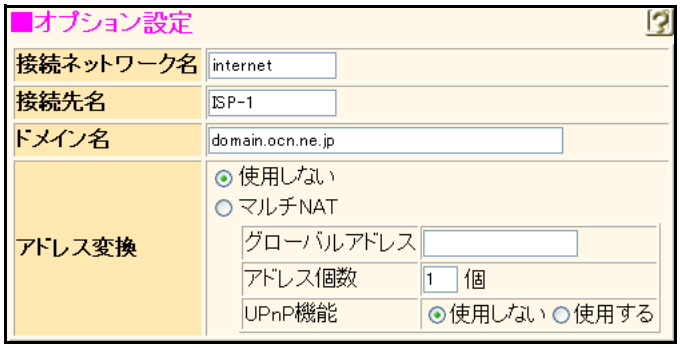


3.　必要に応じて、「オプション設定」で以下の項目を指定します。

- 接続ネットワーク名　→ internet（接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- ドメイン名　→ domain.ocn.ne.jp（OCN より提示されたドメイン名）
- アドレス変換　→初期値は“使用しない”。
  アドレス個数　→アドレス変換で“マルチ NAT”を指定した場合は、グローバルアドレスの個数を指定します。

補足　この例のように割り当てられた IP アドレスよりも接続するパソコンの台数が同数または少ない場合、“使用しない”を選択します。割り当てられた IP アドレスより接続するパソコンの台数が多い場合は、“マルチ NAT”を選択すると、すべてのパソコンがインターネットを利用できます。その際は、「グローバルアドレス」と「アドレス個数」を設定します。

UPnP 機能　→ UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は“使用する”を選択します。



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

ヒント

◆ OCN エコノミーなら「マルチ NAT」機能が便利

OCN エコノミーの契約時に割り当てられた IP アドレスの個数より、パソコンの台数が多い場合は、本装置の「マルチ NAT 機能」が便利です。「マルチ NAT 機能」によって、実際に割り当てられた IP アドレスの数を上回る台数の LAN 上のパソコンでインターネットを利用できるようになります。

◆ マルチ NAT

本装置では、インターネットを利用する際に、プロバイダより割り当てられた IP アドレス（グローバルアドレス）と、ネットワーク上で設定した IP アドレス（プライベートアドレス）を対応付けることによって、従来のネットワークの設定を変更することなくインターネット接続ができるアドレス変換（NAT）機能をサポートしています。

NAT 機能は、プライベートアドレスとグローバルアドレスを 1 対 1 に対応付けるもので、NAT 機能を介して通信できるパソコンの台数は割り当てられる IP アドレスと同じになります。このため、プロバイダと端末型ダイヤルアップ契約の場合、1 つしか IP アドレスが割り当てられないので、同時接続台数が 1 台に制限されます。

マルチ NAT は、この問題を解決するために 1 対 1 の対応付けから、多対 1 の対応付けを実現した機能です。IP アドレスとポート番号を組み合わせた IP 情報の割り当てを行うことによって、プライベートアドレスとグローバルアドレスとを多対 1 に対応付け、同時に複数のパソコンからの利用が可能となります。

参照 「2.16 マルチ NAT 機能（アドレス変換機能）を使う」（P.715）

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

1. **WWW ブラウザで URL「http://www.fujitsu.com」を入力します。**

インターネットに接続できた場合は、弊社のページが表示されます。

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
ブロードキャストアドレス	ネットワークドレス＋オール 1	×
接続ネットワーク名	internet	○
DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋2 64	×
NAT 機能	使用しない（※ 1）	○
UPnP 機能	使用しない	○
かんたんフィルタ	使用しない	×
RIP 機能 ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN 側 ・WAN 側	 なし デフォルトルートを設定する（メトリック値：1）	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression：使用する IP ヘッダ圧縮：使用しない	×
IPv6 経路	使用しない	×
ブリッジ	使用しない	×

※ 1）マルチ NAT 使用時のアドレス割り当てタイマは 5 分を設定します。

1.1.7　オフィスへISDN接続する

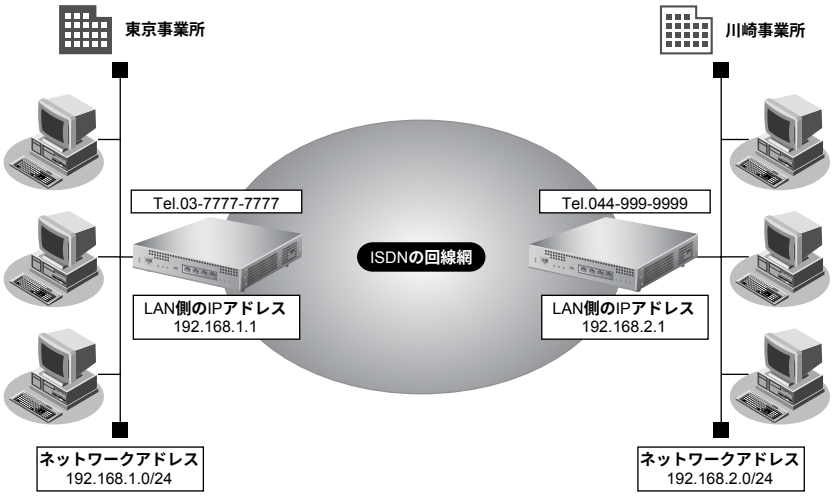
適用機種　*Si-R220B,220C*

事業所 LAN どうしを ISDN で接続するときは、「かんたん設定メニュー」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- DHCP サーバ機能の設定
- ISDN 回線を自動切断するまでの時間の変更（無通信監視タイマ）
- 回線の切断タイミングの調整（課金単位時間）
- 接続ネットワーク名と接続先名の設定
- データの転送速度を早くする（MP-Multilink PPP）
- 送受信するヘッダの圧縮

ここでは、ISDN 回線を介して 2 つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。

補足　「詳細設定」で設定する場合や基幹ネットワーク（大規模ネットワーク）に接続する場合は、「1.9 事業所 LAN を ISDN で接続する」（P.97）を参照してください。



● 設定条件

- DHCP サーバ機能は使用しない

[東京事業所]

- 電話番号　：03-7777-7777
- ユーザ認証 ID とユーザ認証パスワード
  - 発信　：tokyo、tokyopass
  - 着信　：kawasaki、kawapass
- LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24（本装置の IP アドレス：192.168.1.1）

[川崎事業所]

- 電話番号　：044-999-9999
- ユーザ認証 ID とユーザ認証パスワード
  - 発信　：kawasaki、kawapass
  - 着信　：tokyo、tokyopass
- LAN 側のネットワークアドレス／ネットマスク　：192.168.2.0/24（本装置の IP アドレス：192.168.2.1）

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。**
- **本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。**

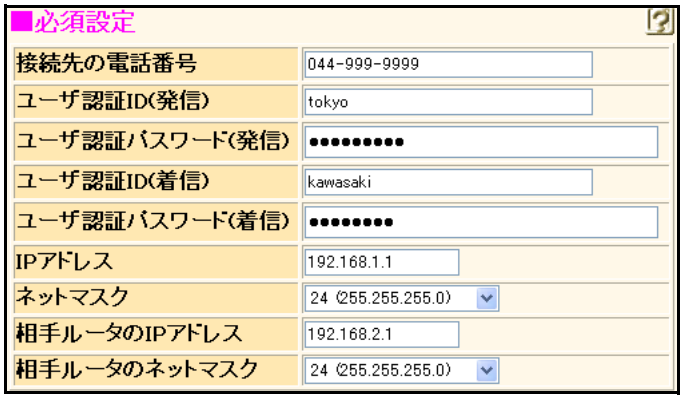
東京事業所の本装置を設定する

1. かんたん設定でオフィスへの「ISDN 接続」をクリックします。

「オフィスへ ISDN 接続かんたん設定」ページが表示されます。

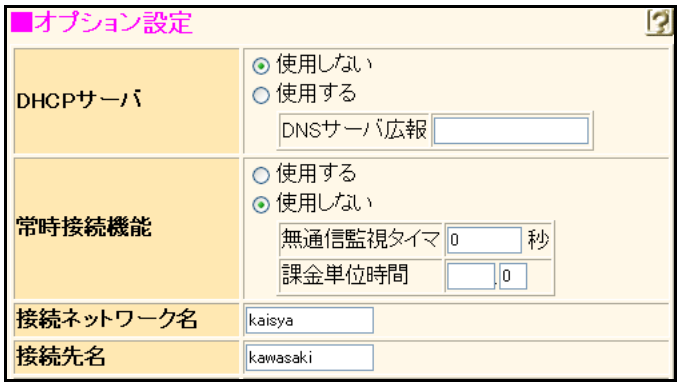
2. 「必須設定」で以下の項目を指定します。

- 接続先の電話番号　→ 044-999-9999
- ユーザ認証 ID（発信）　→ tokyo
- ユーザ認証パスワード（発信）　→ tokyopass
- ユーザ認証 ID（着信）　→ kawasaki
- ユーザ認証パスワード（着信）　→ kawapass
- IP アドレス　→ 192.168.1.1（既存の LAN につなぐときは適宜変更）
- ネットマスク　→ 24（255.255.255.0）（既存の LAN につなぐときは適宜変更）
- 相手ルータの IP アドレス　→ 192.168.2.1（接続先となる本装置のネットワークアドレス）
- 相手ルータのネットマスク　→ 24（255.255.255.0）（接続先となる本装置のネットマスク）



3.　「オプション設定」で以下の項目を指定します。

- DHCP サーバ　→使用しない
- 接続ネットワーク名　→kaisya（接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- 接続先名　→kawasaki（接続先の名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。）



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

川崎事業所の本装置を設定する

「東京事業所の本装置を設定する」を参考に、川崎事業所の本装置を設定します。その際、特に指定のないものは、東京事業所と同じ設定にします。

補足　設定が終わったら、［設定終了］ボタンをクリックします。

「必須設定」

- 接続先の電話番号　→03-7777-7777
- ユーザ認証 ID（発信）　→kawasaki
- ユーザ認証パスワード（発信）　→kawapass
- ユーザ認証 ID（着信）　→tokyo
- ユーザ認証パスワード（着信）　→tokyopass
- IP アドレス　→192.168.2.1（本装置の LAN 側の IP アドレス）
- ネットマスク　→24（255.255.255.0）
- 相手ルータの IP アドレス　→192.168.1.1（接続先となる本装置のネットワークアドレス）
- 相手ルータのネットマスク　→24（255.255.255.0）（接続先となる本装置のネットマスク）

「オプション設定」

- 接続ネットワーク名　→kaisya（接続するネットワークの名称）
- 接続先名　→tokyo

通信する

WWW ブラウザや電子メールソフトなどの通信用アプリケーションを起動しておきます。通信が必要な状態になると、本装置が自動的に回線を接続します。

⚠注意

本装置は、10BASE-T ポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、または LAN の利用条件により、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。本装置の表示メニューで、課金情報を定期的にチェックしてください。

補足 「かんたん設定」で設定した初期設定の状態では、約 60 秒間データの送受信が行われない場合、自動的に回線を切断します。

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
サブアドレス	なし	×
不特定相手着信	許可しない	×
常時接続機能	使用しない	○
無通信監視タイマ	60 秒	○
課金単位時間	なし	○
接続ネットワーク名	localnet	○
接続先名	OFFICE-1	○
該当接続先への着信許可	許可する	×
DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス＋2 64	○
NAT 機能	使用しない	×
MP 機能	使用しない	○
かんたんフィルタ	使用しない	×
RIP 機能 ・RIP 送信（LAN 側） ・RIP 受信（LAN 側） ・RIP 送信（WAN 側） ・RIP 受信（WAN 側）	 送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN 側 ・WAN 側	 なし 相手ルータの IP アドレス、ネットマスクを元にスタティックルートを設定する	×
データ圧縮	LZS：なし	○
ヘッダ圧縮	VJ-Compression：使用する IP ヘッダ圧縮：使用しない	○
IPv6 経路	使用しない	×
ブリッジ	使用しない	×
課金制御	上限　3,000 円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

1.1.8　オフィスへ専用線接続する

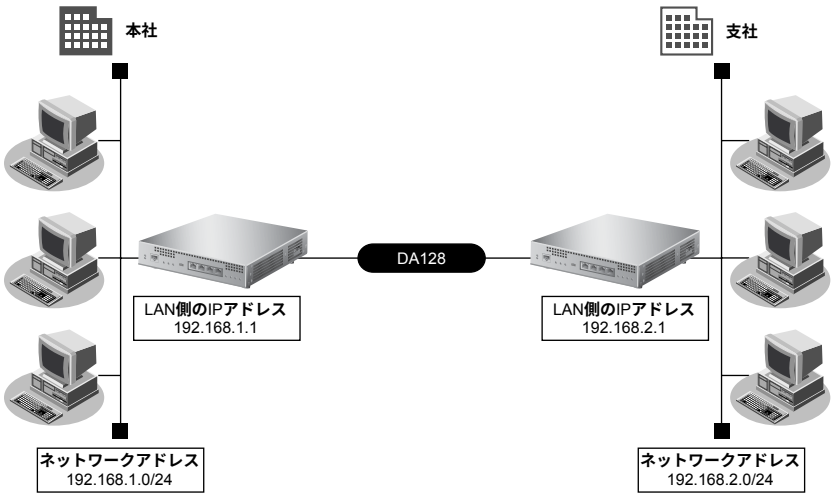
適用機種　***Si-R220B,220C***

事業所 LAN どうしを専用線で接続するときは、「かんたん設定メニュー」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- 接続ネットワーク名の設定
- DHCP サーバ機能の設定
- 送受信するヘッダの圧縮

ここでは、専用線（HSD128Kbps）を介して 2 つの事業所（本社、支社）のネットワークを接続する場合を例に説明します。

補足　「詳細設定」で設定する場合や基幹ネットワーク（大規模ネットワーク）に接続する場合は、「1.10 事業所 LAN を専用線で接続する」（P.103）を参照してください。



● 設定条件

[本社]

- 専用線（128Kbps）を使用する
- DHCP サーバ機能は使用しない
- アドレス変換は使用しない
- LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本装置の IP アドレス　：192.168.1.1

[支社]

- LAN 側のネットワークアドレス／ネットマスク　：192.168.2.0/24
- 本装置の IP アドレス　：192.168.2.1

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。**
- **本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。**

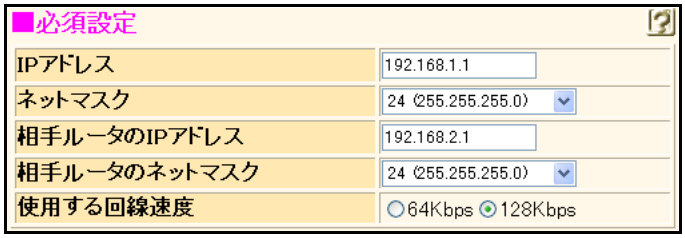
本社の本装置を設定する

1.　かんたん設定でオフィスへの「専用線接続」をクリックします。

「オフィスへ専用線接続かんたん設定」ページが表示されます。

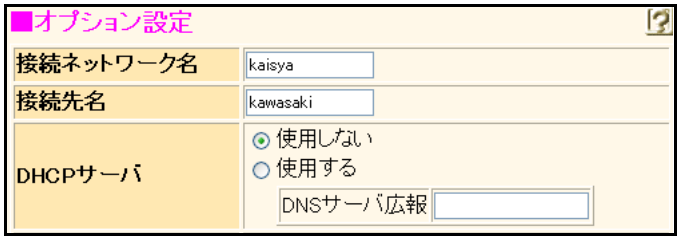
2.　「必須設定」で以下の項目を指定します。

- IP アドレス　→ 192.168.1.1（既存の LAN につなぐときは適宜変更）
- ネットマスク　→ 24（255.255.255.0）（既存の LAN につなぐときは適宜変更）
- 相手ルータの IP アドレス　→ 192.168.2.1（接続先となる本装置の IP アドレス）
- 相手ルータのネットマスク　→ 24（255.255.255.0）（接続先となる本装置のネットマスク）
- 使用する回線速度　→ 128Kbps



3.　「オプション設定」で以下の項目を指定します。

- 接続ネットワーク名　→ kaisya（接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- DHCP サーバ　→使用しない



4.　設定が終了したら、［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

支社の本装置を設定する

「本社の本装置を設定する」を参考に、支社の本装置を設定します。その際、特に指定のないものは、本社と同じ設定にします。

補足 設定が終わったら、［設定終了］ボタンをクリックします。

「必須設定」

- IPアドレス　→192.168.2.1（本装置のLAN側のIPアドレス）
- ネットマスク　→24（255.255.255.0）
- 相手ルータのIPアドレス　→192.168.1.1（接続先となる本装置のIPアドレス）
- 相手ルータのネットマスク　→24（255.255.255.0）（接続先となる本装置のネットマスク）
- 使用する回線速度　→128Kbps

「オプション設定」

- 接続ネットワーク名　→kaisya（接続するネットワークの名称）
- DHCPサーバ　→使用しない

ヒント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
接続ネットワーク名	localnet	○
DHCPサーバ機能 ・割り当て先頭アドレス ・割り当てアドレス数	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス＋2 64	○
NAT機能	使用しない	×
かんたんフィルタ	使用しない	×
RIP機能 ・RIP送信（LAN側） ・RIP受信（LAN側） ・RIP送信（WAN側） ・RIP受信（WAN側）	 送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN側 ・WAN側	 なし 相手ルータのIPアドレス、ネットマスクを元にスタティックルートを設定する	×
データ圧縮	LZS：なし	○
ヘッダ圧縮	VJ-Compression：使用する IPヘッダ圧縮：使用しない	○
IPv6経路	使用しない	×
ブリッジ	使用しない	×

1.2　LAN をネットワーク間接続する

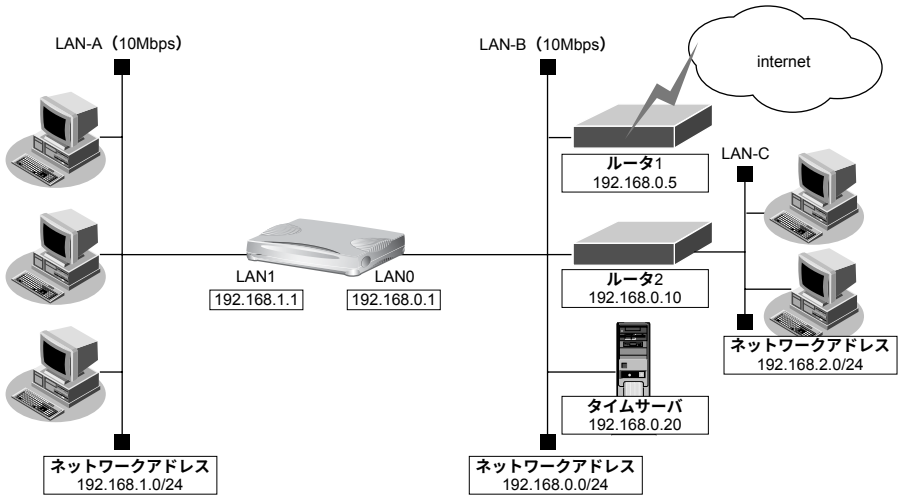
適用機種　全機種

ここでは、既存の LAN-B に新規の LAN-A をネットワーク間接続し、静的に経路情報を設定する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

[LAN-A 側]

- 転送レートは自動認識
- 本装置の LAN1 側の IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- DHCP 機能を使用する
- NAT を使用しない

[LAN-B 側]

- 転送レートは自動認識
- 本装置の LAN0 側の IP アドレス　：192.168.0.1
- ネットワークアドレス/ネットマスク　：192.168.0.0/24
- DHCP 機能を使用しない
- ルーティングプロトコルとして RIP-V1 を使用する
- インターネットにつながるルータ 1 と、事業所内のその他のネットワークにつながるルータ 2 が存在し、静的に経路情報を登録する
  ルータ 1 の IP アドレス　：192.168.0.5
  ルータ 2 の IP アドレス　：192.168.0.10
- LAN-C のネットワークアドレス/ネットマスク　：192.168.2.0/24
- NAT は使用しない

[その他の条件]

- 自動時刻設定にする

タイムサーバ	：使用する
サーバ設定	：設定する
プロトコル	：TIME プロトコル
タイムサーバのアドレス	：192.168.0.20

ヒント

◆ TIME プロトコル、SNTP とは？

TIME プロトコル（RFC868）はネットワーク上で時刻情報を配付するプロトコルです。SNTP（Simple Network Time Protocol、RFC1361、RFC1769）は NTP（Network Time Protocol）のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。

こんな事に気をつけて

本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。Si-R180、180B 以外の機種で「LAN1 情報を設定する」場合は、あらかじめ物理 LAN1 定義を追加する必要があります。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

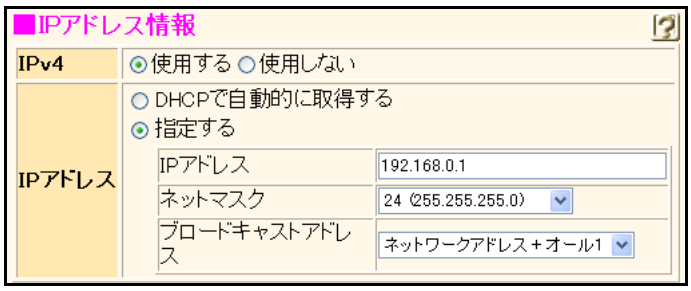
3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する

IP アドレス	→192.168.0.1
ネットマスク	→24（255.255.255.0）
ブロードキャストアドレス	→ネットワークアドレス＋オール 1



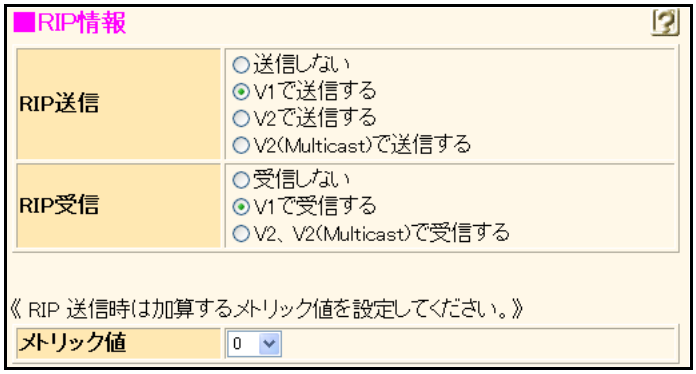
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP送信　→V1 で送信する
- RIP受信　→V1 で受信する
- メトリック値　→0



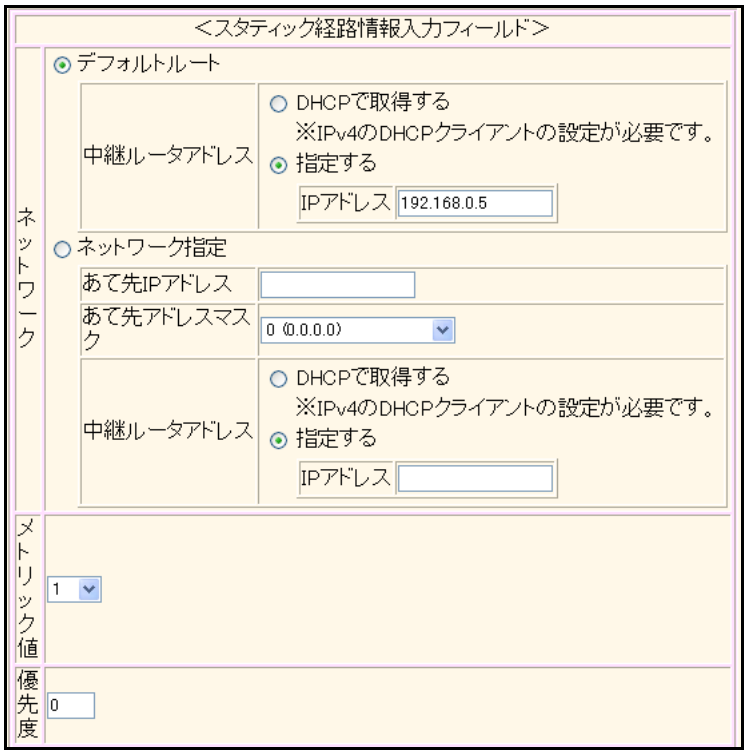
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

10.　以下の項目を指定します。

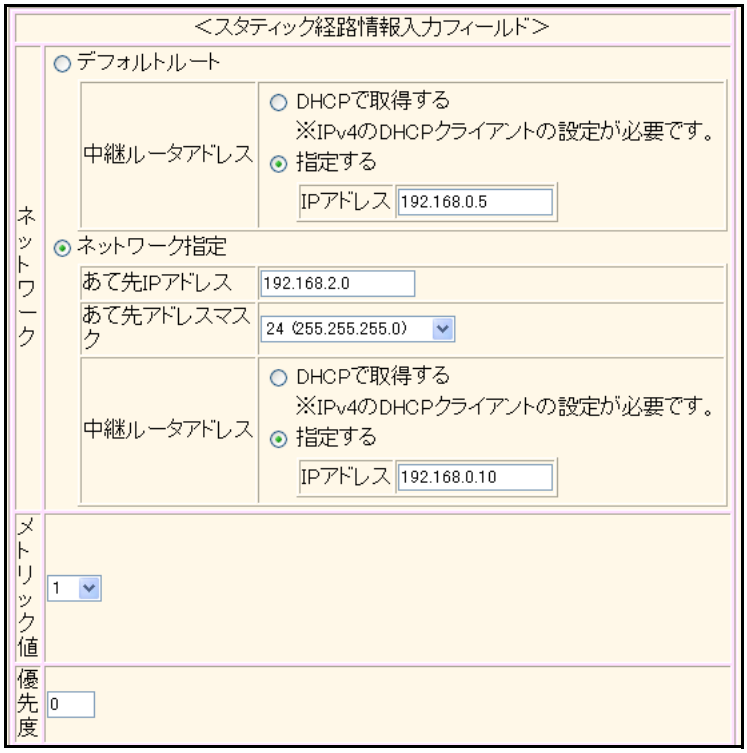
- ネットワーク　→デフォルトルート
  中継ルータアドレス　→指定する
  IPアドレス　→192.168.0.5
- メトリック値　→1
- 優先度　→0



11.　［追加］ボタンをクリックします。

12.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→指定する
  IP アドレス　→ 192.168.0.10
- メトリック値　→ 1
- 優先度　→ 0



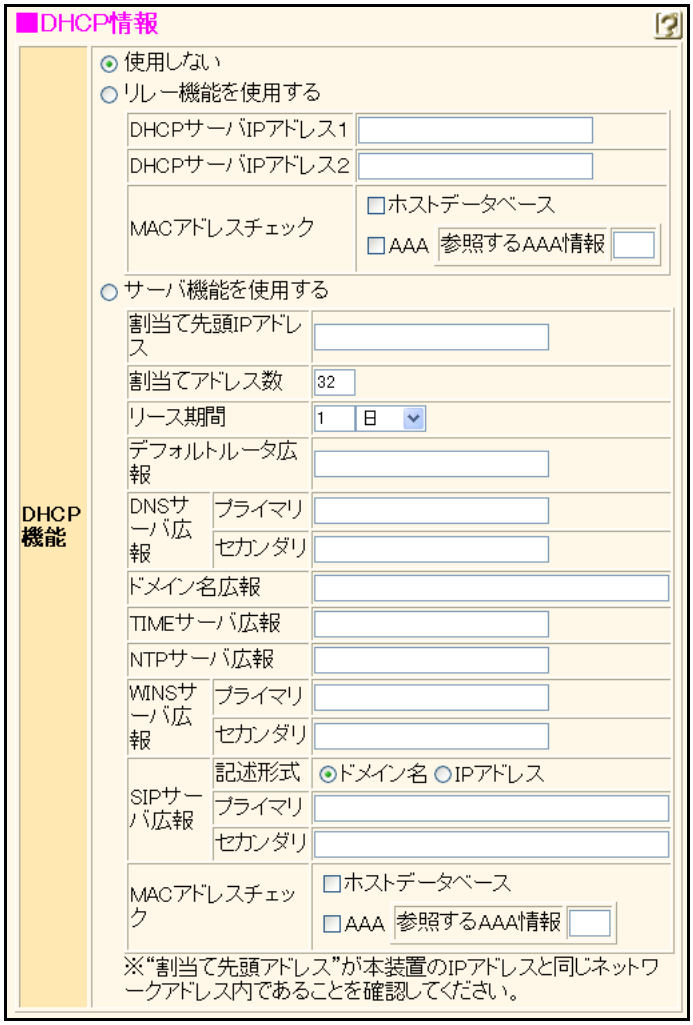
13.　［追加］ボタンをクリックします。

14.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

15.　以下の項目を指定します。

- DHCP 機能　　→使用しない



16.　［保存］ボタンをクリックします。

LAN1 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

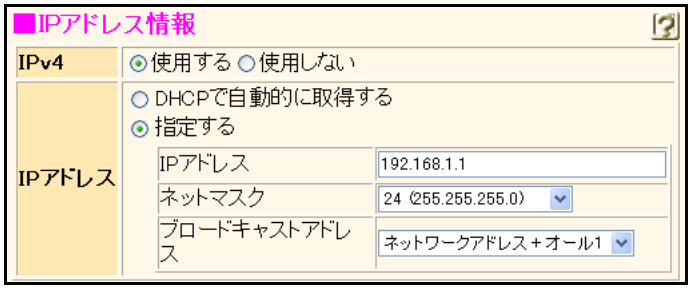
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



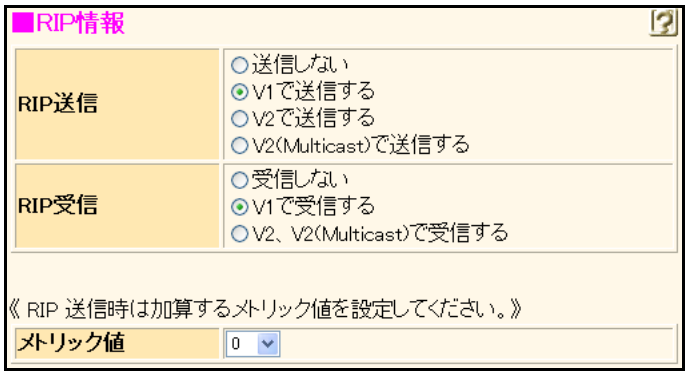
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→ V1 で送信する
- RIP 受信　→ V1 で受信する
- メトリック値　→ 0



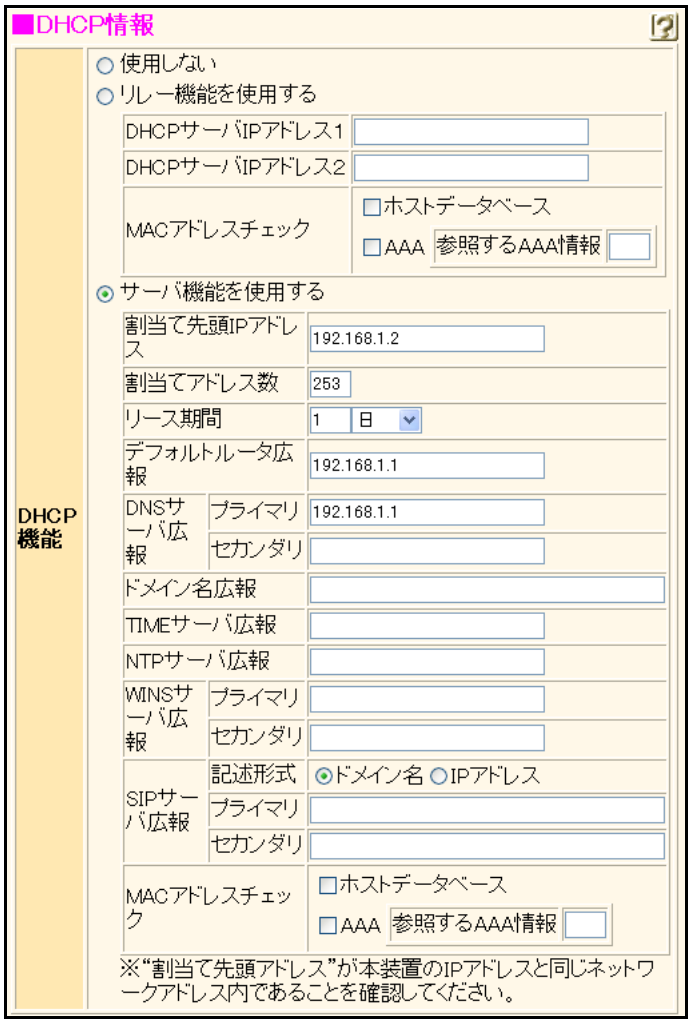
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

10.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.1.2
  割当てアドレス数　→ 253
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.1.1
  DNS サーバ広報
  プライマリ　→ 192.168.1.1
  セカンダリ　→指定しない
  ドメイン名広報　→指定しない
  TIME サーバ広報　→指定しない
  NTP サーバ広報　→指定しない
  WINS サーバ広報　→指定しない
  SIP サーバ広報　→指定しない
  MAC アドレスチェック　→指定しない



11.　［保存］ボタンをクリックします。

自動時刻を設定する

1.　設定メニューの基本設定で「装置情報」をクリックします。

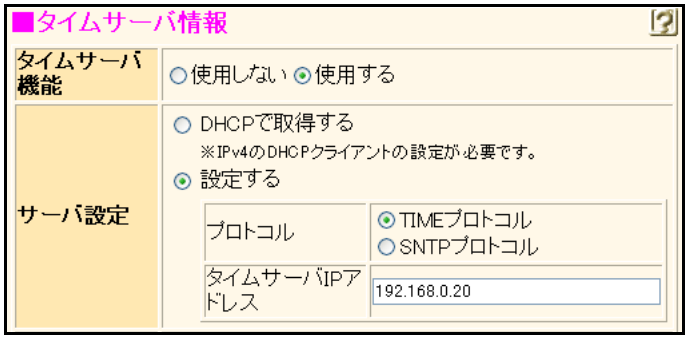
「装置情報」ページが表示されます。

2.　「タイムサーバ情報」をクリックします。

「タイムサーバ情報」が表示されます。

3.　以下の項目を指定します。

- タイムサーバ機能　→使用する
- サーバ設定　→設定する
  プロトコル　→TIME プロトコル
  タイムサーバ IP アドレス　→192.168.0.20



4.　［保存］ボタンをクリックします。

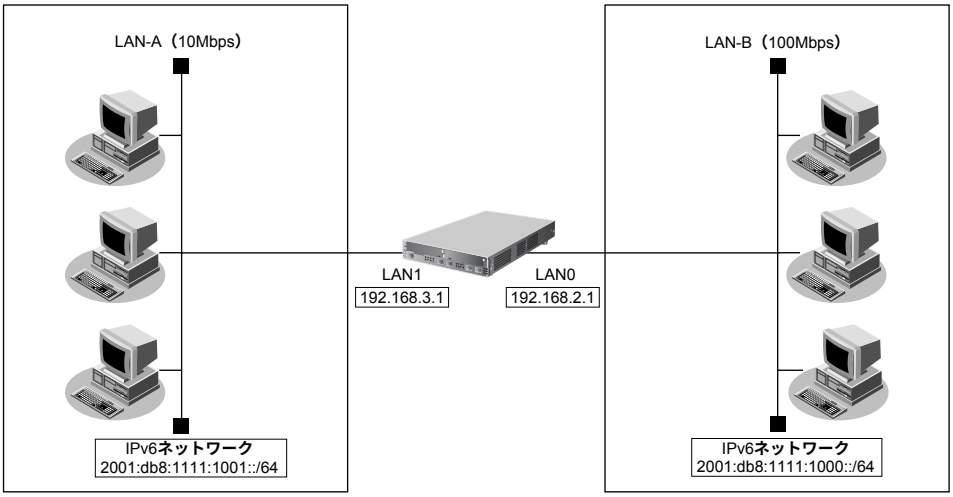
5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

1.3　IPv4 のネットワークに IPv6 ネットワークを追加する

適用機種　全機種

ここでは、IPv4 で通信しているネットワーク環境に IPv6 通信設定を追加する例について説明します。



● 設定条件

【LAN-A 側】

- プレフィックス/プレフィックス長　：2001:db8:1111:1001::/64

【LAN-B 側】

- プレフィックス/プレフィックス長　：2001:db8:1111:1000::/64

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

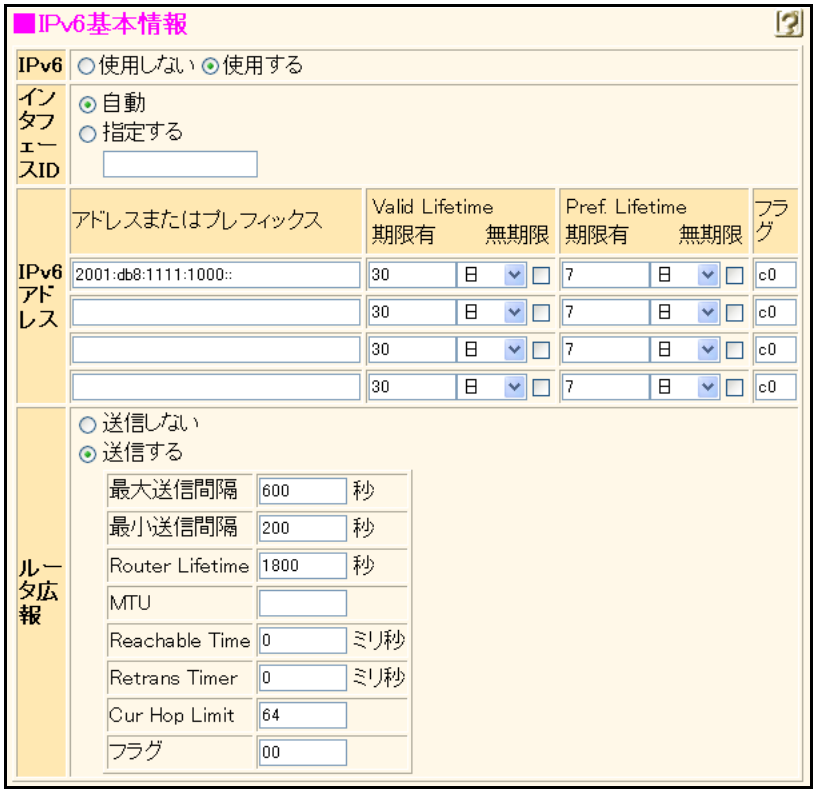
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:1000::
- ルータ広報　→送信する



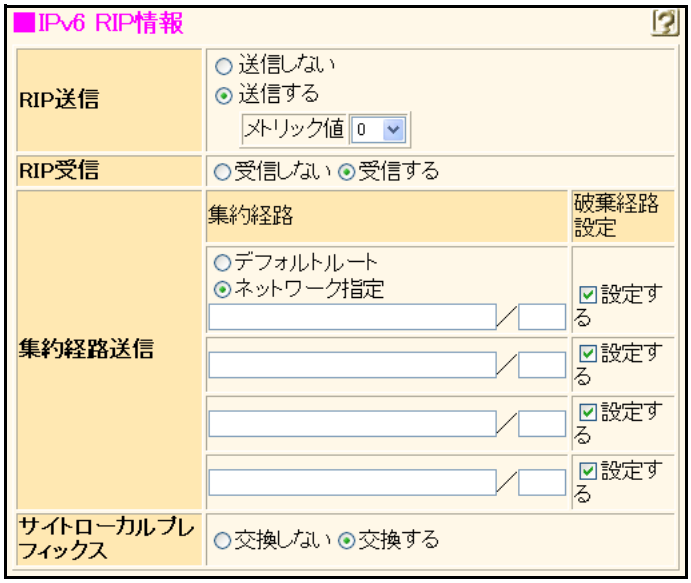
5.　［保存］ボタンをクリックします。

6.　IPv6 関連の設定項目の「IPv6 RIP 情報」をクリックします。

「IPv6 RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→送信する
- RIP 受信　→受信する
- サイトローカルプレフィックス　→交換する



8.　［保存］ボタンをクリックします。

LAN1 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

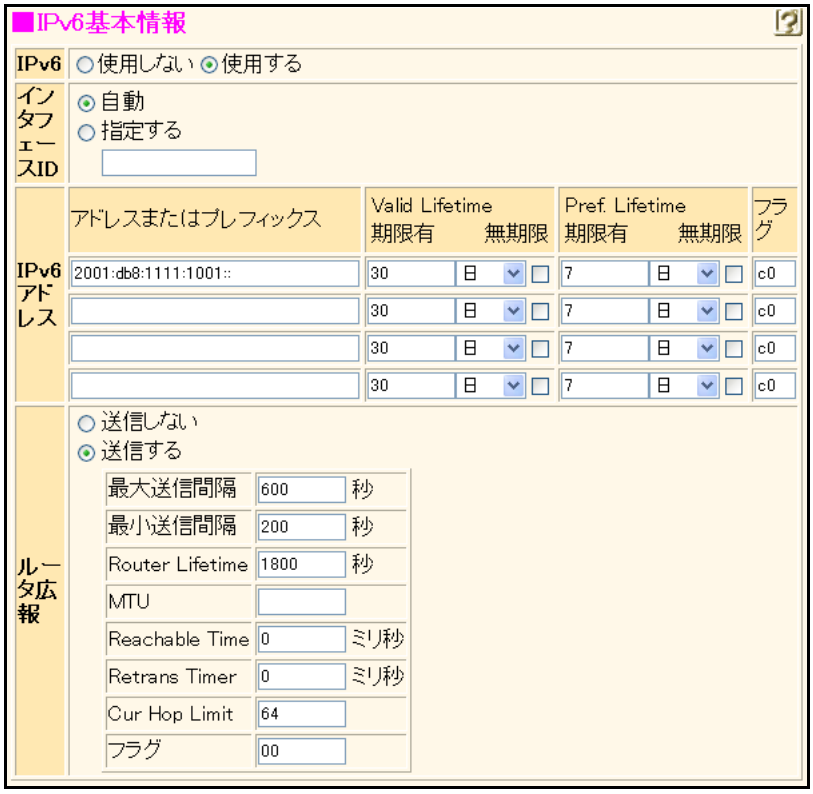
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:1001::
- ルータ広報　→送信する



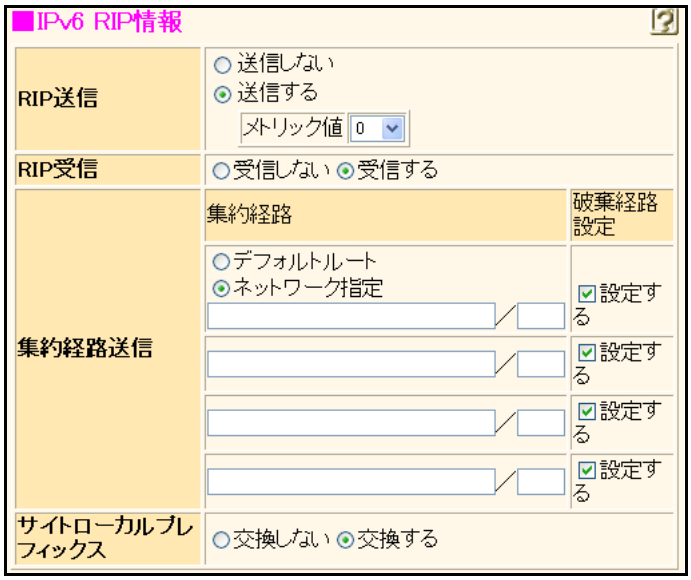
5.　［保存］ボタンをクリックします。

6.　IPv6 関連の設定項目の「IPv6 RIP 情報」をクリックします。

「IPv6 RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→送信する
- RIP 受信　→受信する
- サイトローカルプレフィックス　→交換する



8.　［保存］ボタンをクリックします。

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

1.4　プライベートLANを構築する

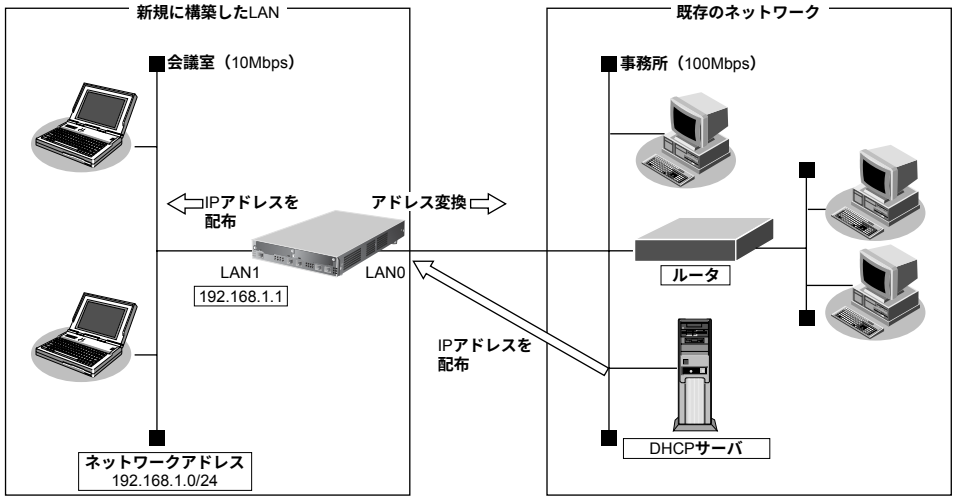
適用機種　全機種

ここでは、以下の条件で会議室 LAN を一時的に構築し、事務所ネットワークと接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

[事務所側 LAN]

- LAN0 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：DHCP サーバから自動的に取得
- マルチ NAT を使用する
  - グローバルアドレス　：事務所側の DHCP サーバから割り当てられた IP アドレスを使用する
  - アドレス個数　：1
  - アドレス割当てタイマ　：5 分

[会議室側 LAN]

- LAN1 ポートを使用する
- 転送レート　：自動認識
- IP アドレス/ネットマスク　：192.168.1.1/24
- DHCP サーバ機能を使用する
  - 割当て先頭 IP アドレス　：192.168.1.2
  - 割当てアドレス数　：253
  - リース期間　：1 日
  - デフォルトルータ広報　：192.168.1.1
  - DNS サーバ広報　：192.168.1.1

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

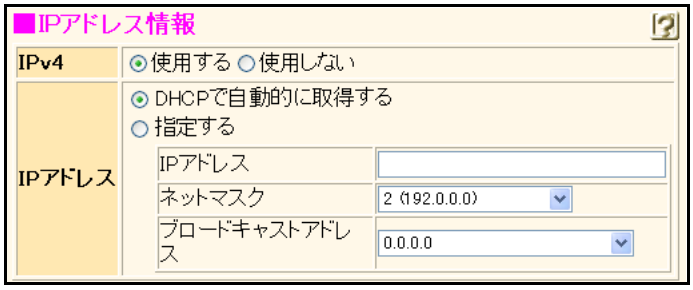
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→DHCP で自動的に取得する



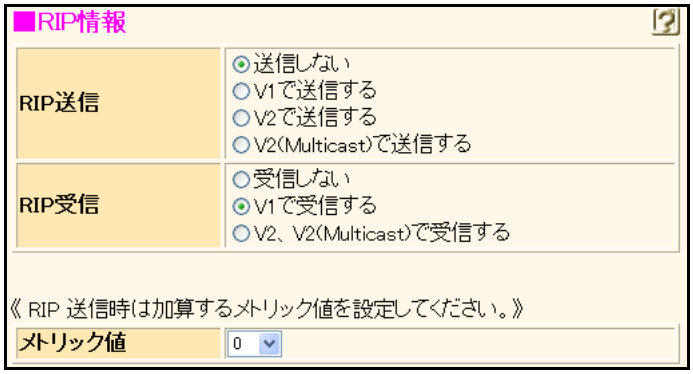
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→送信しない
- RIP 受信　→V1 で受信する
- メトリック値　→0



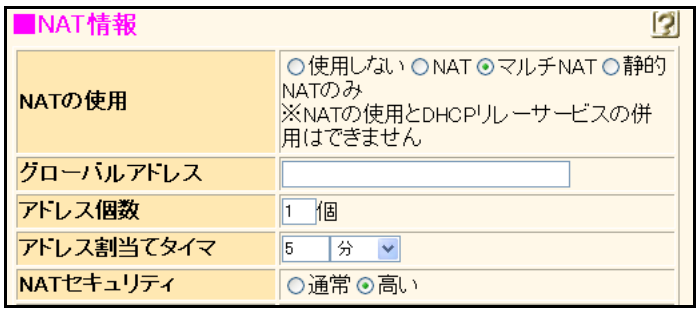
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

10.　以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→指定しない
- アドレス個数　→1
- アドレス割当てタイマ　→5 分
- NAT セキュリティ　→高い



こんな事に気をつけて

アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

11.　［保存］ボタンをクリックします。

LAN1 情報を設定する

こんな事に気をつけて

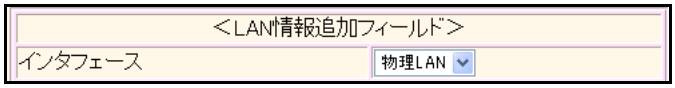
Si-R180、180B では、「LAN1 情報を設定する」以降の設定は、初期値と同じ内容であるため、設定を省略することができます。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→物理 LAN



3.　［追加］ボタンをクリックします。

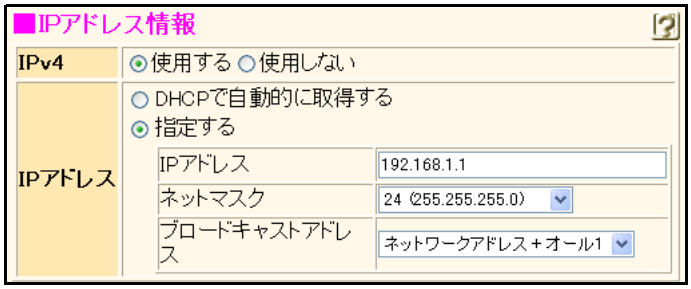
「LAN1 情報（物理 LAN）」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

5.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



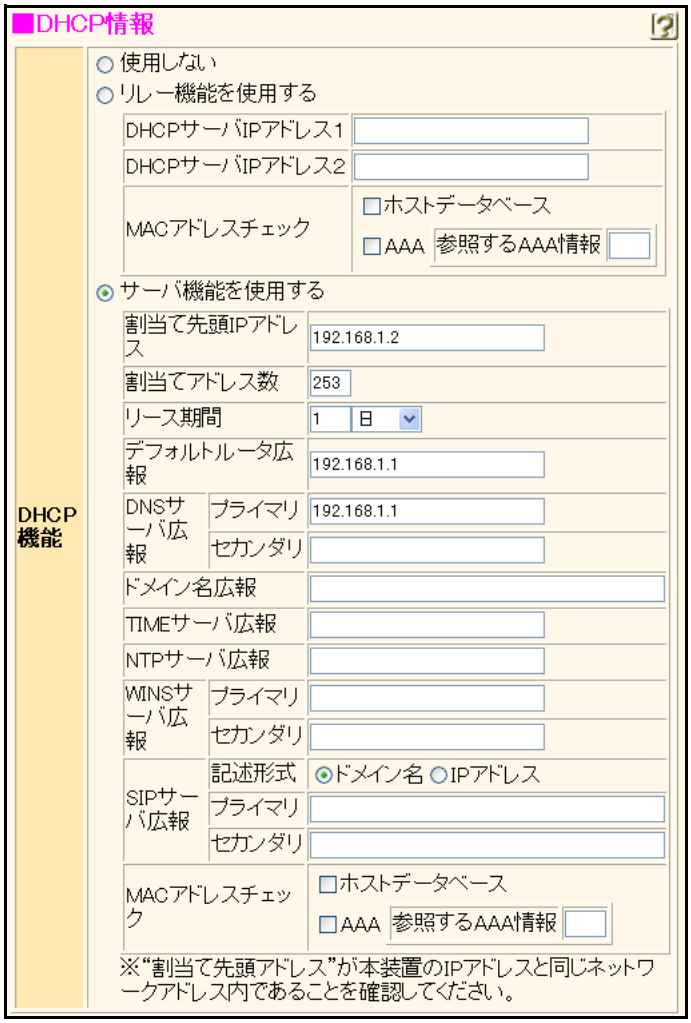
6.　［保存］ボタンをクリックします。

7.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

8.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.1.2
  割当てアドレス数　→ 253
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.1.1
  DNS サーバ広報
  プライマリ　→ 192.168.1.1
  セカンダリ　→指定しない
  ドメイン名広報　→指定しない
  TIME サーバ広報　→指定しない
  NTP サーバ広報　→指定しない
  WINS サーバ広報　→指定しない
  SIP サーバ広報　→指定しない
  MAC アドレスチェック　→指定しない



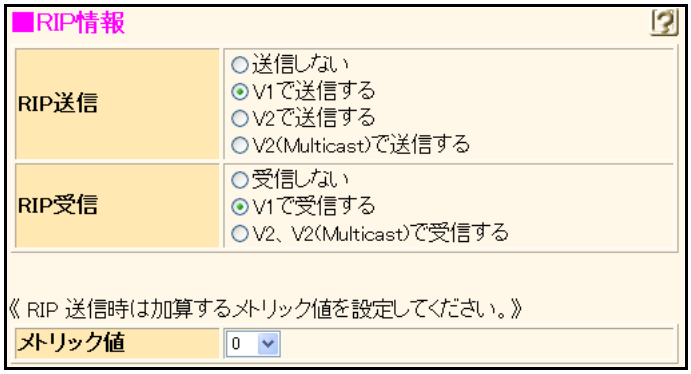
9.　［保存］ボタンをクリックします。

10.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

11.　以下の項目を指定します。

- RIP送信　→V1 で送信する
- RIP受信　→V1 で受信する
- メトリック値　→0



12.　［保存］ボタンをクリックします。

13.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置の設定が終了したら、設定を有効にするためにパソコンのシステムを終了し、パソコンおよび本装置の電源を切断します。各装置をLANケーブルで正しく接続したあと、本装置、パソコンの順に電源を投入します。

こんな事に気をつけて

本装置のDHCPサーバ機能を使用する場合は、以下の点に注意してください。

- **本装置のDHCPサーバ機能を利用するLAN側のパソコンは、IPアドレスを自動的に取得する設定にしてください。固定のIPアドレスを設定していると、本装置が配布するIPアドレスと重なり、矛盾が生じる場合があります。**
- **パソコンに固定のIPアドレスを割り当てる場合は、「2.23.2 DHCPスタティック機能を使う」（P.752）を参考にして、IPアドレスとMACアドレスを設定してください。**

1.5　インターネットへ専用線で接続する

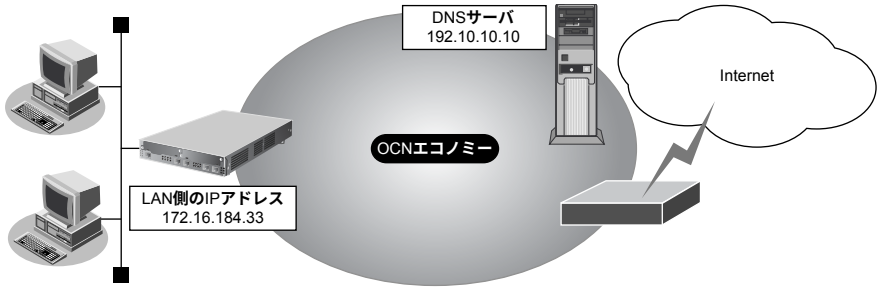
適用機種　*Si-R220B,220C,370,570*

ここでは、以下の設定条件で専用線を利用する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）で OCN エコノミー専用線（128Kbps）を使用する
- LAN0 を使用して、新規に LAN を構築する
- OCN 側の DNS サーバを使用　：192.10.10.10
- OCN より提示されたドメイン名　：domain.ocn.ne.jp
- 接続するパソコンの台数は OCN から割り当てられた IP アドレスよりも少ない
- 割り当て IP アドレス
  ネットワークアドレス/ネットマスク　：172.16.184.32/29
  ホストアドレス　：172.16.184.33 ～ 172.16.184.38
  ブロードキャストアドレス　：172.16.184.39
  本装置の LAN 側の IP アドレス　：172.16.184.33
- 接続ネットワーク名　：internet

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0 ～ 9、A ～ Z、a ～ z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  ☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

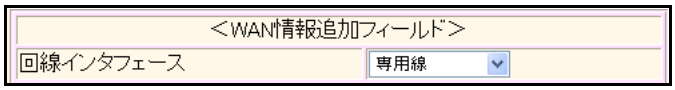
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→専用線



3.　［追加］ボタンをクリックします。

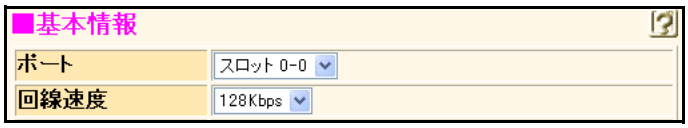
「WAN0 情報（専用線）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→ 128Kbps



Si-R220B、220C では、ポートは固定です。

6.　［保存］ボタンをクリックします。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

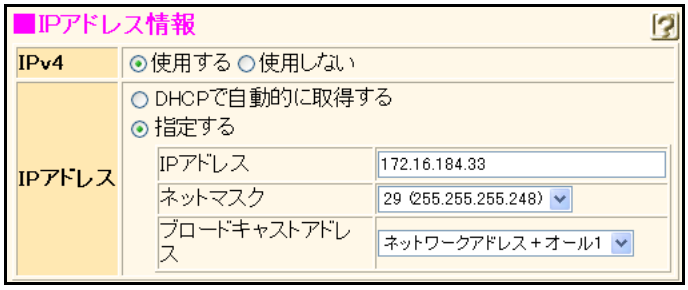
4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する

  IP アドレス　→ 172.16.184.33

  ネットマスク　→ 29（255.255.255.248）

  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

7.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する

  割当て先頭 IP アドレス　→ 172.16.184.34

  割当てアドレス数　→ 6

  リース期間　→ 1 日

  デフォルトルータ広報　→ 172.16.184.33

  DNS サーバ広報

  プライマリ　→ 192.10.10.10

  セカンダリ　→指定しない

  ドメイン名広報　→ domain.ocn.ne.jp

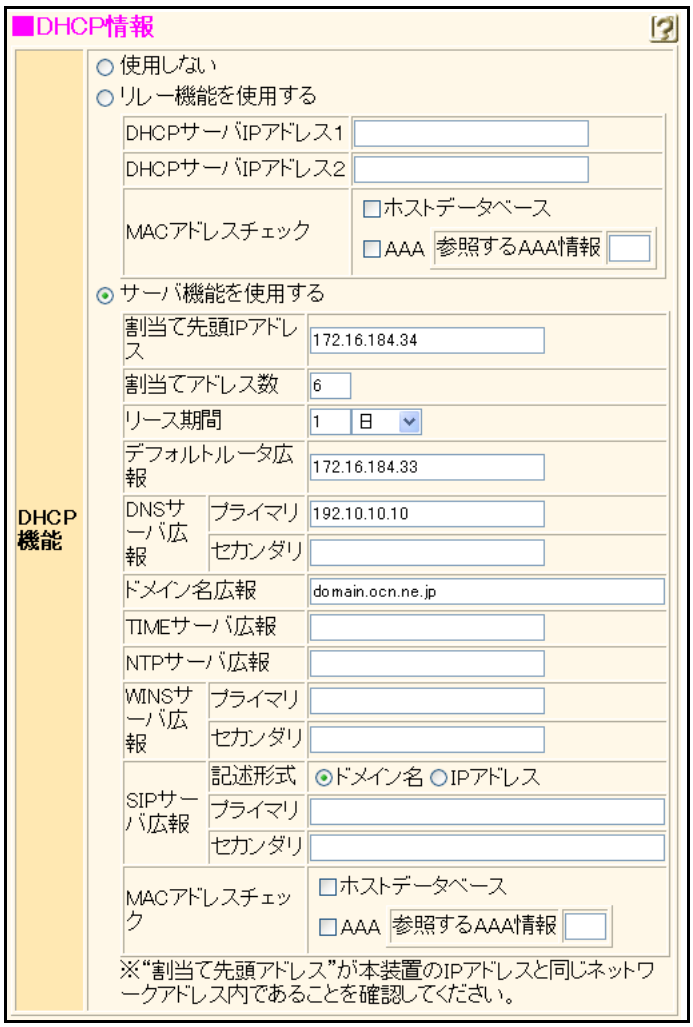
  TIME サーバ広報　→指定しない

  NTP サーバ広報　→指定しない

  WINS サーバ広報　→指定しない

  SIP サーバ広報　→指定しない

  MAC アドレスチェック　→指定しない



8.　［保存］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

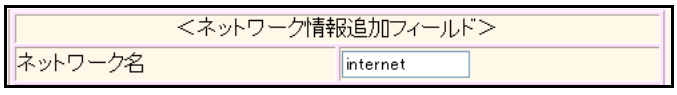
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　　→internet



4.　［追加］ボタンをクリックします。

「ネットワーク情報（internet）」ページが表示されます。

5.　「IP 関連」をクリックします。

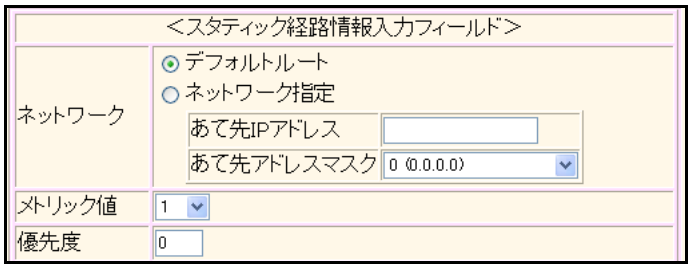
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
- メトリック値　→1
- 優先度　→0



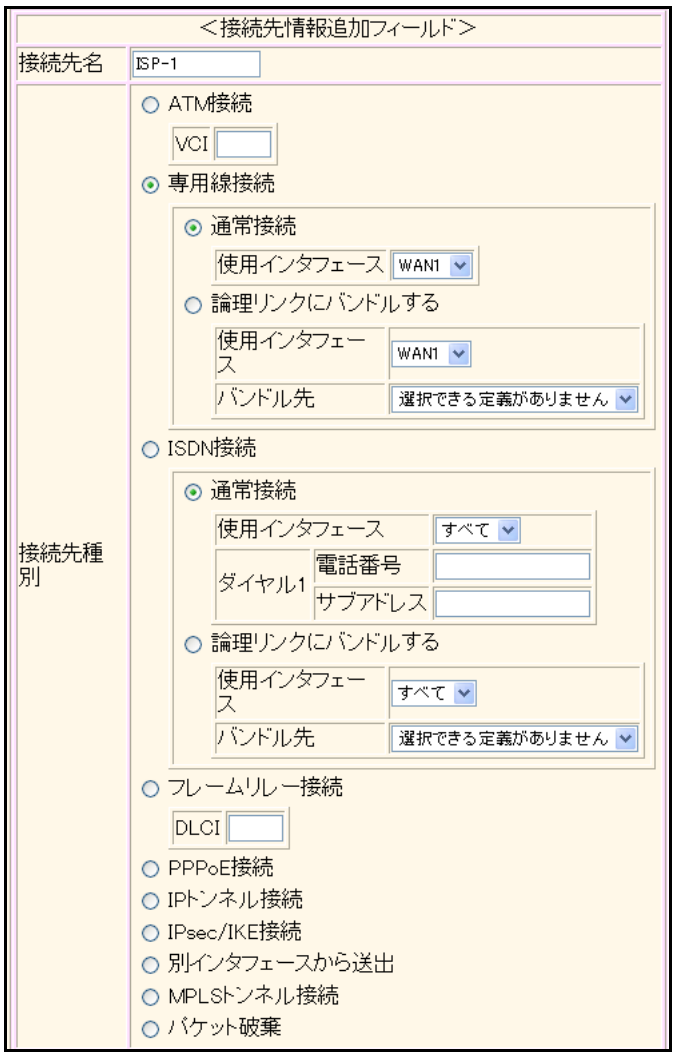
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→ISP-1
- 接続先種別　→専用線接続



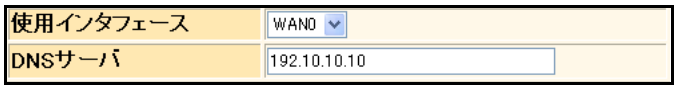
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 使用インタフェース　　→WAN0
- DNS サーバ　　→192.10.10.10



13.　［保存］ボタンをクリックします。

14.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスを変更する必要があります。パソコンを再起動してください。**
- **本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。**

1.6　インターネットへ PPPoE で接続する

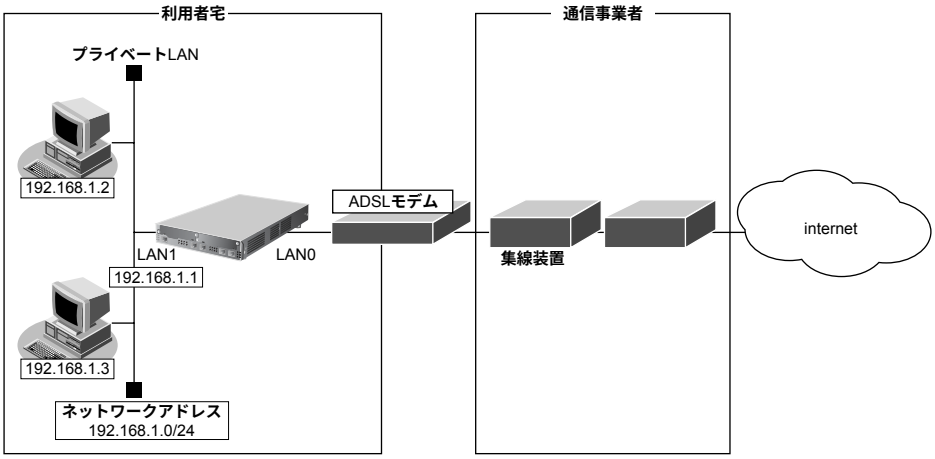
適用機種　全機種

ここでは、PPPoE 接続を使ってフレッツ・ADSL などのサービスを利用し、インターネットへ接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☛ 参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**
- **PPPoE で利用する相手情報の MTU 値は、接続先から指定された MTU 値を設定します。一般的には、1454 を設定すれば問題ありません。**

- PPPoE を利用する物理 LAN インタフェースの情報として、以下の手順で「ポート番号」と「転送レート」を必ず設定してください。「LAN 情報（物理 LAN）」を設定しない場合、通信できなくなります。
  以下に手順を示します。
  1. 設定メニューのルータ設定で「LAN 情報」をクリックします。
  2. インタフェースに“物理インタフェース”を指定して、［追加］ボタンをクリックします。
  3. 「共通情報」－「基本情報」で、ポート番号と転送レートを選択して、［保存］ボタンをクリックします。
- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［削除］ボタンをクリックします。

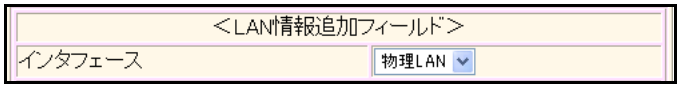
メッセージボックスに「削除していいですか？」というメッセージが表示されます。

3.　［OK］ボタンをクリックします。

インタフェースが LAN0 の定義が削除されます。

4.　以下の項目を指定します。

- インタフェース　→物理 LAN



5.　［追加］ボタンをクリックします。

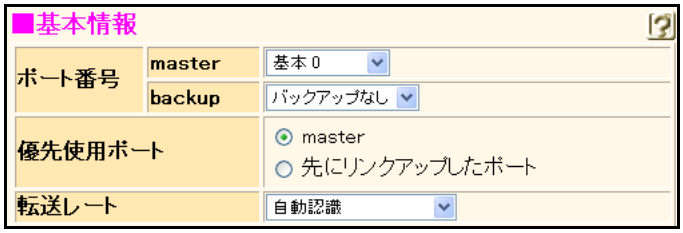
「LAN0 情報（物理 LAN）」ページが表示されます。

6.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

7.　以下の項目を指定します。

- ポート番号
  master　→基本 0
  backup　→バックアップなし（Si-R180、180B 以外の機種だけ指定）
- 転送レート　→自動認識



8.　［保存］ボタンをクリックします。

LAN1 情報を設定する

こんな事に気をつけて

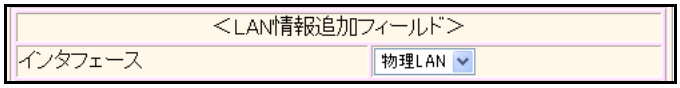
Si-R180、180B では、「LAN1 情報を設定する」以降の設定は、初期値と同じ内容であるため、設定を省略することができます。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→物理 LAN



3.　［追加］ボタンをクリックします。

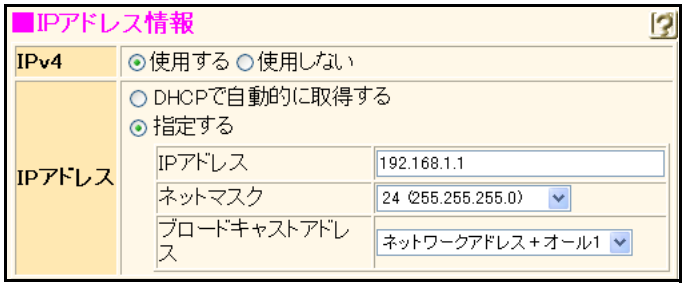
「LAN1 情報（物理 LAN）」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

5.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



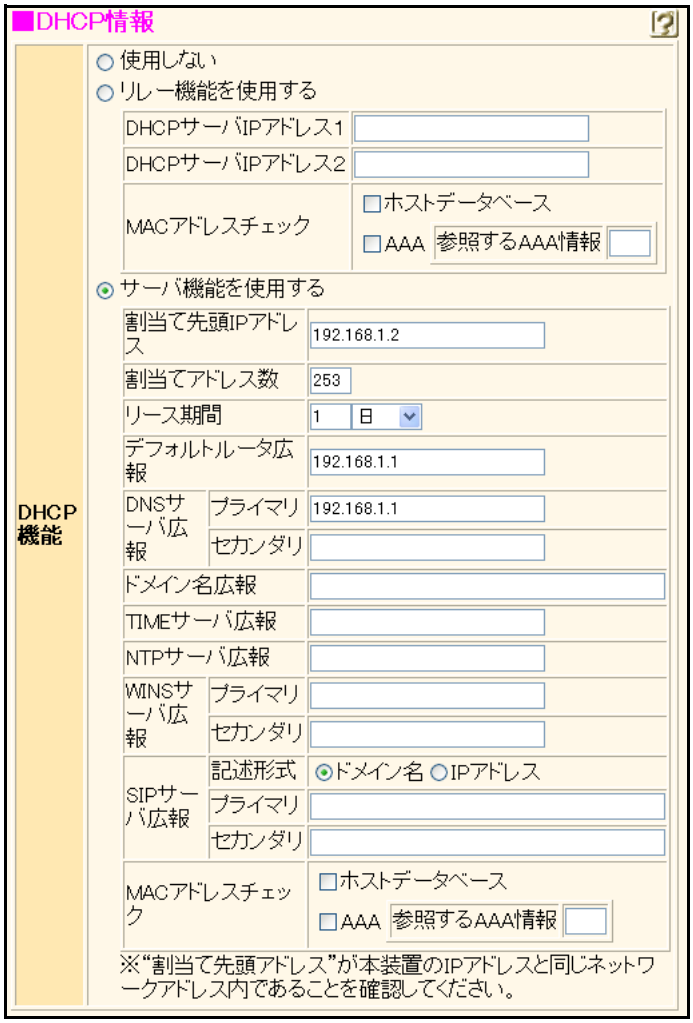
6.　［保存］ボタンをクリックします。

7.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

8.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.1.2
  割当てアドレス数　→ 253
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.1.1
  DNS サーバ広報
  プライマリ　→ 192.168.1.1
  セカンダリ　→指定しない
  ドメイン名広報　→指定しない
  TIME サーバ広報　→指定しない
  NTP サーバ広報　→指定しない
  WINS サーバ広報　→指定しない
  SIP サーバ広報　→指定しない
  MAC アドレスチェック　→指定しない



9.　［保存］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

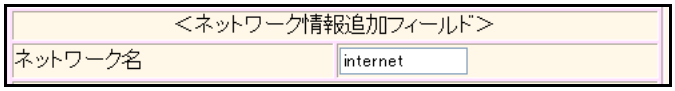
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→internet



4.　［追加］ボタンをクリックします。

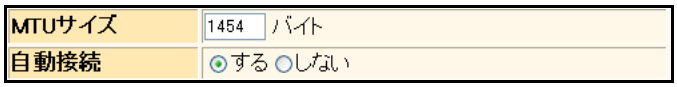
「ネットワーク情報（internet)」ページが表示されます。

5.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

6.　以下の項目を指定します。

- MTU サイズ　→1454
- 自動接続　→する



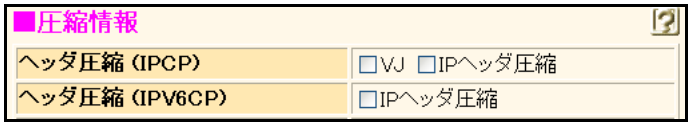
7.　［保存］ボタンをクリックします。

8.　「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

9.　以下の項目を指定します。

- ヘッダ圧縮（IPCP）　→チェックしない
- ヘッダ圧縮（IPV6CP）　→チェックしない



Si-R180、180B、260B では、“データ圧縮”の項目はありません。

10.　［保存］ボタンをクリックします。

11.　「IP 関連」をクリックします。

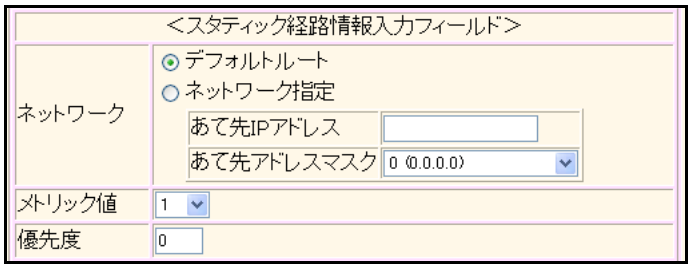
IP 関連の設定項目と「IP 基本情報」が表示されます。

12.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

13.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
- メトリック値　→1
- 優先度　→0



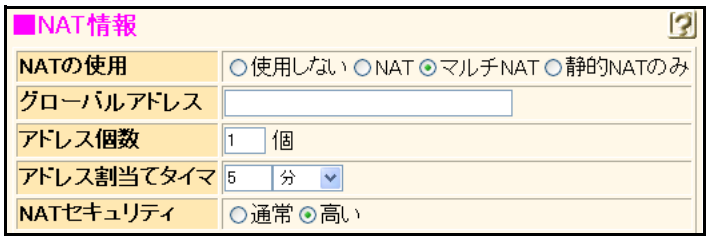
14.　［追加］ボタンをクリックします。

15.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

16.　以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→指定しない
- アドレス個数　→1
- アドレス割当てタイマ　→5 分
- NAT セキュリティ　→高い



こんな事に気をつけて

アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

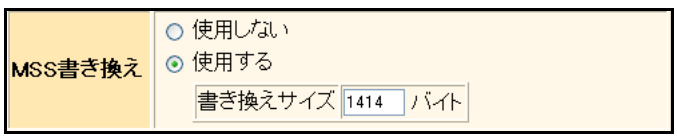
17.　［保存］ボタンをクリックします。

18.　IP 関連の設定項目の「IP 基本情報」をクリックします。

「IP 基本情報」が表示されます。

19.　以下の項目を指定します。

- MSS 書き換え　→使用する
  書き換えサイズ　→1414



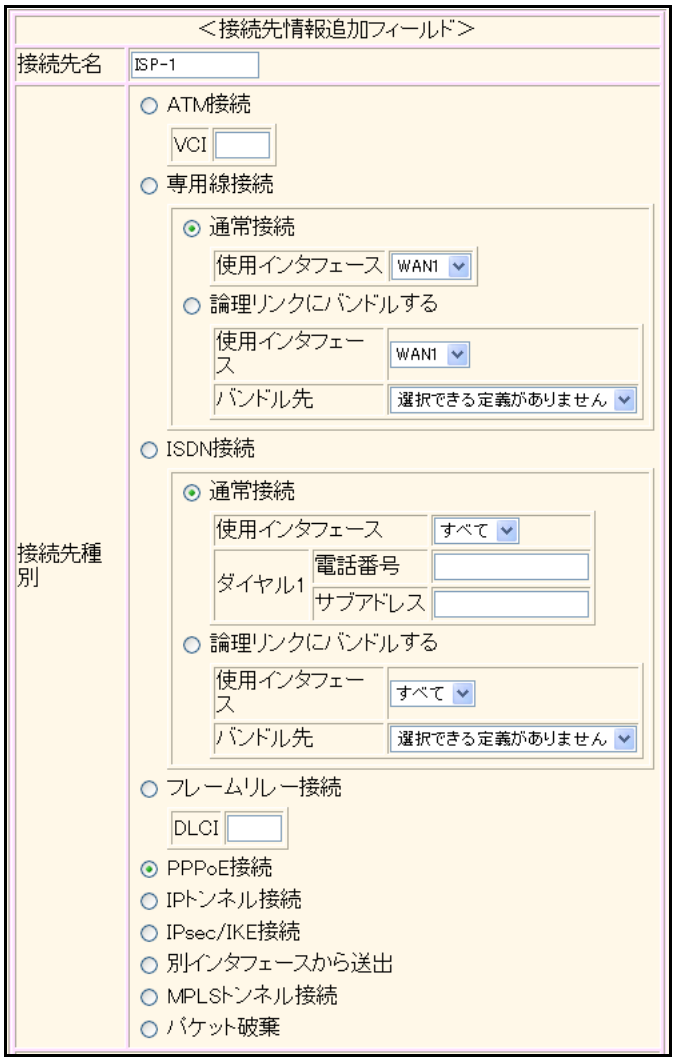
20.　［保存］ボタンをクリックします。

21.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

22.　以下の項目を指定します。

- 接続先名　→ISP-1
- 接続先種別　→PPPoE 接続



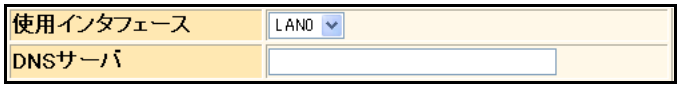
機種により、接続先種別の表示が上記の画面とは異なります。

23.　［追加］ボタンをクリックします。

PPPoE 接続の設定項目と「基本情報」が表示されます。

24.　以下の項目を指定します。

- 使用インタフェース　→LAN0
- DNS サーバ　→指定しない



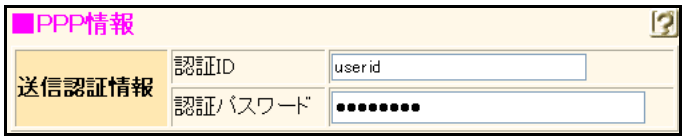
25.　［保存］ボタンをクリックします。

26.　PPPoE 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

27.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→ userid
  認証パスワード　→ userpass



28.　［保存］ボタンをクリックします。

ProxyDNS 情報、URL フィルタ情報を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

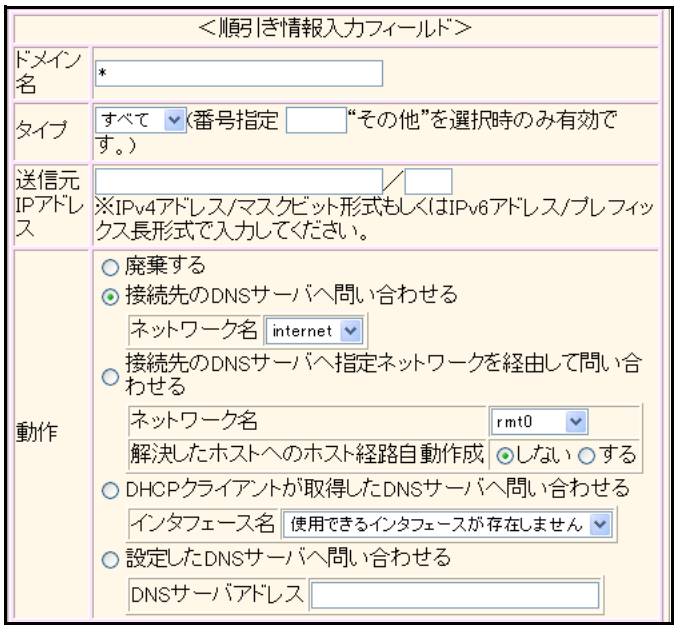
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→ *
- タイプ　→すべて
- 送信元 IP アドレス　→指定しない
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→ internet



4.　［追加］ボタンをクリックします。

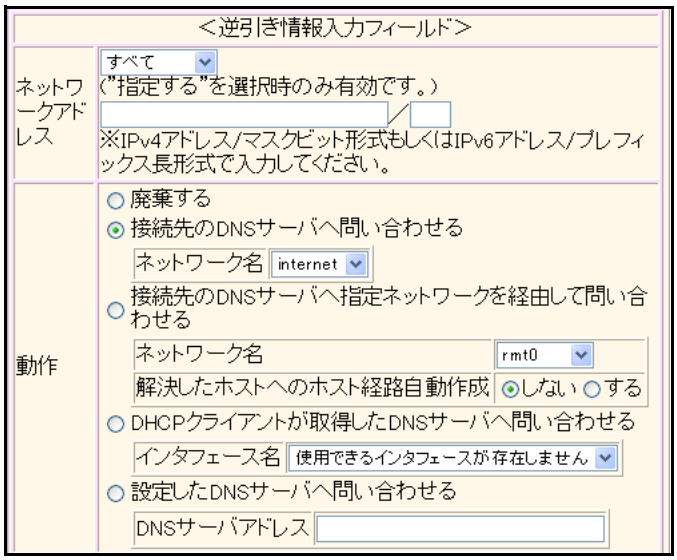
5.　「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

6.　以下の項目を指定します。

- ネットワークアドレス　→すべて
- 動作　→接続先の DNS サーバへ問い合わせる

  ネットワーク名　→internet



7.　[追加] ボタンをクリックします。

8.　画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

1.7　インターネットへデータ通信カードを使用して接続する

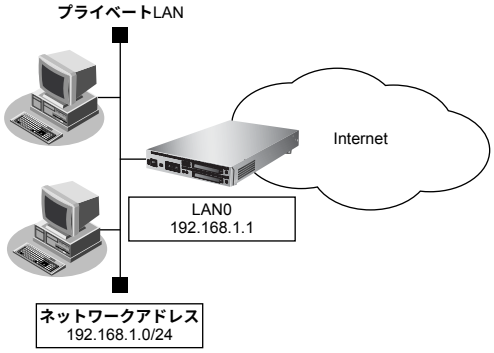
適用機種　*Si-R240,240B*

ここでは、データ通信カードを使用して、ご購入時の設定のままインターネットへ接続する場合を例に説明します。

参照　動作検証済みのデータ通信カード（富士通ホームページ）
- Si-R240
  http://fenics.fujitsu.com/products/sir/sir240/#supportcard
- Si-R240B
  http://fenics.fujitsu.com/products/sir/sir240b/#supportcard

こんな事に気をつけて
- **データ通信カードは、電源投入前に挿入してください。また、電源投入後の抜き差しはしないでください。**
- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。**

参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

[Internet 側]
- データ通信カード装着 SLOT　：SLOT0
- 認証 ID　：通信事業者から提示された内容
- 認証パスワード　：通信事業者から提示された内容
- 電話番号　：通信事業者から提示された内容
- 無通信監視タイマ　：無通信監視時間を 1 分とする
- 強制切断　：100000 パケット（128 バイト単位）を超えた場合に回線を切断し、以降自動発信を行わない

[プライベート LAN 側]
- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/マスク　：192.168.1.0/24

こんな事に気をつけて

- 文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- データ通信カード接続では、以下の機能は動作しません。
  - テンプレート機能
  - 金額による課金制御機能
  - 常時接続機能
- データ通信カードで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信カードによる発信は課金が発生するため、課金情報（アカウント情報）を監視して超過課金が発生していないか、こまめに確認してください。
  また、超過課金を防止する場合は、課金制御機能の累計接続時間か累計パケット数を設定してください。
- 課金制御機能（強制切断）による回線切断が発生した場合、以下のシステムログが出力されます。

  protocol: [<line>] forced disconnection <target> <reason>

  参照 Si-R シリーズ　メッセージ集「課金制御機能による強制切断」

  課金制御機能（強制切断）により切断した場合、以降の手動および自動発信を禁止します。
  接続するにはデータ通信カードのアカウント情報のクリア（clear cardmodem account）を実行する必要があります。
- パケット数による強制切断のパケット数は、累計送受信バイト数（PPP パケット長）を 128 で割った値を用います。
  パケット数による強制切断のパケット数は目安であり、通信事業者でのパケット数と異なる場合があります。

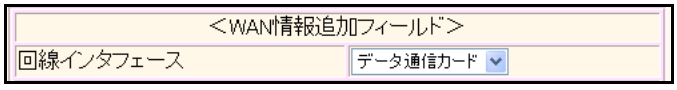
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→データ通信カード

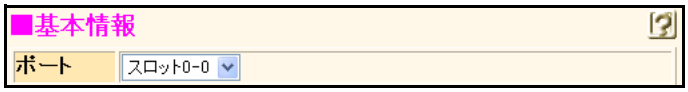


3.　［追加］ボタンをクリックします。

「WAN 情報（データ通信カード）」ページが表示されます。

4.　以下の項目を指定します。

- ポート　→スロット 0-0



5.　［保存］ボタンをクリックします。

こんな事に気をつけて

PIN コード機能を使用する場合は、「WAN 情報」-「基本情報」で設定する必要があります。また、操作メニューの「データ通信カード関連」-「PIN コード照合」でデータ通信カードにも設定する必要があります。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

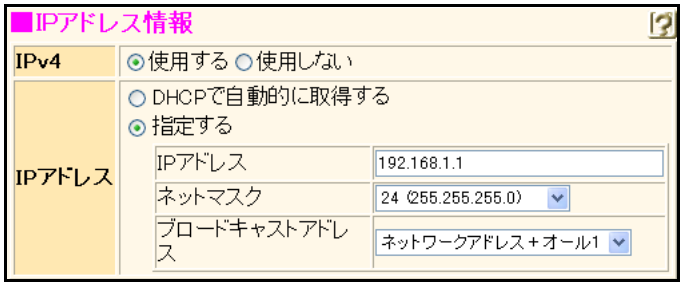
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



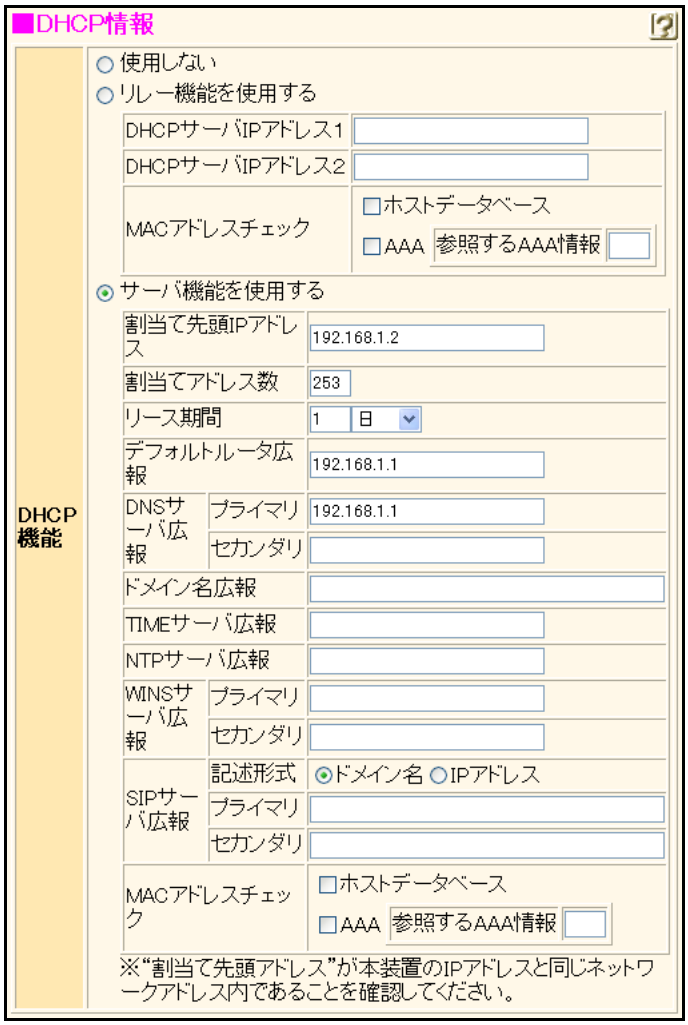
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

7.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.1.2
  割当てアドレス数　→ 253
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.1.1
  DNS サーバ広報
  プライマリ　→ 192.168.1.1
  セカンダリ　→指定しない
  ドメイン名広報　→指定しない
  TIME サーバ広報　→指定しない
  NTP サーバ広報　→指定しない
  WINS サーバ広報　→指定しない
  SIP サーバ広報　→指定しない
  MAC アドレスチェック　→指定しない



8.　［保存］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

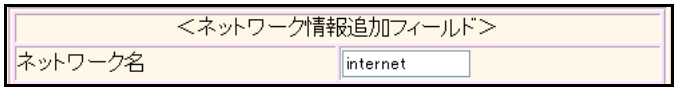
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→internet



4.　［追加］ボタンをクリックします。

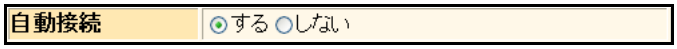
「ネットワーク情報（internet)」ページが表示されます。

5.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

6.　以下の項目を指定します。

- 自動接続　→する



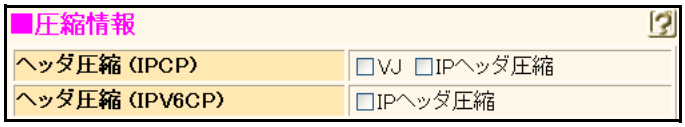
7.　［保存］ボタンをクリックします。

8.　「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

9.　以下の項目を指定します。

- ヘッダ圧縮（IPCP）　→チェックしない
- ヘッダ圧縮（IPV6CP）　→チェックしない



10.　［保存］ボタンをクリックします。

11.　「IP 関連」をクリックします。

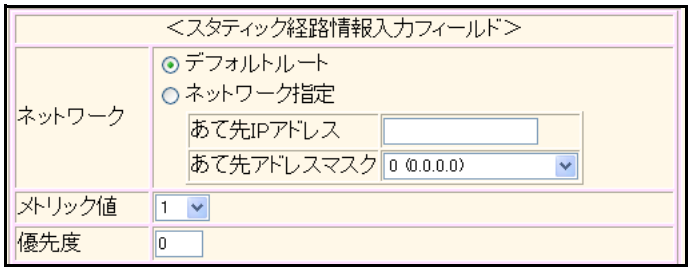
IP 関連の設定項目と「IP 基本情報」が表示されます。

12.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

13.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
- メトリック値　→1
- 優先度　→0



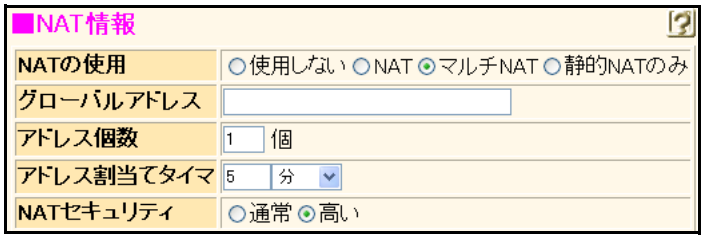
14.　［追加］ボタンをクリックします。

15.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

16.　以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→指定しない
- アドレス個数　→1
- アドレス割当てタイマ　→5 分
- NAT セキュリティ　→高い



こんな事に気をつけて

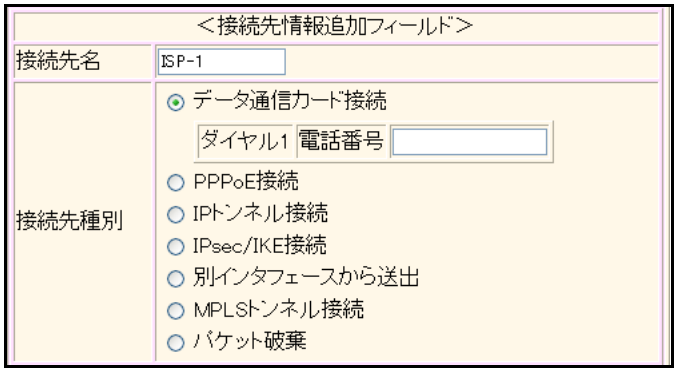
アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→ISP-1
- 接続先種別　→データ通信カード接続
  ダイヤル 1
  電話番号　→（通信事業者から提示された内容）



19.　［追加］ボタンをクリックします。

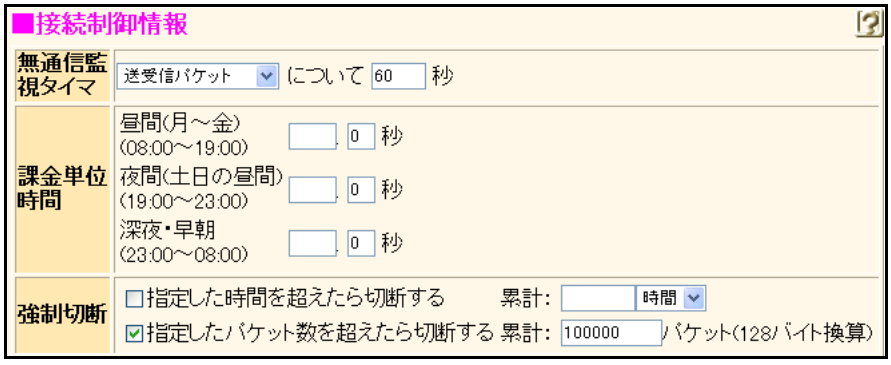
「接続先情報（ISP-1）」が表示されます。

20.　データ通信カード接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

21.　以下の項目を指定します。

- 無通信監視タイマ　→送受信パケットについて 60 秒
- 強制切断
  指定したパケット数を超えたら切断する
  →チェックする
  累計　→100000 パケット



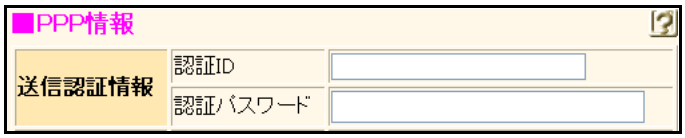
22.　［保存］ボタンをクリックします。

23.　データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

24.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→（通信事業者から提示された内容）
  認証パスワード　→（通信事業者から提示された内容）



25.　［保存］ボタンをクリックします。

補足　各通信事業者の認証 ID、認証パスワード、電話番号を以下に示します。
詳細については、各通信事業者にお問い合わせください。

通信事業者	認証 ID	認証パスワード	電話番号
ウィルコム PRIN つなぎ放題[PRO]	prin	prin	0570570711##64
NTT ドコモ mopera	（任意の文字列）	（任意の文字列）	*99***1#
au by KDDI au.NET	au@au-win.ne.jp	au	*99**24#
ソフトバンクモバイル （旧ボーダフォン） アクセスインターネット	vodafone@connect	vodafone	*99#

ProxyDNS 情報、URL フィルタ情報を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

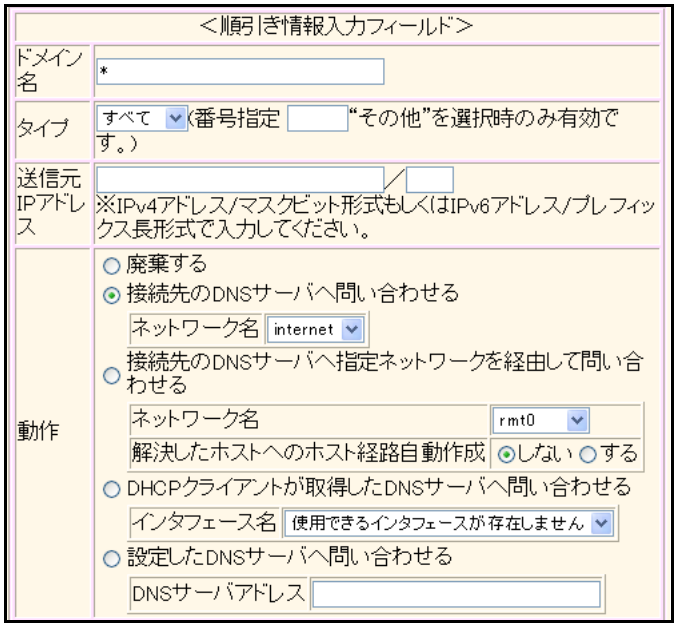
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→ *
- タイプ　→すべて
- 送信元 IP アドレス　→指定しない
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→ internet



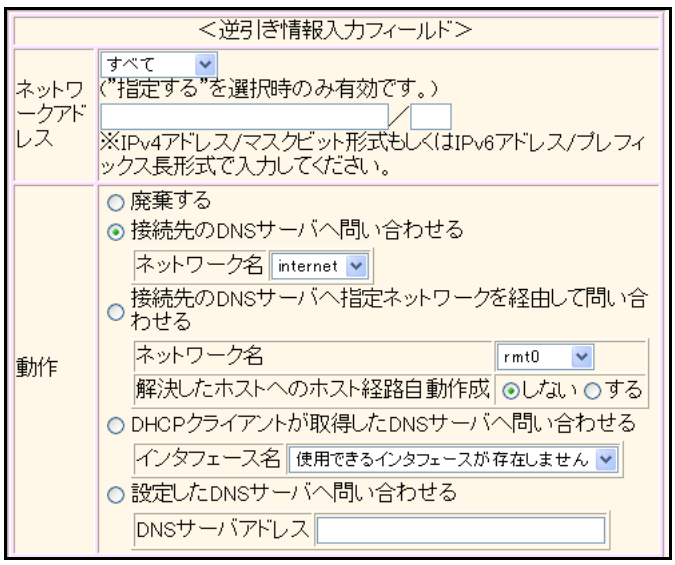
4.　［追加］ボタンをクリックします。

5.　「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

6.　以下の項目を指定します。

- ネットワークアドレス　→すべて
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→ internet



7.　［追加］ボタンをクリックします。

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

1.8 無線 LAN とデータ通信カードで仮設店舗を構築する

適用機種 ***Si-R240,240B***

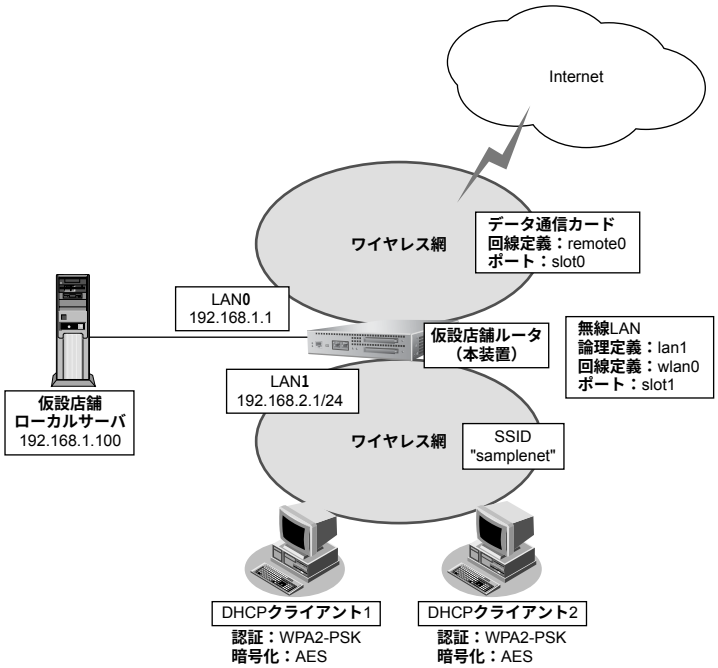
ここでは、無線 LAN カードとデータ通信カードで仮設店舗を構築する場合を例に説明します。

無線 LAN とデータ通信カードによるネットワークのワイヤレス化を行い、LAN ケーブルの配線なしに無線通信によるネットワークを構築することができます。

こんな事に気をつけて

- **無線 LAN カードは、Si-R シリーズ専用の無線 LAN AP カード（SIRWLAP）を使用してください。**
- **無線 LAN カードは、SLOT0 または SLOT1 のどちらか一方に挿入して使用してください。同時に 2 枚の無線 LAN カードを挿入して使用することはできません。**
- **無線 LAN カード／データ通信カードは、電源投入前に挿入してください。また、電源投入後の抜き差しはしないでください。**
- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおりに設定しても通信できないことがあります。**

☛ 参照 Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

有線 LAN を使ってローカルサーバに接続する

- 利用するポート　：lan0
- IP アドレス　：192.168.1.1/24

無線 LAN を使ってアクセスポイントを構築する

- 利用するポート　：slot1
- 利用する論理定義　：lan1
- 利用する回線定義　：wlan0
- 通信モード　：IEEE802.11b/g
- チャネル　：10
- SSID　：samplenet
- 認証モード　：WPA2-PSK
- 暗号化モード　：AES
- 事前共有キー（PSK）　：テキストで“abcdefghijklmnopqrstuvwxyz”
- IP アドレス　：192.168.2.1/24
- その他　：接続端末のアドレスは DHCP 機能を利用する

データ通信カードを使ってインターネットへ接続する

- 利用するポート　：slot0
- 認証 ID　：通信事業者から提示された内容
- 認証パスワード　：通信事業者から提示された内容
- 電話番号　：通信事業者から提示された内容
- 無通信監視タイマ　：無通信監視時間を 1 分とする

端末を設定する

無線 LAN アダプタの設定マニュアルを参考に設定を行ってください。

本装置を設定する

有線 LAN を使ってローカルサーバに接続する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

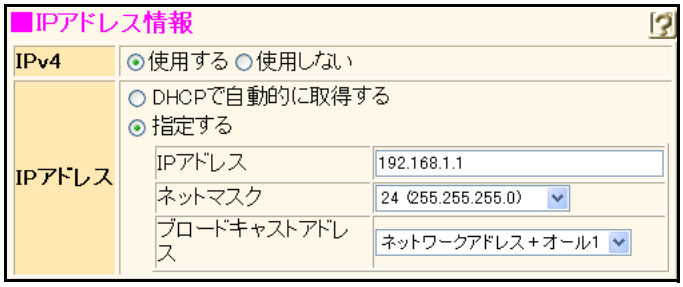
3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する

IPアドレス　→192.168.1.1
ネットマスク　→24（255.255.255.0）
ブロードキャストアドレス　→ネットワークアドレス＋オール1



5.　［保存］ボタンをクリックします。

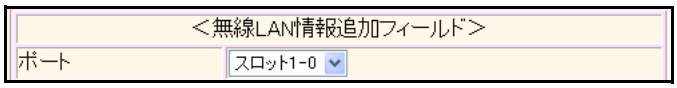
無線 LAN 情報（無線 LAN 情報）を設定する

1.　設定メニューのルータ設定で「無線 LAN 情報」をクリックします。

「無線 LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- ポート　→スロット 1-0

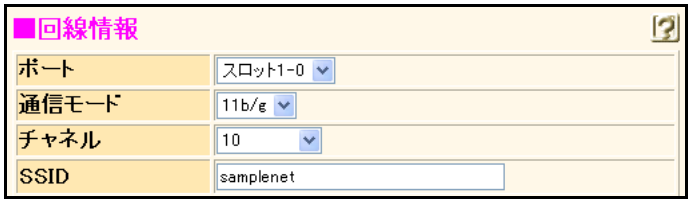


3.　［追加］ボタンをクリックします。

無線 LAN0 情報の設定項目と「回線情報」が表示されます。

4.　以下の項目を指定します。

- ポート　→スロット 1-0
- 通信モード　→11b/g
- チャネル　→10
- SSID　→samplenet



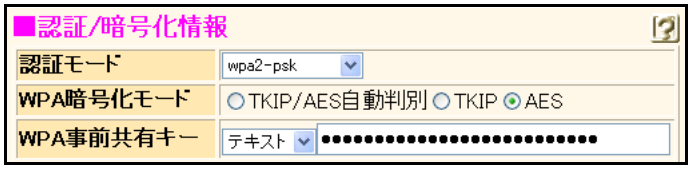
5.　［保存］ボタンをクリックします。

6.　「認証／暗号化情報」をクリックします。

「認証／暗号化情報」が表示されます。

7.　以下の項目を指定します。

- 認証モード　→wpa2-psk
- WPA 暗号化モード　→AES
- WPA 事前共有キー　→テキスト
  →abcdefghijklmnopqrstuvwxyz



8.　［保存］ボタンをクリックします。

無線 LAN を使ってアクセスポイントを構築する

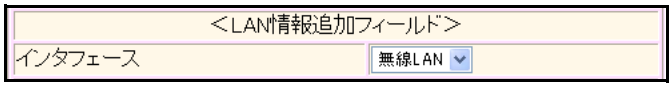
LAN（無線 LAN）情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→無線 LAN



3.　［追加］ボタンをクリックします。

「LAN1 情報（無線 LAN）」ページが表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 無線 LAN 定義　→無線 LAN0

6.　［保存］ボタンをクリックします。

7.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

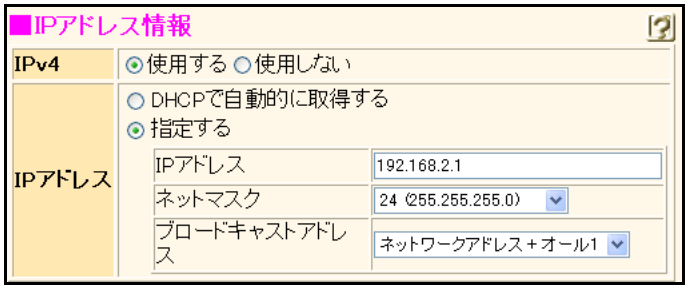
8.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する

  IP アドレス　→ 192.168.2.1

  ネットマスク　→ 24（255.255.255.0）

  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



9.　［保存］ボタンをクリックします。

10.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

11.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する

  割当て先頭 IP アドレス　→ 192.168.2.10

  割当てアドレス数　→ 10

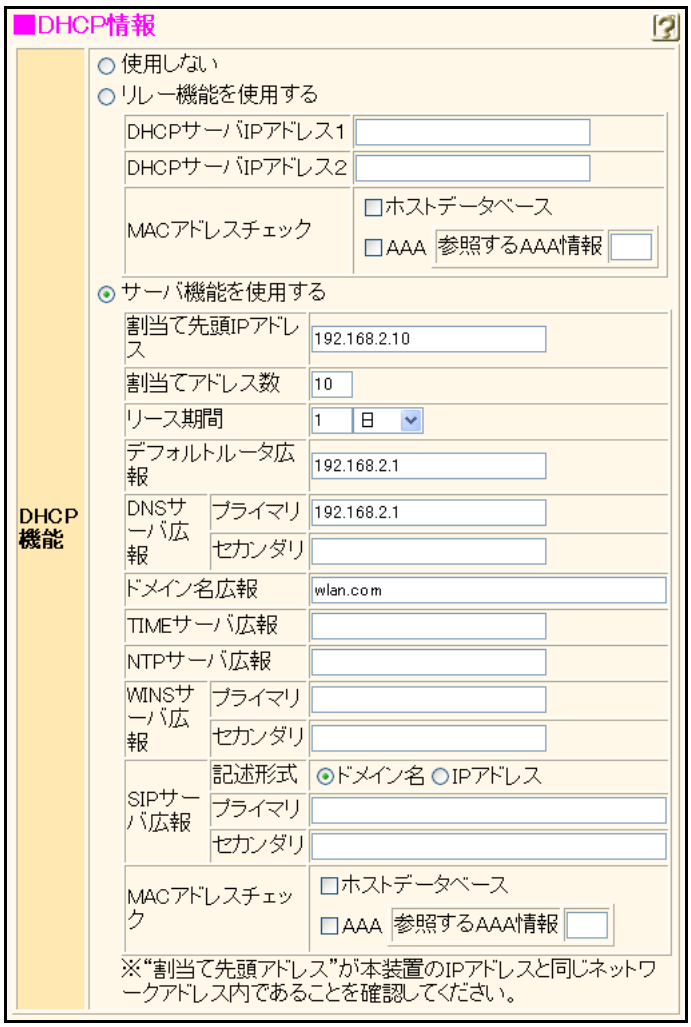
  リース期間　→ 1 日

  デフォルトルータ広報　→ 192.168.2.1

  DNS サーバ広報

  プライマリ　→ 192.168.2.1

  ドメイン名広報　→ wlan.com



12.　［保存］ボタンをクリックします。

データ通信カードを使ってインターネットへ接続する

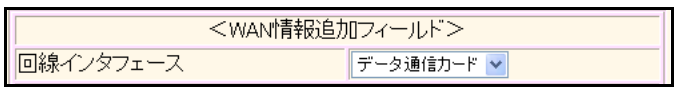
WAN 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　　→データ通信カード

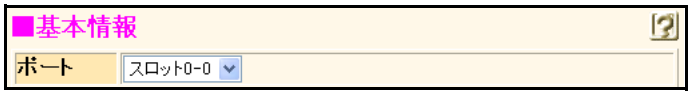


3.　［追加］ボタンをクリックします。

「WAN 情報（データ通信カード）」ページが表示されます。

4.　以下の項目を指定します。

- ポート　　→スロット 0-0



5.　［保存］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

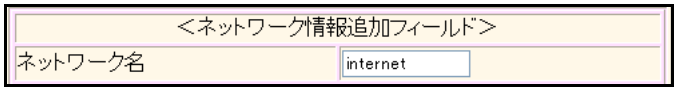
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→internet



4.　［追加］ボタンをクリックします。

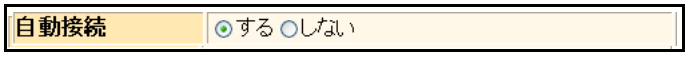
「ネットワーク情報（internet)」ページが表示されます。

5.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

6.　以下の項目を指定します。

- 自動接続　→する



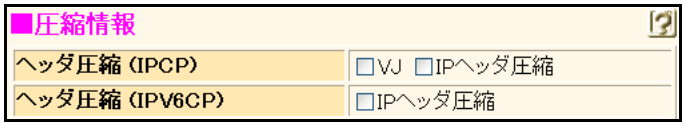
7.　［保存］ボタンをクリックします。

8.　「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

9.　以下の項目を指定します。

- ヘッダ圧縮（IPCP）　→チェックしない
- ヘッダ圧縮（IPV6CP）　→チェックしない



10.　［保存］ボタンをクリックします。

11.　「IP 関連」をクリックします。

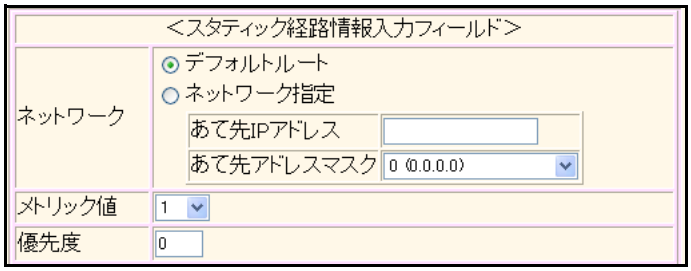
IP 関連の設定項目と「IP 基本情報」が表示されます。

12.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

13.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
- メトリック値　→1
- 優先度　→0



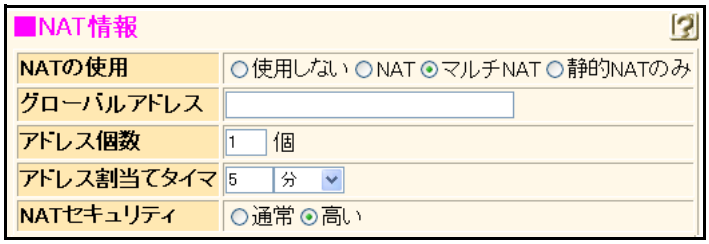
14.　［追加］ボタンをクリックします。

15.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

16.　以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→指定しない
- アドレス個数　→1
- アドレス割当てタイマ　→5 分
- NAT セキュリティ　→高い



こんな事に気をつけて

アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

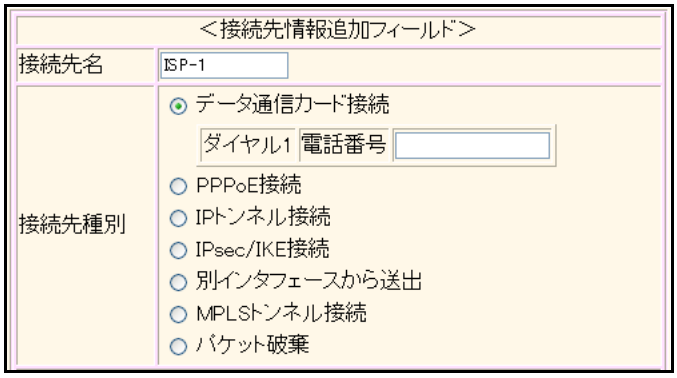
17.　［保存］ボタンをクリックします。

18.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

19.　以下の項目を指定します。

- 接続先名　　→ISP-1
- 接続先種別　　→データ通信カード接続
  電話番号　　→（通信事業者から提示された内容）



20.　［追加］ボタンをクリックします。

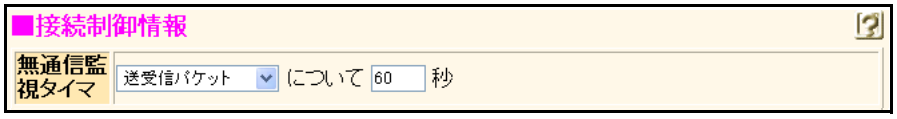
「接続先情報（ISP-1）」が表示されます。

21.　データ通信カード接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

22.　以下の項目を指定します。

- 無通信監視タイマ　　→送受信パケットについて 60 秒



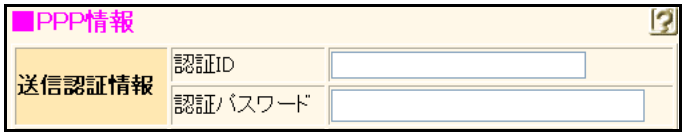
23.　［保存］ボタンをクリックします。

24.　データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

25.　以下の項目を指定します。

- 送信認証情報
  認証 ID　　→（通信事業者から提示された内容）
  認証パスワード　　→（通信事業者から提示された内容）



26.　［保存］ボタンをクリックします。

ProxyDNS 情報、URL フィルタ情報を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

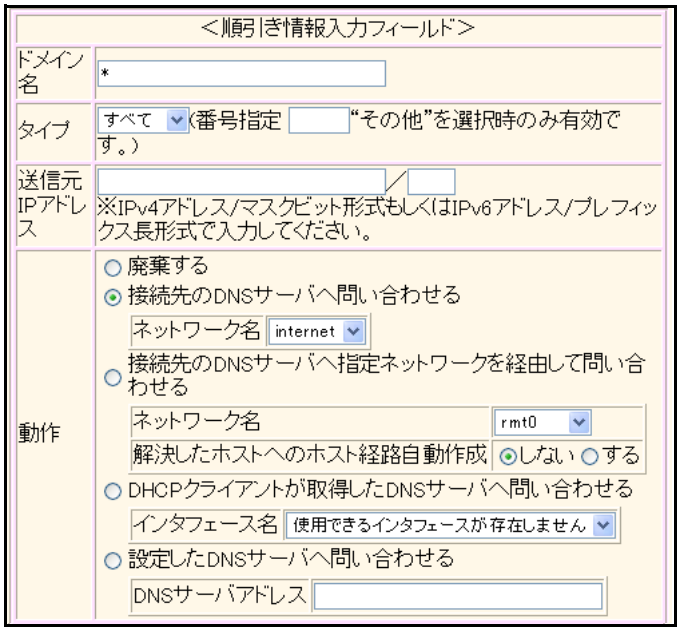
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→ *
- タイプ　→すべて
- 送信元 IP アドレス　→指定しない
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→ internet



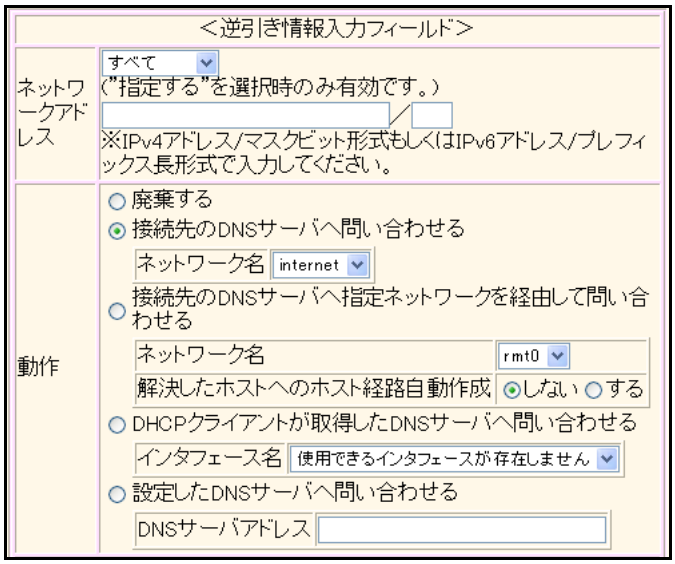
4.　［追加］ボタンをクリックします。

5.　「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

6.　以下の項目を指定します。

- ネットワークアドレス　→すべて
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→internet



7.　［追加］ボタンをクリックします。

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足　データ通信カードの認証 ID、認証パスワード、電話番号を以下に示します。
詳細については、各通信事業者にお問い合わせください。

通信事業者	認証 ID	認証パスワード	電話番号
ウィルコム PRIN つなぎ放題[PRO]	prin	prin	0570570711##64
NTT ドコモ mopera	（任意の文字列）	（任意の文字列）	*99***1#
au by KDDI au.NET	au@au-win.ne.jp	au	*99**24#
ソフトバンクモバイル （旧ボーダフォン） アクセスインターネット	vodafone@connect	vodafone	*99#

こんな事に気をつけて

無線 LAN インタフェース上では、以下の機能は利用できません。

- シェーピング
- 帯域制御（WFQ）
- ダイナミックルーティングプロトコル（IPv4 RIP、IPv6 RIP、BGP、IPv4 OSPF、IPv6 OSPF）
- MAC アドレス認証
- ARP 認証
- VLAN
- MPLS
- VRRP
- STP
- LAN ポートバックアップ
- LAN ポート閉塞

1.9　事業所 LAN を ISDN で接続する

適用機種　*Si-R220B,220C,370,570*

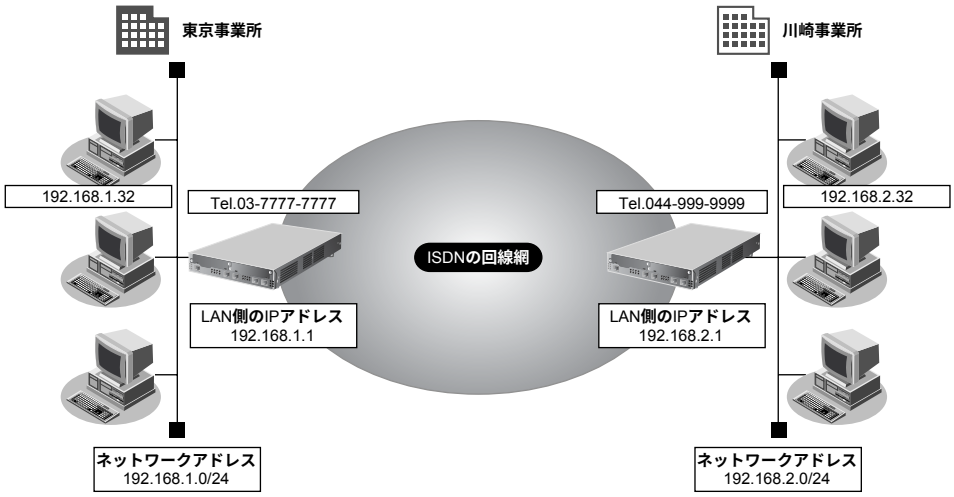
ここでは、ISDN 回線を介して 2 つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。

こんな事に気をつけて

- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。**

☛ 参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）

- **双方の事業所から同時に発信が行われた場合、両方の接続が成立することでその接続が超過課金（2 倍）になる場合があります。これは、接続優先制御機能を利用して片方の接続のみが存続するようにすることで防ぐことができます。この機能を利用する場合は、双方の事業所の装置で同じ接続優先設定を行わないでください。同時発信の際に接続ができなくなります。この機能を利用する場合は、以下の設定を奨励します。**
  - **一方の装置で着信接続を優先する。**
  - **一方の装置で接続優先制御を行わない。**



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）で ISDN 回線（64Kbps）を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名　：intranet
- 無通信監視時間を 1 分とする

[東京事業所]

- 本装置の IP アドレス/ネットマスク　：192.168.1.1/24
- 電話番号　：03-7777-7777
- ユーザ認証 ID とユーザ認証パスワード
  - 発信　：tokyo、tokyopass
  - 着信　：kawasaki、kawapass

[川崎事業所]

- 本装置の IP アドレス/ネットマスク　：192.168.2.1/24
- 電話番号　：044-999-9999

- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass

こんな事に気をつけて

本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

東京事業所を設定する

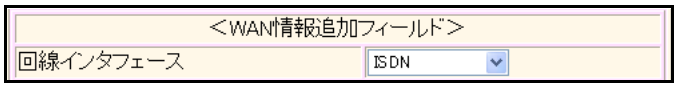
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→ISDN



3.　［追加］ボタンをクリックします。

「WAN0 情報（ISDN）」ページが表示されます。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

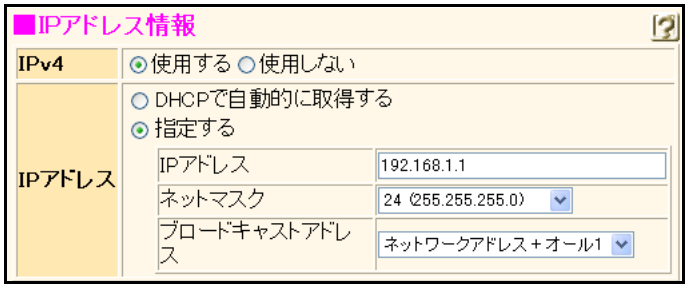
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→192.168.1.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

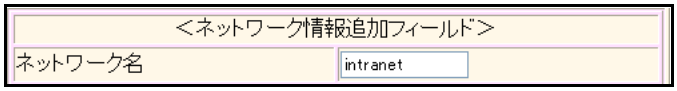
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→intranet



4.　［追加］ボタンをクリックします。

「ネットワーク情報（intranet)」ページが表示されます。

5.　「IP 関連」をクリックします。

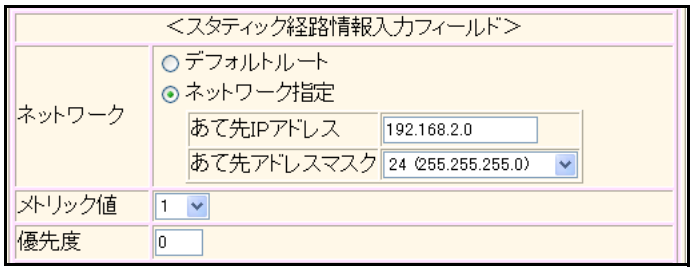
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



8.　［追加］ボタンをクリックします。

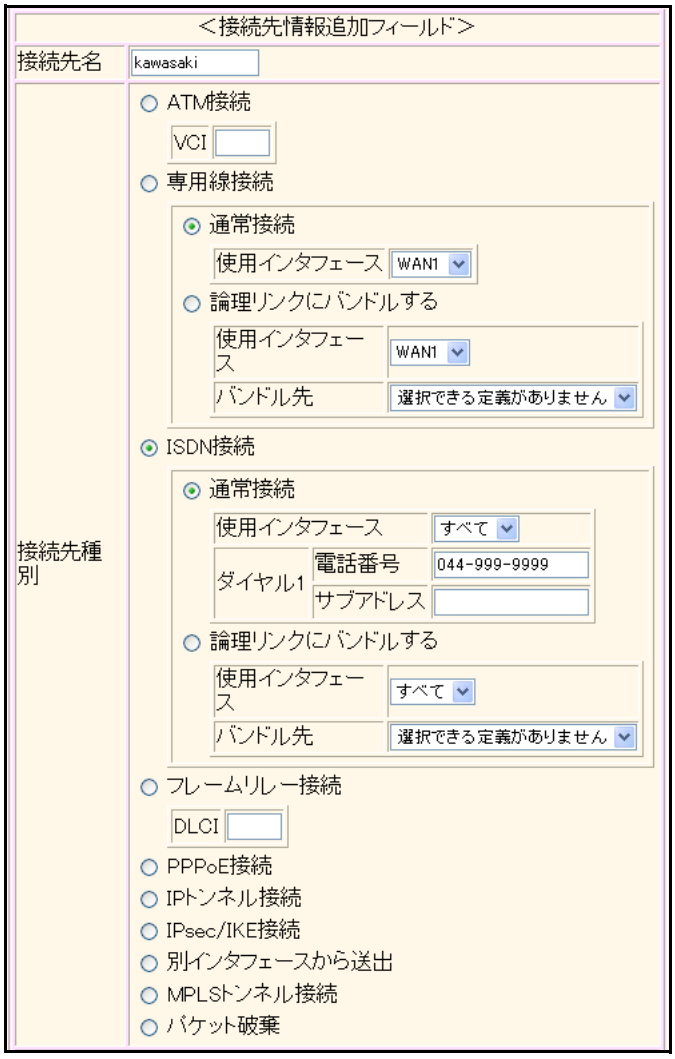
9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→kawasaki
- 接続先種別　→ISDN 接続
  →通常接続

  ダイヤル 1
  電話番号　→044-999-9999
  サブアドレス　→指定しない



機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

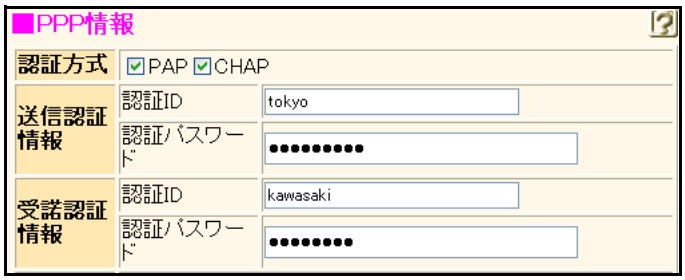
ISDN 接続の設定項目と「基本情報」が表示されます。

12.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

13.　以下の項目を指定します。

- 認証方式　→PAP、CHAP
- 送信認証情報
  認証 ID　→tokyo
  認証パスワード　→tokyopass
- 受諾認証情報
  認証 ID　→kawasaki
  認証パスワード　→kawapass



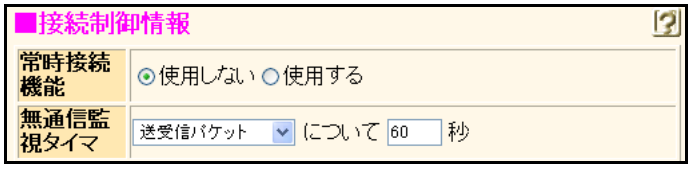
14.　［保存］ボタンをクリックします。

15.　ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

16.　以下の項目を指定します。

- 常時接続情報　→使用しない
- 無通信監視タイマ　→送受信パケットについて 60 秒



こんな事に気をつけて

双方の事業所から同時に発信が行われた場合、両方の接続が成立することでその接続が超過課金（2 倍）になる場合があります。これは、接続優先制御機能を利用して片方の接続のみが存続するようにすることで防ぐことができます。
この機能を利用する場合は、双方の事業所の装置で同じ接続優先設定を行わないでください。同時発信の際に接続ができなくなります。この機能を利用する場合は、以下の設定を奨励します。

- **一方の装置で着信接続を優先する。**
- **一方の装置で接続優先制御を行わない。**

17.　［保存］ボタンをクリックします。

18.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

川崎事業所を設定する

「東京事業所を設定する」を参考に、川崎事業所を設定します。

「WAN0 情報」

- 回線インタフェース　→ ISDN

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ intranet

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ tokyo
- 接続先種別　→ ISDN 接続
  →通常接続
  ダイヤル 1
  電話番号　→ 03-7777-7777
  サブアドレス　→指定しない

「接続先情報」-「ISDN 接続」

「PPP 情報」

- 認証方式　→ PAP、CHAP
- 送信認証情報
  認証 ID　→ kawasaki
  認証パスワード　→ kawapass
- 受諾認証情報
  認証 ID　→ tokyo
  認証パスワード　→ tokyopass

「接続制御情報」

- 常時接続情報　→使用しない
- 無通信監視タイマ　→送受信パケットについて 60 秒

1.10 事業所 LAN を専用線で接続する

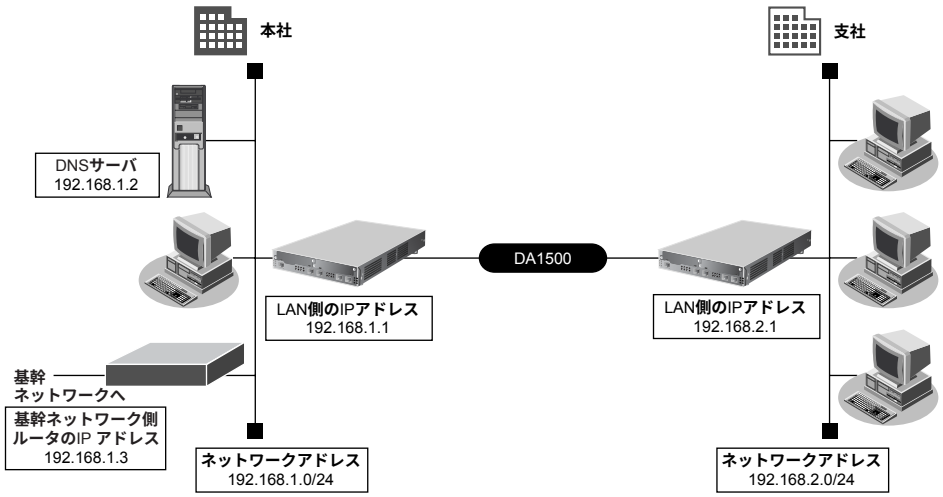
適用機種　*Si-R220B,220C,370,570*

ここでは、高速ディジタル専用線を介して 2 つの事業所（本社、支社）のネットワークを接続する場合について Si-R370 を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

- SLOT0 に実装された PRI 拡張モジュール L2 で専用線（1.5Mbps）を使用する
- DHCP サーバ機能は使用しない

[本社]

- 接続ネットワーク名　：honsya
- 接続先名　：honsya-1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- 本装置の LAN 側の IP アドレス　：192.168.1.1
- DNS サーバ　：192.168.1.2
- 基幹ネットワーク側ルータ IP アドレス　：192.168.1.3

[支社]

- 接続ネットワーク名　：shisya1
- 接続先名　：shisya-1
- ネットワークアドレス/ネットマスク　：192.168.2.0/24
- 本装置の LAN 側の IP アドレス　：192.168.2.1

補足　この例では、本社に DNS サーバが存在し、IP アドレスを固定にする必要があります。そのため、本社側では DHCP サーバ機能は使用しない条件にします。

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

本社を設定する

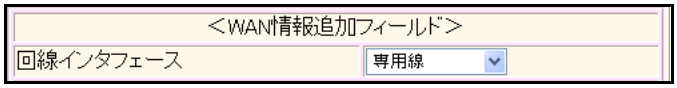
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→専用線



3.　［追加］ボタンをクリックします。

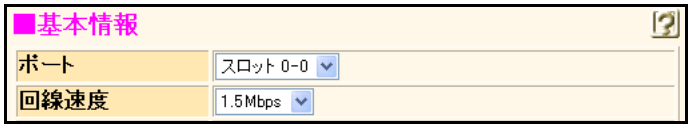
「WAN0 情報（専用線）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→ 1.5Mbps



Si-R220B、220C では、ポートは固定です。

6.　［保存］ボタンをクリックします。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

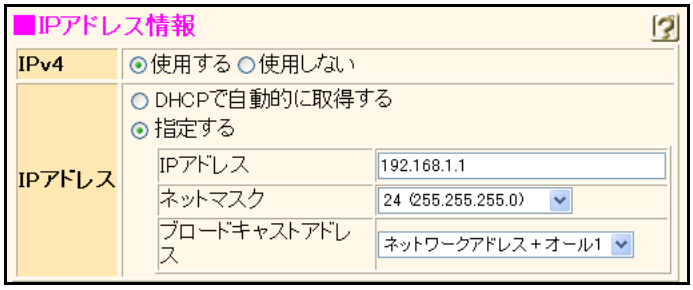
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.1.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1



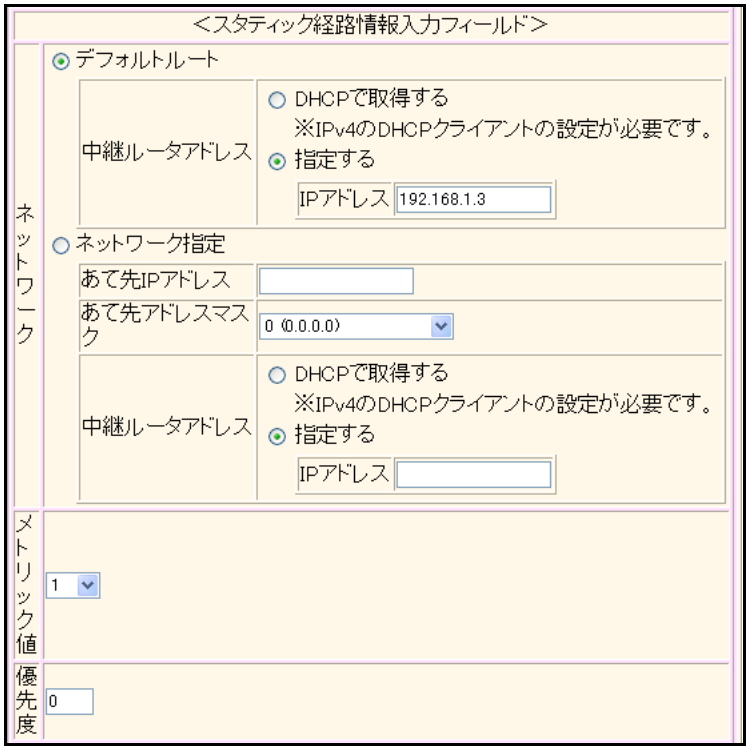
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
  中継ルータアドレス　→指定する
  IPアドレス　→192.168.1.3
- メトリック値　→1
- 優先度　→0



8.　［追加］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

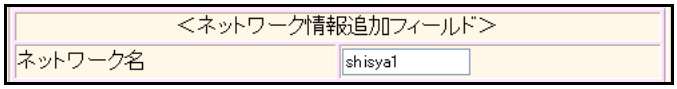
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→shisya1



4.　［追加］ボタンをクリックします。

「ネットワーク情報（shisya1）」ページが表示されます。

5.　「IP 関連」をクリックします。

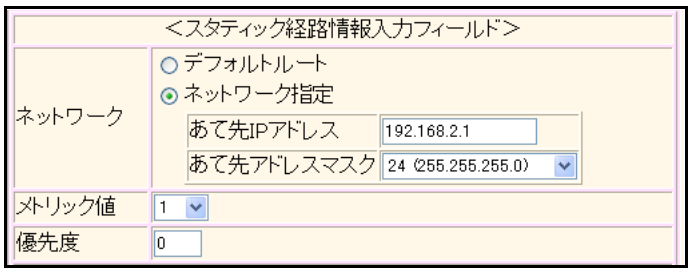
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.1
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



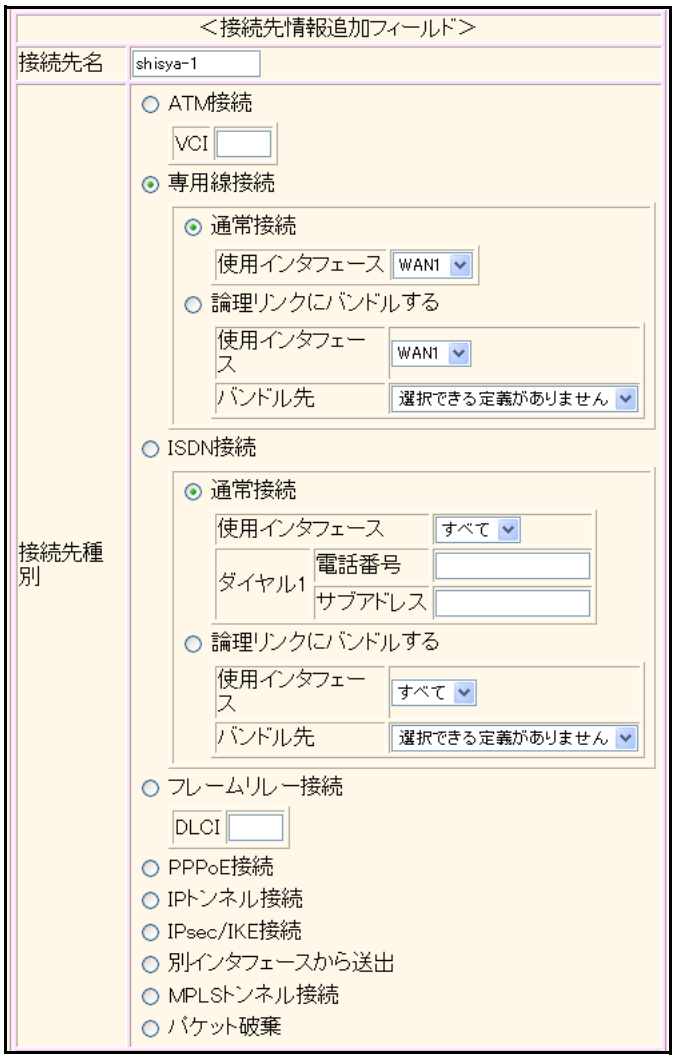
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisya-1
- 接続先種別　→専用線接続



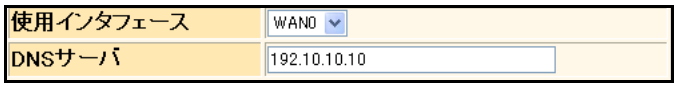
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- DNS サーバ　→192.10.10.10



13.　［保存］ボタンをクリックします。

14.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。

「WAN0 情報」

- 回線インタフェース　→専用線

「専用線」-「基本情報」

- ポート　→スロット 0-0
- 回線速度　→ 1.5Mbps

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「相手情報」-「ネットワーク情報」

- ネットワーク名　→honsya

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→デフォルトルート
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→honsya-1
- 接続先種別　→専用線接続

1.11 複数の事業所 LAN をフレームリレーで接続する

適用機種　*Si-R220B,220C,370,570*

ここでは、フレームリレーで複数の事業所を接続する場合を例に説明します。

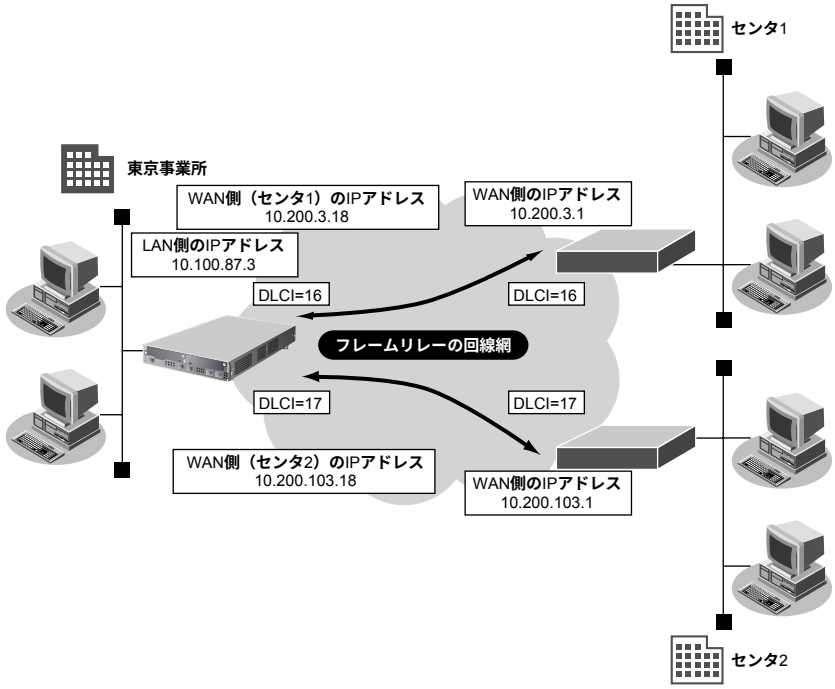
フレームリレーを利用すると複数の事業所の LAN と接続できるため、データを高速に転送することができます。

また、相手ごとに固定的な回線を接続するので、公衆網であるフレームリレー網に閉域ネットワークを構築することができ、セキュリティの確保にも適しています。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）でフレームリレー（128Kbps）を使用する
- RIPv1 を使用する
- 本装置の LAN 側の IP アドレス/ネットマスク　：10.100.87.3/24

[センタ 1 と接続する条件]

- ネットワーク名　：center1
- 接続先名　：ap1
- WAN の自側 IP アドレス　：10.200.3.18
- WAN の相手側 IP アドレス　：10.200.3.1
- DLCI　：16
- CIR　：64Kbps

[センタ 2 と接続する条件]

- ネットワーク名　：center2
- 接続先名　：ap2
- WAN の自側 IP アドレス　：10.200.103.18
- WAN の相手側 IP アドレス　：10.200.103.1
- DLCI　：17
- CIR　：64Kbps

こんな事に気をつけて

- **本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**
- **BRI4 ポート拡張モジュールは、フレームリレーに対応していません。**

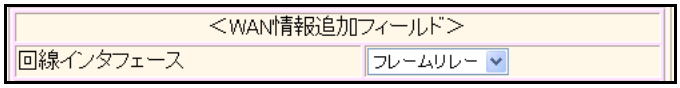
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→フレームリレー



3.　[追加] ボタンをクリックします。

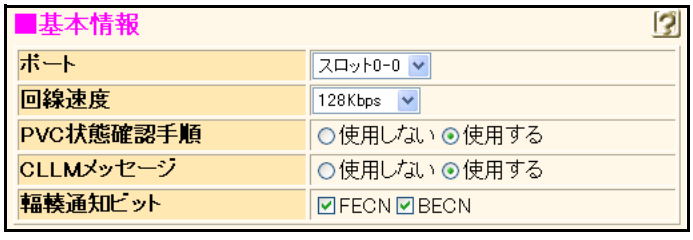
「WAN0 情報（フレームリレー）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→ 128Kbps
- PVC 状態確認手順　→使用する
- CLLM メッセージ　→使用する
- 輻輳通知ビット　→ FECN、BECN



6.　[保存] ボタンをクリックします。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

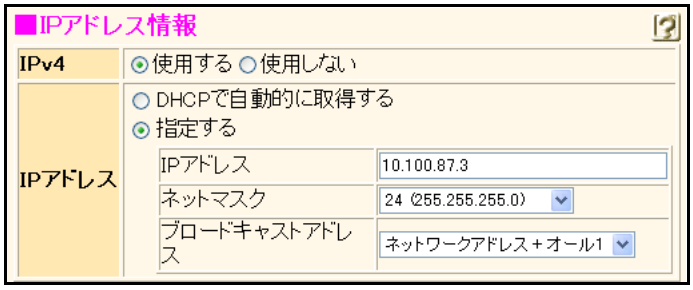
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.100.87.3
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



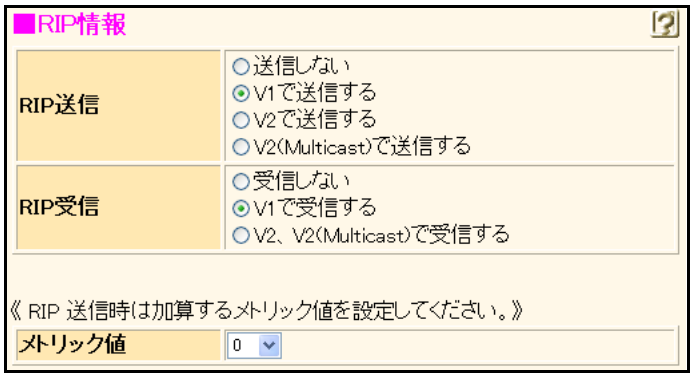
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→ V1 で送信する
- RIP 受信　→ V1 で受信する
- メトリック値　→ 0



8.　［保存］ボタンをクリックします。

接続先（センタ 1）の情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

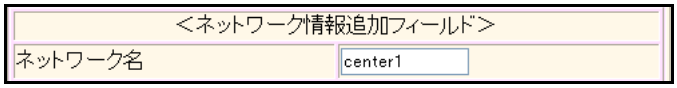
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→center1



4.　［追加］ボタンをクリックします。

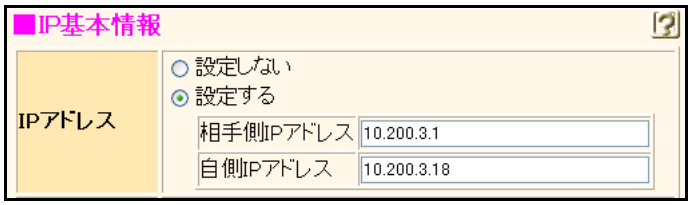
「ネットワーク情報（center1）」ページが表示されます。

5.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　以下の項目を指定します。

- IP アドレス　→設定する
  相手側 IP アドレス　→10.200.3.1
  自側 IP アドレス　→10.200.3.18



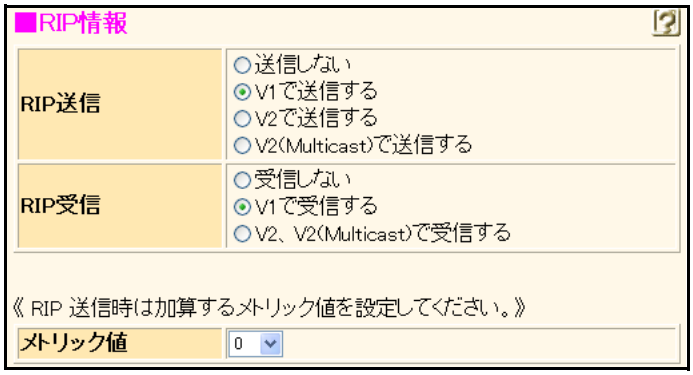
7.　［保存］ボタンをクリックします。

8.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

9.　以下の項目を指定します。

- RIP 送信　→V1 で送信する
- RIP 受信　→V1 で受信する
- メトリック値　→0



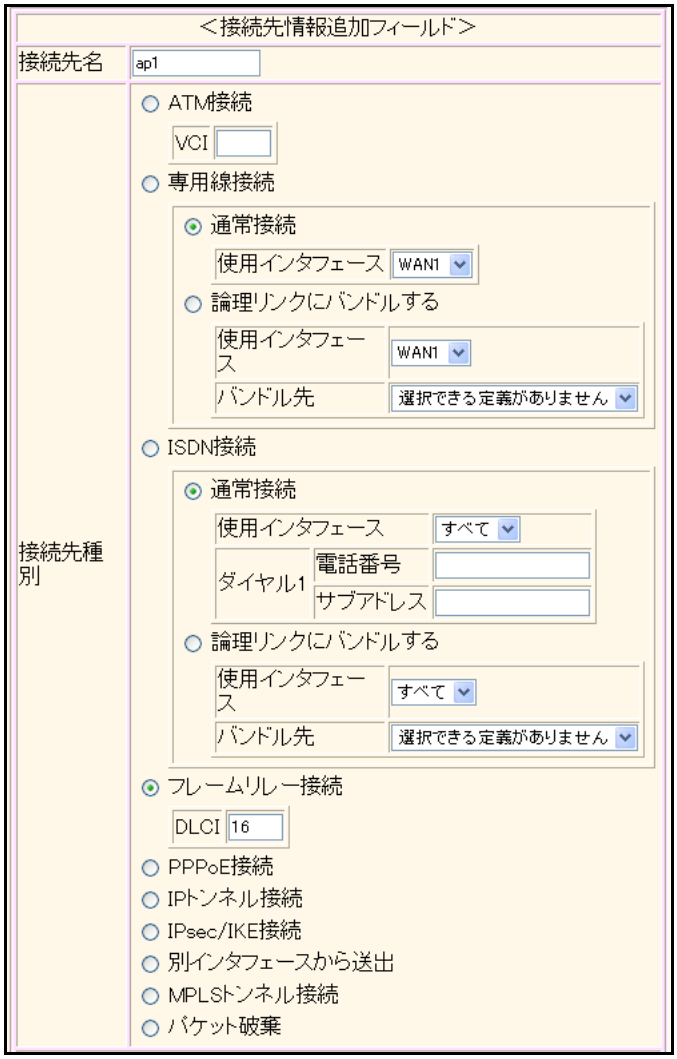
10.　［保存］ボタンをクリックします。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　→ap1
- 接続先種別　→フレームリレー接続
  DLCI　→16



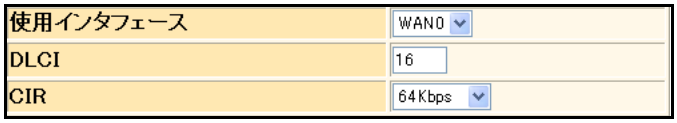
Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

フレームリレー接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- DLCI　→16
- CIR　→64Kbps



15.　［保存］ボタンをクリックします。

接続先（センタ 2）の情報を設定する

「接続先（センタ 1）の情報を設定する」を参考に、接続先（センタ 2）を設定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→center2

「ネットワーク情報」-「IP 関連」

「IP 基本情報」

- IP アドレス　→設定する
  相手側 IP アドレス　→10.200.103.1
  自側 IP アドレス　→10.200.103.18

「RIP 情報」

- RIP 送信　→V1 で送信する
- RIP 受信　→V1 で受信する
- メトリック値　→0

「接続先情報」

- 接続先名　→ap2
- 接続先種別　→フレームリレー接続
  DLCI　→17

「接続先情報」-「フレームリレー接続」

「基本情報」

- 使用インタフェース　→WAN0
- DLCI　→17
- CIR　→64Kbps

1.12 複数の事業所 LAN を ATM で接続する

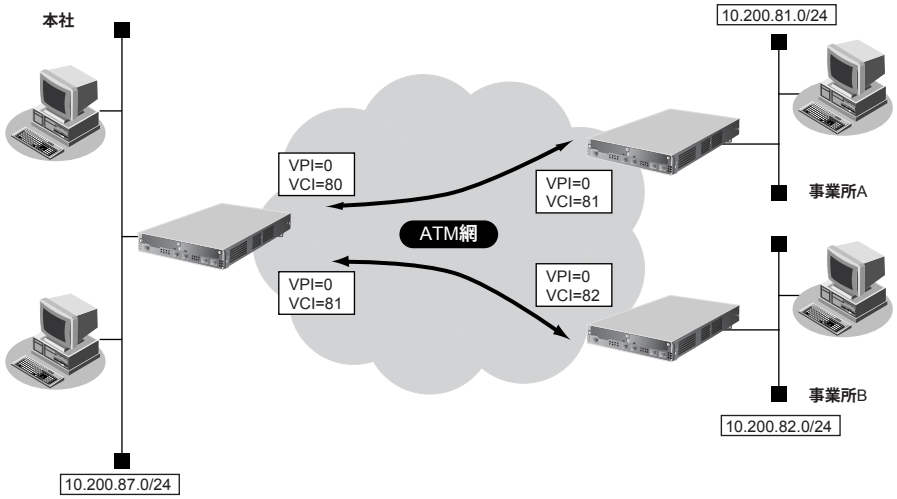
適用機種　*Si-R260B,370,570*

ここでは、ATM 網を利用して複数の事業所のネットワークを接続する場合を例に説明します。

こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：10.200.87.3/24
- 事業所 A 向け接続ネットワーク名　：JigyoA
- 事業所 A 向け接続先名　：jigyo-a
- 事業所 A 向け VPI/VCI　：0/80
- 事業所 A 向けサービスクラス　：CBR（VC 速度：6Mbps）
- 事業所 B 向け接続ネットワーク名　：JigyoB
- 事業所 B 向け接続先名　：jigyo-b
- 事業所 B 向け VPI/VCI　：0/81
- 事業所 B 向けサービスクラス　：CBR（VC 速度：4Mbps）

[事業所 A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：10.200.81.1/24
- 接続ネットワーク名　：Honsya
- 接続先名　：honsya-1

- VPI/VCI　：0/81
- サービスタイプ　：CBR（VC 速度：6Mbps）

[事業所 B]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：10.200.82.1/24
- 接続ネットワーク名　：Honsya
- 接続先名　：honsya-2
- VPI/VCI　：0/82
- サービスタイプ　：CBR（VC 速度：4Mbps）

こんな事に気をつけて

本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

本社を設定する

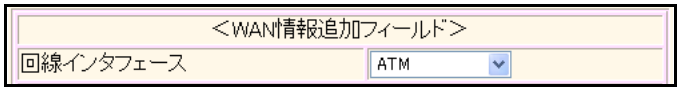
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→ATM



3.　[追加] ボタンをクリックします。

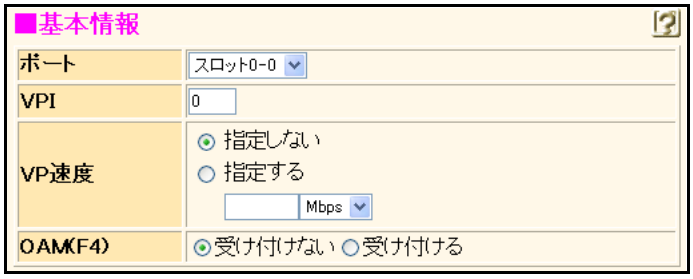
「WAN0 情報（ATM）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- VPI　→0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない



6.　[保存] ボタンをクリックします。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

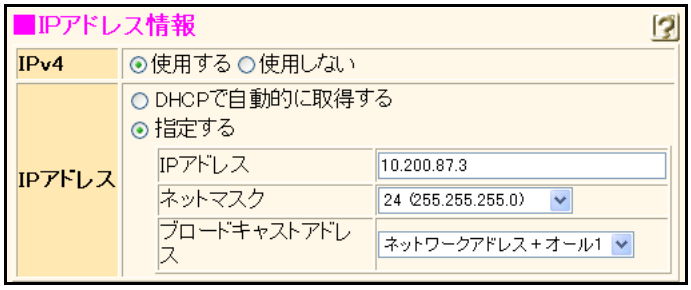
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.200.87.3
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

事業所 A 向けの相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

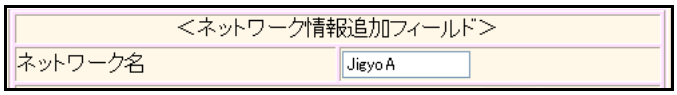
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→ JigyoA



4.　［追加］ボタンをクリックします。

「ネットワーク情報（JigyoA）」ページが表示されます。

5.　「IP 関連」をクリックします。

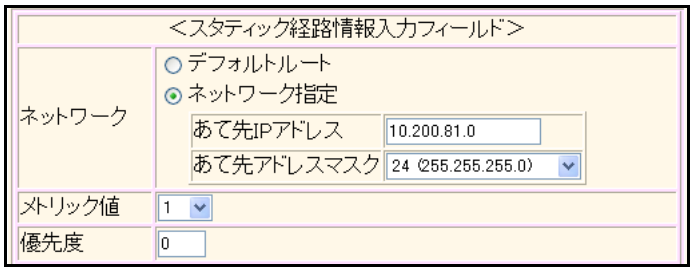
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.200.81.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



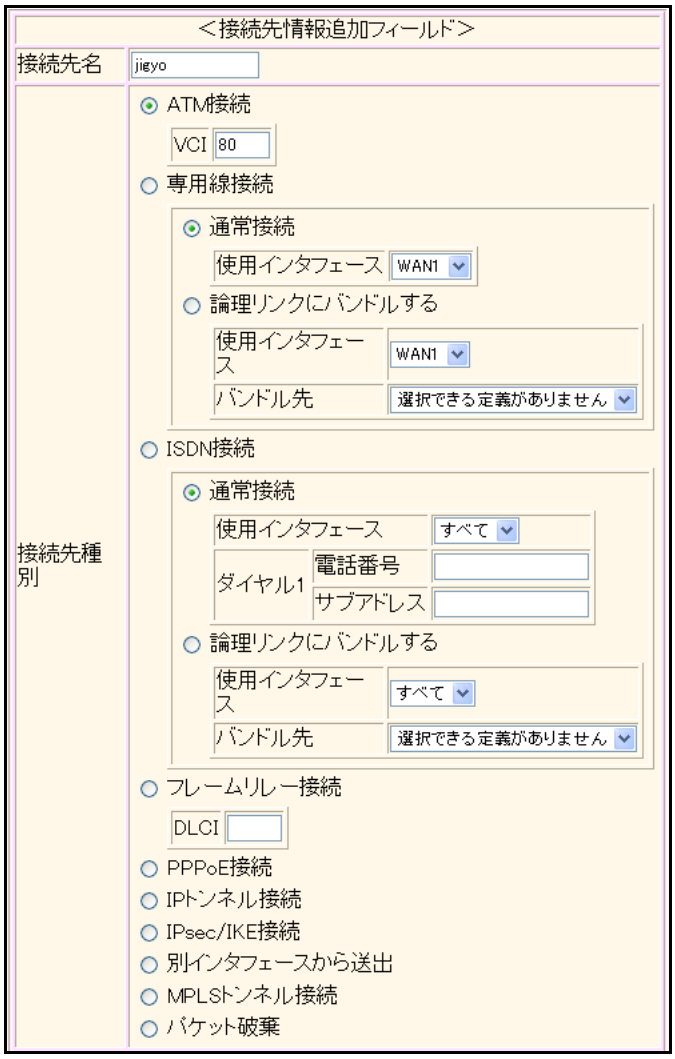
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→jigyo-a
- 接続先種別　→ATM 接続
  VCI　→80



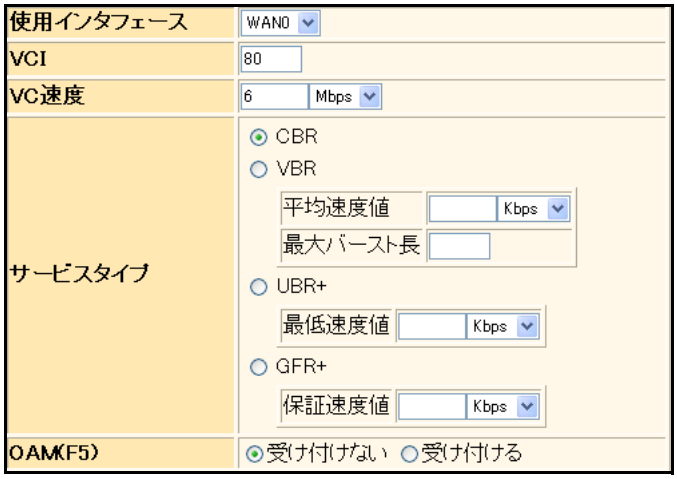
Si-R260B では、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

ATM 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- VCI　→80
- VC 速度　→6Mbps
- サービスタイプ　→CBR
- OAM（F5）　→受け付けない



13.　［保存］ボタンをクリックします。

事業所 B 向けの相手情報を設定する

1.　画面上部の「相手情報」をクリックします。

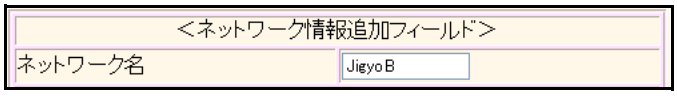
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→JigyoB



4.　［追加］ボタンをクリックします。

「ネットワーク情報（JigyoB）」ページが表示されます。

5.　「IP 関連」をクリックします。

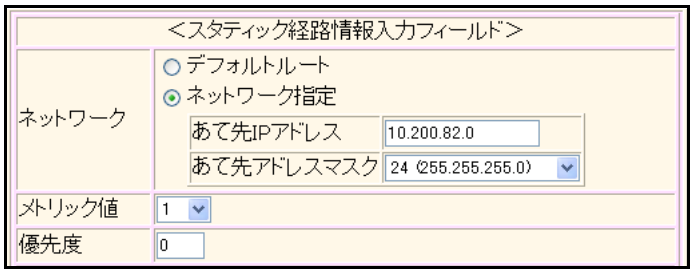
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.200.82.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



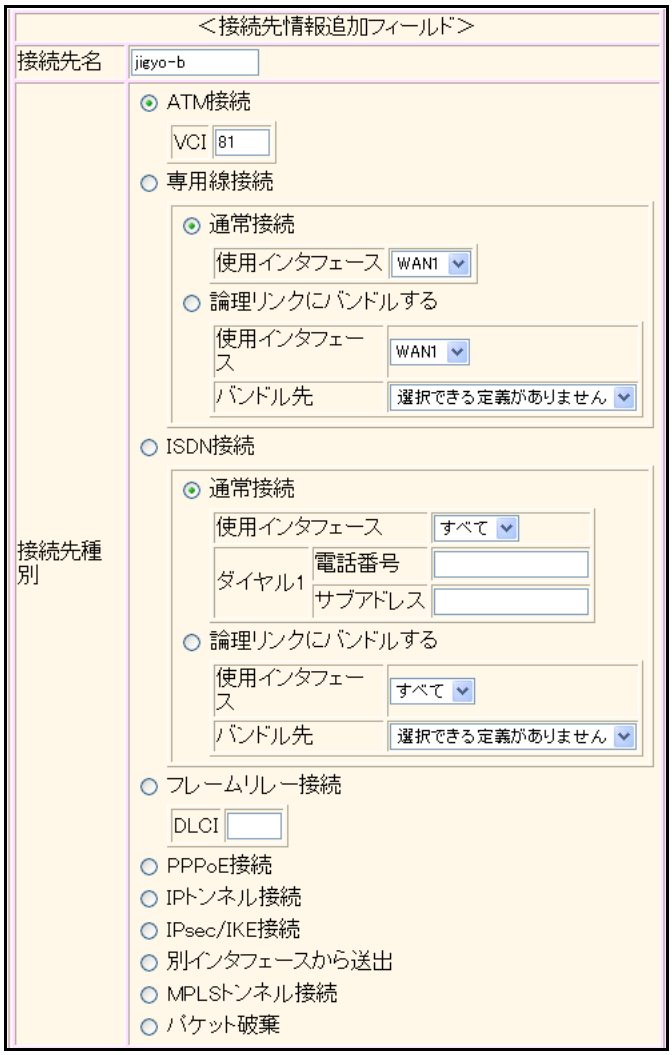
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→jigyo-b
- 接続先種別　→ATM 接続
  VCI　→81



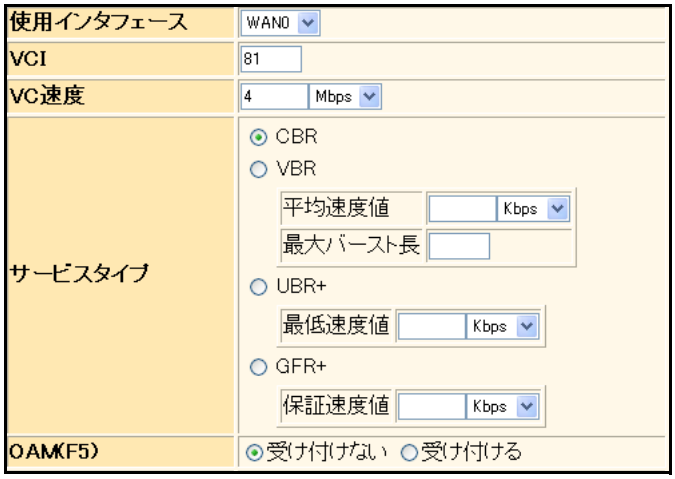
Si-R260B では、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

ATM 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- VCI　→81
- VC 速度　→4Mbps
- サービスタイプ　→CBR
- OAM（F5）　→受け付けない



13.　［保存］ボタンをクリックします。

14.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

使用する拡張モジュールによって、以下の点に注意して設定してください。Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M ／ ATM155M 拡張モジュール L2	• VP ／ VC 速度を設定する場合は、64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 - 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 • VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 • VP シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が VP 速度を超えないようにように設定してください。 • VC シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が 25Mbps を超えないようにように設定してください。

拡張モジュール	注意点
ATM25M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - 64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 25Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。
ATM155M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - VP 速度は、200Kbps ～ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 - VC 速度は、64Kbps ～ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 50Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VPC 内の VC 速度の最高速度は 50Mbps になります。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。 `atm <slot> send clock recovery`

事務所 A を設定する

「本社を設定する」を参考に、事業所 A を設定します。

「WAN0 情報」-「ATM」

「基本情報」

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.200.81.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ Honsya

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→デフォルトルート
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ honsya-1
- 接続先種別　→ ATM 接続
  VCI　→ 81

「接続先情報」-「ATM 接続」

「基本情報」

- 使用インタフェース　→ WAN0
- VCI　→ 81
- VC 速度　→ 6Mbps
- サービスタイプ　→ CBR
- OAM（F5）　→受け付けない

事務所 B を設定する

「本社を設定する」を参考に、事業所 B を設定します。

「WAN0 情報」-「ATM」

「基本情報」

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.200.82.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ Honsya

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→デフォルトルート
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ honsya-2
- 接続先種別　→ ATM 接続
  VCI　→ 82

「接続先情報」-「ATM 接続」

「基本情報」

- 使用インタフェース　→ WAN0
- VCI　→ 82
- VC 速度　→ 4Mbps
- サービスタイプ　→ CBR
- OAM（F5）　→受け付けない

1.13　複数の事業所 LAN を IP-VPN 網を利用して接続する

適用機種　全機種

ここでは、プロトコル BGP4 を使用して、IP-VPN 網で複数の事業所を接続する場合の設定方法を説明します。

こんな事に気をつけて

- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。**

  ☛参照　Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）

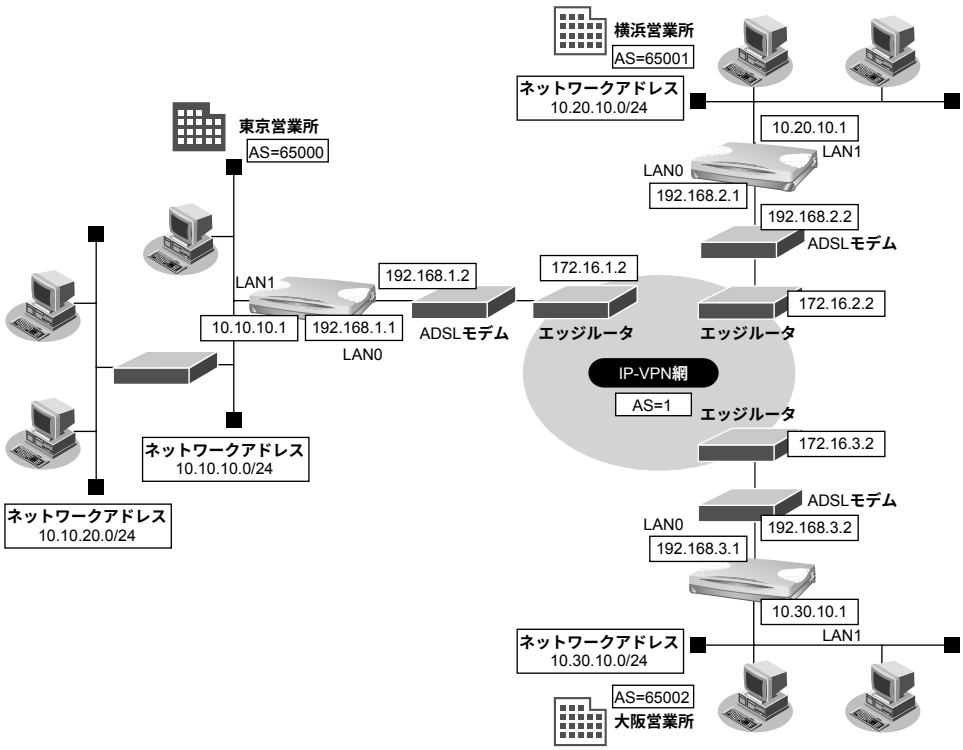
- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  ☛参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- NAT 機能と併用することはできません。
- バージョン 4 だけをサポートしています。
- 本装置のグレースフルリスタート機能のサポート範囲は、以下のとおりです。
  - レシーブルータ機能のみ（リスタート機能は、サポートしていません。）
  - アドレスファミリは IPv4 のみ
- 相手情報で BGP を使用する場合は、IP アドレスを設定してください。
- 経路情報を最大値まで保持している状態では、受信した BGP パケットは破棄されます。破棄した BGP パケットの経路情報は、その後、経路情報に空きができた場合でも反映されません。
- BGP 使用中に［設定反映］ボタンをクリックした場合、接続中のセッションが一度切断されることがあります。

1.13.1　ADSL モデムを使用して IP-VPN 網と接続する

適用機種　全機種



● 設定条件

- LAN0 ポートを ADSL モデムに接続する

[IP-VPN 網]

- 東京営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。また、グレースフルリスタートを使用する。
- 横浜営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 大阪営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 東京営業所向け IP アドレス　：172.16.1.2
- 横浜営業所向け IP アドレス　：172.16.2.2
- 大阪営業所向け IP アドレス　：172.16.3.2
- AS 番号　：1

[東京営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.1.1
- LAN0 側ネットワークアドレス/ネットマスク　：192.168.1.0/24
- LAN1 側 IP アドレス　：10.10.10.1
- LAN1 側ネットワークアドレス/ネットマスク　：10.10.10.0/24
- AS 番号　：65000
- BGP グレースフルリスタート　：使用する
- 営業所内のルーティングプロトコル　：RIPv2

[横浜営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.2.1
- LAN0 側ネットワークアドレス/ネットマスク　：192.168.2.0/24
- LAN1 側 IP アドレス　：10.20.10.1
- LAN1 側ネットワークアドレス/ネットマスク　：10.20.10.0/24
- AS 番号　：65001
- BGP グレースフルリスタート　：使用しない

[大阪営業所]

- IP-VPN 網側ポート　：LAN0
- LAN0 側 IP アドレス　：192.168.3.1
- LAN0 側ネットワークアドレス/ネットマスク　：192.168.3.0/24
- LAN1 側 IP アドレス　：10.30.10.1
- LAN1 側ネットワークアドレス/ネットマスク　：10.30.10.0/24
- AS 番号　：65002
- BGP グレースフルリスタート　：使用しない

東京営業所を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

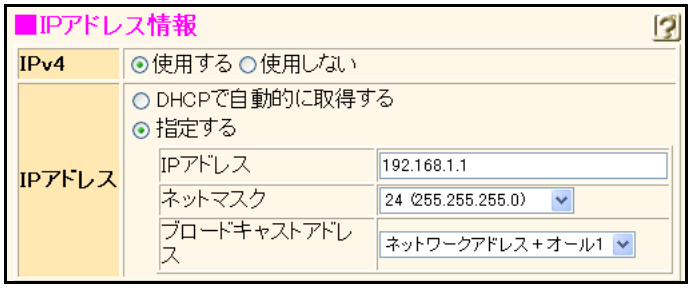
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



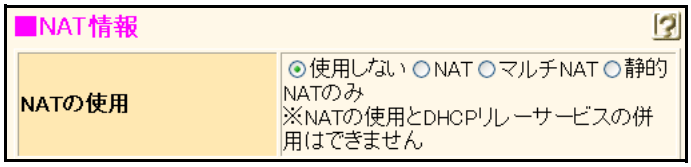
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

7.　以下の項目を指定します。

- NAT の使用　→使用しない



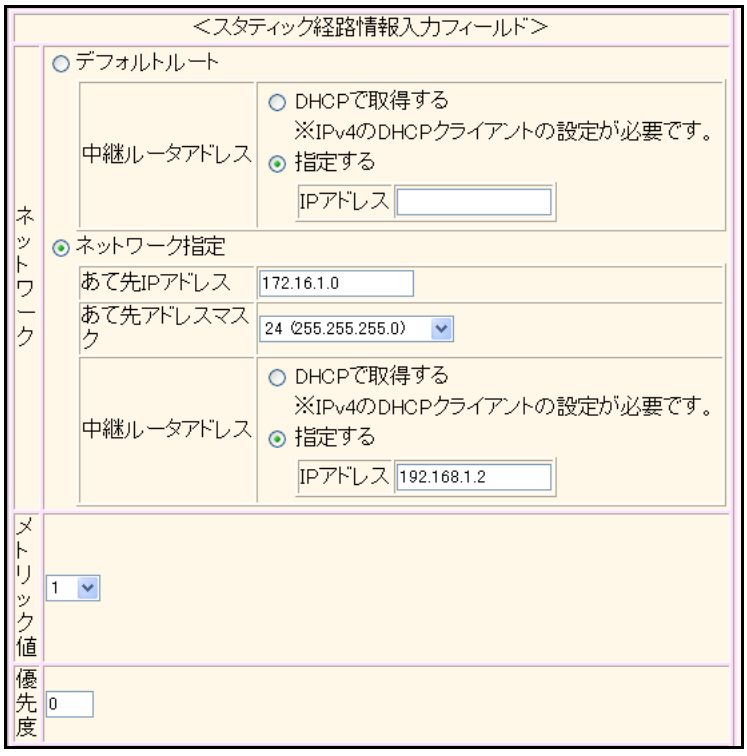
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

10.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 172.16.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→指定する
  IP アドレス　→ 192.168.1.2
- メトリック値　→ 1
- 優先度　→ 0



11.　［追加］ボタンをクリックします。

LAN1 情報を設定する

こんな事に気をつけて

Si-R180、180B 以外の装置で「LAN1 情報を設定する」場合は、あらかじめ物理 LAN1 定義を追加する必要があります。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

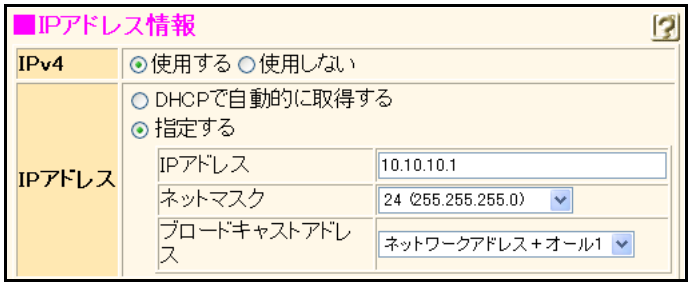
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.10.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



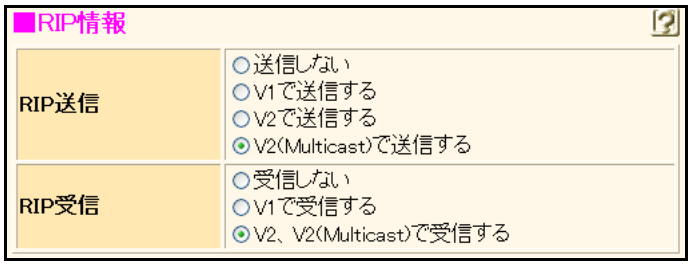
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→ V2（Multicast）で送信する
- RIP 受信　→ V2、V2（Multicast）で受信する



8.　［保存］ボタンをクリックします。

ルーティングプロトコル情報を設定する

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

2.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

3.　以下の項目を指定します。

- RIP
  BGP 経路情報　→再配布する
- BGP
  RIP 経路情報　→再配布する

■再配布情報

RIP	インタフェース経路情報	○再配布しない ◉再配布する
	スタティック経路情報	○再配布しない ◉再配布する
	BGP経路情報	○再配布しない ◉再配布する メトリック値: 0
	OSPF経路情報	◉再配布しない ○再配布する メトリック値: 0
	DNS経路情報	◉再配布しない ○再配布する メトリック値: 0
BGP	インタフェース経路情報	◉再配布しない ○再配布する
	スタティック経路情報	◉再配布しない ○再配布する
	RIP経路情報	○再配布しない ◉再配布する
	OSPF経路情報	◉再配布しない ○再配布する
	DNS経路情報	◉再配布しない ○再配布する

4.　［保存］ボタンをクリックします。

5.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

6.　以下の項目を指定します。

- BGP 機能　→使用する
- 自 AS 番号　→65000

■BGP情報

BGP機能	○使用しない ◉使用する
自AS番号	65000

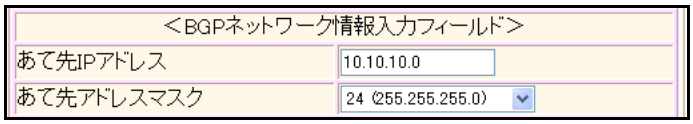
7.　［保存］ボタンをクリックします。

8.　BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。

「BGP ネットワーク情報」が表示されます。

9.　以下の項目を指定します。

- あて先 IP アドレス　→ 10.10.10.0
- あて先アドレスマスク　→ 24（255.255.255.0）



10.　［追加］ボタンをクリックします。

11.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

12.　［追加］ボタンをクリックします。

BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。

13.　以下の項目を指定します。

- 相手側 IP アドレス　→ 172.16.1.2
- 相手 AS 番号　→ 1
- EBGP MULTIHOP　→ 2

必要に応じて上記以外の項目を指定します。

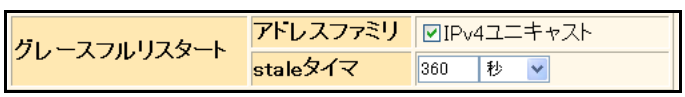
14.　［保存］ボタンをクリックします。

15.　「BGP 拡張機能情報」をクリックします。

「BGP 拡張機能情報」が表示されます。

16.　以下の項目を指定します。

- グレースフルリスタート
  アドレスファミリ　→ IPv4 ユニキャスト



17.　［保存］ボタンをクリックします。

18.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

横浜営業所を設定する

「東京営業所を設定する」を参考に、横浜営業所を設定します。

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「NAT 情報」

- NATの使用　→使用しない

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先IPアドレス　→ 172.16.2.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→指定する
  IPアドレス　→ 192.168.2.2
- メトリック値　→ 1
- 優先度　→ 0

「LAN1 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→ 10.20.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→ 65001

「BGP ネットワーク情報」

- あて先IPアドレス　→ 10.20.10.0
- あて先アドレスマスク　→ 24（255.255.255.0）

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側IPアドレス　→ 172.16.2.2
- 相手 AS 番号　→ 1
- EBGP MULTIHOP　→ 2

大阪営業所を設定する

「東京営業所を設定する」を参考に、大阪営業所を設定します。

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→ 192.168.3.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「NAT 情報」

- NATの使用　→使用しない

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先IPアドレス　→ 172.16.3.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→指定する
  IPアドレス　→ 192.168.3.2
- メトリック値　→ 1
- 優先度　→ 0

「LAN1 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→ 10.30.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→ 65002

「BGP ネットワーク情報」

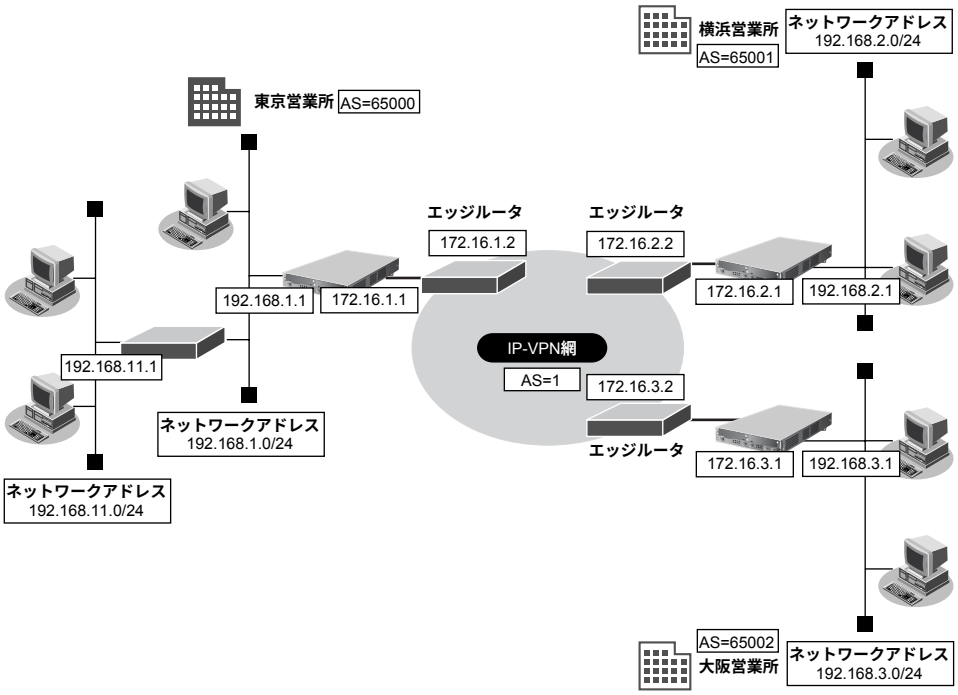
- あて先IPアドレス　→ 10.30.10.0
- あて先アドレスマスク　→ 24（255.255.255.0）

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側IPアドレス　→ 172.16.3.2
- 相手 AS 番号　→ 1
- EBGP MULTIHOP　→ 2

1.13.2　高速ディジタル専用線を使用して IP-VPN 網と接続する

適用機種　***Si-R220B,220C,370,570***



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）で専用線に接続する

[IP-VPN 網]

- 東京営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。また、グレースフルリスタートを使用する。
- 横浜営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 大阪営業所との経路交換に BGP を使用し、IPv4 ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 東京営業所向け IP アドレス　：172.16.1.2
- 横浜営業所向け IP アドレス　：172.16.2.2
- 大阪営業所向け IP アドレス　：172.16.3.2
- AS 番号　：1

[東京営業所]

- LAN 側の IP アドレス　：192.168.1.1
- LAN 側のネットワークアドレス/ネットマスク　：192.168.1.0/24
- サブ LAN 側のネットワークアドレス/ネットマスク　：192.168.11.0/24
- サブ LAN 側のルーティングプロトコル　：RIPv2
- WAN 側の IP アドレス　：172.16.1.1
- AS 番号　：65000
- BGP グレースフルリスタート　：使用する

[横浜営業所]

- LAN 側の IP アドレス　：192.168.2.1
- LAN 側のネットワークアドレス/ネットマスク　：192.168.2.0/24
- WAN 側の IP アドレス　：172.16.2.1
- AS 番号　：65001
- BGP グレースフルリスタート　：使用しない

[大阪営業所]

- LAN 側の IP アドレス　：192.168.3.1
- LAN 側のネットワークアドレス/ネットマスク　：192.168.3.0/24
- WAN 側の IP アドレス　：172.16.3.1
- AS 番号　：65002
- BGP グレースフルリスタート　：使用しない

東京営業所を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

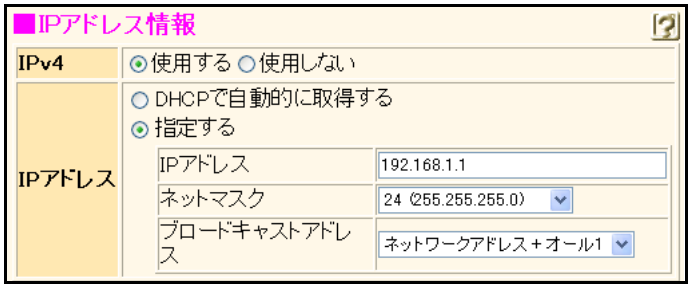
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



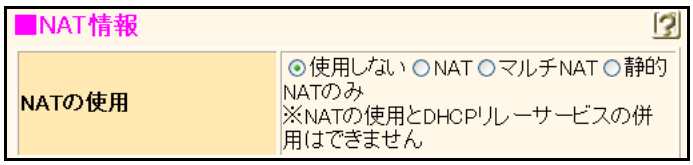
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

7.　以下の項目を指定します。

- NATの使用　→使用しない



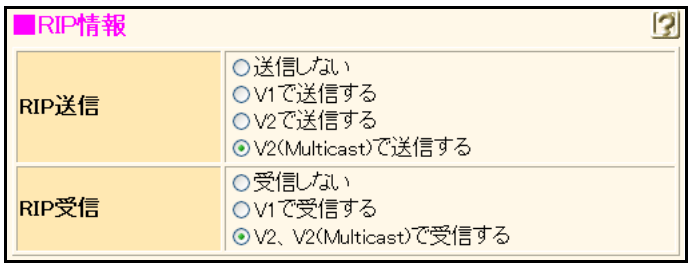
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

10.　以下の項目を指定します。

- RIP送信　→V2（Multicast）で送信する
- RIP受信　→V2、V2（Multicast）で受信する



11.　［保存］ボタンをクリックします。

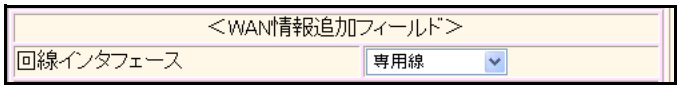
IP-VPN 網と接続する相手情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→専用線



3.　［追加］ボタンをクリックします。

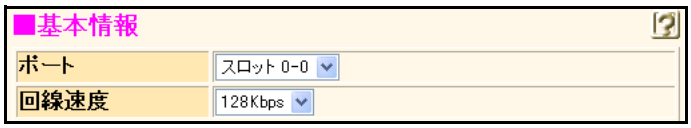
「WAN0 情報（専用線）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→128Kbps



Si-R220B、220C では、ポートは固定です。

6.　［保存］ボタンをクリックします。

7.　設定メニューのルータ設定で「相手情報」をクリックします。

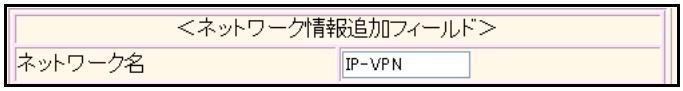
「相手情報」ページが表示されます。

8.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク名　　→IP-VPN



10.　［追加］ボタンをクリックします。

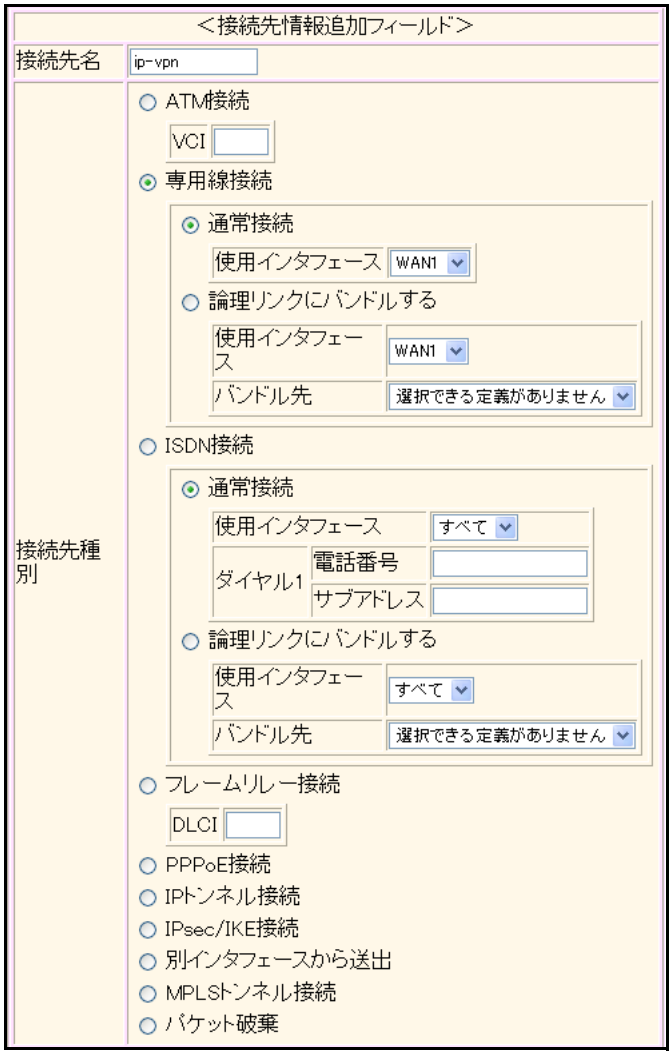
「ネットワーク情報（IP-VPN)」ページが表示されます。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　　→ip-vpn
- 接続先種別　　→専用線接続



Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 使用インタフェース　→WAN0

15.　［保存］ボタンをクリックします。

16.　画面上部の「ネットワーク情報（IP-VPN）」をクリックします。

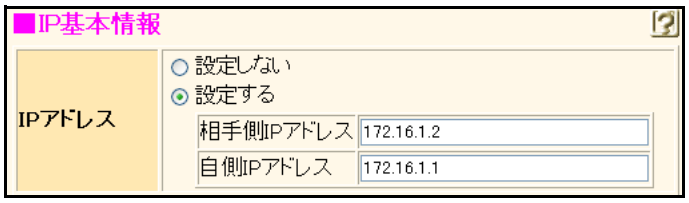
「ネットワーク情報（IP-VPN）」が表示されます。

17.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

18.　以下の項目を指定します。

- IP アドレス　→設定する
  相手側 IP アドレス　→172.16.1.2
  自側 IP アドレス　→172.16.1.1



19.　［保存］ボタンをクリックします。

ルーティングプロトコル情報を設定する

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

2.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

3.　以下の項目を指定します。

- RIP
  BGP 経路情報　→再配布する
- BGP
  RIP 経路情報　→再配布する

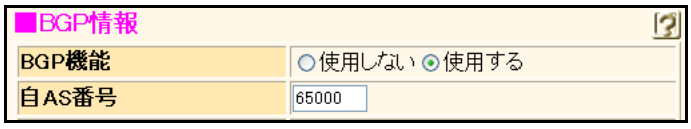
4.　［保存］ボタンをクリックします。

5.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

6.　以下の項目を指定します。

- BGP 機能　→使用する
- 自 AS 番号　→65000



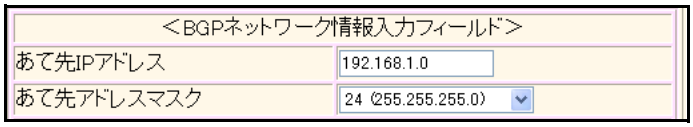
7.　［保存］ボタンをクリックします。

8.　BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。

「BGP ネットワーク情報」が表示されます。

9.　以下の項目を指定します。

- あて先 IP アドレス　→192.168.1.0
- あて先アドレスマスク　→24（255.255.255.0）



10.　［追加］ボタンをクリックします。

11.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

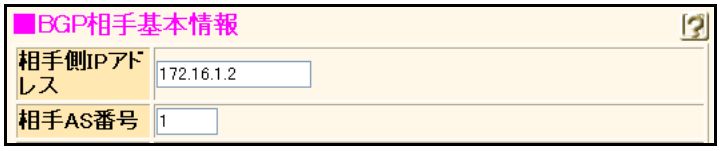
「BGP 相手情報」が表示されます。

12.　［追加］ボタンをクリックします。

BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。

13.　以下の項目を指定します。

- 相手側 IP アドレス　→ 172.16.1.2
- 相手 AS 番号　→ 1



必要に応じて上記以外の項目を指定します。

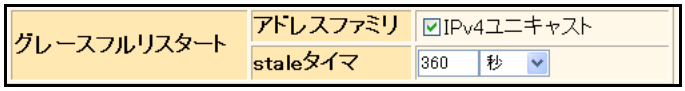
14.　［保存］ボタンをクリックします。

15.　「BGP 拡張機能情報」をクリックします。

「BGP 拡張機能情報」が表示されます。

16.　以下の項目を指定します。

- グレースフルリスタート
  アドレスファミリ　→ IPv4 ユニキャスト



17.　［保存］ボタンをクリックします。

18.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

横浜営業所を設定する

「東京営業所を設定する」を参考に、横浜営業所を設定します。

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「NAT 情報」

- NAT の使用　→使用しない

「WAN0 情報」

- 回線インタフェース　→専用線
- ポート　→スロット 0-0
- 回線速度　→ 128Kbps

「相手情報」-「ネットワーク情報」

- ネットワーク名　→IP-VPN

「接続先情報」

- 接続先名　→ip-vpn
- 接続先種別　→専用線接続

「接続先情報」-「専用線接続」

「基本情報」

- 使用インタフェース　→WAN0

「ネットワーク情報」-「IP 関連」

「IP 基本情報」

- IPアドレス　→設定する
  相手側 IPアドレス　→172.16.2.2
  自側 IPアドレス　→172.16.2.1

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→65001

「BGP ネットワーク情報」

- あて先 IPアドレス　→192.168.2.0
- あて先アドレスマスク　→24（255.255.255.0）

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側 IPアドレス　→172.16.2.2
- 相手 AS 番号　→1

大阪営業所を設定する

「東京営業所を設定する」を参考に、大阪営業所を設定します。

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.3.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「NAT 情報」

- NATの使用　→使用しない

「WAN0 情報」

- 回線インタフェース　→専用線
- ポート　→スロット 0-0
- 回線速度　→128Kbps

「相手情報」-「ネットワーク情報」

- ネットワーク名　→IP-VPN

「接続先情報」

- 接続先名　→ip-vpn
- 接続先種別　→専用線接続

「接続先情報」-「専用線接続」

「基本情報」

- 使用インタフェース　→WAN0

「ネットワーク情報」-「IP 関連」

「IP 基本情報」

- IP アドレス　→設定する
  相手側 IP アドレス　→172.16.3.2
  自側 IP アドレス　→172.16.3.1

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→65002

「BGP ネットワーク情報」

- あて先 IP アドレス　→192.168.3.0
- あて先アドレスマスク　→24（255.255.255.0）

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側 IP アドレス　→172.16.3.2
- 相手 AS 番号　→1

⚠注意

- **BGP4 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、BGP4 機能を使用しないでください。**
- **BGP セッションで使用する WAN インタフェースのインタフェース経路（ホストルート）を BGP で広報した場合、BGP セッションの接続・切断を繰り返す場合があります。該当するインタフェース経路は BGP で広報しないように設定してください。該当しないインタフェース経路を BGP で広報する場合は、以下のどちらかを設定してください。**
- **BGP にインタフェース経路を再配布しないで、広報するインタフェース経路を BGP ネットワークとして設定します。**
- **BGP にインタフェース経路を再配布し、該当するインタフェース経路を BGP フィルタリングで送信を破棄するように設定します。**

1.14 複数の事業所 LAN を VPN（IPsec）で接続する

適用機種　全機種

ここでは、プロトコル VPN（IPsec）を使用して、複数の事業所を接続する場合の設定方法を説明します。

1.14.1 NAT を併用しない固定 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

IPsec 機能を使って自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 A（PPPoE 常時接続）]

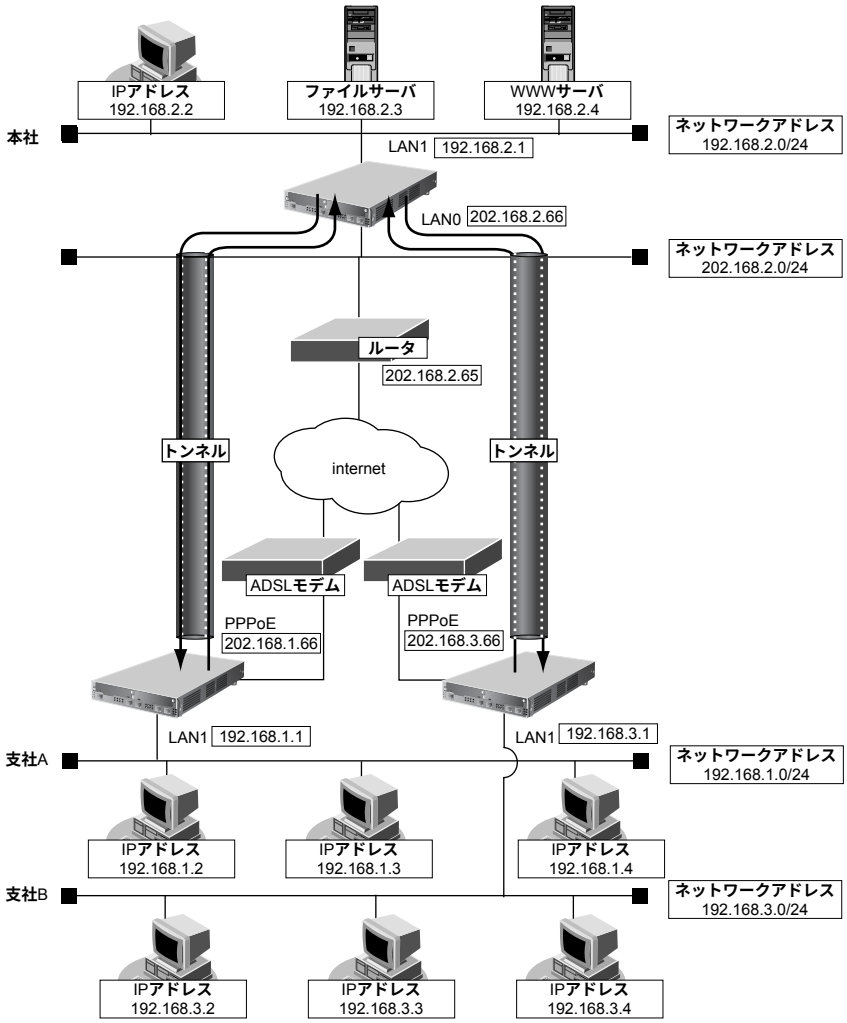
- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[支社 B（PPPoE 常時接続）]

- ローカルネットワーク IP アドレス　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.3.66/24
- PPPoE ユーザ認証 ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65



● 設定条件

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66 - 202.168.2.66
- IPsec 対象範囲　：192.168.1.0/24-any4

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.3.66 - 202.168.2.66
- IPsec 対象範囲　：192.168.3.0/24-any4

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 202.168.1.66
- IPsec 対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB

- IPsec/IKE 区間　：202.168.2.66 - 202.168.3.66
- IPsec 対象範囲　：any4-192.168.3.0/24

[共通 A]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[共通 B]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社 A の IPsec/IKE を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

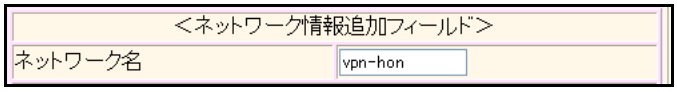
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

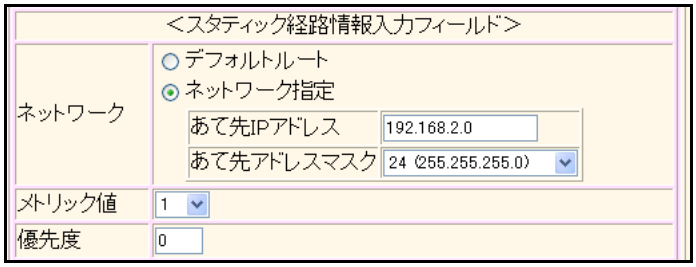
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



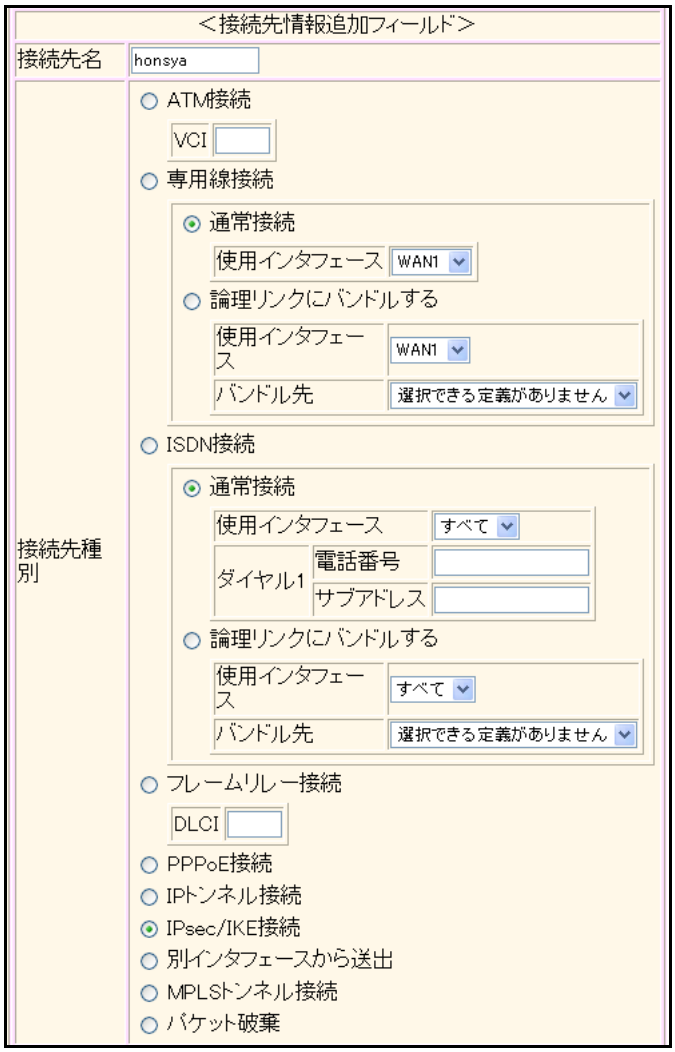
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66

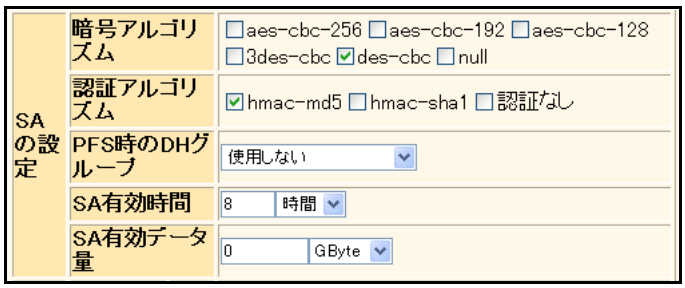
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



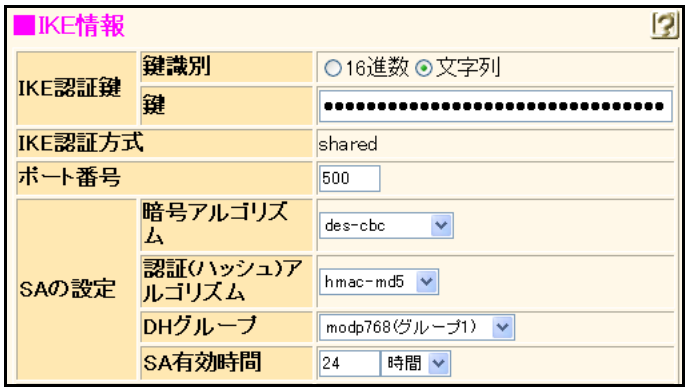
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B の IPsec/IKE を設定する

「支社 A の IPsec/IKE を設定する」を参考に、支社 B を設定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-hon

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.3.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0

「接続先情報」

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.3.66

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証アルゴリズム　→hmac-sha1

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp1024

本社の IPsec/IKE を設定する

支社 A 向けの設定をする

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shiA

4.　［追加］ボタンをクリックします。

「ネットワーク情報（ vpn-shiA)」ページが表示されます。

5.　「IP 関連」をクリックします。

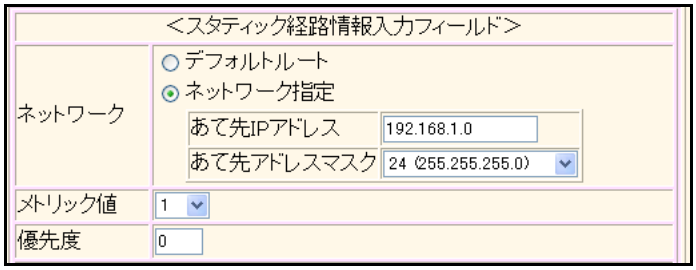
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



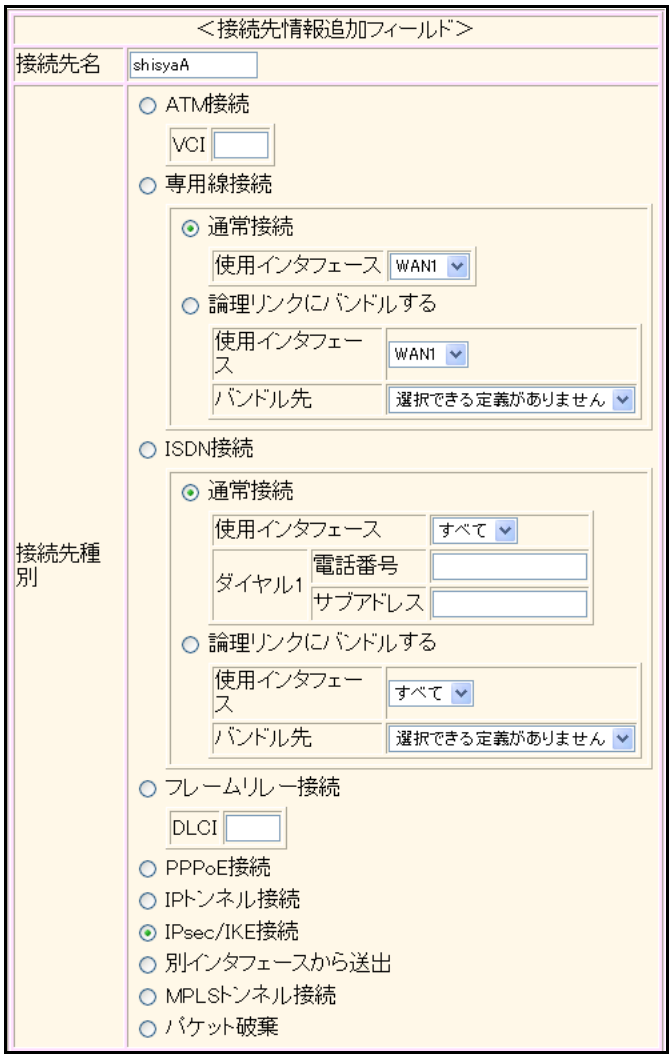
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisyaA
- 接続先種別　→IPsec/IKE 接続



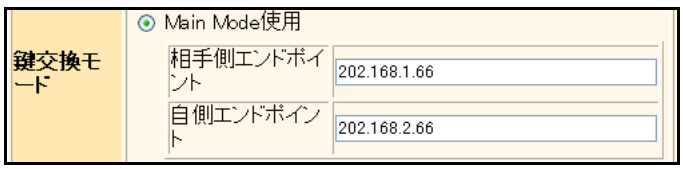
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.1.66
  自側エンドポイント　→202.168.2.66



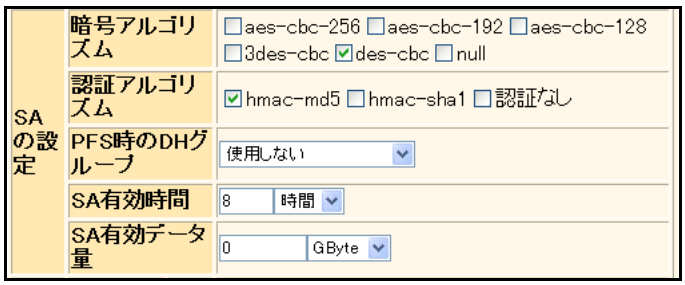
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



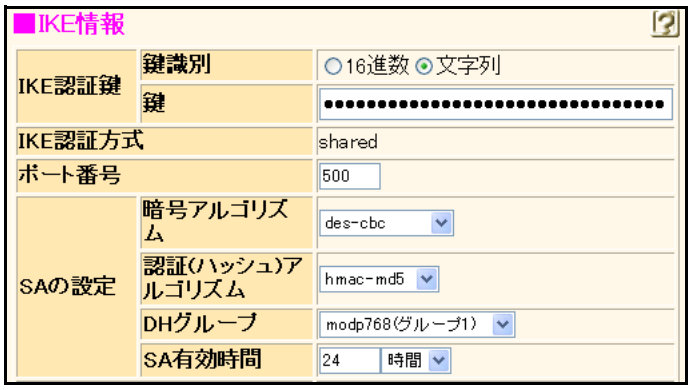
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B 向けの設定をする

「支社 A 向けを設定する」を参考に、支社 B 向けを設定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-shiB

「ネットワーク情報 -「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.3.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0

「接続先情報」

- 接続先名　→shisyaB
- 接続先種別　→IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.3.66
  自側エンドポイント　→202.168.2.66

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証アルゴリズム　→hmac-sha1

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp1024

1.14.2　NAT と併用した固定 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

IPsec 機能を使って自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 A]

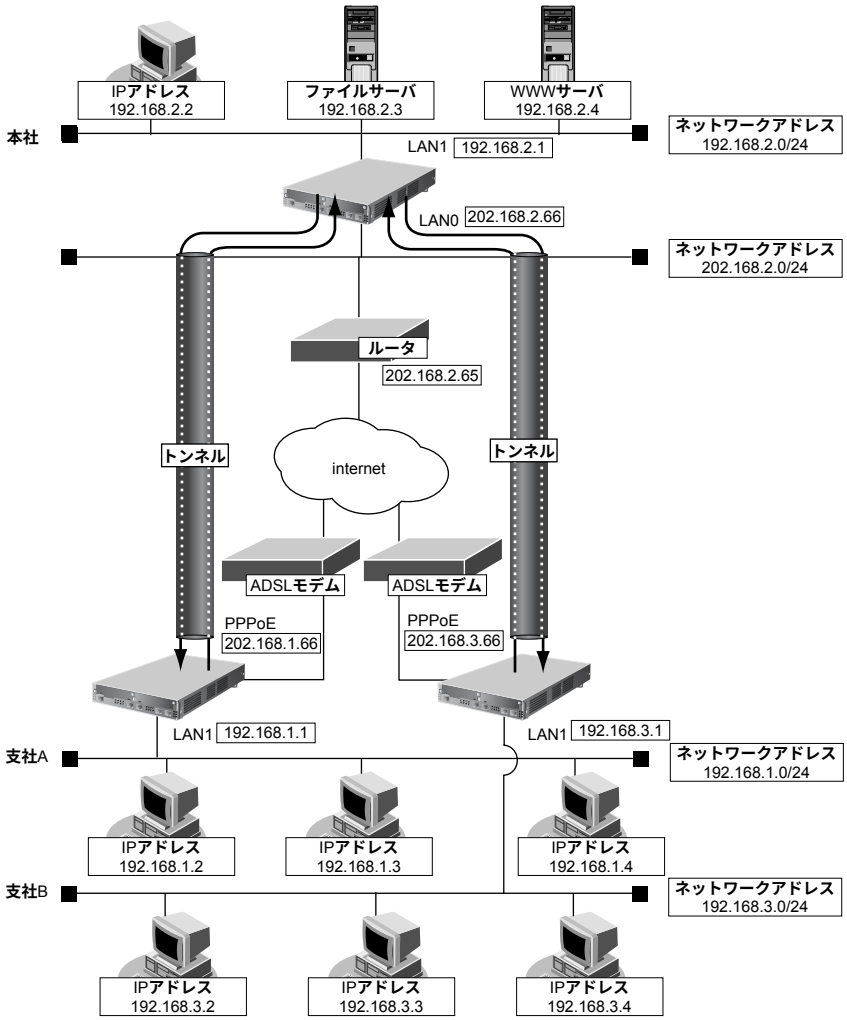
- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- グローバルネットワーク IP アドレス　：10.0.1.1/24
- PPPoE ユーザ認証 ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[支社 B]

- ローカルネットワーク IP アドレス　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.3.66/24
- グローバルネットワーク IP アドレス　：10.0.3.1/24
- PPPoE ユーザ認証 ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65



● 設定条件

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：10.0.1.1 - 202.168.2.66
- IPsec 対象範囲　：192.168.1.0/24-any4

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：10.0.3.1 - 202.168.2.66
- IPsec 対象範囲　：192.168.3.0/24-any4

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 10.0.1.1
- IPsec 対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB

- IPsec/IKE 区間　：202.168.2.66 - 10.0.3.1
- IPsec 対象範囲　：any4-192.168.3.0/24

[共通 A]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[共通 B]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社 A を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（ internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

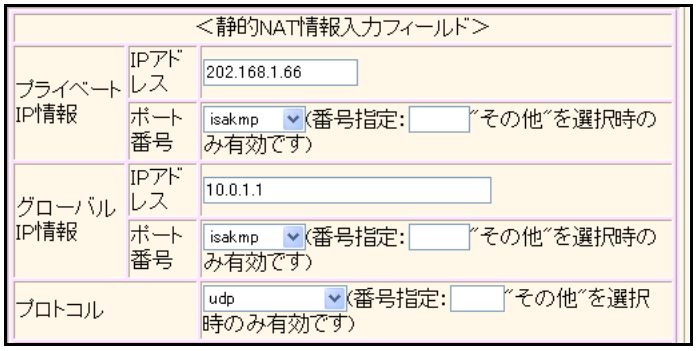
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 202.168.1.66
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→ 10.0.1.1
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6. ～ 7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 202.168.1.66
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→ 10.0.1.1
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

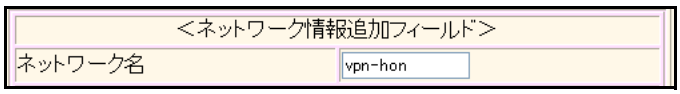
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



12.　［追加］ボタンをクリックします。

「ネットワーク情報（ vpn-hon)」ページが表示されます。

13.　「IP 関連」をクリックします。

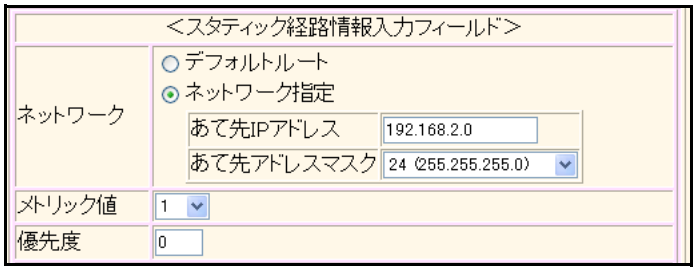
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



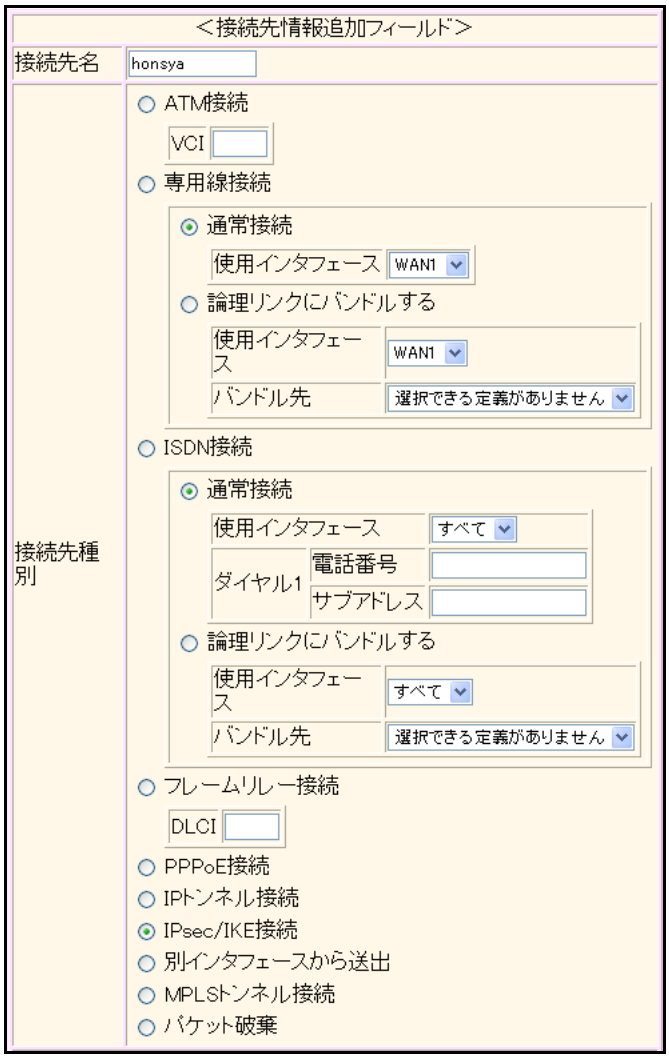
16.　［追加］ボタンをクリックします。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



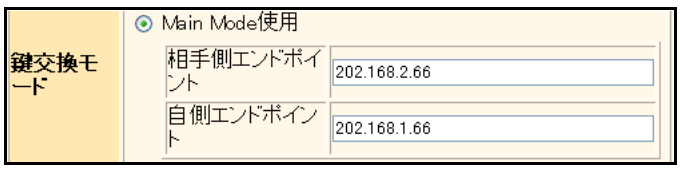
機種により、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66



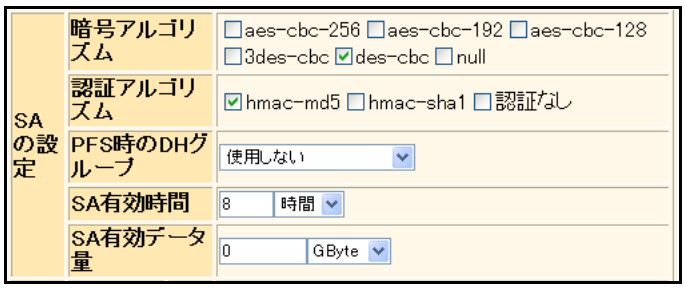
21.　［保存］ボタンをクリックします。

22.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

23.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



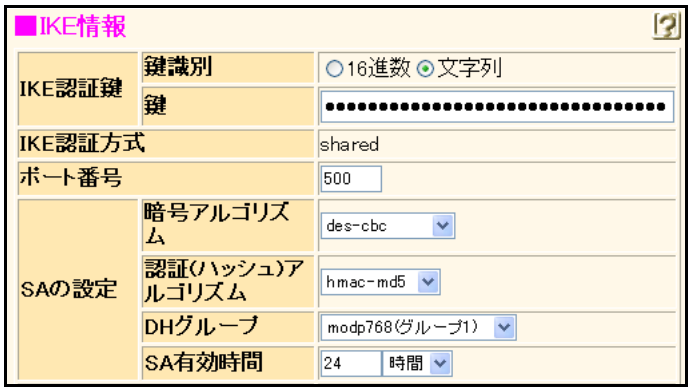
24.　［保存］ボタンをクリックします。

25.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

26.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



27.　［保存］ボタンをクリックします。

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B を設定する

「支社 A を設定する」を参考に、支社 B を設定します。

「相手情報」-「ネットワーク情報」

「ネットワーク情報」-「IP 関連」

「静的 NAT 情報」

- プライベート IP 情報
  IP アドレス　→ 202.168.3.66
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→ 10.0.3.1
  ポート番号　→ isakmp
- プロトコル　→ udp
- プライベート IP 情報
  IP アドレス　→ 202.168.3.66
  ポート番号　→ すべて
- グローバル IP 情報
  IP アドレス　→ 10.0.3.1
  ポート番号　→ すべて
- プロトコル　→ esp

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ vpn-hon

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（ 255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ honshya
- 接続先種別　→ IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→ Main Mode 使用
  相手側エンドポイント　→ 202.168.2.66
  自側エンドポイント　→ 202.168.3.66

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→ 3des-cbc
  認証アルゴリズム　→ hmac-sha1

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp1024

本社の IPsec/IKE を設定する

支社 A 向けの設定をする

1.　設定メニューのルータ設定で「相手情報」をクリックします。

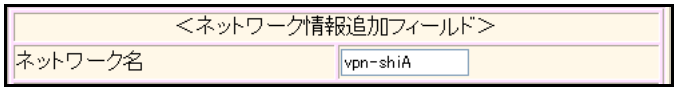
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shiA



4.　［追加］ボタンをクリックします。

「ネットワーク情報（ vpn-shiA)」ページが表示されます。

5.　「IP 関連」をクリックします。

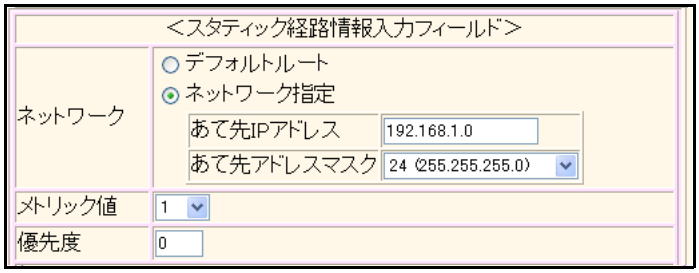
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



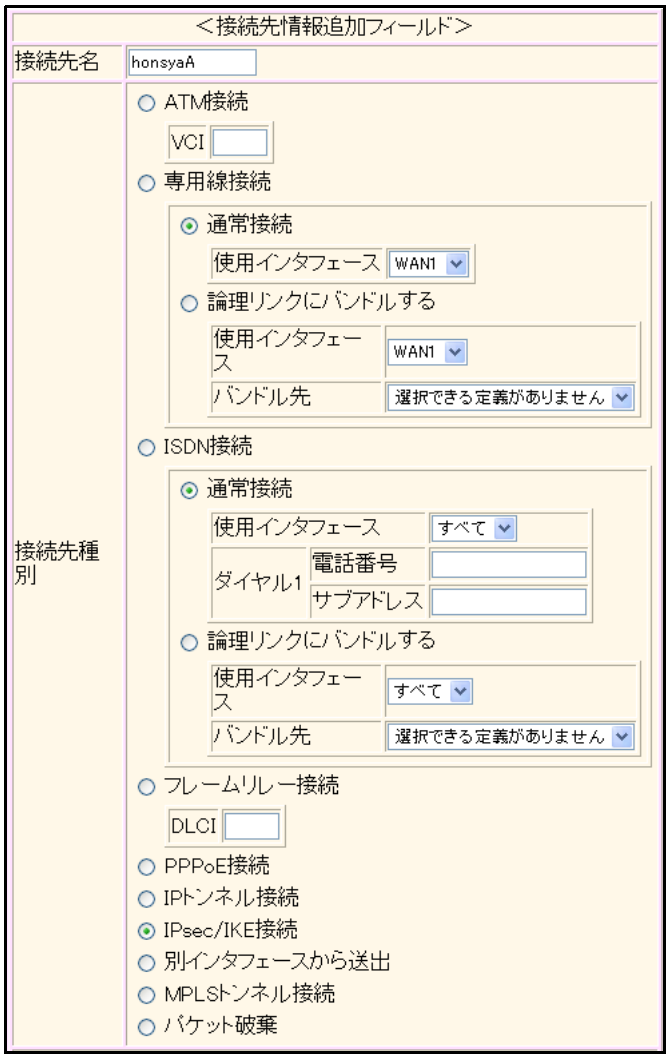
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisyaA
- 接続先種別　→IPsec/IKE 接続



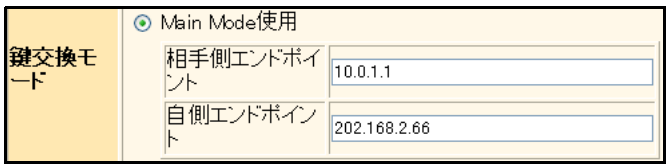
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→10.0.1.1
  自側エンドポイント　→202.168.2.66



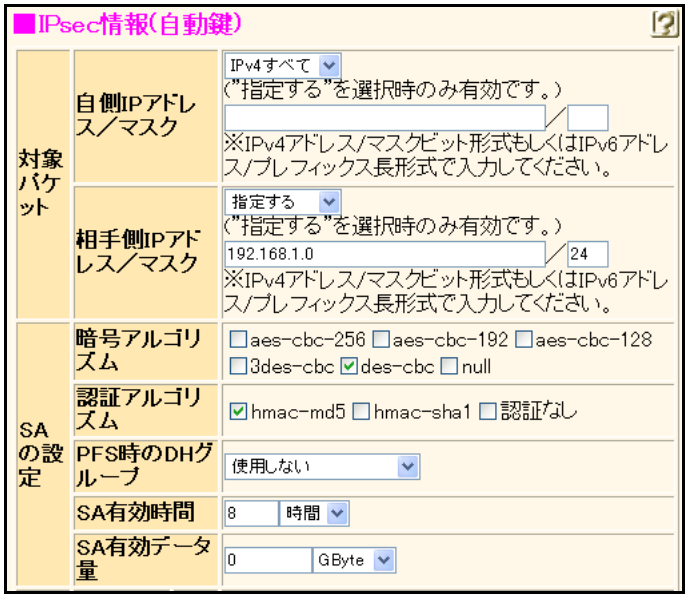
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→指定する
  →192.168.1.0/24
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



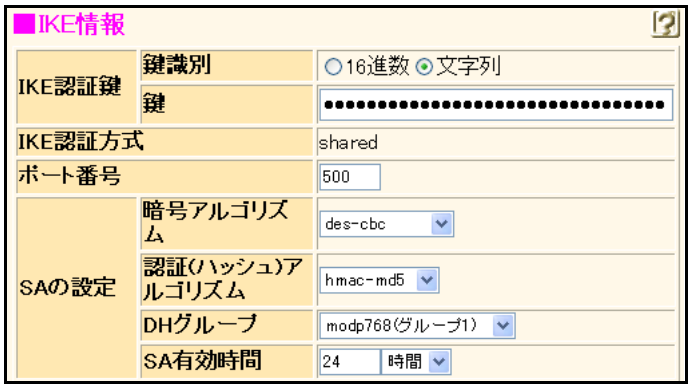
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B 向けの設定をする

「支社 A 向けを設定する」を参考に、支社 B を設定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-shiB

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.3.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0

「接続先情報」

- 接続先名　→shisyaB
- 接続先種別　→IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→10.0.3.1
  自側エンドポイント　→202.168.2.66

「IPsec 情報」

- 対象パケット
  自側 IP アドレス／マスク　→ IPv4 すべて
  相手側 IP アドレス／マスク　→指定する
  → 192.168.3.0/24
- SA の設定
  暗号アルゴリズム　→ 3des-cbc
  認証アルゴリズム　→ hmac-sha1

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  暗号アルゴリズム　→ 3des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-sha1
  DH グループ　→ modp1024

1.14.3　NAT と併用した可変 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

ここでは、以下の条件によって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 A（PPPoE 接続)]

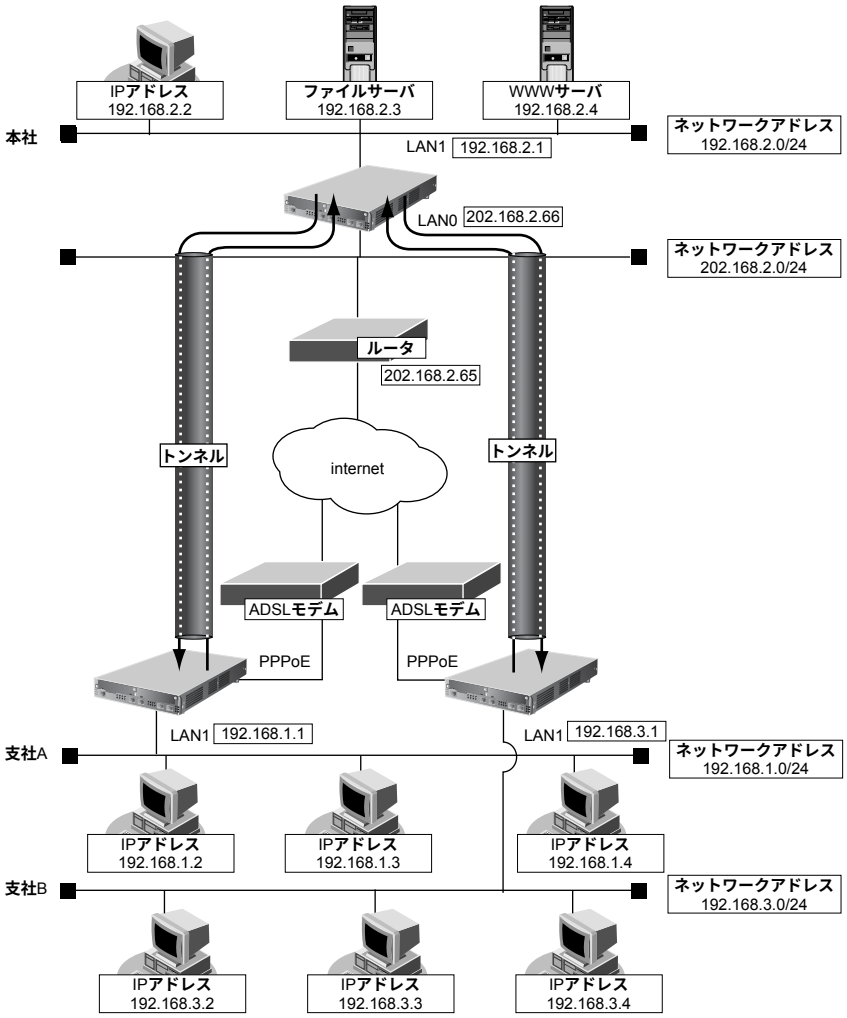
- ローカルネットワーク IP アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[支社 B（PPPoE 接続)]

- ローカルネットワーク IP アドレス　：192.168.3.1/24
- PPPoE ユーザ認証 ID　：userid3（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass3（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65



● 設定条件

[支社 A（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 A - 202.168.2.66
- IPsec 対象範囲　：192.168.1.0/24-any4
- IKE（UDP：500 番ポート）のプライベートアドレス
　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[支社 B（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 B - 202.168.2.66
- IPsec 対象範囲　：192.168.3.0/24-any4
- IKE（UDP：500 番ポート）のプライベートアドレス
　：192.168.3.1
- ESP のプライベートアドレス　：192.168.3.1

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 - 支社 A
- IPsec 対象範囲　：any4-192.168.1.0/24
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 - 支社 B
- IPsec 対象範囲　：any4-192.168.3.0/24

[共通 A]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A ID ／ ID タイプ　：shisyaA（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[共通 B]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：3des-cbc
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IKE 支社 B ID ／ ID タイプ　：shisyaB（自装置名）／ FQDN
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：3des-cbc
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp1024

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

こんな事に気をつけて

可変 IP アドレスでの VPN 接続を行うときは、インターネットプロバイダから割り当てられる IP アドレスが不定であるため、ローカルネットワーク IP アドレスで IKE ネゴシエーションを行う場合があります。このような運用では、送出インタフェースで NAT 機能を使用してください。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社 A（Initiator）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet）」ページが表示されます。

4.　「IP 関連」をクリックします。

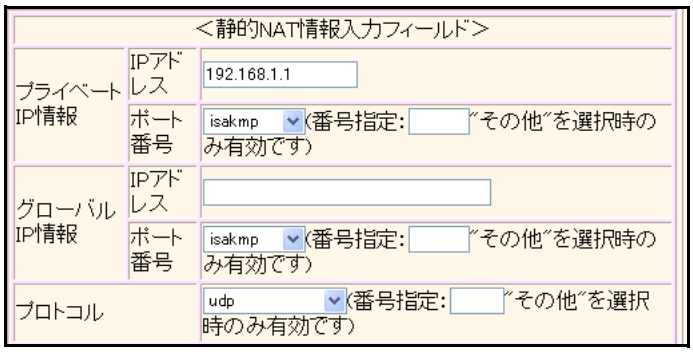
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6.～7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→ vpn-hon

12.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

13.　「IP 関連」をクリックします。

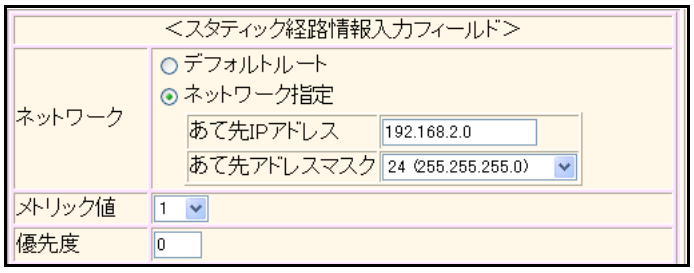
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



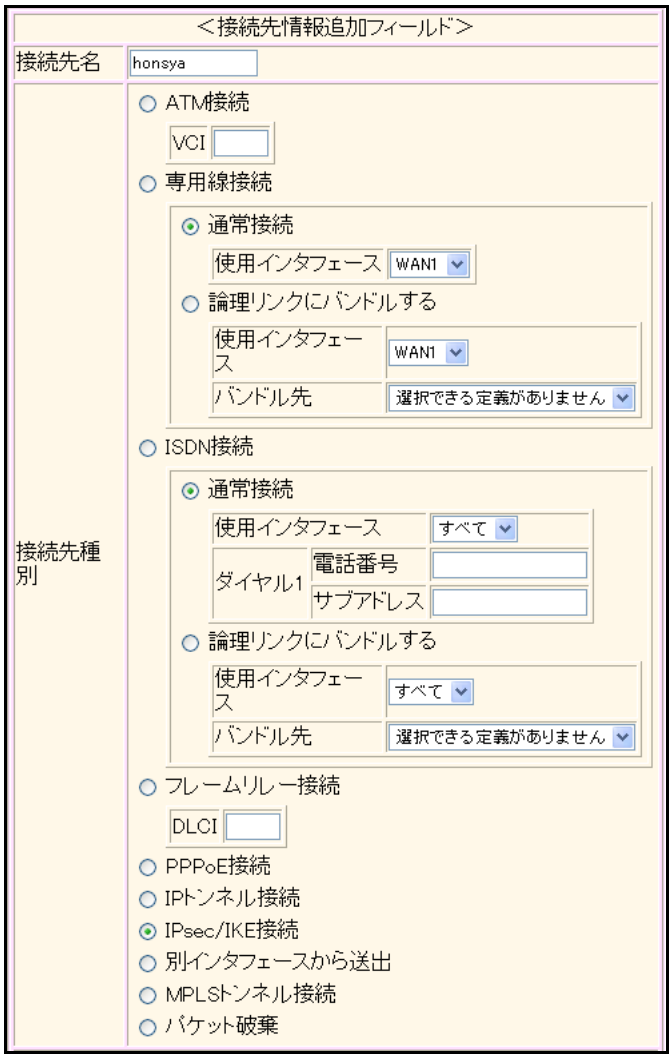
16.　［追加］ボタンをクリックします。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



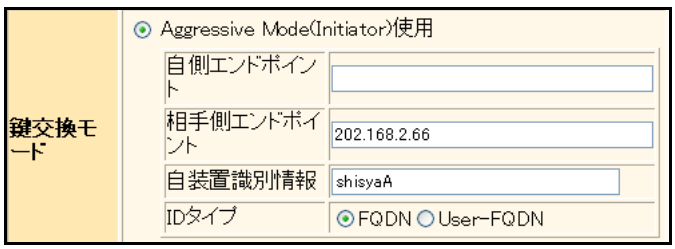
機種により、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisyaA



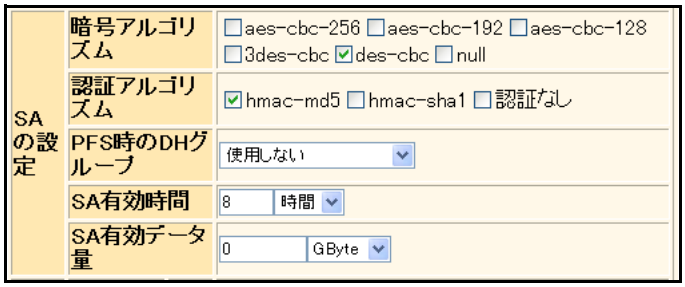
21.　［保存］ボタンをクリックします。

22.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

23.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



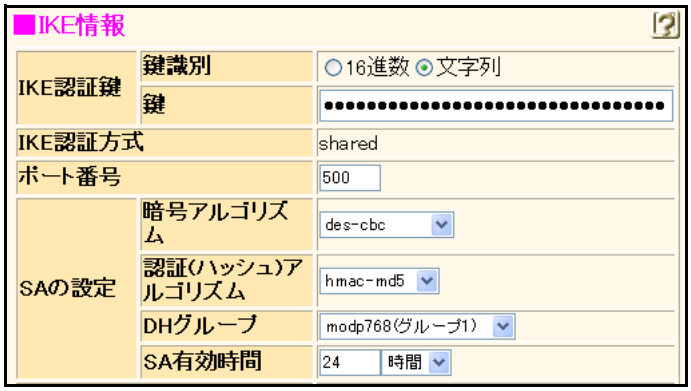
24.　［保存］ボタンをクリックします。

25.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

26.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



27.　［保存］ボタンをクリックします。

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

IKE 認証鍵には、文字列か数値（16 進数）を使用することができます。鍵として数値を入力したつもりでも、鍵識別で文字列を指定していると、文字列として認識されてしまうために、鍵が一致しない原因になります。

支社 B（Initiator）を設定する

「支社 A（Initiator）を設定する」を参考に、支社 B（Initiator）を設定します。

「相手情報」-「ネットワーク情報」

「ネットワーク情報」-「IP 関連」

「静的 NAT 情報」

- プライベート IP 情報
  IP アドレス　→ 192.168.3.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp
- プライベート IP 情報
  IP アドレス　→ 192.168.3.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ vpn-hon

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（ 255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ honshya
- 接続先種別　→ IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→ Aggresive Mode（Initiator）使用
  相手側エンドポイント　→ 202.168.2.66
  自装置識別情報　→ shisyaB

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→ 3des-cbc
  認証アルゴリズム　→ hmac-sha1

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp1024

本社（Responder）を設定する

支社 A 向けの設定をする

1.　設定メニューのルータ設定で「相手情報」をクリックします。

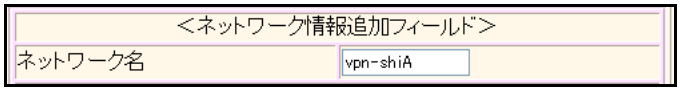
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shiA



4.　［追加］ボタンをクリックします。

「ネットワーク情報（ vpn-shiA)」ページが表示されます。

5.　「IP 関連」をクリックします。

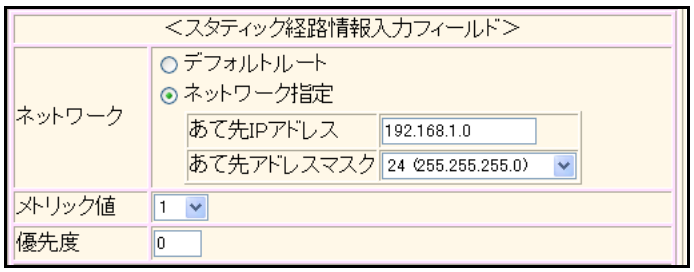
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



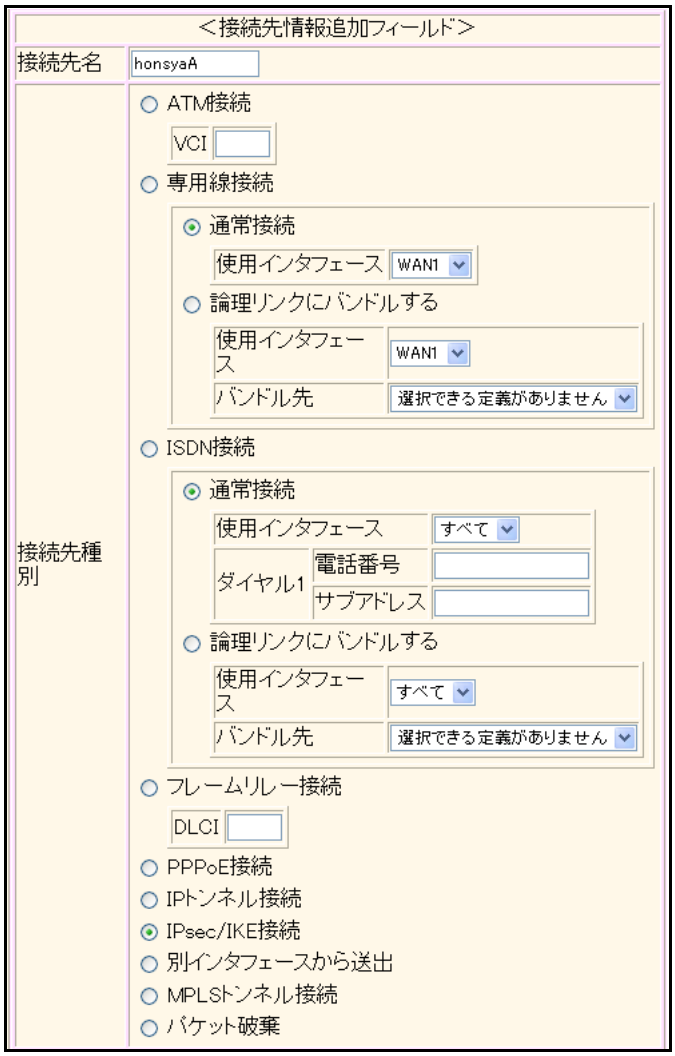
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisyaA
- 接続先種別　→IPsec/IKE 接続



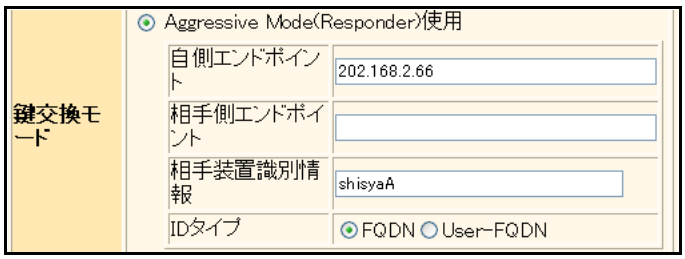
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggresive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  相手装置識別情報　→shisyaA



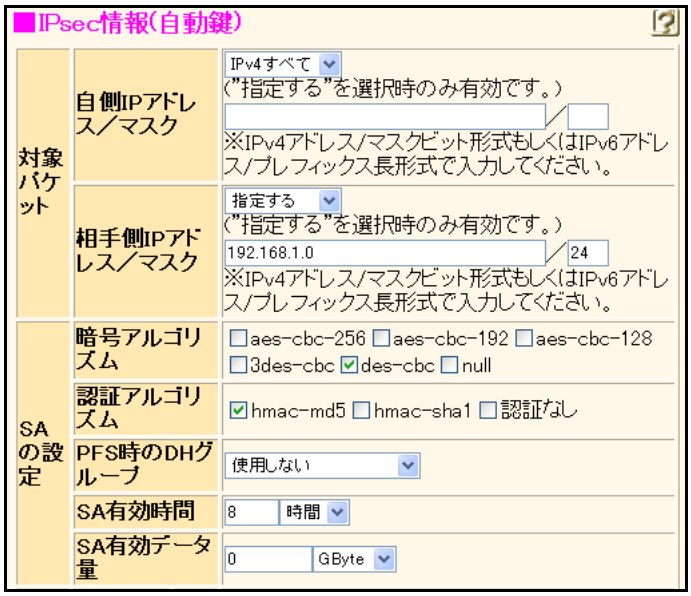
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→指定する
  →192.168.1.0/24
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



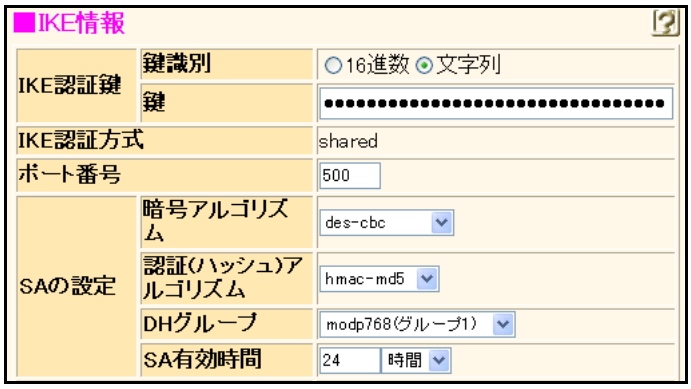
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B 向けの設定をする

「支社 A 向けを設定する」を参考に、支社 B 向けを設定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-shiB

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.3.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0

「ネットワーク情報」-「接続先情報」

- 接続先名　→shisyaB
- 接続先種別　→IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→Aggresive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  相手装置識別情報　→shisyaB

「IPsec 情報」

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→指定する
  →192.168.3.0/24
- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証アルゴリズム　→hmac-sha1

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  暗号アルゴリズム　→3des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp1024S

1.15 IPv6の事業所LANをISDNで接続する

適用機種 *Si-R220B,220C,370,570*

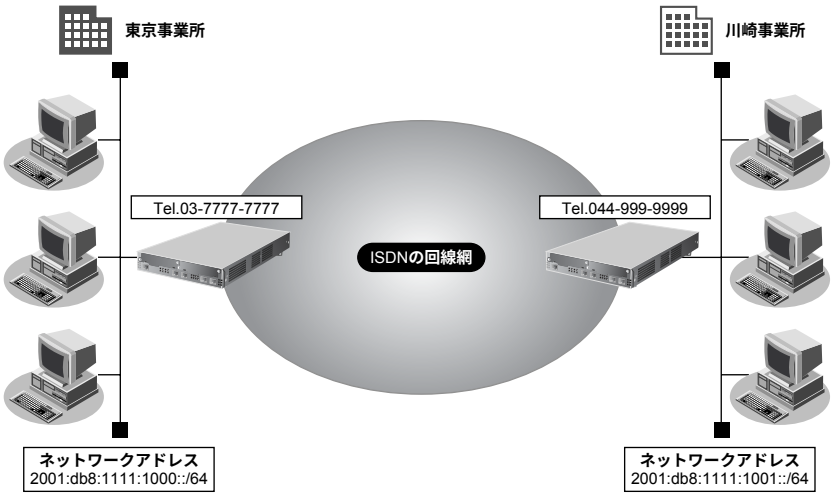
ここでは、ISDN回線を介して2つの事業所（東京、川崎）のIPv6ネットワークを接続する場合を例に説明します。

こんな事に気をつけて

- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。**

☛参照 Si-Rシリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）

- **双方の事業所から同時に発信が行われた場合、両方の接続が成立することでその接続が超過課金（2倍）になる場合があります。これは、接続優先制御機能を利用して片方の接続のみが存続するようにすることで防ぐことができます。この機能を利用する場合は、双方の事業所の装置で同じ接続優先設定を行わないでください。同時発信の際に接続ができなくなります。この機能を利用する場合は、以下の設定を奨励します。**
  - **一方の装置で着信接続を優先する。**
  - **一方の装置で接続優先制御を行わない。**



● 設定条件

- SLOT0に実装されたBRI拡張モジュールL2または基本ボード上のISDNポート（Si-R220B、220Cの場合）でISDN（64Kbps）を使用する
- IPv6を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名　：kaisya
- 無通信監視時間を1分とする

[東京事業所]

- ネットワークアドレス/プレフィックス長　：2001:db8:1111:1000::/64
- 接続先名　：tokyo
- 電話番号　：03-7777-7777
- ユーザ認証IDとユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass

[川崎事業所]

- ネットワークアドレス/プレフィックス長　：2001:db8:1111:1001::/64
- 接続先名　：kawasaki
- 電話番号　：044-999-9999
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

東京事業所を設定する

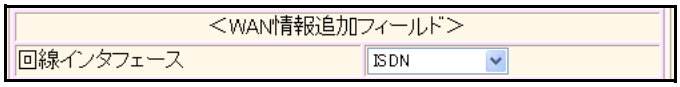
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→ISDN



3.　［追加］ボタンをクリックします。

「WAN0 情報（ISDN）」ページが表示されます。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

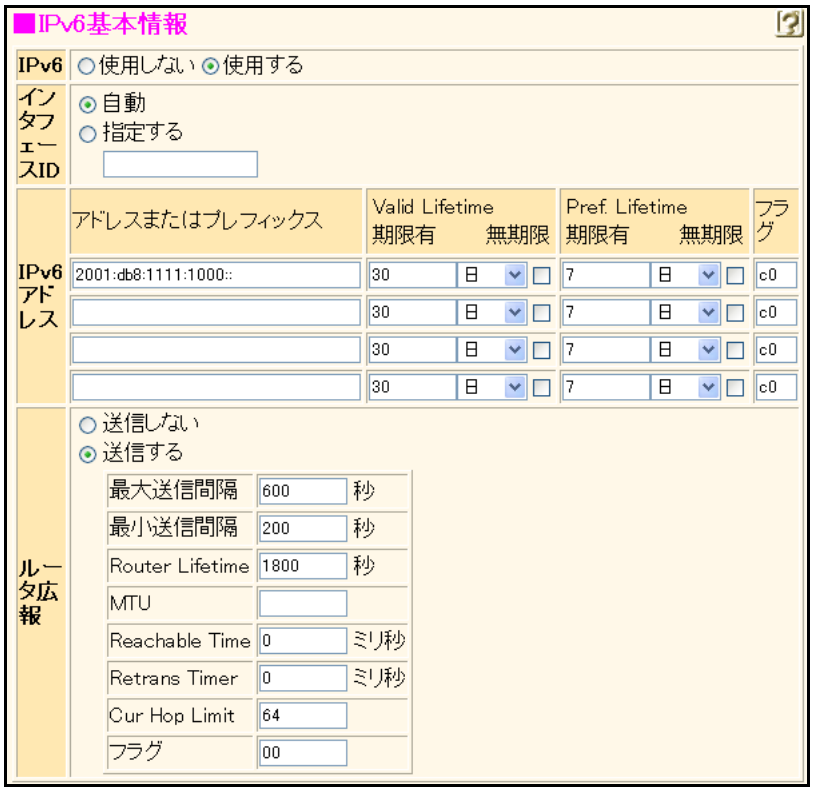
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:1000::
  Valid Lifetime　→ 30 日
  Pref. Lifetime　→ 7 日
  フラグ　→ c0
- ルータ広報　→送信する



5.　［保存］ボタンをクリックします。

相手情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→ kaisya

4.　［追加］ボタンをクリックします。

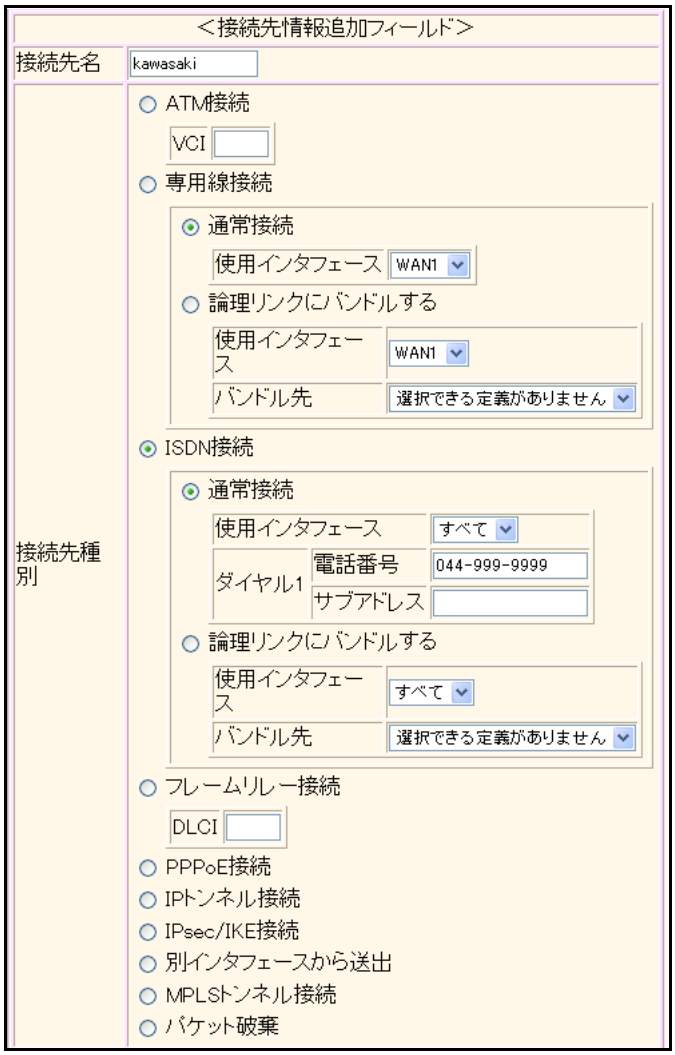
「ネットワーク情報（kaisya）」ページが表示されます。

5.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

6.　以下の項目を指定します。

- 接続先名　→kawasaki
- 接続先種別　→ISDN 接続
  →通常接続
  ダイヤル 1
  電話番号　→044-999-9999
  サブアドレス　→指定しない



機種により、接続先種別の表示が上記の画面とは異なります。

7.　［追加］ボタンをクリックします。

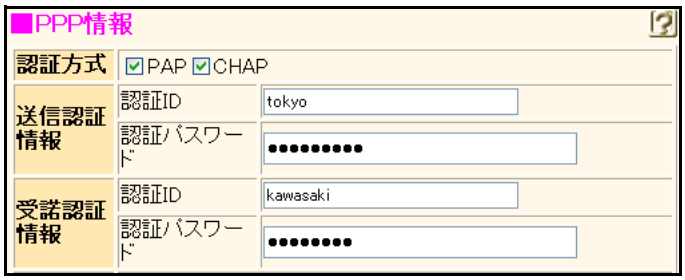
ISDN 接続の設定項目と「基本情報」が表示されます。

8.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

9.　以下の項目を指定します。

- 認証方式　→PAP、CHAP
- 送信認証情報
  認証 ID　→tokyo
  認証パスワード　→tokyopass
- 受諾認証情報
  認証 ID　→kawasaki
  認証パスワード　→kawapass



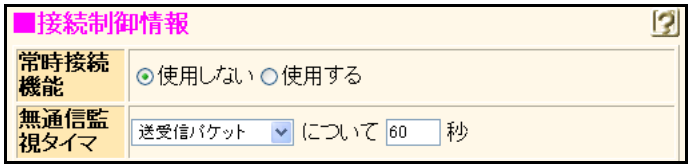
10.　［保存］ボタンをクリックします。

11.　ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

12.　以下の項目を指定します。

- 常時接続情報　→使用しない
- 無通信監視タイマ　→送受信パケットについて 60 秒



13.　［保存］ボタンをクリックします。

14.　画面上部の「ネットワーク情報（kaisya）」をクリックします。

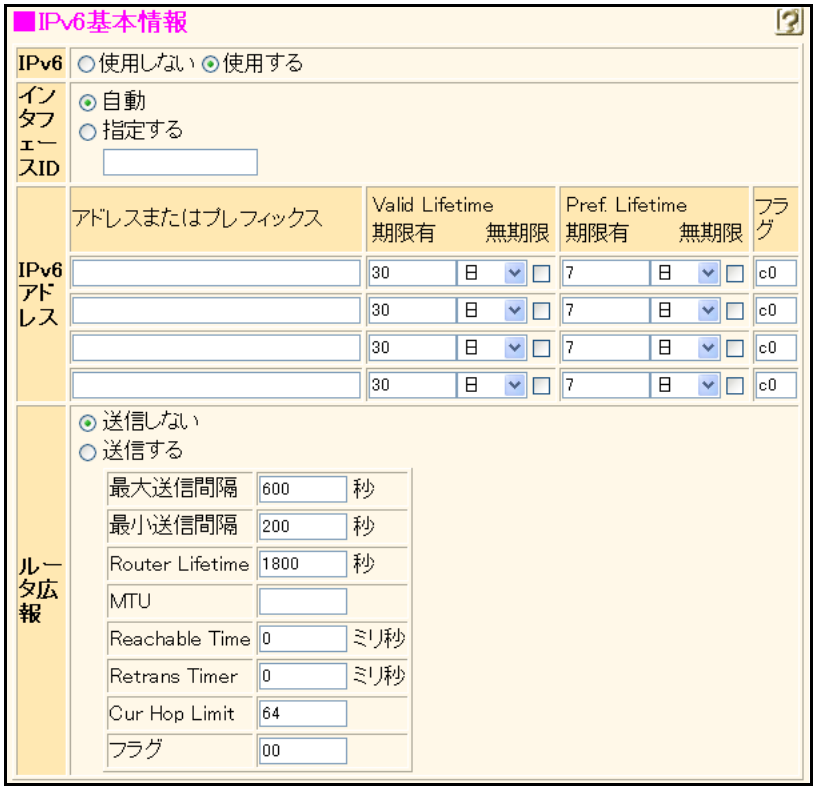
「ネットワーク情報（kaisya）」ページが表示されます。

15.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

16.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス　→指定しない
- ルータ広報　→送信しない



こんな事に気をつけて

双方の事業所から同時に発信が行われた場合、両方の接続が成立することでその接続が超過課金（2 倍）になる場合があります。これは、接続優先制御機能を利用して片方の接続のみが存続するようにすることで防ぐことができます。
この機能を利用する場合は、双方の事業所の装置で同じ接続優先設定を行わないでください。同時発信の際に接続ができなくなります。この機能を利用する場合は、以下の設定を奨励します。

- **一方の装置で着信接続を優先する。**
- **一方の装置で接続優先制御を行わない。**

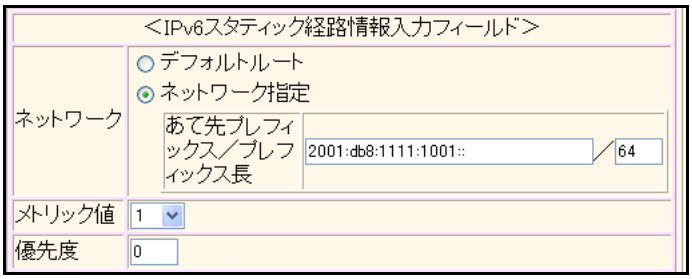
17.　［保存］ボタンをクリックします。

18.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

19.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先ネットワーク／プレフィックス長　→ 2001:db8:1111:1001::/64
- メトリック値　→ 1
- 優先度　→ 0



20.　［追加］ボタンをクリックします。

21.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

⚠注意

ISDN またはフレームリレーの場合、RIP（IPv6）を送信しないでください。RIP（IPv6）を送信すると、思わぬ課金（定期発信または長時間接続）が発生します。

川崎事業所を設定する

「東京事業所を設定する」を参考に、川崎事業所を設定します。

「WAN0 情報」

- 回線インタフェース　→ ISDN

「LAN0 情報」-「IPv6 関連」

「IPv6 基本情報」

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:1001::
  Valid Lifetime　→ 30 日
  Pref. Lifetime　→ 7 日
  フラグ　→ c0
- ルータ広報　→送信する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ tokyo

「接続先情報」

- 接続先名 →tokyo
- 接続先種別 →ISDN 接続
  →通常接続

  ダイヤル 1
  電話番号 →03-7777-7777
  サブアドレス →指定しない

「接続先情報」-「ISDN 接続」

「PPP 情報」

- 認証方式 →PAP、CHAP
- 送信認証情報
  認証 ID →kawasaki
  認証パスワード →kawapass
- 受諾認証情報
  認証 ID →tokyo
  認証パスワード →tokyopass

「接続制御情報」

- 常時接続情報 →使用しない
- 無通信監視タイマ →送受信パケットについて 60 秒

「相手情報」-「IPv6 関連」

「IPv6 基本情報」

- IPv6 →使用する
- インタフェース ID →自動
- IPv6 アドレス →指定しない
- ルータ広報 →送信しない

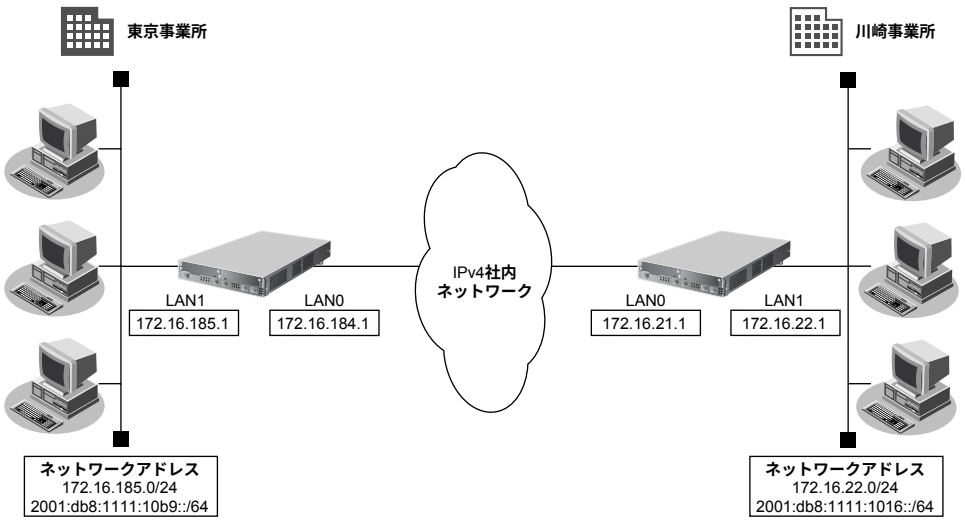
「IPv6 スタティック経路情報」

- ネットワーク →ネットワーク指定
  あて先ネットワーク／プレフィックス長 →2001:db8:1111:1000::/64
- メトリック値 →1
- 優先度 →0

1.16 IPv6の事業所LANをIPv6トンネルで接続する

適用機種　全機種

ここでは、IPv4で構築されたイントラネットを介して、2つの事業所（東京、川崎）のIPv6ネットワークどうしを接続（トンネリング）する場合を例に説明します。



● 設定条件

[東京事業所]

- ダイナミックルーティングを使用する
- LAN0側のIPv4アドレス　：172.16.184.1
- LAN1側のIPv4アドレス　：172.16.185.1
- LAN1側のIPv6プレフィックス/プレフィックス長　：2001:db8:1111:10b9::/64（※）

[川崎事業所]

- ダイナミックルーティングを使用する
- LAN0側のIPv4アドレス　：172.16.21.1
- LAN1側のIPv4アドレス　：172.16.22.1
- LAN1側のIPv6プレフィックス/プレフィックス長　：2001:db8:1111:1016::/64（※）

※）　この例では、プライベートアドレス（IPv4）／ドキュメント記述用アドレス（IPv6）を使用しています。

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  ☛参照　Si-Rシリーズ　Webユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **IPv6 over IPv4トンネルを利用する場合は、カプセル化されたIPv4パケットのフラグメントを防ぐため、トンネルに利用する相手情報のMTUに1280を設定してください。**
- **本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。**

東京事業所の本装置を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

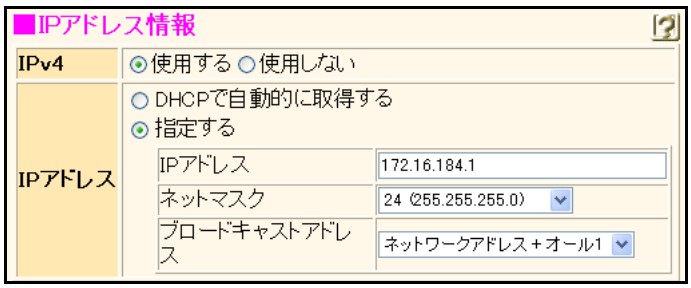
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 172.16.184.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



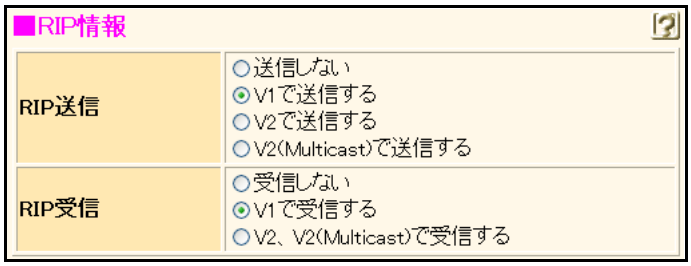
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→ V1 で送信する
- RIP 受信　→ V1 で受信する



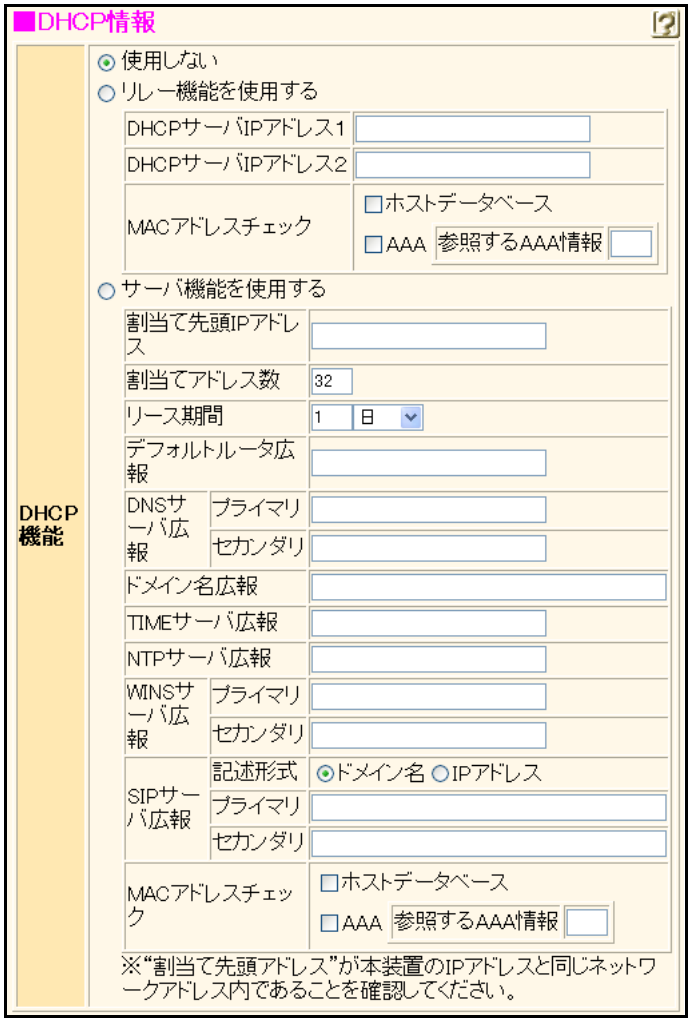
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

10.　以下の項目を指定します。

- DHCP 機能　→使用しない



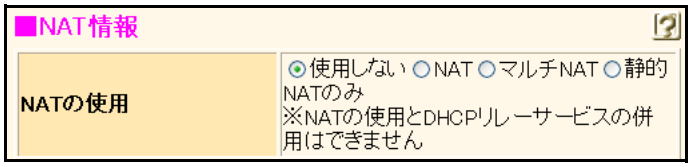
11.　［保存］ボタンをクリックします。

12.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

13.　以下の項目を指定します。

- NAT の使用　→使用しない



14.　［保存］ボタンをクリックします。

LAN1 情報を設定する

こんな事に気をつけて

Si-R180、180B 以外の装置で「LAN1 情報を設定する」場合は、あらかじめ物理 LAN1 定義を追加する必要があります。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

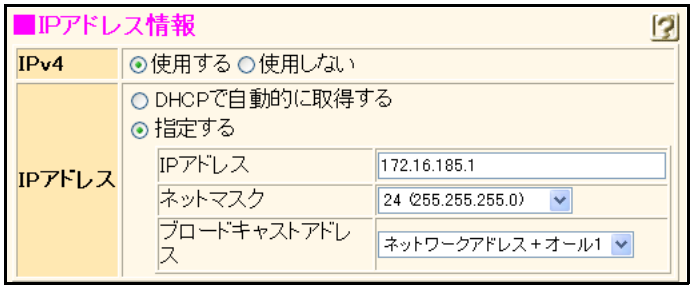
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 172.16.185.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



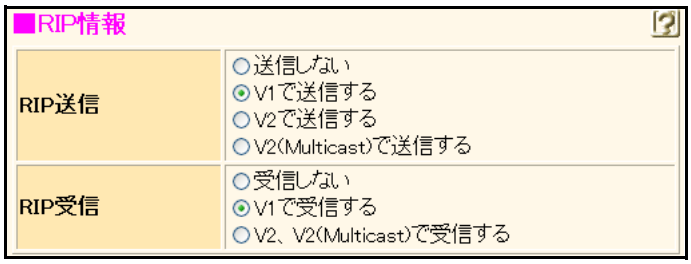
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

7.　以下の項目を指定します。

- RIP 送信　→ V1 で送信する
- RIP 受信　→ V1 で受信する



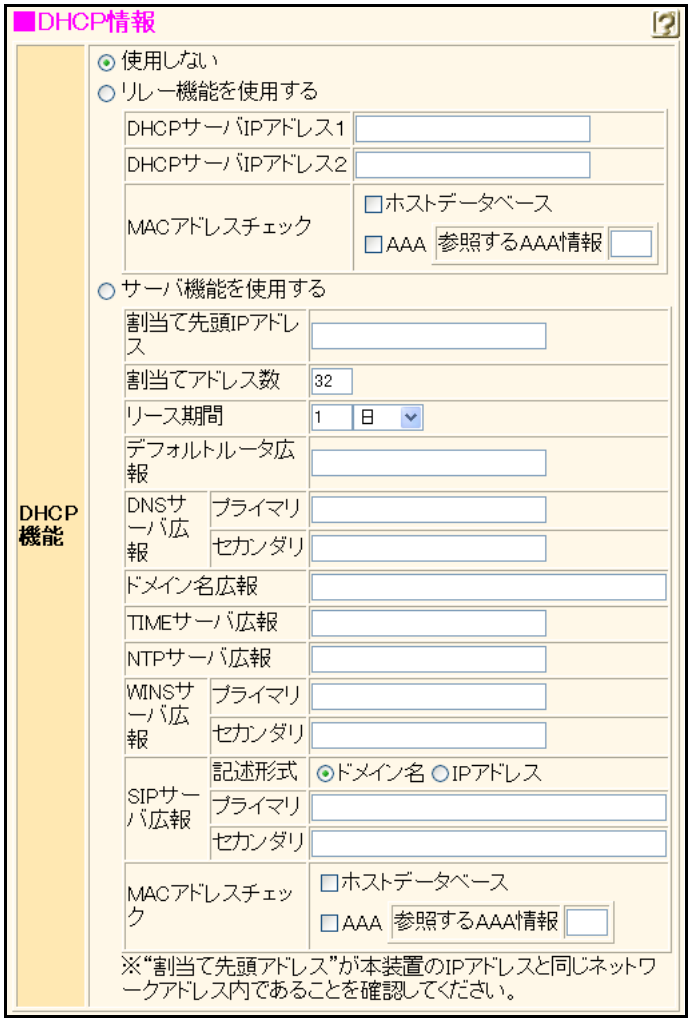
8.　［保存］ボタンをクリックします。

9.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

10.　以下の項目を指定します。

- DHCP 機能　→使用しない



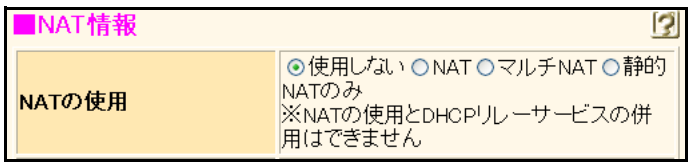
11.　［保存］ボタンをクリックします。

12.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

13.　以下の項目を指定します。

- NAT の使用　→使用しない



14.　［保存］ボタンをクリックします。

LAN 情報（東京事業所）を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

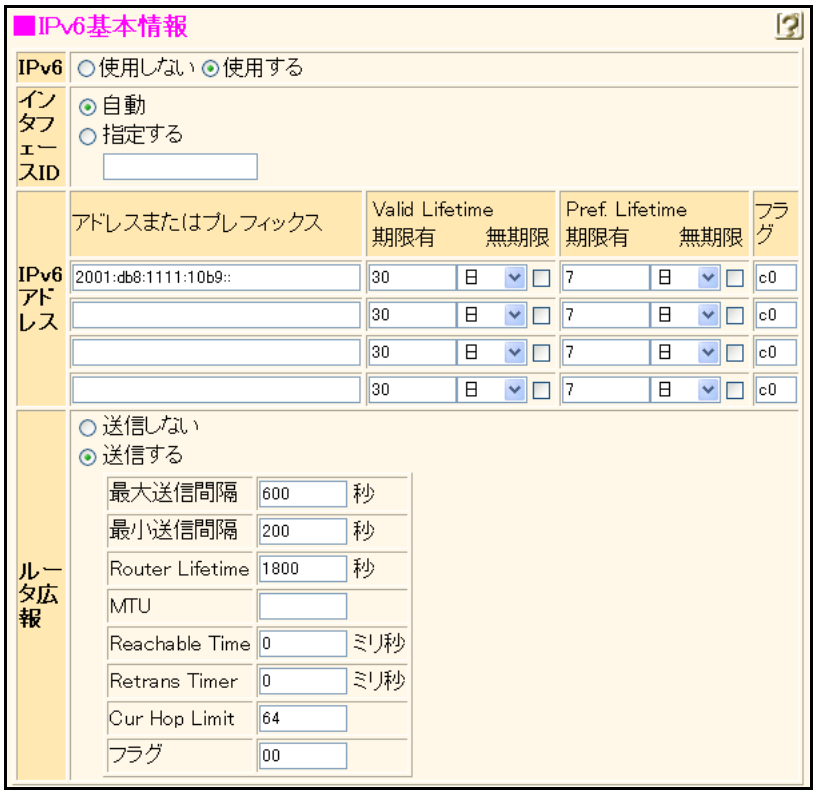
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:10b9::
- ルータ広報　→送信する



5.　［保存］ボタンをクリックします。

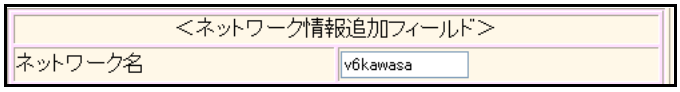
IP トンネル接続の情報（川崎事業所）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「ネットワーク情報」が表示されます。

2.　以下を指定します。

- ネットワーク名　→ v6kawasa（接続するネットワークの名称）



3.　［追加］ボタンをクリックします。

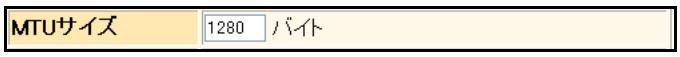
「ネットワーク情報」ページが表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- MTU サイズ　→ 1280



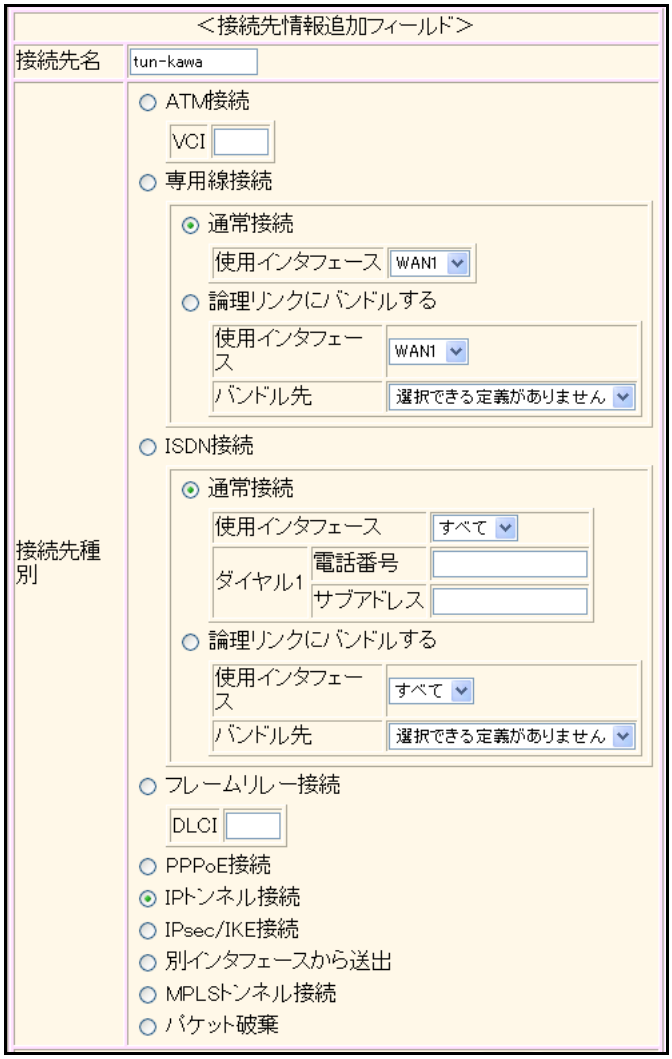
6.　［保存］ボタンをクリックします。

7.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

8.　以下を指定します。

- 接続先名　→ tun-kawa
- 接続先種別　→ IP トンネル接続



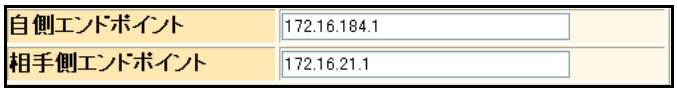
機種により、接続先種別の表示が上記の画面とは異なります。

9.　［追加］ボタンをクリックします。

IP トンネル接続の設定項目と「基本情報」が表示されます。

10.　以下の項目を指定します。

- 自側エンドポイント　→172.16.184.1
- 相手側エンドポイント　→172.16.21.1



11.　［保存］ボタンをクリックします。

12.　画面上部の「ネットワーク情報」をクリックします。

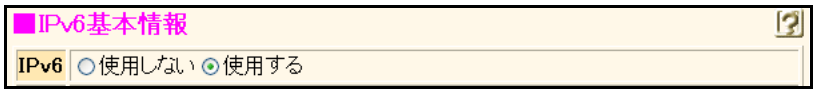
「ネットワーク情報」ページが表示されます。

13.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

14.　以下の項目を指定します。

- IPv6　→使用する



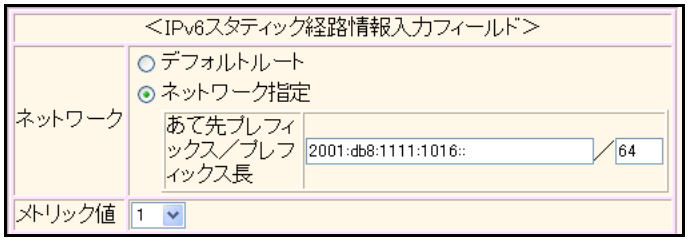
15.　［保存］ボタンをクリックします。

16.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

17.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先ネットワーク/プレフィックス長　→2001:db8:1111:1016::/64
- メトリック値　→1



18.　［追加］ボタンをクリックします。

19.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

川崎事業所の本装置を設定する

「東京事業所の本装置を設定する」を参考に、川崎事業所の本装置を設定します。
その際、特に指定のないものは、東京事業所と同じ設定にします。

LAN 情報（川崎事業所）を設定する

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 172.16.21.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN1 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 172.16.22.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN1 情報」-「IPv6 関連」

「IPv6 基本情報」

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:1016::
- ルータ広報　→送信する

IP トンネル接続の情報（東京事業所）を設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ v6tokyo（接続するネットワークの名称）

「ネットワーク情報」-「共通情報」

「基本情報」

- MTU サイズ　→ 1280

「ネットワーク情報」-「Pv6 関連」

「IPv6 基本情報」

- IPv6　→使用する

「IPv6 スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先ネットワーク/プレフィックス長　→ 2001:db8:1111:10b9::/64
- メトリック値　→ 1

「接続先情報」

- 接続先名　→ tun-tkyo
- 接続先種別　→ IP トンネル接続

「接続先情報」-「IP トンネル接続」

「基本情報」

- 自側エンドポイント　→ 172.16.21.1
- 相手側エンドポイント　→ 172.16.184.1

ヒント

◆ NAT と IPv6 over IPv4 トンネルを併用する

IPv4 環境の NAT と、IPv6 over IPv4 トンネルを利用した IPv6 通信環境を併用する場合は、IPv4 環境の NAT の処理によって、IPv4 アドレスがどのように変換処理されるかを判断して IPv6 over IPv4 トンネル通信の設定を行う必要があります。

本装置では、トンネル処理は NAT 処理の内側（プライベートアドレス側）で行われますので、以下のように設定します。

設定項目	設定内容
自側エンドポイント	以下の IP アドレスのどちらかを設定します。 LAN に設定された IP アドレスまたはセカンダリ IP アドレス 「相手情報」ー「ネットワーク情報」ー「IP 関連」ー「IP 基本情報」の自側 IP アドレスで設定された IP アドレス ※）PPP で割り当てられる IP アドレスは利用できません。
相手側エンドポイント	相手トンネル GW の IP アドレス
静的 NAT	IPv6 over IPv4 トンネル通信が相手トンネル GW 側から開始されることがある場合は、静的 NAT の設定が必要となります。 プライベート IP 情報 IP アドレス自側エンドポイントに設定したアドレス ポート番号すべて グローバル IP 情報 IP アドレス相手トンネル GW に設定された、本装置側のアドレス ポート番号すべて プロトコル IPv6 over IPv4

具体例を以下に示します。

条件：

- 本装置の NAT 変換で利用するグローバルアドレスに 172.16.0.1 を利用
- 本装置のプライベート LAN 側に 192.168.1.1 を利用
- 相手トンネル GW の IP アドレスに 172.31.0.1 を利用

IPv6 over IPv4 トンネル接続：

- 本装置のトンネル通信の設定：
  192.168.1.1 と 172.31.0.1 の間でトンネル通信を行うことを前提に、以下のとおり設定します。
  自側エンドポイント　192.168.1.1
  相手側エンドポイント　172.31.0.1

静的NAT設定：

- プライベートIP情報
  IPアドレス　192.168.1.1
  ポート番号　すべて
- グローバルIP情報
  IPアドレス　172.16.0.1
  ポート番号　すべて
- プロトコル　IPv6 over IPv4

なお、この具体例で、相手トンネルGWの設定は、以下のとおりです。

172.16.0.1と172.31.0.1の間でトンネル通信を行うことを前提とします。

相手トンネルGWにSi-Rシリーズ（NAT未使用）を利用する場合は、相手側のSi-Rに以下を設定します。

自側エンドポイント　172.31.0.1
相手側エンドポイント　172.16.0.1

第２章　活用例

この章では、本装置の便利な機能の活用方法について説明します。

2.1　RIP の経路を制御する（IPv4）

適用機種　全機種

本装置を経由して、ほかのルータに送受信する経路情報に対して、IP アドレスや方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIP による経路情報

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件（IP アドレス／アドレスマスク）
- メトリック値

補足　メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0 を指定すると変更は行いません。経路情報のフィルタリング条件にすべて以外を指定した場合に有効です。送信方向のメトリック値に 1 ～ 16 を指定した場合、インタフェースに設定した RIP の加算メトリック値は加算されません。

ヒント

◆ IP アドレスとアドレスマスクの決め方

フィルタリング条件の要素には、「IP アドレス」と「アドレスマスク」があります。制御対象となる経路情報は、経路情報の IP アドレスとアドレスマスクが指定した IP アドレスとアドレスマスクと一致したものだけです。

例）　指定値　：172.21.0.0/16 の場合

経路情報　：172.21.0.0/16 は制御対象となる

172.21.0.0/24 は制御対象とならない

また、フィルタリング条件の IP アドレスと指定した IP アドレスが、指定したアドレスマスクまで一致した場合に制御対象とすることもできます。

指定値　：172.21.0.0/16 の場合

経路情報　：172.21.0.0/24 は制御対象となる

172.21.10.0/24 は制御対象となる

こんな事に気をつけて

RIPv1 を使用している場合もアドレスマスクの設定が必要です。この場合、インタフェースのアドレスマスクを指定してください。また、アドレスクラスが異なる経路情報を制御する場合は、ナチュラルマスク値を指定してください。
例）192.168.1.1/24 が設定されているインタフェースで 10.0.0.0 の経路情報を制御する場合は、10.0.0.0/8 を指定します。

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する。

B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる。

ここでは、設計方針 A の例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針 B の例として、以下の設定例について説明します。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

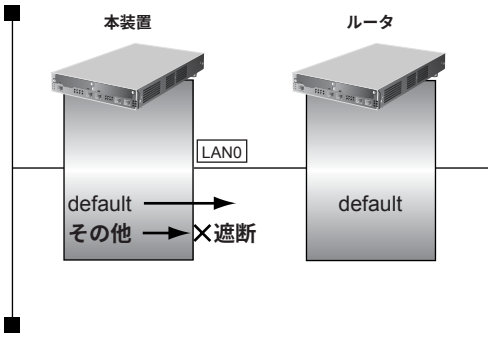
こんな事に気をつけて

- **フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。**
- **RIP 受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しない RIP 経路情報は遮断されます。**
- **RIP 送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しない RIP 経路情報は遮断されます。**

2.1.1　特定の経路情報の送信を許可する

適用機種　全機種

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明します。



● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

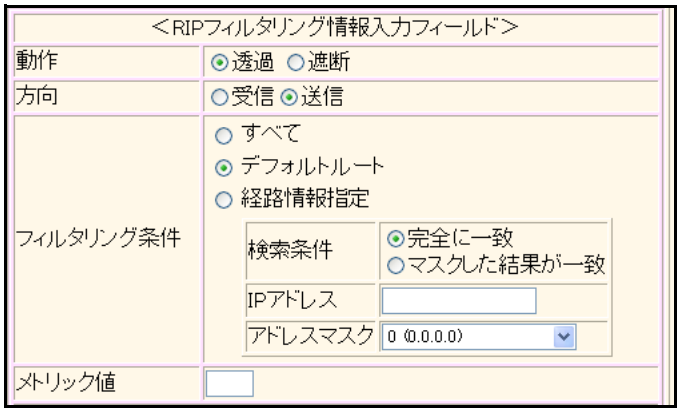
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を指定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

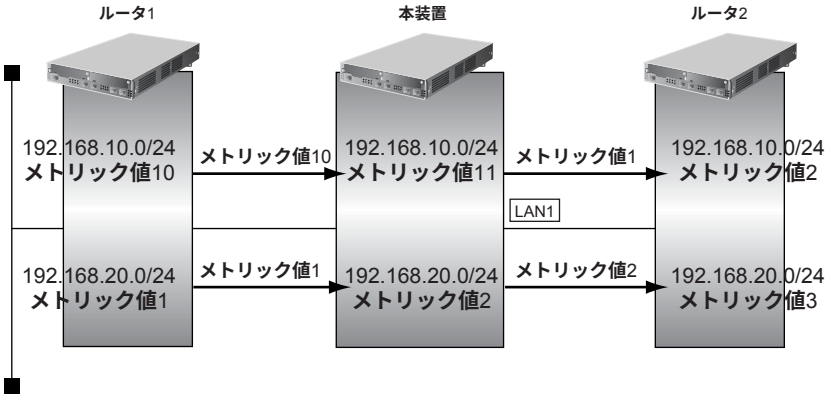
設定した内容が有効になります。

2.1.2　特定の経路情報のメトリック値を変更して送信する

適用機種　全機種

ここでは、本装置がルータ 2 へ 192.168.10.0/24、メトリック値 1 の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ 1 から 192.168.10.0/24 のメトリック値 10 と 192.168.20.0/24 のメトリック値 1 の経路情報を受信するものとします。



● フィルタリング設計

- 本装置から 192.168.10.0/24 の送信を許可する場合、メトリック値 1 に変更
- 192.168.10.0/24 以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

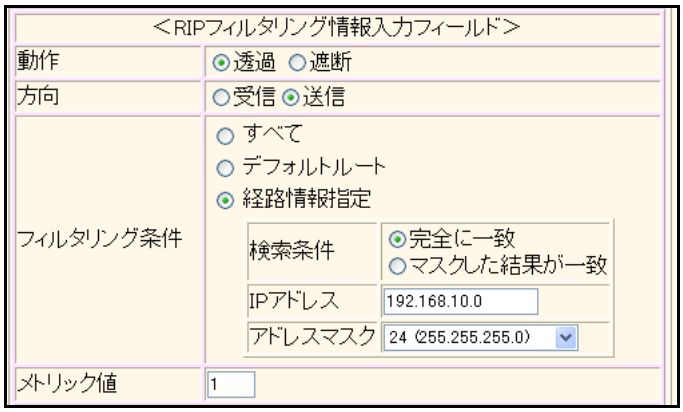
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 192.168.10.0
  アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1



6.　［追加］ボタンをクリックします。

7.　手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

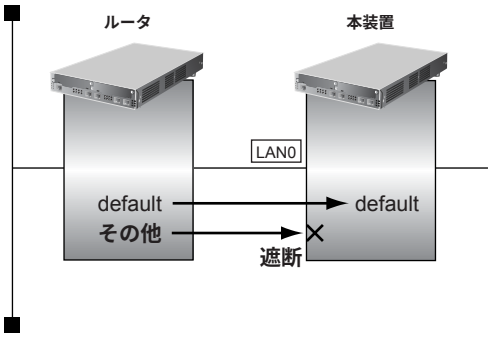
こんな事に気をつけて

- **送信方向でメトリック値が設定されている場合、インタフェースの RIP 加算メトリック値の加算は行われません。**
- **送信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。**

2.1.3　特定の経路情報の受信を許可する

適用機種　全機種

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

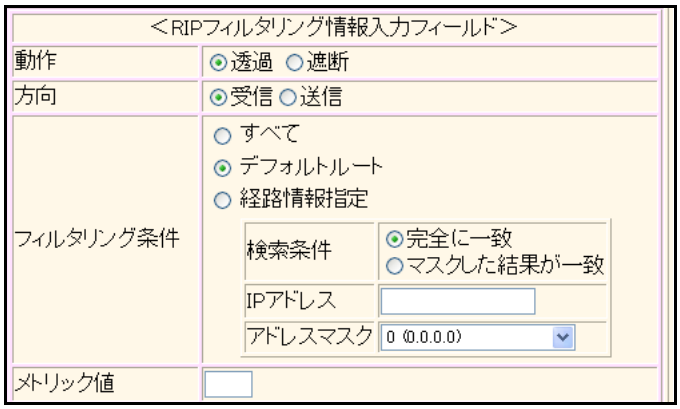
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

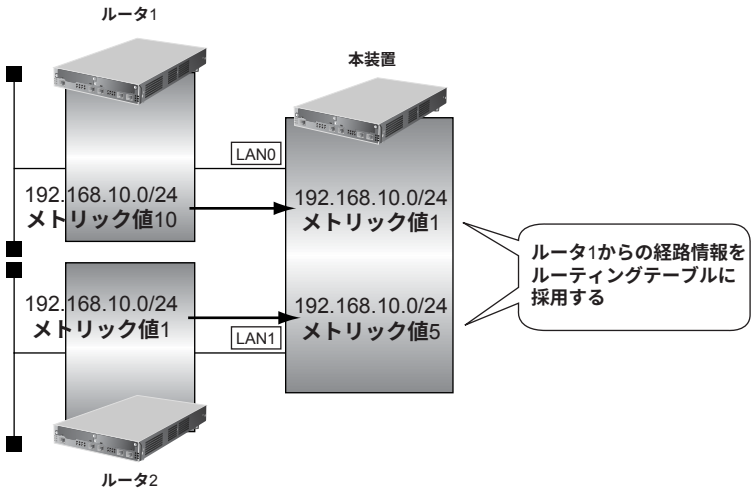
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.1.4　特定の経路情報のメトリック値を変更して受信する

適用機種　全機種

ここでは、本装置が、ルータ 1 とルータ 2 から同じあて先への経路情報 192.168.10.0/24 を受信した場合に、ルータ 1 から受信した経路情報を採用する場合の設定方法を説明します。



● フィルタリング設計

- ルータ 1 から、192.168.10.0/24 の経路情報を受信した場合、メトリック値 1 に変更
- ルータ 2 から、192.168.10.0/24 の経路情報を受信した場合、メトリック値 5 に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

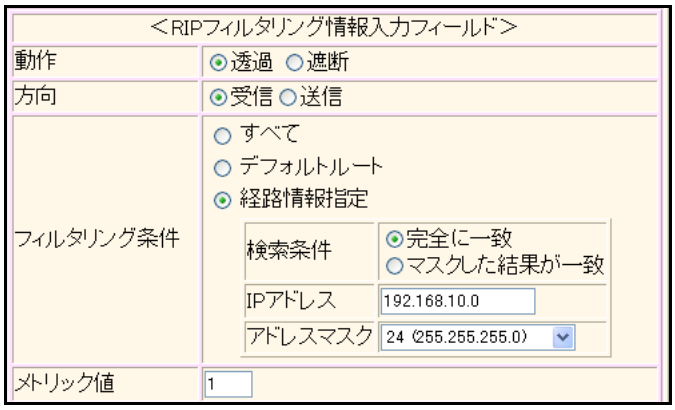
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 192.168.10.0
  アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

9.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

10.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

11.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

12.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 192.168.10.0
  アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 5

13.　手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

14.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

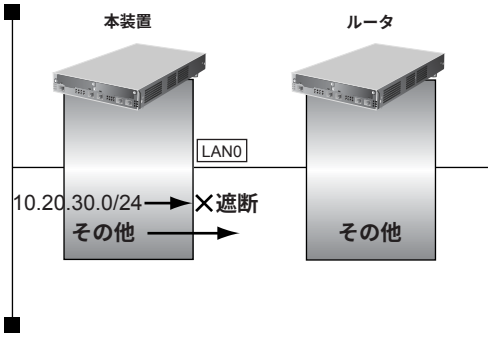
こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

2.1.5　特定の経路情報の送信を禁止する

適用機種　全機種

ここでは、本装置からルータへの 10.20.30.0/24 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置からルータへの 10.20.30.0/24 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

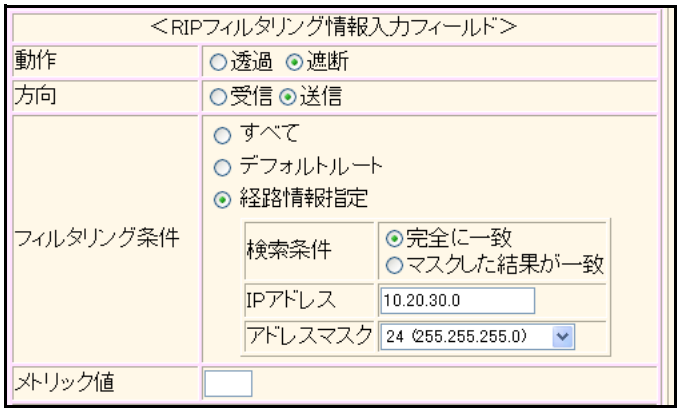
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 10.20.30.0
  アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

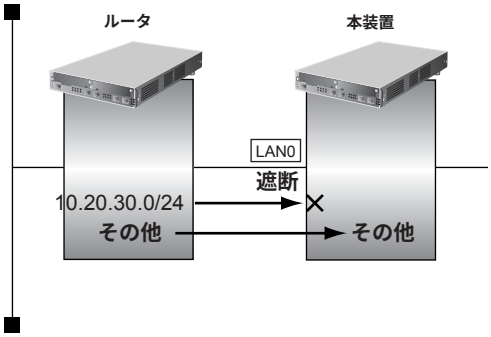
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.1.6　特定の経路情報の受信を禁止する

適用機種　全機種

ここでは、本装置は、ルータから 10.20.30.0/24 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置は 10.20.30.0/24 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

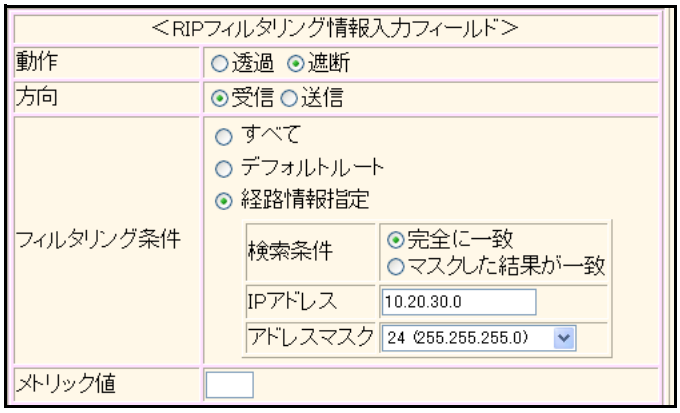
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 10.20.30.0
  アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.2　RIP の経路を制御する（IPv6）

適用機種　全機種

本装置を経由して、ほかのルータに送信する経路情報や、ほかのルータから受信する経路情報に対して、経路情報や方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または、不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIP による経路情報（IPv6）

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング情報（プレフィックス／プレフィックス長）
- メトリック値

補足　メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0 を指定すると変更は行いません。経路情報のフィルタリング条件にすべて以外を指定した場合に有効です。送信方向のメトリック値に 1 ～ 16 を指定した場合、インタフェースに設定した RIP の加算メトリック値は加算されません。

ヒント

◆ プレフィックスとプレフィックス長の決め方

フィルタリング条件の要素には、「プレフィックス」と「プレフィックス長」があります。制御対象となる経路情報は、経路情報のプレフィックスとプレフィックス長が指定したプレフィックスとプレフィックス長と一致したものだけです。

例）　指定値　：2001:db8:1111::/32 の場合

経路情報　：2001:db8:1111::/32 は制御対象となる

2001:db8:1111::/64 は制御対象とはならない

また、経路情報のプレフィックスと指定したプレフィックスが、指定したプレフィックス長まで一致した場合に制御対象とすることもできます。

指定値　：2001:db8::/16 の場合

経路情報　：2001:db8::/32 は制御対象となる

2001:db8:1111::/32 は制御対象となる

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する。

B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる。

ここでは、設計方針 A の例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針 B の例として、以下の設定例について説明します。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

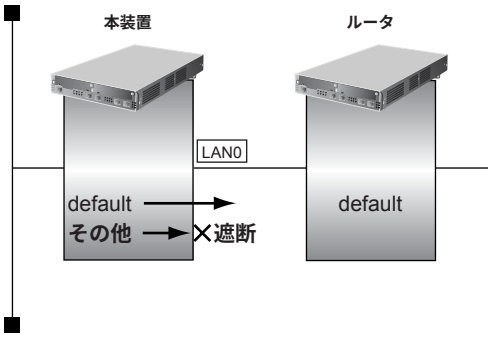
こんな事に気をつけて

フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。
RIP 受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しない RIP 経路情報は遮断されます。
RIP 送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しない RIP 経路情報は遮断されます。

2.2.1　特定の経路情報の送信を許可する

適用機種　全機種

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明しています。



● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

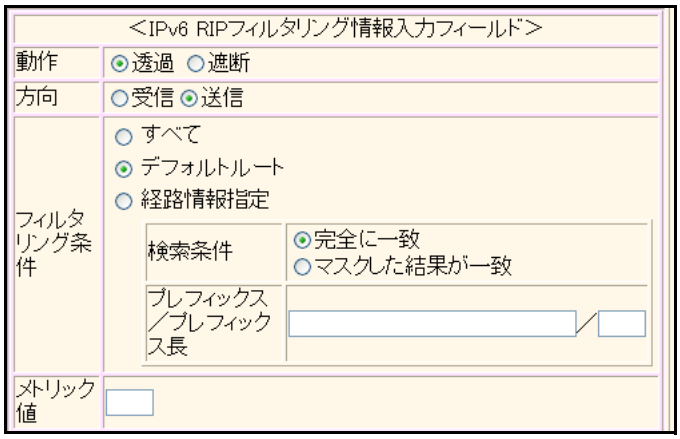
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

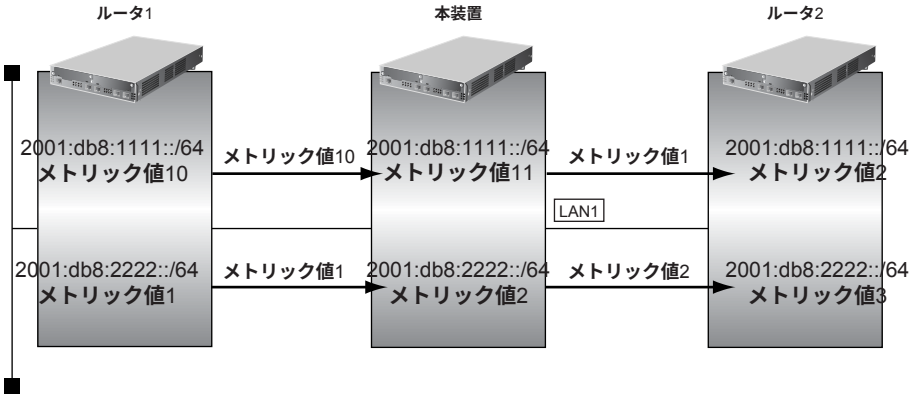
設定した内容が有効になります。

2.2.2　特定の経路情報のメトリック値を変更して送信する

適用機種　全機種

ここでは、本装置がルータ 2 へ 2001:db8:1111::/64、メトリック値 1 の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ 1 から 2001:db8:1111::/64 のメトリック値 10 と 2001:db8:2222::/64 のメトリック値 1 の経路情報を受信するものとします。



● フィルタリング設計

- 本装置から 2001:db8:1111::/64 の送信を許可する場合、メトリック値 1 に変更
- 2001:db8:1111::/64 以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

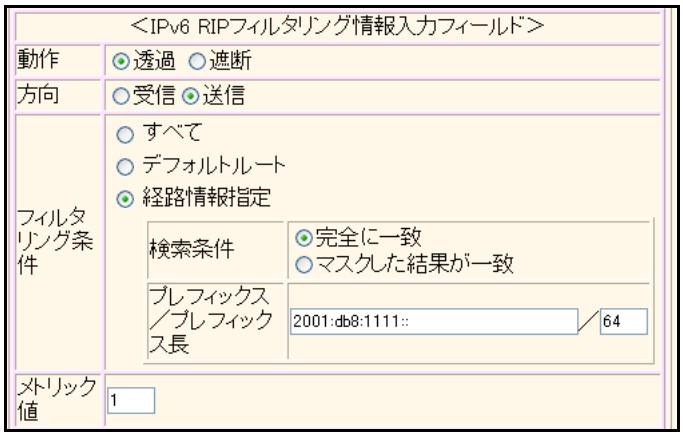
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→2001:db8:1111::/64
- メトリック値　→1



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

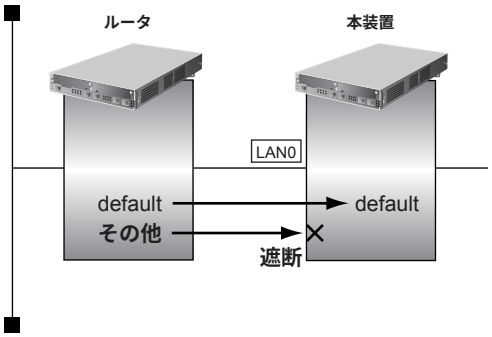
こんな事に気をつけて

- **送信方向でメトリック値が設定されている場合、インタフェースの RIP 加算メトリック値の加算は行われません。**
- **送信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。**

2.2.3　特定の経路情報の受信を許可する

適用機種　全機種

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

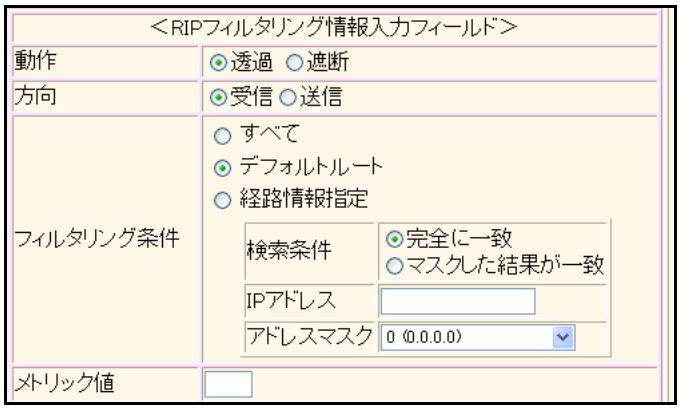
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

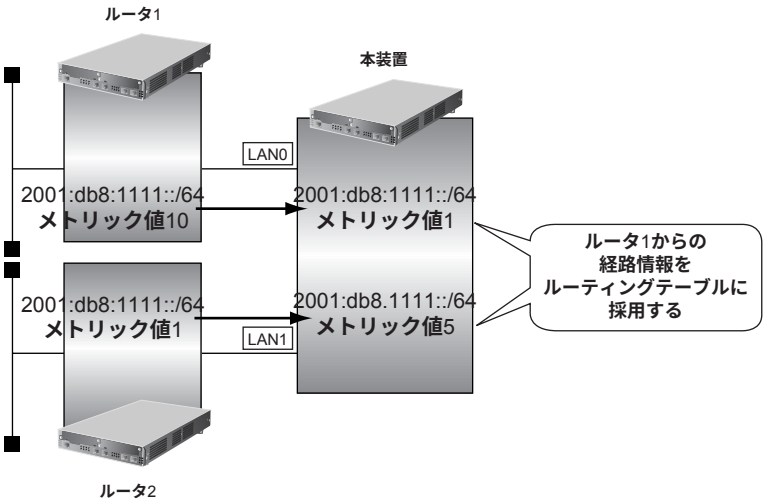
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.2.4　特定の経路情報のメトリック値を変更して受信する

適用機種　全機種

ここでは、本装置が、ルータ 1 とルータ 2 から同じあて先への経路情報 2001:db8:1111::/64 を受信した場合に、ルータ 1 から受信した経路情報を採用する場合の設定方法を説明します。



● フィルタリング設計

- ルータ 1 から、2001:db8:1111::/64 の経路情報を受信した場合、メトリック値 1 に変更
- ルータ 2 から、2001:db8:1111::/64 の経路情報を受信した場合、メトリック値 5 に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

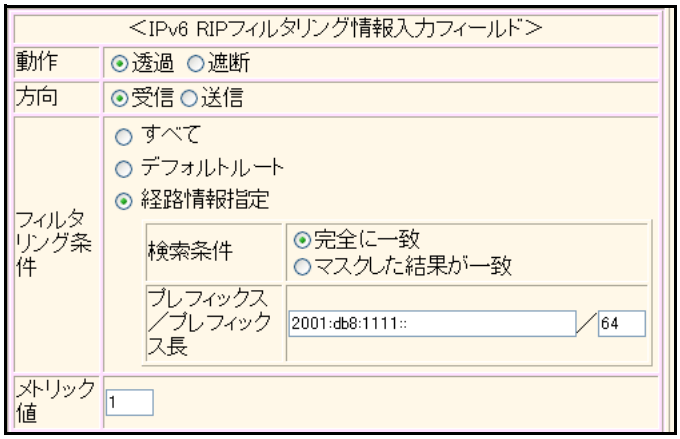
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→ 2001:db8:1111::/64
- メトリック値　→ 1



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

9.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

10.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

11.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

12.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→ 2001:db8:1111::/64
- メトリック値　→ 5

13.　手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

14.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

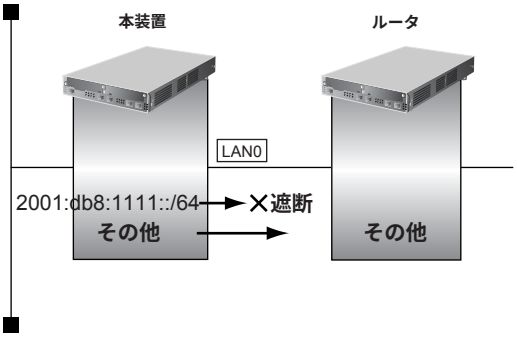
こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

2.2.5　特定の経路情報の送信を禁止する

適用機種　全機種

ここでは、本装置からルータへの 2001:db8:1111::/64 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置からルータへの 2001:db8:1111::/64 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

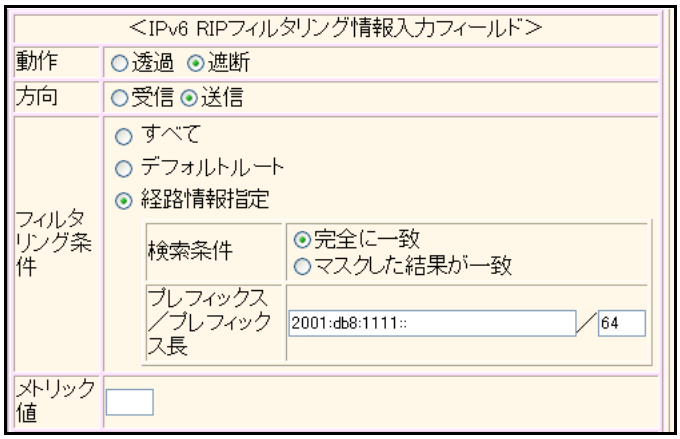
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→ 2001:db8:1111::/64
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

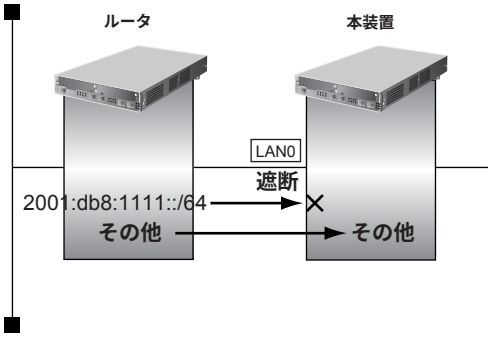
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.2.6　特定の経路情報の受信を禁止する

適用機種　全機種

ここでは、本装置は、ルータから 2001:db8:1111::/64 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● フィルタリング設計

- 本装置は 2001:db8:1111::/64 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IPv6 関連」をクリックします。

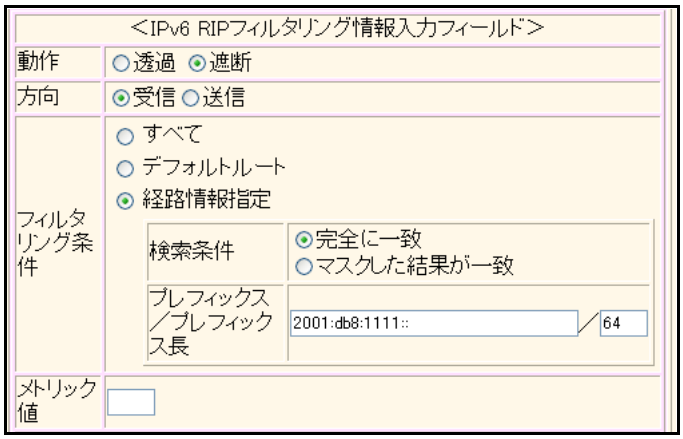
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→ 2001:db8:1111::/64
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順 5.～6. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.3 OSPFv2 を使用したネットワークを構築する（IPv4）

適用機種　全機種

ここでは、OSPFv2 を使用したダイナミックルーティングのネットワークの設定方法について説明します。

OSPF を使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。

エリアには、エリアごとにエリア ID を設定します。バックボーンエリアには必ず 0.0.0.0 のエリア ID を設定し、ほかのエリアには重複しないように 0.0.0.0 以外のエリア ID を設定します。

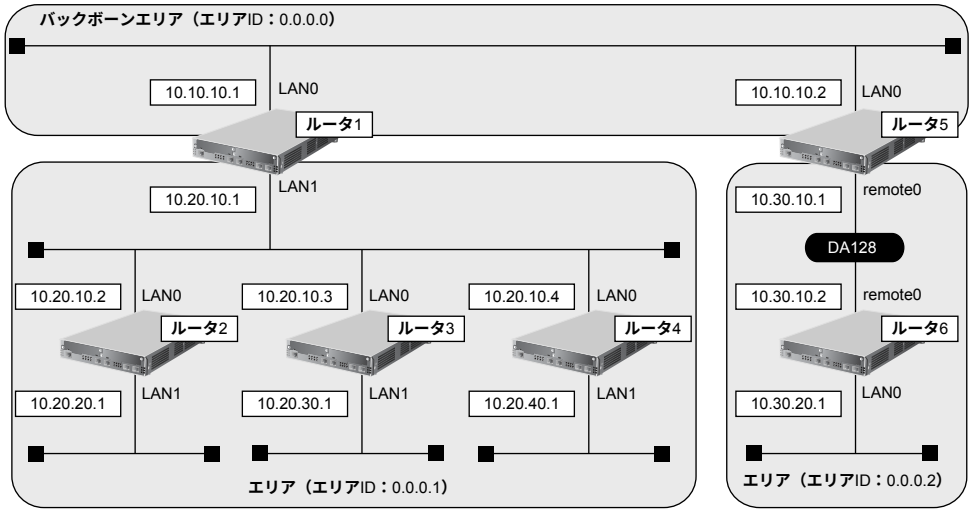
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

参照　Si-R シリーズ　機能説明書「2.5 OSPF 機能」（P.37）

こんな事に気をつけて

- NAT 機能と併用することはできません。
- OSPF を使用するインタフェースは、それぞれ異なったネットワークに属する IP アドレスを設定する必要があります。同じネットワークに属する IP アドレスを設定した場合、OSPF を使用しないと判断されます。
- ルータは、各エリアに 50 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2 つ以上のエリアの指定ルータ（Designated Router）とならないように設定してください。
- 隣接する OSPF ルータどうしは、同じ MTU 値を設定してください。
- 経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができても、OSPF の経路は、経路情報に反映されません
- 本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません（LSDB オーバフロー）。
  また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源を再投入したり、または［設定反映］ボタンや［再起動］ボタンをクリックしても、正常に通信ができるまでに最大 60 分かかることがあります。
- OSPF 使用中に［設定反映］ボタンをクリックした場合、自装置が広報したすべての LSA に対して MaxAge で再広報を行ったあとに、OSPF ネットワークへの経路情報が再作成されることがあります。
- OSPF で使用するインタフェースは、以下の条件で使用してください。

	Si-R180、180B、220B、220C、240、240B、260B	Si-R370、570
インタフェース数	（30000 ÷本装置保有 LSA 数）未満	（50000 ÷本装置保有 LSA 数）未満
通信速度	15Kbps 以上の通信帯域を確保する必要があります。	



ここでは、ルータ 5 とルータ 6 が専用線（remote 定義）で接続され、以下のとおりに設定されていることを前提とします。

● 前提条件

- ルータ 1 からルータ 6 のすべてのインタフェースに IP アドレスを設定する
- ルータ 1 からルータ 6 のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

- ルータ 5 およびルータ 6 は、SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）で専用線に接続する

[ルータ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN1 でのルータ優先度　：0
- エリア 0.0.0.1 への集約経路設定　：10.20.0.0/16

[ルータ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：1
- LAN1 での passive-interface 設定　：設定する

[ルータ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：255
- LAN1 での passive-interface 設定　：設定する

[ルータ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN1 での passive-interface 設定　：設定する
- LAN0 でのルータ優先度　：1

[ルータ 5 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- remote 定義でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- remote 定義での OSPF エリア ID　：0.0.0.2
- エリア 0.0.0.2 への集約経路設定　：10.30.0.0/16

[ルータ 6 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- remote 定義でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- remote 定義での OSPF エリア ID　：0.0.0.2
- LAN0 での passive-interface 設定　：設定する

上記の設定条件に従って設定を行う場合の設定例を示します。

ルータ 1 を設定する

LAN 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

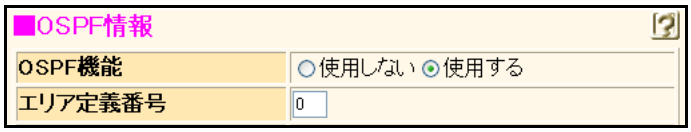
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

7.　手順 2.～6. を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

「LAN1 情報（物理 LAN）」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1
- 指定ルータ優先度　→0

OSPF 関連を設定する

8.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
「ルーティングプロトコル情報」ページが表示されます。

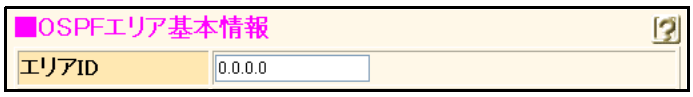
9.　「OSPF 関連」をクリックします。
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。
「OSPF エリア情報」が表示されます。

11.　［追加］ボタンをクリックします。
OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

12.　以下の項目を指定します。

- エリア ID　→0.0.0.0



13.　［保存］ボタンをクリックします。

14.　画面上部のルーティングプロトコル情報をクリックします。
OSPF 関連項目と「OSPF エリア情報」が表示されます。

15.　手順 11.～13. を参考に、以下の項目を指定します。

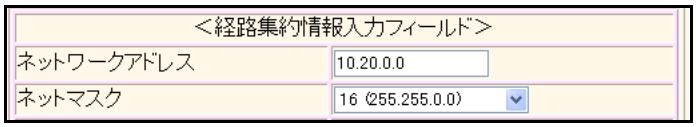
「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

16.　OSPF エリア情報（1）の「経路集約情報」をクリックします。
「経路集約情報」が表示されます。

17.　以下の項目を指定します。

- ネットワークアドレス　→10.20.0.0
- ネットマスク　→16（255.255.0.0）



18.　［追加］ボタンをクリックします。

19.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 2 を設定する

「ルータ 1 を設定する」を参考に、ルータ 2 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- 指定ルータ優先度　→1

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

ルータ 3 を設定する

「ルータ 1 を設定する」を参考に、ルータ 3 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- 指定ルータ優先度　→255

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

ルータ 4 を設定する

「ルータ 1 を設定する」を参考に、ルータ 4 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- 指定ルータ優先度　→1

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

ルータ 5 を設定する

「ルータ 1 を設定する」を参考に、ルータ 5 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.0

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.2
- 経路集約情報
  ネットワークアドレス　→10.30.0.0
  ネットマスク　→16（255.0.0.0）

ルータ 6 と接続する remote 定義に OSPF 機能を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　OSPF 機能を設定するネットワーク欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

4.　「IP 関連」をクリックします。

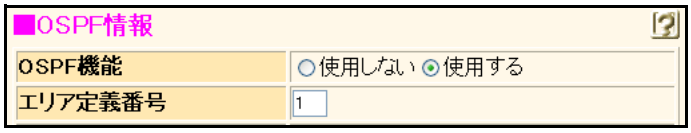
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

6.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→1



7.　［保存］ボタンをクリックします。

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 6 を設定する

「ルータ 1 を設定する」および「ルータ 5 を設定する」を参考に、ルータ 6 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.2

「相手情報」-「IP 関連」

「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

こんな事に気をつけて

remote 定義で使用する場合は、IP アドレスを必ず設定してください。

⚠注意

OSPF 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF 機能は使用しないでください。

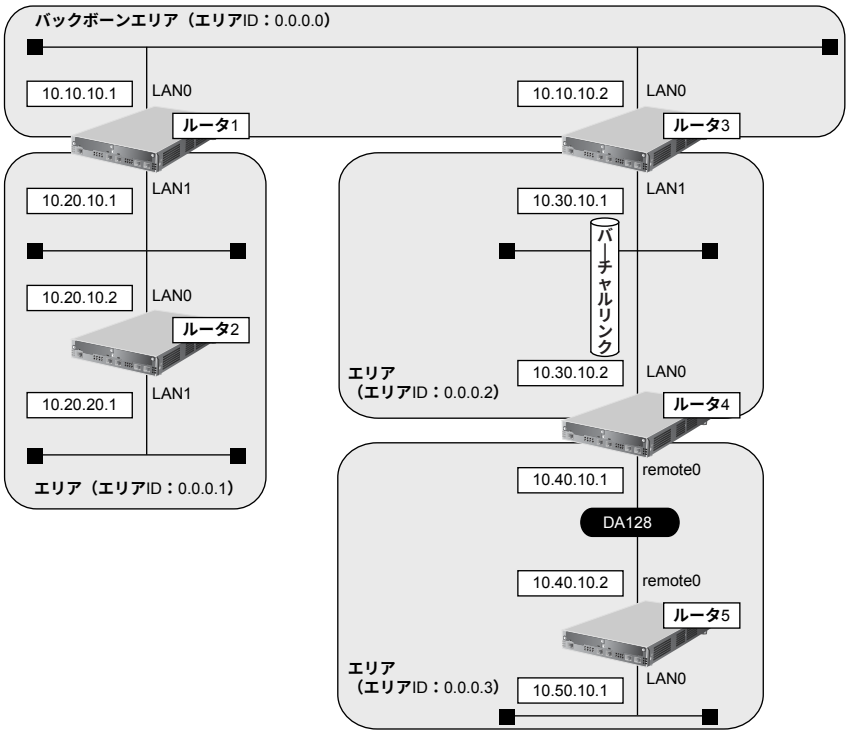
2.3.1　バーチャルリンクを使う

適用機種　全機種

バックボーンエリアと直接接続できないエリアを、バーチャルリンクを使用して接続する設定方法について説明します。

こんな事に気をつけて

- **バーチャルリンクは、スタブエリア、準スタブエリアを経由して使用することはできません。**
- **バーチャルリンクを使用する場合は、OSPF ルータ ID を設定する必要があります。設定する際は、OSPF ルータ ID が重複しないように設定してください。**



ここでは、ルータ 4 とルータ 5 が専用線（remote 定義）で接続され、以下のとおりに設定されていることを前提とします。

● 前提条件

- ルータ 1 からルータ 5 のすべてのインタフェースに IP アドレスを設定する
- ルータ 1 からルータ 5 のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

- ルータ 4 およびルータ 5 は、SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）で専用線に接続する

[ルータ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1

[ルータ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1

[ルータ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.2
- OSPF ルータ ID　：10.30.10.1
- バーチャルリンク接続先 OSPF ルータ ID　：10.40.10.1

[ルータ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- remote 定義でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- remote 定義での OSPF エリア ID　：0.0.0.3
- OSPF ルータ ID　：10.40.10.1
- バーチャルリンク接続先 OSPF ルータ ID　：10.30.10.1

[ルータ 5 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- remote 定義でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.3
- remote 定義での OSPF エリア ID　：0.0.0.3

上記の設定条件に従って設定を行う場合の設定例を示します。

ルータ 1 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

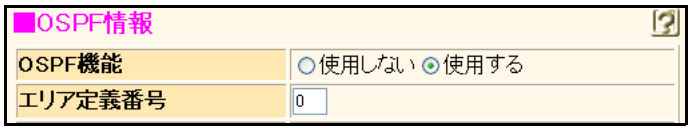
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

7.　手順 2.～6. を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

「LAN1 情報（物理 LAN）」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

OSPF 関連を設定する

8.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

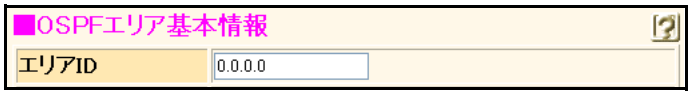
「OSPF エリア情報」が表示されます。

11.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

12.　以下の項目を指定します。

- エリア ID　→0.0.0.0



13.　［保存］ボタンをクリックします。

14.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

15.　手順 11.～13. を参考に、以下の項目を指定します。

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 2 を設定する

「ルータ 1 を設定する」を参考に、ルータ 2 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0)」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

ルータ 3 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN)」ページが表示されます。

3.　「IP 関連」をクリックします。

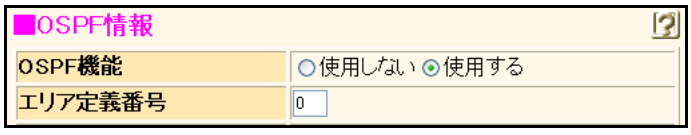
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

7.　手順 2. ～ 6. を参考に、以下の項目を指定します。

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 1

OSPF 関連を設定する

8.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

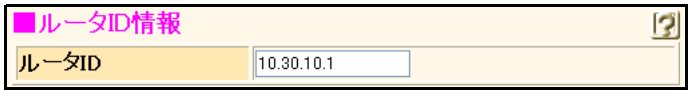
「ルーティングプロトコル情報」ページが表示されます。

9.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10.　以下の項目を指定します。

- ルータ ID　→ 10.30.10.1



11.　［保存］ボタンをクリックします。

12.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPF エリア情報」が表示されます。

13.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

14.　以下の項目を指定します。

- エリア ID　→ 0.0.0.0

15.　［保存］ボタンをクリックします。

16.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

17.　手順 13. ～ 15. を参考に、以下の項目を指定します。

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

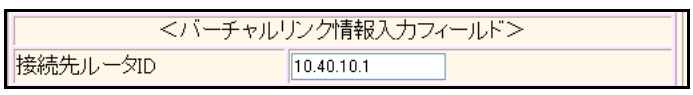
- エリア ID　→ 0.0.0.2

18.　OSPF エリア情報（1）の設定項目の「バーチャルリンク情報」をクリックします。

「バーチャルリンク情報」が表示されます。

19.　以下の項目を指定します。

- 接続先ルータ ID　→ 10.40.10.1



20.　［追加］ボタンをクリックします。

21.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 4 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

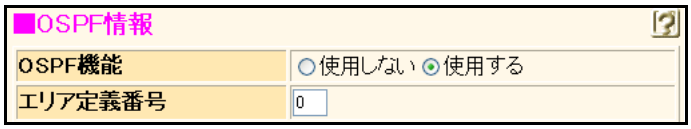
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

ルータ 5 と接続する remote 定義に OSPF 機能を設定する

7.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

8.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

9.　OSPF 機能を設定するネットワーク欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

10.　「IP 関連」をクリックします。

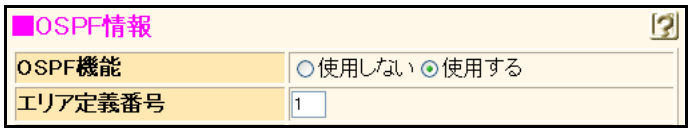
IP 関連の設定項目と「IP 基本情報」が表示されます。

11.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

12.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→1



13.　［保存］ボタンをクリックします。

OSPF 関連を設定する

14.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

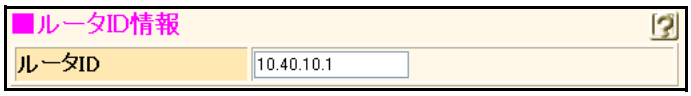
「ルーティングプロトコル情報」ページが表示されます。

15.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

16.　以下の項目を指定します。

- ルータ ID　→10.40.10.1



17.　［保存］ボタンをクリックします。

18.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

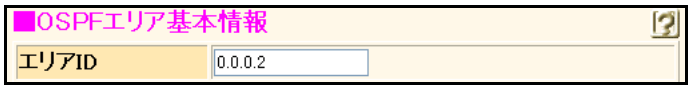
「OSPF エリア情報」が表示されます。

19.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

20.　以下の項目を指定します。

- エリア ID　→0.0.0.2



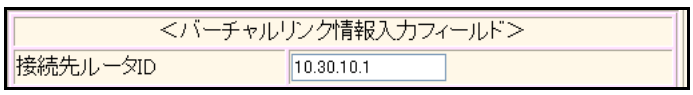
21.　［保存］ボタンをクリックします。

22.　OSPF エリア情報（0）の「バーチャルリンク情報」をクリックします。

「バーチャルリンク情報」が表示されます。

23.　以下の項目を指定します。

- 接続先ルータ ID　→10.30.10.1



24.　［追加］ボタンをクリックします。

25.　画面上部の「ルーティングプロトコル情報」をクリックします。

OSPF 関連の設定項目と「OSPF エリア基本情報」が表示されます。

26.　手順 19. ～ 21. を参考に、以下の項目を指定します。

「OSPF エリア情報（1)」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.3

27.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 5 を設定する

「ルータ 1 を設定する」を参考に、ルータ 5 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「相手情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0)」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.3

2.3.2　スタブエリアを使う

適用機種　全機種

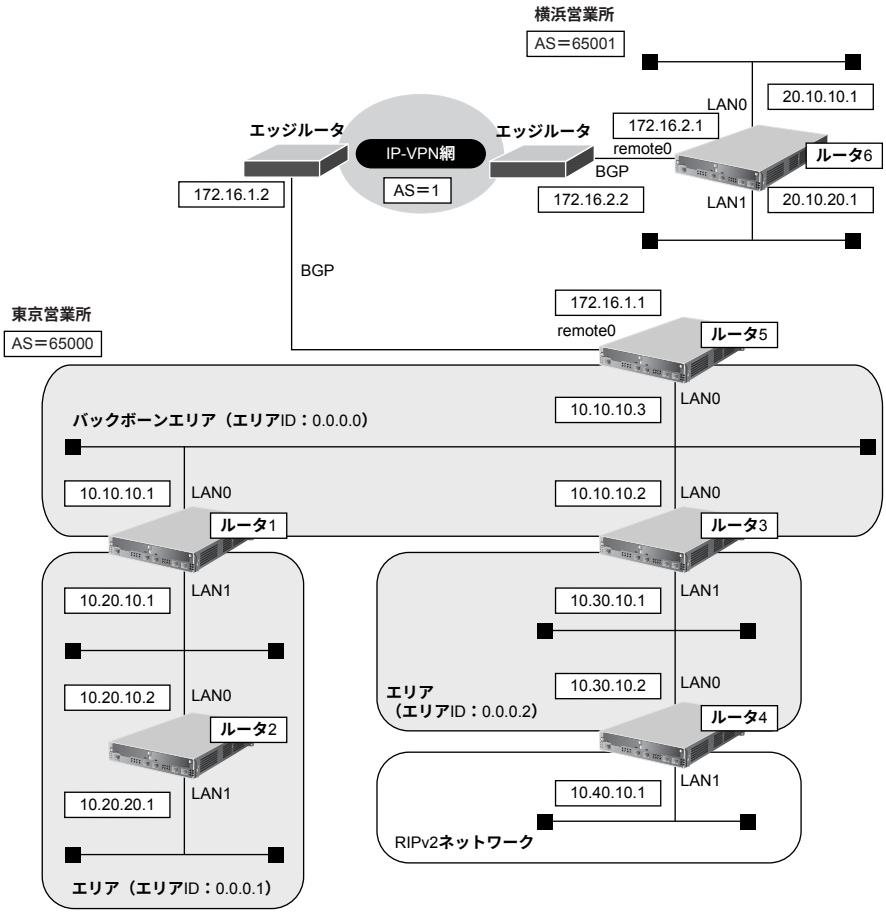
OSPF 以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

OSPF は、RIP または BGP で受信した経路情報、スタティック経路情報およびインタフェース経路情報を OSPF ネットワークに取り入れることができます。また、OSPF の経路情報を RIP および BGP で広報することができます。

OSPF 以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPF ネットワーク外の経路としてデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアから OSPF 以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア（NSSA）として運用します。

こんな事に気をつけて

OSPF 以外のネットワークと接続する場合、OSPF 以外のネットワークで使用するインタフェース経路情報を OSPF ネットワークに取り入れるように設定する必要があります。



ここでは、ルータ 5 とルータ 6 が専用線（remote 定義）で IP-VPN 網に接続され、以下のとおりに設定されていることを前提とします。

● 前提条件

- ルータ 1 からルータ 6 のすべてのインタフェースに IP アドレスを設定する
- ルータ 1 からルータ 6 のすべてのインタフェースで NAT 機能および DHCP クライアント機能を使用しない

● 設定条件

- ルータ 5 およびルータ 6 は、SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート（Si-R220B、220C の場合）で専用線に接続する

[東京営業所]

[ルータ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ　：stub

[ルータ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ　：stub

[ルータ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.2
- エリア ID 0.0.0.2 のエリアタイプ　：nssa

[ルータ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：RIP V2、OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN1 での passive-interface 設定　：設定する
- エリア ID0.0.0.2 のエリアタイプ　：nssa
- OSPF 経路の RIP での広報　：再配布する
- RIP 経路の OSPF での広報　：再配布する

[ルータ 5 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- remote 定義でのルーティングプロトコル　：BGP
- LAN0 での OSPF エリア ID　：0.0.0.0
- BGP 経路の OSPF での広報　：再配布する
- BGP AS 番号　：65000
- BGP ネットワークの IGP との同期　：同期させる
- BGP ネットワーク　：10.10.10.0/24
- BGP 集約経路　：10.0.0.0/8
- AS 外部経路の集約　：20.10.0.0/16

[横浜営業所]

[ルータ 6 でのルーティングプロトコル情報]

- BGP AS 番号　：65001
- BGP ネットワークの IGP との同期　：同期させる
- BGP ネットワーク　：20.10.10.0/24、20.10.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

東京営業所を設定する

ルータ 1 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

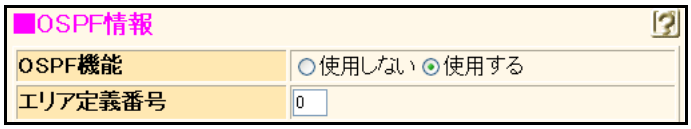
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

7.　手順 2.～6. を参考に、以下の項目を指定します。

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

OSPF 関連を設定する

8.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

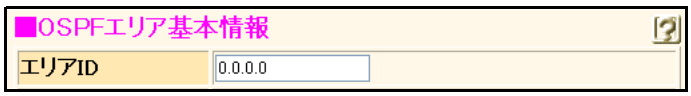
「OSPF エリア情報」が表示されます。

11.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

12.　以下の項目を指定します。

- エリア ID　→0.0.0.0



13.　［保存］ボタンをクリックします。

14.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

15.　手順 11.～13. を参考に、以下の項目を指定します。

OSPF エリア情報（1）の「OSPF エリア基本情報」

- エリア ID　→0.0.0.1
- エリア種別　→スタブエリア

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 2 を設定する

「ルータ 1 を設定する」を参考に、ルータ 2 を設定します。

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「LAN1 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1
- エリア種別　→スタブエリア

ルータ 3 を設定する

「ルータ 1 を設定する」を参考に、ルータ 3 を設定します。

「LAN0 情報」-「IP 関連」

「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「LAN1 情報」-「IP 関連」

「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

「ルーティングプロトコル情報」-「OSPF 関連」

「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.0

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.2
- エリア種別　→準スタブエリア

ルータ 4 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

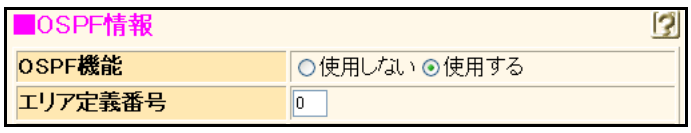
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

LAN1 情報を設定する

7.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

8.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

9.　「IP 関連」をクリックします。

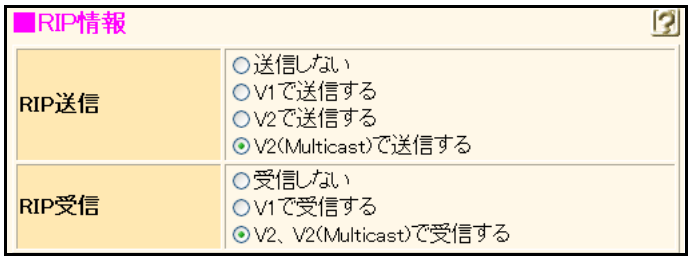
IP 関連の設定項目と「IP アドレス情報」が表示されます。

10.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

11.　以下の項目を指定します。

- RIP 送信　→V2（Multicast）で送信する
- RIP 受信　→V2、V2（Multicast）で受信する



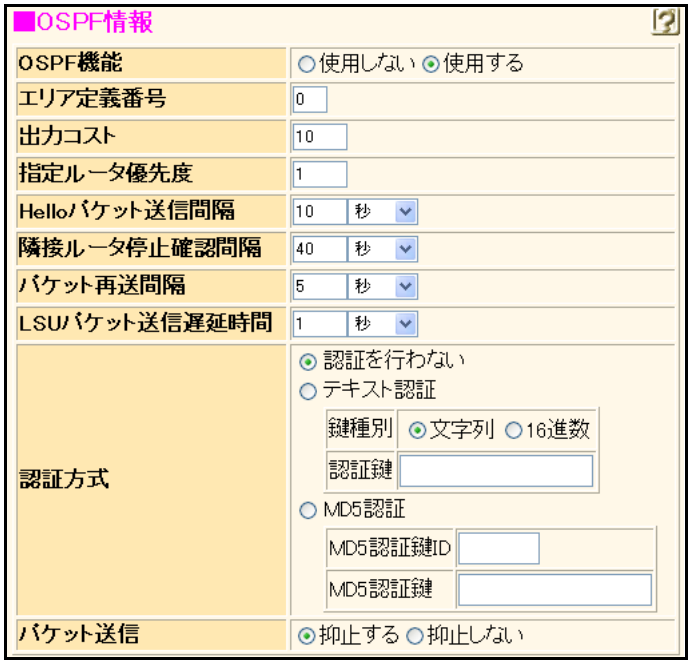
12.　［保存］ボタンをクリックします。

13.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

14.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する



15.　［保存］ボタンをクリックします。

OSPF 関連を設定する

16.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

17.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

18.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

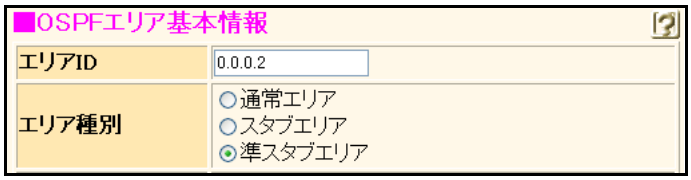
「OSPF エリア情報」が表示されます。

19.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

20.　以下の項目を指定します。

- エリア ID　→0.0.0.2
- エリア種別　→準スタブエリア



21.　［保存］ボタンをクリックします。

ルーティングマネージャ情報を設定する

22.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

23.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

24.　以下の項目を指定します。

- RIP
  OSPF 経路情報　→再配布する
- OSPF
  RIP 経路情報　→再配布する

25.　［保存］ボタンをクリックします。

26.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ルータ 5 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

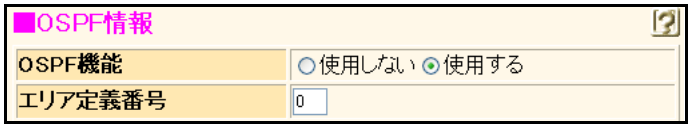
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

ルーティングマネージャ情報を設定する

7.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

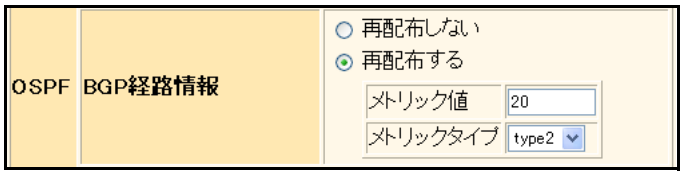
「ルーティングプロトコル情報」ページが表示されます。

8.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

9.　以下の項目を指定します。

- OSPF
  BGP 経路情報　→再配布する



10.　［保存］ボタンをクリックします。

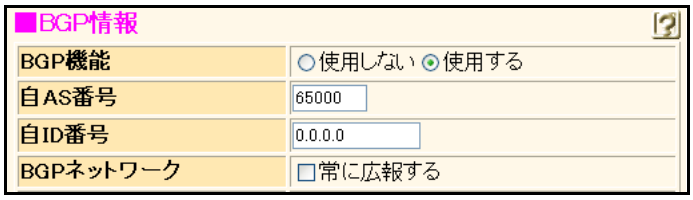
BGP 関連を設定する

11.　ルーティングプロトコル情報の設定項目の「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

12.　以下の項目を指定します。

- BGP 機能　→使用する
- 自 AS 番号　→65000
- BGP ネットワーク　→チェックしない



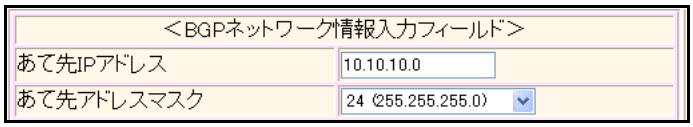
13.　［保存］ボタンをクリックします。

14.　BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。

「BGP ネットワーク情報」が表示されます。

15.　以下の項目を指定します。

- あて先 IP アドレス　→10.10.10.0
- あて先アドレスマスク　→24（255.255.255.0）



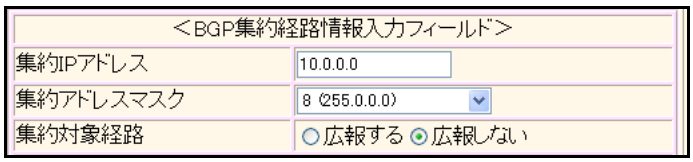
16.　［追加］ボタンをクリックします。

17.　BGP 関連の設定項目の「BGP 集約経路情報」をクリックします。

「BGP 集約経路情報」が表示されます。

18.　以下の項目を指定します。

- 集約 IP アドレス　→10.0.0.0
- 集約アドレスマスク　→8（255.0.0.0）
- 集約対象経路　→広報しない



19.　［追加］ボタンをクリックします。

20.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

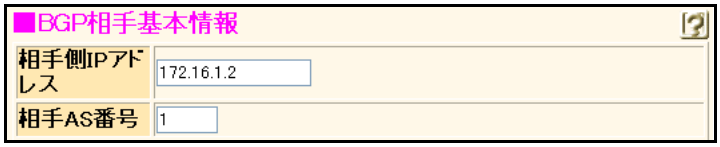
「BGP 相手情報」が表示されます。

21.　［追加］ボタンをクリックします。

BGP 相手情報（0）の設定項目と「BGP 相手基本情報」が表示されます。

22.　以下の項目を指定します。

- 相手側 IP アドレス　→172.16.1.2
- 相手 AS 番号　→1



必要に応じて上記以外の項目を指定します。

23.　［保存］ボタンをクリックします。

OSPF 関連を設定する

24.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

25.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

26.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

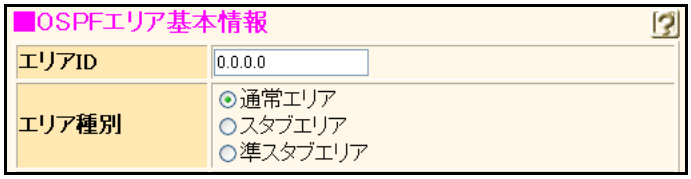
「OSPF エリア情報」が表示されます。

27.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

28.　以下の項目を指定します。

- エリア ID　→0.0.0.0
- エリア種別　→通常エリア



29.　［保存］ボタンをクリックします。

30.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

31.　「AS 外部経路集約情報」をクリックします。

「AS 外部経路集約情報」が表示されます。

32.　以下の項目を指定します。

- ネットワークアドレス　→20.10.0.0
- ネットマスク　→16（255.255.0.0）

33.　［追加］ボタンをクリックします。

34.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

横浜営業所を設定する

ルータ 6 を設定する

「ルータ 5 を設定する」を参考に、ルータ 6 を設定します。

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→65001
- BGP ネットワーク　→チェックしない

「BGP ネットワーク情報」

- あて先 IP アドレス　→20.10.10.0
- あて先アドレスマスク　→24（255.255.255.0）
- あて先 IP アドレス　→20.10.20.0
- あて先アドレスマスク　→24（255.255.255.0）

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側 IP アドレス　→172.16.2.2
- 相手 AS 番号　→1

2.4　OSPFの経路を制御する（IPv4）

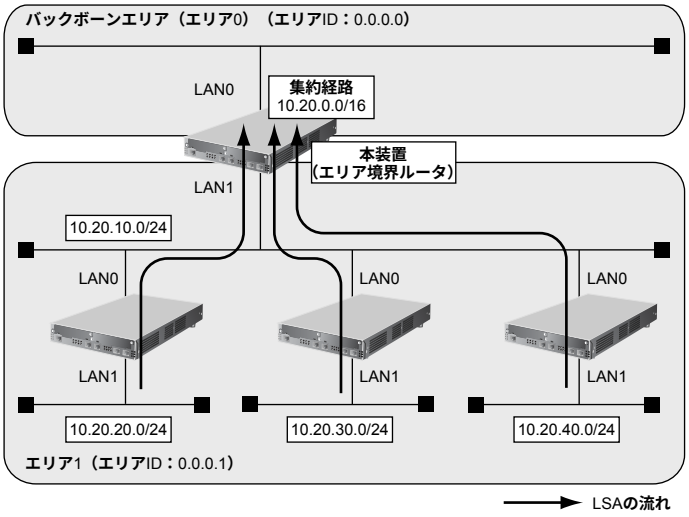
適用機種　全機種

本装置で、ほかのルータから受信する経路情報（LSA）に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

2.4.1　OSPFネットワークでエリアの経路情報（LSA）を集約する

適用機種　全機種

エリア内のLSAを、本装置（エリア境界ルータ）で集約して、バックボーンエリアへ取り込む場合の設定方法を説明します。



● 経路情報の設計

- エリア内のLSAを、本装置（エリア境界ルータ）で集約してバックボーンエリアに取り込む

● 設定条件

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのエリアID　：0.0.0.0
- LAN1でのエリアID　：0.0.0.1
- バックボーンエリアへの集約経路設定　：10.20.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN情報を設定する

1.　設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報（物理LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

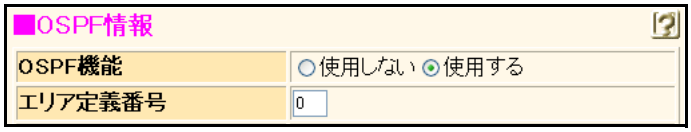
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

OSPF 関連を設定する

8.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

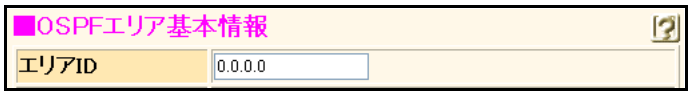
「OSPF エリア情報」が表示されます。

11.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

12.　以下の項目を指定します。

- エリア ID　→0.0.0.0



13.　［保存］ボタンをクリックします。

14.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連項目と「OSPF エリア情報」が表示されます。

15.　手順 11.～13. を参考に、以下の項目を指定します。

OSPF エリア情報（1）の「OSPF エリア基本情報」

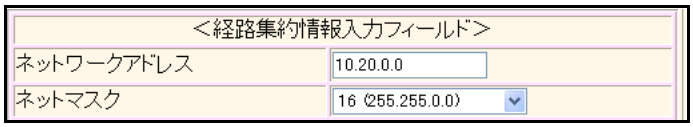
- エリア ID　→0.0.0.1

16.　OSPF エリア情報（1）の「経路集約情報」をクリックします。

「経路集約情報」が表示されます。

17.　以下の項目を指定します。

- ネットワークアドレス　　→10.20.0.0
- ネットマスク　　→16（255.255.0.0）



18.　［追加］ボタンをクリックします。

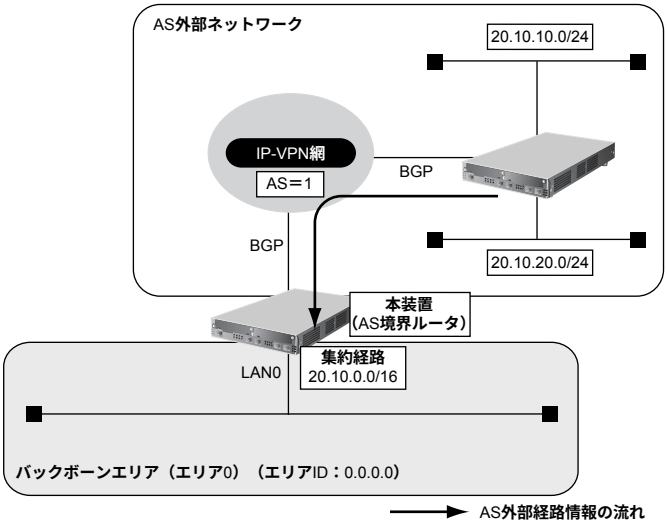
19.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.4.2　AS 外部経路を集約して OSPF ネットワークに広報する

適用機種　全機種

AS 外部（OSPF 以外）のネットワークの経路情報を本装置（AS 境界ルータ）で集約して、バックボーンエリアに広報する場合の設定方法を説明します。



● 経路情報の設計

- AS 外部経路情報を本装置（AS 境界ルータ）で集約して OSPF ネットワーク（バックボーンエリア）に広報する

● 設定条件

- LAN0 でのルーティングプロトコル　：OSPF
- remote0 でのルーティングプロトコル　：BGP
- LAN0 でのエリア ID　：0.0.0.0
- バックボーンエリアへの集約経路設定　：20.10.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

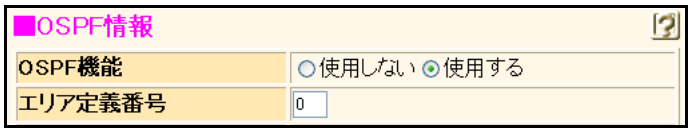
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6.　［保存］ボタンをクリックします。

OSPF 関連を設定する

7.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

8.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

9.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

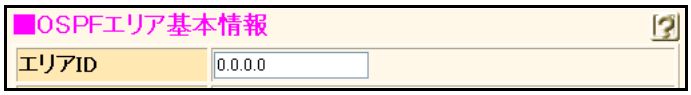
「OSPF エリア情報」が表示されます。

10.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

11.　以下の項目を指定します。

- エリア ID　→0.0.0.0



12.　［保存］ボタンをクリックします。

ルーティングマネージャ情報を設定する

13.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

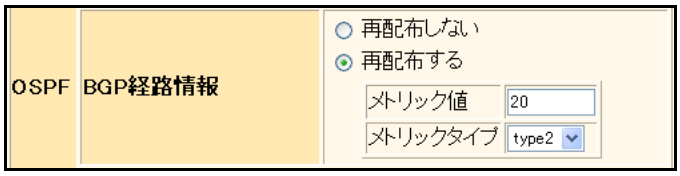
「ルーティングプロトコル情報」ページが表示されます。

14.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

15.　以下の項目を指定します。

- OSPF
  BGP 経路情報　→再配布する



16.　［保存］ボタンをクリックします。

OSPF 関連を設定する

17.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

18.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

19.　「AS 外部経路集約情報」をクリックします。

「AS 外部経路集約情報」が表示されます。

20.　以下の項目を指定します。

- ネットワークアドレス　→20.10.0.0
- ネットマスク　→16（255.255.0.0）

21.　［追加］ボタンをクリックします。

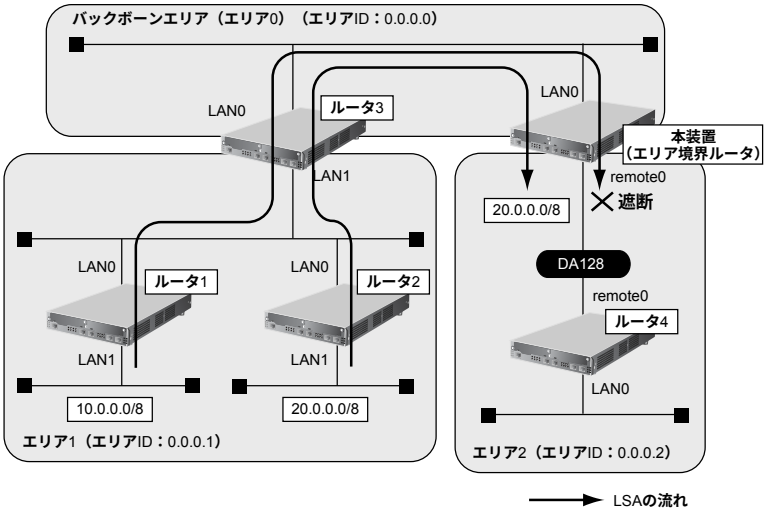
22.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.4.3　エリア境界ルータで不要な経路情報（LSA）を遮断する

適用機種　全機種

エリア境界ルータで、通信に使用しないTYPE3 サマリ LSA の経路情報を遮断する設定方法を説明します。



● 経路情報の設計

- エリア 1 の 10.0.0.0/8 のネットワークとエリア 2 のネットワークでは通信を行わないため、10.0.0.0/8 の経路情報を遮断する
- その他はすべて透過させる

● 前提条件

ここでは、本装置とルータ 4 が、専用線（remote 定義）で接続され、以下のとおりに設定されていることを前提とします。

- 本装置およびルータ 1 ～ 4 までのすべての装置で、使用するすべてのインタフェースに IP アドレスが設定されている

● 設定条件

- LAN0 でのルーティングプロトコル　：OSPF
- remote0 でのルーティングプロトコル　：OSPF
- LAN0 でのエリア ID　：0.0.0.0
- remote0 でのエリア ID　：0.0.0.2
- 10.0.0.0/8 の LSA を遮断

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3. **「IP 関連」をクリックします。**

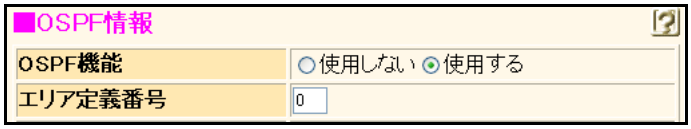
   IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. **IP 関連の設定項目の「OSPF 情報」をクリックします。**

   「OSPF 情報」が表示されます。

5. **以下の項目を指定します。**

   - OSPF 機能　→使用する
   - エリア定義番号　→0



6. **［保存］ボタンをクリックします。**

相手情報を設定する

7. **設定メニューのルータ設定で「相手情報」をクリックします。**

   「相手情報」ページが表示されます。

8. **「ネットワーク情報」をクリックします。**

   「ネットワーク情報」が表示されます。

9. **「相手情報」でネットワーク名が rmt0 の［修正］ボタンをクリックします。**

   「ネットワーク情報（rmt0）」ページが表示されます。

10. **「IP 関連」をクリックします。**

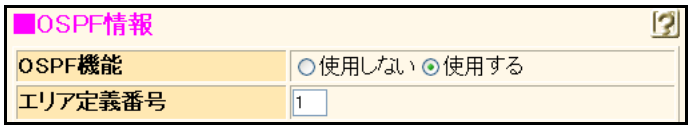
    IP 関連の設定項目と「IP 基本情報」が表示されます。

11. **IP 関連の設定項目の「OSPF 情報」をクリックします。**

    「OSPF 情報」が表示されます。

12. **以下の項目を指定します。**

    - OSPF 機能　→使用する
    - エリア定義番号　→1



13. **［保存］ボタンをクリックします。**

OSPF 関連を設定する

14. **設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。**

    「ルーティングプロトコル情報」ページが表示されます。

15. **「OSPF 関連」をクリックします。**

    OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

16. **OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**

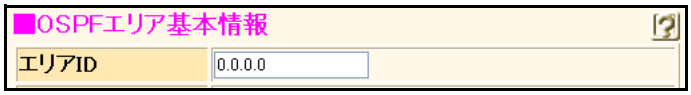
    「OSPF エリア情報」が表示されます。

17.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

18.　以下の項目を指定します。

- エリア ID　→0.0.0.0



19.　［保存］ボタンをクリックします。

20.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連項目と「OSPF エリア情報」が表示されます。

21.　手順 17. ～ 19. を参考に、以下の項目を指定します。

OSPF エリア情報（1）の「OSPF エリア基本情報」

- エリア ID　→0.0.0.2

22.　画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連項目と「OSPF エリア情報」が表示されます。

23.　エリア定義番号（1）の［修正］ボタンをクリックします。

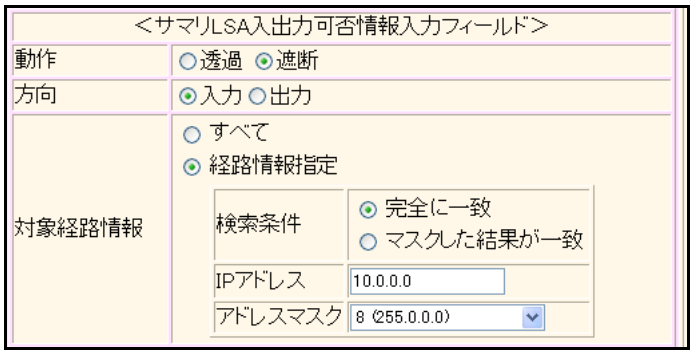
OSPF エリア情報（1）関連項目と「OSPF エリア基本情報」が表示されます。

24.　OSPF エリア情報（1）関連項目の「サマリ LSA 入出力可否情報」をクリックします。

「サマリ LSA 入出力可否情報」が表示されます。

25.　以下の項目を指定します。

- 動作　→遮断
- 方向　→入力
- 対象経路情報　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→10.0.0.0
  アドレスマスク　→8（255.0.0.0）



26.　［追加］ボタンをクリックします。

27.　手順 25. ～ 26. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→入力
- 対象経路情報　→すべて

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.5　OSPF 機能を使う（IPv6）

適用機種　*Si-R180B, 220C, 240B, 570*

2.5.1　OSPF ネットワークを構築する

適用機種　*Si-R180B, 220C, 240B, 570*

OSPF（IPv6）を使用したネットワークの構築について説明します。

⚠注意

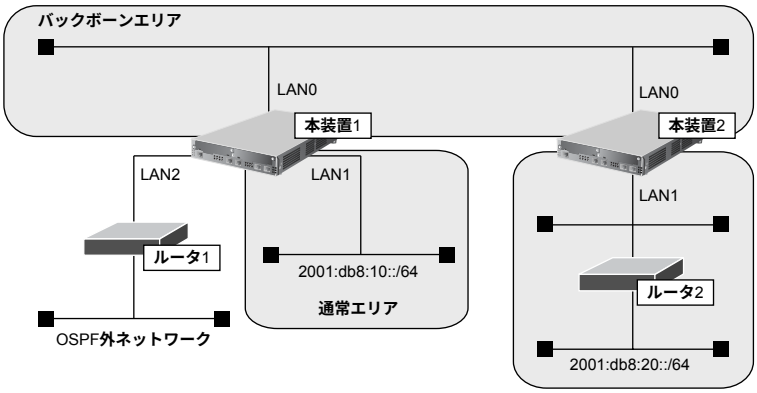
OSPF 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF 機能は使用しないでください。

こんな事に気をつけて

- ルータは、各エリアに 30 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2 つ以上のエリアの指定ルータ（DR：Designated Router）とならないように設定してください。
- LAN を使用した隣接 OSPF ルータと MTU 値が一致しない場合は、隣接関係を構築できません。
- 経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができても、OSPF の経路は、経路情報に反映されません。
- 本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません（LSDB オーバフロー）。
  また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源を再投入したり、［設定反映］ボタンや［再起動］ボタンをクリックしたりしても、正常に通信できるまでに最大 60 分かかることがあります。
- OSPF で使用するインタフェースは、以下の条件で使用してください。

	本装置が DR を兼務する場合	本装置が DR を兼務しない場合
Si-R180B、220C、240B	（10000 ÷本装置保有 LSA 数）未満	（20000 ÷本装置保有 LSA 数）未満
Si-R570	（15000 ÷本装置保有 LSA 数）未満	（30000 ÷本装置保有 LSA 数）未満

  また、通信速度 15Kbps 以上の通信帯域を確保する必要があります。
- OSPF（IPv6）機能を Si-R570 で使用する場合は、拡張用 512M メモリモジュールが必要です。



● 前提条件

- 本装置1、2のすべてのインタフェースでIPv6機能を利用する設定がされている
- 本装置1のLAN1には、グローバルアドレスが設定されている
- 本装置1のLAN2には、OSPF外ネットワークへの経路がスタティック設定されている

● 設定条件

- 本装置1はバックボーンエリアと通常エリアのエリア境界ルータであり、かつ、OSPF外ネットワークへ到達するためのAS境界ルータとして運用する
- 本装置2はバックボーンエリアとスタブエリアのエリア境界ルータとして運用する。また、バックボーンエリアでは指定ルータとして運用する
- 各エリアIDは、以下のとおり

  バックボーンエリア　: 0.0.0.0
  通常エリア　: 0.0.0.1
  スタブエリア　: 0.0.0.2

[本装置1]

- LAN0はバックボーンエリアに属する
- LAN1は通常エリアに属し、ほかにルータが接続されていないため、Passive-interfaceとしてOSPFパケットを送信しないようにする
- OSPFルータIDは 100.0.0.1 とする
- スタティック経路をOSPFに再配布する

[本装置2]

- LAN0はバックボーンエリアに属し、バックボーンエリアの指定ルータとするため、指定ルータ優先度に255を設定する
- LAN1はスタブエリアとする
- OSPFルータIDは 100.0.0.2 とする

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

LAN情報を設定する

1.　設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報（物理LAN）」ページが表示されます。

3.　「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4.　IPv6関連の設定項目の「IPv6 OSPF情報」をクリックします。

「IPv6 OSPF情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0

6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

「LAN1 情報（物理 LAN）」-「IPv6 関連」-「IPv6 OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1
- パケット送信　→抑止する

IPv6 OSPF 関連を設定する

8.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

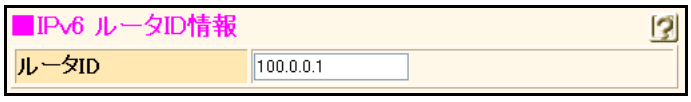
「ルーティングプロトコル情報」ページが表示されます。

9.　「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

10.　以下の項目を指定します。

- ルータ ID　→100.0.0.1



11.　［保存］ボタンをクリックします。

12.　IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。

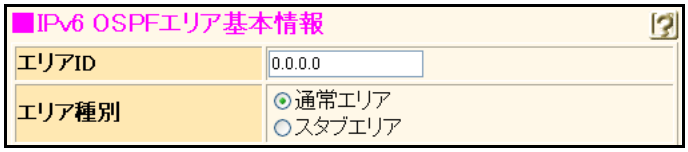
「IPv6 OSPF エリア情報」が表示されます。

13.　［追加］ボタンをクリックします。

IPv6 OSPF エリア情報（0）の「IPv6 OSPF エリア基本情報」が表示されます。

14.　以下の項目を指定します。

- エリア ID　→0.0.0.0
- エリア種別　→通常エリア



15.　［保存］ボタンをクリックします。

16.　画面上部のルーティングプロトコル情報をクリックします。

IPv6 OSPF 関連項目と「IPv6 OSPF エリア情報」が表示されます。

17.　手順 13. ～ 15. を参考に、以下の項目を指定します。

- エリア ID　→0.0.0.1
- エリア種別　→通常エリア

ルーティングマネージャ情報を設定する

18.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

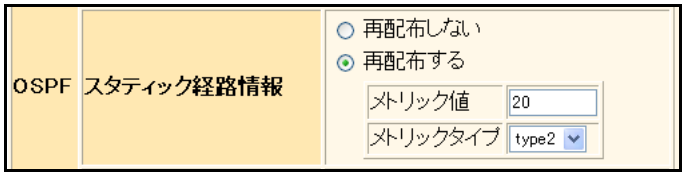
「ルーティングプロトコル情報」ページが表示されます。

19.　「IPv6 ルーティングマネージャ情報」をクリックします。

IPv6 ルーティングマネージャ情報の設定項目と「IPv6 再配布情報」が表示されます。

20.　以下の項目を指定します。

- OSPF
  スタティック経路情報　→再配布する



21.　［保存］ボタンをクリックします。

22.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「LAN0 情報」-「IPv6 関連」

「IPv6 OSPF 情報」

- OSPF 機能　→ 使用する
- エリア定義番号　→0
- 指定ルータ優先度　→255

「LAN1 情報」-「IPv6 関連」

「IPv6 OSPF 情報」

- OSPF 機能　→ 使用する
- エリア定義番号　→1

「ルーティングプロトコル情報」-「IPv6 OSPF 関連」

「IPv6 ルータ ID 情報」

- ルータ ID　→100.0.0.2

「IPv6 OSPF エリア情報（0）」-「IPv6 OSPF 基本情報」

- エリア ID　→0.0.0.0
- エリア種別　→通常エリア

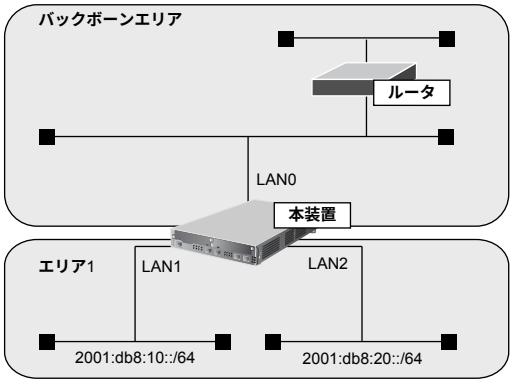
「IPv6 OSPF エリア情報（1）」-「IPv6 OSPF 基本情報」

- エリア ID　→0.0.0.2
- エリア種別　→スタブエリア

2.5.2　エリア境界ルータでエリア内部経路を集約する

適用機種　***Si-R180B,220C,240B,570***

エリア境界ルータで、エリア内経路を集約してほかのエリアに広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- 本装置はバックボーンエリアとエリア 1 のエリア境界ルータとして運用し、LAN0、LAN1、LAN2 で OSPF を使用する
- OSPF ルータ ID は、100.0.0.1
- 各エリア ID は、以下のとおり
  バックボーンエリア　: 0.0.0.0（エリア定義番号 0）
  エリア 1　: 0.0.0.1（エリア定義番号 1）
- 各インタフェースの IP アドレスは、以下のとおり
  LAN1　: 2001:db8:10::1/64
  LAN2　: 2001:db8:20::1/64

● 設定条件

- エリア 1 のエリア内部経路（2001:db8:10::/64、2001:db8:20::/64）は、集約経路（2001:db8::/32、コスト 100）としてバックボーンエリアに広報する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

IPv6 OSPF 関連を設定する

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

2.　「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

3.　IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。

「IPv6 OSPF エリア情報」が表示されます。

4.　エリア定義番号1の［修正］ボタンをクリックします。

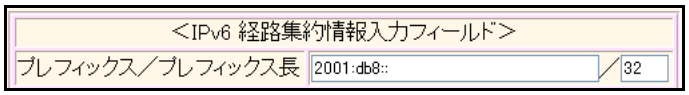
IPv6 OSPF エリア情報（1）の「IPv6 OSPF エリア基本情報」が表示されます。

5.　「IPv6 経路集約情報」をクリックします。

「IPv6 経路集約情報」が表示されます。

6.　以下の項目を指定します。

- プレフィックス／プレフィックス長　→2001:db8::/32



7.　［追加］ボタンをクリックします。

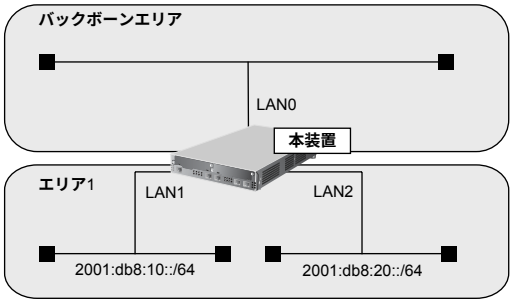
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.5.3　エリア境界ルータで不要な経路情報を遮断する

適用機種　*Si-R180B,220C,240B,570*

エリア境界ルータで、ほかのエリアに対し特定のエリア内経路（エリア間プレフィックス LSA）を遮断して広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- 本装置はバックボーンエリアとエリア 1 のエリア境界ルータとして運用し、LAN0、LAN1、LAN2 で OSPF を使用する
- OSPF ルータ ID は、100.0.0.1
- 各エリア ID は、以下のとおり
  バックボーンエリア　: 0.0.0.0（エリア定義番号 0）
  エリア 1　: 0.0.0.1（エリア定義番号 1）
- 各インタフェースの IP アドレスは、以下のとおり
  LAN1　: 2001:db8:10::1/64
  LAN2　: 2001:db8:20::1/64

● 設定条件

- エリア 1 からバックボーンエリアへの広報で、2001:db8:20::/64 は破棄し、その他のエリア内部経路は透過させる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

2.　「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

3.　IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。

「IPv6 OSPF エリア情報」が表示されます。

4.　エリア定義番号 1 の［修正］ボタンをクリックします。

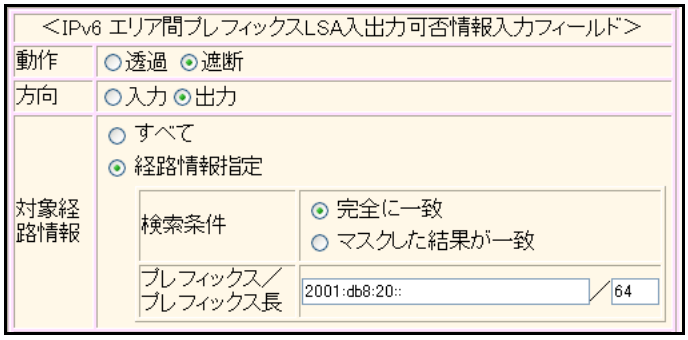
IPv6 OSPF エリア情報（1）の「IPv6 OSPF エリア基本情報」が表示されます。

5.　「IPv6 エリア間プレフィックス LSA 入出力可否情報」をクリックします。

「IPv6 エリア間プレフィックス LSA 入出力可否情報」が表示されます。

6.　以下の項目を指定します。

- 動作　→遮断
- 方向　→出力
- 対象経路情報　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→ 2001:db8:20::/64



7.　［追加］ボタンをクリックします。

8.　手順 6.～7. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→出力
- 対象経路情報　→すべて

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.6　BGP の経路を制御する（IPv4）

適用機種　全機種

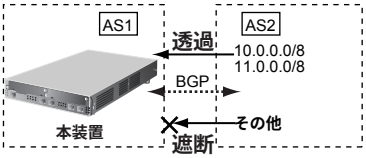
本装置を経由して、ほかのルータに送受信する経路情報に変更を加えることで、意図的にトラフィックを制御することができます。

参照　Si-R シリーズ　機能説明書「2.4 BGP4 機能」（P.33）

2.6.1　特定の経路情報の受信を透過させる

適用機種　全機種

通信が必要なネットワークに限定して経路を透過させる場合の設定方法を説明します。



● 経路情報の設計

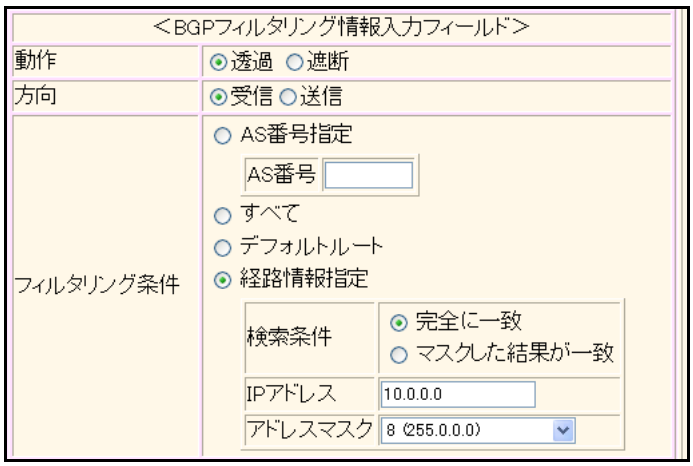
- 10.0.0.0/8 のネットワークの経路情報を透過
- 11.0.0.0/8 のネットワークの経路情報を透過
- その他はすべてを遮断

上記の経路情報に従って設定する場合の設定例を示します。

1. **設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。**
   「ルーティングプロトコル情報」のページが表示されます。
2. **「BGP 関連」をクリックします。**
   BGP 関連の設定項目と「BGP 情報」が表示されます。
3. **BGP 関連の設定項目の「BGP 相手情報」をクリックします。**
   「BGP 相手情報」が表示されます。
4. **フィルタリング設定を行う BGP 相手情報の［修正］ボタンまたは［追加］ボタンをクリックします。**
   BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。
5. **BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。**
   「BGP フィルタリング情報」が表示されます。

6.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 10.0.0.0
  アドレスマスク　→ 8（255.0.0.0）



7.　［追加］ボタンをクリックします。

優先順位 1 の定義が追加されます。

8.　手順 6.～7. を参考に、以下の項目を優先順位 2 の定義として指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 11.0.0.0
  アドレスマスク　→ 8（255.0.0.0）

9.　手順 6.～7. を参考に、以下の項目を優先順位 3 の定義として指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→すべて

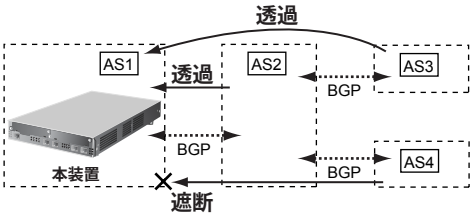
10.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.6.2　特定の AS からの経路情報の受信を遮断する

適用機種　全機種

フルルートを受信するネットワーク（トランジット）に接続されている場合、特定の経路情報を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS4 からの経路情報を遮断
- その他はすべて透過

上記の経路情報に従って設定する場合の設定例を示します。

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」のページが表示されます。

2.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

3.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

4.　フィルタリング設定を行う BGP 相手情報の［修正］ボタンまたは［追加］ボタンをクリックします。

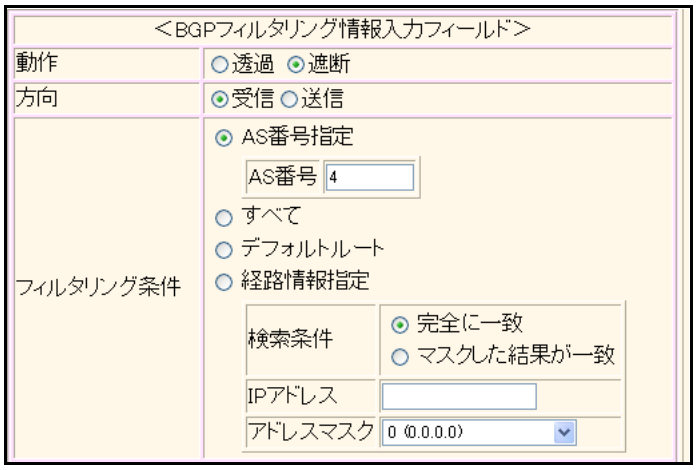
BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。

5.　BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。

「BGP フィルタリング情報」が表示されます。

6.　以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→AS 番号指定
  AS 番号　→4



7.　［追加］ボタンをクリックします。

優先順位 1 の定義が追加されます。

8.　手順 6. ～ 7. を参考に、以下の項目を優先順位 2 の定義として指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて

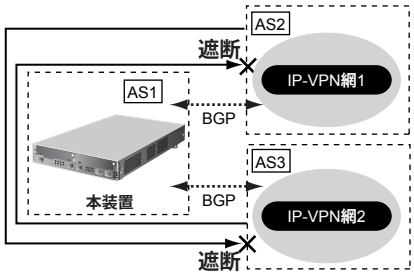
9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.6.3　IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する

適用機種　全機種

異なる IP-VPN 網を使用し、冗長化ネットワークを構成する場合、IP-VPN 網 1 から受信した経路情報の IP-VPN 網 2 への送信を遮断、および IP-VPN 網 2 から受信した経路情報の IP-VPN 網 1 への送信を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS2 から AS3 への経路情報を遮断
- AS3 から AS2 への経路情報を遮断

上記の経路情報に従って設定する場合の設定例を示します。

AS2 への広報時の BGP フィルタリングを設定する

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」のページが表示されます。

2.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

3.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

4.　フィルタリング設定を行う BGP 相手情報の［修正］ボタンまたは［追加］ボタンをクリックします。

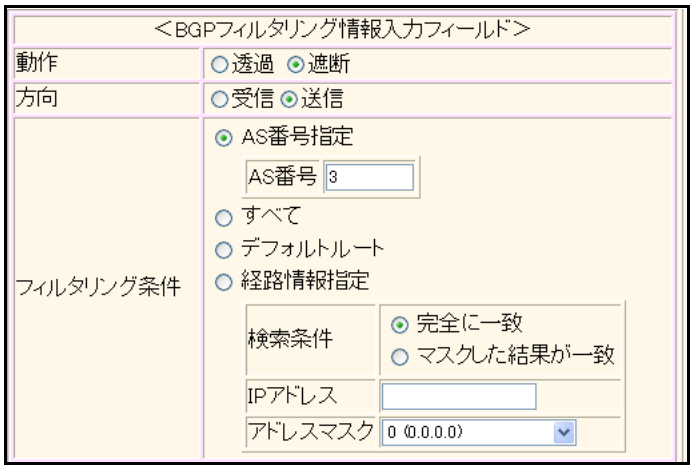
BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。

5.　BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。

「BGP フィルタリング情報」が表示されます。

6.　以下の項目を指定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→AS 番号指定
  AS 番号　→3



7.　［追加］ボタンをクリックします。

優先順位 1 の定義が追加されます。

8.　手順 6. ～ 7. を参考に、以下の項目を指定します。

BGP 相手情報（0）の優先順位 2 の定義

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて

AS3 への広報時の BGP フィルタリングを設定する

9.　「AS2 への広報時の BGP フィルタリングを設定する」を参考に、以下の項目を指定します。

BGP 相手情報（1）の優先順位 1 の定義

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→AS 番号指定
  AS 番号　→2

BGP 相手情報（1）の優先順位 2 の定義

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて

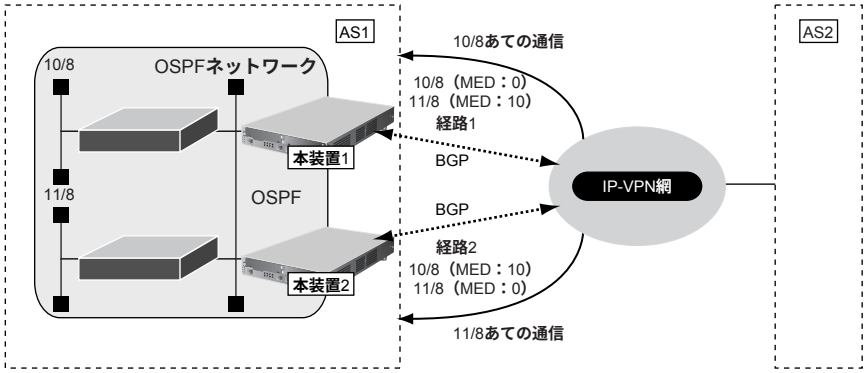
10.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.6.4　冗長構成の通信経路を使用する

適用機種　全機種

IP-VPN 網に接続する経路を 2 つ使用した冗長構成で、通信の負荷分散および通信網異常による経路切り替えを行う場合の設定方法を説明します。



● 経路情報の設計

- OSPF ネットワークである AS1 で IP-VPN 網を経由した AS2 への通信経路を冗長化する
- 10/8 への通信は経路 1 を優先経路とし、11/8 への通信経路は経路 2 を優先経路とする。それぞれの経路で異常が発生した場合、異常が発生していない経路に切り替わる。優先順位を設定するときは MED メトリック値を使用する
- AS1 内の OSPF ネットワークでの経路変更は BGP で AS2 に広報する

上記の経路情報に従って設定する場合の設定例を示します。

本装置 1 を設定する

ルーティングプロトコル情報を設定する

1.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」のページが表示されます。

2.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

3.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

4.　フィルタリング設定を行う BGP 相手情報の［修正］ボタンまたは［追加］ボタンをクリックします。

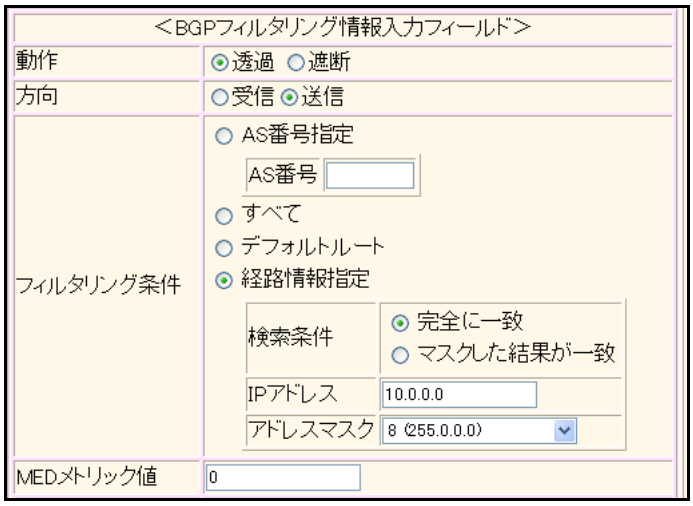
BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。

5.　BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。

「BGP フィルタリング情報」が表示されます。

6.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 10.0.0.0
  アドレスマスク　→ 8（255.0.0.0）
- MED メトリック値　→ 0



7.　［追加］ボタンをクリックします。

優先順位 1 の定義が追加されます。

8.　手順 6.～7. を参考に、以下の項目を優先順位 2 の定義として指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 11.0.0.0
  アドレスマスク　→ 8（255.0.0.0）
- MED メトリック値　→ 10

9.　手順 6.～7. を参考に、以下の項目を優先順位 3 の定義として指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて

10.　画面上部の「ルーティングプロトコル情報」をクリックします。

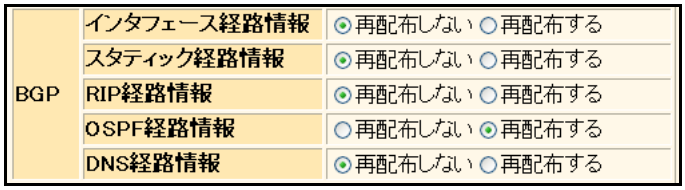
「ルーティングプロトコル情報」ページが表示されます。

11.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

12.　以下の項目を指定します。

- BGP
  OSPF 経路情報　→再配布する



13.　［保存］ボタンをクリックします。

14.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「ルーティングプロトコル情報」-「BGP 関連」

「BGP フィルタリング情報」

BGP 相手情報（0）の優先順位 1 の定義

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 10.0.0.0
  アドレスマスク　→ 8（255.0.0.0）
- MED メトリック値　→ 10

BGP 相手情報（0）の優先順位 2 の定義

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 11.0.0.0
  アドレスマスク　→ 8（255.0.0.0）
- MED メトリック値　→ 0

BGP 相手情報（0）の優先順位 3 の定義

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」

「再配布情報」

- BGP
  OSPF 経路情報　→再配布する

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- BGP/MPLS VPN 機能では、BGP フィルタリング情報は無効となります。
- 送信時のフィルタを設定した場合、相手装置に広報する MED メトリック値、AS パスプリペンドはフィルタの設定値が使用されます。
- MED メトリック値の設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- AS パスプリペンドの設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- BGP 使用中に［設定反映］をクリックした場合、接続中のセッションが一度切断されることがあります。

2.7　事業所間を MPLS 接続サービスを利用して接続する

適用機種　全機種

本装置では MPLS の LSP（label Switching Path：トンネルラベルスイッチングパス）をトンネルとしてインタフェースに対応させるため、シェーピングや帯域制御などの機能を LSP ごとに使用することができます（MPLS LSP トンネル）。

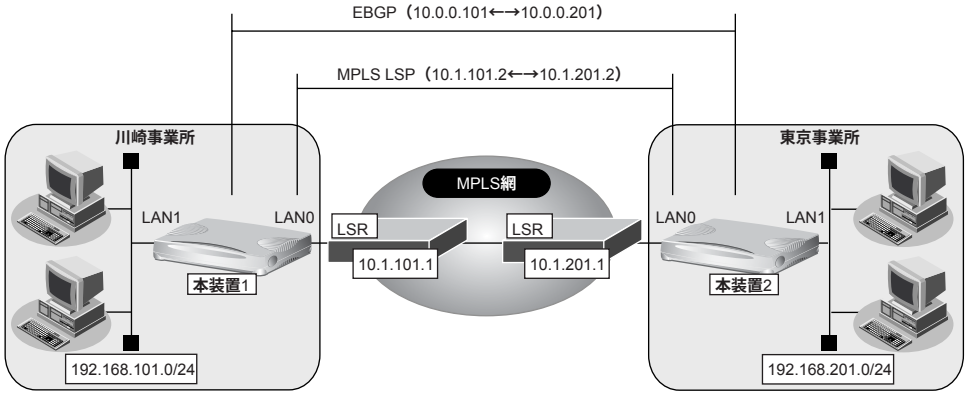
ここでは、MPLS 接続サービス（キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送サービスを想定しています）と本装置の MPLS LSP トンネルを使用して、事業所の間を接続する場合の設定方法を説明します。

こんな事に気をつけて

- **隣接 LSR は、ダイナミックルーティングを用いて最適経路から決定することはできません。**MPLS LSP **の送出先の設定と** MPLS LSP **での次ホップのラベルスイッチルータの設定で静的に指定する必要があります。**
- MPLS LSP **トンネルでは、**IPv4、IPv6 **のプロトコルだけをサポートしています。ブリッジは使用できません。**MPLS LSP **トンネル上にさらにラベルをスタックできるのは、**BGP/MPLS VPN **機能だけです。**LDP over LDP **の形態はサポートしていません。**MPLS LSP **トンネルを使用するインタフェースでは、**MPLS **を利用しないように設定してください。**
- MPLS LSP **トンネルで** IPv6 **通信を行う場合は、2 層目のラベルスタックに** IPv6 Explicit NULL **ラベルを用いた多重スタックとなります。また、**MPLS TTL **伝達の設定で指定した値に関係なく、**TTL **の継承は行われません。**
- **複数の** MPLS LSP **トンネルを使用する場合は、それぞれ別の自側トンネルエンドポイントアドレスと相手側トンネルエンドポイントアドレスを設定してください。同じ自側トンネルエンドポイントアドレスが複数設定されている場合は、それぞれの** LSP **で受信したパケットが期待した** LSP **のインタフェースとは別のインタフェースで受信されてしまうため、受信インタフェースに依存して動作する** IP **フィルタリング機能、**TOS **値書き換え機能、**NAT **機能、マルチキャスト機能、ダイナミックルーティング（**RIP、OSPF**）機能などは正しく動作しません。**
- **複数の** MPLS LSP **トンネルで相手側トンネルエンドポイントアドレスの設定が同じアドレスであった場合は、**MPLS LSP **の送出先の設定と** MPLS LSP **での次ホップのラベルスイッチルータは同じ値を設定してください。違う値を設定した場合、どれかの値だけが使用されます。**
- MPLS **通信で、優先制御機能、**EXP **値書き換え機能、およびシェーピング機能を利用する場合は、**MPLS LSP **トンネルを使用してください。**

2.7.1 トンネルエンドポイントをインタフェースアドレスにして MPLS LSP を使用する

適用機種　全機種



● 前提条件

[本装置 1]

- LAN0 が MPLS 網、LAN1 が事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS 網とのラベル交換はインタフェースアドレスに対して行う
- 本装置 1 と本装置 2 の間は、EBGP でループバックインタフェースどうしで経路情報を交換する

[本装置 2]

- LAN0 が MPLS 網、LAN1 が事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS 網とのラベル交換は、インタフェースアドレスに対して行う
- 本装置 2 と本装置 1 の間は、EBGP でループバックインタフェースどうしで経路情報を交換する

● 設定条件

[本装置 1]

- LAN0（MPLS 網側）の IP アドレス　：10.1.101.2
- 接続する MPLS 網の次ホップ LSR の IP アドレス　：10.1.101.1
- LAN1（事業所内側）の IP アドレス　：192.168.101.1
- ループバックインタフェースの IP アドレス　：10.0.0.101
- 本装置 1 の属する AS 番号　：101
- 本装置 2 の属する AS 番号　：201

[本装置 2]

- LAN0（MPLS 網側）の IP アドレス　：10.1.201.2
- 接続する MPLS 網の次ホップ LSR の IP アドレス　：10.1.201.1
- LAN1（事業所内側）の IP アドレス　：192.168.201.1
- ループバックインタフェースの IP アドレス　：10.0.0.201
- 本装置 2 の属する AS 番号　：201
- 本装置 1 の属する AS 番号　：101

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

MPLS 網との接続情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

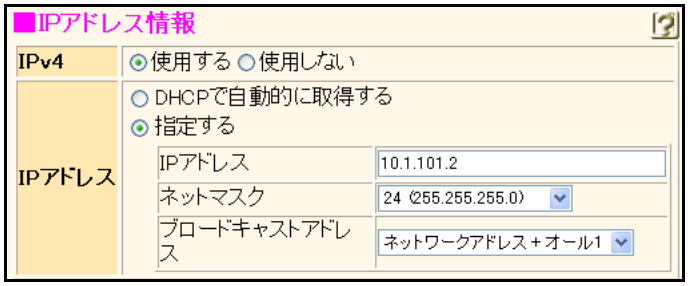
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.1.101.2
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

6.　「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

7.　以下の項目を指定します。

- MPLS 機能　→使用する
- ラベル配布プロトコル　→ LDP

8.　［保存］ボタンをクリックします。

9.　設定メニューのルータ設定で「MPLS 情報」をクリックします。

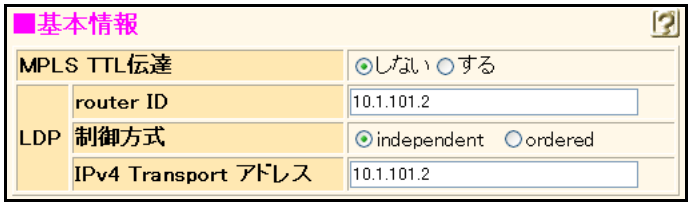
「MPLS 情報」ページが表示されます。

10.　「基本情報」をクリックします。

「基本情報」が表示されます。

11.　以下の項目を指定します。

- MPLS TTL 伝達　→しない
- LDP
  router ID　→10.1.101.2
  制御方式　→independent
  IPv4 Transport アドレス　→10.1.101.2



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

14.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

15.　以下の項目を指定します。

- LDP
  インタフェース経路情報　→再配布しない
  RIP 経路情報　→再配布しない
  OSPF 経路情報　→再配布しない

16.　［保存］ボタンをクリックします。

MPLS トンネルを設定する

17.　設定メニューのルータ設定で「相手情報」をクリックします。

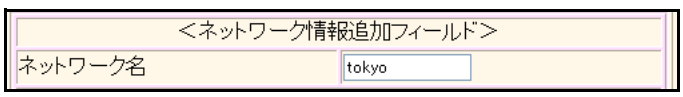
「相手情報」ページが表示されます。

18.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

19.　以下の項目を指定します。

- ネットワーク名　→tokyo



20.　［追加］ボタンをクリックします。

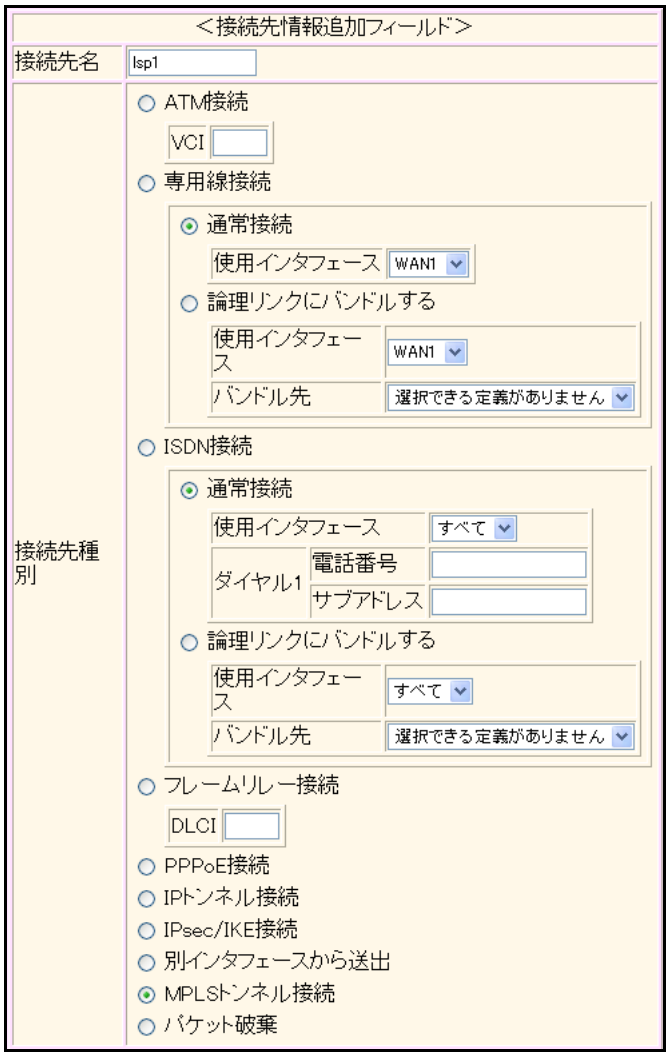
「ネットワーク情報（tokyo）」ページが表示されます。

21.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

22.　以下の項目を指定します。

- 接続先名　→lsp1
- 接続先種別　→MPLS トンネル接続



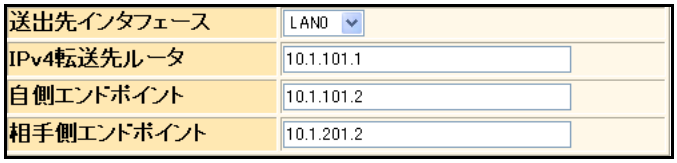
機種により、接続先種別の表示が上記の画面とは異なります。

23.　［追加］ボタンをクリックします。

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

24.　以下の項目を指定します。

- 送出先インタフェース　→LAN0
- IPv4 転送先ルータ　→10.1.101.1
- 自側エンドポイント　→10.1.101.2
- 相手側エンドポイント　→10.1.201.2



25.　［保存］ボタンをクリックします。

ループバックインタフェースを設定する

26.　設定メニューの基本設定で「装置情報」をクリックします。

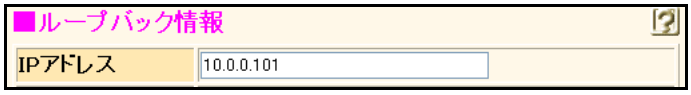
「装置情報」ページが表示されます。

27.　「ループバック情報」をクリックします。

「ループバック情報」が表示されます。

28.　以下の項目を指定します。

- IPアドレス　→10.0.0.101



29.　［保存］ボタンをクリックします。

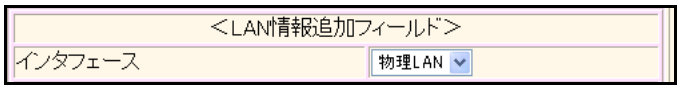
LAN1 情報を設定する

30.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

31.　以下の項目を指定します。

- インタフェース　→物理 LAN



32.　［追加］ボタンをクリックします。

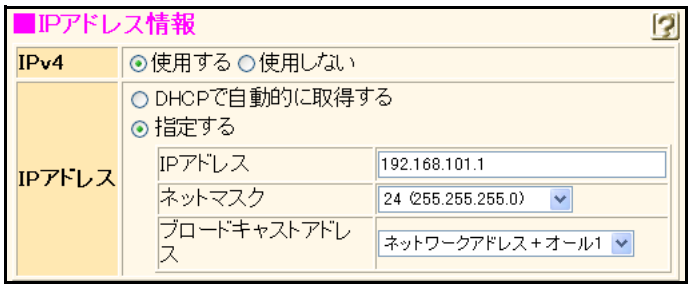
「LAN1 情報（物理 LAN）」ページが表示されます。

33.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

34.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.101.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



35.　［保存］ボタンをクリックします。

本装置 1 との間で経路交換を設定する

36.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

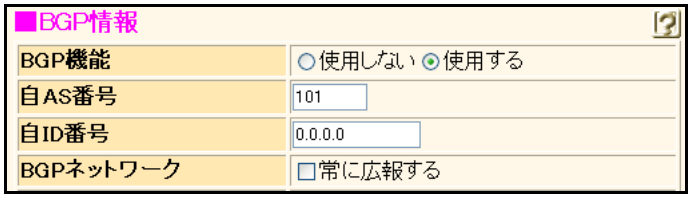
「ルーティングプロトコル情報」ページが表示されます。

37.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

38.　以下の項目を指定します。

- BGP 機能　→使用する
- 自 AS 番号　→ 101
- BGP ネットワーク　→チェックしない



39.　［保存］ボタンをクリックします。

40.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

41.　［追加］ボタンをクリックします。

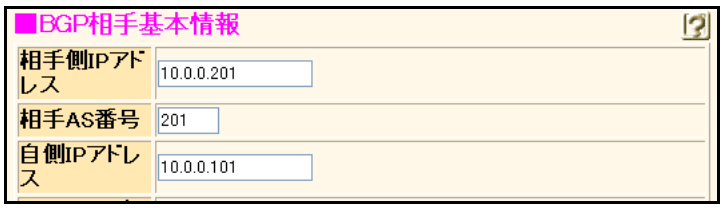
BGP 相手情報（0）の設定項目と「BGP 相手基本情報」が表示されます。

42.　以下の項目を指定します。

- 相手側 IP アドレス　→ 10.0.0.201
- 相手 AS 番号　→ 201
- 自側 IP アドレス　→ 10.0.0.101

こんな事に気をつけて

- ルートリフレクタの IP アドレスを相手側 IP アドレスに設定してください。
- 自側 IP アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。



43.　［保存］ボタンをクリックします。

44.　BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。

「BGP ネットワーク情報」が表示されます。

45.　以下の項目を指定します。

- あて先 IP アドレス　→192.168.101.0
- あて先アドレスマスク　→24（255.255.255.0）

46.　［追加］ボタンをクリックします。

47.　BGP 相手情報（0）の設定項目の「BGP 拡張機能情報」をクリックします。

「BGP 拡張機能情報」が表示されます。

48.　以下の項目を指定します。

- エンフォースマルチホップ　→使用する

49.　［保存］ボタンをクリックします。

50.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

51.　「ネットワーク情報」で相手定義番号が 0 の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

52.　「IP 関連」をクリックします。

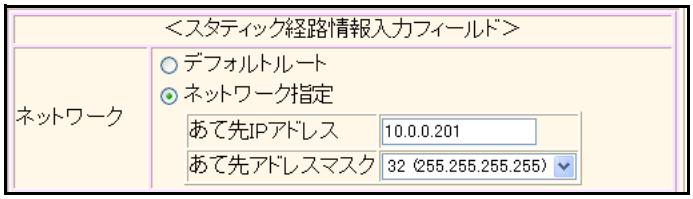
IP 関連の設定項目と「IP 基本情報」が表示されます。

53.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

54.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→10.0.0.201
  あて先アドレスマスク　→32（255.255.255.255）



55.　［追加］ボタンをクリックします。

56.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

MPLS 網との接続情報を設定する

「LAN0 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.1.201.2
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「LAN0 情報（物理 LAN）」-「MPLS 関連」

「MPLS 基本情報」

- MPLS 機能　→使用する
  ラベル配布プロトコル　→ LDP

「MPLS 情報」

「基本情報」

- MPLS TTL 伝達　→しない
  router ID　→ 10.1.201.2
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.1.201.2

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」

「再配布情報」

- LDP
  インタフェース経路情報　→再配布しない
  RIP 経路情報　→再配布しない
  OSPF 経路情報　→再配布しない

MPLS トンネルを設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ kawasaki

「ネットワーク情報」-「接続先情報」

- 接続先名　→ lsp1
- 接続先種別　→ MPLS トンネル接続

「接続先情報」-「MPLS トンネル接続」

「基本情報」

- 送出先インタフェース　→ LAN0
- IPv4 転送先ルータ　→ 10.1.201.1
- 自側エンドポイント　→ 10.1.201.2
- 相手側エンドポイント　→ 10.1.101.2

ループバックインタフェースを設定する

「装置情報」-「ループバック情報」

- IPアドレス　→10.0.0.201

LAN1 情報を設定する

「LAN1 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.201.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN1 情報（物理 LAN）」-「MPLS 関連」

「MPLS 基本情報」

- MPLS 機能　→使用する
  ラベル配布プロトコル　→LDP

本装置 1 との間で経路交換を設定する

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→201

「BGP 相手情報」

「BGP 相手基本情報」

- 相手側 IP アドレス　→10.0.0.101
- 相手 AS 番号　→101
- 自側 IP アドレス　→10.0.0.201

「BGP 拡張機能情報」

- エンフォースマルチホップ　→使用する

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」

「再配布情報」

- BGP
  インタフェース経路情報　→再配布する

「相手情報」-「ネットワーク情報」

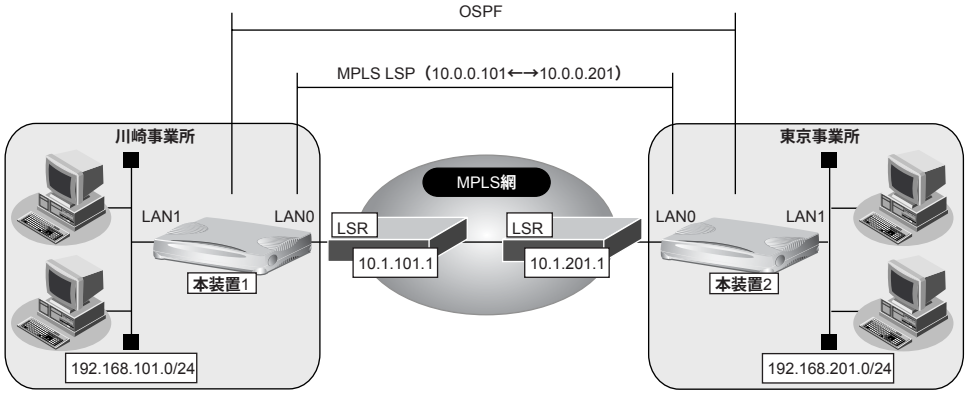
「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク指定
  あて先 IP アドレス　→10.0.0.101
  あて先アドレスマスク　→32（255.255.255.255）

2.7.2　トンネルエンドポイントをインタフェースアドレスとは別のアドレスにしてMPLS LSPを使用する

適用機種　全機種



● 前提条件

[本装置 1]

- LAN0 がMPLS 網、LAN1 が事業所内 LAN とする
- 接続するMPLS 網の次ホップLSR とは、インタフェースアドレスでコネクションを確立する
- MPLS 網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置 1 と本装置 2 の間は、LSP 上で OSPF を用いて経路情報を交換する
- MPLS 網を使用した LSP 上の通信は 5Mbps に帯域を制限する
- LSP でセッション監視を行い、セッションの切断を検知する

[本装置 2]

- LAN0 がMPLS 網、LAN1 が事業所内 LAN とする
- 接続するMPLS 網の次ホップLSR とは、インタフェースアドレスでコネクションを確立する
- MPLS 網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置 1 と本装置 2 の間は、LSP 上で OSPF を用いて経路情報を交換する
- MPLS 網を使用した LSP 上の通信は 5Mbps に帯域を制限する
- LSP でセッション監視を行い、セッションの切断を検知する

● 設定条件

[本装置 1]

- LAN0（MPLS 網側）のIP アドレス　：10.1.101.2
- 接続するMPLS 網の次ホップLSR のIP アドレス　：10.1.101.1
- LAN1（事業所内側）のIP アドレス　：192.168.101.1
- MPLS トンネルの自側IP アドレス　：10.0.0.101
- MPLS トンネルの相手側IP アドレス　：10.0.0.201

[本装置 2]

- LAN0（MPLS 網側）のIP アドレス　：10.1.201.2
- 接続するMPLS 網の次ホップLSR のIP アドレス　：10.1.201.1
- LAN1（事業所内側）のIP アドレス　：192.168.201.1

- MPLS トンネルの自側 IP アドレス　：10.0.0.101
- MPLS トンネルの相手側 IP アドレス　：10.0.0.201

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

MPLS 網との接続情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

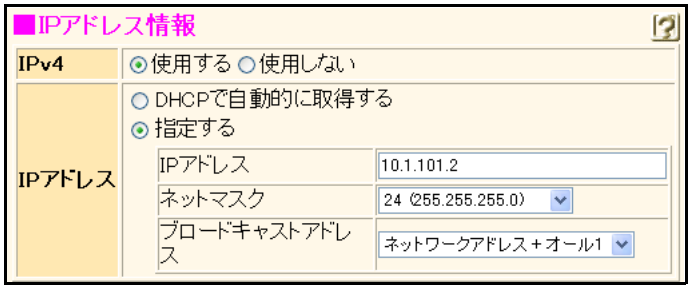
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.1.101.2
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

6.　「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

7.　以下の項目を指定します。

- MPLS 機能　→使用する
- ラベル配布プロトコル　→ LDP

8.　［保存］ボタンをクリックします。

9.　設定メニューのルータ設定で「MPLS 情報」をクリックします。

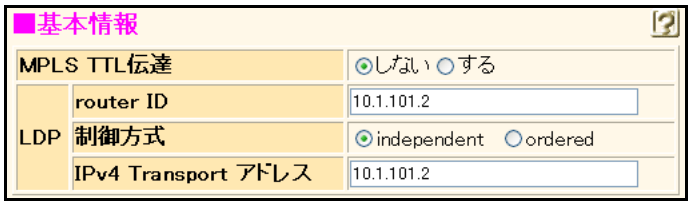
「MPLS 情報」ページが表示されます。

10.　「基本情報」をクリックします。

「基本情報」が表示されます。

11.　以下の項目を指定します。

- MPLS TTL 伝達　→しない
- LDP
  router ID　→ 10.1.101.2
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.1.101.2



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

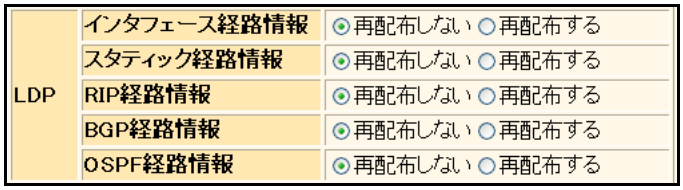
「ルーティングプロトコル情報」ページが表示されます。

14.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

15.　以下の項目を指定します。

- LDP
  インタフェース経路情報　→再配布しない
  RIP 経路情報　→再配布しない
  OSPF 経路情報　→再配布しない



16.　［保存］ボタンをクリックします。

MPLS トンネルを設定する

17.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

18.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

19.　以下の項目を指定します。

- ネットワーク名　→tokyo

20.　［追加］ボタンをクリックします。

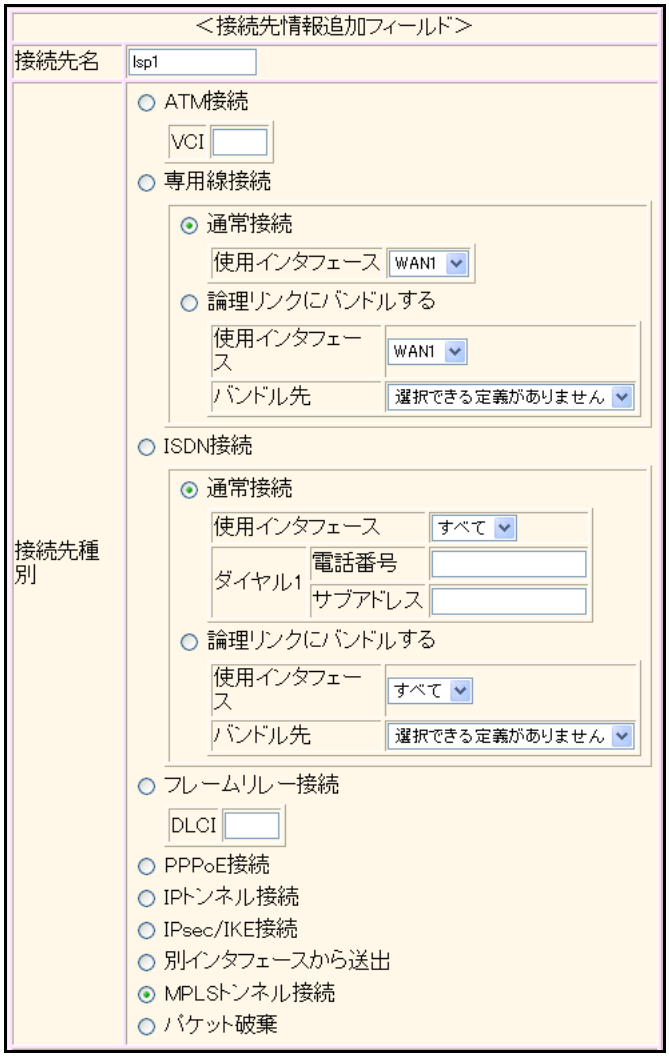
「ネットワーク情報（tokyo）」ページが表示されます。

21.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

22.　以下の項目を指定します。

- 接続先名　→lsp1
- 接続先種別　→MPLS トンネル接続



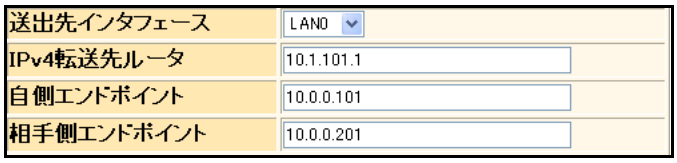
機種により、接続先種別の表示が上記の画面とは異なります。

23.　［追加］ボタンをクリックします。

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

24.　以下の項目を指定します。

- 送出先インタフェース　→LAN0
- IPv4 転送先ルータ　→10.1.101.1
- 自側エンドポイント　→10.0.0.101
- 相手側エンドポイント　→10.0.0.201



25.　［保存］ボタンをクリックします。

26.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

27.　「ネットワーク情報」で相手定義番号が 0 の［修正］ボタンをクリックします。

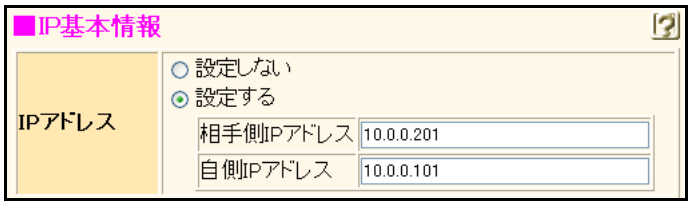
「ネットワーク情報」ページが表示されます。

28.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

29.　以下の項目を指定します。

- IP アドレス　→設定する
  相手側 IP アドレス　→10.0.0.201
  自側 IP アドレス　→10.0.0.101



30.　［保存］ボタンをクリックします。

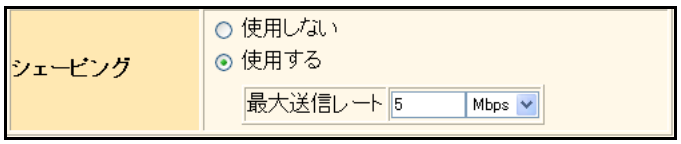
MPLS トンネルでシェーピングを設定する

31.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

32.　以下の項目を指定します。

- シェーピング　→使用する
  最大送信レート　→5Mbps



33.　［保存］ボタンをクリックします。

MPLS トンネルでセッション監視を設定する

34.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

35.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

36.　「ネットワーク情報」で相手定義番号が 0 の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

37.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

38.　「接続先情報」で接続先定義番号が 0 の［修正］ボタンをクリックします。

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

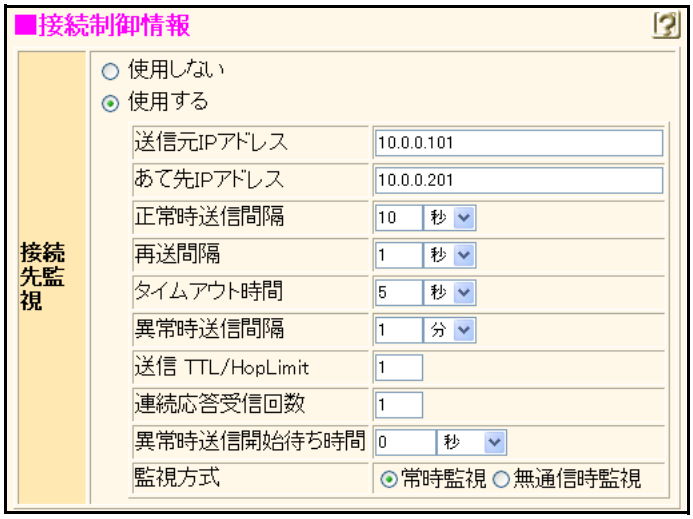
39.　MPLS トンネル接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

40.　以下の項目を指定します。

- 常時接続機能　→使用する
- 接続先監視　→使用する

  送信元 IP アドレス　→ 10.0.0.101
  あて先 IP アドレス　→ 10.0.0.201
  正常時送信間隔　→ 10 秒
  再送間隔　→ 1 秒
  タイムアウト時間　→ 5 秒
  異常時送信間隔　→ 1 分
  送信 TTL/HopLimit　→ 1



41.　［保存］ボタンをクリックします。

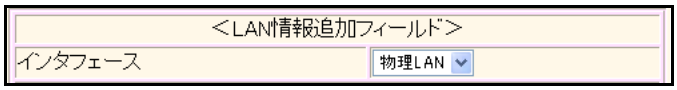
LAN1 情報を設定する

42.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

43.　以下の項目を指定します。

- インタフェース　→物理 LAN



44.　［追加］ボタンをクリックします。

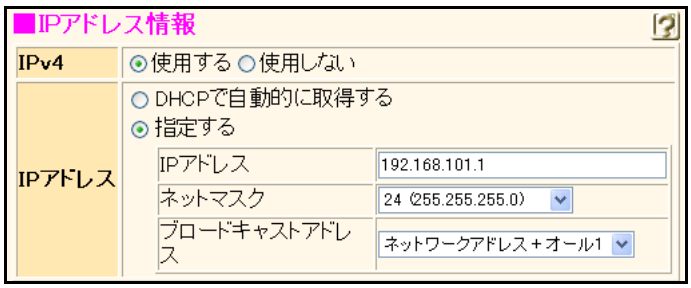
「LAN1 情報（物理 LAN）」ページが表示されます。

45.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

46.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.101.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



47.　［保存］ボタンをクリックします。

本装置 2 との間で経路交換を設定する

48.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

49.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

50.　「ネットワーク情報」で相手定義番号が 0 の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

51.　「IP 関連」をクリックします。

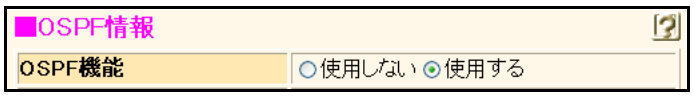
IP 関連の設定項目と「IP 基本情報」が表示されます。

52.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

53.　以下の項目を指定します。

- OSPF 機能　→使用する



54.　［保存］ボタンをクリックします。

55.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

56.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

57.　「IP 関連」をクリックします。

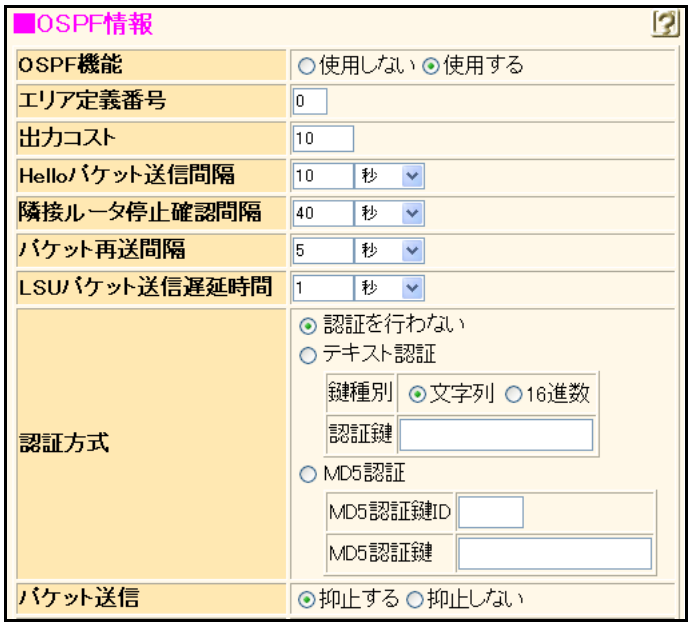
IP 関連の設定項目と「IP アドレス情報」が表示されます。

58.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

59.　以下の項目を指定します。

- OSPF 機能　→使用する
- パケット送信　→抑止する



60.　［保存］ボタンをクリックします。

61.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

62.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

63.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

64.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

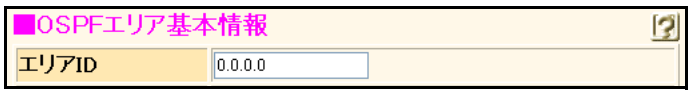
「OSPF エリア情報」が表示されます。

65.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

66.　以下の項目を指定します。

- エリア ID　→0.0.0.0



67.　［保存］ボタンをクリックします。

68.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

MPLS 網との接続情報を設定する

「LAN0 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.1.201.2
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「LAN0 情報（物理 LAN）」-「MPLS 関連」

「MPLS 基本情報」

- MPLS 機能　→使用する
  ラベル配布プロトコル　→ LDP

「MPLS 情報」

「基本情報」

- MPLS TTL 伝達　→しない
  router ID　→ 10.1.201.2
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.1.201.2

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」

「再配布情報」

- LDP
  インタフェース経路情報　→再配布しない
  RIP 経路情報　→再配布しない
  OSPF 経路情報　→再配布しない

MPLS トンネルを設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→kawasaki

「ネットワーク情報」-「接続先情報」

- 接続先名　→lsp1
- 接続先種別　→MPLS トンネル接続

「接続先情報」-「MPLS トンネル接続」

「基本情報」

- 送出先インタフェース　→LAN0
- IPv4 転送先ルータ　→10.1.201.1
- 自側エンドポイント　→10.0.0.201
- 相手側エンドポイント　→10.0.0.101

「ネットワーク情報」-「IP 関連」

- IPアドレス　→設定する
  相手側 IPアドレス　→10.0.0.101
  自側 IPアドレス　→10.0.0.201

MPLS トンネルでシェーピングを設定する

「相手情報」-「ネットワーク情報」

「ネットワーク情報」-「共通情報」

- シェーピング　→使用する
  最大送信レート　→5Mbps

MPLS トンネルでセッション監視を設定する

「相手情報」-「ネットワーク情報」

「接続先情報」-「MPLS トンネル接続」

「接続制御情報」

- 接続先監視　→使用する
  送信元 IPアドレス　→10.0.0.201
  あて先 IPアドレス　→10.0.0.101
  正常時送信間隔　→10 秒
  再送間隔　→1 秒
  タイムアウト時間　→5 秒
  異常時送信間隔　→1 分
  送信 TTL/Hoplimit　→1

LAN1 情報を設定する

「LAN1 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.201.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

本装置 1 との間で経路交換を設定する

「相手情報」-「ネットワーク情報」

「ネットワーク情報」-「IP 関連」

「OSPF 情報」

- OSPF 機能　→使用する

「LAN1 情報（物理 LAN）」-「IP 関連」

「OSPF 情報」

- OSPF 機能　→使用する
- パケット送信　→抑止する

「ルーティングプロトコル情報」-「OSPF 関連」

「OSPF エリア情報」

- エリア ID　→0.0.0.0

2.8 MPLS を使用したレイヤ 2VPN（EoMPLS）を構築する

適用機種　全機種

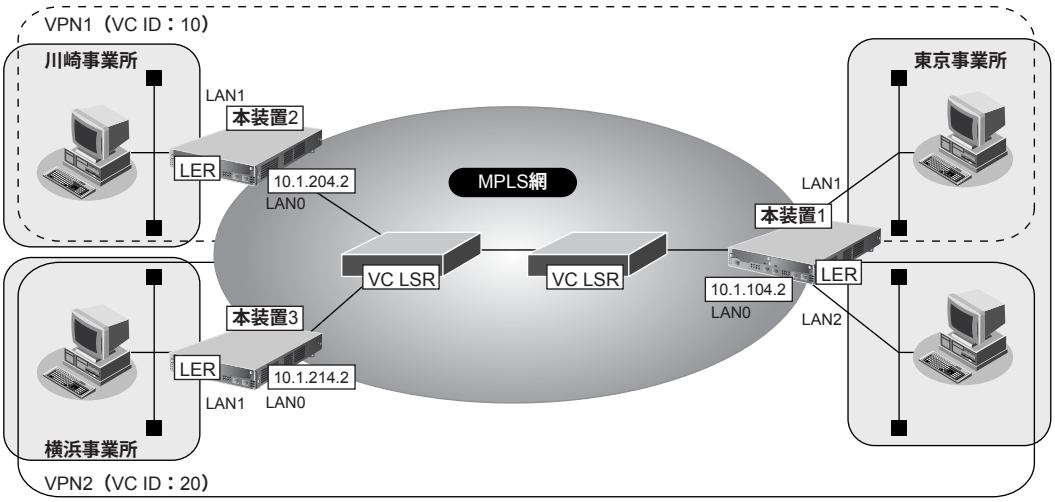
本装置では、MPLS 網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

参照　Si-R シリーズ　機能説明書「2.8.1 MPLS を使用したレイヤ 2VPN（EoMPLS）」（P.45）

ここでは、MPLS 接続サービス（キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送サービスを想定しています）と、MPLS LSP トンネルを使用して事業所でレイヤ 2VPN を EoMPLS で構築する事例を紹介します。

こんな事に気をつけて

- **複数のインタフェースを同一の VC に含めることはできません。**
- **トンネル LSP を使用するインタフェースでは、MPLS を利用する設定にしてください。**
- **VC インタフェースでは、シェーピング機能、LAN ポートバックアップ機能および VLAN 機能を併用して動作させることができます。IP 機能、IPv6 機能、ブリッジ機能（MAC フィルタ機能を含む）、VRRP 機能は動作できません。**
- **EoMPLS 通信を行う場合は、MAC 学習や STP のサポートを行わないため、パケットのループが発生しないように構成してください。Ethernet フレームがループし続けて通信できなくなります。また、EoMPLS 通信を用いて冗長構成を行う場合も、LAN インタフェース側に、STP などを使用できるスイッチ装置を設置し、Ethernet フレームがループしないように設定してください。**
- **VLAN Tag が異なる VLAN インタフェースどうしで VC を構成し、LAN 側で STP を使用する場合は、VLAN Tag の値をそろえてください。**



● 前提条件

[本装置 1]

- LAN0 は MPLS 網とし、LAN1、LAN2 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

[本装置 2]

- LAN0 は MPLS 網とし、LAN1 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

[本装置 3]

- LAN0 は MPLS 網とし、LAN1 は事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

● 設定条件

[本装置 1]

- LAN0（MPLS 網側）の IP アドレス：10.1.104.2
- ループバックの IP アドレス　：10.0.0.104
- LAN1 の VC 番号　：10
- LAN2 の VC 番号　：20

[本装置 2]

- LAN0（MPLS 網側）の IP アドレス：10.1.204.2
- ループバックの IP アドレス　：10.0.0.204
- LAN1 の VC 番号　：10

[本装置 3]

- LAN0（MPLS 網側）の IP アドレス：10.1.214.2
- ループバックの IP アドレス　：10.0.0.214
- LAN1 の VC 番号　：20

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

MPLS 網との接続情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

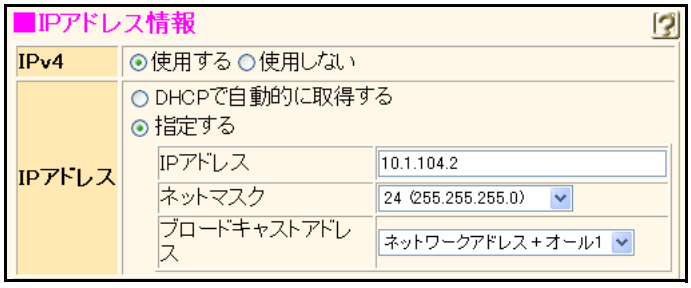
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→10.1.104.2
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1



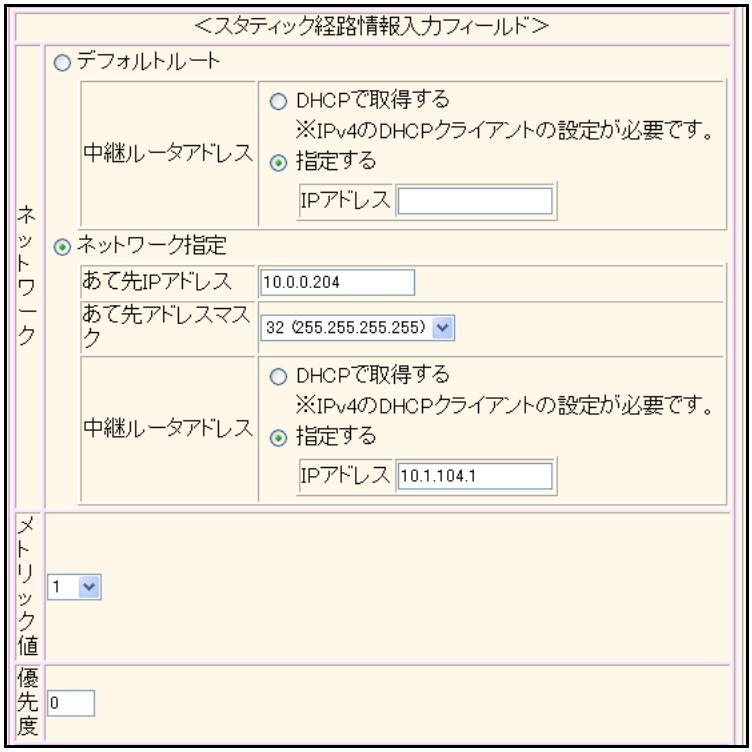
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」ページが表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先IPアドレス　→10.0.0.204
  あて先アドレスマスク　→32（255.255.255.255）
  中継ルータアドレス　→指定する
  IPアドレス　→10.1.104.1
- メトリック値　→1
- 優先度　→0



8.　［追加］ボタンをクリックします。

9.　手順 7.～8. を参考に、以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.0.0.214
  あて先アドレスマスク　→ 32（255.255.255.255）
  中継ルータアドレス　→指定する
  IP アドレス　→ 10.1.104.1
- メトリック値　→ 1
- 優先度　→ 0

10.　「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

11.　以下の項目を指定します。

- MPLS 機能　→使用する
- ラベル配布プロトコル　→ LDP

12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「MPLS 情報」をクリックします。

「MPLS 情報」ページが表示されます。

14.　「基本情報」をクリックします。

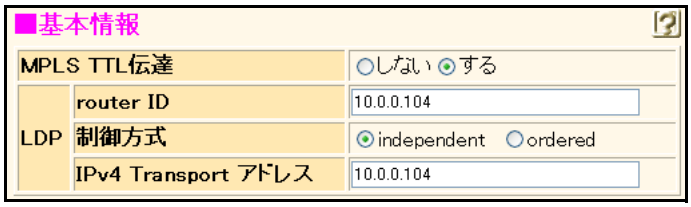
「基本情報」が表示されます。

15.　以下の項目を指定します。

- MPLS TTL 伝達　→する
- LDP
  router ID　→ 10.0.0.104
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.0.0.104

こんな事に気をつけて

router ID と IPv4 Transport アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。



16.　［保存］ボタンをクリックします。

17.　設定メニューの基本設定で「装置情報」をクリックします。

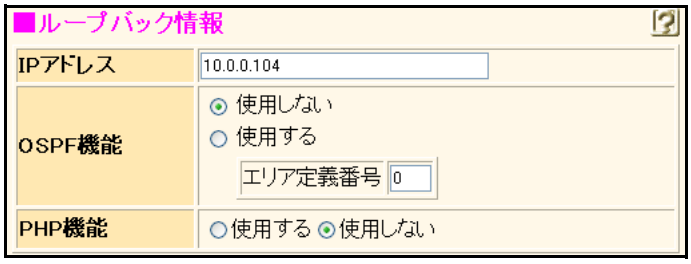
「装置情報」ページが表示されます。

18.　「ループバック情報」をクリックします。

「ループバック情報」が表示されます。

19.　以下の項目を指定します。

- IP アドレス　→ 10.0.0.104
- OSPF 機能　→使用しない
- PHP 機能　→使用しない



20.　［保存］ボタンをクリックします。

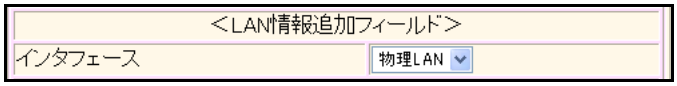
各拠点への VC を設定する

21.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

22.　以下の項目を指定します。

- インタフェース　→物理 LAN



23.　［追加］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

24.　「MPLS 関連」をクリックします。

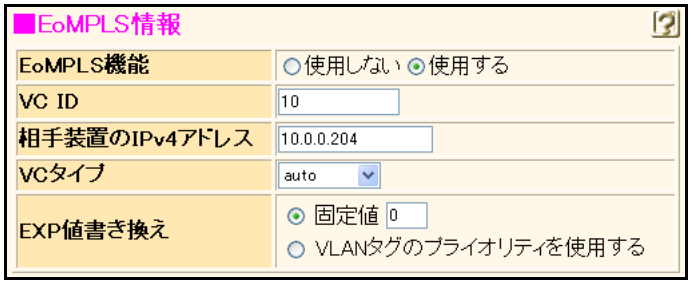
MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

25.　MPLS 関連の設定項目の「EoMPLS 情報」をクリックします。

「EoMPLS 情報」が表示されます。

26.　以下の項目を指定します。

- EoMPLS 機能　→使用する
- VC ID　→ 10
- 相手装置の IPv4 アドレス　→ 10.0.0.204
- VC タイプ　→ auto
- EXP 値書き換え　→固定値 0



27.　［保存］ボタンをクリックします。

28.　手順 21. ～ 27. を参考に、以下の項目を指定します。

「LAN2 情報（物理 LAN）」

- EoMPLS 機能　→使用する
- VC ID　→ 20
- 相手装置の IPv4 アドレス　→ 10.0.0.214
- VC タイプ　→ auto
- EXP 値書き換え　→固定値 0

29.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

MPLS 網との接続情報を設定する

「LAN0 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.1.204.2
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.0.0.104
  あて先アドレスマスク　→ 32（255.255.255.0）
  中継ルータアドレス　→指定する
  IP アドレス　→ 10.1.204.1

- メトリック値　→1
- 優先度　→0

「LAN0 情報」-「MPLS 関連」

「MPLS 基本情報」

- MPLS 機能　→使用する
- ラベル配布プロトコル　→LDP

「MPLS 情報」-「MPLS 関連」

「基本情報」

- MPLS TTL 伝達　→する
- LDP
  router ID　→10.0.0.204
  制御方式　→independent
  IPv4 Transport アドレス　→10.0.0.204

「装置情報」

「ループバック情報」

- IP アドレス　→10.0.0.204
- OSPF 機能　→使用しない
- PHP 機能　→使用しない

各拠点への VC を設定する

「LAN 情報」-「MPLS 関連」

「MPLS 基本情報」-「EoMPLS 情報」

- EoMPLS 機能　→使用する
- VC ID　→10
- 相手装置の IPv4 アドレス　→10.0.0.104
- VC タイプ　→auto
- EXP 値書き換え　→固定値 0

本装置 3 を設定する

「本装置 2 を設定する」を参考に、本装置 3 を設定します。

MPLS 網との接続情報を設定する

「LAN0 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→10.1.214.2
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.0.0.104
  あて先アドレスマスク　→ 32（255.255.255.0）
  中継ルータアドレス　→指定する
  IP アドレス　→ 10.1.214.1
- メトリック値　→ 1
- 優先度　→ 0

「LAN0 情報」-「MPLS 関連」

「MPLS 基本情報」

- MPLS 機能　→使用する
- ラベル配布プロトコル　→ LDP

「MPLS 情報」-「MPLS 関連」

「基本情報」

- MPLS TTL 伝達　→する
- LDP
  router ID　→ 10.0.0.214
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.0.0.214

「装置情報」

「ループバック情報」

- IP アドレス　→ 10.0.0.214
- OSPF 機能　→使用しない
- PHP 機能　→使用しない

各拠点への VC を設定する

「LAN 情報」-「MPLS 関連」

「MPLS 基本情報」-「EoMPLS 情報」

- EoMPLS 機能　→使用する
- VC ID　→ 10
- 相手装置の IPv4 アドレス　→ 10.0.0.104
- VC タイプ　→ auto
- EXP 値書き換え　→固定値 0

2.9 MPLS を使用したレイヤ 3VPN（BGP/MPLS VPN）を構築する

適用機種　全機種

本装置では、MPLS 網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

参照　Si-R シリーズ　機能説明書「2.8.2 MPLS を使用したレイヤ 3VPN（BGP/MPLS VPN）」（P.47）

ここでは、MPLS を使用した VPN ネットワークを構築する場合の設定方法を説明します。

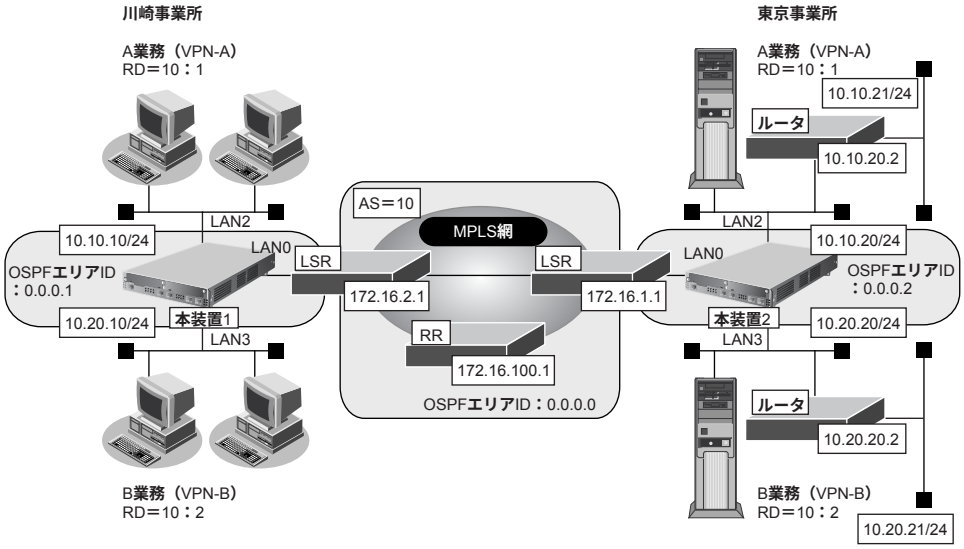
東京事業所と川崎事業所が MPLS 網に接続し、業務ごとに異なる VPN ネットワークを構築します。このとき、本装置 1、2 がそれぞれの前提条件を満たしていることを前提とします。

こんな事に気をつけて

- BGP/MPLS VPN 機能は IPv4 の場合だけ利用できます。IPv6 では使用できません。
- BGP で接続できる相手は 1 セッションだけです。このため、ルートリフレクタと接続する必要があります。
- IP-VPN 接続と併用することはできません。
- BGP ネットワーク、BGP 集約経路および BGP フィルタリングの機能は使用できません。
- BGP/MPLS VPN 機能と NAT 機能を併用することはできません。
- 本装置は、LER としてだけ動作します。
- BGP/MPLS VPN で構成された VPN ネットワーク内では、EBGP、OSPF および RIP は使用できません。
- 異なる VPN を収容する場合、VPN のインタフェースに設定した IP アドレスおよび属するネットワークアドレスを他 VPN インタフェースに設定できません。必ず異なるネットワークアドレスを設定してください。
- MPLS 網と接続するインタフェースで RIP を使用する場合、VPN で使用するインタフェース経路を RIP で広報します。MPLS への広報に対してフィルタリングを行ってください。
- LER では、受信した IP パケットを IP 処理層を通さずにラベルを付加します。IP フィルタリング機能、TOS 値書き換え機能およびソートフラグメント機能は、VPN に設定したインタフェースへの入力に限り動作します。ただし、VPN からの入力を IPsec によって暗号化し、対向ルータに送信する運用や帯域制御（WFQ）機能、イコールコストマルチパスなどの他 IP 機能を使用した運用は行うことはできません。
- VRRP と併用する場合は、トリガとしてインタフェースダウントリガまたはルートダウントリガ（VPN 内経路は対象外）が利用できます。ノードダウントリガは利用できません。
- BGP/MPLS VPN 構成では、LER は MTU 長の設定にかかわらず、IP パケットのフラグメント処理を行いません。受信したパケットはそのままラベルを付加して送信します。このため、MTU 長を調整する必要がある運用（VoIP 通信でのインターリーブなど）はできません。
- ループバックインタフェースで設定した IP アドレスを BGP の自側 IP アドレスとして使用しなければいけません。
- IP アドレスが設定されていないインタフェースでは MPLS は使用できません。隣接 MPLS 装置間で LDP セッションを構築する際、インタフェースのアドレスを用いる場合があります。
- BRI などの低速回線での高負荷時や装置の転送能力を超える高負荷が発生する場合、LDP セッションが切断されることがあります。LDP の Hello ホールドタイマを長め（例：30 秒）に設定してください。
- MPLS を利用すると、Ethernet フレームに 4 バイトのシムヘッダが最大 2 つ付加されます。最大 1526 バイトの Ethernet フレームが送出されることになります。通常の Ethernet フレームの最大サイズは 1518 バイトです。1526 バイトのフレームに対応していない機器と接続する場合は、MPLS を利用するインタフェースの MTU サイズを初期値の 1500 バイトから 1492 バイトに変更することで通信することができます。
- VPN 通信で使用するネットワークアドレスと、本装置に設定するすべてのネットワークアドレスが重複しないように設定してください。たとえば、本装置の MPLS ドメイン側 IP アドレスが 10.1.1.1/24 のとき、10.1.1.0/24 のネットワークを VPN として収容することはできません。
- VPN 以外の SNMP マネージャは VPN 内の装置を管理することはできません。
- BGP セッションの通信に使用するループバックインタフェースに設定したアドレスへの経路は集約しないでください。集約すると、トンネル LSP が正しく生成されません。

2.9.1　MPLS 網と LAN を使用して接続する

適用機種　全機種



LSR（Label Switching Router）：MPLS**コアルータ**
RR（Route Reflector）　　：**ルートリフレクタ**

● 前提条件

[本装置 1]

- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　　ネットワークアドレス：10.10.10.0/24
  VLAN ID：3　　ネットワークアドレス：10.20.10.0/24
- LAN1 は VLAN 出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN1 とする
- LAN0 の IP アドレス　　：172.16.2.2
- LAN2 の IP アドレス　　：10.10.10.1
- LAN3 の IP アドレス　　：10.20.10.1
- LAN0 ～ 3 では、NAT 機能および DHCP クライアント機能は使用しない

[本装置 2]

- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　　ネットワークアドレス：10.10.20.0/24
  VLAN ID：3　　ネットワークアドレス：10.20.20.0/24
- LAN1 は VLAN 出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN1 とする
- LAN0 の IP アドレス　　：172.16.1.2
- LAN2 の IP アドレス　　：10.10.20.1
- LAN3 の IP アドレス　　：10.20.20.1
- LAN0 ～ 3 では、NAT 機能および DHCP クライアント機能は使用しない

● 設定条件

- MPLS 網の使用条件
  BGP AS 番号　：10
  RR の IP アドレス　：172.16.100.1
  MPLS 網で使用する IPv4 ネットワーク　：OSPF
  　：バックボーンエリア
- VPN-A の使用条件
  ルート識別子　：10:1
  使用するネットワーク　：10.10.10/24 川崎事業所
  　：10.10.20/24 東京事業所
  　：10.10.21/24 東京事業所
- VPN-B の使用条件
  ルート識別子　：10:2
  使用するネットワーク　：10.20.10/24 川崎事業所
  　：10.20.20/24 東京事業所
  　：10.20.21/24 東京事業所

[本装置 1]

- ループバックインタフェースの IP アドレス　：10.1.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.1
- LAN0 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN2 で使用する VPN　：VPN-A
- LAN3 で使用する VPN　：VPN-B

[本装置 2]

- ループバックインタフェースの IP アドレス　：10.2.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.2
- LAN0 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN2 で使用する VPN　：VPN-A
- LAN2 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.10.21.0/24
  中継ルータアドレス　：10.10.20.2
- LAN3 で使用する VPN　：VPN-B
- LAN3 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.20.21.0/24
  中継ルータアドレス　：10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 2 を設定する

ループバック情報を設定する

1.　設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

2.　「ループバック情報」をクリックします。

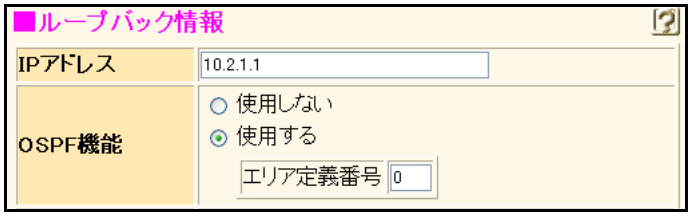
「ループバック情報」が表示されます。

3.　以下の項目を指定します。

- IP アドレス　→ 10.2.1.1
- OSPF 機能　→使用する
  エリア定義番号　→ 0

こんな事に気をつけて

エリア定義は、ルータ設定の「ルーティングプロトコル情報」－「OSPF エリア情報」で設定します。



4.　［保存］ボタンをクリックします。

MPLS 網と接続する LAN0 に OSPF 機能を設定する

5.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

6.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

7.　「IP 関連」をクリックします。

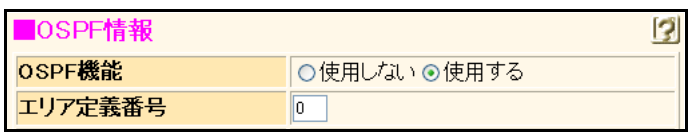
IP 関連の設定項目と「IP アドレス情報」が表示されます。

8.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

9.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→ 0



10.　［保存］ボタンをクリックします。

OSPF 関連を設定する

11.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

12.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

13.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPF エリア情報」が表示されます。

14.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

15.　以下の項目を指定します。

- エリア ID　→0.0.0.2

16.　［保存］ボタンをクリックします。

MPLS 網と接続する LAN0 に MPLS 機能を設定する

17.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

18.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

19.　「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

20.　以下の項目を指定します。

- MPLS 機能　→使用する
- ラベル配布プロトコル　→LDP

21.　［保存］ボタンをクリックします。

22.　設定メニューのルータ設定で「MPLS 情報」をクリックします。

「MPLS 情報」ページが表示されます。

23.　「基本情報」をクリックします。

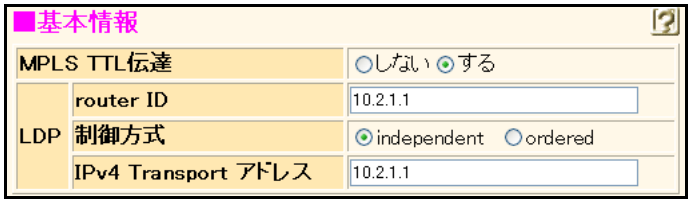
「基本情報」が表示されます。

24.　以下の項目を指定します。

- MPLS TTL 伝達　→する
- LDP
  router ID　→ 10.2.1.1
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.2.1.1

こんな事に気をつけて

router ID と IPv4 Transport アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。



25.　［保存］ボタンをクリックします。

ルートリフレクタの接続情報を設定する

26.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

27.　「BGP 関連」をクリックします。

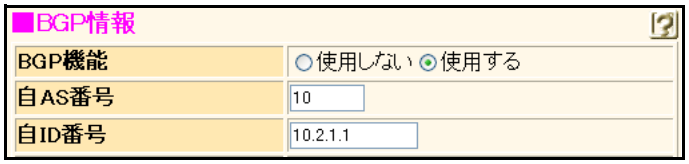
BGP 関連の設定項目と「BGP 情報」が表示されます。

28.　以下の項目を指定します。

- BGP 機能　→使用する
- 自 AS 番号　→ 10
- 自 ID 番号　→ 10.2.1.1

こんな事に気をつけて

自 ID 番号には、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。



29.　［保存］ボタンをクリックします。

30.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

31.　［追加］ボタンをクリックします。

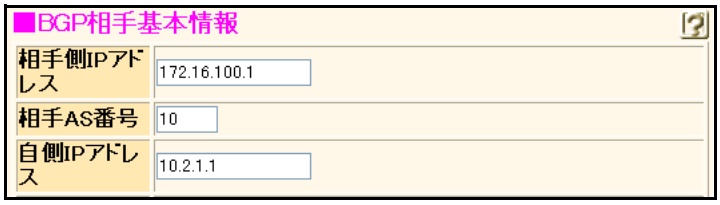
BGP 相手情報（0）の設定項目と「BGP 相手基本情報」が表示されます。

32.　以下の項目を指定します。

- 相手側 IP アドレス　→ 172.16.100.1
- 相手 AS 番号　→ 10
- 自側 IP アドレス　→ 10.2.1.1

こんな事に気をつけて

- **ルートリフレクタの IP アドレスを相手側 IP アドレスに設定してください。**
- **自側 IP アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。**



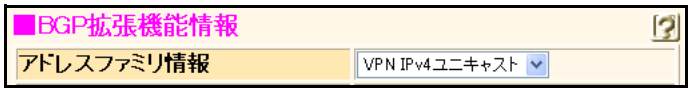
33.　［保存］ボタンをクリックします。

34.　BGP 相手情報（0）の設定項目の「BGP 拡張機能情報」をクリックします。

「BGP 拡張機能情報」が表示されます。

35.　以下の項目を指定します。

- アドレスファミリ情報　→ VPN IPv4 ユニキャスト



36.　［保存］ボタンをクリックします。

VPN-A および VPN-B 情報として VRF 情報を設定する

37.　画面上部の「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」のページが表示されます。

38.　「BGP 関連」をクリックします。

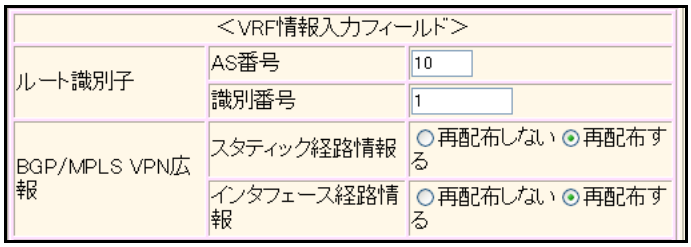
BGP 関連の設定項目と「BGP 情報」が表示されます。

39.　BGP 関連の設定項目の「VRF 情報」をクリックします。

「VRF 情報」が表示されます。

40.　以下の項目を指定します。

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 1
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布する
  インタフェース経路情報　→再配布する



41.　［追加］ボタンをクリックします。

42.　手順 40. ～ 41. を参考に、以下の項目を指定します。

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 2
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布する
  インタフェース経路情報　→再配布する

LAN2 情報を設定する

43.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

44.　「LAN 情報」でインタフェースが LAN2 の［修正］ボタンをクリックします。

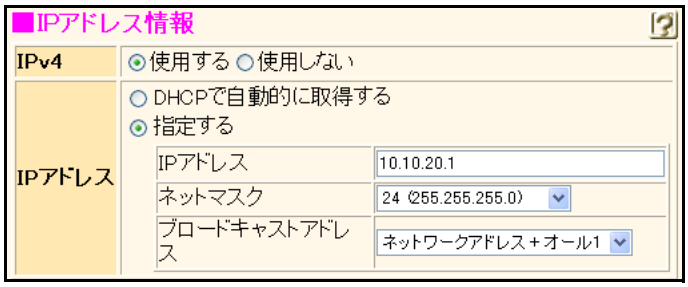
「LAN2 情報（物理 LAN）」ページが表示されます。

45.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

46.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.10.20.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



47.　［保存］ボタンをクリックします。

48.　IP 関連の設定項目の「BGP/MPLS VPN 情報」をクリックします。

「BGP/MPLS VPN 情報」が表示されます。

49.　以下の項目を指定します。

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→0

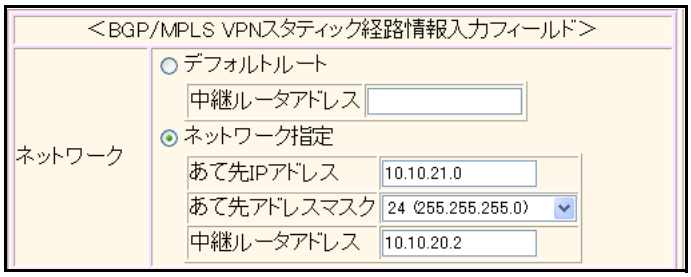
50.　［保存］ボタンをクリックします。

51.　IP 関連の設定項目の「BGP/MPLS VPN スタティック経路情報」をクリックします。

「BGP/MPLS VPN スタティック経路情報」が表示されます。

52.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→10.10.21.0
  あて先アドレスマスク　→24（255.255.255.0）
  中継ルータアドレス　→10.10.20.2



53.　［追加］ボタンをクリックします。

54.　手順 43. ～ 53. を参考に、「LAN3 情報（物理 LAN）」で以下の項目を指定します。

LAN3 情報を設定する

「LAN 情報 3 情報（物理 LAN）」-「IP 関連」
「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→10.20.20.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→1

「BGP/MPLS VPN スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.20.21.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→ 10.20.20.2

55. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 1 を設定する

「本装置 2 を設定する」を参考に、本装置 1 を設定します。

ループバック情報を設定する

「装置情報」-「ループバック情報」

- IP アドレス　→ 10.1.1.1
- OSPF 機能　→使用する
  エリア定義番号　→ 0

MPLS 網と接続する LAN0 に OSPF 機能を設定する

「LAN0 情報」-「IP 関連」
「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 0

「ルーティングプロトコル情報」-「OSPF 関連」
「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→ 0.0.0.1

MPLS 網と接続する LAN0 に MPLS 機能を設定する

「LAN0 情報」-「MPLS 関連」

「MPLS 基本情報」

- MPLS 機能　→使用する
- ラベル配布プロトコル　→ LDP

「MPLS 情報 -「基本情報」

- MPLS TTL 伝達　→する
- LDP
  router ID　→ 10.1.1.1
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.1.1.1

ルートリフレクタの接続情報を設定する

「ルーティングプロトコル情報」-「BGP 関連」

「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→ 10
- 自 ID 番号　→ 10.1.1.1

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側 IP アドレス　→ 172.16.100.1
- 相手 AS 番号　→ 10
- 自側 IP アドレス　→ 10.1.1.1

「BGP 相手情報」-「BGP 拡張機能情報」

- アドレスファミリ情報　→ VPN IPv4 ユニキャスト

VPN-A および VPN-B 情報として VRF 情報を設定する

「ルーティングプロトコル情報」-「BGP 関連」

「VRF 情報（0）」

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 1
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布しない
  インタフェース経路情報　→再配布する

「VRF 情報（1）」

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 2
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布しない
  インタフェース経路情報　→再配布する

LAN2 情報を設定する

「LAN2 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.10.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN2 情報」-「BGP 関連」

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→ 0

LAN3 情報を設定する

「LAN3 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.20.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

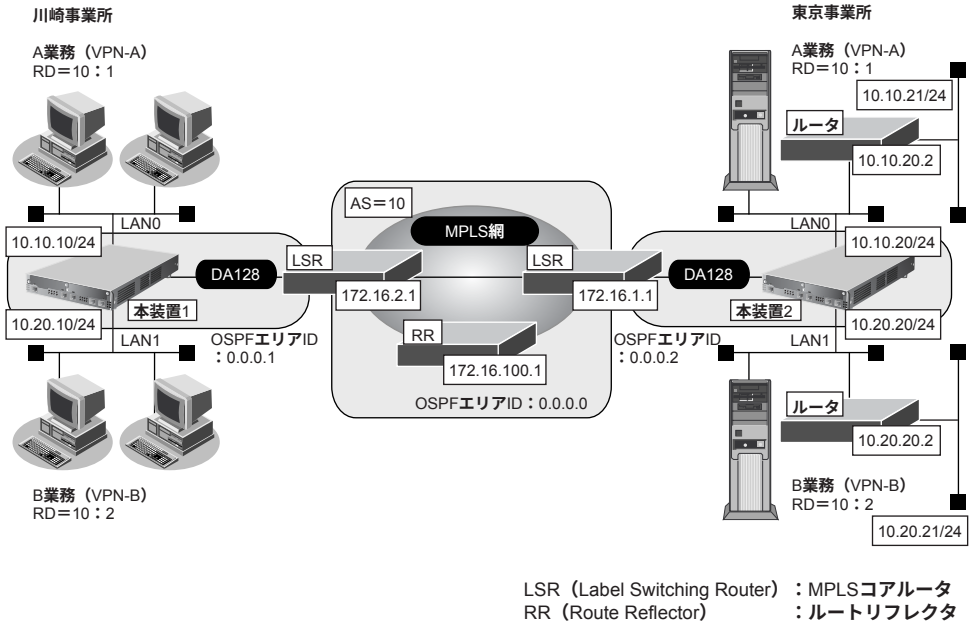
「LAN3 情報」-「BGP 関連」

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→ 1

2.9.2　MPLS網と専用線を使用して接続する

適用機種　***Si-R220B,220C,370,570***



● 前提条件

- すべてのインタフェースにIPアドレスを設定する
- すべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

● 設定条件

- MPLS網の使用条件
  BGP AS番号　：10
  RRのIPアドレス　：172.16.100.1
  MPLS網で使用するIPv4ネットワーク　：OSPF
  　：バックボーンエリア
- VPN-Aの使用条件
  ルート識別子　：10:1
  使用するネットワーク　：10.10.10/24 川崎事業所
  　：10.10.20/24 東京事業所
  　：10.10.21/24 東京事業所
- VPN-Bの使用条件
  ルート識別子　：10:2
  使用するネットワーク　：10.20.10/24 川崎事業所
  　：10.20.20/24 東京事業所
  　：10.20.21/24 東京事業所

[本装置1（川崎事業所)]

- ループバックインタフェースのIPアドレス　：10.1.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでのOSPFエリアID　：0.0.0.1
- rmt0でのルーティングプロトコル　：OSPF
- rmt0でのOSPFエリアID　：0.0.0.1

- LAN0 で使用する VPN　：VPN-A
- LAN1 で使用する VPN　：VPN-B

【本装置 2（東京事業所）】

- ループバックインタフェースの IP アドレス　：10.2.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.2
- rmt0 でのルーティングプロトコル　：OSPF
- rmt0 での OSPF エリア ID　：0.0.0.2
- LAN0 で使用する VPN　：VPN-A
- LAN0 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.10.21.0/24
  中継ルータアドレス　：10.10.20.2
- LAN1 で使用する VPN　：VPN-B
- LAN1 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.20.21.0/24
  中継ルータアドレス　：10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 2 を設定する

ループバック情報を設定する

1.　設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

2.　「ループバック情報」をクリックします。

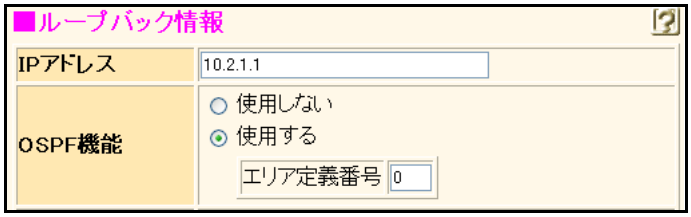
「ループバック情報」が表示されます。

3.　以下の項目を指定します。

- IP アドレス　→ 10.2.1.1
- OSPF 機能　→使用する
  エリア定義番号　→ 0

こんな事に気をつけて

エリア定義は、ルータ設定の「ルーティングプロトコル情報」－「OSPF エリア情報」で設定します。



4.　［保存］ボタンをクリックします。

MPLS 網と接続するインタフェースに OSPF 機能を設定する

5.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

6.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

7.　OSPF 機能を設定するネットワーク欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

8.　「IP 関連」をクリックします。

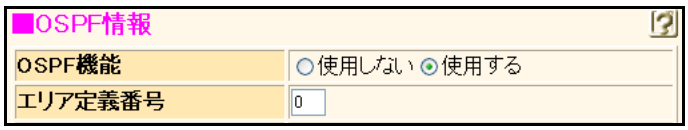
IP 関連の設定項目と「IP 基本情報」が表示されます。

9.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

10.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



11.　［保存］ボタンをクリックします。

12.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

13.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

14.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

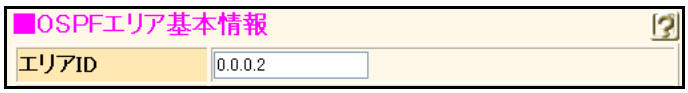
「OSPF エリア情報」が表示されます。

15.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

16.　以下の項目を指定します。

- エリア ID　→0.0.0.2



17.　［保存］ボタンをクリックします。

MPLS 網と接続するインタフェースに MPLS 機能を設定する

18.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

19.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

20.　MPLS 機能を設定するネットワーク欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

21.　「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

22.　以下の項目を指定します。

- MPLS 機能　→使用する
- ラベル配布プロトコル　→LDP

23.　［保存］ボタンをクリックします。

24.　設定メニューのルータ設定で「MPLS 情報」をクリックします。

「MPLS 情報」ページが表示されます。

25.　「基本情報」をクリックします。

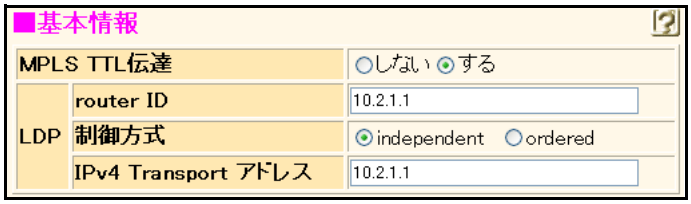
「基本情報」が表示されます。

26.　以下の項目を指定します。

- MPLS TTL 伝達　→する
- LDP
  - router ID　→10.2.1.1
  - 制御方式　→independent
  - IPv4 Transport アドレス　→10.2.1.1

こんな事に気をつけて

router ID と IPv4 Transport アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。



27.　［保存］ボタンをクリックします。

ルートリフレクタへの接続情報を設定する

28.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

29.　「BGP 関連」をクリックします。

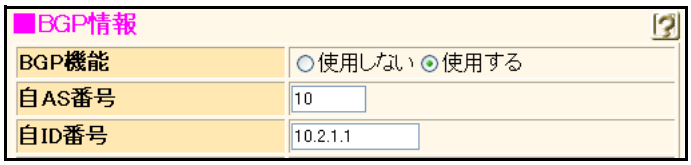
BGP 関連の設定項目と「BGP 情報」が表示されます。

30.　以下の項目を指定します。

- BGP 機能　→使用する
- 自 AS 番号　→ 10
- 自 ID 番号　→ 10.2.1.1

こんな事に気をつけて

自 ID 番号には、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。



31.　［保存］ボタンをクリックします。

32.　BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

33.　［追加］ボタンをクリックします。

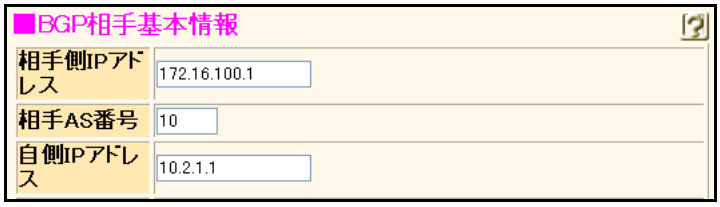
BGP 相手情報（0）の設定項目と「BGP 相手基本情報」が表示されます。

34.　以下の項目を指定します。

- 相手側 IP アドレス　→ 172.16.100.1
- 相手 AS 番号　→ 10
- 自側 IP アドレス　→ 10.2.1.1

こんな事に気をつけて

- **ルートリフレクタの IP アドレスを相手側 IP アドレスに設定してください。**
- **自側 IP アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。**



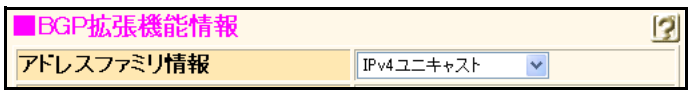
35.　［保存］ボタンをクリックします。

36.　BGP 相手情報（0）の設定項目の「BGP 拡張機能情報」をクリックします。

「BGP 拡張機能情報」が表示されます。

37.　以下の項目を指定します。

- アドレスファミリ情報　→ VPN IPv4 ユニキャスト



38.　［保存］ボタンをクリックします。

VPN-A および VPN-B 情報として VRF 情報を設定する

39.　画面上部の「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」のページが表示されます。

40.　「BGP 関連」をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

41.　BGP 関連の設定項目の「VRF 情報」をクリックします。

「VRF 情報」が表示されます。

42.　以下の項目を指定します。

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 1
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布する
  インタフェース経路情報　→再配布する

＜VRF情報入力フィールド＞		
ルート識別子	AS番号	10
	識別番号	1
BGP/MPLS VPN広報	スタティック経路情報	○再配布しない ◉再配布する
	インタフェース経路情報	○再配布しない ◉再配布する

43.　［追加］ボタンをクリックします。

44.　手順 42. ～ 43. を参考に、以下の項目を指定します。

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 2
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布する
  インタフェース経路情報　→再配布する

LAN0 情報を設定する

45.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

46.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

47.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

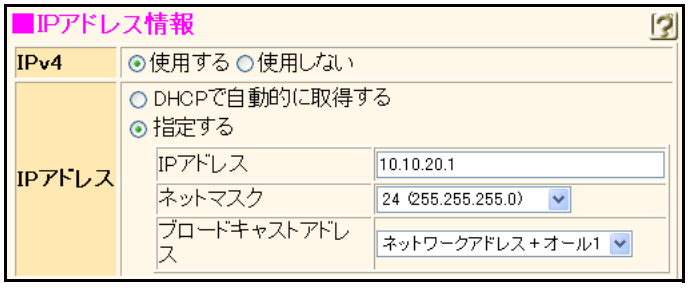
48.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する

  IPアドレス　→10.10.20.1

  ネットマスク　→24（255.255.255.0）

  ブロードキャストアドレス　→ネットワークアドレス＋オール1



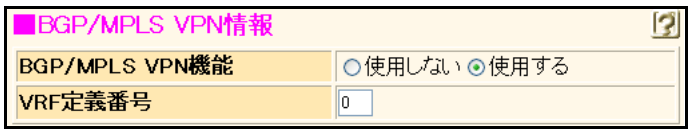
49.　［保存］ボタンをクリックします。

50.　IP 関連の設定項目の「BGP/MPLS VPN 情報」をクリックします。

「BGP/MPLS VPN 情報」が表示されます。

51.　以下の項目を指定します。

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→0



52.　［保存］ボタンをクリックします。

53.　IP 関連の設定項目の「BGP/MPLS VPN スタティック経路情報」をクリックします。

「BGP/MPLS VPN スタティック経路情報」が表示されます。

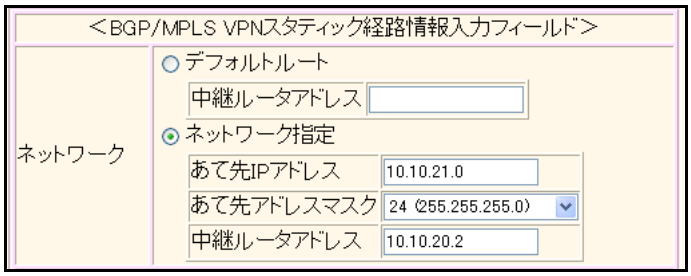
54.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定

  あて先IPアドレス　→10.10.21.0

  あて先アドレスマスク　→24（255.255.255.0）

  中継ルータアドレス　→10.10.20.2



55.　［追加］ボタンをクリックします。

56.　手順 45. ～ 55. を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

LAN1 情報を設定する

「LAN1 情報（物理 LAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.20.20.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN1 情報（物理 LAN）」-「BGP 関連」

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→ 1

「BGP/MPLS VPN スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.20.21.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→ 10.20.20.2

57.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 1 を設定する

「本装置 2 を設定する」を参考に、本装置 1 を設定します。

ループバック情報を設定する

「装置情報」-「ループバック情報」

- IP アドレス　→ 10.1.1.1
- OSPF 機能　→使用する
  エリア定義番号　→ 0

MPLS 網と接続するインタフェースに OSPF 機能を設定する

「LAN 情報」-「IP 関連」

「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 0

「ルーティングプロトコル情報」-「OSPF 関連」

「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→ 0.0.0.1

MPLS 網と接続するインタフェースに MPLS 機能を設定する

「相手情報」-「ネットワーク情報」
「ネットワーク情報」-「MPLS 関連」
「MPLS 基本情報」

- MPLS 機能　→使用する
- ラベル配布プロトコル　→ LDP

「MPLS 情報」-「基本情報」

- MPLS TTL 伝達　→する
- LDP
  router ID　→ 10.1.1.1
  制御方式　→ independent
  IPv4 Transport アドレス　→ 10.1.1.1

ルートリフレクタへの接続情報を設定する

「ルーティングプロトコル情報」-「BGP 関連」
「BGP 情報」

- BGP 機能　→使用する
- 自 AS 番号　→ 10
- 自 ID 番号　→ 10.1.1.1

「BGP 相手情報」-「BGP 相手基本情報」

- 相手側 IP アドレス　→ 172.16.100.1
- 相手 AS 番号　→ 10
- 自側 IP アドレス　→ 10.1.1.1

「BGP 相手情報」-「BGP 拡張機能情報」

- アドレスファミリ情報　→ VPN IPv4 ユニキャスト

VPN-A および VPN-B 情報として VRF 情報を設定する

「ルーティングプロトコル情報」-「BGP 関連」
「VRF 情報（0）」

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 1
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布しない
  インタフェース経路情報　→再配布する

「VRF 情報（1）」

- ルート識別子
  AS 番号　→ 10
  識別番号　→ 2
- BGP/MPLS VPN 広報
  スタティック経路情報　→再配布しない
  インタフェース経路情報　→再配布する

LAN0 情報を設定する

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.10.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→ 0

LAN1 情報を設定する

「LAN1 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 10.20.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能　→使用する
- VRF 定義番号　→ 1

こんな事に気をつけて

サポートインタフェースは PRI（ISDN、HSD）、BRI（ISDN、HSD）、ATM と LAN です。モデムや FR には対応していません。

⚠注意

MPLS、BGP、OSPF および RIP を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、BGP/MPLS VPN 機能は使用しないでください。

2.10 マルチリンク機能を使う

適用機種 *Si-R220B,220C,370,570*

2.10.1 ISDN でマルチリンク機能を使う

適用機種 *Si-R220B,220C,370,570*

ISDN によって相手装置と接続するときに、マルチリンク機能を使用することができます。マルチリンク機能では、B チャネル（64Kbps）を論理的に複数本束ねることによって、最大 1472Kbps で通信できます。また、回線使用率によって動的にチャネル数を増減することができ、回線を効率良く利用することができます。

参照 Si-R シリーズ　機能説明書「2.9 マルチリンク機能」（P.50）

ここでは、ISDN 接続をネットワーク情報（intranet）で定義してある環境に対してマルチリンクを行う場合の設定方法を説明します。

● 設定条件

- ネットワーク情報（intranet）で ISDN による通信環境が設定済み
- 接続直後のリンク数は 2 チャンネル
- 最大リンク数は 4 チャネル（2 本の INS ネット 64 回線を利用する）
- チャネルの使用率 90% 以上が 10 秒以上続いたら、チャネルを増加する
- チャネルの使用率 40% 以下が 60 秒以上続いたら、チャネルを減少する
- 受信順序制御機能（MP）を使用する

上記の設定条件に従ってマルチリンクを行う場合の設定例を示します。

回線情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

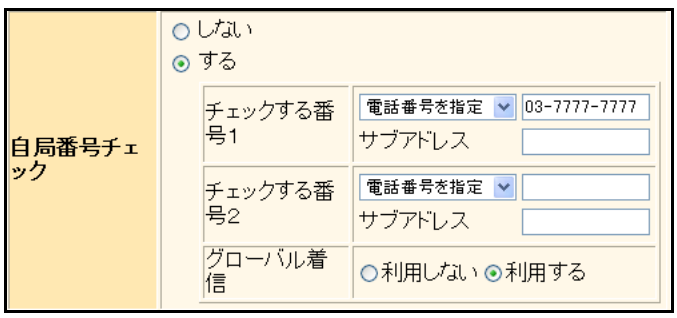
「WAN 情報」ページが表示されます。

2.　インタフェースが WAN0 の［修正］ボタンをクリックします。

「基本情報」ページが表示されます。

3.　以下の項目を指定します。

- 自局番号チェック　→する
  チェックする番号 1　→電話番号を指定
  →03-7777-7777（回線自局電話番号）



4.　［保存］ボタンをクリックします。

5.　手順 1.～4. を参考に、WAN1 情報を設定します。

相手情報を設定する

6.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

7.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

8.　ネットワーク名が intranet の［修正］ボタンをクリックします。

「ネットワーク情報（intranet)」ページが表示されます。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　「接続先情報」でマルチリンクを設定する接続先の［修正］ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

11.　以下の項目を指定します。

- 使用インタフェース　→すべて

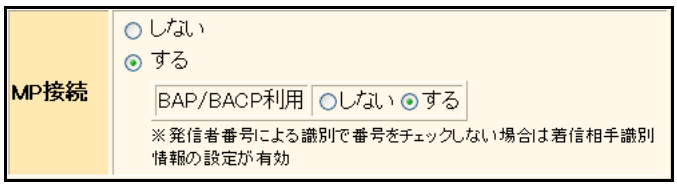
12.　［保存］ボタンをクリックします。

13.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

14.　以下の項目を指定します。

- MP 接続　→する
  BAP/BACP 利用　→する



15.　［保存］ボタンをクリックします。

PPP 関連を設定する

16.　画面上部の「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

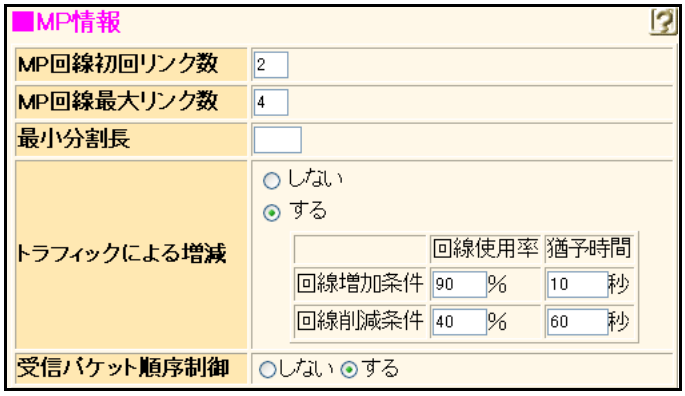
17.　「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

18.　PPP 関連の設定項目の「MP 情報」をクリックします。

19.　以下の項目を指定します。

- MP 回線初期リンク数　→2
- MP 回線最大リンク数　→4
- トラフィックによる増減　→する
  回線増加条件
  回線使用率　→90
  猶予時間　→10
  回線削除条件
  回線使用率　→40
  猶予時間　→60
- 受信パケット順序制御　→する



20.　［保存］ボタンをクリックします。

21.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **複数の ISDN 回線を利用してマルチリンク機能を利用する場合は、以下のどちらかが必要です。**
  - **着信側回線で代表取り扱いサービスを契約し、同じ番号でどちらの回線でも着信できるようにする。**
  - **装置に自局電話番号を正しく設定したうえで、BAP を利用する。**
- **初期接続時はすべて同じ電話番号に発信するため、相手側が電話番号の異なる複数の回線で構成される場合は、指定された初期接続回線数まで増やせないことがあります。この場合は着信側回線で代表取り扱いサービスを契約し、同じ番号でどちらの回線でも着信できるようにしてください。**

2.10.2　複数専用線でマルチリンク機能を使う

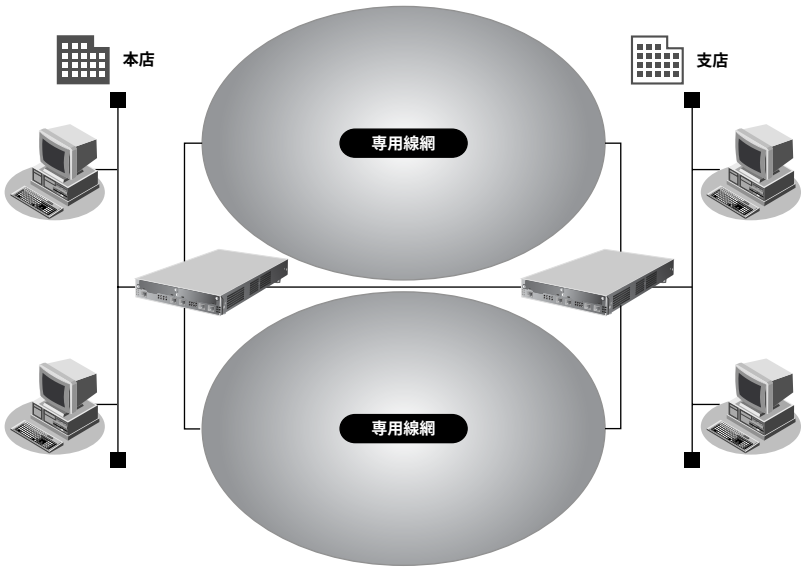
適用機種　***Si-R370,570***

複数の専用線によって単一の論理リンクを構成することができます。この場合、定義上は 1 つの専用線を主たる回線（マスタ回線）として定義し、残りの専用線は補助回線（バンドル回線）として定義します。
ここでは、論理リンクを介して 2 つの事業所（本店、支店）のネットワークを接続する場合について説明します。

参照　Si-R シリーズ　機能説明書「2.9 マルチリンク機能」（P.50）

こんな事に気をつけて

速度の異なる回線を論理回線として結合した場合、期待する速度が出ない場合があります。また、専用線だけで論理リンクを構成した場合は、PPP 最大接続チャネル数および初期接続チャネル数は無視されます。



● 設定条件

- マスタ回線として、スロット 0 に実装された BRI 拡張モジュール L2 で専用線（128Kbps）を使用する
- バンドル回線として、スロット 1 に実装された BRI 拡張モジュール L2 で専用線（128Kbps）を使用する

[本店]

- 接続ネットワーク名　：honten
- 接続先名　：honten-1
- 本装置の IP アドレス/ネットマスク　：192.168.1.1/24
- マルチリンクのためのユーザ認証 ID とユーザ認証パスワード
  発信　：honten hontenpasswd
  着信　：shiten shitenpasswd

[支店]

- 接続ネットワーク名　：shiten
- 接続先名　：shiten-1
- 本装置の IP アドレス/ネットマスク　：192.168.2.1/24

- マルチリンクのためのユーザ認証 ID とユーザ認証パスワード
  発信　：shiten shitenpasswd
  着信　：honten hontenpasswd

上記の設定条件に従って本店の論理リンクの設定例を示します。

回線情報を設定する

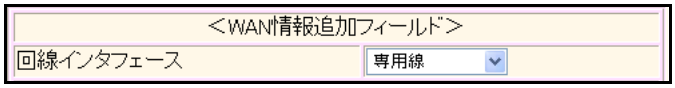
スロット 0-0：WAN0
スロット 1-0：WAN1
として以下の手順で設定します。

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→専用線



3.　［追加］ボタンをクリックします。

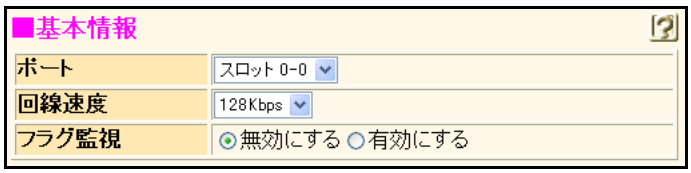
「WAN0 情報（専用線）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→ 128kbps
- フラグ監視　→無効にする



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、WAN1 情報を設定します。

相手情報を設定する

8.　設定メニューのルータ情報で「相手情報」をクリックします。

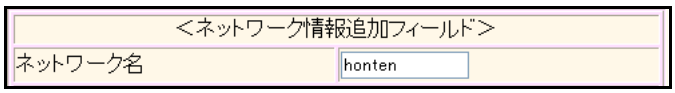
「相手情報」ページが表示されます。

9.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

10.　以下の項目を指定します。

- ネットワーク名　　→honten



11.　［追加］ボタンをクリックします。

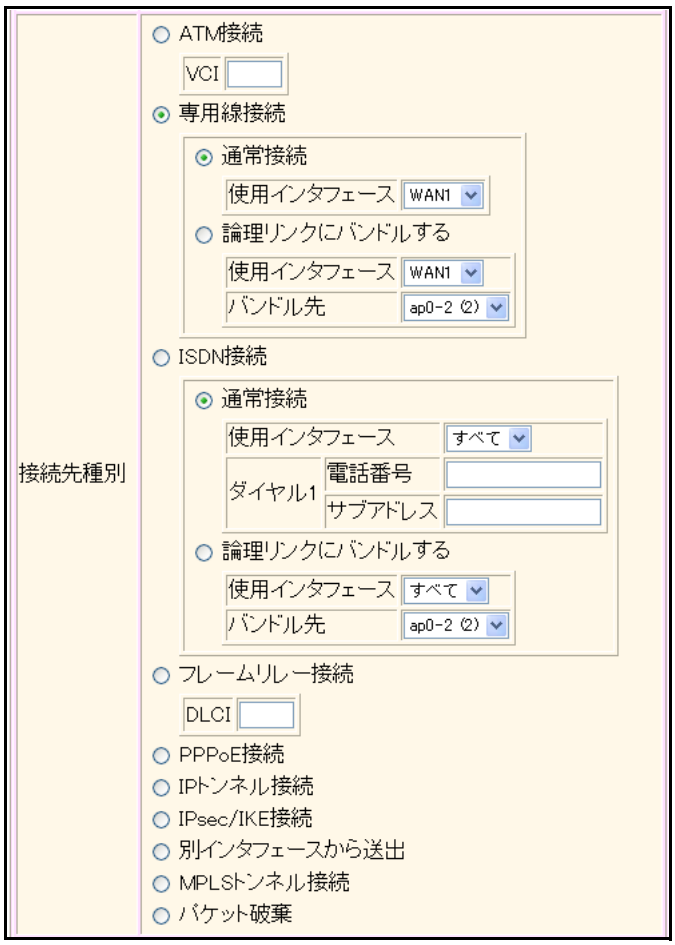
「ネットワーク情報（honten）」ページが表示されます。

12.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

13.　以下の項目を指定します。

- 接続先種別　　→専用線接続

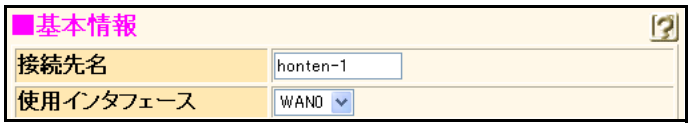


14.　［追加］ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

15.　以下の項目を指定します。

- 接続先名　　→honten-1
- 使用インタフェース　　→WAN0



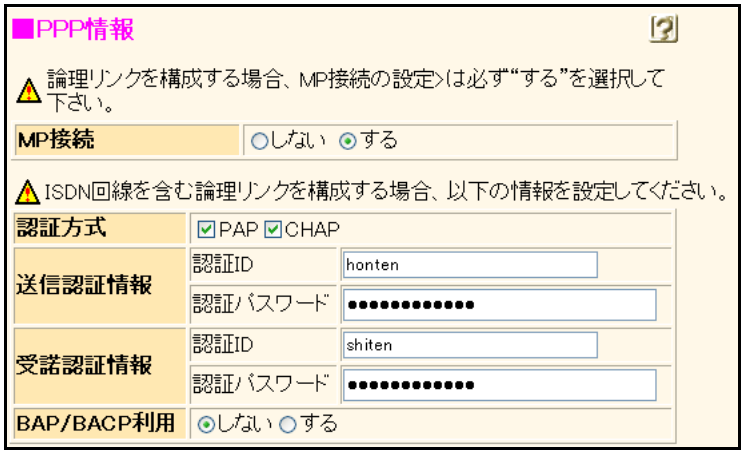
16.　［保存］ボタンをクリックします。

17.　設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

18.　以下の項目を指定します。

- MP 接続　→する
- 認証方式　→PAP、CHAP
- 送信認証情報
  認証 ID　→honten
  認証パスワード　→hontenpasswd
- 受諾認証情報
  認証 ID　→shiten
  認証パスワード　→shitenpasswd
- BAP/BACP 利用　→しない



19.　［保存］ボタンをクリックします。

20.　画面上部の「ネットワーク情報（honten）」をクリックします。

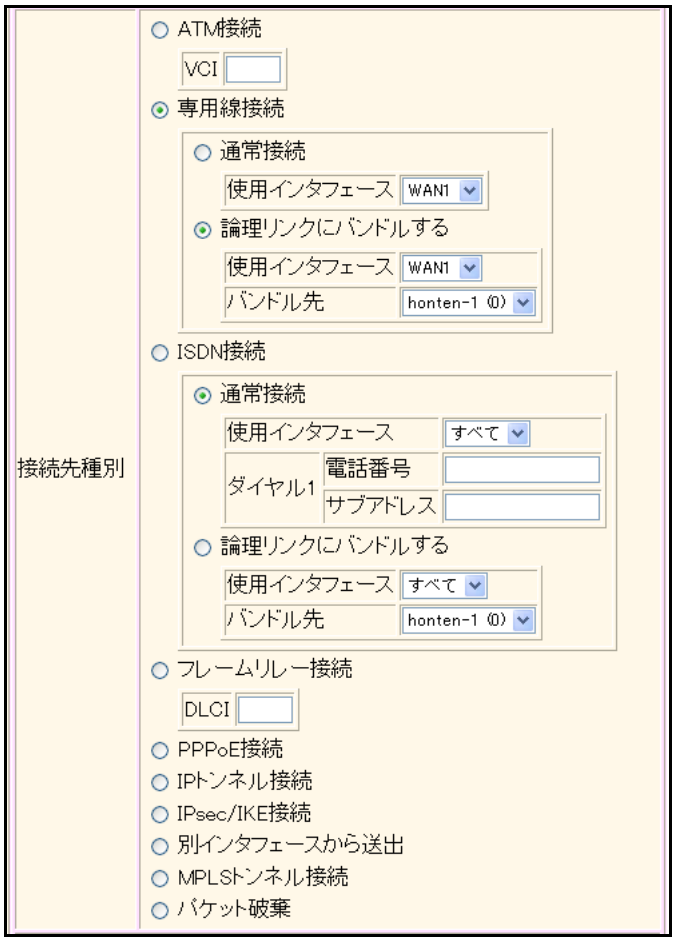
「ネットワーク情報（honten）」ページが表示されます。

21.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

22.　以下の項目を指定します。

- 接続先種別　→専用線接続
  →論理リンクにバンドルする
  使用インタフェース　→WAN1
  バンドル先　→honten-1（0）



23.　［追加］ボタンをクリックします。

専用線接続（バンドル）の設定項目と「基本情報」が表示されます。

24.　［保存］ボタンをクリックします。

PPP 関連を設定する

25.　画面上部の「ネットワーク情報（honten）」をクリックします。

「ネットワーク情報（honten）」ページが表示されます。

26.　「PPP 関連」をクリックします。

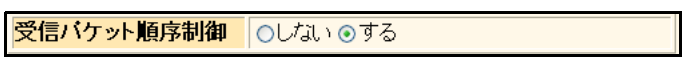
PPP 関連の設定項目と「圧縮情報」が表示されます。

27.　「MP 情報」をクリックします。

「MP 情報」が表示されます。

28.　以下の項目を指定します。

- 受信パケット順序制御　→ する



29.　［保存］ボタンをクリックします。

30.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

専用線だけで論理リンクを構成した場合、少なくとも 1 つの専用線で接続が可能であれば通信が維持されます。

- セッション監視機能は、論理リンクに対して機能します。マスタ回線で通信できない場合は、論理リンク内の通信可能な回線を探し、監視を継続します。
- 自動復旧モードは、論理リンクに対して機能します。自動復旧しない設定の場合でも、論理リンク内の少なくとも 1 つの回線が接続中であれば通信を維持します。
- 論理リンクを構成した場合、対向する装置間で正しく認証情報を設定するか、認証を off に設定してください。

2.10.3　専用線と ISDN 回線でマルチリンク機能を使う

適用機種　*Si-R370,570*

専用線と ISDN によって単一の論理リンクを構成することができます。この場合、ISDN でのマルチリンク機能と同様、回線使用率により動的に接続チャネル数を増減することができます。

論理リンクを構成する場合、主に使用する回線として専用線を設定します。これをマスタ回線と呼びます。ISDN は補助回線として設定します。これをバンドル回線と呼びます。

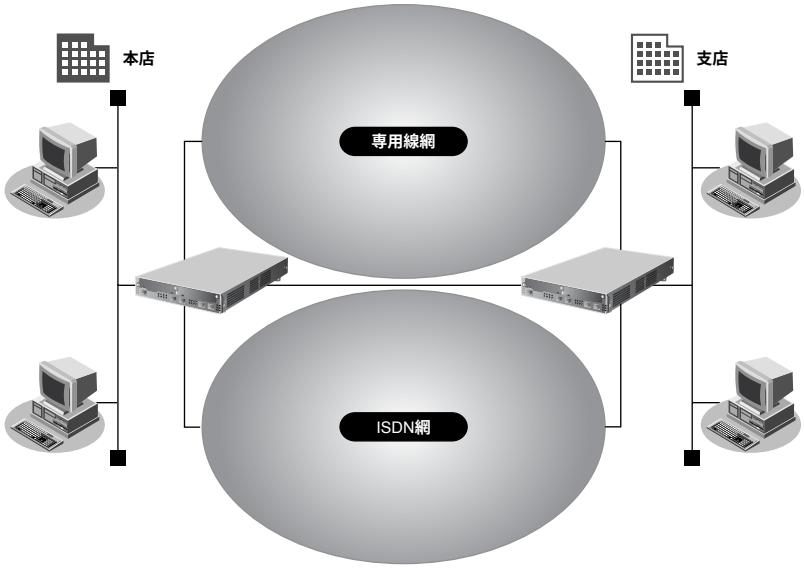
論理リンクの接続情報は、ISDN の接続情報を含めマスタ回線定義にすべて設定します。

参照　Si-R シリーズ 機能説明書「2.9 マルチリンク機能」（P.50）

ここでは、論理リンクを介して 2 つの事業所（本店、支店）のネットワークを接続する場合について説明します。

こんな事に気をつけて

速度の異なる回線を論理回線として結合した場合、期待する速度が出ない場合があります。



● 設定条件

- マスタ回線として、スロット 0 に実装された BRI 拡張モジュール L2 で専用線（128Kbps）を使用する
- バンドル回線として、スロット 1 に実装された BRI 拡張モジュール L2 で ISDN 回線を使用する
- 最大リンク数は 3 チャネル
- ISDN 回線はマルチリンク機能を使用する
- 回線使用率 90% 以上が 10 秒以上続いたら、チャネルを増加する
- 回線使用率 40% 以下が 60 秒以上続いたら、チャネルを減少する
- 無通信監視時間をしない

[本店]

- 接続ネットワーク名　：honten
- 接続先名　：honten-1
- 本装置の IP アドレス/ネットマスク　：192.168.1.1/24
- 電話番号　：03-7777-7777

- ユーザ認証 ID とユーザ認証パスワード
  発信　：honten、hontenpass
  着信　：shiten、shitenpass

[支店]

- 接続ネットワーク名　：shiten
- 接続先名　：shiten-1
- 本装置の IP アドレス/ネットマスク　：192.168.2.1/24
- 電話番号　：044-999-9999
- ユーザ認証 ID とユーザ認証パスワード
  発信　：shiten、shitenpass
  着信　：honten、hontenpass

上記の設定条件に従って本店の論理リンクの設定例を示します。

回線情報を設定する

スロット 0-0：WAN0、専用線

スロット 1-0：WAN1、ISDN

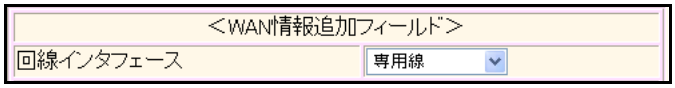
として以下の手順で設定します。

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→専用線



3.　[追加] ボタンをクリックします。

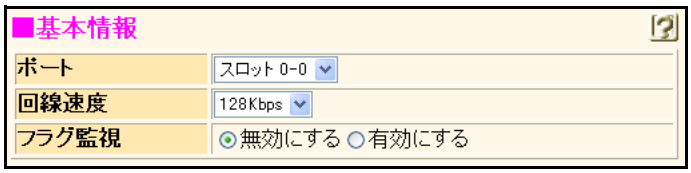
「WAN0 情報（専用線）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→ 128kbps
- フラグ監視　→無効にする



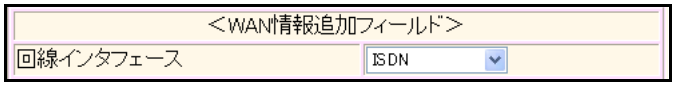
6.　[保存] ボタンをクリックします。

7.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

8.　以下の項目を指定します。

- 回線インタフェース　→ISDN



9.　［追加］ボタンをクリックします。

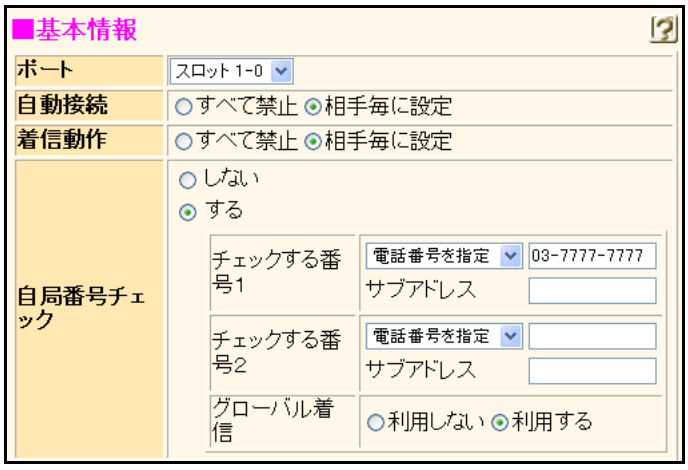
「WAN1 情報（ISDN）」ページが表示されます。

10.　「基本情報」をクリックします。

「基本情報」が表示されます。

11.　以下の項目を指定します。

- ポート　→スロット 1-0
- 自局番号チェック　→する
  チェックする番号 1　→03-7777-7777



12.　［保存］ボタンをクリックします。

相手情報を設定する

13.　設定メニューのルータ情報で「相手情報」をクリックします。

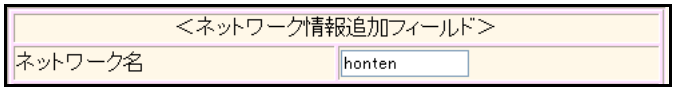
「相手情報」ページが表示されます。

14.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク名　→honten



16.　［追加］ボタンをクリックします。

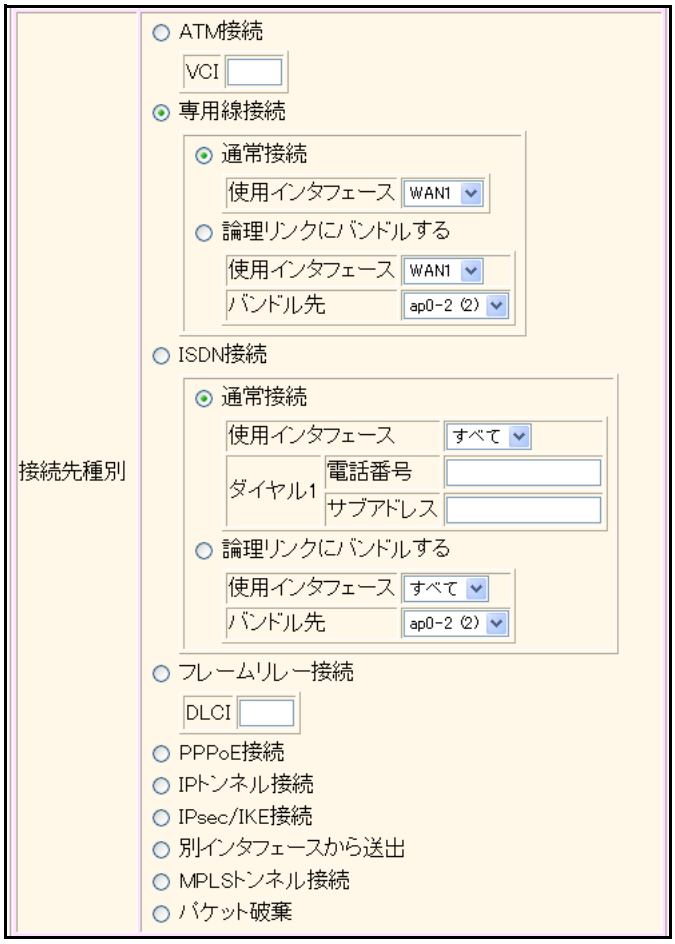
「ネットワーク情報（honten）」ページが表示されます。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先種別　→専用線接続

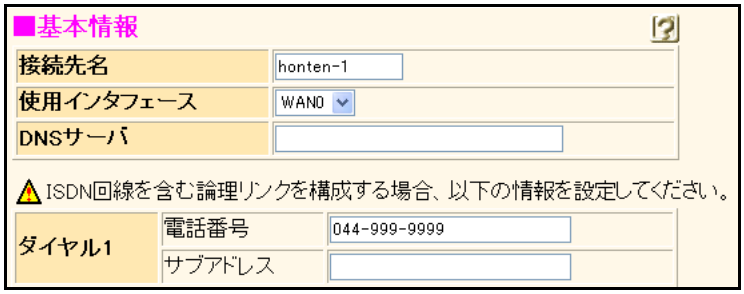


19.　［追加］ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 接続先名　→honten-1
- 使用インタフェース　→WAN0
- ダイヤル 1
  電話番号　→044-999-9999



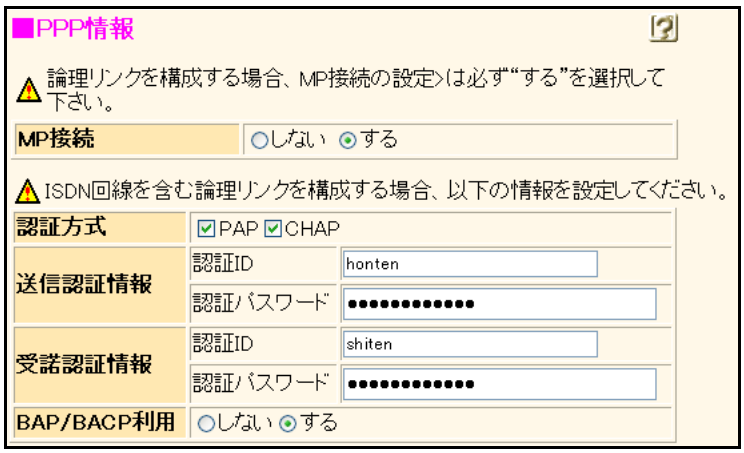
21.　［保存］ボタンをクリックします。

22.　設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

23.　以下の項目を指定します。

- MP 接続　→する
- 認証方式　→PAP、CHAP
- 送信認証情報
  認証 ID　→honten
  認証パスワード　→hontenpasswd
- 受諾認証情報
  認証 ID　→shiten
  認証パスワード　→shitenpasswd
- BAP/BACP 利用　→する



24.　［保存］ボタンをクリックします。

25.　画面上部の「ネットワーク情報（honten）」をクリックします。

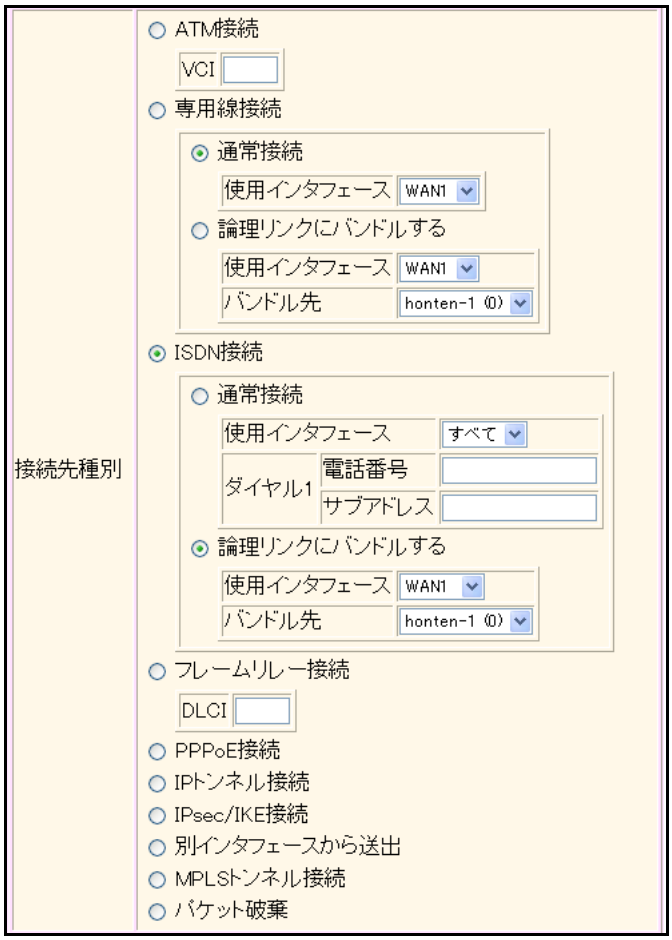
「ネットワーク情報（honten）」ページが表示されます。

26.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

27.　以下の項目を指定します。

- 接続先種別　→ISDN 接続
  →論理リンクにバンドルする
  使用インタフェース　→WAN1
  バンドル先　→honten-1（0）



28.　［追加］ボタンをクリックします。

ISDN 接続（バンドル）の設定項目と「基本情報」が表示されます。

29.　［保存］ボタンをクリックします。

PPP 関連を設定する

30.　画面上部の「ネットワーク情報（honten）」をクリックします。

「ネットワーク情報（honten）」ページが表示されます。

31.　「PPP 関連」をクリックします。

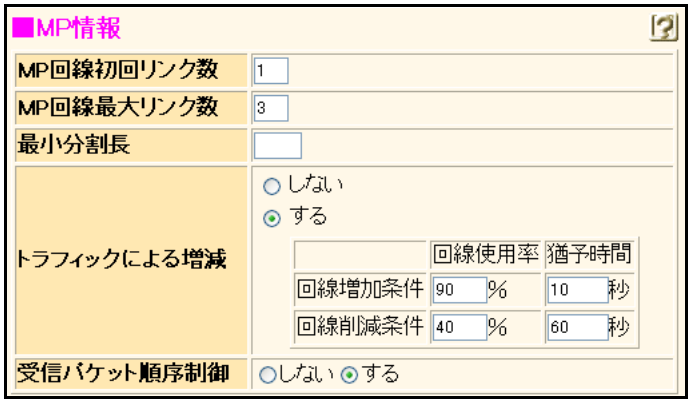
PPP 関連の設定項目と「圧縮情報」が表示されます。

32.　「MP 情報」をクリックします。

「MP 情報」が表示されます。

33.　以下の項目を指定します。

- MP 回線初回リンク数　→1
- MP 回線最大リンク数　→3
- トラフィックによる増減　→する
  回線増加条件
  回線使用率　→90
  猶予時間　→10
  回線削減条件
  回線使用率　→40
  猶予時間　→60
- 受信パケット順序制御　→する



34.　［保存］ボタンをクリックします。

35.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

専用線の通信障害を検出した場合、ISDN 接続だけでも論理リンクの維持を試みます。ISDN 接続だけで、論理リンクを維持する場合は、以下の点に注意してください。

- 常時接続が有効の場合は、即時 ISDN 接続を行います。
- 常時接続が無効の場合は、発信契機により ISDN 接続を行います。
  ただし、ほかの設定によっては無通信時に ISDN は切断されます。
- セッション監視が有効な場合、発信契機がセッション監視パケットだけの期間は、接続・切断が繰り返されることがあります。このような場合は、常時接続設定を有効にしてください。
- 対向する両装置で着番認証を無効に設定すると、ISDN 接続ができないことがあります。着番認証を無効にする場合は、相手局の認証を無効に設定してください。
- 専用線と ISDN 接続での論理リンク構成時に、専用線が通信障害などで使用できない場合、ISDN 接続が切断されないことがあります。専用線と ISDN 接続での論理リンク構成時には、必ず回線使用率によるチャネル制御を設定してください。

2.11 マルチキャスト機能を使う

適用機種　全機種

本装置には、マルチキャスト機能を動作させるために以下の 2 種類のプロトコルがあります。

- PIM-DM プロトコル
- PIM-SM プロトコル

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

参照　Si-R シリーズ　機能説明書「2.10 マルチキャスト機能」（P.52）

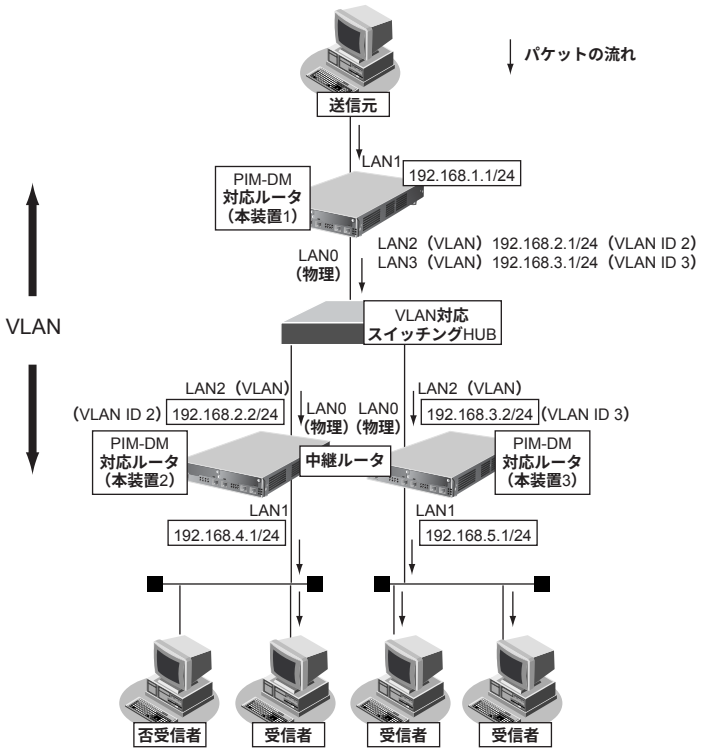
2.11.1 マルチキャスト機能（PIM-DM）を使う

適用機種　全機種

マルチキャスト機能（PIM-DM）を使用すると、会社などの LAN 内で、動画や音声などを配送することができます。

こんな事に気をつけて

- **マルチキャストでパケットを配送するルータは、すべて PIM-DM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。**
- **IP アドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側 IP アドレスと相手側 IP アドレスの両方を正しく設定する必要があります。**



ここでは、PIM-DM を利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

本装置 1、本装置 2、本装置 3 が以下のとおり設定されていることを前提とします。

● 前提条件

- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　　ネットワークアドレス：192.168.3.0/24

[本装置 1]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1 の IP アドレス　　：192.168.1.1/24
- LAN2 の IP アドレス　　：192.168.2.1/24
- LAN3 の IP アドレス　　：192.168.3.1/24

[本装置 2]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1 の IP アドレス　　：192.168.4.1/24
- LAN2 の IP アドレス　　：192.168.2.2/24

[本装置 3]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1 の IP アドレス　　：192.168.5.1/24
- LAN2 の IP アドレス　　：192.168.3.2/24

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-DM を利用する

[本装置 1]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2、LAN3 を使用する

[本装置 2]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する

[本装置 3]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

LAN1 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

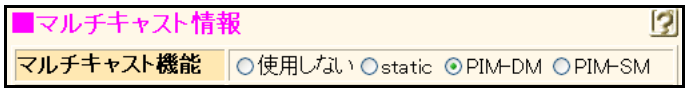
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」が表示されます。

5.　以下の項目を指定します。

- マルチキャスト機能　→PIM-DM



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、以下の項目を指定します。

「LAN2 情報（VLAN）」

- マルチキャスト機能　→PIM-DM

「LAN3 情報（VLAN）」

- マルチキャスト機能　→PIM-DM

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

LAN1 情報を設定する

「LAN1 情報」-「IP 関連」
「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

LAN2 情報を設定する

「LAN2 情報」-「IP 関連」
「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

本装置 3 を設定する

「本装置 1 を設定する」を参考に、本装置 3 を設定します。

LAN1 情報を設定する

「LAN1 情報」-「IP 関連」
「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

LAN2 情報を設定する

「LAN2 情報」-「IP 関連」
「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

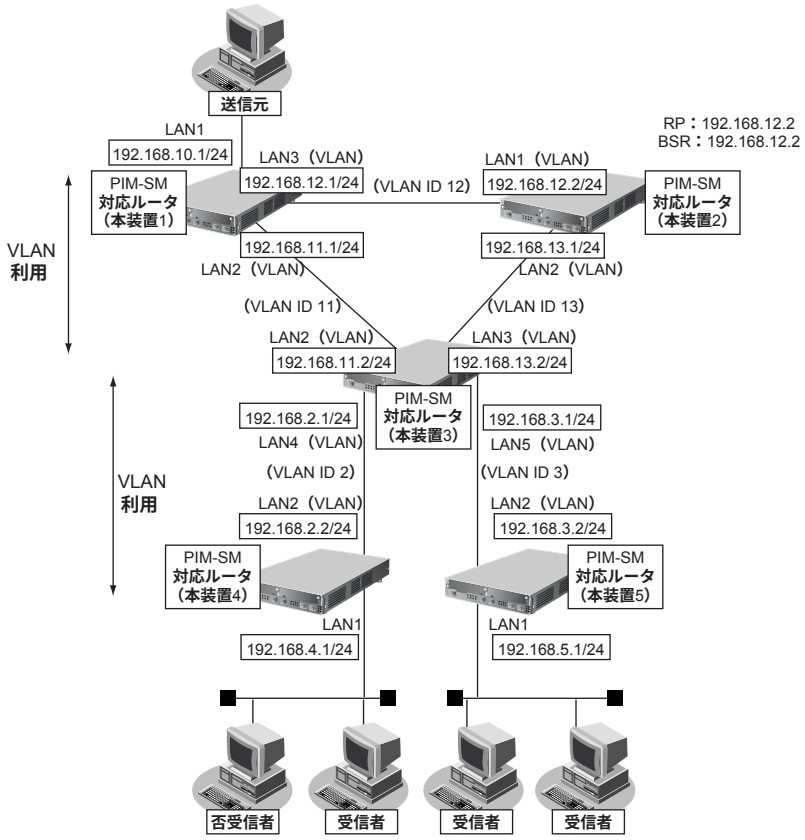
2.11.2　マルチキャスト機能（PIM-SM）を使う

適用機種　全機種

マルチキャスト機能（PIM-SM）を使用すると、インターネットなど、十分な帯域を保証されないネットワーク上で、マルチキャスト・パケットを配送することができます。

こんな事に気をつけて

- **マルチキャスト・パケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。**
- **IP アドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側 IP アドレスと相手側 IP アドレスの両方を正しく設定する必要があります。**
- **ネットワーク内に BSR（Bootstrap Router：ブートストラップルータ）として動作するルータを 1 台以上置く必要があります。BSR は RP（Rendezvous Point：ランデブーポイント）の情報を広報します。**
- **ネットワーク内に RP として動作するルータを 1 台以上置く必要があります。パケットの配送は、RP を配送樹の頂点として開始され、その後、最短経路（SPT：Shortest Path Tree）に切り替わります。**
- **PIM-SM ではマルチキャスト・パケットの配送を RP を配送樹の頂点として開始するため、RP はネットワークの中心付近に置くことをお勧めします。**
- **SPT への切り替えは、マルチキャスト・パケットの受信者の直前のルータ（lasthop router）が行います。lasthop router で設定することで SPT への切り替えを無効にすることができます。**



ここでは、PIM-SM を利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

この設定例では、VLAN を利用して、上図のネットワークを仮想的に構築します。

マルチキャスト・パケットは、はじめは RP である本装置 2 を経由して、本装置 1 →本装置 2 →本装置 3 →本装置 4 の順に配送されます（一度、本装置 1 から本装置 2 に送られ、本装置 2 を配送樹の頂点として配送されます）。本装置 4 へのパケット転送開始直後に、本装置 4 は SPT への切り替えを開始します。切り替えが行われると、本装置 1 →本装置 3 →本装置 4 のように、最短経路を利用して配送されます（本装置 1 を配送樹の頂点として配送されます）。同様の切り替えが本装置 5 でも行われます。

ここでは、本装置 1、本装置 2、本装置 3、本装置 4、本装置 5 が以下のとおりに設定されていることを前提とします。

● 前提条件

- VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　ネットワークアドレス：192.168.3.0/24
  VLAN ID：11　ネットワークアドレス：192.168.11.0/24
  VLAN ID：12　ネットワークアドレス：192.168.12.0/24
  VLAN ID：13　ネットワークアドレス：192.168.13.0/24
- ユニキャストのルーティングテーブルの作成に RIP を使用する

[本装置 1]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.10.1/24
- LAN2 の IP アドレス　：192.168.11.1/24
- LAN3 の IP アドレス　：192.168.12.1/24

[本装置 2]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN1、LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.12.2/24
- LAN2 の IP アドレス　：192.168.13.1/24

[本装置 3]

- LAN0、LAN1 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN4、LAN5 は VLAN とし、出力先の物理インタフェースは LAN1 とする
- LAN2 の IP アドレス　：192.168.11.2/24
- LAN3 の IP アドレス　：192.168.13.2/24
- LAN4 の IP アドレス　：192.168.2.1/24
- LAN5 の IP アドレス　：192.168.3.1/24

[本装置 4]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.4.1/24
- LAN2 の IP アドレス　：192.168.2.2/24

[本装置 5]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.5.1/24
- LAN2 の IP アドレス　：192.168.3.2/24

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-SM を利用する
- RP、BSR は本装置 2 が行う
- SPT への切り替えを行う（初期値）

[本装置 1]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2、LAN3 を使用する

[本装置 2]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する
- RP　：192.168.12.2
- BSR　：192.168.12.2

[本装置 3]

- マルチキャスト・パケットを転送するインタフェースとして LAN2 ～ 5 を使用する

[本装置 4]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する

[本装置 5]

- マルチキャスト・パケットを転送するインタフェースとして LAN1、LAN2 を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

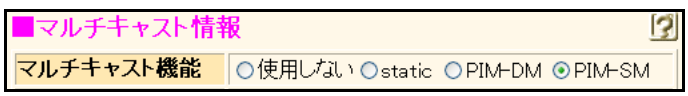
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」が表示されます。

5.　以下の項目を指定します。

- マルチキャスト機能　→ PIM-SM



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、以下の項目を指定します。

「LAN2 情報（VLAN）」

- マルチキャスト機能　→PIM-SM

「LAN3 情報（VLAN）」

- マルチキャスト機能　→PIM-SM

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

1.　「本装置 1 を設定する」を参考に、以下の項目を指定します。

「LAN1 情報（VLAN）」

- マルチキャスト機能　→PIM-SM

「LAN2 情報（VLAN）」

- マルチキャスト機能　→PIM-SM

2.　設定メニューのルータ設定で「マルチキャスト情報」をクリックします。

「マルチキャスト情報」ページが表示されます。

3.　「IP マルチキャスト情報」をクリックします。

「IP マルチキャスト情報」が表示されます。

4.　以下の項目を指定します。

- PIM-SM
  RP 候補　→する
  IP アドレス　→192.168.12.2
  BSR 候補　→する
  IP アドレス　→192.168.12.2

5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 3 を設定する

「本装置 1 を設定する」を参考に、本装置 3 を設定します。

「LAN2（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

「LAN3（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

「LAN4（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

「LAN5（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

本装置 4 を設定する

「本装置 1 を設定する」を参考に、本装置 4 を設定します。

「LAN1（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

「LAN2（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

本装置 5 を設定する

「本装置 1 を設定する」を参考に、本装置 5 を設定します。

「LAN1（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

「LAN2（VLAN）情報」-「IP 関連」
「マルチキャスト情報」
- マルチキャスト機能　→ PIM-SM

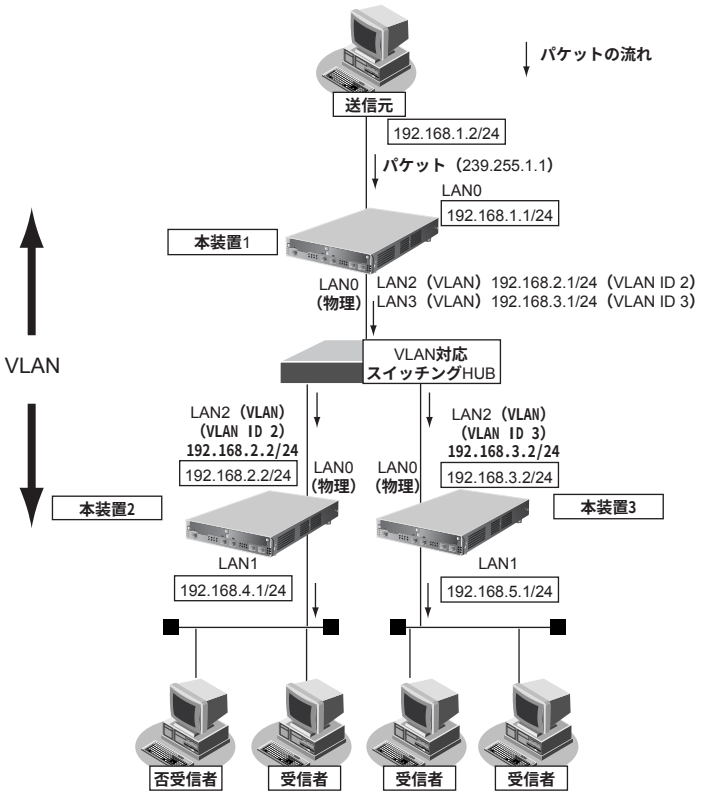
2.11.3　マルチキャスト機能（スタティックルーティング）を使う

適用機種　全機種

マルチキャスト機能（スタティックルーティング）を使用すると、マルチキャストパケットが配送される経路を静的に設定することができます。

こんな事に気をつけて

マルチキャスト・スタティックルーティングでは、入力インタフェースでの IGMP グループ参加を指定することができます。
上流側に PIM-DM などの IGMP 参加要求を受け付けるマルチキャスト・ルータが存在する場合は、入力インタフェースで IGMP グループ参加を行うことで、パケットを強制的に転送させることができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。
本装置 1、本装置 2、本装置 3 が以下のとおり設定されていることを前提とします。

● 前提条件

- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：2　　ネットワークアドレス：192.168.2.0/24
  VLAN ID：3　　ネットワークアドレス：192.168.3.0/24

[本装置 1]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　　：192.168.1.1/24
- LAN2 の IP アドレス　　：192.168.2.1/24
- LAN3 の IP アドレス　　：192.168.3.1/24

[本装置 2]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1 の IP アドレス　：192.168.4.2/24
- LAN2 の IP アドレス　：192.168.2.1/24

[本装置 3]

- LAN0 は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN4、LAN5 は VLAN とし、出力先の物理インタフェースは LAN1 とする
- LAN1 の IP アドレス　：192.168.5.2/24
- LAN2 の IP アドレス　：192.168.3.2/24

● 設定条件

- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする
- 入力インタフェースでの IGMP グループ参加は行わない

[本装置 1]

- マルチキャストパケットを転送するインタフェースとして LAN1、LAN2、LAN3 を使用する

[本装置 2]

- マルチキャストパケットを転送するインタフェースとして LAN1、LAN2 を使用する

[本装置 3]

- マルチキャストパケットを転送するインタフェースとして LAN1、LAN2 を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

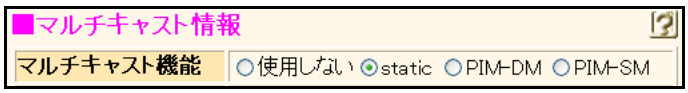
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」が表示されます。

5.　以下の項目を指定します。

- マルチキャスト機能　→static



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、以下の項目を指定します。

「LAN2 情報（VLAN）」

- マルチキャスト機能　→ static

「LAN3 情報（VLAN）」

- マルチキャスト機能　→ static

8.　設定メニューのルータ設定で「マルチキャスト情報」をクリックします。

「マルチキャスト情報」ページが表示されます。

9.　「IP マルチキャストスタティック経路情報」をクリックします。

「IP マルチキャストスタティック経路情報」ページが表示されます。

10.　以下の項目を指定します。

- 配送元ホストアドレス　→ 192.168.1.2
- マルチキャストグループアドレス　→ 239.255.1.1
- 入力インタフェース　→ LAN1
- 出力インタフェース　→ lan2-lan3
- グループ参加　→ しない

11.　［追加］ボタンをクリックします。

12.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「LAN1 情報」-「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能　→ static

「LAN2 情報」-「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能　→ static

「マルチキャスト情報」-「IP マルチキャストスタティック経路情報」

- 配送元ホストアドレス　→ 192.168.1.2
- 配送元ホストアドレス　→ 192.168.1.2
- 配送元ホストアドレス　→ 192.168.1.2
- 配送元ホストアドレス　→ 192.168.1.2
- グループ参加　→ しない

本装置 3 を設定する

「本装置 1 を設定する」を参考に、本装置 3 を設定します。

「LAN1 情報」-「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能　→ static

「LAN2 情報」-「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能　→ static

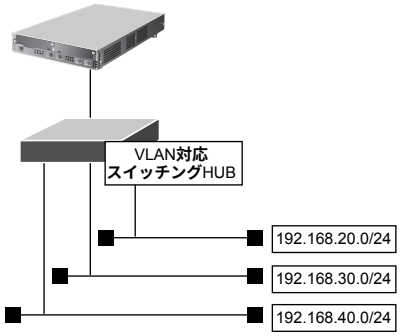
「マルチキャスト情報」-「IP マルチキャストスタティック経路情報」

- 配送元ホストアドレス　→ 192.168.1.2
- マルチキャストグループアドレス　→ 192.168.1.1
- 入力インタフェース　→ LAN2
- 出力インタフェース　→ lan1
- グループ参加　→ しない

2.12 VLAN 機能を使う

適用機種　全機種

ここでは、VLAN 機能を利用して、1 つの物理ポートで 3 つのネットワークを組む場合を例に説明します。



参照 Si-R シリーズ　機能説明書「2.11 VLAN 機能」（P.55）

● 設定条件

- LAN0 ポートを使用する
- VLAN ID として 2、3、4 を使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける

VLAN ID：2	ネットワークアドレス：192.168.20.0/24
VLAN ID：3	ネットワークアドレス：192.168.30.0/24
VLAN ID：4	ネットワークアドレス：192.168.40.0/24

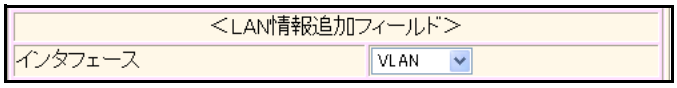
上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→VLAN



3.　［追加］ボタンをクリックします。

「LAN1 情報（VLAN）」ページが表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 出力先　→LAN0
- VLAN ID　→2
- プライオリティ　→0

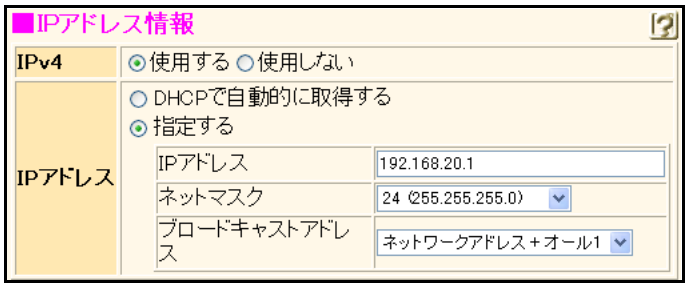
6.　［保存］ボタンをクリックします。

7.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

8.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→192.168.20.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



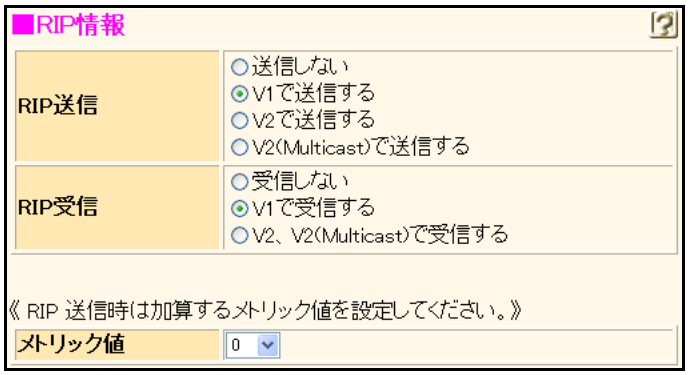
9.　［保存］ボタンをクリックします。

10.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

11.　以下の項目を指定します。

- RIP 送信　→V1 で送信する
- RIP 受信　→V1 で受信する
- メトリック値　→0



12.　［保存］ボタンをクリックします。

13.　手順 1. ～ 12. を参考に、以下の項目を指定します。

［192.168.30.0/24 のネットワーク］

- インタフェース情報　→VLAN
  出力先　→lan0
  VLAN ID　→3
  プライオリティ　→0
- IP アドレス　→指定する
  IP アドレス　→192.168.30.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1
- RIP 送信　→V1 で送信する
- RIP 受信　→V1 で受信する
- メトリック値　→0

14.　手順 1. ～ 12. を参考に、以下の項目を指定します。

［192.168.40.0/24 のネットワーク］

- インタフェース情報　→VLAN
  出力先　→lan0
  VLAN ID　→4
  プライオリティ　→0
- IP アドレス　→指定する
  IP アドレス　→192.168.40.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1
- RIP 送信　→V1 で送信する
- RIP 受信　→V1 で受信する
- メトリック値　→0

15.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **VLAN 機能を利用すると、Ethernet フレームに 4 バイトの VLAN タグが付加され、最大 1522 バイトの Ethernet フレームが送出されることになります。通常の Ethernet フレームの最大サイズは 1518 バイトです。そのため、その状態では 1522 バイトのフレームに対応していない機器とは接続することはできません。1522 バイトのフレームに対応していない機器と接続する場合は、VLAN インタフェースの MTU サイズを 1496 に変更してください。**
- **VLAN の物理インタフェースに、VLAN インタフェースを使用することはできません。**
- **同じ物理インタフェースを使用する複数の VLAN インタフェース上で、重複する VLAN ID を使用することはできません。**
- **VLAN 対応スイッチング HUB やルータ製品の中には、VLAN が設定されていない LAN ポートで、VLAN タグ付きフレームを受信してしまう装置があります。**
  このような装置と接続する際には、スイッチング HUB（またはルータ）の設定を「VLAN あり」から「VLAN なし」に設定を変更してください。
  また、フレームを送信する PC の arp エントリが本装置に残っていると、arp エントリの生存時間中だけ通信するという現象が発生する場合があります。これを防ぐために、設定後に本装置の［設定反映］ボタンをクリックしてください。

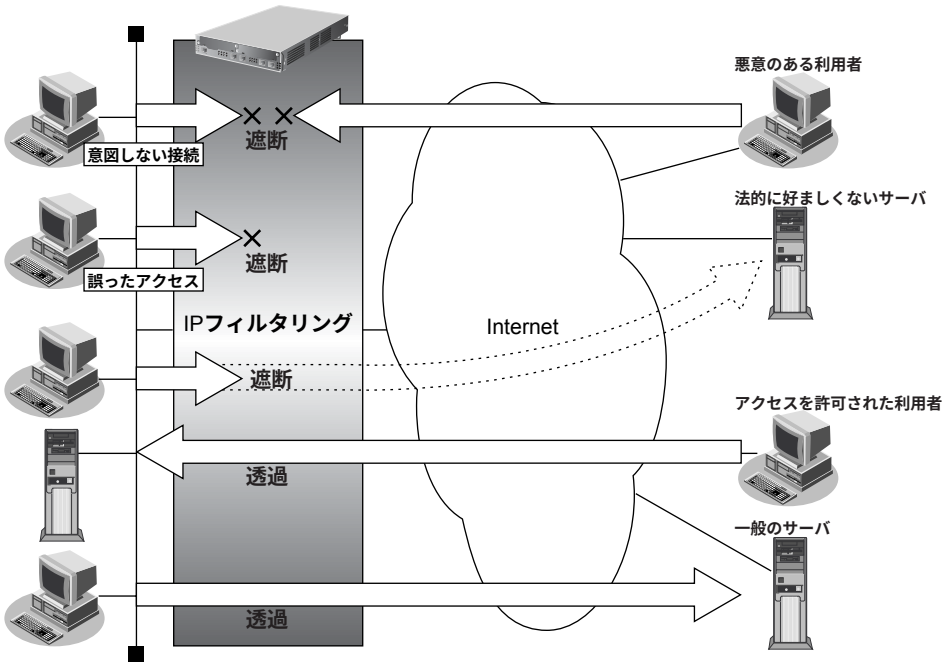
- VLAN を利用する物理 LAN インタフェースの情報として、以下の手順で「ポート番号」と「転送レート」を必ず設定してください。「LAN 情報（物理 LAN）」を設定しない場合、VLAN を利用する LAN 情報は設定できません。
  以下に手順を示します。
  1. 設定メニューのルータ設定で「LAN 情報」をクリックします。
  2. インタフェースに“物理インタフェース”を指定して、［追加］ボタンをクリックします。
  3.「共通情報」－「基本情報」で、ポート番号と転送レートを選択して、［保存］ボタンをクリックします。
- VLAN インタフェースを追加する場合は、先に物理 LAN インタフェースを設定してください。

2.13 IP フィルタリング機能を使う

適用機種　全機種

参照　Si-R シリーズ　機能説明書「2.12 IP フィルタリング機能」（P.56）

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットを IP アドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。



IP フィルタリングの条件

本装置では、以下の条件を指定することによって、データの流れを制御できます。

- 動作
- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- あて先情報（IP アドレス／アドレスマスク／ポート番号）
- TCP 接続要求
- TOS 値
- 方向

ヒント

◆ TCP 接続要求とは

TCP プロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうか指定するものです。フィルタリングの動作に透過、プロトコルに TCP を指定した場合に有効です。TCP プロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することによって、コネクションを開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

次に、TCP パケットとフラグ設定について説明します。TCP パケット内には SYN フラグと ACK フラグの 2 つの制御フラグがあります。このフラグの組み合わせによって、TCP パケットの内容が分かります。以下に、対応表を示します。

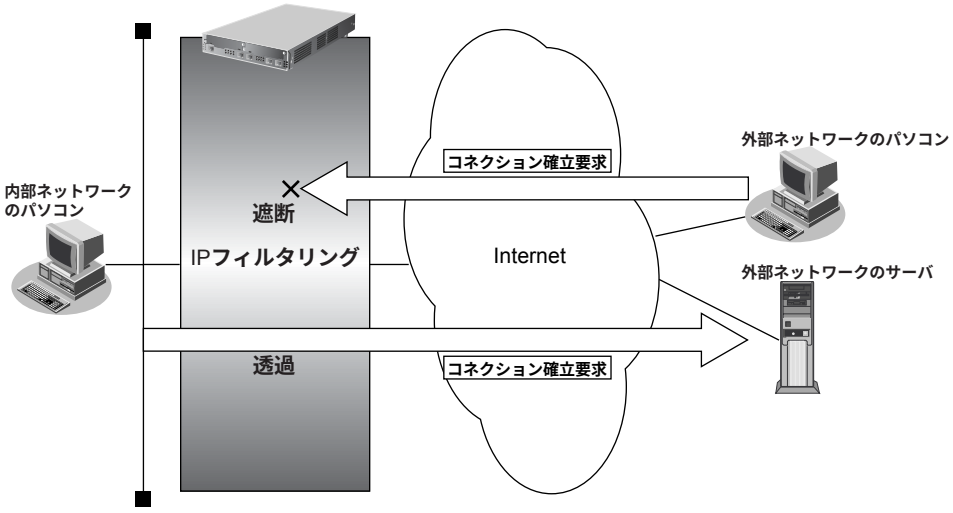
制御フラグ		TCP パケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

この表から、制御フラグの組み合わせが SYN ＝ 1、ACK ＝ 0 の場合に、TCP パケットがコネクションの確立要求を行うことが分かります。つまり、IP パケットが禁止されている IP アドレスからの送信を禁止すれば、TCP/IP サービスのフィルタリングを行えます。

以下に、telnet（ポート番号 23）を例に説明します。

・外部ネットワークからのコネクション確立要求は遮断

・内部ネットワークからのコネクション確立要求は透過



◆ IP アドレスとアドレスマスクの決め方

IP フィルタリング条件の要素には「IP アドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットの IP アドレスとアドレスマスクの論理積の結果が、指定した IP アドレスと一致したものに限ります。

◆ IP フィルタリングの方向

IP フィルタリングの方向に「リバース（reverse)」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元 IP アドレス／アドレスマスクとあて先 IP アドレス／アドレスマスク
- 送信元ポート番号とあて先ポート番号

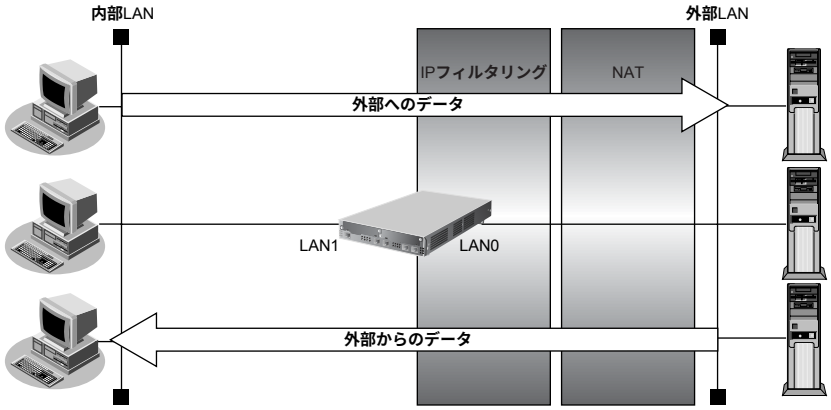
補足 IP フィルタリング機能と NAT 機能を併用する場合、回線切断時に NAT 機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IP フィルタリング機能によってパケットは破棄されてしまいます。

ヒント

◆ アドレス変換（NAT）機能利用時の IP フィルタリングのかかるタイミング

内部 LAN から外部 LAN に向かう場合は、アドレス変換でアドレスが変更される前に IP フィルタリング処理を通過します。また、外部 LAN から内部 LAN に向かう場合は、アドレス変換でアドレスが変更されたあとで、IP フィルタリング処理を通過します。つまり、IP フィルタリングは「プライベートアドレス」を対象に行います。

本装置の IP フィルタリングとアドレス変換の位置付けは以下のとおりです。



IP フィルタリングの設計方針

IP フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる。

B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する。

ここでは、設計方針 A の例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけ許可して SPI を併用する
- 外部の特定サービスへのアクセスだけを許可する（IPv6 フィルタリング）

また、設計方針 B の例として、以下の設定例について説明します。

- 外部の特定サーバへのアクセスだけを禁止する
- 利用者が意図しない発信を防ぐ
- 回線が接続しているときだけ許可する

補足 TCP 接続要求の設定は、プロトコルに TCP またはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

こんな事に気をつけて

- **IP フィルタリングで WWW（ポート番号 80）でのアクセスを制限する設定を行った場合、外部の WWW ブラウザから設定ができなくなる場合があります。**
- **IP フィルタリングで DHCP（ポート番号 67、68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。**
- **IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。PPPoE の場合は、remote 側にフィルタをかけるようにしてください。**
- **IP フィルタリングの方向に「reverse」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。**
  - **送信元 IP アドレス／アドレスマスクとあて先 IP アドレス／アドレスマスク**
  - **送信元ポート番号とあて先ポート番号**

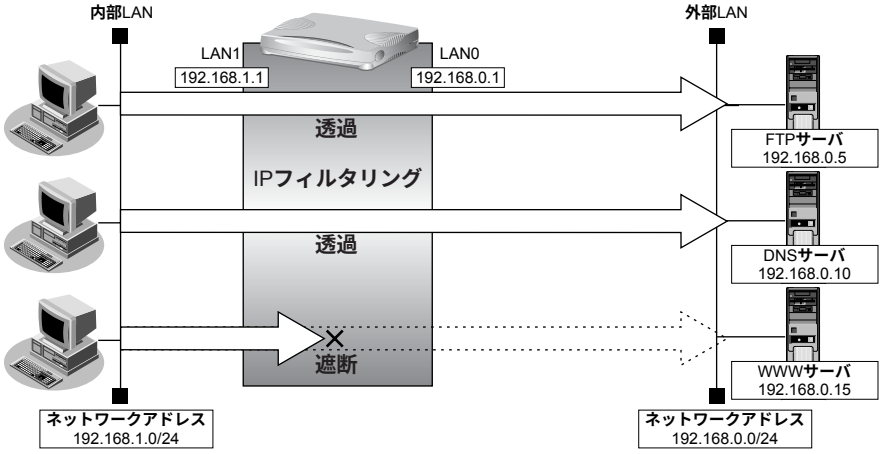
2.13.1　外部の特定サービスへのアクセスだけ許可する

適用機種　全機種

LAN 定義の場合

ここでは、一時的に LAN を作成し、外部 LAN のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する FTP サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP サーバへのアクセスを許可
- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN への DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには

  （1）192.168.1.0/24 の任意のポートから、任意の FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる

- DNS サーバへのアクセスを許可するには

  （1）192.168.1.0/24 の任意のポートから、DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる

- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- その他をすべて遮断するには
  （1）すべてのパケットを遮断する

補足 このルールでは、ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

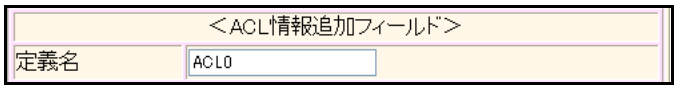
任意の FTP サーバのポート 21 への TCP パケットを透過させる（内部 LAN→外部 LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

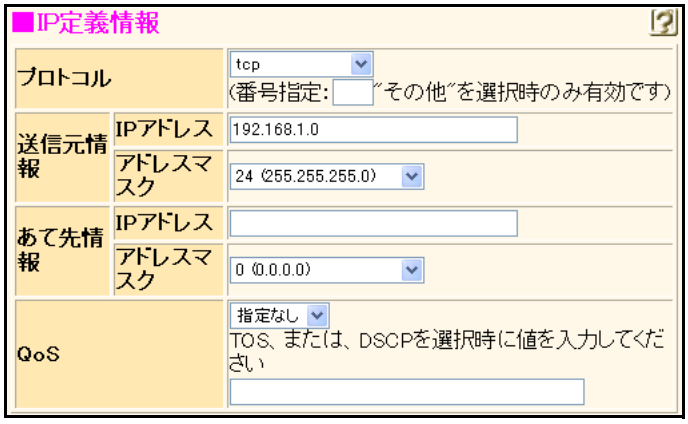
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし



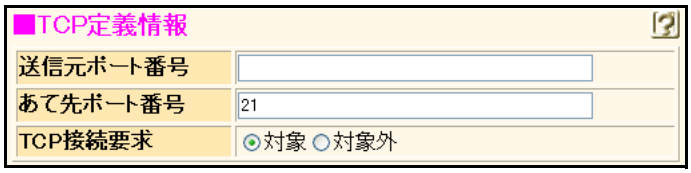
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

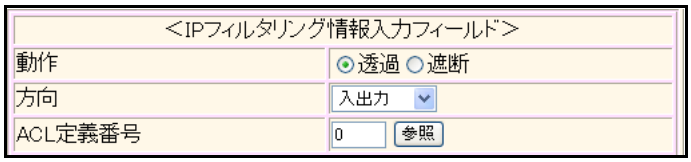
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

FTP サーバからの応答パケットを透過させる（外部 LAN →内部 LAN）

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→ 21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 1

DNS サーバのポート 53 への UDP パケットを透過させる（内部 LAN →外部 LAN）

17.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

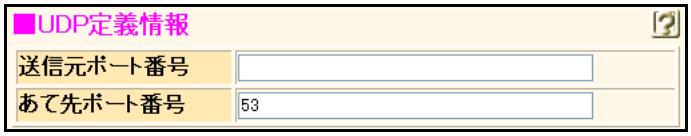
- プロトコル　→ udp
- 送信元情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→ 192.168.0.10
  アドレスマスク　→ 32（255.255.255.255）
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53（domain のポート番号）



20.　［保存］ボタンをクリックします。

21.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→2

DNS サーバからの応答パケットを透過させる（外部 LAN→内部 LAN）

22.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→udp
- 送信元情報
  IP アドレス　→192.168.0.10
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

23.　手順 18.～20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→53（domain のポート番号）
- あて先ポート番号　→指定しない

24.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→3

ICMP のパケットを透過させる

25.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL4

「ACL 定義情報（ACL4）」-「IP 定義情報」

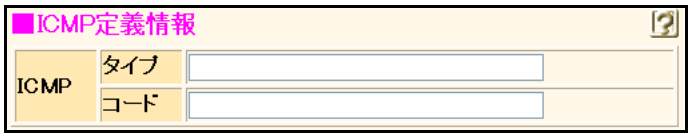
- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

26.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

27.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



28.　［保存］ボタンをクリックします。

29.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

残りのパケットをすべて遮断する

30.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL5

「ACL 定義情報（ACL5）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

31.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→5

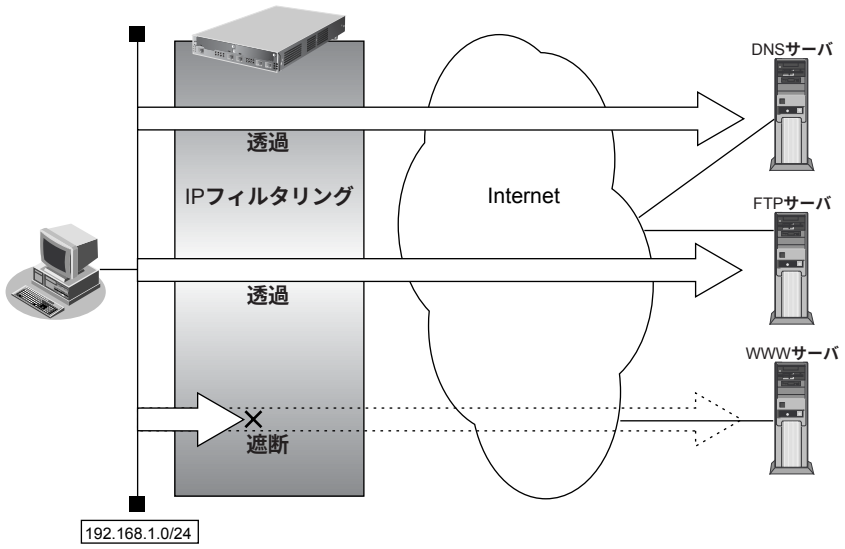
32.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、LAN 上のパソコンからインターネット上のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する FTP サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。
- 本装置は、ftp-data の転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）から任意の FTP サーバへのアクセスを許可
- LAN 上のホスト（192.168.1.0/24）から WAN の先の DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには

  (1)192.168.1.0/24 の任意のポートから、任意の FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  (2)(1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには

  (1)192.168.1.0/24 の任意のポートから、DNS サーバのポート 53（domain）への UDP パケットを透過させる
  (2)(1）の応答パケットを透過させる
- ICMP の通信を許可するためには

  (1)ICMP パケットを透過させる

- その他をすべて遮断するには
  (1)すべてのパケットを遮断する

補足 このルールでは ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

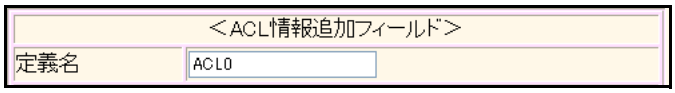
任意の FTP サーバのポート 21 への TCP パケットを透過させる（LAN→インターネット）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

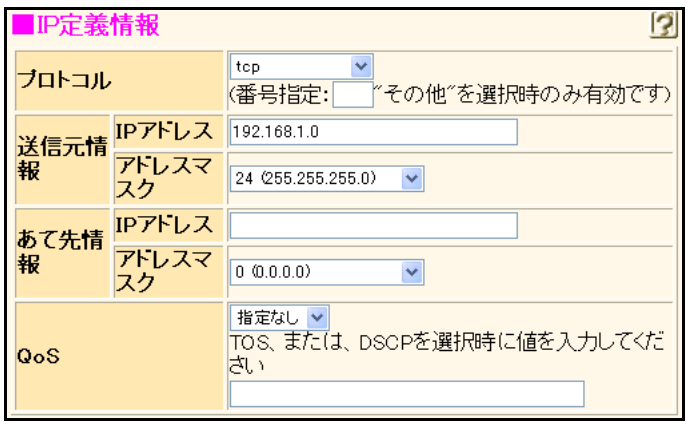
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし



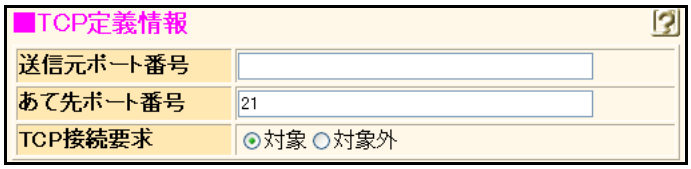
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

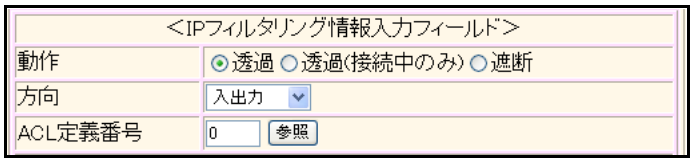
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

FTP サーバからの応答パケットを透過させる（インターネット→LAN）

16.　手順 1.～15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

DNS サーバのポート 53 への UDP パケットを透過させる（LAN→インターネット）

17.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

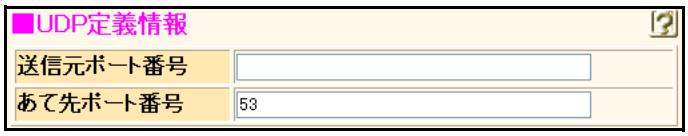
- プロトコル　→udp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.0.10
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53（domain のポート番号）



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→2

DNS サーバからの応答パケットを透過させる（インターネット→LAN）

22.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→udp
- 送信元情報
  IP アドレス　→192.168.0.10
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

23.　手順 18. ～ 20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→53（domain のポート番号）
- あて先ポート番号　→指定しない

24.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→3

ICMP のパケットを透過させる

25.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL4

「ACL 定義情報（ACL4）」-「IP 定義情報」

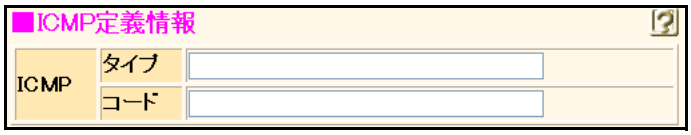
- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

26.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

27.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



28.　［保存］ボタンをクリックします。

29.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

残りのパケットをすべて遮断する

30.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL5

「ACL 定義情報（ACL5）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

31.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→5

32.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

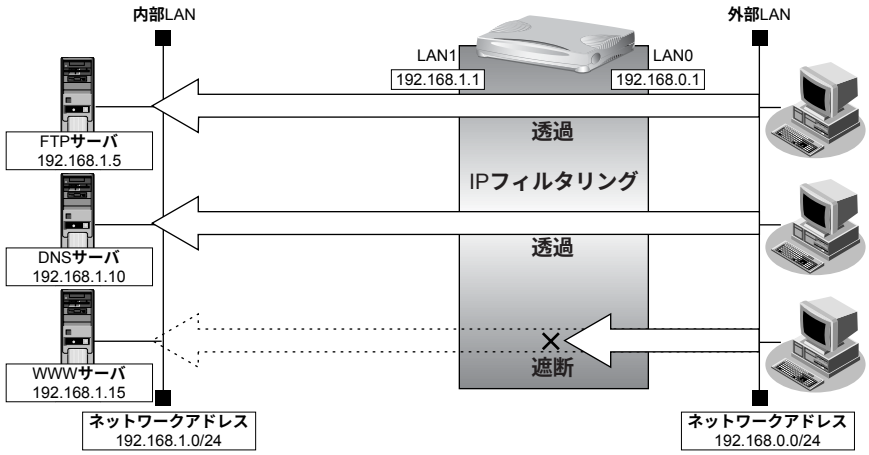
2.13.2　外部から特定サーバへのアクセスだけ許可する

適用機種　全機種

LAN 定義の場合

ここでは、内部 LAN の特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの問い合わせが発生します。あらかじめ接続する ftp サーバが決まっている場合は、本装置の DNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.5/32）を FTP サーバとして利用を許可
- 内部 LAN のネットワークへの DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部 LAN のホストの FTP サーバとしての利用を許可するには
  （1）192.168.1.5/32 のポート 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.0.0/24 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる

- その他をすべて遮断するには

  (1)すべてのパケットを遮断する

補足 このルールでは、ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

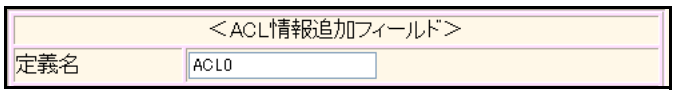
内部 LAN のホストのポート 21 への TCP パケットを透過させる（外部 LAN→内部 LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

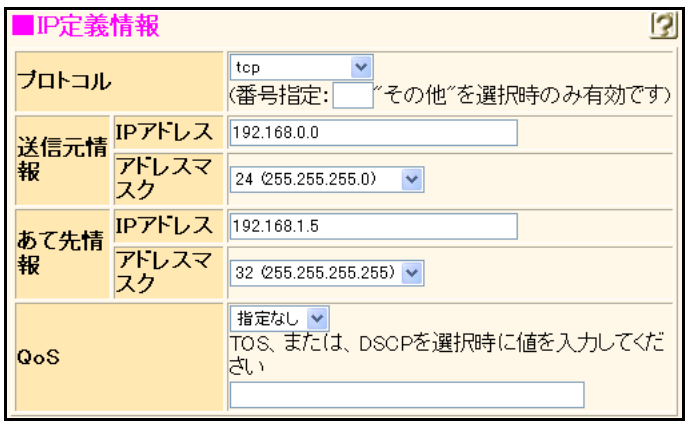
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



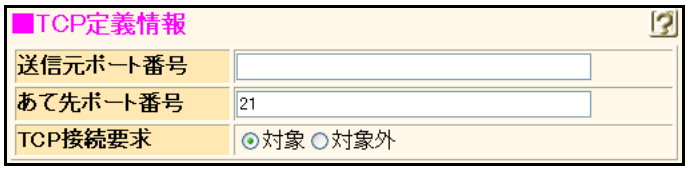
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。

15.　［追加］ボタンをクリックします。

内部 LAN のホストからの応答パケットを透過させる（内部 LAN →外部 LAN）

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→ 192.168.1.5
  アドレスマスク　→ 32（255.255.255.255）
- あて先情報
  IP アドレス　→ 192.168.0.0
  アドレスマスク　→ 24（255.255.255.0）
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→ 21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 1

DNS サーバのポート 53 への UDP パケットを透過させる（外部 LAN →内部 LAN）

17.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

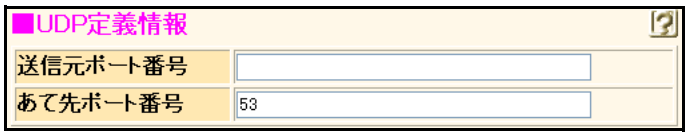
- プロトコル　→ udp
- 送信元情報
  IP アドレス　→ 192.168.0.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→ 192.168.1.10
  アドレスマスク　→ 32（255.255.255.255）
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53（domain のポート番号）



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→2

DNS サーバからの応答パケットを透過させる（内部 LAN →外部 LAN）

22.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→udp
- 送信元情報
  IP アドレス　→192.168.1.10
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

23.　手順 18. ～ 20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→53（domain のポート番号）
- あて先ポート番号　→指定しない

24.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→3

ICMP のパケットを透過させる

25.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL4

「ACL 定義情報（ACL4）」-「IP 定義情報」

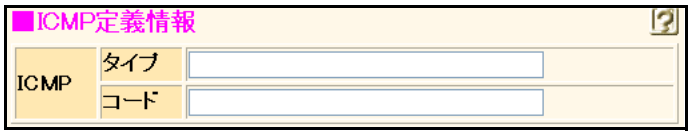
- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

26.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

27.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



28.　［保存］ボタンをクリックします。

29.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

残りのパケットをすべて遮断する

30.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL5

「ACL 定義情報（ACL5）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

31.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

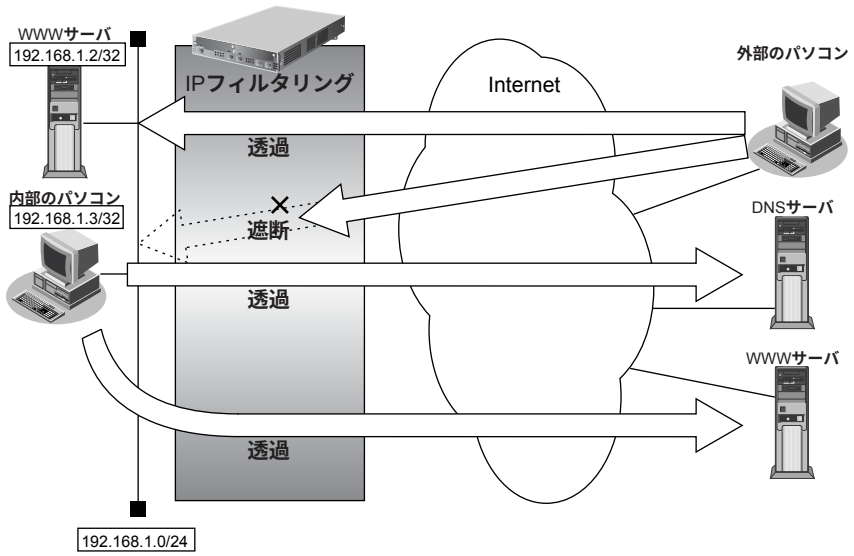
- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→5

32.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、LAN 上の WWW サーバに対する外部のパソコンからのアクセスを許可し、LAN 上のほかのパソコンへのアクセスは禁止する場合の設定方法を説明します。また、LAN 上のほかのパソコンはインターネット上の WWW サーバに対してアクセスすると想定されるため、そのアクセスには制限をつけません。



● フィルタリング設計

- LAN 上のホスト（192.168.1.2/32）を WWW サーバとして利用することを許可
- LAN 上のホスト（192.168.1.3/32）から任意の WWW サーバへのアクセスを許可
- LAN 上のホスト（192.168.1.0/24）から WAN の先の DNS サーバへのアクセスを許可
- ICMP の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- LAN 上のホストの WWW サーバとしての利用を許可するには
  （1）192.168.1.2/32 のポート 80（www-http）へのパケットを透過させる
  （2）（1）の応答パケットを透過させる
- 任意の WWW サーバへのアクセスを許可するには
  （1）192.168.1.3/32 の任意のポートから任意の WWW サーバのポート 80（www-http）へのパケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.1.0/24 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- その他をすべて遮断するには
  （1）すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

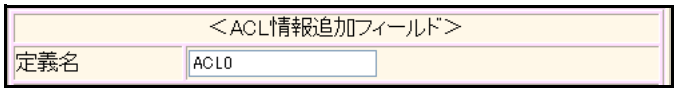
LAN 上のホストのポート 80 へのパケットを透過させる（インターネット→LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

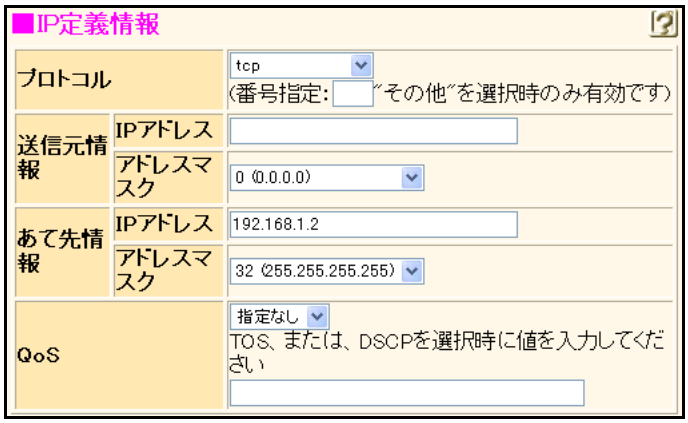
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→192.168.1.2
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



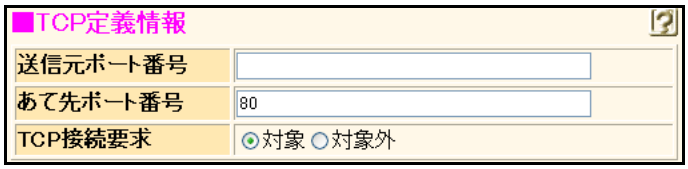
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→80（www-http のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

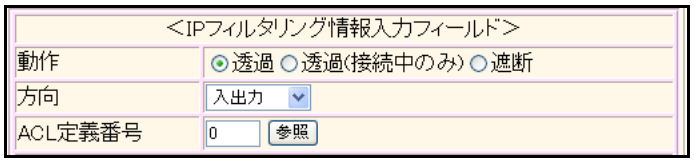
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

LAN 上のホストからの応答パケットを透過させる（LAN →インターネット）

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→ 192.168.1.2
  アドレスマスク　→ 32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→ 80（www-http のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 1

任意の WWW サーバのポート 80 へのパケットを透過させる（LAN →インターネット）

17.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→ 192.168.1.3
  アドレスマスク　→ 32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「ACL 定義情報（ACL2）」-「TCP 定義情報」

- 送信元ポート番号　→指定しない
- あて先ポート番号　→ 80（www-http のポート番号）
- TCP 接続要求　→対象

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→2

任意の WWW サーバからの応答パケットを透過させる（インターネット→ LAN）

18.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→ 192.168.1.3
  アドレスマスク　→ 32（255.255.255.255）
- QoS　→指定なし

「ACL 定義情報（ACL3）」-「TCP 定義情報」

- 送信元ポート番号　→ 80（www-http のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→3

DNS サーバのポート 53 への UDP パケットを透過させる（LAN →インターネット）

19.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL4

「ACL 定義情報（ACL4）」-「IP 定義情報」

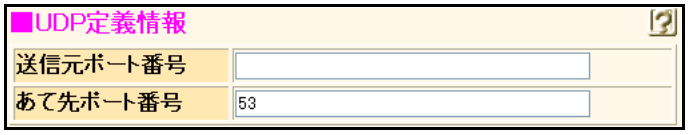
- プロトコル　→ udp
- 送信元情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

20.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

21.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53（domain のポート番号）



22.　［保存］ボタンをクリックします。

23.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

DNS サーバからの応答パケットを透過させる（インターネット→LAN）

24.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL5

「ACL 定義情報（ACL5）」-「IP 定義情報」

- プロトコル　→udp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

25.　手順 18.～20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL5）」-「UDP 定義情報」

- 送信元ポート番号　→53（domain のポート番号）
- あて先ポート番号　→指定しない

26.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→5

ICMP のパケットを透過させる

27.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL6

「ACL 定義情報（ACL6）」-「IP 定義情報」

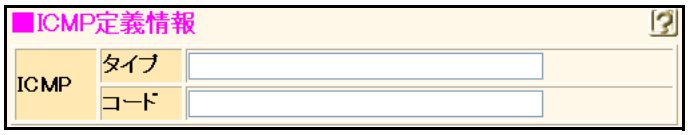
- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

28.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

29.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



30.　［保存］ボタンをクリックします。

31.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→6

残りのパケットをすべて遮断する

32.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL7

「ACL 定義情報（ACL7）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

33.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→7

34.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

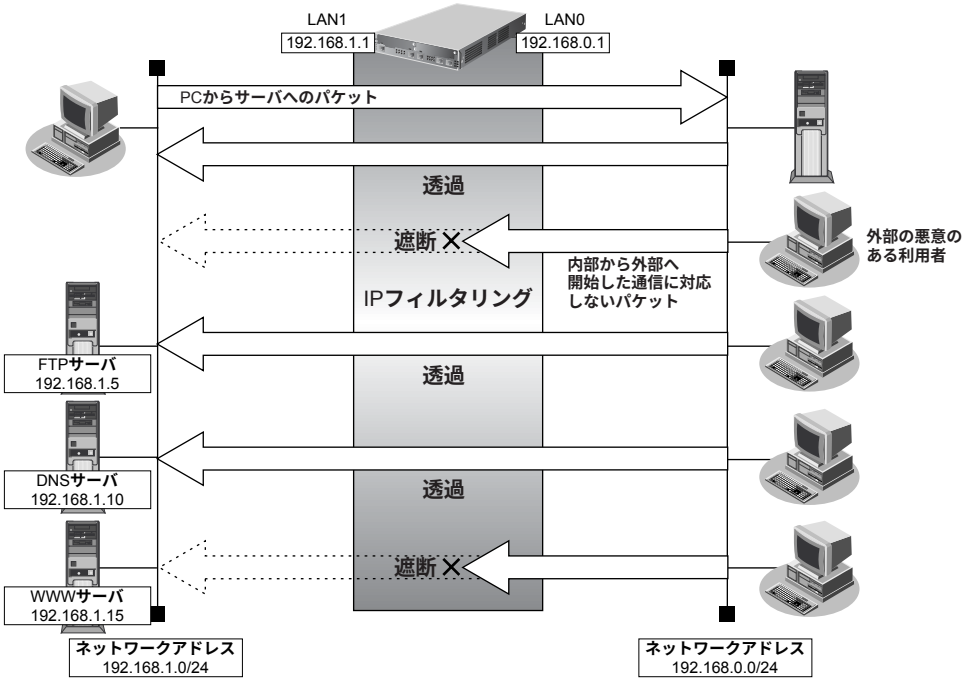
2.13.3　外部から特定サーバへのアクセスだけ許可して SPI を併用する

適用機種　全機種

LAN 定義の場合

ここでは、内部 LAN の特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止し、SPI を利用して外部へアクセスする場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスは許可します。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの問い合わせが発生します。あらかじめ接続する ftp サーバが決まっている場合は、本装置の DNS サーバ機能を利用することで、DNS サーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト（192.168.1.5/32）を FTP サーバとして利用を許可
- 内部 LAN のネットワークへの DNS サーバへのアクセスを許可
- ICMP の通信を許可
- 内部 LAN から外部へ開始するアクセスを許可し、その他はすべて遮断

こんな事に気をつけて

ICMP は、IP 通信を行う際にさまざまな制御メッセージを交換します。ICMP の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMP の通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部 LAN のホストの FTP サーバとしての利用を許可するには
  （1）192.168.1.5/32 のポート 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）192.168.0.0/24 の任意ポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMP の通信を許可するためには
  （1）ICMP パケットを透過させる
- 内部 LAN から外部へ開始するアクセスは許可し、その他をすべて遮断するには
  （1）残りのパケットに SPI を利用して IP フィルタリングを行う

上記のフィルタリングルールの設定を行う場合の設定例を示します。

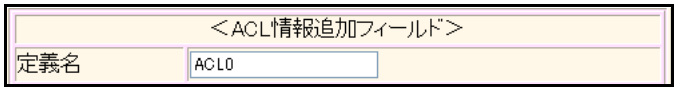
内部 LAN のホストのポート 21 への TCP パケットを透過させる（外部 LAN →内部 LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

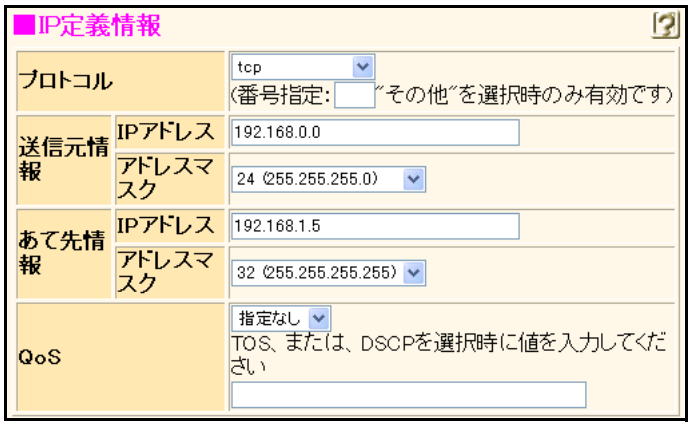
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



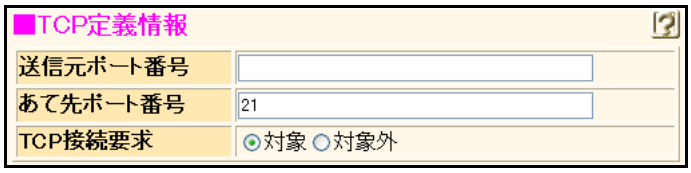
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

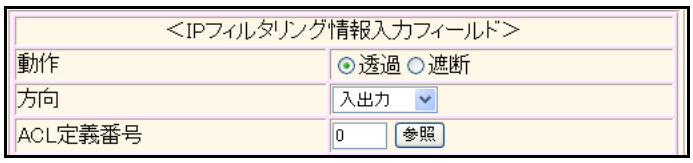
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

内部 LAN のホストからの応答パケットを透過させる（内部 LAN →外部 LAN）

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.5
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

DNS サーバのポート 53 への UDP パケットを透過させる（外部 LAN →内部 LAN）

17.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

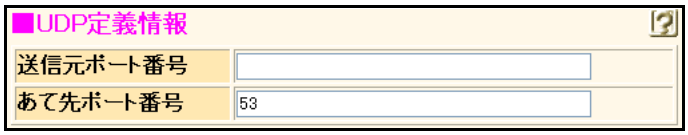
- プロトコル　→ udp
- 送信元情報
  IP アドレス　→ 192.168.0.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→ 192.168.1.10
  アドレスマスク　→ 32（255.255.255.255）
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→ 53（domain のポート番号）



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 2

DNS サーバからの応答パケットを透過させる（内部 LAN →外部 LAN）

22.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→ udp
- 送信元情報
  IP アドレス　→ 192.168.1.10
  アドレスマスク　→ 32（255.255.255.255）
- あて先情報
  IP アドレス　→ 192.168.0.0
  アドレスマスク　→ 24（255.255.255.0）
- QoS　→指定なし

23.　手順 18. ～ 20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→ 53（domain のポート番号）
- あて先ポート番号　→指定しない

24.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 3

ICMP のパケットを透過させる

25.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL4

「ACL 定義情報（ACL4）」-「IP 定義情報」

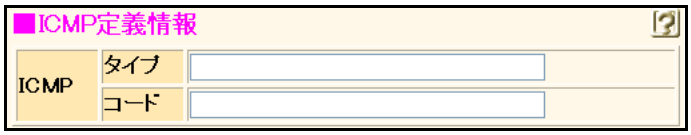
- プロトコル　→ icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

26.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

27.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



28.　［保存］ボタンをクリックします。

29.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

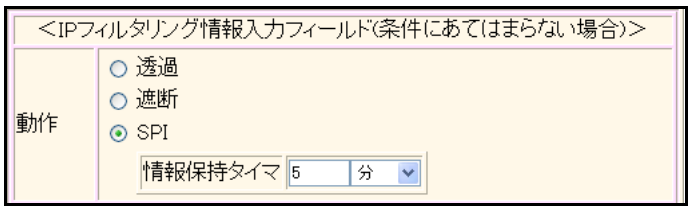
- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

残りのパケットに SPI を利用して IP フィルタリングを行う

30.　条件にあてはまらない場合の［修正］ボタンをクリックします。
「IP フィルタリング情報」（条件にあてはまらない場合）が表示されます。

31.　以下の項目を指定します。

- 動作　→SPI

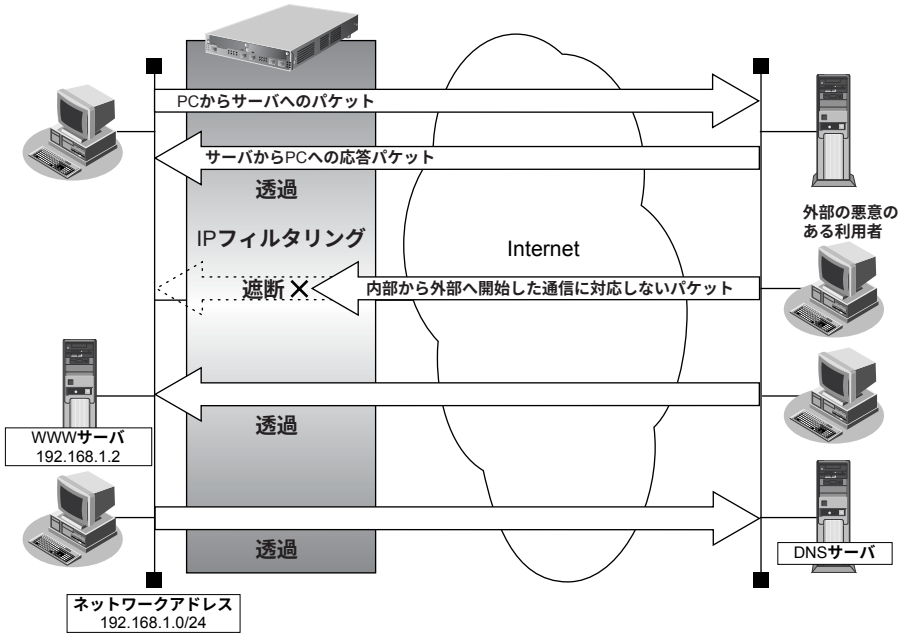


32.　［保存］ボタンをクリックします。

33.　画面左側の［設定反映］ボタンをクリックします。
設定した内容が有効になります。

リモート定義の場合

ここでは、外部からLAN上のWWWサーバに対するアクセスを許可し、ほかのLAN上のパソコンへのアクセスを禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のサーバに対してアクセスしますが、これらのアクセスに対してはSPIによるIPフィルタリングの対象とします。



● フィルタリング設計

- LAN上のホスト（192.168.1.2/32）をWWWサーバとして利用を許可
- ICMPの通信を許可
- 内部LANから外部へ開始するアクセスは許可し、その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部LANのホストのWWWサーバとしての利用を許可するには
  （1）192.168.1.2/32のポート80（www-http）へのTCPパケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMPの通信を許可するためには
  （1）ICMPパケットを透過させる
- 内部LANから外部へ開始するアクセスは許可し、その他をすべて遮断するには
  （1）残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルールの設定を行う場合の設定例を示します。

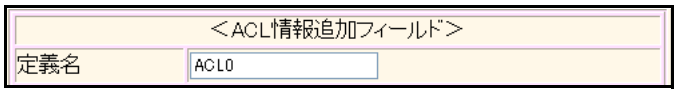
LAN 上のホストのポート 80 へのパケットを透過させる（インターネット→LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

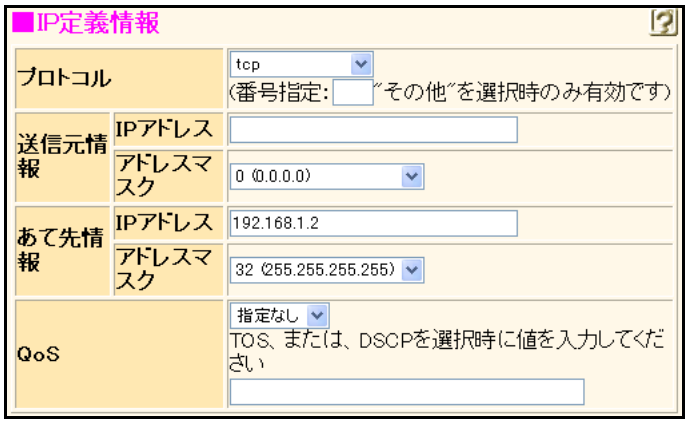
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→192.168.1.2
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



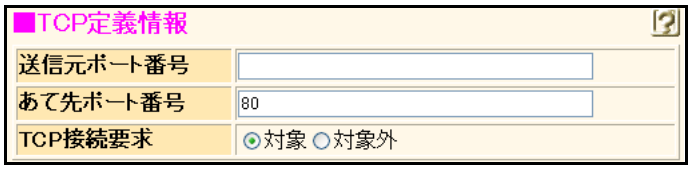
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→80（www-http のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを設定するネットワークの欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

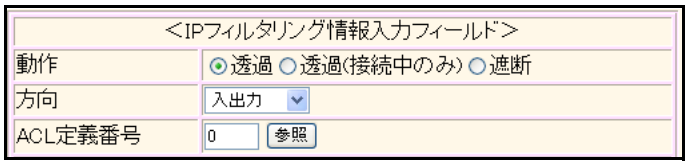
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

LAN 上のホストからの応答パケットを透過させる（LAN →インターネット）

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→ 192.168.1.2
  アドレスマスク　→ 32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→ 80（www-http のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 1

ICMP のパケットを透過させる

17.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

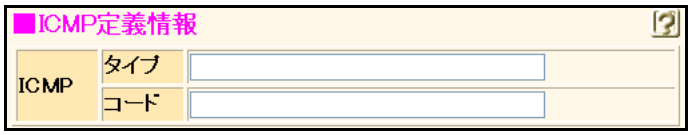
- プロトコル　→ icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

18.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

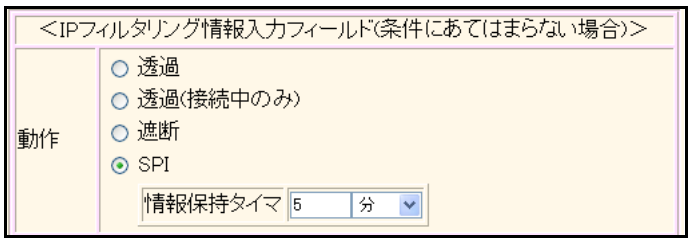
- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→2

残りのパケットに SPI を利用して IP フィルタリングを行う

22.　条件にあてはまらない場合の［修正］ボタンをクリックします。
「IP フィルタリング情報」（条件にあてはまらない場合）が表示されます。

23.　以下の項目を指定します。

- 動作　→SPI



24.　［保存］ボタンをクリックします。

25.　画面左側の［設定反映］ボタンをクリックします。
設定した内容が有効になります。

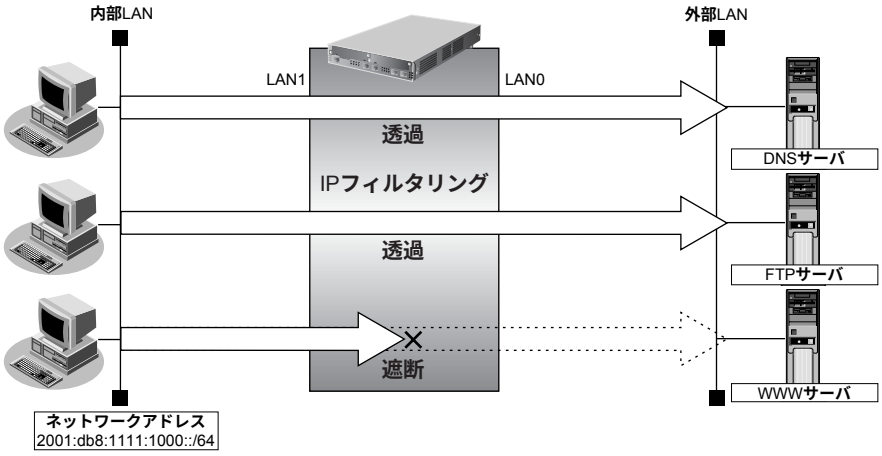
2.13.4 外部の特定サービスへのアクセスだけ許可する（IPv6 フィルタリング）

適用機種　全機種

LAN 定義の場合

ここでは、IPv6 フィルタリングを使って、内部 LAN 上のパソコンから外部 LAN 上のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの通信が発生します。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN 上のホスト（2001:db8:1111:1000::/64）から任意の FTP サーバへのアクセスを許可
- 内部 LAN 上のホスト（2001:db8:1111:1000::/64）から外部 LAN の DNS サーバへのアクセスを許可
- ICMPv6 の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6 の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6 の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには

  （1）2001:db8:1111:1000::/64 の任意のポートから、任意のアドレスのポート 21（ftp）への TCP パケットを透過させる

  （2）（1）の応答パケットを透過させる

- DNS サーバへのアクセスを許可するには

  （1）2001:db8:1111:1000::/64 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる

  （2）（1）の応答パケットを透過させる

- ICMPv6 の通信を許可するためには

  （1）ICMPv6 パケットを透過させる

- その他をすべて遮断するには

  （1）すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

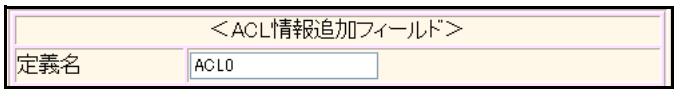
FTP サーバのポート 21（ftp）への TCP パケットを透過させる（内部 LAN →外部 LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IPv6 定義情報」をクリックします。

「IPv6 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元　IPv6 アドレス / プレフィックス長　→2001:db8:1111:1000::/64
- あて先　IPv6 アドレス / プレフィックス長　→指定しない
- QoS　→指定なし

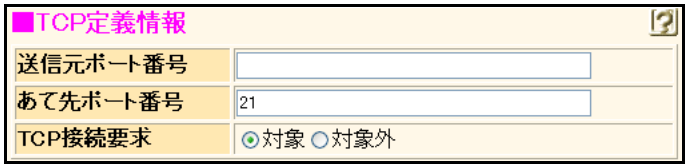
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

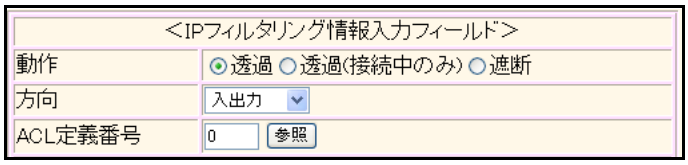
13.　IPv6 関連の設定項目の「IPv6 フィルタリング情報」をクリックします。

「IPv6 フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

FTP サーバからの応答パケットを透過させる（外部 LAN →内部 LAN）

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL1

「ACL 定義情報（ACL1）」-「IPv6 定義情報」

- プロトコル　→ tcp
- 送信元　IPv6 アドレス / プレフィックス長　→指定しない
- あて先　IPv6 アドレス / プレフィックス長　→ 2001:db8:1111:1000::/64
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→ 21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「LAN 情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 1

DNS サーバのポート 53 への UDP パケットを透過させる（内部 LAN →外部 LAN）

17.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IPv6 定義情報」

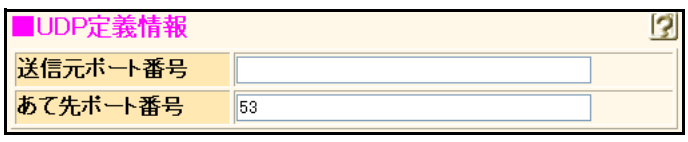
- プロトコル　→ udp
- 送信元　IPv6 アドレス / プレフィックス長　→ 2001:db8:1111:1000::/64
- あて先　IPv6 アドレス / プレフィックス長　→指定しない
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→ 53（domain のポート番号）



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 2

DNS サーバからの応答パケットを透過させる（外部 LAN →内部 LAN）

22.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL3

「ACL 定義情報（ACL3）」-「IPv6 定義情報」

- プロトコル　→ udp
- 送信元　IPv6 アドレス / プレフィックス長　→指定しない
- あて先　IPv6 アドレス / プレフィックス長　→ 2001:db8:1111:1000::/64
- QoS　→指定なし

23.　手順 18. ～ 20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→ 53（domain のポート番号）
- あて先ポート番号　→指定しない

24.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 3

ICMPv6 のパケットを透過させる

25.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL4

「ACL 定義情報（ACL4）」-「IPv6 定義情報」

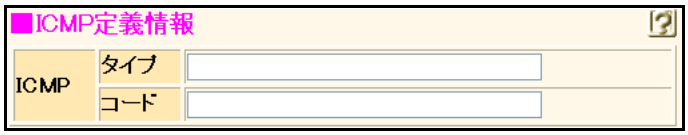
- プロトコル　→ icmpv6
- 送信元　IPv6 アドレス / プレフィックス長　→指定しない
- あて先　IPv6 アドレス / プレフィックス長　→指定しない
- QoS　→指定なし

26.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

27.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



28.　［保存］ボタンをクリックします。

29.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

残りのパケットをすべて遮断する

30.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL5

「ACL 定義情報（ACL5）」-「IPv6 定義情報」

- プロトコル　→すべて
- 送信元　IPv6 アドレス/プレフィックス長　→指定しない
- あて先　IPv6 アドレス/プレフィックス長　→指定しない
- QoS　→指定なし

31.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→5

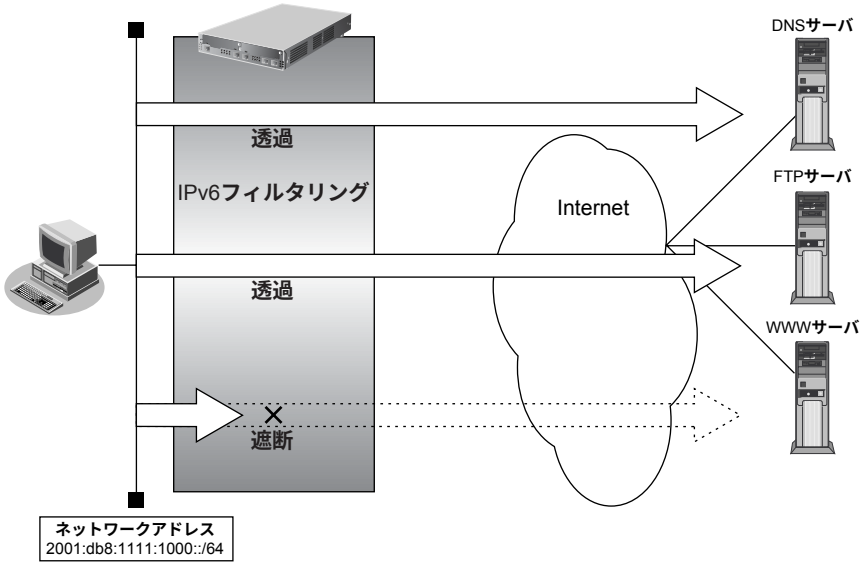
32.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、IPv6 フィルタリングを使って、LAN 上のパソコンからイントラネット上のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ（WWW サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。

補足
- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でドメイン名を指定する場合も DNS サーバへの発信が発生します。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- LAN 上のホスト（2001:db8:1111:1000::/64）から任意の FTP サーバへのアクセスを許可
- LAN 上のホスト（2001:db8:1111:1000::/64）から WAN の先の DNS サーバへのアクセスを許可
- ICMPv6 の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6 の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6 の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  （1）2001:db8:1111:1000::/64 の任意のポートから、任意の FTP サーバのポート 21（ftp）への TCP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）2001:db8:1111:1000::/64 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
  （2）（1）の応答パケットを透過させる
- ICMPv6 の通信を許可するためには
  （1）ICMPv6 パケットを透過させる

- その他をすべて遮断するには
  (1)すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

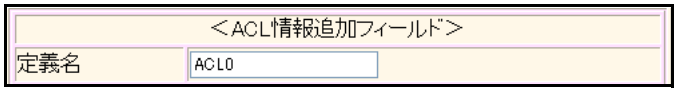
任意のFTPサーバのポート21（ftp）へのTCPパケットを透過させる（LAN→イントラネット）

1.　設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

「ACL定義情報（ACL0)」ページが表示されます。

4.　「IPv6定義情報」をクリックします。

「IPv6定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元　IPv6アドレス/プレフィックス長　→2001:db8:1111:1000::/64
- あて先　IPv6アドレス/プレフィックス長　→指定しない
- QoS　→指定なし

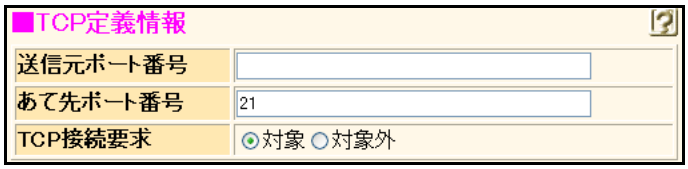
6.　［保存］ボタンをクリックします。

7.　「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

12.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

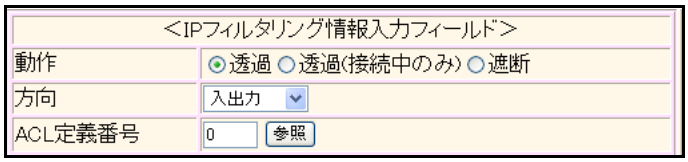
13.　IPv6 関連の設定項目の「IPv6 フィルタリング情報」をクリックします。

「IPv6 フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

FTP サーバからの応答パケットを透過させる（イントラネット→LAN）

16.　手順 1.～15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IPv6 定義情報」

- プロトコル　→tcp
- 送信元　IPv6 アドレス/プレフィックス長　→指定しない
- あて先　IPv6 アドレス/プレフィックス長　→2001:db8:1111:1000::/64
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

「相手情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

DNS サーバのポート 53 への UDP パケットを透過させる（LAN→イントラネット）

17.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL2

「ACL 定義情報（ACL2）」-「IPv6 定義情報」

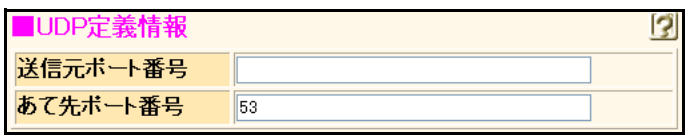
- プロトコル　→udp
- 送信元　IPv6 アドレス/プレフィックス長　→2001:db8:1111:1000::/64
- あて先　IPv6 アドレス/プレフィックス長　→指定しない
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53（domain のポート番号）



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 2

DNS サーバからの応答パケットを透過させる（イントラネット→ LAN）

22.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL3

「ACL 定義情報（ACL3）」-「IPv6 定義情報」

- プロトコル　→ udp
- 送信元　IPv6 アドレス / プレフィックス長　→指定しない
- あて先　IPv6 アドレス / プレフィックス長　→ 2001:db8:1111:1000::/64
- QoS　→指定なし

23.　手順 18. ～ 20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→ 53（domain のポート番号）
- あて先ポート番号　→指定しない

24.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→ 3

ICMPv6 のパケットを透過させる

25.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL4

「ACL 定義情報（ACL4）」-「IPv6 定義情報」

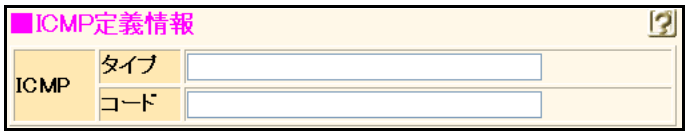
- プロトコル　→ icmpv6
- 送信元　IPv6 アドレス / プレフィックス長　→指定しない
- あて先　IPv6 アドレス / プレフィックス長　→指定しない
- QoS　→指定なし

26.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

27.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



28.　［保存］ボタンをクリックします。

29.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→4

残りのパケットをすべて遮断する

30.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL5

「ACL 定義情報（ACL5）」-「IPv6 定義情報」

- プロトコル　→すべて
- 送信元　IPv6 アドレス/プレフィックス長　→指定しない
- あて先　IPv6 アドレス/プレフィックス長　→指定しない
- QoS　→指定なし

31.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IPv6 関連」
「IPv6 フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→5

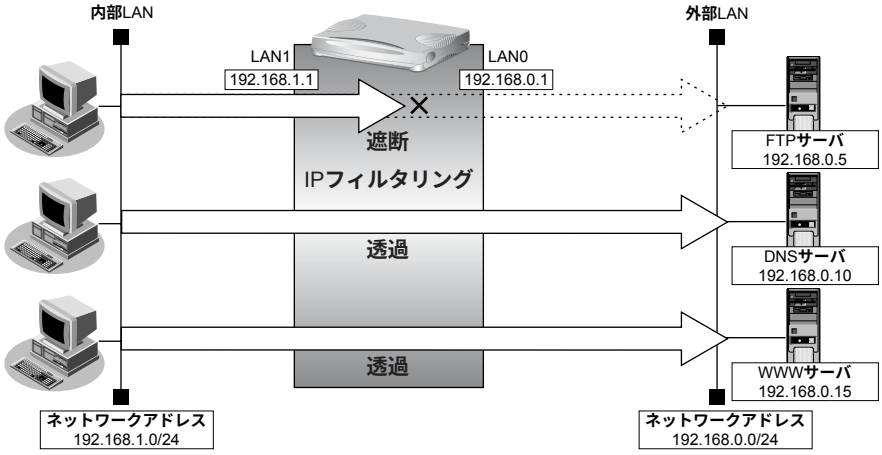
32.　画面左側の［設定反映］ボタンをクリックします。
設定した内容が有効になります。

2.13.5　外部の特定サーバへのアクセスだけを禁止する

適用機種　全機種

LAN 定義の場合

ここでは、外部 LAN の FTP サーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設定

- 内部 LAN のホスト（192.168.1.0/24）から外部 LAN の FTP サーバ（192.168.0.5）へのアクセスを禁止

● フィルタリングルール

- FTP サーバへのアクセスを禁止するには

  （1）192.168.1.0/24 から 192.168.0.5 のポート 21（ftp）への TCP パケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

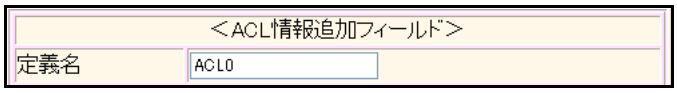
FTP サーバ（192.168.0.5）への TCP パケットを遮断する（内部 LAN →外部 LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

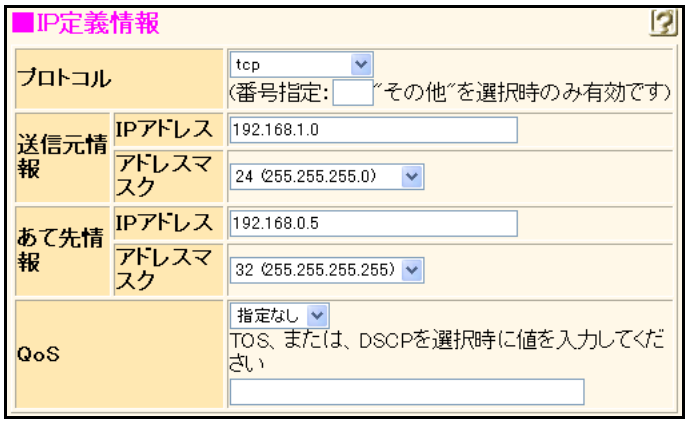
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.0.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



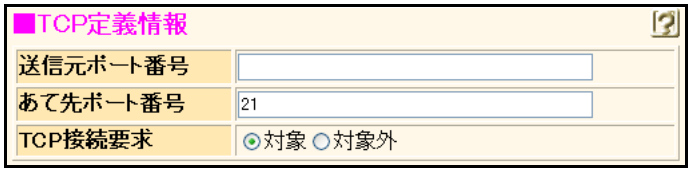
6.　[保存] ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）
- TCP 接続要求　→対象



9.　[保存] ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。

<IPフィルタリング情報入力フィールド>	
動作	○透過 ◉遮断
方向	入出力
ACL定義番号	0 参照

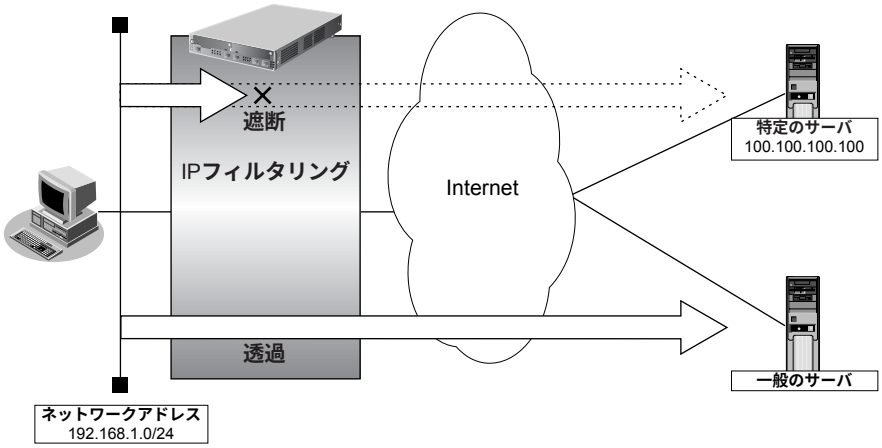
15.　［追加］ボタンをクリックします。

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、インターネット上の特定のサーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設計

- LAN 上のホスト（192.168.1.0/24）からアドレス 100.100.100.100 へのアクセスを禁止

● フィルタリングルール

- 特定アドレスへのアクセスを禁止するには
  （1）192.168.1.0/24 から 100.100.100.100 の任意のポートへのすべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

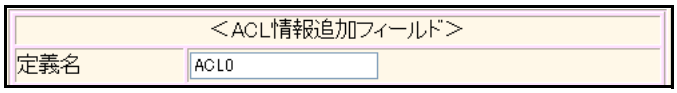
アドレス（100.100.100.100）へのすべてのパケットを遮断する（LAN→インターネット）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

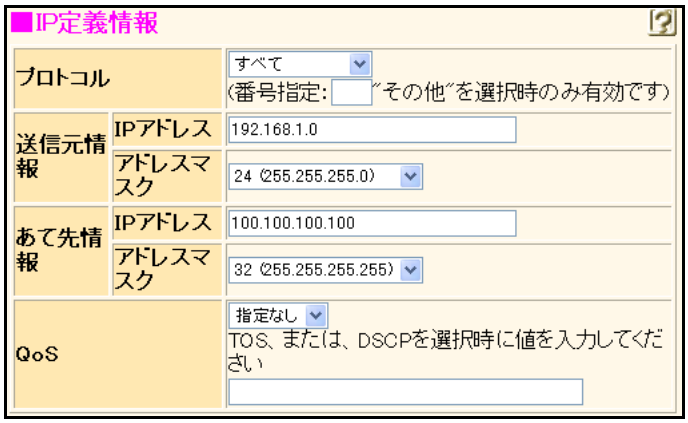
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→100.100.100.100
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



6.　［保存］ボタンをクリックします。

7.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

8.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

9.　フィルタリングを設定するネットワークの欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

10.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

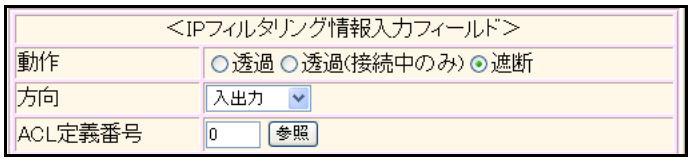
11.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

12.　以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



13.　［追加］ボタンをクリックします。

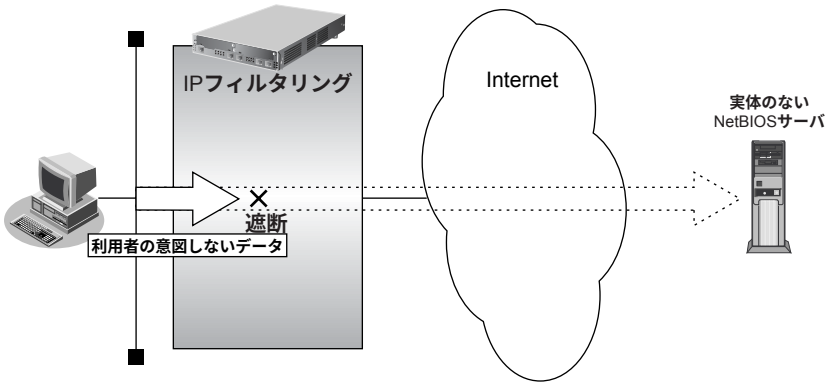
14.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.13.6　利用者が意図しない発信を防ぐ

適用機種　全機種

LAN 上のパソコンは、利用者の意志とは無関係に、実体のない NetBIOS サーバにアクセスすることがあります。その際、回線が接続され、利用者が意識しないところで通信料金がかかってしまいます。
ここでは、上記のような、回線に対するむだな発信を抑止する場合のフィルタリング設定方法を説明します。



● フィルタリング設計

- ポート 137 ～ 139（NetBIOS サービス）へのアクセスを禁止

● フィルタリングルール

- ポート 137 ～ 139 へのアクセスを禁止するには
  (1) ポート 137 ～ 139 へのすべてのパケットを遮断する
  (2) ポート 137 ～ 139 からのすべてのパケットを遮断する

補足　Windows®（TCP 上の NetBIOS）環境のネットワークでは、セキュリティ上の問題とむだな課金を抑えるために、ポート番号 137 ～ 139 の外向きの転送経路をふさいでおく必要があります。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

ポート 137 ～ 139 への TCP パケットを遮断する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0

＜ACL情報追加ﾌｨｰﾙﾄﾞ＞	
定義名	ACL0

3.　［追加］ボタンをクリックします。

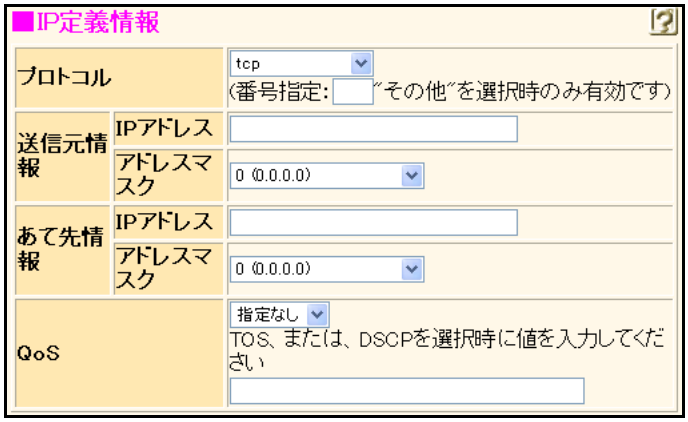
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし



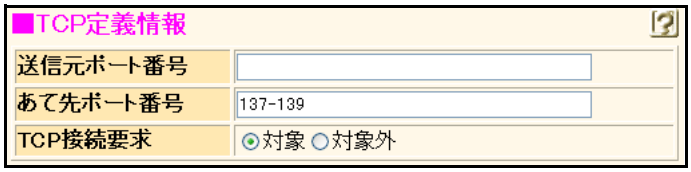
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→137-139
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

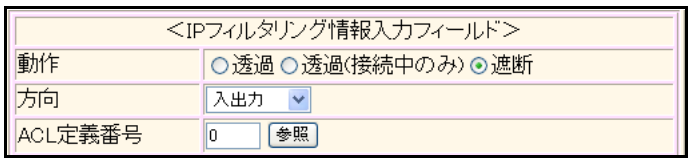
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→0

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

ポート 137 ～ 139 からの TCP パケットを遮断する

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→137-139
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→1

ポート 137 ～ 139 への UDP パケットを遮断する

17.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

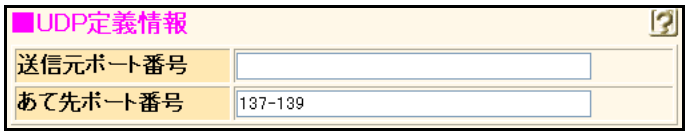
- プロトコル　→ udp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

18.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

19.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→ 137-139



20.　［保存］ボタンをクリックします。

21.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→ 2

ポート 137 ～ 139 からの UDP パケットを遮断する

22.　手順 1. ～ 6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→ udp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

23.　手順 18. ～ 20. を参考に、以下の項目を指定します。

「ACL 定義情報（ACL3）」-「UDP 定義情報」

- 送信元ポート番号　→ 137-139
- あて先ポート番号　→指定しない

24.　手順 10. ～ 15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→ 3

25.　画面左側の［設定反映］ボタンをクリックします。

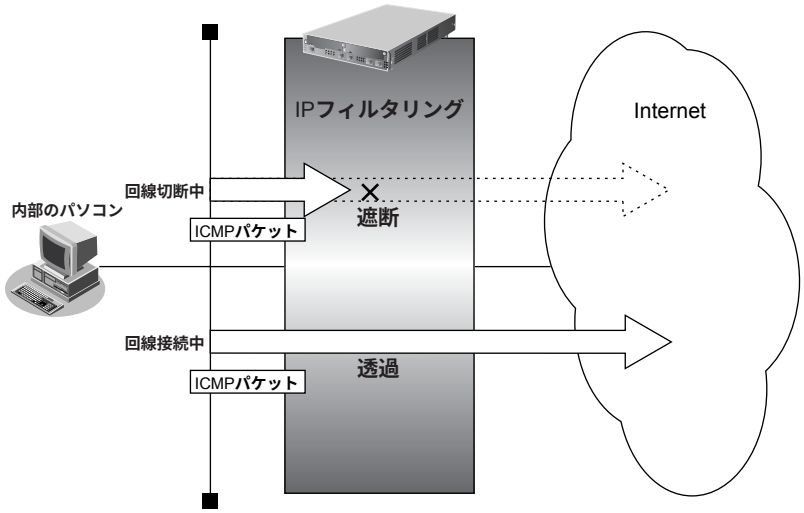
設定した内容が有効になります。

2.13.7　回線が接続しているときだけ許可する

適用機種　全機種

一部のパソコンでは、ネットワークの設定によって、ログイン時に自動的に PING を発行して PPPoE または ISDN 回線を接続してしまうものがあります。回線接続を必要とする ICMP パケットを遮断することによって、意図しない PING によるむだな発信を抑止することができます。ここでは、回線が接続されているときにだけ ICMP パケットを透過させる場合の設定方法を説明します。

補足　IP アドレスを直接指定せず、DNS による名前アドレス変換を利用した場合、発信を抑止することはできません。



● フィルタリング設計

- すでに回線が接続している場合にだけ PING を許可

● フィルタリングルール

- すでに回線が接続している場合にだけ PING を許可するには
  (1)回線接続中だけ ICMP パケットを透過させる

上記のフィルタリングルールの設定を行う場合の設定例を示します。

回線が接続しているときだけ ICMP パケットを透過させる

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0

＜ACL情報追加フィールド＞	
定義名	ACL0

3.　［追加］ボタンをクリックします。

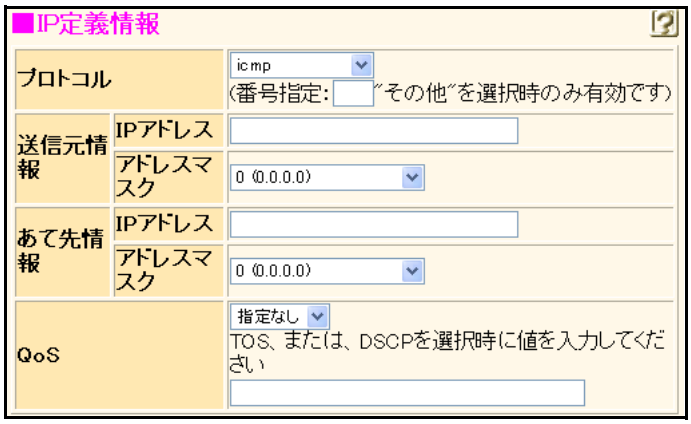
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし



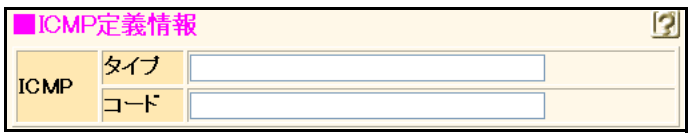
6.　［保存］ボタンをクリックします。

7.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- ICMP
  タイプ　→指定しない
  コード　→指定しない



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

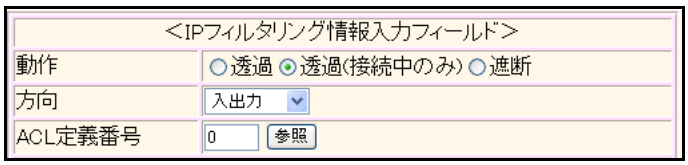
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過（接続中のみ）
- 方向　→入出力
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

16.　画面左側の［設定反映］ボタンをクリックします。

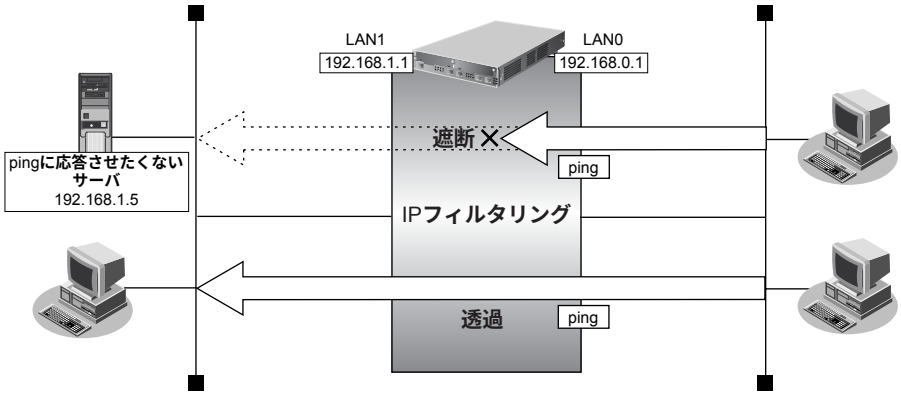
設定した内容が有効になります。

2.13.8　外部から特定サーバへの ping だけを禁止する

適用機種　全機種

LAN 定義の場合

ここでは、内部 LAN の特定のサーバに対する ping（ICMP ECHO）を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。



● フィルタリング設定

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止
- その他はすべて通過

● フィルタリングルール

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには
  (1) 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  (1) すべてのパケットを透過させる

上記のフィルタリングルールの設定を行う場合の設定例を示します。

アドレス（192.168.1.5/32）への ICMP TYPE 8 の ICMP パケットを遮断する（外部 LAN →内部 LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0

＜ACL情報追加フィールド＞	
定義名	ACL0

3.　［追加］ボタンをクリックします。

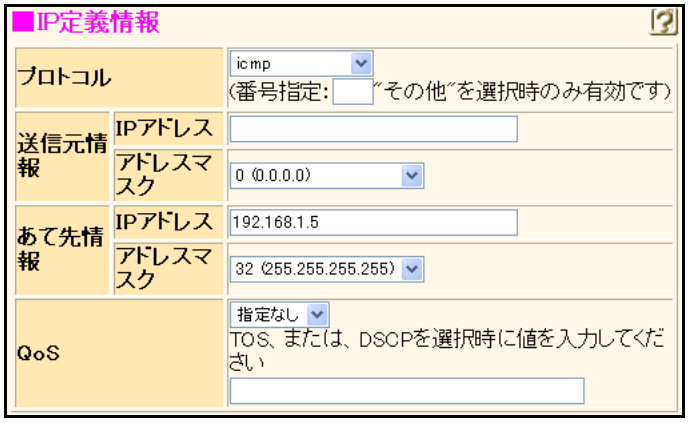
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→192.168.1.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



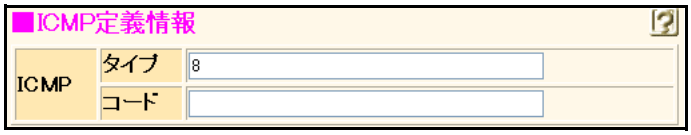
6.　［保存］ボタンをクリックします。

7.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- ICMP
  タイプ　→8
  コード　→指定しない



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

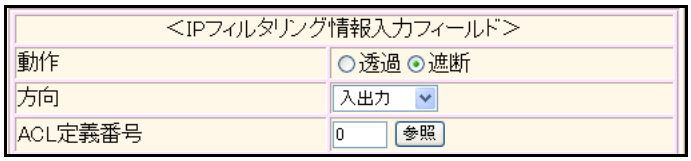
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

残りのパケットをすべて透過させる

16.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

17.　手順 10.～15. を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」
「IP フィルタリング情報」

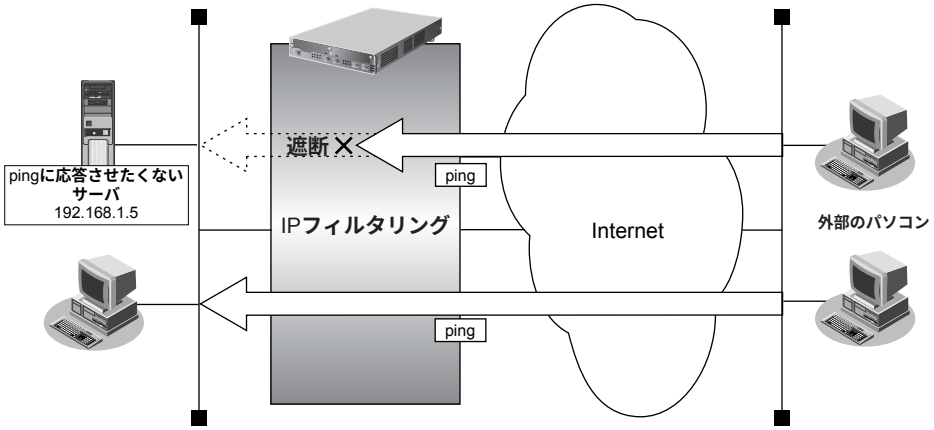
- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

18.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、LAN 上の特定のサーバに対する ping（ICMP ECHO）を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。



● フィルタリング設計

- LAN 上のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止
- その他はすべて通過

● フィルタリングルール

- LAN 上のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには
  (1)192.168.1.5/32 の ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  (1)すべてのパケットを透過させる

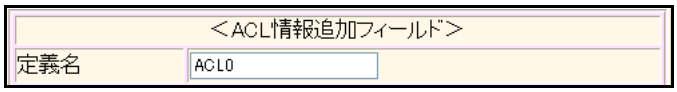
アドレス（192.168.1.5/32）への ICMP TYPE 8 の ICMP パケットを遮断する（インターネット→LAN）

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

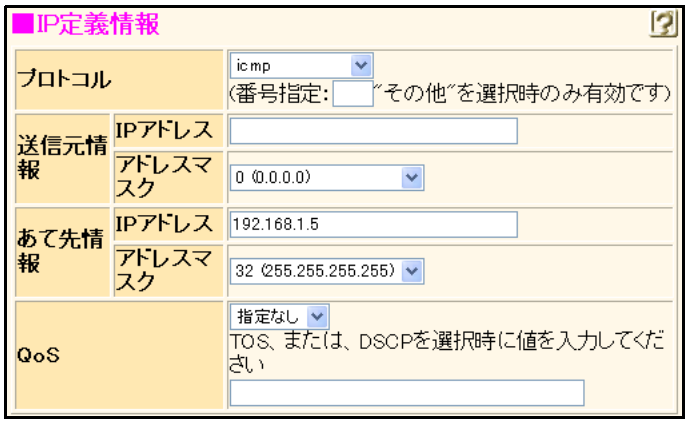
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→icmp
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IPアドレス　→192.168.1.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



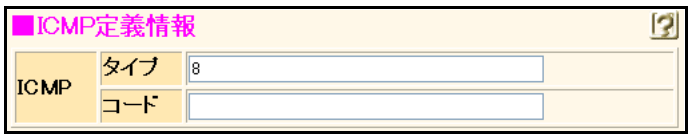
6.　［保存］ボタンをクリックします。

7.　「ICMP 定義情報」をクリックします。

「ICMP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- ICMP
  タイプ　→8
  コード　→指定しない



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　フィルタリングを行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

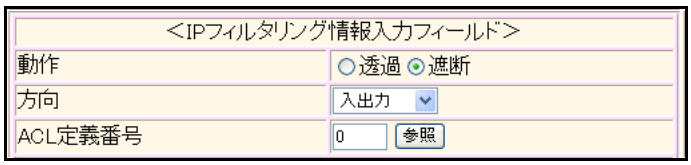
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→0

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

残りのパケットをすべて透過させる

16.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

17.　手順 10.～15. を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」
「IP フィルタリング情報」

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

18.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14 IPsec機能を使う

適用機種　全機種

VPN（Virtual Private Network）は、インターネットを利用して遠隔地のLANをつなぐと、遠隔地のLAN上のアプリケーションやデータが、あたかも同じオフィスのLANのように利用できる機能です。また、認証情報や暗号情報を設定することにより、インターネット上を流れるデータのセキュリティを確保することができます。

本装置では、VPNを実現するためにIPsecというプロトコルを使用して、以下の接続形態が利用できます。

- 固定IPアドレスでのVPN（手動鍵交換）
  固定IPアドレスで送信元、送信先のIPアドレス範囲を指定してVPN通信を行います。
  認証情報、暗号情報の鍵は手動で設定します。
- 固定IPアドレスでのVPN（自動鍵交換）
  固定IPアドレスで送信元、送信先のIPアドレス範囲を指定してVPN通信を行います。
  認証情報、暗号情報の鍵は自動で交換します。
- 可変IPアドレスでのVPN（自動鍵交換）
  自側のIPアドレスが動的に割り当てられる環境で、経路情報（送信先のIPアドレス）に従ってVPN通信を行います。認証情報、暗号情報の鍵は自動で交換します。
- 1つのIKEセッションに複数のIPsecトンネル構成でのVPN（自動鍵交換）
  複数のIPsec対象範囲が存在し、IPsec対象範囲をすべて（any）とすることができない環境で、IKEセッション（トンネル）を1つとしてVPN通信を行います。
  認証情報、暗号情報の鍵は自動で交換します。
- IPsec機能と他機能との併用
  IPsec機能と他機能を併用する場合のいくつかの設定例を説明します。
- 固定IPアドレスでバックアップ用に使用するVPN（自動鍵交換）（Si-R370、570）
  固定IPアドレスでのVPNに加えて、異常を検出した場合に、自動でバックアップを行い、処理を引き継ぐことができます。
- テンプレート着信機能（AAA認証）を使用した固定IPアドレスでのVPN（自動鍵交換）
  IKE不特定着信のIKE認証鍵取得にAAA認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（AAA認証）を使用した可変IPアドレスでのVPN（自動鍵交換）
  相手側のIPアドレスが動的に割り当てられる環境で、IKE不特定着信のIKE認証鍵取得にAAA認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（RADIUS認証）を使用した固定IPアドレスでのVPN（自動鍵交換）
  IKE不特定着信のIKE認証鍵取得にRADIUS認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（RADIUS認証）を使用した可変IPアドレスでのVPN（自動鍵交換）
  相手側のIPアドレスが動的に割り当てられる環境で、IKE不特定着信のIKE認証鍵取得にRADIUS認証機能を使用してVPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能（動的VPN）を使用した固定IPアドレスでのVPN（自動鍵交換）
  動的VPN接続契機パケットを監視して動的にVPN通信を行います。
  自装置のIPsecトンネルIPアドレス、IPsec対象範囲、IPsec経路情報および接続先監視アドレスは、動的VPN情報交換機能で自動に交換します。
- NATトラバーサルを使用した可変IPアドレスでのVPN（自動鍵交換）
  自側のIPアドレスが動的に割り当てられる環境で、IKE区間にあるNATを介したIPsec通信を可能にするために、NATトラバーサル機能を使用してVPN通信を行います。

- テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN（自動鍵交換）
  相手側の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用し、また IKE 区間にある NAT を介した IPsec 通信を可能にするために、NAT トラバーサル機能を使用して VPN 通信を行います。認証情報および暗号情報の鍵は自動で交換します。

☛ 参照 Si-R シリーズ　機能説明書「2.14 IPsec 機能」（P.67）

こんな事に気をつけて

- IPsec は IPv4、IPv6 で使用できます。
- NAT 変換には、IPsec の前の変換と IPsec のあとの変換があります。IPsec 前に変換する場合は IPsec 用の「ネットワーク情報」で設定します。IPsec 後に変換する場合は、回線接続用の「ネットワーク情報」または「LAN 情報」で設定します。
- インターネット VPN では、VPN 装置どうしがインターネットを介して通信する必要があるため、VPN 装置にはインターネット上で使用可能なグローバルな IP アドレスを使用してください（NAT を使用している場合は、マルチ NAT（静的 NAT）で IP アドレスを割り当てます）。
- VPN 相互接続するアドレスがプライベートアドレスの場合、重複しないように設計してください。
- IPsec では、IPv4、IPv6 パケット通信だけをサポートしています。IPv4、IPv6 パケット以外は VPN の対象とならないため中継されません。
- 暗号パケットが多重に暗号化される形態で使用しないでください。暗号パケットが二重に暗号化され、復号処理が正常に行えないため通信異常となります。
- IPsec と NAT 機能を併用する場合は、マルチ NAT を使用してください。
- IPsec とマルチ NAT を併用する場合は、静的 NAT の設定が必要となることがあります。
- 経路情報を設定する場合、IPsec/IKE ネゴシエーションパケットが VPN のトンネルに入らないように設定してください。
- 複数の接続先情報定義に同じ IPsec トンネルアドレスを定義しないでください。
- IKE セッションに対して複数の IPsec トンネル構成を使用する場合は、同じ IPsec 対象範囲がないように設定してください。
- IPsec 対象範囲が複数ネットワーク存在し、IPsec 対象範囲にすべて（any）を設定できない環境の場合だけ、“IKE セッションに対して複数の IPsec トンネル構成”を使用することをお勧めします。ネットワークごとに IPsec SA を作成する構成や IPsec 対象範囲にすべて（any）を定義できない装置と接続する場合は、“IKE セッションに対して複数の IPsec トンネル構成”を使用してください。
- テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、以下の点に注意してください。
  - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
  - 初回 IKE ネゴシエーションは Responder でのみ動作します。
  - 自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
  - テンプレート定義の接続先監視アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
  - AAA 設定または RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- RADIUS および AAA の登録情報を変更して IPsec が接続できない場合は、手動切断を行い、再度テンプレート着信機能で接続してください。
- 動的 VPN 情報交換機能を使用する場合、システム全体で一意となるユーザ ID を設定してください。
- テンプレート着信機能（動的 VPN）を使用した IPsec では、以下の点に注意してください。
  - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
  - IKE モードは Main Mode で動作します。
  - 動的 VPN で作成されたインタフェースにスタティック経路情報が設定されるように動的 VPN 接続契機パケットを監視するインタフェースの経路情報を設定してください。
  - V31 以降のファームウェアと V30 ファームウェアで IPsec を行う場合は、V31 以降のファームウェアの動的 VPN クライアント情報設定で交換情報のエンコードタイプを“off”に指定する必要があります。また、動的 VPN サーバを V31 以降のファームウェアにする必要があります。
- 動的 VPN で接続する自側ネットワークを異なるアドレスファミリで設定した場合、拡張 IPsec 対象範囲が 1 定義分追加されます。
- 拡張 IPsec 対象範囲機能未対応版数（V30）の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異なるアドレスファミリを設定しないでください。

- 拡張 IPsec 対象範囲機能を使用して IPsec パケットを通過させた場合、IPsec 対象範囲をチェックする相手装置の場合は IPsec が遮断されます。この場合は、拡張 IPsec 対象範囲機能を使用することはできません。
- 拡張 IPsec 対象範囲を使用して双方向通信を行う場合、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合、片側通信のみ暗号化し、折り返しの通信は暗号化されない場合があります。
- NAT トラバーサル機能を利用するときは、以下の点に注意してください。
  - IKE を行う双方の装置で設定してください。片方の装置での利用や NAT トラバーサルのバージョンが異なると、NAT トラバーサルはできません。
    NAT トラバーサルは、以下の RFC、Internet Draft のバージョンをサポートします。
    “Negotiation of NAT-Traversal in the IKE”
    RFC3947
    draft-ietf-ipsec-nat-t-ike-03
    draft-ietf-ipsec-nat-t-ike-02
    “UDP Encapsulation of IPsec ESP Packets”
    RFC3948
  - IPsec トンネルに存在する NAT 装置の変換テーブルが解放されると、NAT トラバーサルは動作できなくなります。変換テーブルを保持するために、接続先監視機能と併用することを推奨します。
  - IPsec 通信プロトコルは暗号（ESP）を使用するように設定してください。IPsec 通信プロトコルが認証（AH）の場合は動作しません。
  - 自側トンネルエンドポイントアドレス、および相手側エンドポイントアドレスに IPv4 アドレスを設定してください。IPv6 アドレスを設定した場合は動作しません。
  - IKE を使用する設定をしてください。動的 VPN（dvpn）および手動鍵（manual）を設定した場合は動作しません。
  - 初回 IKE ネゴシエーションが、initiator 装置側で NAT される環境でのみ動作します。
  - テンプレート着信機能（AAA 認証および RADIUS 認証）を使用した IPsec では、IKE モードを Aggressive Mode で設定してください。Main Mode で設定した場合は動作しません。
- 接続優先制御の設定は、IKE ネゴシエーションのすれ違いが頻発する場合にそれぞれ異なる優先方法を設定してください。同じ優先制御を行うと、競合した場合に IKE ネゴシエーションが失敗します。この機能を利用する場合は、以下の設定を奨励します。
  - 一方の装置で Initiator を優先し、一方の装置で Responder を優先する。

ヒント

◆ VPN とは？

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPN を使ってつないだルータ間の通信経路のことをトンネルと言います。

◆ 自動鍵交換とは？

IPsec の通信に使用される暗号化・認証用の鍵素材を、自動で作成・更新します。鍵素材を定期的に自動更新させることにより、セキュリティの強度を高めることができます。自動鍵交換を使用しない場合は、手動で鍵を設定する必要があります。

◆ NAT と IPsec を併用する

IPsec で使用するグローバルアドレスで NAT を使用している場合（IPsec 後の NAT 変換後）は、IPsec パケットが NAT を通過できるように、「LAN 情報」または「ネットワーク情報」で、以下の静的 NAT を設定します。

利用形態	設定内容
固定 IP アドレスでの VPN（手動鍵交換）	ESP パケットの受信を設定します。 • プライベート IP 情報 IP アドレス　自側エンドポイントに設定したアドレス ポート番号　すべて • グローバル IP 情報 IP アドレス　相手 VPN 装置に設定された本装置側の IP アドレス ポート番号　すべて • プロトコル　ESP

利用形態	設定内容
固定IPアドレスでのVPN（自動鍵交換）	IKEパケットの受信を設定します。 • プライベートIP情報 IPアドレス　自側エンドポイントに設定したアドレス ポート番号　500 • グローバルIP情報 IPアドレス　相手VPN装置に設定された本装置側のIPアドレス ポート番号　500 • プロトコル　UDP ESPパケットの受信を設定します。 • プライベートIP情報 IPアドレス　自側エンドポイントに設定したアドレス ポート番号　すべて • グローバルIP情報 IPアドレス　相手VPN装置に設定された本装置側のIPアドレス ポート番号　すべて • プロトコル　ESP 例） 本装置のWAN（ネットワーク情報）の自側IPアドレスが202.168.1.66（固定）であり、202.168.1.66（自側）と202.168.2.66（相手側）の間でIPsec/IKE通信を行う場合、IPsec/IKE通信の自側エンドポイントに202.168.1.66を設定します。このとき静的NATのプライベートアドレスおよびグローバルアドレスには、202.16.1.66を設定します。
可変IPアドレスでのVPN（Initiator）	IKEパケットの受信を設定します。 • プライベートIP情報 IPアドレス　本装置のLAN側IPアドレス ポート番号　500 • グローバルIP情報 IPアドレス　指定しない ポート番号　500 • プロトコル　UDP
可変IPアドレスでのVPN（Initiator）	ESPパケットの受信を設定します。 • プライベートIP情報 IPアドレス　本装置のLAN側IPアドレス ポート番号　すべて • グローバルIP情報 IPアドレス　指定しない ポート番号　すべて • プロトコル　ESP

2.14.1　IPv4 over IPv4 で固定 IP アドレスでの VPN（手動鍵交換）

適用機種　全機種

IPsec 機能を使って手動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IP アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス　：202.168.2.65

● 設定条件

[支社]

- IPsec 区間　：202.168.1.66 - 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IPsec プロトコル　：esp
- IPsec 送信用 SPI　：100（16 進数）
- IPsec 送信用 SA 暗号アルゴリズムと暗号秘密鍵　：des-cbc、0123456789（16 進数）
- IPsec 送信用 SA 認証アルゴリズムと認証秘密鍵　：hmac-md5、123456789a（16 進数）
- IPsec 受信用 SPI　：101（16 進数）
- IPsec 受信用 SA 暗号アルゴリズムと暗号秘密鍵　：des-cbc、23456789ab（16 進数）
- IPsec 受信用 SA 認証アルゴリズムと認証秘密鍵　：hmac-md5、3456789abc（16 進数）

[本社]

- IPsec 区間　：202.168.2.66 - 202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IPsec プロトコル　：esp
- IPsec 送信用 SPI　：101（16 進数）
- IPsec 送信用 SA 暗号アルゴリズムと暗号秘密鍵　：des-cbc、23456789ab（16 進数）
- IPsec 送信用 SA 認証アルゴリズムと認証秘密鍵　：hmac-md5、3456789abc（16 進数）
- IPsec 受信用 SPI　：100（16 進数）
- IPsec 受信用 SA 暗号アルゴリズムと暗号秘密鍵　：des-cbc、0123456789（16 進数）
- IPsec 受信用 SA 認証アルゴリズムと認証秘密鍵　：hmac-md5、123456789a（16 進数）

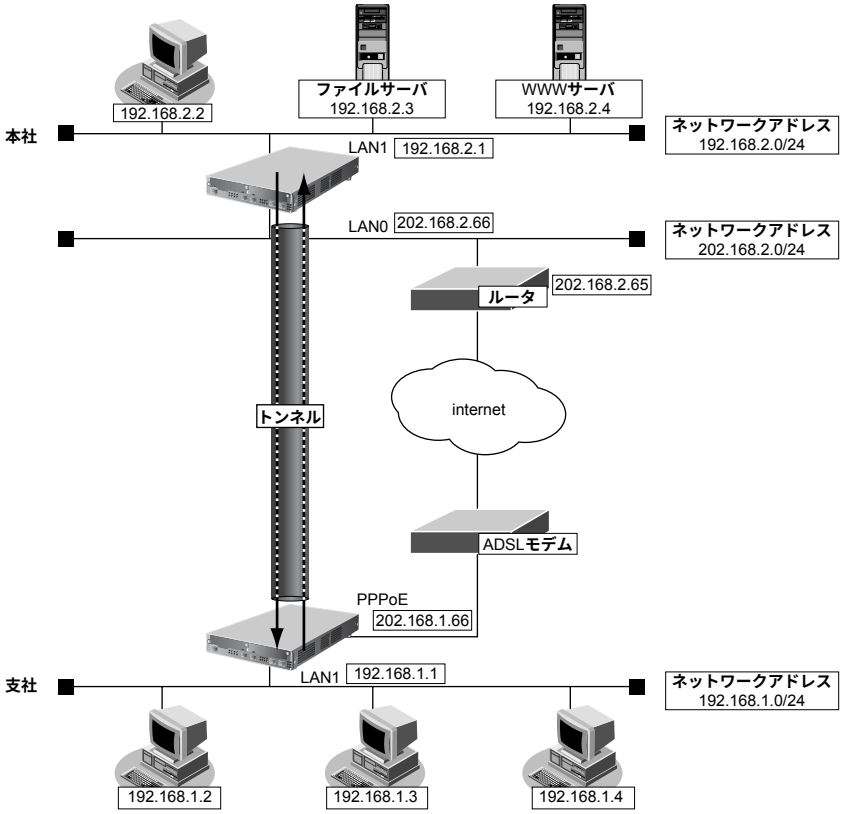
ヒント

◆ SPI とは？

トンネルの識別子です。SPI はトンネルの往路と復路でそれぞれ異なる値を設定します。トンネルをつなぐ本装置を設定するときには、同じ方向のトンネルには同じ SPI を設定します。

こんな事に気をつけて

- 暗号アルゴリズムに des-cbc を選択する場合、鍵に単純な文字列（同じ文字だけ、文字列の繰り返しなど）を指定すると、暗号強度が低下するおそれがあるので指定しないでください。暗号アルゴリズムに 3des-cbc を選択する場合は、鍵を 16 桁ごとに 3 つに分割した、それぞれ 3 つの暗号強度が低下する鍵（弱い鍵）にならないように指定してください。
  des-cbc で弱い鍵として具体的に知られているものには以下のようなものがあります。本装置は、これらの文字列で始まる鍵で通信できないようにしています。
  0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、FEFE FEFE FEFE FEFE、
  01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、FE01 FE01 FE01 FE01、
  E01F E01F F10E F10E、E001 E001 F101 F101、1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、
  E0FE E0FE F1FE F1FE、FE1F FE1F FE0E FE0E、1F01 1F01 0E01 0E01、FEE0 FEE0 FEF1 FEF1
- 暗号アルゴリズムに 3des を選択する場合は、以下のように鍵を 16 桁ごとに 3 つに分割し、鍵 1 ≠鍵 2 ≠鍵 3 となるように鍵を設定してください。
  鍵:　1122334455667788　　9900aabbccddeeff　　1122334455667788
  　　鍵 1（16 桁）　　鍵 2（16 桁）　　鍵 3（16 桁）
  鍵 1 ＝鍵 3 のように鍵を設定すると、16 バイトの鍵で暗号化するのと同じ結果になります。また、鍵 1 ＝鍵 2、鍵 2 ＝鍵 3 のように鍵を設定すると、それぞれ鍵 3、鍵 1 の des-cbc 暗号と同じ結果になります（鍵 1 ＝鍵 2 ＝鍵 3 の場合も同様です）。



上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

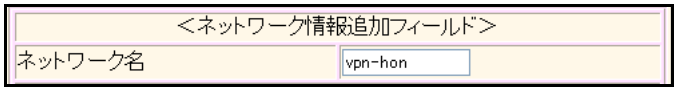
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

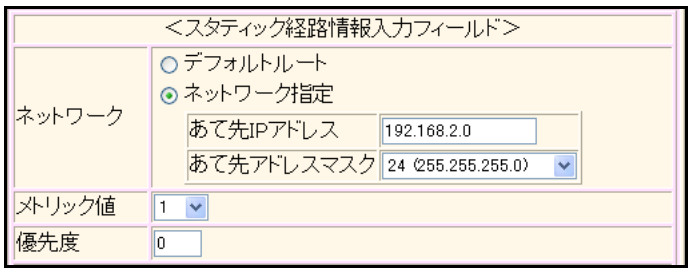
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



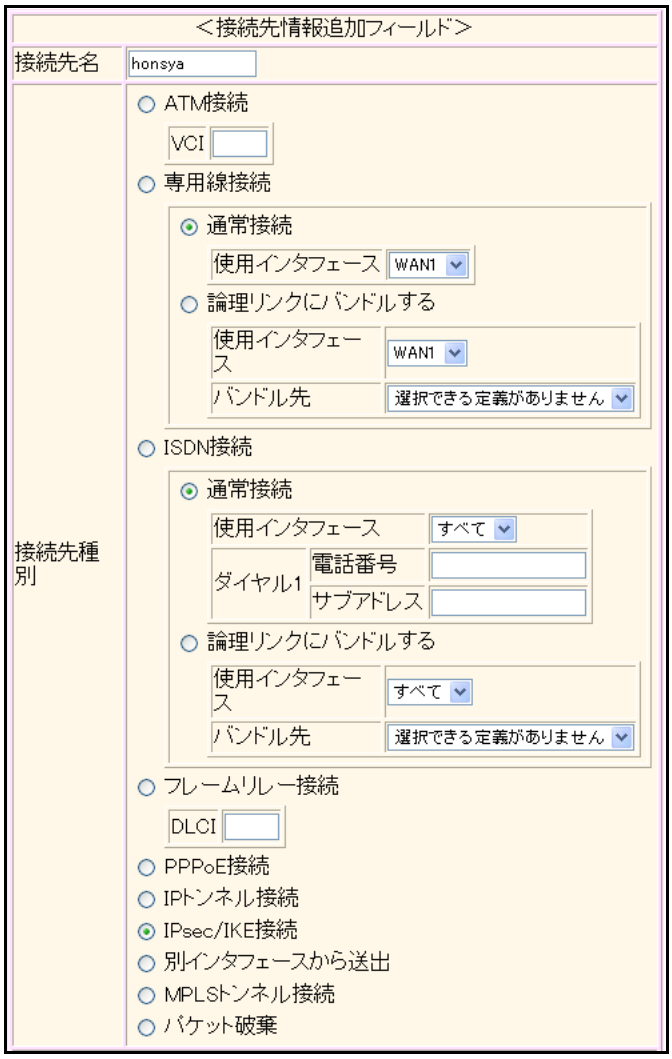
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



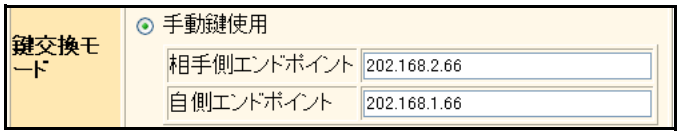
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→手動鍵使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66



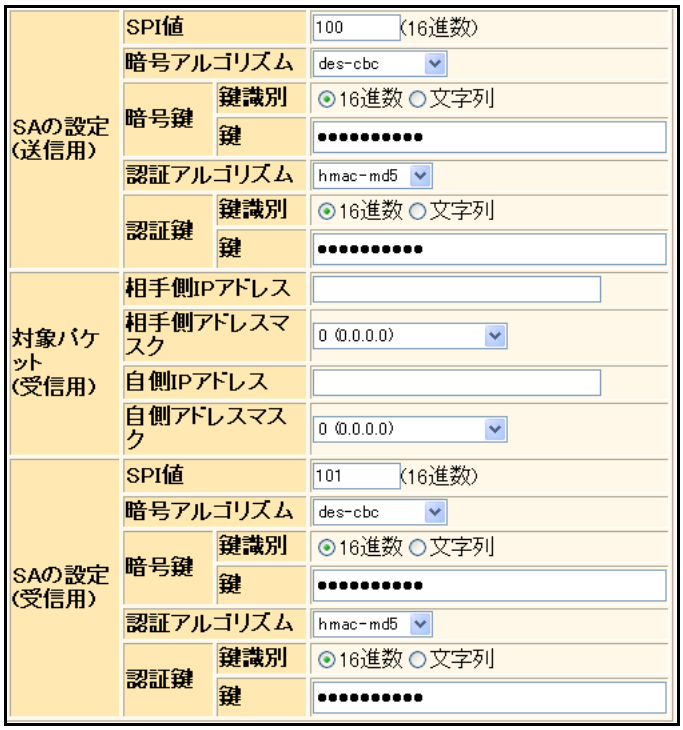
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定（送信用）
  SPI 値　→ 100
  暗号アルゴリズム　→ des-cbc
  暗号鍵
  鍵識別　→ 16 進数
  鍵　→ 0123456789
  認証アルゴリズム　→ hmac-md5
  認証鍵
  鍵識別　→ 16 進数
  鍵　→ 123456789a
- SA の設定（受信用）
  SPI 値　→ 101
  暗号アルゴリズム　→ des-cbc
  暗号鍵
  鍵識別　→ 16 進数
  鍵　→ 23456789ab
  認証アルゴリズム　→ hmac-md5
  認証鍵
  鍵識別　→ 16 進数
  鍵　→ 3456789abc



16.　［保存］ボタンをクリックします。

17.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi

4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi)」ページが表示されます。

5.　「IP 関連」をクリックします。

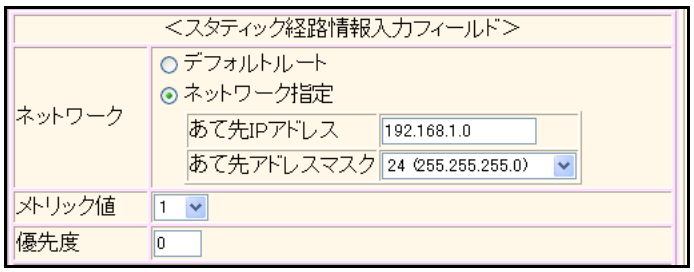
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



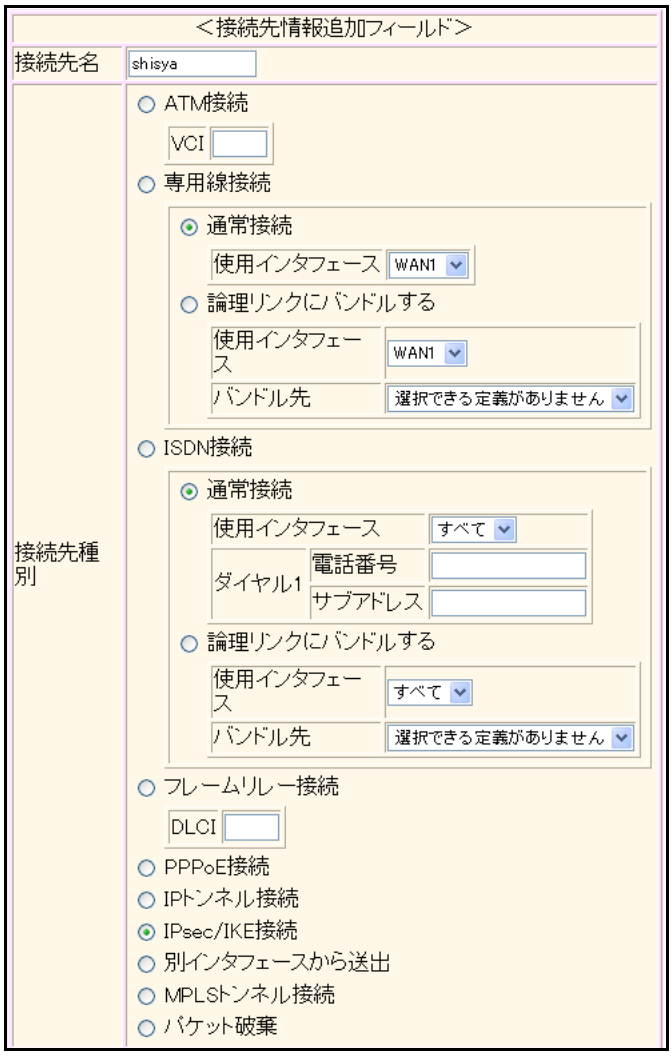
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



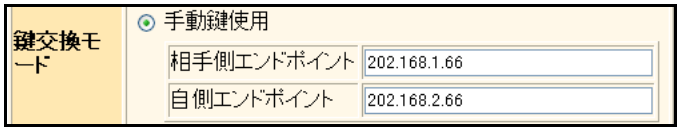
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→手動鍵使用
  相手側エンドポイント　→202.168.1.66
  自側エンドポイント　→202.168.2.66



13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

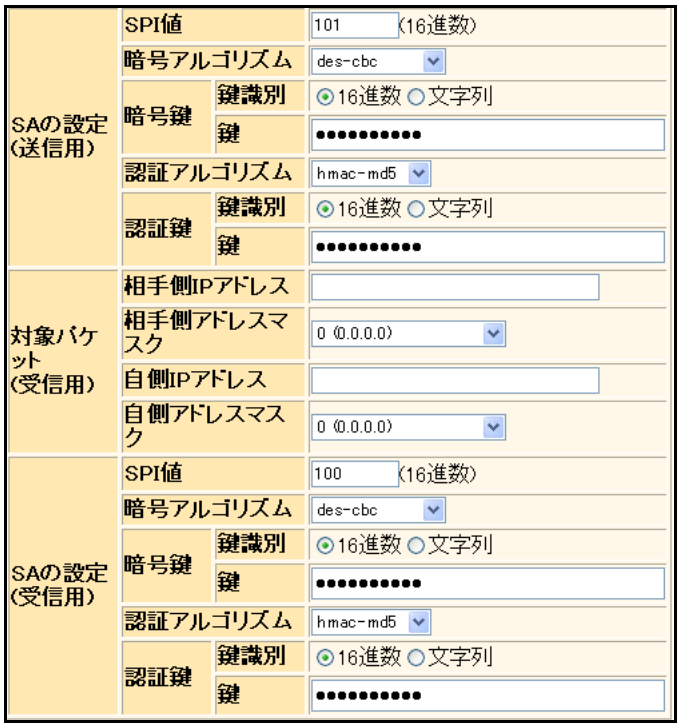
15.　以下の項目を指定します。

- SA の設定（送信用）

  SPI 値　→ 101
  暗号アルゴリズム　→ des-cbc
  暗号鍵
  鍵識別　→ 16 進数
  鍵　→ 23456789ab
  認証アルゴリズム　→ hmac-md5
  認証鍵
  鍵識別　→ 16 進数
  鍵　→ 3456789abc

- SA の設定（受信用）

  SPI 値　→ 100
  暗号アルゴリズム　→ des-cbc
  暗号鍵
  鍵識別　→ 16 進数
  鍵　→ 0123456789
  認証アルゴリズム　→ hmac-md5
  認証鍵
  鍵識別　→ 16 進数
  鍵　→ 123456789a



16.　［保存］ボタンをクリックします。

17.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.2　IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

IPsec 機能を使って IPv4 ローカルネットワーク間を IPv6 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

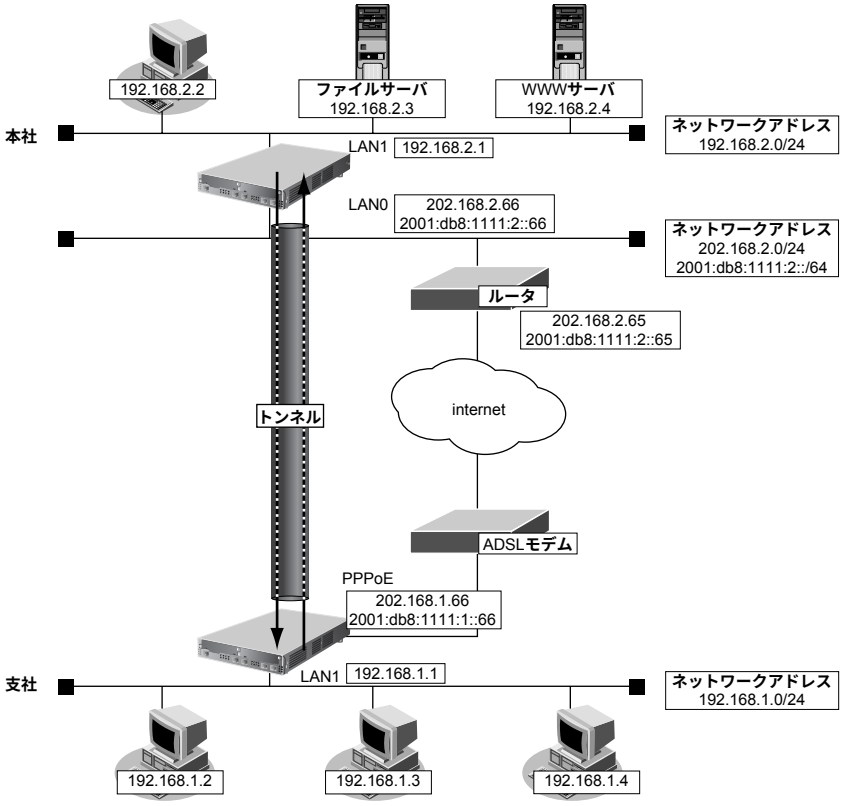
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-2001:db8:1111:1::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

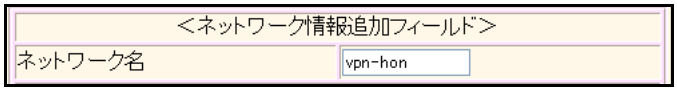
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

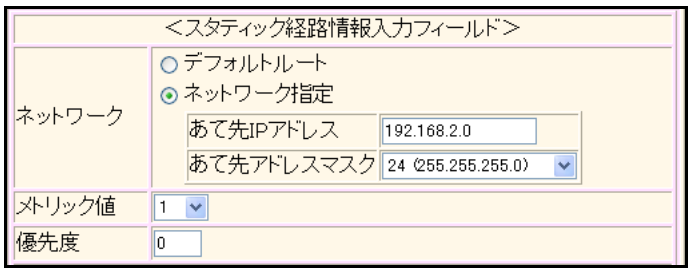
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



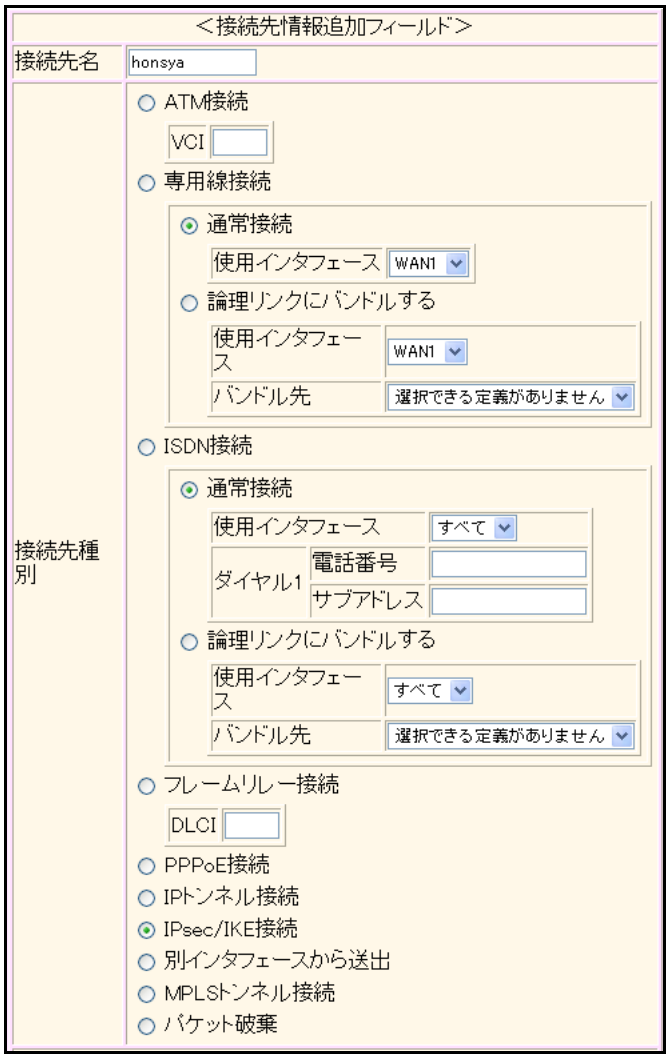
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→2001:db8:1111:2::66
  自側エンドポイント　→2001:db8:1111:1::66

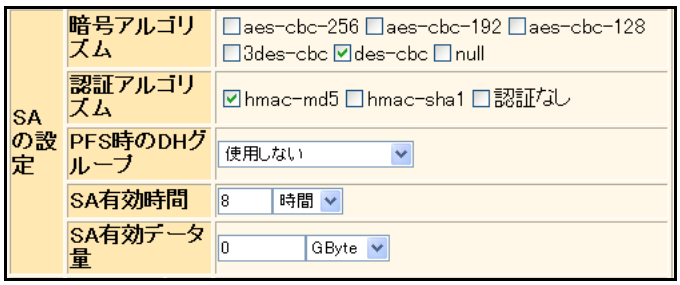
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



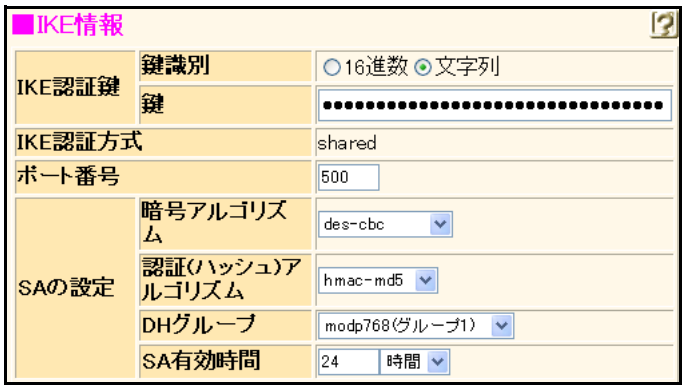
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi

4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi)」ページが表示されます。

5.　「IP 関連」をクリックします。

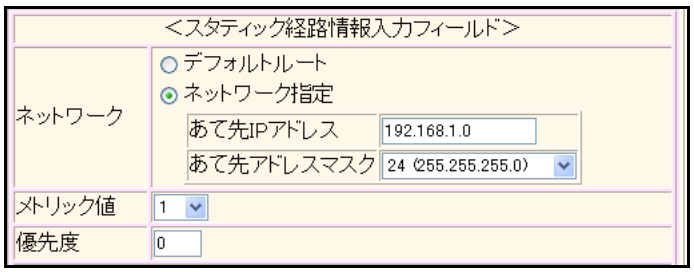
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



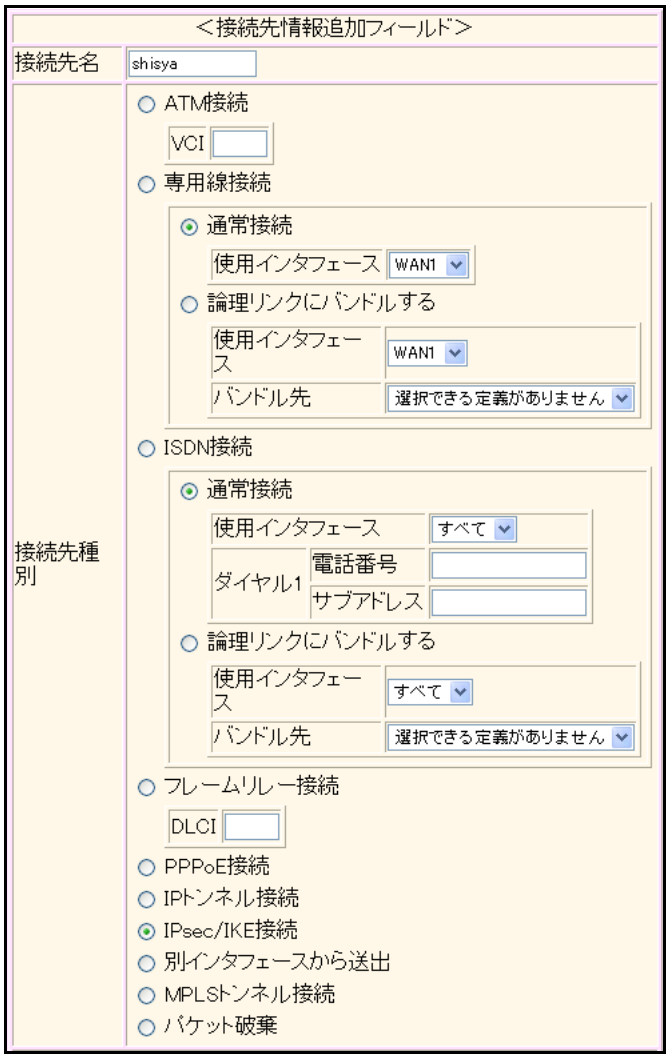
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→2001:db8:1111:1::66
  自側エンドポイント　→2001:db8:1111:2::66

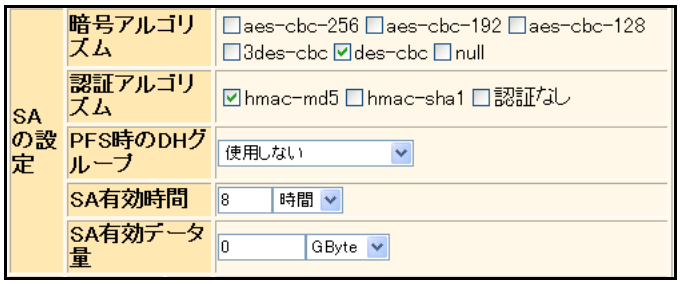
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



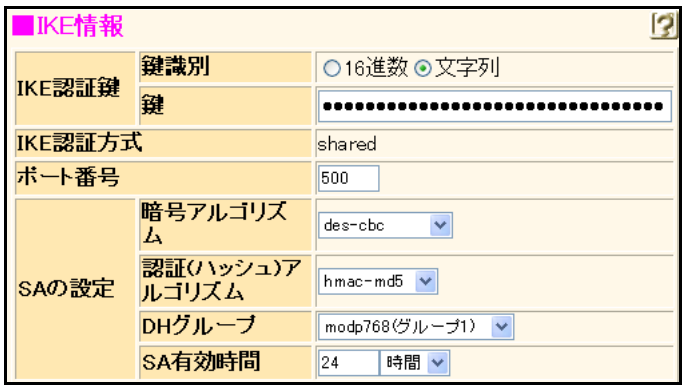
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.3　IPv4 over IPv6 で可変 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

IPv4 ローカルネットワーク間を IPv6 インターネットで結んで IPsec を行います。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

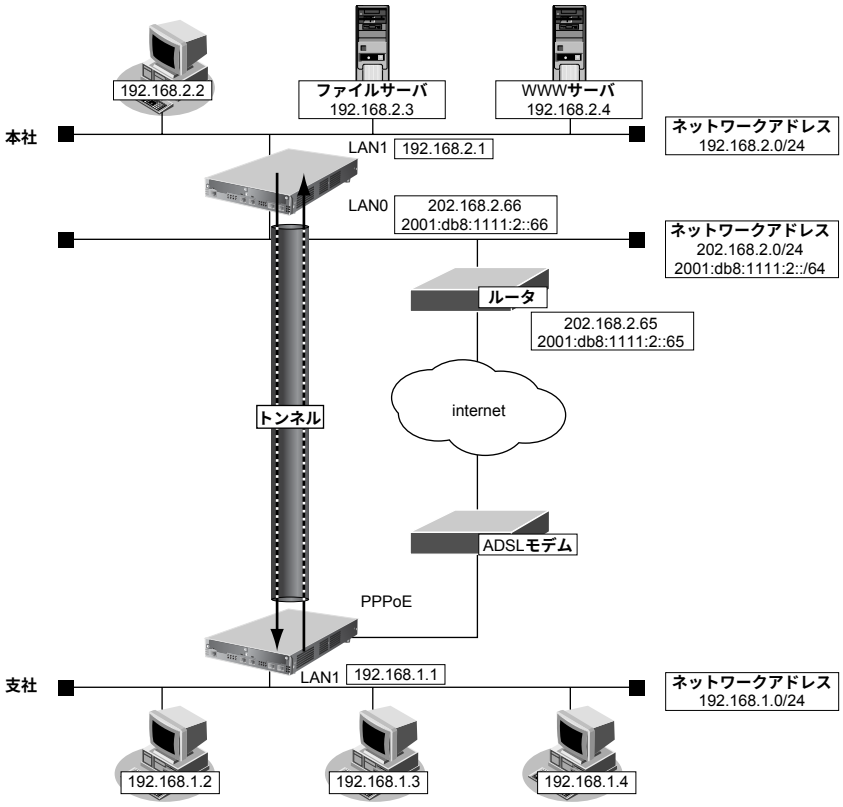
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス
  ：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）
- ESP のプライベートアドレス　：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社（Initiator）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon

4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

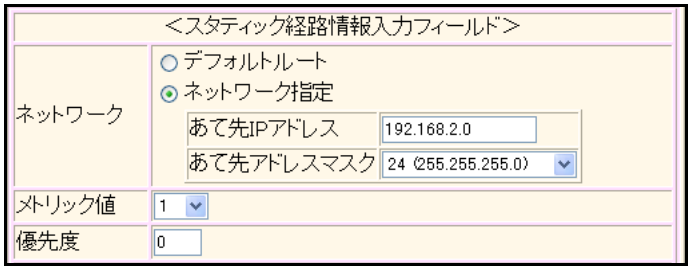
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



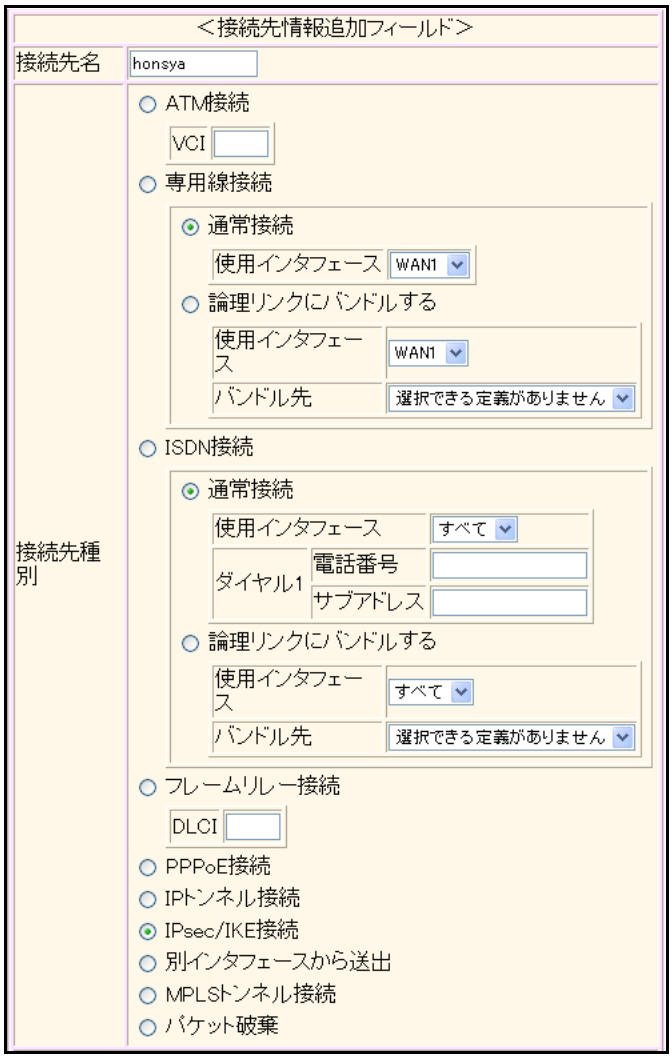
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



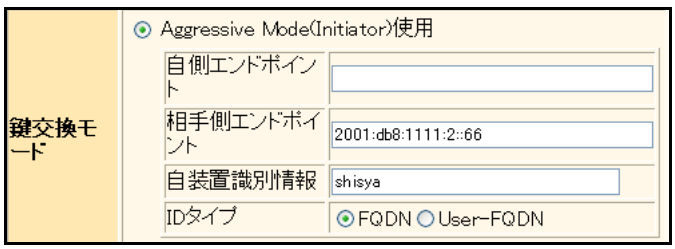
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggresive Mode（Initiator）使用
  相手側エンドポイント　→2001:db8:1111:2::66
  自装置識別情報　→shisya



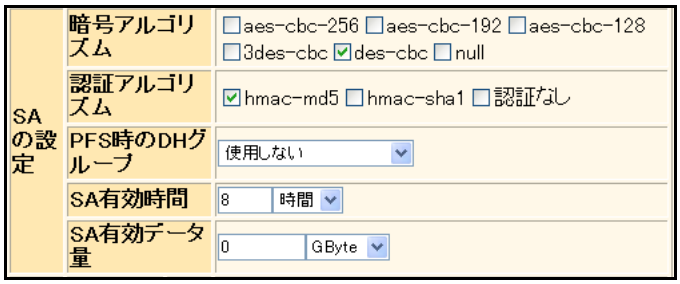
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



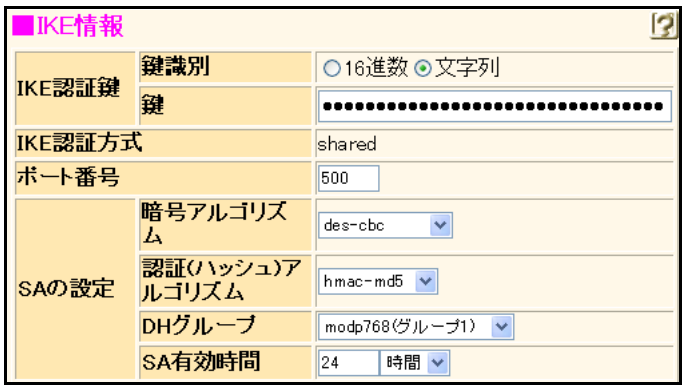
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社（Responder）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

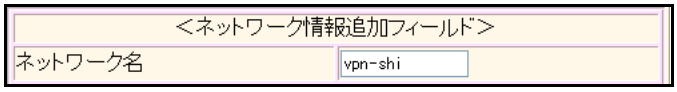
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi）」ページが表示されます。

5.　「IP 関連」をクリックします。

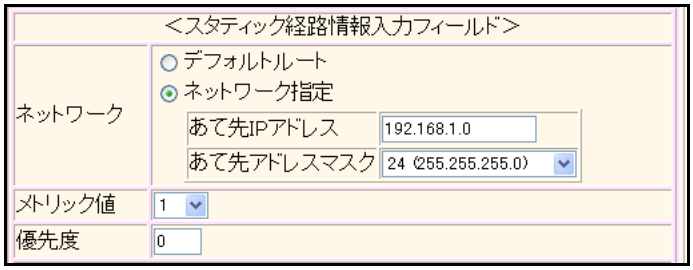
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



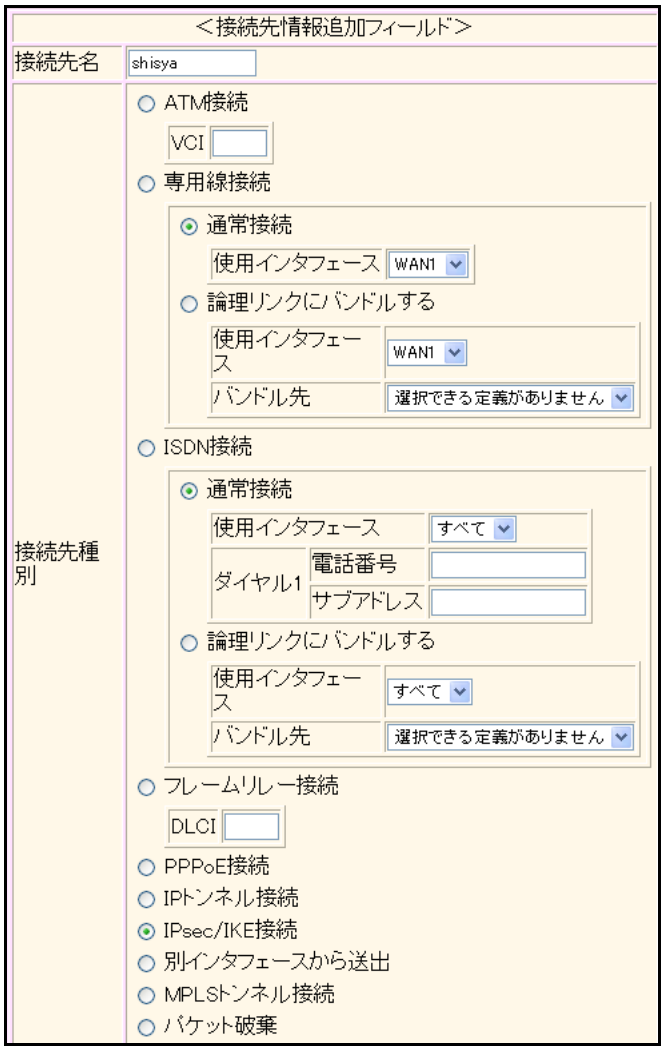
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



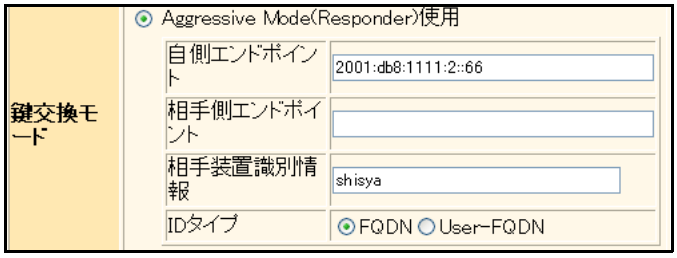
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggresive Mode（Responder）使用
  自側エンドポイント　→2001:db8:1111:2::66
  相手装置識別情報　→shisya



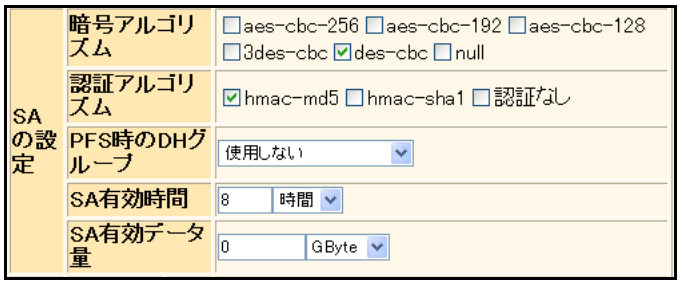
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



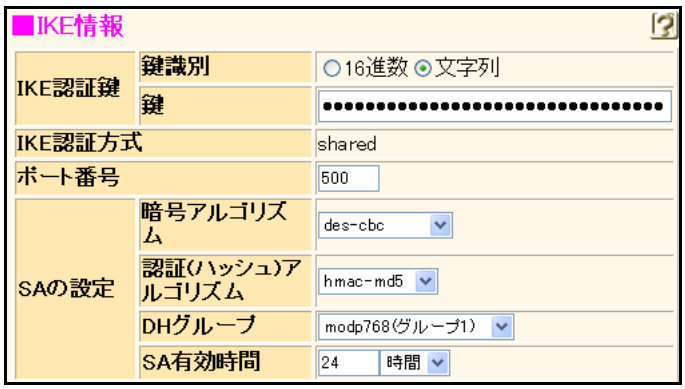
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.4　IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

IPsec 機能を使って IPv6 ローカルネットワーク間を IPv4 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

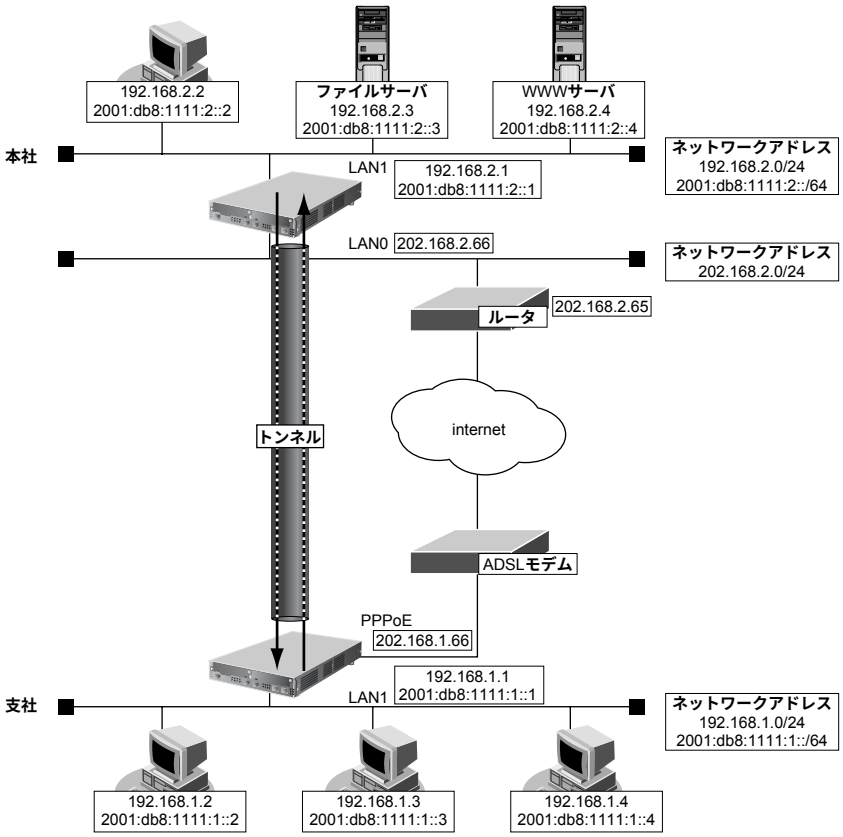
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:1::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス　：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66-202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66-202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon

4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

6.　以下の項目を指定します。

- IPv6　→使用する

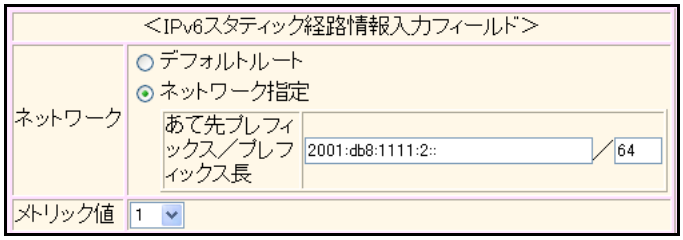
7.　［保存］ボタンをクリックします。

8.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:2::/64
- メトリック値　→1



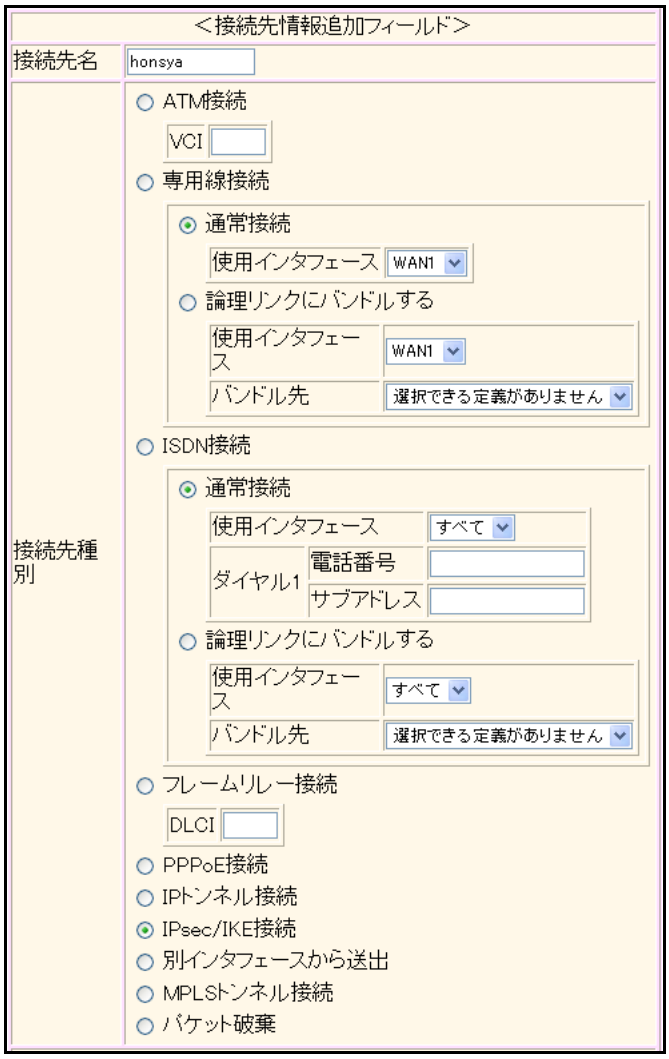
10.　［追加］ボタンをクリックします。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



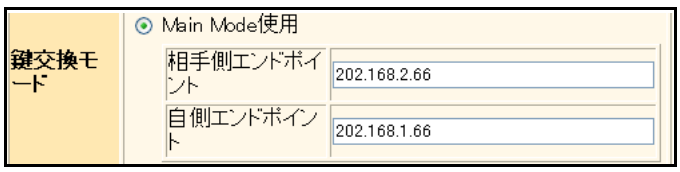
機種により、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66



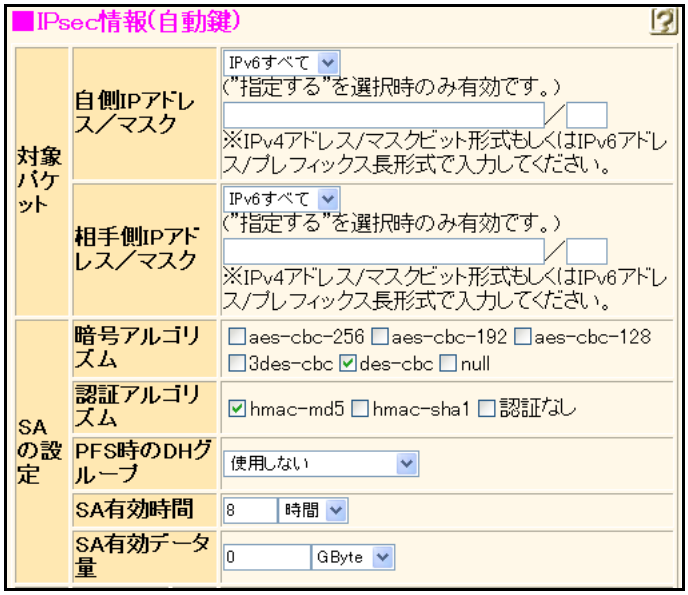
15.　［保存］ボタンをクリックします。

16.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

17.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



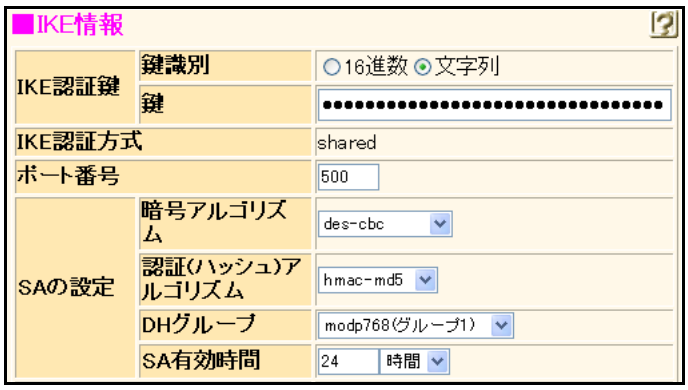
18.　［保存］ボタンをクリックします。

19.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

20.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



21.　［保存］ボタンをクリックします。

22.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi

4.　［追加］ボタンをクリックします。

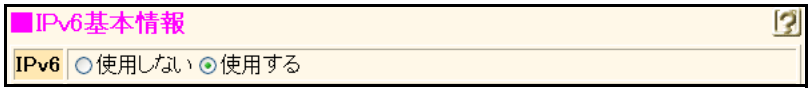
「ネットワーク情報（vpn-shi)」ページが表示されます。

5.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

6.　以下の項目を指定します。

- IPv6　→使用する



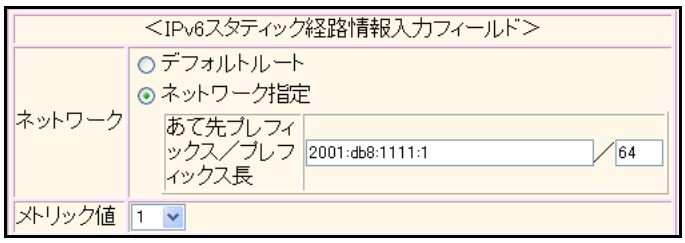
7.　［保存］ボタンをクリックします。

8.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:1::/64
- メトリック値　→1



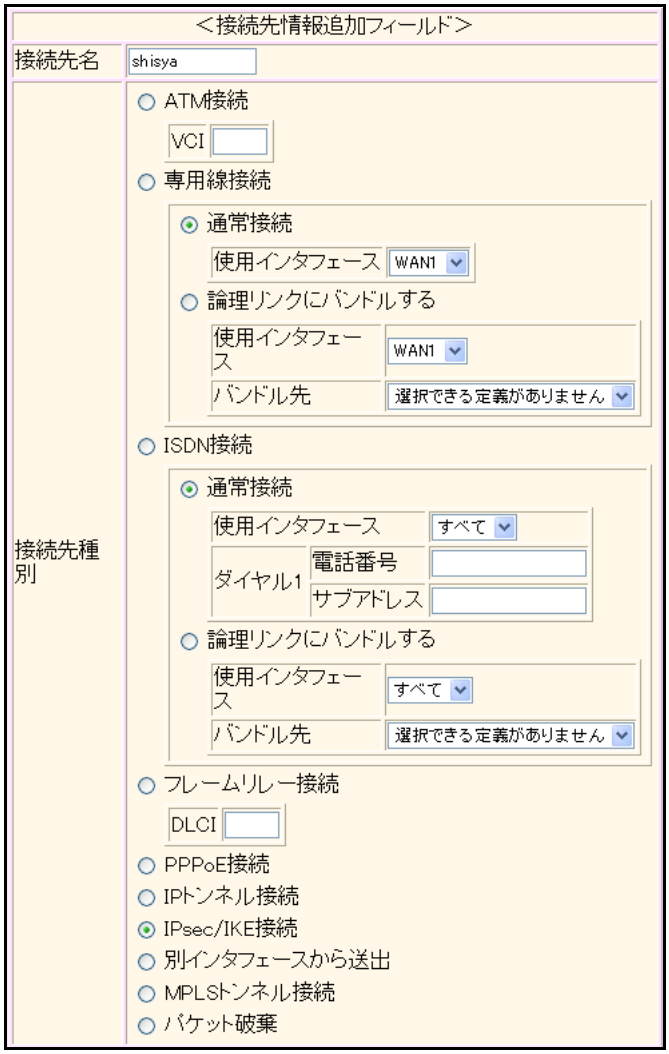
10.　［追加］ボタンをクリックします。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



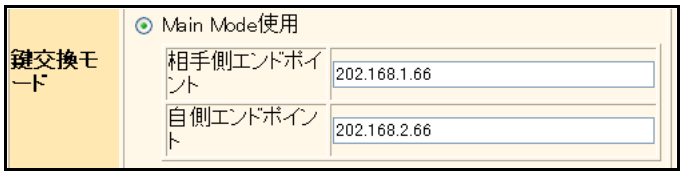
機種により、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 鍵交換モード　→ Main Mode 使用
  相手側エンドポイント　→ 202.168.1.66
  自側エンドポイント　→ 202.168.2.66



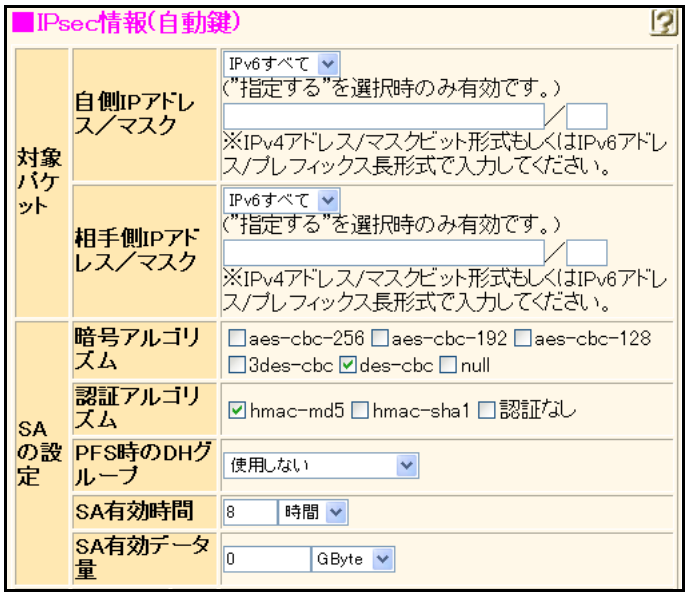
15.　［保存］ボタンをクリックします。

16.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

17.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→ IPv6 すべて
  相手側 IP アドレス／マスク　→ IPv6 すべて
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



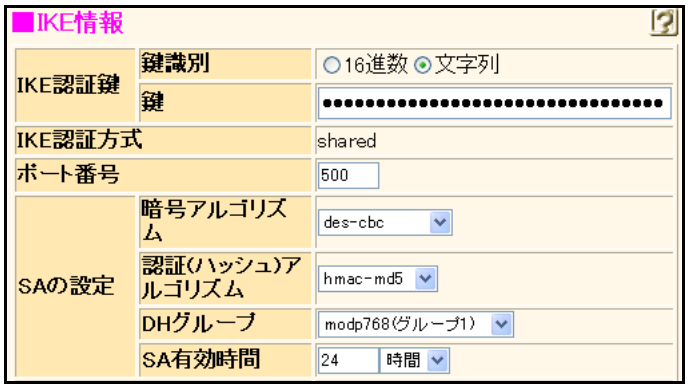
18.　［保存］ボタンをクリックします。

19.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

20.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



21.　［保存］ボタンをクリックします。

22.　画面左側の［設定反映］ボタンをクリックします。
設定した内容が有効になります。

2.14.5　IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

IPv6 ローカルネットワーク間を IPv4 インターネットで結んで IPsec を行います。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

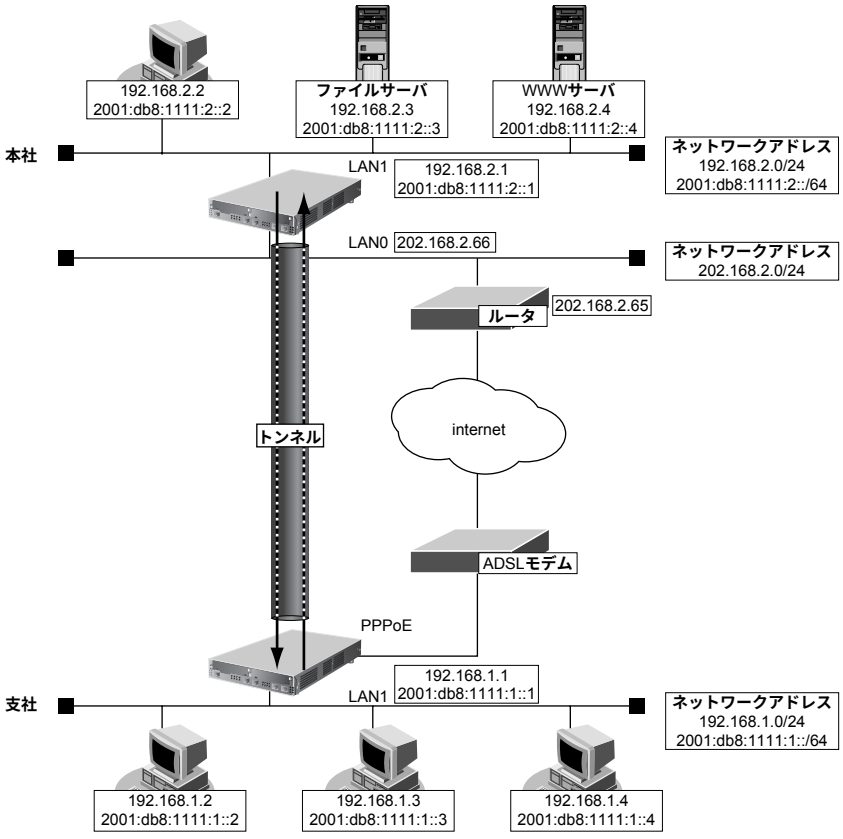
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:1::1/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社-202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66-支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社（Initiator）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（ internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

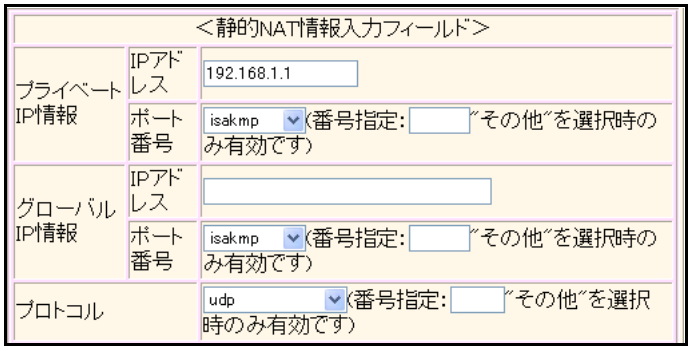
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6. ～ 7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

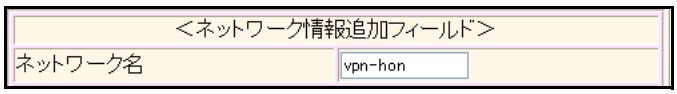
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



12.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

13.　「IP 関連」をクリックします。

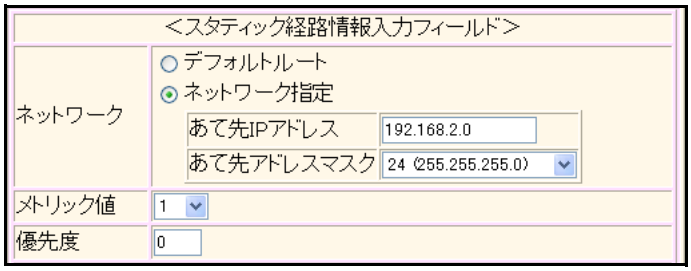
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



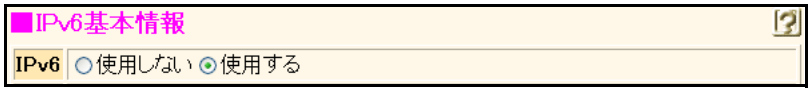
16.　［追加］ボタンをクリックします。

17.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

18.　以下の項目を指定します。

- IPv6　→使用する



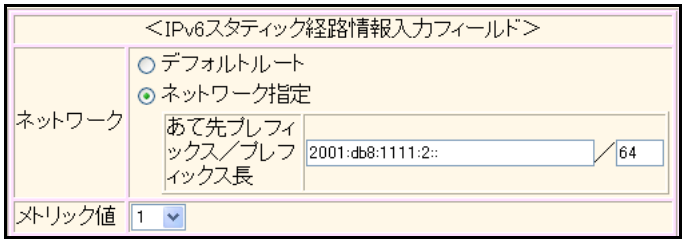
19.　［保存］ボタンをクリックします。

20.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

21.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:2::/64
- メトリック値　→1



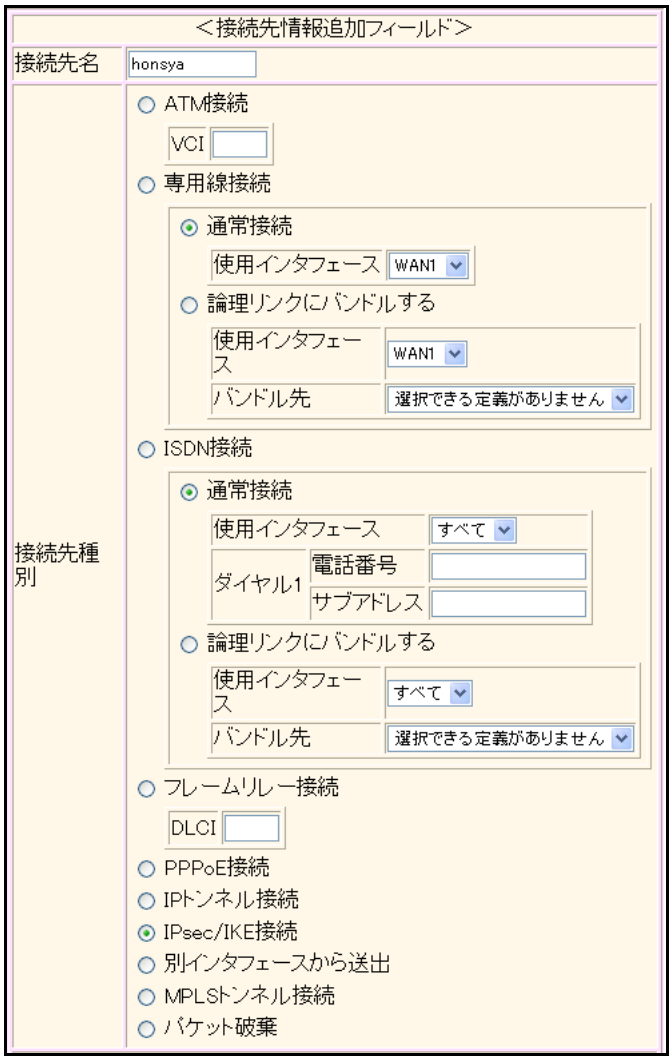
22.　［追加］ボタンをクリックします。

23.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

24.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



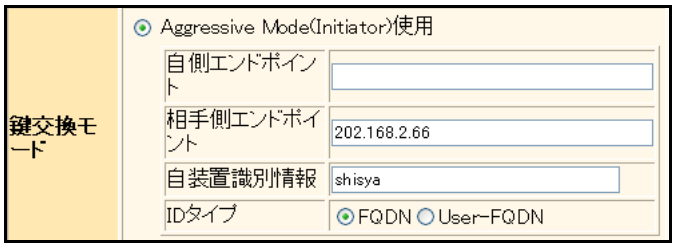
機種により、接続先種別の表示が上記の画面とは異なります。

25.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

26.　以下の項目を指定します。

- 鍵交換モード　→Aggresive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisya



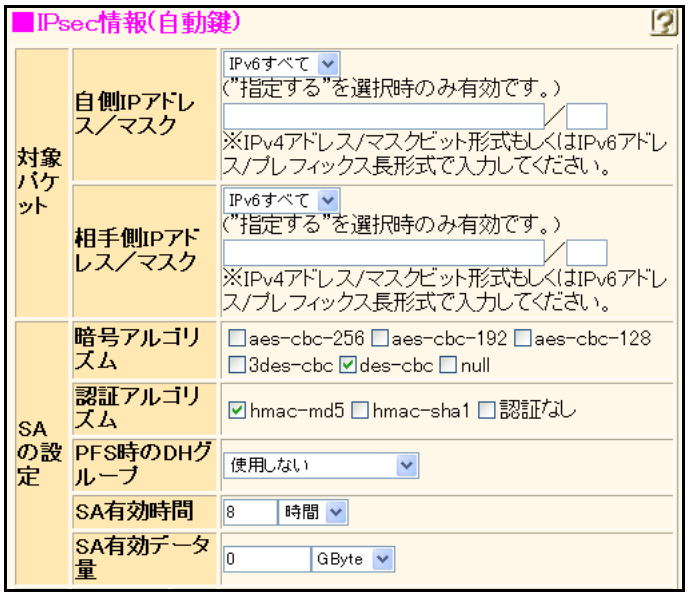
27.　［保存］ボタンをクリックします。

28.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

29.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



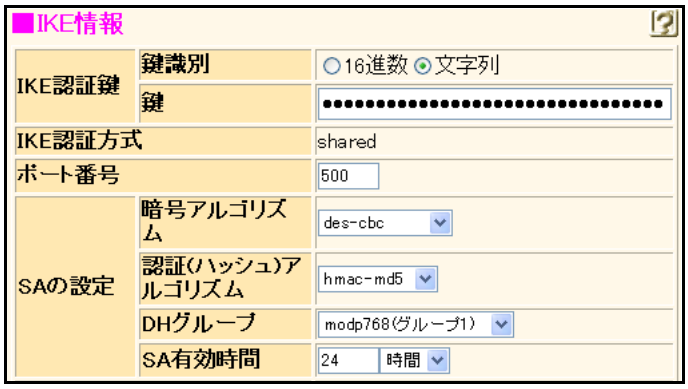
30.　［保存］ボタンをクリックします。

31.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

32.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



33.　［保存］ボタンをクリックします。

34.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社（Responder）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

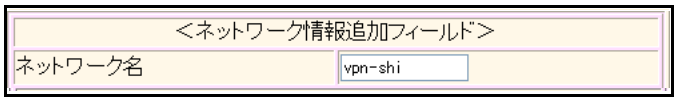
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi）」ページが表示されます。

5.　「IP 関連」をクリックします。

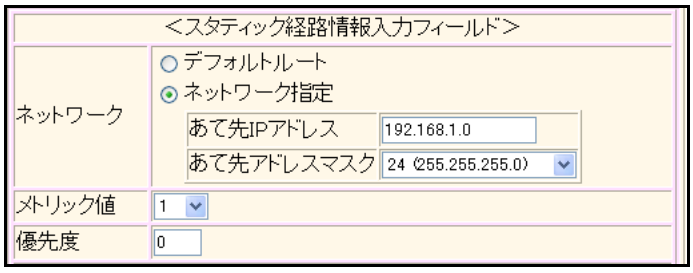
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



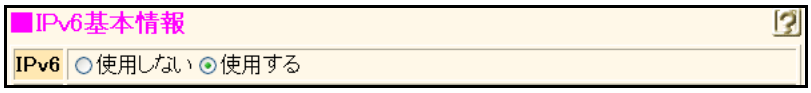
8.　［追加］ボタンをクリックします。

9.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

10.　以下の項目を指定します。

- IPv6　→使用する



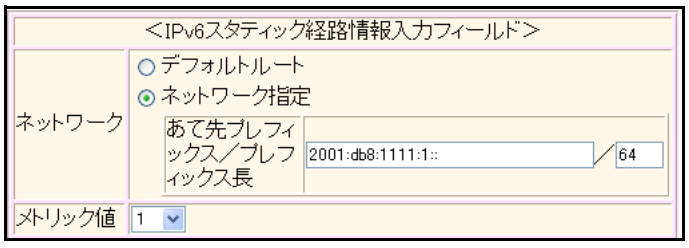
11.　［保存］ボタンをクリックします。

12.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

13.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:1::/64
- メトリック値　→1



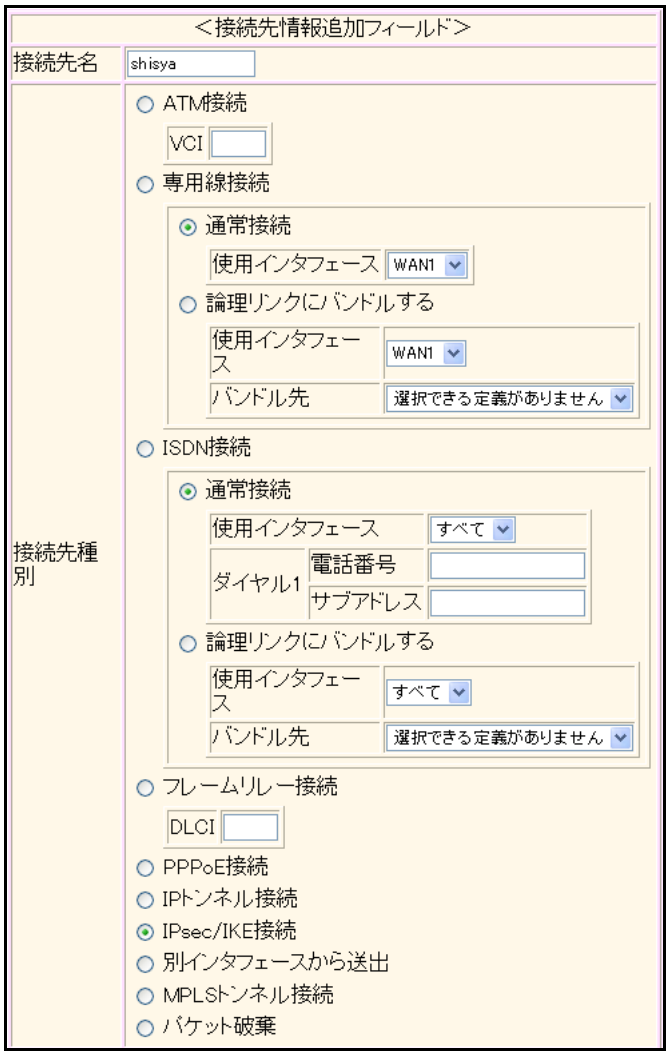
14.　［追加］ボタンをクリックします。

15.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

16.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



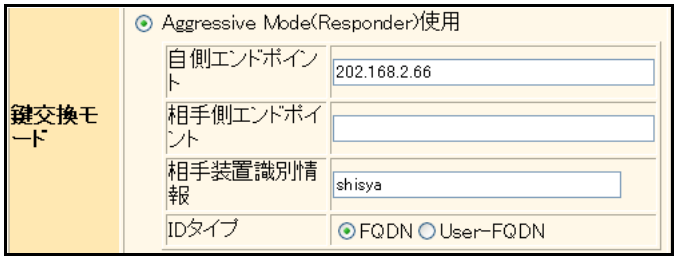
機種により、接続先種別の表示が上記の画面とは異なります。

17.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

18.　以下の項目を指定します。

- 鍵交換モード　→Aggresive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  相手装置識別情報　→shisya



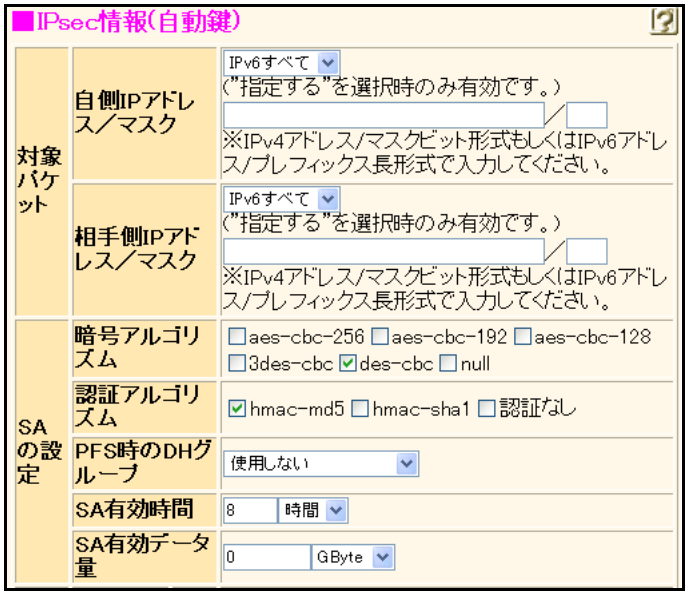
19.　［保存］ボタンをクリックします。

20.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

21.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



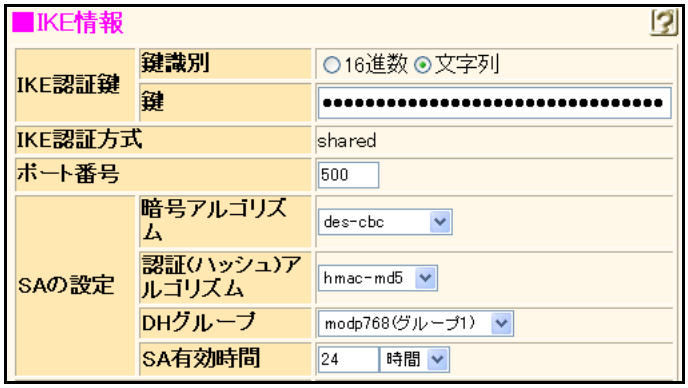
22.　［保存］ボタンをクリックします。

23.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

24.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



25.　［保存］ボタンをクリックします。

26.　画面左側の［設定反映］ボタンをクリックします。
設定した内容が有効になります。

2.14.6　IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

IPsec 機能を使って IPv6 で自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

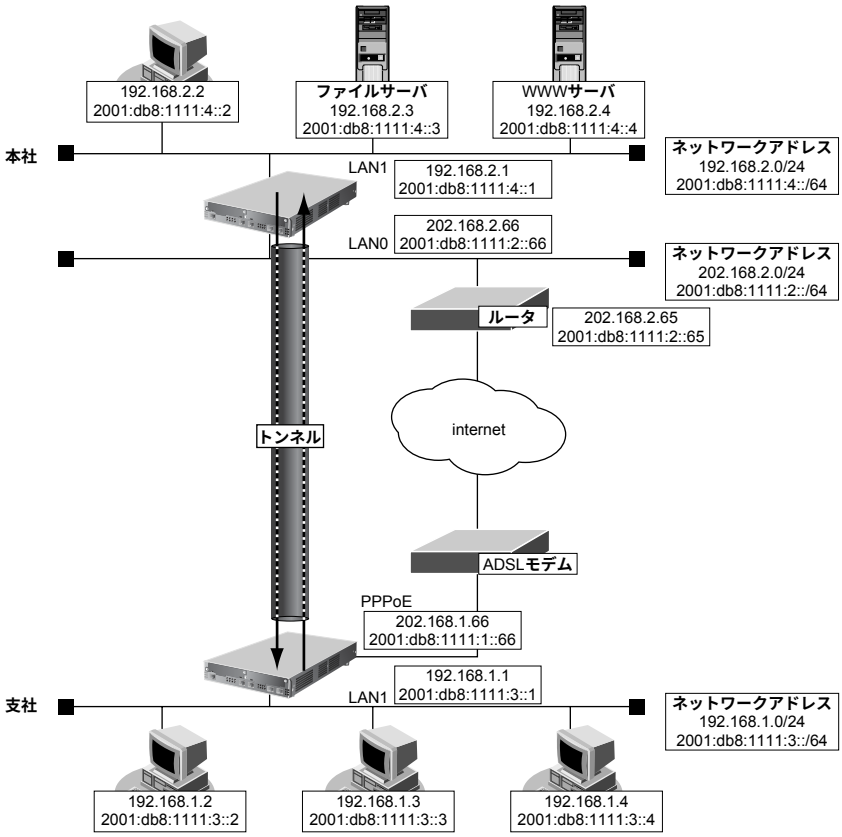
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス
  ：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス
  ：2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-2001:db8:1111:1::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode 使用
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

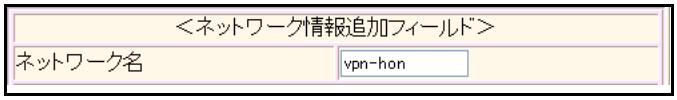
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

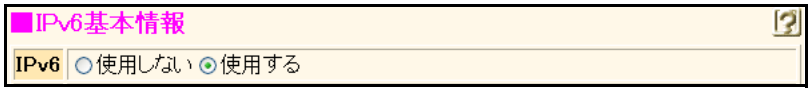
「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

6.　以下の項目を指定します。

- IPv6　→使用する



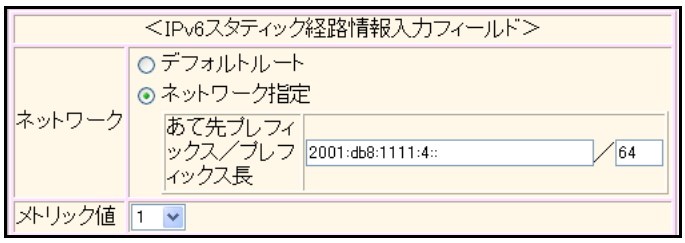
7.　［保存］ボタンをクリックします。

8.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→ 2001:db8:1111:4::/64
- メトリック値　→ 1



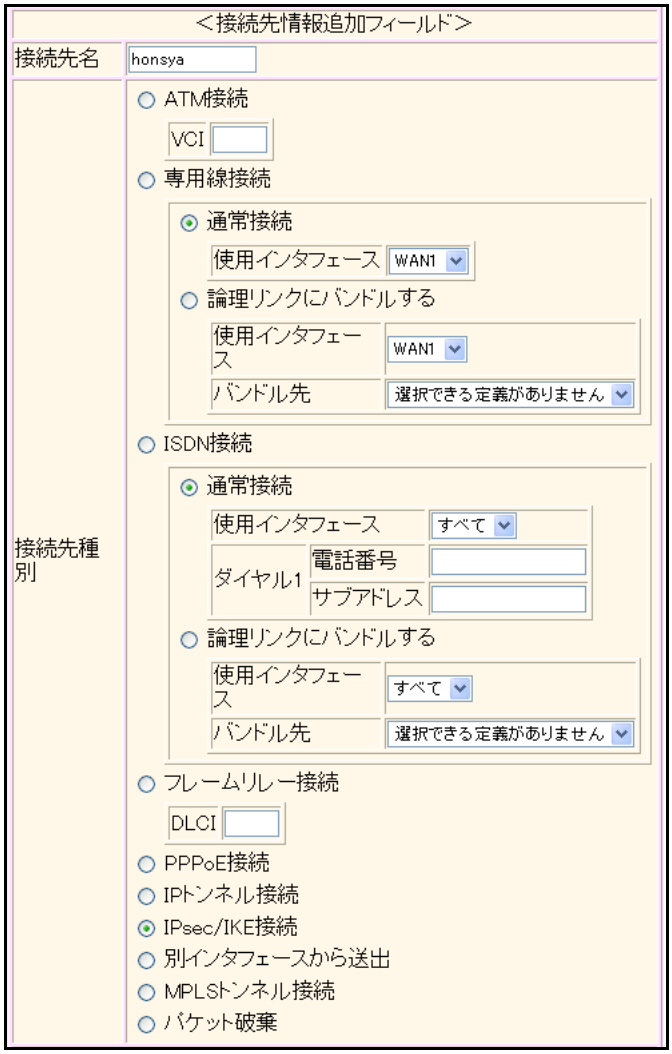
10.　［追加］ボタンをクリックします。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　→ honsya
- 接続先種別　→ IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 鍵交換モード　→ Main Mode 使用
  相手側エンドポイント　→ 2001:db8:1111:2::66
  自側エンドポイント　→ 2001:db8:1111:1::66

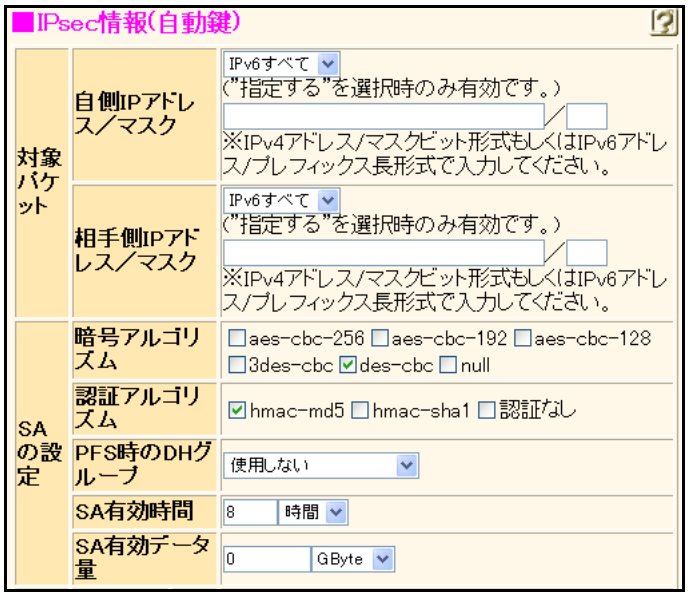
15.　［保存］ボタンをクリックします。

16.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

17.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→ IPv6 すべて
  相手側 IP アドレス／マスク　→ IPv6 すべて
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



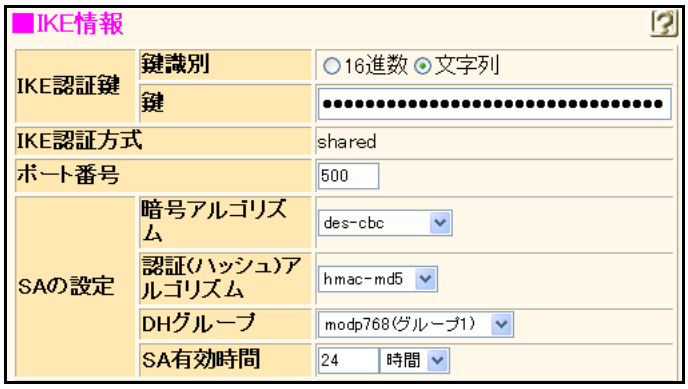
18.　［保存］ボタンをクリックします。

19.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

20.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



21.　［保存］ボタンをクリックします。

22.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

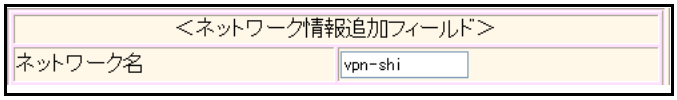
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi



4.　［追加］ボタンをクリックします。

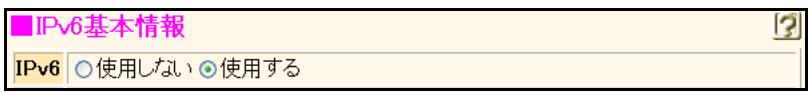
「ネットワーク情報（vpn-shi)」ページが表示されます。

5.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

6.　以下の項目を指定します。

- IPv6　→使用する



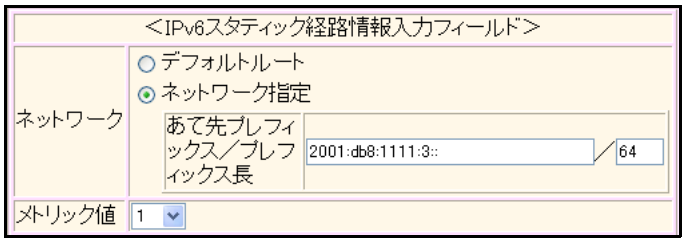
7.　［保存］ボタンをクリックします。

8.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:3::/64
- メトリック値　→1



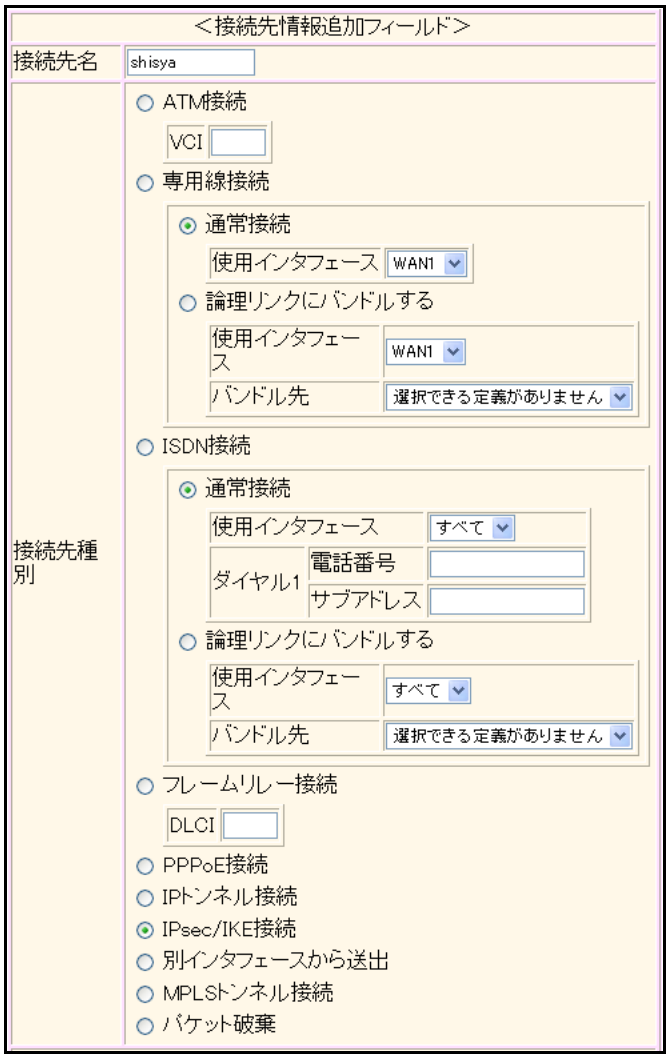
10.　［追加］ボタンをクリックします。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　　→shisya
- 接続先種別　　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 鍵交換モード　　→Main Mode 使用
  相手側エンドポイント　　→2001:db8:1111:1::66
  自側エンドポイント　　→2001:db8:1111:2::66

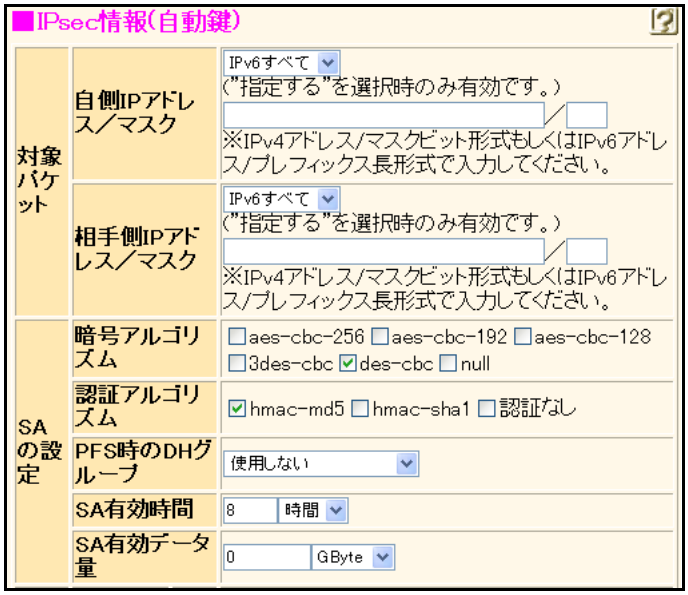
15.　［保存］ボタンをクリックします。

16.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

17.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→ IPv6 すべて
  相手側 IP アドレス／マスク　→ IPv6 すべて
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



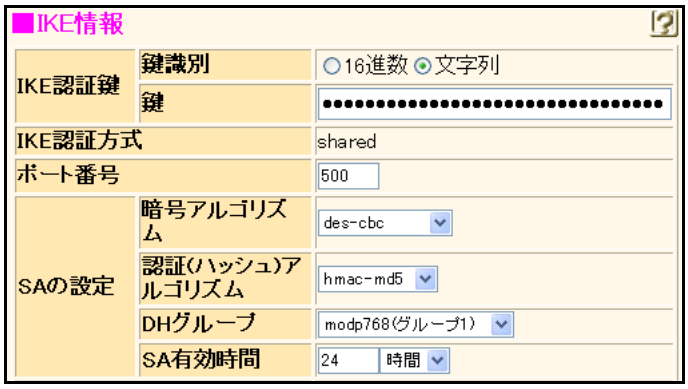
18.　［保存］ボタンをクリックします。

19.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

20.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



21.　［保存］ボタンをクリックします。

22.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.7　IPv6 over IPv6 で可変 IP アドレスでの VPN（自動鍵交換）

適用機種　全機種

接続するたびに IPv6 アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

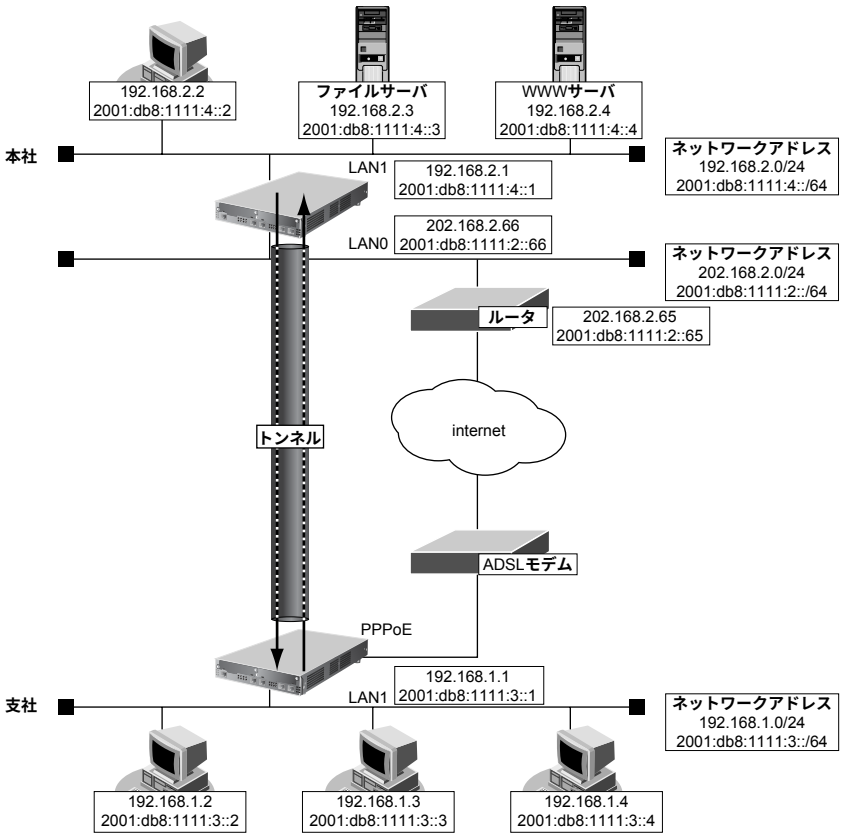
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:3::1/64
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- ローカルネットワーク IPv6 アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス：2001:db8:1111:2::65



● 設定条件

[支社（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社-2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP:500 番ポート）のプライベートアドレス
  ：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）
- ESP のプライベートアドレス　：2001:db8:1111:1::66
  （インターネットプロバイダから割り当てられた IPv6 アドレス）

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：2001:db8:1111:2::66-支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社（Initiator）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

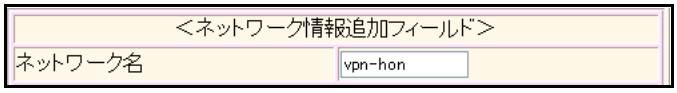
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

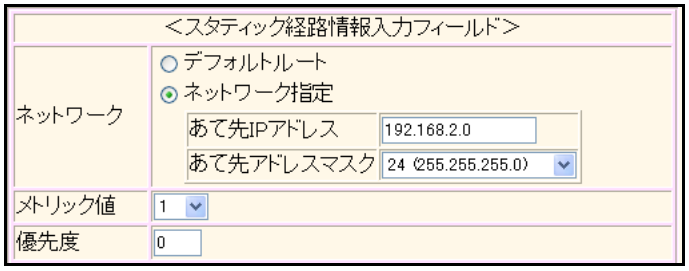
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



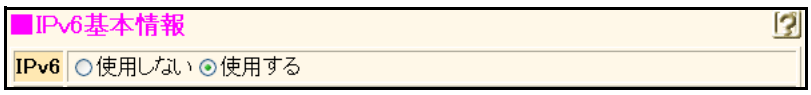
8.　［追加］ボタンをクリックします。

9.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

10.　以下の項目を指定します。

- IPv6　→使用する



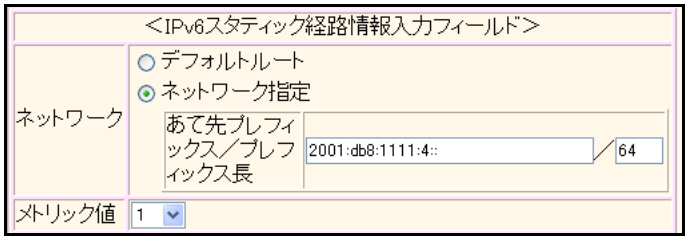
11.　［保存］ボタンをクリックします。

12.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

13.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:4::/64
- メトリック値　→1



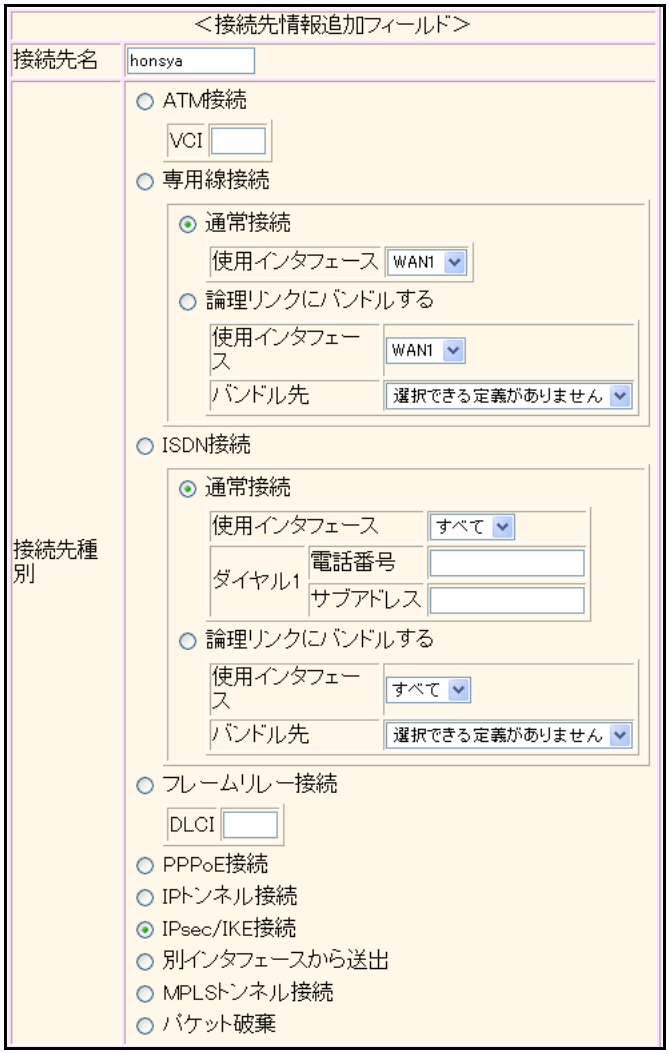
14.　［追加］ボタンをクリックします。

15.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

16.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



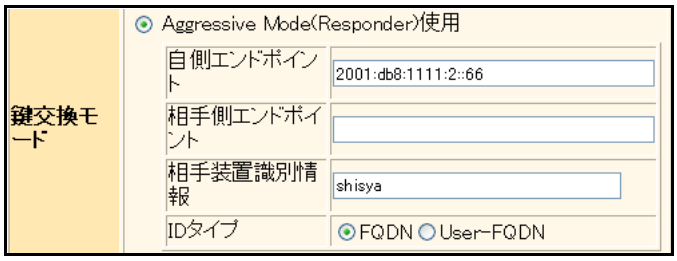
機種により、接続先種別の表示が上記の画面とは異なります。

17.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

18.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→2001:db8:1111:2::66
  自装置識別情報　→shisya



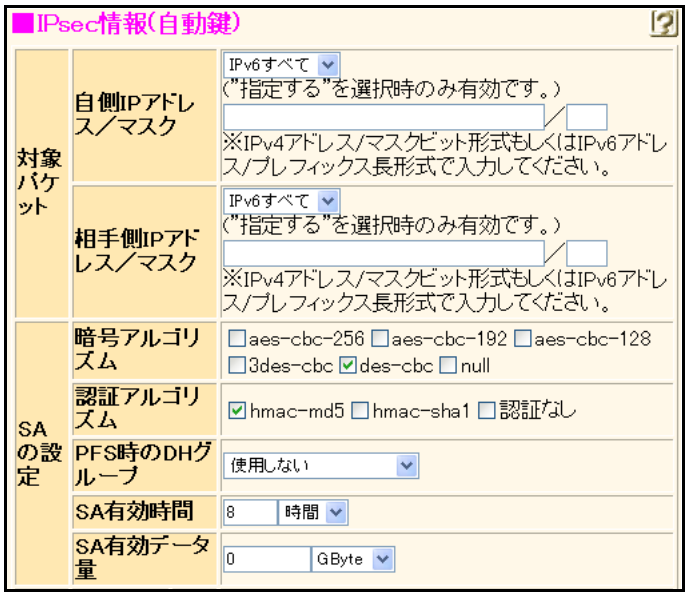
19.　［保存］ボタンをクリックします。

20.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

21.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



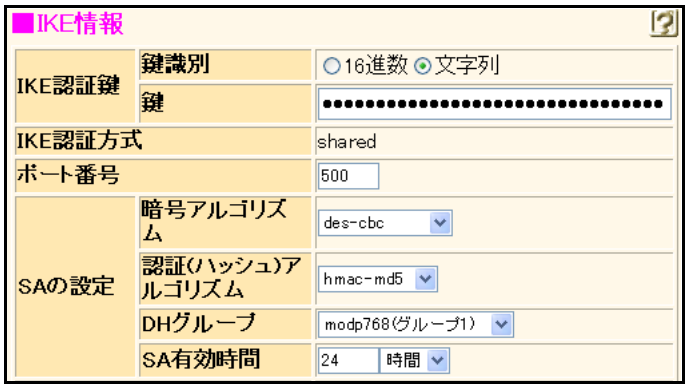
22.　［保存］ボタンをクリックします。

23.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

24.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



25.　［保存］ボタンをクリックします。

26.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社（Responder）を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

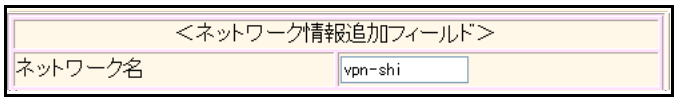
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi）」ページが表示されます。

5.　「IP 関連」をクリックします。

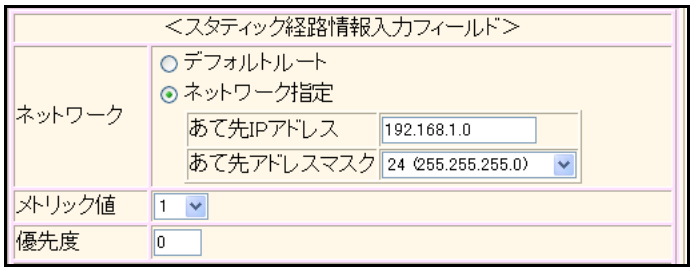
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



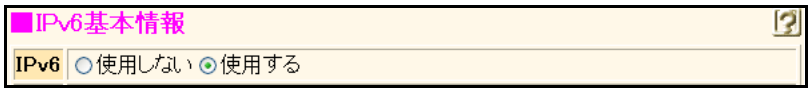
8.　［追加］ボタンをクリックします。

9.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

10.　以下の項目を指定します。

- IPv6　→使用する



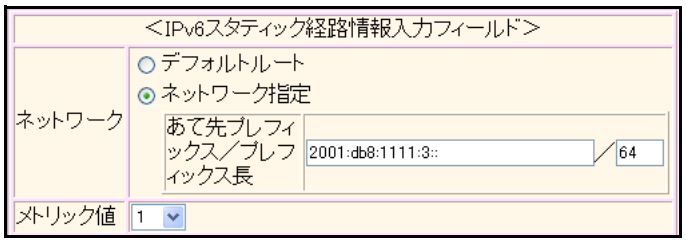
11.　［保存］ボタンをクリックします。

12.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

13.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:3::/64
- メトリック値　→1



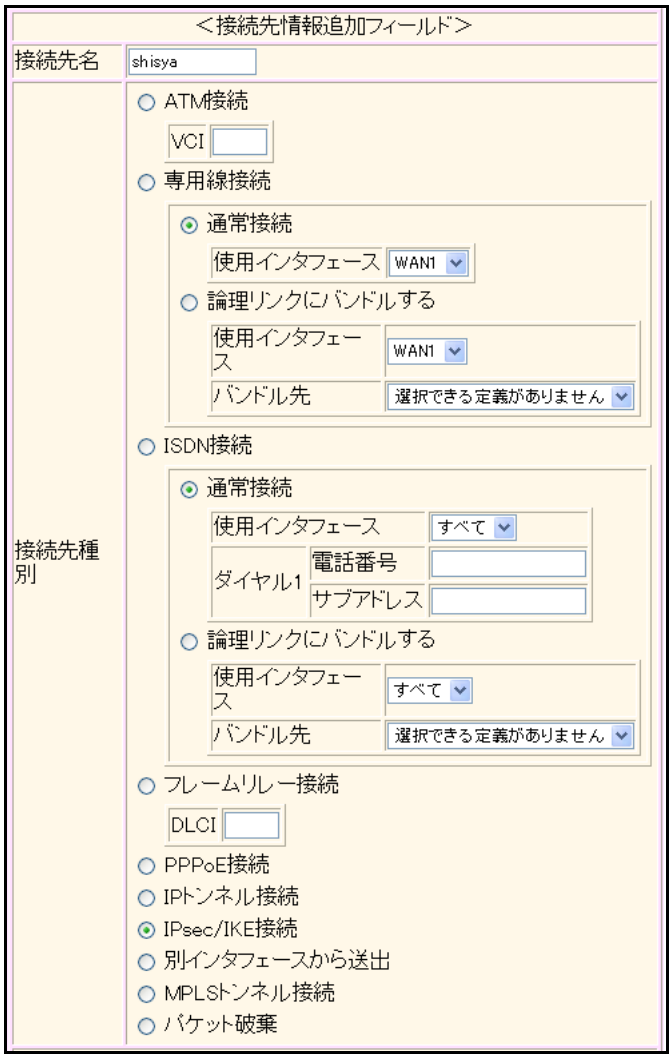
14.　［追加］ボタンをクリックします。

15.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

16.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



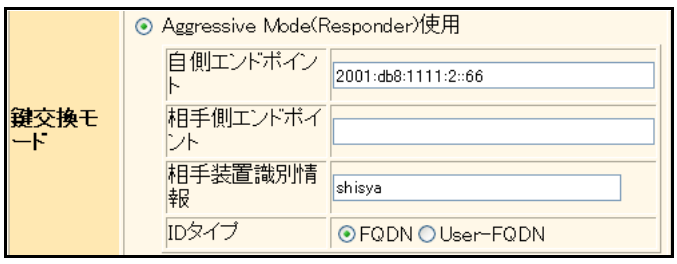
機種により、接続先種別の表示が上記の画面とは異なります。

17.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

18.　以下の項目を指定します。

- 鍵交換モード　→Aggresive Mode（Responder）使用
  自側エンドポイント　→2001:db8:1111:2::66
  相手装置識別情報　→shisya



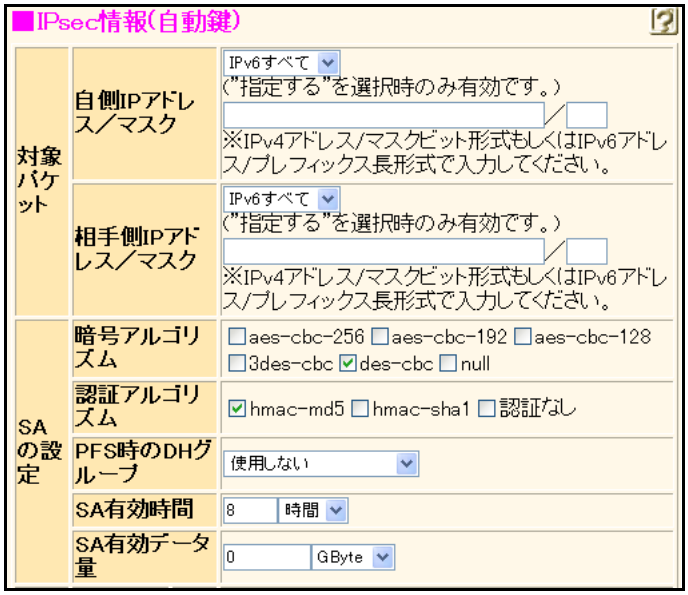
19.　［保存］ボタンをクリックします。

20.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

21.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



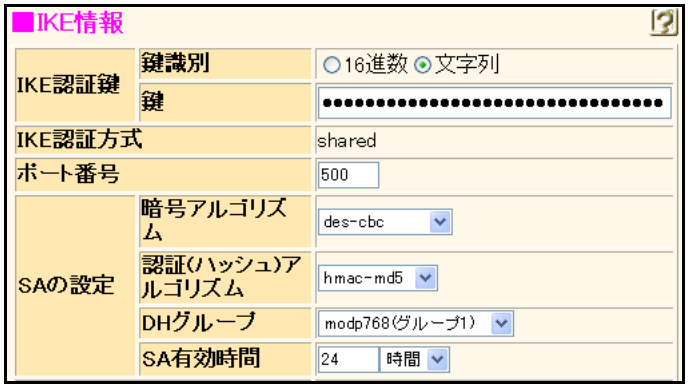
22.　［保存］ボタンをクリックします。

23.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

24.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



25.　［保存］ボタンをクリックします。

26.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.8 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN（自動鍵交換）

適用機種　全機種

IPsec機能を使って複数のネットワークにそれぞれのIPsec SAを作成する環境を構築する場合を例に説明します（自動鍵交換の固定IPアドレスを使用した構成です）。

ここでは以下の条件により、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社（PPPoE常時接続）]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス　：202.168.1.66/24
- PPPoEユーザ認証ID　：userid（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPアドレス1　：LAN0ポート使用
- ローカルネットワークIPアドレス2　：192.168.3.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス　：202.168.2.65

● 設定条件

[支社]

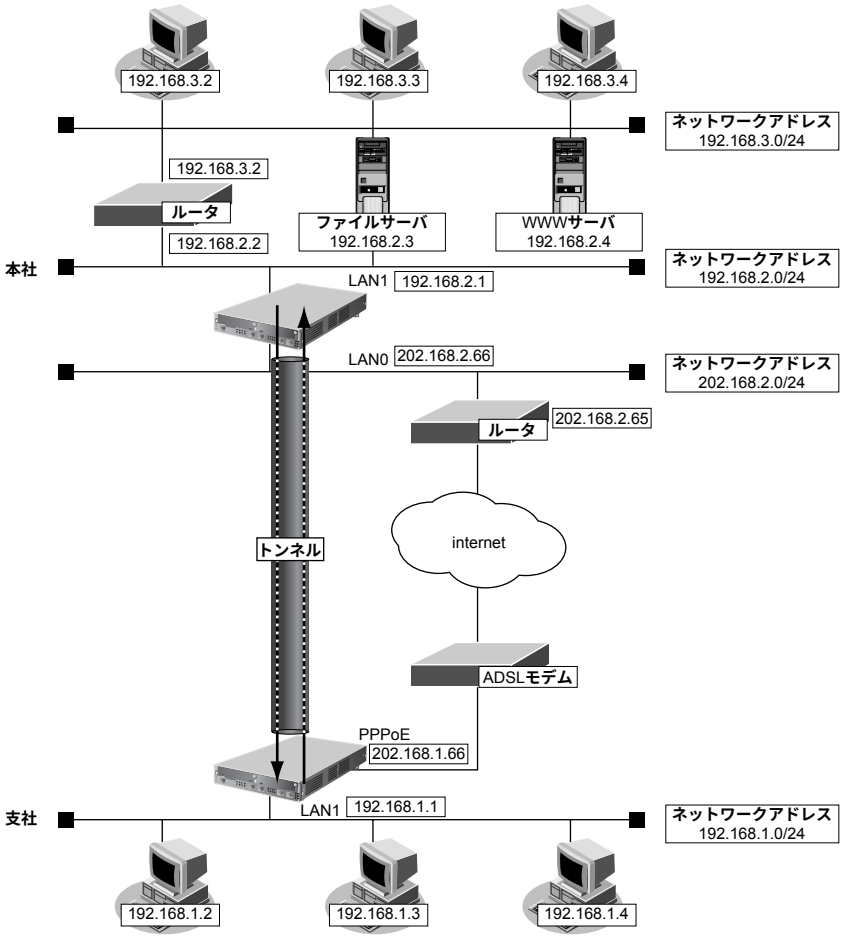
- IPsec/IKE区間　：202.168.1.66 - 202.168.2.66
- IPsec対象範囲（1）　：any - 192.168.2.0/24（マルチルーティングにも定義する）
- IPsec対象範囲（2）　：any - 192.168.3.0/24

[本社]

- IPsec/IKE区間　：202.168.2.66 - 202.168.1.66
- IPsec対象範囲（1）　：192.168.2.0/24 - any（マルチルーティングにも定義する）
- IPsec対象範囲（2）　：192.168.3.0/24 - any

[共通]

- 鍵交換モード　：Main Mode使用
- IPsecプトロコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec PFS時のDHグループ　：なし
- IKE共有鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方式　：shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：des-cbc
- IKE認証（ハッシュ）アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768（グループ1）



上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　　→vpn-hon

＜ネットワーク情報追加フィールド＞	
ネットワーク名	vpn-hon

4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

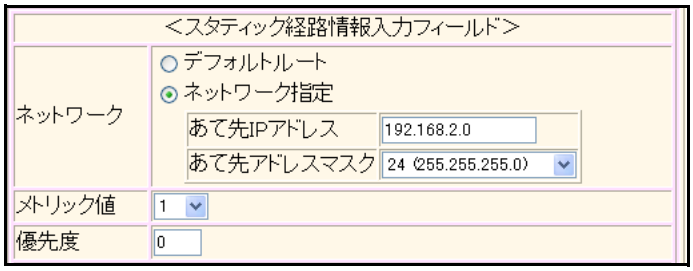
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



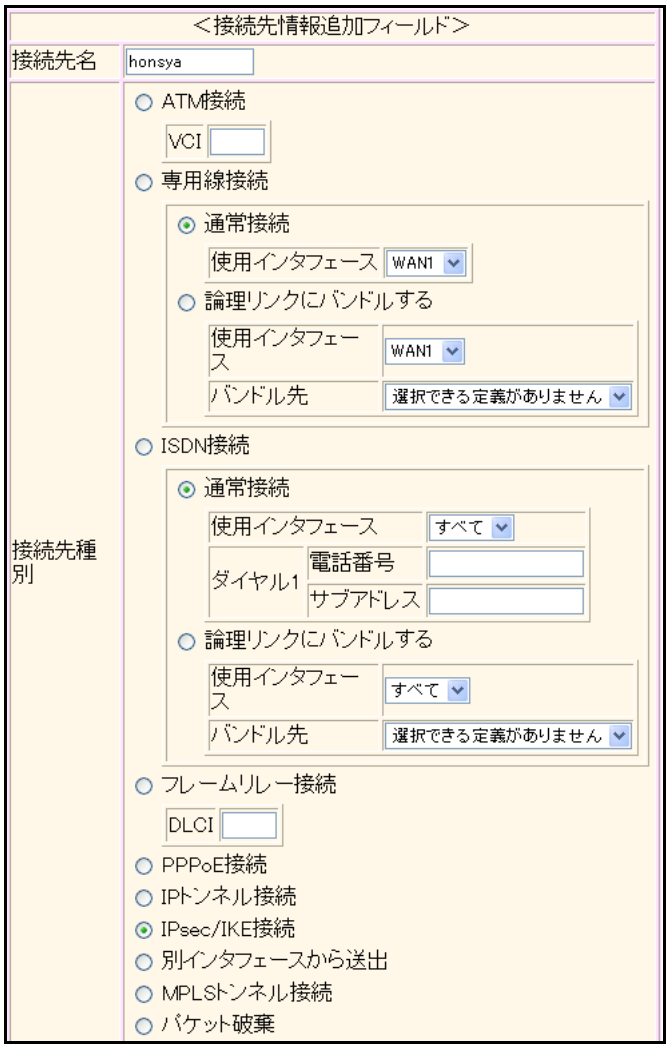
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



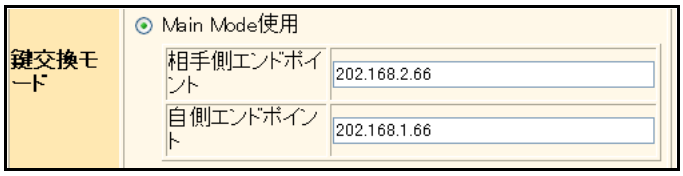
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66



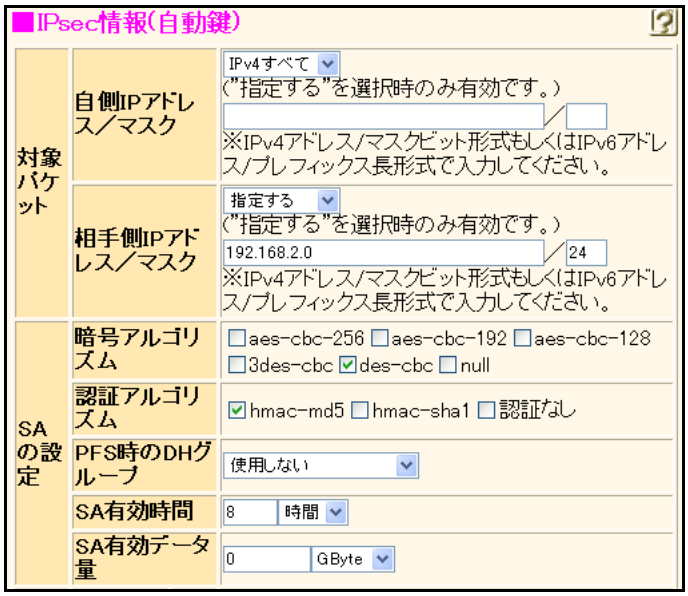
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- 対象パケット
  相手側 IP アドレス／マスク　→指定する
  →192.168.2.0/24
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



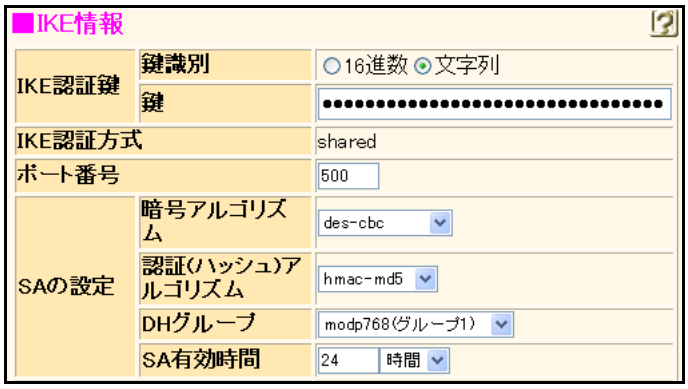
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



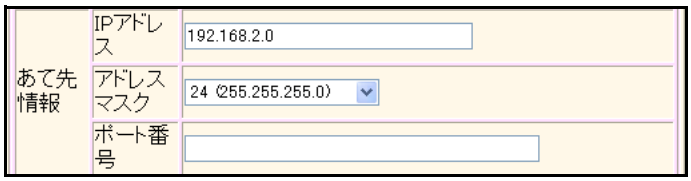
19.　［保存］ボタンをクリックします。

20.　IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。

「マルチルーティング情報」が表示されます。

21.　以下の項目を指定します。

- あて先情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）



22.　画面左側の［設定反映］ボタンをクリックします。

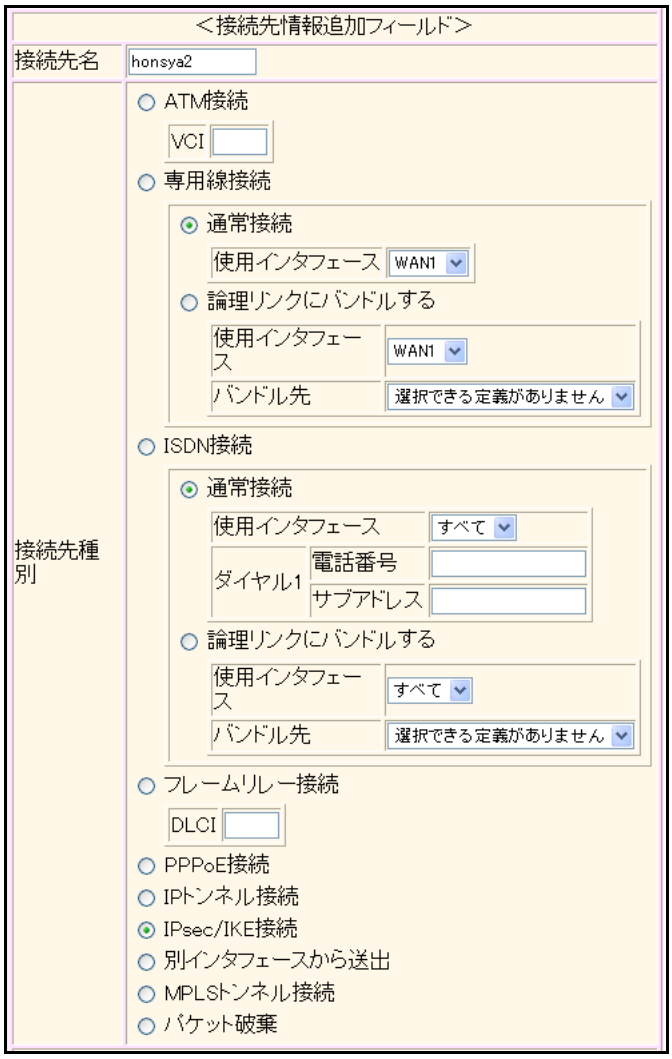
設定した内容が有効になります。

23.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

24.　以下の項目を指定します。

- 接続先名　→honsya2
- 接続先種別　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

25.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

26.　以下の項目を指定します。

- 鍵交換モード　→IKE は他の接続先情報を使用
  接続先名　→honsya

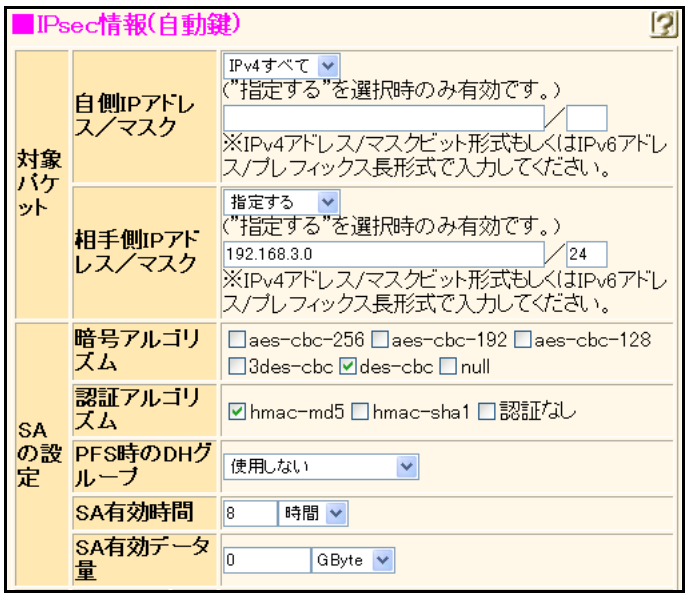
27.　［保存］ボタンをクリックします。

28.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

29.　以下の項目を指定します。

- 対象パケット
  相手側 IP アドレス／マスク　→指定する
  →192.168.3.0/24
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



30.　［保存］ボタンをクリックします。

31.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社の IPsec/IKE を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

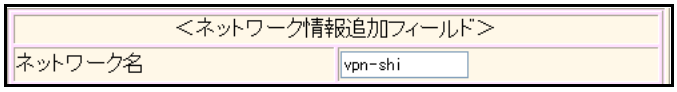
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi)」ページが表示されます。

5.　「IP 関連」をクリックします。

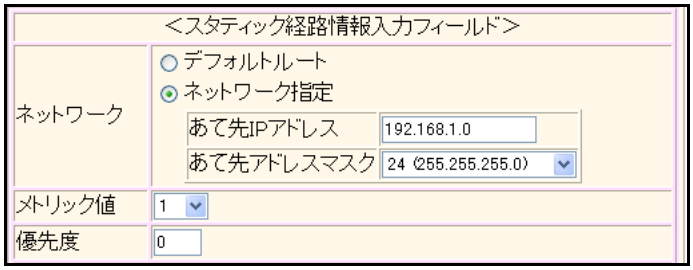
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



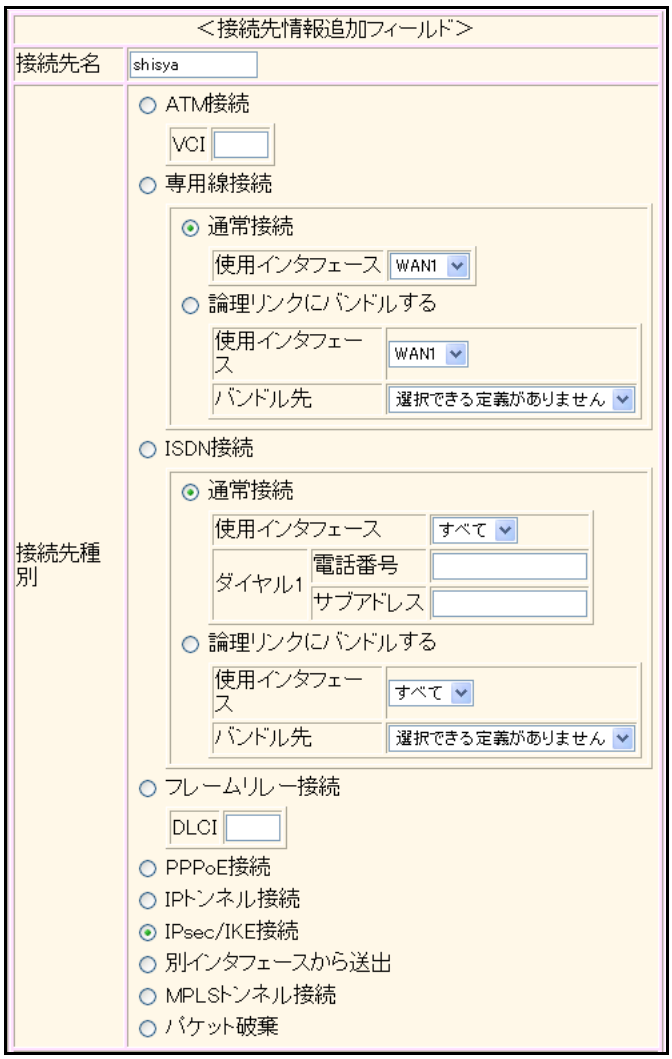
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→ shisya
- 接続先種別　→ IPsec/IKE 接続



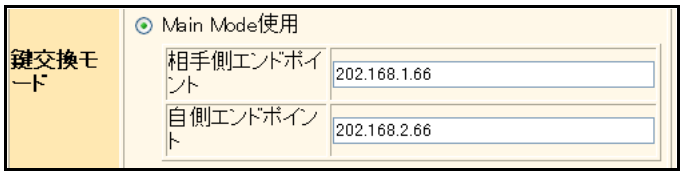
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.1.66
  自側エンドポイント　→202.168.2.66



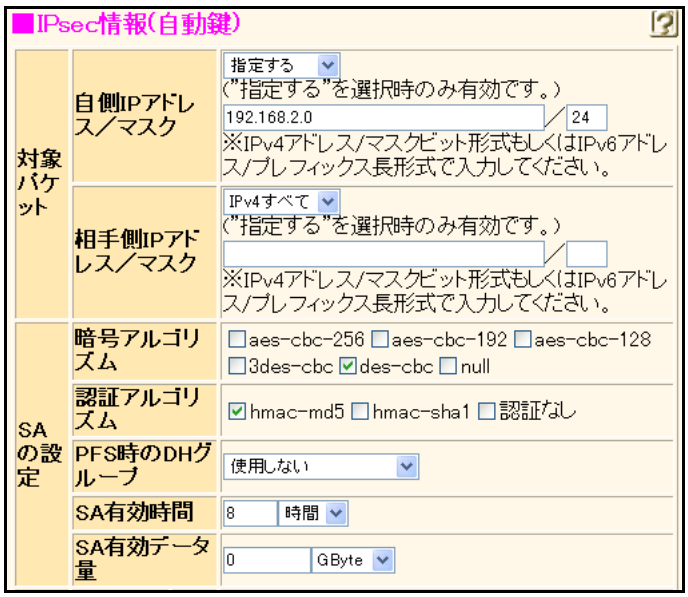
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→指定する
  →192.168.2.0/24
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



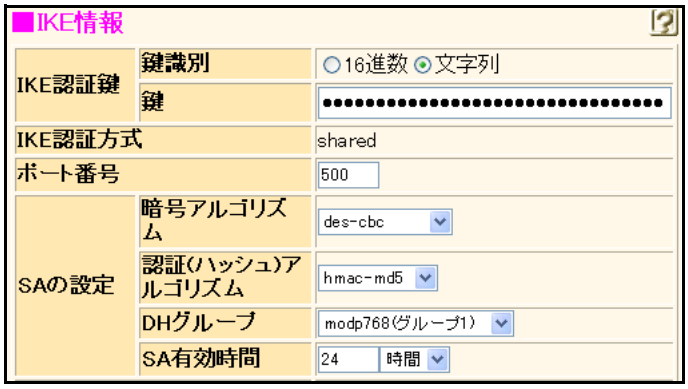
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



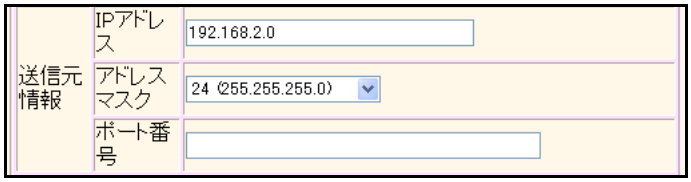
19.　［保存］ボタンをクリックします。

20.　IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。

「マルチルーティング情報」が表示されます。

21.　以下の項目を指定します。

- 送信元情報
  IP アドレス　→ 192.168.2.0
  アドレスマスク　→ 24（255.255.255.0）



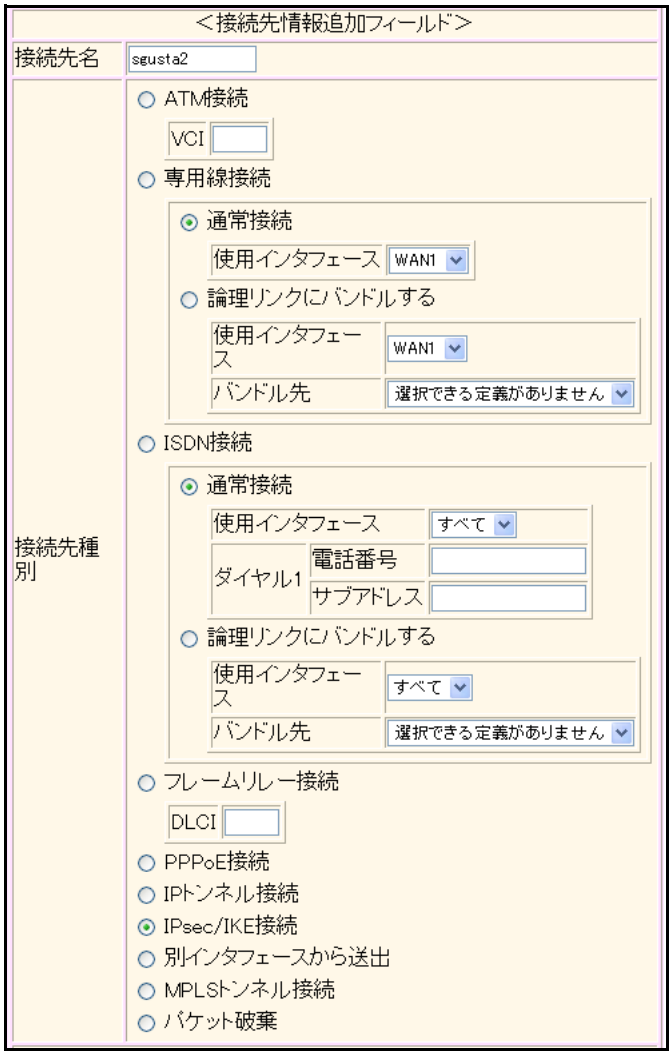
22.　［追加］ボタンをクリックします。

23.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

24.　以下の項目を指定します。

- 接続先名　→ shisya2
- 接続先種別　→ IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

25.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

26.　以下の項目を指定します。

- 鍵交換モード　→ IKE は他の接続先情報を使用
  接続先名　→ shisya

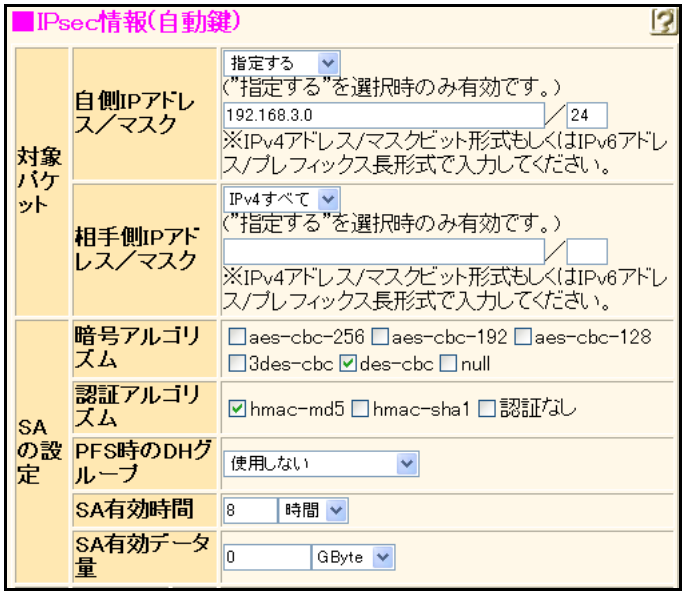
27.　［保存］ボタンをクリックします。

28.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

29.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→指定する
  → 192.168.3.0/24
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



30.　［保存］ボタンをクリックします。

31.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.9　IPsec 機能と他機能との併用

適用機種　全機種

IPsec 機能と他機能を併用する場合のいくつかの設定例を、以下に説明します。

ここでは、「1.14 複数の事業所 LAN を VPN（IPsec）で接続する」（P.145）の設定が行われていることを前提とします。

- IPsec 変換前のマルチ NAT ／ IP フィルタリング／ TOS 値書き換え機能
- IPsec 変換前のシェーピング機能と帯域制御（WFQ）機能
- IPsec 変換前の MSS 書換え機能
- IPsec 変換前の MTU 分割機能
- 接続先監視機能
- IKE セッション監視機能
- 動的経路（RIP）機能

補足　以下の機能については、IPv6 アドレスで使用することはできません。
- IPsec 変換前のマルチ NAT 機能
- IKE セッション監視機能

IPsec 変換前のマルチ NAT ／ IP フィルタリング／ TOS 値書き換え機能との併用例

● 設定条件

[支社]

- NAT の使用　：マルチ NAT を使用する
  グローバルアドレス　：192.168.1.1
  アドレス個数　：1
  アドレス割当てタイマ　：5 分
- IP フィルタリング　：支社 - 本社間の telnet ／ ftp 通信以外遮断
- TOS 値書き換え　：ftp 通信を 0xa0 に変換

[本社]

- IP フィルタリング　：支社 - 本社間の telnet ／ ftp 通信以外遮断
- TOS 値書き換え　：ftp 通信を 0xa0 に変換

上記の設定条件に従って設定を行う場合の設定例を示します。

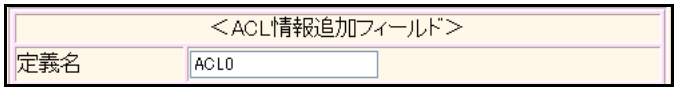
支社を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ ACL0



3.　［追加］ボタンをクリックします。

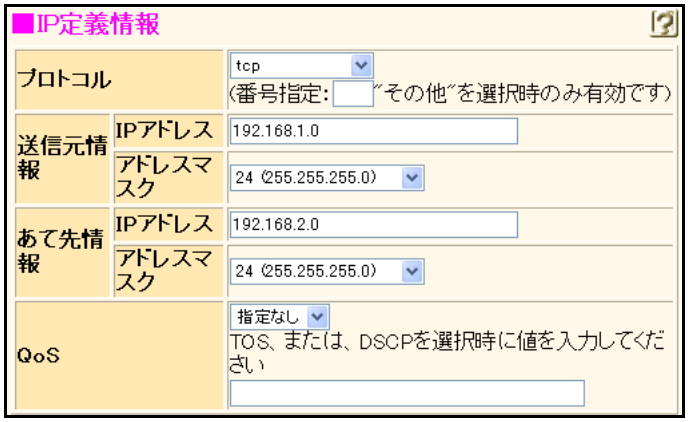
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし



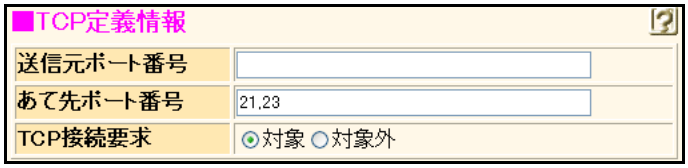
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）、23（telnet のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　手順 1.～9. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→21（ftp のポート番号）、23（telnet のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

11.　手順 1.～9. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「ACL 定義情報（ACL2）」-「TCP 定義情報」

- 送信元ポート番号　→指定しない
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象

12.　手順 1.～9. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）

- あて先情報
  IP アドレス　→ 192.168.2.0
  アドレスマスク　→ 24（255.255.255.0）
- QoS　→ TOS
  → 0

「ACL 定義情報（ACL3）」-「TCP 定義情報」

- 送信元ポート番号　→指定しない
- あて先ポート番号　→ 20（ftp-data のポート番号）、21（ftp のポート番号）
- TCP 接続要求　→対象

13. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

14. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

15. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

16. 「IP 関連」をクリックします。

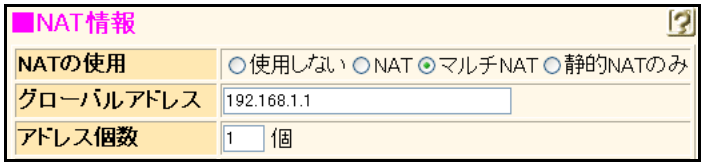
IP 関連の設定項目と「IP 基本情報」が表示されます。

17. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

18. 以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→ 192.168.1.1
- アドレス個数　→ 1



19. ［保存］ボタンをクリックします。

20. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

21.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。

＜IPフィルタリング情報入力フィールド＞	
動作	◉透過 ○遮断
方向	入出力
ACL定義番号	0 参照

22.　［追加］ボタンをクリックします。

23.　手順 20. ～ 22. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

24.　手順 20. ～ 22. を参考に、以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→2

25.　IP 関連の設定項目の「TOS 値書き換え情報」をクリックします。

「TOS 値書き換え情報」が表示されます。

26.　以下の項目を指定します。

- 新 TOS　→a0
- ACL 定義番号　→3

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。

＜TOS値書き換え情報入力フィールド＞	
新TOS	a0
ACL定義番号	3 参照

27.　［追加］ボタンをクリックします。

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

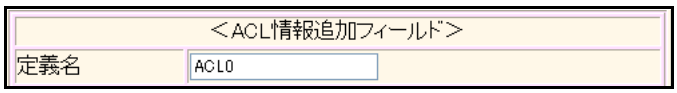
本社を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

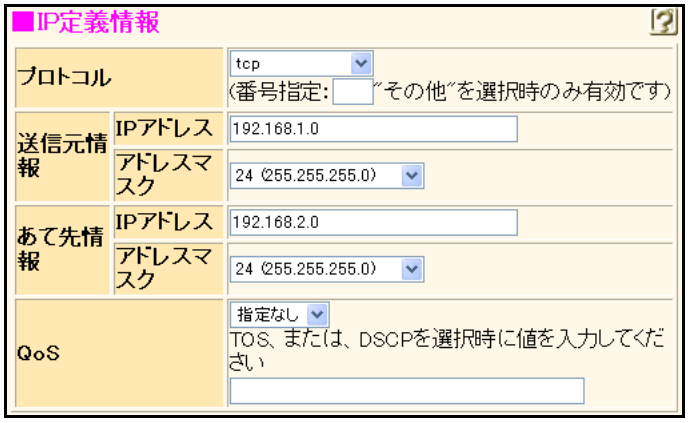
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし



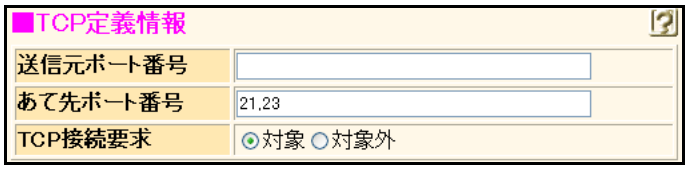
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→21（ftp のポート番号）、23（telnet のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　手順 1.～9. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

「ACL 定義情報（ACL1）」-「TCP 定義情報」

- 送信元ポート番号　→21（ftp のポート番号）、23（telnet のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象外

11.　手順 1.～9. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL2

「ACL 定義情報（ACL2）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「ACL 定義情報（ACL2）」-「TCP 定義情報」

- 送信元ポート番号　→指定しない
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象

12.　手順 1.～9. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL3

「ACL 定義情報（ACL3）」-「IP 定義情報」

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→TOS
  →0

「ACL 定義情報（ACL3）」-「TCP 定義情報」

- 送信元ポート番号　→20（ftp-data のポート番号）、21（ftp のポート番号）
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象

13.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

14.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

15.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-shi）」ページが表示されます。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

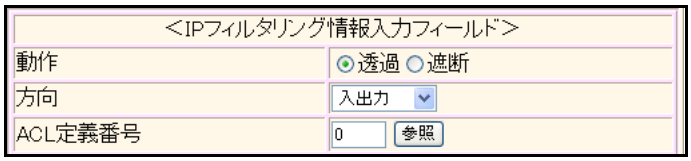
17.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

18.　以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



19.　［追加］ボタンをクリックします。

20.　手順 17.～19. を参考に、以下の項目を指定します。

- 動作　→透過
- 方向　→入出力
- ACL 定義番号　→1

21.　手順 17.～19. を参考に、以下の項目を指定します。

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→2

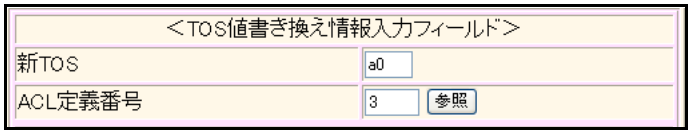
22.　IP 関連の設定項目の「TOS 値書き換え情報」をクリックします。

「TOS 値書き換え情報」が表示されます。

23.　以下の項目を指定します。

- 新 TOS　→a0
- ACL 定義番号　→3

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



24.　［追加］ボタンをクリックします。

25.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

IPsec 変換前のシェーピング機能と帯域制御（WFQ）機能の併用例

● 設定条件

[本社]

- シェーピングレート　：2Mbps
- 帯域制御対象送信元 IP アドレス　：192.168.2.0/24
- 帯域制御対象送信元ポート番号　：すべて
- 帯域制御対象あて先 IP アドレス　：192.168.1.0/24
- 帯域制御対象あて先ポート番号　：すべて
- 帯域制御対象プロトコル　：TCP
- 帯域制御対象 TOS 値　：すべて
- 割り当て帯域　：最優先

上記の設定条件に従って設定を行う場合の設定例を示します。

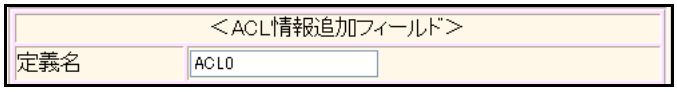
本社を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　[追加] ボタンをクリックします。

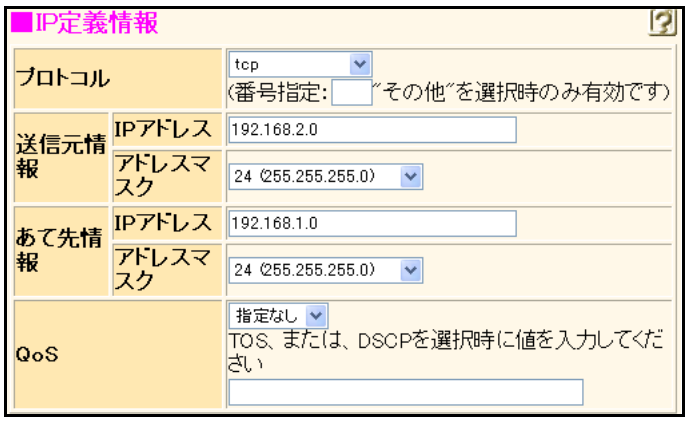
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし



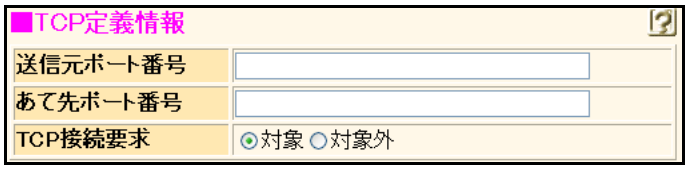
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→指定しない
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

12.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の［修正］ボタンをクリックします。

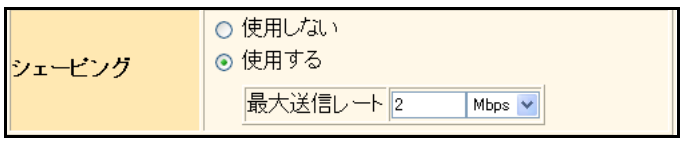
「ネットワーク情報（vpn-shi)」ページが表示されます。

13.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- シェーピング　→使用する
  最大送信レート　→2Mbps



15.　［保存］ボタンをクリックします。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

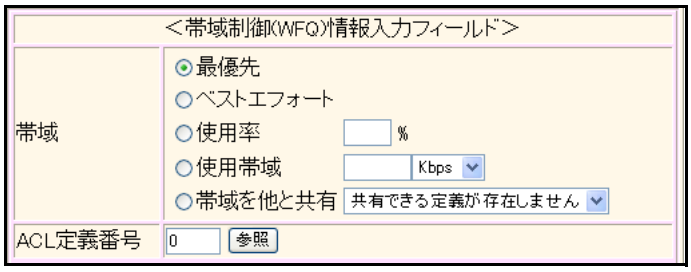
17.　IP 関連の設定項目の「帯域制御（WFQ）情報」をクリックします。

「帯域制御（WFQ）情報」が表示されます。

18.　以下の項目を指定します。

- 帯域　→最優先
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



19.　［追加］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

IPsec 機能と帯域制御（WFQ）機能を併用する場合、IPsec 前のパケットに対して帯域制御を行うときには、IPsec 用の「相手情報」－「ネットワーク情報」で設定します。この場合、IPsec 用の「ネットワーク情報」でシェーピングを行うか、または、実回線の「ネットワーク情報」で IPsec 後のパケットに対して帯域制御を設定する必要があります。

IPsec 変換前の MSS 書き換え機能との併用例

● 設定条件

［共通］

- MSS 書き換え値　：1414Byte

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の［修正］ボタンをクリックします。

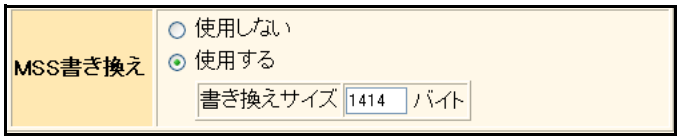
「ネットワーク情報（vpn-hon）」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　以下の項目を指定します。

- MSS 書き換え　→使用する
  書き換えサイズ　→ 1414



6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の［修正］ボタンをクリックします。

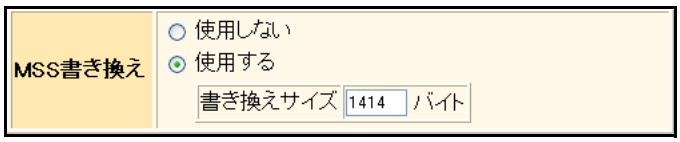
「ネットワーク情報（vpn-shi）」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　以下の項目を指定します。

- MSS 書き換え　→使用する
  書き換えサイズ　→ 1414



6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

IPsec 変換前の MTU 分割機能との併用例

● 設定条件

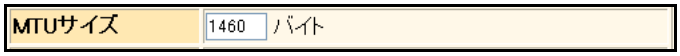
[共通]

- MTU 長　：1460Byte

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

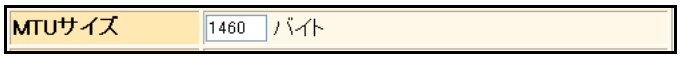
1. **設定メニューのルータ設定で「相手情報」をクリックします。**
   「相手情報」ページが表示されます。
2. **「ネットワーク情報」をクリックします。**
   「ネットワーク情報」が表示されます。
3. **「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の［修正］ボタンをクリックします。**
   「ネットワーク情報（vpn-hon)」ページが表示されます。
4. **「共通情報」をクリックします。**
   共通情報の設定項目と「基本情報」が表示されます。
5. **以下の項目を指定します。**
   - MTU サイズ　→ 1460



6. **［保存］ボタンをクリックします。**
7. **画面左側の［設定反映］ボタンをクリックします。**
   設定した内容が有効になります。

本社を設定する

1. **設定メニューのルータ設定で「相手情報」をクリックします。**
   「相手情報」ページが表示されます。
2. **「ネットワーク情報」をクリックします。**
   「ネットワーク情報」が表示されます。
3. **「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の［修正］ボタンをクリックします。**
   「ネットワーク情報（vpn-shi)」ページが表示されます。
4. **「共通情報」をクリックします。**
   共通情報の設定項目と「基本情報」が表示されます。
5. **以下の項目を指定します。**
   - MTU サイズ　→ 1460



6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

接続先監視機能との併用例

● 設定条件

［支社］

- 送信元 IP アドレス　：192.168.1.1
- あて先 IP アドレス　：192.168.2.1
- タイムアウト時間　：5 秒
- 正常時送信間隔　：10 秒
- 異常時送信間隔　：1 分

補足　監視対象装置は、本社側 VPN 装置を指定します。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

4.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

5.　「接続先情報」で IPsec/IKE 接続で接続先名が honsya の［修正］ボタンをクリックします。

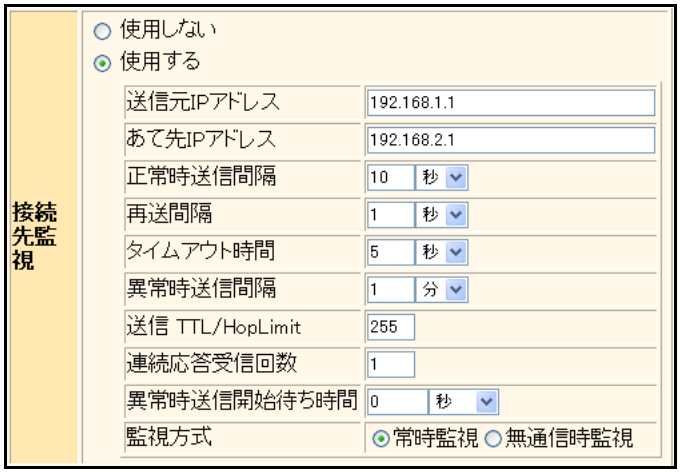
IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

6.　IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

7.　以下の項目を指定します。

- 接続先監視　→使用する
  送信元 IP アドレス　→ 192.168.1.1
  あて先 IP アドレス　→ 192.168.2.1
  正常時送信間隔　→ 10 秒
  再送間隔　→ 1 秒
  タイムアウト時間　→ 5 秒
  異常時送信間隔　→ 1 分



8.　［保存］ボタンをクリックします。

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

IKE セッション監視機能との併用例

● 設定条件

［支社］

- あて先 IP アドレス　：192.168.2.1
- タイムアウト時間　：5 秒
- 正常時送信間隔　：10 秒
- 異常時送信間隔　：1 分

補足　監視対象装置は、本社側 VPN 装置を指定します。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon)」ページが表示されます。

4.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

5.　「接続先情報」で IPsec/IKE 接続で接続先名が honsya の［修正］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

6.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

7.　以下の項目を指定します。

- IKE セッション監視

  あて先 IP アドレス　→ 192.168.2.1
  タイムアウト時間　→ 5 秒
  正常時送信間隔　→ 10 秒
  異常時送信間隔　→ 1 分

8.　［保存］ボタンをクリックします。

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- **IKE セッション監視のあて先 IP アドレスは、「IPsec 情報」の“対象パケット”に含まれる IP アドレスを指定してください。**
- **IKE セッション監視のあて先 IP アドレスに、常時運転している IPsec 対象の装置を指定してください。あて先 IP アドレスに相手 IKE サーバとは異なる装置を指定した場合、あて先 IP アドレスからの応答が受信できなくなります。その場合、相手 IKE サーバが生存していても IPsec/IKE SA は解放されます。そのため通信が不安定になることがあります。**

動的経路（RIP）機能と併用する場合

● 設定条件

[共通]

- RIP送信　：v1
- RIP受信　：v1
- RIP送信時加算メトリック値　：0

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon)」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

6.　［全削除］ボタンをクリックします。

「削除していいですか？」の確認画面が表示されます。

7.　［OK］ボタンをクリックします。

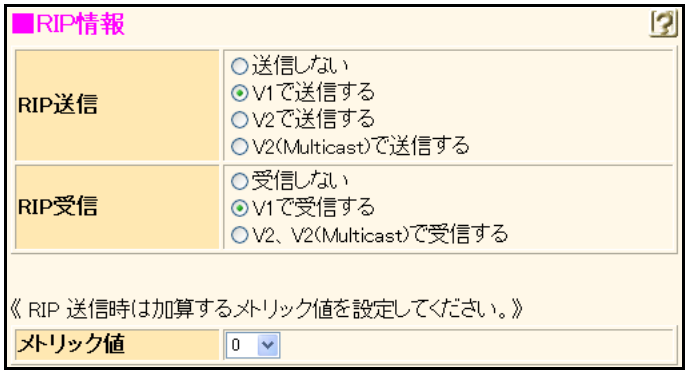
「スタティック経路情報」が削除されます。

8.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

9.　以下の項目を指定します。

- RIP送信　→V1 で送信する
- RIP受信　→V1 で受信する
- メトリック値　→0



10.　［保存］ボタンをクリックします。

11.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-shi）」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

6.　［全削除］ボタンをクリックします。

「削除していいですか？」の確認画面が表示されます。

7.　［OK］ボタンをクリックします。

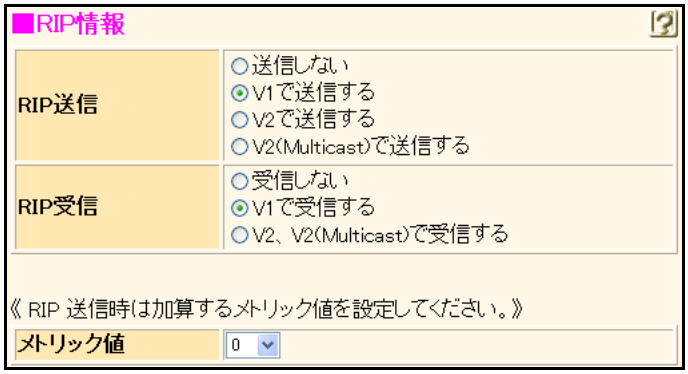
「スタティック経路情報」が削除されます。

8.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

9.　以下の項目を指定します。

- RIP送信　　→V1 で送信する
- RIP受信　　→V1 で受信する
- メトリック値　　→0



10.　［保存］ボタンをクリックします。

11.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.10 IPv4 over IPv4で固定IPアドレスでバックアップ用に使用するVPN（自動鍵交換）

適用機種　***Si-R220B,220C,370,570***

専用線側の通信パスに障害が発生した場合にISDN回線を利用し、ISDN回線側ではIPsec機能を使って自動鍵交換でVPNを構築することによって通信をバックアップする場合の設定方法を説明します。

ここでは、以下のとおり支社と本社が専用線で接続されていることを前提とします。

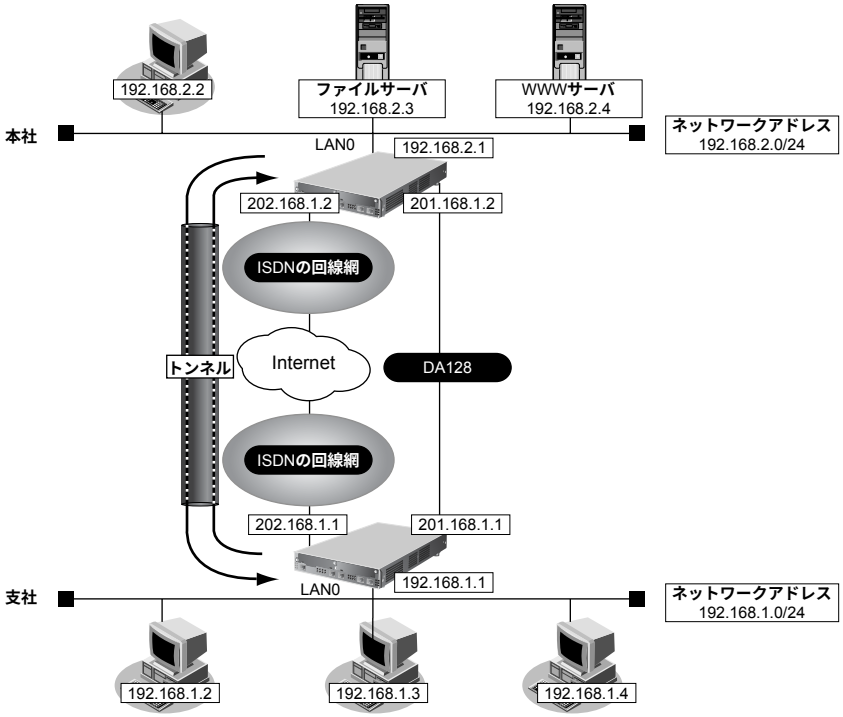
● 前提条件

[支社]

- ローカルネットワークIPアドレス　：192.168.1.1/24
- 専用線使用スロット　：SLOT0
- 専用線回線速度　：128K
- 専用線自側IPアドレス　：201.168.1.1
- ネットワーク名　：honsya
- 接続先名　：honsya

[本社]

- ローカルネットワークIPアドレス　：192.168.2.1/24
- 専用線使用スロット　：SLOT0
- 専用線回線速度　：128K
- 専用線自側IPアドレス　：201.168.1.2
- ネットワーク名　：shisya
- 接続先名　：shisya



● 設定条件

[支社]

- 接続先名　：vpn-hon

[バックアップ回線（ISDN）]

- ネットワーク名　：hon-back
- 接続先名　：hon-back
- ISDN 回線使用スロット　：SLOT1
- ISP 電話番号　：123-4567-891
- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- ISDN 自側 IP アドレス　：202.168.1.1
- ISDN 回線無通信監視　：5 分
- IPsec/IKE 区間　：202.168.1.1 - 202.168.1.2
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- 専用線（レギュラー回線）ダウン時動作　：ISDN 回線で IPsec/IKE を使用
- 接続先監視機能　：使用する
- 接続優先制御　：Initiator を優先する

[本社]

- 接続先名　：vpn-shi

[バックアップ回線（ISDN）]

- ネットワーク名　：shi-back
- 接続先名　：shi-back
- ISDN 回線使用スロット　：SLOT1
- ISP 電話番号　：123-4567-890
- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- ISDN 自側 IP アドレス　：202.168.1.2
- 常時接続　：する
- IPsec/IKE 区間　：202.168.1.2 - 202.168.1.1
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- 専用線（レギュラー回線）ダウン時動作　：ISDN 回線で IPsec/IKE を使用
- 接続先監視機能　：使用する
- 接続優先制御　：Responder を優先する

[共通]

- 鍵交換モード　：Main Mode 使用
- IPsec プトロコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc

- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768（グループ 1）

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

支社の VPN を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で専用線接続を行うネットワーク名が honsya の［修正］ボタンをクリックします。

「ネットワーク情報（honsya）」ページが表示されます。

4.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

5.　「接続先情報」で専用線接続で接続先名が honsya の［修正］ボタンをクリックします。

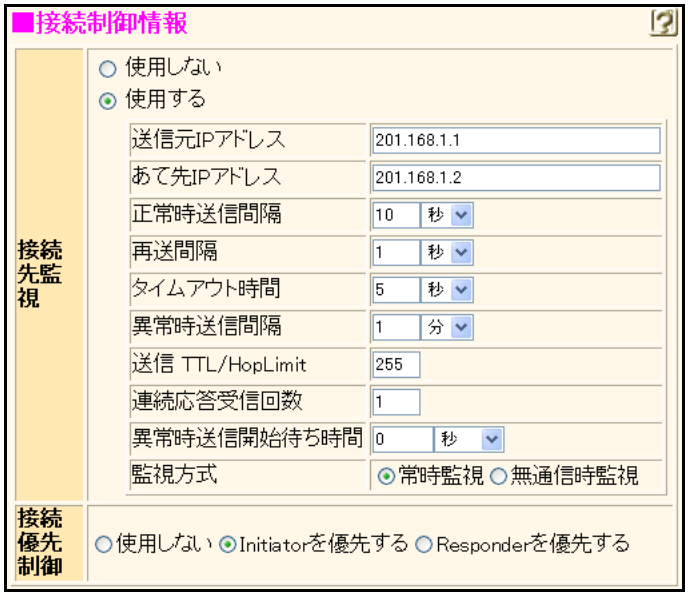
専用線接続の設定項目と「基本情報」が表示されます。

6.　専用線接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

7.　以下の項目を指定します。

- 接続先監視　→使用する
  送信元 IP アドレス　→201.168.1.1
  あて先 IP アドレス　→201.168.1.2
  正常時送信間隔　→10 秒
  再送間隔　→1 秒
  タイムアウト時間　→5 秒
  異常時送信間隔　→1 分
  接続優先制御　→Initiator を優先する



8.　［保存］ボタンをクリックします。

9.　画面上部の「ネットワーク情報（honsya)」をクリックします。

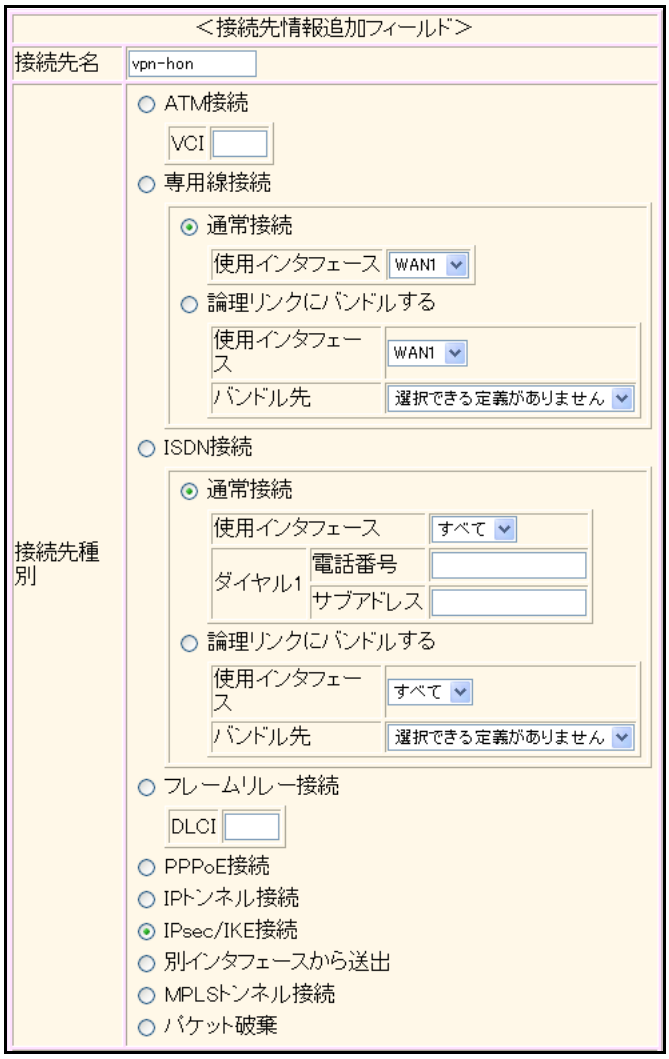
「ネットワーク情報（honsya)」ページが表示されます。

10.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

11.　以下の項目を指定します。

- 接続先名　→vpn-hon
- 接続先種別　→IPsec/IKE 接続



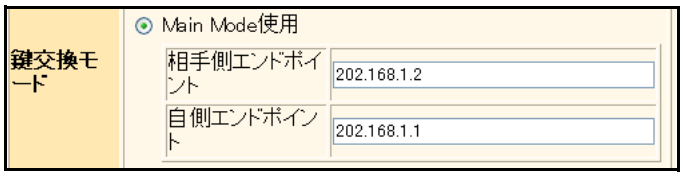
Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

12.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

13.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.1.2
  自側エンドポイント　→202.168.1.1



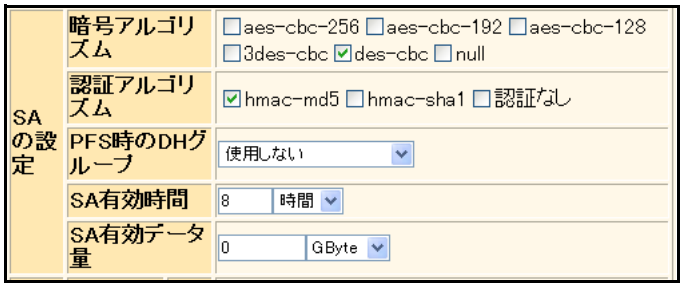
14.　［保存］ボタンをクリックします。

15.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

16.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



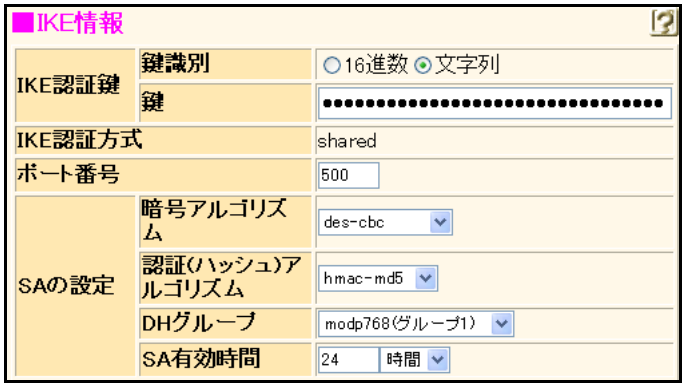
17.　［保存］ボタンをクリックします。

18.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

19.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ）



20.　［保存］ボタンをクリックします。

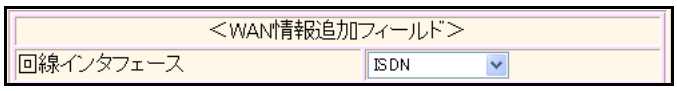
支社のバックアップ回線を設定する

21.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

22.　以下の項目を指定します。

- 回線インタフェース　→ISDN



23.　［追加］ボタンをクリックします。

「WAN1 情報（ISDN）」ページが表示されます。

24.　「基本情報」をクリックします。

「基本情報」が表示されます。

25.　以下の項目を指定します。

- ポート　→スロット 1-0

26.　［保存］ボタンをクリックします。

27.　設定メニューのルータ設定で「相手情報」をクリックします。

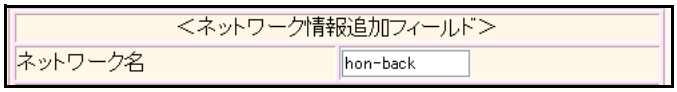
「相手情報」ページが表示されます。

28.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

29.　以下の項目を指定します。

- ネットワーク名　→hon-back



30.　［追加］ボタンをクリックします。

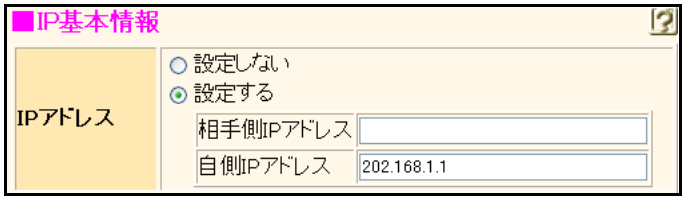
「ネットワーク情報（hon-back）」ページが表示されます。

31.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

32.　以下の項目を指定します。

- IP アドレス　→設定する
  相手側 IP アドレス　→指定しない
  自側 IP アドレス　→202.168.1.1



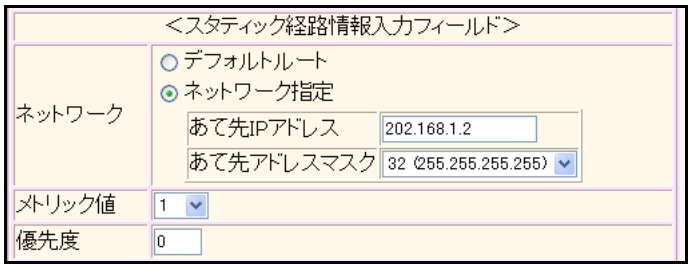
33.　［保存］ボタンをクリックします。

34.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

35.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→202.168.1.2
  あて先アドレスマスク　→32（255.255.255.255）
- メトリック値　→1
- 優先度　→0



36.　［追加］ボタンをクリックします。

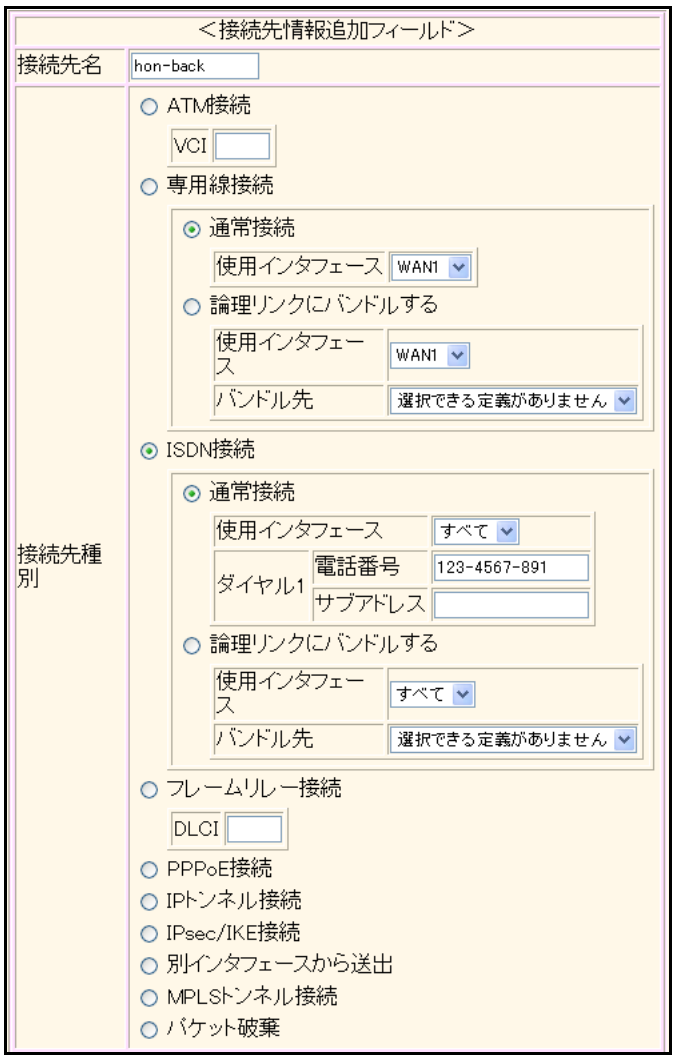
37.　「ネットワーク情報（hon-back)」で「接続先情報」をクリックします。

「接続先情報」が表示されます。

38.　以下の項目を指定します。

- 接続先名　→hon-back
- 接続先種別　→ISDN 接続
  →通常接続

  ダイヤル 1
  電話番号　→123-4567-891



Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

39.　［追加］ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

40.　以下の項目を指定します。

- 使用インタフェース　→WAN1

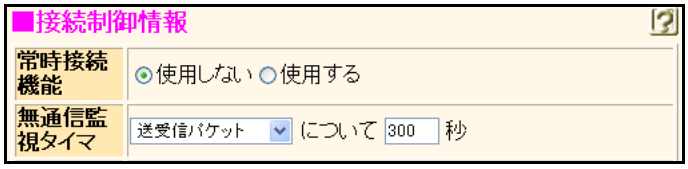
41.　［保存］ボタンをクリックします。

42.　ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

43.　以下の項目を指定します。

- 常時接続機能　→使用しない
- 無通信監視タイマ　→送受信パケットについて 300 秒



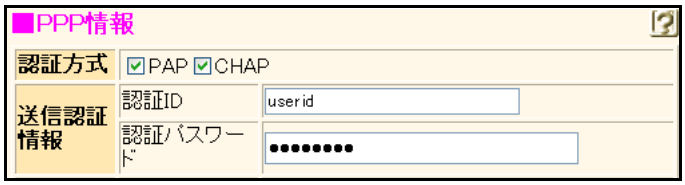
44.　［保存］ボタンをクリックします。

45.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

46.　以下の項目を指定します。

- 認証方式　→ PAP、CHAP
- 送信認証情報
  認証 ID　→ userid
  認証パスワード　→ userpass



47.　［保存］ボタンをクリックします。

48.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

本社の VPN を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で専用線接続を行うネットワーク名が shisya の［修正］ボタンをクリックします。

「ネットワーク情報（shisya）」ページが表示されます。

4.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

5.　「接続先情報」で専用線接続で接続先名が shisya の［修正］ボタンをクリックします。

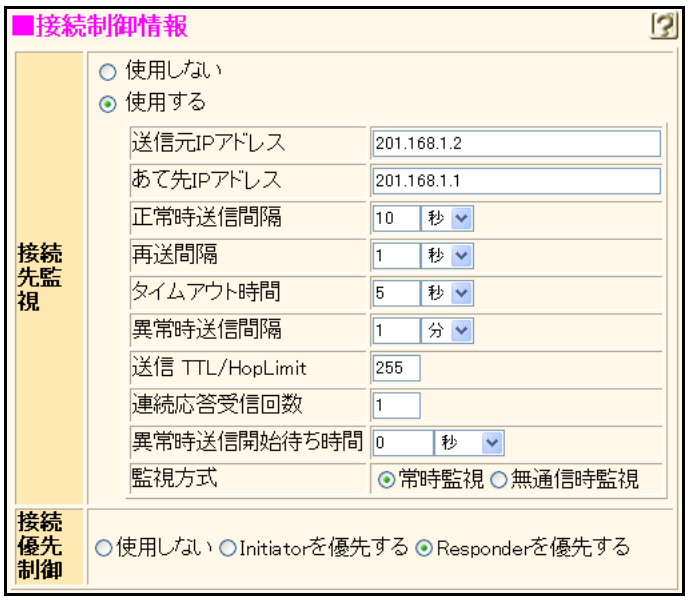
専用線接続の設定項目と「基本情報」が表示されます。

6.　専用線接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

7.　以下の項目を指定します。

- 接続先監視　→使用する
  送信元 IP アドレス　→ 201.168.1.2
  あて先 IP アドレス　→ 201.168.1.1
  正常時送信間隔　→ 10 秒
  再送間隔　→ 1 秒
  タイムアウト時間　→ 5 秒
  異常時送信間隔　→ 1 分
  接続優先制御　→ Responder を優先する



8.　［保存］ボタンをクリックします。

9.　画面上部の「ネットワーク情報（shisya）」をクリックします。

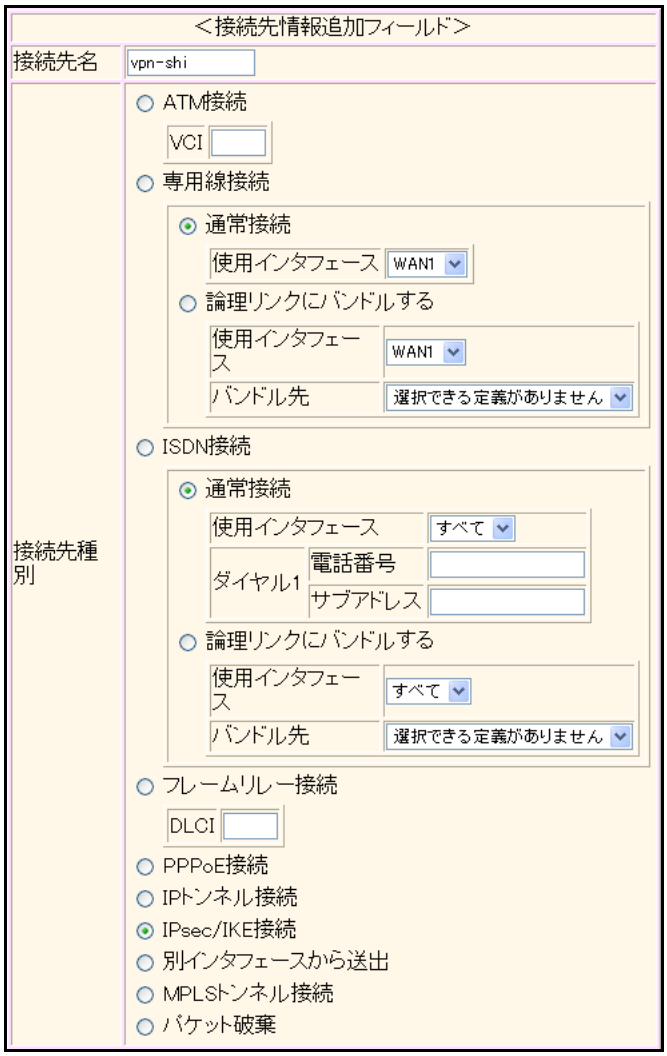
「ネットワーク情報（shisya）」ページが表示されます。

10.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

11.　以下の項目を指定します。

- 接続先名　→vpn-shi
- 接続先種別　→IPsec/IKE 接続



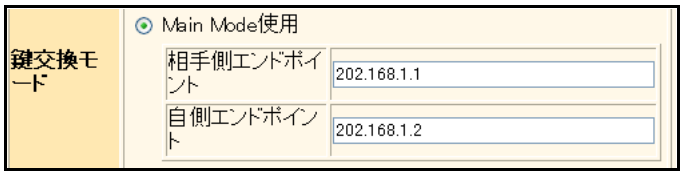
Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

12.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

13.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.1.1
  自側エンドポイント　→202.168.1.2



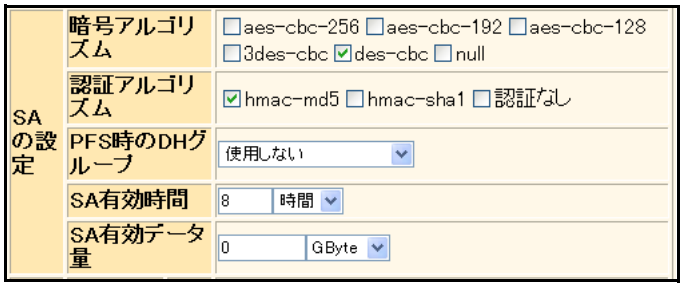
14.　［保存］ボタンをクリックします。

15.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

16.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



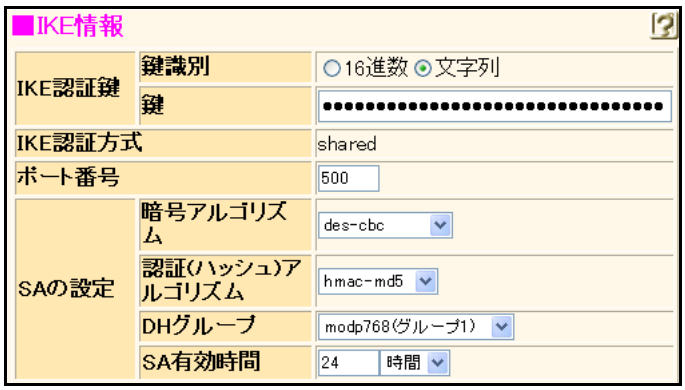
17.　［保存］ボタンをクリックします。

18.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

19.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



20.　［保存］ボタンをクリックします。

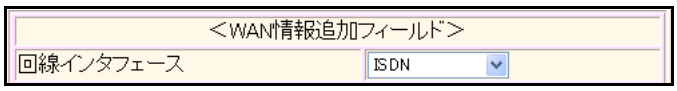
本社のバックアップ回線を設定する

21.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

22.　以下の項目を指定します。

- 回線インタフェース　→ISDN



23.　［追加］ボタンをクリックします。

「WAN1 情報（ISDN）」ページが表示されます。

24.　「基本情報」をクリックします。

「基本情報」が表示されます。

25.　以下の項目を指定します。

- ポート　→スロット 1-0

26.　［保存］ボタンをクリックします。

27.　設定メニューのルータ設定で「相手情報」をクリックします。

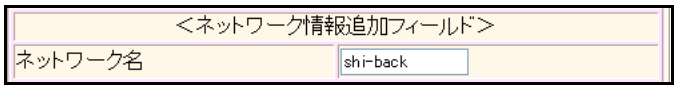
「相手情報」ページが表示されます。

28.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

29.　以下の項目を指定します。

- ネットワーク名　→shi-back



30.　［追加］ボタンをクリックします。

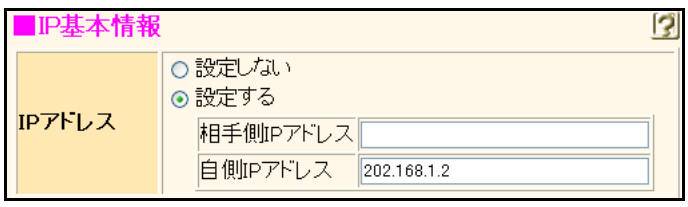
「ネットワーク情報（shi-back）」ページが表示されます。

31.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

32.　以下の項目を指定します。

- IP アドレス　→設定する
  相手側 IP アドレス　→指定しない
  自側 IP アドレス　→202.168.1.2



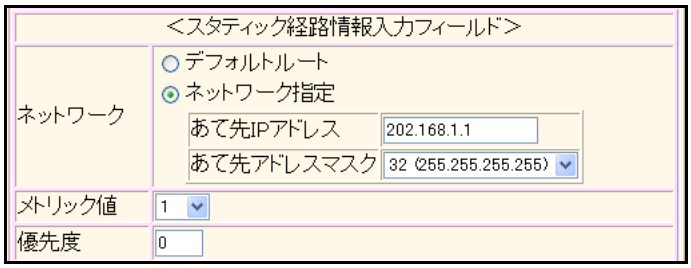
33.　［保存］ボタンをクリックします。

34.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

35.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→202.168.1.1
  あて先アドレスマスク　→32（255.255.255.255）
- メトリック値　→1
- 優先度　→0



36.　［追加］ボタンをクリックします。

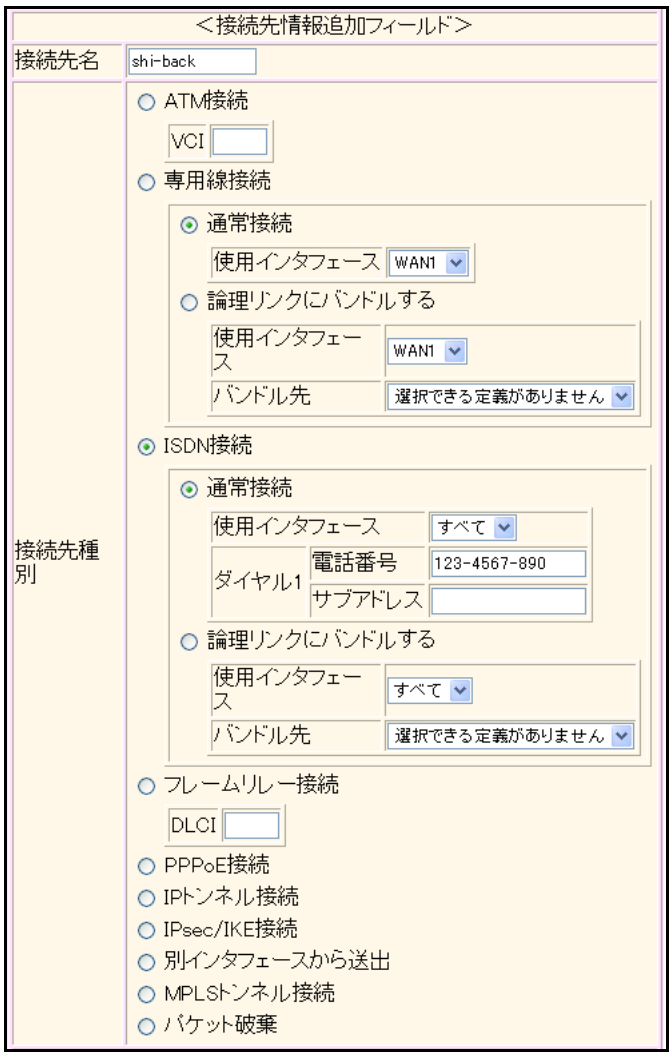
37.　「ネットワーク情報（shi-back）」で「接続先情報」をクリックします。

「接続先情報」が表示されます。

38.　以下の項目を指定します。

- 接続先名　→shi-back
- 接続先種別　→ISDN 接続
  →通常接続

  ダイヤル 1
  電話番号　→123-4567-890



Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

39.　［追加］ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

40.　以下の項目を指定します。

- 使用インタフェース　→WAN1

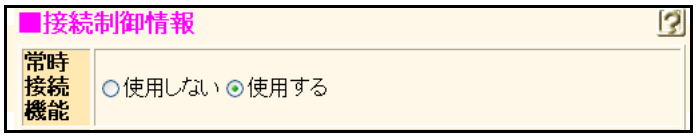
41.　［保存］ボタンをクリックします。

42.　ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

43.　以下の項目を指定します。

- 常時接続機能　→使用する



補足「常時接続機能」で“使用する”を選択すると、表示される「接続制御情報」画面が変わります。

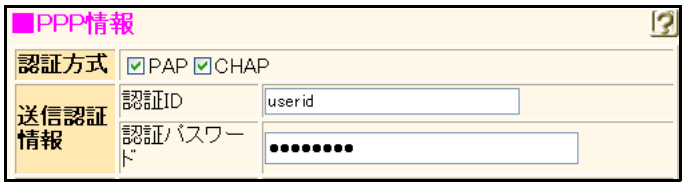
44.　［保存］ボタンをクリックします。

45.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

46.　以下の項目を指定します。

- 認証方式　→PAP、CHAP
- 送信認証情報
  認証 ID　→userid
  認証パスワード　→userpass



47.　［保存］ボタンをクリックします。

48.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.11 テンプレート着信機能（AAA 認証）を使用した固定 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

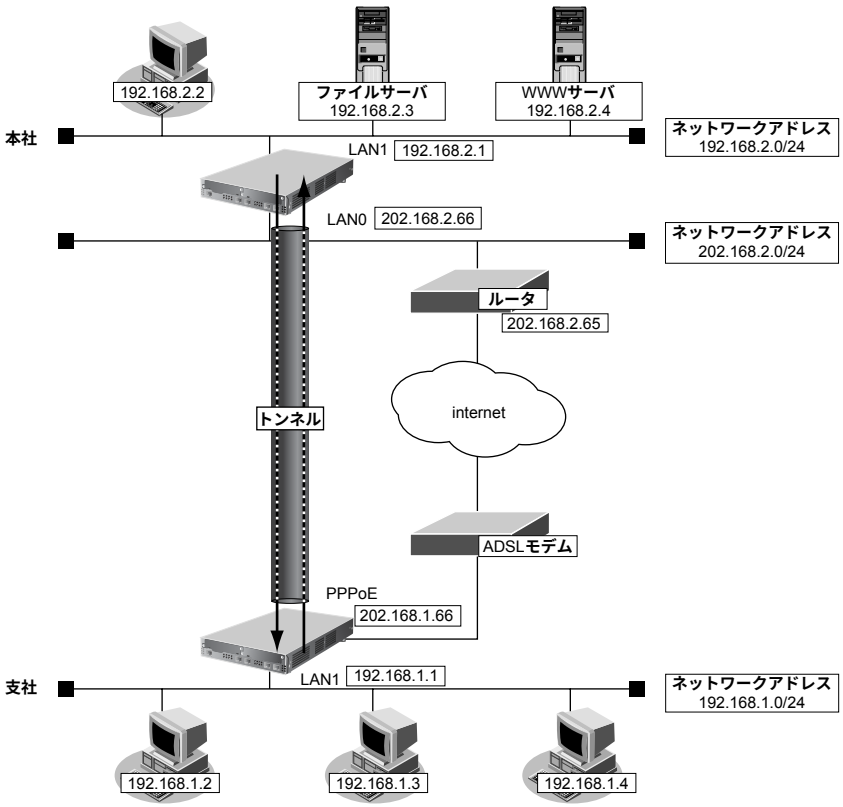
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- **テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

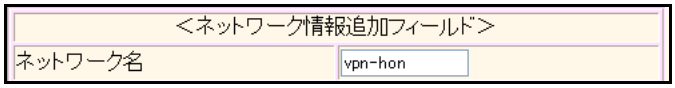
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

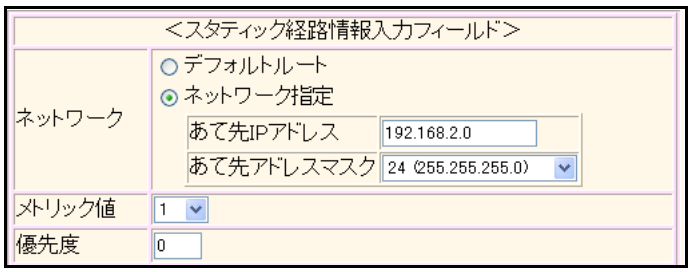
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



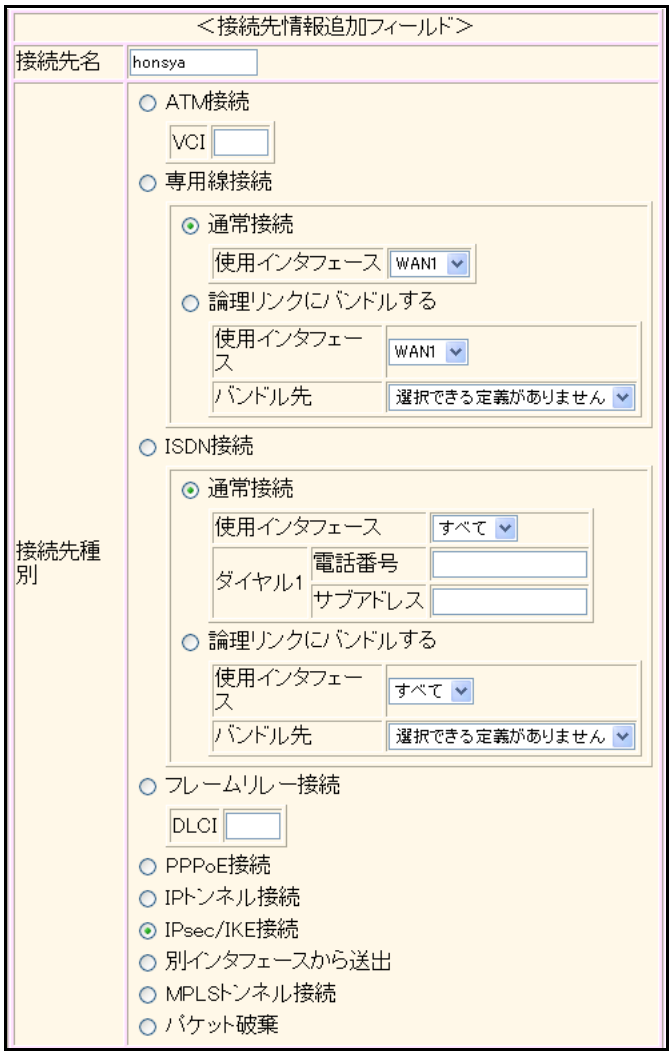
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



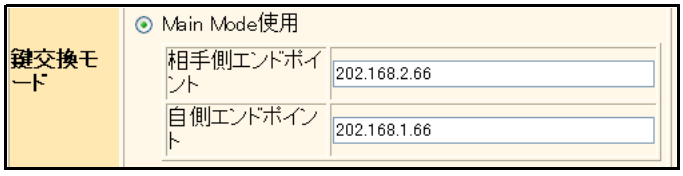
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66



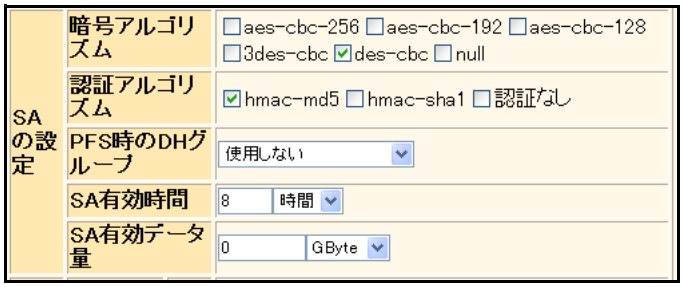
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



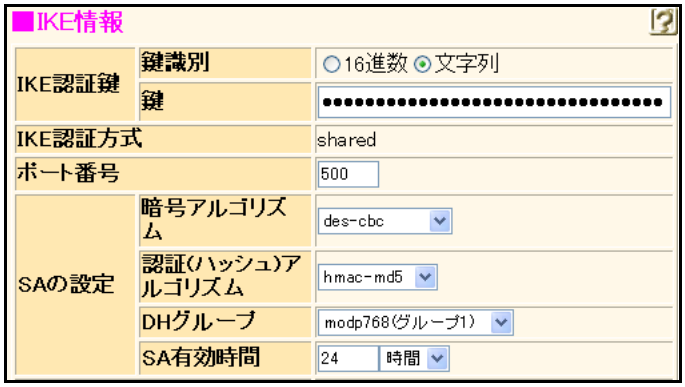
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

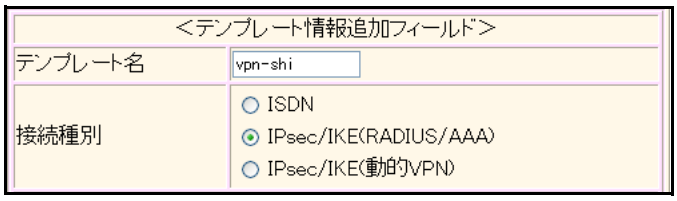
本社を設定する（Responder）

1.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

2.　以下の項目を指定します。

- テンプレート名　→vpn-shi
- 接続種別　→IPsec/IKE（RADIUS/AAA）



機種により、接続種別の表示が上記の画面とは異なります。

3.　［追加］ボタンをクリックします。

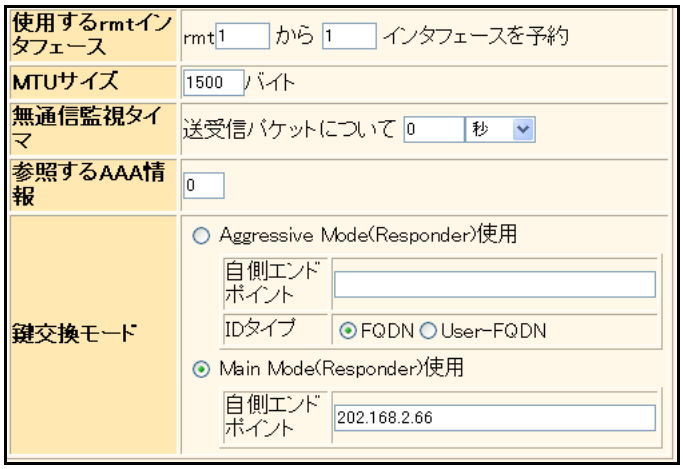
「テンプレート情報（vpn-shi)」と設定項目が表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt1 から 1 インタフェースを予約
- 参照する AAA 情報　→0
- 鍵交換モード　→Main Mode（Responder）使用
  自側エンドポイント　→202.168.2.66



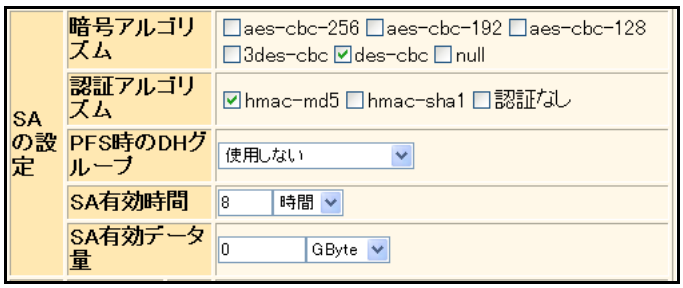
6.　［保存］ボタンをクリックします。

7.　テンプレート情報（vpn-shi）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

8.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



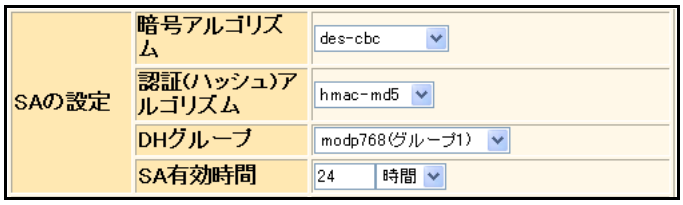
9.　［保存］ボタンをクリックします。

10.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

11.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「AAA 情報」をクリックします。

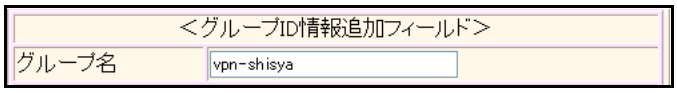
「AAA 情報」ページが表示されます。

14.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

15.　以下の項目を指定します。

- グループ名　→ vpn-shisya



16.　［追加］ボタンをクリックします。

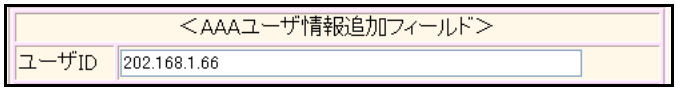
「グループ ID 情報（0）」と設定項目が表示されます。

17.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

18.　以下の項目を指定します。

- ユーザ ID　→202.168.1.66



19.　［追加］ボタンをクリックします。

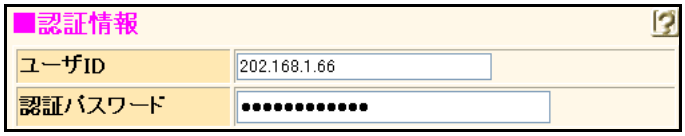
「AAA ユーザ情報（0）」と設定項目が表示されます。

20.　「認証情報」をクリックします。

「認証情報」が表示されます。

21.　以下の項目を指定します。

- ユーザ ID　→202.168.1.66
- 認証パスワード　→202.168.1.66



22.　［保存］ボタンをクリックします。

23.　AAA ユーザ情報（0）の設定項目の「IP 関連」をクリックします。

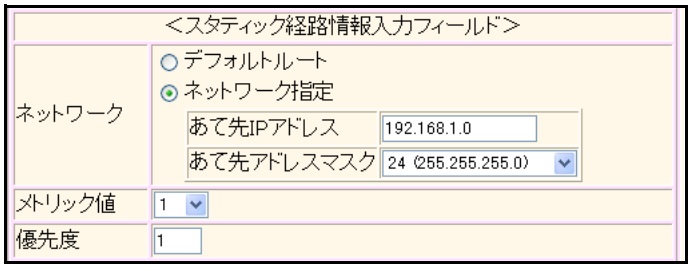
IP 関連の設定項目と「IP 基本情報」が表示されます。

24.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

25.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→1



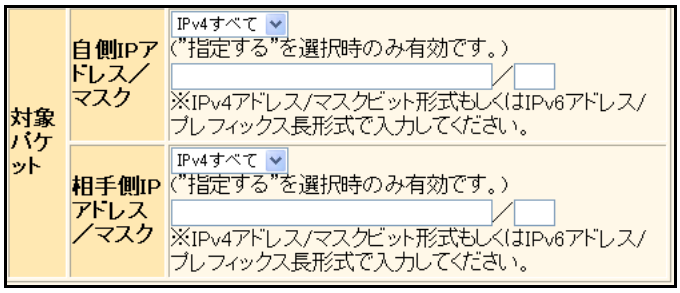
26.　［追加］ボタンをクリックします。

27.　AAA ユーザ情報（0）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

28.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→IPv4 すべて



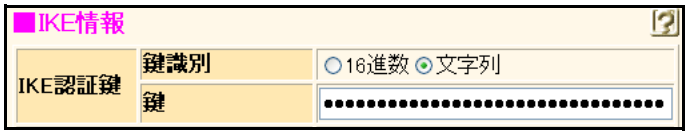
29.　［保存］ボタンをクリックします。

30.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

31.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890



32.　［保存］ボタンをクリックします。

33.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.12 テンプレート着信機能（AAA 認証）を使用した可変 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

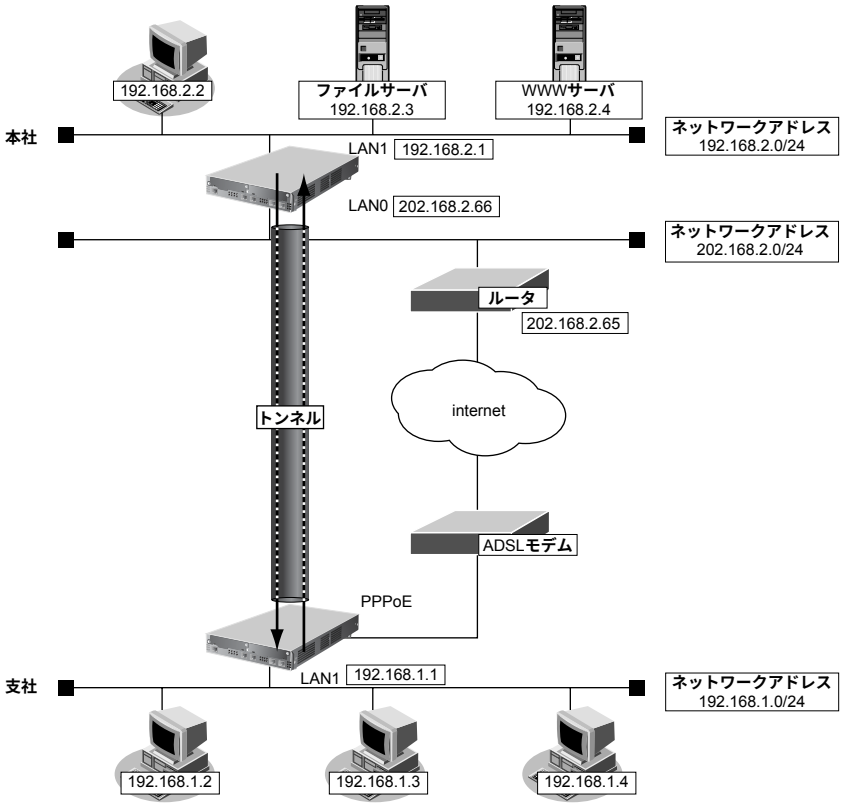
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 ー 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 ー 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

こんな事に気をつけて

- **テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

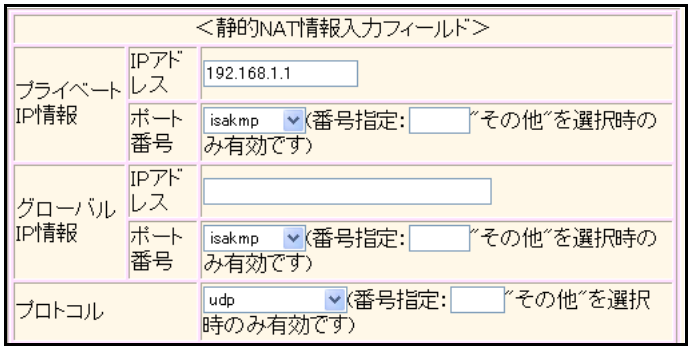
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6. ～ 7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

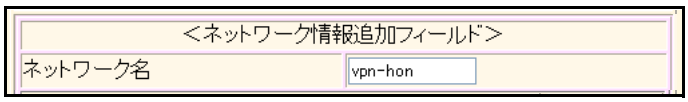
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　　→vpn-hon



12.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

13.　「IP 関連」をクリックします。

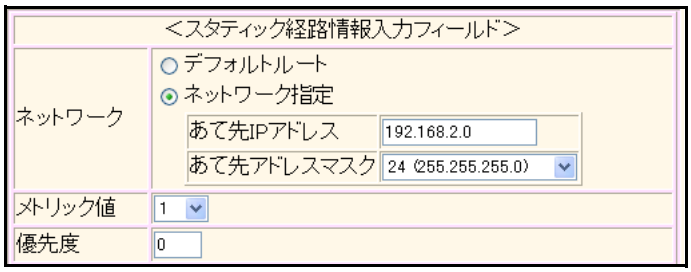
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　　→ネットワーク指定
  あて先 IP アドレス　　→192.168.2.0
  あて先アドレスマスク　　→24（255.255.255.0）
- メトリック値　　→1
- 優先度　　→0



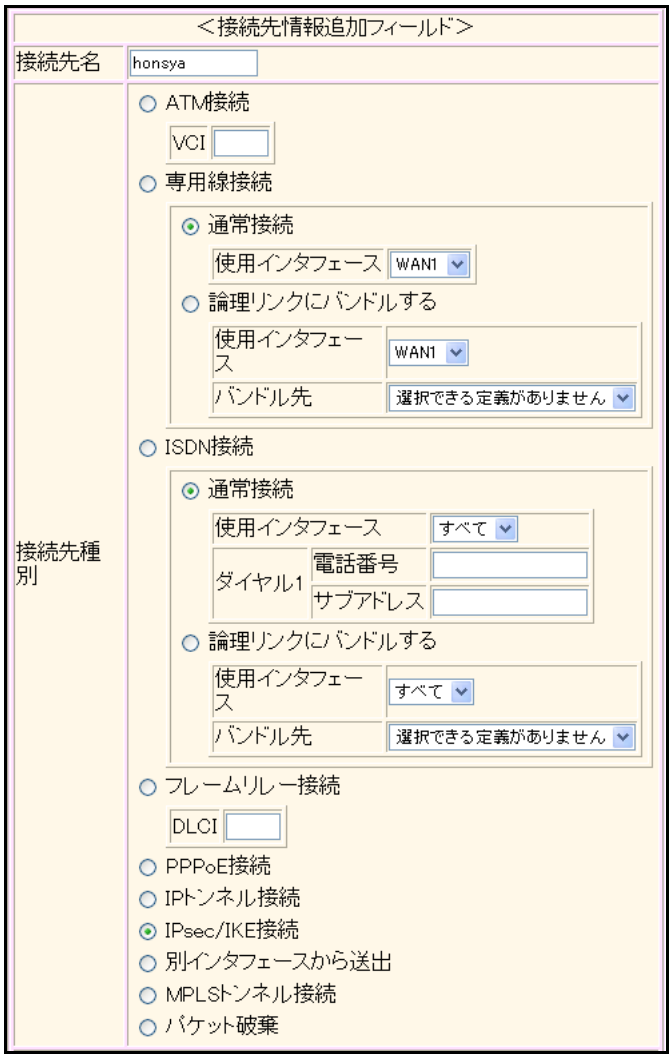
16.　［追加］ボタンをクリックします。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



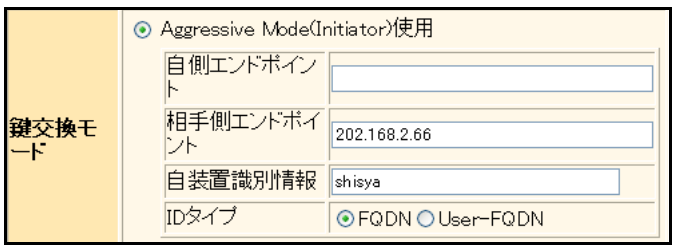
機種により、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisya



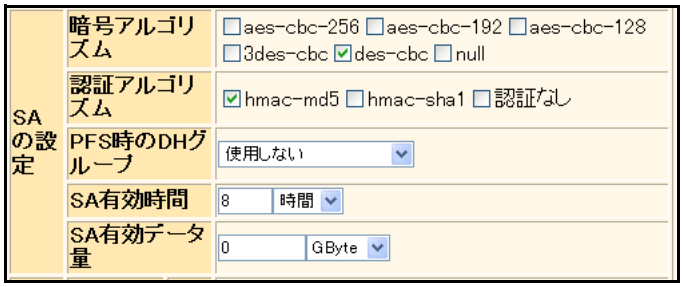
21.　［保存］ボタンをクリックします。

22.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

23.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



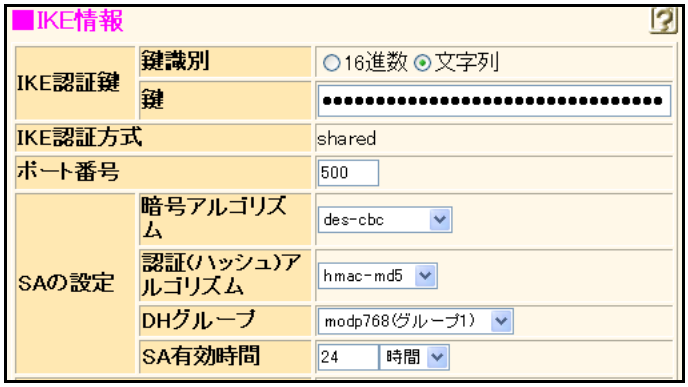
24.　［保存］ボタンをクリックします。

25.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

26.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



27.　［保存］ボタンをクリックします。

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

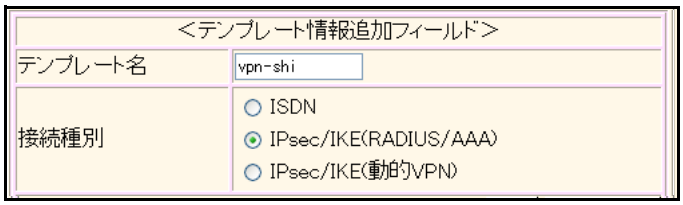
本社を設定する（Responder）

1.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

2.　以下の項目を指定します。

- テンプレート名　→vpn-shi
- 接続種別　→IPsec/IKE（RADIUS/AAA）



機種により、接続種別の表示が上記の画面とは異なります。

3.　［追加］ボタンをクリックします。

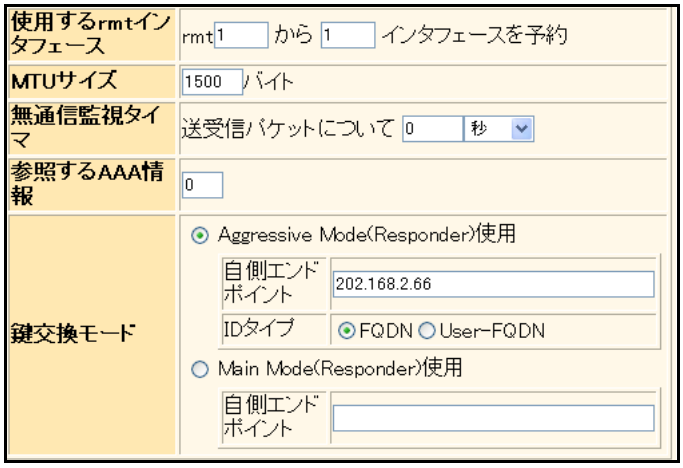
「テンプレート情報（vpn-shi)」と設定項目が表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt1 から 1 インタフェースを予約
- 参照する AAA 情報　→0
- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  ID タイプ　→FQDN



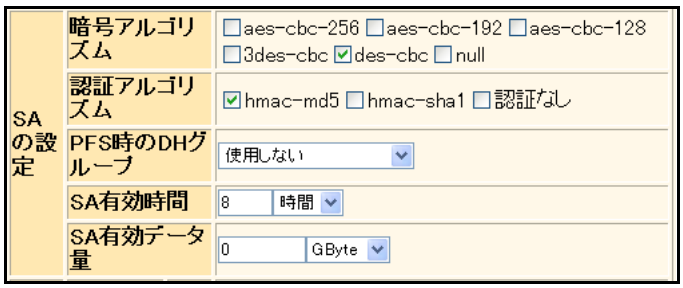
6.　［保存］ボタンをクリックします。

7.　テンプレート情報（vpn-shi）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

8.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



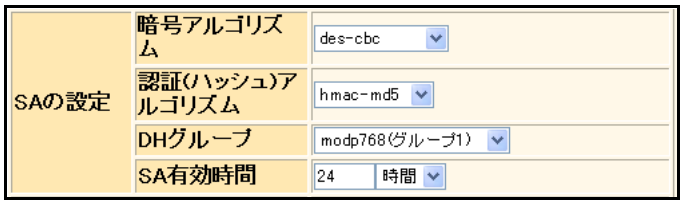
9.　［保存］ボタンをクリックします。

10.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

11.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「AAA 情報」をクリックします。

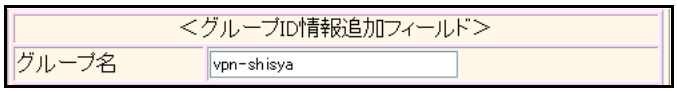
「AAA 情報」ページが表示されます。

14.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

15.　以下の項目を指定します。

- グループ名　→ vpn-shisya



16.　［追加］ボタンをクリックします。

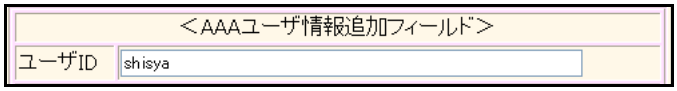
「グループ ID 情報（0）」と設定項目が表示されます。

17.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

18.　以下の項目を指定します。

- ユーザ ID　→shisya



19.　［追加］ボタンをクリックします。

「AAA ユーザ情報（0）」と設定項目が表示されます。

20.　「認証情報」をクリックします。

「認証情報」が表示されます。

21.　以下の項目を指定します。

- ユーザ ID　→shisya
- 認証パスワード　→shisya

22.　［保存］ボタンをクリックします。

23.　AAA ユーザ情報（0）の設定項目の「IP 関連」をクリックします。

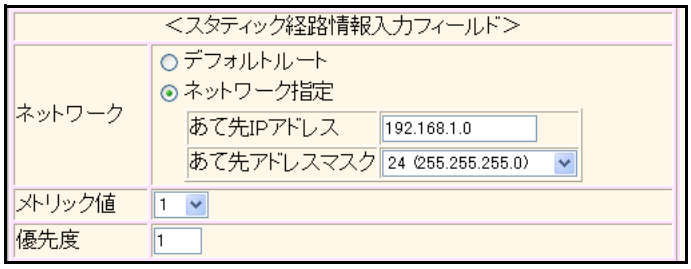
IP 関連の設定項目と「IP 基本情報」が表示されます。

24.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

25.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→1



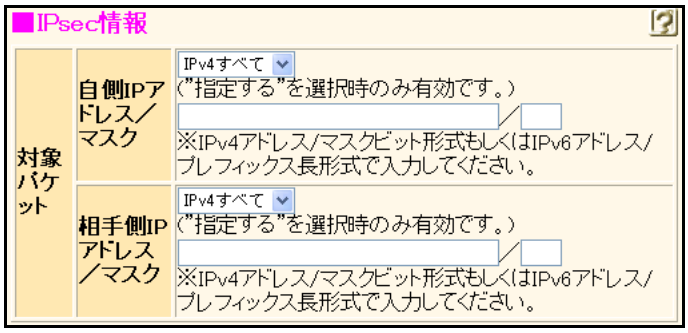
26.　［追加］ボタンをクリックします。

27.　AAA ユーザ情報（0）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

28.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　　→IPv4 すべて
  相手側 IP アドレス／マスク　　→IPv4 すべて



29.　［保存］ボタンをクリックします。

30.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

31.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　　→文字列
  鍵　　→abcdefghijklmnopqrstuvwxyz1234567890

32.　［保存］ボタンをクリックします。

33.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.13 テンプレート着信機能（RADIUS 認証）を使用した固定 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

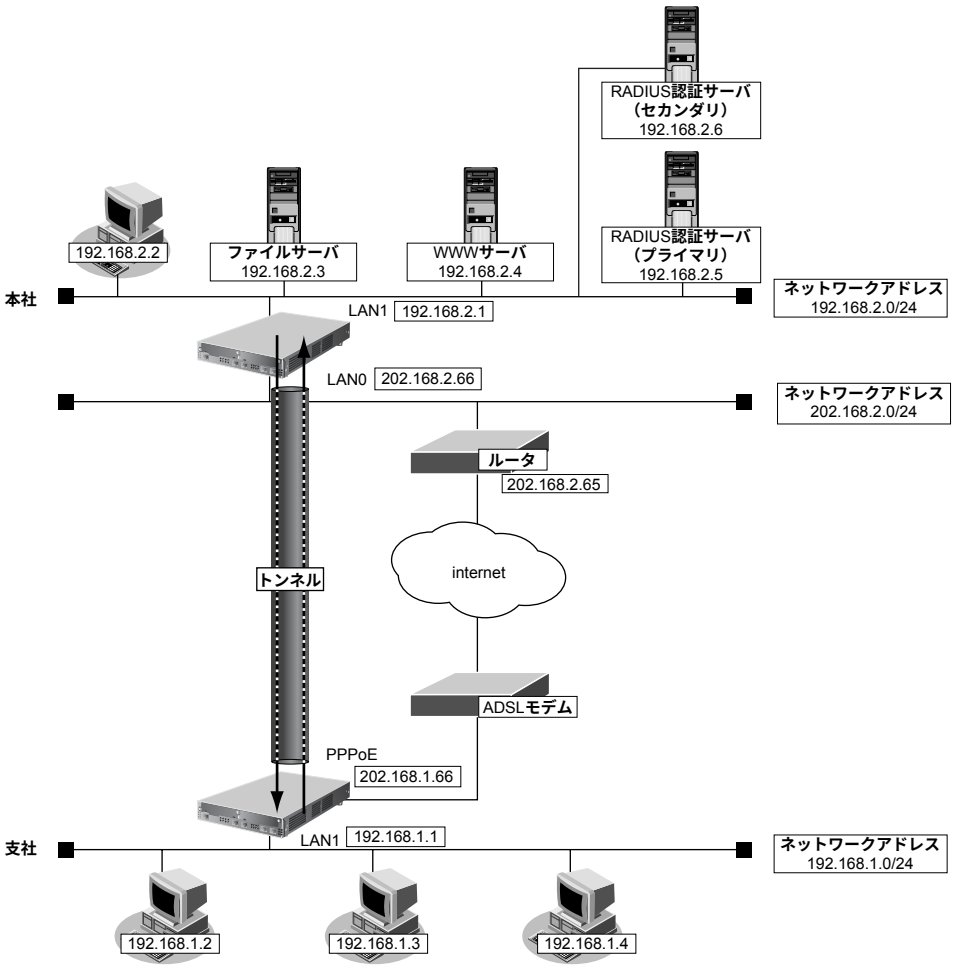
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.1.66/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：202.168.1.66 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 202.168.1.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス　：クライアント機能
  ：認証、アカウンティング
- 自側認証 IP アドレス　：192.168.2.1
- 自側アカウンティング IP アドレス　：192.168.2.1
- 認証情報 1（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0
- 認証情報 2（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100
- アカウンティング情報 1（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0
- アカウンティング情報 2（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100

[共通]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5

- IKE DH グループ　：modp768

[RADIUS サーバに登録する情報（プライマリ、セカンダリ共通)]

- 認証ユーザ ID　：202.168.1.66
- 認証ユーザパスワード　：202.168.1.66
- IPsec 対象範囲　：any4 any4
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IPv4 スタティック経路情報　：192.168.1.0/24

こんな事に気をつけて

- **テンプレート着信機能（RADIUS 認証）を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

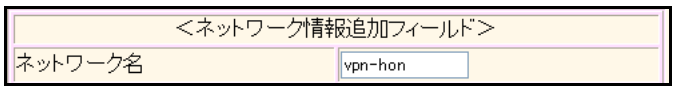
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon)」ページが表示されます。

5.　「IP 関連」をクリックします。

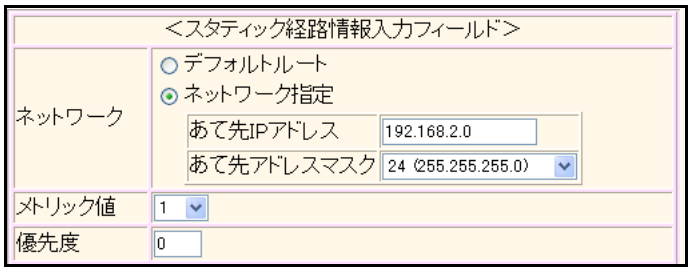
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



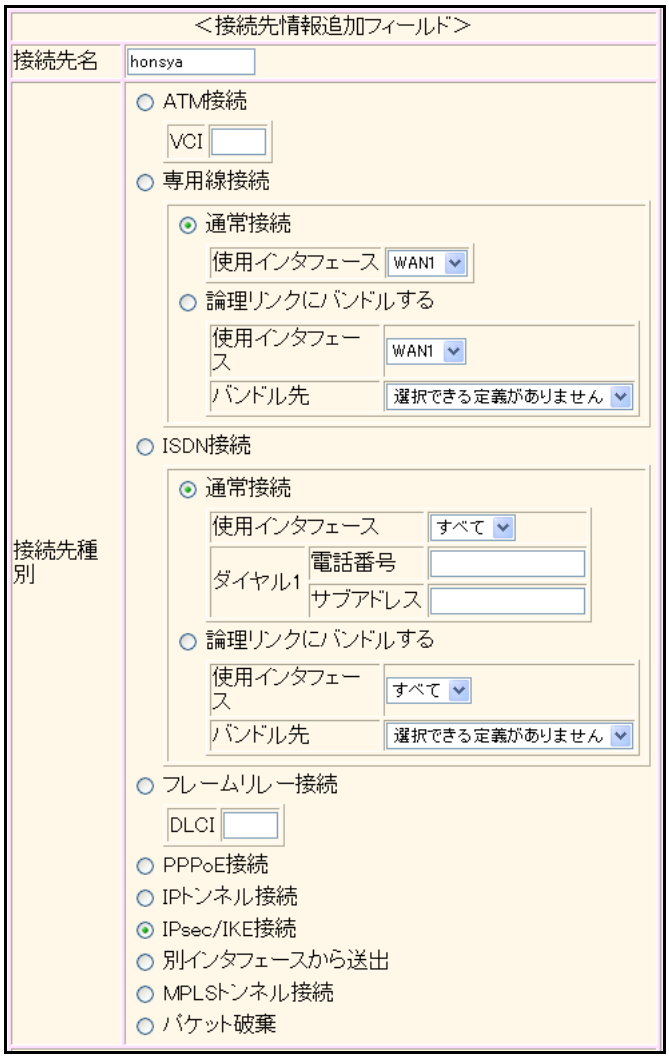
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



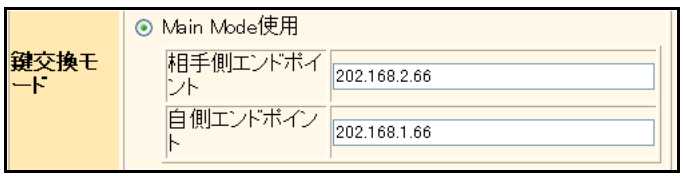
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→202.168.2.66
  自側エンドポイント　→202.168.1.66



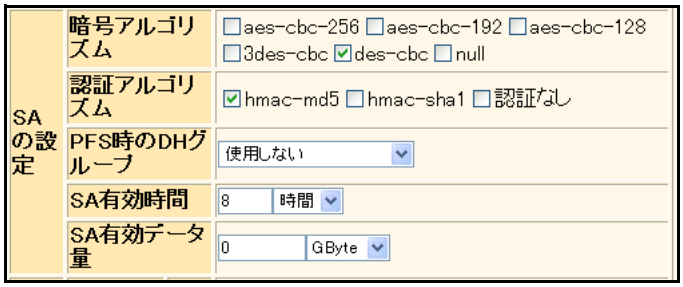
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



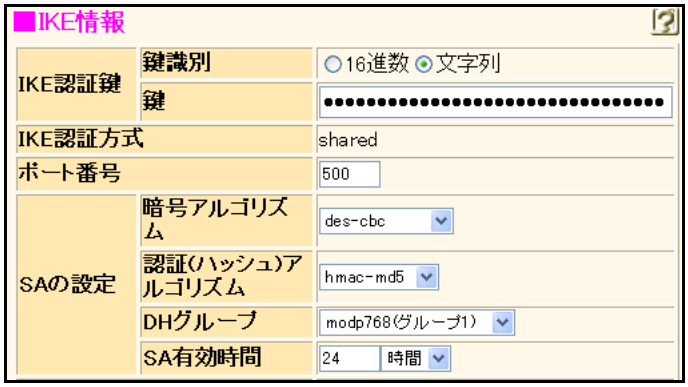
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

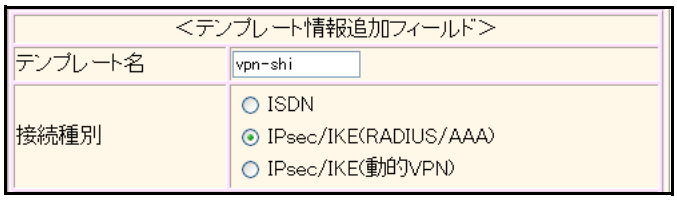
本社を設定する（Responder）

1.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

2.　以下の項目を指定します。

- テンプレート名　→vpn-shi
- 接続種別　→IPsec/IKE（RADIUS/AAA）



機種により、接続種別の表示が上記の画面とは異なります。

3.　［追加］ボタンをクリックします。

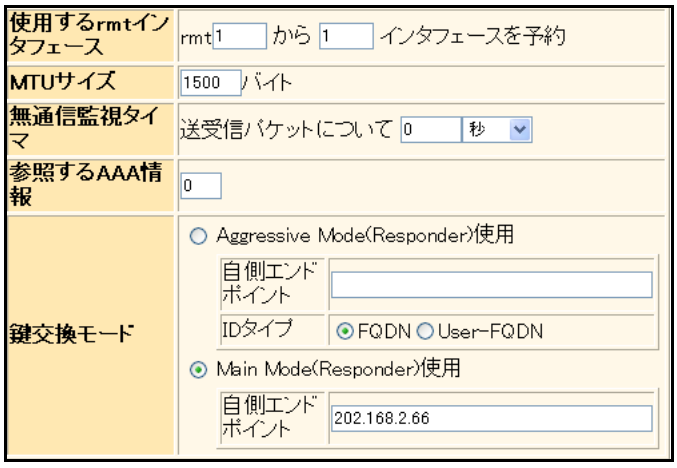
「テンプレート情報（vpn-shi)」と設定項目が表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt1 から 1 インタフェースを予約
- 参照する AAA 情報　→0
- 鍵交換モード　→Main Mode（Responder）使用
  自側エンドポイント　→202.168.2.66



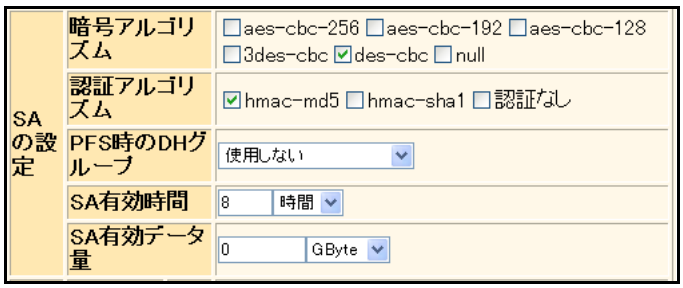
6.　［保存］ボタンをクリックします。

7.　テンプレート情報（vpn-shi）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

8.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



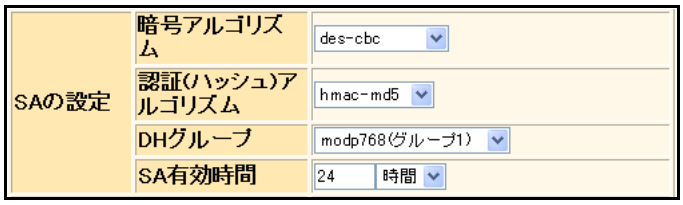
9.　［保存］ボタンをクリックします。

10.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

11.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「AAA 情報」をクリックします。

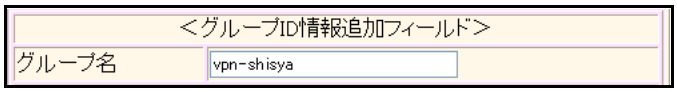
「AAA 情報」ページが表示されます。

14.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

15.　以下の項目を指定します。

- グループ名　→ vpn-shisya



16.　［追加］ボタンをクリックします。

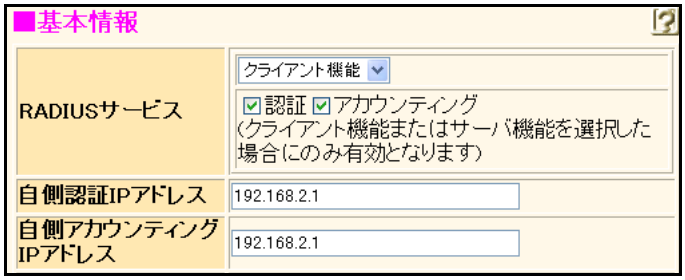
「グループ ID 情報（0）」と設定項目が表示されます。

17.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

18.　以下の項目を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックする
- 自側認証 IP アドレス　→192.168.2.1
- 自側アカウンティング IP アドレス　→192.168.2.1



19.　［保存］ボタンをクリックします。

20.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」ページが表示されます。

21.　認証情報 1 の［修正］ボタンをクリックします。

22.　以下の項目を指定します。

- 認証情報 1
  共有鍵　→192.168.2.1
  サーバ IP アドレス　→192.168.2.5
  復旧待機時間　→30 分
  優先度　→0

23.　認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

24.　認証情報 2 の［修正］ボタンをクリックします。

25.　以下の項目を指定します。

- 認証情報 2

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.2.6
  復旧待機時間　→ 30 分
  優先度　→ 100

26.　認証情報 2 の［保存］ボタンをクリックします。

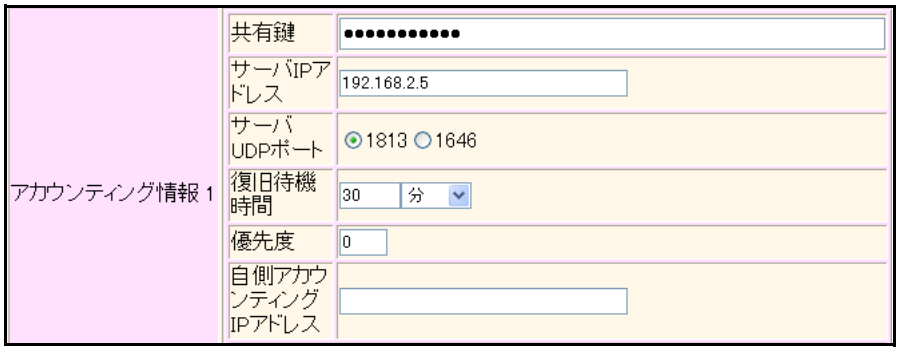
「サーバ情報（クライアント機能）」に戻ります。

27.　アカウンティング情報 1 の［修正］ボタンをクリックします。

28.　以下の項目を指定します。

- アカウンティング情報 1

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.2.5
  復旧待機時間　→ 30 分
  優先度　→ 0



29.　アカウンティング情報 1 の［保存］ボタンをクリックします。

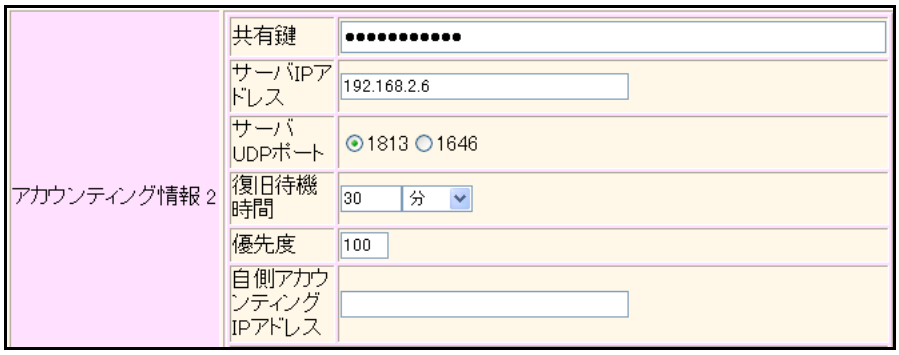
「サーバ情報（クライアント機能）」に戻ります。

30.　アカウンティング情報 2 の［修正］ボタンをクリックします。

31.　以下の項目を指定します。

- アカウンティング情報 2

  共有鍵　　→ 192.168.2.1
  サーバ IP アドレス　　→ 192.168.2.6
  復旧待機時間　　→ 30 分
  優先度　　→ 100



32.　アカウンティング情報 2 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

33.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.14 テンプレート着信機能（RADIUS 認証）を使用した可変 IP アドレスでの VPN

適用機種　全機種

IPsec 機能とテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

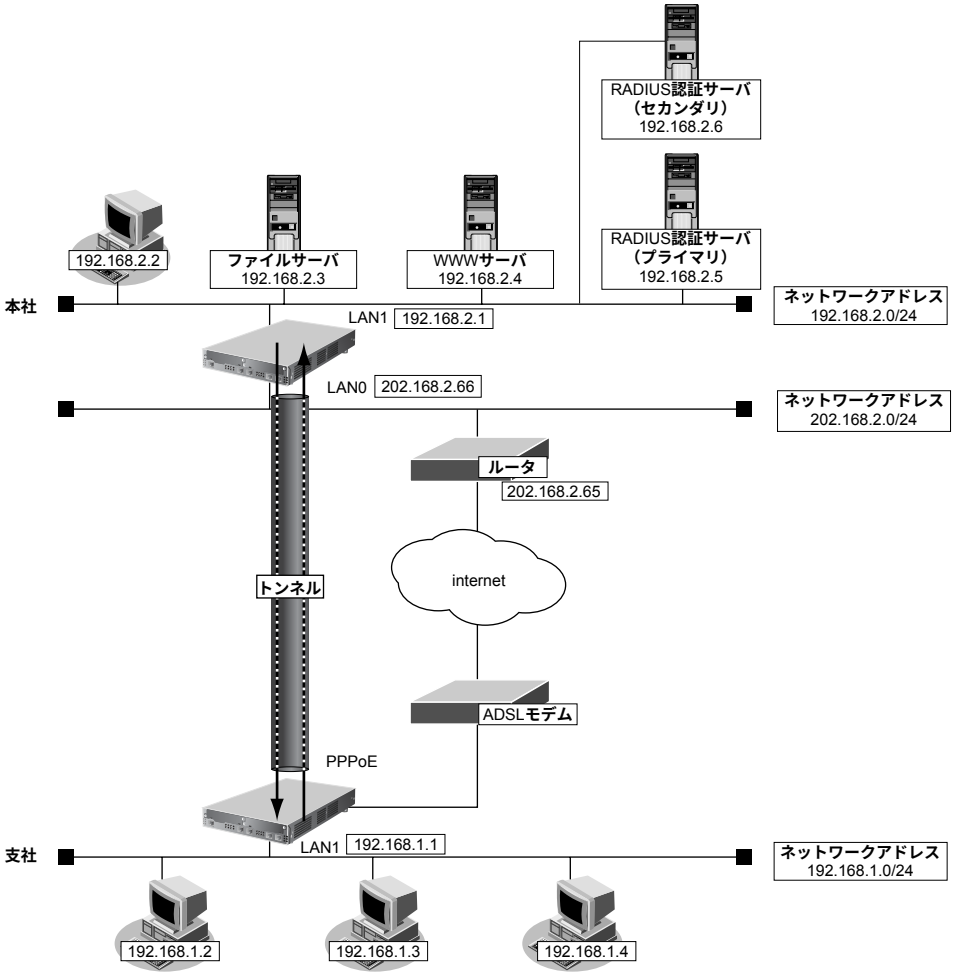
● 前提条件

[支社（PPPoE 常時接続）]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス
  ：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス　：クライアント機能
  ：認証、アカウンティング
- 自側認証 IP アドレス　：192.168.2.1
- 自側アカウンティング IP アドレス　：192.168.2.1
- 認証情報 1（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0
- 認証情報 2（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100
- アカウンティング情報 1（プライマリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.5
  復旧待機時間　：30 分
  優先度　：0
- アカウンティング情報 2（セカンダリ）
  共有鍵　：192.168.2.1
  サーバ IP アドレス　：192.168.2.6
  復旧待機時間　：30 分
  優先度　：100

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）

- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

[RADIUS サーバに登録する情報（プライマリ、セカンダリ共通)]

- 認証ユーザ ID　：shisya
- 認証ユーザパスワード　：shisya
- IPsec 対象範囲　：any4 any4
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IPv4 スタティック経路情報　：192.168.1.0/24

こんな事に気をつけて

- **テンプレート着信機能（RADIUS 認証）を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

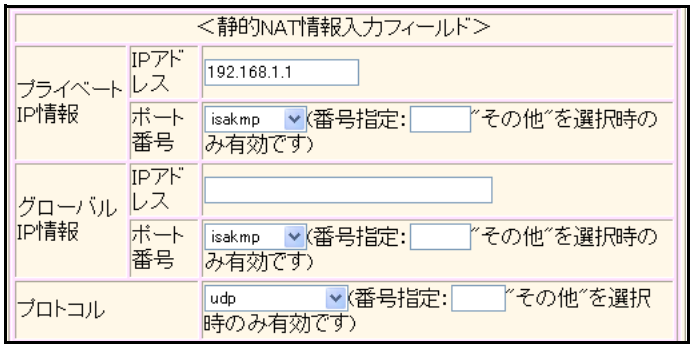
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6.～7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

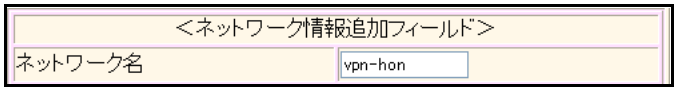
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→ vpn-hon



12.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

13.　「IP 関連」をクリックします。

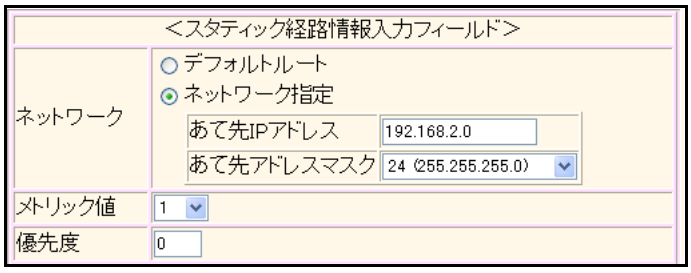
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



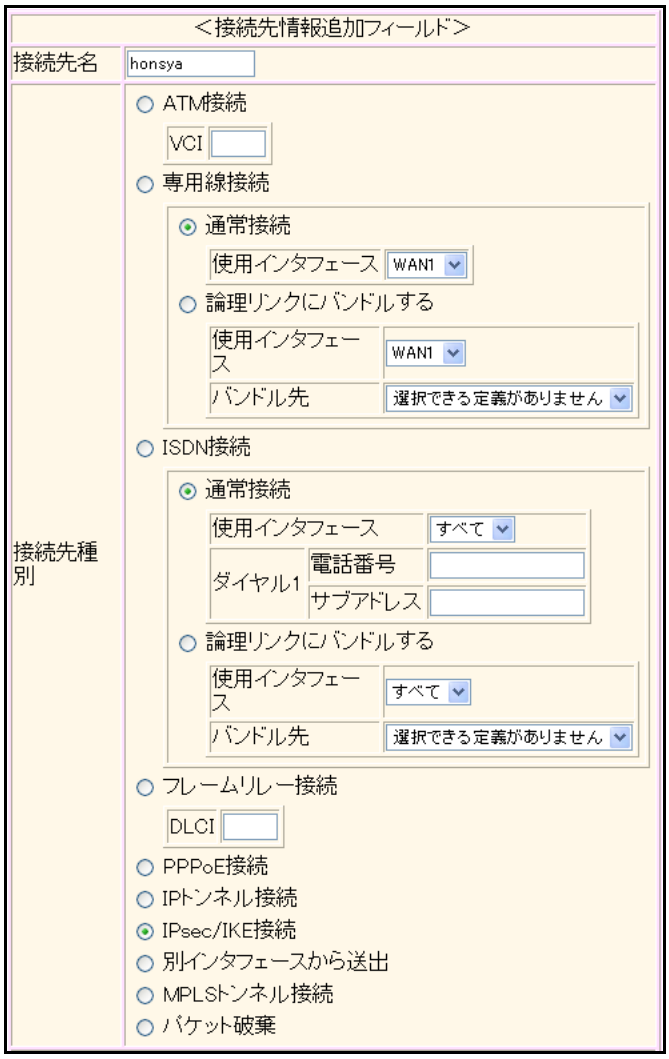
16.　［追加］ボタンをクリックします。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



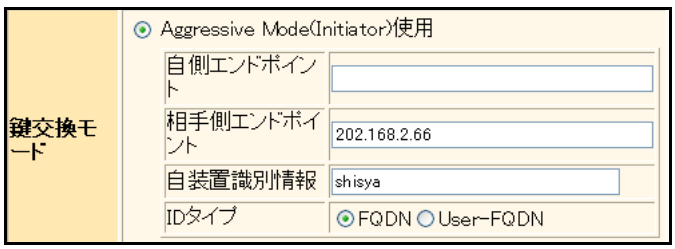
機種により、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisya



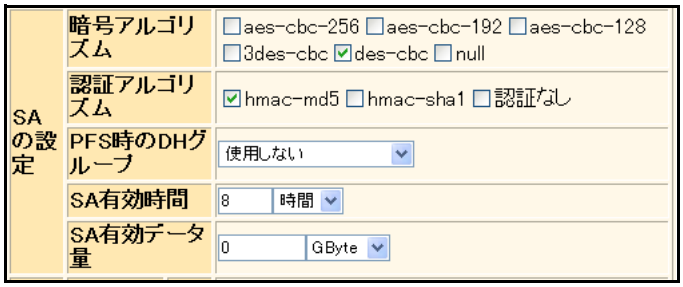
21.　［保存］ボタンをクリックします。

22.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

23.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



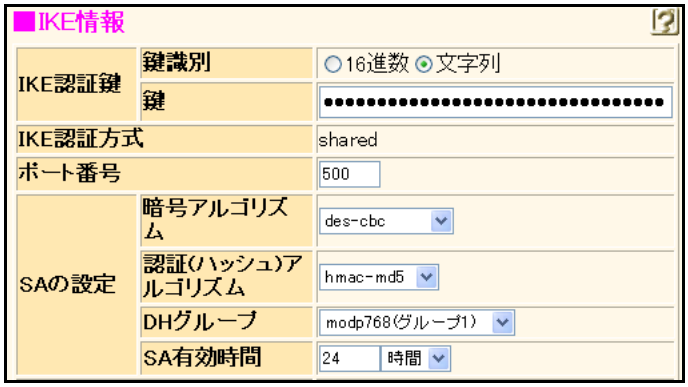
24.　［保存］ボタンをクリックします。

25.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

26.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



27.　［保存］ボタンをクリックします。

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

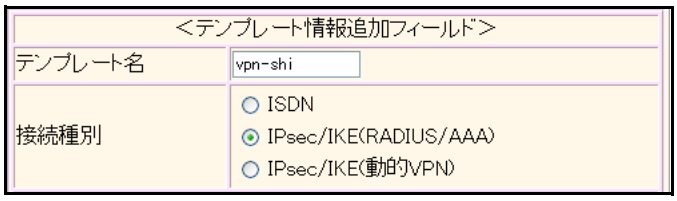
本社を設定する（Responder）

1.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

2.　以下の項目を指定します。

- テンプレート名　→vpn-shi
- 接続種別　→IPsec/IKE（RADIUS/AAA）



機種により、接続種別の表示が上記の画面とは異なります。

3.　［追加］ボタンをクリックします。

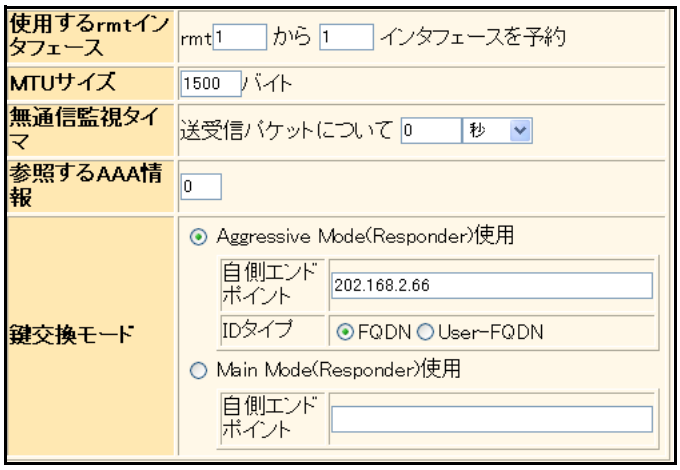
「テンプレート情報（vpn-shi)」と設定項目が表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt1 から 1 インタフェースを予約
- 参照する AAA 情報　→0
- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  ID タイプ　→FQDN



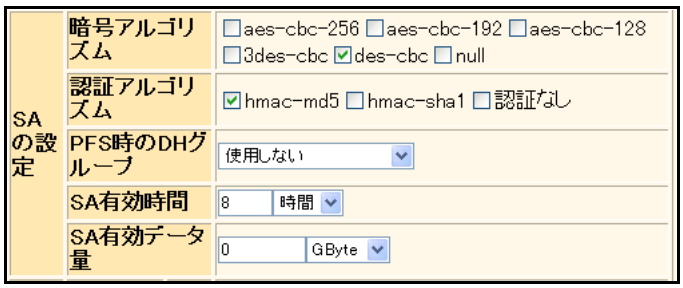
6.　［保存］ボタンをクリックします。

7.　テンプレート情報（vpn-shi）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

8.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



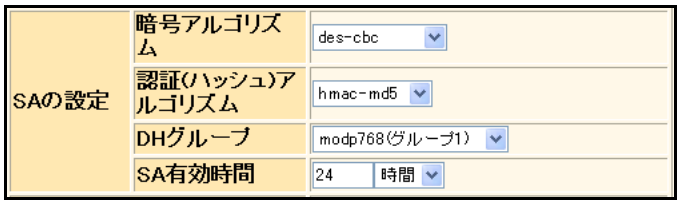
9.　［保存］ボタンをクリックします。

10.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

11.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「AAA 情報」をクリックします。

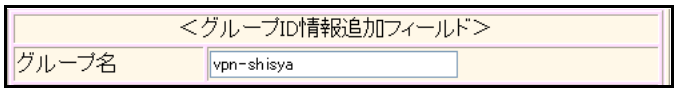
「AAA 情報」ページが表示されます。

14.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

15.　以下の項目を指定します。

- グループ名　→ vpn-shisya



16.　［追加］ボタンをクリックします。

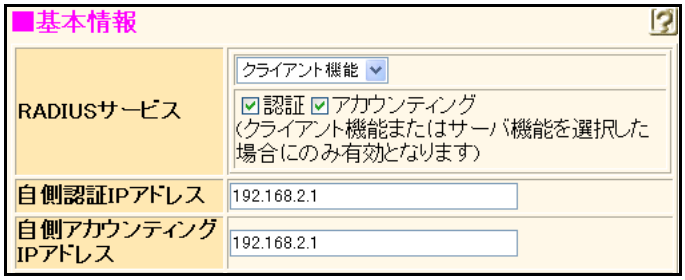
「グループ ID 情報（0）」と設定項目が表示されます。

17.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

18.　以下の項目を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックする
- 自側認証 IP アドレス　→192.168.2.1
- 自側アカウンティング IP アドレス　→192.168.2.1



19.　［保存］ボタンをクリックします。

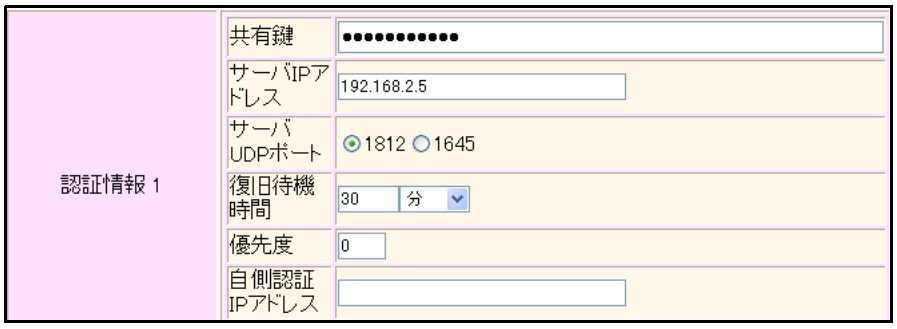
20.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

21.　認証情報 1 の［修正］ボタンをクリックします。

22.　以下の項目を指定します。

- 認証情報 1
  共有鍵　→192.168.2.1
  サーバ IP アドレス　→192.168.2.5
  復旧待機時間　→30 分
  優先度　→0



23.　認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

24.　認証情報 2 の［修正］ボタンをクリックします。

25.　以下の項目を指定します。

- 認証情報 2

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.2.6
  復旧待機時間　→ 30 分
  優先度　→ 100

26.　認証情報 2 の［保存］ボタンをクリックします。

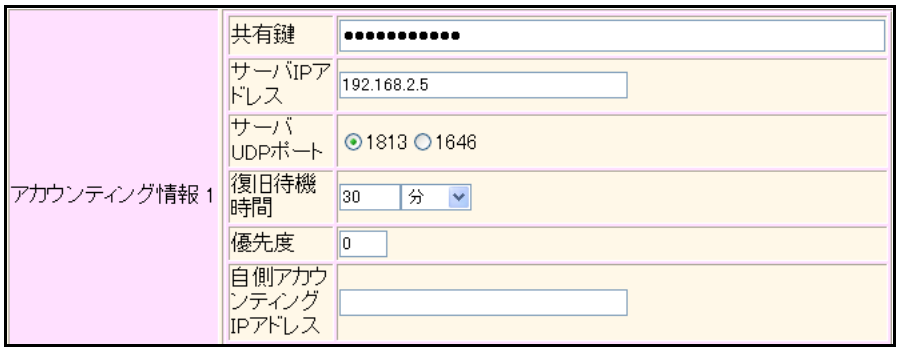
「サーバ情報（クライアント機能）」に戻ります。

27.　アカウンティング情報 1 の［修正］ボタンをクリックします。

28.　以下の項目を指定します。

- アカウンティング情報 1

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.2.5
  復旧待機時間　→ 30 分
  優先度　→ 0



29.　アカウンティング情報 1 の［保存］ボタンをクリックします。

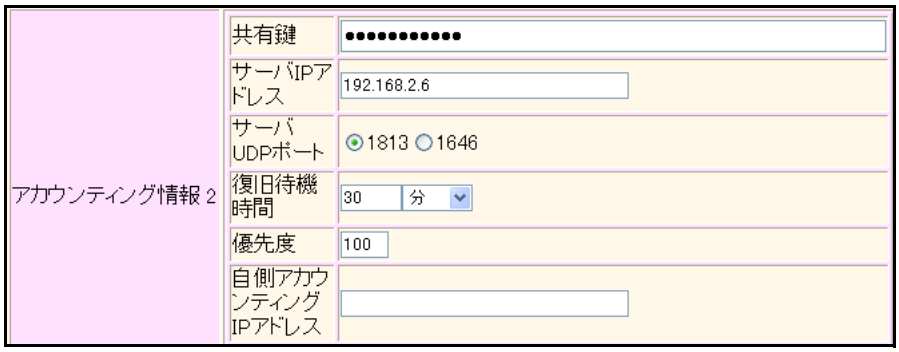
「サーバ情報（クライアント機能）」に戻ります。

30.　アカウンティング情報 2 の［修正］ボタンをクリックします。

31.　以下の項目を指定します。

- アカウンティング情報 2

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.2.6
  復旧待機時間　→ 30 分
  優先度　→ 100



32.　アカウンティング情報 2 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

33.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.15 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN

適用機種　全機種

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、支社間を本社を経由しないで自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

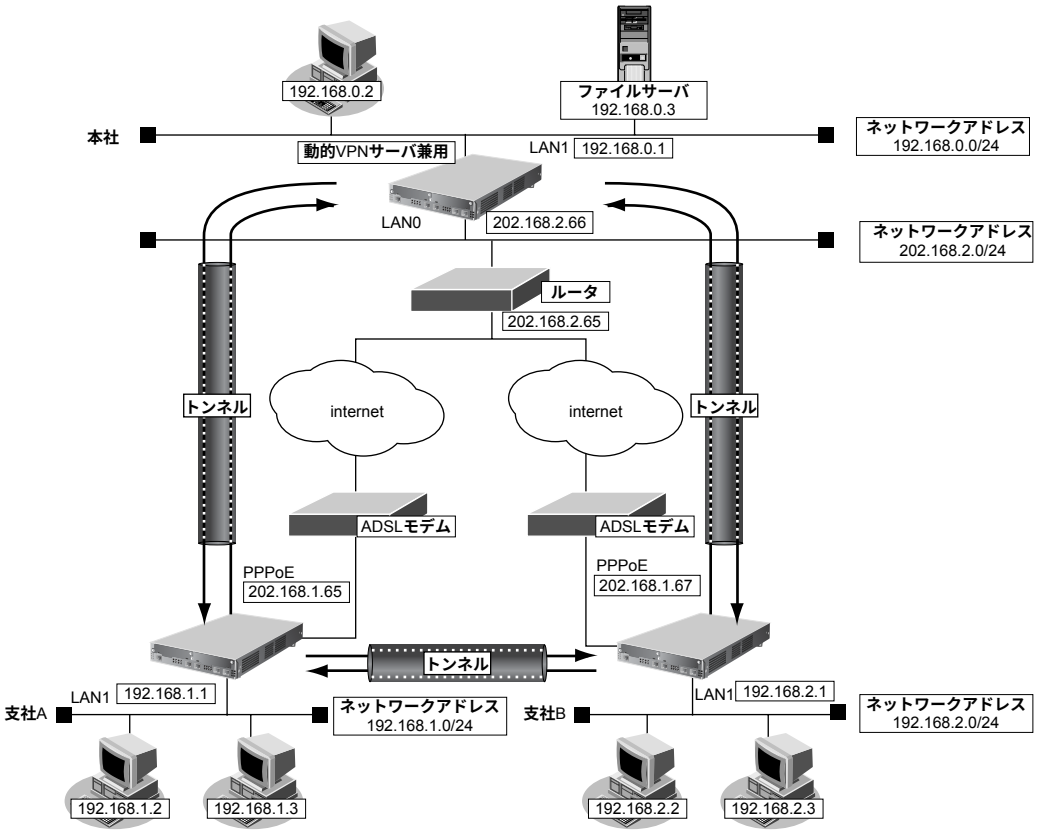
- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用
- NAT機能　：マルチNATを使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[本社]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65



● 設定条件（VPN 接続）

[支社 A（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 A － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1
- テンプレート名　：vpn-shiB
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた IPv4 アドレスを使用する
- 接続先監視アドレス　：192.168.1.1

[支社 B（Initiator)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 B － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.2.1
- ESP のプライベートアドレス　：192.168.2.1
- テンプレート名　：vpn-shiA
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた IPv4 アドレス を使用する
- 接続先監視アドレス　：192.168.2.1

[本社（Responder)]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：202.168.2.66 ー 支社 A
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：202.168.2.66 ー 支社 B
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通（本社 - 支社 A、B)]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A ID/ID タイプ　：shisyaA（自装置識別情報）/FQDN
- IKE 支社 B ID/ID タイプ　：shisyaB（自装置識別情報）/FQDN
- IKE 支社 A IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

● 設定条件（動的 VPN 接続）

[支社 A]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.0.1
  ポート番号　：5070
  認証 ID　：shisyaAid
  認証パスワード　：shisyaApass
- 有効期間　：1 時間
- セッション更新間隔　：更新する
  時間　：5 分
- クライアント IP アドレス　：192.168.1.1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv4 経路情報の優先度　：1

[支社 B]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.0.1
  ポート番号　：5070
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- 有効期間　：1 時間
- セッション更新間隔　：更新する
  時間　：5 分
- クライアント IP アドレス　：192.168.2.1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv4 経路情報の優先度　：1

[本社]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

[共通（支社 A-支社 B）]

- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode **の場合に、ネゴシエーションで使用する自装置を識別する** ID **の種別です。相手** VPN **装置の設定に合わせます。**

上記の設定条件に従って設定を行う場合の設定例を示します。

支社 A を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet **の［修正］ボタンをクリックします。**

「ネットワーク情報（internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

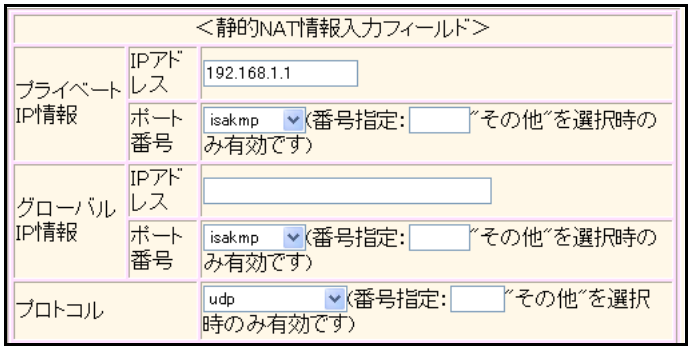
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6.～7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

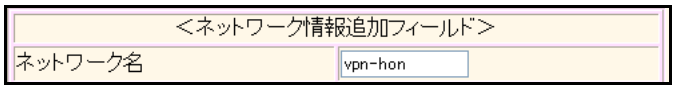
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→ vpn-hon



12.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

13.　「IP 関連」をクリックします。

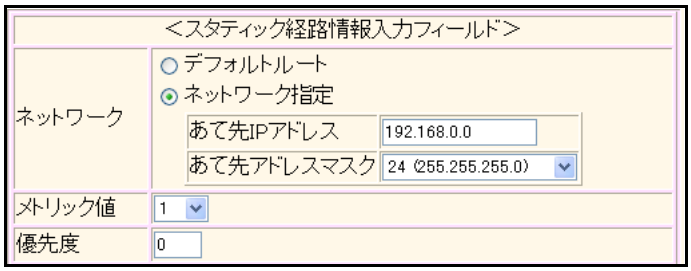
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.0.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



16.　［追加］ボタンをクリックします。

17.　手順 15.～16. を参考に、以下の項目を指定します。

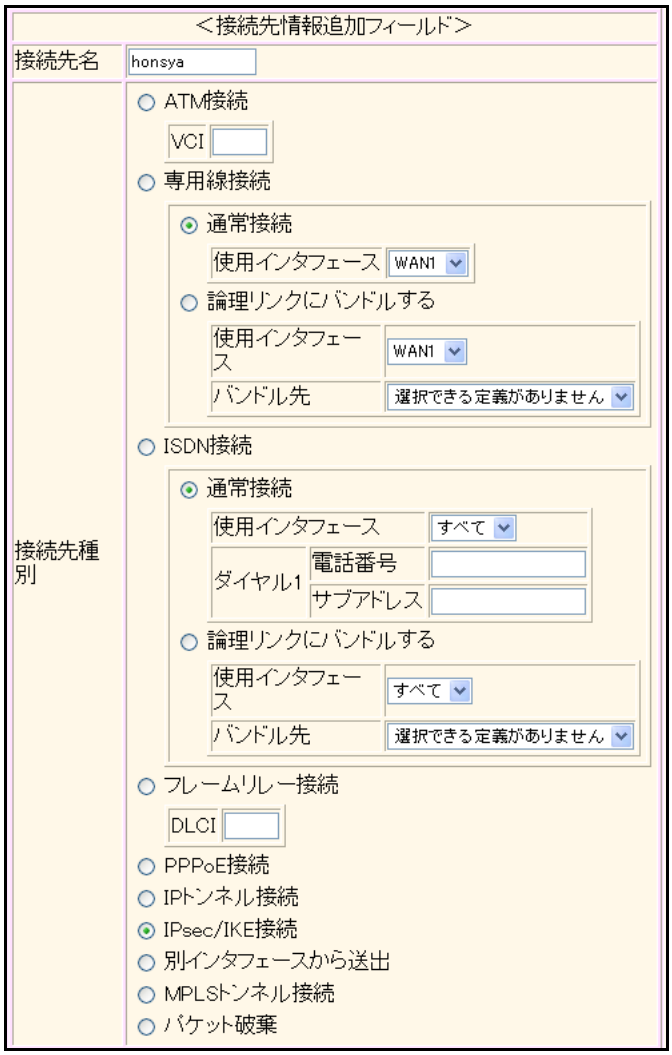
- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 2

18.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

19.　以下の項目を指定します。

- 接続先名　→ honsya
- 接続先種別　→ IPsec/IKE 接続



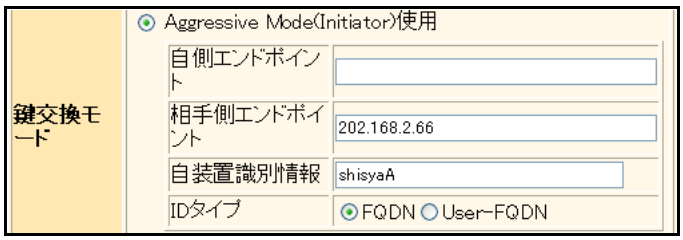
機種により、接続先種別の表示が上記の画面とは異なります。

20.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

21.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisyaA



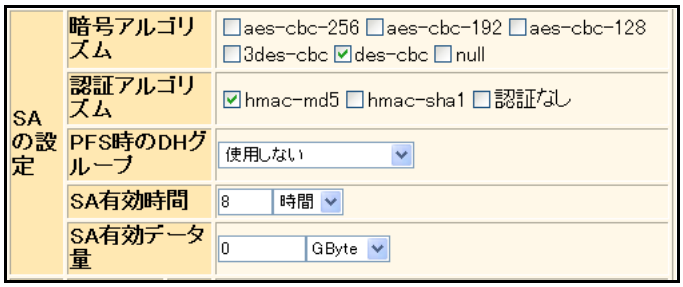
22.　［保存］ボタンをクリックします。

23.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

24.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



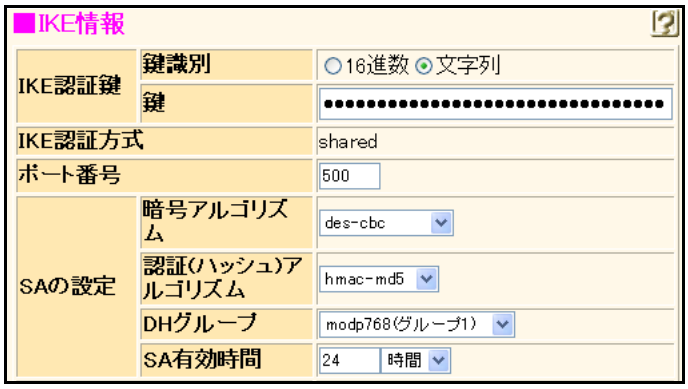
25.　［保存］ボタンをクリックします。

26.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

27.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



28.　［保存］ボタンをクリックします。

29.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

「動的 VPN 情報」ページが表示されます。

30.　「クライアント関連情報」をクリックします。

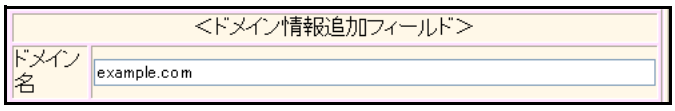
クライアント関連情報の設定項目と「基本情報」が表示されます。

31.　クライアント関連情報の設定項目の「ドメイン情報」をクリックします。

「ドメイン情報」が表示されます。

32.　以下の項目を指定します。

- ドメイン名　→example.com



33.　［追加］ボタンをクリックします。

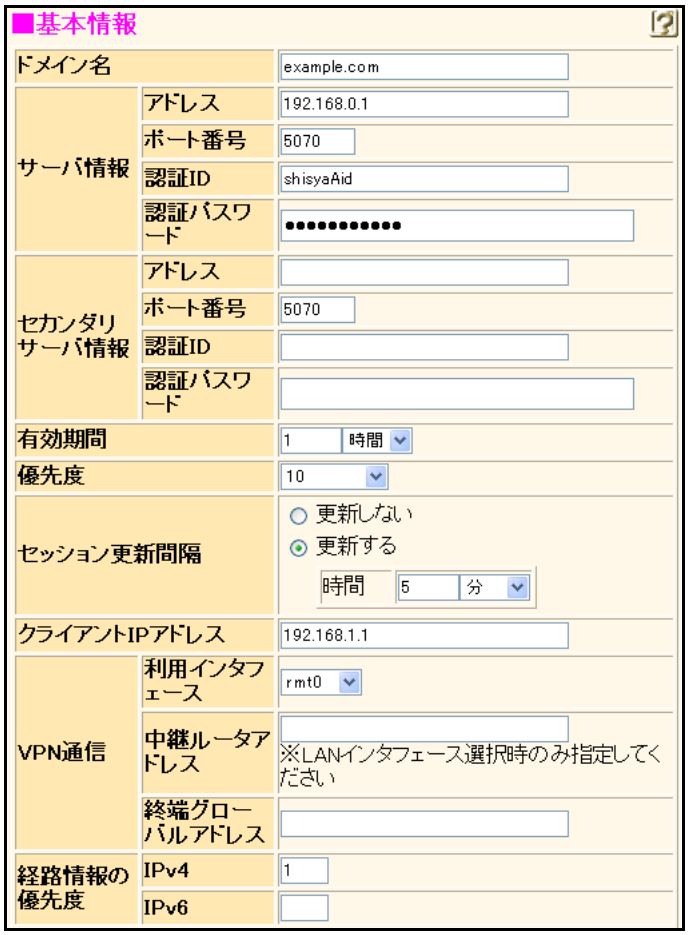
「ドメイン情報（0）」ページが表示されます。

34.　「基本情報」をクリックします。

「基本情報」が表示されます。

35.　以下の項目を指定します。

- ドメイン名　→example.com
- サーバ情報
  アドレス　→192.168.0.1
  ポート番号　→5070
  認証 ID　→shisyaAid
  認証パスワード　→shisyaApass
- 有効期間　→1 時間
- 優先度　→10
- セッション更新間隔　→更新する
  時間　→5 分
- クライアント IP アドレス　→192.168.1.1
- VPN 通信
  利用インタフェース　→rmt0
- 経路情報の優先度
  IPv4　→1



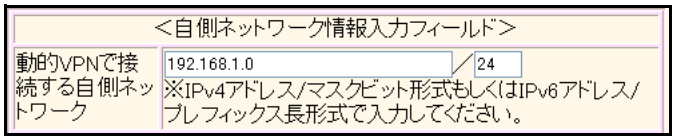
36.　［保存］ボタンをクリックします。

37.　ドメイン情報（0）の設定項目の「自側ネットワーク情報」をクリックします。

「自側ネットワーク情報」が表示されます。

38.　以下の項目を指定します。

- 動的 VPN で接続する自側ネットワーク　→ 192.168.1.0/24



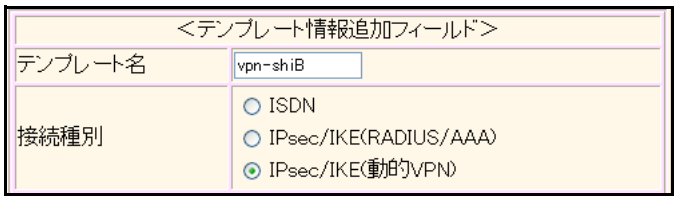
39.　［追加］ボタンをクリックします。

40.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

41.　以下の項目を指定します。

- テンプレート名　→ vpn-shiB
- 接続種別　→ IPsec/IKE（動的 VPN）



機種により、接続種別の表示が上記の画面とは異なります。

42.　［追加］ボタンをクリックします。

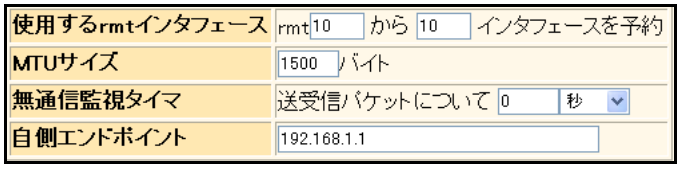
「テンプレート情報（vpn-shiB）」と設定項目が表示されます。

43.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

44.　以下の項目を指定します。

- 使用する rmt インタフェース　→ rmt10 から 10 インタフェースを予約
- 自側エンドポイント　→ 192.168.1.1



45.　［保存］ボタンをクリックします。

46.　テンプレート情報（vpn-shiB）の設定項目の「動的 VPN 関連」をクリックします。

動的 VPN 関連の設定項目と「基本情報」が表示されます。

47.　以下の項目を指定します。

- ドメイン情報　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- ドメイン情報　→ 0（example.com）

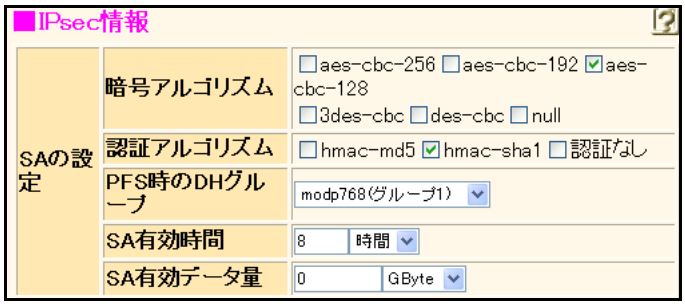
48.　［保存］ボタンをクリックします。

49.　テンプレート情報（vpn-shiB）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

50.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証アルゴリズム　→hmac-sha1
  PFS 時の DH グループ　→modp768（グループ 1）



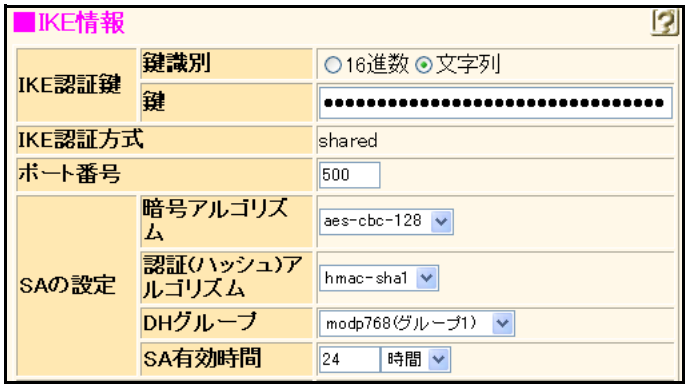
51.　［保存］ボタンをクリックします。

52.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

53.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp768（グループ 1）



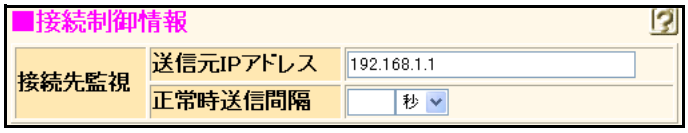
54.　［保存］ボタンをクリックします。

55.　IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

56.　以下の項目を指定します。

- 接続先監視
  送信元 IP アドレス　→192.168.1.1



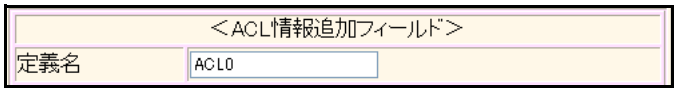
57.　［保存］ボタンをクリックします。

58.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

59.　以下の項目を指定します。

- 定義名　→ACL0



60.　［追加］ボタンをクリックします。

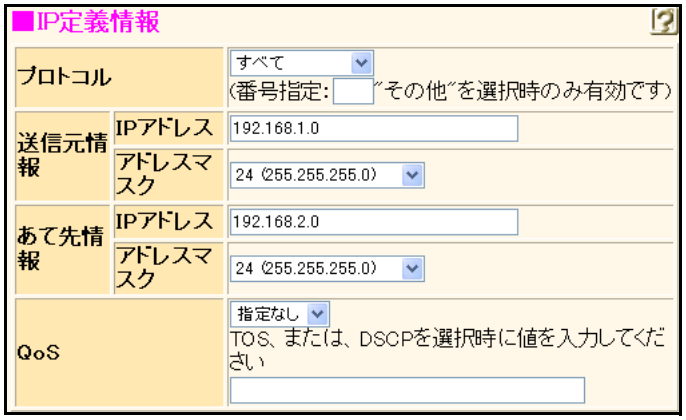
「ACL 情報（ACL0）」ページが表示されます。

61.　「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

62.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- Qos　→指定なし



63.　［保存］ボタンをクリックします。

64.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

65.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

66.　「ネットワーク情報」でネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

67.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

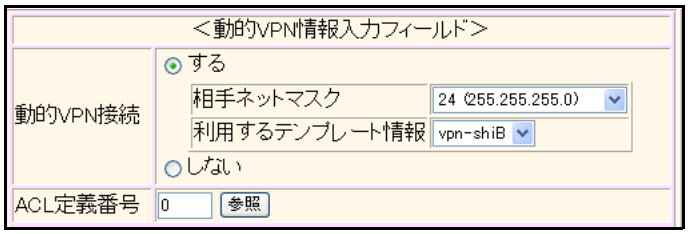
68.　「動的 VPN 情報」をクリックします。

「動的 VPN 情報」が表示されます。

69.　以下の項目を指定します。

- 動的 VPN 接続　→する
  相手ネットマスク　→24（255.255.255.0）
  利用するテンプレート情報　→vpn-shiB
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



70.　［追加］ボタンをクリックします。

71.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B を設定する（Initiator）

「支社 A を設定する」を参考に、支社 B を設定します。

「相手情報」-「ネットワーク情報」

「ネットワーク情報（internet）」-「IP 関連」

「静的 NAT 情報」

- プライベート IP 情報
  IP アドレス　→ 192.168.2.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp
- プライベート IP 情報
  IP アドレス　→ 192.168.2.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ vpn-hon

「ネットワーク情報（vpn-hon）」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.0.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0
- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 2

「接続先情報」

- 接続先名　→ honsya
- 接続先種別　→ IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→ Aggressive Mode（Initiator）使用
  相手側エンドポイント　→ 202.168.2.66
  自装置識別情報　→ shisyaB

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ 1234567890abcdefghijklmnopqrstuvwxyz
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）

「動的 VPN 情報」-「クライアント関連情報」-「ドメイン情報」

「基本情報」

- ドメイン名　→ example.com
- サーバ情報
  アドレス　→ 192.168.0.1
  ポート番号　→ 5070
  認証 ID　→ shisyaBid
  認証パスワード　→ shisyaBpass
- 有効期間　→ 1 時間
- 優先度　→ 10
- セッション更新間隔　→ 更新する
  時間　→ 5 分
- クライアント IP アドレス　→ 192.168.2.1
- VPN 通信
  利用インタフェース　→ rmt0
- 経路情報の優先度
  IPv4　→ 1

「自側ネットワーク情報」

- 動的 VPN で接続する自側ネットワーク　→ 192.168.2.0/24
- 動的 VPN サーバ登録　→ する

「テンプレート情報」

- テンプレート名　→ vpn-shiA
- 接続種別　→ IPsec/IKE（動的 VPN）

「テンプレート情報（vpn-shiA）」-「共通情報」

「基本情報」

- 使用する rmt インタフェース　→ rmt10 から 10 インタフェースを予約
- 自側エンドポイント　→ 192.168.2.1

「テンプレート情報（vpn-shiA）」-「動的 VPN 関連」

「基本情報」

- ドメイン情報　→使用する

「テンプレート情報（vpn-shiA）」-「IPsec/IKE 関連」

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証アルゴリズム　→hmac-sha1
  PFS 時の DH グループ　→modp768（グループ 1）

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp768（グループ 1）

「接続制御情報」

- 接続先監視
  送信元 IP アドレス　→192.168.2.1

「ACL 情報」

- 定義名　→ACL0

「ACL 定義情報（ACL0）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- QoS　→指定なし

「相手情報」-「ネットワーク情報」

「ネットワーク情報（vpn-hon）」-「IP 関連」

「動的 VPN 情報」

- 動的 VPN 接続　→する
  相手ネットマスク　→24（255.255.255.0）
  利用するテンプレート情報　→vpn-shiA
- ACL 定義番号　→0

本社を設定する（Responder）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

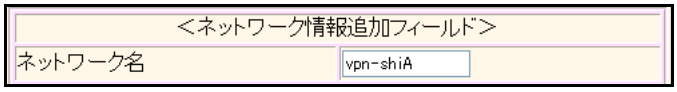
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shiA



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shiA)」ページが表示されます。

5.　「IP 関連」をクリックします。

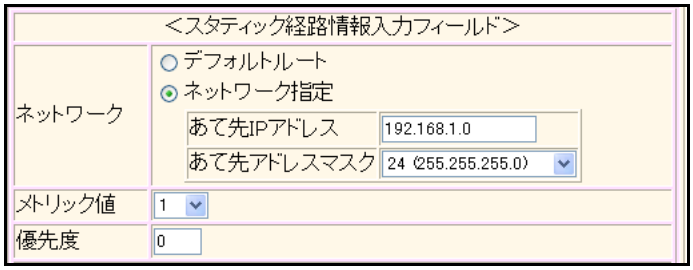
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



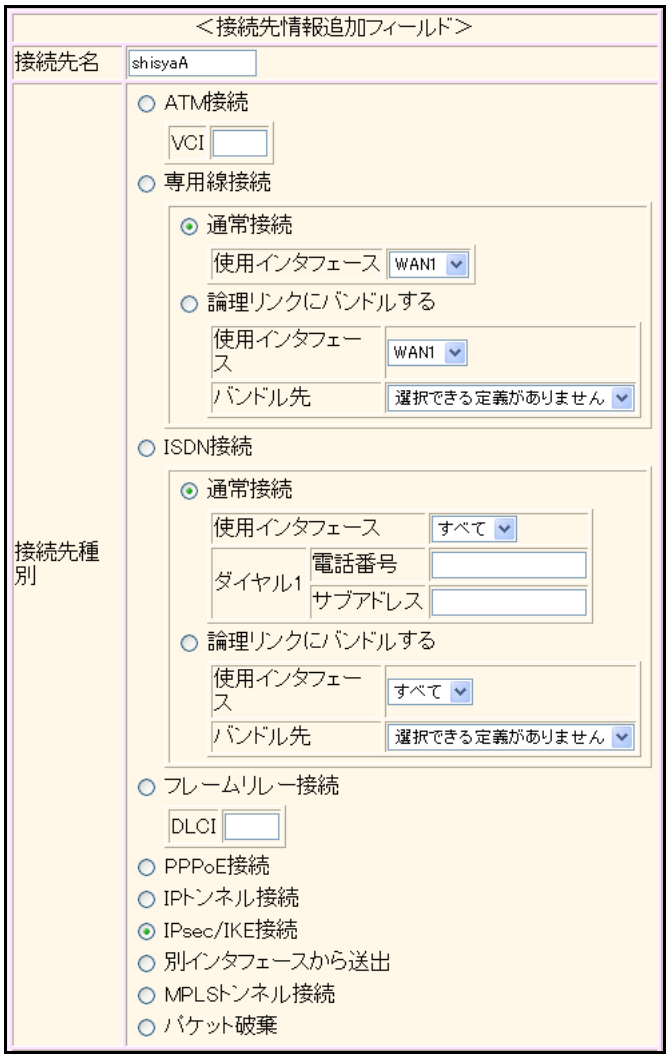
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisyaA
- 接続先種別　→IPsec/IKE 接続



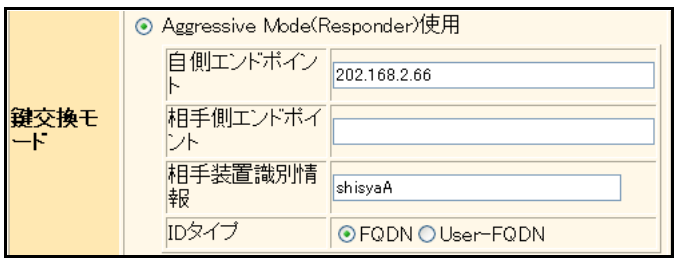
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  相手装置識別情報　→shisyaA



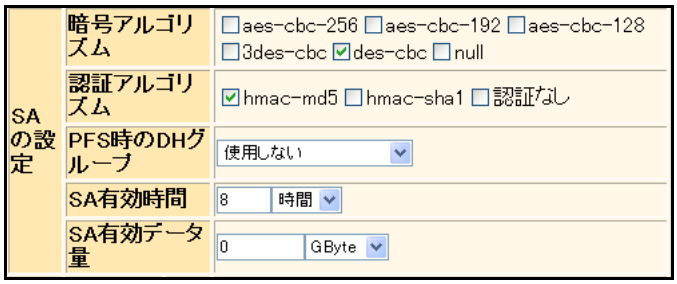
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



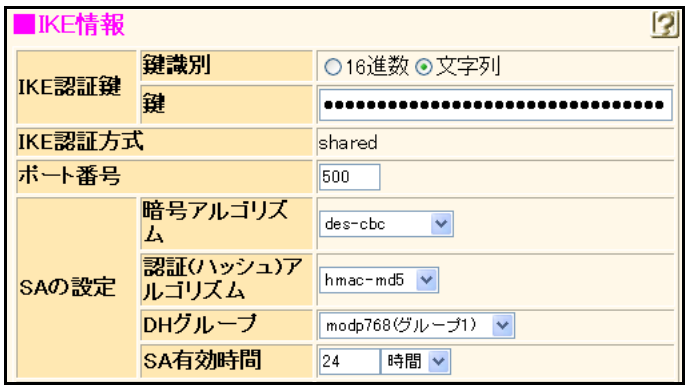
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



19.　［保存］ボタンをクリックします。

20.　手順 1.～19. を参考に、支社 B を設定します。

21.　設定メニューのルータ設定で「AAA 情報」をクリックします。

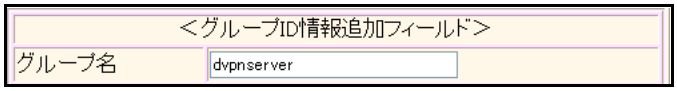
「AAA 情報」ページが表示されます。

22.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

23.　以下の項目を指定します。

- グループ名　→dvpnserver



24.　［追加］ボタンをクリックします。

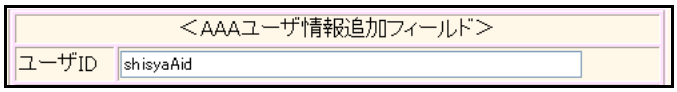
「グループ ID 情報（0）」と設定項目が表示されます。

25.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

26.　以下の項目を指定します。

- ユーザ ID　→shisyaAid



27.　［追加］ボタンをクリックします。

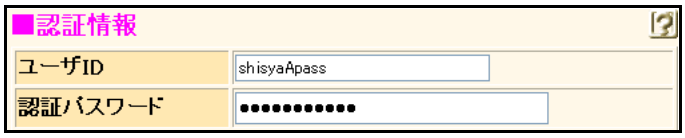
「AAA ユーザ情報（0）」と設定項目が表示されます。

28.　「認証情報」をクリックします。

「認証情報」が表示されます。

29.　以下の項目を指定します。

- 認証パスワード　→shisyaApass



30.　［保存］ボタンをクリックします。

31.　手順 21. ～ 29. を参考に、支社 B を設定します。

32.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

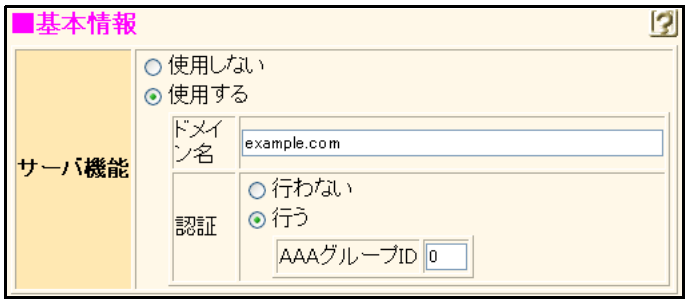
「動的 VPN 情報」ページが表示されます。

33.　「サーバ関連情報」をクリックします。

サーバ関連情報の設定項目と「基本情報」が表示されます。

34.　以下の項目を指定します。

- サーバ機能　→使用する
  ドメイン名　→example.com
  認証　→行う
  AAA グループ ID　→0



35.　［保存］ボタンをクリックします。

36.　画面左側の［設定反映］ボタンをクリックします。

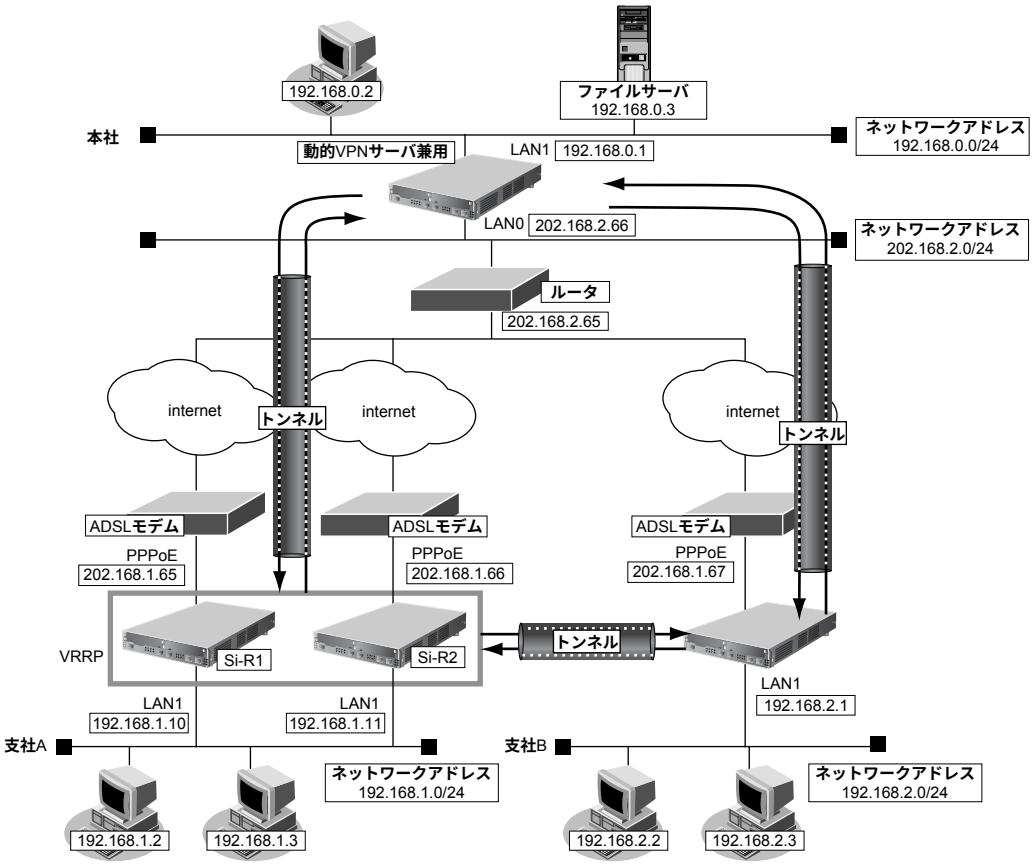
設定した内容が有効になります。

2.14.16 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN（冗長構成）

適用機種　全機種

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを冗長構成で構築する場合の設定方法を説明します。

ここでは「2.14.15 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.611）で説明したネットワーク構成で、支社と本社が動的VPNによって接続されていることを前提とします。ただし、支社AはVRRPによる冗長構成の設定を行います。



● 設定条件（冗長構成）

[支社A（Si-R1)]

- ローカルネットワークIPv4アドレス　：192.168.1.10/24
- VRRP優先度　：254
- 動的VPNクライアントの優先度　：1
- ノードダウントリガ　：202.168.2.66

[支社A（Si-R2)]

- ローカルネットワークIPv4アドレス　：192.168.1.11/24
- VRRP優先度　：100
- 動的VPNクライアントの優先度　：2

[支社 A（共通)]

- VRRP 仮想 IP アドレス　：192.168.1.1/24
- VRRP グループ ID　：10
- OSPF エリア ID　：0.0.0.0

上記の設定条件に従って設定を行う場合の設定例を示します。

支社 A を設定する（Si-R1）

「2.14.15 テンプレート着信機能（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN」（P.611）を参考に、動的 VPN での設定を事前に行います。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

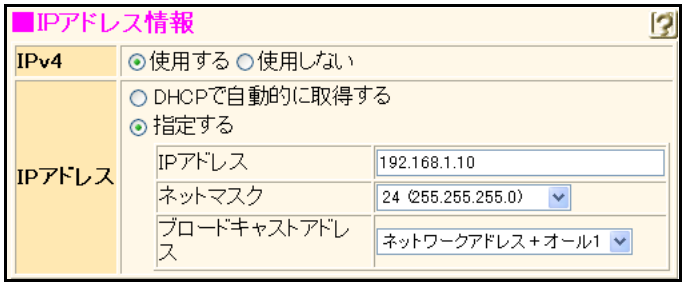
「LAN1 情報（物理 LAN)」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.10
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



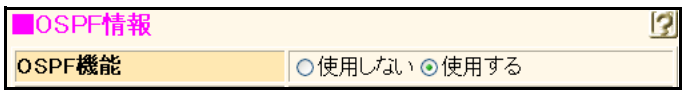
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます

7.　以下の項目を指定します。

- OSPF 機能　→使用する



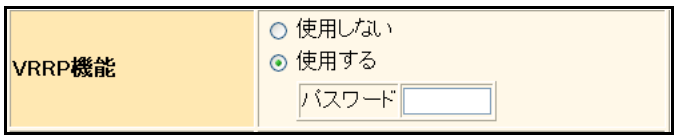
8.　［保存］ボタンをクリックします。

9.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

10.　以下の項目を指定します。

- VRRP 機能　→使用する



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

11.　［保存］ボタンをクリックします。

12.　共通情報の設定項目の「VRRP グループ情報」をクリックします。

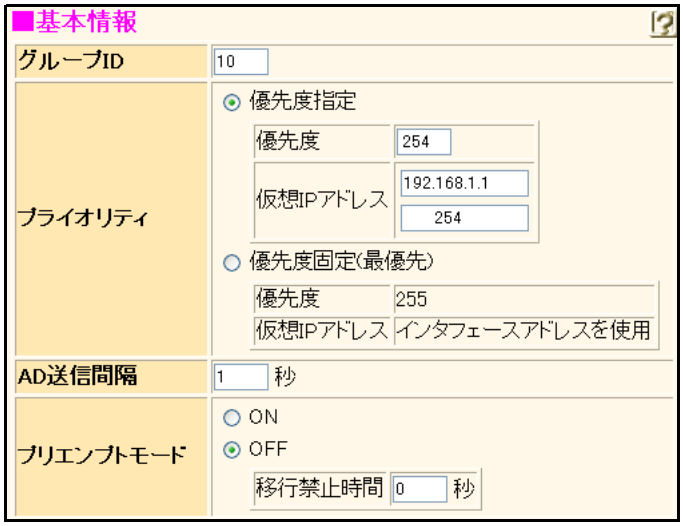
「VRRP グループ情報」が表示されます。

13.　「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ OFF



15.　［保存］ボタンをクリックします。

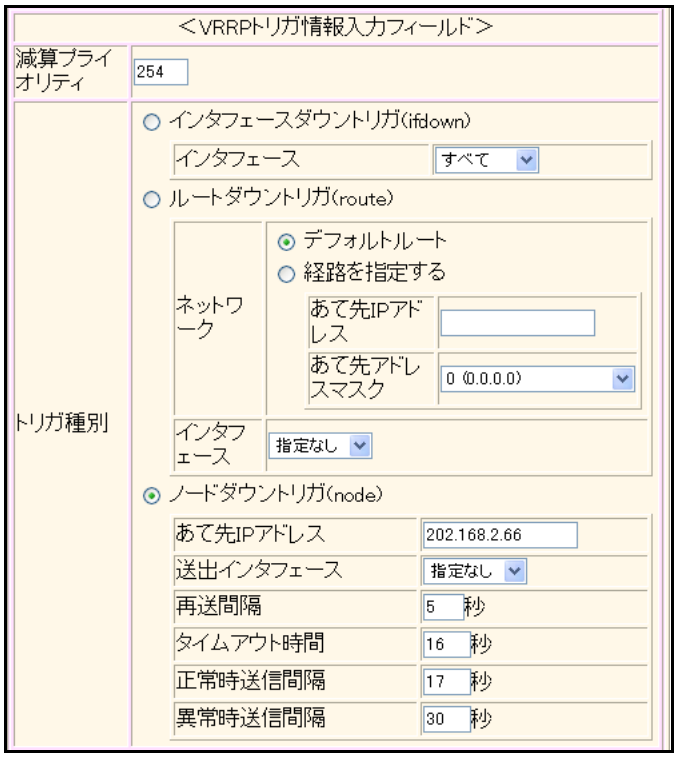
16.　VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

17.　以下の項目を指定します。

- 減算プライオリティ　→254
- トリガ種別　→ノードダウントリガ（node）

  あて先 IP アドレス　→202.168.2.66
  送出インタフェース　→指定なし
  再送間隔　→5
  タイムアウト時間　→16
  正常時送信間隔　→17
  異常時送信間隔　→30



18.　［追加］ボタンをクリックします。

19.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

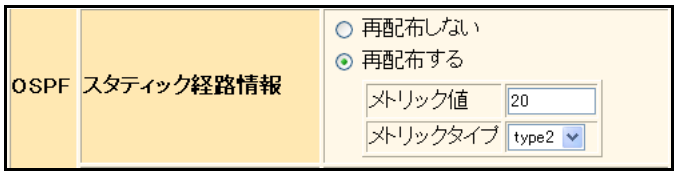
20.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

21.　以下の項目を指定します。

- OSPF

  スタティック経路情報　→ 再配布する
  メトリック値　→ 20
  メトリックタイプ　→ type2



22.　［保存］ボタンをクリックします。

23.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

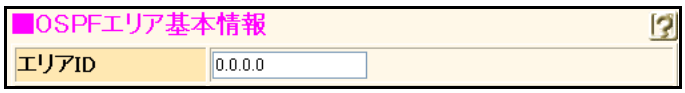
24.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPF エリア情報」が表示されます。

25.　［追加］ボタンをクリックします。

26.　以下の項目を指定します。

- エリア ID　→ 0.0.0.0



27.　［保存］ボタンをクリックします。

28.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

「動的 VPN 情報」ページが表示されます。

29.　「クライアント関連情報」をクリックします。

クライアント関連情報の設定項目と「基本情報」が表示されます。

30.　クライアント関連情報の設定項目の「ドメイン情報」をクリックします。

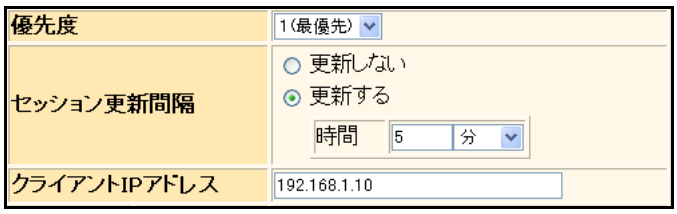
「ドメイン情報」が表示されます。

31.　「ドメイン情報」で定義番号が 0 の［修正］ボタンをクリックします。

「ドメイン情報（0）」ページが表示されます。

32.　以下の項目を指定します。

- 優先度　→ 1（最優先）
- クライアント IP アドレス　→ 192.168.1.10



33.　［保存］ボタンをクリックします。

34.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

35.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

36.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet）」ページが表示されます。

37.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

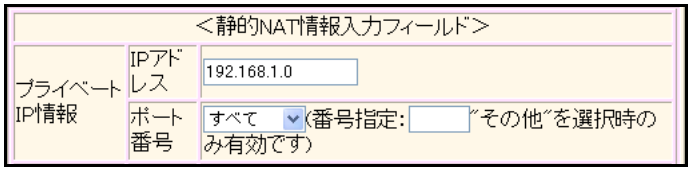
38.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

39.　「静的 NAT 情報」でプライベートアドレスが 192.168.1.1 の［修正］ボタンをクリックします。

40.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.10



41.　［保存］ボタンをクリックします。

42.　手順 39. ～ 41. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.10

43.　画面上部の「相手情報」をクリックします。

「相手情報」ページが表示されます。

44.　「ネットワーク情報」でネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon)」ページが表示されます。

45.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

46.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

47.　「スタティック経路情報」であて先 IP アドレス / マスクが 192.168.2.0/24 の［修正］ボタンをクリックします。

48.　以下の項目を指定します。

- 優先度　→ 200

49.　［保存］ボタンをクリックします。

50.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

51.　「テンプレート情報」でテンプレート名が vpn-shiB の［修正］ボタンをクリックします。

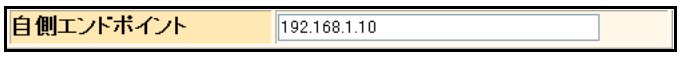
「テンプレート情報（vpn-shiB)」ページが表示されます。

52.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

53.　以下の項目を指定します。

- 自側エンドポイント　→192.168.1.10



54.　［保存］ボタンをクリックします。

55.　「IPsec/IKE 関連」をクリックします。

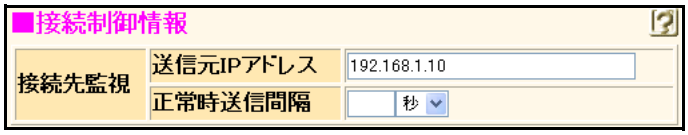
IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

56.　IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

57.　以下の項目を指定します。

- 接続先監視
  送信元 IP アドレス　→192.168.1.10



58.　［保存］ボタンをクリックします。

59.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 A を設定する（Si-R2）

「支社 A を設定する（Si-R1）」を参考に、Si-R2 を設定します。

LAN1 情報を設定する

「LAN1 情報」-「IP 関連」

「IP アドレス情報」

- IP アドレス　→192.168.1.11

「OSPF 情報」

- OSPF 機能　→使用する

「LAN1 情報」-「共通情報」

「基本情報」

- VRRP 機能　→使用する

「VRRP グループ 0 情報」

「基本情報」

- グループ ID　→10
- プライオリティ　→優先度指定
  優先度　→100
  仮想 IP アドレス　→192.168.1.1
- プリエンプトモード　→OFF

OSPF 情報を設定する

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」

「再配布情報」

- OSPF
  スタティック経路情報　→再配布する
  メトリック値　→20
  メトリックタイプ　→type2

「ルーティングプロトコル情報」-「OSPF 関連」-「ルータ ID 情報」

「OSPF エリア情報」

- エリア ID　→0.0.0.0

動的 VPN 情報を設定する

「動的 VPN 情報」-「クライアント関連情報」-「ドメイン情報」

「基本情報」

- 優先度　→2
- クライアント IP アドレス　→192.168.1.11

相手情報を設定する

「相手情報」-「ネットワーク情報（internet)」-「IP 関連」

「静的 NAT 情報」

- プライベート IP 情報
  IP アドレス　→192.168.1.11

「相手情報」-「ネットワーク情報（vpn-hon)」-「IP 関連」

「スタティック経路情報」

- 優先度　→200

テンプレート情報を設定する

「テンプレート情報」-「共通情報」

「基本情報」

- 自側エンドポイント　→192.168.1.11

「テンプレート情報」-「IPsec/IKE 関連」

「接続制御情報」

- 接続先監視
  送信元 IP アドレス　→192.168.1.11

本社を設定する

「2.14.15 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN」（P.611）を参考に、本社を設定します。

相手情報を設定する

「相手情報」-「ネットワーク情報（vpn-shiA）」-「IP関連」

「スタティック経路情報」

- 優先度　→10

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-shia

「ネットワーク情報（vpn-shia）」-「IP関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先IPアドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→254

「接続先情報」

- 接続先名　→shisyaa
- 接続先種別　→IPsec/IKE接続

「接続先情報」-「IPsec/IKE接続」

「基本情報」

- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  相手装置識別情報　→shisyaa

「IPsec情報」

- SAの設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5

「IKE情報」

- IKE認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SAの設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DHグループ　→modp768（グループ1）

2.14.17 テンプレート着信機能（動的VPN）を使用した IPv6 over IPv6で固定IPアドレスでのVPN

適用機種　全機種

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、支社間を本社を経由しないで自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A（PPPoE常時接続）]

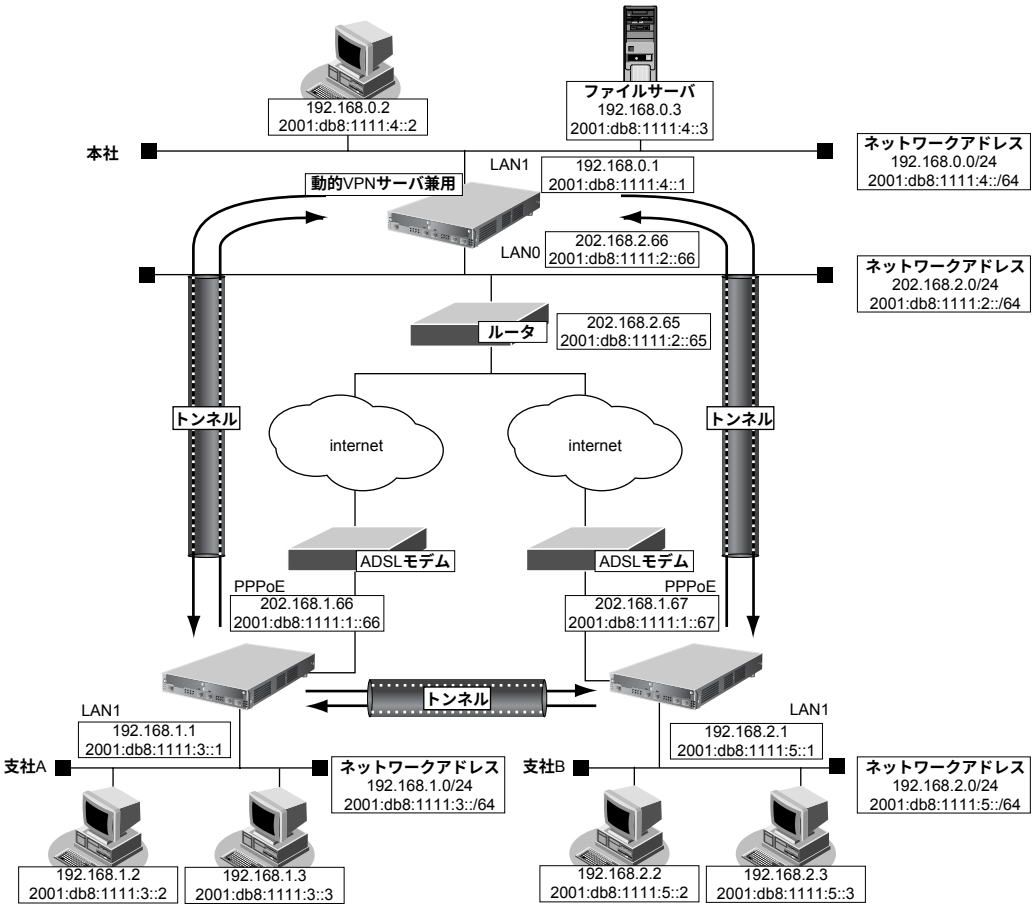
- ローカルネットワークIPv4アドレス　：192.168.1.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.1.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:1::66/64
- PPPoEユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[支社B（PPPoE常時接続）]

- ローカルネットワークIPv4アドレス　：192.168.2.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:5::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.1.67/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:1::67/64
- PPPoEユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LANポート　：LAN0ポート使用

[本社]

- ローカルネットワークIPv4アドレス　：192.168.0.1/24
- ローカルネットワークIPv6アドレス　：2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス　：202.168.2.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス　：2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス　：202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートのIPv6アドレス　：2001:db8:1111:2::65



● 設定条件（VPN 接続）

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::66 － 2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- テンプレート名　：vpn-shiB
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた固定 IPv6 アドレスを使用する
- 接続先監視アドレス　：2001:db8:1111:3::1

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：2001:db8:1111:1::67 － 2001:db8:1111:2::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- テンプレート名　：vpn-shiA
- IPsec/IKE 始点　：インターネットプロバイダから割り当てられた固定 IPv6 アドレス を使用する
- 接続先監視アドレス　：2001:db8:1111:5::1

[本社]

- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE 区間　：2001:db8:1111:2::66 － 2001:db8:1111:1::66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE 区間　：2001:db8:1111:2::66 － 2001:db8:1111:1::67
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通（本社 - 支社 A、B)]

- 鍵交換タイプ　：Main Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 A IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768

● 設定条件（動的 VPN 接続）

[支社 A]

- クライアント情報　：0
- サーバ情報
  アドレス　：2001:db8:1111:4::1
  ポート番号　：5070
  認証 ID　：shisyaAid
  認証パスワード　：shisyaApass
- 有効期間　：1 時間
- セッション更新間隔　：更新する
  時間　：5 分
- クライアント IP アドレス　：2001:db8:1111:3::1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv6 経路情報の優先度　：1

[支社 B]

- クライアント情報　：0

- サーバ情報
  アドレス　：2001:db8:1111:4::1
  ポート番号　：5070
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- 有効期間　：1 時間
- セッション更新間隔　：更新する
  時間　：5 分
- クライアント IP アドレス　：2001:db8:1111:5::1
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv6 経路情報の優先度　：1

[本社]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

[共通（支社 A-支社 B）]

- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社 A を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

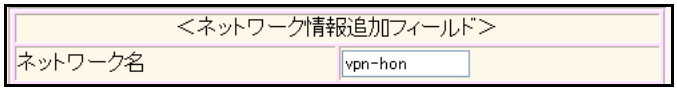
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

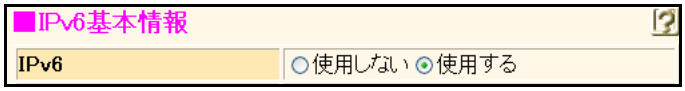
「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

6.　以下の項目を指定します。

- IPv6　→使用する



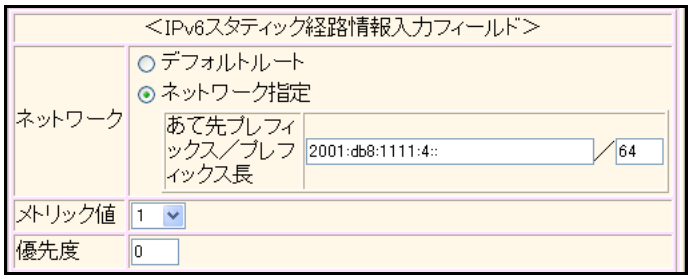
7.　［保存］ボタンをクリックします。

8.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:4::/64
- メトリック値　→1
- 優先度　→0



10.　［追加］ボタンをクリックします。

11.　手順 9.～10. を参考に、以下の項目を指定します。

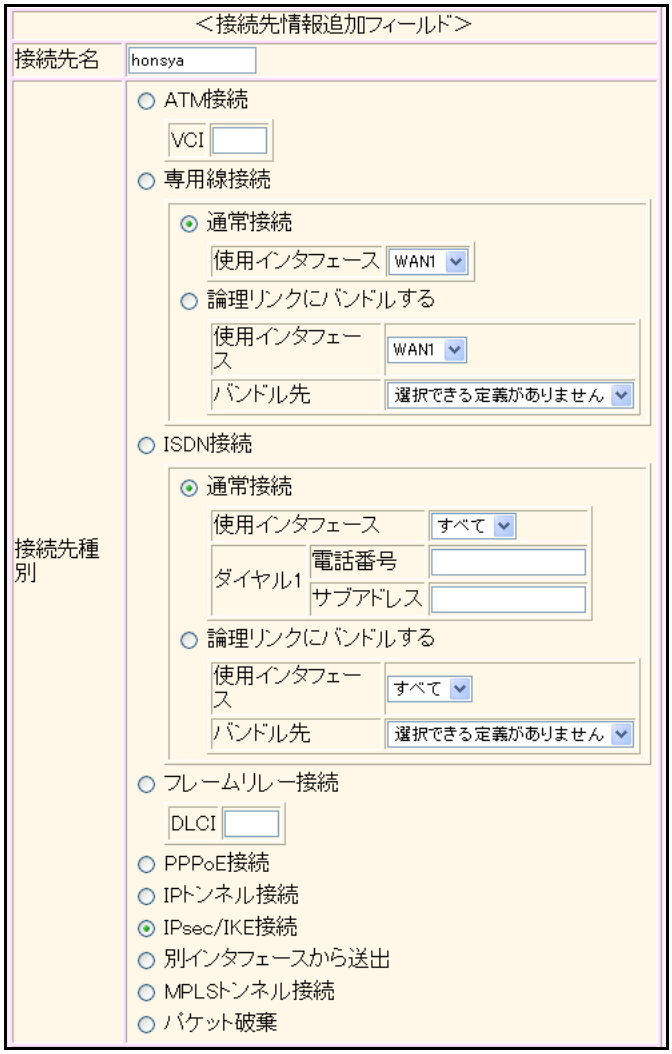
- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:5::/64
- メトリック値　→1
- 優先度　→2

12.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

13.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

14.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

15.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→2001:db8:1111:2::66
  自側エンドポイント　→2001:db8:1111:1::66

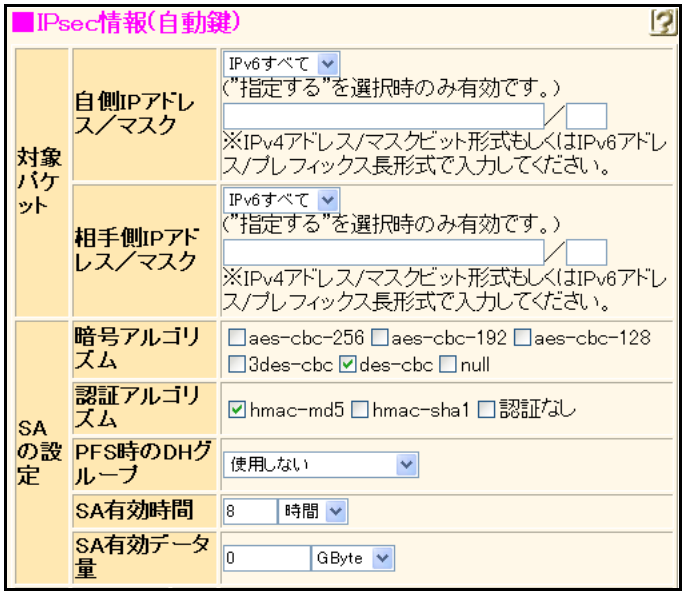
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

18.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



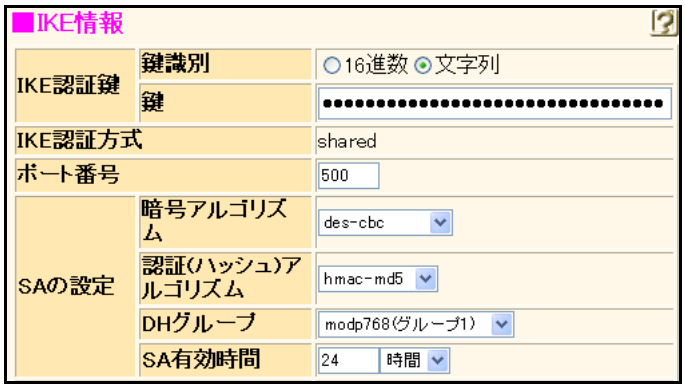
19.　［保存］ボタンをクリックします。

20.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

21.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



22.　［保存］ボタンをクリックします。

23.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

「動的 VPN 情報」ページが表示されます。

24.　「クライアント関連情報」をクリックします。

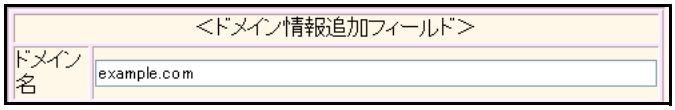
クライアント関連情報の設定項目と「基本情報」が表示されます。

25.　クライアント関連情報の設定項目の「ドメイン情報」をクリックします。

「ドメイン情報」が表示されます。

26.　以下の項目を指定します。

- ドメイン名　→example.com



27.　［追加］ボタンをクリックします。

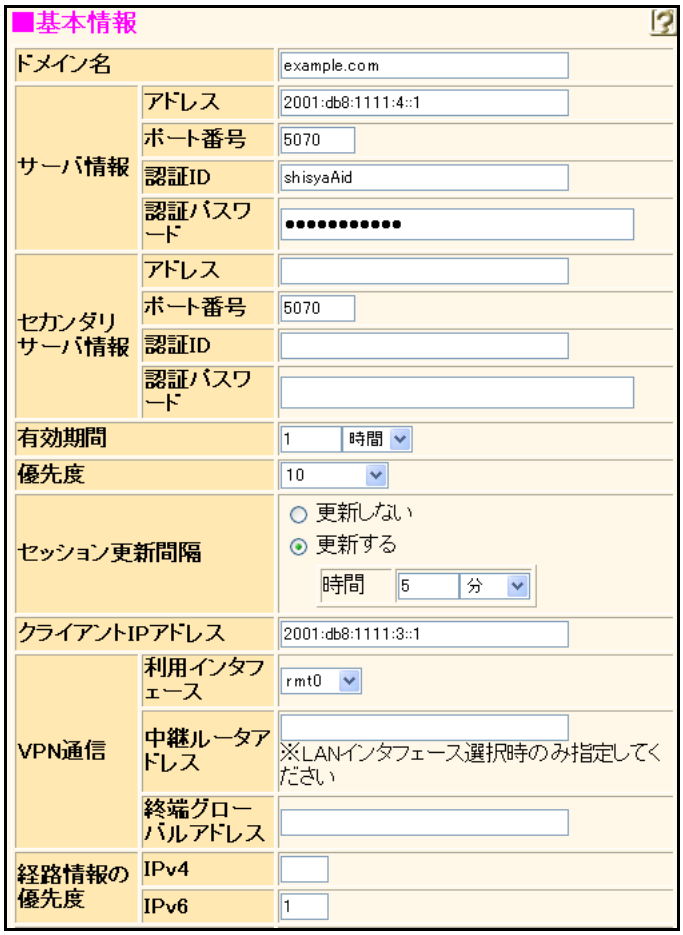
「ドメイン情報（0）」ページが表示されます。

28.　「基本情報」をクリックします。

「基本情報」が表示されます。

29.　以下の項目を指定します。

- ドメイン名　→example.com
- サーバ情報
  アドレス　→2001:db8:1111:4::1
  ポート番号　→5070
  認証 ID　→shisyaAid
  認証パスワード　→shisyaApass
- 有効期間　→1 時間
- 優先度　→10
- セッション更新間隔　→更新する
  時間　→5 分
- クライアント IP アドレス　→2001:db8:1111:3::1
- VPN 通信
  利用インタフェース　→rmt0
- 経路情報の優先度
  IPv6　→1



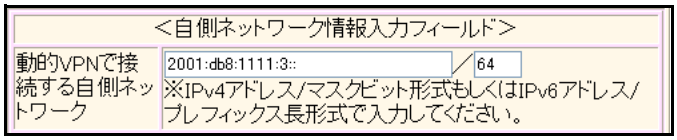
30.　［保存］ボタンをクリックします。

31.　ドメイン情報（0）の設定項目の「自側ネットワーク情報」をクリックします。

「自側ネットワーク情報」が表示されます。

32.　以下の項目を指定します。

- 動的 VPN で接続する自側ネットワーク　→ 2001:db8:1111:3::/64



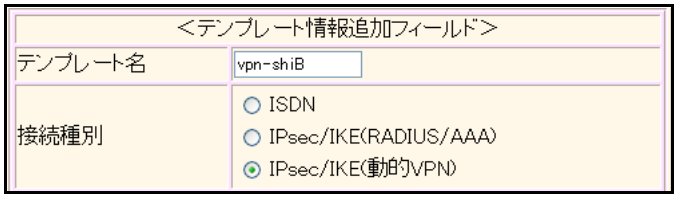
33.　［追加］ボタンをクリックします。

34.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

35.　以下の項目を指定します。

- テンプレート名　→ vpn-shiB
- 接続種別　→ IPsec/IKE（動的 VPN）



機種により、接続種別の表示が上記の画面とは異なります。

36.　［追加］ボタンをクリックします。

「テンプレート情報（vpn-shiB）」と設定項目が表示されます。

37.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

38.　以下の項目を指定します。

- 使用する rmt インタフェース　→ rmt10 から 10 インタフェースを予約
- 自側エンドポイント　→ 2001:db8:1111:1::66

39.　［保存］ボタンをクリックします。

40.　テンプレート情報（vpn-shiB）の設定項目の「動的 VPN 関連」をクリックします。

動的 VPN 関連の設定項目と「基本情報」が表示されます。

41.　以下の項目を指定します。

- ドメイン情報　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- ドメイン情報　→0（example.com）

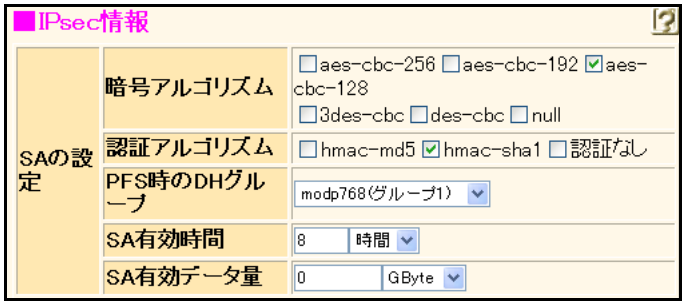
42.　［保存］ボタンをクリックします。

43.　テンプレート情報（vpn-shiB）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

44.　以下の項目を指定します。

- SA の設定
  - 暗号アルゴリズム　→aes-cbc-128
  - 認証アルゴリズム　→hmac-sha1
  - PFS 時の DH グループ　→modp768（グループ 1）



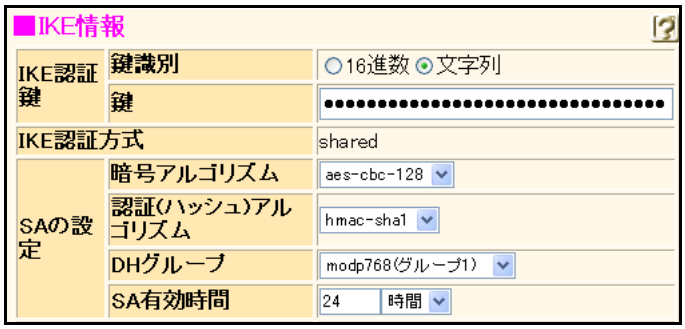
45.　［保存］ボタンをクリックします。

46.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

47.　以下の項目を指定します。

- IKE 認証鍵
  - 鍵識別　→文字列
  - 鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  - 暗号アルゴリズム　→aes-cbc-128
  - 認証（ハッシュ）アルゴリズム　→hmac-sha1
  - DH グループ　→modp768（グループ 1）



48.　［保存］ボタンをクリックします。

49.　IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

50.　以下の項目を指定します。

- 接続先監視
  送信元 IP アドレス　→2001:db8:1111:3::1

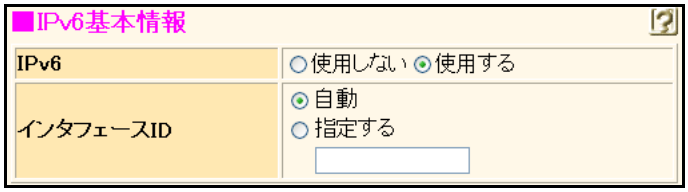
51.　［保存］ボタンをクリックします。

52.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

53.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動



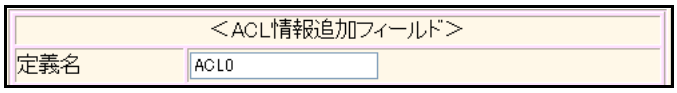
54.　［保存］ボタンをクリックします。

55.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

56.　以下の項目を指定します。

- 定義名　→ACL0



57.　［追加］ボタンをクリックします。

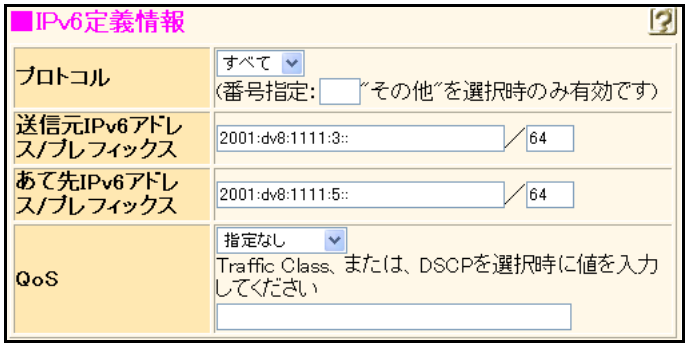
「ACL 定義情報（ACL0）」ページが表示されます。

58.　「IPv6 定義情報」をクリックします。

「IPv6 定義情報」ページが表示されます。

59.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元　IPv6アドレス/プレフィックス長　→2001:db8:1111:3::/64
- あて先　IPv6アドレス/プレフィックス長　→2001:db8:1111:5::/64
- QoS　→指定なし



60.　［保存］ボタンをクリックします。

61.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

62.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

63.　「ネットワーク情報」でネットワーク名がvpn-honの［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon)」ページが表示されます。

64.　「IPv6関連」をクリックします。

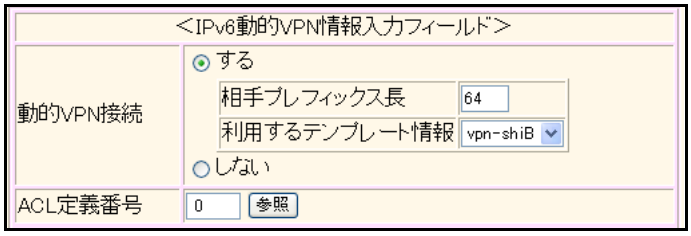
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

65.　「IPv6動的VPN情報」をクリックします。

66.　以下の項目を指定します。

- 動的VPN接続　→する
  相手プレフィックス長　→64
  利用するテンプレート情報　→vpn-shiB
- ACL定義番号　→0

補足　「ACL定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



67.　［追加］ボタンをクリックします。

68.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B を設定する

「支社 A を設定する」を参考に、支社 B を設定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-hon

「ネットワーク情報」-「IPv6 関連」

「IPv6 基本情報」

- IPv6　→使用する

「IPv6 スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:4::/64
- メトリック値　→1
- 優先度　→0
- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:3::/64
- メトリック値　→1
- 優先度　→2

「接続先情報」

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→2001:db8:1111:2::66
  自側エンドポイント　→2001:db8:1111:1::67

「IPsec 情報」

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→1234567890abcdefghijklmnopqrstuvwxyz
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）

「動的VPN情報」-「クライアント関連情報」-「ドメイン情報」

「基本情報」

- ドメイン名　→ example.com
- サーバ情報
  - アドレス　→ 2001:db8:1111:4::1
  - ポート番号　→ 5070
  - 認証ID　→ shisyaBid
  - 認証パスワード　→ shisyaBpass
- 有効期間　→ 1 時間
- 優先度　→ 10
- セッション更新間隔　→ 更新する
  - 時間　→ 5 分
- クライアントIPアドレス　→ 2001:db8:1111:5::1
- VPN通信
  - 利用インタフェース　→ rmt0
- 経路情報の優先度
  - IPv6　→ 1

「自側ネットワーク情報」

- 動的VPNで接続する自側ネットワーク　→ 2001:db8:1111:5::/24
- 動的VPNサーバ登録　→ する

「テンプレート情報」

- テンプレート名　→vpn-shiA
- 接続種別　→IPsec/IKE（動的VPN）

「テンプレート情報（vpn-shiA）」-「共通情報」

「基本情報」

- 使用するrmtインタフェース　→rmt10から10インタフェースを予約
- 自側エンドポイント　→2001:db8:1111:1::67

「テンプレート情報（vpn-shiA）」-「動的VPN関連」

「基本情報」

- ドメイン情報　→使用する

「テンプレート情報（vpn-shiA）」-「IPsec/IKE関連」

「IPsec情報」

- SAの設定
  - 暗号アルゴリズム　→aes-cbc-128
  - 認証アルゴリズム　→hmac-sha1
  - PFS時のDHグループ　→modp768（グループ1）

「IKE情報」

- IKE認証鍵
  - 鍵識別　→文字列
  - 鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SAの設定
  - 暗号アルゴリズム　→aes-cbc-128
  - 認証（ハッシュ）アルゴリズム　→hmac-sha1
  - DHグループ　→modp768（グループ1）

「接続制御情報」

- 接続先監視
  送信元 IP アドレス　→2001:db8:1111:5::1

「テンプレート情報（vpn-shiA)」-「IPv6 関連」

「IPv6 基本情報」

- IPv6　→使用する
- インタフェース ID　→自動

「ACL 情報」

- 定義名　→ACL0

「ACL 定義情報（ACL0)」-「IPv6 定義情報」

- プロトコル　→すべて
- 送信元　IPv6 アドレス / プレフィックス長　→2001:db8:1111:5::/64
- あて先　IPv6 アドレス / プレフィックス長　→2001:db8:1111:3::/64
- QoS　→指定なし

「相手情報」-「ネットワーク情報」

「ネットワーク（vpn-hon）情報」-「IPv6 関連」

「IPv6 動的 VPN 情報」

- 動的 VPN 接続　→する
  相手プレフィックス長　→64
  利用するテンプレート情報　→vpn-shiA
- ACL 定義番号　→0

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

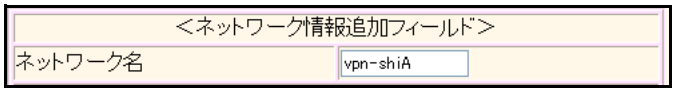
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shiA



4.　［追加］ボタンをクリックします。

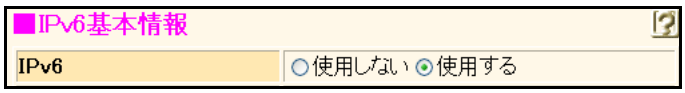
「ネットワーク情報（vpn-shiA)」ページが表示されます。

5.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

6.　以下の項目を指定します。

- IPv6　→使用する



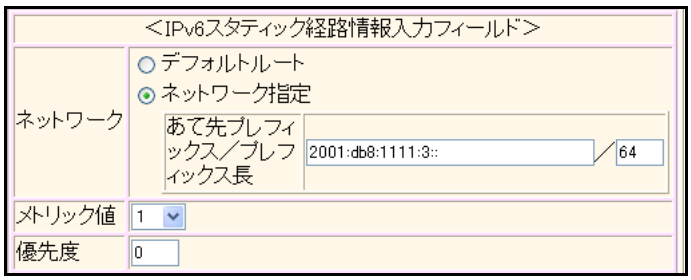
7.　［保存］ボタンをクリックします。

8.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

9.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:3::/64
- メトリック値　→1
- 優先度　→0



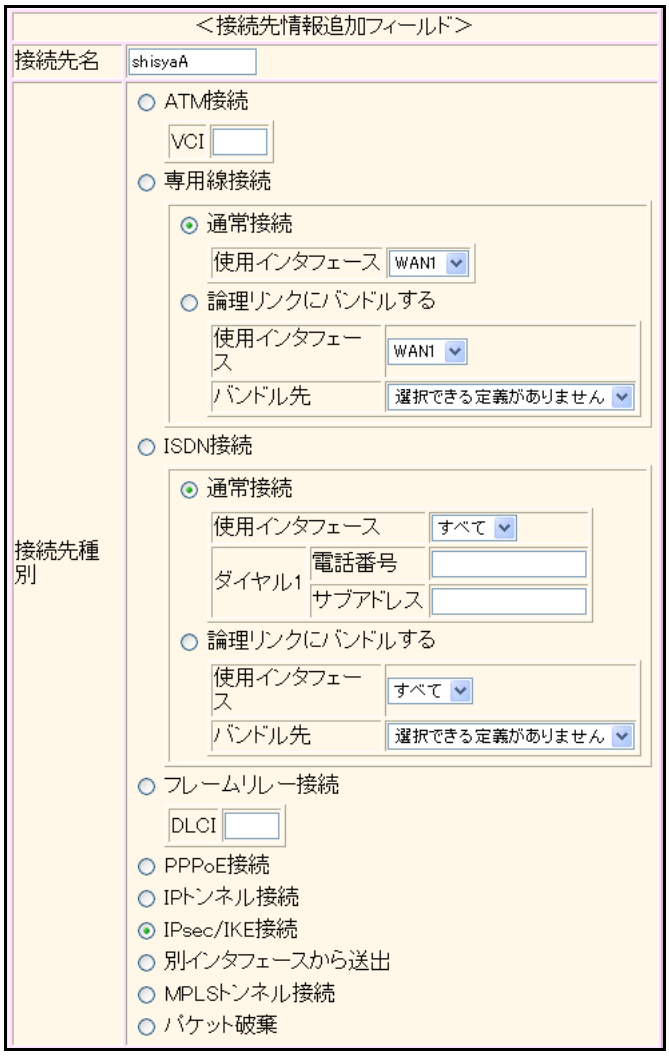
10.　［追加］ボタンをクリックします。

11.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

12.　以下の項目を指定します。

- 接続先名　→shisyaA
- 接続先種別　→IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

13.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 鍵交換モード　→Main Mode 使用
  相手側エンドポイント　→2001:db8:1111:1::66
  自側エンドポイント　→2001:db8:1111:2::66

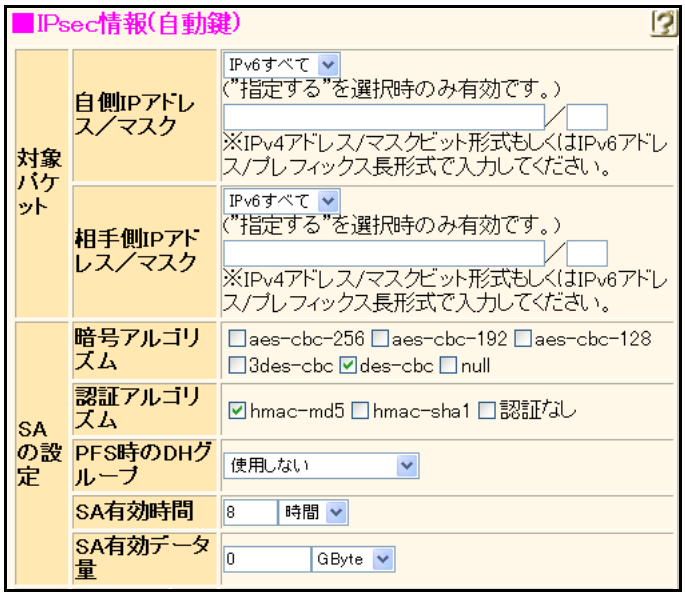
15.　［保存］ボタンをクリックします。

16.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

17.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv6 すべて
  相手側 IP アドレス／マスク　→IPv6 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5



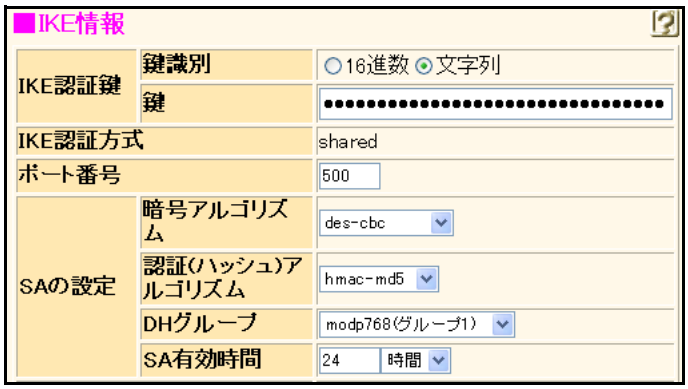
18.　［保存］ボタンをクリックします。

19.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

20.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証（ハッシュ）アルゴリズム　→hmac-md5
  DH グループ　→modp768（グループ 1）



21.　［保存］ボタンをクリックします。

22.　手順 1.～21. を参考に、支社 B を設定します。

23.　設定メニューのルータ設定で「AAA 情報」をクリックします。

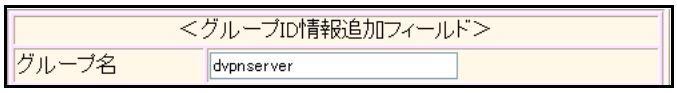
「AAA 情報」ページが表示されます。

24.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

25.　以下の項目を指定します。

- グループ名　→dvpnserver



26.　［追加］ボタンをクリックします。

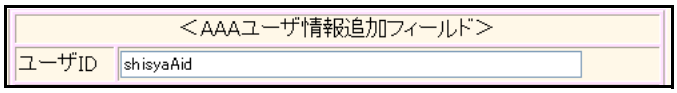
「グループ ID 情報（0）」と設定項目が表示されます。

27.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

28.　以下の項目を指定します。

- ユーザ ID　→shisyaAid



29.　［追加］ボタンをクリックします。

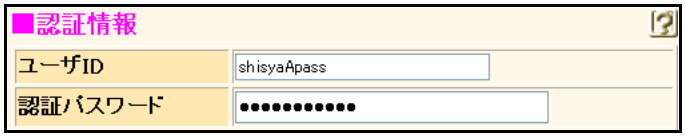
「AAA ユーザ情報（0）」と設定項目が表示されます。

30.　「認証情報」をクリックします。

「認証情報」が表示されます。

31.　以下の項目を指定します。

- 認証パスワード　→shisyaApass



32.　［保存］ボタンをクリックします。

33.　手順 23. ～ 31. を参考に、支社 B を設定します。

34.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

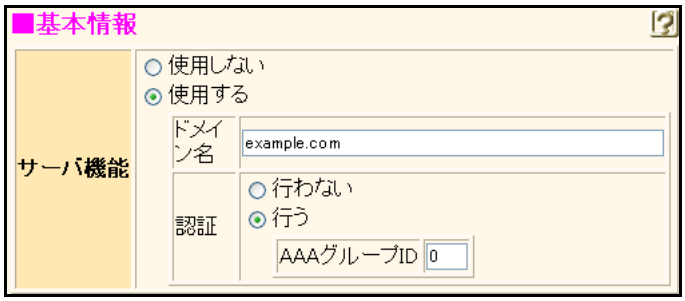
「動的 VPN 情報」ページが表示されます。

35.　「サーバ関連情報」をクリックします。

サーバ関連情報の設定項目と「基本情報」が表示されます。

36.　以下の項目を指定します。

- サーバ機能　→使用する
  ドメイン名　→example.com
  認証　→行う
  AAA グループ ID　→0



37.　［保存］ボタンをクリックします。

38.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.18 NAT トラバーサルを使用した可変 IP アドレスでの VPN

適用機種　全機種

接続するたびに IP アドレスが変わる環境で NAT トラバーサルを使って、VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

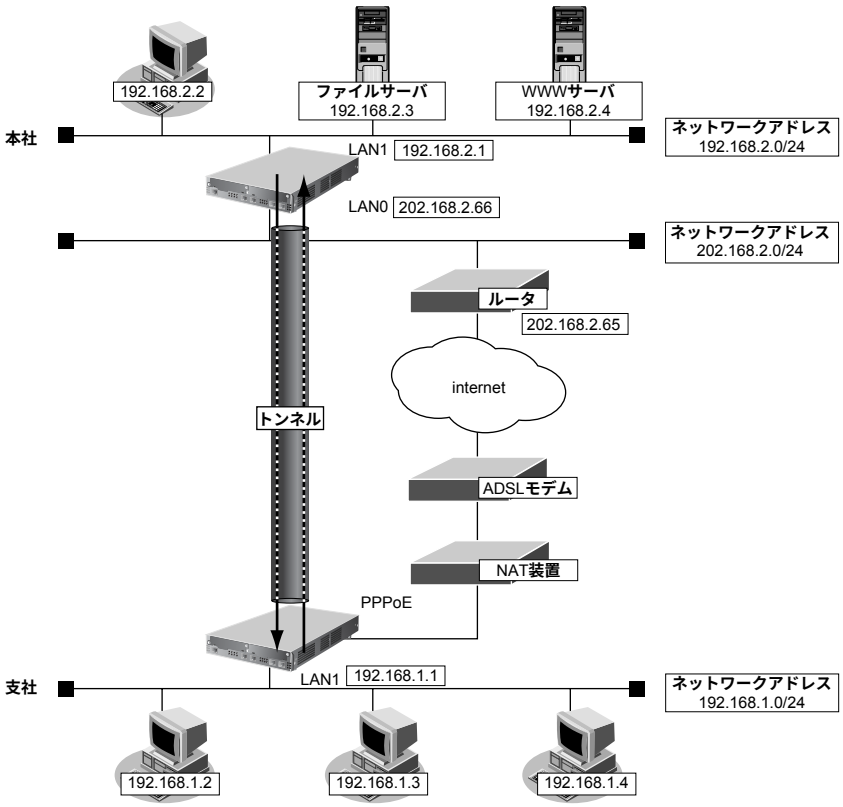
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- ネットワーク名　：vpn-shi
- 接続先名　：shisya
- IPsec/IKE 区間　：202.168.2.66 － 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768
- IKE NAT トラバーサル機能　：使用する

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

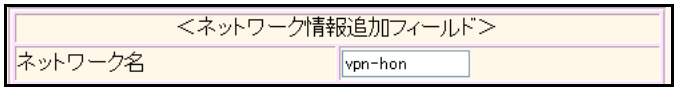
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

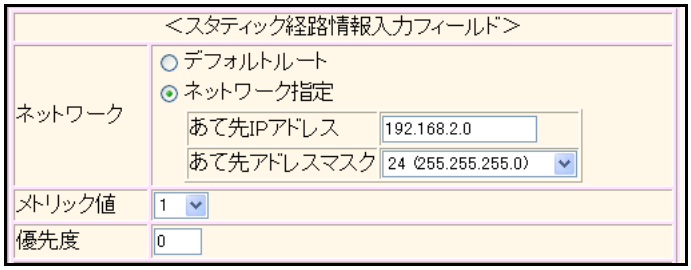
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



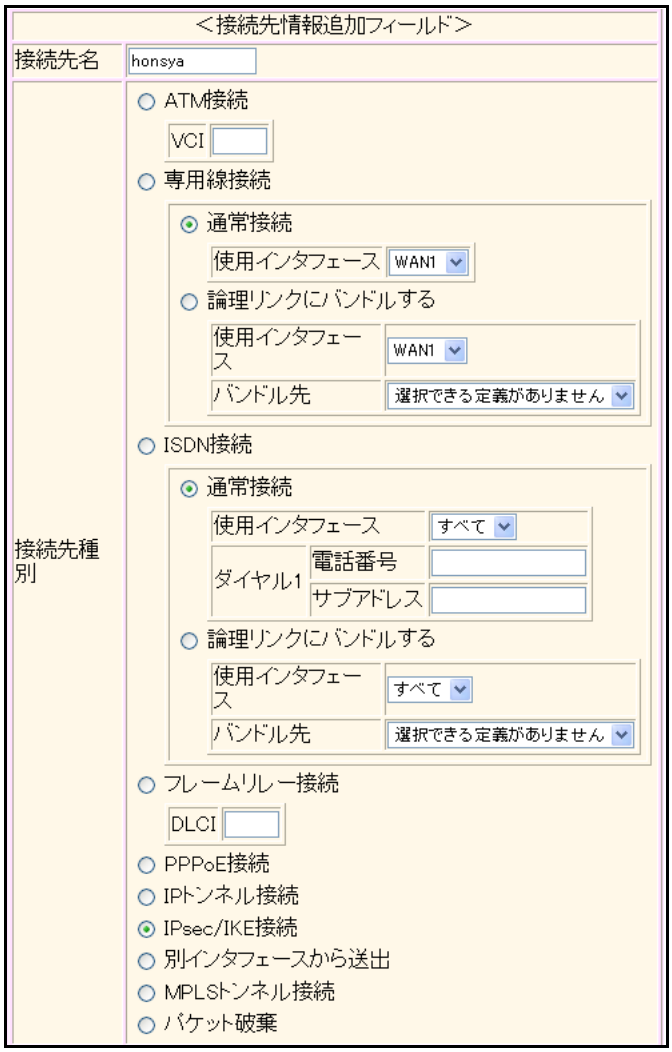
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



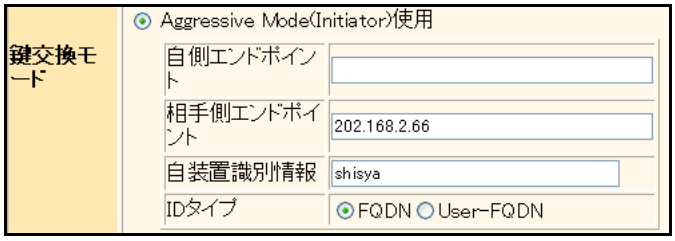
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisya



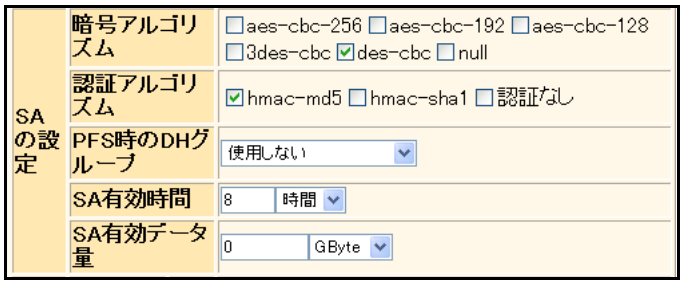
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



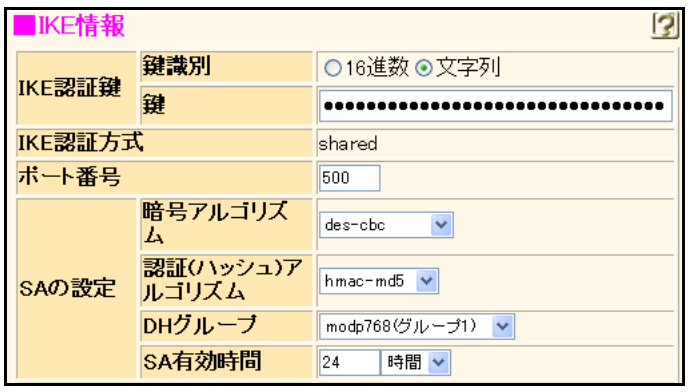
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）
- NAT トラバーサル機能　→使用する



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本社を設定する（Responder）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

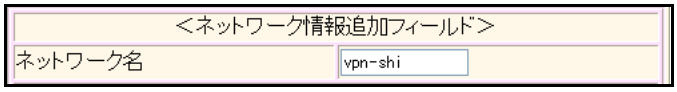
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-shi



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-shi)」ページが表示されます。

5.　「IP 関連」をクリックします。

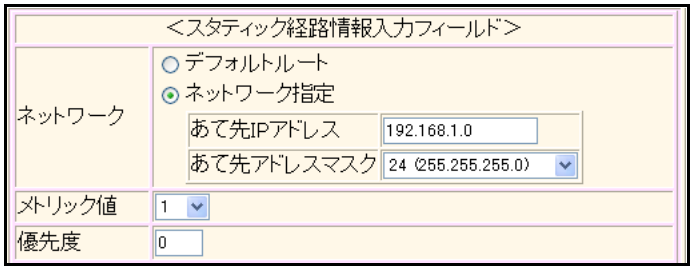
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



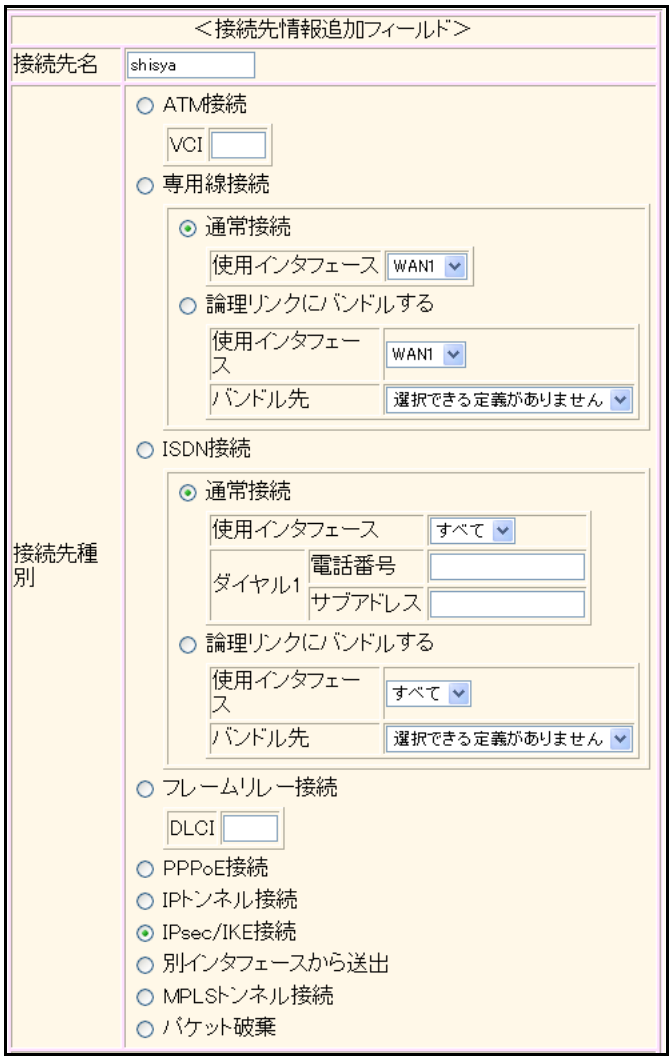
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→shisya
- 接続先種別　→IPsec/IKE 接続



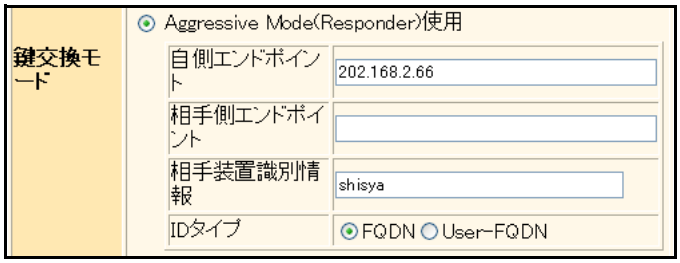
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  相手装置識別情報　→shisya



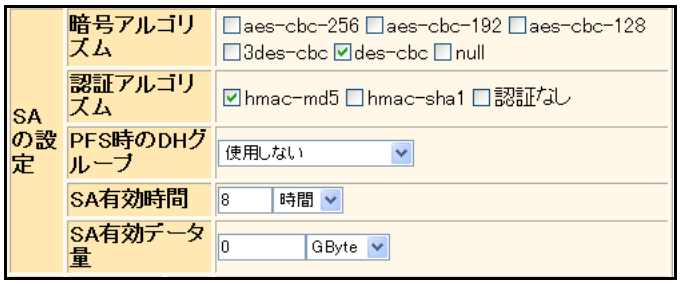
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



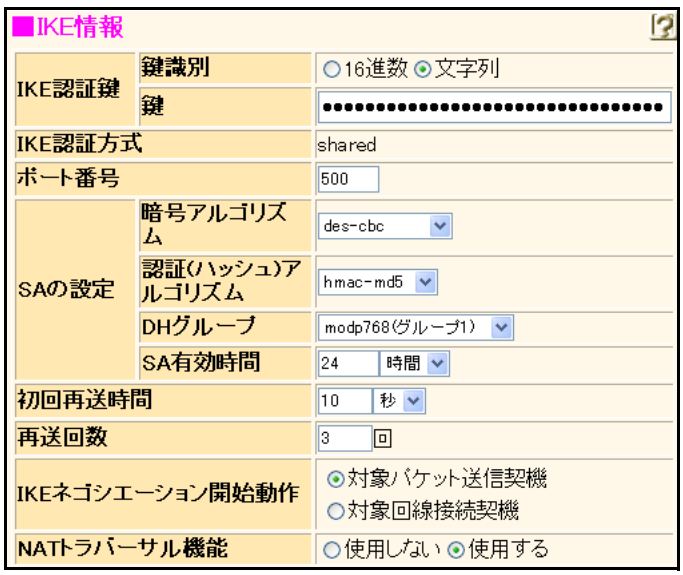
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）
- NAT トラバーサル機能　→使用する



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.19 テンプレート着信機能（AAA 認証）および NAT トラバーサルを使用した可変 IP アドレスでの VPN

適用機種　全機種

IPsec 機能、テンプレート機能および NAT トラバーサルを使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

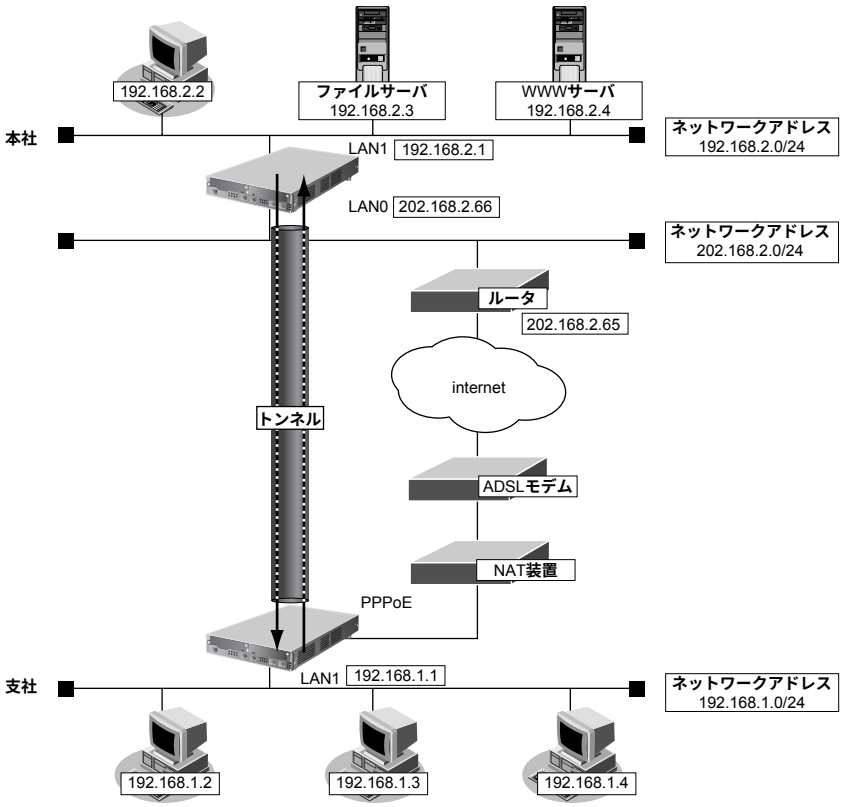
● 前提条件

[支社（PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証 ID　：userid（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス：202.168.2.65



● 設定条件

[支社]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE 区間　：支社 － 202.168.2.66
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[本社]

- テンプレート名　：vpn-shi
- IPsec/IKE 区間　：202.168.2.66 － 支社
- IPsec 対象範囲　：IPsec 相手情報を使用するすべてのパケット

[共通]

- 鍵交換タイプ　：Aggressive Mode
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：des-cbc
- IPsec 認証アルゴリズム　：hmac-md5
- IPsec DH グループ　：なし
- IKE 支社 ID ／ ID タイプ　：shisya（自装置名）／ FQDN
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：des-cbc
- IKE 認証アルゴリズム　：hmac-md5
- IKE DH グループ　：modp768
- IKE NAT トラバーサル機能　：使用する

こんな事に気をつけて

- **テンプレート着信機能（AAA 認証）を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。**
- **ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。**
  Main Mode の場合　：相手側 IPsec トンネルアドレス
  Aggressive Mode の場合　：相手側の装置識別情報

ヒント

◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（Initiator）

1.　設定メニューのルータ設定で「相手情報」をクリックします。

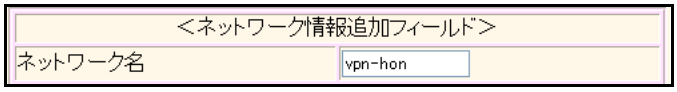
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→vpn-hon



4.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

5.　「IP 関連」をクリックします。

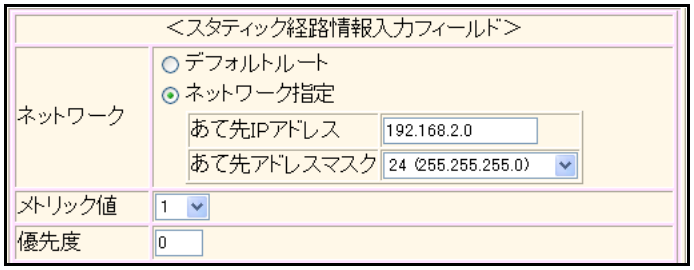
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



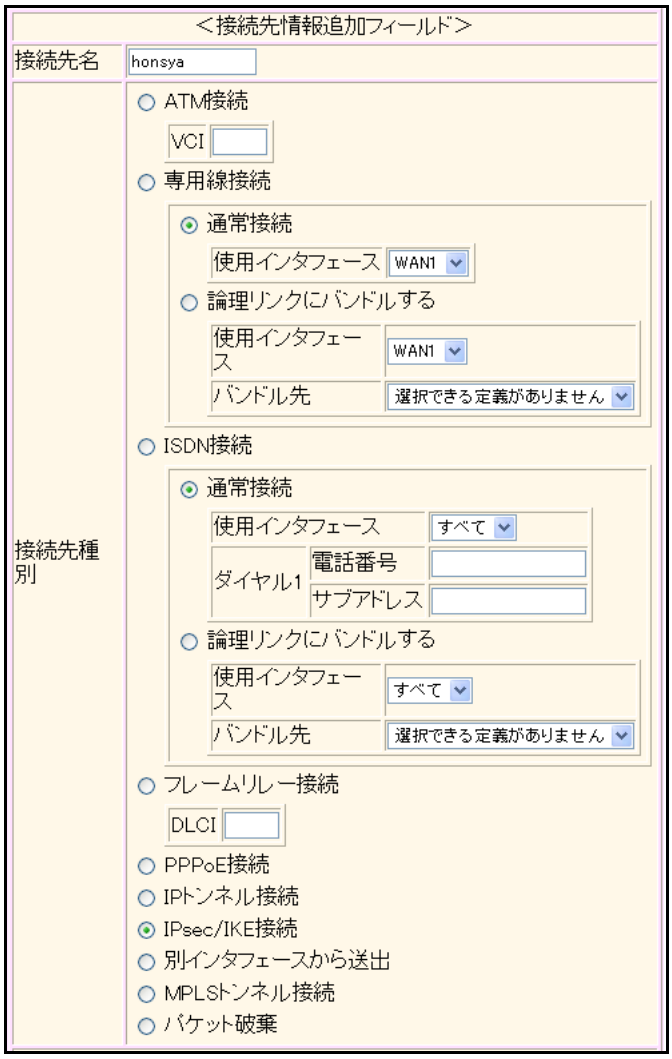
8.　［追加］ボタンをクリックします。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→honsya
- 接続先種別　→IPsec/IKE 接続



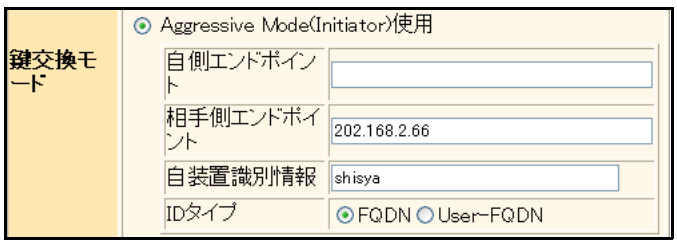
機種により、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→shisya



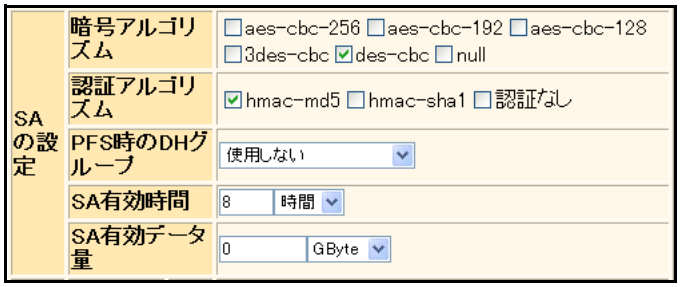
13.　［保存］ボタンをクリックします。

14.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

15.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



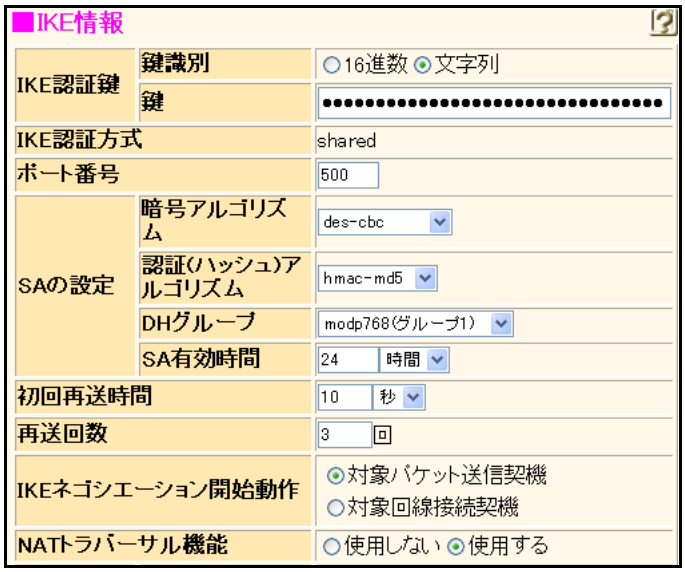
16.　［保存］ボタンをクリックします。

17.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）
- NAT トラバーサル機能　→使用する



19.　［保存］ボタンをクリックします。

20.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

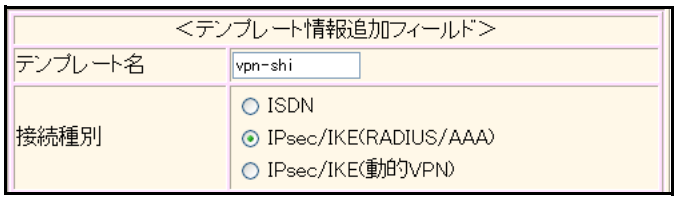
本社を設定する（Responder）

1.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

2.　以下の項目を指定します。

- テンプレート名　→vpn-shi
- 接続種別　→IPsec/IKE（RADIUS/AAA）



機種により、接続先種別の表示が上記の画面とは異なります。

3.　［追加］ボタンをクリックします。

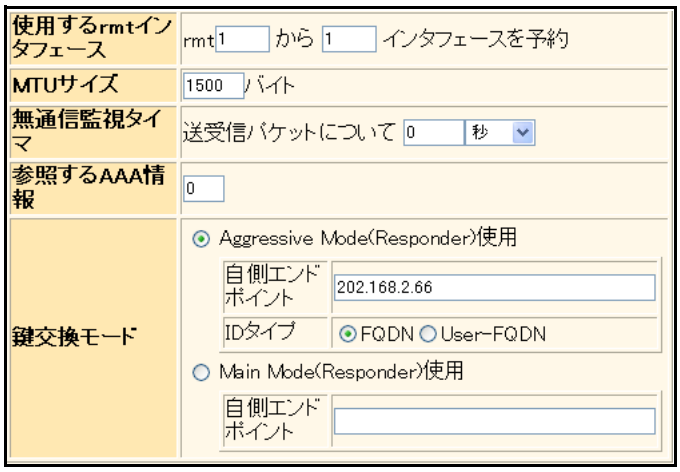
「テンプレート情報（vpn-shi）」ページが表示されます。

4.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt1 から 1 インタフェースを予約
- 参照する AAA 情報　→0
- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.2.66
  ID タイプ　→FQDN



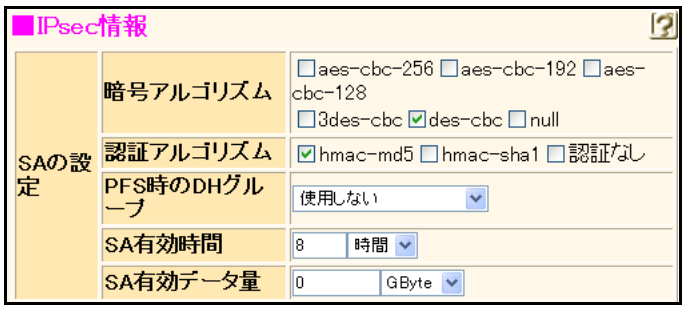
6.　［保存］ボタンをクリックします。

7.　テンプレート情報（vpn-shi）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

8.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



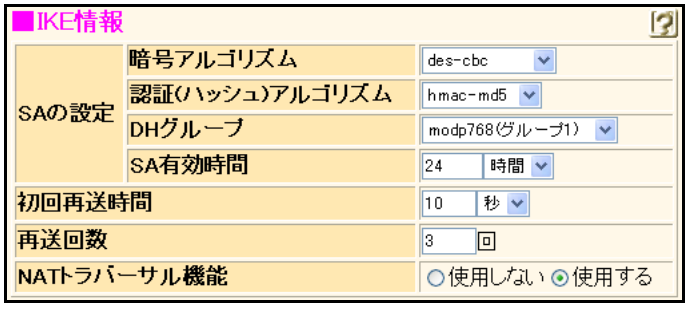
9.　［保存］ボタンをクリックします。

10.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

11.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）
- NAT トラバーサル機能　→使用する



12.　［保存］ボタンをクリックします。

13.　設定メニューのルータ設定で「AAA 情報」をクリックします。

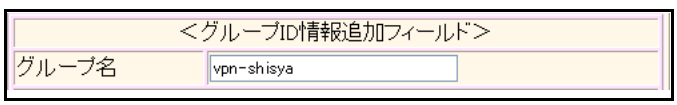
「AAA 情報」ページが表示されます。

14.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

15.　以下の項目を指定します。

- グループ名　→ vpn-shisya



16.　［追加］ボタンをクリックします。

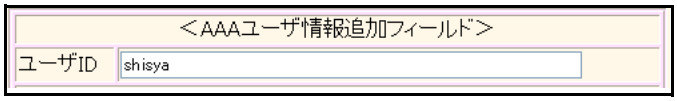
「グループ ID 情報（0）」と設定項目が表示されます。

17.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

18.　以下の項目を指定します。

- ユーザ ID　→shisya



19.　［追加］ボタンをクリックします。

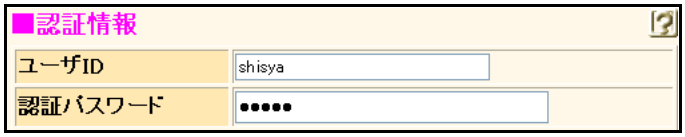
「AAA ユーザ情報（0）」と設定項目が表示されます。

20.　「認証情報」をクリックします。

「認証情報」が表示されます。

21.　以下の項目を指定します。

- ユーザ ID　→shisya
- 認証パスワード　→shisya



22.　［追加］ボタンをクリックします。

23.　AAA ユーザ情報（0）の設定項目の「IP 関連」をクリックします。

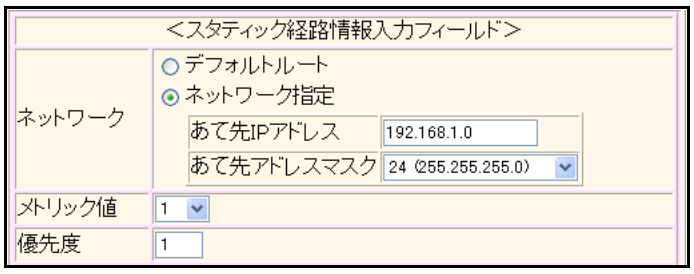
IP 関連の設定項目と「IP 基本情報」が表示されます。

24.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

25.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→1



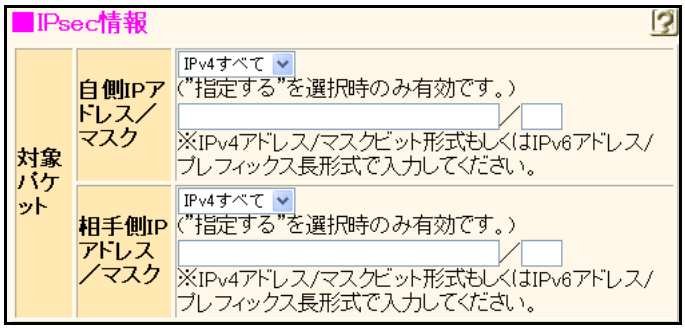
26.　［追加］ボタンをクリックします。

27.　AAA ユーザ情報（0）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

28.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→IPv4 すべて



29.　［保存］ボタンをクリックします。

30.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

31.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→abcdefghijklmnopqrstuvwxyz1234567890

32.　［保存］ボタンをクリックします。

33.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.14.20 接続先情報（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN

適用機種　全機種

IPsec 機能、動的VPN 情報交換機能、接続先およびテンプレート機能を使って、自動鍵交換でVPN を構築する場合の設定方法を説明します。

ここでは以下の条件によって、支社および本社はPPPoE でインターネットに接続され、動的VPN サーバはグローバルアドレス空間の終端装置として本装置が接続されていることを前提とします。

● 前提条件

[本社（PPPoE 常時接続)]

- ローカルネットワークIPv4 アドレス　：192.168.0.1/24
- PPPoE ユーザ認証ID　：userid0（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass0（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能　：マルチNAT を使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社A（PPPoE 常時接続)]

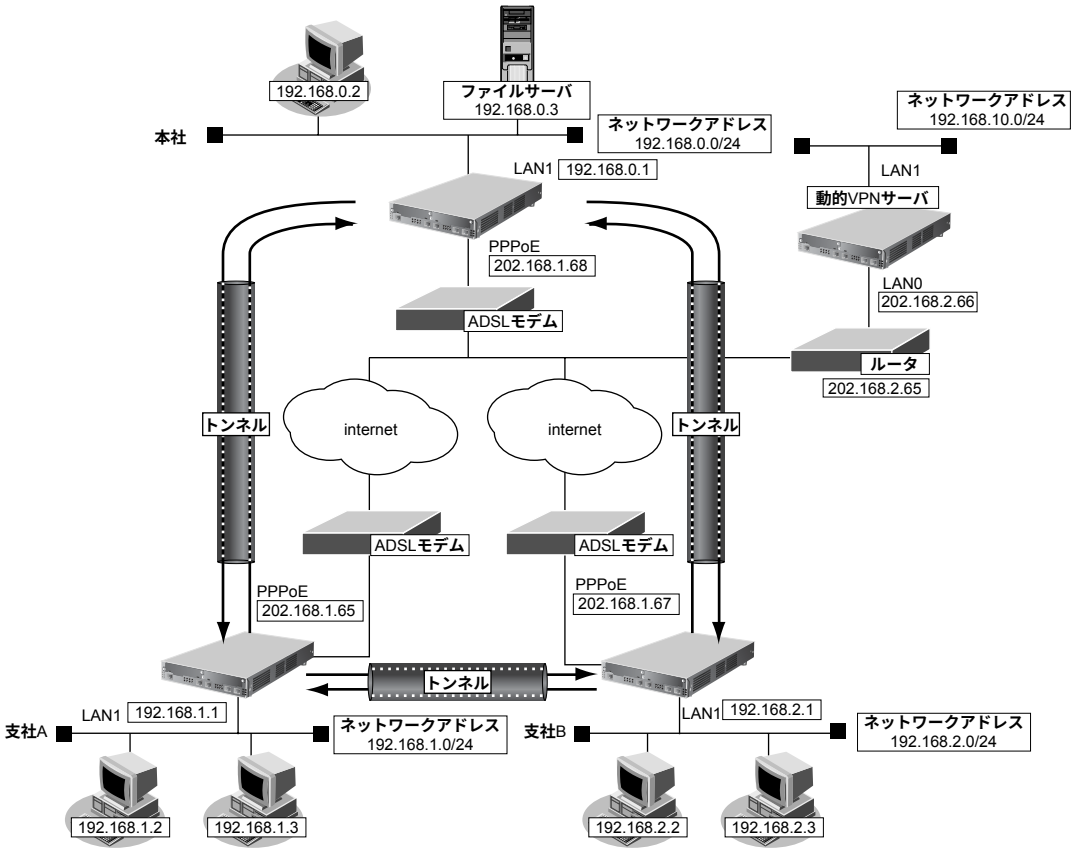
- ローカルネットワークIPv4 アドレス　：192.168.1.1/24
- PPPoE ユーザ認証ID　：userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass1（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能　：マルチNAT を使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[支社B（PPPoE 常時接続)]

- ローカルネットワークIPv4 アドレス　：192.168.2.1/24
- PPPoE ユーザ認証ID　：userid2（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード　：userpass2（プロバイダから提示された内容）
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能　：マルチNAT を使用する
- ネットワーク名　：internet
- 接続先名　：ISP-1

[動的VPN サーバ]

- ローカルネットワークIPv4 アドレス　：192.168.10.1/24
- インターネットプロバイダから割り当てられた固定IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4 アドレス　：202.168.2.65



● 設定条件（動的VPNサーバ-本社、支社A、B）

[本社（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE 区間　：本社－ 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.0.1
- ESPのプライベートアドレス　：192.168.0.1

[支社A（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE区間　：支社A－ 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.1.1
- ESPのプライベートアドレス　：192.168.1.1

[支社B（Initiator)]

- ネットワーク名　：vpn-srv
- 接続先名　：dvpn-srv
- IPsec/IKE区間　：支社B－ 202.168.2.66
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.2.1
- ESPのプライベートアドレス　：192.168.2.1

[動的VPNサーバ（Responder)]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- IPsec/IKE区間　：202.168.2.66 ー本社
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiA
- 接続先名　：shisyaA
- IPsec/IKE区間　：202.168.2.66 ー支社A
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット
- ネットワーク名　：vpn-shiB
- 接続先名　：shisyaB
- IPsec/IKE区間　：202.168.2.66 ー支社B
- IPsec対象範囲　：IPsec相手情報を使用するすべてのパケット

[共通（本社、支社A、B-動的VPNサーバ)]

- 鍵交換タイプ　：Aggressive Mode
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec認証アルゴリズム　：hmac-md5
- IPsec DHグループ　：なし
- IKE本社 ID/IDタイプ　：honsya （自装置識別情報）/FQDN
- IKE支社A ID/IDタイプ　：shisyaA（自装置識別情報）/FQDN
- IKE支社B ID/IDタイプ　：shisyaB（自装置識別情報）/FQDN
- IKE本社 IKE認証鍵　：1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
- IKE支社A IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890
- IKE支社B IKE認証鍵　：1234567890abcdefghijklmnopqrstuvwxyz
- IKE認証方法　：shared
- IKE暗号アルゴリズム　：des-cbc
- IKE認証アルゴリズム　：hmac-md5
- IKE DHグループ　：modp768

● 設定条件（本社 - 支社A、B）

[本社]

- テンプレート名　：vpn-shi
- IKE（UDP：500番ポート）のプライベートアドレス
  ：192.168.0.1
- ESPのプライベートアドレス　：192.168.0.1
- テンプレート接続先監視アドレス　：192.168.0.1

[支社 A]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- テンプレート名　：vpn-shiB
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.1.1
- ESP のプライベートアドレス　：192.168.1.1
- 接続先監視アドレス　：192.168.1.1-192.168.0.1
- テンプレート接続先監視アドレス　：192.168.1.1

[支社 B]

- ネットワーク名　：vpn-hon
- 接続先名　：honsya
- テンプレート名　：vpn-shiA
- IKE（UDP：500 番ポート）のプライベートアドレス　：192.168.2.1
- ESP のプライベートアドレス　：192.168.2.1
- 接続先監視アドレス　：192.168.2.1-192.168.0.1
- テンプレート接続先監視アドレス　：192.168.2.1

● 設定条件（動的 VPN 接続）

[本社 - 支社 A/B 間の動的 VPN 共通設定]

- クライアント情報　：0
- サーバ情報
  アドレス　：192.168.10.1
  ポート番号　：5070
- 有効期間　：1 時間
- セッション更新間隔　：5 分
- ドメイン名　：example.com
- VPN 通信
  利用インタフェース　：rmt0
- 動的 VPN クライアントの優先度　：10
- 動的 VPN IPv4 経路情報の優先度　：1
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-128
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsecDH グループ　：modp768
- IKE 認証鍵　：ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法　：shared
- IKE 暗号アルゴリズム　：aes-cbc-128
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768

[本社の動的 VPN 設定]

- サーバ情報
  認証 ID　：honsyaid
  認証パスワード　：honsyapass
- クライアントの IP アドレス（本社）　：192.168.0.1
- ローカル ID　：honsya

[支社 A の動的 VPN 設定]

- サーバ情報
  認証 ID　：shisyaAid
  認証パスワード　：shisyaApass
- クライアントの IP アドレス（支社 A）　：192.168.1.1

[支社 B の動的 VPN 設定]

- サーバ情報
  認証 ID　：shisyaBid
  認証パスワード　：shisyaBpass
- クライアントの IP アドレス（支社 B）　：192.168.2.1

[動的 VPN サーバ設定]

- サーバ機能　：使用する
  ドメイン名　：example.com
  認証　：行う
  AAA グループ ID　：0
- AAA ユーザ情報（本社認証情報）
  ユーザ ID　：honsyaid
  認証パスワード　：honsyapass
- AAA ユーザ情報（支社 A 認証情報）
  ユーザ ID　：shisyaAid
  認証パスワード　：shisyaApass
- AAA ユーザ情報（支社 B 認証情報）
  ユーザ ID　：shisyaBid
  認証パスワード　：shisyaBpass

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet）」ページが表示されます。

4.　「IP 関連」をクリックします。

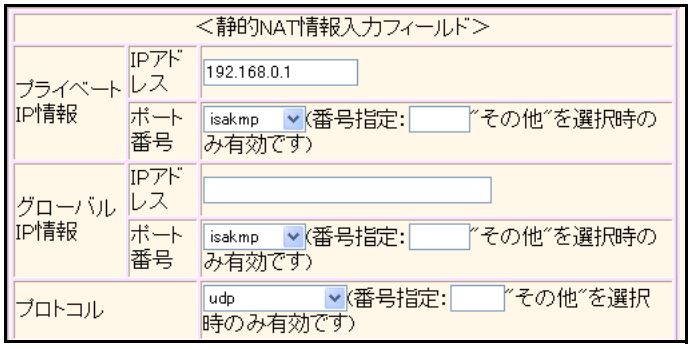
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.0.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6. ～ 7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.0.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　画面上部の「相手情報」をクリックします。

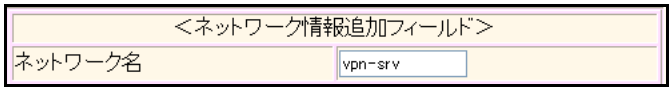
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→ vpn-srv



12.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-srv）」ページが表示されます。

13.　「IP 関連」をクリックします。

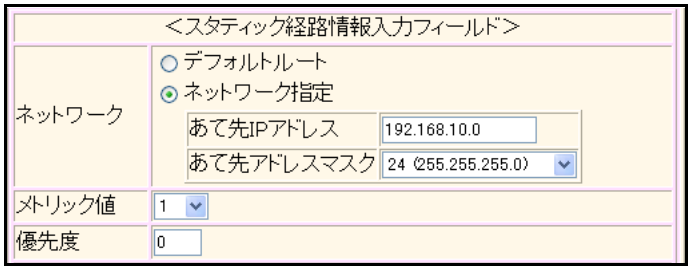
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.10.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



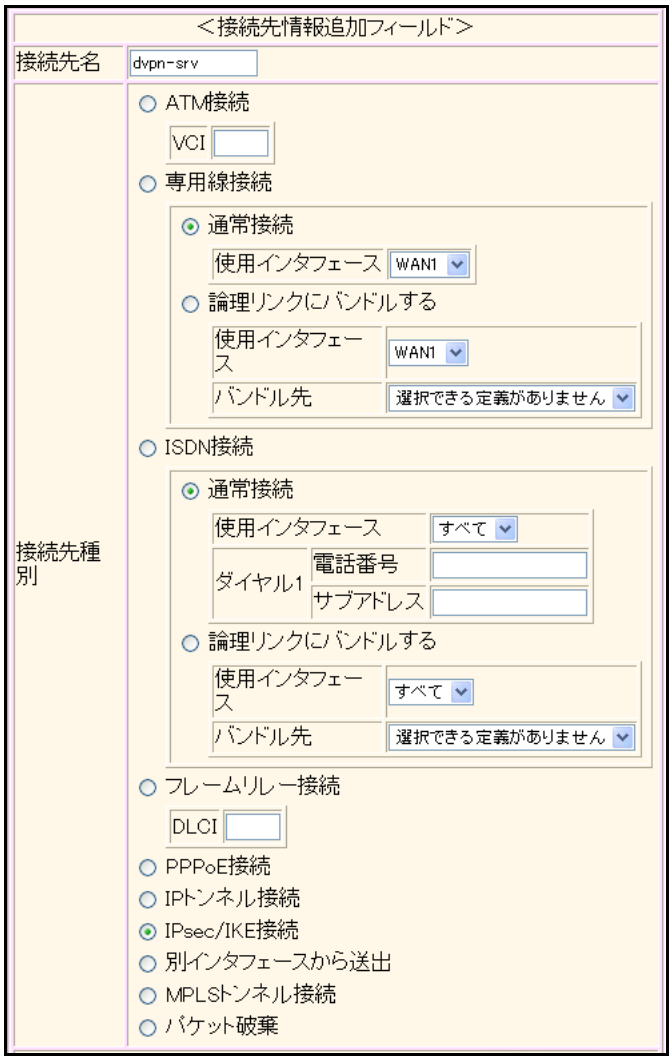
16.　［追加］ボタンをクリックします。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→dvpn-srv
- 接続先種別　→IPsec/IKE 接続



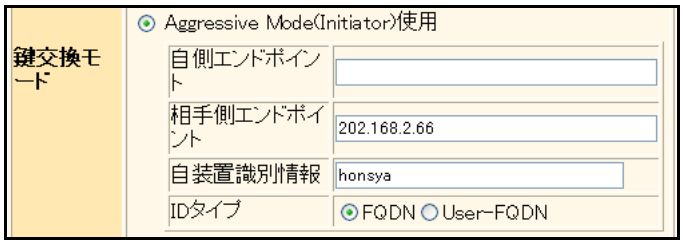
機種により、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.2.66
  自装置識別情報　→honsya



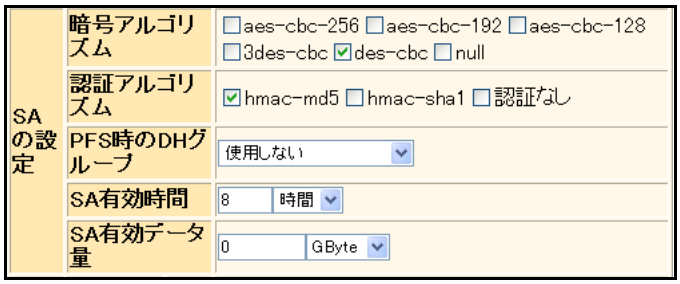
21.　［保存］ボタンをクリックします。

22.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

23.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5



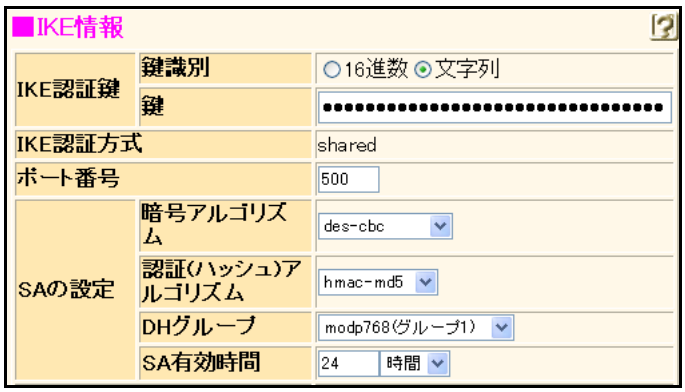
24.　［保存］ボタンをクリックします。

25.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

26.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）



27.　［保存］ボタンをクリックします。

28.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

「動的 VPN 情報」ページが表示されます。

29.　「クライアント関連情報」をクリックします。

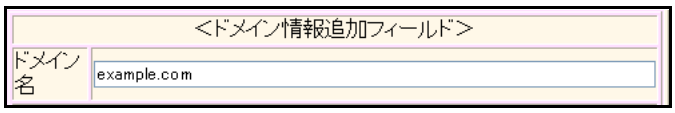
クライアント関連情報の設定項目と「基本情報」が表示されます。

30.　クライアント関連情報の設定項目の「ドメイン情報」をクリックします。

「ドメイン情報」が表示されます。

31.　以下の項目を指定します。

- ドメイン名　→example.com



32.　［追加］ボタンをクリックします。

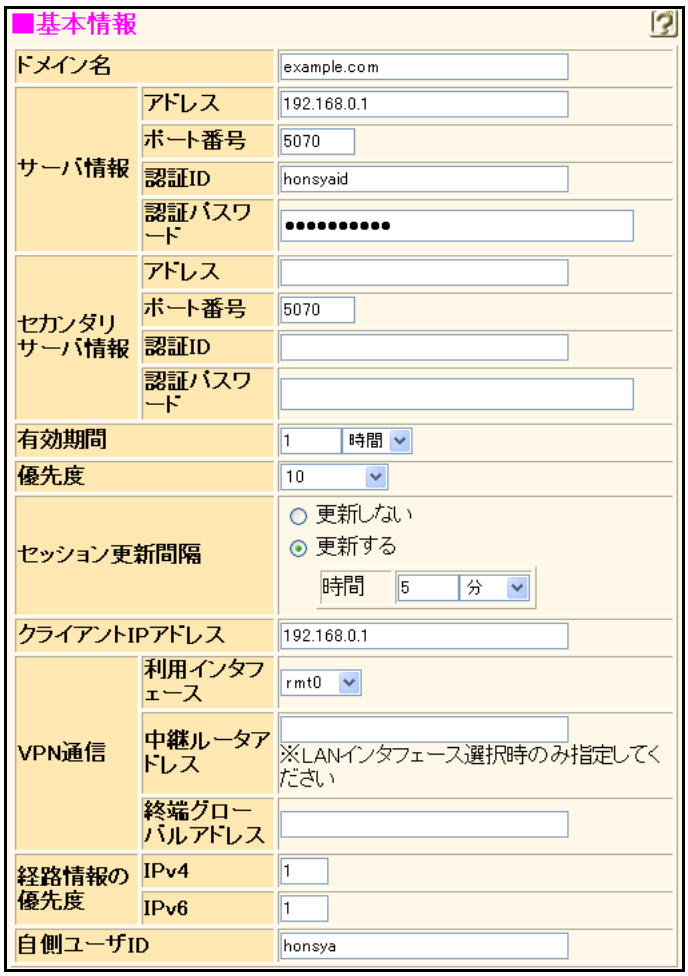
「ドメイン情報（0)」ページが表示されます。

33.　「基本情報」をクリックします。

「基本情報」が表示されます。

34.　以下の項目を指定します。

- ドメイン名　→example.com
- サーバ情報
  アドレス　→192.168.10.1
  ポート番号　→5070
  認証 ID　→honsyaid
  認証パスワード　→honsyapass
- 有効期間　→1 時間
- 優先度　→10
- セッション更新間隔　→更新する
  時間　→5 分
- クライアント IP アドレス　→192.168.0.1
- VPN 通信
  利用インタフェース　→rmt0
- 経路情報の優先度
  IPv4　→1
  IPv6　→1
- 自側ユーザ ID　→honsya



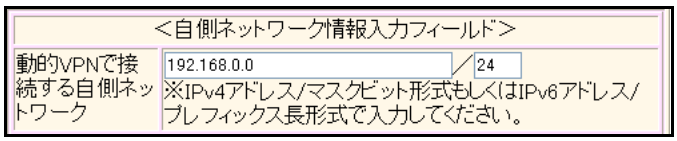
35.　［保存］ボタンをクリックします。

36.　ドメイン情報（0）の設定項目の「自側ネットワーク情報」をクリックします。

「自側ネットワーク情報」が表示されます。

37.　以下の項目を指定します。

- 動的 VPN で接続する自側ネットワーク　　→ 192.168.0.0/24



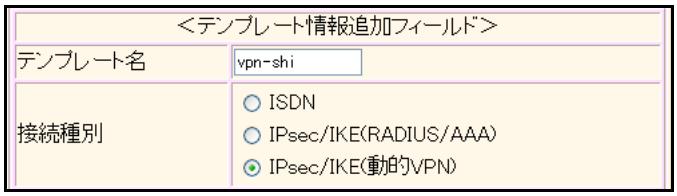
38.　［追加］ボタンをクリックします。

39.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

40.　以下の項目を指定します。

- テンプレート名　→vpn-shi
- 接続種別　→IPsec/IKE（動的 VPN）



機種により、接続先種別の表示が上記の画面とは異なります。

41.　［追加］ボタンをクリックします。

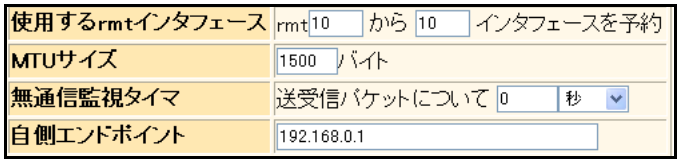
「テンプレート情報（vpn-shi）」ページが表示されます。

42.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

43.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt10 から 10 インタフェースを予約
- 自側エンドポイント　→192.168.0.1



44.　［保存］ボタンをクリックします。

45.　テンプレート情報（vpn-shi）の設定項目の「動的 VPN 関連」をクリックします。

動的 VPN 関連の設定項目と「基本情報」が表示されます。

46.　以下の項目を指定します。

- ドメイン情報　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- ドメイン情報　→0（example.com）

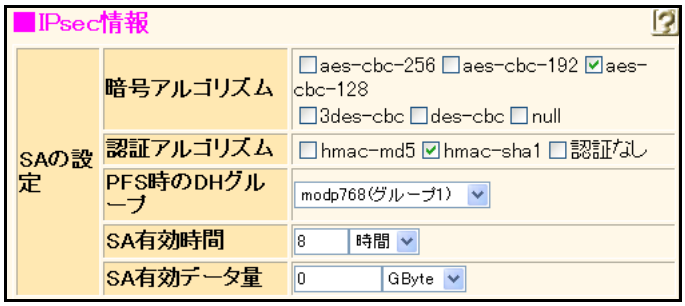
47.　［保存］ボタンをクリックします。

48.　テンプレート情報（vpn-shi）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

49.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証アルゴリズム　→hmac-sha1
  PFS 時の DH グループ　→modp768（グループ 1）



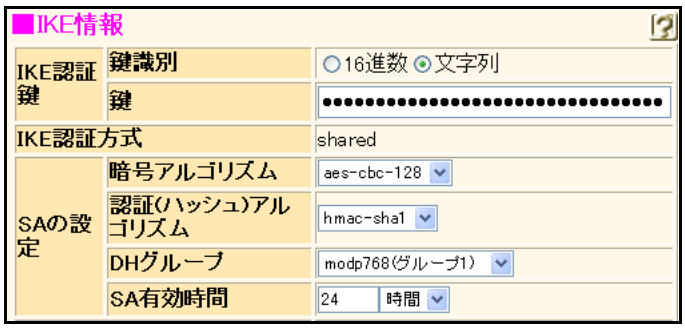
50.　［保存］ボタンをクリックします。

51.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

52.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp768（グループ 1）



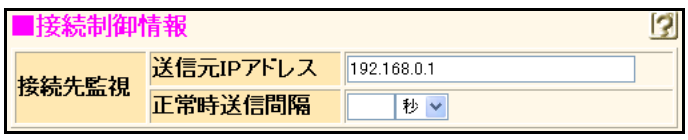
53.　［保存］ボタンをクリックします。

54.　IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

55.　以下の項目を指定します。

- 接続先監視
  送信元 IP アドレス　→192.168.0.1



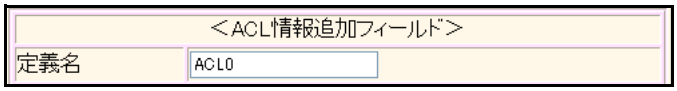
56.　［保存］ボタンをクリックします。

57.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

58.　以下の項目を指定します。

- 定義名　→ACL0



59.　［追加］ボタンをクリックします。

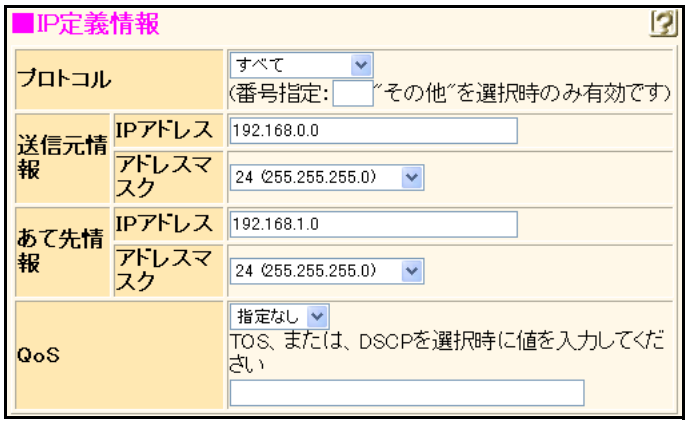
「ACL 情報（ACL0）」ページが表示されます。

60.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

61.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- Qos　→指定なし



62.　［保存］ボタンをクリックします。

63.　手順 61. ～ 62. を参考に、以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- Qos　→指定なし

64.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

65.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

66.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet）」ページが表示されます。

67.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

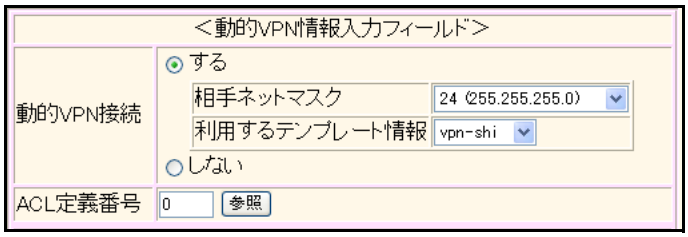
68.　「動的 VPN 情報」をクリックします。

「動的 VPN 情報」が表示されます。

69.　以下の項目を指定します。

- 動的 VPN 接続　→する
  相手ネットマスク　→24（255.255.255.0）
  利用するテンプレート情報　→vpn-shi
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



70.　［追加］ボタンをクリックします。

71.　手順 69. ～ 70. を参考に、以下の項目を指定します。

- 動的 VPN 接続　→する
  相手ネットマスク　→24（255.255.255.0）
  利用するテンプレート情報　→vpn-shi
- ACL 定義番号　→1

72.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 A を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が internet の［修正］ボタンをクリックします。

「ネットワーク情報（internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

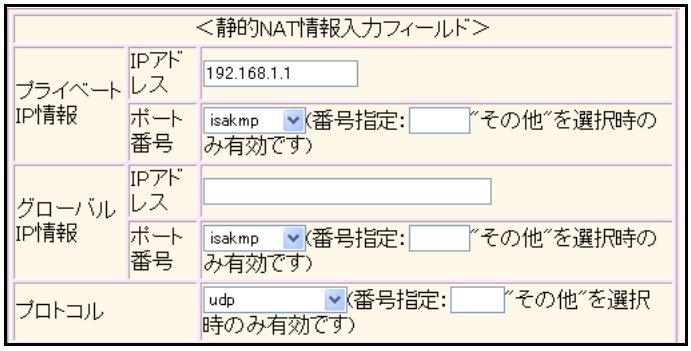
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



7.　［追加］ボタンをクリックします。

8.　手順 6. ～ 7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

9.　「本社を設定する」の手順 9. ～ 27. を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ vpn-srv

「ネットワーク情報（vpn-srv）」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.10.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ dvpn-srv
- 接続先種別　→ IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→ Aggressive Mode（Initiator）使用
  相手側エンドポイント　→ 202.168.2.66
  自装置識別情報　→ shisyaA

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）

10.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

「動的 VPN 情報」ページが表示されます。

11.　「クライアント関連情報」をクリックします。

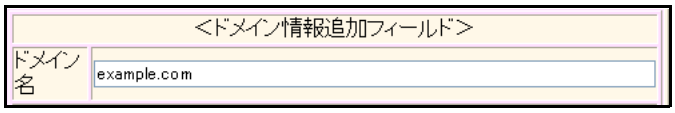
クライアント関連情報の設定項目と「基本情報」が表示されます。

12.　クライアント関連情報の設定項目の「ドメイン情報」をクリックします。

「ドメイン情報」が表示されます。

13.　以下の項目を指定します。

- ドメイン名　→ example.com



14.　［追加］ボタンをクリックします。

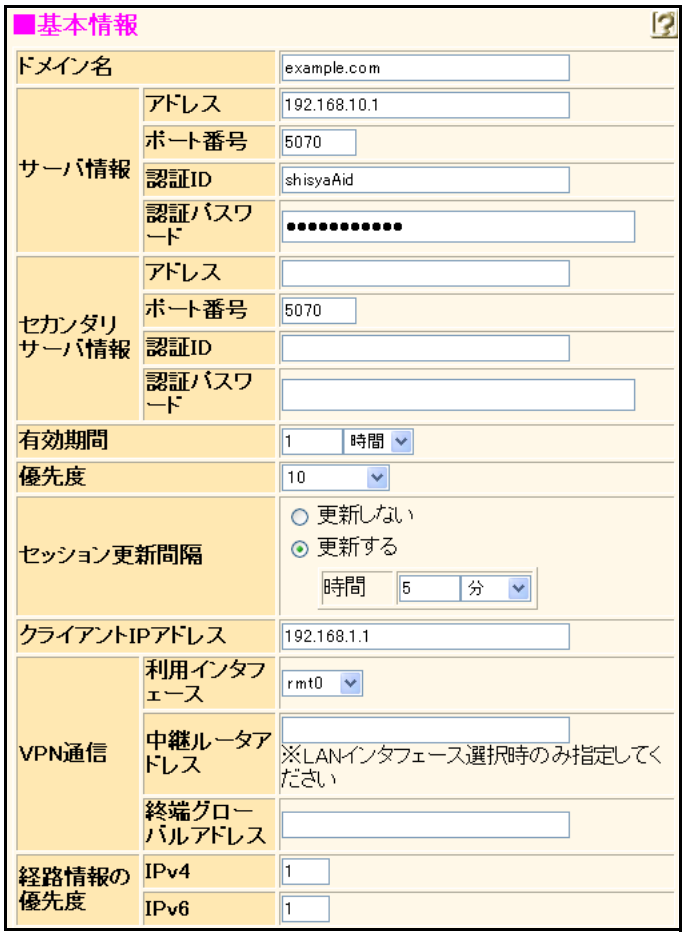
「ドメイン情報（0)」ページが表示されます。

15.　「基本情報」をクリックします。

「基本情報」が表示されます。

16.　以下の項目を指定します。

- ドメイン名　→example.com
- サーバ情報
  アドレス　→192.168.10.1
  ポート番号　→5070
  認証 ID　→shisyaAid
  認証パスワード　→shisyaApass
- 有効期間　→1 時間
- 優先度　→10
- セッション更新間隔　→更新する
  時間　→5 分
- クライアント IP アドレス　→192.168.1.1
- VPN 通信
  利用インタフェース　→rmt0
- 経路情報の優先度
  IPv4　→1
  IPv6　→1



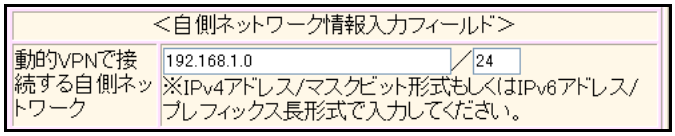
17.　［保存］ボタンをクリックします。

18.　ドメイン情報（0）の設定項目の「自側ネットワーク情報」をクリックします。

「自側ネットワーク情報」が表示されます。

19.　以下の項目を指定します。

- 動的 VPN で接続する自側ネットワーク　　→ 192.168.1.0/24



20.　［追加］ボタンをクリックします。

21.　設定メニューのルータ設定で「相手情報」をクリックします。

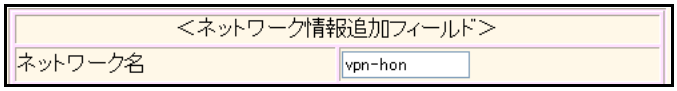
「相手情報」ページが表示されます。

22.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

23.　以下の項目を指定します。

- ネットワーク名　　→ vpn-hon



24.　［追加］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

25.　「IP 関連」をクリックします。

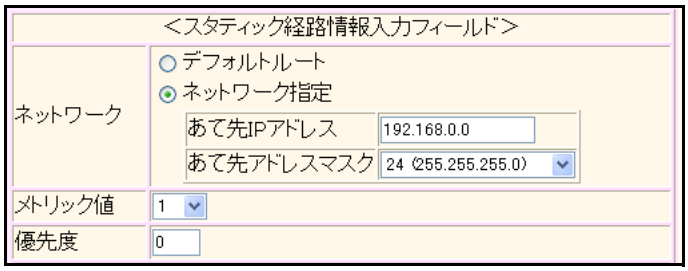
IP 関連の設定項目と「IP 基本情報」が表示されます。

26.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

27.　以下の項目を指定します。

- ネットワーク　　→ネットワーク指定
  あて先 IP アドレス　　→ 192.168.0.0
  あて先アドレスマスク　　→ 24（255.255.255.0）
- メトリック値　　→ 1
- 優先度　　→ 0



28.　［追加］ボタンをクリックします。

29.　手順 27. ～ 28. を参考に、以下の項目を指定します。

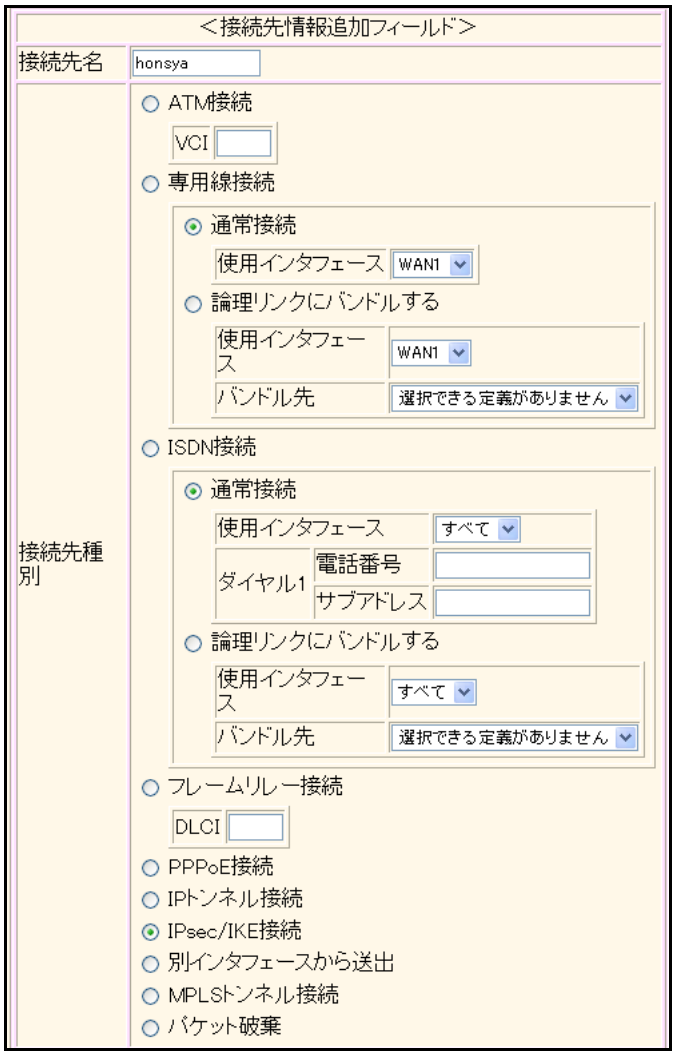
- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 2

30.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

31.　以下の項目を指定します。

- 接続先名　→honsya
- 接続種別　→IPsec/IKE 接続



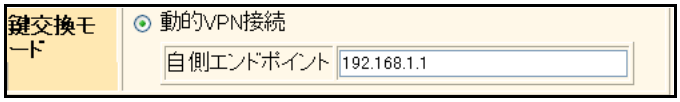
機種により、接続先種別の表示が上記の画面とは異なります。

32.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

33.　以下の項目を指定します。

- 鍵交換モード　→動的 VPN 接続
  自側エンドポイント　→ 192.168.1.1



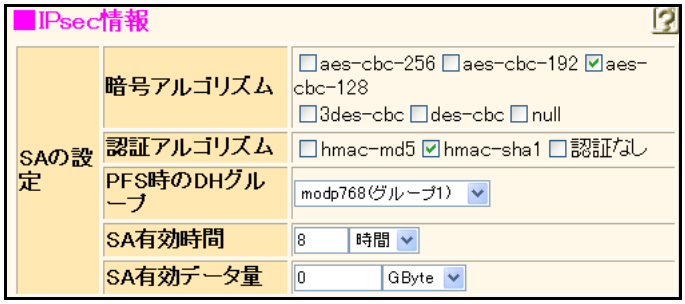
34.　［保存］ボタンをクリックします。

35.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報（動的 VPN）」が表示されます。

36.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→ aes-cbc-128
  認証アルゴリズム　→ hmac-sha1
  PFS 時の DH グループ　→ modp768（グループ 1）



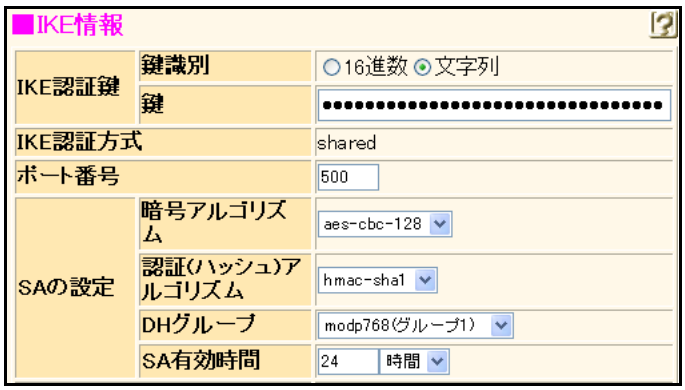
37.　［保存］ボタンをクリックします。

38.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

39.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→ aes-cbc-128
  認証（ハッシュ）アルゴリズム　→ hmac-sha1
  DH グループ　→ modp768（グループ 1）



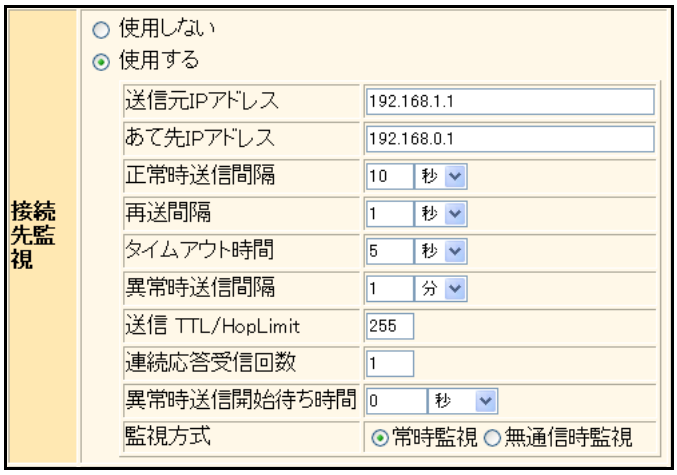
40.　［保存］ボタンをクリックします。

41.　IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

42.　以下の項目を指定します。

- 接続先監視　→使用する
  送信元 IP アドレス　→ 192.168.1.1
  あて先 IP アドレス　→ 192.168.0.1



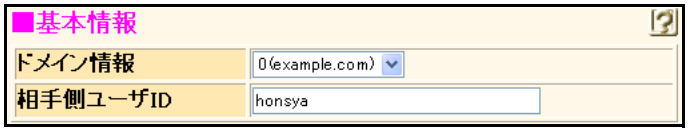
43.　［保存］ボタンをクリックします。

44.　IPsec/IKE 接続の設定項目の「動的 VPN 関連」をクリックします。

「基本情報」が表示されます。

45.　以下の項目を指定します。

- ドメイン情報　→ 0（example.com）
- 相手側ユーザ ID　→ honsya



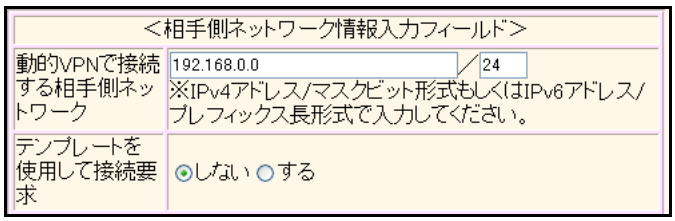
46.　［保存］ボタンをクリックします。

47.　動的 VPN 関連の設定項目の「相手側ネットワーク情報」をクリックします。

「相手側ネットワーク情報」が表示されます。

48.　以下の項目を指定します。

- 動的 VPN で接続する相手側ネットワーク　→ 192.168.0.0/24
- テンプレートを使用して接続要求　→しない



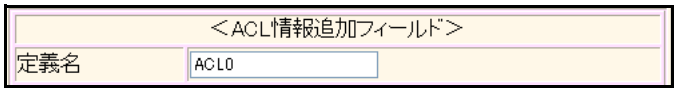
49.　［追加］ボタンをクリックします。

50.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

51.　以下の項目を指定します。

- 定義名　→ACL0



52.　［追加］ボタンをクリックします。

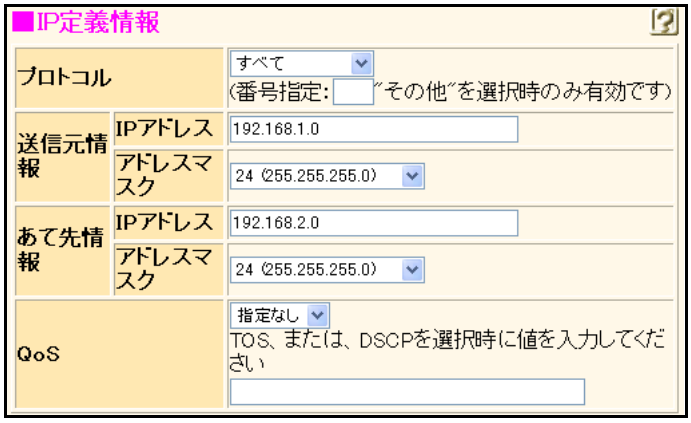
「ACL 情報（ACL0）」ページが表示されます。

53.　「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

54.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.2.0
  アドレスマスク　→24（255.255.255.0）
- Qos　→指定なし



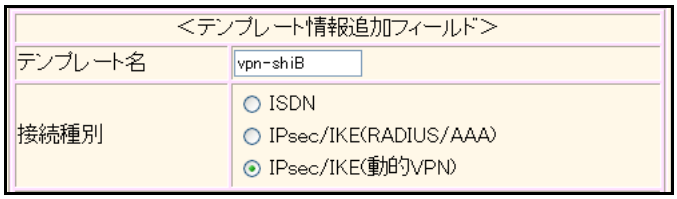
55.　［保存］ボタンをクリックします。

56.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

57.　以下の項目を指定します。

- テンプレート名　→vpn-shiB
- 接続種別　→IPsec/IKE（動的 VPN）



機種により、接続先種別の表示が上記の画面とは異なります。

58.　［追加］ボタンをクリックします。

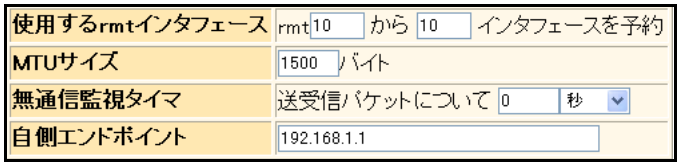
「テンプレート情報（vpn-shiB）」と設定項目が表示されます。

59.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

60.　以下の項目を指定します。

- 使用する rmt インタフェース　→rmt10 から 10 インタフェースを予約
- 自側エンドポイント　→192.168.1.1



61.　［保存］ボタンをクリックします。

62.　テンプレート情報（vpn-shiB）の設定項目の「動的 VPN 関連」をクリックします。

動的 VPN 関連の設定項目と「基本情報」が表示されます。

63.　以下の項目を指定します。

- ドメイン情報　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- ドメイン情報　→0（example.com）

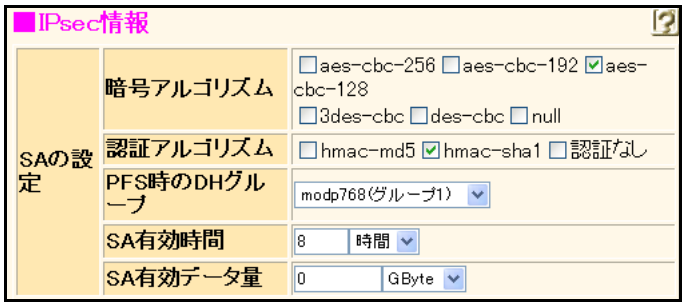
64.　［保存］ボタンをクリックします。

65.　テンプレート情報（vpn-shiB）の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

66.　以下の項目を指定します。

- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証アルゴリズム　→hmac-sha1
  PFS 時の DH グループ　→modp768（グループ 1）



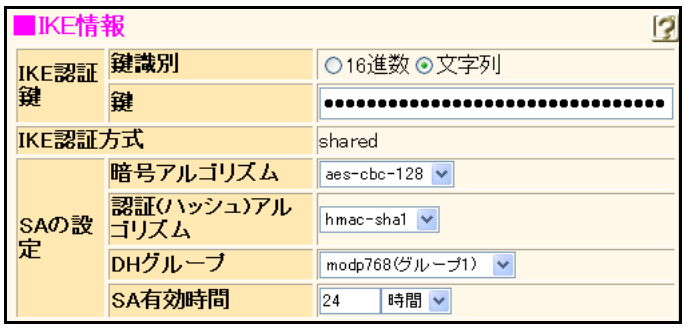
67.　［保存］ボタンをクリックします。

68.　IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

69.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→aes-cbc-128
  認証（ハッシュ）アルゴリズム　→hmac-sha1
  DH グループ　→modp768（グループ 1）



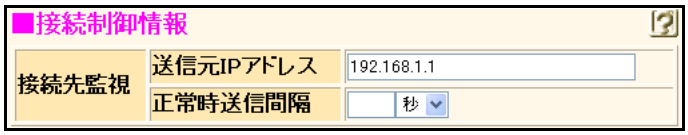
70.　［保存］ボタンをクリックします。

71.　IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

72.　以下の項目を指定します。

- 接続先監視
  送信元 IP アドレス　→192.168.1.1



73.　［保存］ボタンをクリックします。

74.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

75.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

76.　「ネットワーク情報」でネットワーク名が vpn-hon の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-hon）」ページが表示されます。

77.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

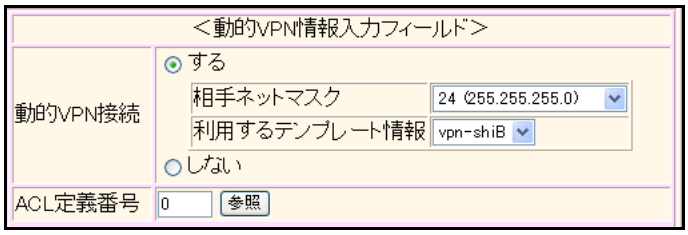
78.　「動的 VPN 情報」をクリックします。

「動的 VPN 情報」が表示されます。

79.　以下の項目を指定します。

- 動的 VPN 接続　→する
  相手ネットマスク　→24（255.255.255.0）
  利用するテンプレート情報　→vpn-shiB
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



80.　［追加］ボタンをクリックします。

81.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社 B を設定する

「支社 A を設定する」を参考に、支社 B を設定します。

「相手情報」-「ネットワーク情報」

「ネットワーク情報（internet）」-「IP 関連」

「静的 NAT 情報」

- プライベート IP 情報
  IP アドレス　→ 192.168.2.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp
- プライベート IP 情報
  IP アドレス　→ 192.168.2.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

「相手情報」-「ネットワーク情報」

- ネットワーク名　→vpn-srv

「ネットワーク情報（vpn-srv）」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.10.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0

「接続先情報」

- 接続先名　→ dvpn-srv
- 接続先種別　→ IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→ Aggressive Mode（Initiator）使用
  相手側エンドポイント　→ 202.168.2.66
  自装置識別情報　→ shisyaB

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証アルゴリズム　→ hmac-md5

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ 1234567890abcdefghijklmnopqrstuvwxyz
- SA の設定
  暗号アルゴリズム　→ des-cbc
  認証（ハッシュ）アルゴリズム　→ hmac-md5
  DH グループ　→ modp768（グループ 1）

「動的 VPN 情報」-「クライアント関連情報」

「ドメイン情報」

- ドメイン名　→ example.com

「ドメイン情報（0）」-「基本情報」

「基本情報」

- ドメイン名　→ example.com
- サーバ情報
  アドレス　→ 202.168.2.66
  ポート番号　→ 5070
  認証 ID　→ shisyaBid
  認証パスワード　→ shisyaBpass
- 有効期間　→ 1 時間
- 優先度　→ 10
- セッション更新間隔　→ 更新する
  時間　→ 5 分
- クライアント IP アドレス　→ 192.168.2.1
- VPN 通信
  利用インタフェース　→ rmt0
- 経路情報の優先度
  IPv4　→ 1
  IPv6　→ 1

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ vpn-hon

「ネットワーク情報（vpn-hon）」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.0.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0
- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 2

「接続先情報」

- 接続先名　→ honsya
- 接続先種別　→ IPsec/IKE 接続

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 鍵交換モード　→動的VPN 接続
  自側エンドポイント　→ 192.168.2.1

「IPsec 情報（動的VPN）」

- SA の設定
  暗号アルゴリズム　→ aes-cbc-128
  認証アルゴリズム　→ hmac-sha1
  PFS 時の DH グループ　→ modp768（グループ 1）

「IKE 情報（動的VPN）」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→ aes-cbc-128
  認証（ハッシュ）アルゴリズム　→ hmac-sha1
  DH グループ　→modp768（グループ 1）

「接続制御情報」

- 接続先監視　→使用する
  送信元 IP アドレス　→192.168.2.1
  あて先 IP アドレス　→192.168.0.1

「動的VPN 関連」-「基本情報」

「基本情報」

- ドメイン情報　→ 0（example.com）
- 相手側ユーザ ID　→ honsya

「相手側ネットワーク情報」

- 動的VPN で接続する相手側ネットワーク　→ 192.168.0.0/24
- テンプレートを使用して接続要求　→ しない

「ACL 情報」

- 定義名　→ACL0

「ACL 情報（ACL0）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→ 192.168.2.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）
- Qos　→指定なし

「相手情報」-「ネットワーク情報」

「ネットワーク情報（vpn-hon)」-「IP 関連」

「動的VPN 情報」

- 動的VPN 接続　→する
  相手ネットマスク　→ 24（255.255.255.0）
  利用するテンプレート情報　→ vpn-shiB
- ACL 定義番号　→ 0

「テンプレート情報」

- テンプレート名　→ vpn-shiA
- 接続種別　→ IPsec/IKE（動的VPN）

「テンプレート情報（vpn-shiA)」-「共通情報」

「基本情報」

- 使用する rmt インタフェース　→ rmt10 から 10 インタフェースを予約
- 自側エンドポイント　→ 192.168.2.1

「テンプレート情報（vpn-shiA)」-「動的VPN 関連」

「基本情報」

- ドメイン情報　→ 使用する

「テンプレート情報（vpn-shiA)」-「IPsec/IKE 関連」

「IPsec 情報」

- SA の設定
  暗号アルゴリズム　→ aes-cbc-128
  認証アルゴリズム　→ hmac-sha1
  PFS 時の DH グループ　→ modp768（グループ 1）

「IKE 情報」

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- SA の設定
  暗号アルゴリズム　→ aes-cbc-128
  認証（ハッシュ）アルゴリズム　→ hmac-sha1
  DH グループ　→ modp768（グループ 1）

「接続制御情報」

- 接続先監視
  送信元 IP アドレス　→ 192.168.2.1

動的VPN サーバを設定する

1.　設定メニューのルータ設定で「AAA 情報」をクリックします。

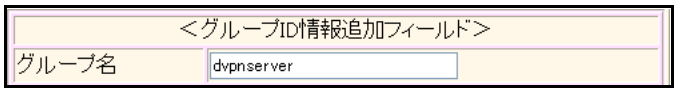
「AAA 情報」ページが表示されます。

2.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

3.　以下の項目を指定します。

- グループ名　→dvpnserver



4.　［追加］ボタンをクリックします。

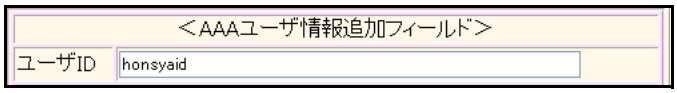
「グループ ID 情報（0）」と設定項目が表示されます。

5.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

6.　以下の項目を指定します。

- ユーザ ID　→honsyaid



7.　［追加］ボタンをクリックします。

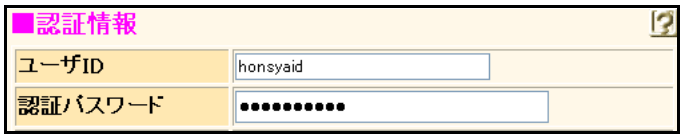
「AAA ユーザ情報（0）」と設定項目が表示されます。

8.　「認証情報」をクリックします。

「認証情報」が表示されます。

9.　以下の項目を指定します。

- ユーザ ID　→honsyaid
- 認証パスワード　→honsyapass



10.　［保存］ボタンをクリックします。

11.　手順 2.～ 10. を参考に、支社 A を設定します。

12.　手順 2.～ 10. を参考に、支社 B を設定します。

13.　設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

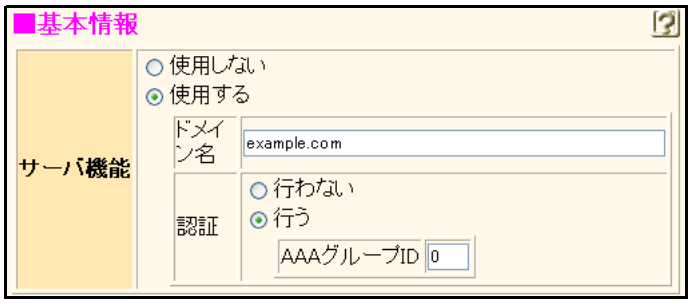
「動的 VPN 情報」ページが表示されます。

14.　「サーバ関連情報」をクリックします。

「サーバ関連情報」ページが表示されます。

15.　以下の項目を指定します。

- サーバ機能　→使用する
  ドメイン名　→example.com
  認証　→行う
  AAA グループ ID　→0



16.　［保存］ボタンをクリックします。

17.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

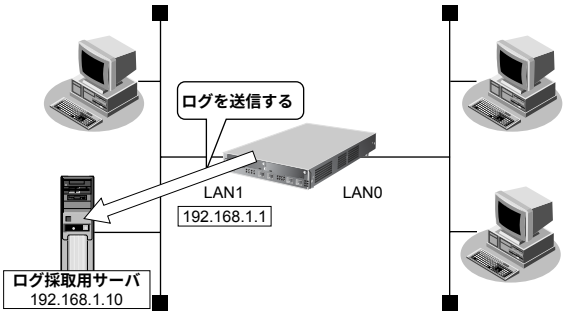
2.15 システムログを採取する

適用機種　全機種

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のシステムログサーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- PPP（着信拒否）
- IP フィルタ（遮断したパケット）
- URL フィルタ（遮断したパケット）
- NAT（遮断したパケット、変換テーブル作成）
- DHCP（配布した IPv4 アドレス、IPv6 プレフィックス）
- IDS（検出されたパケット）
- IEEE802.1X 認証（不正端末の MAC アドレス）
- MAC アドレス認証（不正端末の MAC アドレス）
- ARP 認証（不正端末の MAC アドレス）

ここでは、採取したログをサーバに送信する場合の設定方法を説明します。



● 設定条件

- 以下のセキュリティログを採取する
  - PPP
  - IP フィルタ
  - URL フィルタ
  - NAT
  - DHCP
  - IDS
  - IEEE802.1X 認証
  - MAC アドレス認証
  - ARP 認証
- ログ受信用サーバの IP アドレス　：192.168.1.10

上記の設定条件に従って設定を行う場合の設定例を示します。

システムログ情報を設定する

1.　設定メニューの基本設定で「装置情報」をクリックします。

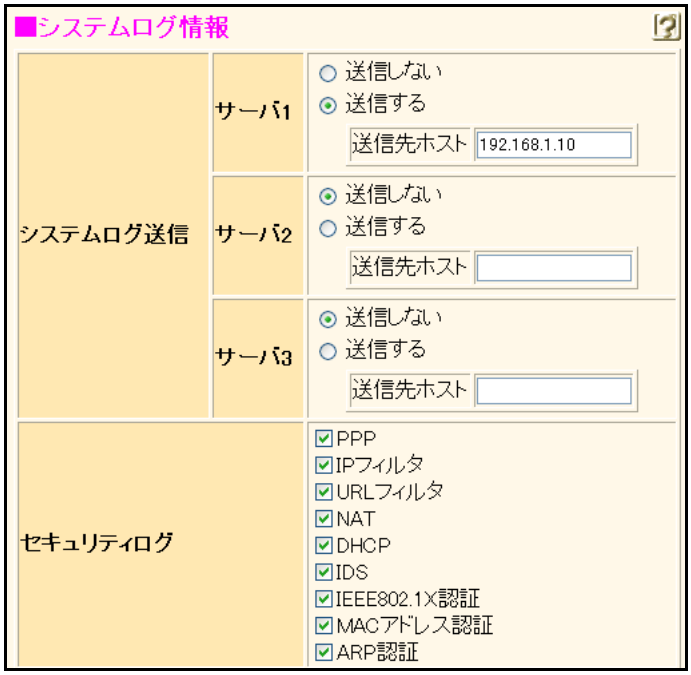
「装置情報」ページが表示されます。

2.　「システムログ情報」をクリックします。

「システムログ情報」が表示されます。

3.　以下の項目を指定します。

- システムログ送信
  サーバ 1　→送信する
  送信先ホスト　→ 192.168.1.10
- セキュリティログ　→ PPP、IP フィルタ、URL フィルタ、NAT、DHCP、IDS、IEEE802.1X 認証、MAC アドレス認証、ARP 認証



Si-R240、240B 以外では、セキュリティログの表示が上記の画面とは異なります。

4.　［保存］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

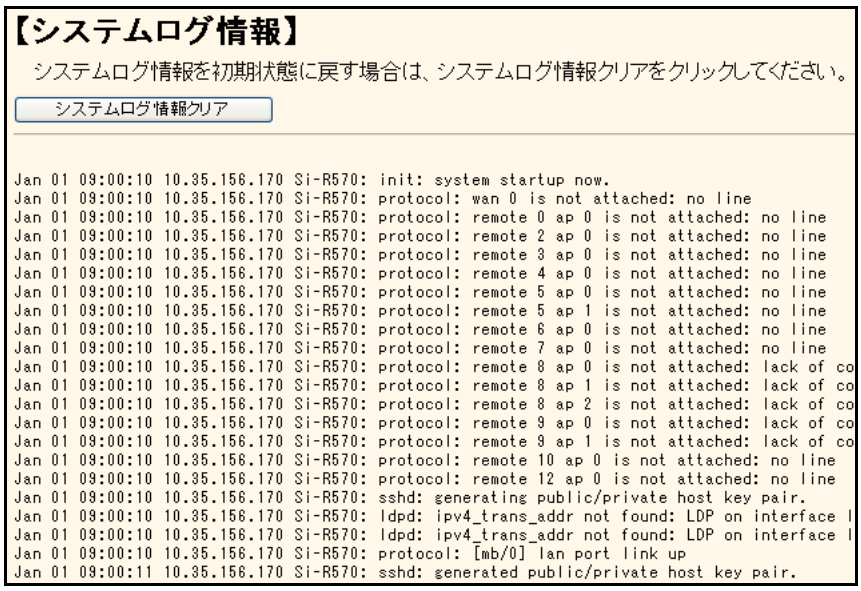
設定した内容が有効になります。

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。
ここでは、本装置で確認する方法を説明します。

1.　表示メニューの「システム関連」の「システムログ情報」をクリックします。

「システムログ情報」ページが表示されます。



2.16 マルチ NAT 機能（アドレス変換機能）を使う

適用機種　全機種

本装置のマルチ NAT 機能を使用すると、通信発生のたびにあいているグローバルアドレスを割り当てるので、限られた数のグローバルアドレスでそれ以上のパソコンを接続できます。
ここでは、静的 NAT を使って、サーバを公開する場合を例に説明します。静的 NAT は、特定のパソコンやアプリケーションに同じ IP アドレス、ポート番号を割り当てます。そのために Web を公開するような場合に適しています。

参照 Si-R シリーズ　機能説明書「2.15 マルチ NAT 機能」（P.77）

ヒント

◆ 同時に接続できる台数

機能	同時接続台数およびセッション数	備考
基本 NAT	グローバルアドレス数 セッション数制限なし	割り当て時間内は外部からの通信もできる 基本 NAT と静的 NAT で同一グローバルアドレスを使用しないでください
動的 NAT	Si-R180、180B、260B は最大 1024 セッション、 Si-R220B、220C、240、240B は最大 2000 セッション、 Si-R370 は最大 3000 セッション、 Si-R570 は最大 5000 セッションまで	外部からの通信はできない
静的 NAT	Si-R180、180B、260B は最大 64 個、 Si-R220B、220C、240、240B は最大 200 個、 Si-R370 は最大 300 個、 Si-R570 は最大 500 個まで割り当て可能	プライベートアドレスとポートをグローバルアドレスとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの通信もできる
あて先変換	Si-R180、180B、260B は最大 64 個、 Si-R220B、220C、240、240B は最大 200 個、 Si-R370 は最大 300 個、 Si-R570 は最大 500 個まで割り当て可能	グローバルアドレスをプライベートアドレスに割り当てできる

こんな事に気をつけて

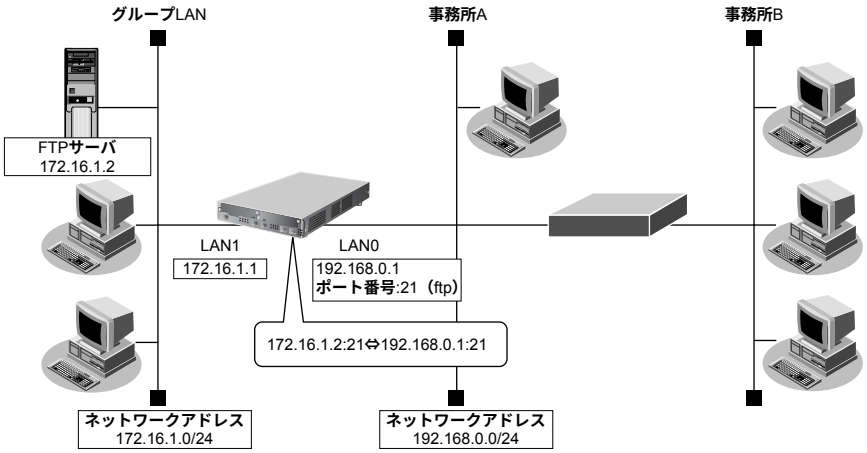
文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

2.16.1　プライベートLAN 接続でサーバを公開する

適用機種　全機種

ここでは、静的NAT を使って、FTP サーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所 A 側]

- LAN0 ポートを使用する
- 静的NAT を使用する

[グループ LAN 側]

- IP アドレス　：172.16.1.1
- ネットワークアドレス/ネットマスク　：172.16.1.0/24
- FTP サーバの IP アドレス　：172.16.1.2

上記の設定条件に従って設定を行う場合の設定例を示します。

静的NAT 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースがLAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

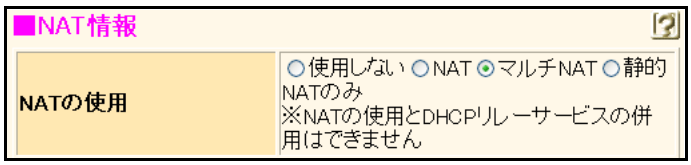
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

5.　以下の項目を指定します。

- NAT の使用　→マルチ NAT



6.　［保存］ボタンをクリックします。

7.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

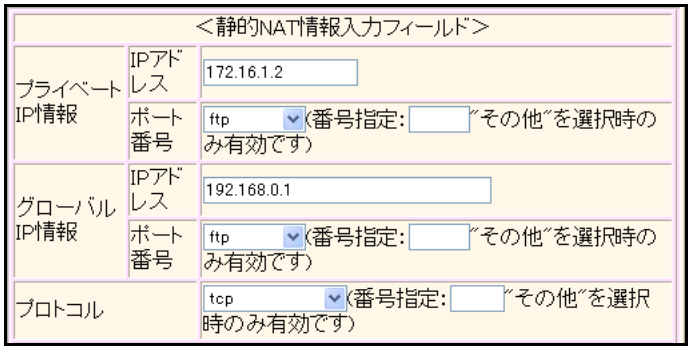
「静的 NAT 情報」が表示されます。

こんな事に気をつけて

動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないように設定してください。

8.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 172.16.1.2
  ポート番号　→ ftp
- グローバル IP 情報
  IP アドレス　→ 192.168.0.1
  ポート番号　→ ftp
- プロトコル　→ tcp



9.　［追加］ボタンをクリックします。

10.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

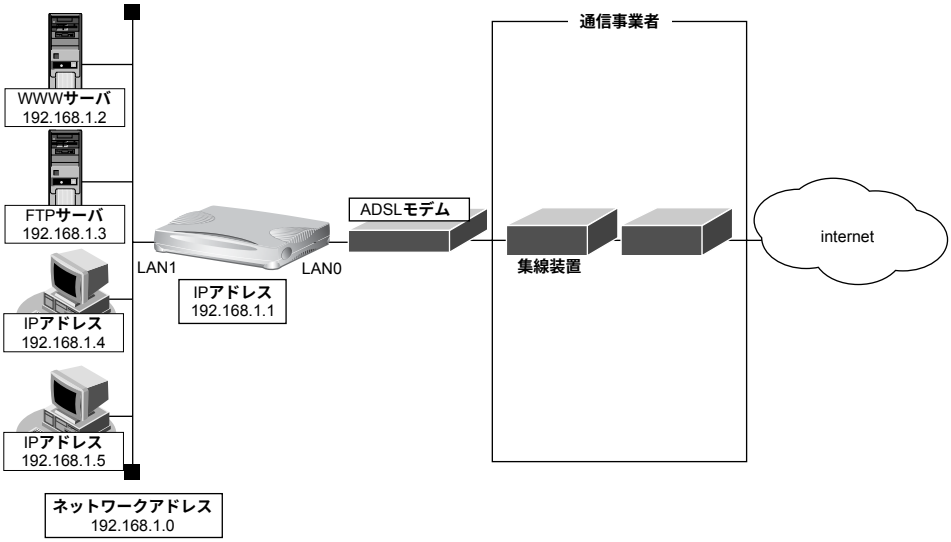
NAT セキュリティは、“高い”が初期値として選択されています。ftp や dns の要求した相手からの応答時には“高い”を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には“通常”を選択してください。
また、アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

2.16.2　PPPoE 接続でサーバを公開する

適用機種　*Si-R180,180B*

PPPoE を使ってインターネットへ接続している場合の例です。

ここでは、PPPoE 接続時に静的 NAT を使ってサーバを公開する場合の設定方法を説明します。



● 設定条件

- 既存の LAN を使用する
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

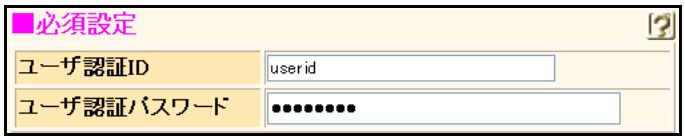
かんたん設定で PPPoE 接続の情報を設定する

1.　かんたん設定メニューで「PPPoE 接続」をクリックします。

「PPPoE かんたん設定」ページが表示されます。

2.　［必須設定］で以下の項目を指定します。

- ユーザ認証 ID　→userid（プロバイダから提示された内容）
- ユーザ認証パスワード　→userpass（プロバイダから提示された内容）



3.　［設定終了］ボタンをクリックします。

再起動後に、通信できる状態になります。

アドレス変換情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」で登録したネットワークの欄の［修正］ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

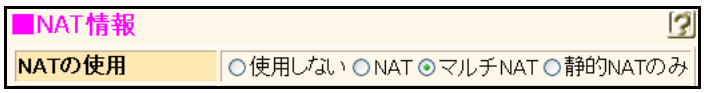
6.　以下の項目を指定します。

- NAT の使用　→マルチ NAT

補足 NAT セキュリティで“高い”を選択した場合、ftp や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT を使用している場合など、要求先とは別のアドレスから応答する場合は、“通常”を選択してください。

こんな事に気をつけて

ネットワーク型接続でマルチ NAT を使用する際、グローバルアドレスの設定が必須となります。なお、端末型接続では、接続時にグローバルアドレスが割り当てられるため、設定は不要です。



7.　［保存］ボタンをクリックします。

8.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

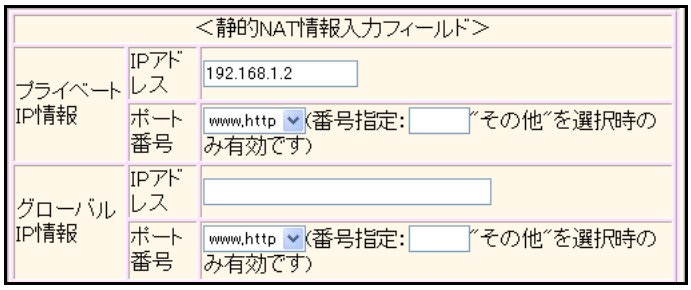
「静的 NAT 情報」が表示されます。

9.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.2
  ポート番号　→ www,http
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ www,http

こんな事に気をつけて

動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないようにしてください。
また、アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。



10.　［追加］ボタンをクリックします。

11.　手順 9. ～ 10. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.3
  ポート番号　→ ftp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ ftp

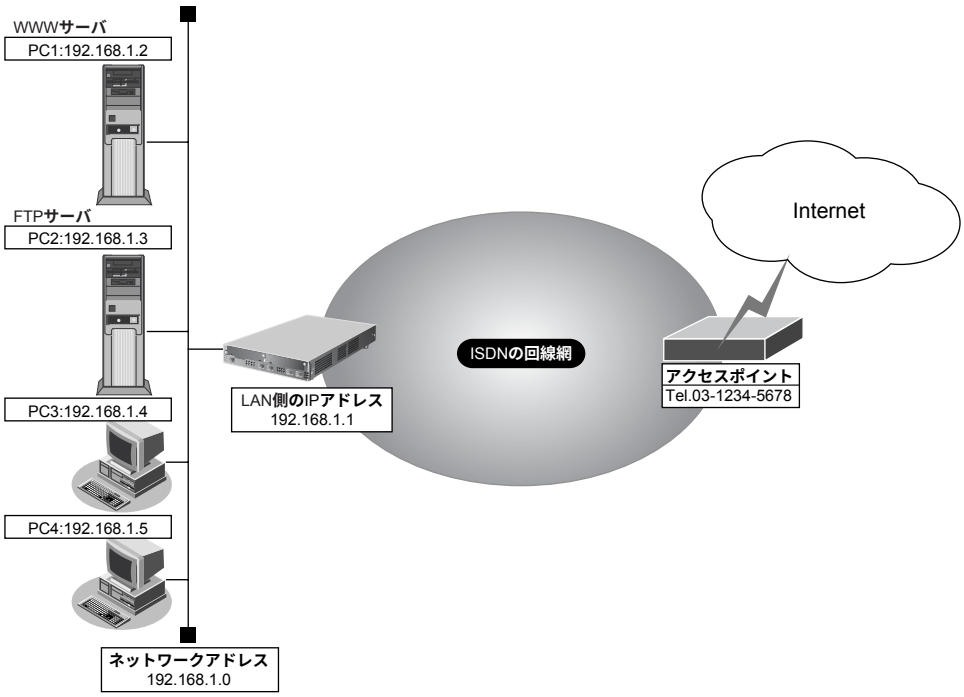
12.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.16.3　ネットワーク型接続でサーバを公開する

適用機種　***Si-R220B,220C,370,570***

ここでは、静的NATを使ってサーバを公開する場合の設定方法を説明します。



● 設定条件

- slot0に実装されたBRI拡張モジュールL2または基本ボード上のISDNポート（Si-R220B、220Cの場合）でISDNでインターネットに接続する
- ISDNに接続する
- ユーザ認証ID　：userid
- ユーザ認証パスワード　：userpass
- ネットワーク型接続を行う
- 既存のLANを使用する
- 割り当てネットワークアドレス　：10.10.10.96/29
- wwwに割り当てるIPアドレス　：10.10.10.98
- ftpに割り当てるIPアドレス　：10.10.10.99
- 動的NATで使用するIPアドレス　：10.10.10.100～102
- ネットワークアドレス/ネットマスク　：192.168.1.0/24
- ブロードキャストアドレス　：192.168.1.255

ここでは、設定条件に従って、ISDN接続する設定が行われていることを前提として、設定例を示します。

NAT 情報を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　NAT 情報を行うネットワーク情報の［修正］ボタンをクリックします。

「ネットワーク情報（internet)」ページが表示されます。

4.　「IP 関連」をクリックします。

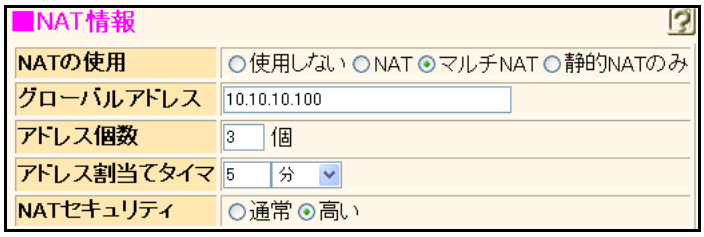
IP 関連の設定項目と「IP 基本情報」が表示されます。

5.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

6.　以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→ 10.10.10.100
- アドレス個数　→ 3
- アドレス割当てタイマ　→ 5 分
- NAT セキュリティ　→高い



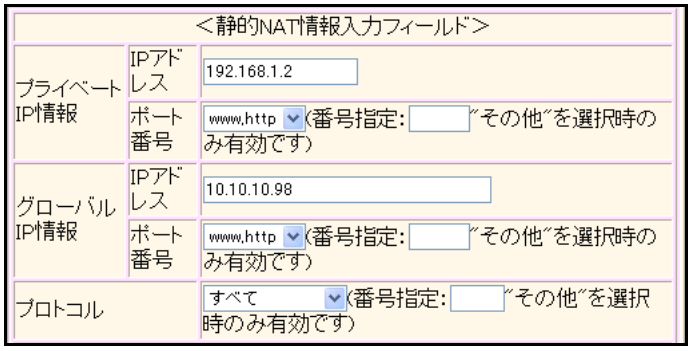
7.　［保存］ボタンをクリックします。

8.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

9.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.2
  ポート番号　→ www,http
- グローバル IP 情報
  IP アドレス　→ 10.10.10.98
  ポート番号　→ www,http
- プロトコル　→すべて



10.　［追加］ボタンをクリックします。

11.　手順 10. ～ 11. を参考に、以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.3
  ポート番号　→ ftp（21）
- グローバル IP 情報
  IP アドレス　→ 10.10.10.99
  ポート番号　→ ftp（21）
- プロトコル　→すべて

12.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

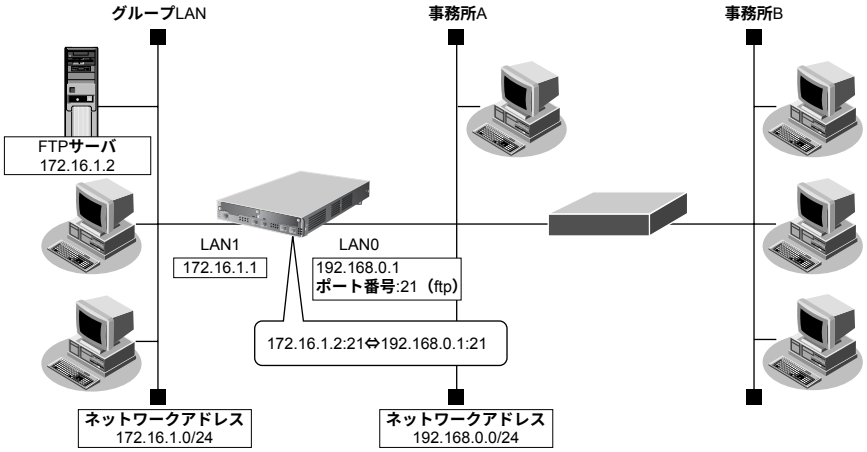
こんな事に気をつけて

NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答するときには、「相手情報」－「ネットワーク情報」－「IP 関連」－「NAT 情報」で、「NAT セキュリティ」を“通常”に設定してください。
また、アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

2.16.4 サーバ以外のアドレス変換をしないで、プライベートLAN接続でサーバを公開する

適用機種　全機種

ここでは、静的NATだけを使って、サーバ以外のアドレス変換をしないで、FTPサーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所A側]

- LAN0ポートを使用する
- 静的NATだけを使用する

[グループLAN側]

- IPアドレス　：172.16.1.1
- ネットワークアドレス/ネットマスク　：172.16.1.0/24
- FTPサーバのIPアドレス　：172.16.1.2

上記の設定条件に従って設定を行う場合の設定例を示します。

静的NAT情報を設定する

1.　設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報（物理LAN）」ページが表示されます。

3.　「IP関連」をクリックします。

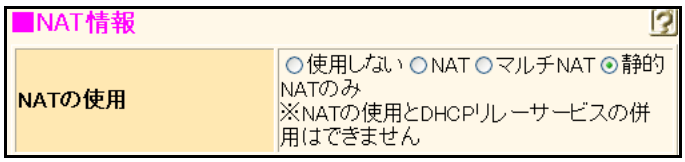
IP関連の設定項目と「IPアドレス情報」が表示されます。

4.　IP関連の設定項目の「NAT情報」をクリックします。

「NAT情報」が表示されます。

5.　以下の項目を指定します。

- NAT の使用　→静的 NAT のみ



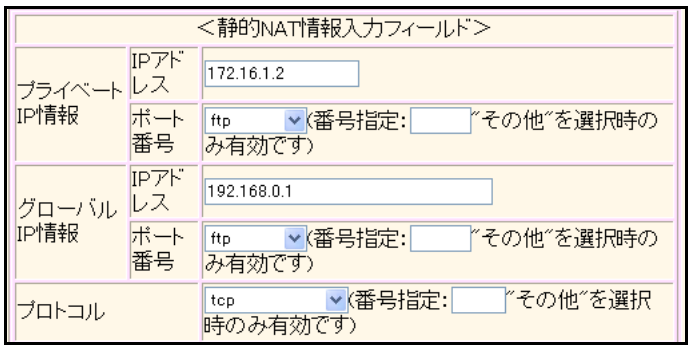
6.　［保存］ボタンをクリックします。

7.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

8.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 172.16.1.2
  ポート番号　→ ftp
- グローバル IP 情報
  IP アドレス　→ 192.168.0.1
  ポート番号　→ ftp
- プロトコル　→ tcp



9.　［追加］ボタンをクリックします。

10.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

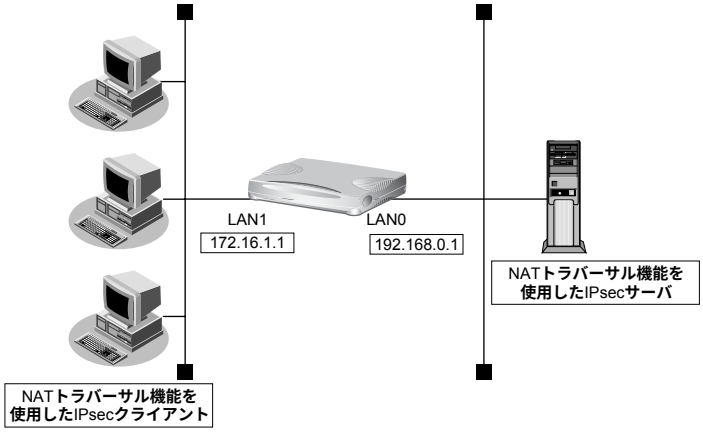
こんな事に気をつけて

NAT セキュリティは、“高い”が初期値として選択されています。ftp や dns の要求した相手からの応答時には“高い”を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には“通常”を選択してください。
また、アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

2.16.5 複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する

適用機種　全機種

ここでは、静的 NAT を使って、複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する場合の設定方法を説明します。



● 設定条件

[IPsec サーバ側]

- LAN0 ポートを使用する
- マルチ NAT を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

NAT 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

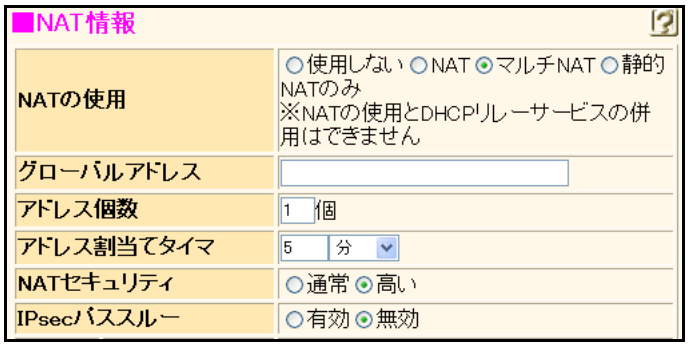
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

5.　以下の項目を指定します。

- NAT の使用　　→マルチ NAT
- IPsec パススルー　　→無効



こんな事に気をつけて

- NAT セキュリティは、“高い”が初期値として選択されています。ftp や dns の要求した相手からの応答時には“高い”を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には“通常”を選択してください。
  また、アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。
- IPsec クライアントが NAT トラバーサル機能を使用する場合は、IPsec パススルーを“無効”に設定します。IPsec パススルーを“有効”に設定すると、相手ごとに 1 つの IPsec パスしか接続することができません。

6.　［保存］ボタンをクリックします。

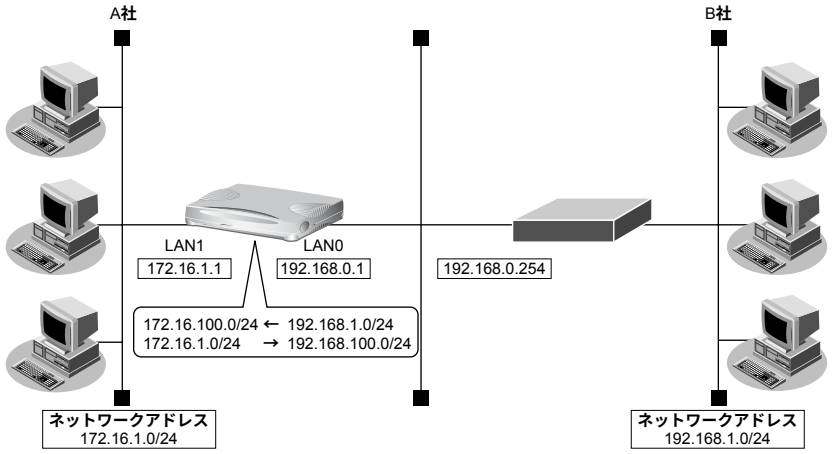
7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.16.6　NAT あて先変換で双方向のアドレスを変換する

適用機種　全機種

ここでは、NAT あて先変換を使って、双方向の IP アドレスを変換する場合の設定方法を説明します。
この機能を使用して異なるアドレス体系をもつ A 社と B 社を接続した場合、同じアドレス体系であるかのように見せることができます。



● 設定条件

【A 社】

- IP アドレス　：172.16.1.1
- ネットワークアドレス/ネットマスク　：172.16.1.0/24

【B 社】

- LAN0 ポートを使用する
- マルチ NAT を使用する
- NAT あて先変換を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

NAT あて先変換情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

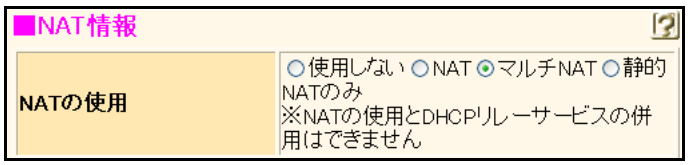
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

5.　以下の項目を指定します。

- NAT の使用　→マルチ NAT



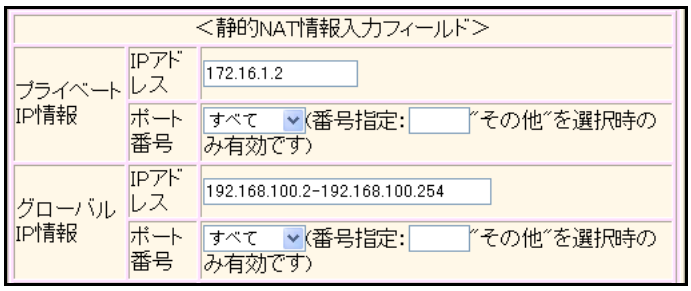
6.　［保存］ボタンをクリックします。

7.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

8.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 172.16.1.2
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→ 192.168.100.2-192.168.100.254
  ポート番号　→すべて



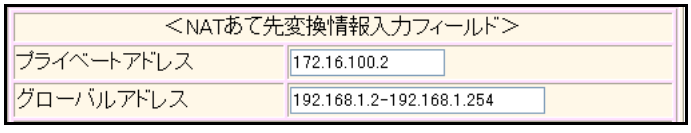
9.　［追加］ボタンをクリックします。

10.　IP 関連の設定項目の「NAT あて先変換情報」をクリックします。

「NAT あて先変換情報」が表示されます。

11.　以下の項目を指定します。

- プライベートアドレス　→ 172.16.100.2
- グローバルアドレス　→ 192.168.1.2-192.168.1.254



12.　［追加］ボタンをクリックします。

13.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

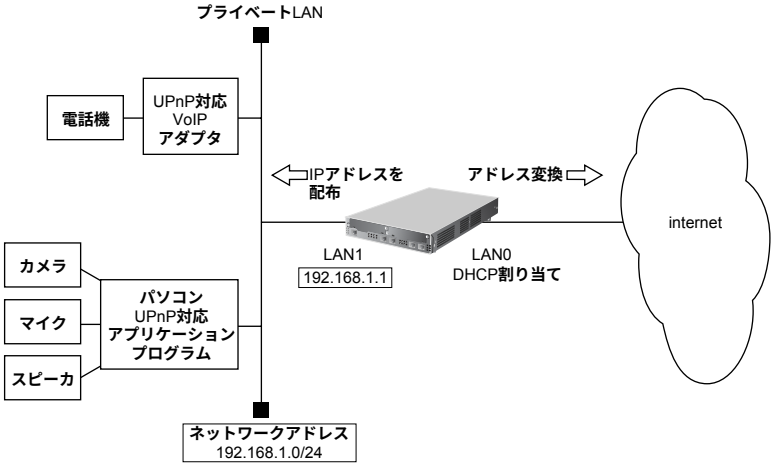
2.17 VoIP NAT トラバーサル機能を使う

適用機種　全機種

マルチ NAT 機能を使用すると動作しない VoIP アダプタが UPnP に対応している場合、本装置の VoIP NAT トラバーサル機能を使用することによって動作できるようになることがあります。同様に、UPnP に対応した装置やアプリケーションプログラムもマルチ NAT 機能を使用しても動作できるようになることがあります。

参照　Si-R シリーズ　機能説明書「2.16 VoIP NAT トラバーサル機能」（P.81）

ここでは、UPnP 対応 VoIP アダプタや UPnP 対応アプリケーションプログラムを使用する設定方法を説明します。



● 設定条件

[インターネット側 LAN]

- LAN0 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：DHCP サーバから自動的に取得
- マルチ NAT を使用する
  グローバルアドレス　：インターネットプロバイダから割り当てられた IP アドレスを使用する
  アドレス個数　：1
  アドレス割り当てタイマ　：5 分
- NAT での SIP アプリ対応を無効にする

[UPnP 対応装置（プライベート LAN）側]

- LAN1 ポートを使用する
- 転送レート　：自動認識
- IP アドレス　：192.168.1.1/24
- DHCP サーバ機能を使用する
  割り当て先頭アドレス　：192.168.1.2
  割り当てアドレス数　：253
  リース期間　：1 日
  デフォルトルータ広報　：192.168.1.1
  DNS サーバ広報　：192.168.1.1

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

ここでは、設定条件に従って、LAN の設定が行われていることを前提とします。

上記の設定条件に従って設定を行う場合の設定例を示します。

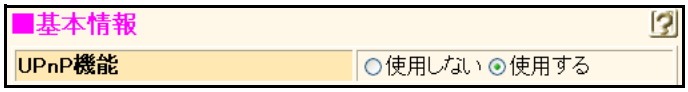
UPnP 情報を設定する

1.　設定メニューのルータ設定で「UPnP 情報」をクリックします。

「UPnP 情報」ページが表示されます。

2.　以下の項目を指定します。

- UPnP 機能　→使用する



3.　［保存］ボタンをクリックします。

4.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.18 TOS/Traffic Class 値書き換え機能を使う

適用機種　全機種

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットを IP アドレスとポート番号の組み合わせで TOS/Traffic Class 値を変更することにより、ポリシーベースネットワークのポリシーに合わせることができます。

参照　Si-R シリーズ　機能説明書「2.17 TOS/Traffic Class 値書き換え機能」（P.84）

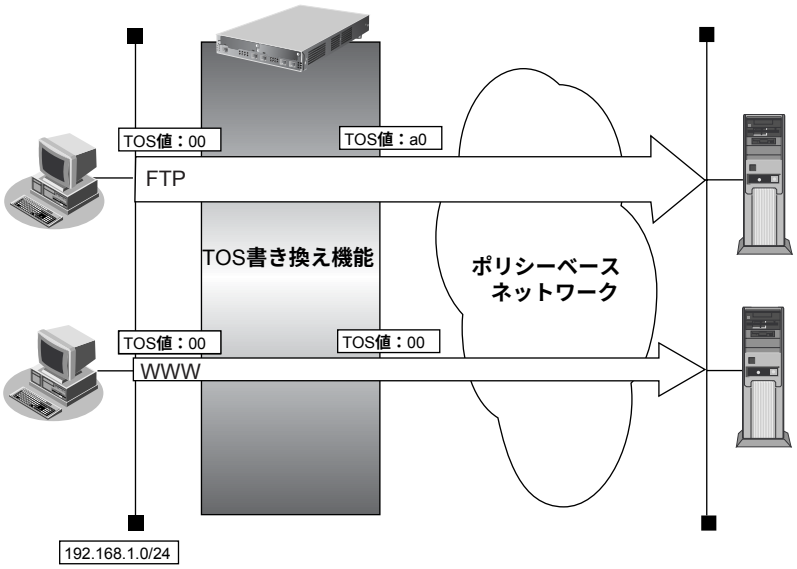
TOS/Traffic Class 値書き換え機能の条件

本装置では、以下の条件を指定することによって、ポリシーベースネットワークのポリシーに合った TOS/Traffic Class 値に書き換えることができます。

- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- あて先情報（IP アドレス／アドレスマスク／ポート番号）
- IP パケットの TOS 値または IPv6 パケットの Traffic Class 値
- 新 TOS または Traffic Class

ここではネットワークが以下のポリシーをもつ場合の設定方法を説明します。

- FTP（TOS 値 a0）を最優先とする
- その他はなし



● 設定条件

- 送信元 IP アドレス/アドレスマスク　：192.168.1.0/24
- 送信元ポート番号　：指定しない
- あて先 IP アドレス/アドレスマスク　：指定しない
- あて先ポート番号　：20（ftp-data のポート番号）、21（ftp のポート番号）
- プロトコル　：TCP

- TOS 値　：00
- 新 TOS 値　：a0

上記の設定条件に従って設定を行う場合の設定例を示します。

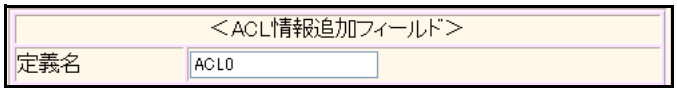
FTP サーバのアクセスで TOS 値を 00 から a0 に変更する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

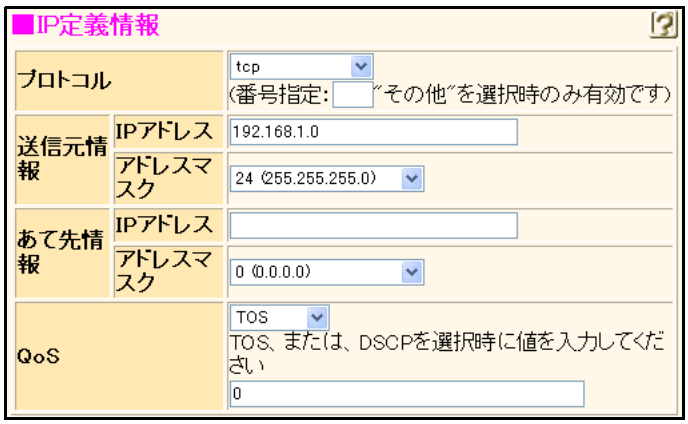
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→TOS
  →0



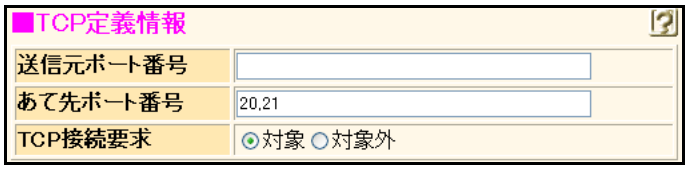
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→20（ftp-data のポート番号）、21（ftp のポート番号）
- TCP 接続要求　→対象



9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

11.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

12.　「ネットワーク情報」で TOS 値書き換えの設定を行うネットワーク名の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

13.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

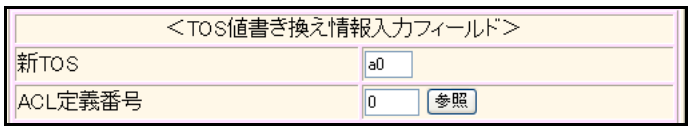
14.　「TOS 値書き換え情報」をクリックします。

「TOS 値書き換え情報」が表示されます。

15.　以下の項目を指定します。

- 新 TOS　→a0
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



16.　［追加］ボタンをクリックします。

17.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.19 VLANプライオリティマッピング機能を使う

適用機種　全機種

VLAN プライオリティマッピング機能を使用して、レイヤ 2 スイッチなどで QoS 制御を行うことができます。

本装置から送信される VLAN パケットの VLAN のプライオリティ値を、IP パケットの TOS フィールドおよび IPv6 パケットのトラフィッククラスフィールドの値から設定します。

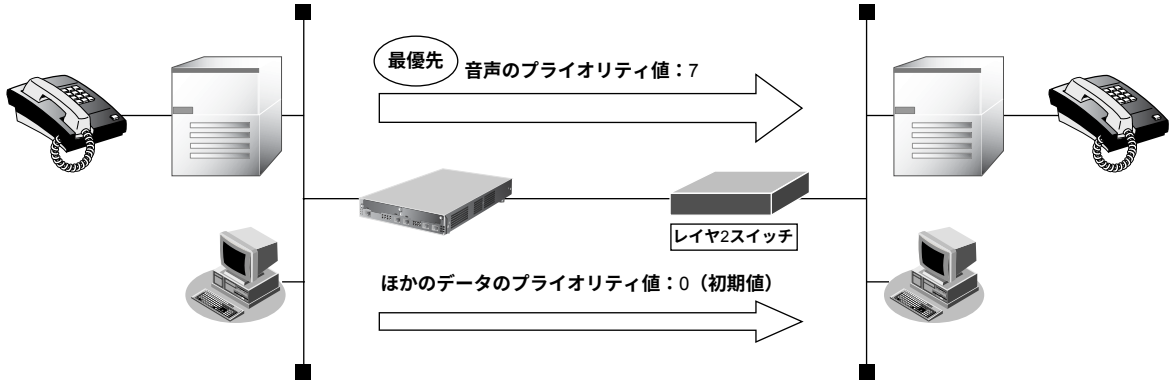
参照　Si-R シリーズ　機能説明書「2.18 VLAN プライオリティマッピング機能」（P.86）

本装置では、以下の条件を指定することによって、VLAN のプライオリティフィールドを設定することができます。

- プロトコル
- TOS/Traffic Class
- プライオリティ

ここでは、本装置が以下の音声データを転送する場合の設定方法を説明します。

- 音声（IP で TOS 値が a0）を最優先とする（プライオリティ値が 7）
- その他は初期値（プライオリティ値が 0）



● 設定条件

- プロトコル　：IPv4
- TOS 値　：a0
- プライオリティ値　：7

上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」で VLAN プライオリティマッピングの設定を行う LAN の［修正］ボタンをクリックします。

「LAN 情報（VLAN）」ページが表示されます。

3.　「共通情報」をクリックします。

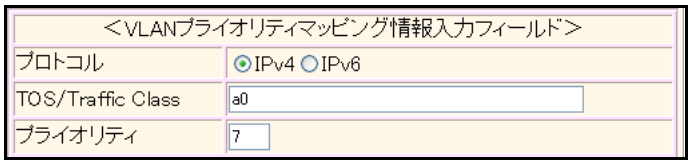
共通情報の設定項目と「基本情報」が表示されます。

4.　共通情報の設定項目の「VLAN プライオリティマッピング情報」をクリックします。

「VLAN プライオリティマッピング情報」が表示されます。

5.　以下の項目を指定します。

- プロトコル　→IPv4
- TOS/Traffic Class　→a0
- プライオリティ　→7



6.　［追加］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.20 シェーピング機能を使う

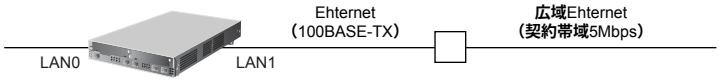
適用機種　全機種

シェーピング機能を使用すると、LAN および WAN 回線に送出するデータ量を制限することができます。

2.20.1 特定のインタフェースでシェーピング機能を使う

適用機種　全機種

ここでは、Ethernet 回線の送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約帯域は 5Mbps

上記の設定条件に設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

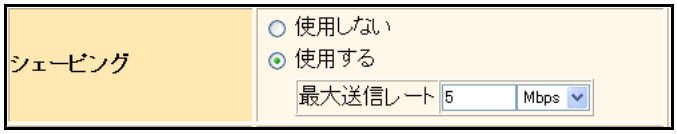
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- シェーピング　→使用する
  最大送信レート　→ 5Mbps



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

5.　［保存］ボタンをクリックします。

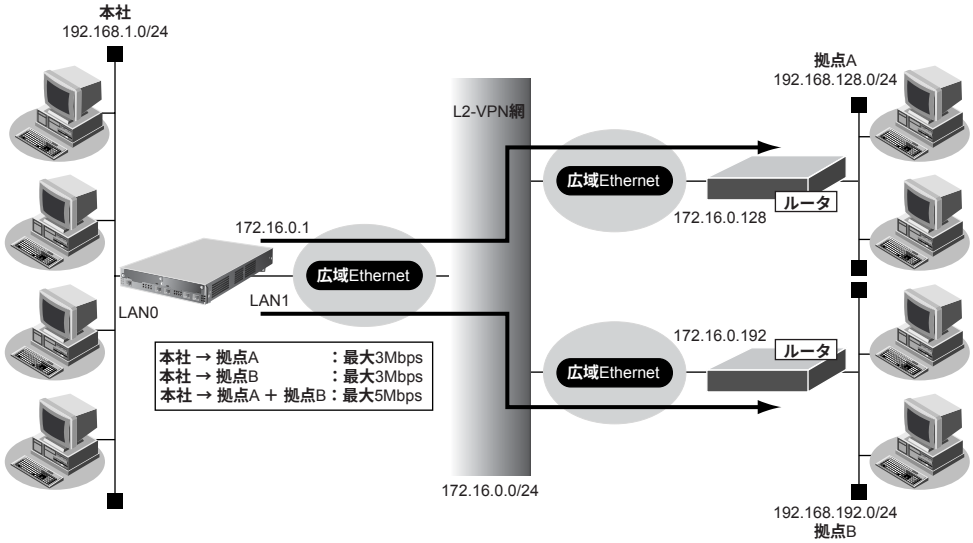
6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.20.2　送信先ごとにシェーピング機能を使う

適用機種　全機種

ここでは、各拠点に送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet をアクセスラインとする。L2-VPN 網を利用して本社と各拠点を接続する
- 本社から拠点 A への送信データは、最大 3Mbps に制限する
- 本社から拠点 B への送信データは、最大 3Mbps に制限する
- 本社から拠点 A と拠点 B への送信データの合計は、最大 5Mbps に制限する
- 本社の本装置は LAN ポートのアドレス設定ができた状態から設定を始める

上記の設定条件に設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

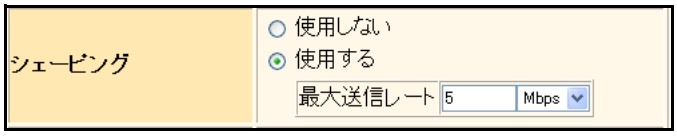
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- シェーピング　→使用する
  最大送信レート　→ 5Mbps



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

5.　［保存］ボタンをクリックします。

6.　設定メニューのルータ設定で「相手情報」をクリックします。

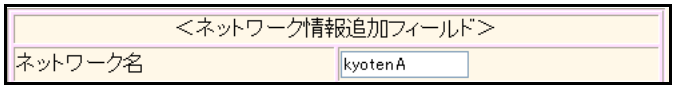
「相手情報」ページが表示されます。

7.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

8.　以下の項目を指定します。

- ネットワーク名　→kyotenA



9.　［追加］ボタンをクリックします。

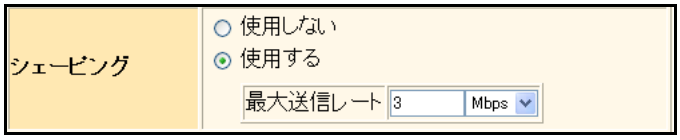
「ネットワーク情報（kyotenA)」が表示されます。

10.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

11.　以下の項目を指定します。

- シェーピング　→使用する
  最大送信レート　→3Mbps



12.　［保存］ボタンをクリックします。

13.　「IP 関連」をクリックします。

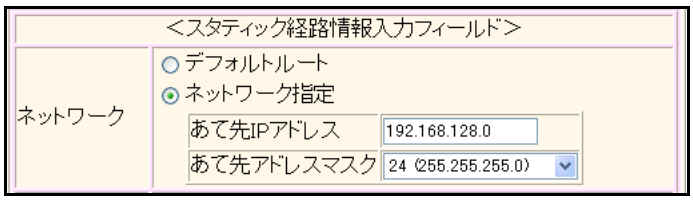
IP 関連の設定項目と「IP 基本情報」が表示されます。

14.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.128.0
  あて先アドレスマスク　→24（255.255.255.0）



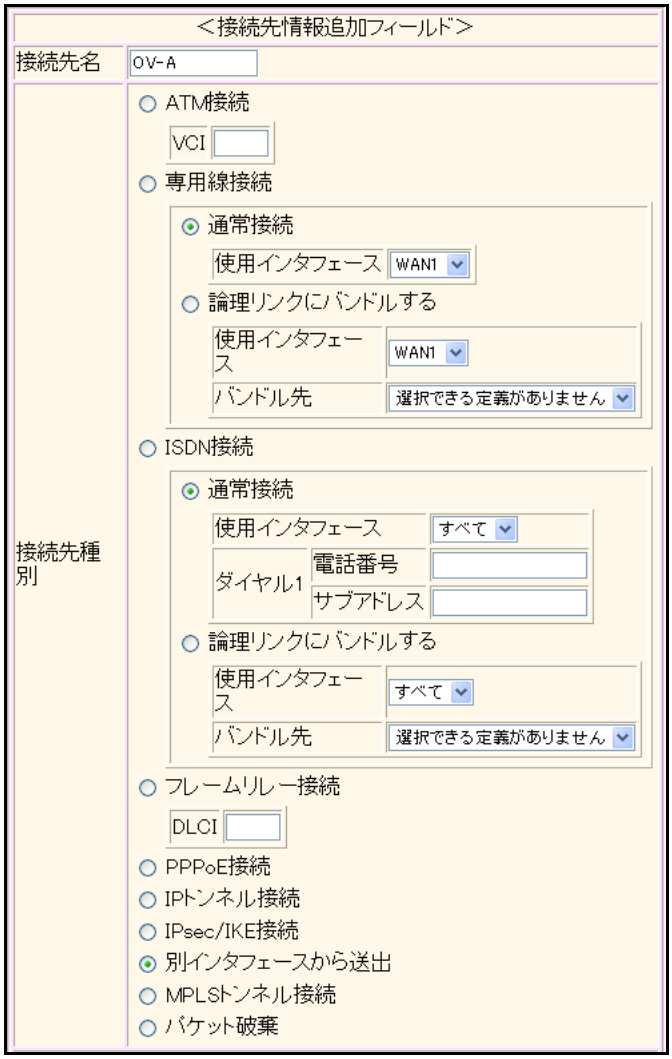
16.　［追加］ボタンをクリックします。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→OV-A
- 接続先種別　→別インタフェースから送出



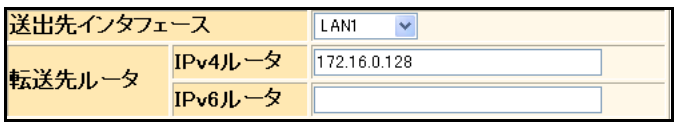
機種により、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

別インタフェースから送出の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 送出先インタフェース　→LAN1
- 転送先ルータ
  IPv4 ルータ　→172.16.0.128



21.　［保存］ボタンをクリックします。

22.　手順6.～21.を参考にして、拠点Bを設定します。

「ネットワーク情報」

- ネットワーク名　→kyotenB

「共通情報」

- シェーピング　→使用する
  最大送信レート　→3Mbps

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先IPアドレス　→192.168.192.0
  あて先アドレスマスク　→24（255.255.255.0）

「接続先情報」

- 接続先名　→OV-B
- 接続先種別　→別インタフェースから送出

「基本情報」

- 送出先インタフェース　→LAN1
- 転送先ルータ
  IPv4ルータ　→172.16.0.192

23.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.21 データ圧縮／ヘッダ圧縮機能を使う

適用機種　全機種

PPP を使った相手装置との接続時に、データ圧縮およびヘッダ圧縮機能によって回線の利用効率を高めることができます。

データ圧縮は、ISDN 接続、専用線接続、およびモデム接続をサポートしています。

データ圧縮およびヘッダ圧縮機能を利用する場合、接続する相手装置側でも同じ圧縮機能をサポートしている必要があります。以下に、サポートしている圧縮機能を示します。

- データ圧縮（Si-R220B、220C、370、570）
  - LZS
- ヘッダ圧縮
  - VJ　：VJ ヘッダ圧縮（RFC1144 に準拠）の利用
  - IPHC　：IP ヘッダ圧縮（圧縮方法：RFC2507/RFC2508、ネゴシエーション方法：RFC2509 に準拠）の利用

ヘッダ圧縮の場合

ここでは、PPPoE 接続をネットワーク 0（rmt0）で定義している環境に対して、ヘッダ圧縮を行う場合の設定方法を説明します。

● 設定条件

- ネットーク情報（rmt0）で PPPoE による通信環境が設定済み
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってヘッダ圧縮を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

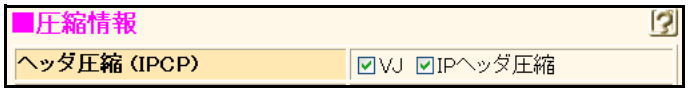
「ネットワーク情報」が表示されます。

3.　「PPP 関連」をクリックします。

PPP 関連に関する項目と「圧縮情報」が表示されます。

4.　以下の項目を指定します。

- ヘッダ圧縮（IPCP）　→VJ、IP ヘッダ圧縮



5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

ヘッダ圧縮機能は、シェーピングによって通信速度が低速の場合に効果があります。高速回線で使用した場合は、処理のオーバーヘッドによって回線の利用効率が低くなることがあります。

ISDN、専用線、モデム接続の場合

ここでは、ISDN 接続、専用線接続、およびモデム接続をネットワーク 0（remote0）で定義している環境に対してデータ圧縮およびヘッダ圧縮を併用する場合の設定方法を説明します。

● 設定条件

- ネットワーク情報（rmt0）で ISDN による通信環境が設定済み
- データ圧縮機能を使用する
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってデータ圧縮およびヘッダ圧縮を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　ネットワーク名が rmt0 の［修正］ボタンをクリックします。

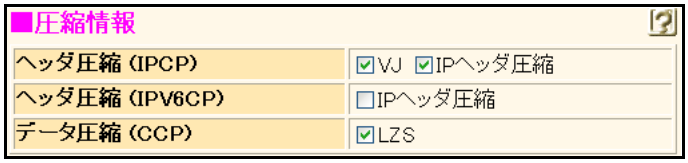
「ネットワーク情報（rmt0）」ページが表示されます。

4.　「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

5.　以下の項目を指定します。

- ヘッダ圧縮（IPCP）　→VJ、IP ヘッダ圧縮
- データ圧縮（CCP）　→LZS



6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

MP と併用する場合は、「相手情報」－「ネットワーク情報」－「PPP 関連」－「MP 情報」－「受信パケット順序制御」を“する”に設定してください。

2.22 帯域制御（WFQ）機能を使う

適用機種　全機種

本装置の帯域制御（WFQ）機能では、IP アドレスやポート番号の組み合わせで帯域を割り当てることによって、特定のデータを優先的に通すことができます。

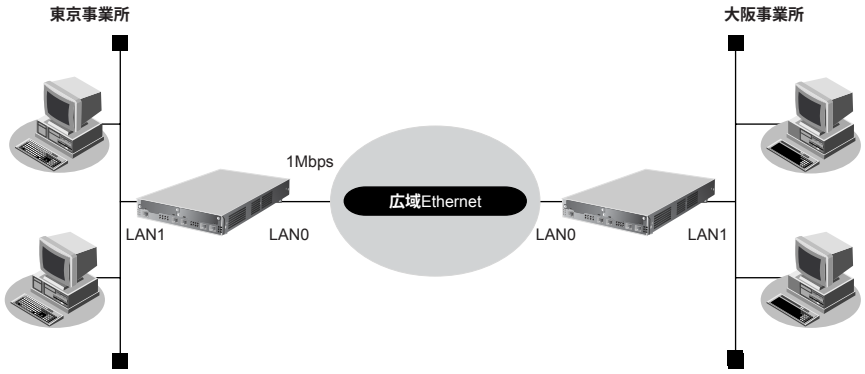
参照　Si-R シリーズ　機能説明書「2.20 帯域制御（WFQ）機能」（P.88）

帯域制御（WFQ）機能の条件

本装置では、以下の条件を指定することによって、優先的にデータを通すように帯域を割り当てることができます。

- プロトコル
- IP アドレス
- ポート番号
- IP パケットの TOS 値または IPv6 パケットの Traffic Class 値

ここでは、広域 Ethernet による拠点間の接続がすでに設定されている場合を例に帯域制御を利用する設定方法を説明します。



● 設定条件

- LAN0 インタフェースで広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約速度は 1Mbps
- 音声データ（TOS 値：a0）を最優先で透過させる

上記の設定条件に従って帯域制御する場合の設定例を示します。

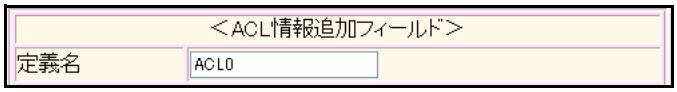
東京事業所を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

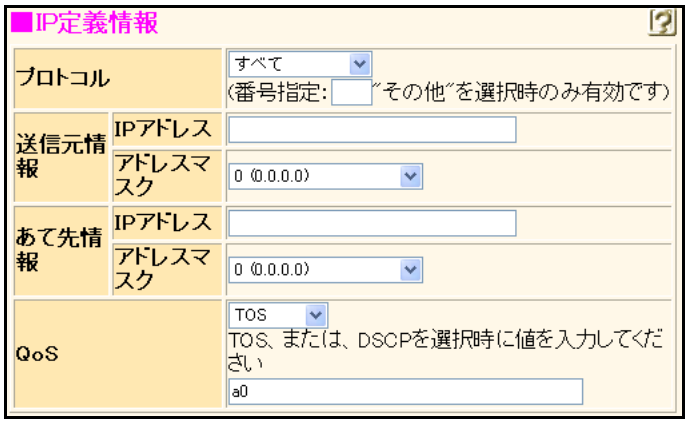
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→TOS
  →a0



6.　［保存］ボタンをクリックします。

7.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

8.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

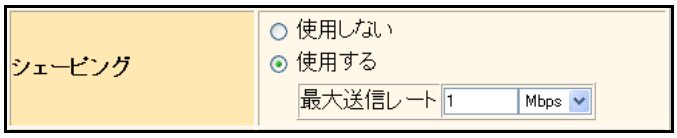
「LAN0 情報（物理 LAN）」ページが表示されます。

9.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

10.　以下の項目を指定します。

- シェーピング　→使用する
  最大送信レート　→1Mbps



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

11.　［保存］ボタンをクリックします。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

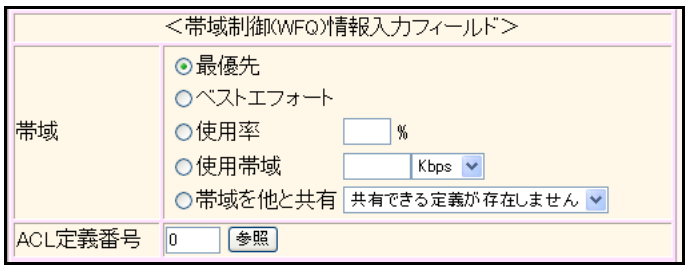
13.　IP 関連の設定項目の「帯域制御（WFQ）情報」をクリックします。

「帯域制御（WFQ）情報」が表示されます。

14.　以下の項目を指定します。

- 帯域　→最優先
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

大阪事業所を設定する

「東京事業所を設定する」を参考に、大阪事業所を設定します。

「ACL 情報」

- 定義名　→ACL0

「ACL 定義情報（ACL0）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→TOS
  →a0

「LAN0 情報」-「共通情報」

「基本情報」

- インタフェース情報　→物理インタフェース
  シェーピング　→使用する
  最大送信レート　→1Mbps

「LAN0 情報」-「IP 関連」

「帯域制御（WFQ）情報」

- 帯域　→最優先
- ACL 定義番号　→0

2.23 DHCP 機能を使う

適用機種　全機種

本装置の IPv4 DHCP には、以下の機能があります。

- DHCP サーバ機能
- DHCP スタティック機能
- DHCP クライアント機能
- DHCP リレーエージェント機能

☛ 参照　Si-R シリーズ　機能説明書「2.21.1 IPv4 DHCP 機能」（P.91）

本装置では、それぞれのインタフェースで DHCP 機能が使用できます。

こんな事に気をつけて

- **1 つのインタフェースでは、1 つの機能だけ動作します。同時に複数の機能を動作することはできません。**
- **本装置の DHCP サーバは、リレーエージェントを経由して運用することはできません。**

本装置の IPv6 DHCP には、以下の機能があります。ここでは、IPv6 DHCP クライアント機能を使用する場合について説明しています。

- IPv6 DHCP サーバ機能
- IPv6 DHCP クライアント機能

☛ 参照　Si-R シリーズ　機能説明書「2.21.2 IPv6 DHCP 機能」（P.94）

2.23.1　DHCP サーバ機能を使う

適用機種　全機種

DHCP サーバ機能は、ネットワークに接続されているパソコンに対して、IP アドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびに IP アドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCP クライアント機能を持つパソコンは IP アドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置の DHCP サーバ機能は、以下の情報を広報することができます。

- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- ドメイン名
- NTP サーバの IP アドレス
- TIME サーバの IP アドレス
- WINS サーバの IP アドレス
- SIP サーバのドメイン名または IP アドレス

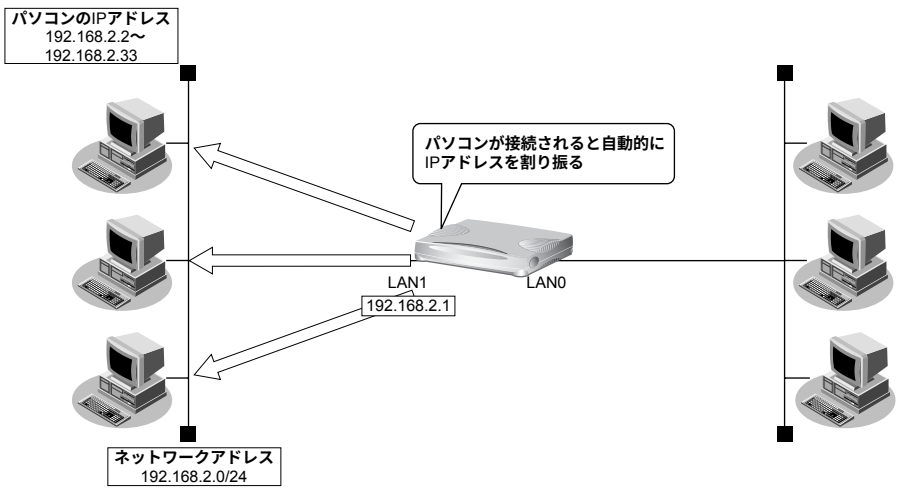
こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **本装置の DHCP サーバ機能は、DHCP リレーエージェントのサーバにはなれません。**

ここでは、DHCP サーバ機能を使用する場合の設定方法説明します。



● 設定条件

- 本装置の IP アドレス　：192.168.2.1
- ブロードキャストアドレス　：3（ネットワークアドレス＋オール 1）
- パソコンに割り当てる IP アドレス　：192.168.2.2 ～ 192.168.2.33
- パソコンに割り当て可能 IP アドレス数　：32
- ネットワークアドレス/ネットマスク　：192.168.2.0/24
- DHCP サーバ機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP サーバ機能を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

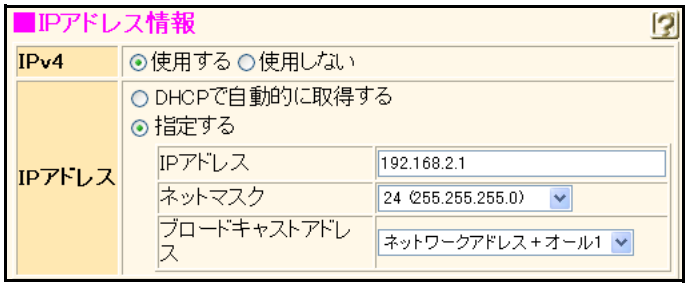
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

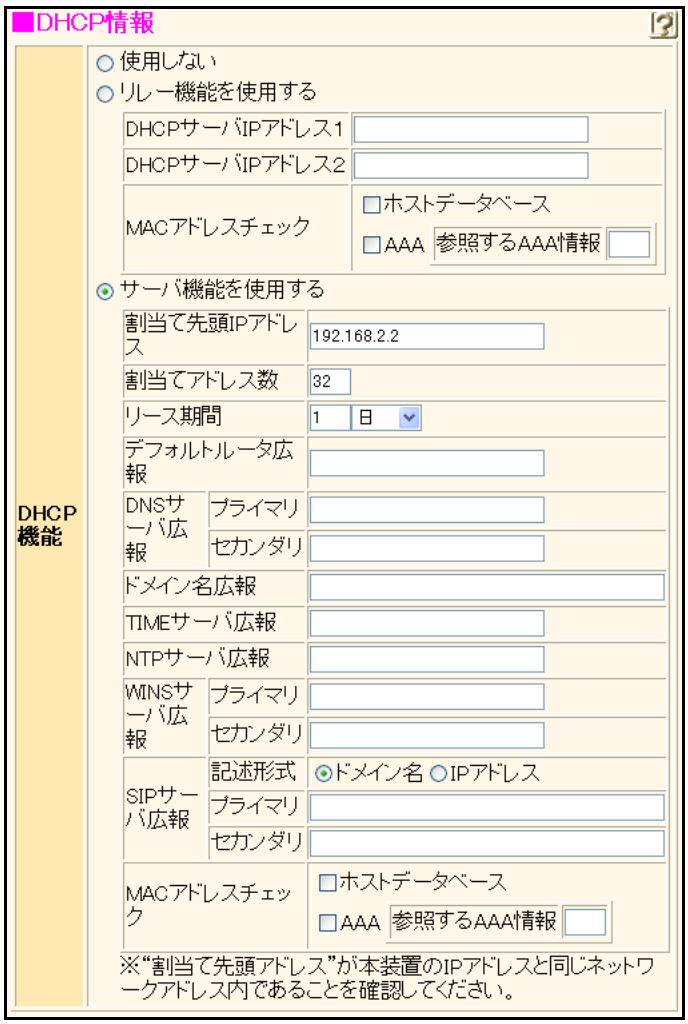
6.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

7.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.2.2
  割当てアドレス数　→ 32

補足 DHCP サーバ機能で割り当てることのできる最大数は 253 です。



必要に応じて上記以外の項目を指定します。

8.　［保存］ボタンをクリックします。

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.23.2　DHCP スタティック機能を使う

適用機種　全機種

DHCP サーバは、使用していない IP アドレスを一定期間（またはパソコンが IP アドレスを返却するまで）割り当てます。不要になった IP アドレスは自動的に再利用されるため、パソコンの IP アドレスが変わることがあります。本装置では、IP アドレスと MAC アドレスを対応付けることによって、登録されたパソコンから DHCP 要求が発行されると、常に同じ IP アドレスを割り当てることができます。これを DHCP スタティック機能と言います。

DHCP スタティック機能を利用する場合は、ホストデータベース情報に IP アドレスと MAC アドレスを設定してください。

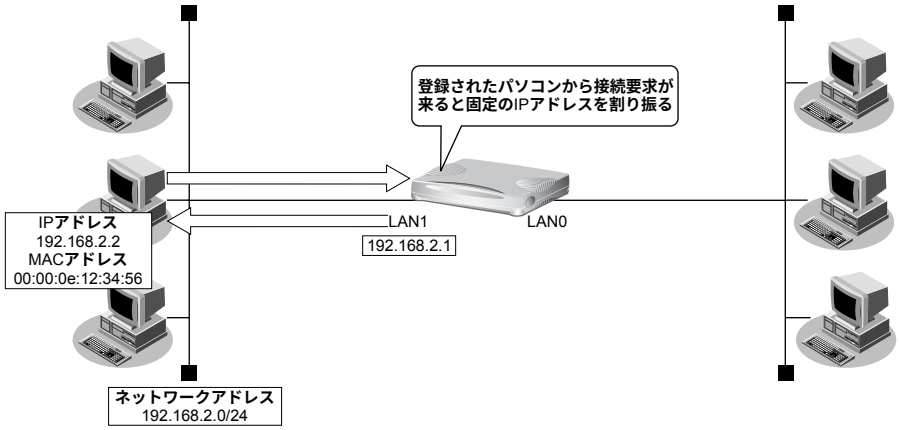
補足　MAC アドレスとは、LAN 機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
本装置がサポートしている「IP フィルタリング機能」、「マルチルーティング機能」などはパソコンの IP アドレスが固定されていないと使いにくい場合があります。これらの機能と DHCP サーバ機能の併用を実現するために、本装置では「DHCP スタティック機能」をサポートしています。

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

ここでは、DHCP スタティック機能を使用する場合の設定方法を説明します。



● 設定条件

- ネットワークアドレス/ネットマスク　：192.168.2.0/24
- IP アドレスを固定するパソコンの MAC アドレス：00:00:0e:12:34:56
- 割り当て IP アドレス　：192.168.2.2
- DHCP サーバ機能を使用する

こんな事に気をつけて

設定の「LAN0 情報」、「LAN1 情報」で DHCP サーバ機能を使用する設定をしていない場合は、DHCP スタティック機能の設定は有効になりません。

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP スタティック機能を設定する

1.　設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

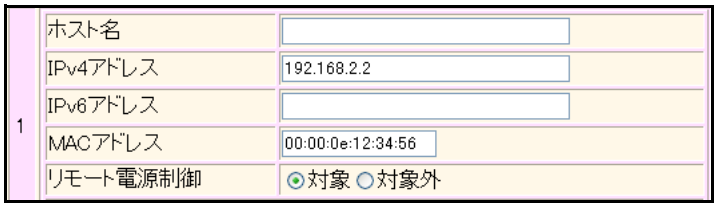
「ホストデータベース情報」ページが表示されます。

2.　未設定の欄の［修正］ボタンをクリックします。

3.　以下の項目を指定します。

- IPv4 アドレス　→ 192.168.2.2
- MAC アドレス　→ 00:00:0e:12:34:56

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。



必要に応じて上記以外の項目を指定します。

4.　［保存］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足 DHCP スタティック機能で設定できるホストの最大数は 64 です。

2.23.3　DHCP クライアント機能を使う

適用機種　全機種

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は、DHCP サーバが動作している LAN に接続する必要があります。利用者は、IP アドレスを意識することなくネットワークを利用できます。

本装置の DHCP クライアント機能は、以下の情報を受け取って動作します。

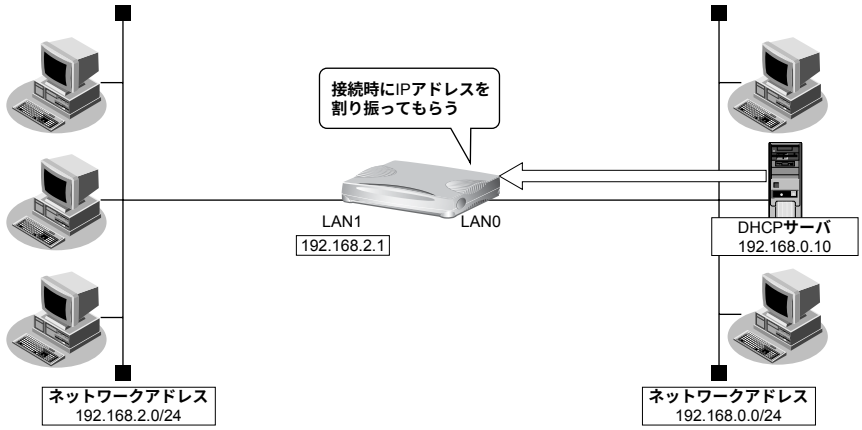
- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- TIME サーバの IP アドレス
- NTP サーバの IP アドレス
- ドメイン名
- リース更新時間

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

ここでは、DHCP クライアント機能を使用する場合の設定方法を説明します。



● 設定条件

- 本装置の IP アドレス　　：DHCP サーバから取得する

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP クライアント機能を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

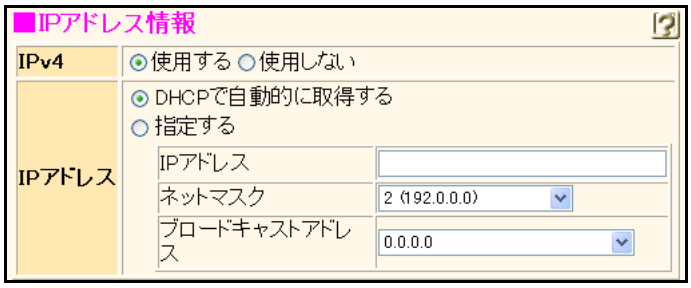
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→DHCP で自動的に取得する



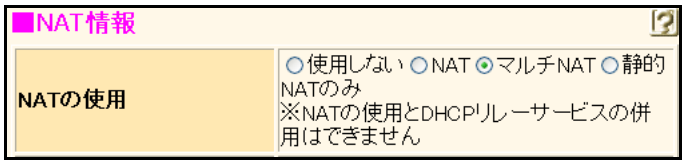
5.　［保存］ボタンをクリックします。

6.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

7.　以下の項目を指定します。

- NAT の使用　→マルチ NAT



8.　［保存］ボタンをクリックします。

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.23.4　DHCP リレーエージェント機能を使う

適用機種　全機種

DHCPクライアントは、同じネットワーク上にあるサーバから、IPアドレスなどの情報を獲得することができます。

DHCP リレーエージェントは、遠隔地にある DHCP クライアントの要求を DHCP サーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークに DHCP サーバが存在する場合も同様に情報を獲得することができます。

こんな事に気をつけて

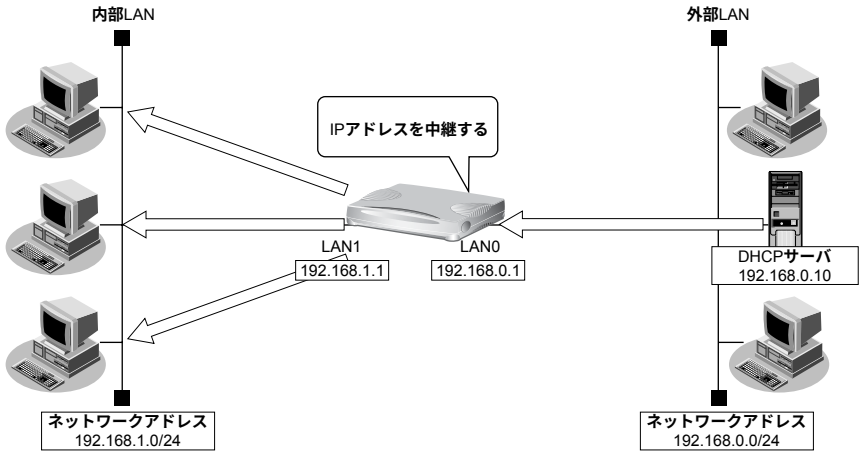
文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

ここでは、DHCP リレーエージェント機能を使用する場合の設定方法を説明します。

LAN 接続の場合

適用機種　全機種



● 設定条件

[内部 LAN 側]

- 本装置の IP アドレス　：192.168.1.1
- DHCP リレーエージェント機能を使用する

[外部 LAN 側]

- 本装置の IP アドレス　：192.168.0.1
- DHCP サーバ　：192.168.0.10

補足　DHCP リレーエージェント機能を使用するときは、NAT 機能を使用できません。

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP リレーエージェント機能を設定する

ここでは、LAN1 を使用した場合を例に説明します。LAN0 の場合も同様の手順で設定できます。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

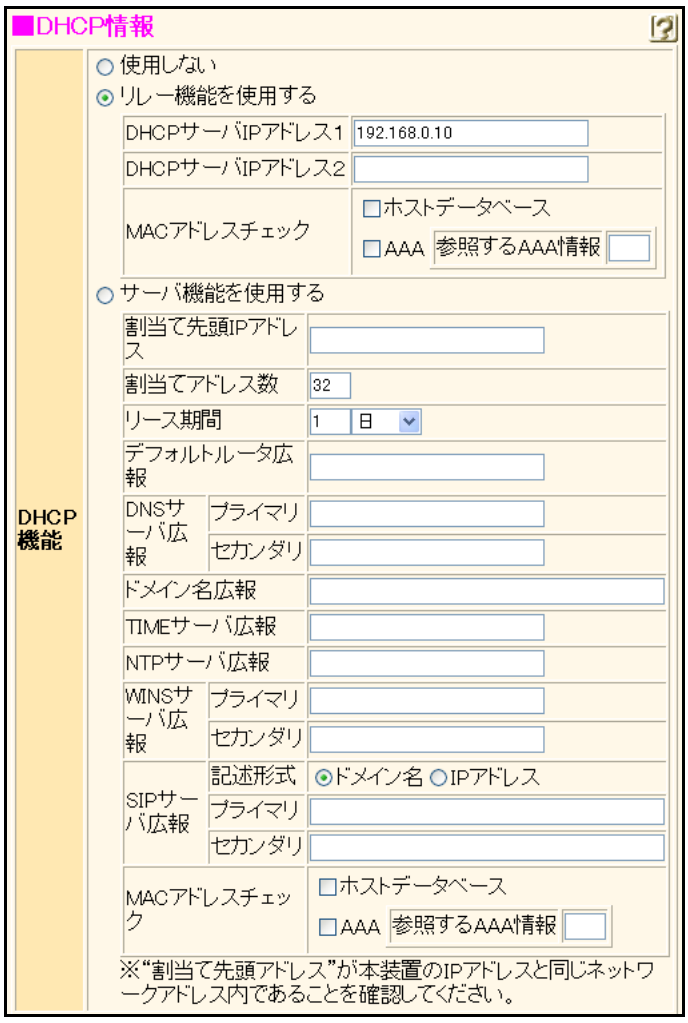
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

5.　以下の項目を指定します。

- DHCP 機能　→リレー機能を使用する
  DHCP サーバ IP アドレス 1　→ 192.168.0.10



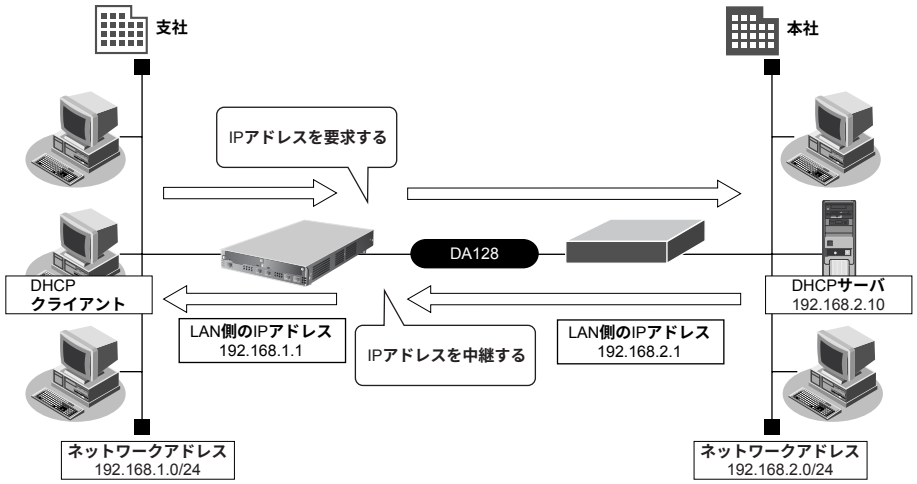
6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート接続の場合

適用機種　***Si-R220B,220C,260B,370,570***



● 設定条件

- DHCP リレーエージェント機能を使用する
- 支社に DHCP クライアントが存在する
- 本社に DHCP サーバが存在する

[本社]

- ルータの IP アドレス　：192.168.2.1
- ネットワークアドレス/ネットマスク　：192.168.2.0/24
- DHCP サーバの IP アドレス　：192.168.2.10

[支社]

- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

ここでは、本社、支社のネットワークがすでに専用線接続されていることを前提としています。

参照 「1.10 事業所 LAN を専用線で接続する」（P.103）

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する（DHCP リレーエージェント機能を設定する）

ここでは、LAN0 を使用した場合を例に説明します。LAN1 の場合も同様の手順で設定できます。

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

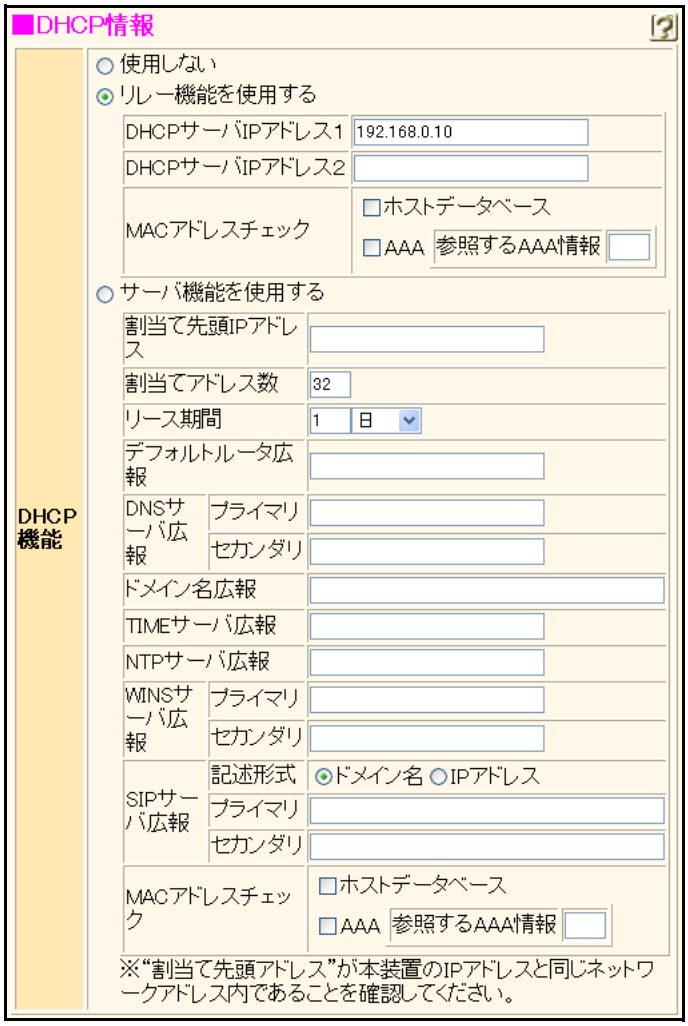
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

5.　以下の項目を指定します。

- DHCP 機能　→リレー機能を使用する
  DHCP サーバ IP アドレス 1　→ 192.168.0.10



6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

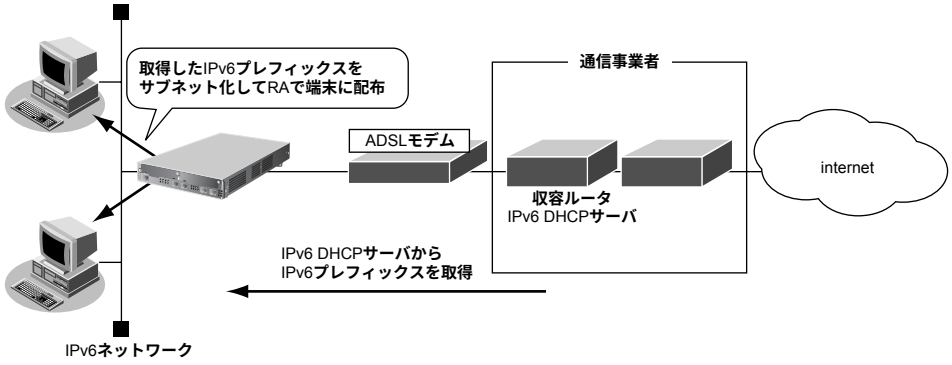
設定した内容が有効になります。

2.23.5　IPv6 DHCP クライアント機能を使う

適用機種　全機種

IPv6 DHCP クライアント機能は、プロバイダの IPv6 DHCP サーバから IPv6 プレフィックスなどの情報を取得する機能です。この機能を利用すると、プロバイダから取得した IPv6 プレフィックスをサブネット化して、Router Advertisement Message（RA）で下流ネットワークに 64 ビットの IPv6 プレフィックスを配布することができます。

ここでは、PPPoE でインターネットに接続して、IPv6 DHCP クライアント機能を使用する場合の設定方法を説明します。



● 設定条件

- PPPoE で使用する LAN ポート　：LAN0 ポート
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長　：48 ビット
- IPv6 プレフィックスを配布する LAN ポート　：LAN1 ポート
- RA で配布する IPv6 プレフィックスのサブネット ID　：0001

上記の設定条件に従って設定を行う場合の設定例を示します。

IPv6 DHCP クライアントを設定する

1.　「1.6 インターネットへ PPPoE で接続する」（P.67）を参考に、PPPoE での接続を設定します。

2.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

3.　クライアントの設定を行うネットワーク情報の［修正］ボタンをクリックします。

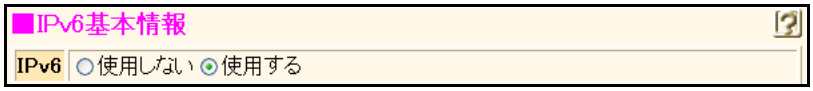
「ネットワーク情報」が表示されます。

4.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

5.　以下の項目を指定します。

- IPv6　→使用する



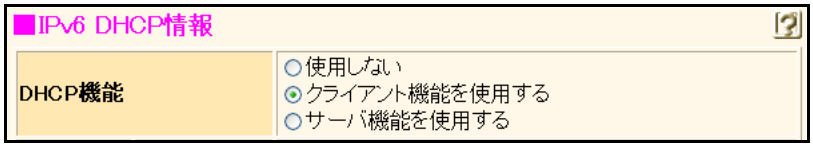
6.　［保存］ボタンをクリックします。

7.　IPv6 関連の設定項目の「IPv6 DHCP 情報」をクリックします。

「IPv6 DHCP 情報」が表示されます。

8.　以下の項目を指定します。

- DHCP 機能　→クライアント機能を使用する



9.　［保存］ボタンをクリックします。

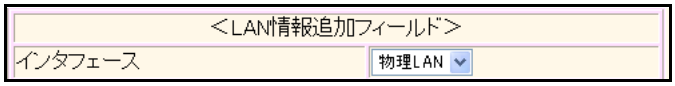
LAN 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→物理 LAN



3.　［追加］ボタンをクリックします。

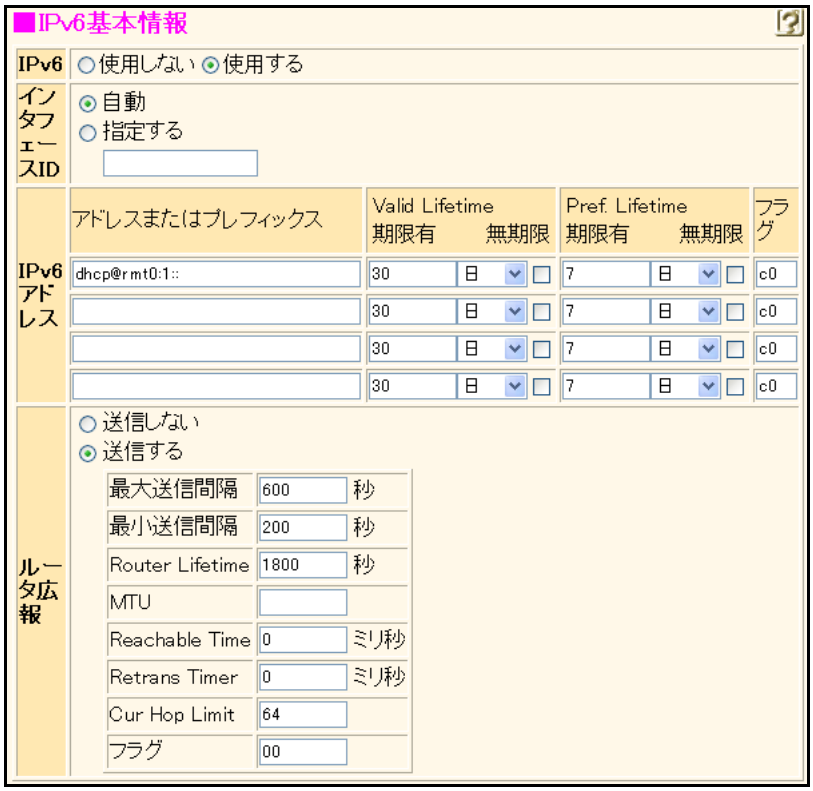
「LAN1 情報（物理 LAN）」ページが表示されます。

4.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

5.　以下の項目を指定します。

- IPv6　→使用する
- IPv6 アドレス
  アドレスまたはプレフィックス　→ dhcp@rmt0:1::
- ルータ広報　→送信する



6.　［保存］ボタンをクリックします。

ProxyDNS を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

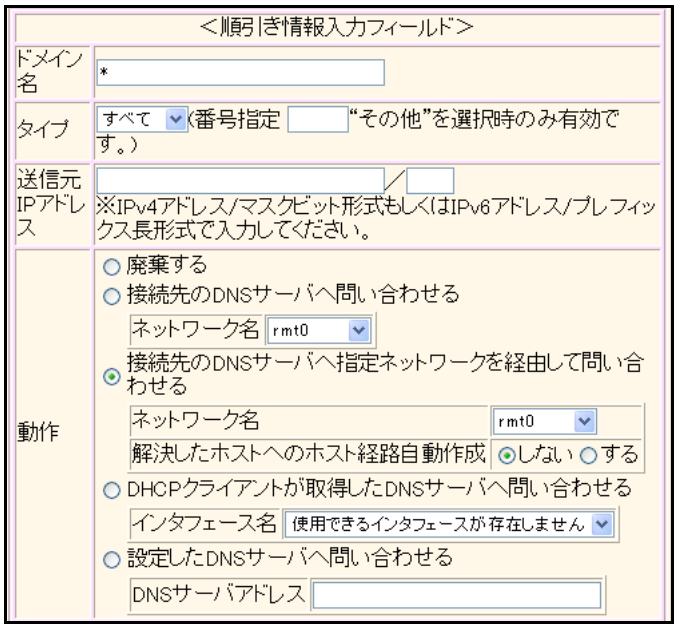
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- 動作　→接続先の DNS サーバへ指定ネットワークを経由して問い合わせる



4.　［追加］ボタンをクリックします。

5.　「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

6.　以下の項目を指定します。

- 動作　→接続先の DNS サーバへ指定ネットワークを経由して問い合わせる

7.　［追加］ボタンをクリックします。

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.24 DNS サーバ機能を使う（ProxyDNS）

適用機種　全機種

本装置の ProxyDNS には、以下の機能があります。

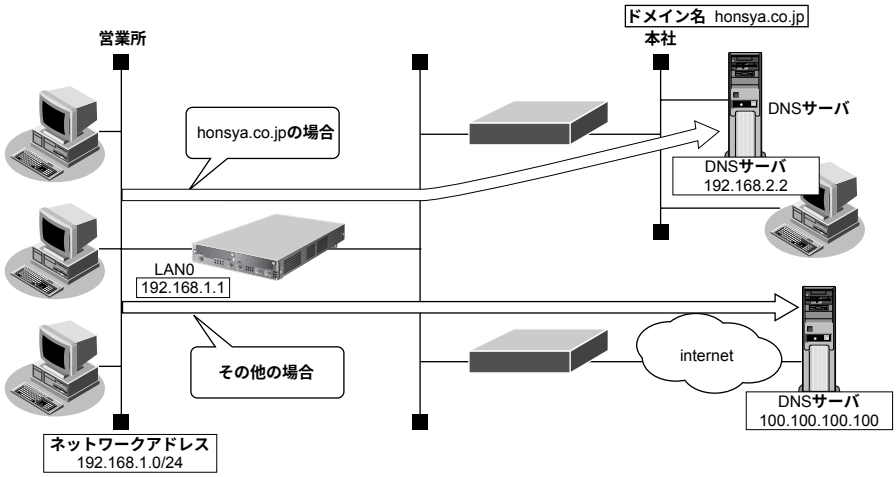
- DNS サーバの自動切り替え機能
- DNS サーバアドレスの自動取得機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

参照　Si-R シリーズ　機能説明書「2.22 DNS サーバ機能」（P.96）

2.24.1 DNS サーバの自動切り替え機能（順引き）を使う

適用機種　全機種

ProxyDNS は、パソコン側で本装置の IP アドレスを DNS サーバの IP アドレスとして登録するだけで、ドメインごとに使用する DNS サーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  使用するドメイン　：honsya.co.jp
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  使用するドメイン　：honsya.co.jp 以外
  DNS サーバの IP アドレス　：100.100.100.100

パソコン側の設定を確認する

1.　パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS 情報を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

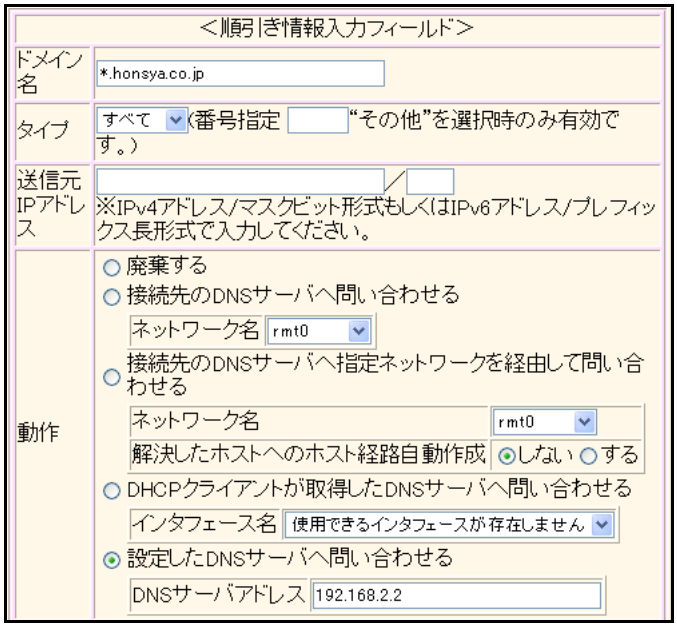
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊ .honsya.co.jp
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 192.168.2.2



4.　［追加］ボタンをクリックします。

5.　手順 3.～4. を参考に、以下の項目を指定します。

- ドメイン名　→＊
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 100.100.100.100

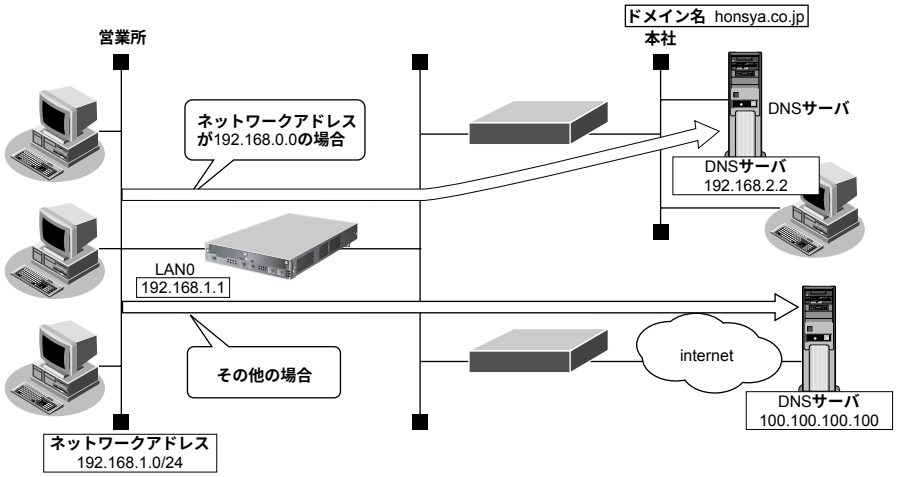
6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.24.2　DNS サーバの自動切り替え機能（逆引き）を使う

適用機種　全機種

ProxyDNS は、先に説明した順引きとは逆に、IP アドレスごとに使用する DNS サーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0 以外
  DNS サーバの IP アドレス　：100.100.100.100

パソコン側の設定を確認する

1.　パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS 情報を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

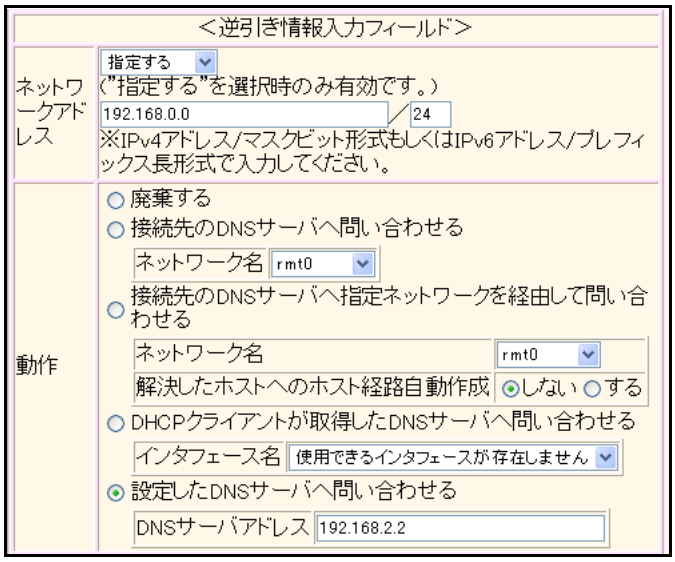
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

3.　以下の項目を指定します。

- ネットワークアドレス　→指定する
  → 192.168.0.0/24
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 192.168.2.2



4.　［追加］ボタンをクリックします。

5.　手順 3.～4. を参考に、以下の項目を指定します。

- ネットワークアドレス　→すべて
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 100.100.100.100

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.24.3　DNS サーバアドレスの自動取得機能を使う

適用機種　全機種

この機能を利用すると、ProxyDNS が DNS サーバのアドレスを、回線接続時に接続先から自動的に取得します。そのため、DNS サーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、接続先が DNS サーバアドレスの配布機能（RFC1877）に対応している場合にだけ利用できます。

● 設定条件

- ドメイン名　：＊
- 動作　：接続先の DNS サーバへ指定ネットワークを経由して問い合わせる

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

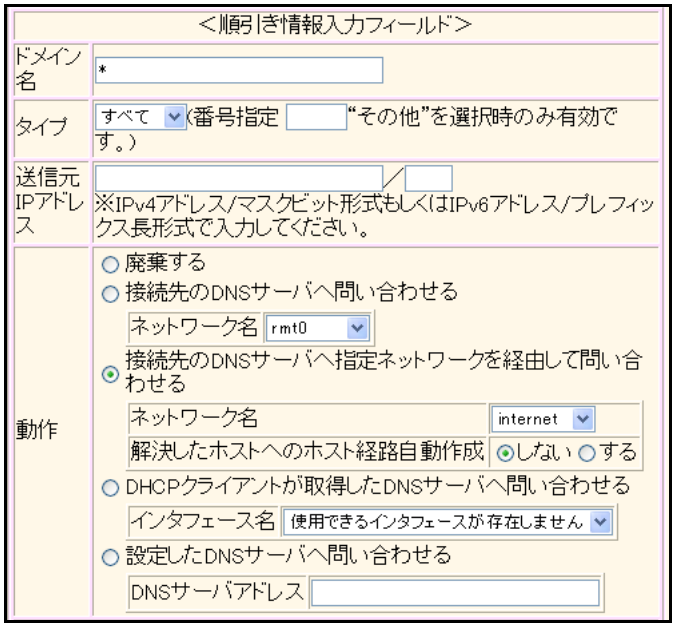
2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- 動作　→接続先の DNS サーバへ指定ネットワークを経由して問い合わせる

  ネットワーク名　→internet（DNS サーバを使用するネットワーク名）



4.　［追加］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

ここでは、Windows® 2000 の場合を例に説明します。

1.　［コントロールパネル］ウィンドウで［ネットワークとダイヤルアップ接続］アイコンをダブルクリックします。

2.　［ローカルエリア接続］アイコンを右クリックし、プロパティを選択します。

［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。

3.　一覧から「インターネットプロトコル（TCP/IP）」をクリックして選択します。

4.　［プロパティ］ボタンをクリックします。

5.　「次の DNS サーバーのアドレスを使う」を選択します。

6.　「優先 DNS サーバー」に、本装置の IP アドレスを入力します。

7.　［OK］ボタンをクリックします。

8.　［はい］ボタンをクリックし、パソコンを再起動します。

再起動後に、設定した内容が有効になります。

ヒント

◆ 本装置の「DHCP サーバ機能」を使わない場合の設定は？

パソコン側の「DNS 設定」で本装置の IP アドレスを指定すると、ProxyDNS 機能だけ使用できます。また、本装置以外の DHCP サーバを使用している場合でも、DHCP サーバで広報する DNS サーバの IP アドレスとして本装置の IP アドレスを指定すると ProxyDNS 機能を使用できます。

◆ DNS 解決したホストへのホスト経路を自動で作成する設定は？

「ProxyDNS 情報 URL フィルタ情報」－「順引き情報」の動作に“接続先の DNS サーバへ指定ネットワークを経由して問い合わせる”を指定した場合は、「解決したホストへのホスト経路自動作成」に“する”を指定することにより、DNS 解決したホストへのホスト経路を自動で作成することができます。

◆「接続先の DNS サーバへ問い合わせる」と「接続先の DNS サーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先の DNS サーバへ問い合わせる」は、経路情報に従って、接続先から取得した DNS サーバへ問い合わせるのに対して、「接続先の DNS サーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得した DNS サーバへ問い合わせます。

2.24.4　DNS サーバアドレスを DHCP サーバから取得して使う

適用機種　全機種

この機能を利用すると、ProxyDNS が DNS サーバのアドレスを、DHCP サーバから自動的に取得します。そのため、DNS サーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、DHCP サーバが DNS サーバのアドレスを広報している場合にだけ利用できます。

● 設定条件

- ドメイン名　：＊
- 動作　：lan0 の DNS サーバへ問い合わせる

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

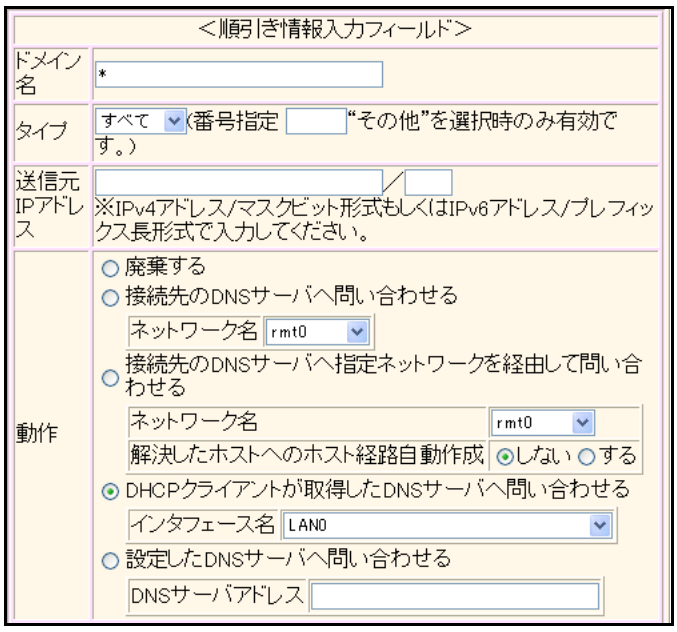
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- 動作　→DHCP クライアントが取得した DNS サーバへ問い合わせる
  インタフェース名　→LAN0（DNS サーバのアドレスを取得しているインタフェース）



4. **［追加］ボタンをクリックします。**

5. **画面左側の［設定反映］ボタンをクリックします。**
設定した内容が有効になります。

パソコン側の設定を行う

ここでは、Windows® 2000の場合を例に説明します。

1. **［コントロールパネル］ウィンドウで［ネットワークとダイヤルアップ接続］アイコンをダブルクリックします。**

2. **［ローカルエリア接続］アイコンを右クリックし、プロパティを選択します。**
［ローカルエリア接続のプロパティ］ダイアログボックスが表示されます。

3. **一覧から「インターネットプロトコル（TCP/IP)」をクリックして選択します。**

4. **［プロパティ］ボタンをクリックします。**

5. **「次のDNSサーバーのアドレスを使う」を選択します。**

6. **「優先DNSサーバー」に、本装置のIPアドレスを入力します。**

7. **［OK］ボタンをクリックします。**

8. **［はい］ボタンをクリックし、パソコンを再起動します。**
再起動後に、設定した内容が有効になります。

ヒント

◆ 本装置の「DHCPサーバ機能」を使わない場合の設定は？

パソコン側の「DNS設定」で本装置のIPアドレスを指定すると、ProxyDNS機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS機能を使用できます。

◆ DNS解決したホストへのホスト経路を自動で作成する設定は？

「ProxyDNS情報 URLフィルタ情報」－「順引き情報」の動作に“接続先のDNSサーバへ指定ネットワークを経由して問い合わせる”を指定した場合は、「解決したホストへのホスト経路自動作成」に“する”を指定することにより、DNS解決したホストへのホスト経路を自動で作成することができます。

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わせるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.24.5　DNS 問い合わせタイプフィルタ機能を使う

適用機種　全機種

端末が送信する DNS パケットのうち、特定の問い合わせタイプ（QTYPE）のパケットを破棄することができます。

たとえば、Windows® 2000 が送信する予期しない DNS パケットによって、自動発信する問題を回避するために、かんたん設定のかんたんフィルタを「使用する」に設定します。このとき、問い合わせタイプが SOA（6）と SRV（33）のパケットを破棄する場合の設定方法を説明します。

こんな事に気をつけて

ProxyDNS 機能を使用する場合、問い合わせタイプが A（1）の DNS 問い合わせパケットを破棄するように指定にすると、正常な通信が行えなくなります。

● 設定条件

- ドメイン名　：＊
- 問い合わせタイプ　：SOA（6）
- 動作　：破棄する

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

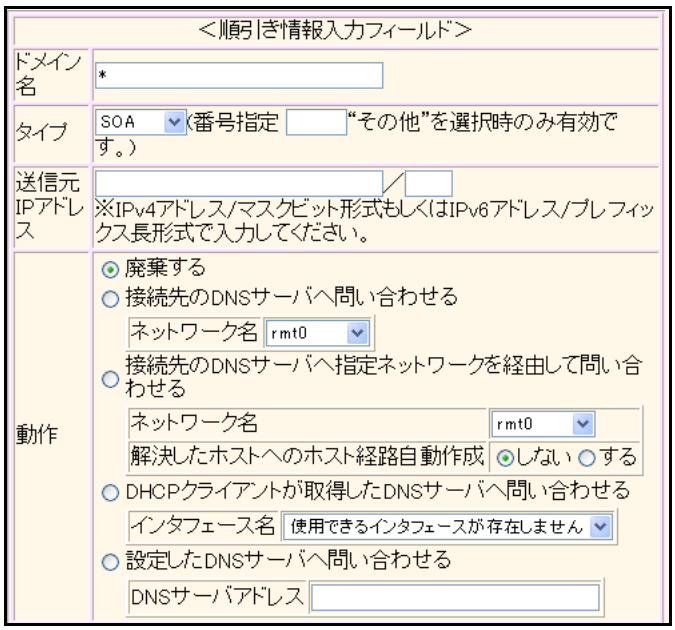
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- タイプ　→SOA
- 動作　→廃棄する



4.　［追加］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「2.24.3 DNS サーバアドレスの自動取得機能を使う」（P.768）の「パソコン側の設定を行う」（P.769）を参照してください。

2.24.6　DNS サーバ機能を使う

適用機種　全機種

本装置のホストデータベースにホスト名と IP アドレスを登録します。登録したホストに対して DNS 要求があった場合は、ProxyDNS が DNS サーバの代わりに応答します。LAN 内の情報をホストデータベースにあらかじめ登録しておくと、LAN 内のホストの DNS 要求によって回線が接続されるといったトラブルを防止できます。

● 設定条件

- ホスト名　：host.com
- IPv4 アドレス　：192.168.1.2
- IPv6 アドレス　：2001:db8::2

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1.　設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

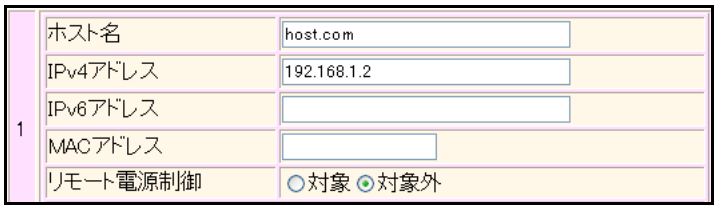
「ホストデータベース情報」ページが表示されます。

2.　未設定の欄の［修正］ボタンをクリックします。

3.　以下の項目を指定します。

- ホスト名　→host.com（パソコンの名前）
- IPv4 アドレス　→192.168.1.2（パソコンの IP アドレス）
- リモート電源制御　→対象外

補足　ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。



4.　［保存］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

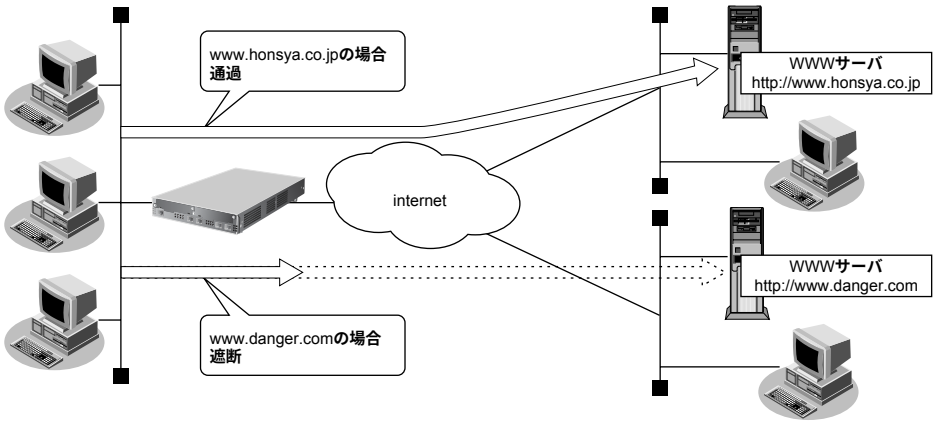
設定方法は、「2.24.3 DNS サーバアドレスの自動取得機能を使う」（P.768）の「 パソコン側の設定を行う」（P.769）を参照してください。

2.25 特定の URL へのアクセスを禁止する（URL フィルタ機能）

適用機種　全機種

URL フィルタ機能は、特定の URL へのアクセスを禁止することができます。本機能を使用する場合は、ProxyDNS 情報で設定します。

以下に URL フィルタを行う場合の設定方法を説明します。



☛参照　Si-R シリーズ　機能説明書「2.22 DNS サーバ機能」（P.96）

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS 情報は何も設定されていないものとします。

● 設定条件

- アクセスを禁止するドメイン名　：www.danger.com

こんな事に気をつけて

- **URL フィルタ機能を使用する場合は、LAN 内のパソコンが本装置の IP アドレスを DNS サーバの IP アドレスとして登録する必要があります。**
- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

☛参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

ヒント

◆「＊」は使えるの？

たとえば「www.danger.com」と「XXX.danger.com」の両方を URL フィルタの対象とする場合は「＊.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合の設定例を示します。

URL フィルタの情報を設定する

1.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

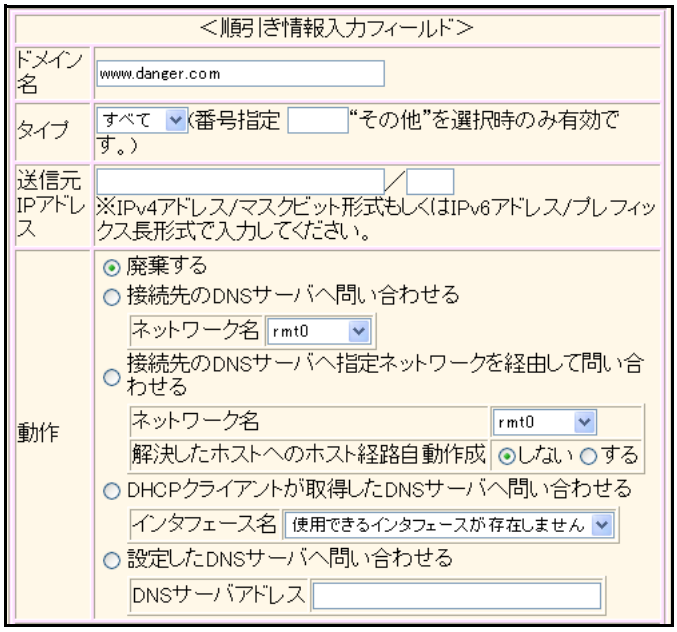
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します

- ドメイン名　→www.danger.com
- 動作　→廃棄する



4.　［追加］ボタンをクリックします。

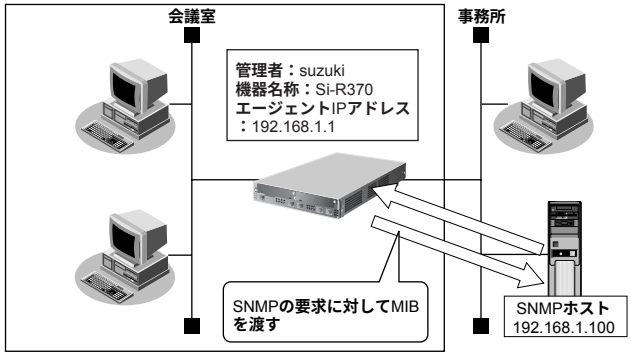
5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.26 SNMP エージェント機能を使う

適用機種　全機種

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。
ここでは、Si-R370 が SNMP ホストに対して MIB 情報を通知する場合の設定方法を説明します。



参照　Si-R シリーズ　機能説明書「2.23 SNMP 機能」（P.98）

ヒント

◆ SNMP とは？

SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMP ホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、SNMP ホストの要求に対して MIB（Management Information Base）という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMP エージェントから SNMP ホストに対して非同期通知を行うことができます。

参照　Si-R シリーズ　仕様一覧「3.1 標準 MIB 定義」（P.50）、「3.2 富士通拡張 MIB」（P.79）、「3.3 Trap 一覧」（P.83）

こんな事に気をつけて

文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

参照　Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：Si-R370
- 機器設置場所　：1F（1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- コミュニティ名　：public00（SNMPv1/SNMPv2c 時）
- ユーザ名　：user00（SNMPv3 時）

上記の設定条件に従って設定を行う場合の設定例を示します。

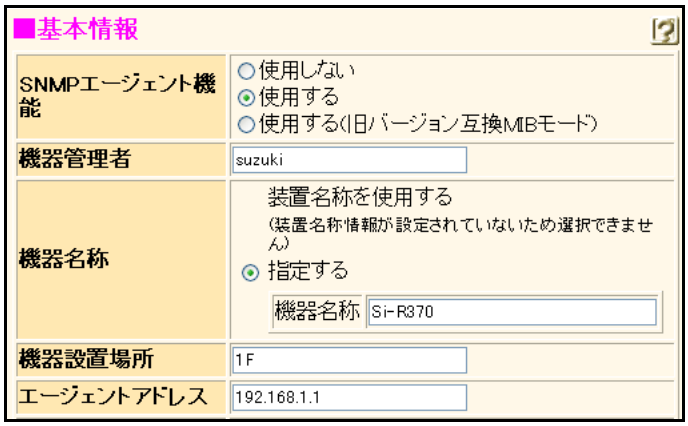
SNMP 情報を設定する

1.　設定メニューの詳細設定で「SNMP 情報」をクリックします。

「SNMP 情報」ページが表示されます。

2.　以下の項目を指定します。

- SNMP エージェント機能　→使用する
- 機器管理者　→ suzuki
- 機器名称　→指定する
  機器名称　→ Si-R370
- 機器設置場所　→ 1F
- エージェントアドレス　→ 192.168.1.1



3.　［保存］ボタンをクリックします。

SNMPv1 または SNMPv2c でアクセスする場合

SNMPv1 または SNMPv2c でアクセスする場合は、以下の情報を設定します。

4.　設定メニューの詳細設定で「SNMP 情報」をクリックします。

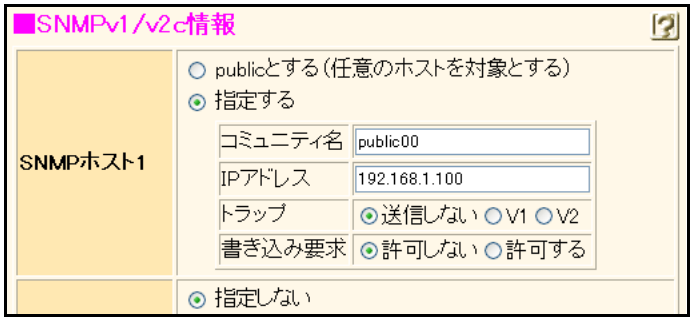
「SNMP 情報」ページが表示されます。

5.　「SNMPv1/v2c 情報」をクリックします。

「SNMPv1/v2c 情報」が表示されます。

6.　以下の項目を指定します。

- SNMP ホスト 1　→指定する
  コミュニティ名　→public00
  IP アドレス　→192.168.1.100
- SNMP ホスト 2 以降　→指定しない



7.　［保存］ボタンをクリックします。

SNMPv3 でアクセスする場合

SNMPv3 でアクセスする場合は、以下の情報を設定します。

8.　設定メニューの詳細設定で「SNMP 情報」をクリックします。

「SNMP 情報」ページが表示されます。

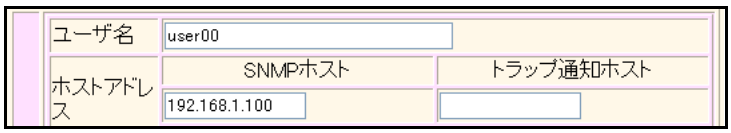
9.　「SNMPv3 情報」をクリックします。

「SNMPv3 情報」が表示されます。

10.　SNMPv3 情報リストの［修正］ボタンをクリックします。

11.　以下の項目を指定します。

- ユーザ名　→user00
- SNMP ホスト　→192.168.1.100



12.　［保存］ボタンをクリックします。

13.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

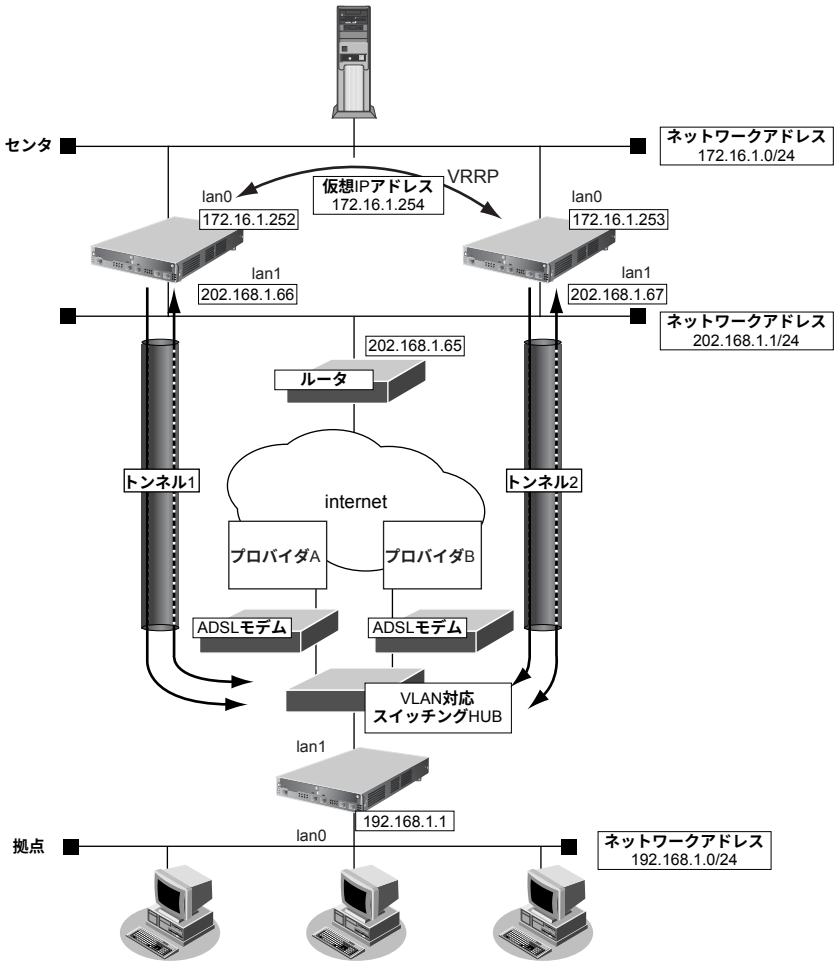
- エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SNMP ホストとの通信ができなくなります。
- ATM 網によっては、物理リンクが確立してから通信ができるようになるまでに時間がかかるものがあります。装置起動時に、ATM 網の先の SNMP ホストに送信した trap が、相手に正常に届かない場合があります。

2.27 ECMP 機能を使う

適用機種　全機種

ここでは、ECMP 機能を利用した負荷分散通信を行う場合の設定方法を説明します。

ADSL では、受信速度は高速ですが、送信速度はそれほど高速ではありません。この例では、ADSL を 2 本利用して負荷を分散することで、送信速度の向上をはかります。さらに、片方のトンネルに障害が発生した場合に、通信可能なトンネルを利用して通信のバックアップを実現します。



参照 Si-R シリーズ　機能説明書「2.24 ECMP 機能」（P.104）

● 設定条件

- 拠点では、センタへの通信は、トンネル 1 とトンネル 2 を利用して負荷分散して送信します。どちらかのトンネルで通信障害が発生した場合は、通信可能なトンネルだけを利用して送信します。
- センタでは、拠点への通信は、トンネル 1 だけを利用して送信します。トンネル 1 で通信障害が発生した場合は、トンネル 2 を利用して送信します。
- トンネル 1 の通信障害は、両端の本装置が接続先監視で検出します。
  この監視は、ISP A の通信障害およびセンタ側本装置（左）の故障を検出します。
- トンネル 2 の通信障害は、両端の本装置が接続先監視で検出します。
  この監視は、ISP B の通信障害およびセンタ側本装置（右）の故障を検出します。

上記の設定条件に従って設定を行う場合の設定例を示します。

センタ側本装置（左）を設定する

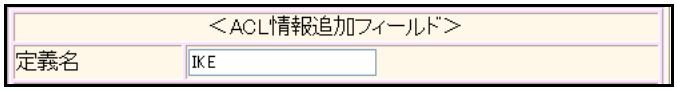
IPsec に関する ACL を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→IKE



3.　［追加］ボタンをクリックします。

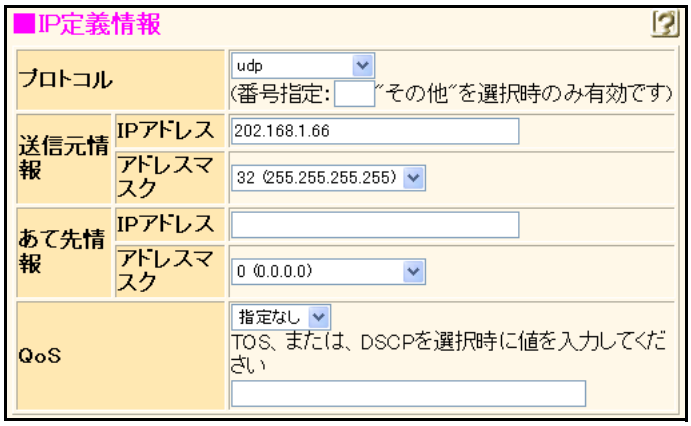
「ACL 定義情報（IKE）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→udp
- 送信元情報
  IP アドレス　→202.168.1.66
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし



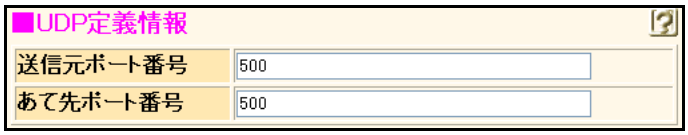
6.　［保存］ボタンをクリックします。

7.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→500
- あて先ポート番号　→500



9.　［保存］ボタンをクリックします。

10.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ESP

「ACL 定義情報（ESP）」-「IP 定義情報」

- プロトコル　→その他（50）
- 送信元情報
  IP アドレス　→202.168.1.66
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

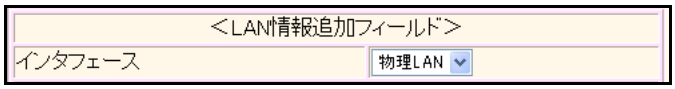
LAN1 側を設定する

11.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

12.　以下の項目を指定します。

- インタフェース　→物理 LAN



13.　［追加］ボタンをクリックします。

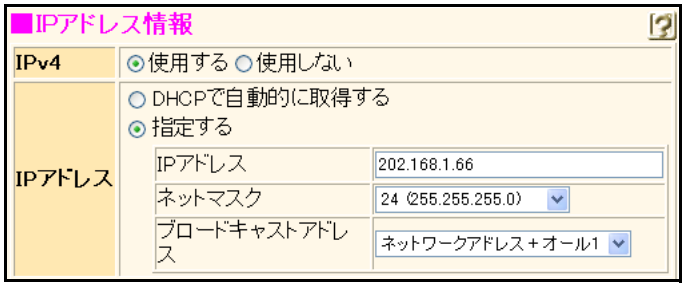
「LAN1 情報（物理 LAN）」ページが表示されます。

14.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

15.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→202.168.1.66
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1



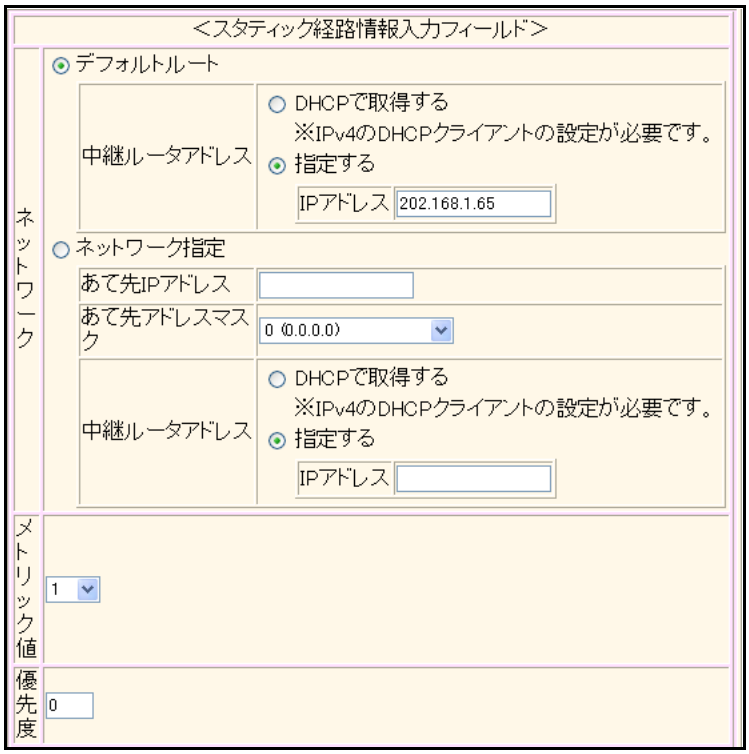
16.　［保存］ボタンをクリックします。

17.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

18.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
  中継ルータアドレス　→指定する
  IPアドレス　→202.168.1.65
- メトリック値　→1
- 優先度　→0



19.　［追加］ボタンをクリックします。

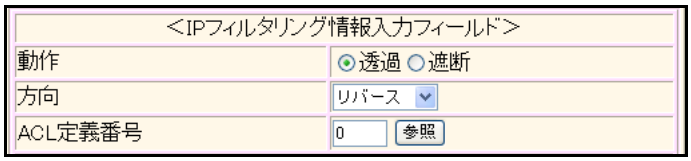
20.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

21.　以下の項目を指定します。

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



22.　［追加］ボタンをクリックします。

23.　手順 20.～22. を参考に、以下の項目を指定します。

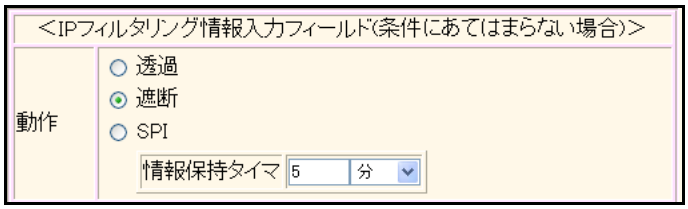
- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→1

24.　条件にあてはまらない場合の［修正］ボタンをクリックします。

「IP フィルタリング情報」（条件にあてはまらない場合）が表示されます。

25.　以下の項目を指定します。

- 動作　→遮断



26.　［保存］ボタンをクリックします。

トンネルを設定する

27.　設定メニューのルータ設定で「相手情報」をクリックします。

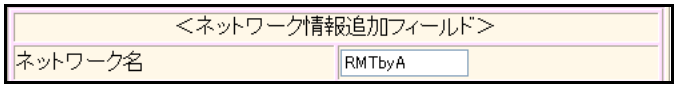
「相手情報」ページが表示されます。

28.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

29.　以下の項目を指定します。

- ネットワーク名　→RMTbyA



30.　［追加］ボタンをクリックします。

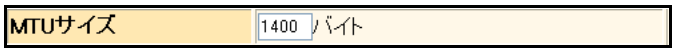
「ネットワーク情報（RMTbyA)」が表示されます。

31.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

32.　以下の項目を指定します。

- MTU サイズ　→ 1400



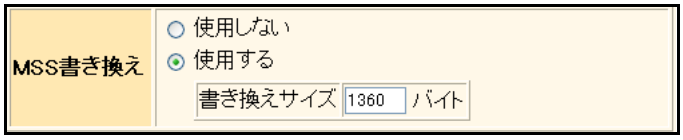
33.　［保存］ボタンをクリックします。

34.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

35.　以下の項目を指定します。

- MSS 書き換え　→使用する
  書き換えサイズ　→ 1360



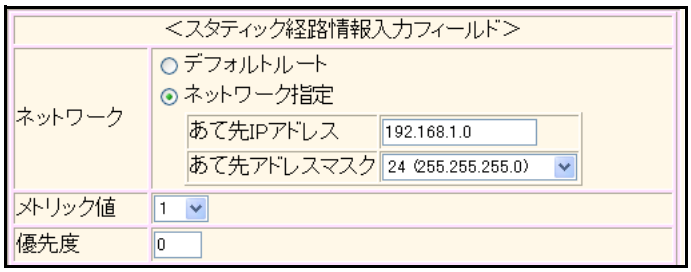
36.　［保存］ボタンをクリックします。

37.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

38.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



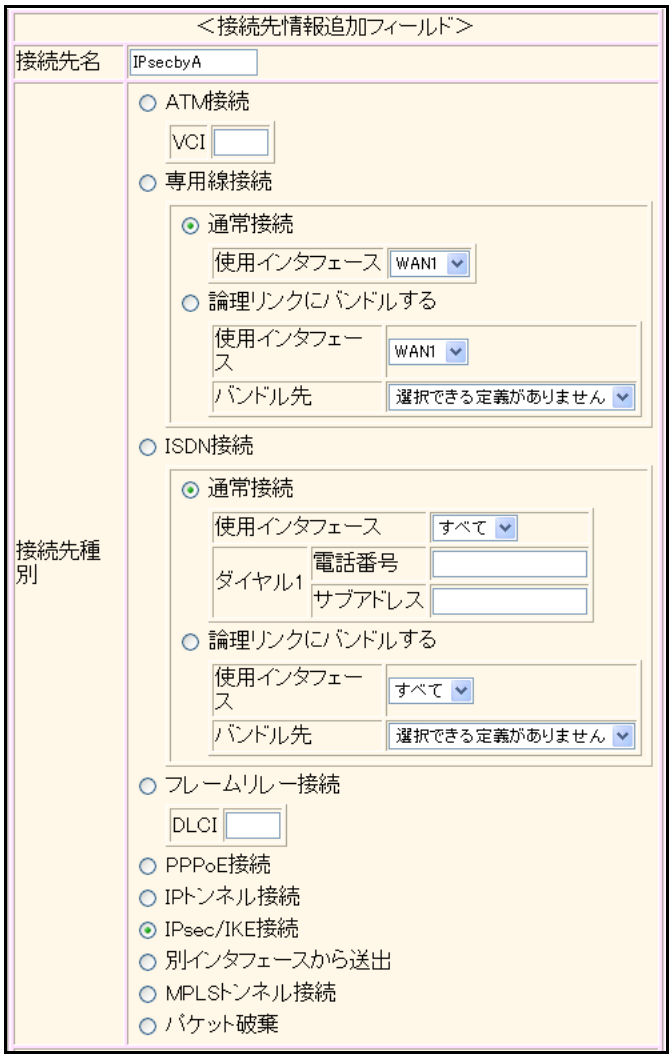
39.　［追加］ボタンをクリックします。

40.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

41.　以下の項目を指定します。

- 接続先名　→IPsecbyA
- 接続先種別　→IPsec/IKE 接続



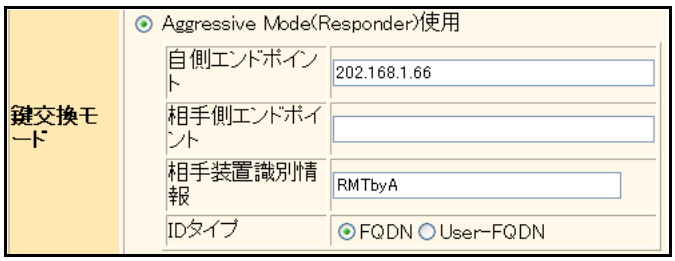
機種により、接続先種別の表示が上記の画面とは異なります。

42.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

43.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.1.66
  相手装置識別情報　→RMTbyA
  ID タイプ　→FQDN



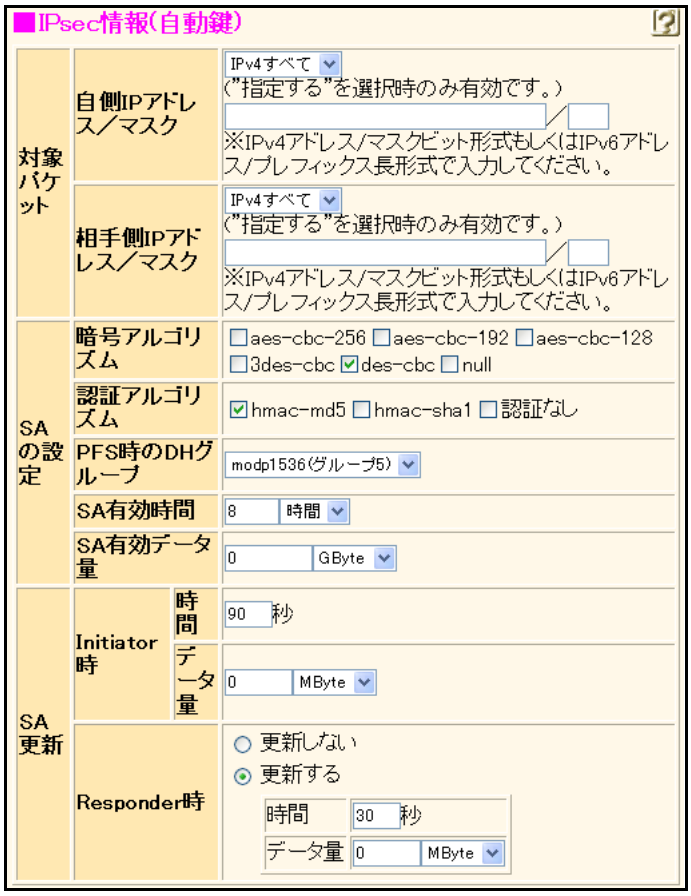
44.　［保存］ボタンをクリックします。

45.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

46.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→IPv4 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5
  PFS 時の DH グループ　→modp1536（グループ 5）
  SA 有効時間　→8 時間
- SA 更新
  Responder 時　→更新する
  時間　→30



47.　［保存］ボタンをクリックします。

48.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

49.　以下の項目を指定します。

- IKE 認証鍵

  鍵識別　→文字列

  鍵　→12345678-A

50.　［保存］ボタンをクリックします。

51.　IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

52.　以下の項目を指定します。

- 接続先監視　→使用する

  送信元 IP アドレス　→172.16.1.252

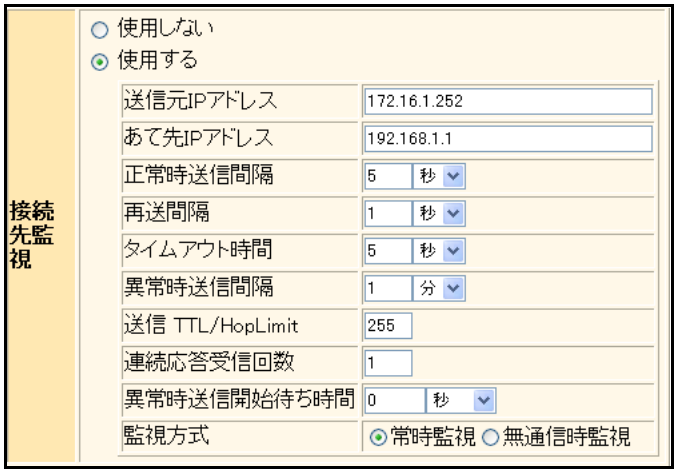
  あて先 IP アドレス　→192.168.1.1

  正常時送信間隔　→5 秒

  再送間隔　→1 秒

  タイムアウト時間　→5 秒

  異常時送信間隔　→1 分



53.　［保存］ボタンをクリックします。

LAN0 側を設定する

54.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

55.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

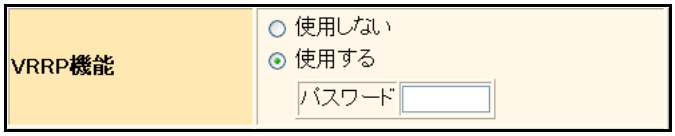
「LAN0 情報（物理 LAN）」ページが表示されます。

56.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

57.　以下の項目を指定します。

- VRRP 機能　→使用する



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

58.　［保存］ボタンをクリックします。

59.　共通情報の設定項目の「VRRP グループ情報」をクリックします。

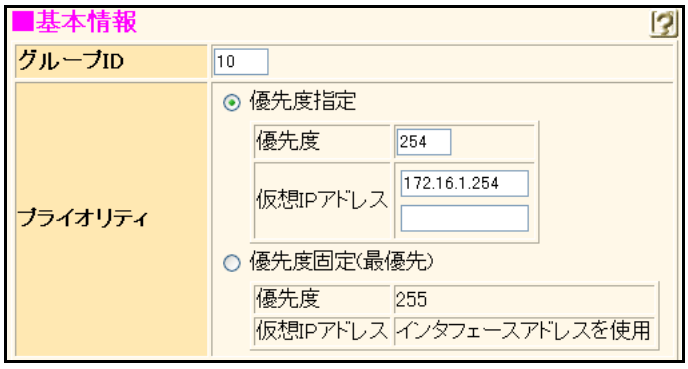
「VRRP グループ情報」が表示されます。

60.　「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

61.　以下の項目を指定します。

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 172.16.1.254



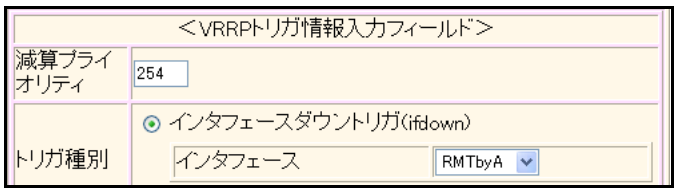
62.　［保存］ボタンをクリックします。

63.　VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

64.　以下の項目を指定します。

- 減算プライオリティ　→ 254
- トリガ種別　→インタフェースダウントリガ（ifdown）
  インタフェース　→ RMTbyA



65.　［追加］ボタンをクリックします。

66.　画面上部の「LAN0 情報」をクリックします。

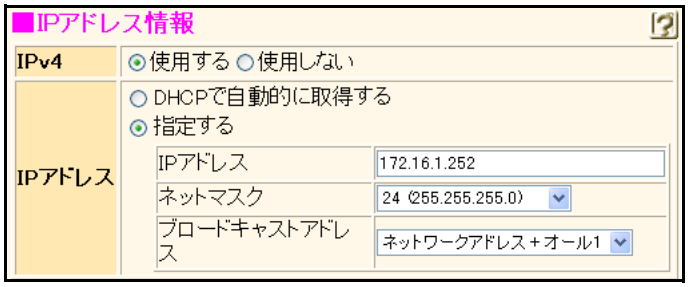
「LAN0 情報（物理 LAN）」ページが表示されます。

67.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

68.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 172.16.1.252
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



69.　［保存］ボタンをクリックします。

70.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

センタ側本装置（右）を設定する

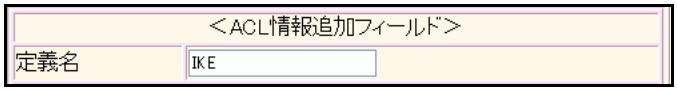
IPsec に関する ACL を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ IKE



3.　［追加］ボタンをクリックします。

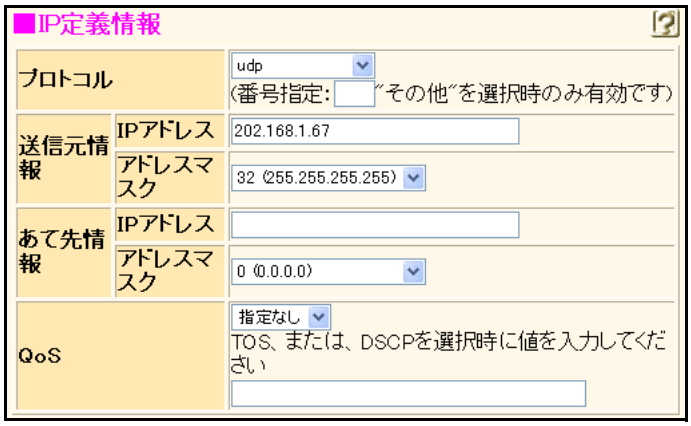
「ACL 定義情報（IKE）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→udp
- 送信元情報
  IPアドレス　→202.168.1.67
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし



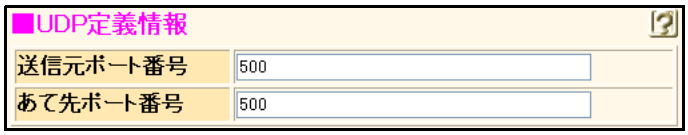
6.　[保存] ボタンをクリックします。

7.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→500
- あて先ポート番号　→500



9.　[保存] ボタンをクリックします。

10.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ESP

「ACL 定義情報（ESP）」-「IP 定義情報」

- プロトコル　→その他（50）
- 送信元情報
  IPアドレス　→202.168.1.67
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

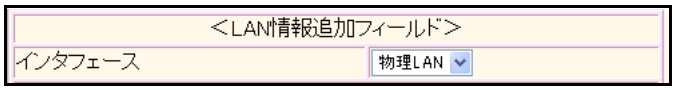
LAN1 側を設定する

11.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

12.　以下の項目を指定します。

- インタフェース　→物理 LAN



13.　［追加］ボタンをクリックします。

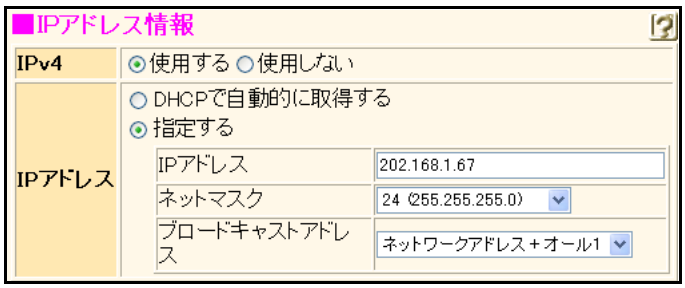
「LAN1 情報（物理 LAN）」ページが表示されます。

14.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

15.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→202.168.1.67
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



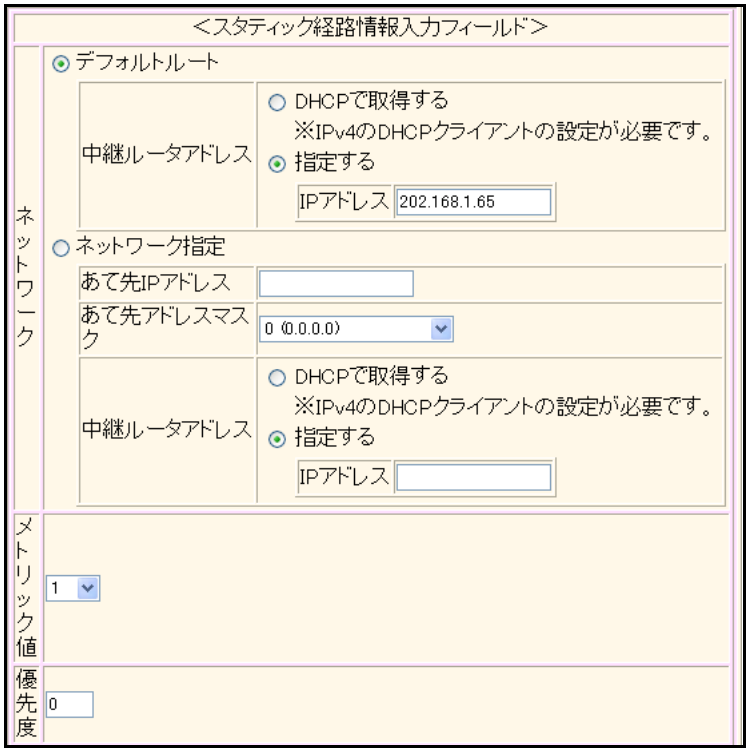
16.　［保存］ボタンをクリックします。

17.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

18.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
  中継ルータアドレス　→指定する
  IP アドレス　→202.168.1.65
- メトリック値　→1
- 優先度　→0



19.　［追加］ボタンをクリックします。

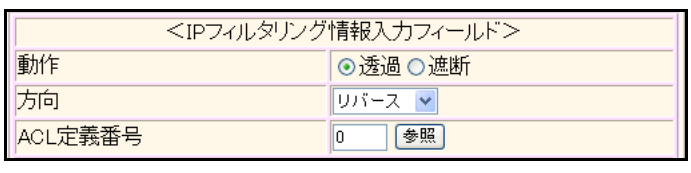
20.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

21.　以下の項目を指定します。

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



22.　［追加］ボタンをクリックします。

23.　手順 20. ～ 22. を参考に、以下の項目を指定します。

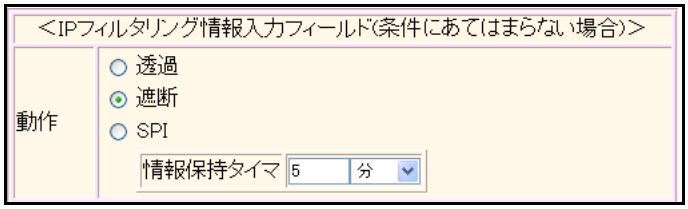
- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→ 1

24.　条件にあてはまらない場合の［修正］ボタンをクリックします。

「IP フィルタリング情報」（条件にあてはまらない場合）が表示されます。

25.　以下の項目を指定します。

- 動作　→遮断



26.　［保存］ボタンをクリックします。

トンネルを設定する

27.　設定メニューのルータ設定で「相手情報」をクリックします。

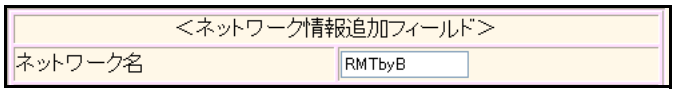
「相手情報」ページが表示されます。

28.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

29.　以下の項目を指定します。

- ネットワーク名　→ RMTbyB



30.　［追加］ボタンをクリックします。

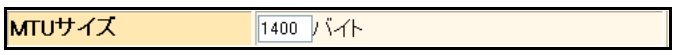
「ネットワーク情報（RMTbyB）」が表示されます。

31.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

32.　以下の項目を指定します。

- MTU サイズ　→ 1400



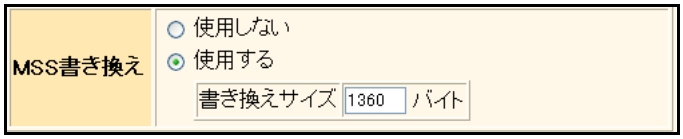
33.　［保存］ボタンをクリックします。

34.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

35.　以下の項目を指定します。

- MSS 書き換え　→使用する
  書き換えサイズ　→1360



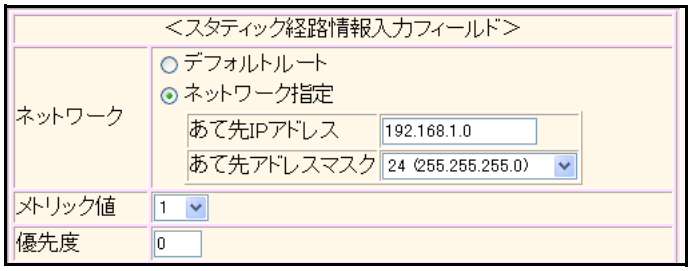
36.　［保存］ボタンをクリックします。

37.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

38.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



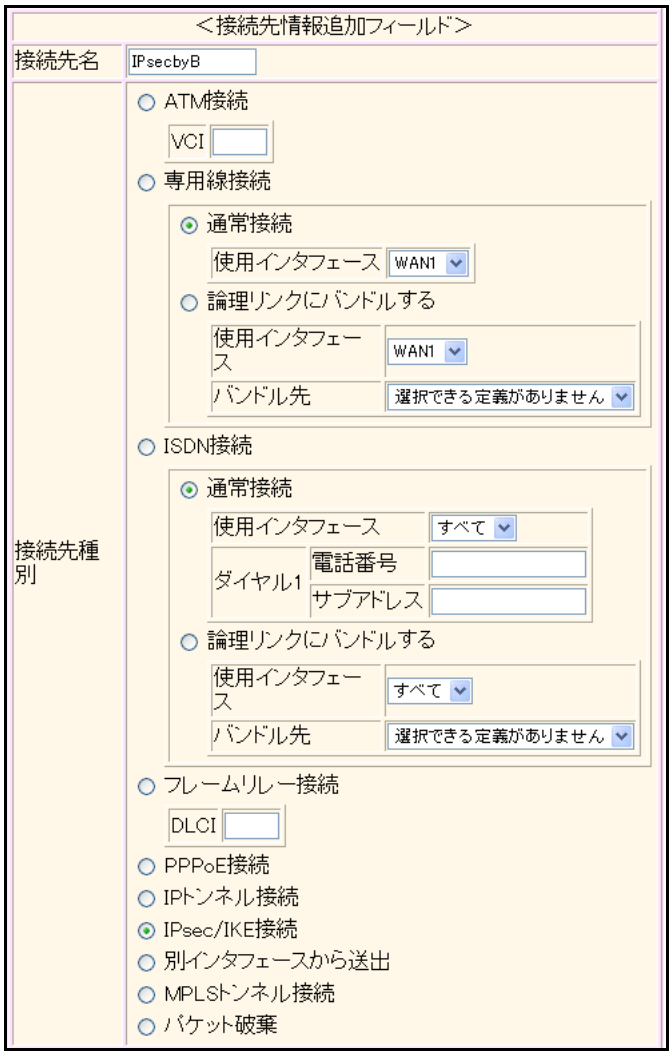
39.　［追加］ボタンをクリックします。

40.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

41.　以下の項目を指定します。

- 接続先名　→IPsecbyB
- 接続先種別　→IPsec/IKE 接続



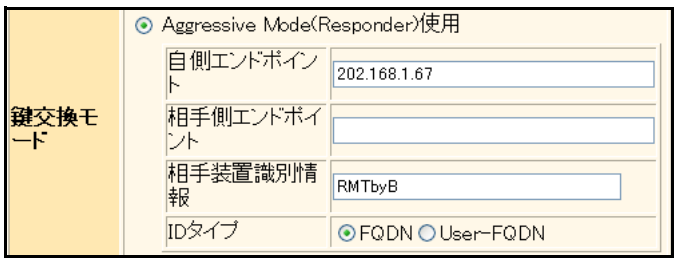
機種により、接続先種別の表示が上記の画面とは異なります。

42.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

43.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Responder）使用
  自側エンドポイント　→202.168.1.67
  相手装置識別情報　→RMTbyB
  ID タイプ　→FQDN



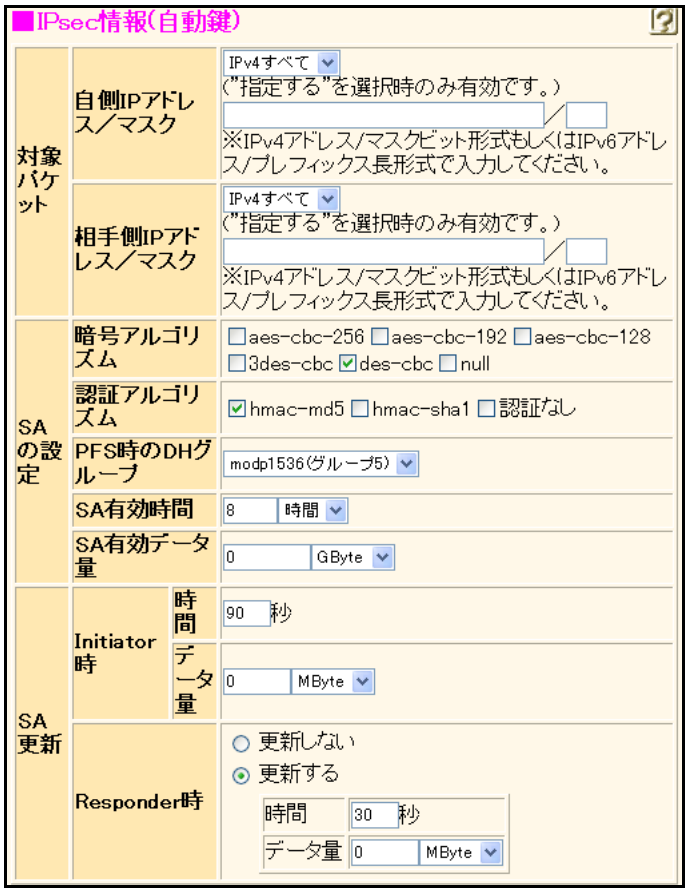
44.　［保存］ボタンをクリックします。

45.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

46.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→IPv4 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5
  PFS 時の DH グループ　→modp1536（グループ 5）
  SA 有効時間　→8 時間
- SA 更新
  Responder 時　→更新する
  時間　→30



47.　［保存］ボタンをクリックします。

48.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

49.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→12345678-B

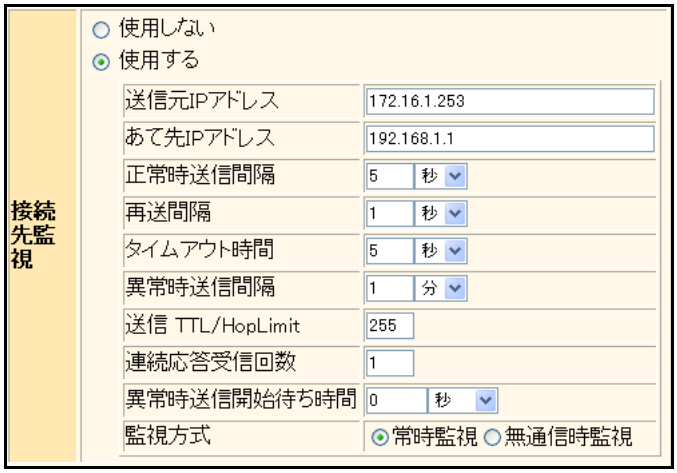
50.　［保存］ボタンをクリックします。

51.　IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

52.　以下の項目を指定します。

- 接続先監視　→使用する
  送信元 IP アドレス　→172.16.1.253
  あて先 IP アドレス　→192.168.1.1
  正常時送信間隔　→5 秒
  再送間隔　→1 秒
  タイムアウト時間　→5 秒
  異常時送信間隔　→1 分



53.　［保存］ボタンをクリックします。

LAN0 側を設定する

54.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

55.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

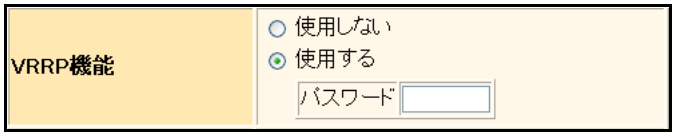
「LAN0 情報（物理 LAN）」ページが表示されます。

56.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

57.　以下の項目を指定します。

- VRRP 機能　　→使用する



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

58.　［保存］ボタンをクリックします。

59.　共通情報の設定項目の「VRRP グループ情報」をクリックします。

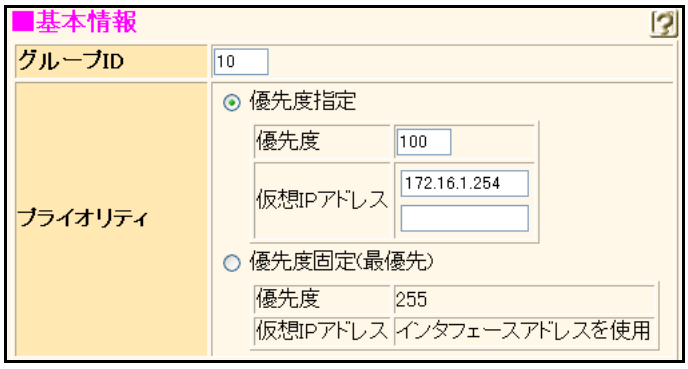
「VRRP グループ情報」が表示されます。

60.　「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

61.　以下の項目を指定します。

- グループ ID　　→ 10
- プライオリティ　　→優先度指定
  優先度　　→ 100
  仮想 IP アドレス　　→ 172.16.1.254



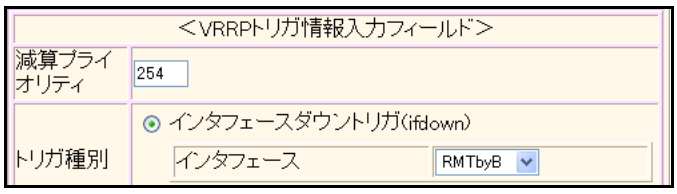
62.　［保存］ボタンをクリックします。

63.　VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

64.　以下の項目を指定します。

- 減算プライオリティ　　→ 254
- トリガ種別　　→インタフェースダウントリガ（ifdown）
  インタフェース　　→ RMTbyB



65.　［追加］ボタンをクリックします。

66.　画面上部の「LAN0 情報」をクリックします。

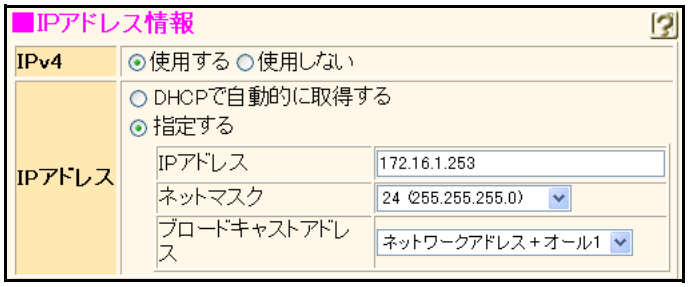
「LAN0 情報（物理 LAN）」ページが表示されます。

67.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

68.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 172.16.1.253
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



69.　［保存］ボタンをクリックします。

70.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

拠点側本装置を設定する

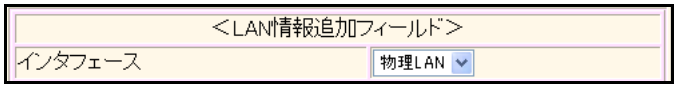
PPPoE で利用する LAN を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→物理 LAN



3.　［追加］ボタンをクリックします。

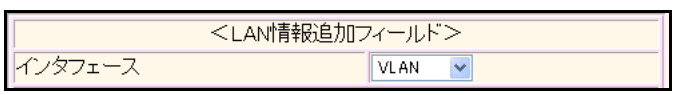
「LAN1 情報（物理 LAN）」ページが表示されます。

4.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

5.　以下の項目を指定します。

- インタフェース　→VLAN



6.　［追加］ボタンをクリックします。

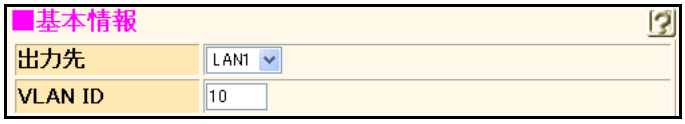
「LAN2 情報（VLAN）」ページが表示されます。

7.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

8.　以下の項目を指定します。

- 出力先　→ LAN1
- VLAN ID　→ 10



9.　［保存］ボタンをクリックします。

10.　手順 4. ～ 9. を参考に、以下の項目を指定します。

「LAN3 情報（VLAN）」ー「共通情報」

- 出力先　→ LAN1
- VLAN ID　→ 20

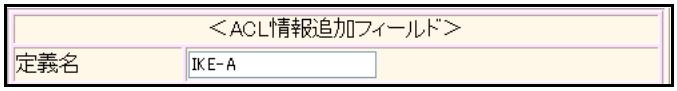
IPsec に関する ACL を設定する

11.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

12.　以下の項目を指定します。

- 定義名　→ IKE-A



13.　［追加］ボタンをクリックします。

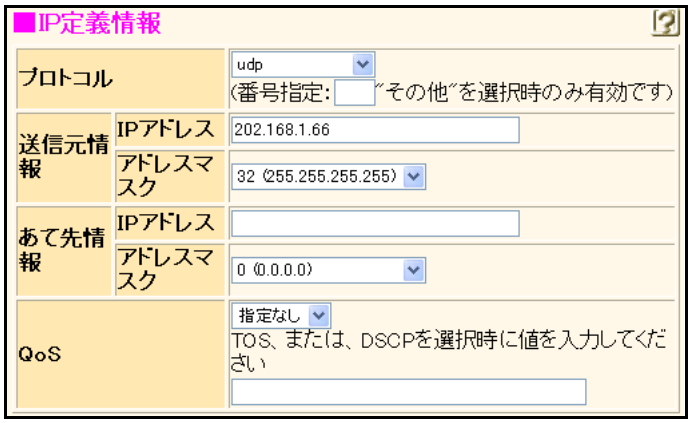
「ACL 定義情報（IKE-A）」ページが表示されます。

14.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

15.　以下の項目を指定します。

- プロトコル　→udp
- 送信元情報
  IPアドレス　→202.168.1.66
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし



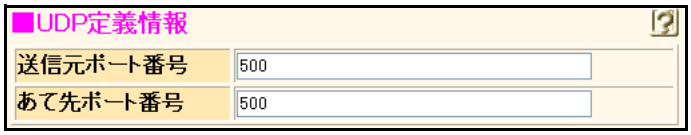
16.　［保存］ボタンをクリックします。

17.　「UDP 定義情報」をクリックします。

「UDP 定義情報」ページが表示されます。

18.　以下の項目を指定します。

- 送信元ポート番号　→500
- あて先ポート番号　→500



19.　［保存］ボタンをクリックします。

20.　手順 11.～16. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ESP-A

「ACL 定義情報（ESP-A）」-「IP 定義情報」

- プロトコル　→その他（50）
- 送信元情報
  IPアドレス　→202.168.1.66
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

21.　手順 11.～19. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→IKE-B

「ACL 定義情報（IKE-B)」-「IP 定義情報」

- プロトコル　→udp
- 送信元情報
  IP アドレス　→202.168.1.67
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

「ACL 定義情報（IKE-B)」-「UDP 定義情報」

- 送信元ポート番号　→500
- あて先ポート番号　→500

22.　手順 11.～16. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ESP-B

「ACL 定義情報（ESP-B)」-「IP 定義情報」

- プロトコル　→その他（50）
- 送信元情報
  IP アドレス　→202.168.1.67
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

プロバイダ A を利用する PPPoE 接続を設定する

23.　設定メニューのルータ設定で「相手情報」をクリックします。

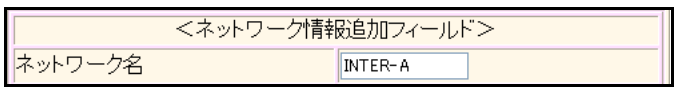
「相手情報」ページが表示されます。

24.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

25.　以下の項目を指定します。

- ネットワーク名　→INTER-A



26.　［追加］ボタンをクリックします。

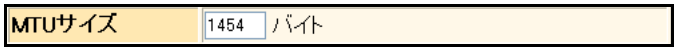
「ネットワーク情報（INTER-A)」が表示されます。

27.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

28.　以下の項目を指定します。

- MTU サイズ　　→1454



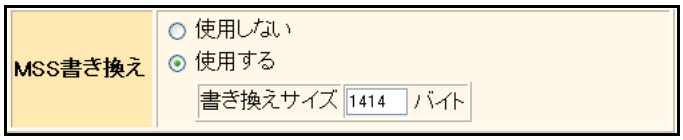
29.　［保存］ボタンをクリックします。

30.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

31.　以下の項目を指定します。

- MSS 書き換え　　→使用する
  書き換えサイズ　　→1414



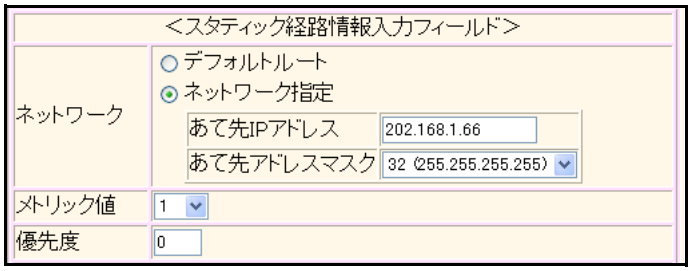
32.　［保存］ボタンをクリックします。

33.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

34.　以下の項目を指定します。

- ネットワーク　　→ネットワーク指定
  あて先 IP アドレス　　→202.168.1.66
  あて先アドレスマスク　　→32（255.255.255.255）
- メトリック値　　→1
- 優先度　　→0



35.　［追加］ボタンをクリックします。

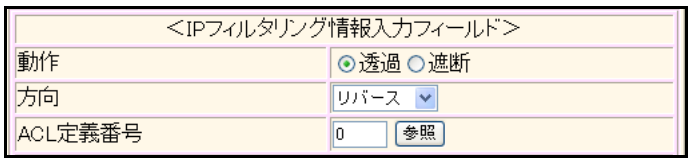
36.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

37.　以下の項目を指定します。

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→0

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



38.　［追加］ボタンをクリックします。

39.　手順 36. ～ 38. を参考に、以下の項目を指定します。

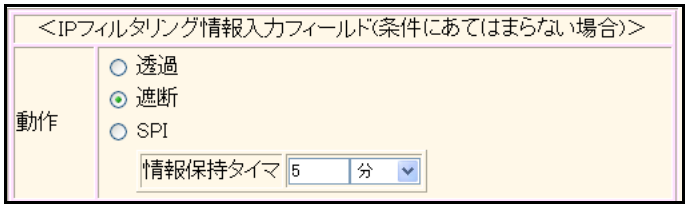
- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→1

40.　条件にあてはまらない場合の［修正］ボタンをクリックします。

「IP フィルタリング情報」（条件にあてはまらない場合）が表示されます。

41.　以下の項目を指定します。

- 動作　→遮断



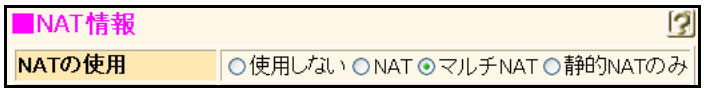
42.　［保存］ボタンをクリックします。

43.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

44.　以下の項目を指定します。

- NAT の使用　→マルチ NAT



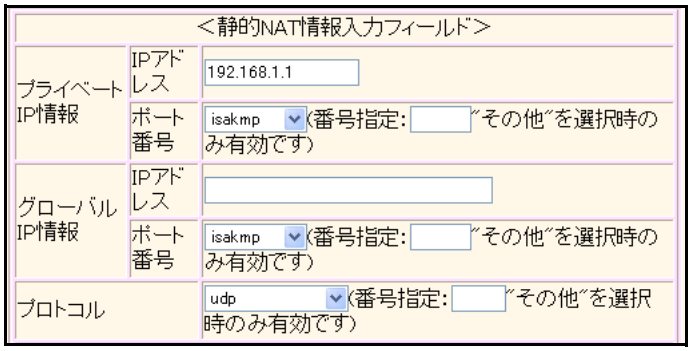
45.　［保存］ボタンをクリックします。

46.　IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

47.　以下の項目を指定します。

- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→ isakmp
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→ isakmp
- プロトコル　→ udp



48.　［追加］ボタンをクリックします。

49.　手順 46. ～ 48. を参考に、以下の項目を指定します。

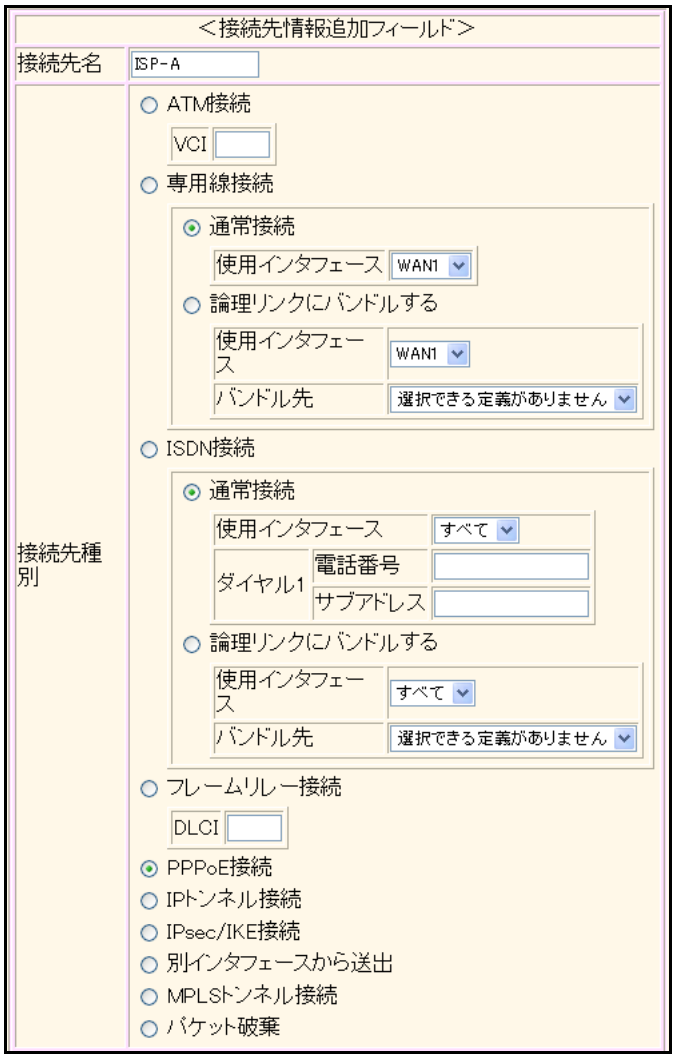
- プライベート IP 情報
  IP アドレス　→ 192.168.1.1
  ポート番号　→すべて
- グローバル IP 情報
  IP アドレス　→指定しない
  ポート番号　→すべて
- プロトコル　→ esp

50.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

51.　以下の項目を指定します。

- 接続先名　→ISP-A
- 接続先種別　→PPPoE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

52.　［追加］ボタンをクリックします。

PPPoE 接続の設定項目と「基本情報」が表示されます。

53.　以下の項目を指定します。

- 使用インタフェース　→LAN2

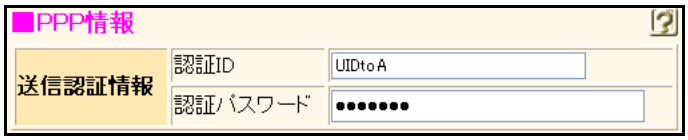
54.　［保存］ボタンをクリックします。

55.　PPPoE 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

56.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→ UIDtoA
  認証パスワード　→ PASStoA



57.　［保存］ボタンをクリックします。

プロバイダ B を利用する PPPoE 接続を設定する

58.　手順 23. ～ 58. を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ INTER-B

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 202.168.1.67
  あて先アドレスマスク　→ 32（255.255.255.255）
- メトリック値　→ 1
- 優先度　→ 0

「IP フィルタリング情報」

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→ 2
- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→ 3

「IP フィルタリング情報」-「条件にあてはまらない場合の動作」

- 動作　→遮断

「ネットワーク情報」-「接続先情報」

- 接続先名　→ ISP-B

「基本情報」

- 使用インタフェース　→ LAN3

「PPP 情報」

- 送信認証情報
  認証 ID　→ UIDtoB
  認証パスワード　→ PASStoB

センタ側本装置（左）とのトンネルを設定する

59.　設定メニューのルータ設定で「相手情報」をクリックします。

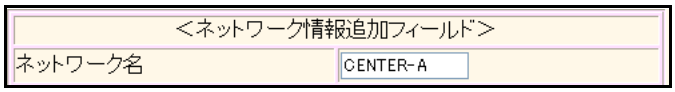
「相手情報」ページが表示されます。

60.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

61.　以下の項目を指定します。

- ネットワーク名　→CENTER-A



62.　［追加］ボタンをクリックします。

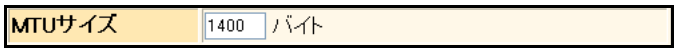
「ネットワーク情報（CENTER-A)」が表示されます。

63.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

64.　以下の項目を指定します。

- MTU サイズ　→1400



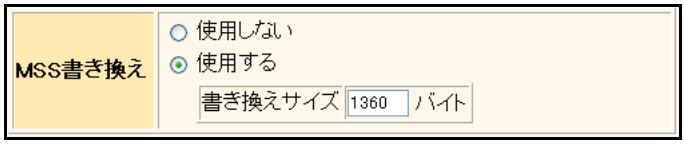
65.　［保存］ボタンをクリックします。

66.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

67.　以下の項目を指定します。

- MSS 書き換え　→使用する
  書き換えサイズ　→1360



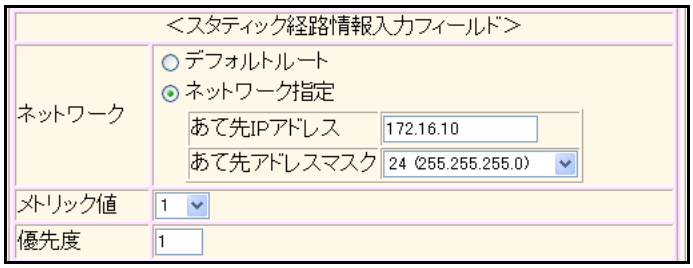
68.　［保存］ボタンをクリックします。

69.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

70.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→172.16.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→1



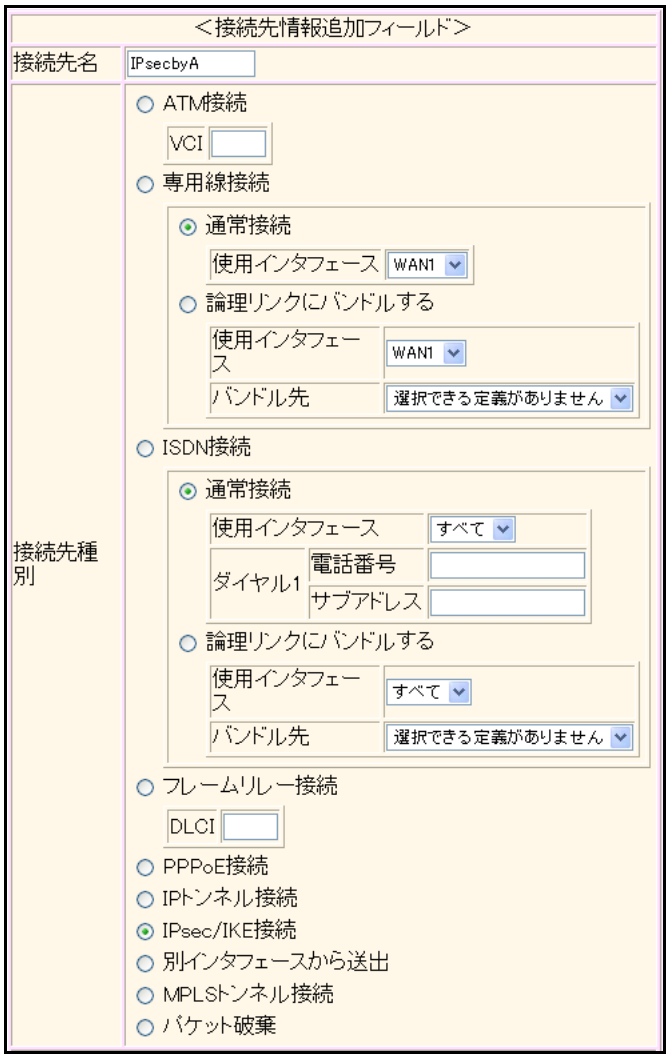
71.　［追加］ボタンをクリックします。

72.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

73.　以下の項目を指定します。

- 接続先名　→IPsecbyA
- 接続先種別　→IPsec/IKE 接続



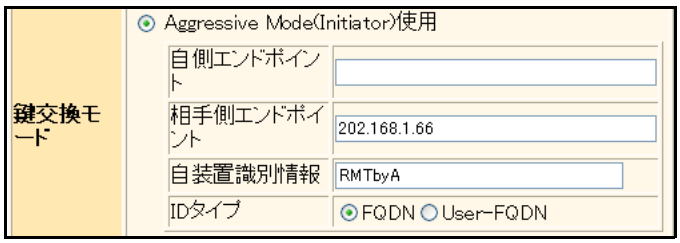
機種により、接続先種別の表示が上記の画面とは異なります。

74.　［追加］ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

75.　以下の項目を指定します。

- 鍵交換モード　→Aggressive Mode（Initiator）使用
  相手側エンドポイント　→202.168.1.66
  自装置識別情報　→RMTbyA
  ID タイプ　→FQDN



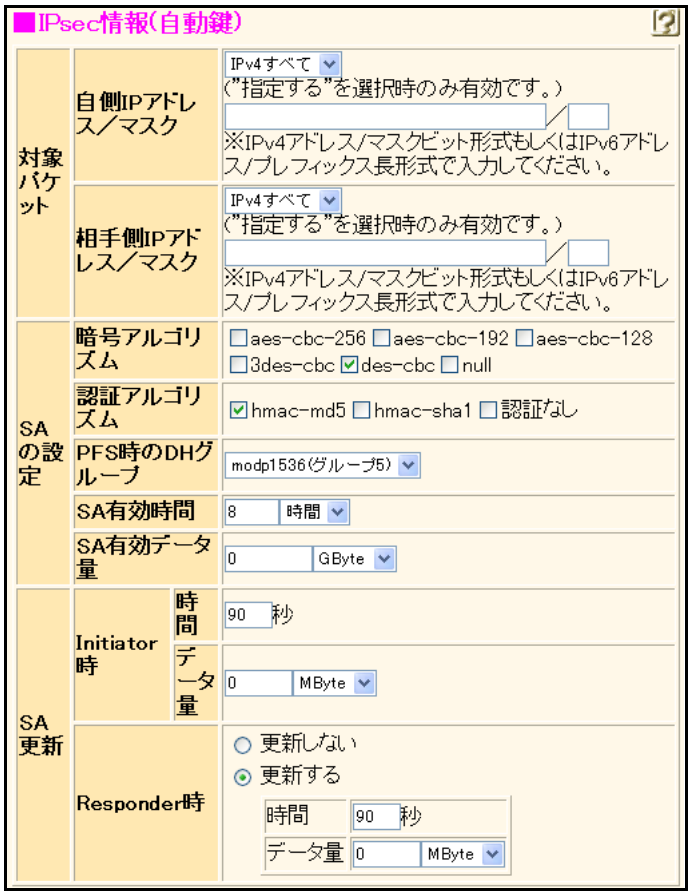
76.　［保存］ボタンをクリックします。

77.　IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

78.　以下の項目を指定します。

- 対象パケット
  自側 IP アドレス／マスク　→IPv4 すべて
  相手側 IP アドレス／マスク　→IPv4 すべて
- SA の設定
  暗号アルゴリズム　→des-cbc
  認証アルゴリズム　→hmac-md5
  PFS 時の DH グループ　→modp1536（グループ 5）
  SA 有効時間　→8 時間
- SA 更新
  Initiator 時
  時間　→90
  Responder 時　→更新する
  時間　→90



79.　［保存］ボタンをクリックします。

80.　IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

81.　以下の項目を指定します。

- IKE 認証鍵
  鍵識別　→文字列
  鍵　→12345678-A

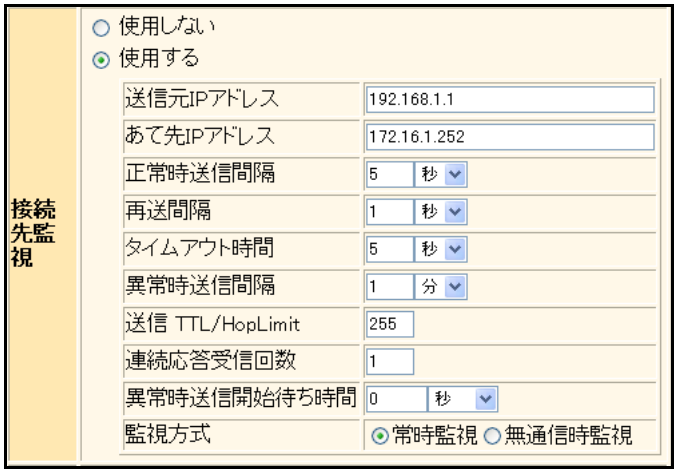
82.　［保存］ボタンをクリックします。

83.　IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

84.　以下の項目を指定します。

- 接続先監視　→使用する
  送信元 IP アドレス　→192.168.1.1
  あて先 IP アドレス　→172.16.1.252
  正常時送信間隔　→5 秒
  再送間隔　→1 秒
  タイムアウト時間　→5 秒
  異常時送信間隔　→1 分



85.　［保存］ボタンをクリックします。

センタ側本装置（右）とのトンネルを設定する

86.　手順 60. ～ 86. を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ CENTER-B

「ネットワーク情報」-「接続先情報」

- 接続先名　→ IPsecbyB

「接続先情報」-「IPsec/IKE 接続」

「基本情報」

- 相手側エンドポイント　→ 202.168.1.67
- 自装置識別情報　→ RMTbyB

「IKE 情報」

- 鍵　→ 12345678-B

「接続制御情報」

- あて先 IP アドレス　→ 172.16.1.253

ECMP を設定する

87.　設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

88.　「ルーティングマネージャ情報」をクリックします

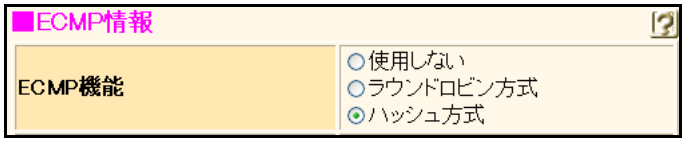
ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

89.　ルーティングマネージャ情報の設定項目の「ECMP 情報」をクリックします。

「ECMP 情報」が表示されます。

90.　以下の項目を指定します。

- ECMP 機能　→ハッシュ方式



91.　［保存］ボタンをクリックします。

92.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.28 VRRP 機能を使う

適用機種　全機種

VRRP 機能は 2 つ以上のルータがグループを形成し、1 台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ（実際にルーティングを行う装置）とバックアップルータ（マスタルータで異常を検出したときにルーティング処理を引き継ぐ装置）を決定します。

本装置には、以下の VRRP 機能があります。

- 簡易ホットスタンバイ機能
  動的に経路制御（RIP など）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能
  VRRP のグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、2 台のルータを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

☛ 参照　Si-R シリーズ　機能説明書「2.25 VRRP 機能」（P.107）

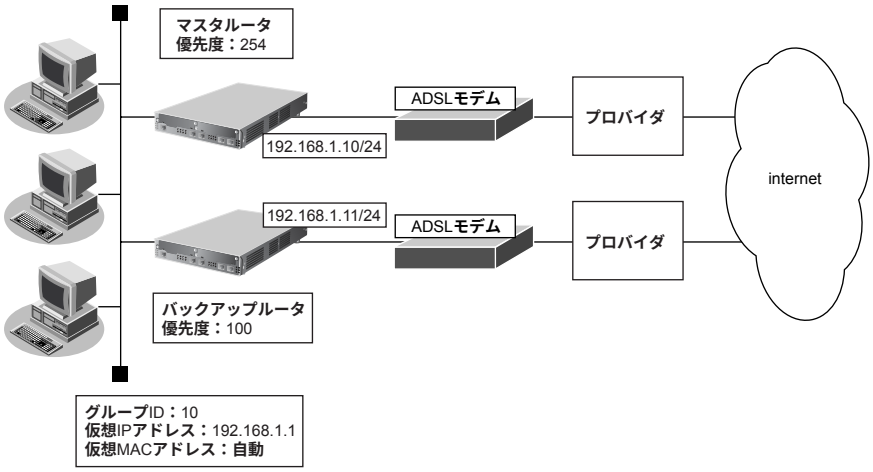
こんな事に気をつけて

- **本装置の電源の投入、マスタルータでの動的定義変更、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。プリエンプトモードが on の場合は自動で切り戻りますが、プリエンプトモードが off の場合は、操作メニューの「VRRP 手動切り戻し」で切り戻しを行う必要があります。**
- **優先度の値が大きい方が優先的にマスタルータとなります。**
- **LAN に接続される装置はデフォルトルートとして仮想 IP アドレスを設定してください。**
- **ルータに設定される IP アドレスと仮想 IP アドレスを同じにした場合、その IP アドレスで装置にアクセスすることはできなくなることがありますので、異なる IP アドレスを設定することをお勧めします。なお、ルータに設定される IP アドレスと仮想 IP アドレスを同じにする場合は、必ず、そのルータの優先度を優先度固定（最優先）に設定してください（優先度として優先度固定（最優先）を設定した場合、仮想 IP アドレスは設定できません）。**
- **優先度に“優先度固定（最優先）”を定義した場合は、プリエンプトモードの on/off にかかわらず、プリエンプトモードが on のときと同様に動作します。**
- **VRRP 機能では、VRRP-AD メッセージに以下のパケットを使用します。IP フィルタ設定時には、このパケットを遮断しないように設定する必要があります。**
  あて先 IP アドレス　：224.0.0.18
  プロトコル番号　：112
- **トリガ機能を使用する場合は VRRP グループの優先度に“優先度固定（最優先）”を指定しないでください。**

2.28.1　簡易ホットスタンバイ機能を使う

適用機種　全機種

本装置では、2 台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現できます。2 台のルータを PPPoE でインターネットに接続して、ホットスタンバイを構成する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータは WAN 側経路をノードダウントリガによって監視する

[マスタルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス/ネットマスク　：192.168.1.10/24
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- ノードダウントリガの監視 IP アドレス　：202.168.2.1（プロバイダ側の DNS サーバアドレスなど）

[バックアップルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス/ネットマスク　：192.168.1.11/24
- ユーザ認証 ID　：userid2
- ユーザ認証パスワード　：userpass2

上記の設定条件に従って設定を行う場合の設定例を示します。

マスタルータを設定する

1.　「1.6 インターネットへ PPPoE で接続する」（P.67）を参考に、PPPoE での接続を設定します。

2.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

3.　「LAN 情報」で LAN1 の［修正］ボタンをクリックします。

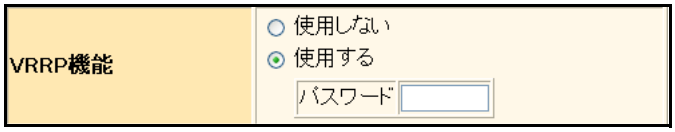
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

4.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- VRRP 機能　→使用する



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

6.　［保存］ボタンをクリックします。

7.　共通情報の設定項目の「VRRP グループ情報」をクリックします。

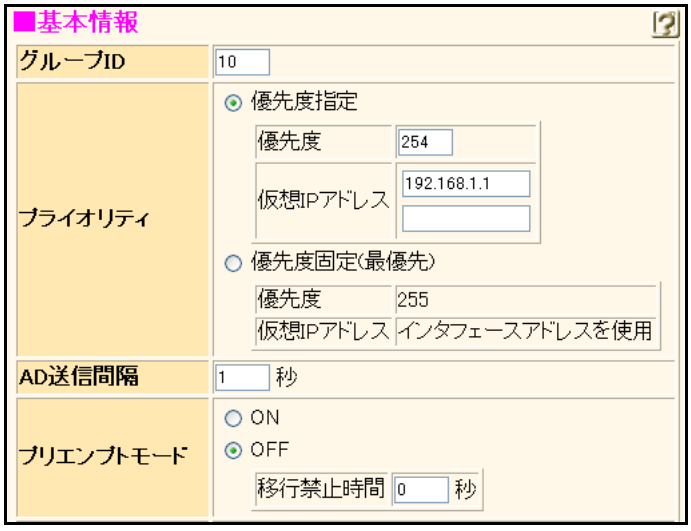
「VRRP グループ情報」が表示されます。

8.　「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ OFF



10.　［保存］ボタンをクリックします。

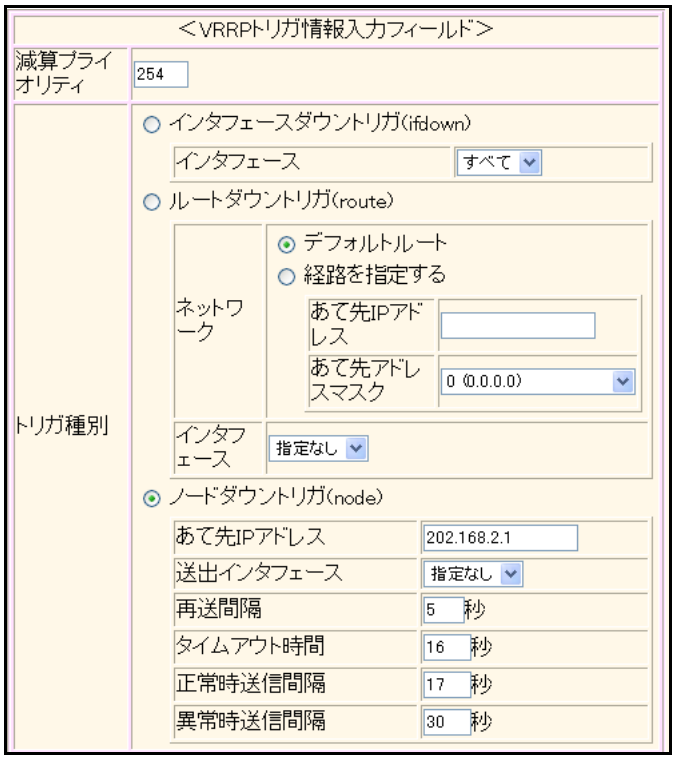
11.　VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

12.　以下の項目を指定します。

- 減算プライオリティ　→254
- トリガ種別　→ノードダウントリガ（node）

  あて先 IP アドレス　→202.168.2.1
  送出インタフェース　→指定なし
  再送間隔　→5
  タイムアウト時間　→16
  正常時送信間隔　→17
  異常時送信間隔　→30



13.　［追加］ボタンをクリックします。

14.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

LAN1 情報を設定する

「LAN1 情報」-「共通情報」

「基本情報」

- VRRP 機能　→使用する

「VRRP グループ 0 情報」

「基本情報」

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 100
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ OFF

手順 12. の設定例で、インタフェースダウントリガを使用して WAN 側（PPPoE）インタフェース状態を監視する場合は、マスタルータ側に以下の設定を追加します。

LAN1 情報を設定する

「LAN1 情報」-「共通情報」

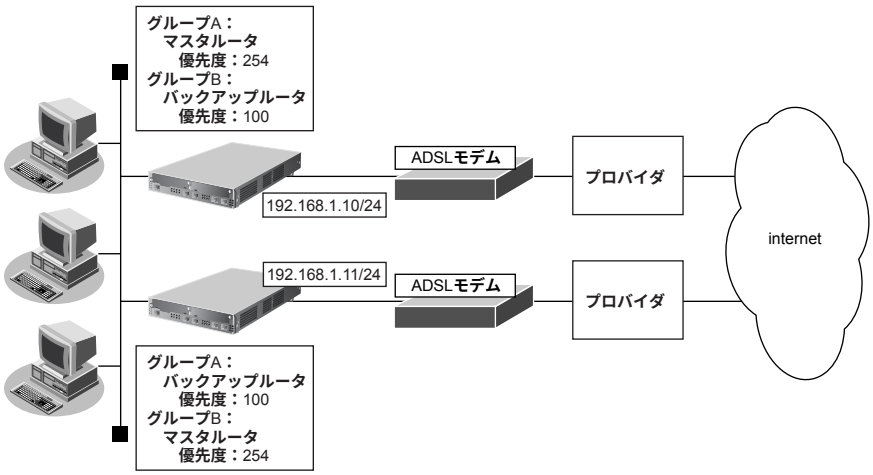
「VRRP グループ 0 情報」-「VRRP トリガ情報」

- VRRP 機能　→使用する
- 減算プライオリティ　→ 254
- トリガ種別　→インタフェースダウントリガ（ifdown）
  インタフェース　→ rmt0

2.28.2　クラスタリング機能を使う

適用機種　全機種

本装置では、2 台のルータに複数のグループ ID を設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。2 台のルータを PPPoE でインターネットに接続する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータは PPPoE 側のインタフェースをインタフェースダウントリガにより監視する

[グループ A]

- グループ ID　：10
- 仮想 IP アドレス　：192.168.1.1

[グループ B]

- グループ ID　：11
- 仮想 IP アドレス　：192.168.1.2

[マスタルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス/ネットマスク　：192.168.1.10/24
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass

[バックアップルータ]

- PPPoE で使用する LAN ポート　：LAN0 ポート
- 本装置の IP アドレス/ネットマスク　：192.168.1.11/24
- ユーザ認証 ID　：userid2
- ユーザ認証パスワード　：userpass2

こんな事に気をつけて

クラスタリング機能を有効に利用するには、PC からのトラフィック量に応じて、PC 側で設定するデフォルトルートの定義を適切に分散する必要があります。

上記の設定条件に従って設定を行う場合の設定例を示します。

ここでは、インターネットへ PPPoE で接続されていることを前提とします。

☛ 参照 「1.6 インターネットへ PPPoE で接続する」（P.67）

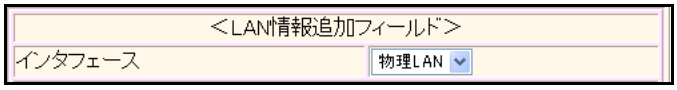
マスタルータを設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→物理 LAN



3.　［追加］ボタンをクリックします。

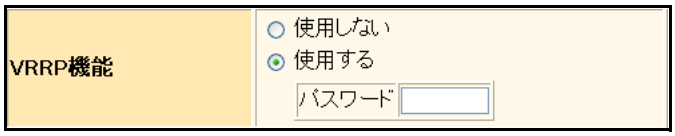
「LAN1 情報（物理 LAN）」ページが表示されます。

4.　「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

5.　以下の項目を指定します。

- VRRP 機能　→使用する



Si-R180、180B では、LAN バックアップ機能をサポートしていないため、“優先使用ポート”の項目はありません。また、“ポート番号”の表示内容が異なります。

6.　［保存］ボタンをクリックします。

7.　共通情報の設定項目の「VRRP グループ情報」をクリックします。

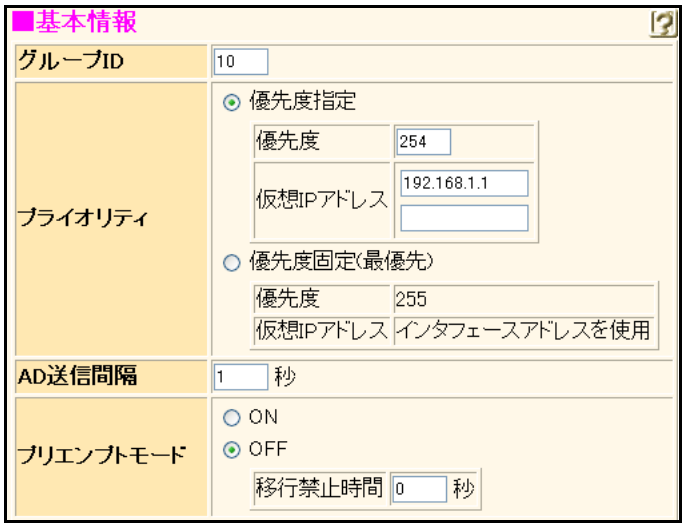
「VRRP グループ情報」が表示されます。

8.　「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ OFF



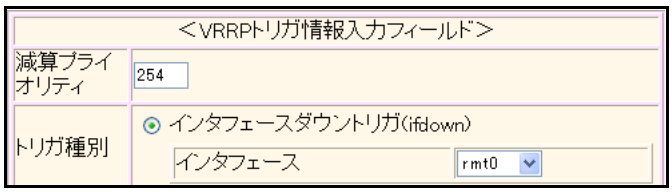
10.　［保存］ボタンをクリックします。

11.　VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

12.　以下の項目を指定します。

- 減算プライオリティ　→ 254
- トリガ種別　→インタフェースダウントリガ（ifdown）
  インタフェース　→ rmt0



13.　［追加］ボタンをクリックします。

14.　画面上部の「LAN1 情報（物理 LAN）」をクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

15.　共通情報の設定項目の「VRRP グループ情報」をクリックします。

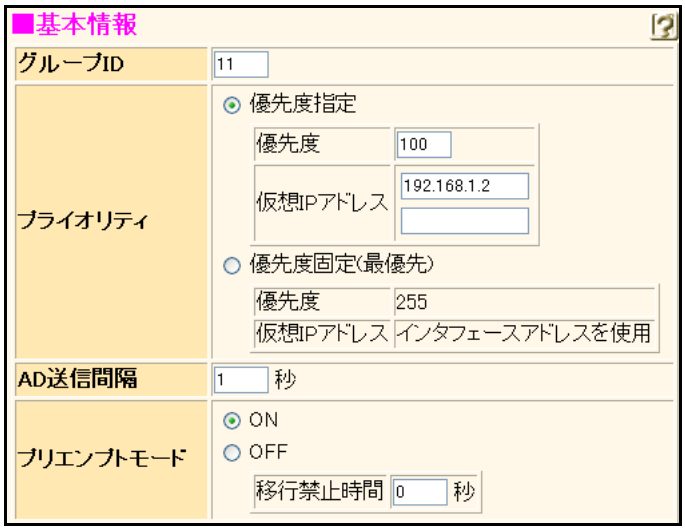
「VRRP グループ情報」が表示されます。

16.　「VRRP グループ情報」でグループ番号が 1 の［修正］ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

17.　以下の項目を指定します。

- グループID　→11
- プライオリティ　→優先度指定
  優先度　→100
  仮想IPアドレス　→192.168.1.2
- プリエンプトモード　→ON



18.　［保存］ボタンをクリックします。

19.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

LAN1 情報を設定する

「LAN1 情報」-「共通情報」

「基本情報」

- VRRP 機能　→使用する

「VRRP グループ 0 情報」

「基本情報」

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 100
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ ON

「VRRP グループ 1 情報」

「基本情報」

- グループ ID　→ 11
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 192.168.1.2
- プリエンプトモード　→ OFF

「VRRP トリガ情報」

- 減算プライオリティ　→ 254
- トリガ種別　→インタフェースダウントリガ（ifdown）
  インタフェース　→ rmt0

2.29 ポリシールーティング機能を使う

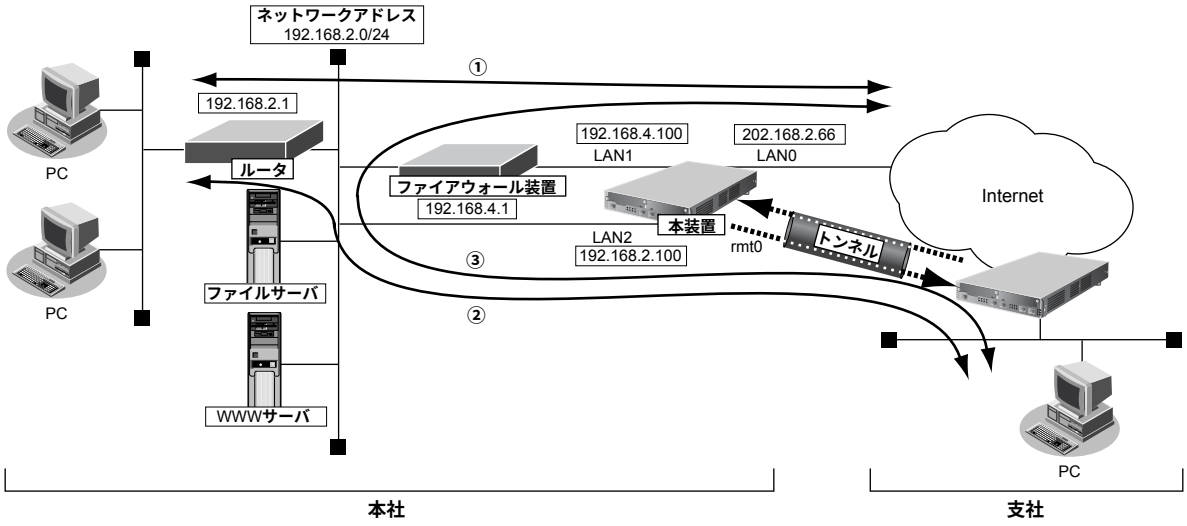
適用機種　全機種

本装置では、入力側でポリシールーティングを行う Ingress ポリシールーティングと、出力側でポリシールーティングを行うマルチルーティングの 2 つを設定することができます。

2.29.1 Ingress ポリシールーティング機能を使う

適用機種　全機種

Ingress ポリシールーティング機能とは、ルーティングによる経路情報の参照前に、入力パケットのあて先 IP アドレスだけではなく、送信元 IP アドレスやポート番号などの情報も利用して、設定した送出先へパケットを転送する機能です。この機能を利用することによって、受信インタフェースごとに経路情報に従わないパケット転送を行うことができます。ここでは、支社←→本社は本社ネットワークのファイアウォールを通さずに通信し、支社←→インターネットは本社ネットワークのファイアウォールを通して通信する場合の設定方法を説明します。



● 前提条件

- 本社←→インターネットの通信パス（①の通信パス）
  - 本社の本装置にインターネットへの通信が設定済み（lan 0）
- 支社←→本社の通信パス（②の通信パス）
  - 本社の本装置に IPsec を利用した VPN 通信が設定済み（remote 0 ap 0）

● 設定条件

- 支社←→インターネットの通信は、本社のファイアウォールを経由する（③の通信パス）
  - lan 0 インタフェースに、本装置あてパケット以外を lan1 の 192.168.4.1（ファイアウォール）に転送する Ingress ポリシールーティングを設定する
  - remote 0 インタフェースに、本装置あてパケット以外を lan2 の 192.168.2.1 に転送する Ingress ポリシールーティングを設定する

上記の設定条件に従って設定を行う場合の設定例を示します。

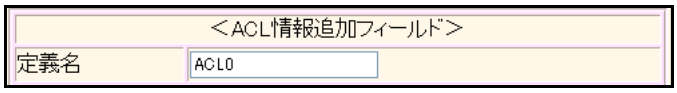
本装置あて IPv4 パケットに一致する ACL 定義を設定する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

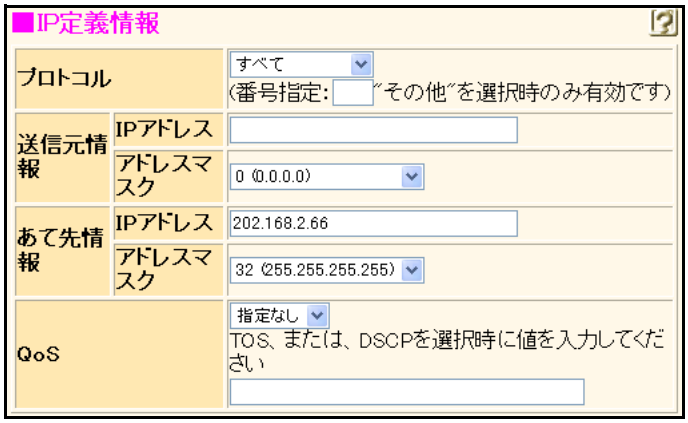
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→202.168.2.66
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



6.　［保存］ボタンをクリックします。

すべての IPv4 パケットに一致する ACL 定義を設定する

7.　手順 1.～6. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

本装置あてパケット以外を lan1 の 192.168.4.1 に転送するポリシーグループを設定する

8.　設定メニューのルータ設定で「ポリシーグループ情報」をクリックします。

「ポリシーグループ情報」ページが表示されます。

9.　［追加］ボタンをクリックします。

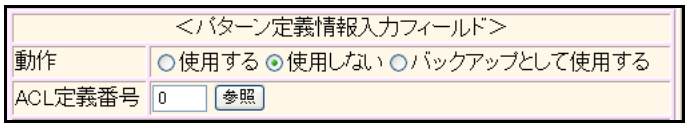
「ポリシーグループ定義情報（0）」ページが表示されます。

10.　「パターン定義情報」をクリックします。

「パターン定義情報」が表示されます。

11.　以下の項目を指定します。

- 動作　→使用しない
- ACL 定義番号　→0



12.　［追加］ボタンをクリックします。

「パターン定義情報」が表示されます。

13.　手順 11. ～ 12. を参考に、以下の項目を指定します。

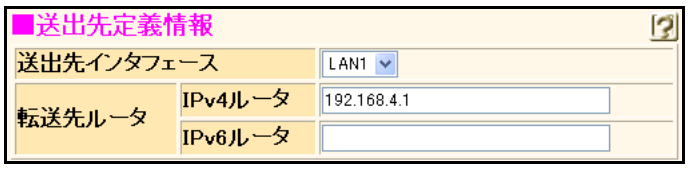
- 動作　→使用する
- ACL 定義番号　→1

14.　「送出先定義情報」をクリックします。

「送出先定義情報」が表示されます。

15.　以下の項目を指定します。

- 送出インタフェース　→LAN1
- 転送先ルータ
  IPv4 ルータ　→192.168.4.1
  IPv6 ルータ　→指定しない



16.　［保存］ボタンをクリックします。

本装置あてパケット以外を lan2 の 192.168.2.1 に転送するポリシーグループを設定する

17.　手順 8. ～ 16. を参考に、以下の項目を指定します。

「ポリシーグループ情報」
「ポリシーグループ定義情報（1）」-「パターン定義情報」
優先順位 0

- 動作　→使用しない
- ACL 定義番号　→0

優先順位 1

- 動作　→使用する
- ACL 定義番号　→1

「ポリシーグループ定義情報（1）」-「送出先定義情報」

- 送出インタフェース　→LAN2
- 転送先ルータ
  IPv4 ルータ　→192.168.2.1
  IPv6 ルータ　→指定しない

lan 0 インタフェースに Ingress ポリシールーティングを設定する

18.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

19.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

20.　「IP 関連」をクリックします。

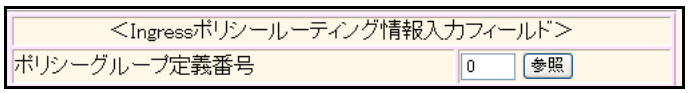
IP 関連の設定項目と「IP アドレス情報」が表示されます。

21.　IP 関連の設定項目の「Ingress ポリシールーティング情報」をクリックします。

「Ingress ポリシールーティング情報」が表示されます。

22.　以下の項目を指定します。

- ポリシーグループ定義番号　→0



23.　［追加］ボタンをクリックします。

「Ingress ポリシールーティング情報」が表示されます。

remote 0 インタフェースに Ingress ポリシールーティングを設定する

24.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

25.　VPN 接続をしているネットワーク情報（vpn-shiA）の［修正］ボタンをクリックします。

「ネットワーク情報（vpn-shiA)」ページが表示されます。

26.　「IP 関連」をクリックします。

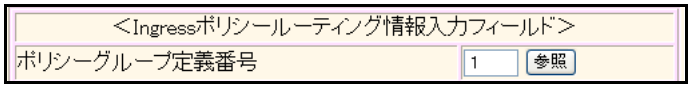
IP 関連の設定項目と「IP アドレス情報」が表示されます。

27.　IP 関連の設定項目の「Ingress ポリシールーティング情報」をクリックします。

「Ingress ポリシールーティング情報」が表示されます。

28.　以下の項目を指定します。

- ポリシーグループ定義番号　→1



29.　［追加］ボタンをクリックします。

「Ingress ポリシールーティング情報」が表示されます。

30.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

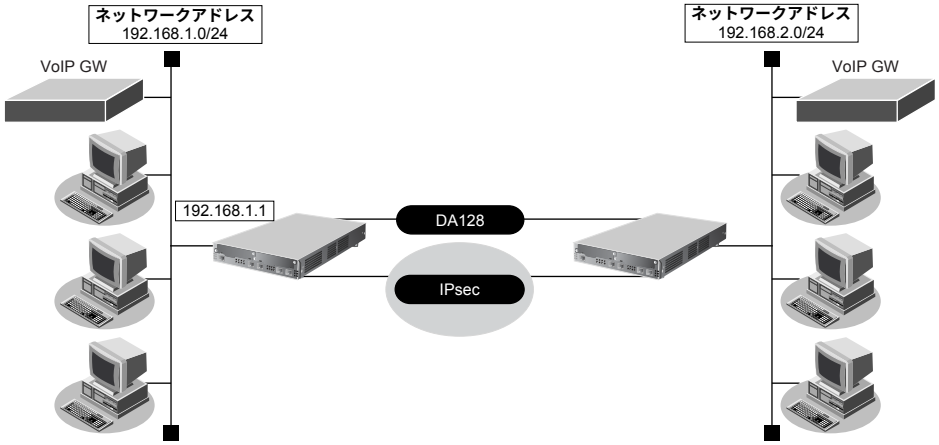
こんな事に気をつけて

Ingress ポリシールーティング機能は、ポリシーに一致した場合、ブロードキャストパケットやマルチキャストパケット、本装置あてパケットも転送します。

2.29.2　マルチルーティング機能を使う

適用機種　全機種

マルチルーティング機能を使用すると、同じあて先ネットワークへの送信データを、別の通信パスを利用して送信することができます。



● 設定条件

- IPsec を利用した VPN 通信が設定済み（remote 0 ap 0）

参照　「1.14.1 NAT を併用しない固定 IP アドレスでの VPN（自動鍵交換）」（P.145）、
「1.14.2 NAT と併用した固定 IP アドレスでの VPN（自動鍵交換）」（P.156）

- 新規に音声データ用の専用線（BRI:128Kbps）を追加する
- 通常、音声データ（TOS 値：a0）は専用線を利用する
- 通常、その他のデータは IP-VPN を利用する
- 専用線（音声用）がダウンした場合は、音声データも IP-VPN を使用する
- IP-VPN（データ用）がダウンした場合は、その他のデータも専用線を使用する

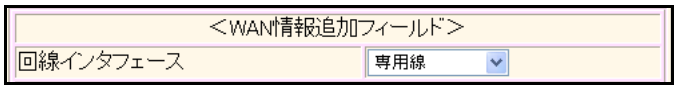
上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→専用線



3.　［追加］ボタンをクリックします。

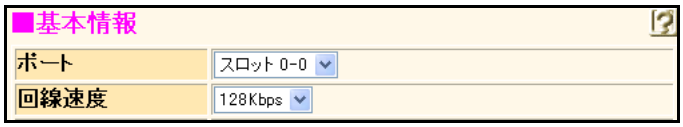
「WAN0 情報（専用線）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 回線速度　→ 128Kbps



Si-R220B、220C では、ポートは固定です。

6.　［保存］ボタンをクリックします。

7.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

8.　「ネットワーク情報」でマルチルーティングを設定するネットワーク名の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　「接続先情報」で IP-VPN を使用している接続先名の［修正］ボタンをクリックします。

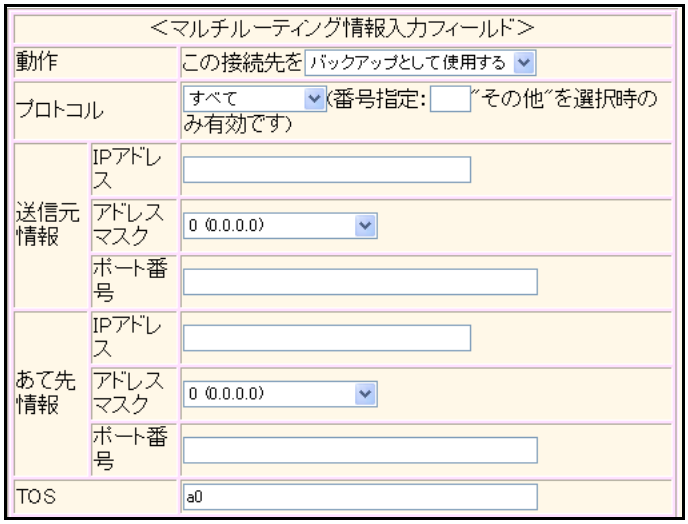
IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

11.　IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。

「マルチルーティング情報」が表示されます。

12.　以下の項目を指定します。

- 動作　→バックアップとして使用する
- TOS　→a0



13.　［追加］ボタンをクリックします。

14.　手順 12. ～ 13. を参考に、以下の項目を指定します。

- 動作　→使用する

15.　画面上部の「ネットワーク情報」をクリックします。

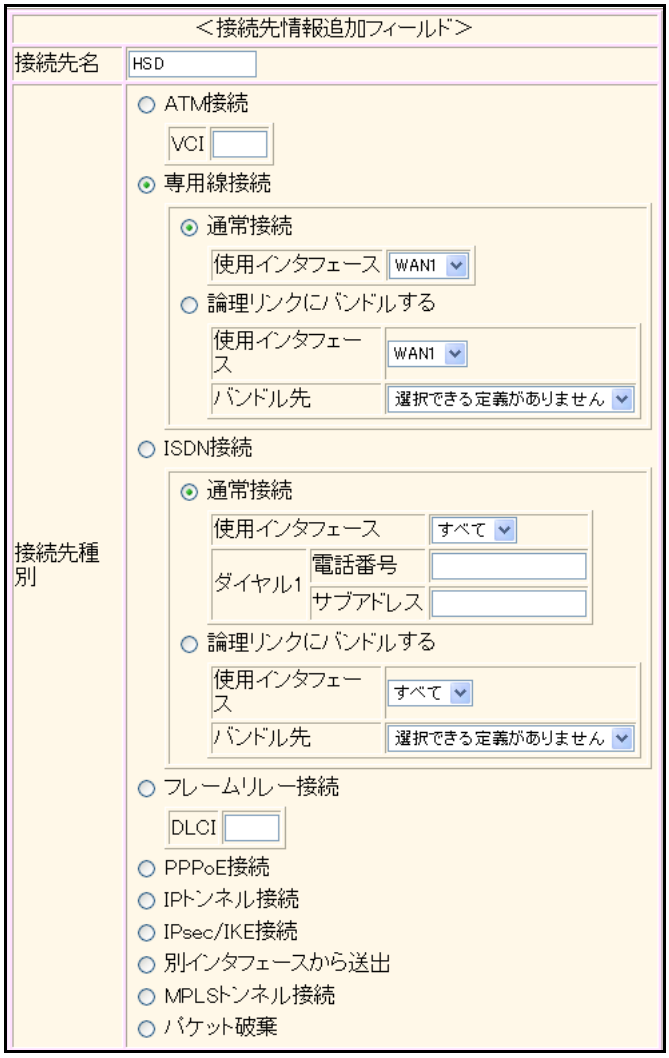
「ネットワーク情報」が表示されます。

16.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

17.　以下の項目を指定します。

- 接続先名　→HSD
- 接続先種別　→専用線接続



機種により、接続先種別の表示が上記の画面とは異なります。

18.　［追加］ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

19.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

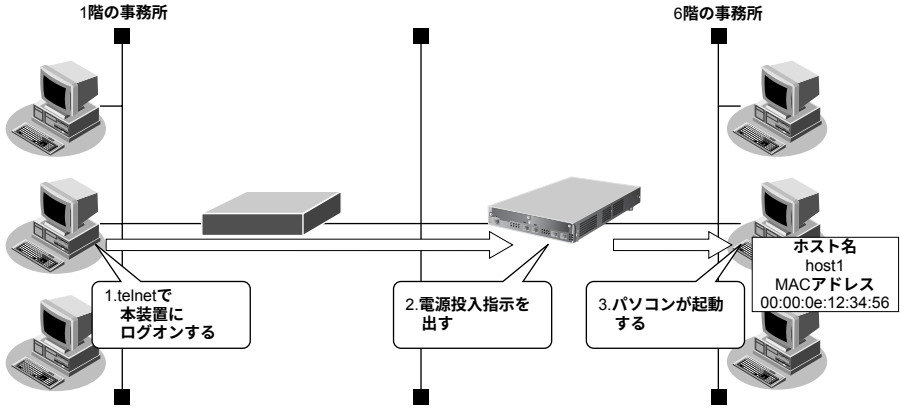
2.30 遠隔地のパソコンを起動させる（リモートパワーオン機能）

適用機種　全機種

リモートパワーオン機能は、本装置につながっている離れた所にあるパソコンを、WWW ブラウザから Wakeup on LAN 機能を使用して起動させることができます。

本機能は、WWW ブラウザで本装置のトップページが表示できる環境で利用できます。

ここでは、1 階の事務所のパソコンから 6 階の事務所のパソコンを起動する場合の設定方法を説明します。



● 設定条件

[本社側]

- 起動するパソコンのホスト名　：host1
- 起動するパソコンの MAC アドレス　：00:00:0e:12:34:56

ヒント

◆ Wakeup on LAN 機能とは？

AMD 社が開発したネットワーク上の電源 OFF 状態のパソコンを遠隔操作で起動する機能です。起動は Magic Packet と呼ばれるパケットを送付して行います。なお、Wakeup on LAN 機能はパソコンを起動するだけで電源 OFF は行いません。

電源 OFF する場合は、別途、電源制御用ソフトウェアが必要になります。

こんな事に気をつけて

- **本機能は、Wakeup on LAN に対応したパソコンだけで利用できます。Wakeup on LAN 対応機種については、パソコンのメーカーにお問い合わせください。**
- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

補足 ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。

2.30.1　リモートパワーオン情報を設定する

適用機種　全機種

1.　設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

2.　未設定の欄の［修正］ボタンをクリックします。

3.　以下の項目を指定します。

- ホスト名　→host1
- MAC アドレス　→00:00:0e:12:34:56
- リモート電源制御　→対象

補足
- ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。
- ホスト名は必須の設定項目ではありませんが、実際にリモートパワーオンを実行する場合にホスト情報一覧から目標とするパソコンを選択するのに有効な情報になります。

4.　［保存］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.30.2　リモートパワーオン機能を使う

適用機種　全機種

1.　パソコン上の WWW ブラウザで、起動させるパソコンがつながっている本装置のトップページを表示します。

2.　操作メニューで「リモートパワーオン」をクリックします。

「リモートパワーオン」ページが表示されます。

3.　起動させるパソコンの［オン］ボタンをクリックします。

本装置が、該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。

補足　パソコンが Magic Packet を受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種や OS によって異なります）。

2.31 スケジュール機能を使う

適用機種　全機種

本装置のスケジュール機能には、以下のとおりです。

- スケジュール予約
  特定の動作とそれを行う時間をスケジュール予約情報として登録できます。スケジュール予約情報を登録しておくと、特定時間帯のデータの発着信を制限したり、定期的に課金情報をクリアしたりする作業を、本装置が自動的に行います。スケジュール予約情報は、最大 16 件まで登録できます。
- 電話番号変更予約（Si-R220B、220C、370、570）
  指定した日時に構成定義情報の電話番号を一括して変更することができます。電話番号変更予約情報は、最大 4 件まで登録できます。電話番号は、予約情報 1 件に対して 4 つまで登録することができます。
- 構成定義情報切り替え予約
  本装置は、内部に 2 つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

☛ 参照　Si-R シリーズ　Web ユーザーズガイド「1.5 時刻を設定する」（P.14）

2.31.1　スケジュールを予約する

適用機種　全機種

発信抑止を予約する

ここでは、毎日午後 11 時から午前 8 時までの発信を抑止する場合の設定方法を説明します。

● 設定条件

- 動作　：発信抑止
- 日／曜日　：毎日
- 開始時刻　：23:00
- 終了時刻　：08:00

上記の設定条件に従ってスケジュールを予約する場合の設定例を示します。

1.　設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

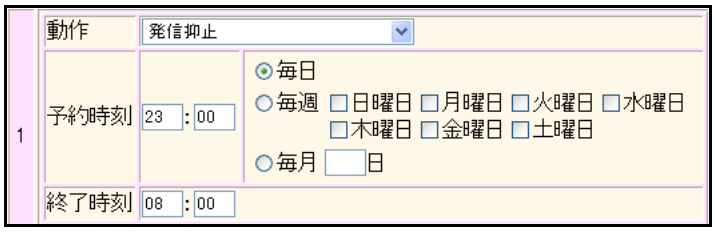
2.　「月間／週間予約情報」をクリックします。

「月間／週間予約情報」が表示されます。

3.　「月間／週間予約情報」で未設定の欄の［修正］ボタンをクリックします。

4.　以下の項目を指定します。

- 動作　→発信抑止
- 予約時刻　→23：00
  →毎日
- 終了時刻　→08:00



こんな事に気をつけて

回線接続中に、発信抑止または着信抑止が実行されても、回線は切断されません。

5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモートパワーオンを予約する

ここでは、毎朝8時に特定のパソコンを起動する場合を例に説明します。

1.　設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

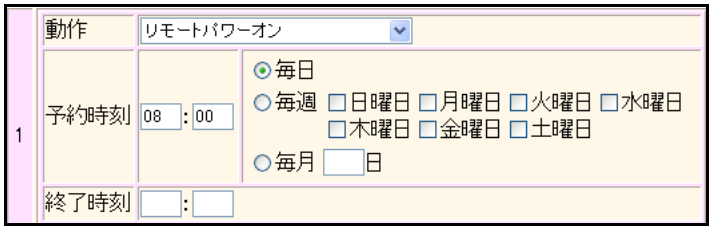
2.　「月間／週間予約情報」をクリックします。

「月間／週間予約情報」が表示されます。

3.　未設定の欄の［修正］ボタンをクリックします。

4.　以下の項目を指定します。

- 動作　→リモートパワーオン
- 予約時刻　→08:00
  →毎日



Si-R180、180B、260B では、表示内容が上記の画面とは異なります。

こんな事に気をつけて

リモートパワーオン機能を利用するには、あらかじめ利用するパソコンを「ホストデータベース情報」－「リモート電源制御」を「対象」として登録しておく必要があります。また、スケジュール機能を使ってリモートパワーオンする場合、「リモート電源制御」が「対象」となっているすべてのパソコンが起動します。

☛ 参照 「2.30 遠隔地のパソコンを起動させる（リモートパワーオン機能）」（P.835）

5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.31.2　電話番号変更を予約する

適用機種　***Si-R220B,220C,240,240B,370,570***

ここでは、2004 年 7 月 1 日午前 2 時に電話番号を「06-123-4567」から「06-6123-4567」に変更する場合の設定方法を説明します。

● 設定条件

- 実行日時　　：2004 年 7 月 1 日　2 時 00 分
- 電話番号変更前情報　　：06-123-4567
- 電話番号変更後情報　　：06-6123-4567

上記の設定条件に従って電話番号変更を予約する場合の設定例を示します。

1.　設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

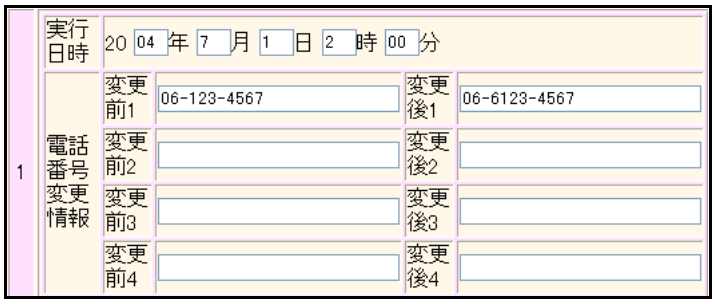
2.　「電話番号変更予約情報」をクリックします。

「電話番号変更予約情報」が表示されます。

3.　「電話番号変更予約情報」で未設定の欄の［修正］ボタンをクリックします。

4.　以下の項目を指定します。

- 実行日時　　→2004 年 7 月 1 日 2 時 00 分
- 電話番号変更情報
  変更前 1　　→06-123-4567
  変更後 1　　→06-6123-4567



5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

指定時刻になると自動的に本装置が再起動され、電話番号が更新されます。その際、データ通信中の場合は、回線が切断されます。

2.31.3　構成定義情報の切り替えを予約する

適用機種　全機種

本装置は、構成定義情報を内部に 2 つ持つことができます。

ここでは、2004 年 7 月 1 日 6 時 30 分に構成定義情報を 1 から 2 に切り替える場合の設定方法を説明します。

● 設定条件

- 実行日時　　：2004 年 7 月 1 日　6 時 30 分
- 構成定義情報切り替え　　：構成定義情報 1 →構成定義情報 2

上記の設定条件に従って構成定義情報を切り替える場合の設定例を示します。

1.　設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

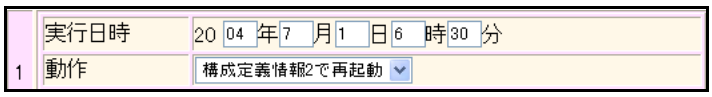
2.　「構成定義切り替え予約情報」をクリックします。

「構成定義切り替え予約情報」が表示されます。

3.　「構成定義切り替え予約情報」で未設定の欄の［修正］ボタンをクリックします。

4.　以下の項目を指定します。

- 実行日時　　→2004 年 7 月 1 日 6 時 30 分
- 動作　　→構成定義情報 2 で再起動



5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.32 通信料金を節約する（課金制御機能）

適用機種　*Si-R220B,220C,240,240B,370,570*

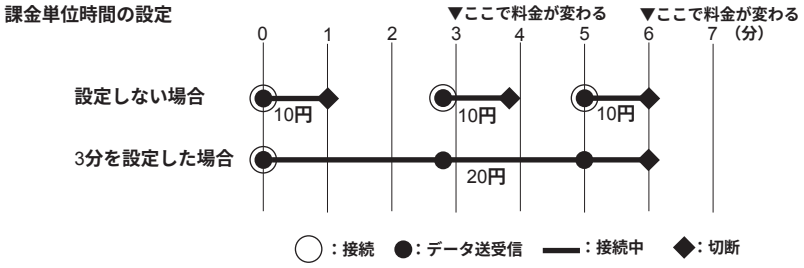
本装置は通信料金を節約するための機能をサポートしています。この機能は、通信料金のむだ、使い過ぎを防ぐことができます。以下に、各機能について説明します。

● 課金単位時間

ISDN 回線やプロバイダの多くは、一定時間単位で料金を算定する従量課金制度を採用して料金を決めています。通信料金が 3 分 10 円で計算される場合、3 分の中で何度も切断／接続を繰り返すと、料金額はその回数× 10 円になります。

そこで課金単位時間（通信料金が計算されるときの単位時間）を設定し、無通信監視タイマ（初期値：60 秒）と連動することで、単位時間内は回線を切断させないようにします。無通信監視タイマとは、設定した時間を超えてアクセスがなければ自動的に切断するという機能です。

課金単位時間に 3 分間を指定した場合、以下のようになります。



● 課金制御機能（発信抑止／強制切断）

データ通信に費やした通信時間や通信料金が一定の値を超えた場合、接続を禁止したり、ログにアラームを出したりする課金制御機能（発信抑止）もあります。また、Si-R240、240B のデータ通信カード接続では、通信時間や送受信パケット数の累計が一定の値を超えた場合、接続中の回線を切断し、以降の手動および自動発信を禁止する課金制御機能（強制切断）もあります。無意識のうちに通信料金を使いすぎるのを防ぐことができます。

こんな事に気をつけて

- **設定前に本装置の内部時刻を正しくセットしてください。**
- **課金制御機能（発信抑止）は、指定された料金を超えた場合に発信を制御する機能であり、運用中の回線を切断する機能ではありません。回線の接続中に指定された料金を超えても、回線を接続したままだと料金がかかり続けます。その結果、通信料金が指定した金額を超えてしまうのでご注意ください。**
- **モデムでは、回線の切断に時間がかかるため、課金単位を超えて切断される場合があります。**
- **通信料金による課金制御機能（発信抑止）は、ISDN 接続の場合のみ有効です。**

2.32.1　課金単位時間を設定する

適用機種　***Si-R220B,220C,240,240B,370,570***

ここでは、相手情報として remote0、接続先情報として ap0 がすでに登録済みであることを前提とします。

● 設定条件

- 無通信監視タイマ　：60 秒
- 課金単位時間
  昼間（08:00 ～ 19:00）　：180 秒
  夜間（19:00 ～ 23:00）　：180 秒
  深夜・早朝（23:00 ～ 08:00）　：240 秒

上記の設定条件に従って課金単位時間を設定する場合の設定例を示します。

1.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　「ネットワーク情報」でネットワーク名が「rmt0」の［修正］ボタンをクリックします。

「ネットワーク情報（rmt0）」が表示されます。

4.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

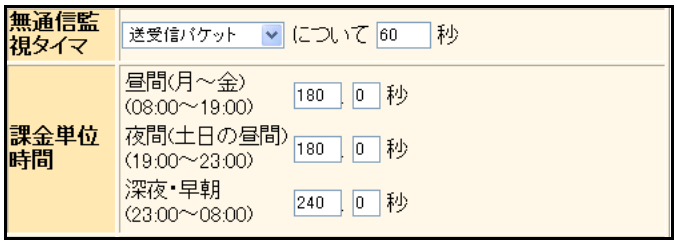
5.　「接続先情報」で接続先名が「ap0」の［修正］ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

6.　ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

- 無通信監視タイマ　→送受信パケットについて 60 秒
- 課金単位時間
  昼間　→ 180
  夜間　→ 180
  深夜・早朝　→ 240



7.　［保存］ボタンをクリックします。

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.32.2　課金制御機能（発信抑止）を設定する

適用機種　***Si-R220B,220C,370,570***

ここでは、接続累計時間が 50 時間、または通信料金の合計が 10,000 円になると接続要求を抑止する場合の設定方法を説明します。

● 設定条件

- 通信時間累計の上限時間　：50 時間
- 通信料金の上限金額　：10,000 円

上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　回線インタフェースが ISDN の［修正］ボタンをクリックします。

「WAN 情報（ISDN）」ページが表示されます。

3.　「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

4.　以下の項目を指定します。

- 通信時間による発信抑止　→する
  上限時間　→50 時間
- 課金金額による発信抑止　→する
  上限金額　→10000

5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足　現在の課金情報は、表示メニューで「課金情報」をクリックすると表示されます。
課金情報をクリアすることで、再度、発信ができるようになります。課金情報をクリアするには、表示メニューの「課金情報」から行います。

こんな事に気をつけて

- **本書の表記で使われる通信料金とは、INS ネット 64 基本サービスの「料金情報通知」をもとに、本装置のソフトウェアが算出した値です。算出される値は、お客様の契約や回線利用状況によって異なりますので、請求金額とは必ずしも一致しません。**
  たとえば以下のような場合があります。
  - INS テレホーダイサービス利用時
  - 各種料金割り引きサービス利用時
- **本装置の電源を切ると、課金情報（通信時間累計、通信料金累計など）はすべてクリアされます。**

2.33 ブリッジ／STP 機能を使う

適用機種　全機種

ここでは、ブリッジで FNA をつないで STP 機能を使用する場合、ブリッジグルーピング機能を使用する場合および IP トンネルでブリッジ通信を行う場合の設定方法を説明します。

こんな事に気をつけて

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

  参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

- **STP 機能は、グループ 0 でだけ動作します。VLAN インタフェースでは、STP を使用できません。**
- **WAN インタフェースでブリッジを利用する場合は、1 つの相手情報（remote）に対して、1 つの接続先情報（ap）となるように設計してください。**
- **本装置では、ファームウェアの更新や SNMP での監視などの目的で IPv4 の IP アドレスを使用します。そのため、IPv4 の IP アドレスを設定しないで運用することはできません。IPv6 およびブリッジだけを使用しているネットワークで運用する場合でも、どれかの LAN インタフェースに必ず IPv4 の IP アドレスを設定してください。**
- **VLAN でバインドされたインタフェースでブリッジを行うことはできません。**
- **本装置のブリッジ MAC 学習は、異なる VLAN 上で同一の MAC アドレスを学習することはできません。本装置は、唯一装置がもつ学習テーブルを各 VLAN が共有する SVL（Shared VLAN Learning）と呼ばれる方式で学習を行っています。VLAN インタフェースでブリッジを行う場合は、異なる VLAN 上に同一の MAC アドレスを持つネットワークと接続しないでください。**
- **設定を間違えてループ構成を構成し、ブロードキャストストームが発生してコンソールなどが反応しなくなった場合は、ブリッジが有効な WAN や LAN のケーブルを抜くとブロードキャストストームが収まります。ブロードキャストストームが収まったところで設定を修正してください。**

2.33.1 ブリッジで FNA をつないで STP 機能を使う

適用機種　全機種

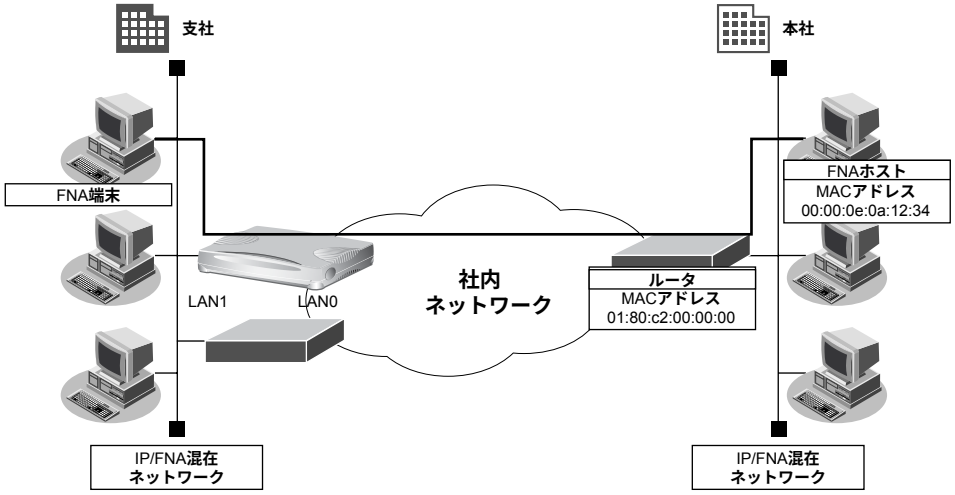
ブリッジ機能を使用すると、離れた LAN どうしを 1 つのサブネットワークとして使用することができます。また、STP 機能を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

参照 Si-R シリーズ　機能説明書「2.25 VRRP 機能」（P.107）

LAN 接続の場合

適用機種　全機種

ここでは、離れたLAN（FNA）をブリッジでつなぐ場合を例に説明します。



● 設定条件

- 本社へFNAのデータだけをブリッジする
- STP 機能を使用する

こんな事に気をつけて

ブリッジ機能によりネットワークを接続する場合は、ブリッジ通信をするパケット以外をフィルタリングする設定にしてください。フィルタリングしないと不要なトラフィックが発生するだけでなく、IP 通信できなくなる場合があります。

上記の設定条件に従って設定を行う場合の設定例を示します。

ブリッジ情報を設定する（LAN1）

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースがLAN1 の［修正］ボタンをクリックします。

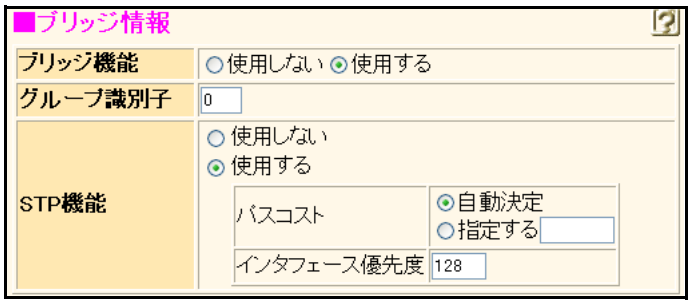
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

3.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

4.　以下の項目を指定します。

- ブリッジ機能　→使用する
- STP 機能　→使用する



5.　［保存］ボタンをクリックします。

ブリッジ情報を設定する（LAN0）

6.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

7.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

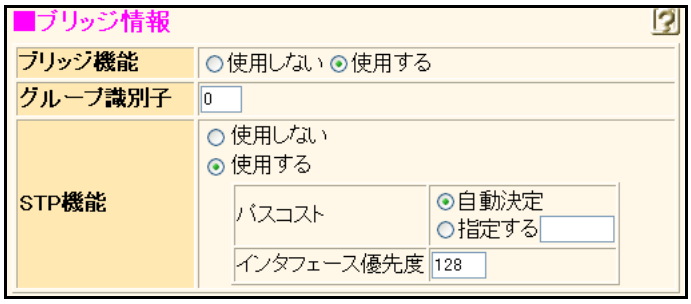
「LAN0 情報（物理 LAN）」ページが表示されます。

8.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

9.　以下の項目を指定します。

- ブリッジ機能　→使用する
- STP 機能　→使用する



10.　［保存］ボタンをクリックします。

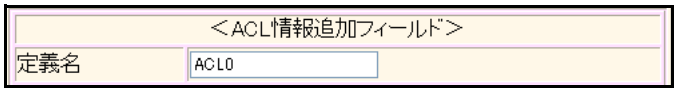
フィルタリング情報で FNA を透過させる（支社→本社）

11.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

12.　以下の項目を指定します。

- 定義名　→ACL0



13.　［追加］ボタンをクリックします。

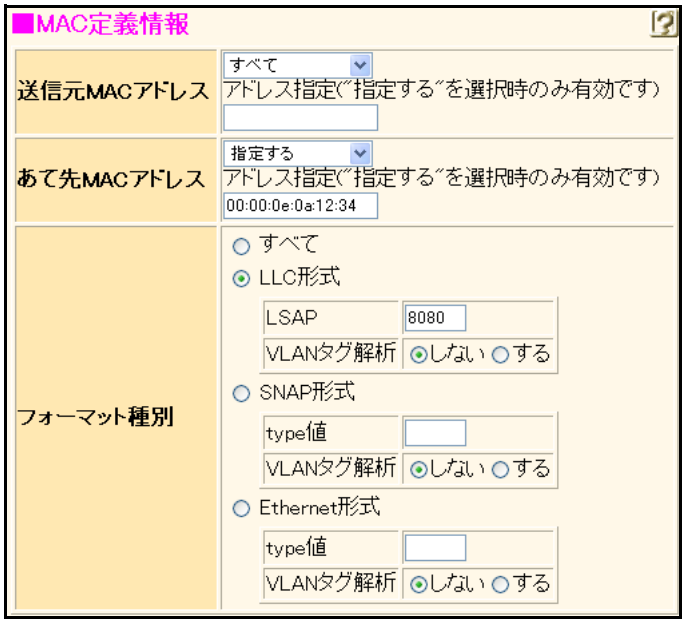
「ACL 定義情報（ACL0）」ページが表示されます。

14.　「MAC 定義情報」クリックします。

「MAC 定義情報」ページが表示されます。

15.　以下の項目を指定します。

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→指定する
  アドレス指定　→ 00:00:0e:0a:12:34
- フォーマット種別　→LLC 形式
  LSAP　→ 8080
  VLAN タグ解析　→しない



16.　［保存］ボタンをクリックします。

17.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

18.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

19.　「ブリッジ関連」をクリックします。

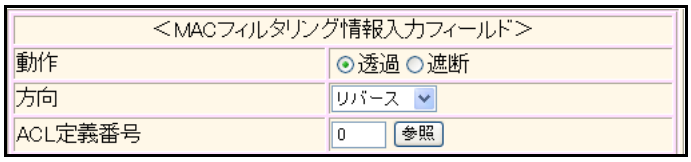
ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

20.　ブリッジ関連の設定項目の「MAC フィルタリング情報」をクリックします。

「MAC フィルタリング情報」が表示されます。

21.　以下の項目を指定します。

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→0



22.　［保存］ボタンをクリックします。

フィルタリング情報で STP を透過させる

23.　手順 11.～22. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 情報（ACL1)」-「MAC 定義情報」

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→指定する
  アドレス指定　→ 01:80:c2:00:00:00
- フォーマット種別　→LLC 形式
  LSAP　→ 4242
  VLAN タグ解析　→しない

「LAN 情報」-「ブリッジ関連」
「MAC フィルタリング情報」

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→1

残りの通信をすべて遮断する

24.　手順 11.～22. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL2

「ACL 情報（ACL2)」-「MAC 定義情報」

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→すべて
- フォーマット種別　→すべて

「LAN 情報」-「ブリッジ関連」
「MAC フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→2

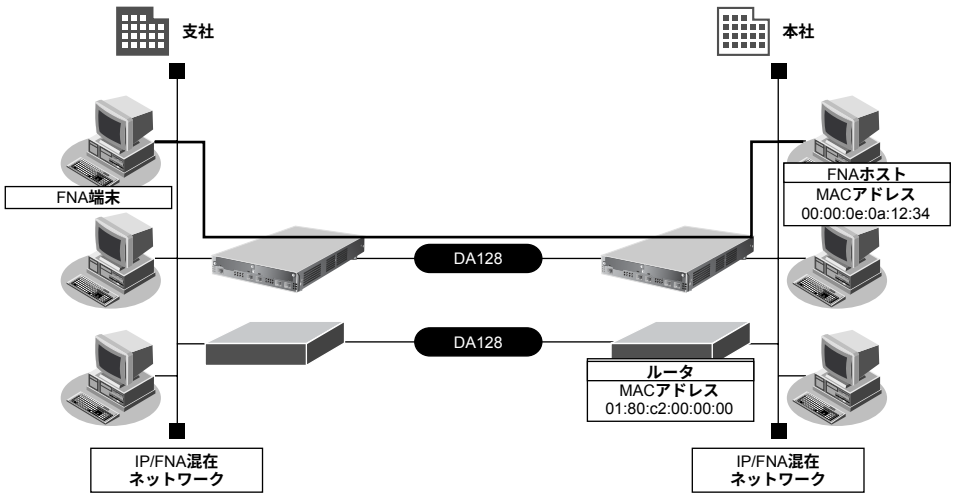
25.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

リモート接続の場合

適用機種　***Si-R220B,220C,260B,370,570***

ここでは、専用線をはさんで離れたLAN（FNA）をブリッジでつなぐ場合の設定方法を説明します。WANインタフェースの種類によって設定が異なりますので、使用するWANインタフェースに応じてWAN関連定義を行ってください。



● 設定条件

- SLOT0に実装されたBRI拡張モジュールL2または基本ボード上のISDNポート（Si-R220B、220Cの場合）で専用線（128kbps）を使用する
- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

こんな事に気をつけて

ブリッジ機能を使用すると定期的に発信するため、超過課金が発生します。ISDN回線やモデム接続でSTP機能を使用しないでください。

この例では、本社と支社がすでに専用線接続されていることを前提としています。

☛ 参照 「1.10 事業所LANを専用線で接続する」（P.103）

上記の設定条件に従って設定を行う場合の設定例を示します。

ブリッジ情報を設定する

1.　設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

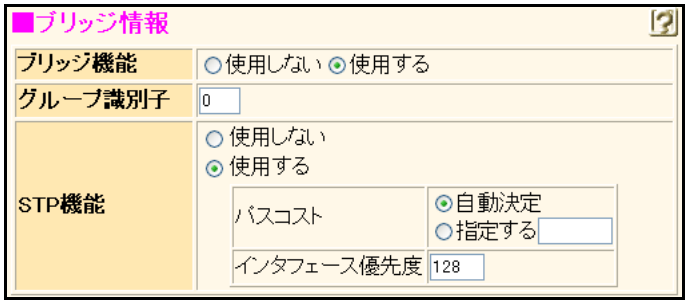
「LAN0情報（物理LAN）」ページが表示されます。

3.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

4.　以下の項目を指定します。

- ブリッジ機能　→使用する
- STP 機能　→使用する



5.　［保存］ボタンをクリックします。

6.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

7.　「ネットワーク情報」でブリッジ設定を行うネットワーク名の［修正］ボタンをクリックします。

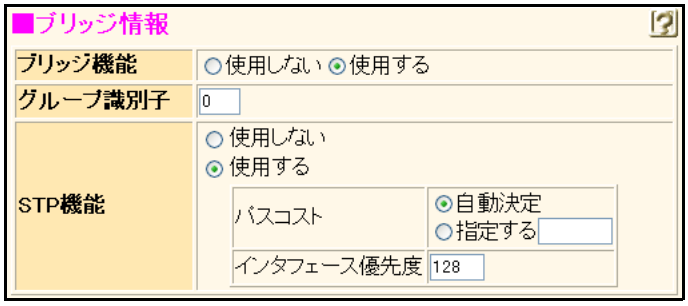
「ネットワーク情報」が表示されます。

8.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

9.　以下の項目を指定します。

- ブリッジ機能　→使用する
- STP 機能　→使用する



10.　［保存］ボタンをクリックします。

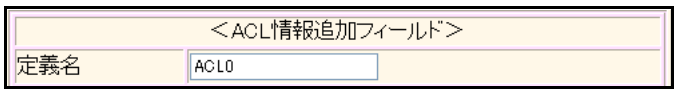
フィルタリング情報で FNA を透過させる（支社→本社）

11.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

12.　以下の項目を指定します。

- 定義名　→ACL0



13.　［追加］ボタンをクリックします。

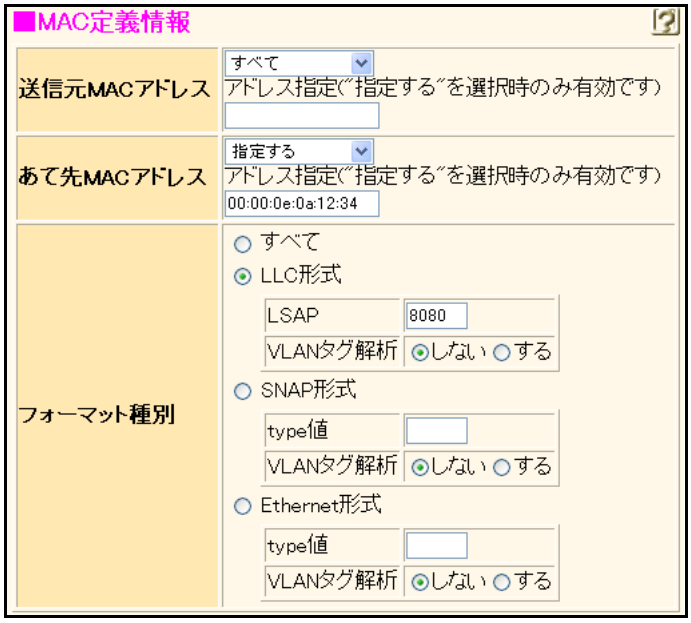
「ACL 定義情報（ACL0）」ページが表示されます。

14.　「MAC 定義情報」クリックします。

「MAC 定義情報」ページが表示されます。

15.　以下の項目を指定します。

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→指定する
  アドレス指定　→ 00:00:0e:0a:12:34
- フォーマット種別　→ LLC 形式
  LSAP　→ 8080
  VLAN タグ解析　→しない



16.　［保存］ボタンをクリックします。

17.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

18.　「ネットワーク情報」でブリッジ設定を行うネットワーク名の［修正］ボタンをクリックします。

「ネットワーク情報」が表示されます。

19.　「ブリッジ関連」をクリックします。

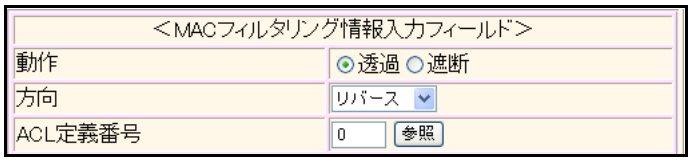
ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

20.　ブリッジ関連の設定項目の「MAC フィルタリング情報」をクリックします。

「MAC フィルタリング情報」が表示されます。

21.　以下の項目を指定します。

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→0



22.　［保存］ボタンをクリックします。

フィルタリング情報で STP を透過させる

23.　手順 11.～22. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL1

「ACL 情報（ACL1)」-「MAC 定義情報」

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→指定する
  アドレス指定　→ 01:80:c2:00:00:00
- フォーマット種別　→LLC 形式
  LSAP　→ 4242
  VLAN タグ解析　→しない

「LAN 情報」-「ブリッジ関連」

「MAC フィルタリング情報」

- 動作　→透過
- 方向　→リバース
- ACL 定義番号　→1

残りの通信をすべて遮断する

24.　手順 11.～22. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ACL2

「ACL 情報（ACL2)」-「MAC 定義情報」

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→すべて
- フォーマット種別　→すべて

「相手情報」-「ブリッジ関連」

「MAC フィルタリング情報」

- 動作　→遮断
- 方向　→入出力
- ACL 定義番号　→2

25.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.33.2　ブリッジグルーピング機能を使う

適用機種　全機種

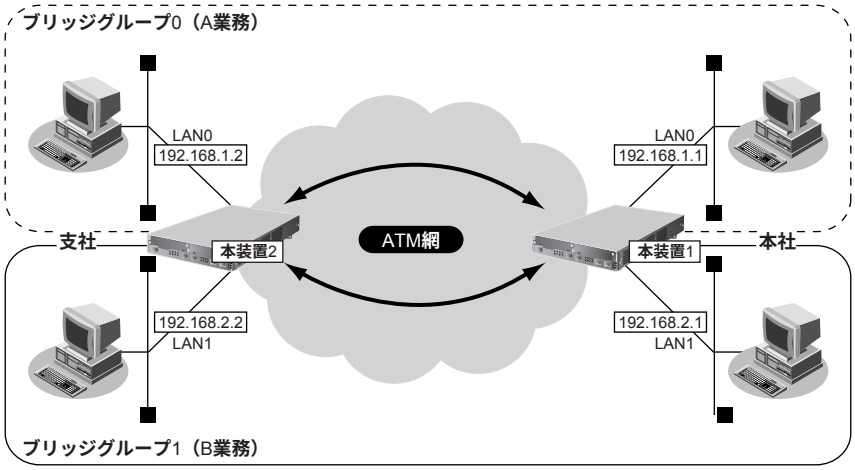
ブリッジグルーピング機能とは、各インタフェースにグループ識別子を設定し、それぞれのインタフェースにグループを割り当てることによって、ブリッジ転送が、そのグループ内に閉じた形で行われるようにする機能です。グループを分けることで、ブリッジ通信を各グループに分離することができます。

こんな事に気をつけて

- ブリッジ学習テーブル生存時間は、グループ 0 に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1 つまたは複数のリモートインタフェースと VLAN インタフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数の LAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さい LAN インタフェースでだけ以下の機能を利用できます。
  - FTP（ファームアップデートなど）
  - telnet
  - Web ブラウザによる設定
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング
- IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使用してください。
- ブリッジグループを複数定義する場合は、グループ識別子を 0 から順番に、間をあけないで設定してください。
- STP はグループ 0 でだけ動作するため、グループ 0 以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ 0 でループを構成するブリッジ構成を行う場合は、必ず STP を有効にしてください。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではない IP パケットを送受信することはできません。よって、IP をブリッジする運用形態では、IP に関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- WAN 経由で IP をブリッジし、ブリッジ転送を許す場合（転送ポリシが Loose）、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジによって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題なく WAN の先に存在するあて先ネットワークにブリッジで転送されて到達します。

ここでは、ブリッジグルーピング機能を使用して、本社と特定の支社との間で業務ごとに異なる通信を分離して実現する場合の設定方法を説明します。

本社の LAN0 と支社の LAN0 との間は A 業務関連だけを通信し、本社の LAN1 と支社の LAN1 との間は B 業務関連だけを通信します。互いの通信は IP も含めて完全に分離します。



すでに ATM 網を利用して、本社と支社の間で VPC を 2 つ接続し、以下のとおりに設定されていることを前提とします。

参照 「2.35 ATM 網を使う」（P.871）

● 前提条件

[本社、支社共通]

- ATM 網を利用して、本社と支社の間で VPC を 2 つ接続している

[本社]

- LAN0 の IPv4 アドレス　：192.168.1.1/24
- LAN1 の IPv4 アドレス　：192.168.2.1/24

[支社]

- LAN0 の IPv4 アドレス　：192.168.1.2/24
- LAN1 の IPv4 アドレス　：192.168.2.2/24

● 設定条件

[本社、支社共通]

- ブリッジグループ数　：2 グループ（A 業務用と B 業務用）
- IPv4 の転送方式　：ブリッジで転送
- 転送ポリシ　：strict（完全に IPv4 通信を分離）

本社を設定する

ブリッジグループ 0 に属するインタフェースを設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

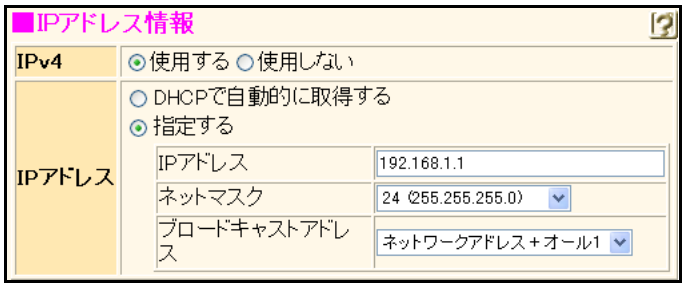
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



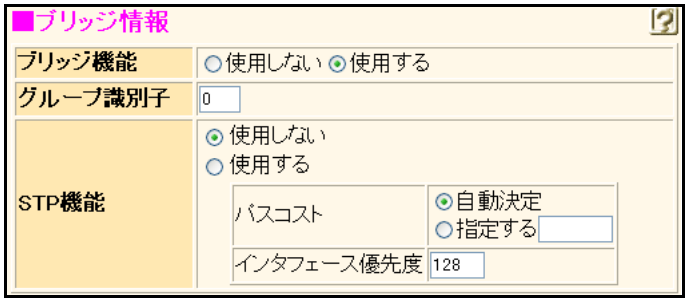
5.　［保存］ボタンをクリックします。

6.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

7.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→ 0
- STP 機能　→使用しない



8.　［保存］ボタンをクリックします。

9.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　「ネットワーク情報」でブリッジグループ 0 に属する（A 業務用 VPC）ネットワーク名の［修正］ボタンをクリックします。

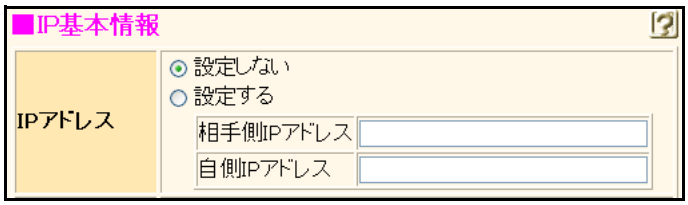
「ネットワーク情報」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

13.　以下の項目を指定します。

- IP アドレス　→設定しない



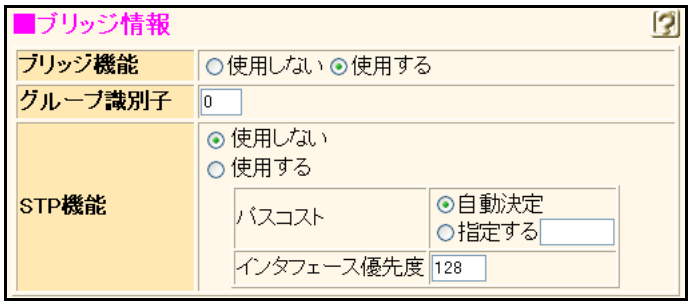
14.　［保存］ボタンをクリックします。

15.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

16.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→0
- STP 機能　→使用しない



17.　［保存］ボタンをクリックします。

ブリッジグループ 0 を設定する

18.　設定メニューのルータ設定で「ブリッジ情報」をクリックします。

「ブリッジ情報」ページが表示されます。

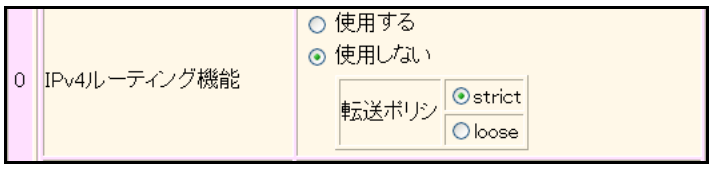
19.　「ブリッジグループ情報」をクリックします。

「ブリッジグループ情報」が表示されます。

20.　「ブリッジグループ情報」でグループ識別子が 0 の［修正］ボタンをクリックします。

21.　以下の項目を指定します。

- IPv4 ルーティング機能　→使用しない
  転送ポリシ　→ strict



22.　［保存］ボタンをクリックします。

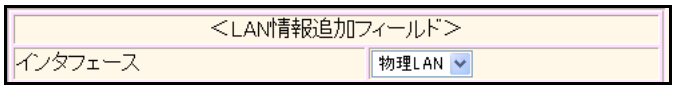
ブリッジグループ 1 に属するインタフェースを設定する

23.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

24.　以下の項目を指定します。

- インタフェース　→物理 LAN



25.　［追加］ボタンをクリックします。

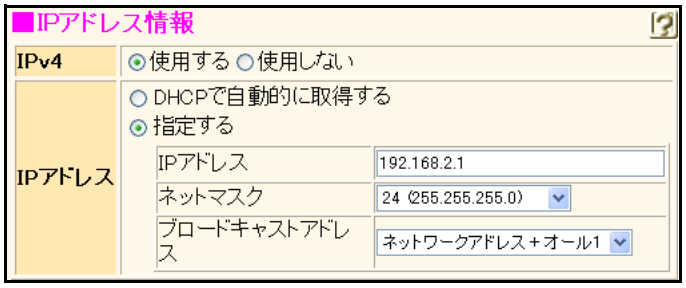
「LAN1 情報（物理 LAN）」ページが表示されます。

26.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

27.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



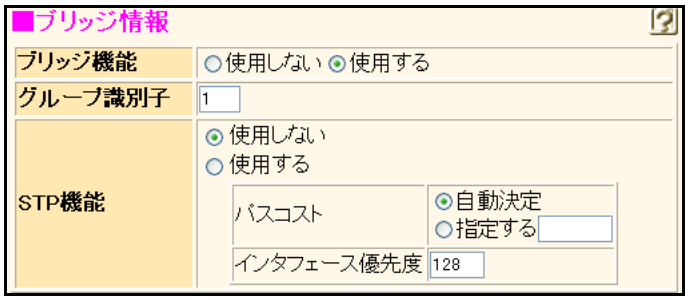
28.　［保存］ボタンをクリックします。

29.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

30.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→1
- STP 機能　→使用しない



31.　［保存］ボタンをクリックします。

32.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

33.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

34.　「ネットワーク情報」でブリッジグループ 1 に属する（B 業務用 VPC）ネットワーク名の［修正］ボタンをクリックします。

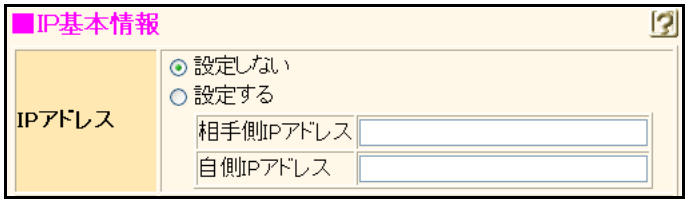
「ネットワーク情報」ページが表示されます。

35.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

36.　以下の項目を指定します。

- IP アドレス　→設定しない



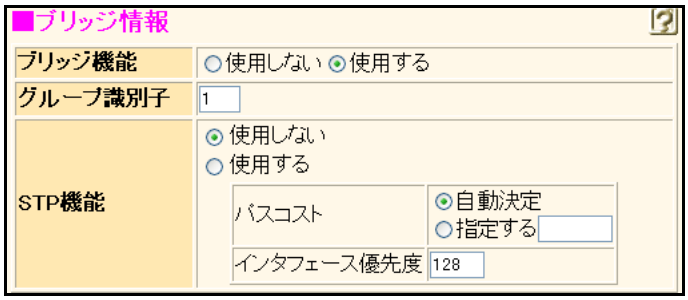
37.　［保存］ボタンをクリックします。

38.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

39.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→ 1
- STP 機能　→使用しない



40.　［保存］ボタンをクリックします。

ブリッジグループ 1 を設定する

41.　設定メニューのルータ設定で「ブリッジ情報」をクリックします。

「ブリッジ情報」ページが表示されます。

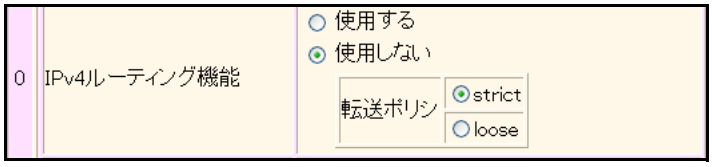
42.　「ブリッジグループ情報」をクリックします。

「ブリッジグループ情報」が表示されます。

43.　「ブリッジグループ情報」でグループ識別子が 1 の［修正］ボタンをクリックします。

44.　以下の項目を指定します。

- IPv4 ルーティング機能　→使用しない
  転送ポリシ　→ strict



45.　［保存］ボタンをクリックします。

46.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。

この例では、LAN 側の IP アドレス以外は、本社とすべて同じです。

2.33.3 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ）

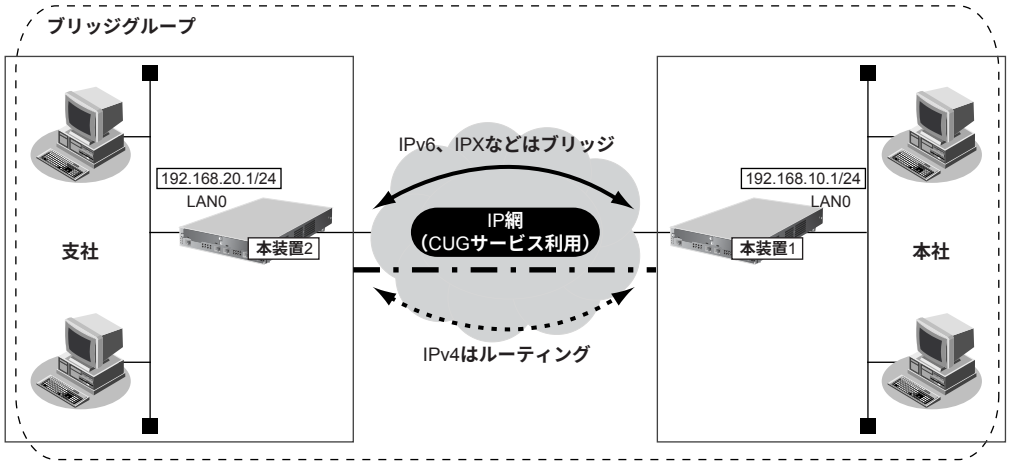
適用機種　*Si-R220B,220C,260B,370,570*

IP トンネル上でブリッジ機能を使用することにより、IP 通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

こんな事に気をつけて

- ブリッジ学習テーブル生存時間は、グループ 0 に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1 つまたは複数のリモートインタフェースと VLAN インタフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数の LAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さい LAN インタフェースでだけ以下の機能を利用できます。
  - FTP（ファームアップデートなど）
  - telnet
  - Web ブラウザによる設定
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング
- IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とルーティングが行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使用してください。
- ブリッジグループを複数定義する場合は、グループ識別子を 0 から順番に、間をあけないで設定してください。
- STP はグループ 0 でだけ動作するため、グループ 0 以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ 0 でループを構成するブリッジ構成を行う場合は、必ず STP を有効にしてください。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではない IP パケットを送受信することはできません。よって、IP をブリッジする運用形態では、IP に関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- WAN 経由で IP をブリッジし、ルーティングを許す場合（転送ポリシが Loose）、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジによって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題なく WAN の先に存在するあて先ネットワークにブリッジで転送されて到達します。
- Ethernet over IP ブリッジの接続先に対して接続先監視を行うことができません。接続先監視の設定は行わないでください。

ここでは、本社と特定の支社との間で、IP 網を経由し、IPv4 以外のフレームに対してブリッジ通信を行う場合の設定方法を説明します。



● 前提条件

- IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG（Closed Users Group）サービスを利用する

[本社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN0 ポートに設定）
  ：192.168.10.1/24
- PPPoE ユーザ認証 ID　：userid1@groupname
- PPPoE ユーザ認証パスワード　：userpass1
- PPPoE LAN ポート　：LAN1 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

[支社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN0 ポートに設定）
  ：192.168.20.1/24
- PPPoE ユーザ認証 ID　：userid2@groupname
- PPPoE ユーザ認証パスワード　：userpass2
- PPPoE LAN ポート　：LAN1 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

- 接続ネットワーク名　：honsya
- 接続先名　：honsya1
- 自側エンドポイントアドレス　：192.168.10.1
- 相手側エンドポイントアドレス　：192.168.20.1

[支社]

- 接続ネットワーク名　：shisya
- 接続先名　：shisya1

- 自側エンドポイントアドレス　：192.168.20.1
- 相手側エンドポイントアドレス　：192.168.10.1

［本社、支社共通］

- ブリッジ対象インタフェース　：LAN0 ポートと IP トンネル
- IPv4 の転送方式　：ルーティングで転送
- IPv6 の転送方式　：ブリッジで転送

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

PPPoE 接続を設定する

1.　「1.6 インターネットへ PPPoE で接続する」（P.67）を参考に、PPPoE での接続を設定します。

こんな事に気をつけて

「1.6 インターネットへ PPPoE で接続する」（P.67）の設定例と本設定例は、PPPoE で使用する拠点ネットワークの LAN が逆になっています。

IPv4 トンネルを設定する

2.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

3.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

4.　以下の項目を指定します。

- ネットワーク名　→shisya

＜ネットワーク情報追加フィールド＞	
ネットワーク名	shisya

5.　［追加］ボタンをクリックします。

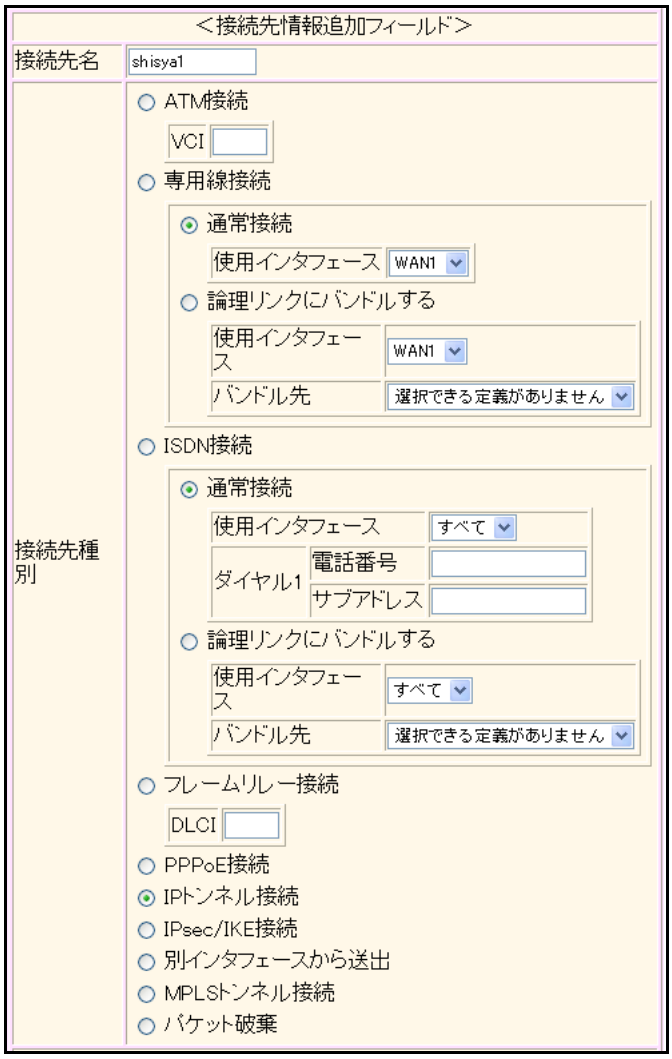
「ネットワーク情報（shisya）」ページが表示されます。

6.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

7.　以下の項目を指定します。

- 接続先名　→shisya1
- 接続先種別　→IP トンネル接続



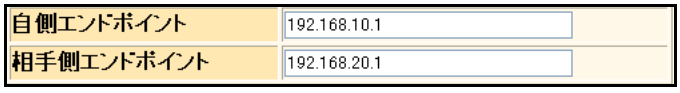
機種により、接続先種別の表示が上記の画面とは異なります。

8.　［追加］ボタンをクリックします。

IP トンネル接続の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- 自側エンドポイント　→192.168.10.1
- 相手側エンドポイント　→192.168.20.1



10.　［保存］ボタンをクリックします。

ブリッジグループ 0 に属するインタフェースを設定する

11.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

12.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

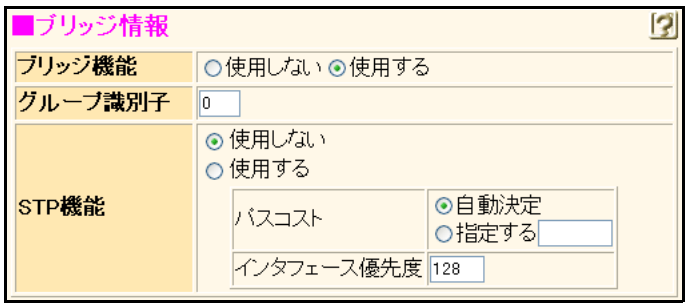
「LAN0 情報（物理 LAN）」ページが表示されます。

13.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

14.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→0
- STP 機能　→使用しない



15.　［保存］ボタンをクリックします。

16.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

17.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

18.　「ネットワーク情報」で IP トンネルを設定したネットワーク名（shisya）の［修正］ボタンをクリックします。

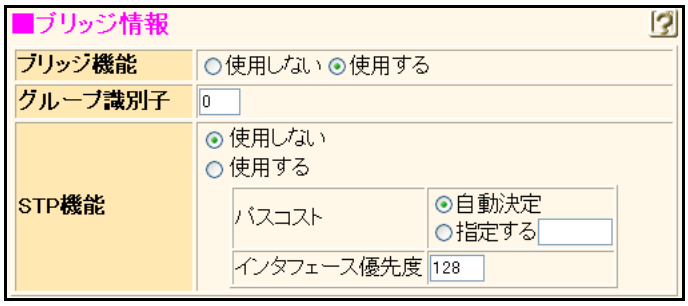
「ネットワーク情報（shisya）」ページが表示されます。

19.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

20.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→0
- STP 機能　→使用しない



21.　［保存］ボタンをクリックします。

ブリッジグループ 0 を設定する

22.　設定メニューのルータ設定で「ブリッジ情報」をクリックします。

「ブリッジ情報」ページが表示されます。

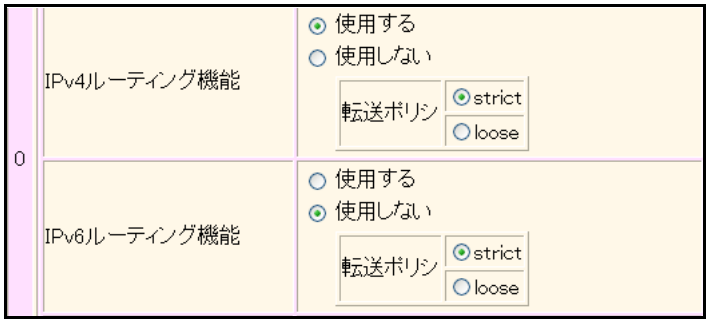
23.　「ブリッジグループ情報」をクリックします。

「ブリッジグループ情報」が表示されます。

24.　「ブリッジグループ情報」でグループ識別子が 0 の［修正］ボタンをクリックします。

25.　以下の項目を指定します。

- IPv4 ルーティング機能　→使用する
- IPv6 ルーティング機能　→使用しない
  転送ポリシ　→strict



26.　［保存］ボタンをクリックします。

27.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。

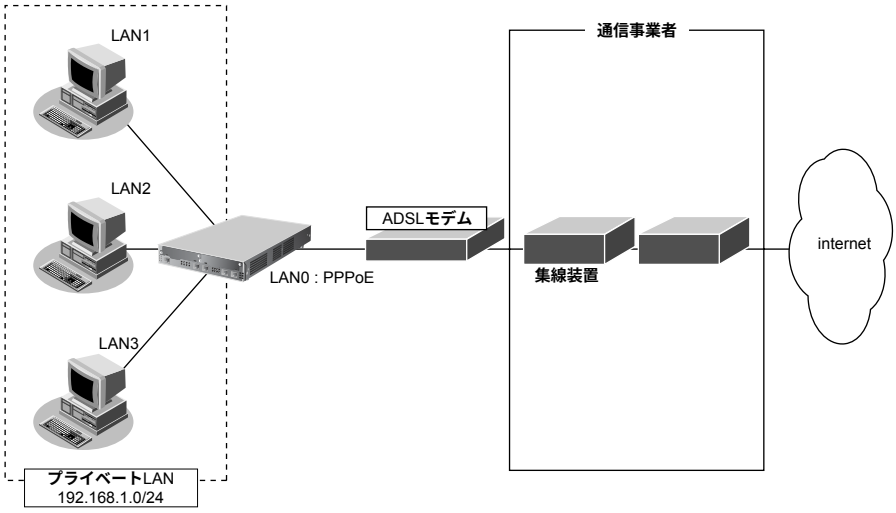
この例では、LAN 側の IP アドレス、PPPoE の接続先情報（認証情報）、IPv4 トンネルのエンドポイントアドレス以外は、本社とすべて同じです。

2.34 複数の LAN ポートをスイッチング HUB のように使う

適用機種　*Si-R220B,220C,260B,370,570*

ここでは、1 つの LAN ポートを PPPoE で使用し、残りの LAN ポートをスイッチング HUB のように設定してプライベート LAN を構築し、インターネットを利用する例を説明します。

まず、この機能を使用する前に Si-R シリーズ　機能説明書「2.26 ブリッジ機能」（P.112）を参照して、ブリッジグルーピングの機能と注意事項を理解してから設定してください。



こんな事に気をつけて

- **パソコンの LAN インタフェースと本装置の切り替えスイッチのない LAN ポートを接続する場合は、クロスケーブルを使って接続してください。**
- **IPv4 や IPv6 をブリッジする場合、IP 関連の定義は、ブリッジグループ内で定義番号がもっとも小さい LAN インタフェース（レイヤ 3 代表インタフェース）を設定してください。ブリッジグループ内では、レイヤ 3 代表インタフェースでだけ、レイヤ 3 の機能が有効になります。**
- **LAN ポートのリンク状態によって動作する機能（例：OSPF や VRRP など）は、これらの機能が定義されたレイヤ 3 代表インタフェースのリンク状態だけを監視して動作しています。レイヤ 3 代表インタェースが同期はずれを起こし、これ機能が代表インタフェースへの出力を止めた場合、同じグループ内のほかのポートからも、これの機能が出力するパケットが出なくなります。よって、リンク状態をみて動作する機能は、レイヤ 3 代表インタフェースの LAN ポートだけを使用してください。**

「1.6 インターネットへ PPPoE で接続する」（P.67）の設定が終了し、以下のとおりに設定されていることを前提とします。

☛ 参照　Si-R シリーズ　機能説明書「2.26 ブリッジ機能」（P.112）

● 前提条件

- プライベート LAN 側のネットワーク　：192.168.1.0/24
- レイヤ 3 代表インタフェース　：LAN1

● 設定条件

- LAN1、LAN2、LAN3 をグルーピングして、スイッチング HUB のように利用して、プライベート LAN 側に使用する
- IPv4 をブリッジ対象とする
- プライベート LAN 側のブリッジグループとインターネット側の間のルーティングを許可する

上記の設定条件に従って設定を行う場合の設定例を示します。

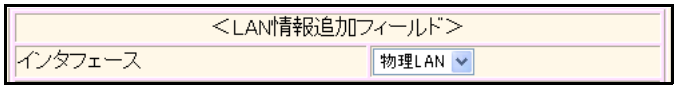
スイッチング HUB のように利用する LAN インタフェースを設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- インタフェース　→物理 LAN



3.　［追加］ボタンをクリックします。

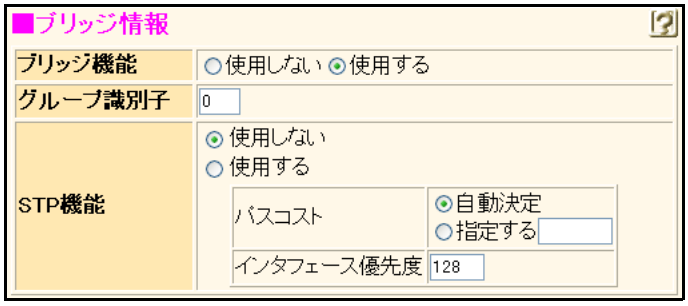
「LAN1 情報（物理 LAN）」ページが表示されます。

4.　「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

5.　以下の項目を指定します。

- ブリッジ機能　→使用する
- グループ識別子　→0
- STP 機能　→使用しない



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考にして、LAN2、LAN3 を設定します。

ブリッジグループ 0 を設定する

8.　設定メニューのルータ設定で「ブリッジ情報」をクリックします。

「ブリッジ情報」ページが表示されます。

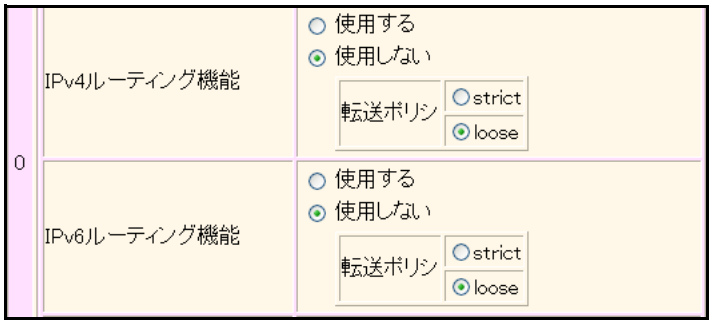
9.　「ブリッジグループ情報」をクリックします。

「ブリッジグループ情報」が表示されます。

10.　「ブリッジグループ情報」でグループ識別子が 0 の［修正］ボタンをクリックします。

11.　以下の項目を指定します。

- IPv4 ルーティング機能　→使用しない
  転送ポリシ　→ loose
- IPv6 ルーティング機能　→使用しない
  転送ポリシ　→ loose



12.　［保存］ボタンをクリックします。

13.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

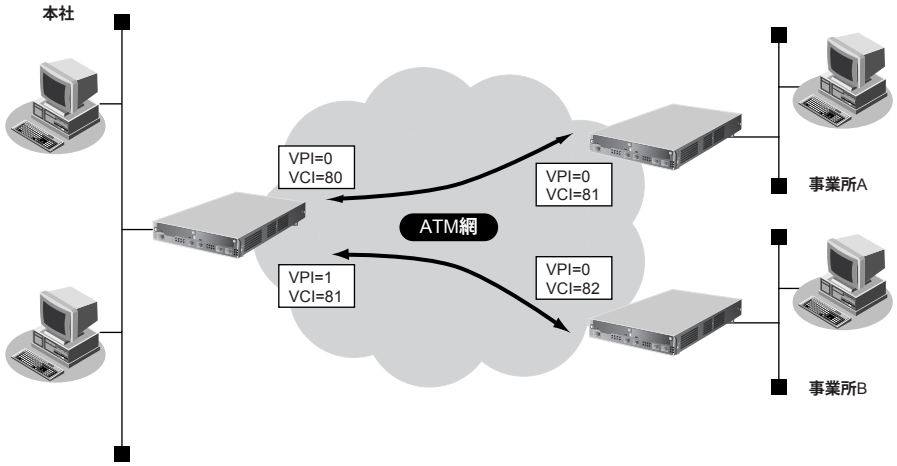
2.35 ATM網を使う

適用機種 *Si-R260B,370,570*

ここでは、ATM 網を利用して複数の事業所のネットワークを接続し、複数の VPC を使用する場合と VPC と VCC の同時シェーピングを使用する場合の設定方法を説明します。

2.35.1 事業所ごとに別の VPC を使用する

適用機種 *Si-R260B,370,570*



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：192.168.1.1/24（LAN0）
- 事業所 A 向けネットワーク名　：JigyoA
- 事業所 A 向け接続先名　：jigyo-a
- 事業所 A 向け VPI/VCI　：0/80
- 事業所 A 向け VP 速度　：6Mbps
- 事業所 B 向けネットワーク名　：JigyoB
- 事業所 B 向け接続先名　：jigyo-b
- 事業所 B 向け VPI/VCI　：1/81
- 事業所 B 向け VP 速度　：4Mbps

[事業所 A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側の IP アドレス　：192.168.101.1/24（LAN0）
- ネットワーク名　：Honsya
- 接続先名　：honsya-1
- VPI/VCI　：0/81
- VP 速度　：6Mbps

[事業所 B]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- LAN 側 IP アドレス　：192.168.102.1/24（LAN0）
- ネットワーク名　：Honsya
- 接続先名　：honsya-2
- VPI/VCI　：0/82
- VP 速度　：4Mbps

こんな事に気をつけて

使用する拡張モジュールによって、以下の点に注意して設定してください。Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M ／ ATM155M 拡張モジュール L2	• VP ／ VC 速度を設定する場合は、64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 - 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 • VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 • VP シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が VP 速度を超えないようにように設定してください。 • VC シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が 25Mbps を超えないようにように設定してください。
ATM25M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - 64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 25Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。

拡張モジュール	注意点
ATM155M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - VP 速度は、200Kbps ～ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 - VC 速度は、64Kbps ～ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 50Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VPC 内の VC 速度の最高速度は 50Mbps になります。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。 `atm <slot> send clock recovery`

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

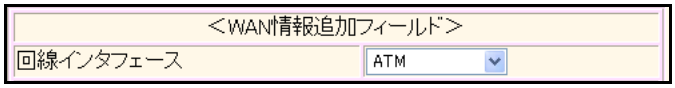
VPC の情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→ ATM



3.　［追加］ボタンをクリックします。

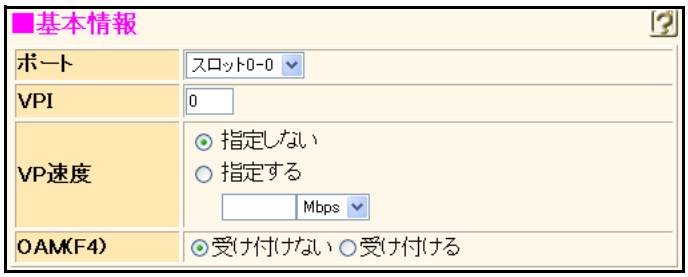
「WAN0 情報（ATM）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、以下の項目を指定します。

- 回線インタフェース　→ ATM

「WAN1 情報（ATM）」－「基本情報」

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない

本装置の IP アドレスを設定する

8.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

9.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

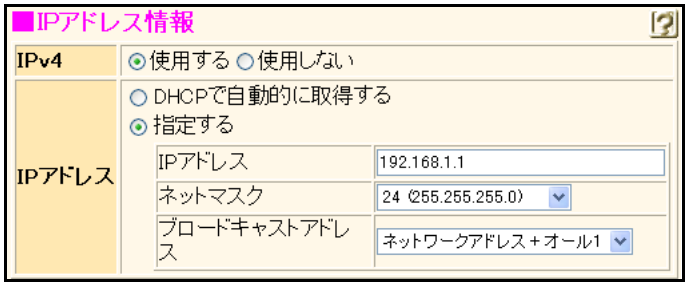
「LAN0 情報（物理 LAN）」ページが表示されます。

10.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

11.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



12.　［保存］ボタンをクリックします。

事業所 A 向けの情報を設定する

13.　設定メニューのルータ設定で「相手情報」をクリックします。

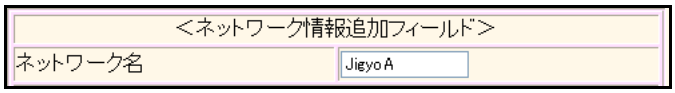
「相手情報」ページが表示されます。

14.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

15.　以下の項目を指定します。

- ネットワーク名　→JigyoA



16.　［追加］ボタンをクリックします。

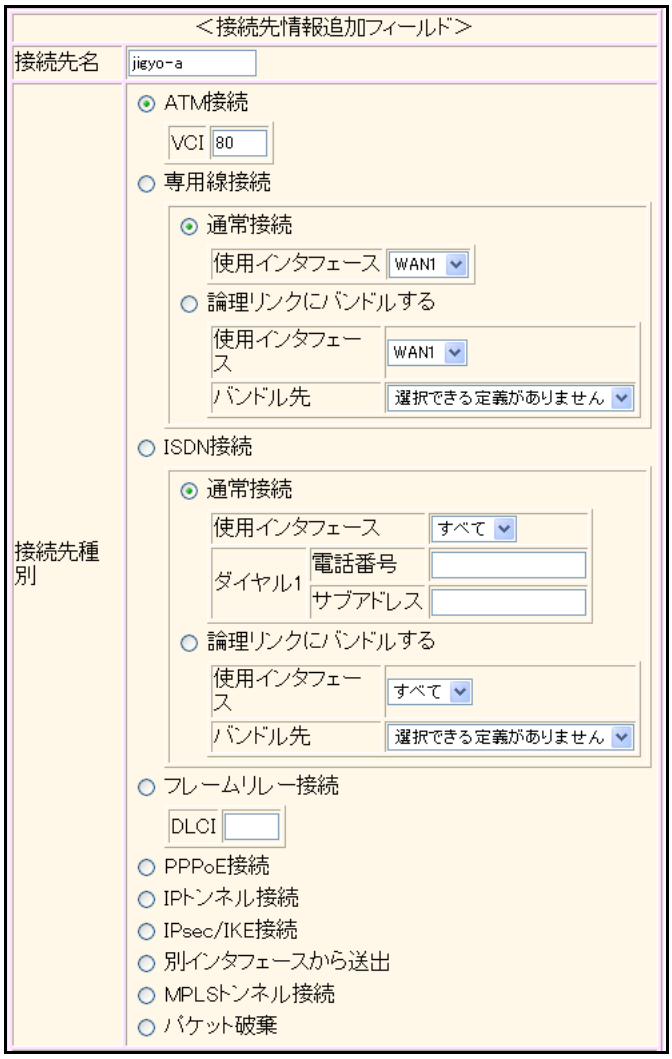
「ネットワーク情報（JigyoA）」ページが表示されます。

17.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

18.　以下の項目を指定します。

- 接続先名　→jigyo-a
- 接続先種別　→ATM 接続
  VCI　→80



Si-R260B では、接続先種別の表示が上記の画面とは異なります。

19.　［追加］ボタンをクリックします。

ATM 接続の設定項目と「基本情報」が表示されます。

20.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- VCI　→80
- VC 速度　→6Mbps
- サービスタイプ　→CBR
- OAM（F5）　→受け付けない

21.　［保存］ボタンをクリックします。

22.　画面上部の「ネットワーク情報（JigyoA）をクリックします。

「ネットワーク情報（JigyoA）」が表示されます。

23.　「IP 関連」をクリックします。

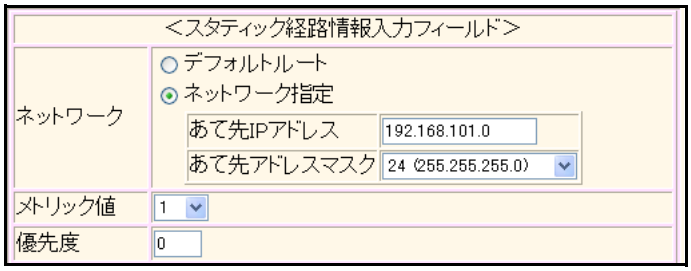
IP 関連の設定項目と「IP 基本情報」が表示されます。

24.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

25.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.101.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0



26.　［追加］ボタンをクリックします。

事業所 B 向けの情報を設定する

27.　手順 13. ～ 26. を参考に、以下の項目を指定します。

「ネットワーク情報」

- ネットワーク名　→ JigyoB

「接続先情報」

- 接続先名　→ jigyo-b
- 接続先種別　→ ATM 接続
  VCI　→ 81

「基本情報」

- 使用インタフェース　→ WAN1
- VCI　→ 81
- VC 速度　→ 4Mbps
- サービスタイプ　→ CBR
- OAM（F5）　→受け付けない

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.102.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0

28.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

事業所 A を設定する

「本社を設定する」を参考に、事業所 A を設定します。

VPC の情報を設定する

「WAN0 情報」

- 回線インタフェース　→ ATM

「基本情報」

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない

本装置の IP アドレスを設定する

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.101.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

本社向けの情報を設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ Honsya

「ネットワーク情報」-「接続先情報」

- 接続先名　→ honsya-1
- 接続先種別　→ ATM 接続
  VCI　→ 81

「接続先情報」-「ATM 接続」

「基本情報」

- 使用インタフェース　→ WAN0
- VCI　→ 81
- VC 速度　→ 6Mbps
- サービスタイプ　→ CBR
- OAM（F5）　→受け付けない

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→デフォルトルート
- メトリック値　→ 1
- 優先度　→ 0

事業所 B を設定する

「本社を設定する」を参考に、事業所 B を設定します。

VPC の情報を設定する

「WAN0 情報」

- 回線インタフェース　→ ATM

「基本情報」

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定しない
- OAM（F4）　→受け付けない

本装置の IP アドレスを設定する

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.102.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

本社向けの情報を設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ Honsya

「ネットワーク情報」-「接続先情報」

- 接続先名　→ honsya-1
- 接続先種別　→ ATM 接続
  VCI　→ 82

「接続先情報」-「ATM 接続」

「基本情報」

- 使用インタフェース　→ WAN0
- VCI　→ 82
- VC 速度　→ 4Mbps
- サービスタイプ　→ CBR
- OAM（F5）　→受け付けない

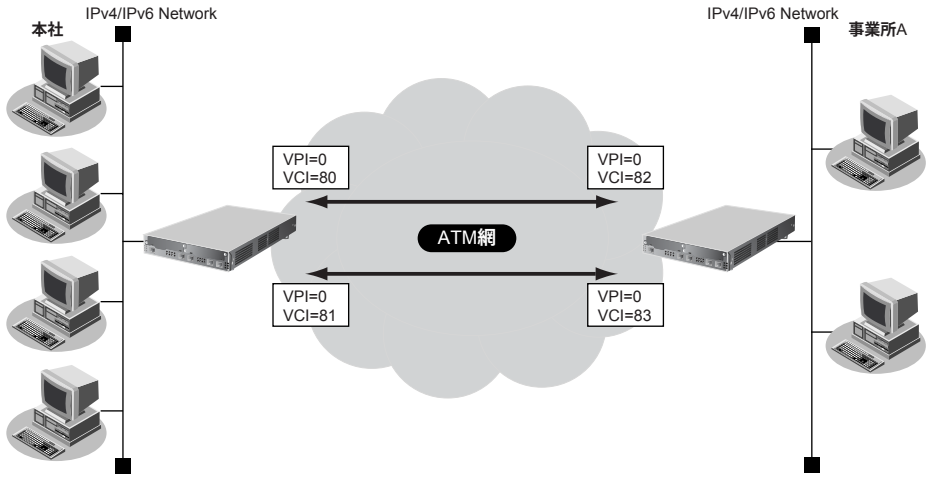
「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→デフォルトルート
- メトリック値　→ 1
- 優先度　→ 0

2.35.2　VPC と VCC の同時シェーピングを使用する

適用機種　***Si-R260B,370,570***



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- IPv4 アドレス　：192.168.1.1/24（LAN0）
- IPv4 通信向けネットワーク名　：JigyoA1
- IPv4 通信向け接続先名　：jigyoa-1
- IPv4 通信向け VPI/VCI　：0/80
- IPv6 アドレス　：2001:db8:1111:1000::/64（LAN0）
- IPv6 通信向けネットワーク名　：JigyoA2
- IPv6 通信向け接続先名　：jigyoa-2
- IPv6 通信向け VPI/VCI　：0/81
- VP 速度　：8Mbps
- IPv4 通信向けサービスタイプ　：VBR（VC 速度：6Mbps、平均速度：5Mbps）
- IPv6 通信向けサービスタイプ　：UBR+（VC 速度：5Mbps、最低速度：3Mbps）

[事業所 A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース（Si-R260B の場合）で ATM 網を使用する
- IPv4 アドレス　：192.168.2.1/24（LAN0）
- IPv4 通信向けネットワーク名　：Honsya1
- IPv4 通信向け接続先名　：honsya-1
- IPv4 通信向け VPI/VCI　：0/82
- IPv6 アドレス　：2001:db8:1111:1001::/64（LAN0）
- IPv6 通信向けネットワーク名　：Honsya2
- IPv6 通信向け接続先名　：honsya-2
- IPv6 通信向け VPI/VCI　：0/83
- VP 速度　：8Mbps

- IPv4 通信向けサービスタイプ　：VBR（VC 速度：6Mbps、平均速度：5Mbps）
- IPv6 通信向けサービスタイプ　：UBR+（VC 速度：5Mbps、最低速度：3Mbps）

こんな事に気をつけて

使用する拡張モジュールによって、以下の点に注意して設定してください。Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M ／ ATM155M 拡張モジュール L2	• VP ／ VC 速度を設定する場合は、64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 - 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 • VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 • VP シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が VP 速度を超えないようにように設定してください。 • VC シェーピング時は、VC 速度（CBR、GFR+）、平均速度（SCR）および最低速度（UBR+）の総和が 25Mbps を超えないようにように設定してください。
ATM25M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - 64Kbps ～ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 25Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。

拡張モジュール	注意点
ATM155M 拡張モジュール H1	• VP ／ VC 速度を設定する場合は、以下の設定範囲で設定してください。 - VP 速度は、200Kbps ～ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 - VC 速度は、64Kbps ～ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。 • VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 - VP 速度の総和を 50Mbps 以下に設定してください。 - 1-VPC での VP ／ VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP ／ VC シェーピング時は VBR を設定してください。 - サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。 - サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。 - VPC 内の VC 速度の最高速度は 50Mbps になります。 - VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 • DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。 `atm <slot> send clock recovery`

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

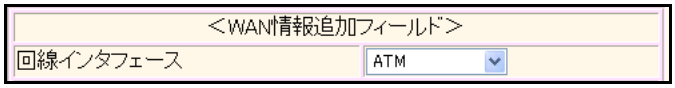
VPC の情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→ATM



3.　［追加］ボタンをクリックします。

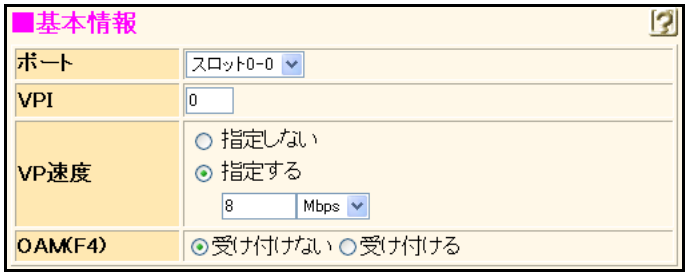
「WAN0 情報（ATM）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→指定する
  →8Mbps
- OAM（F4）　→受け付けない



6.　［保存］ボタンをクリックします。

LAN 情報を設定する

7.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

8.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

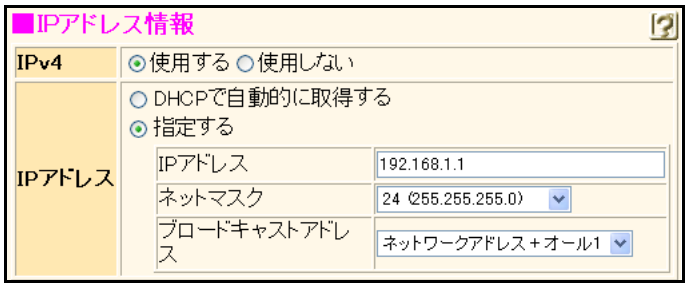
「LAN0 情報（物理 LAN）」ページが表示されます。

9.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

10.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



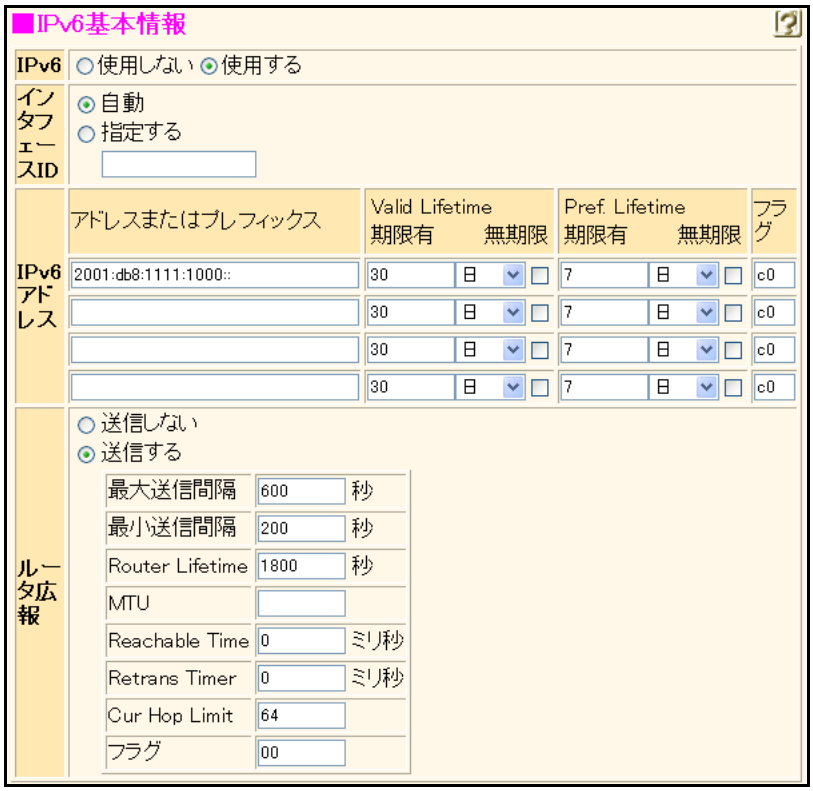
11.　［保存］ボタンをクリックします。

12.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

13.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→2001:db8:1111:1000::
  Valid Lifetime　→30 日
  Pref. Lifetime　→7 日
  フラグ　→c0
- ルータ広報　→送信する



14.　［保存］ボタンをクリックします。

IPv4 の相手情報を設定する

15.　設定メニューのルータ設定で「相手情報」をクリックします。

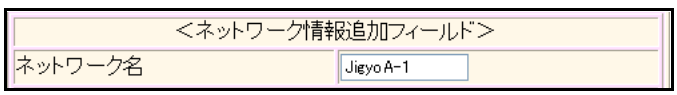
「相手情報」ページが表示されます。

16.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

17.　以下の項目を指定します。

- ネットワーク名　→JigyoA-1



18.　［追加］ボタンをクリックします。

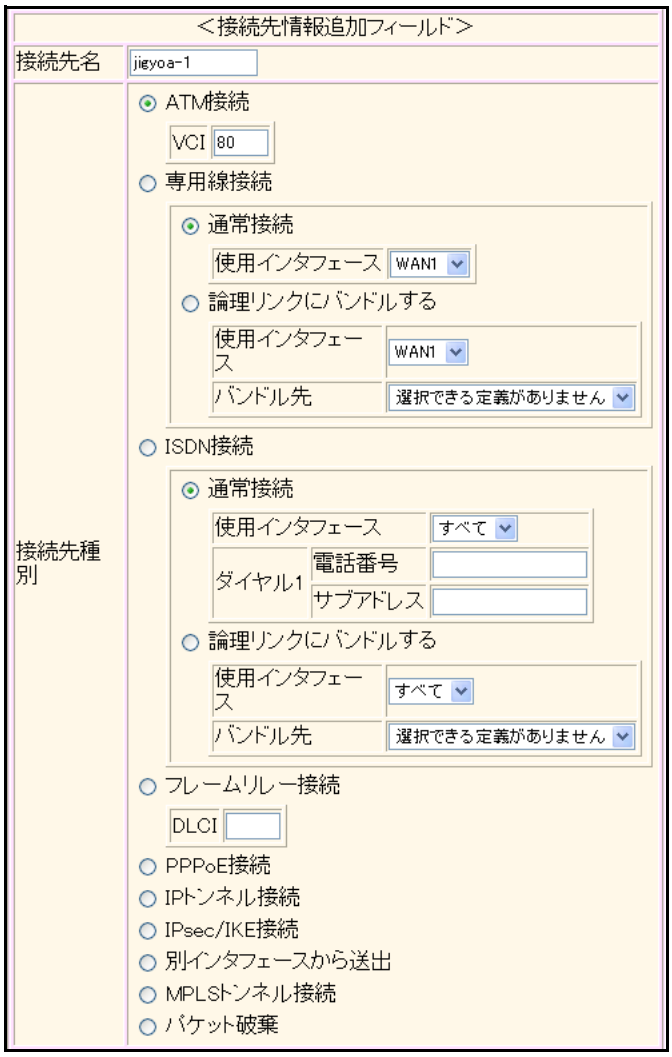
「ネットワーク情報（JigyoA-1）」ページが表示されます。

19.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

20.　以下の項目を指定します。

- 接続先名　→jigyoa-1
- 接続先種別　→ATM 接続
  VCI　→80



Si-R260B では、接続先種別の表示が上記の画面とは異なります。

21.　［追加］ボタンをクリックします。

ATM 接続の設定項目と「基本情報」が表示されます。

22.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- VCI　→80
- VC 速度　→6Mbps
- サービスタイプ　→VBR
  平均速度値　→5Mbps
  最大バースト長　→32
- OAM（F5）　→受け付けない

23.　［保存］ボタンをクリックします。

24.　画面上部の「ネットワーク情報（JigyoA-1）をクリックします。

「ネットワーク情報（JigyoA-1）」が表示されます。

25.　「IP 関連」をクリックします。

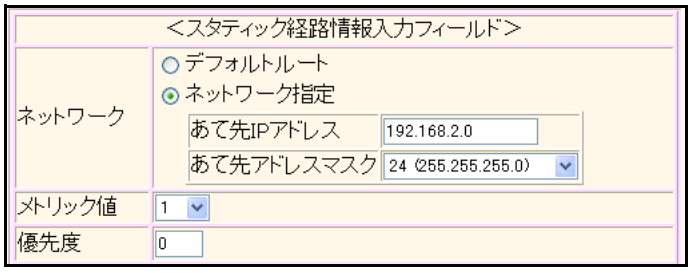
IP 関連の設定項目と「IP 基本情報」が表示されます。

26.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

27.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 192.168.2.0
  あて先アドレスマスク　→ 24（255.255.255.0）
- メトリック値　→ 1
- 優先度　→ 0



28.　［追加］ボタンをクリックします。

IPv6 の相手情報を設定する

29.　画面上部の「相手情報」をクリックします。

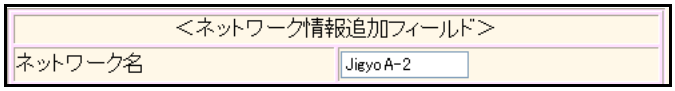
「相手情報」ページが表示されます。

30.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

31.　以下の項目を指定します。

- ネットワーク名　→JigyoA-2



32.　［追加］ボタンをクリックします。

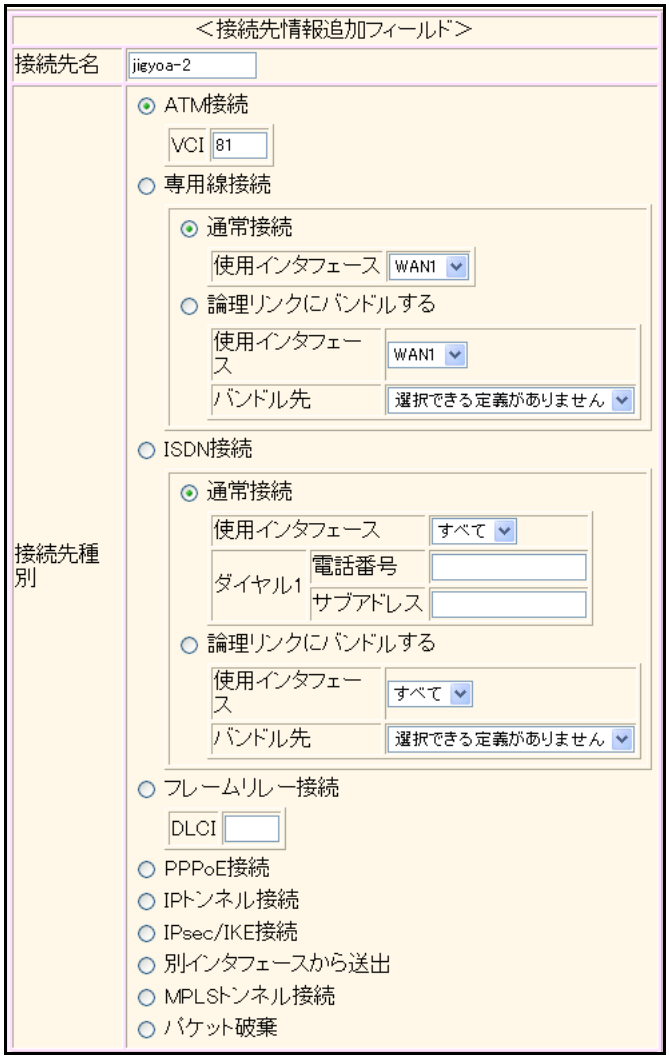
「ネットワーク情報（JigyoA-2）」ページが表示されます。

33.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

34.　以下の項目を指定します。

- 接続先名　→jigyoa-2
- 接続先種別　→ATM 接続
  VCI　→81



Si-R260B では、接続先種別の表示が上記の画面とは異なります。

35.　［追加］ボタンをクリックします。

ATM 接続の設定項目と「基本情報」が表示されます。

36.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- VCI　→81
- VC 速度　→5Mbps
- サービスタイプ　→UBR+
  最低速度値　→3Mbps
- OAM（F5）　→受け付けない

37.　［保存］ボタンをクリックします。

38.　画面上部の「ネットワーク情報（JigyoA-2）をクリックします。

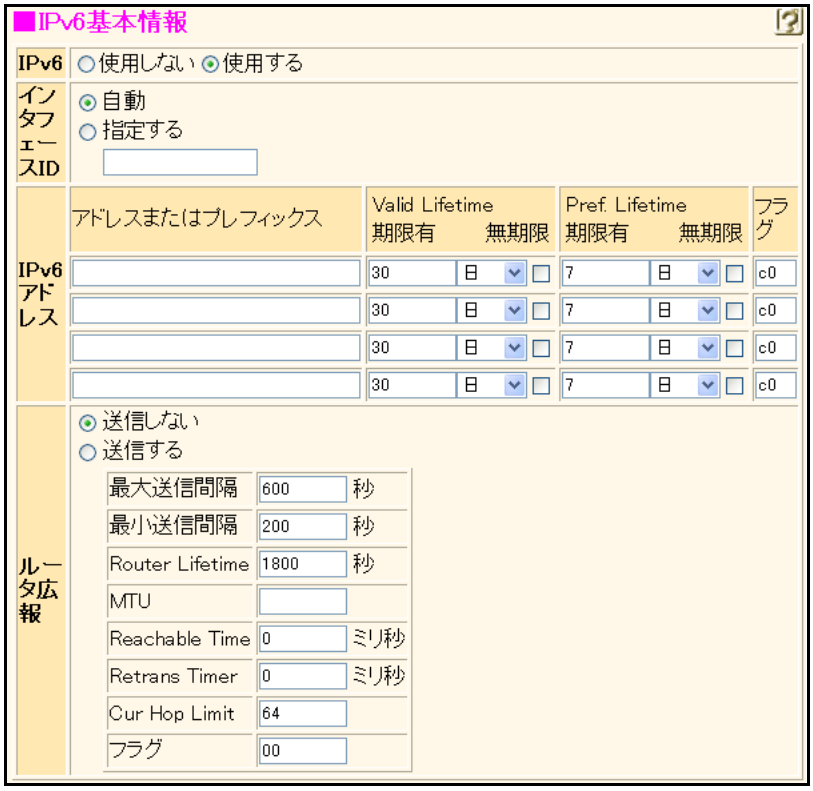
「ネットワーク情報（JigyoA-2）」が表示されます。

39.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

40.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス　→指定しない
- ルータ広報　→送信しない



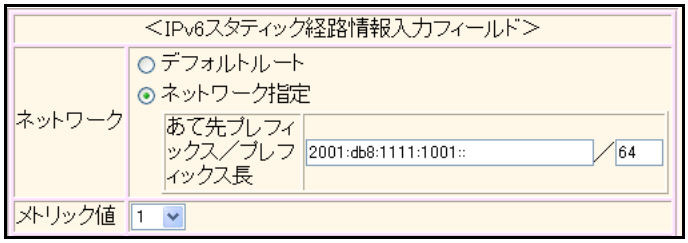
41.　［保存］ボタンをクリックします。

42.　IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

43.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先プレフィックス／プレフィックス長　→2001:db8:1111:1001::/64
- メトリック値　→1



44.　［追加］ボタンをクリックします。

45.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

事業所 A を設定する

「本社を設定する」を参考に、事業所 A を設定します。

VPC の情報を設定する

「WAN0 情報」

- 回線インタフェース　→ ATM

「基本情報」

- ポート　→スロット 0-0
- VPI　→ 0
- VP 速度　→ 8Mbps
- OAM（F4）　→受け付けない

LAN 情報を設定する

「LAN0 情報」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.2.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1

「LAN0 情報」-「IPv6 関連」

「IPv6 基本情報」

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス
  アドレスまたはプレフィックス　→ 2001:db8:1111:1001::
  Valid Lifetime　→ 30 日
  Pref. Lifetime　→ 7 日
  フラグ　→ c0
- ルータ広報　→送信する

IPv4 の相手情報を設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→ Honsya-1

「ネットワーク情報」-「接続先情報」

- 接続先名　→ honsya-1
- 接続先種別　→ ATM 接続
  VCI　→ 82

「接続先情報」-「ATM 接続」

「基本情報」

- 使用インタフェース　→WAN0
- VCI　→82
- VC 速度　→6Mbps
- サービスタイプ　→VBR
  平均速度値　→5Mbps
  最大バースト長　→32
- OAM（F5）　→受け付けない

「ネットワーク情報」-「IP 関連」

「スタティック経路情報」

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）
- メトリック値　→1
- 優先度　→0

IPv6 の相手情報を設定する

「相手情報」-「ネットワーク情報」

- ネットワーク名　→Honsya-2

「ネットワーク情報」-「接続先情報」

- 接続先名　→honsya-2
- 接続先種別　→ATM 接続
  VCI　→83

「接続先情報」-「ATM 接続」

「基本情報」

- 使用インタフェース　→WAN0
- VCI　→83
- VC 速度　→5Mbps
- サービスタイプ　→UBR+
  最低速度値　→3Mbps
- OAM（F5）　→受け付けない

「ネットワーク情報」-「IPv6 関連」

「IPv6 基本情報」

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス　→指定しない
- ルータ広報　→送信しない

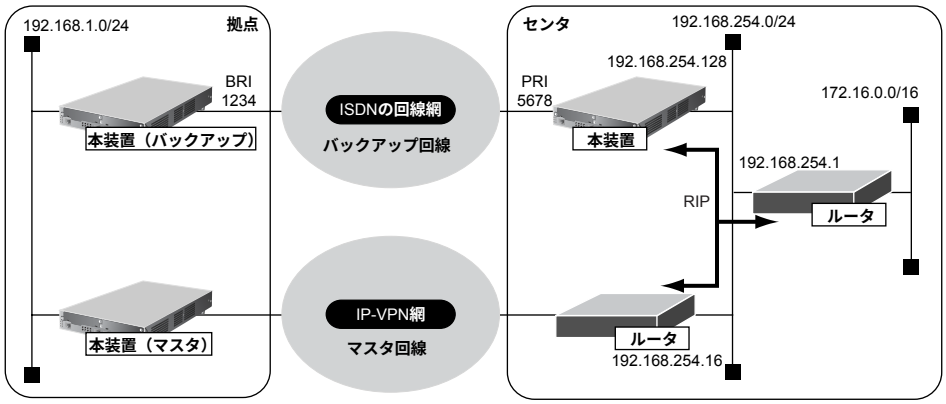
「IPv6 スタティック経路情報」

- ネットワーク　→ネットワーク指定
- あて先プレフィックス／プレフィックス長　→2001:db8:1111:1000::/64
- メトリック値　→1

2.36 ISDN 接続を契機とした通信バックアップを使う

適用機種　***Si-R220B,220C,370,570***

マスタ回線側で経路制御ができなくても、バックアップ回線である ISDN 回線の接続状態によって、通信をバックアップ側に切り替えることができます。



● 設定条件

- センタ側は、本装置以外の装置は設定が完了済み
- センタ側の 192.168.254.0/24 に接続されたそれぞれのルータは、本装置が広報する経路が選択されるように設定されている
- センタから拠点への発信は行わない
- 拠点側本装置は、ISDN 接続の設定以外は設定が完了済み

上記の設定条件に従って設定を行う場合の設定例を示します。

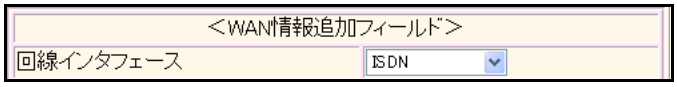
センタ側本装置を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　　→ISDN



3.　［追加］ボタンをクリックします。

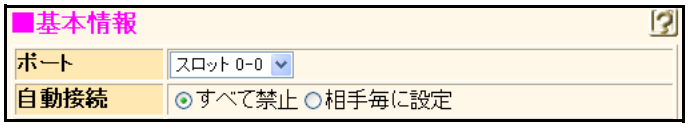
「WAN0 情報（ISDN）」ページが表示されます。

4.　「基本情報」をクリックします。

「基本情報」が表示されます。

5.　以下の項目を指定します。

- ポート　→スロット 0-0
- 自動接続　→すべて禁止



6.　［保存］ボタンをクリックします。

7.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

8.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

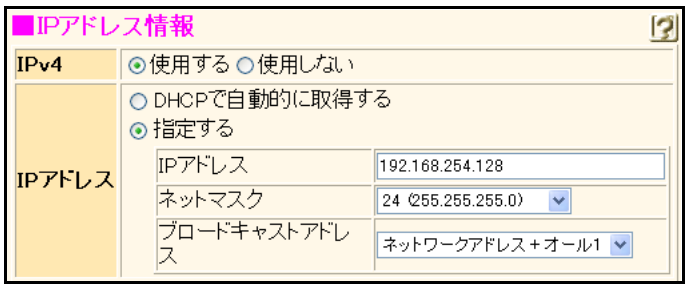
「LAN0 情報（物理 LAN）」ページが表示されます。

9.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

10.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.254.128
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



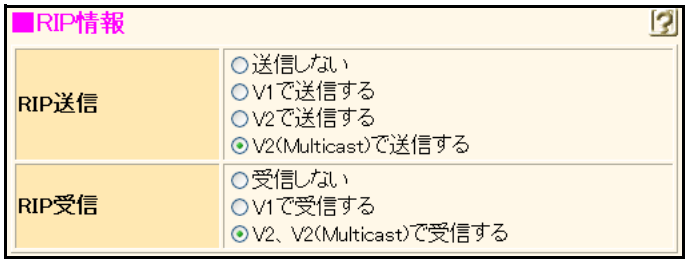
11.　［保存］ボタンをクリックします。

12.　IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

13.　以下の項目を指定します。

- RIP 送信　→V2（Multicast）で送信する
- RIP 受信　→V2、V2（Multicast）で受信する



14.　［保存］ボタンをクリックします。

15.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

16.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

17.　以下の項目を指定します。

- ネットワーク名　→kyoten

18.　［追加］ボタンをクリックします。

「ネットワーク情報（kyoten）」ページが表示されます。

19.　「IP 関連」をクリックします。

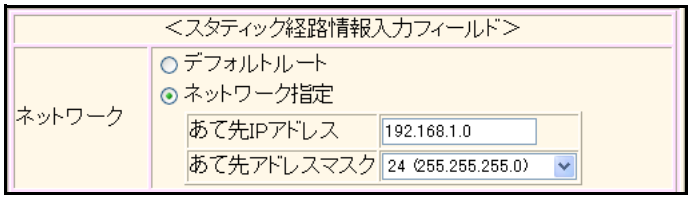
IP 関連の設定項目と「IP 基本情報」が表示されます。

20.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

21.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→192.168.1.0
  あて先アドレスマスク　→24（255.255.255.0）



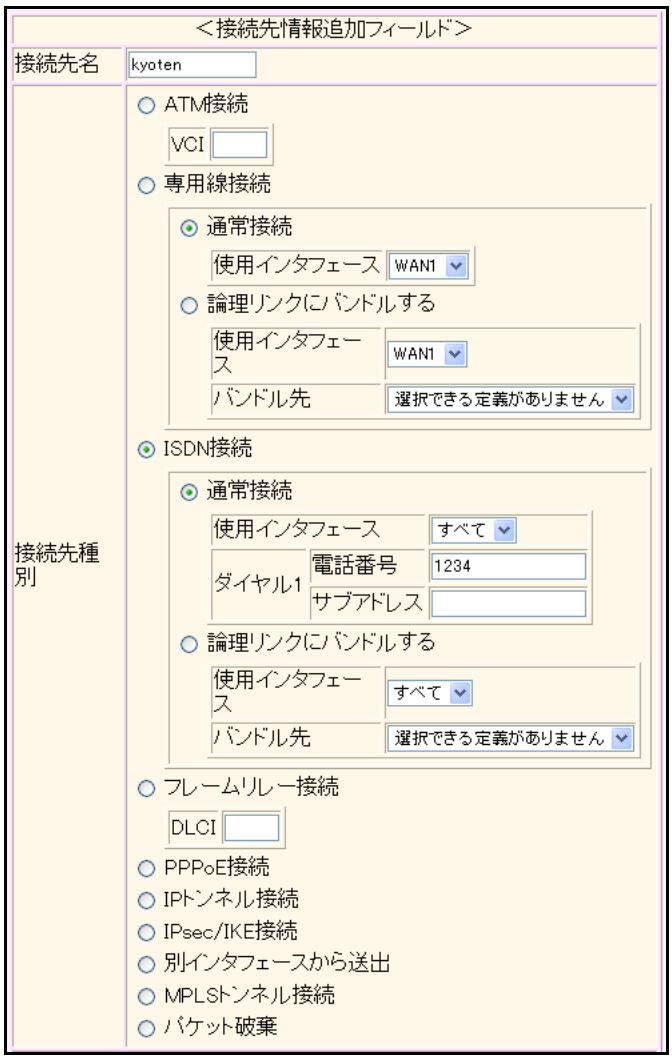
22.　［追加］ボタンをクリックします。

23.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

24.　以下の項目を指定します。

- 接続先名　→kyoten
- 接続先種別　→ISDN 接続
  →通常接続
  ダイヤル 1
  電話番号　→1234



Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

25.　［追加］ボタンをクリックします。

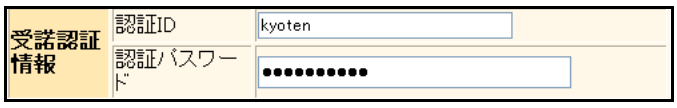
ISDN 接続の設定項目と「基本情報」が表示されます。

26.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

27.　以下の項目を指定します。

- 受諾認証情報
  認証 ID　→kyoten
  認証パスワード　→kyotenpass



28.　［保存］ボタンをクリックします。

29.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

拠点側本装置を設定する

1.　設定メニューのルータ設定で「相手情報」をクリックします。

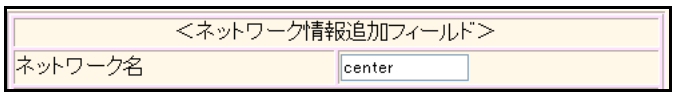
「相手情報」ページが表示されます。

2.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3.　以下の項目を指定します。

- ネットワーク名　→center



4.　［追加］ボタンをクリックします。

「ネットワーク情報（center）」ページが表示されます。

5.　「IP 関連」をクリックします。

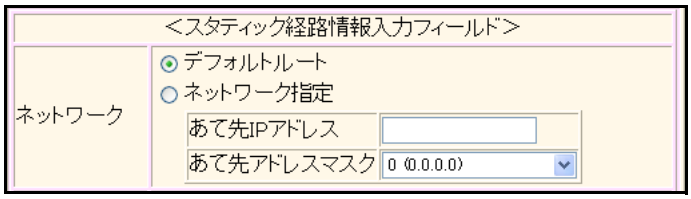
IP 関連の設定項目と「IP 基本情報」が表示されます。

6.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク　→デフォルトルート



8.　［追加］ボタンをクリックします。

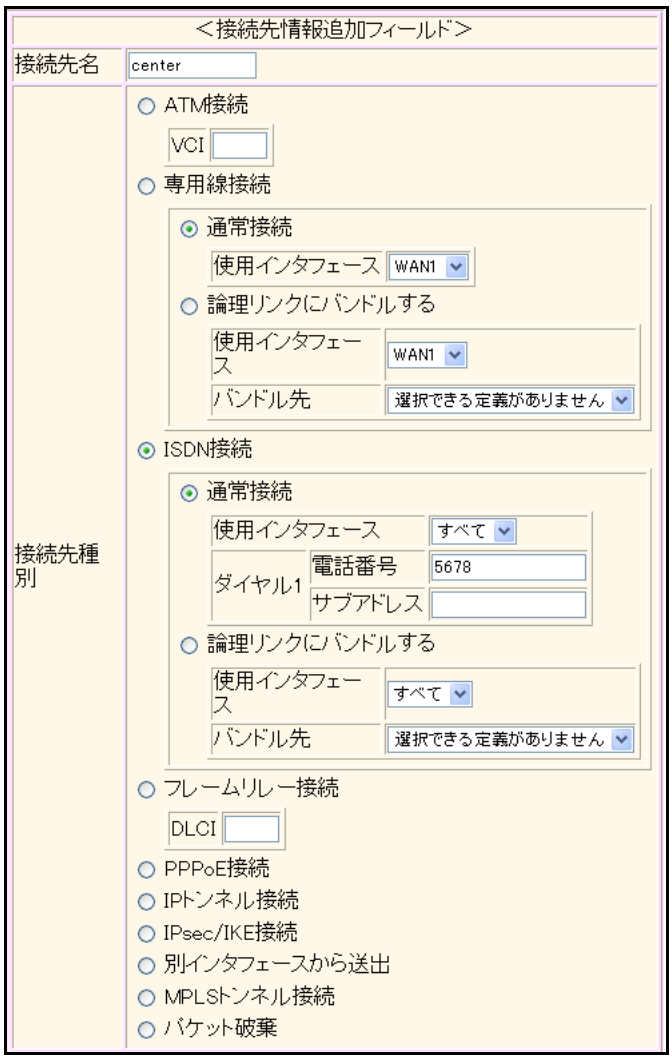
9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→center
- 接続先種別　→ISDN 接続
  →通常接続

  ダイヤル 1
  電話番号　→5678



Si-R220B、220C では、接続先種別の表示が上記の画面とは異なります。

11.　［追加］ボタンをクリックします。

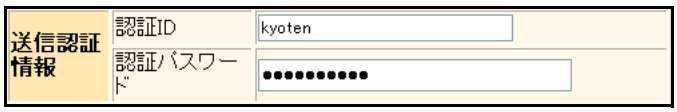
ISDN 接続の設定項目と「基本情報」が表示されます。

12.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

13.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→kyoten
  認証パスワード　→kyotenpass



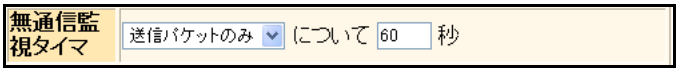
14.　［保存］ボタンをクリックします。

15.　ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

16.　以下の項目を指定します。

- 無通信監視タイマ　　→送信パケットのみについて 60 秒



17.　［保存］ボタンをクリックします。

18.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.37 外部のパソコンから PIAFS 接続する

適用機種 *Si-R220B,220C,370*

ここでは、PIAFS 対応の PHS を使用して外部のパソコンから本装置へ着信接続する例を説明します。接続先のパソコンの設定に関する説明は省略しています。

こんな事に気をつけて

- **本装置の PIAFS 接続は PIAFS 1.0/2.0/2.1 に対応します。**
- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。**

  ☛ 参照 Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）

- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

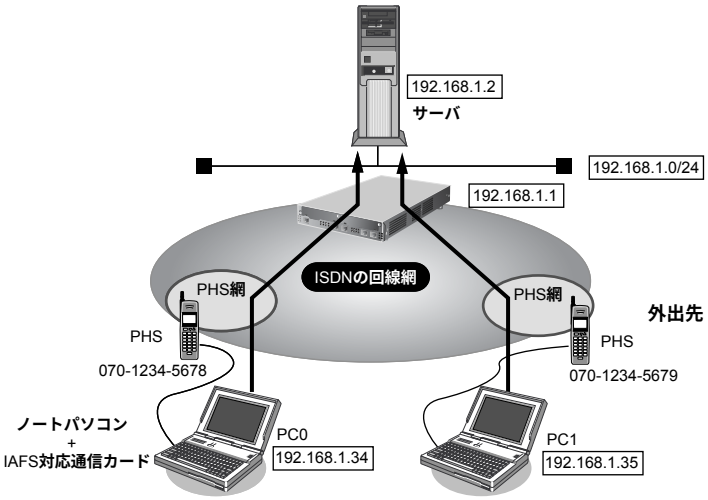
  ☛ 参照 Si-R シリーズ　Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」（P.19）

本装置の LAN 側のネットワークと同じネットワークアドレスを別ネットワークのパソコンに割り当てることによって、Proxy ARP が自動的に動作し、ISDN 回線経由で接続されたパソコンが LAN 上に存在するように扱えます。

ヒント

◆ Proxy ARP とは

Ethernet 上で通信する場合、相手を識別するために MAC アドレスが使用されます。このとき、IP アドレスと MAC アドレスの対応付けを行う手段として ARP（Address Resolution Protocol）が使用されます。
ブロードキャストで ARP 要求を発行すると、LAN 上で自分の IP アドレスに関連する ARP 要求であると認識したパソコンは、自分の MAC アドレスを送り返します。
Proxy ARP とは、パソコンから送られてくる ARP 要求に対して、実際のパソコンの代わりに応答する機能です。



● 設定条件

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R370）または ISDN U ポート（Si-R220B、220C）を使用して ISDN 回線に接続する
- 本装置の LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24

[PC0（ノートパソコン＋ PHS）と接続する条件]

- 接続先ネットワーク名　：pc0
- 接続先名　：phs0
- 割り当て IP アドレス　：192.168.1.34
- 電話番号　：070-1234-5678
- 受諾認証 ID　：mobileid
- 受諾認証パスワード　：mobilepass

[PC1（ノートパソコン＋ PHS）と接続する条件]

- 接続先ネットワーク名　：pc1
- 接続先名　：phs1
- 割り当て IP アドレス　：192.168.1.35
- 電話番号　：070-1234-5679
- 受諾認証 ID　：mobileid
- 受諾認証パスワード　：mobilepass

上記の設定条件に従って設定を行う場合の設定例を示します。

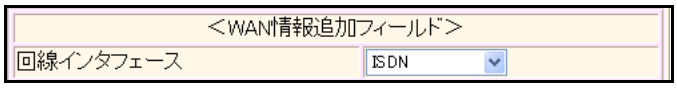
回線情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→ISDN



3.　［追加］ボタンをクリックします。

「WAN0 情報（ISDN）」ページが表示されます。

LAN 情報を設定する

4.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

5.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

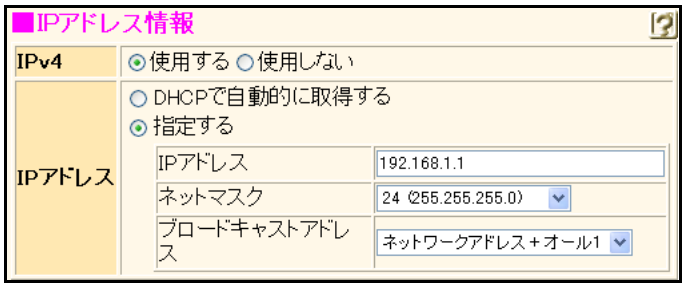
6.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

7.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する

IP アドレス　→ 192.168.1.1
ネットマスク　→ 24（255.255.255.0）
ブロードキャストアドレス　→ネットワークアドレス＋オール 1



8.　［保存］ボタンをクリックします。

接続先情報（PC0）を設定する

9.　設定メニューのルータ設定で「相手情報」をクリックします。

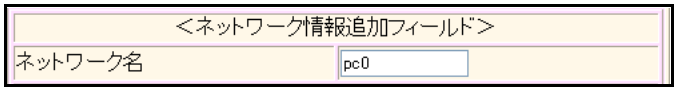
「相手情報」ページが表示されます。

10.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11.　以下の項目を指定します。

- ネットワーク名　→pc0



12.　［追加］ボタンをクリックします。

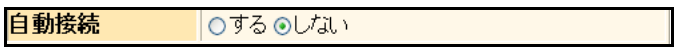
「ネットワーク情報（pc0）」ページが表示されます。

13.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 自動接続　→しない



必要に応じて上記以外の項目を指定します。

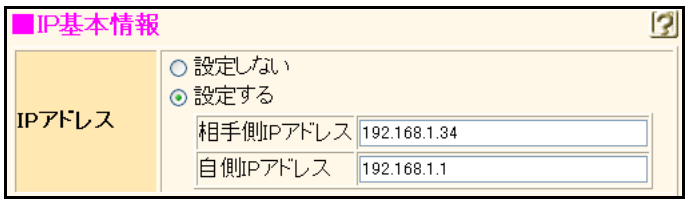
15.　［保存］ボタンをクリックします。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

17.　以下の項目を指定します。

- IPアドレス　→設定する
  相手側IPアドレス　→192.168.1.34
  自側IPアドレス　→192.168.1.1



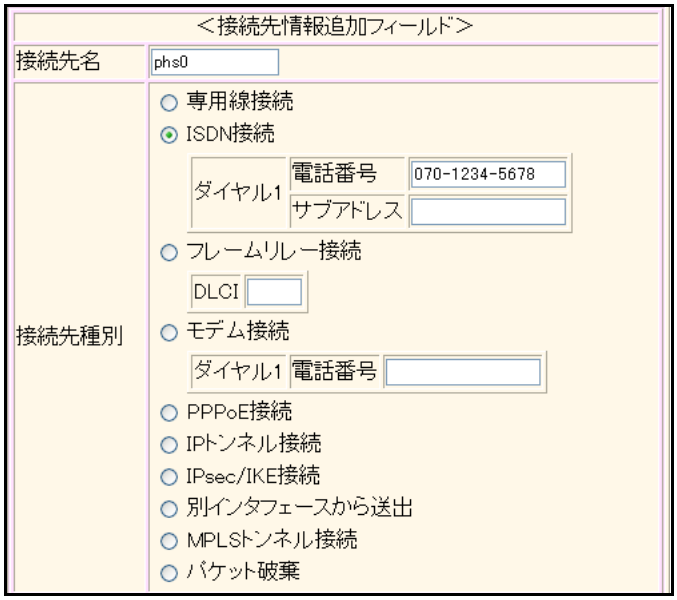
18.　［保存］ボタンをクリックします。

19.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

20.　以下の項目を指定します。

- 接続先名　→phs0
- 接続先種別　→ISDN 接続
  ダイヤル 1
  電話番号　→070-1234-5678



Si-R370 では、接続先種別の表示が上記の画面とは異なります。

21.　［追加］ボタンをクリックします。

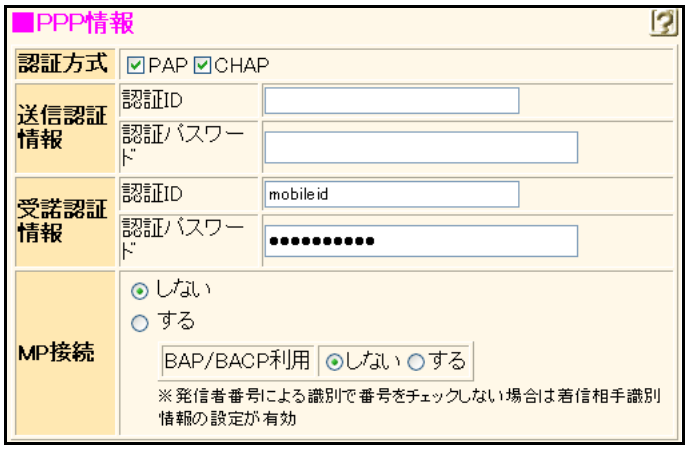
ISDN 接続の設定項目と「基本情報」が表示されます。

22.　ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

23.　以下の項目を指定します。

- 認証方式　→PAP、CHAP
- 送信認証情報　→設定しない
- 受諾認証情報
  認証 ID　→mobileid
  認証パスワード　→mobilepass
- MP 接続　→しない



24.　［保存］ボタンをクリックします。

接続先情報（PC1）を設定する

25.　「接続先情報（PC0）を設定する」を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」

- ネットワーク名　→pc1

「ネットワーク情報」-「共通情報」

「基本情報」

- 自動接続　→しない

「ネットワーク情報」-「IP 関連」

「IP 基本情報」

- IP アドレス　→設定する
  相手側 IP アドレス　→192.168.1.35
  自側 IP アドレス　→192.168.1.1
  必要に応じて上記以外の項目を設定します。

「ネットワーク情報」-「接続先情報」

- 接続先名　→phs1
- 接続先種別　→ISDN 接続
  ダイヤル 1
  電話番号　→070-1234-5679
  サブアドレス　→設定しない

「接続先情報」-「ISDN 接続」

「PPP 情報」

- 認証方式　→ PAP、CHAP
- 送信認証情報　→設定しない
- 受諾認証情報
  認証 ID　→ mobileid
  認証パスワード　→ mobilepass
- MP 接続　→しない

26.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

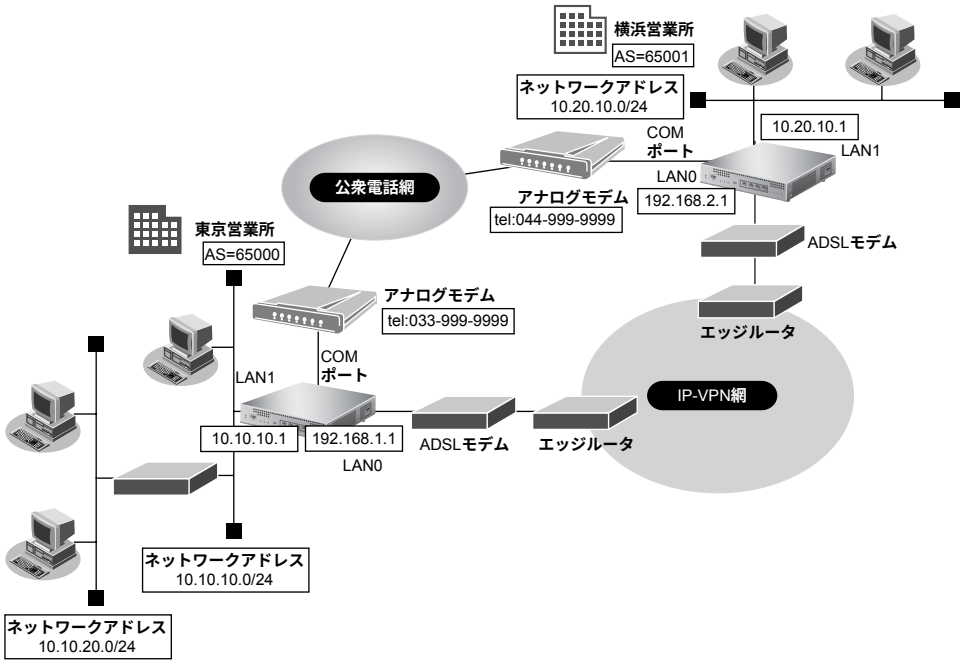
2.38 アナログモデムで通信バックアップをする

適用機種　***Si-R220B,220C***

本装置のCOMポートに外付けのアナログモデムを接続することによって、アナログ回線を使用して通信することができます。

ここでは、営業所間をIP-VPN網で接続し、IP-VPN網側の通信が通信不能になった場合にアナログ回線側で通信バックアップする場合を例に説明します。

この例では、BGP経路よって優先度の低いスタティックルートをバックアップ回線側に設定します。メインのIP-VPN側が通信不能になってBGPセッションが切断され、相手拠点のBGP経路が消えた際に、バックアップ回線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



本装置に接続できるモデムの条件は、以下のとおりです。

- COMポート側の通信速度が9600/19200/38400/57600/115200/230400bpsのどれかの速度で通信できる
- 工場出荷時の設定で、RS/CS信号によるハードフロー制御が有効になっている
- 通信中に`+++`をCOMポートから受信することによってエスケープモードになる
- 以下のATコマンドに対応している

カテゴリ	サポートコマンド
ソフトリセット	ATZ
リザルトコードを文字列にする	ATV1
エコーバックを抑止する	ATE0
CONNECTリザルトコードにDCE速度を付加する	ATW2
切断	ATH
応答	ATA
コマンド送出時先行文字	AT
電話番号送出時先行文字	ATD
パルス	P
トーン	T

カテゴリ	サポートコマンド
ダイヤルトーン検知なし	X3
ダイヤルトーン検知あり	X4
スピーカを OFF にする	M0
発呼時だけスピーカを ON にする	M1
スピーカを ON にする	M2
スピーカをダイヤル終了からキャリア検出まで ON にする	M3
音量 LOW	L0
音量 Midium	L2
音量 High	L3

- 以下のリザルトコードを返す

カテゴリ	サポートコマンド
正常実行	OK
接続完了	CONNECT <回線速度>（※）
コマンドエラー	ERROR、+FCERROR、+FCON、+F4、FAX、DATA、VOICE
回線接続	NO CARRIER
ダイヤルトーン未検出	NO DIALTONE、NO DIAL TONE
話し中音検出	BUSY、PHONE IN USE、HAND SET IN USE
無音未検出	NO ANSWER
呼び出し検出	RING

※）回線速度 : 接続した回線速度
0-9 の数字文字列の場合だけ回線速度として扱います。
0-9 以外の文字が含まれる場合は、無視するため、回線速度を取得できません。

動作確認済みのアナログモデムは、以下のとおりです。

会社名	製品名
（株）アイ・オー・データ機器	DFML-560EL
（株）バッファロー	IGM-B56KS
オムロン（株）	ME5614E2

こんな事に気をつけて

- アナログモデムは、COM ポートに接続してください。コンソールポートは、コンソール専用ですので、モデム接続はできません。
- モデムの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからモデムを接続してください。
- モデムでは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。
- アナログモデム接続では、以下の機能は動作しません。
  - 電話番号による相手識別機能
  - 金額による課金制御機能
  - 常時接続機能
  - シェーピング機能
- モデムで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- アナログモデムによる発信は超過課金が発生するため、課金情報（アカウント情報）を監視して超過課金が発生していないか、こまめに確認してください。
  また、超過課金を防止する場合は、課金制御機能の接続時間制限を設定してください。
- アナログモデムでの通信速度は 56Kbps とみなして動作しますが、モデムの接続完了リザルトコードから速度を取得できた場合は取得した速度を採用して動作します。

ここでは、以下を参照して、IP-VPN 網接続が設定されていることを前提とします。

☛ 参照 「1.13 複数の事業所 LAN を IP-VPN 網を利用して接続する」（P.127）

● 設定条件

- ADSL モデムを使用して IP-VPN 網と接続する

[東京営業所]

＜横浜営業所とモデムで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：yokohama
- WAN の自側 IP アドレス　：172.17.1.1
- WAN の相手側 IP アドレス　：172.17.1.2
- 電話番号　：044-999-9999
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass
- ダイヤル方式　：トーン
- バックアップ用のスタティックルート　：10.20.0.0/16（優先度 30）

[横浜営業所]

＜東京営業所とモデムで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：tokyo
- WAN の自側 IP アドレス　：172.17.1.2
- WAN の相手側 IP アドレス　：172.17.1.1
- 電話番号　：033-999-9999
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass
- ダイヤル方式　：トーン
- バックアップ用のスタティックルート　：10.10.0.0/16（優先度 30）

上記の設定条件に従って設定を行う場合の設定例を示します。

東京営業所の設定する

COM ポートを設定する

1.　設定メニューのルータ設定で「シリアル情報」をクリックします。

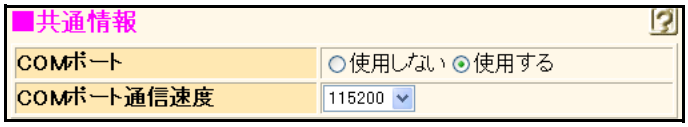
「シリアル情報」ページが表示されます。

2.　「共通情報」をクリックします。

「共通情報」が表示されます。

3.　以下の項目を指定します。

- COM ポート　→使用する
- COM ポート通信速度　→ 115200



4.　［保存］ボタンをクリックします。

バックアップ回線を設定する

5.　設定メニューのルータ設定で「相手情報」をクリックします。

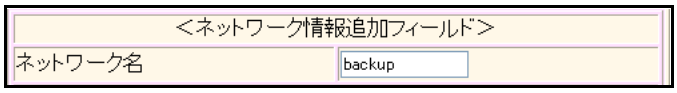
「相手情報」ページが表示されます。

6.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

7.　以下の項目を指定します。

- ネットワーク名　→backup



8.　［追加］ボタンをクリックします。

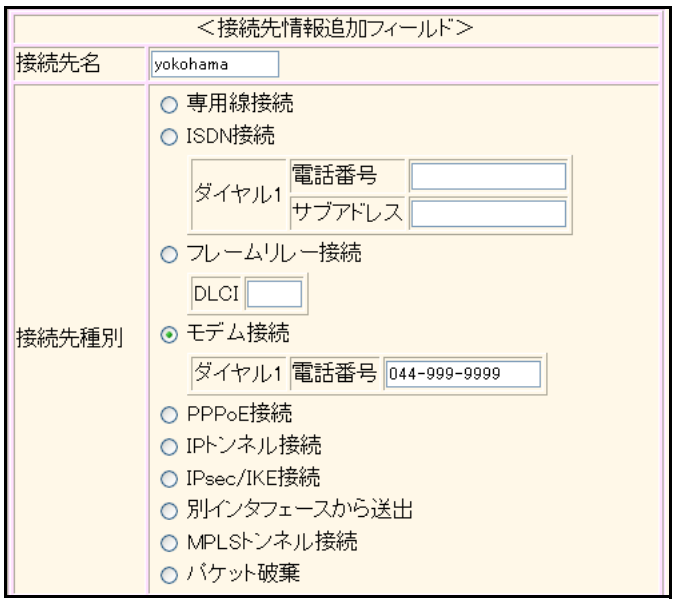
「ネットワーク情報（backup）」ページが表示されます。

9.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

10.　以下の項目を指定します。

- 接続先名　→yokohama
- 接続先種別　→モデム接続
  ダイヤル 1
  電話番号　→044-999-9999



11.　［追加］ボタンをクリックします。

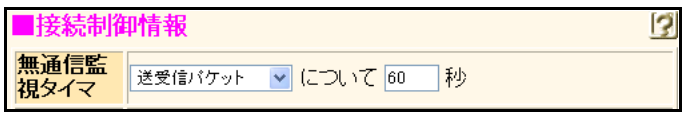
「接続先情報（yokohama）」ページが表示されます。

12.　モデム接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

13.　以下の項目を指定します。

- 無通信監視タイマ　→送受信パケットについて 60 秒



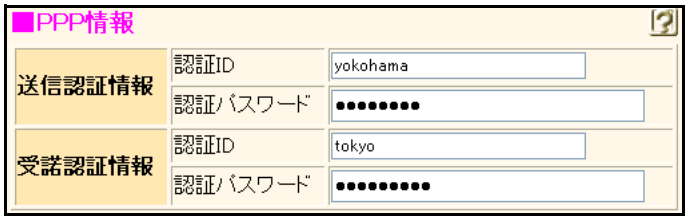
14.　［保存］ボタンをクリックします。

15.　モデム接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

16.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→ yokohama
  認証パスワード　→ yokopass
- 受諾認証情報
  認証 ID　→ tokyo
  認証パスワード　→ tokyopass



17.　［保存］ボタンをクリックします。

着信デフォルト情報を設定する

18.　設定メニューのルータ設定で「相手情報」をクリックします。

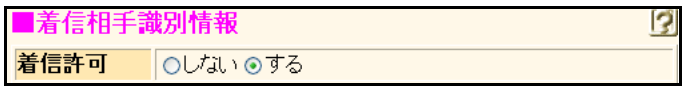
「相手情報」ページが表示されます。

19.　「着信相手識別情報」をクリックします。

「着信相手識別情報」が表示されます。

20.　以下の項目を指定します。

- 着信許可　→する



21.　［保存］ボタンをクリックします。

BGP より優先度の低いスタティックルートを設定する

22.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

23.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

24.　ネットワーク名が backup の［修正］ボタンをクリックします。

「ネットワーク情報（backup）」ページが表示されます。

25.　「IP 関連」をクリックします。

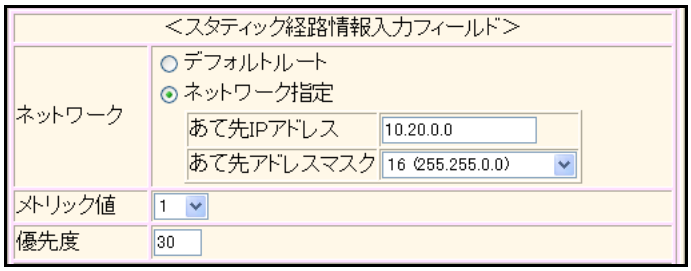
IP 関連の設定項目と「IP 基本情報」が表示されます。

26.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

27.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.20.0.0
  あて先アドレスマスク　→ 16（255.255.0.0）
- メトリック値　→ 1
- 優先度　→ 30



28.　［追加］ボタンをクリックします。

29.　画面左側の［設定反映］ボタンをクリックします。

横浜営業所を設定する

「東京営業所を設定する」を参考に、横浜営業所を設定します。

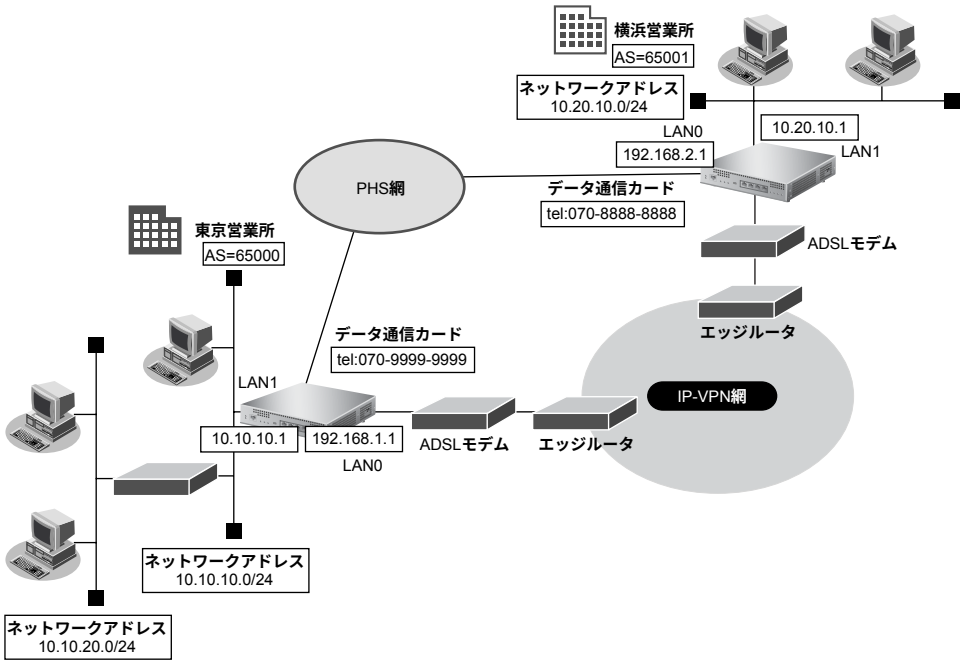
2.39 データ通信カードで通信バックアップをする

適用機種 ***Si-R240,240B***

本装置に PIAFS 着信対応のデータ通信カードを装着することによって、PHS 回線を使用して通信することができます。
ここでは、営業所間を IP-VPN 網で接続し、IP-VPN 網側の通信が通信不能になった場合にウィルコムの PHS 回線側で通信バックアップする場合を例に説明します。

参照 動作検証済みのデータ通信カード（富士通ホームページ）
- Si-R240
  http://fenics.fujitsu.com/products/sir/sir240/#supportcard
- Si-R240B
  http://fenics.fujitsu.com/products/sir/sir240b/#supportcard

この例では、BGP 経路よって優先度の低いスタティックルートをバックアップ回線側に設定します。メインの IP-VPN 側が通信不能になって BGP セッションが切断され、相手拠点の BGP 経路が消えた際に、バックアップ回線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



こんな事に気をつけて

- **データ通信カードの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからデータ通信カードを装着してください。**
- **データ通信カードでは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。**
- **データ通信カード接続では、以下の機能は動作しません。**
  - **電話番号による相手識別機能**
  - **コールバック機能**
  - **金額による課金制御機能**
  - **常時接続機能**
  - **回線接続保持タイマ機能**
- **データ通信カードで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。**
- **データ通信カードによる発信は従量課金が発生するため、データ通信カード統計情報を監視して異常課金が発生していないか、こまめに確認してください。また、異常課金を防止する場合は、課金制御機能や強制切断機能の接続時間制限を設定してください。**

- **データ通信カードの通信速度は 64Kbps とみなして動作します。**
- **ウィルコム、FENICS、NTT コミュニケーションズの PHS 接続時には、通信方式に応じて、以下の番号を電話番号に付加してください。**

通信方式	電話番号に付加する番号
32kPIAFS 方式	##3
64kPIAFS（ベストエフォート）方式	##4
1x パケット方式	##61
4x パケット方式または 8x パケット方式	##64
フレックスチェンジ方式	##7

ここでは、以下を参照して、IP-VPN 網接続が設定されていることを前提とします。

☛ 参照 「1.13 複数の事業所 LAN を IP-VPN 網を利用して接続する」（P.127）

● 設定条件

- ADSL モデムを使用して IP-VPN 網と接続する
- データ通信カードは SLOT0 に装着する

[東京営業所]

＜横浜営業所とデータ通信カードで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：yokohama
- WAN の自側 IP アドレス　：172.17.1.1
- WAN の相手側 IP アドレス　：172.17.1.2
- 電話番号　：070-8888-8888
- 通信方式　：64kPIAFS（ベストエフォート）方式
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：kawasaki、kawapass
- バックアップ用のスタティックルート　：10.20.0.0/16（優先度 30）

[横浜営業所]

＜東京営業所とデータ通信カードで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：tokyo
- WAN の自側 IP アドレス　：172.17.1.2
- WAN の相手側 IP アドレス　：172.17.1.1
- 電話番号　：070-9999-9999
- 通信方式　：64kPIAFS（ベストエフォート）方式
- 無通信監視　：1 分
- ユーザ認証 ID とユーザ認証パスワード
  発信　：kawasaki、kawapass
  着信　：tokyo、tokyopass
- バックアップ用のスタティックルート　：10.10.0.0/16（優先度 30）

上記の設定条件に従って設定を行う場合の設定例を示します。

東京営業所のバックアップ回線を設定する

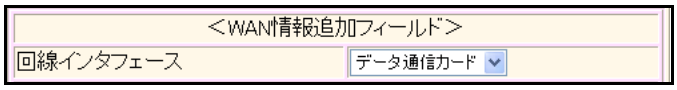
WAN0 情報を設定する

1.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- 回線インタフェース　→データ通信カード

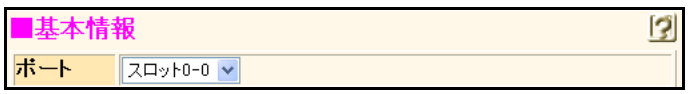


3.　［追加］ボタンをクリックします。

「WAN 情報（データ通信カード）」ページが表示されます。

4.　以下の項目を指定します。

- ポート　→スロット 0-0



5.　［保存］ボタンをクリックします。

こんな事に気をつけて

PIN コード機能を使用する場合は、「WAN 情報」-「基本情報」で設定する必要があります。また、操作メニューの「データ通信カード関連」-「PIN コード照合」でデータ通信カードにも設定する必要があります。

バックアップ回線を設定する

6.　設定メニューのルータ設定で「相手情報」をクリックします。

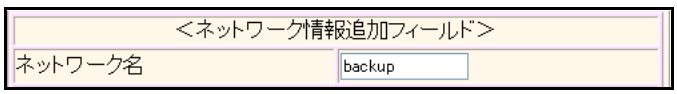
「相手情報」ページが表示されます。

7.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

8.　以下の項目を指定します。

- ネットワーク名　→backup



9.　［追加］ボタンをクリックします。

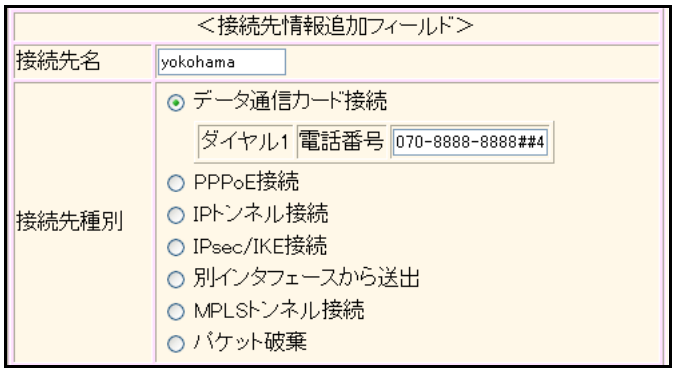
「ネットワーク情報（backup）」ページが表示されます。

10.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

11.　以下の項目を指定します。

- 接続先名　→yokohama
- 接続先種別　→データ通信カード接続
  ダイヤル 1
  電話番号　→070-8888-8888##4



12.　［追加］ボタンをクリックします。

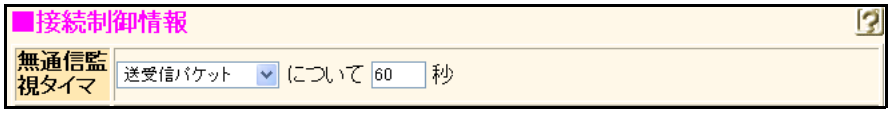
「接続先情報（yokohama）」ページが表示されます。

13.　データ通信カード接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

14.　以下の項目を指定します。

- 無通信監視タイマ　→送受信パケットについて 60 秒



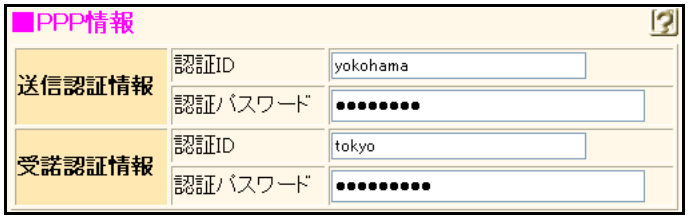
15.　［保存］ボタンをクリックします。

16.　データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

17.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→yokohama
  認証パスワード　→yokopass
- 受諾認証情報
  認証 ID　→tokyo
  認証パスワード　→tokyopass



18.　［保存］ボタンをクリックします。

着信デフォルト情報を設定する

19.　設定メニューのルータ設定で「相手情報」をクリックします。

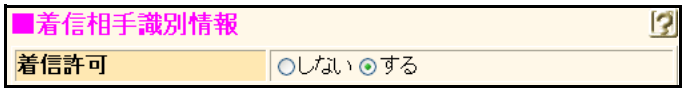
「相手情報」ページが表示されます。

20.　「着信相手識別情報」をクリックします。

「着信相手識別情報」が表示されます。

21.　以下の項目を指定します。

- 着信許可　→する



22.　［保存］ボタンをクリックします。

BGP より優先度の低いスタティックルートを設定する

23.　設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

24.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

25.　ネットワーク名が backup の［修正］ボタンをクリックします。

「ネットワーク情報（backup）」ページが表示されます。

26.　「IP 関連」をクリックします。

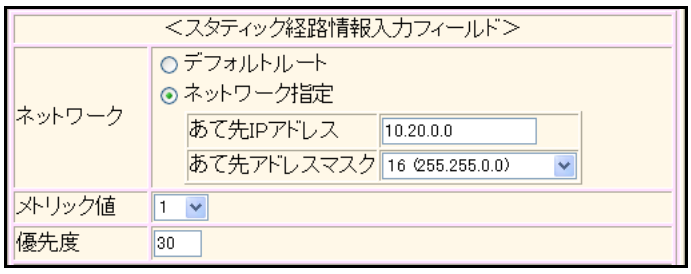
IP 関連の設定項目と「IP 基本情報」が表示されます。

27.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

28.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.20.0.0
  あて先アドレスマスク　→ 16（255.255.0.0）
- メトリック値　→ 1
- 優先度　→ 30



29.　［追加］ボタンをクリックします。

30.　画面左側の［設定反映］ボタンをクリックします。

横浜営業所のバックアップ回線を設定する

「東京営業所のバックアップ回線を設定する」を参考に、横浜営業所を設定します。

2.40 外部のパソコンから着信接続する（リモートアクセスサーバ）

適用機種 ***Si-R220B,220C,370,570***

ISDN 回線を使用して、外部のパソコンから本装置に着信接続する場合、本装置をリモートアクセスサーバとして使用することができます。以下の環境の場合に、リモートアクセスを行うことができます。

- デスクトップパソコン +TA →（ISDN）→本装置
- ノート型パソコン +ISDN カード→（ISDN）→本装置
- ノート型パソコン +PIAFS 通信カード +PHS →（PHS 網）→（ISDN）→本装置
- 本装置→（ISDN）→本装置

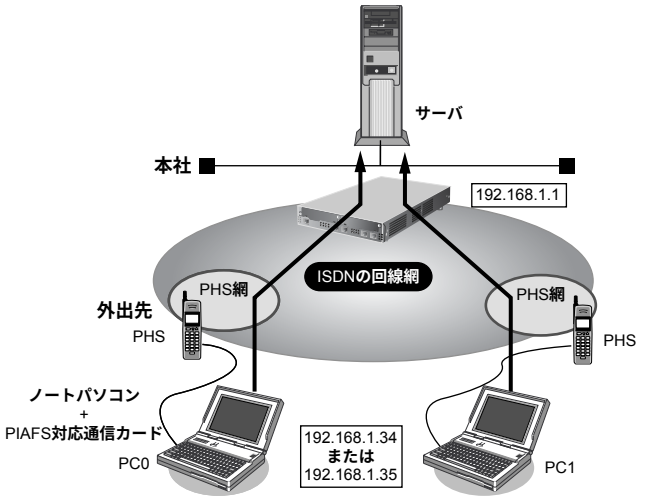
本装置では、テンプレート着信機能を使用した不特定着信と、AAA による認証（ローカル認証、RADIUS 認証）を組み合わせることで、リモートアクセスサーバを実現することができます。

参照 Si-R シリーズ　機能説明書「2.28 テンプレート着信機能」（P.139）

2.40.1 1 台の装置でリモートアクセスサーバを構成する

適用機種 ***Si-R220B,220C,370,570***

ここでは、ノートパソコンに PHS を繋いで外出先から本社のネットワークに接続する場合を例に説明します。



● 設定条件

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B、220C 以外）または ISDN U ポート（Si-R220B、220C）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- 以下からの着信を許可する

  [PC0 ＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 受諾認証 ID　：mobile-a
  - 受諾認証パスワード　：mobilepass-a
  - PHS の電話番号は未登録

[PC1＜ノートパソコン＋ PHS ＞で外出先から接続]

- 受諾認証 ID　：mobile-b
- 受諾認証パスワード　：mobilepass-b
- PHS の電話番号は未登録

- 本社の LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 外部のパソコンに割り当てる IP アドレス　：192.168.1.34、192.168.1.35

こんな事に気をつけて

- テンプレート着信機能をサポートする回線は ISDN です（MP 接続はできません）。
- テンプレート着信で使用するインタフェースはテンプレート専用になります。テンプレート用に予約された rmt インタフェースには、remote 定義を設定しないでください。
  たとえば、rmt30 ～ 47 インタフェースをテンプレート用に予約した場合、remote 30 ～ 47 までの remote 定義を設定しないでください。
- テンプレート情報を定義する場合（IP フィルタリングなど）、定義数は「テンプレート情報で設定した定義数×テンプレートで使用する rmt インタフェース数」で計算されるため、それを含めて装置最大定義数の範囲に収まるように定義してください。装置最大定義数を超えたときは、資源不足により該当機能が動作しない場合があります。
- 接続先情報を設定する場合、テンプレート用のインタフェースの個数分は設定しないでください。
  たとえば、接続先定義を最大 48 定義可能な装置で、10 インタフェースをテンプレート用に使用する場合、接続先定義の定義数は 38 となります。
- テンプレート情報と AAA 情報のユーザ側の設定に同じ項目がある場合は、個人情報である AAA 情報が適用されます。AAA 情報の未登録の項目に対しては、テンプレート情報の設定値が適用されます。
- 発信者番号による識別（CLID 相手判定）を AAA 情報に設定していない場合は、発信者番号による相手判定は行いません（PPP のユーザ認証の結果だけで接続できるかどうかが決まります）。
- AAA 情報に同一ユーザ（パスワードも同一）が存在するときには、定義番号が小さい AAA ユーザ情報が優先されます。定義番号が大きいユーザ情報に発信者番号が一致する定義があり、定義番号が小さいユーザ情報に発信番号で識別を行わない定義がある場合も、定義番号の小さいユーザで着信が行われます。
- 共通 ID で複数の着信を行う場合は、AAA 情報のユーザ定義に、ID とパスワードだけを定義してください（個別情報を定義しないで、ID とパスワードだけのユーザ情報を定義すると共有 ID として扱われます）。

上記の設定条件に従って設定を行う場合の設定例を示します。

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

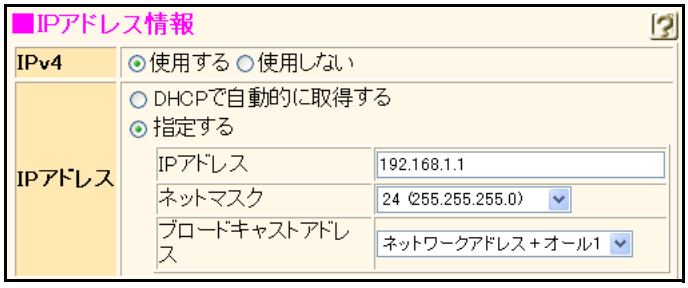
4.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する

  IPアドレス　→192.168.1.1

  ネットマスク　→24（255.255.255.0）

  ブロードキャストアドレス　→ネットワークアドレス＋オール1



5.　［保存］ボタンをクリックします。

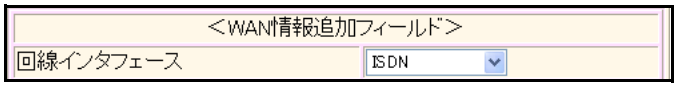
WAN0 情報を設定する

6.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- 回線インタフェース　→ISDN



8.　［追加］ボタンをクリックします。

「WAN1 情報（ISDN）」ページが表示されます。

9.　［保存］ボタンをクリックします。

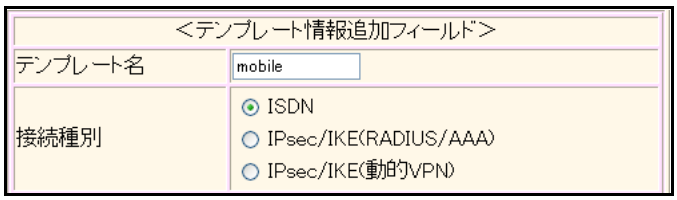
テンプレート情報を設定する

10.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

11.　以下の項目を指定します。

- テンプレート名　→mobile
- 接続先種別　→ISDN



機種により、接続先種別の表示が上記の画面とは異なります。

12.　［追加］ボタンをクリックします。

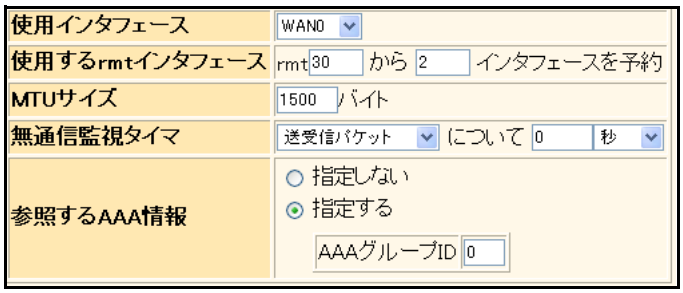
「テンプレート情報（mobile）」ページが表示されます。

13.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- 使用する rmt インタフェース　→rmt30 から 2 インタフェースを予約
- 参照する AAA 情報　→指定する
  AAA グループ ID　→0



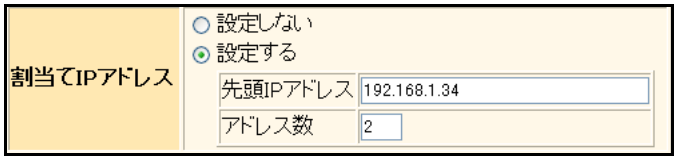
15.　［保存］ボタンをクリックします。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

17.　以下の項目を指定します。

- 割当て IP アドレス　→設定する
  先頭 IP アドレス　→192.168.1.34
  アドレス数　→2



18.　［保存］ボタンをクリックします。

19.　設定メニューのルータ設定で「AAA 情報」をクリックします。

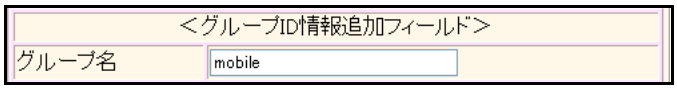
「AAA 情報」ページが表示されます。

20.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

21.　以下の項目を指定します。

- グループ名　→mobile



22.　［追加］ボタンをクリックします。

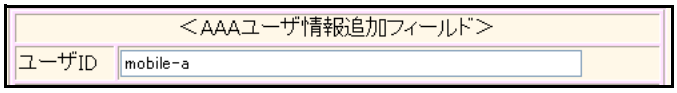
「グループ ID 情報（0）」と設定項目が表示されます。

23.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

24.　以下の項目を指定します。

- ユーザ ID　→ mobile-a

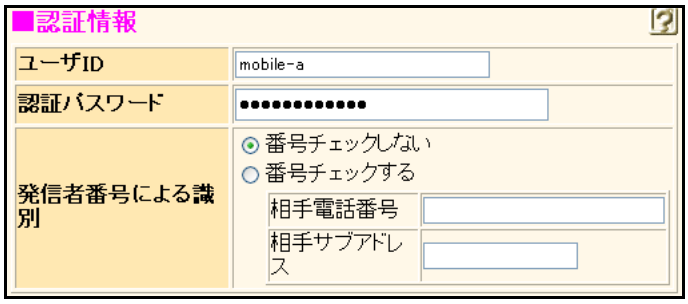


25.　［追加］ボタンをクリックします。

「AAA ユーザ情報（0）」と「認証情報」が表示されます。

26.　以下の項目を指定します。

- ユーザ ID　→ mobile-a
- 認証パスワード　→ mobilepass-a
- 発信者番号による識別　→番号チェックしない



27.　［保存］ボタンをクリックします。

28.　手順 26. ～ 27. を参考に、以下の項目を指定します。

- ユーザ ID　→ mobile-b
- 認証パスワード　→ mobilepass-b

29.　画面左側の［設定反映］ボタンをクリックします。

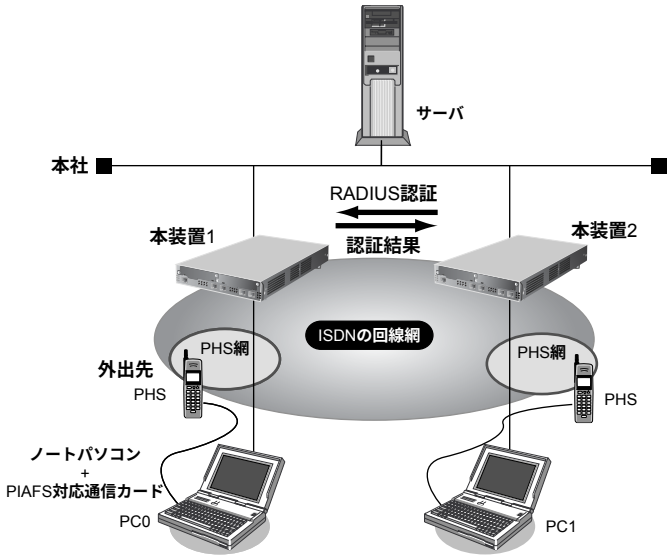
設定した内容が有効になります。

2.40.2　複数台の装置でリモートアクセスサーバを構成する

適用機種　*Si-R220B,220C,370,570*

RADIUS 機能を用いることで、アクセスユーザの情報を RADIUS サーバで一元管理し、複数のリモートアクセスサーバから同一のアクセスユーザ情報を利用できるようにすることができます。

ここでは、「2.40.1 1 台の装置でリモートアクセスサーバを構成する」（P.919）の構成から、さらにリモートアクセスサーバを増設し着信可能な回線数を増やす場合を例に説明します。



● 設定条件

[本装置 1]

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B、220C 以外）または ISDN U ポート（Si-R220B、220C）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- 以下からの着信を許可する

  [PC0＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 受諾認証 ID　：mobile-a
  - 受諾認証パスワード　：mobilepass-a
  - PHS の電話番号は未登録

  [PC1＜ノートパソコン＋ PHS ＞で外出先から接続]

  - 受諾認証 ID　：mobile-b
  - 受諾認証パスワード　：mobilepass-b
  - PHS の電話番号は未登録
- 本社の LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本社の LAN 側の IP アドレス　：192.168.1.1
- 外部のパソコンに割り当てる IP アドレス　：192.168.1.34、192.168.1.35
- 本装置に接続する RADIUS クライアントの IP アドレス　：192.168.1.2
- RADIUS 共有鍵　：rassharepass

[本装置 2]

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B、220C 以外）または ISDN U ポート（Si-R220B、220C）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- RADIUS サーバに問い合わせて着信を許可する
- 本社の LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本社の LAN 側の IP アドレス　：192.168.1.2
- 外部のパソコンに割り当てる IP アドレス　：192.168.1.36、192.168.1.37
- 本装置が問い合わせる RADIUS サーバの IP アドレス　：192.168.1.1
- RADIUS 共有鍵　：rassharepass

こんな事に気をつけて

- **1 台の本装置上で、RADIUS サーバ機能と RADIUS クライアント機能を併用することはできません。**
- **1 台の本装置上で、RADIUS サーバ機能を複数設定することはできません。**
- **RADIUS プロトコルの制約で、同時に認証およびアカウンティングが行える数は 256 です。同時に 257 以上の認証とアカウンティングを行った場合は、両方とも失敗します。**
- **本装置の RADIUS 機能は 4096 バイトを超える RADIUS のパケットを扱えません。RADIUS サーバ機能を用いる場合は、経路情報を大量に設定すると（たとえば AAA 情報のスタティック経路情報だけの場合は約 130 個）この上限を超えてしまい、パケットが送出できず RADIUS クライアント側で認証が失敗します。**
- **「AAA 情報」－「グループ ID 情報」－「AAA ユーザ情報」－「IP 関連」（「IPv6 関連」）－「スタティック経路情報」（「IPv6 スタティック経路情報」）で設定した優先度は RADIUS サーバ機能では伝達することはできません。**
- **「AAA 情報」－「グループ ID 情報」－「AAA ユーザ情報」－「IP 関連」－「IP 基本情報」で設定した自側 IP アドレスは RADIUS サーバ機能では伝達することはできません。**
- **RADIUS クライアント機能で受信した Framed-Route、Framed-IPv6-Route の情報は、優先度 100 の経路情報として扱われます。また、これらの経路情報を受け入れた結果、装置の経路数の上限を超えてしまう場合は回線は切断されます。**
- **RADIUS クライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAA グループに RADIUS クライアント機能とユーザ情報の両方を定義した場合、まず RADIUS で認証が行われます。RADIUS での認証が成功した場合はのユーザ情報は利用されませんが、RADIUS で認証に失敗した場合は、次にユーザ情報で認証を行います。**

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

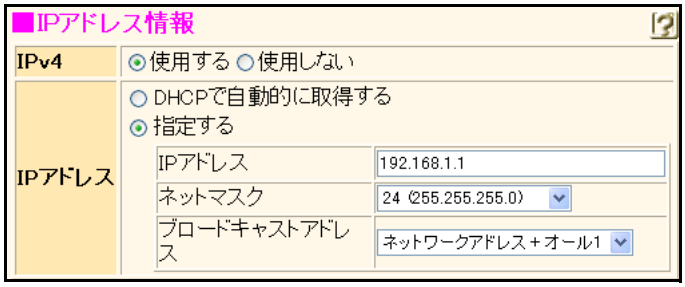
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.1.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1



5.　［保存］ボタンをクリックします。

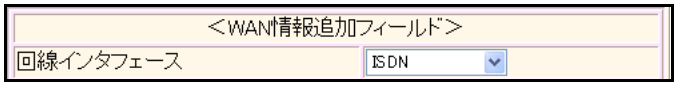
WAN0 情報を設定する

6.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- 回線インタフェース　→ISDN



8.　［追加］ボタンをクリックします。

「WAN1 情報（ISDN）」ページが表示されます。

9.　［保存］ボタンをクリックします。

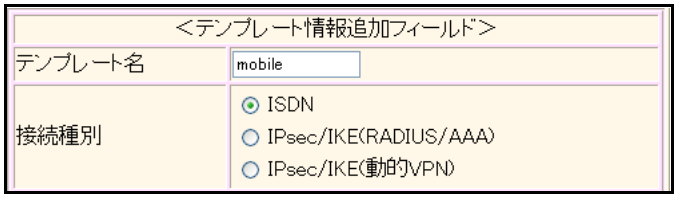
テンプレート情報を設定する

10.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

11.　以下の項目を指定します。

- テンプレート名　→mobile
- 接続先種別　→ISDN



機種により、接続先種別の表示が上記の画面とは異なります。

12.　［追加］ボタンをクリックします。

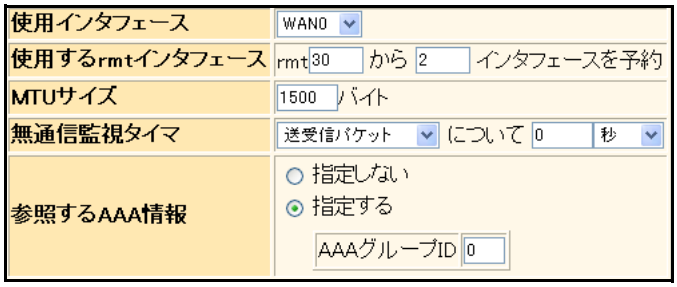
「テンプレート情報（mobile）」ページが表示されます。

13.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- 使用する rmt インタフェース　→rmt30 から 2 インタフェースを予約
- 参照する AAA 情報　→指定する
  AAA グループ ID　→0



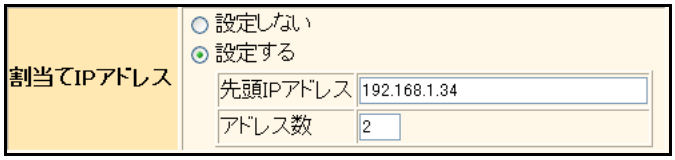
15.　［保存］ボタンをクリックします。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

17.　以下の項目を指定します。

- 割当て IP アドレス　→設定する
  先頭 IP アドレス　→192.168.1.34
  アドレス数　→2



18.　［保存］ボタンをクリックします。

19.　設定メニューのルータ設定で「AAA 情報」をクリックします。

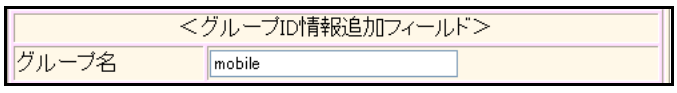
「AAA 情報」ページが表示されます。

20.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

21.　以下の項目を指定します。

- グループ名　→mobile



22.　［追加］ボタンをクリックします。

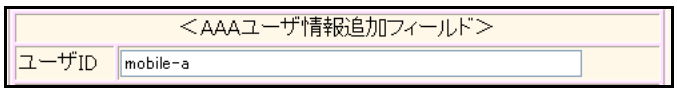
「グループ ID 情報（0）」と設定項目が表示されます。

23.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

24.　以下の項目を指定します。

- ユーザ ID　→mobile-a

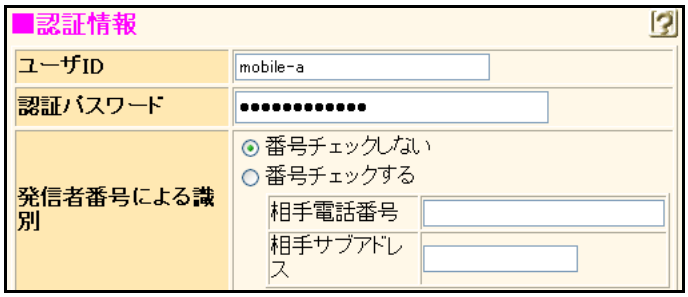


25.　［追加］ボタンをクリックします。

「AAA ユーザ情報（0）」と「認証情報」が表示されます。

26.　以下の項目を指定します。

- ユーザ ID　→mobile-a
- 認証パスワード　→mobilepass-a
- 発信者番号による識別　→番号チェックしない



27.　［保存］ボタンをクリックします。

28.　手順 26. ～ 27. を参考に、以下の項目を指定します。

- ユーザ ID　→mobile-b
- 認証パスワード　→mobilepass-b

RADIUS サーバを設定する

29.　設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

30.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

31.　「グループ ID 情報」でグループ ID が 0 の［修正］ボタンをクリックします。

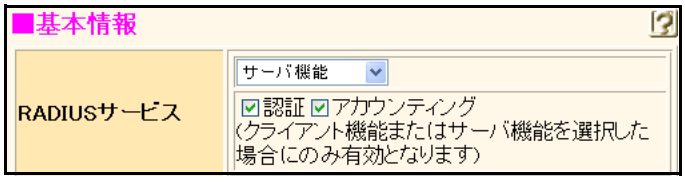
「グループ ID 情報（0）」と設定項目が表示されます。

32.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

33.　以下の項目を指定します。

- RADIUS サービス　→サーバ機能
  認証　→チェックする
  アカウンティング　→チェックする



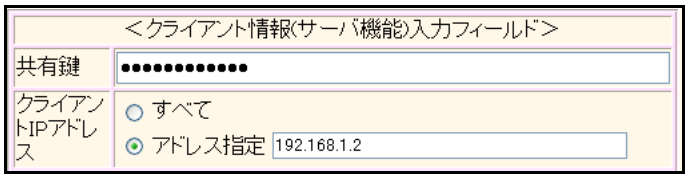
34.　［保存］ボタンをクリックします。

35.　「クライアント情報」をクリックします。

「クライアント情報（サーバ機能）」ページが表示されます。

36.　以下の項目を指定します。

- 共有鍵　→rassharepass
- クライアント IP アドレス　→アドレス指定
  →192.168.1.2



37.　［追加］ボタンをクリックします。

38.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

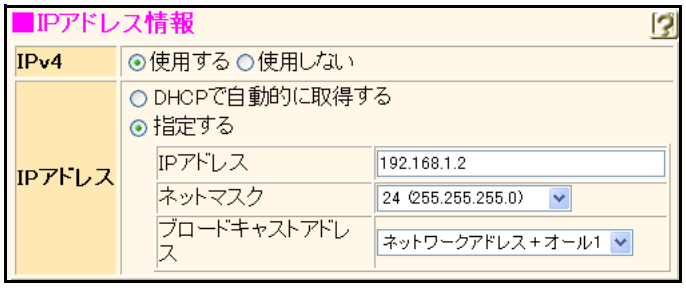
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→192.168.1.2
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

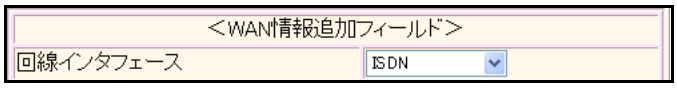
WAN0 情報を設定する

6.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- 回線インタフェース　→ISDN



8.　［追加］ボタンをクリックします。

「WAN1 情報（ISDN）」ページが表示されます。

9.　［保存］ボタンをクリックします。

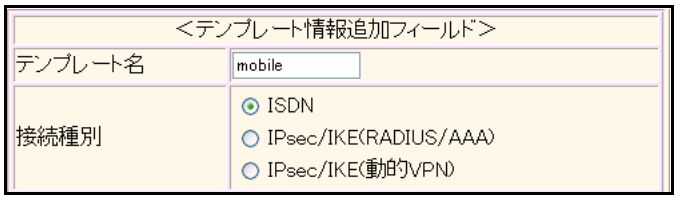
テンプレート情報を設定する

10.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

11.　以下の項目を指定します。

- テンプレート名　→mobile
- 接続先種別　→ISDN



機種により、接続先種別の表示が上記の画面とは異なります。

12.　［追加］ボタンをクリックします。

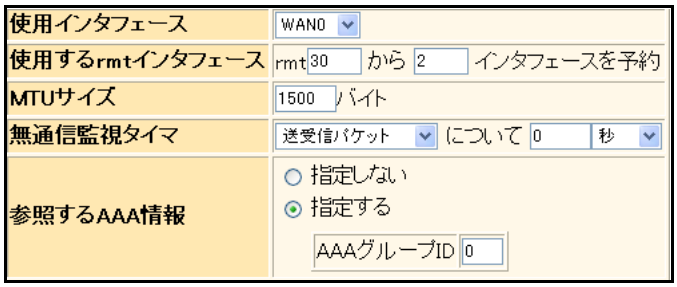
「テンプレート情報（mobile）」ページが表示されます。

13.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- 使用する rmt インタフェース　→rmt30 から 2 インタフェースを予約
- 参照する AAA 情報　→指定する
  AAA グループ ID　→0



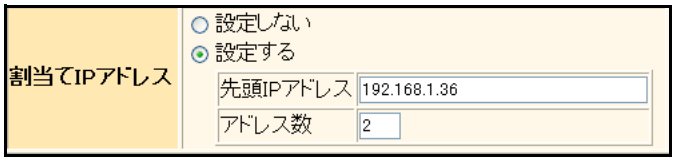
15.　［保存］ボタンをクリックします。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

17.　以下の項目を指定します。

- 割当て IP アドレス　→設定する
  先頭 IP アドレス　→ 192.168.1.36
  アドレス数　→ 2



18.　［保存］ボタンをクリックします。

RADIUS クライアントを設定する

19.　設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

20.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

21.　「グループ ID 情報」でグループ ID が 0 の［修正］ボタンをクリックします。

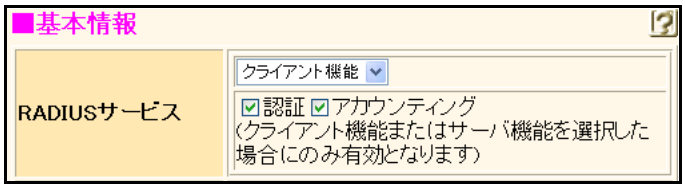
「グループ ID 情報（0）」と設定項目が表示されます。

22.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

23.　以下の項目を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックする



24.　［保存］ボタンをクリックします。

25.　「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

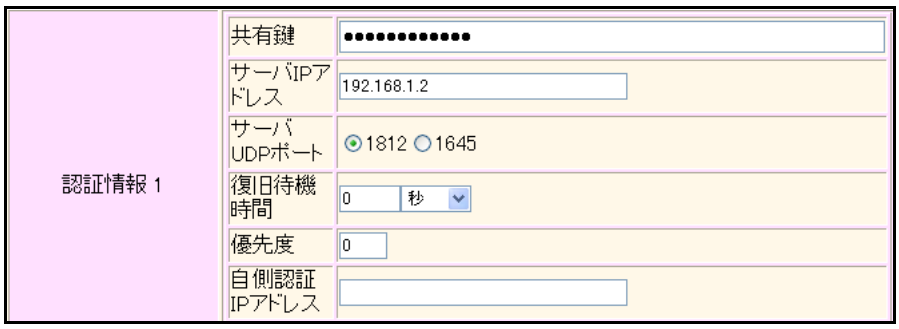
26.　認証情報 1 の［修正］ボタンをクリックします。

27.　以下の項目を指定します。

- 認証情報 1

  共有鍵　→rassharepass

  サーバ IP アドレス　→192.168.1.2



28.　認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

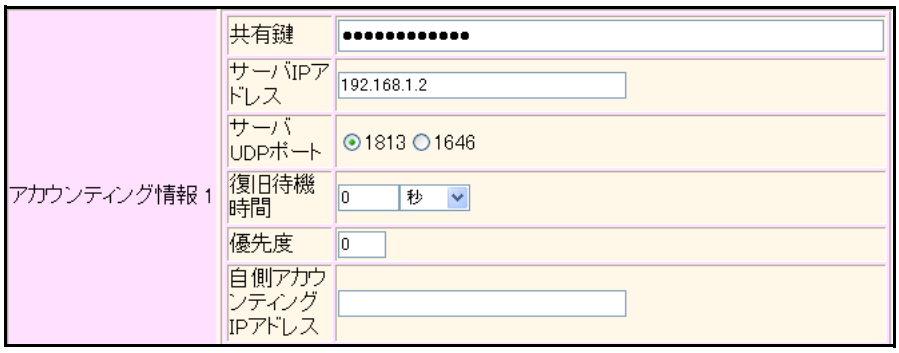
29.　アカウンティング情報 1 の［修正］ボタンをクリックします。

30.　以下の項目を指定します。

- アカウンティング情報 1

  共有鍵　→rassharepass

  サーバ IP アドレス　→192.168.1.2



31.　アカウンティング情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

32.　画面左側の［設定反映］ボタンをクリックします。

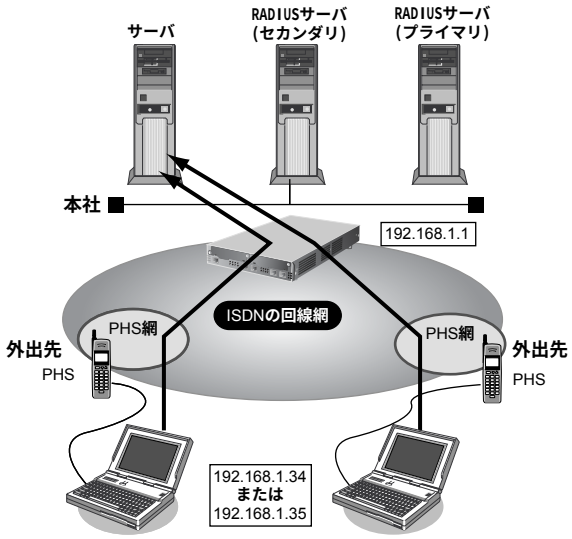
設定した内容が有効になります。

2.40.3　リモートアクセスサーバが使用する RADIUS サーバを多重化する

適用機種　*Si-R220B,220C,370,570*

RADIUS 機能を用いて、複数台の RADIUS サーバを使用することで、RADIUS サーバの信頼性を向上させることができます

ここでは、「2.40.1 1 台の装置でリモートアクセスサーバを構成する」（P.919）の構成から、さらにリモートアクセスサーバを増設し着信可能な回線数を増やす場合を例に説明します。



着信時にプール内で使用していないIPアドレスが割り当てられる

● 設定条件

[本装置]

- SLOT0 に装着した BRI 拡張モジュール L2（Si-R220B、220C 以外）または ISDN U ポート（Si-R220B、220C）を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース　：rmt30 から 2 個
- 本社の LAN 側のネットワークアドレス／ネットマスク　：192.168.1.0/24
- 本社の LAN 側の IP アドレス　：192.168.1.1
- RADIUS 認証サーバ（プライマリ）の IP アドレス　: 192.168.1.2
- RADIUS 認証サーバ（プライマリ）の共有鍵　: rassharepass
- RADIUS 認証サーバ（セカンダリ）の IP アドレス　: 192.168.1.3
- RADIUS 認証サーバ（セカンダリ）の共有鍵　: rassharepass
- RADIUS アカウンティングサーバ（プライマリ）の IP アドレス : 192.168.1.2
- RADIUS アカウンティングサーバ（プライマリ）の共有鍵　: rassharepass
- RADIUS アカウンティングサーバ（セカンダリ）の IP アドレス : 192.168.1.3
- RADIUS アカウンティングサーバ（セカンダリ）の共有鍵　: rassharepass

RADIUS サーバに登録する情報（プライマリ、セカンダリ共、共通）

[PC0<ノートパソコン+PHS>で外出先から接続]

- 認証ユーザ ID　mobile-a
- 認証ユーザパスワード　mobilepass-a

[PC1<ノートパソコン+PHS>で外出先から接続]

- 認証ユーザ ID　mobile-b
- 認証ユーザパスワード　mobilepass-b

こんな事に気をつけて

- テンプレート着信で使用するインタフェースはテンプレート専用になりますので、範囲に含まれる rmt インタフェースには remote 定義を設定しないでください。
  例：rmt30 から rmt47 をテンプレートで予約した場合、remote 30 から remote 47 までの remote 定義に対して設定を行わないでください。
- テンプレート着信で使用するインタフェースの個数分、接続先情報定義をあけておく必要があります。
  例：接続先定義を最大 48 定義可能な装置で、10 インタフェースをテンプレートで使用する場合、接続先定義の定義数は 38 定義までにしてください。
- テンプレート情報内で設定されている定義の中で、RADIUS サーバのユーザ側にも同じ項目の定義が存在する場合は、RADIUS サーバでの設定値が適用されます。
  RADIUS サーバで未登録の項目に対しては、テンプレート情報の設定値が適用されます。

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

LAN0 情報を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

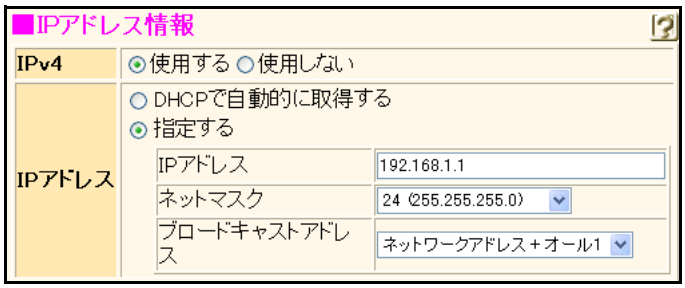
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.1.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス + オール 1



5.　［保存］ボタンをクリックします。

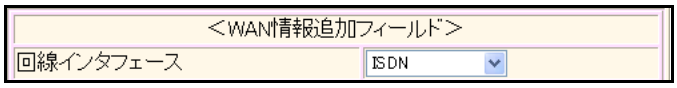
WAN0 情報を設定する

6.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- 回線インタフェース　→ISDN



8.　［追加］ボタンをクリックします。

「WAN1 情報（ISDN）」ページが表示されます。

9.　［保存］ボタンをクリックします。

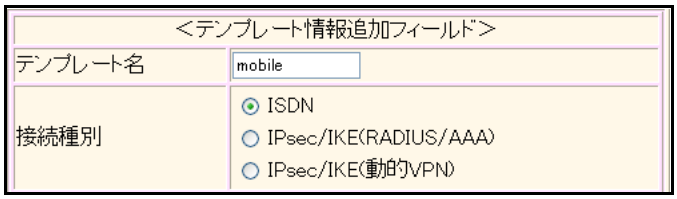
テンプレート情報を設定する

10.　設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

11.　以下の項目を指定します。

- テンプレート名　→mobile
- 接続先種別　→ISDN



機種により、接続先種別の表示が上記の画面とは異なります。

12.　［追加］ボタンをクリックします。

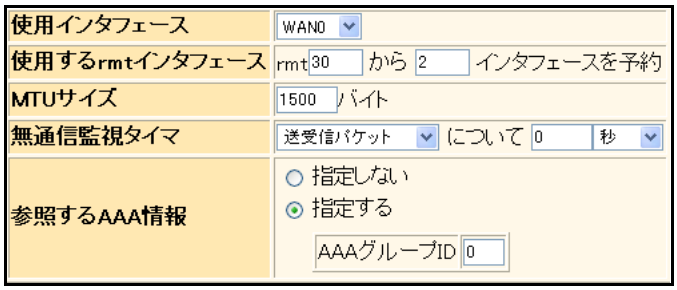
「テンプレート情報（mobile）」ページが表示されます。

13.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14.　以下の項目を指定します。

- 使用インタフェース　→WAN0
- 使用する rmt インタフェース　→rmt30 から 2 インタフェースを予約
- 参照する AAA 情報　→指定する
  AAA グループ ID　→0



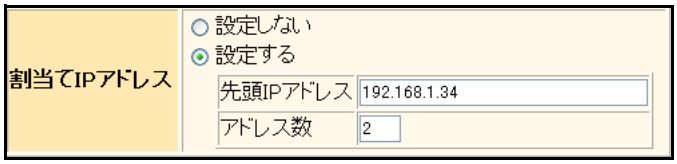
15.　［保存］ボタンをクリックします。

16.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

17.　以下の項目を指定します。

- 割当て IP アドレス　→設定する
  先頭 IP アドレス　→ 192.168.1.34
  アドレス数　→ 2



18.　［保存］ボタンをクリックします。

19.　設定メニューのルータ設定で「AAA 情報」をクリックします。

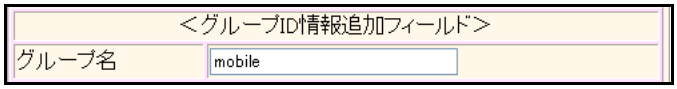
「AAA 情報」ページが表示されます。

20.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

21.　以下の項目を指定します。

- グループ名　→ mobile



22.　［追加］ボタンをクリックします。

「グループ ID 情報（0）」と設定項目が表示されます。

RADIUS サーバを設定する

23.　グループ ID の設定項目の「RADIUS 関連」をクリックします。

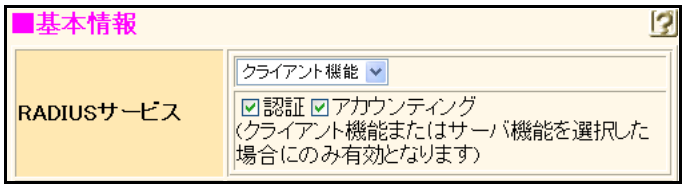
「RADIUS 基本情報」項目と「RADIUS 情報」項目が表示されます。

24.　RADIUS 関連の設定項目の「基本情報」をクリックします。

「RADIUS 基本情報」ページが表示されます。

25.　以下の項目を指定します。

- RADIUS サービス　→クライント機能
  認証　→チェックする
  アカウンティング　→ チェックする



26.　［保存］ボタンをクリックします。

27.　「サーバ情報」をクリックします。

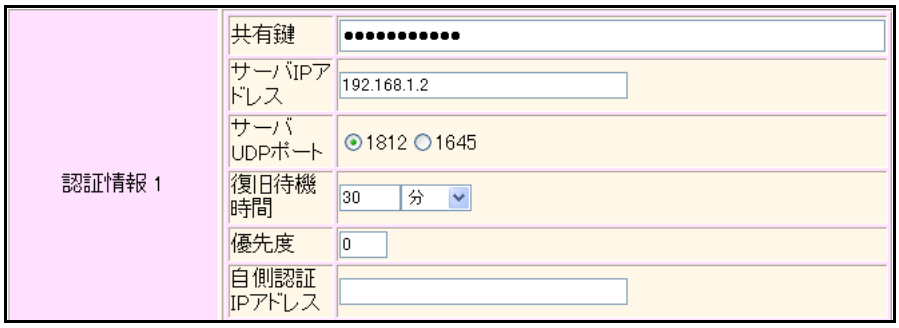
「サーバ情報（クライアント機能）」が表示されます。

28.　認証情報 1 の［修正］ボタンをクリックします。

29.　以下の項目を指定します。

- 認証情報 1

共有鍵	→192.168.2.1
サーバ IP アドレス	→192.168.1.2
復旧待機時間	→30 分
優先度	→0



30.　認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

31.　認証情報 2 の［修正］ボタンをクリックします。

32.　以下の項目を指定します。

- 認証情報 2

共有鍵	→192.168.2.1
サーバ IP アドレス	→192.168.1.3
復旧待機時間	→30 分
優先度	→100

33.　認証情報 2 の［保存］ボタンをクリックします。

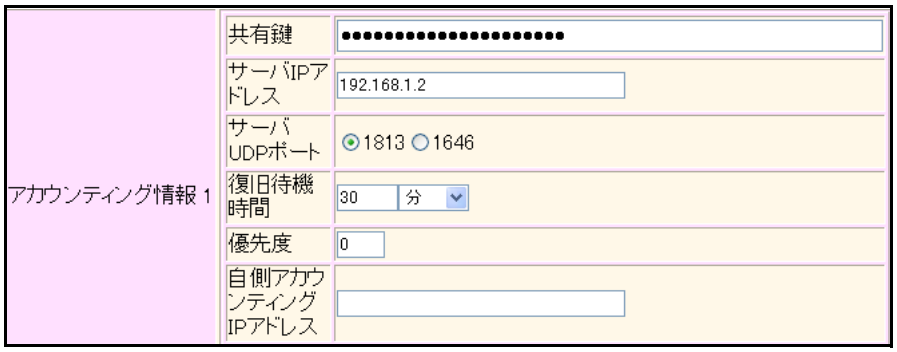
「サーバ情報（クライアント機能）に戻ります。

34.　アカウンティング情報 1 の［修正］ボタンをクリックします。

35.　以下の項目を指定します。

- アカウンティング情報 1

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.1.2
  復旧待機時間　→ 30 分
  優先度　→ 0



36.　アカウンティング情報 1 の［保存］ボタンをクリックします。

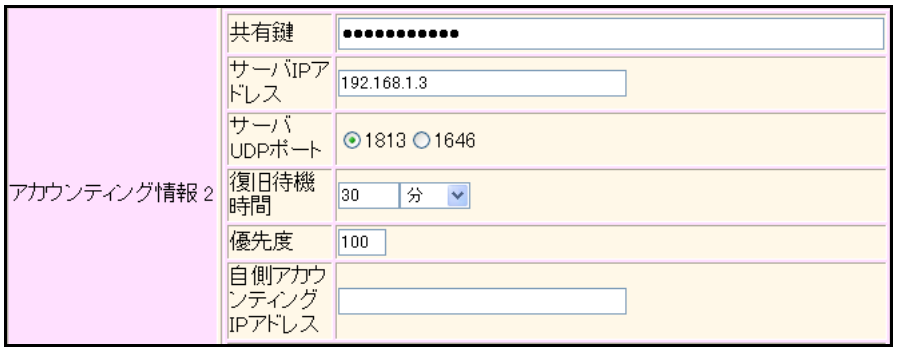
「サーバ情報（クライアント機能）」に戻ります。

37.　アカウンティング情報 2 の［修正］ボタンをクリックします。

38.　以下の項目を指定します。

- アカウンティング情報 2

  共有鍵　→ 192.168.2.1
  サーバ IP アドレス　→ 192.168.1.3
  復旧待機時間　→ 30 分
  優先度　→ 100



39.　アカウンティング情報 2 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

40.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.41 スイッチポートを使う

適用機種 ***Si-R180,180B***

本装置ではLAN1 側のポートをスイッチングHUBとして使用するか、従来の単独ポートとして使用するかを構成定義により選択できます。また、スイッチングHUBとして使用する場合はVLAN 機能を併用することでスイッチポート（SW1～4）を独立ポートとして使用することもできます。

本装置のスイッチポートでは以下のような形態が利用できます。

- スイッチポートをHUBとして使用する
  以下の2つ方法で使用できます。
  - VLANヘッダを含む場合は、一致するVLAN IDのみ転送を行う
    VLANを使用しない場合、またはVLANを使用する場合でVLAN IDに応じた転送を行うときに選択します。

    ☛ 参照 「2.41.1 スイッチポートをHUBとして使用する」（P.940）

  - VLANヘッダに依存しないで、MACアドレスのみでスイッチポート間の転送を行う
    VLANを使用していてVLANヘッダごと転送する場合、またはブリッジ機能をVLANタグ転送モードで使用する場合に選択します。

    ☛ 参照 「2.41.2 VLAN 透過モードを使用する」（P.944）

- スイッチポートを独立した4ポートとして使用する
  スイッチポートをすべて別のインタフェースとして使用する場合に選択します。

  ☛ 参照 「2.41.3 スイッチポートを独立ポートとして使用する」（P.947）

- スイッチポートを独立した2ポートずつに分割して使用する
  スイッチポートをすべて別のインタフェースとして使用する場合に選択します。

  ☛ 参照 「2.41.4 スイッチポートを分割して使用する」（P.952）

こんな事に気をつけて

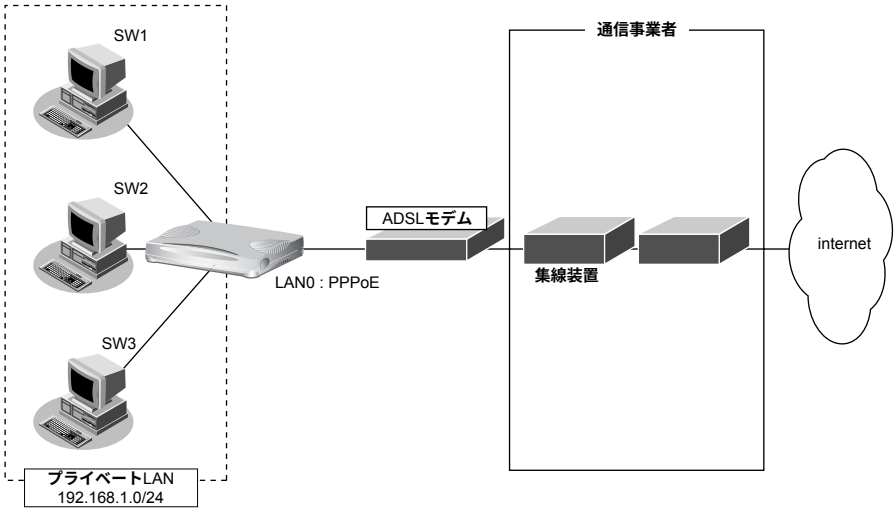
- **本装置のスイッチポートのMTUは1532バイトです。EoMPLSなどのトンネルプロトコルを利用する場合はMTUをスイッチポートのMTUサイズ以下になるように設定するか、スイッチポートを無効にし、使用するパケットの最大長の転送が可能な外付けのスイッチを使用してください。**
- **スイッチポートを使用しかつVLAN透過モードを使用しない場合は、LAN定義をVLANとして定義します。そのため、VLANを使用した場合と同じ注意事項が適用されます。スイッチポートを使用する前に必ず「VLAN機能」に関する記述を確認してください。**

  ☛ 参照 「2.12 VLAN機能を使う」（P.372）

2.41.1　スイッチポートを HUB として使用する

適用機種　*Si-R180,180B*

接続するスイッチポートを HUB としてインターネットに接続する場合の設定方法を説明します。



ここでは以下の条件によって、PPPoE を利用したインターネットとの接続が設定されていることを前提とします。

参照 「1.6 インターネットへ PPPoE で接続する」（P.67）

● 前提条件

- LAN0 側の PPPoE 設定は完了している
- LAN1 設定がない

● 設定条件

[通信事業者側]

- ユーザ認証 ID　：userid（プロバイダから提示された内容）
- ユーザ認証パスワード　：userpass（プロバイダから提示された内容）
- LAN0 ポートを使用する

[プライベート LAN 側]

- LAN1 側をスイッチポートとして使用する
- ローカルネットワークでは VLAN は使用しない
- ローカルネットワークでは DHCP サーバを使用し、パソコンに割り当てるアドレスは 192.168.1.2 から 64 個用意する
- 本装置の IP アドレス　：192.168.1.1
- ネットワークアドレス/ネットマスク　：192.168.1.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューのルータ設定で「スイッチ情報」をクリックします。

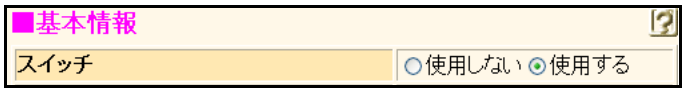
「スイッチ情報」ページが表示されます。

2.　「基本情報」をクリックします。

「基本情報」が表示されます。

3.　以下の項目を指定します。

- スイッチ　→使用する



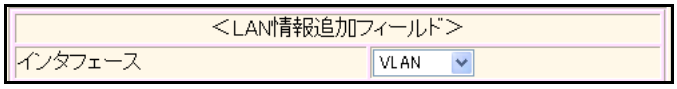
4.　［保存］ボタンをクリックします。

5.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

6.　以下の項目を指定します。

- インタフェース　→VLAN



7.　［追加］ボタンをクリックします。

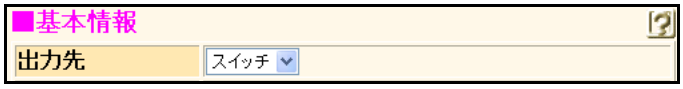
「LAN1 情報（VLAN）」ページが表示されます。

8.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- 出力先　→スイッチ



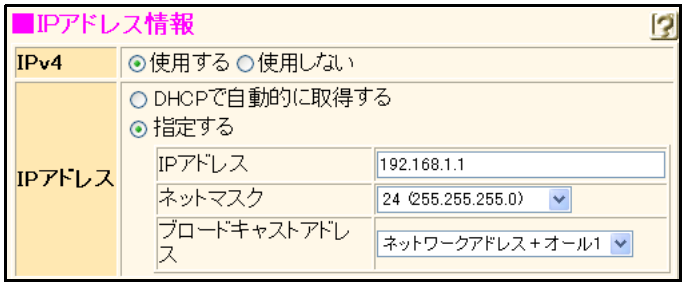
10.　［保存］ボタンをクリックします。

11.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

12.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→192.168.1.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



13.　［保存］ボタンをクリックします。

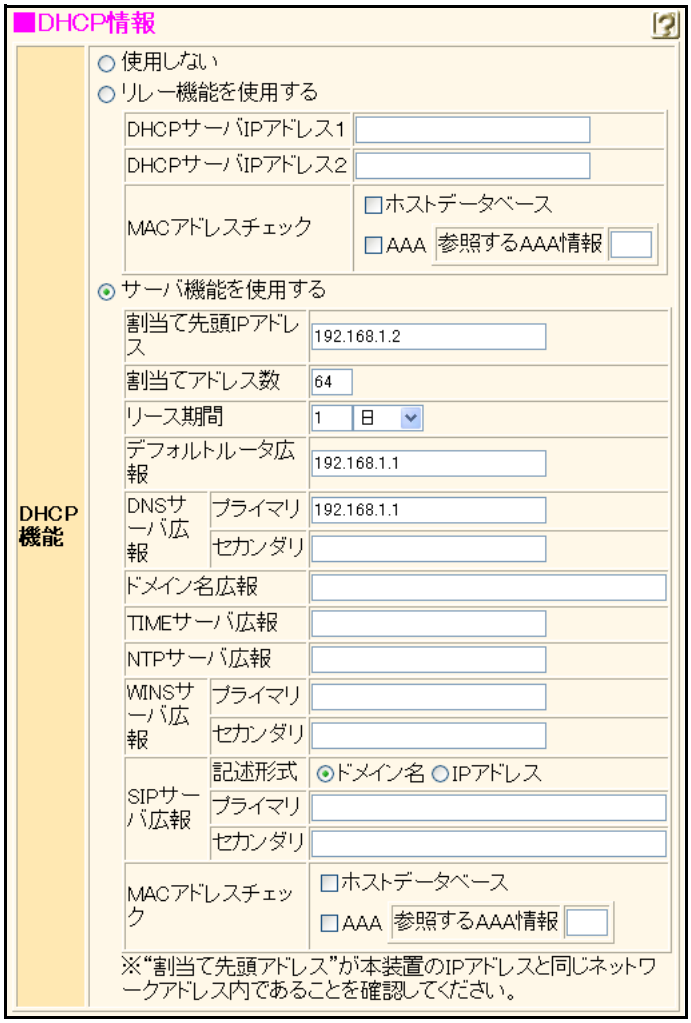
14.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

15.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.1.2
  割り当てアドレス数　→ 64
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.1.1
  DNS サーバ広報
  プライマリ　→ 192.168.1.1
  セカンダリ　→指定しない

補足　DHCP サーバ機能で割り当てることのできる最大数は 253 です。



16.　［保存］ボタンをクリックします。

17.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

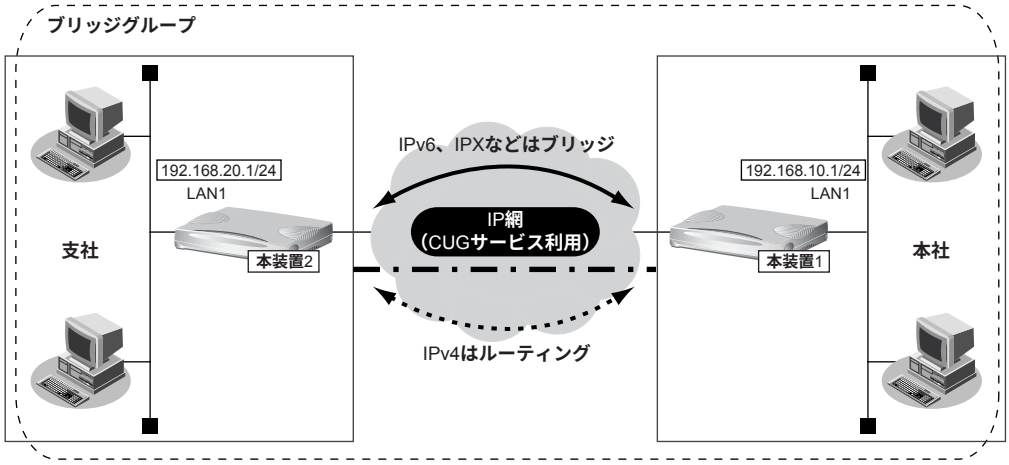
- 本装置では VLAN ID の設定を省略した場合、VLAN ID として 1 が設定されたものとして動作します。
- 設定されたタグなし VLAN ID と同じ VLAN タグが付加されたパケットは、タグなし VLAN からパケットを受信したものとして処理されます。タグなし VLAN ID とネットワークで使用しているタグ付き VLAN ID が一致しないよう VLAN ID を設定してください。詳細については、「Si-R シリーズ　Web リファレンス」を参照してください。

2.41.2 VLAN 透過モードを使用する

適用機種 ***Si-R180,180B***

VLAN 透過モードを使用すると、VLAN を使用しているネットワークで VLAN ヘッダも含めてスイッチングすることができます。

VLAN 透過モードを使用する場合の設定方法を説明します。



● 前提条件

- IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG（Closed Users Group）サービスを利用する

[本社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN1 ポートに設定）　：192.168.10.1/24
- PPPoE ユーザ認証 ID　：userid1@groupname
- PPPoE ユーザ認証パスワード　：userpass1
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

[支社（PPPoE 常時接続)]

- 払い出される IPv4 アドレス（LAN1 ポートに設定）　：192.168.20.1/24
- PPPoE ユーザ認証 ID　：userid2@groupname
- PPPoE ユーザ認証パスワード　：userpass2
- PPPoE LAN ポート　：LAN0 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

- 自側エンドポイントアドレス　：192.168.10.1
- 相手側エンドポイントアドレス　：192.168.20.1

[支社]

- 自側エンドポイントアドレス　：192.168.20.1
- 相手側エンドポイントアドレス　：192.168.10.1

[本社、支社共通]

- ブリッジ対象インタフェース　：LAN0 ポートと IP トンネル
- IPv4 の転送方式　：ルーティングで転送
- IPv6 の転送方式　：ブリッジで転送

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

1.　設定メニューのルータ設定で「スイッチ情報」をクリックします。

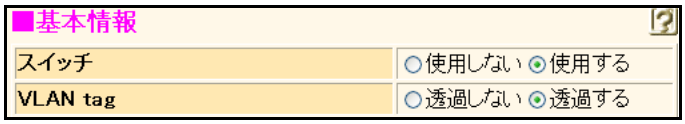
「スイッチ情報」ページが表示されます。

2.　「基本情報」をクリックします。

「基本情報」が表示されます。

3.　以下の項目を指定します。

- スイッチ　→使用する
- VLAN tag　→透過する



4.　[保存] ボタンをクリックします。

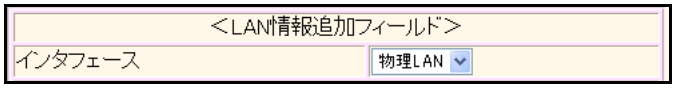
5.　「2.33.3 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ）」（P.862）の手順 1. ～ 10. を参考に、PPPoE および IPv4 トンネルを設定します。

6.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- インタフェース　→物理 LAN



8.　[追加] ボタンをクリックします。

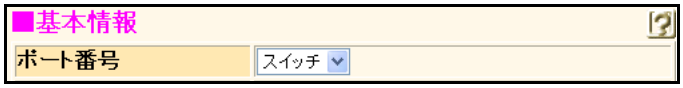
「LAN1 情報（物理 LAN）」ページが表示されます。

9.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

10.　以下の項目を指定します。

- ポート番号　→スイッチ



11.　[保存] ボタンをクリックします。

12. **「2.33.3 IP トンネルで事業所間をブリッジ接続する（Ethernet over IP ブリッジ）」（P.862）の手順 13. ～ 26. を参考に、ブリッジ情報を設定します。**

13. **画面左側の［再起動］ボタンをクリックします。**

設定した内容が有効になります。

支社を設定する

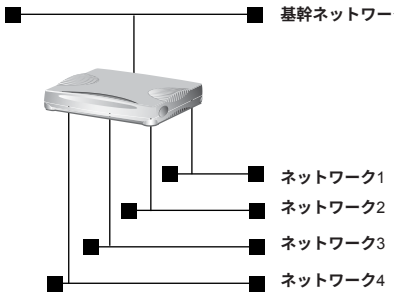
「本社を設定する」を参考に、支社を設定します。

この例では、LAN 側の IP アドレス、PPPoE の接続先情報（認証情報）、IPv4 トンネルのエンドポイントアドレス以外は、本社とすべて同じです。

2.41.3　スイッチポートを独立ポートとして使用する

適用機種　*Si-R180,180B*

スイッチポートをそれぞれ独立したLANポートとして使用する場合の設定方法を説明します。



● 設定条件

[基幹ネットワーク側]

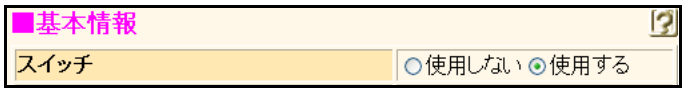
- 本装置のIPアドレス　：10.200.100.1
- 本装置のネットワークアドレス/ネットマスク　：10.200.100.0/24
- ルーティング制御としてRIP（Version2）を使う

[ネットワーク1～4側]

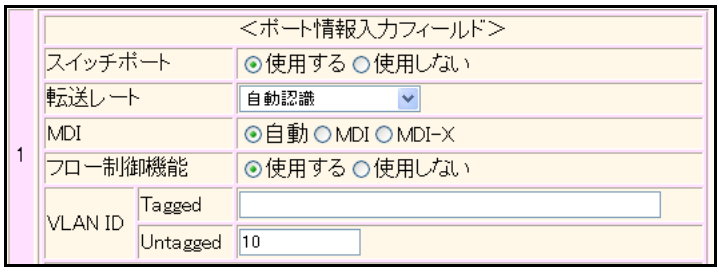
- 本装置のIPアドレスは以下のとおり
  ネットワーク1　：192.168.1.1
  ネットワーク2　：192.168.2.1
  ネットワーク3　：192.168.3.1
  ネットワーク4　：192.168.4.1
- 本装置のネットワークアドレスおよびネットマスクは以下のとおり
  ネットワーク1　：192.168.1.0/24
  ネットワーク2　：192.168.2.0/24
  ネットワーク3　：192.168.3.0/24
  ネットワーク4　：192.168.4.0/24
- ネットワーク1～4ではVLANタグは使用しない
- ネットワーク1～4に対して、タグなしVLAN IDとしてそれぞれ10～13を割り当てる
- ネットワーク1～4ではDHCPサーバ機能を使用する
- ネットワーク1～4はそれぞれSW1～SW4ポートを使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

1. **設定メニューのルータ設定で「スイッチ情報」をクリックします。**
   「スイッチ情報」ページが表示されます。
2. **「基本情報」をクリックします。**
   「基本情報」が表示されます。
3. **以下の項目を指定します。**
   - スイッチ　→使用する



4. **［保存］ボタンをクリックします。**
5. **スイッチ情報の設定項目の「ポート情報」をクリックします。**
   「ポート情報」が表示されます。
6. **ポート 1 の［修正］ボタンをクリックします。**
   「ポート情報」ページが表示されます。
7. **以下の項目を指定します。**
   - VLAN ID
     Untagged　→ 10



8. **［保存］ボタンをクリックします。**
9. **手順 6. ～ 8. を参考に、ポート 2 ～ 4 をそれぞれ VLAN ID 11 ～ 13 に設定します。**
10. **設定メニューのルータ設定で「LAN 情報」をクリックします。**
    「LAN 情報」ページが表示されます。
11. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**
    「LAN0 情報（物理 LAN）」ページが表示されます。
12. **「IP 関連」をクリックします。**
    IP 関連の設定項目と「IP アドレス情報」が表示されます。

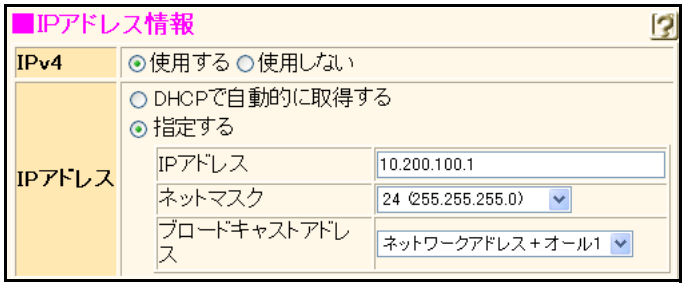
13.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する

  IPアドレス　→10.200.100.1

  ネットマスク　→24（255.255.255.0）

  ブロードキャストアドレス　→ネットワークアドレス＋オール1



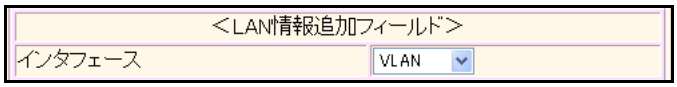
14.　［保存］ボタンをクリックします。

15.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

16.　以下の項目を指定します。

- インタフェース　→VLAN



17.　［追加］ボタンをクリックします。

「LAN1 情報（VLAN）」ページが表示されます。

18.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

19.　以下の項目を指定します。

- 出力先　→スイッチ
- VLAN ID　→10

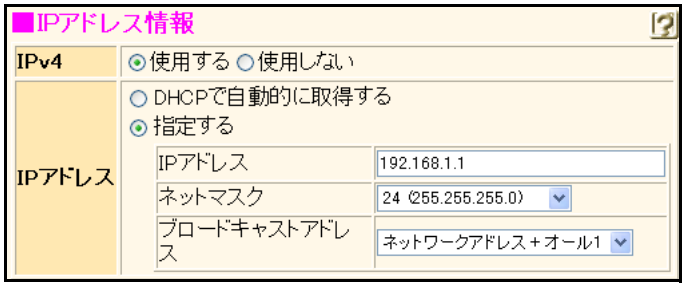
20.　［保存］ボタンをクリックします。

21.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

22.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.1.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1



23.　［保存］ボタンをクリックします。

24.　「2.41.1 スイッチポートを HUB として使用する」（P.940）の手順 14. ～ 16. を参考に、以下の項目を設定します。

- DHCP 機能　→サーバ機能
- 割当て先頭 IP アドレス　→192.168.130.2
- 割当てアドレス数　→64
- リース期間　→1 日
- デフォルトルータ広報　→192.168.130.1
- DNS サーバ広報　→10.200.100.10

25.　手順 15. ～ 23. を参考に、以下の項目を設定します。

「LAN2 情報（VLAN）」-「共通情報」

「基本情報」

- 出力先　→スイッチ
- VLAN ID　→11

「LAN2 情報（VLAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→192.168.2.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1

「LAN3 情報（VLAN）」-「共通情報」

「基本情報」

- 出力先　→スイッチ
- VLAN ID　→12

「LAN3 情報（VLAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.3.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN4 情報（VLAN）」-「共通情報」

「基本情報」

- 出力先　→スイッチ
- VLAN ID　→ 13

「LAN4 情報（VLAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.4.1
  ネットマスク　→ 24（255.255.255.0）

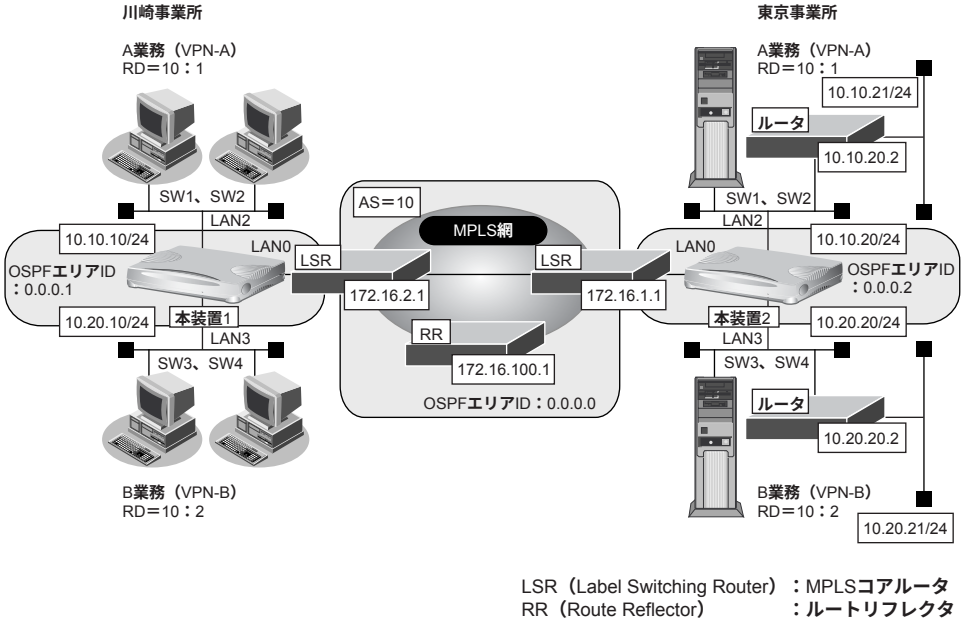
26.　画面左側の［再起動］ボタンをクリックします。

設定した内容が有効になります。

2.41.4 スイッチポートを分割して使用する

適用機種 ***Si-R180,180B***

4 つのスイッチポートを 2 ポートずつに分割して使用する場合の設定方法を説明します。



LSR（Label Switching Router）：MPLSコアルータ
RR（Route Reflector）：ルートリフレクタ

● 設定条件

- MPLS 網の使用条件
  BGP AS 番号　：10
  RR の IP アドレス　：172.16.100.1
  MPLS 網で使用する IPv4 ネットワーク　：OSPF
  　：バックボーンエリア
- VPN-A の使用条件
  ルート識別子　：10:1
  使用するネットワーク　：10.10.10/24 川崎事業所
  　：10.10.20/24 東京事業所
  　：10.10.21/24 東京事業所
- VPN-B の使用条件
  ルート識別子　：10:2
  使用するネットワーク　：10.20.10/24 川崎事業所
  　：10.20.20/24 東京事業所
  　：10.20.21/24 東京事業所

[本装置 1]

- スイッチポートを事業所内ネットワークの接続ポートとして使用する
- 川崎事業所のネットワークでは VLAN タグを使用しない
- スイッチポートの 2 ポートずつを異なるネットワークとし、VLAN ID、LAN 定義およびネットワークアドレスを以下のように対応付ける
  - SW1、SW2
    VLAN ID：2　　LAN 定義：LAN1　　ネットワークアドレス：10.10.10.0/24
  - SW3、SW4
    VLAN ID：3　　LAN 定義：LAN2　　ネットワークアドレス：10.20.10.0/24

- LAN0 の IP アドレス　：172.16.2.2
- LAN1 の IP アドレス　：10.10.10.1
- LAN2 の IP アドレス　：10.20.10.1
- LAN0 ～ 2 では、NAT 機能および DHCP クライアント機能は使用しない
- ループバックインタフェースの IP アドレス　：10.1.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.1
- LAN0 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN2 で使用する VPN　：VPN-A
- LAN3 で使用する VPN　：VPN-B

[本装置 2]

- スイッチポートを事業所内ネットワークの接続ポートとして使用する
- 川崎事業所のネットワークでは VLAN タグを使用しない
- スイッチポートの 2 ポートずつを異なるネットワークとし、VLAN ID、LAN 定義およびネットワークアドレスを以下のように対応付ける
  - SW1、SW2
    VLAN ID：2　LAN 定義：LAN1　ネットワークアドレス：10.10.20.0/24
  - SW3、SW4
    VLAN ID：3　LAN 定義：LAN2　ネットワークアドレス：10.20.20.0/24
- LAN0 の IP アドレス　：172.16.1.2
- LAN1 の IP アドレス　：10.10.20.1
- LAN2 の IP アドレス　：10.20.20.1
- LAN0 ～ 2 では、NAT 機能および DHCP サーバ／クライアント機能は使用しない
- ループバックインタフェースの IP アドレス　：10.2.1.1
- ループバックインタフェースでのルーティングプロトコル　：OSPF
- ループバックインタフェースでの OSPF エリア ID　：0.0.0.2
- LAN0 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN1 で使用する VPN　：VPN-A
- LAN1 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.10.21.0/24
  中継ルータアドレス　：10.10.20.2
- LAN2 で使用する VPN　：VPN-B
- LAN2 で使用する BGP/MPLS VPN スタティック経路情報
  あて先 IP アドレス　：10.20.21.0/24
- 中継ルータアドレス　：10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューのルータ設定で「スイッチ情報」をクリックします。

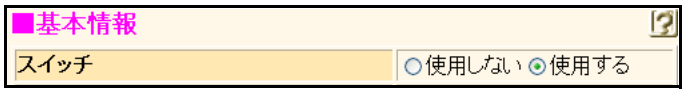
「スイッチ情報」ページが表示されます。

2.　「基本情報」をクリックします。

「基本情報」が表示されます。

3.　以下の項目を指定します。

- スイッチ　→使用する



4.　［保存］ボタンをクリックします。

5.　スイッチ情報の設定項目の「ポート情報」をクリックします。

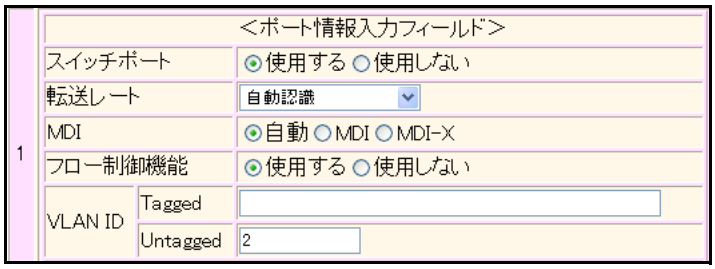
「ポート情報」が表示されます。

6.　ポート 1 の［修正］ボタンをクリックします。

「ポート情報」ページが表示されます。

7.　以下の項目を指定します。

- VLAN ID
  Untagged　→2



8.　［保存］ボタンをクリックします。

9.　手順 6.～8. を参考に、ポート 2、3 を VLAN ID 2 に、ポート 4 を VLAN ID 3 に設定します。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

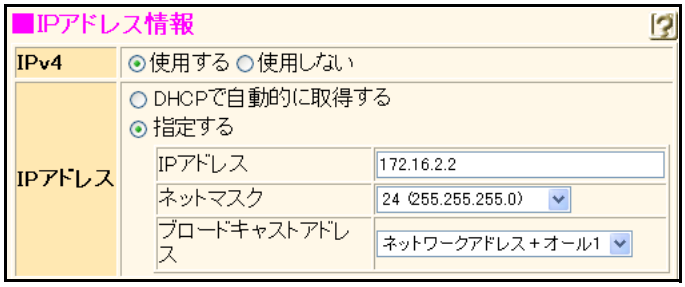
13.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する

  IPアドレス　→172.16.2.2

  ネットマスク　→24（255.255.255.0）

  ブロードキャストアドレス　→ネットワークアドレス＋オール1



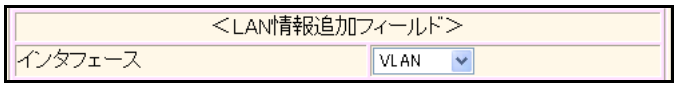
14.　［保存］ボタンをクリックします。

15.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

16.　以下の項目を指定します。

- インタフェース　→VLAN



17.　［追加］ボタンをクリックします。

「LAN1 情報（VLAN）」ページが表示されます。

18.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

19.　以下の項目を指定します。

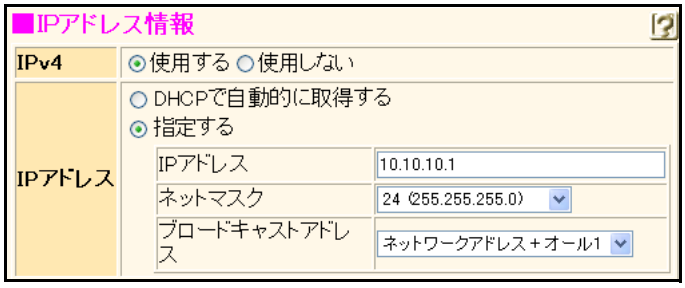
- 出力先　→スイッチ
- VLAN ID　→2

20.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

21.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→10.10.10.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1



22.　［保存］ボタンをクリックします。

23.　手順 15.～22. を参考に、以下の項目を設定します。

「LAN2 情報（VLAN）」-「共通情報」

「基本情報」

- 出力先　→スイッチ
- VLAN ID　→3

「LAN2 情報（VLAN）」-「IP 関連」

「IP アドレス情報」

- IPv4　→使用する
- IPアドレス　→指定する
  IPアドレス　→10.20.10.1
  ネットマスク　→24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール1

24.　「2.9.1 MPLS 網と LAN を使用して接続する」（P.322）を参考に、ループバック情報、OSPF 機能、MPLS 機能、ルートリフレクタ機能、VRF 情報を設定します。

25.　画面左側の［再起動］ボタンをクリックします。

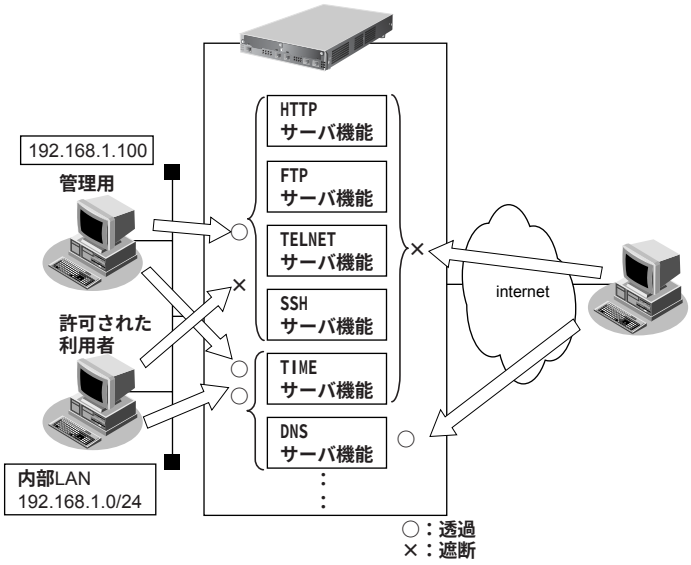
設定した内容が有効になります。

2.42 アプリケーションフィルタ機能を使う

適用機種　全機種

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト（192.168.1.100）からのみ HTTP/TELNET/FTP/SSH サーバ機能へのアクセスを許可する。
- 内部 LAN のホスト（192.168.1.0/24）からのみ TIME サーバ機能へのアクセスを許可する。
- その他のサーバ機能は制限しない。

こんな事に気をつけて

IP フィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行っていてもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合の設定例を示します。

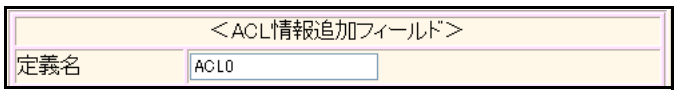
メンテナンス用のサーバ機能（TELNET/FTP/SSH）にアクセスできる PC を制限する

1.　設定メニューのルータ設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ACL0



3.　［追加］ボタンをクリックします。

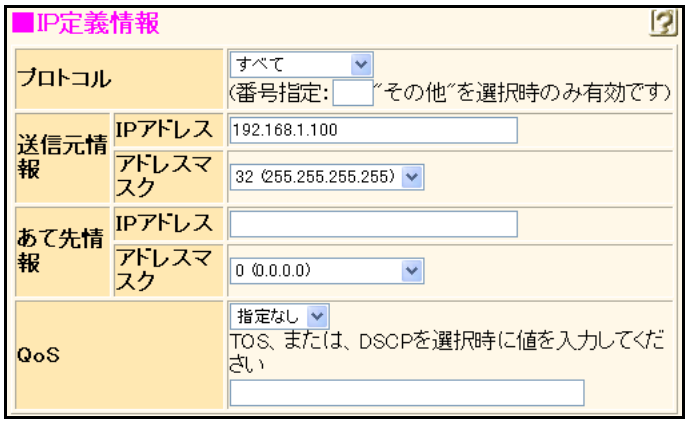
「ACL 定義情報（ACL0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」ページが表示されます。

5.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→192.168.1.100
  アドレスマスク　→32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし



6.　［保存］ボタンをクリックします。

7.　設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

8.　「サーバ機能情報」をクリックします。

「サーバ機能情報」ページが表示されます。

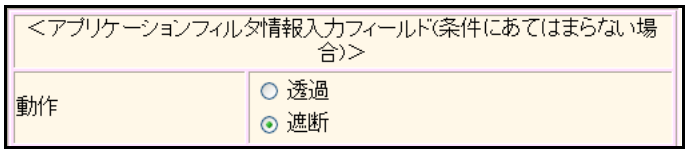
9.　「FTP サーバ機能」のアプリケーションフィルタ機能に対する［設定］ボタンをクリックします。

「アプリケーションフィルタ情報」ページが表示されます。

10.　「条件にあてはまらない場合の動作」の［修正］ボタンをクリックします。

11.　以下の項目を指定します。

- 動作　→ 遮断

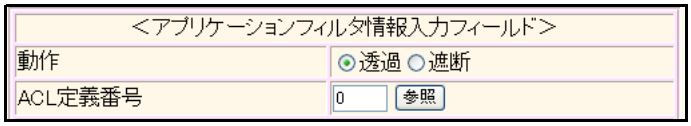


12.　［保存］ボタンをクリックします。

「アプリケーションフィルタ情報」ページが表示されます。

13.　以下の項目を指定します。

- 動作　→透過
- ACL 定義番号　→ 0



補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。

14.　［追加］ボタンをクリックします。

15.　手順 7. ～ 15. を参考に、TELNET サーバ機能、SSH サーバ機能、HTTP サーバ機能に対しても同様の設定を行います。

TIME サーバ機能を使用できる PC を 192.168.1.0/24 のネットワークに制限する

16.　手順 1. ～ 15. を参考に、以下の項目を指定します。

「ACL 情報」

- 定義名　→ ACL1

「ACL 定義情報（ACL1）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→指定しない
- QoS　→指定なし

「サーバ機能情報」-「アプリケーションフィルタ情報（TIME）」条件にあてはまらない場合の動作

- 動作　→遮断

アプリケーションフィルタ情報

- 動作　→透過
- ACL 定義番号　→ 1

17.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

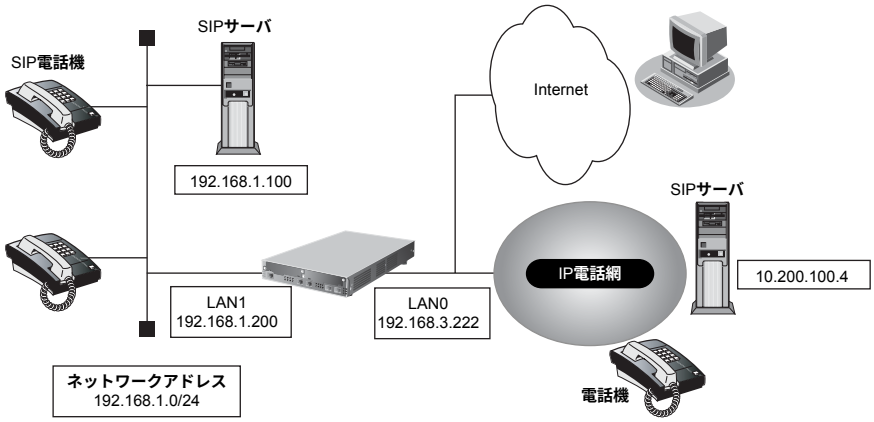
2.43 SIP-SIP ゲートウェイ機能を使う

適用機種　全機種

本装置は、SIP 電話サービス間の相互接続を行う SIP-SIP ゲートウェイ機能をサポートしています。

こんな事に気をつけて

- **動的 VPN 機能と併用することはできません。**
- **ゲートウェイの IP アドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SIP-SIP ゲートウェイ機能は正常に動作しません。**
- **データ通信の負荷が高い場合、音声品質が低下する場合があります。**



ここでは、IP Pathfinder および CL シリーズで構成された IP 電話サービスからひかり電話ビジネスタイプへ接続するゲートウェイ装置として、利用する場合の設定方法を説明します。

● 前提条件

- 内線側は IP Pathfinder および CL シリーズによる IP 電話網が構築されているものとする。
- 外線側はひかり電話ビジネスタイプに接続されているものとする。

● 設定条件

[内線側（IP Pathfinder および CL シリーズ）]

- ゲートウェイの IP アドレス　：192.168.1.200
- SIP サーバ　：192.168.1.100
- SIP ドメイン　：voip.fujitsu.com
- ゲートウェイ番号　：9000
- 着信転送先ユーザ名　：2000

[外線側（ひかり電話ビジネスタイプ）]

- ゲートウェイの IP アドレス　：192.168.3.222
- 網アドレス　：10.200.100.4
- IP 電話番号　：0123456789
- ユーザ ID　：userid
- パスワード　：userpass

上記の設定条件に従って設定を行う場合の設定例を示します。

SIP-SIP ゲートウェイ機能を設定する

1.　設定メニューのルータ設定で「SIP-SIP ゲートウェイ情報」をクリックします。

「SIP-SIP ゲートウェイ情報」ページが表示されます。

2.　「基本情報」をクリックします。

「基本情報」が表示されます。

3.　以下の項目を指定します。

- SIP-SIP ゲートウェイ情報　→使用する

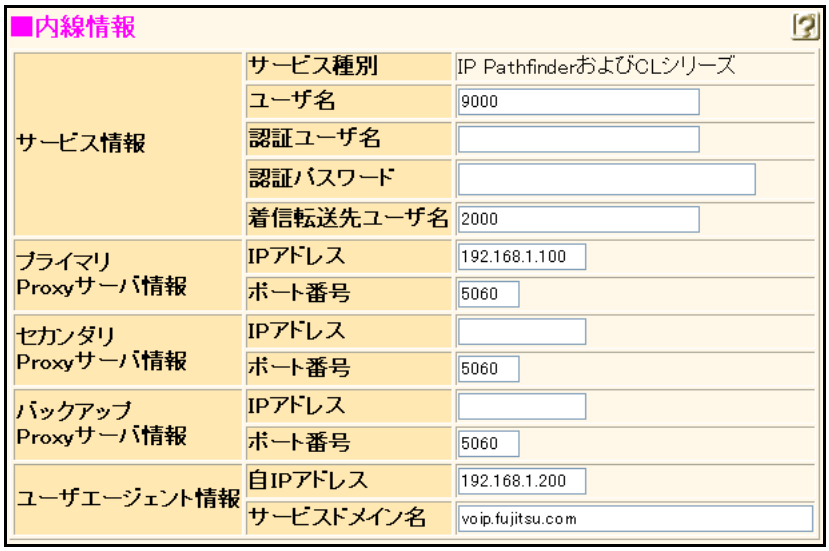
4.　［保存］ボタンをクリックします。

5.　「内線情報」をクリックします。

「内線情報」が表示されます。

6.　以下の項目を指定します。

- サービス情報
  ユーザ名　→9000
  着信転送先ユーザ名　→2000
- プライマリ Proxy サーバ情報
  IP アドレス　→192.168.1.100
- ユーザエージェント情報
  自 IP アドレス　→192.168.1.200
  サービスドメイン名　→voip.fujitsu.com



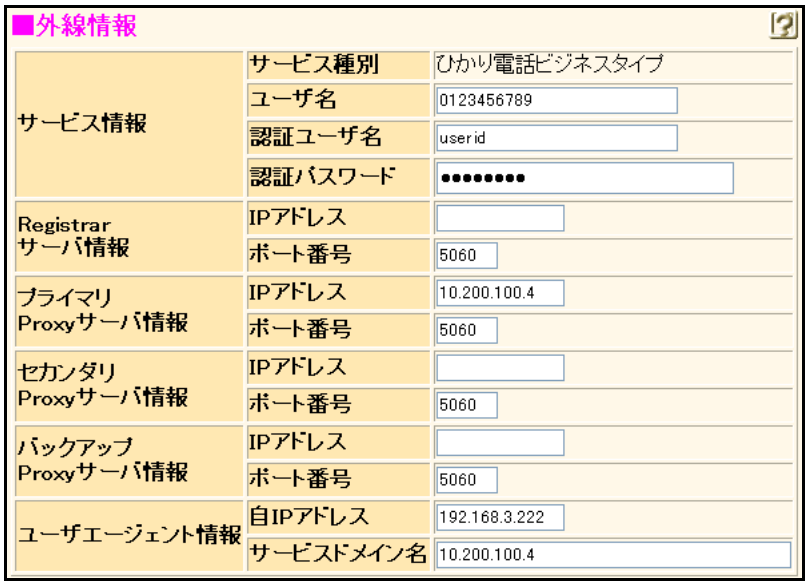
7.　［保存］ボタンをクリックします。

8.　「外線情報」をクリックします。

「外線情報」が表示されます。

9.　以下の項目を指定します。

- サービス情報
  ユーザ名　→0123456789
  認証ユーザ名　→userid
  認証パスワード　→userpass
- プライマリ Proxy サーバ情報
  IP アドレス　→10.200.100.4
- ユーザエージェント情報
  自 IP アドレス　→192.168.3.222
  サービスドメイン名　→10.200.100.4



10.　［保存］ボタンをクリックします。

11.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2.44 IEEE802.1X認証機能を使う

適用機種 ***Si-R240,240B***

IEEE802.1X認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権限を持っているかを検証することができます。

参照 Si-R シリーズ　機能説明書「2.30 IEEE802.1X認証機能」（P.146）

2.44.1 有線LANと無線LANでIEEE802.1X認証機能を使う

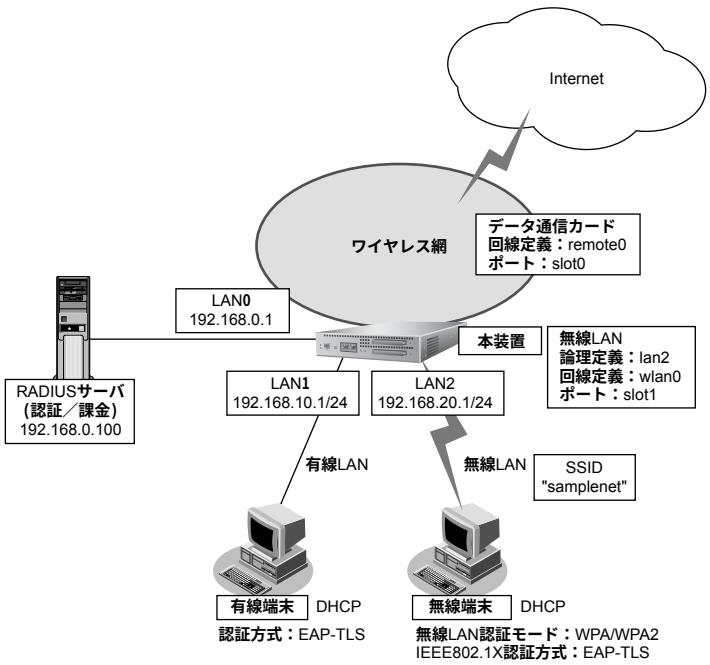
適用機種 ***Si-R240,240B***

ここでは、有線LANおよび無線LANインタフェースでIEEE802.1X認証を行う場合の設定方法を説明します。

こんな事に気をつけて

- **無線LANカードは、Si-Rシリーズ専用の無線LAN APカード（SIRWLAP）を使用してください。**
- **無線LANカードは、SLOT0またはSLOT1のどちらか一方に挿入して使用してください。**
- **同時に2枚の無線LANカードを挿入して使用することはできません。**
- **無線LANカード／データ通信カードは、電源投入前に挿入してください。また、電源投入後の抜き差しはしないでください。**
- **この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。**

参照 Si-R シリーズ　トラブルシューティング「5 ご購入時の状態に戻すには」（P.52）



● 設定条件

有線 LAN を使ってローカルサーバに接続する

- 利用するポート　：lan0
- IP アドレス　：192.168.0.1/24

有線 LAN で IEEE802.1X 認証を行って端末を収容する

- 利用するポート　：lan1
- IP アドレス　：192.168.10.1/24
- IEEE802.1X 認証　：有効
- IEEE802.1X 認証（認証サーバ）　：aaa1
- その他　：接続端末のアドレスは DHCP 機能を利用する

無線 LAN で IEEE802.1X 認証を行って端末を収容する

- 利用するポート　：slot1
- 利用する論理定義　：lan2
- 利用する回線定義　：wlan0
- 通信モード　：IEEE802.11g
- チャネル　：10
- SSID　：samplenet
- 認証モード　：WPA/WPA2 自動判別認証
- IEEE802.1X 認証　：有効
- IEEE802.1X 認証（認証サーバ）　：aaa1
- IP アドレス　：192.168.20.1/24
- その他　：接続端末のアドレスは DHCP 機能を利用する

データ通信カードを使ってインターネットへ接続する

- 利用するポート　：slot0
- 認証 ID　：通信事業者から提示された内容
- 認証パスワード　：通信事業者から提示された内容
- 電話番号　：通信事業者から提示された内容
- 無通信監視タイマ　：無通信監視時間を 1 分とする

認証／課金サーバを AAA 定義で指定する

- aaa 定義番号　：aaa1
- 認証サーバ IP アドレス　：192.168.0.100
- 認証サーバシークレットキー　：passwd
- 課金サーバ IP アドレス　：192.168.0.100
- 課金サーバシークレットキー　：passwd

上記の設定条件に従って設定を行う場合の設定例を示します。

端末を設定する

無線 LAN アダプタの設定マニュアルを参考に設定を行ってください。

本装置を設定する

有線 LAN を使ってローカルサーバに接続する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

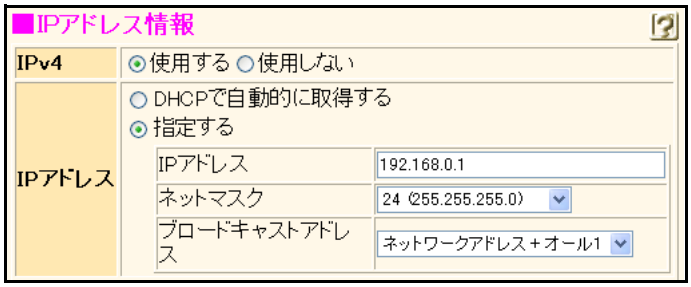
「LAN0 情報（物理 LAN）」ページが表示されます。

3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.0.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



5.　［保存］ボタンをクリックします。

有線 LAN で IEEE802.1X 認証を行って端末を収容する

6.　設定メニューのルータ設定で「認証情報」をクリックします。

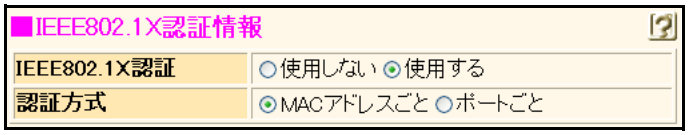
「認証情報」ページが表示されます。

7.　「IEEE802.1X 認証情報」をクリックします。

「IEEE802.1X 認証情報」が表示されます。

8.　以下の項目を指定します。

- IEEE802.1X 認証　→使用する
- 認証方式　→ MAC アドレスごと



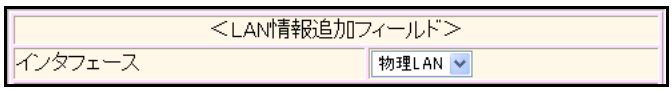
9.　［保存］ボタンをクリックします。

10.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　以下の項目を指定します。

- インタフェース　→物理 LAN



12.　［追加］ボタンをクリックします。

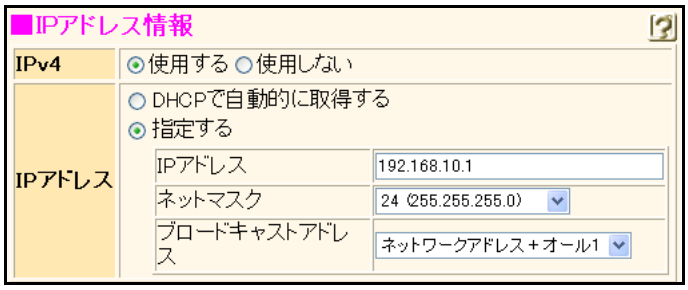
「LAN1 情報（物理 LAN）」ページが表示されます。

13.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

14.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.10.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



15.　［保存］ボタンをクリックします。

16.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

17.　「IEEE802.1X 認証情報」をクリックします。

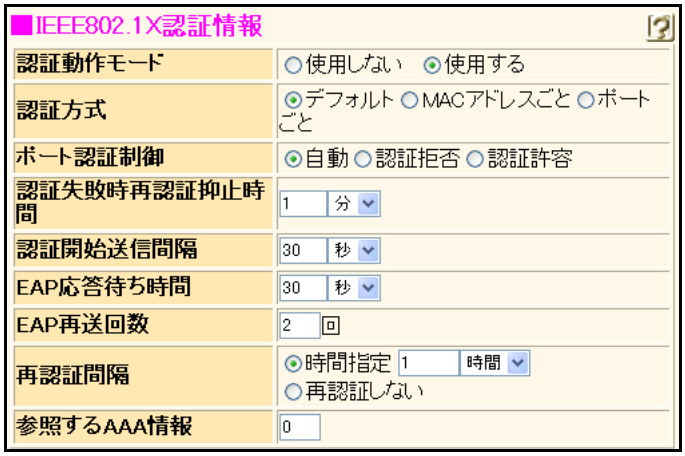
「IEEE802.1X 認証情報」が表示されます。

18.　以下の項目を指定します。

- 認証動作モード　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- 認証方式　→デフォルト
- ポート認証制御　→自動
- 認証失敗時再認証抑止時間　→1 分
- 認証開始送信間隔　→30 秒
- EAP 応答待ち時間　→30 秒
- EAP 再送回数　→2
- 再認証間隔　→時間指定　1 時間
- 参照する AAA 情報　→0



19.　［保存］ボタンをクリックします。

20.　「IP 関連」をクリックします。

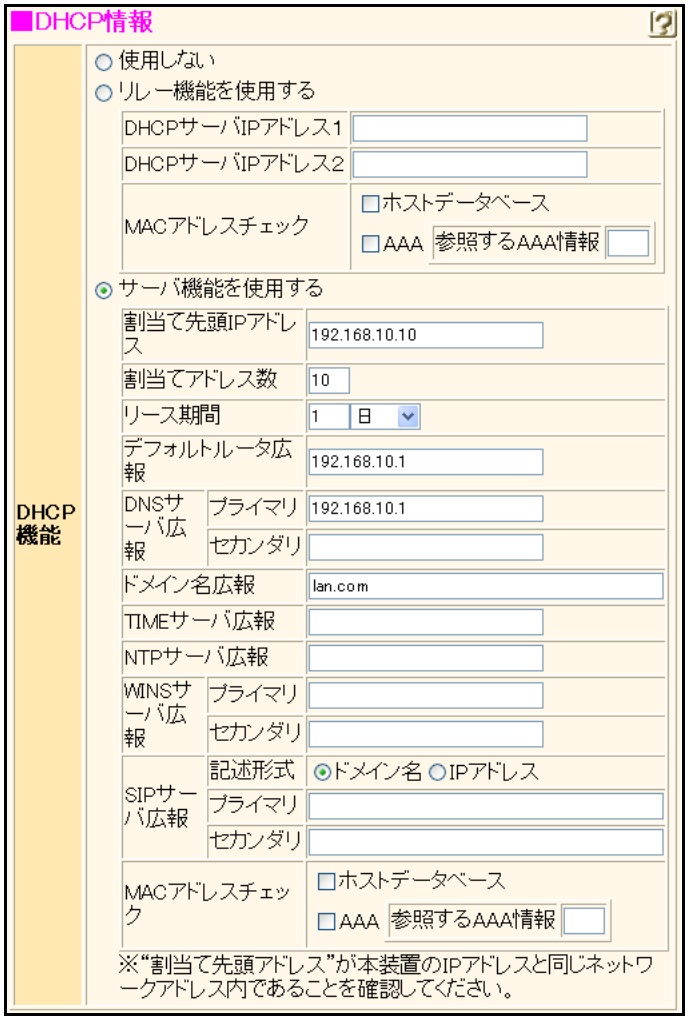
IP 関連の設定項目と「IP アドレス情報」が表示されます。

21.　「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

22.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.10.10
  割当てアドレス数　→ 10
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.10.1
  DNS サーバ広報
  プライマリ　→ 192.168.10.1
  ドメイン名広報　→ lan.com



23.　［保存］ボタンをクリックします。

無線 LAN で IEEE802.1X 認証を行って端末を収容する

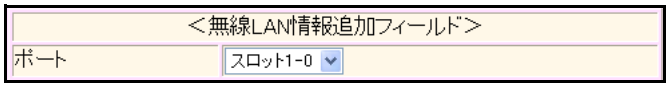
無線 LAN 情報を設定する

24.　設定メニューのルータ設定で「無線 LAN 情報」をクリックします。

「無線 LAN 情報」ページが表示されます。

25.　以下の項目を指定します。

- ポート　→スロット 1-0

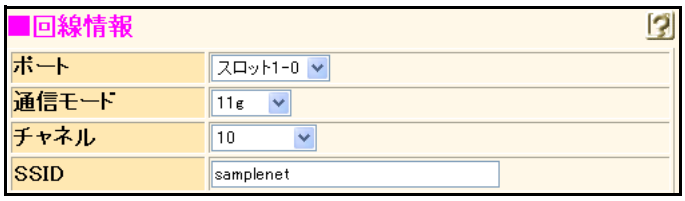


26.　［追加］ボタンをクリックします。

無線 LAN0 情報の設定項目と「回線情報」が表示されます。

27.　以下の項目を指定します。

- ポート　→スロット 1-0
- 通信モード　→ 11g
- チャネル　→ 10
- SSID　→ samplenet



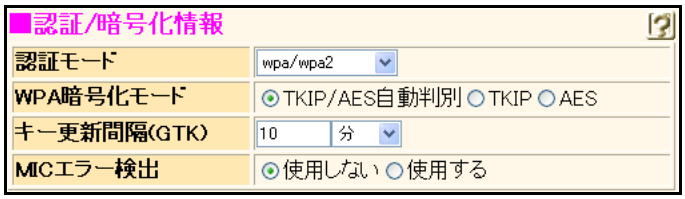
28.　［保存］ボタンをクリックします。

29.　「認証／暗号化情報」をクリックします。

「認証／暗号化情報」が表示されます。

30.　以下の項目を指定します。

- 認証モード　→ wpa/wpa2
- WPA 暗号化モード　→ TKIP/AES 自動判別
- キー更新間隔（GTK）　→ 10 分
- MIC エラー検出　→使用しない



31.　［保存］ボタンをクリックします。

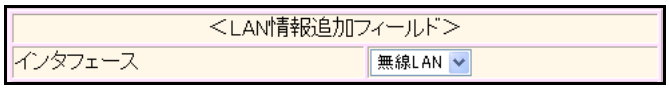
LAN（無線 LAN）情報を設定する

32.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

33.　以下の項目を指定します。

- インタフェース　→無線 LAN



34.　［追加］ボタンをクリックします。

「LAN2 情報（無線 LAN）」ページが表示されます。

35.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

36.　以下の項目を指定します。

- 無線 LAN 定義　→無線 LAN0

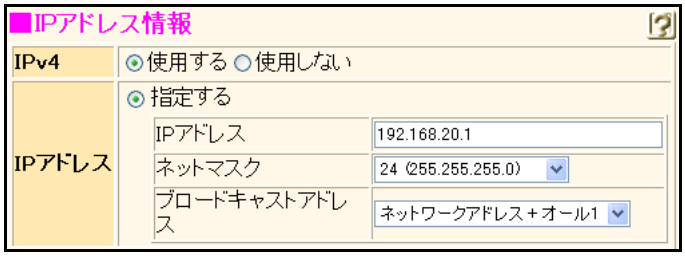
37.　［保存］ボタンをクリックします。

38.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

39.　以下の項目を指定します。

- IPv4　→使用する
- IP アドレス　→指定する
  IP アドレス　→ 192.168.20.1
  ネットマスク　→ 24（255.255.255.0）
  ブロードキャストアドレス　→ネットワークアドレス＋オール 1



40.　［保存］ボタンをクリックします。

41.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

42.　「IEEE802.1X 認証情報」をクリックします。

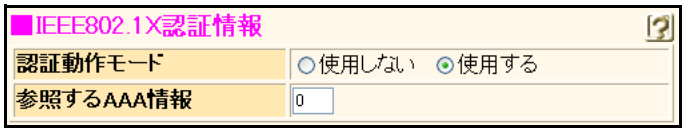
「IEEE802.1X 認証情報」が表示されます。

43.　以下の項目を指定します。

- 認証動作モード　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- 参照する AAA 情報　→ 0



44.　［保存］ボタンをクリックします。

45.　「IP 関連」をクリックします。

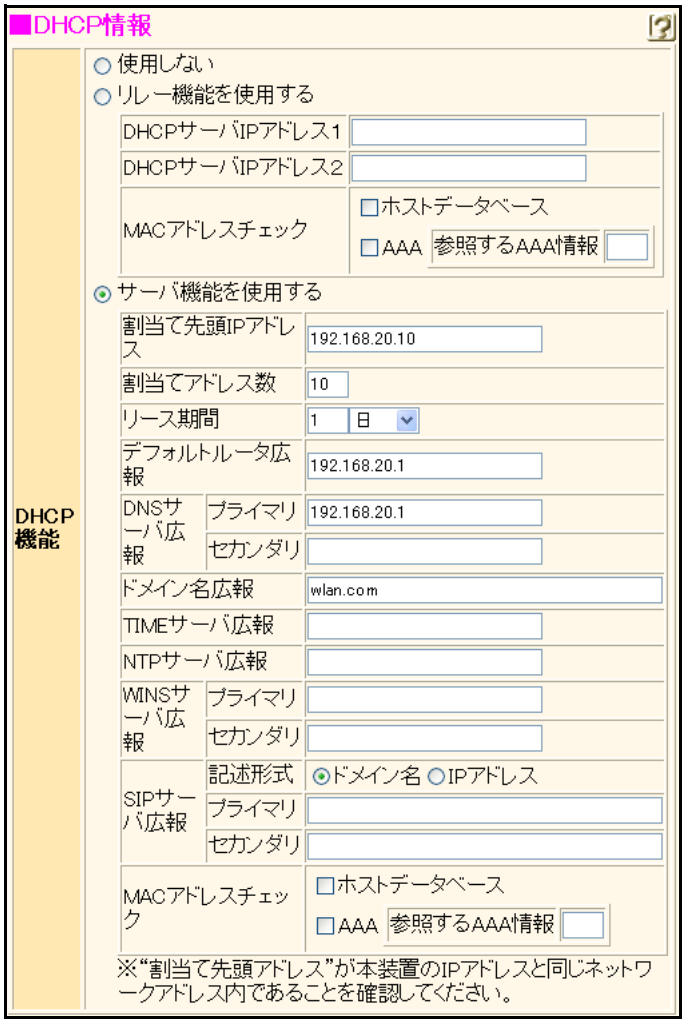
IP 関連の設定項目と「IP アドレス情報」が表示されます。

46.　「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

47.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→ 192.168.20.10
  割当てアドレス数　→ 10
  リース期間　→ 1 日
  デフォルトルータ広報　→ 192.168.20.1
  DNS サーバ広報
  プライマリ　→ 192.168.20.1
  ドメイン名広報　→ wlan.com



48.　［保存］ボタンをクリックします。

データ通信カードを使ってインターネットへ接続する

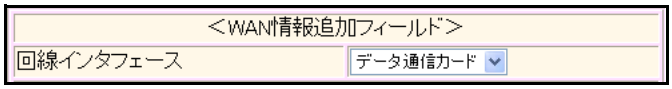
WAN 情報を設定する

49.　設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

50.　以下の項目を指定します。

- 回線インタフェース　→データ通信カード

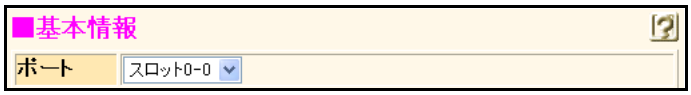


51.　［追加］ボタンをクリックします。

「WAN 情報（データ通信カード）」ページが表示されます。

52.　以下の項目を指定します。

- ポート　→スロット 0-0



53.　［保存］ボタンをクリックします。

相手情報を設定する

54.　設定メニューのルータ設定で「相手情報」をクリックします。

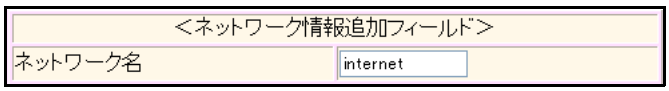
「相手情報」ページが表示されます。

55.　「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

56.　以下の項目を指定します。

- ネットワーク名　→internet



57.　［追加］ボタンをクリックします。

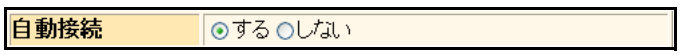
「ネットワーク情報（internet）」ページが表示されます。

58.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

59.　以下の項目を指定します。

- 自動接続　→する



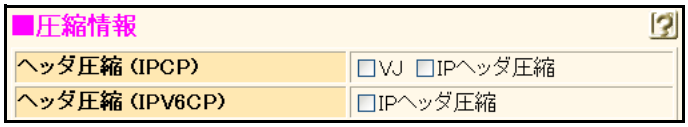
60.　［保存］ボタンをクリックします。

61.　「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

62.　以下の項目を指定します。

- ヘッダ圧縮（IPCP）　→チェックしない
- ヘッダ圧縮（IPV6CP）　→チェックしない



63.　［保存］ボタンをクリックします。

64.　「IP 関連」をクリックします。

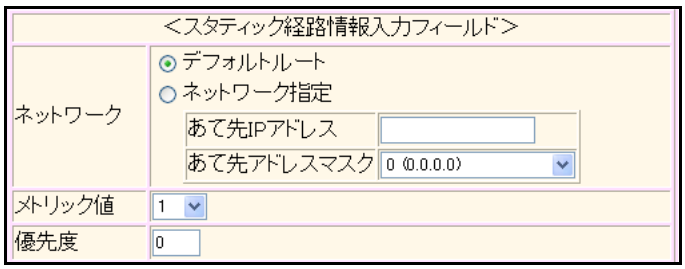
IP 関連の設定項目と「IP 基本情報」が表示されます。

65.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

66.　以下の項目を指定します。

- ネットワーク　→デフォルトルート
- メトリック値　→1
- 優先度　→0



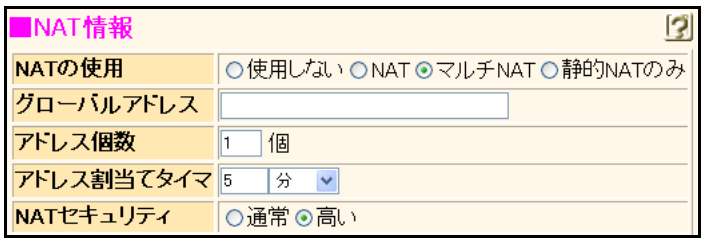
67.　［追加］ボタンをクリックします。

68.　IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

69.　以下の項目を指定します。

- NAT の使用　→マルチ NAT
- グローバルアドレス　→指定しない
- アドレス個数　→1
- アドレス割当てタイマ　→5 分
- NAT セキュリティ　→高い



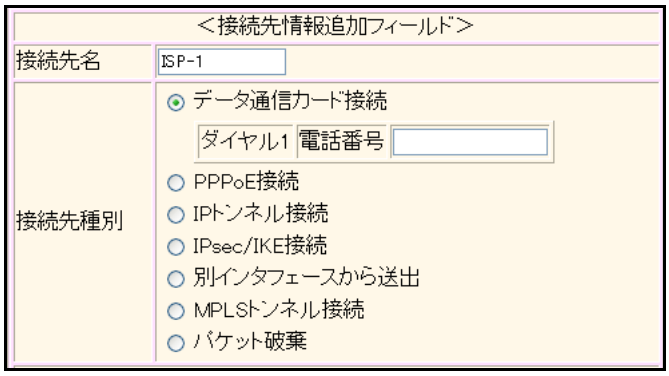
70.　［保存］ボタンをクリックします。

71.　「接続先情報」をクリックします。

「接続先情報」が表示されます。

72.　以下の項目を指定します。

- 接続先名　→ISP-1
- 接続先種別　→データ通信カード接続
- 電話番号　→（通信事業者から提示された内容）



73.　[追加] ボタンをクリックします。

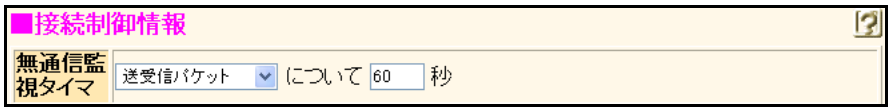
「接続先情報（ISP-1）」ページが表示されます。

74.　データ通信カード接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

75.　以下の項目を指定します。

- 無通信監視タイマ　→送受信パケットについて 60 秒



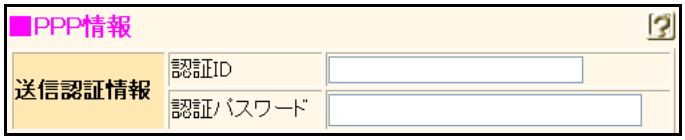
76.　[保存] ボタンをクリックします。

77.　データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

78.　以下の項目を指定します。

- 送信認証情報
  認証 ID　→（通信事業者から提示された内容）
  認証パスワード　→（通信事業者から提示された内容）



79.　[保存] ボタンをクリックします。

ProxyDNS 情報、URL フィルタ情報を設定する

80.　設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

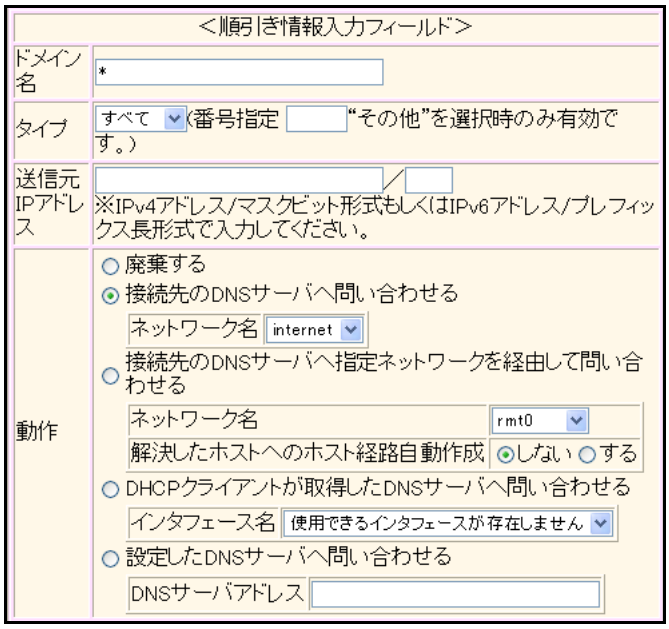
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

81.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

82.　以下の項目を指定します。

- ドメイン名　→ *
- タイプ　→すべて
- 送信元 IP アドレス　→指定しない
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→ internet



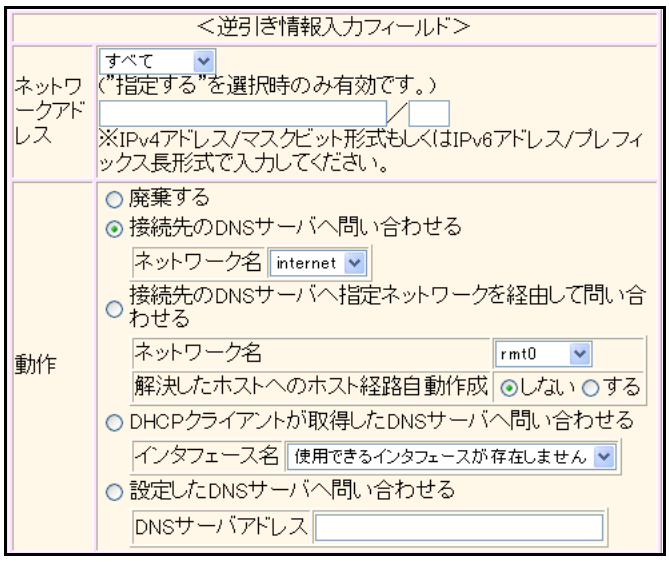
83.　[追加] ボタンをクリックします。

84.　「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

85.　以下の項目を指定します。

- ネットワークアドレス　→すべて
- 動作　→接続先の DNS サーバへ問い合わせる
  ネットワーク名　→ internet



86.　[追加] ボタンをクリックします。

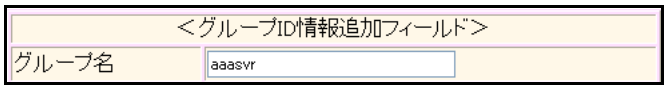
認証／課金サーバを AAA 定義で指定する

87.　設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

88.　以下の項目を指定します。

- グループ名　　→aaasvr



89.　［追加］ボタンをクリックします。

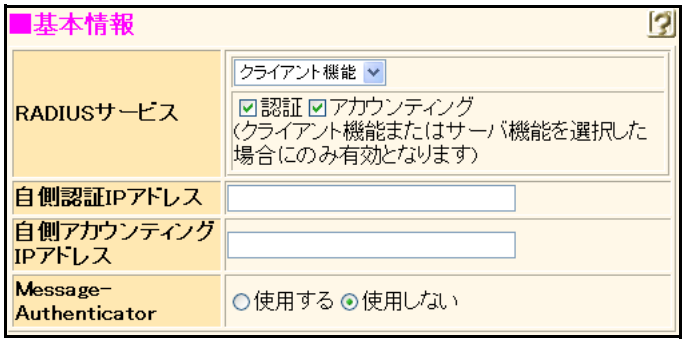
「グループ ID 情報（0）」と設定項目が表示されます。

90.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

91.　以下の項目を指定します。

- RADIUS サービス　　→クライアント機能
  認証　　→チェックする
  アカウンティング　　→チェックする
- Message-Authenticator　　→使用しない



92.　［保存］ボタンをクリックします。

93.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

94.　認証情報 1 の［修正］ボタンをクリックします。

95.　以下の項目を指定します。

- 認証情報 1

  共有鍵　→ passwd
  サーバ IP アドレス　→ 192.168.0.100
  サーバ UDP ポート　→ 1812
  復旧待機時間　→ 0 秒
  優先度　→ 0
  自側認証 IP アドレス　→ 192.168.0.1

96.　認証情報 1 の［保存］ボタンをクリックします。

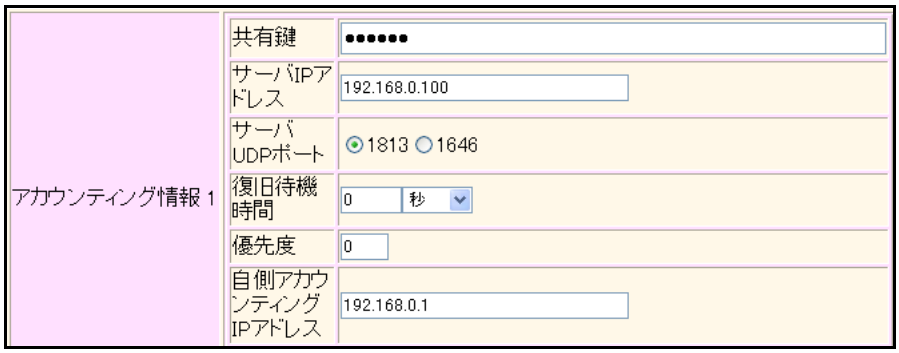
「サーバ情報（クライアント機能）」に戻ります。

97.　アカウンティング情報 1 の［修正］ボタンをクリックします。

98.　以下の項目を指定します。

- アカウンティング情報 1

  共有鍵　→ passwd
  サーバ IP アドレス　→ 192.168.0.100
  サーバ UDP ポート　→ 1813
  復旧待機時間　→ 0 秒
  優先度　→ 0
  自側アカウンティング IP アドレス　→ 192.168.0.1



99.　アカウンティング情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

100.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足　データ通信カードの認証 ID、パスワード、電話番号については、「1.7 インターネットへデータ通信カードを使用して接続する」（P.76）の補足を参照してください。

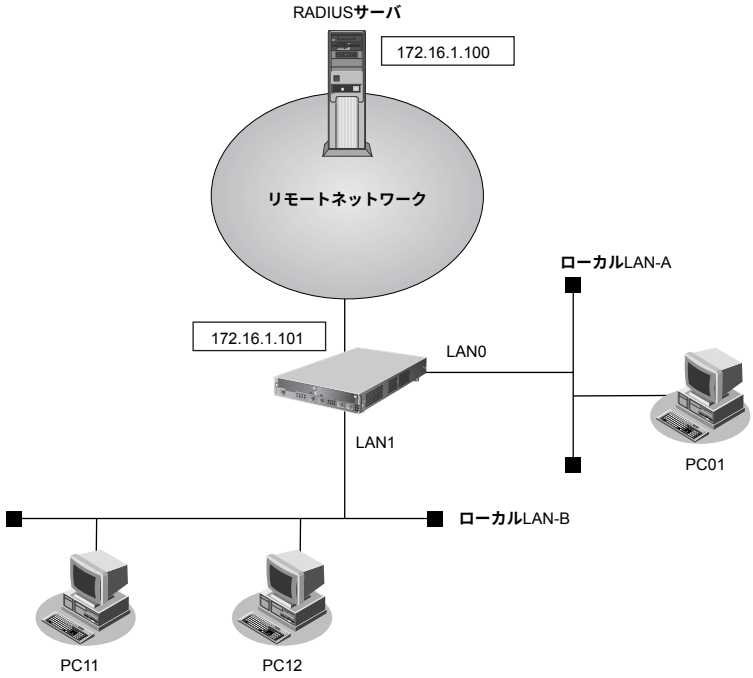
2.45 不正端末アクセス防止機能（MACアドレス認証）を使う

適用機種　全機種

不正端末アクセス防止機能（MACアドレス認証）を使用すると、本装置のローカルLANに接続する端末がリモートネットワークへのアクセス権限を持っているかを認証することができます。

こんな事に気をつけて

MACアドレス認証で利用するAAAのグループIDを正しく設定してください。



ここでは、リモートネットワークへの接続がすでに設定されている場合を例にMACアドレス認証機能を利用する設定方法を説明します。

● 設定条件

- LAN0、LAN1ポートでMACアドレス認証を使用する
- LAN0、LAN1ポートで利用する認証データベース
  LAN0ポート　：RADIUSサーバ
  LAN1ポート　：ローカルで設定した認証情報
- AAAグループID
  LAN0ポート　：0
  LAN1ポート　：1
- ローカルLAN-Bで利用可能なユーザは以下のとおり

ユーザ	MACアドレス
PC11	00:11:11:00:00:01
PC12	00:22:22:00:00:02

- リモートネットワークへの接続定義は設定済み

- RADIUS サーバはリモートネットワークに接続
- RADIUS サーバの IP アドレス　：172.16.1.100
- RADIUS サーバのシークレット　：radius-secret

上記の設定条件に従って設定を行う場合の設定例を示します。

MAC アドレス認証で使用するパスワードを設定する

1.　設定メニューのルータ設定で「認証情報」をクリックします。

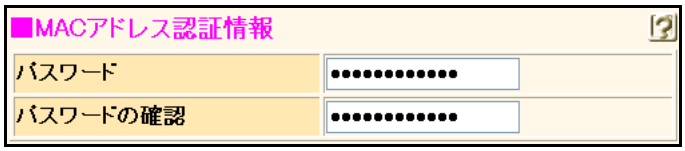
「認証情報」ページが表示されます。

2.　「MAC アドレス認証情報」をクリックします。

「MAC アドレス認証情報」が表示されます。

3.　以下の項目を指定します。

- パスワード　→macauth-pass
- パスワードの確認　→macauth-pass



4.　［保存］ボタンをクリックします。

MAC アドレス認証を使用する

5.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

6.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

7.　「共通情報」をクリックします。

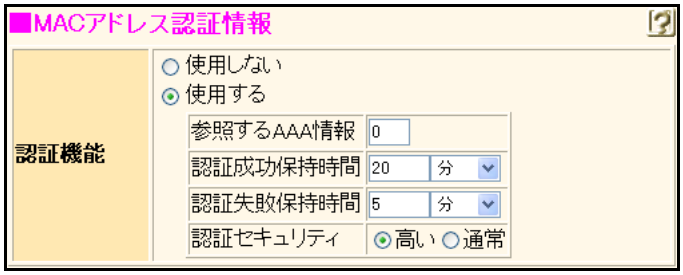
共通情報の設定項目と「基本情報」が表示されます。

8.　「MAC アドレス認証情報」をクリックします。

「MAC アドレス認証情報」が表示されます。

9.　以下の項目を指定します。

- 認証機能　→使用する
  参照する AAA 情報　→0



10.　［保存］ボタンをクリックします。

11.　手順 5. ～ 10. を参考に、LAN1 ポートを指定します。

「LAN1 情報（物理 LAN）」-「共通情報」
「MAC アドレス認証情報」

- 認証機能　→使用する
- 参照する AAA 情報　→ 1

RADIUS サーバを利用する AAA グループ情報を設定する

12.　設定メニューのルータ設定で「AAA 情報」をクリックします。

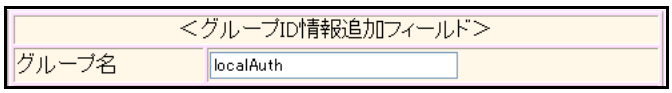
「AAA 情報」ページが表示されます。

13.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

14.　以下の項目を指定します。

- グループ名　→ localAuth



15.　［追加］ボタンをクリックします。

「グループ ID 情報（0）」と設定項目が表示されます。

16.　手順 12. ～ 15. を参考に、グループ名を追加します。

- グループ名　→ radiusAuth

17.　［追加］ボタンをクリックします。

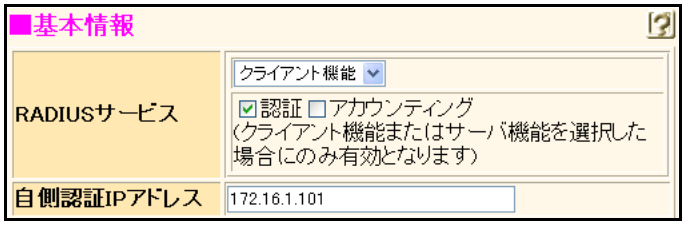
「グループ ID 情報（1）」と設定項目が表示されます。

18.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

19.　以下の項目を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックしない
- 自側認証 IP アドレス　→ 172.16.1.101



20.　［保存］ボタンをクリックします。

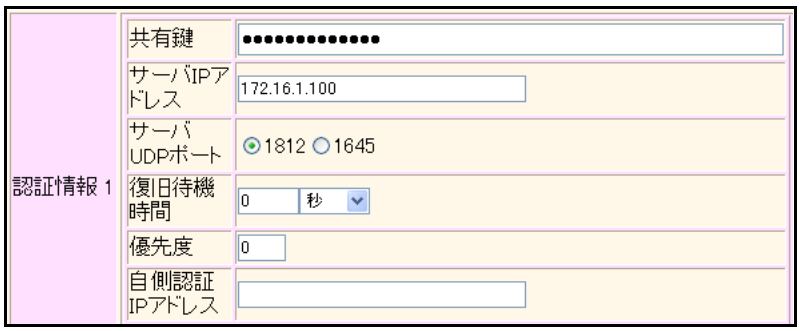
21.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

22.　認証情報 1 の［修正］ボタンをクリックします。

23.　以下の項目を指定します。

- 認証情報 1
  共有鍵　→ radius-secret
  サーバ IP アドレス　→ 172.16.1.100



24.　認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

ローカル認証情報を利用する AAA グループ情報を設定する

25.　設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

26.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

27.　「グループ ID 情報」でグループ ID が 0 の［修正］ボタンをクリックします。

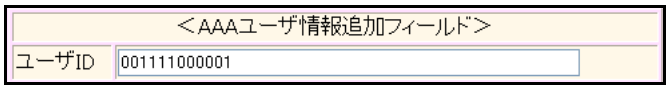
「グループ ID 情報（0）」と設定項目が表示されます。

28.　「AAA ユーザ情報」をクリックします。

「AAA ユーザ情報」が表示されます。

29.　以下の項目を指定します。

- ユーザ ID　→ 001111000001



30.　［追加］ボタンをクリックします。

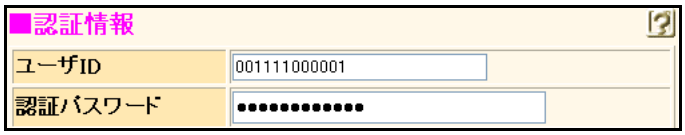
「AAA ユーザ情報（0）」と設定項目が表示されます。

31.　「認証情報」をクリックします。

「認証情報」が表示されます。

32.　以下の項目を設定します。

- ユーザ ID　→ 001111000001
- 認証パスワード　→ macauth-pass



33.　［保存］ボタンをクリックします。

34.　手順 25. ～ 33. を参考に、以下の項目を指定します。

「AAA ユーザ情報（0）」-「認証情報」

「認証情報」

- ユーザ ID　→ 002222000002
- 認証パスワード　→ macauth-pass

35.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

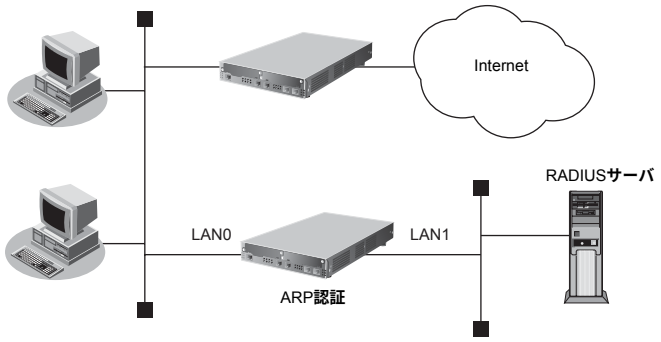
2.46 ARP 認証機能を使う

適用機種　全機種

ここでは、既存のネットワークに本装置を追加して、ARP 認証を行う場合の設定方法を説明します。

こんな事に気をつけて

ARP 認証で利用する AAA のグループ ID を正しく設定してください。



● 設定条件

- LAN0 で ARP 認証を使用する
- ARP 認証で利用する認証データベース　：RADIUS サーバ
- AAA グループの ID　：0
- RADIUS サーバの IP アドレス　：172.16.1.100
- RADIUS サーバは LAN1 に接続されている
- RADIUS サーバのシークレット　：radius-secret
- 認証失敗時の通信妨害を行う

上記の設定条件に従って設定を行う場合の設定例を示します。

RADIUS サーバの LAN を設定する

1.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN1 の［修正］ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

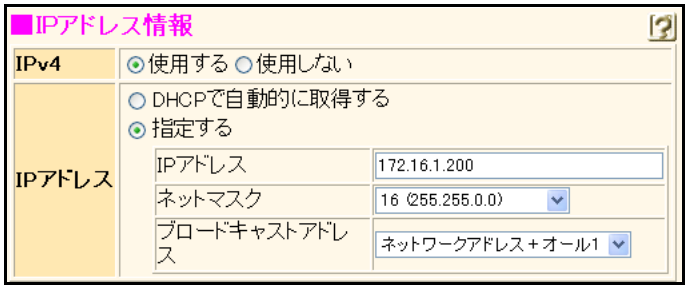
3.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　以下の項目を指定します。

- IPv4　→使用する
- IPアドレス　→指定する

IPアドレス　→172.16.1.200
ネットマスク　→16（255.255.0.0）
ブロードキャストアドレス　→ネットワークアドレス＋オール1



5.　［保存］ボタンをクリックします。

ARP 認証を設定する

6.　設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

7.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

8.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

9.　「ARP 認証情報」をクリックします。

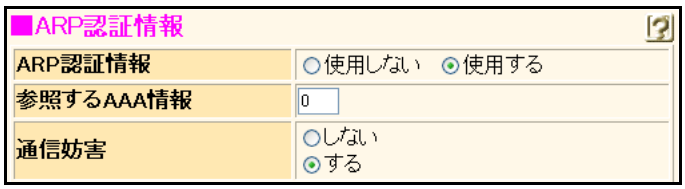
「ARP 認証情報」が表示されます。

10.　以下の項目を指定します。

- ARP 認証情報　→使用する

“使用する”を選択すると、以下の項目が指定できます。

- 参照する AAA 情報　→0
- 通信妨害　→する



11.　［保存］ボタンをクリックします。

RADIUS サーバを利用する AAA グループ情報を設定する

12.　設定メニューのルータ設定で「AAA 情報」をクリックします。

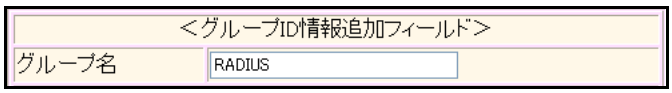
「AAA 情報」ページが表示されます。

13.　「グループ ID 情報」をクリックします。

「グループ ID 情報」が表示されます。

14.　以下の項目を指定します。

- グループ名　→RADIUS



15.　［追加］ボタンをクリックします。

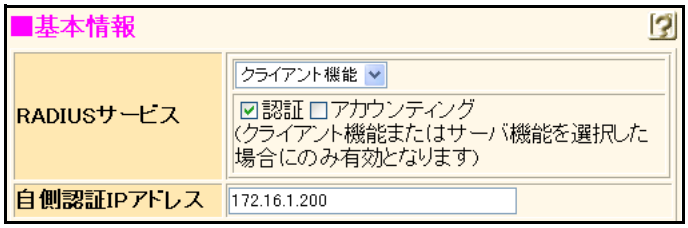
「グループ ID 情報（0）」と設定項目が表示されます。

16.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

17.　以下の項目を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックしない
- 自側認証 IP アドレス　→172.16.1.200



18.　［保存］ボタンをクリックします。

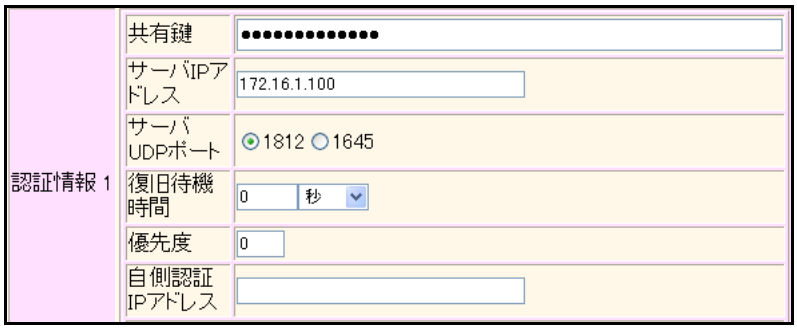
19.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

20.　「認証情報 1」の［修正］ボタンをクリックします。

21.　以下の項目を指定します。

- 認証情報 1
  共有鍵　→radius-secret
  サーバ IP アドレス　→172.16.1.100



22.　認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

23.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

索引

O

P

R

S

T

U

V

W

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ふ

へ

ほ

ま

む

め

ゆ

り

れ

Si-R シリーズ　Web 設定事例集

P3NK-2652-02Z0

発行日　　2007 年 11 月

発行責任　　富士通株式会社