P3NK-5712-05Z0

Fujitsu Network Si-R
Si-R Gシリーズ

コマンド設定事例集　V4

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。

2017年3月　初版
2017年5月　第2版
2017年10月 第3版
2018年5月　第4版
2023年5月　第5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。

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。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

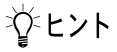
本書の構成

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。

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。

設定例の記述について

コマンド例では configure コマンドを実行して、構成定義モードに入ったあとのコマンドを記述しています。

また、プロンプトは設定や機種によって変化するため、“#” に統一しています。

マニュアル「コマンドユーザーズガイド」

本書における商標の表記について

Windows 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。

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® 10 Home 64 ビット版	Windows 10 または Windows
Microsoft® Windows® 10 Pro 64 ビット版	

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 G100B　ご利用にあたって	Si-R G100B 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 G110B　ご利用にあたって	Si-R G110B 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 G200B　ご利用にあたって	Si-R G200B 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。
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。
コマンドリファレンス	構成定義コマンド、運用管理コマンド、および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。
コマンド設定事例集（本書）	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。
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。
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。
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。
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。
Web ユーザーズガイド	Web 画面を使用して、基本的な操作やメンテナンスについて説明しています。 また、Web 画面の項目の詳細な情報を説明しています。
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。

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。

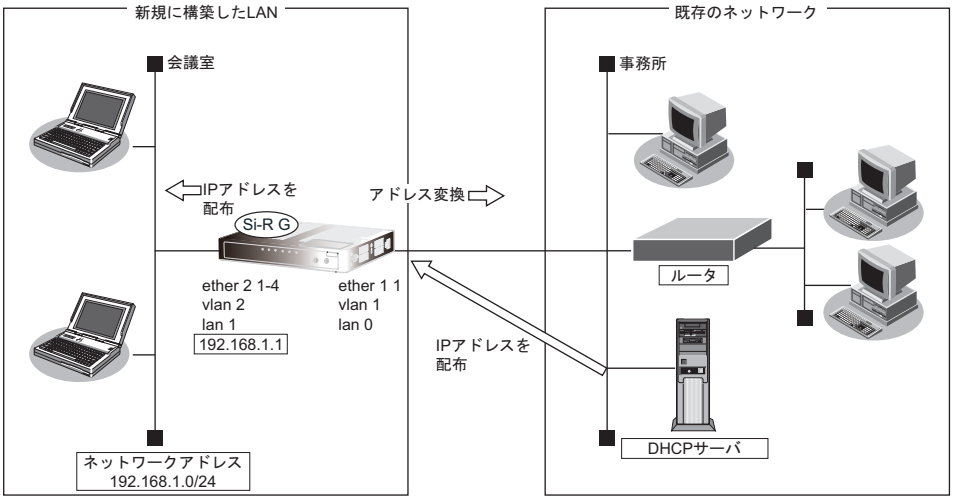
1.1　プライベートLANを構築する

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　マニュアル「トラブルシューティング」



● 設定条件

[事務所側LAN]

- ETHERポート　：グループ1ポート1
- VLAN番号　：1
- lan定義番号　：0
- 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]

- ETHERポート　：グループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：1
- 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

こんな事に気をつけて

- コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

- 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。

● コマンド

```
事務所側のLAN情報を設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip dhcp service client
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1
# lan 0 vlan 1

会議室側のLAN情報を設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off
# lan 1 vlan 2

設定終了
# save

再起動
# reset
```

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、「2.22.2 DHCPスタティック機能を使う」（P.331）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。

1.2　CATVインターネットに接続する

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。

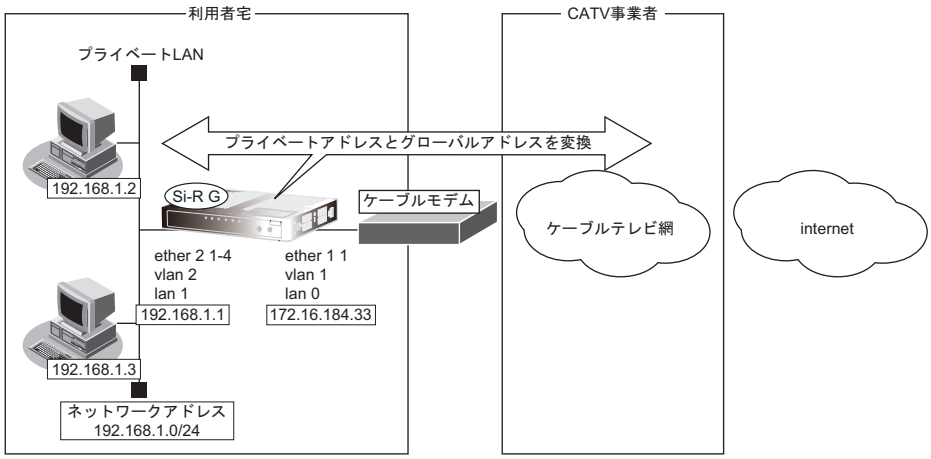
本装置を使ったCATVインターネット接続は、CATV事業者が提供するインターネット接続サービスをプライベートLAN上の複数のパソコンから利用するための接続形態です。本装置とCATV事業者が提供するケーブルモデムを接続することで、プライベートLAN上のパソコンからインターネット接続サービスを利用できます。

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。

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　マニュアル「トラブルシューティング」



● 設定条件

[CATV事業者側]

- ETHERポート　：グループ1ポート1
- VLAN番号　：1
- lan定義番号　：0
- 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]

- ETHERポート　：グループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：1
- 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。
- 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。

● コマンド

```
CATV事業者側を設定する
# ether 1 1 vlan untag 1

# delete lan

# lan 0 ip address 172.16.184.33/24 3
# lan 0 ip dhcp info time 1d
# lan 0 ip route 0 default 172.16.184.100 1 1
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1 5m
# lan 0 vlan 1

プライベートLAN側を設定する
# ether 2 1-4 vlan untag 2

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.10.10.10
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off
# lan 1 vlan 2
```

ProxyDNS を設定する
proxydns domain 0 any * any static 192.10.10.10
proxydns address 0 any static 192.10.10.10

設定終了
save

再起動
reset

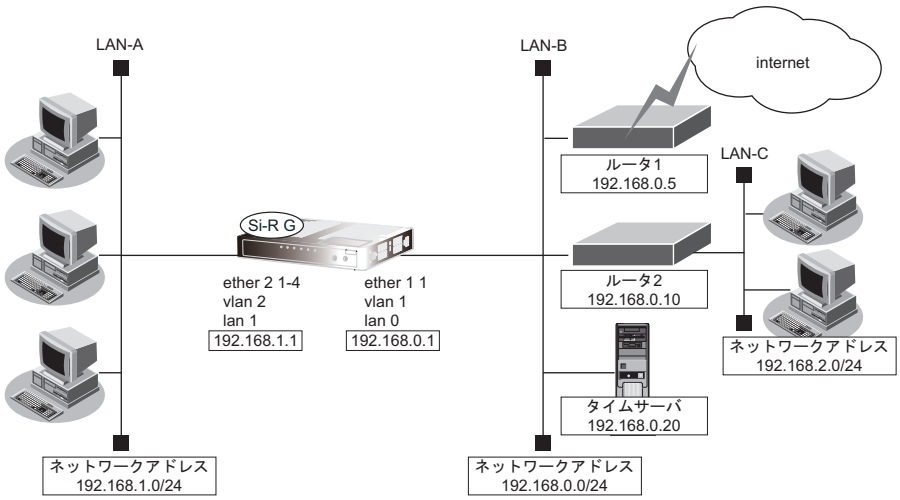
1.3　LANをネットワーク間接続する

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　マニュアル「トラブルシューティング」



● 設定条件

[LAN-A側]

- ETHERポート　：グループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：1
- 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
- DHCP機能　：DHCPサーバ機能を使用する
  - 貸出IPアドレス先頭　：192.168.1.2
  - 貸出IPアドレス個数　：253個
  - 貸出IPアドレス有効期限　：1日
- NAT機能　：使用しない
- 経路情報通知　：RIP V1 を使用する

[LAN-B側]

- ETHERポート　：グループ1ポート1
- VLAN番号　：1
- lan定義番号　：0
- 本装置のIPアドレス　：192.168.0.1
- ネットワークマスク　：255.255.255.0
- DHCP機能　：使用しない

- NAT機能　：使用しない
- ルータ１の接続先　：インターネット
- ルータ１のIPアドレス　：192.168.0.5
- ルータ２の接続先　：LAN-C （事業所内サブネットワーク）
- 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／マスク　：192.168.2.0/24
- 経路情報通知　：RIP V1 を使用する
- 静的経路情報
  LAN-Cあて　：ルータ２へ
  その他すべて（デフォルト）　：ルータ１へ

[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布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。

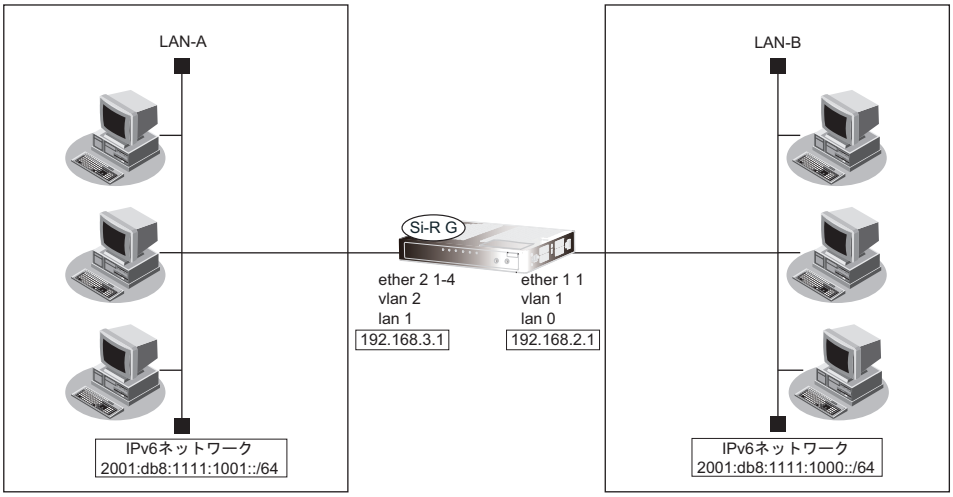
● コマンド

```
LAN-B側情報を設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip address 192.168.0.1/24 3
# lan 0 ip dhcp service off
# lan 0 ip route 0 192.168.2.0/24 192.168.0.10 1 1
# lan 0 ip route 1 default 192.168.0.5 1 1
# lan 0 ip rip use v1 v1 0 off
# lan 0 vlan 1

LAN-A側情報を設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off
```

```
# lan 1 vlan 2

自動時刻を設定する
# time auto server 192.168.0.20 time
# time auto interval start

ProxyDNS を設定する
# proxydns domain 0 any * any static 192.168.0.30
# proxydns address 0 any static 192.168.0.30

設定終了
# save

再起動
# reset
```

1.4　IPv4のネットワークにIPv6ネットワークを追加する

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]

- ETHERポート　：グループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：1
- プレフィックス／プレフィックス長　：2001:db8:1111:1001::/64

[LAN-B側]

- ETHERポート　：グループ1ポート1
- VLAN番号　：1
- lan定義番号　：0
- プレフィックス／プレフィックス長　：2001:db8:1111:1000::/64

● コマンド

```
LAN-B側情報を設定する
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:1000::/64
# lan 0 ipv6 ra mode send
# lan 0 ipv6 rip use on on 0
# lan 0 ipv6 rip site-local on

LAN-A側情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:1001::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 2001:db8:1111:1001::/64 30d 7d 0
# lan 1 ipv6 rip use on on 0
# lan 1 ipv6 rip site-local on

設定終了
# save
# commit
```

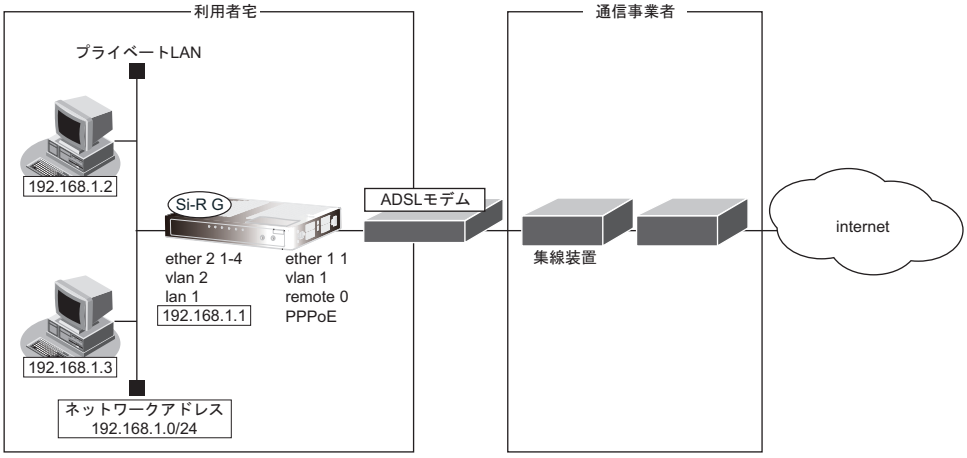
1.5　インターネットへPPPoEで接続する

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　マニュアル「トラブルシューティング」



● 設定条件

[通信事業者側]

- ETHERポート　：グループ1ポート1
- VLAN番号　：1
- 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）
- ETHERポート　：グループ1ポート1

[プライベートLAN側]

- ETHERポート　：グループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：1
- 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

- コマンド入力時は、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　マニュアル「コマンドユーザーズガイド」

- 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。

● コマンド

```
通信事業者側のETHERポートを設定する
# ether 1 1 vlan untag 1

プライベートLAN側のETHERポートを設定する
# ether 2 1-4 vlan untag 2

LAN情報を削除する
# delete lan

本装置のIPアドレスを設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

DHCPサーバを設定する
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip dhcp service server
# lan 1 ip nat mode off

通信事業者との接続情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip rip use off off 0 off
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect

ProxyDNSを設定する
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

設定終了
# save

再起動
# reset
```

1.6　インターネットへデータ通信モジュールを使用して接続する

ここでは、データ通信モジュールを使用して、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。

1.6.1　データ通信モジュール（wan コマンド設定）で接続する

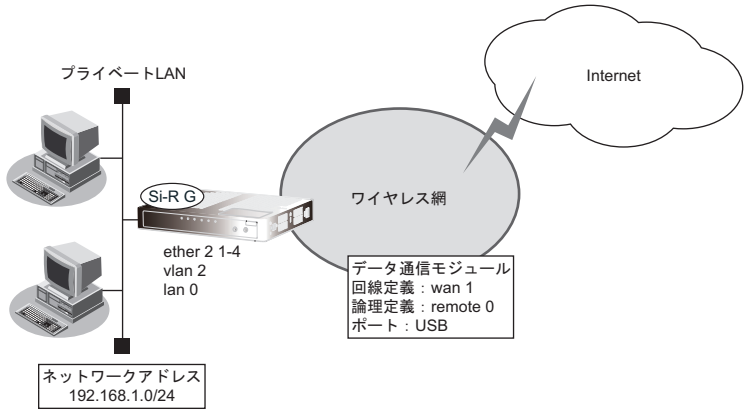
ここでは、データ通信モジュールを wan コマンド設定を使用して、ご購入時の設定のままインターネットへ接続する場合を例に説明します。

☛ 参照　対応データ通信モジュール（富士通ホームページ）
http://www.fujitsu.com/jp/products/network/router/sir/sirg100b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg110b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg200b/#supportcard

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　マニュアル「トラブルシューティング」



● 設定条件

[Internet 側]

- データ通信モジュール　：USB
- 認証 ID　：userid（通信事業者から提示された内容）
- 認証パスワード　：userpass（通信事業者から提示された内容）
- 電話番号　：*99***1#（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]

- 利用するポート　：ETHER グループ 2 ポート 1～4
- 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

- コマンド入力時は、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。だたし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛参照 マニュアル「コマンドユーザーズガイド」

- 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。
- データ通信モジュール接続では、以下の機能は動作しません。
  - テンプレート機能
  - 常時接続機能
- データ通信モジュールで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信モジュールによる発信は従量課金が発生するため、データ通信モジュール接続のアカウント情報を監視して不要な接続が行われていないか、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、強制切断を行う累計接続時間、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: {[USB]|[USB1]|[USB2]|[SLOT]} forced disconnection <target> <reason>

  ☛参照 マニュアル「メッセージ集」

  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モジュールのアカウント情報のクリア（clear modemmodule 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。

● 設定コマンド

```
ETHERグループ2のポート1～4を設定する
# ether 2 1-4 vlan untag 2

IPアドレスを設定する
# delete lan
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 2

DHCPサーバを設定する
# lan 0 ip dhcp info dns 192.168.1.1
# lan 0 ip dhcp info address 192.168.1.2/24 253
# lan 0 ip dhcp info time 1d
# lan 0 ip dhcp info gateway 192.168.1.1
# lan 0 ip dhcp service server

回線情報を設定する
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule
# wan 1 description L-03F

接続先の情報を設定する
# remote 0 description internet
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ap 0 description ISP-1
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 dial 0 number *99***1#
# remote 0 ap 0 idle 1m

強制切断を行う累計パケット数を設定する
# remote 0 ap 0 disconnect packet 100000 per128
```

```
ProxyDNS を設定する
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

設定終了
# save
# commit
```

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
NTT ドコモ mopera	（任意の文字列）	（任意の文字列）	*99***1#

1.6.2　データ通信モジュール（pseudo-ether コマンド設定）で接続する

ここでは、データ通信モジュールを pseudo-ether コマンド設定を使用して、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。

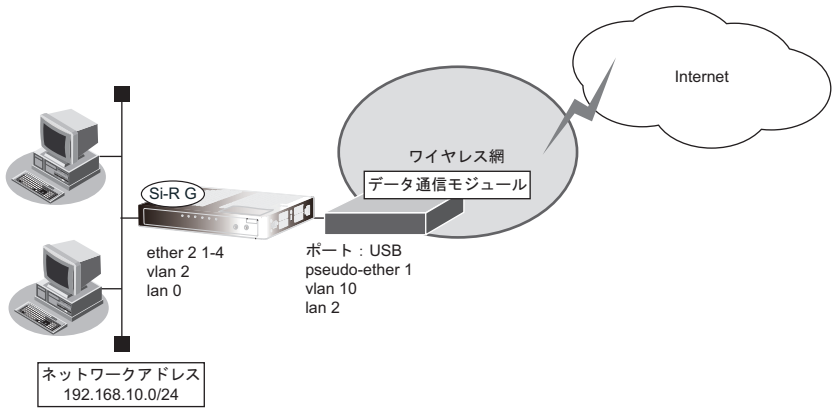
ルータタイプのデータ通信モジュールは、USB 上の ETHER ポート（pseudo-ether）で LAN 接続します。

☛参照　対応データ通信モジュール（富士通ホームページ）
http://www.fujitsu.com/jp/products/network/router/sir/sirg100b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg110b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg200b/#supportcard

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　マニュアル「トラブルシューティング」



● 設定条件

[Internet 側]

- データ通信モジュール　：USB
- pseudo-ether　：1
- IP アドレス　：DHCP クライアントで獲得する

[プライベート LAN 側]

- 利用するポート　：ETHER グループ 2 ポート 1～4
- IP アドレス　：192.168.10.1
- ネットワークアドレス／マスク　：192.168.10.0/24

こんな事に気をつけて

- コマンド入力時は、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。だたし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

  ☛参照　マニュアル「コマンドユーザーズガイド」

- 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。
- データ通信モジュールから DHCP で割り当てられるネットワークアドレスがほかの lan アドレスと重複しないように設計してください。

- 本装置からデータ通信モジュール（pseudo-ether）を操作してワイヤレス網に接続・切断することはできません。データ通信モジュールの設定に従ってワイヤレス網に接続します。
- ワイヤレス網との接続が失われてもpseudo-etherインタフェースはリンクアップしたままです。
- offlineコマンドでpseudo-etherを閉塞してもワイヤレス網とは切断しません。
- pseudo-etherインタフェースでは、以下の機能は利用できません。
  - タグVLAN機能
  - バックアップポート機能
  - STP機能
  - VLANプライオリティマッピング機能
  - シェーピング機能
  - 優先制御（WFQ）機能
  - IEEE802.1X認証機能
  - 不正端末アクセス防止機能（MACアドレス認証）

● 設定コマンド

```
ETHERグループ2のポート1～4を設定する
# ether 2 1-4 vlan untag 2

プライベートLAN側のIP アドレスを設定する
# delete lan
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 2

プライベートLAN側のDHCPサーバを設定する
# lan 0 ip dhcp info dns 192.168.10.1
# lan 0 ip dhcp info address 192.168.10.2/24 253
# lan 0 ip dhcp info time 1d
# lan 0 ip dhcp info gateway 192.168.10.1
# lan 0 ip dhcp service server

Internet側のETHERポート（pseudo-ether）を設定する
# pseudo-ether 1 description DATA_MODULE
# pseudo-ether 1 use on
# pseudo-ether 1 bind usb
# pseudo-ether 1 vlan untag 10

Internet側のLANのDHCPクライアントを設定する
# lan 2 ip dhcp service client
# lan 2 ip dhcp info time 1d
# lan 2 ip nat mode multi any 1 5m
# lan 2 vlan 10

ProxyDNSを設定する
# proxydns domain 0 any * any dhcp lan2
# proxydns address 0 any dhcp lan2

設定終了
# save
# reset
```

1.7　事業所LANをISDN（INS-TA）で接続する

適用機種　***Si-R G200B, Si-R G100B***

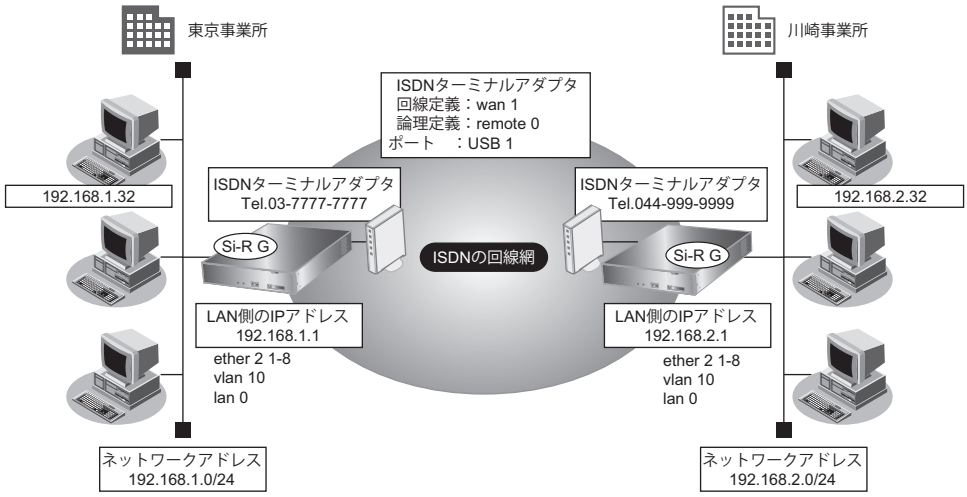
ここでは、データ通信モジュールとしてISDNターミナルアダプタを使用し、2つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。

☛参照　対応データ通信モジュール（富士通ホームページ）
http://www.fujitsu.com/jp/products/network/router/sir/sirg200b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg100b/#supportcard

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　マニュアル「トラブルシューティング」



ここでは、Si-R G200Bを例に説明します。

● 設定条件

- ISDNターミナルアダプタ　：USB1
- 発信者番号認証を使用する
- 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。

東京事業所の本装置を設定する

● コマンド

```
ETHERグループ2のポート1～8を設定する
# ether 2 1-8 vlan untag 10

IPアドレスを設定する
# delete lan
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

回線情報を設定する
# wan 1 use on
# wan 1 bind usb 1
# wan 1 line modemmodule
# wan 1 description V30slim

接続先の情報を設定する
# remote 0 name intranet
# remote 0 ap 0 name kawasaki
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth type any
# remote 0 ap 0 ppp auth send tokyo tokyopass
# remote 0 ap 0 ppp auth receive kawasaki kawapass
# remote 0 ap 0 dial 0 number 044-999-9999
# remote 0 ap 0 idle 1m
# remote 0 ip route 0 192.168.2.0/24 1

設定終了
# save
# commit
```

川崎事業所の本装置を設定する

● コマンド

```
ETHERグループ2のポート1～8を設定する
# ether 2 1-8 vlan untag 10

IPアドレスを設定する
# delete lan
# lan 0 ip address 192.168.2.1/24 3
# lan 0 vlan 10

回線情報を設定する
# wan 1 use on
# wan 1 bind usb 1
# wan 1 line modemmodule
# wan 1 description V30slim

接続先の情報を設定する
# remote 0 name intranet
# remote 0 ap 0 name tokyo
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth type any
# remote 0 ap 0 ppp auth send kawasaki kawapass
# remote 0 ap 0 ppp auth receive tokyo tokyopass
# remote 0 ap 0 dial 0 number 03-7777-7777
# remote 0 ap 0 idle 1m
# remote 0 ip route 0 192.168.1.0/24 1

設定終了
# save
# commit
```

1.8　複数の事業所LANをIP-VPN網を利用して接続する

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。

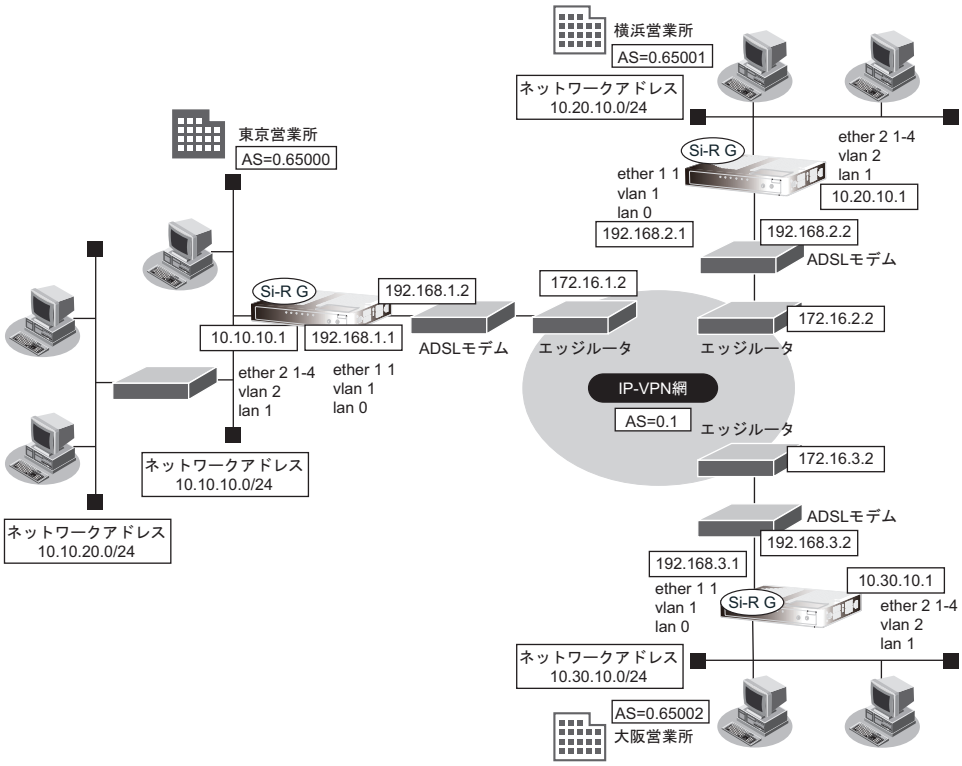
  ☛参照　マニュアル「トラブルシューティング」

- コマンド入力時は、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　マニュアル「コマンドユーザーズガイド」

- 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
- 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commitコマンドを実行した場合、接続中のセッションが一度切断されることがあります。

1.8.1　ADSL モデムを使用して IP-VPN 網と接続する



● 設定条件

- 本装置の ETHER グループ 1 ポート 1 と ADSL モデムの LAN ポートを LAN ケーブルで接続する。

[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　：0.1

[東京営業所]

IP-VPN 網側

- ETHER ポート　：グループ 1 ポート 1
- VLAN 番号　：1
- 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

東京営業所内

- ETHERポート　：グループ２ポート１～４
- VLAN番号　：2
- IPアドレス　：10.10.10.1
- ネットワークアドレス／マスク　：10.10.10.0/24
- ルーティングプロトコル　：RIPv2

BGP情報

- AS番号　：0.65000
- グレースフルリスタート　：使用する

［横浜営業所］

IP-VPN網側

- ETHERポート番号　：グループ１ポート１
- VLAN番号　：1
- LAN定義番号　：0
- 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

横浜営業所内

- ETHERポート番号　：グループ２ポート１～４
- VLAN番号　：2
- LAN定義番号　：1
- IP アドレス　：10.20.10.1
- ネットワークアドレス／ネットマスク　：10.20.10.0/24

BGP情報

- AS番号　：0.65001
- 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
- ETHERポート番号　：グループ１ポート１
- VLAN番号　：1
- LAN定義番号　：0
- IPアドレス　：192.168.3.1
- ネットワークアドレス／ネットマスク　：192.168.3.0/24

大阪営業所内

- ETHERポート番号　：グループ２ポート１～４
- VLAN番号　：2
- LAN定義番号　：1
- IP アドレス　：10.30.10.1
- ネットワークアドレス／ネットマスク　：10.30.10.0/24

BGP情報

- AS番号　: 0.65002
- 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

● コマンド

```
IP-VPN網側のインタフェースを設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip route 0 172.16.1.0/24 192.168.1.2 1
# lan 0 vlan 1

東京営業所内のインタフェースを設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 10.10.10.1/24 3
# lan 1 ip rip use v2m v2 0 off
# lan 1 vlan 2

ルーティングプロトコル情報を設定する
# routemanage ip redist rip bgp on
# routemanage ip redist bgp rip on
# bgp as 0.65000
# bgp ip network route 0 10.10.10.0/24
# bgp neighbor 0 address 172.16.1.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2
# bgp neighbor 0 graceful-restart family ipv4

設定終了
# save
# commit
```

横浜営業所を設定する

● コマンド

```
IP-VPN網側のインタフェースを設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip address 192.168.2.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.2.0/24 192.168.2.2 1
# lan 0 vlan 1

横浜営業所内のインタフェースを設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 10.20.10.1/24 3
# lan 1 vlan 2

ルーティングプロトコル情報を設定する
# bgp as 0.65001
# bgp ip network route 0 10.20.10.0/24
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

大阪営業所を設定する

● コマンド

```
IP-VPN網側のインタフェースを設定する
# ether 1 1 vlan untag 1

# lan 0 ip address 192.168.3.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.3.0/24 192.168.3.2 1
# lan 0 vlan 1

大阪営業所内のインタフェースを設定する
# ether 2 1-4 vlan untag 2

# lan 1 ip address 10.30.10.1/24 3
# lan 1 vlan 2

ルーティングプロトコル情報を設定する
# bgp as 0.65002
# bgp ip network route 0 10.30.10.0/24
# bgp neighbor 0 address 172.16.3.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

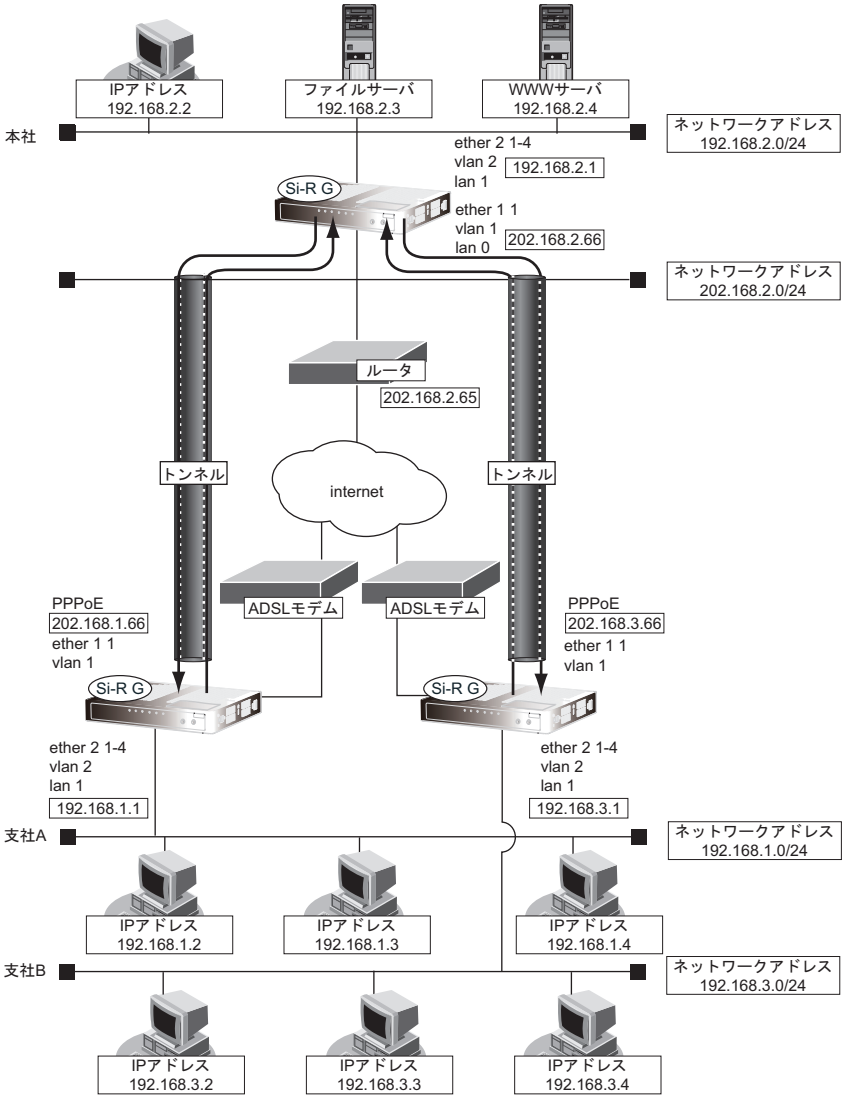
1.9　複数の事業所LANをVPN（IPsec）で接続する

ここでは、VPN（IPsec）で複数の事業所を接続する場合を例に説明します。

1.9.1　NATと併用しない固定IPアドレスでのVPN（自動鍵交換）

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。

ここでは以下のコマンドによって、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）］

PPPoE接続インターネット

- VLAN番号　：1
- lan定義番号　：0
- ユーザ認証ID　：userid1（プロバイダから提示された内容）
- 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ポート　：ETHERグループ１ポート１

支社Ａ内ローカルネットワーク

- ETHERポート　：グループ２ポート１～４
- VLAN番号　：2
- lan定義番号　：1
- プライベートIPアドレス　：192.168.1.1/24
- グローバルIPアドレス　：202.168.1.66（プロバイダから提示された内容）

［支社Ｂ（PPPoE常時接続）］

PPPoE接続インターネット

- VLAN番号　：1
- lan定義番号　：0
- ユーザ認証ID　：userid3（プロバイダから提示された内容）
- 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ポート　：ETHERグループ１ポート１

支社Ｂ内ローカルネットワーク

- ETHERポート　：グループ２ポート１～４
- VLAN番号　：2
- lan定義番号　：1
- プライベートIPアドレス　：192.168.3.1/24
- グローバルIPアドレス　：202.168.3.66（プロバイダから提示された内容）

［本社］

VPN終端装置側

- ETHERポート　：グループ１ポート１
- VLAN番号　：1
- lan定義番号　：0
- IPアドレス　：20.168.2.66/24
（プロバイダから割り当てられた固定IPアドレス）
- デフォルトルートのIPアドレス　：202.168.2.65（プロバイダから指定されたIPアドレス）

本社内ローカルネットワーク

- Etherポート　：グループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：1
- IPアドレス　：192.168.2.1/24

● 設定コマンド

[支社A（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

[支社B（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.3.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
# delete lan
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

● 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
- 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　：pre-shared（事前共有鍵方式）
- 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
- IPsec プロトコル　：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コマンド例を示します。

支社 A を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

本社を設定する

● コマンド

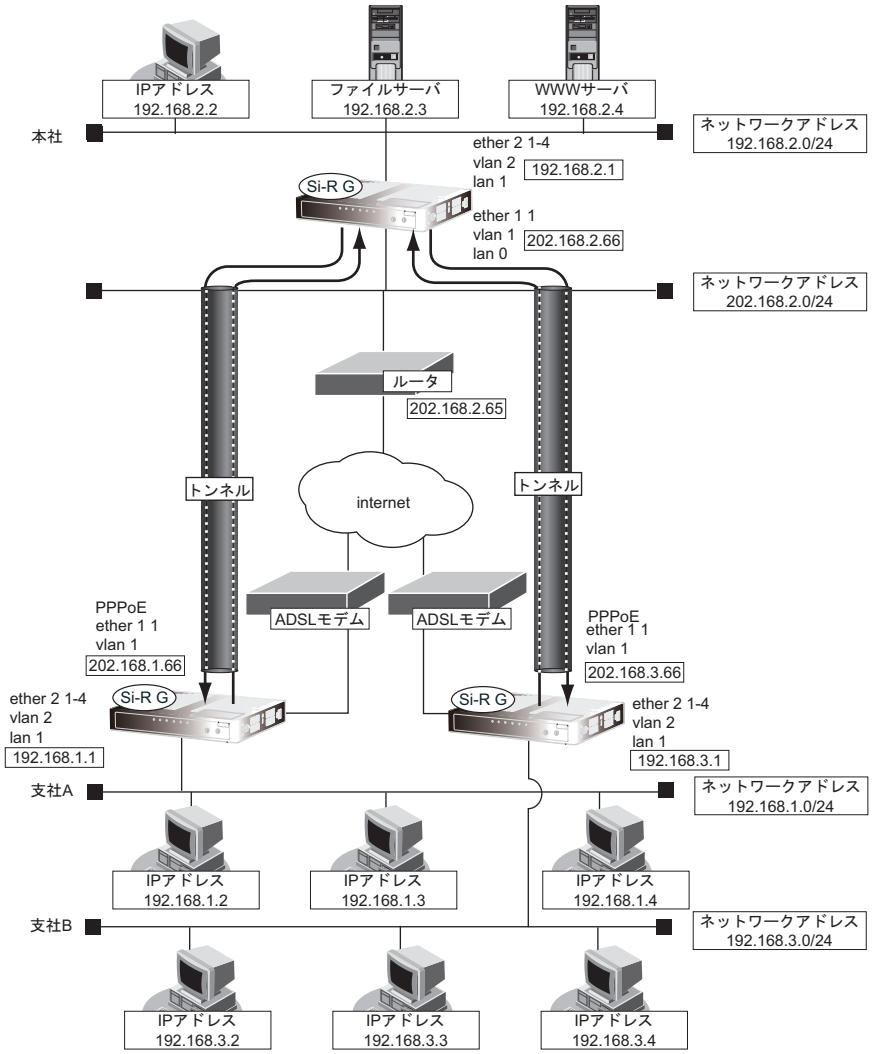
```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.3.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
```

```
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.9.2　NATと併用した固定IPアドレスでのVPN（自動鍵交換）

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。

ここでは以下のコマンドによって、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
- 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ポート　：ETHERグループ1ポート1

[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
- 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ポート　：ETHERグループ１ポート１

[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

● 設定コマンド

[支社Ａ（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi 202.168.1.66 1 5m
# remote 0 ip msschange 1414
```

[支社Ｂ（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.3.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi 202.168.3.66 1 5m
# remote 0 ip msschange 1414
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

● 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
- 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　：pre-shared（事前共有鍵方式）
- 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
- IPsec プロトコル　：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コマンド例を示します。

支社 A を設定する

● コマンド

```
インターネットへ IPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.1.66 500 10.0.1.1 500 17
# remote 0 ip nat static 1 202.168.1.66 any 10.0.1.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
インターネットへ IPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.3.66 500 10.0.3.1 500 17
# remote 0 ip nat static 1 202.168.3.66 any 10.0.3.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

本社を設定する

● コマンド

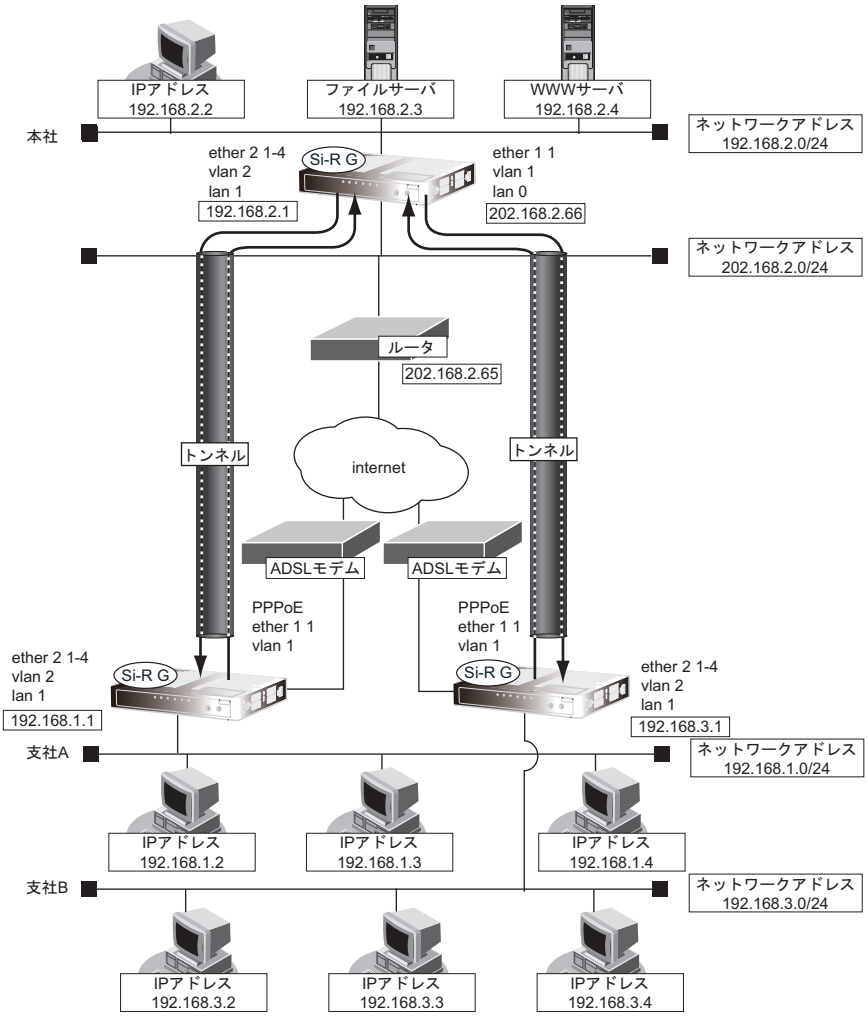
```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 10.0.1.1
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 10.0.3.1
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
```

```
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.9.3　NATと併用した可変IPアドレスでのVPN（自動鍵交換）

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、以下のコマンドによって、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 ポート　：ETHERグループ1ポート1

[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 ポート　：ETHERグループ1ポート1

[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

● 設定コマンド

[支社A（PPPoE接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
```

[支社B（PPPoE接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.3.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid3 userpass3
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

● 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（自装置名）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- 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プロトコル　：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コマンド例を示します。

支社 A（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

支社 B（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.3.1 500 any 500 17
# remote 0 ip nat static 1 192.168.3.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

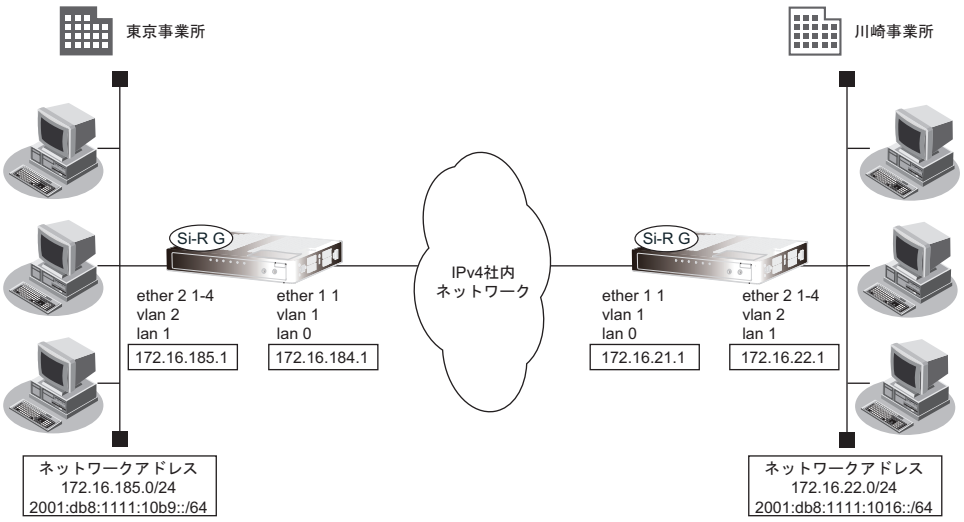
本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

1.10 IPv6の事業所LANをIPv4トンネルで接続する

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
- イントラネット側のIPv4アドレス　：172.16.184.1
- 東京事業所側のIPv4アドレス　：172.16.185.1
- 東京事業所側の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
- イントラネット側のIPv4アドレス　：172.16.21.1
- 川崎事業所側のIPv4アドレス　：172.16.22.1
- 川崎事業所側の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

- コマンド入力時は、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　マニュアル「コマンドユーザーズガイド」

- 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。

東京事業所を設定する

● コマンド

```
IPv4 で事業所間を接続する
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 172.16.184.1/24 3
# lan 0 ip rip use v1 v1 0
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 0 vlan 1
# lan 1 ip address 172.16.185.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off
# lan 1 vlan 2

IPv6 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 ifid auto
# lan 1 ipv6 address 0 2001:db8:1111:10b9::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 2001:db8:1111:10b9::/64 30d 7d c0

IP トンネル接続（川崎事業所）の情報を設定する
# remote 0 name v6kawasa
# remote 0 mtu 1280
# remote 0 ap 0 name tn-kawa
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.184.1
# remote 0 ap 0 tunnel remote 172.16.21.1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1016::/64 1

設定終了
# save

再起動
# reset
```

川崎事業所を設定する

● コマンド

```
IPv4 で事業所間を接続する
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan 0
# delete lan 1

# lan 0 ip address 172.16.21.1/24 3
# lan 0 ip rip use v1 v1 0 off
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 0 vlan 1
# lan 1 ip address 172.16.22.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off
# lan 1 vlan 2

IPv6 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 ifid auto
# lan 1 ipv6 address 0 2001:db8:1111:1016::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 2001:db8:1111:1016::/64 30d 7d c0

IP トンネル接続（東京事業所）の情報を設定する
# remote 0 name v6tokyo
# remote 0 mtu 1280
# remote 0 ap 0 name tn-tokyo
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.21.1
# remote 0 ap 0 tunnel remote 172.16.184.1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:10b9::/64 1

設定終了
# save

再起動
# reset
```

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 • remote ip address local コマンドで設定した自側 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。
  remote 0 ap 0 tunnel local 192.168.1.1
  remote 0 ap 0 tunnel remote 172.31.0.1

静的 NAT 設定：

- lan 0 ip nat static 0 192.168.1.1 any 172.16.0.1 any 41

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

remote 0 ap 0 tunnel local 172.31.0.1
remote 0 ap 0 tunnel remote 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）

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any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）lan 0 ip address 192.168.1.1/24に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。

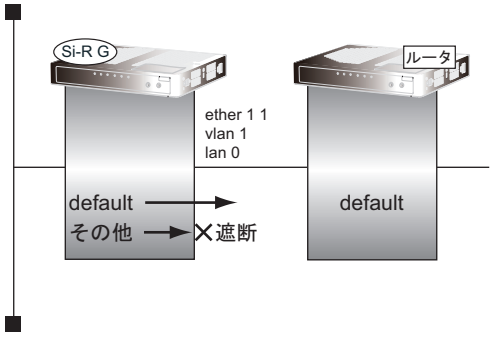
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

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

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。



● 前提条件

- ETHERグループ 1 ポート 1 に lan 0 定義が使用されている

● 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コマンド例を示します。

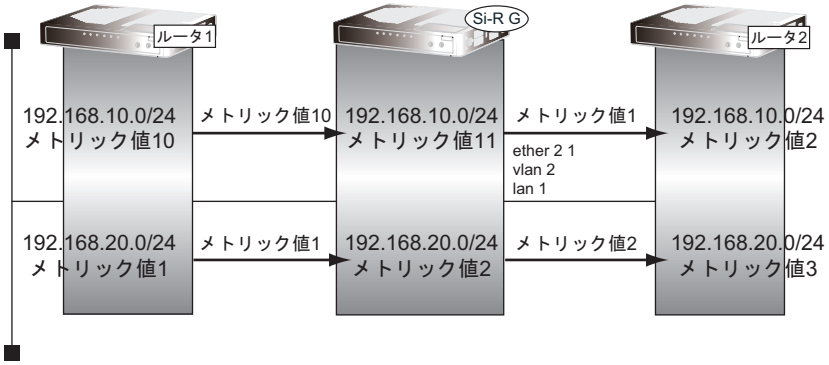
● コマンド

```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass out
# lan 0 ip rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject out
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ETHERグループ２ポート１にlan １定義が使用されている

● 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コマンド例を示します。

● コマンド

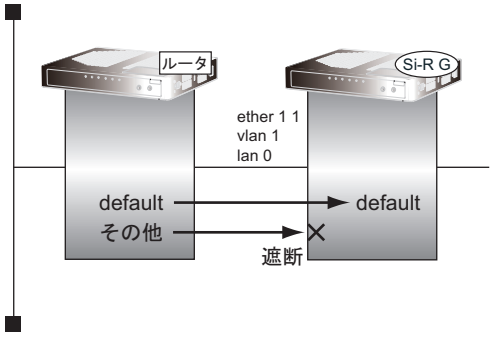
```
192.168.10.0/24をメトリック値１で送信する
# lan 1 ip rip filter 0 act pass out
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 1

その他の経路情報はメトリック値を変更しないで送信する
# lan 1 ip rip filter 1 act pass out
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ETHERグループ 1 ポート 1 に lan 0 定義が使用されている

● 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

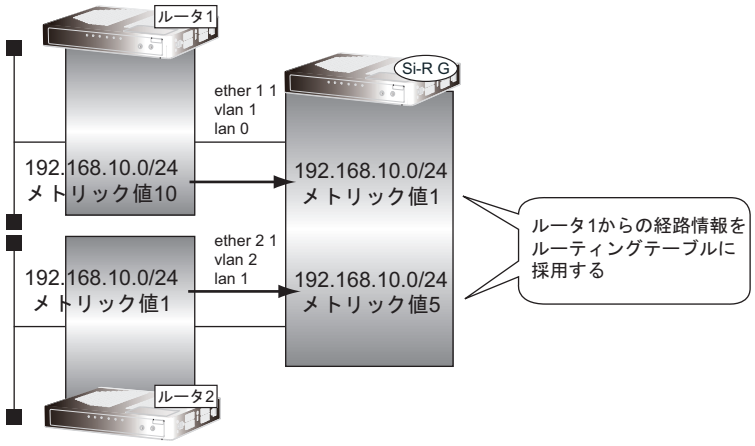
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject in
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている
- ether 2 1 に lan 1 定義が使用されている

● 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コマンド例を示します。

● コマンド

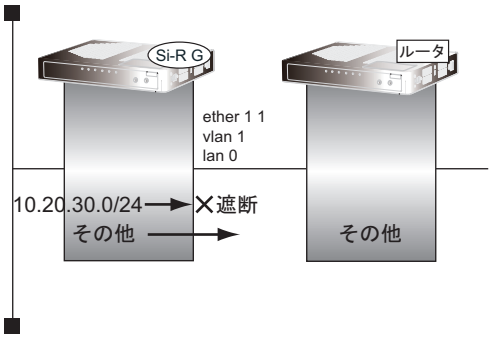
```
lan 0 で 192.168.10.0/24 の経路情報を受信した場合、メトリック値 1 で受信する
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route 192.168.10.0/24
# lan 0 ip rip filter 0 set metric 1

lan 0 でのその他の経路情報はすべて受信する
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

lan 1 で 192.168.10.0/24 の経路情報を受信した場合、メトリック値 5 で受信する
# lan 1 ip rip filter 0 act pass in
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 5

lan 1 でのその他の経路情報はすべて受信する
# lan 1 ip rip filter 1 act pass in
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている

● 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

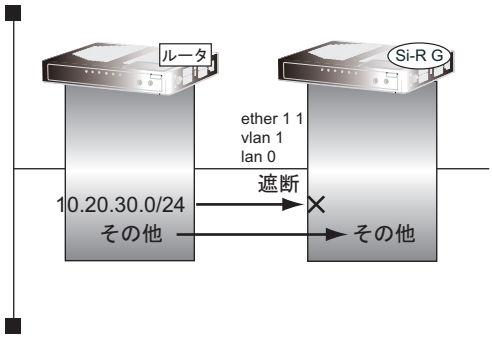
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject out
# lan 0 ip rip filter 0 route 10.20.30.0/24

その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass out
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

2.1.6　特定の経路情報の受信を禁止する

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている

● 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コマンド例を示します。

● コマンド

```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject in
# lan 0 ip rip filter 0 route 10.20.30.0/24

その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

設定終了
# save
# commit
```

2.2　RIPの経路を制御する（IPv6）

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
- フィルタリング条件（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any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。

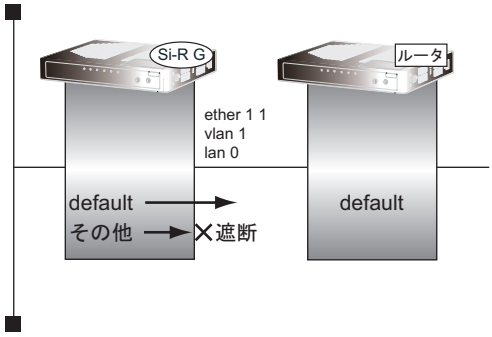
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

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

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている

● 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コマンド例を示します。

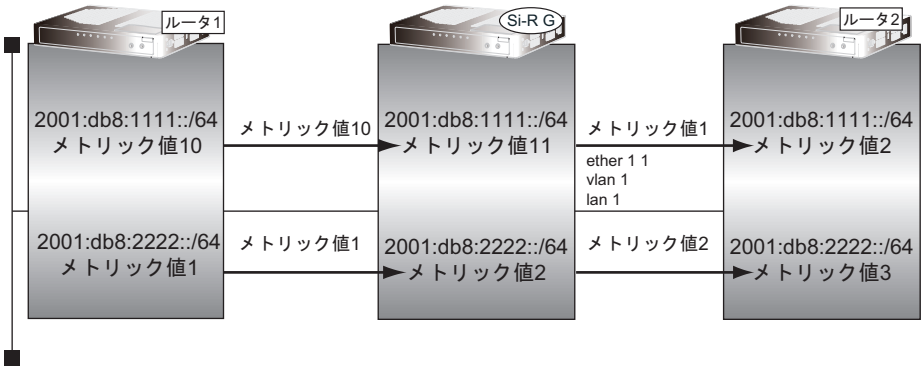
● コマンド

```
デフォルトルートの経路情報を透過させる
# lan 0 ipv6 rip filter 0 act pass out
# lan 0 ipv6 rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ipv6 rip filter 1 act reject out
# lan 0 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ether 1 1にlan 0定義が使用されている
- lan 0にIPv6の基本情報が定義されている

● 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コマンド例を示します。

● コマンド

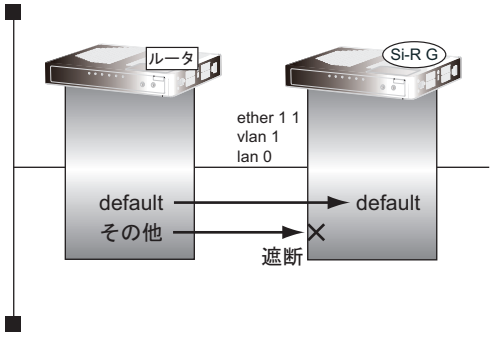
```
2001:db8:1111::/64の経路情報をメトリック値１で送信する
# lan 1 ipv6 rip filter 0 act pass out
# lan 1 ipv6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ipv6 rip filter 0 set metric 1

その他の経路情報はメトリック値を変更しないで送信する
# lan 1 ipv6 rip filter 1 act pass out
# lan 1 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている

● 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

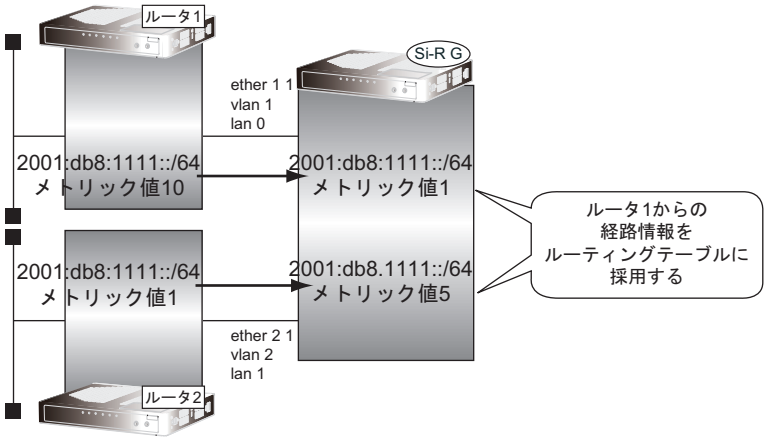
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
デフォルトルートの経路情報を透過させる
# lan 0 ipv6 rip filter 0 act pass in
# lan 0 ipv6 rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ipv6 rip filter 1 act reject in
# lan 0 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている
- ether 2 1 に lan 1 定義が使用されている
- lan0 に IPv6 の基本情報が定義されている
- lan1 に IPv6 の基本情報が定義されている

● 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コマンド例を示します。

● コマンド

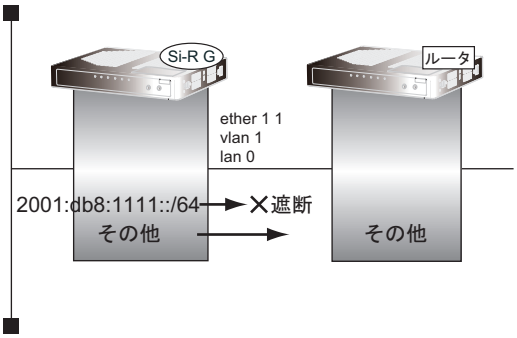
```
lan 0 で 2001:db8:1111::/64 の経路情報を受信した場合、メトリック値 1 で受信する
# lan 0 ipv6 rip filter 0 act pass in
# lan 0 ipv6 rip filter 0 route 2001:db8:1111::/64
# lan 0 ipv6 rip filter 0 set metric 1

lan 0 でのその他の経路情報はすべて受信する
# lan 0 ipv6 rip filter 1 act pass in
# lan 0 ipv6 rip filter 1 route any

lan 1 で 2001:db8:1111::/64 の経路情報を受信した場合、メトリック値 5 で受信する
# lan 1 ipv6 rip filter 0 act pass in
# lan 1 ipv6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ipv6 rip filter 0 set metric 5

lan 1 でのその他の経路情報はすべて受信する
# lan 1 ipv6 rip filter 1 act pass in
# lan 1 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

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

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている

● 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

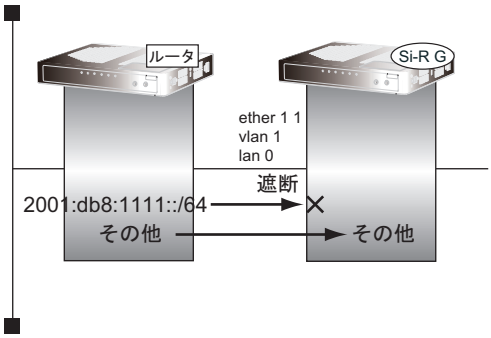
上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

● コマンド

```
2001:db8:1111::/64 の経路情報を遮断する
# lan 0 ipv6 rip filter 0 act reject out
# lan 0 ipv6 rip filter 0 route 2001:db8:1111::/64

その他の経路情報はすべて透過させる
# lan 0 ipv6 rip filter 1 act pass out
# lan 0 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

2.2.6　特定の経路情報の受信を禁止する

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。



● 前提条件

- ether 1 1 に lan 0 定義が使用されている

● 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コマンド例を示します。

● コマンド

```
2001:db8:1111::/64 の経路情報を遮断する
# lan 0 ipv6 rip filter 0 act reject in
# lan 0 ipv6 rip filter 0 route 2001:db8:1111::/64

その他の経路情報はすべて透過させる
# lan 0 ipv6 rip filter 1 act pass in
# lan 0 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

2.3 OSPFv2 を使用したネットワークを構築する（IPv4）

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。

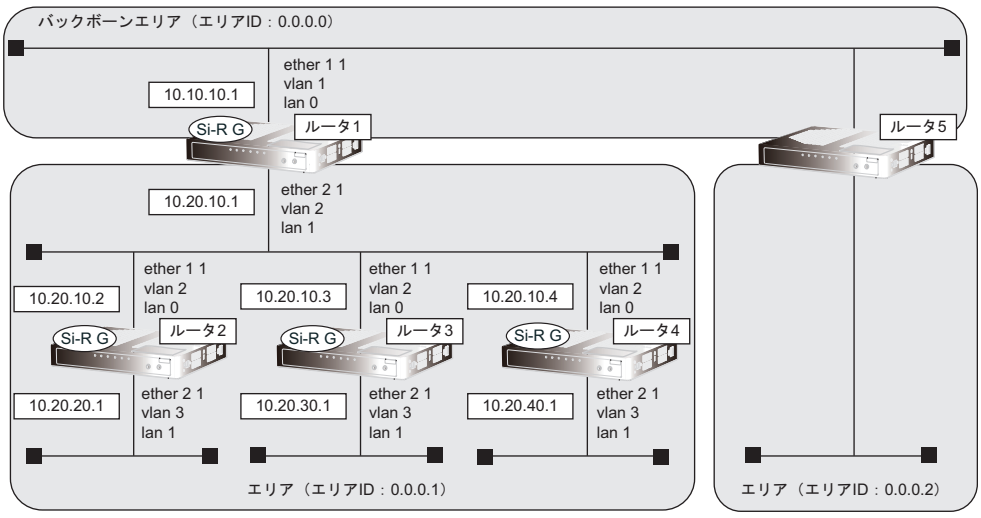
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

参照 マニュアル「機能説明書」

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、本装置の電源再投入、commit/reset コマンド実行にかかわらず、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 commit コマンドを実行した場合、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。

インタフェース数	（30000÷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。



● 前提条件

- すべての Si-R G で NAT 機能および DHCP クライアント機能を使用しない
- 各装置で経路情報以外の設定がされている

● 設定条件

[ルータ 1 でのルーティングプロトコル情報]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.0
- lan 1 での OSPF エリア ID　：0.0.0.1
- lan 1 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]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.1
- lan 1 での OSPF エリア ID　：0.0.0.1
- lan 0 でのルータ優先度　：1
- lan 1 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]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.1
- lan 1 での OSPF エリア ID　：0.0.0.1
- lan 0 でのルータ優先度　：255
- lan 1 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]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.1
- lan 1 での OSPF エリア ID　：0.0.0.1
- lan 1 での passive-interface 設定　：設定する
- lan 0 でのルータ優先度　：1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

ルータ 1 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1
# lan 1 ip ospf priority 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 range 0 10.20.0.0/16

設定終了
# save
# commit
```

ルータ 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 255
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

ルータ 4 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

2.3.1　スタブエリアを使う

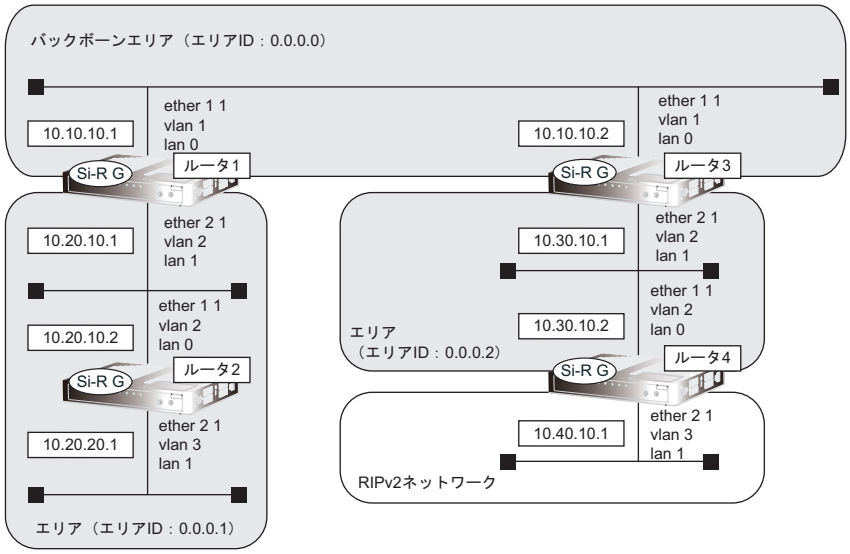
OSPF 以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

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。



● 前提条件

- すべての Si-R G で NAT 機能および DHCP クライアント機能を使用しない
- 各装置で経路情報以外の設定がされている

● 設定条件

[東京営業所]

[ルータ 1 でのルーティングプロトコル情報]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.0
- lan 1 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]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.1
- lan 1 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]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 での OSPF エリア ID　：0.0.0.0
- lan 1 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]

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：RIP V2,OSPF
- lan 0 での OSPF エリア ID　：0.0.0.2
- lan 1 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

ルータ 1 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 type stub

設定終了
# save
# commit
```

ルータ 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1
# ospf ip area 0 type stub

設定終了
# save
# commit
```

ルータ 3 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 type nssa

設定終了
# save
# commit
```

ルータ 4 を設定する

● コマンド

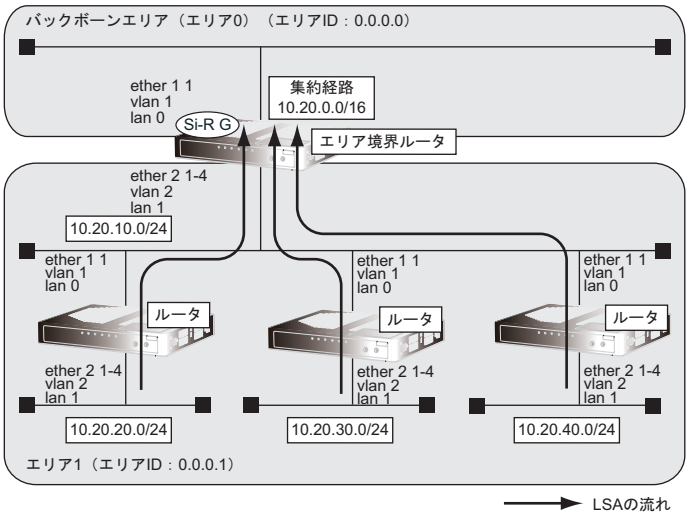
```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip rip use v2m v2 0 off
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

ルーティングマネージャ情報を設定する
# routemanage ip redist ospf rip on
# routemanage ip redist rip ospf on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.2
# ospf ip area 0 type nssa

設定終了
# save
# commit
```

2.4　OSPF の経路を制御する（IPv4）

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

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。



● 前提条件

- 各装置で経路情報以外の設定がされている

● 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

- lan 0 でのルーティングプロトコル　：OSPF
- lan 1 でのルーティングプロトコル　：OSPF
- lan 0 でのエリア ID　：0.0.0.0
- lan 1 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

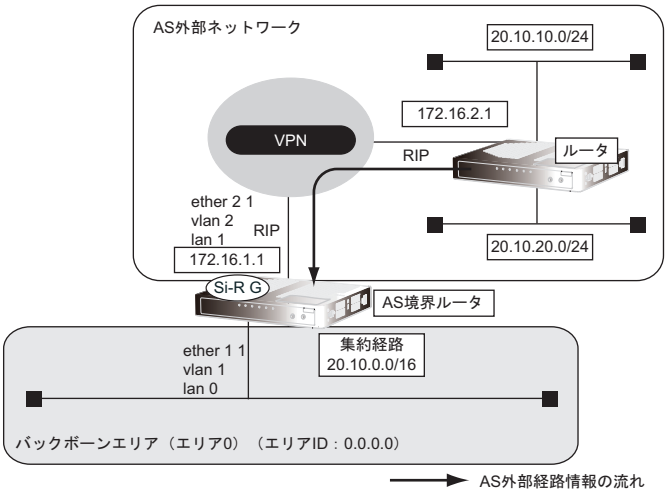
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
OSPF で使用するインタフェースを設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1

集約経路を設定する
# ospf ip area 1 range 0 10.20.0.0/16

設定終了
# save
# commit
```

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

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。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- lan 1 インタフェースに RIPv2 を使用する設定がされている

● 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

- lan 0 でのルーティングプロトコル　：OSPF
- lan 0 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
- OSPF に再配布する RIP 経路　：20.10.0.0/16 でマスクした結果が一致する経路だけを再配布

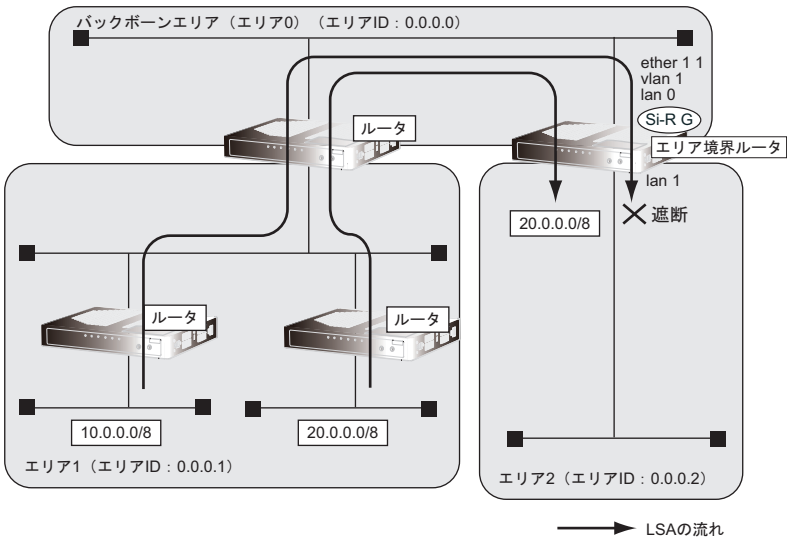
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
OSPF で使用するインタフェースを設定する
# lan 0 ip ospf use on 0

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0

OSPF に広報する AS 外部経路を設定する
# routemanage ip redist ospf rip on

集約経路を設定する
# ospf ip summary 0 20.10.0.0/16

設定終了
# save
# commit
```

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

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

- OSPF以外のlan 0およびremote 0設定がされている

● 設定条件

- lan 0でのルーティングプロトコル　：OSPF
- lan 1でのルーティングプロトコル　：OSPF
- lan 0でのエリアID　：0.0.0.0
- lan 1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コマンド例を示します。

● コマンド

```
OSPFで使用するインタフェースを設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2

エリア２に注入する経路情報を制限する
# ospf ip area 1 type3-lsa 0 reject 10.0.0.0/8 in exact
# ospf ip area 1 type3-lsa 1 pass any in

設定終了
# save
# commit
```

2.5　OSPF機能を使う（IPv6）

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。

2.5.1　OSPFネットワークを構築する

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

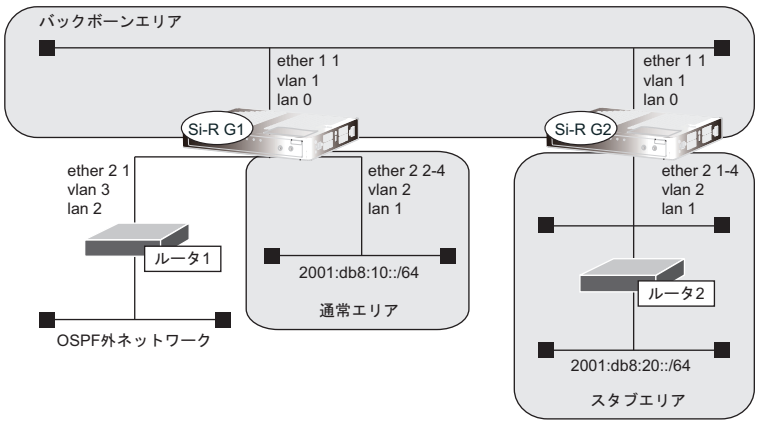
OSPF機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF機能は使用しないでください。

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、本装置の電源再投入、commit/resetコマンドの実行にかかわらず、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
（10000÷本装置保有LSA数）未満	（20000÷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。



● 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（lan ipv6 use on）がされている
- 本装置 1 の lan 1 には、グローバルアドレスが設定されている
- 本装置 1 の lan 2 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]

- lan 0 はバックボーンエリアに属する
- lan 1 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]

- lan 0 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
- lan 1 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コマンド例を示します。

本装置 1 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ipv6 ospf use on 0
# lan 1 ipv6 ospf use on 1
# lan 1 ipv6 ospf passive on

OSPF 情報を設定する
# ospf ipv6 id 100.0.0.1
# ospf ipv6 area 0 id 0.0.0.0
# ospf ipv6 area 1 id 0.0.0.1

ルーティングマネージャ情報を設定する
# routemanage ipv6 redist ospf static on

設定終了
# save
# commit
```

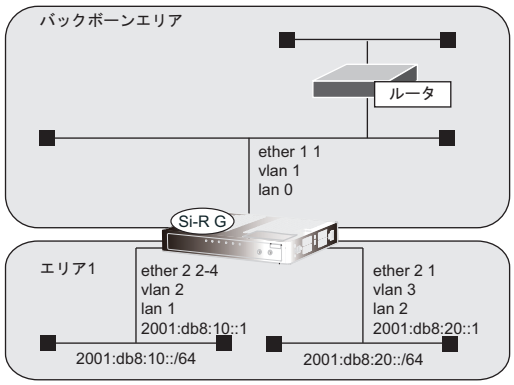
本装置 2 を設定する

● コマンド

```
LAN 情報を設定する
# lan 0 ipv6 ospf use on 0
# lan 0 ipv6 ospf priority 255
# lan 1 ipv6 ospf use on 1

OSPF 情報を設定する
# ospf ipv6 id 100.0.0.2
# ospf ipv6 area 0 id 0.0.0.0
# ospf ipv6 area 1 id 0.0.0.2
# ospf ipv6 area 1 type stub

設定終了
# save
# commit
```

2.5.2　エリア境界ルータでエリア内部経路を集約する

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（lan ipv6 use on）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、lan 0、lan 1、lan 2 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
  lan 1　　: 2001:db8:10::1/64
  lan 2　　: 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コマンド例を示します。

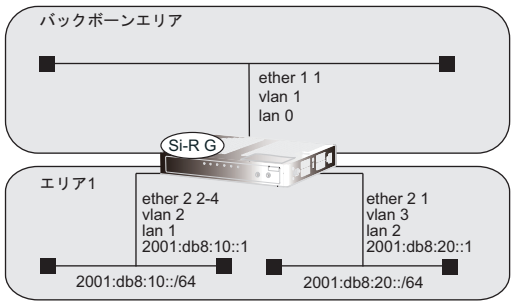
本装置を設定する

● コマンド

```
OSPF 情報を設定する
# ospf ipv6 area 1 range 0 2001:db8::/32 100

設定終了
# save
# commit
```

2.5.3　エリア境界ルータで不要な経路情報を遮断する

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（lan ipv6 use on）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、lan 0、lan 1、lan 2 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
  lan 1　　: 2001:db8:10::1/64
  lan 2　　: 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コマンド例を示します。

本装置を設定する

● コマンド

```
OSPF 情報を設定する
#  ospf ipv6 area 1 inter-area-prefix 0 reject 2001:db8:20::/64 out
#  ospf ipv6 area 1 inter-area-prefix 1 pass any  out

設定終了
# save
# commit
```

2.6　BGP の経路を制御する（IPv4）

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。

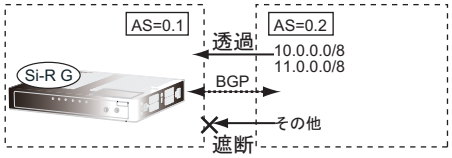
☛参照 マニュアル「機能説明書」

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。
- 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 commit コマンドを実行した場合、接続中のセッションが一度切断されることがあります。
- 動的定義反映で BGP IPv4 フィルタを設定した場合、動的定義反映後に送受信する経路情報に対してフィルタリングを実施します。動的定義反映前に送受信した経路情報に対してフィルタリングを実施する場合は、BGP IPv4 セッションのクリア機能を使用してください。

2.6.1　特定の経路情報の受信を透過させる

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

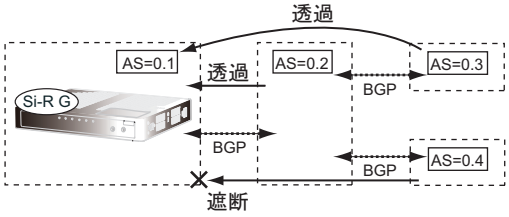
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 ip filter 0 act pass in
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 1 act pass in
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 2 act reject in
# bgp neighbor 0 ip filter 2 route any

設定終了
# save
# commit
```

2.6.2　特定の AS からの経路情報の受信を遮断する

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

- AS0.4 からの経路情報を遮断
- その他はすべて透過

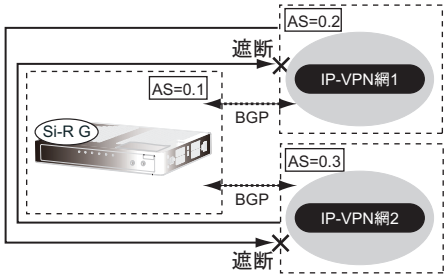
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 ip filter 0 act reject in
# bgp neighbor 0 ip filter 0 as 0.4
# bgp neighbor 0 ip filter 1 act pass in
# bgp neighbor 0 ip filter 1 route any

設定終了
# save
# commit
```

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

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

- AS0.2 から AS0.3 への経路情報を遮断
- AS0.3 から AS0.2 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コマンド例を示します。

● コマンド

フィルタリング条件を設定する

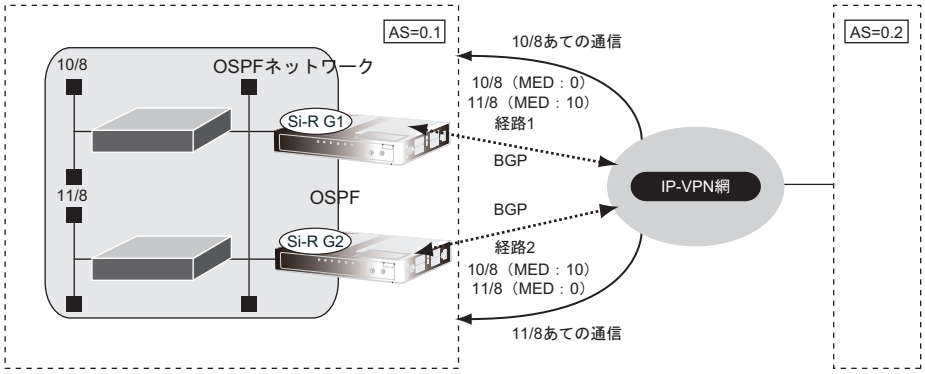
IP-VPN 網 1 への送信を遮断する
```
# bgp neighbor 0 ip filter 0 act reject out
# bgp neighbor 0 ip filter 0 as 0.3
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route any
```

IP-VPN 網 2 への送信を遮断する
```
# bgp neighbor 1 ip filter 0 act reject out
# bgp neighbor 1 ip filter 0 as 0.2
# bgp neighbor 1 ip filter 1 act pass out
# bgp neighbor 1 ip filter 1 route any
```

設定終了
```
# save
# commit
```

2.6.4　冗長構成の通信経路を使用する

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 AS0.1 で IP-VPN 網を経由した AS0.2 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
- AS0.1 内の OSPF ネットワークでの経路変更は BGP で AS0.2 に広報する

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

[本装置 1]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 ip filter 0 act pass out
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 0 set medmetric 0
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 1 set medmetric 10

その他のすべての経路は透過する
# bgp neighbor 0 ip filter 2 act pass out
# bgp neighbor 0 ip filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on

設定終了
# save
# commit
```

[本装置 2]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 ip filter 0 act pass out
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 0 set medmetric 10
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 1 set medmetric 0

その他のすべての経路は透過する
# bgp neighbor 0 ip filter 2 act pass out
# bgp neighbor 0 ip filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on

設定終了
# save
# commit
```

2.7　BGP機能を使う（IPv6）

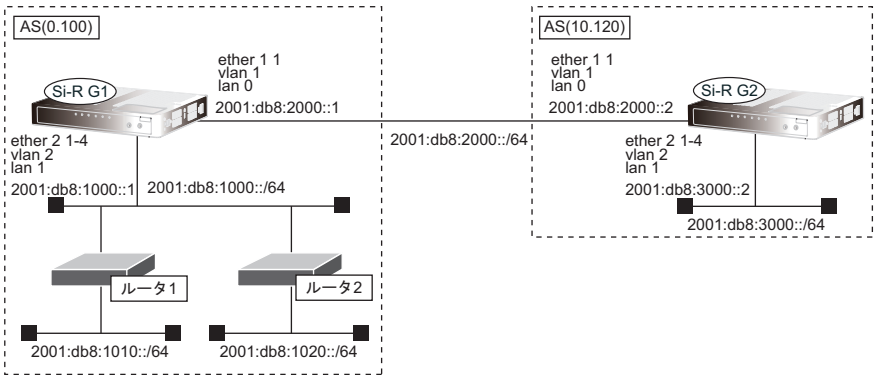
本装置を経由して、ほかのルータに送受信する経路情報に変更を加えることで、意図的にトラフィックを制御することができます。

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。
- 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commitコマンドを実行した場合、接続中のセッションが一度切断されることがあります。
- 動的定義反映でBGP IPv6フィルタを設定した場合、動的定義反映後に送受信する経路情報に対してフィルタリングを実施します。動的定義反映前に送受信した経路情報に対してフィルタリングを実施する場合は、BGP IPv6セッションのクリア機能を使用してください。

2.7.1　BGPでIPv6経路情報を交換する

BGPを使用したIPv6経路情報の交換について説明します。



● 前提条件

- 本装置1、2間でEBGPを使用し、IPv6経路情報の交換を行う
- 本装置1のlan 0には、2001:db8:2000::1/64のアドレスが設定されている
- 本装置1のlan 1には、2001:db8:1000::1/64のアドレスが設定されている
- 本装置1のlan 1側では、RIP（IPv6）による経路交換が行われている
- 本装置2のlan 0には、2001:db8:2000::2/64のアドレスが設定されている
- 本装置2のlan 1には、2001:db8:3000::2/64のアドレスが設定されている

● 設定条件

[本装置 1]

- RIP（IPv6）経路情報を BGP で再配布
- BGP（IPv6）経路情報を RIP で再配布
- AS 番号（0.100）に属している
- BGP-ID は、1.0.0.0

[本装置 2]

- AS 番号（10.120）に属している
- BGP-ID は、2.0.0.0
- BGP ネットワークを使用し、lan 1 のインタフェース経路を BGP で広報

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置 1 を設定する

● コマンド

```
ルーティングマネージャ情報を設定する
# routemanage ipv6 redist rip bgp on
# routemanage ipv6 redist bgp rip on

BGP 情報を設定する
# bgp as 0.100
# bgp id 1.0.0.0
# bgp neighbor 0 address 2001:db8:2000::2
# bgp neighbor 0 as 10.120
# bgp neighbor 0 family ipv6
# bgp neighbor 0 source 2001:db8:2000::1

設定終了
# save
# commit
```

本装置 2 を設定する

● コマンド

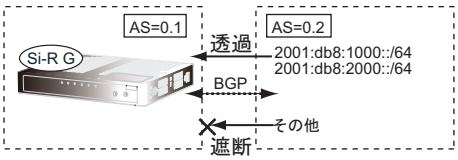
```
BGP 情報を設定する
# bgp as 10.120
# bgp id 2.0.0.0
# bgp ipv6 network route 0 2001:db8:3000::/64
# bgp ipv6 network igp on
# bgp neighbor 0 address 2001:db8:2000::1
# bgp neighbor 0 as 0.100
# bgp neighbor 0 family ipv6
# bgp neighbor 0 source 2001:db8:2000::2

設定終了
# save
# commit
```

こんな事に気をつけて

IPv6 で BGP を使用する場合は、BGP 自側 IP アドレスを必ず設定してください。

2.7.2　特定の経路情報の受信を透過させる

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

- 2001:db8:1000::/64 のネットワークの経路情報を透過
- 2001:db8:2000::/64 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

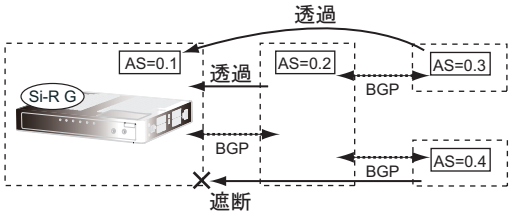
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 ipv6 filter 0 act pass in
# bgp neighbor 0 ipv6 filter 0 route 2001:db8:1000::/64
# bgp neighbor 0 ipv6 filter 1 act pass in
# bgp neighbor 0 ipv6 filter 1 route 2001:db8:2000::/64
# bgp neighbor 0 ipv6 filter 2 act reject in
# bgp neighbor 0 ipv6 filter 2 route any

設定終了
# save
# commit
```

2.7.3　特定の AS からの経路情報の受信を遮断する

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

- AS0.4 からの経路情報を遮断
- その他はすべて透過

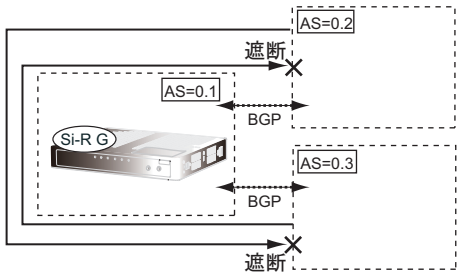
上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

```
フィルタリング条件を設定する
# bgp neighbor 0 ipv6 filter 0 act reject in
# bgp neighbor 0 ipv6 filter 0 as 0.4
# bgp neighbor 0 ipv6 filter 1 act pass in
# bgp neighbor 0 ipv6 filter 1 route any

設定終了
# save
# commit
```

2.7.4　特定の AS から受信した経路情報の送信を遮断する

本装置で AS0.2 と AS0.3 の通信を中継しないようにする設定方法を説明します。



● 経路情報の設計

- AS0.2 から AS0.3 への経路情報を遮断
- AS0.3 から AS0.2 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コマンド例を示します。

● コマンド

フィルタリング条件を設定する

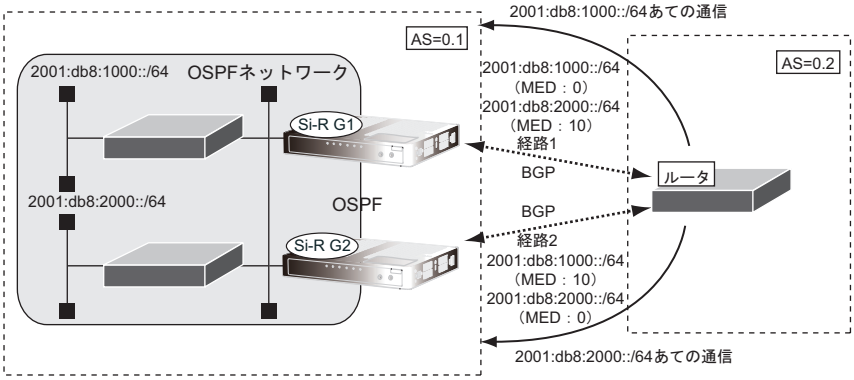
AS0.2 への送信を遮断する
```
# bgp neighbor 0 ipv6 filter 0 act reject out
# bgp neighbor 0 ipv6 filter 0 as 0.3
# bgp neighbor 0 ipv6 filter 1 act pass out
# bgp neighbor 0 ipv6 filter 1 route any
```

AS0.3 への送信を遮断する
```
# bgp neighbor 1 ipv6 filter 0 act reject out
# bgp neighbor 1 ipv6 filter 0 as 0.2
# bgp neighbor 1 ipv6 filter 1 act pass out
# bgp neighbor 1 ipv6 filter 1 route any
```

設定終了
```
# save
# commit
```

2.7.5　冗長構成の通信経路を使用する

ルータに接続する経路を 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 AS0.1 でルータを経由した AS0.2 への通信経路を冗長化する
- 2001:db8:1000::/64 への通信は経路 1 を優先経路とし、2001:db8:2000::/64 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
- AS0.1 内の OSPF ネットワークでの経路変更は BGP で AS0.2 に広報する

上記の経路情報に従って設定する場合のコマンド例を示します。

● コマンド

[本装置 1]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 ipv6 filter 0 act pass out
# bgp neighbor 0 ipv6 filter 0 route 2001:db8:1000::/64
# bgp neighbor 0 ipv6 filter 0 set medmetric 0
# bgp neighbor 0 ipv6 filter 1 act pass out
# bgp neighbor 0 ipv6 filter 1 route 2001:db8:2000::/64
# bgp neighbor 0 ipv6 filter 1 set medmetric 10

その他のすべての経路は透過する
# bgp neighbor 0 ipv6 filter 2 act pass out
# bgp neighbor 0 ipv6 filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ipv6 redist bgp ospf on

設定終了
# save
# commit
```

[本装置 2]

```
経路情報に MED メトリック値を付加する
# bgp neighbor 0 ipv6 filter 0 act pass out
# bgp neighbor 0 ipv6 filter 0 route 2001:db8:1000::/64
# bgp neighbor 0 ipv6 filter 0 set medmetric 10
# bgp neighbor 0 ipv6 filter 1 act pass out
# bgp neighbor 0 ipv6 filter 1 route 2001:db8:2000::/64
# bgp neighbor 0 ipv6 filter 1 set medmetric 0

その他のすべての経路は透過する
# bgp neighbor 0 ipv6 filter 2 act pass out
# bgp neighbor 0 ipv6 filter 2 route any

BGP で OSPF 経路を広報する
# routemanage ipv6 redist bgp ospf on

設定終了
# save
# commit
```

2.8　マルチキャスト機能を使う

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。

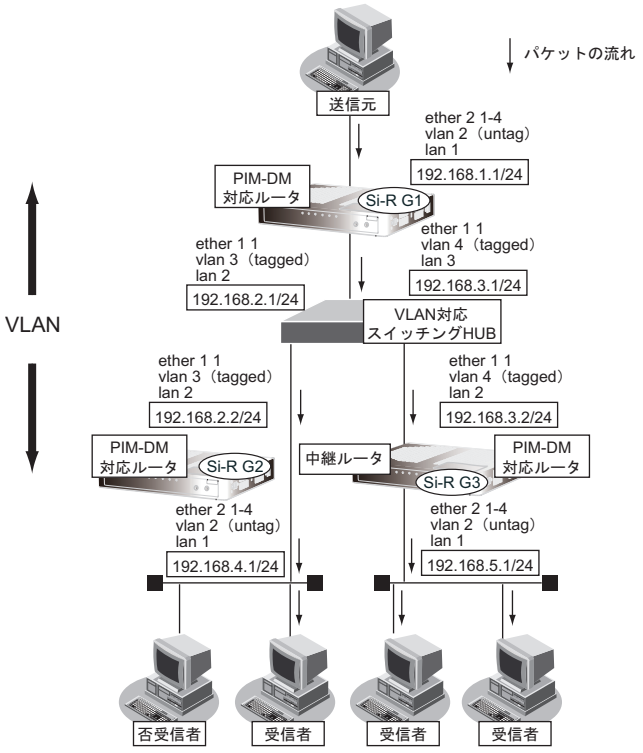
☛参照 マニュアル「機能説明書」

2.8.1　マルチキャスト機能（PIM-DM）を使う

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。

● 設定条件

- 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：3　　ネットワークアドレス：192.168.2.0/24
  VLAN ID：4　　ネットワークアドレス：192.168.3.0/24
- 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]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　　：192.168.1.1/24、VLAN ID 2（タグなし）、ETHERグループ2ポート1～4
  lan 2　　：192.168.2.1/24、VLAN ID 3（タグあり）、ETHERグループ1ポート1
  lan 3　　：192.168.3.1/24、VLAN ID 4（タグあり）、ETHERグループ1ポート1
- 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2]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　　：192.168.4.1/24、VLAN ID 2（タグなし）、ETHERグループ2ポート1～4
  lan 2　　：192.168.2.2/24、VLAN ID 3（タグあり）、ETHERグループ1ポート1
- 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3]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　　：192.168.5.1/24、VLAN ID 2（タグなし）、ETHERグループ2ポート1～4
  lan 2　　：192.168.3.2/24、VLAN ID 4（タグあり）、ETHERグループ1ポート1
- 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 3,4
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode pimdm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan 3

lan 3 情報を設定する
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimdm
# lan 3 vlan 4

設定終了
# save
# commit
```

[本装置2]

```
ether ポートを設定する
# ether 1 1 vlan tag 3
# ether 2 1-4 vlan untag 2

lan 設定を削除する
# delete lan

lan 1 を設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode pimdm
# lan 1 vlan 2

lan 2 を設定する
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan 3

設定終了
# save
# commit
```

[本装置 3]

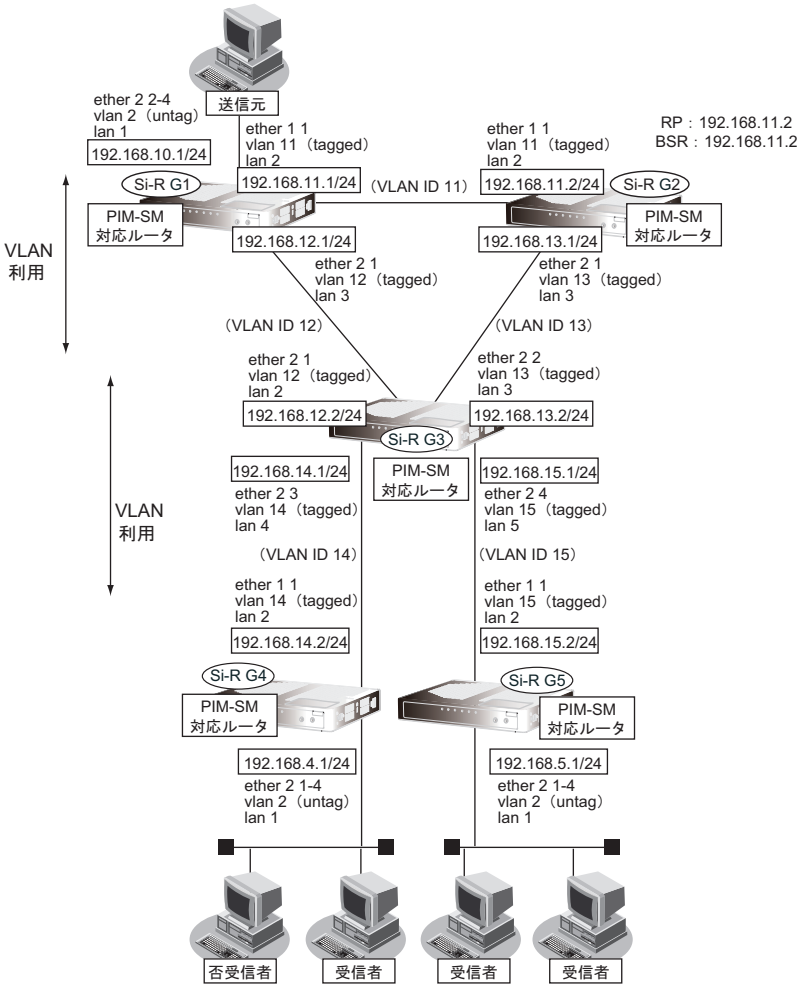
```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 4
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode pimdm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan 4

設定終了
# save
# commit
```

2.8.2　マルチキャスト機能（PIM-SM）を使う

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。

● 設定条件

- 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：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
  VLAN ID：14　ネットワークアドレス：192.168.14.0/24
  VLAN ID：15　ネットワークアドレス：192.168.15.0/24
- 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
  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
  RP　：本装置２（192.168.11.2）
  BSR　：本装置２（192.168.11.2）
- SPTへの切り替えを行う（初期値）

[本装置１]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　：192.168.10.1/24、VLAN ID 2（タグなし）、ETHERグループ２ポート２～４
  lan 2　：192.168.11.1/24、VLAN ID 11（タグあり）、ETHERグループ１ポート１
  lan 3　：192.168.12.1/24、VLAN ID 12（タグあり）、ETHERグループ２ポート１

[本装置２]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 2　：192.168.11.2/24、VLAN ID 11（タグあり）、ETHERグループ１ポート１
  lan 3　：192.168.13.1/24、VLAN ID 13（タグあり）、ETHERグループ２ポート１
- RP　：192.168.11.2
- BSR　：192.168.11.2

[本装置３]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 2　：192.168.12.2/24、VLAN ID 12（タグあり）、ETHERグループ２ポート１
  lan 3　：192.168.13.2/24、VLAN ID 13（タグあり）、ETHERグループ２ポート２
  lan 4　：192.168.14.1/24、VLAN ID 14（タグあり）、ETHERグループ２ポート３
  lan 5　：192.168.15.1/24、VLAN ID 15（タグあり）、ETHERグループ２ポート４

[本装置４]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　：192.168.4.1/24、VLAN ID 2（タグなし）、ETHERグループ２ポート１～４
  lan 2　：192.168.14.2/24、VLAN ID 14（タグあり）、ETHERグループ１ポート１

[本装置５]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　：192.168.5.1/24、VLAN ID 2（タグなし）、ETHERグループ２ポート１～４
  lan 2　：192.168.15.2/24、VLAN ID 15（タグあり）、ETHERグループ１ポート１

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHER ポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 11
# ether 2 1 vlan tag 12
# ether 2 2-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.10.1/24 3
# lan 1 ip multicast mode pimsm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.11.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 11

lan 3 情報を設定する
# lan 3 ip address 192.168.12.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan 12

設定終了
# save
# commit
```

[本装置2]

```
ETHER ポート情報を設定する
# delete ether 1 1 vlan  untag

# ether 1 1 vlan tag 11
# ether 2 1 vlan tag 13

lan 情報を削除する
# delete lan

lan 2 情報を設定する
# lan 2 ip address 192.168.11.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 11

lan 3 情報を設定する
# lan 3 ip address 192.168.13.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan 13

マルチキャスト情報を設定する
# multicast ip pimsm candrp mode on
# multicast ip pimsm candrp address 192.168.11.2
# multicast ip pimsm candbsr mode on
# multicast ip pimsm candbsr address 192.168.11.2

設定終了
# save
# commit
```

[本装置3]

```
ETHERポート情報を設定する
# delete ether 2 1-4 vlan untag

# ether 2 1 vlan tag 12
# ether 2 2 vlan tag 13
# ether 2 3 vlan tag 14
# ether 2 4 vlan tag 15

lan情報を削除する
# delete lan

lan 2 情報を設定する
# lan 2 ip address 192.168.12.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 12

lan 3 情報を設定する
# lan 3 ip address 192.168.13.2/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan 13

lan 4 情報を設定する
# lan 4 ip address 192.168.14.1/24 3
# lan 4 ip rip use v2 v2 0 on
# lan 4 ip multicast mode pimsm
# lan 4 vlan 14

lan 5 情報を設定する
# lan 5 ip address 192.168.15.1/24 3
# lan 5 ip rip use v2 v2 0 on
# lan 5 ip multicast mode pimsm
# lan 5 vlan 15

設定終了
# save
# commit
```

[本装置4]

```
ETHERポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 14
# ether 2 1-4 vlan untag 2

lan情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode pimsm
# lan 1 vlan 2

lan 2 を情報設定する
# lan 2 ip address 192.168.14.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 14

設定終了
# save
# commit
```

[本装置5]

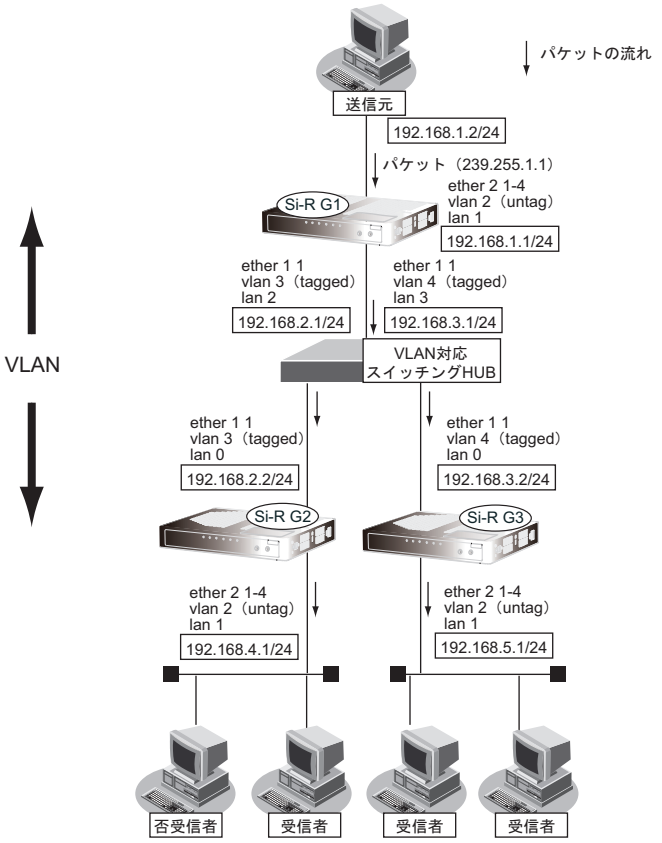
```
ETHERポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 15
# ether 2 1-4 vlan untag 2

lan情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode pimsm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.15.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 15

設定終了
# save
# commit
```

2.8.3　マルチキャスト機能（スタティックルーティング）を使う

マルチキャスト機能（スタティックルーティング）を利用すると、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、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。

● 設定条件

- 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：3　　ネットワークアドレス：192.168.2.0/24
  VLAN ID：4　　ネットワークアドレス：192.168.3.0/24
- 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]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　　：192.168.1.1/24、VLAN ID 2（タグなし）、ETHERグループ２ポート１～4
  lan 2　　：192.168.2.1/24、VLAN ID 3（タグあり）、ETHERグループ１ポート１
  lan 3　　：192.168.3.1/24、VLAN ID 4（タグあり）、ETHERグループ１ポート１

[本装置２]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　　：192.168.4.1/24、VLAN ID 2（タグなし）、ETHERグループ２ポート１～4
  lan 2　　：192.168.2.2/24、VLAN ID 3（タグあり）、ETHERグループ１ポート１

[本装置３]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  lan 1　　：192.168.5.1/24、VLAN ID 2（タグなし）、ETHERグループ２ポート１～4
  lan 2　　：192.168.3.2/24、VLAN ID 3（タグあり）、ETHERグループ１ポート１

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置１]

```
ETHERポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 3,4
# ether 2 1-4 vlan untag 2

lan情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode static
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip multicast mode static
# lan 2 vlan 3

lan 3 情報を設定する
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip multicast mode static
# lan 3 vlan 4

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan1 lan2-lan3 off

設定終了
# save
# commit
```

[本装置２]

```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 3
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode static
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan 3

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

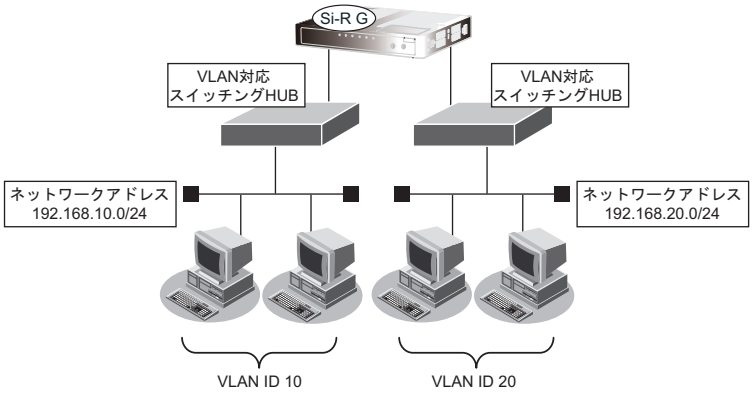
[本装置３]

```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 4
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode static
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan 4

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

2.9 VLAN 機能を使う

2.9.1 ポート VLAN 機能を使う

ここでは、ポート単位でグループ化したタグなしパケットをポート VLAN で送受信する場合の設定方法を説明します。



● 設定条件

- ETHER グループ 2 ポート 1、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：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

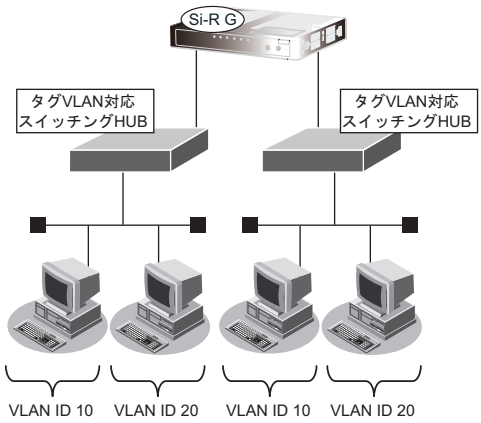
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER グループ 2 ポート 1 を設定する
# ether 2 1 vlan untag 10

ETHER グループ 2 ポート 4 を設定する
# ether 2 4 vlan untag 20

192.168.10.1/24 のネットワークを設定する
# delete lan 0
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24 のネットワークを設定する
# delete lan 1
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

2.9.2　タグ VLAN 機能を使う

ここでは、1 つのポートで、2 つの VLAN からのタグ付きパケットを、それぞれの VLAN で送受信する場合の設定方法を説明します。



● 設定条件

- ETHER グループ 2 ポート 1、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：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

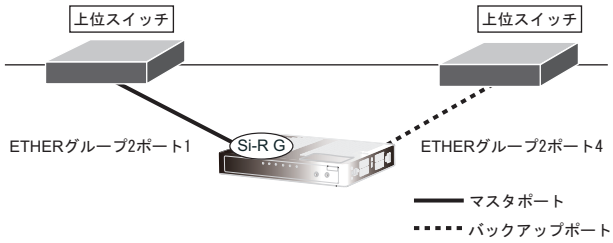
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER グループ 2 ポート 1 を設定する
# ether 2 1 vlan tag 10,20

ETHER グループ 2 ポート 4 を設定する
# ether 2 4 vlan tag 10,20

192.168.10.1/24 のネットワークを設定する
# delete lan 0
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24 のネットワークを設定する
# delete lan 1
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

2.10 バックアップポート機能を使う

ここでは、ETHERグループ２をバックアップポートとして利用する場合の設定方法について説明します。
アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。



● 設定条件

- ETHERグループ２ポート1、４をバックアップポートとして使用する
  （ETHERグループ２ポート１をマスタポート、ETHERグループ２ポート４をバックアップポートとする）
- マスタポートを優先的に使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1]

```
ETHERグループ２ポート１をバックアップポート（グループ１）のマスタポートに設定する
# ether 2 1 type backup 1 master

ETHERグループ２ポート４をバックアップポート（グループ１）のバックアップポートに設定する
# ether 2 4 type backup 1 backup

バックアップグループ１をマスタポート優先モードに設定する
# backup 1 mode master

設定終了
# save
# commit
```

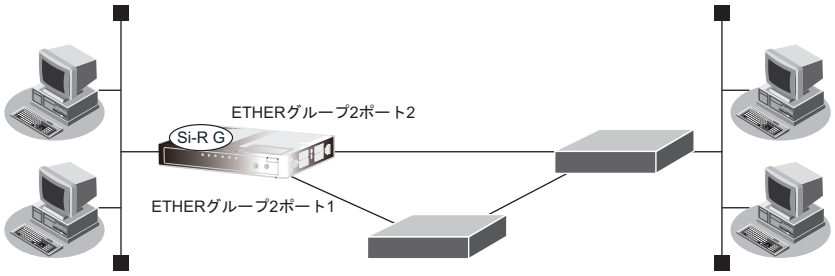
2.11 STP 機能を使う

ここでは、STP 機能を使用する場合の設定方法を説明します。

2.11.1 STP を使う

STP 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 マニュアル「機能説明書」



● 設定条件

- STP を使用する
- ETHER グループ 2 ポート 1、ポート 2 を VID 10 のポート VLAN とする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

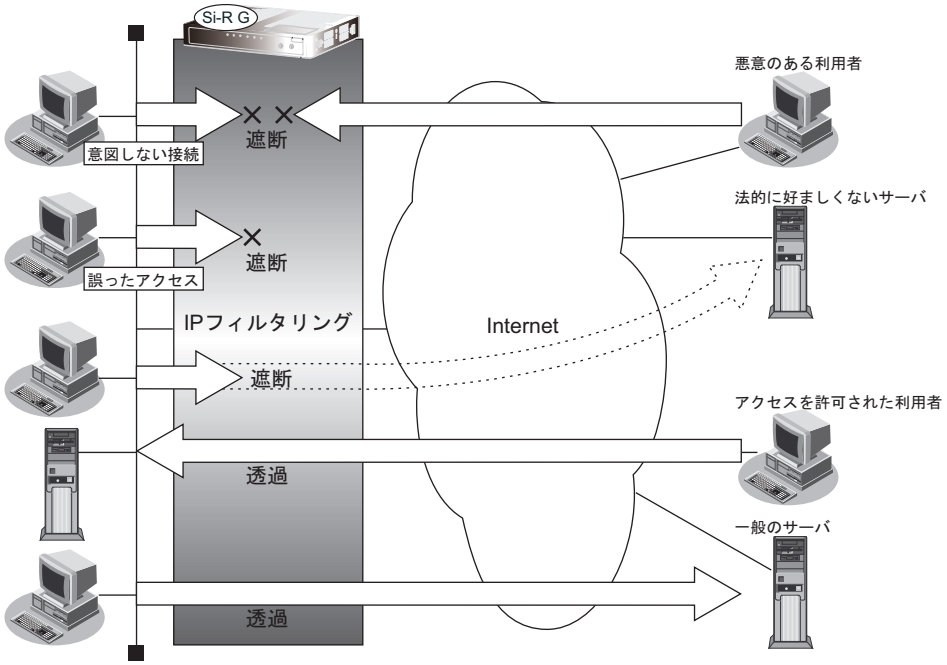
● コマンド

```
VLAN を設定する
# ether 2 1 vlan untag 10
# ether 2 2 vlan untag 10

STP を設定する
# stp mode stp
# ether 2 1 stp use on
# ether 2 2 stp use on

設定終了
# save
# commit
```

2.12 IPフィルタリング機能を使う

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。

参照 マニュアル「機能説明書」



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。

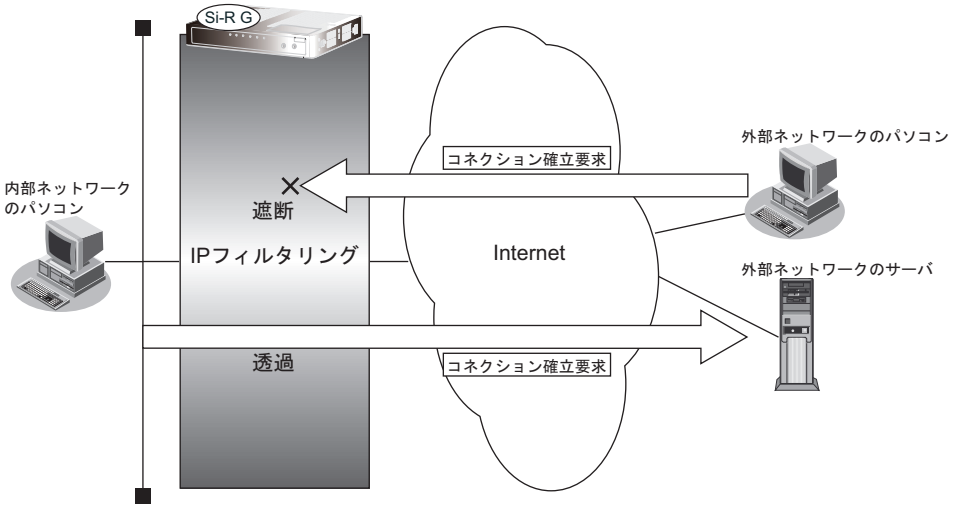
制御フラグ		TCP パケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

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

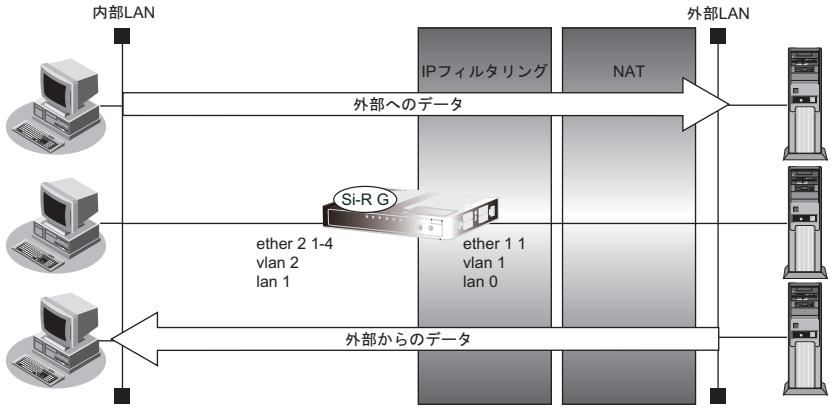
補足 IP フィルタリング機能と NAT 機能を併用する場合、回線切断時に NAT 機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IP フィルタリング機能によってパケットは破棄されてしまいます。

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

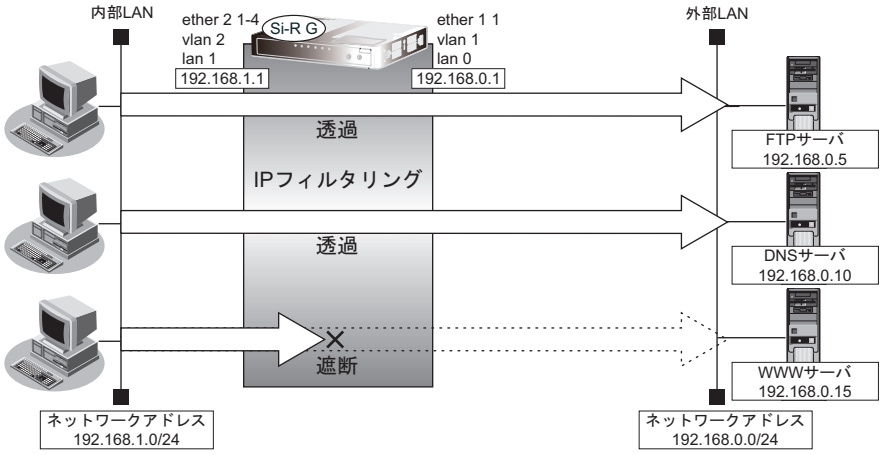
- IP フィルタリングで WWW（ポート番号 80）でのアクセスを制限する設定を行った場合、外部の WWW ブラウザからアクセスができなくなる場合があります。
- IP フィルタリングで DHCP（ポート番号 67、68）でのアクセスを制限する設定を行った場合、DHCP 機能が使用できなくなる場合があります。
- IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。PPPoE の場合は、remote 側にフィルタをかけるようにしてください。
- 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

2.12.1　外部の特定サービスへのアクセスだけを許可する

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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

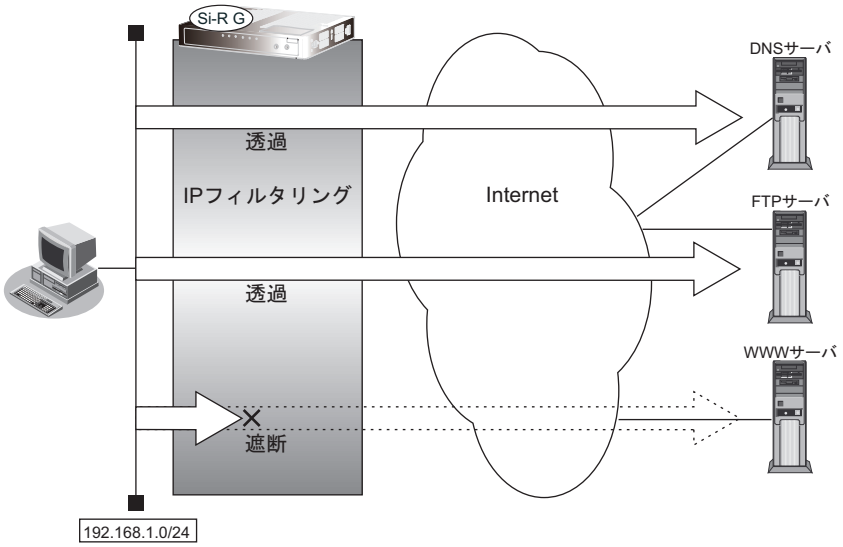
● コマンド

```
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
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.1.0/24 192.168.0.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.0.10/32 192.168.1.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

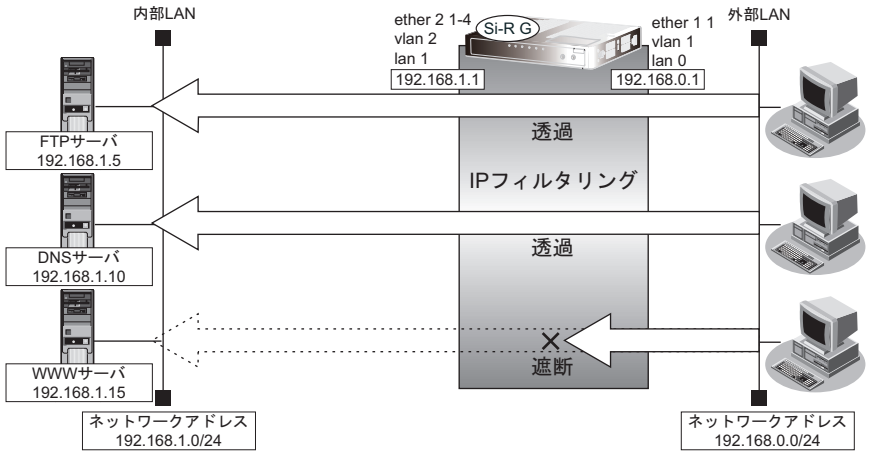
```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# remote 0 ip filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# remote 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.1.0/24 any 17
# acl 2 udp any 53
# remote 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.0/24 17
# acl 3 udp 53 any
# remote 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# remote 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# remote 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

2.12.2 外部から特定サーバへのアクセスだけを許可する

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

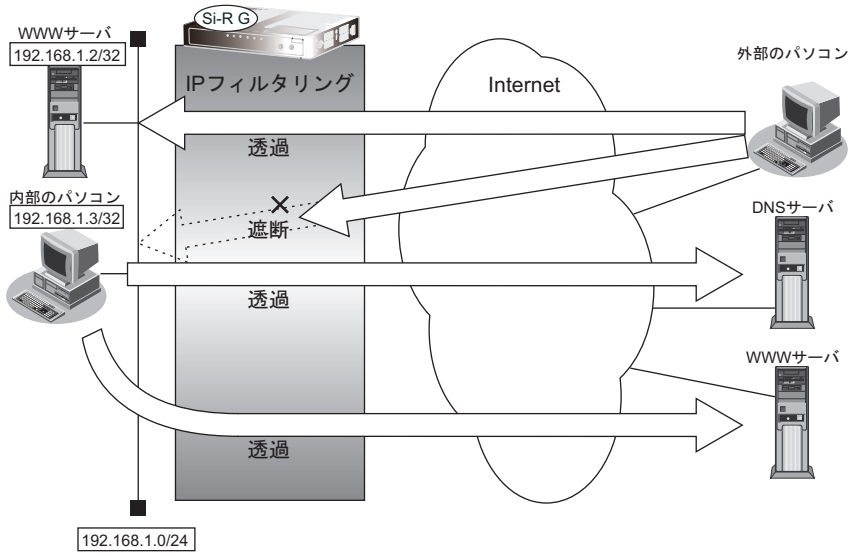
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

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に従って設定を行う場合のコマンド例を示します。

● コマンド

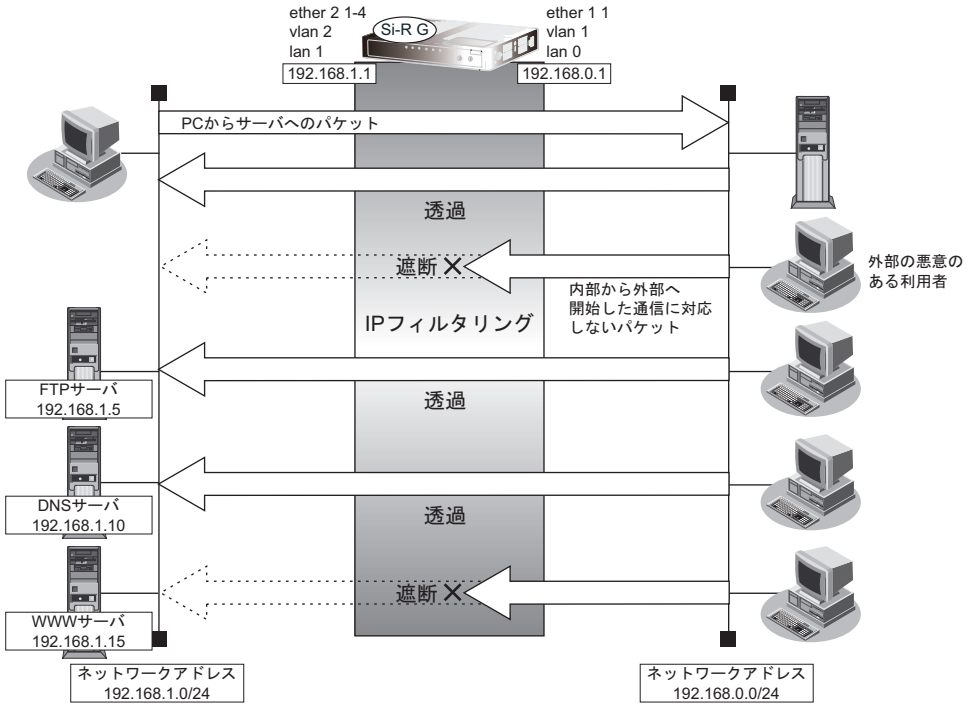
```
LAN 上のホストのポート 80 へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

任意の WWW サーバのポート 80 へのパケットを透過させる
# acl 2 ip 192.168.1.3/32 any 6
# acl 2 tcp any 80 yes
# remote 0 ip filter 2 pass acl 2 any

任意の WWW サーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.3/32 6
# acl 3 tcp 80 any no
# remote 0 ip filter 3 pass acl 3 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 4 ip 192.168.1.0/24 any 17
# acl 4 udp any 53
# remote 0 ip filter 4 pass acl 4 any

DNS サーバからの応答パケットを透過させる
# acl 5 ip any 192.168.1.0/24 17
# acl 5 udp 53 any
# remote 0 ip filter 5 pass acl 5 any

ICMP のパケットを透過させる
# acl 6 ip any any 1
# acl 6 icmp any any
# remote 0 ip filter 6 pass acl 6 any

残りのパケットをすべて遮断する
# acl 7 ip any any any
# remote 0 ip filter 7 reject acl 7 any

設定終了
# save
# commit
```

2.12.3 外部から特定サーバへのアクセスだけを許可してSPIを併用する

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

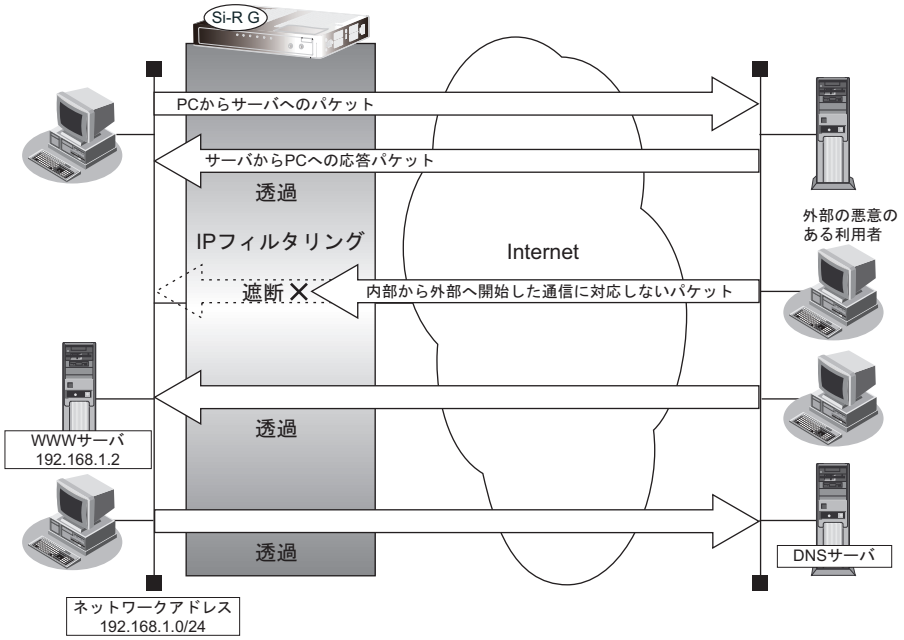
上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

● コマンド

```
LAN 上のホストのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

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
# lan 0 ip filter default spi

設定終了
# save
# commit
```

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に従って設定する場合のコマンド例を示します。

● コマンド

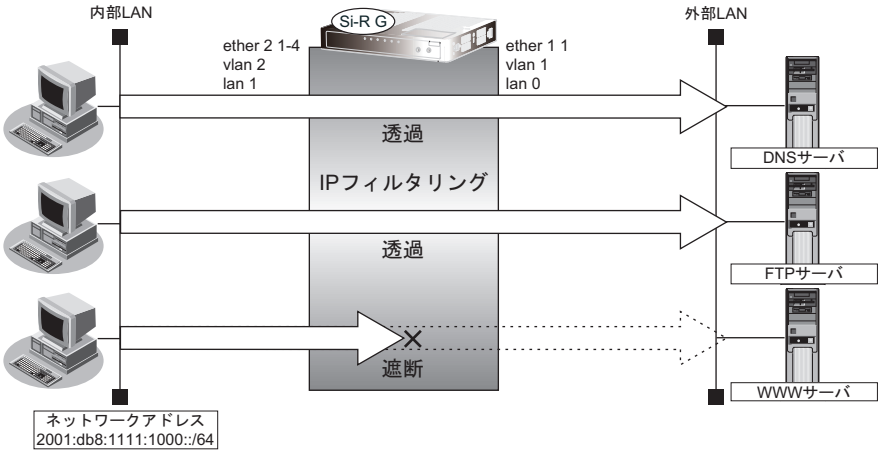
```
LAN 上のホストのポート 80 へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN 上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

ICMP のパケットを透過させる
# acl 2 ip any any 1
# acl 2 icmp any any
# remote 0 ip filter 2 pass acl 2 any

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
# remote 0 ip filter default spi

設定終了
# save
# commit
```

2.12.4 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）

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に従って設定を行う場合のコマンド例を示します。

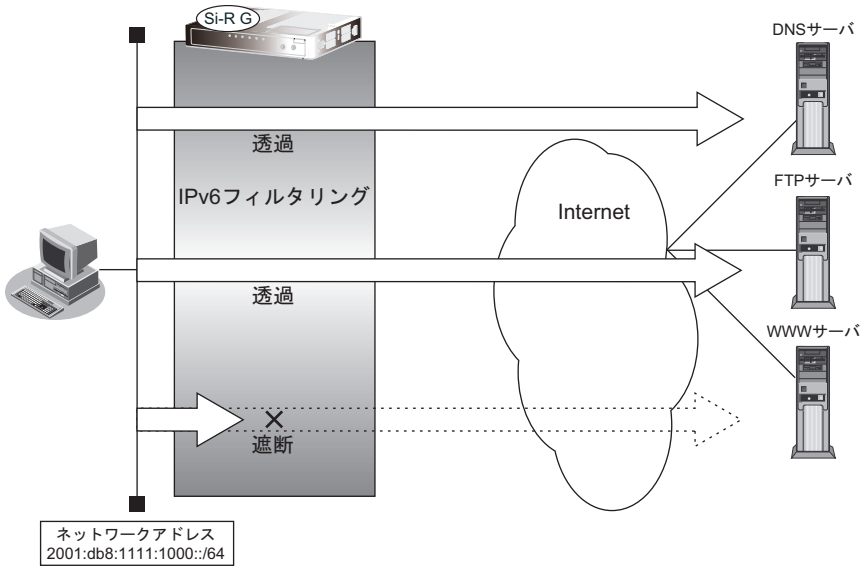
● コマンド

```
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
# acl 0 ipv6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# lan 0 ipv6 filter 0 pass acl 0 any

FTPサーバからの応答パケットを透過させる
# acl 1 ipv6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# lan 0 ipv6 filter 1 pass acl 1 any

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ipv6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# lan 0 ipv6 filter 2 pass acl 2 any

DNSサーバからの応答パケットを透過させる
# acl 3 ipv6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# lan 0 ipv6 filter 3 pass acl 3 any

ICMPv6のパケットを透過させる
# acl 4 ipv6 any any 58
# acl 4 icmp any any
# lan 0 ipv6 filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ipv6 any any any
# lan 0 ipv6 filter 5 reject acl 5 any

設定終了
# save
# commit
```

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に従って設定を行う場合のコマンド例を示します。

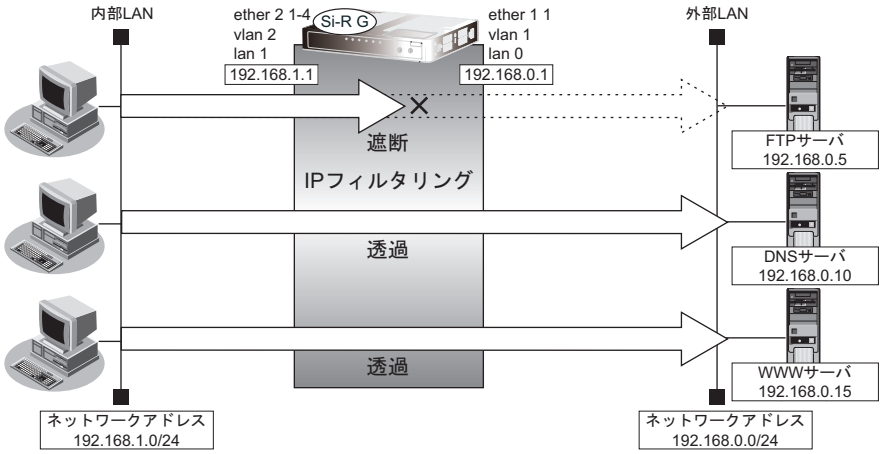
● コマンド

```
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
# acl 0 ipv6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# remote 0 ipv6 filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ipv6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# remote 0 ipv6 filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ipv6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# remote 0 ipv6 filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ipv6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# remote 0 ipv6 filter 3 pass acl 3 any

ICMPv6 のパケットを透過させる
# acl 4 ipv6 any any 58
# acl 4 icmp any any
# remote 0 ipv6 filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ipv6 any any any
# remote 0 ipv6 filter 5 reject acl 5 any

設定終了
# save
# commit
```

2.12.5 外部の特定サーバへのアクセスだけを禁止する

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。



● フィルタリング設計

- 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

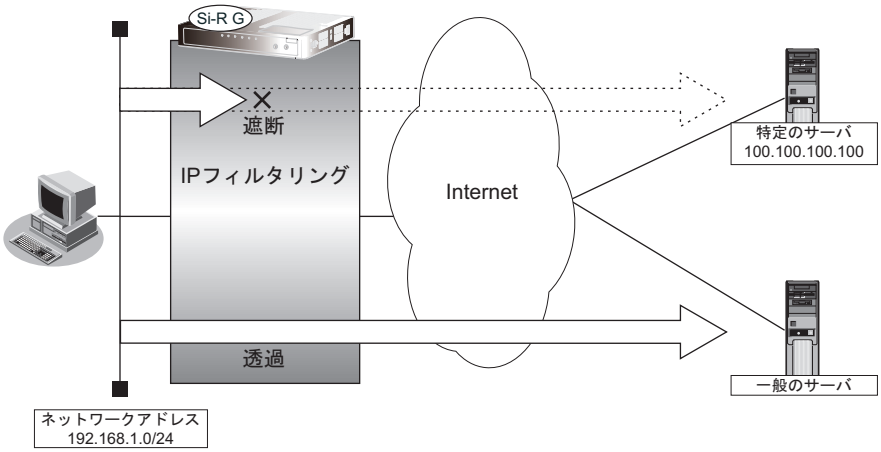
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
内部の LAN から 192.168.0.5 への FTP パケットを遮断する
# acl 0 ip 192.168.1.0/24 192.168.0.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 reject acl 0 any

設定終了
# save
# commit
```

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に従って設定を行う場合のコマンド例を示します。

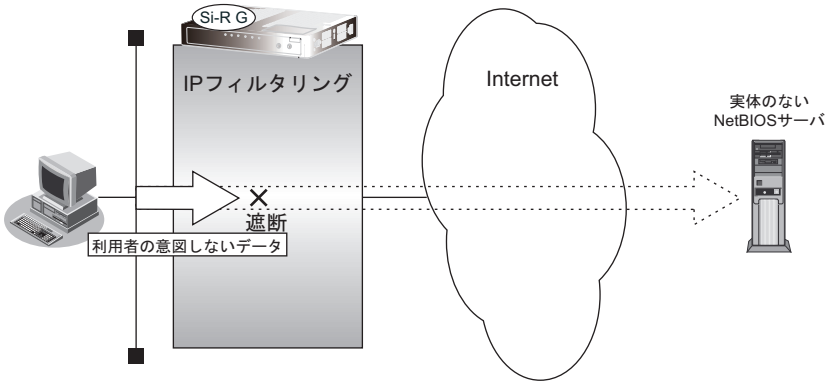
● コマンド

```
アドレス 100.100.100.100 へのすべてのパケットを遮断する
# acl 0 ip 192.168.1.0/24 100.100.100.100/32 any
# remote 0 ip filter 0 reject acl 0 any

設定終了
# save
# commit
```

2.12.6　利用者が意図しない発信を防ぐ

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に従って設定を行う場合のコマンド例を示します。

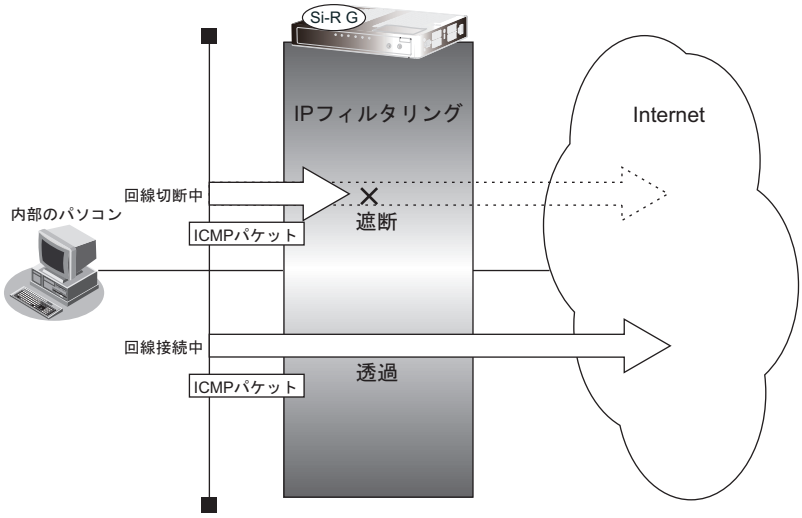
● コマンド

```
ポート 137 ～ 139 へのすべての TCP パケットを遮断する
# acl 0 ip any any 6
# acl 0 tcp any 137-139 yes
# remote 0 ip filter 0 reject acl 0 any

ポート 137 ～ 139 からのすべての TCP パケットを遮断する
# acl 1 ip any any 6
# acl 1 tcp 137-139 any yes
# remote 0 ip filter 1 reject acl 1 any

ポート 137 ～ 139 へのすべての UDP パケットを遮断する
# acl 2 ip any any 17
# acl 2 udp any 137-139
# remote 0 ip filter 2 reject acl 2 any

ポート 137 ～ 139 からのすべての UDP パケットを遮断する
# acl 3 ip any any 17
# acl 3 udp 137-139 any
# remote 0 ip filter 3 reject acl 3 any

設定終了
# save
# commit
```

2.12.7　回線が接続しているときだけを許可する

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 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に従って設定を行う場合のコマンド例を示します。

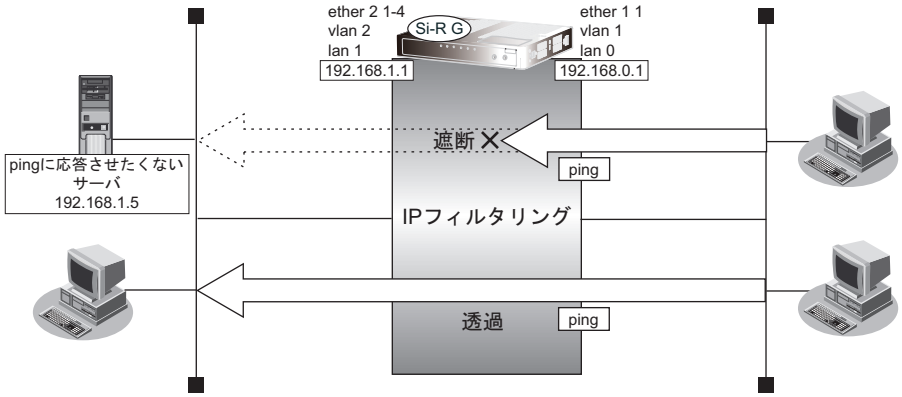
● コマンド

```
回線が接続しているときだけICMPパケットを透過させる
# acl 0 ip any any 1
# acl 0 icmp any any
# remote 0 ip filter 0 restrict acl 0 any

設定終了
# save
# commit
```

2.12.8 外部から特定サーバへの ping だけを禁止する

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。



● フィルタリング設計

- 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

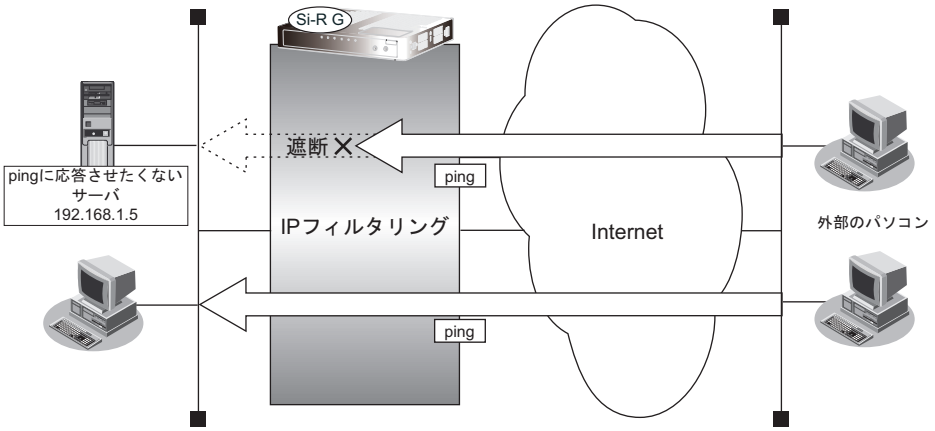
上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
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
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# lan 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# lan 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
```

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

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

● コマンド

```
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
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# remote 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# remote 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
```

2.13 IPsec機能を使う

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。

- IPv4 over IPv4で固定IPアドレスでのVPN（手動鍵交換）（P.157）
  自装置および相手装置のIPv4トンネルエンドポイントアドレスが固定で、送信元、送信先がIPv4アドレス範囲である環境の場合に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。
- IPv4 over IPv4で固定IPアドレスでのVPN（自動鍵交換）
  自装置および相手装置のIPv4トンネルエンドポイントアドレスが固定で、送信元、送信先がIPv4アドレス範囲である環境の場合にVPN通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはMain Modeを使用します。構成例は、「第１章 導入例」（P.9）を参照してください。
- IPv4 over IPv4で可変IPアドレスでのVPN（自動鍵交換）
  自装置または相手装置のどちらかがIPv4トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先がIPv4アドレス範囲である環境の場合にVPN通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはAggressive Modeを使用します。構成例は、「第１章 導入例」（P.9）を参照してください。
- IPv4 over IPv6で固定IPアドレスでのVPN（自動鍵交換）（P.161）
  自装置および相手装置のIPv6トンネルエンドポイントアドレスが固定で、送信元、送信先がIPv4アドレス範囲である環境の場合にVPN通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはMain Modeを使用します。
- IPv6 over IPv4で固定IPアドレスでのVPN（自動鍵交換）（P.165）
  自装置および相手装置のIPv4トンネルエンドポイントアドレスが固定で、送信元、送信先がIPv6アドレス範囲である環境の場合にVPN通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはMain Modeを使用します。
- IPv6 over IPv4で可変IPアドレスでのVPN（自動鍵交換）（P.169）
  自装置または相手装置のどちらかがIPv4トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先がIPv6アドレス範囲である環境の場合にVPN通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはAggressive Modeを使用します。
- IPv6 over IPv6で固定IPアドレスでのVPN（自動鍵交換）（P.173）
  自装置および相手装置のIPv6トンネルエンドポイントアドレスが固定で、送信元、送信先がIPv6アドレス範囲である環境の場合にVPN通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはMain Modeを使用します。
- 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）（P.177）
  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鍵交換（IKE）を使用して作成し、IKEの鍵交換タイプはMain Mode、Aggressive Modeが使用できます。ただし、設定例ではMain Modeのみで説明します。
- IPsec機能と他機能との併用（P.181）
  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。

- 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（P.186）
  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鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- 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（P.190）
  相手装置の 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鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- 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（P.195）
  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鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- 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（P.200）
  相手装置の 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鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- 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.206）
  不特定着信の環境で、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 IPv4 トンネルエンドポイントアドレス、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的に交換されます。
- 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）（P.215）
  VRRP 機能を使用した冗長構成環境で、動的 VPN 機能を使用した構成を説明します。
- 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（P.218）
  不特定着信の環境で、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 IPv6 トンネルエンドポイントアドレス、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的に交換されます。
- NAT トラバーサルを使用した可変 IP アドレスでの VPN（P.228）
  自装置側の IPv4 トンネルエンドポイント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。
  認証情報、暗号情報の鍵は自動鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Main Mode、Aggressive Mode が使用できます。ただし、設定例では Aggressive Mode のみで説明します。

- 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（P.232）
  相手装置の IP アドレスが動的に割り当てられ、IKE 区間にある NAT を介した環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能と 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鍵交換（IKE）を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- 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（P.236）
  動的 VPN 機能で、送出インタフェースを固定にした場合の構成を説明します。
  また、設定例にはテンプレート着信機能の動的 VPN との併用動作で記載されています。
- RSA デジタル署名認証で接続先情報（動的 VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN（P.255）
  動的 VPN 機能で、IKE 認証方式の RSA デジタル署名認証機能を使用します。
  構成例は前述にある構成と同等です。
- IPv4 over IPv4 で NAT と併用しない固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.268）
  自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「第 1 章 導入例」（P.9）を参照してください。
- IPv4 over IPv4 で NAT と併用した可変 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.272）
  自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「第 1 章 導入例」（P.9）を参照してください。
- IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.276）
  自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）」（P.161）を参照してください。
- IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.279）
  自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成ます。
  構成例は、「2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）」（P.165）を参照してください。
- IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.282）
  自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「2.13.4 IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）」（P.169）を参照してください。
- IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.285）
  自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「2.13.5 IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）」（P.173）を参照してください。
- 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 IKE Version2）（P.288）
  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鍵交換（IKE Version2）を使用して作成します。
  構成例は、「2.13.6 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）」（P.177）を参照してください。

- 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 IKE Version2）（P.291）
  自装置側の IPv4 トンネルエンドポイント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。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN」（P.228）を参照してください。
- EAP 認証を使用した固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）（P.300）
  EAP 認証機能で、IKE 認証方式は事前共有鍵認証機能を使用します。
  認証情報、暗号情報の鍵は自動鍵交換（IKE Version2）を使用して作成します。
  構成例は、「2.13.31 EAP 認証を使用した固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）」（P.300）を参照してください。

☛ 参照　マニュアル「機能説明書」

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 remote ip nat コマンドで設定します。IPsec 後に変換する場合は、プロバイダ接続用の remote ip nat コマンドで設定します。
- 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。
  - Si-R シリーズ（V31）以降のソフトウェアと Si-R シリーズ（V30）ソフトウェアで IPsec を行う場合は、Si-R シリーズ（V31）以降のソフトウェアの動的 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 Si-R シリーズ（V31）以降のソフトウェアにする必要があります。

- 動的VPN機能を使用する場合に経路情報再登録（clear ip route コマンドまたはclear ipv6 route コマンド）を行うと、経路削除により動的VPNのセッションが切断されることがあります。
- 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Si-Rシリーズ（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。
  - 自側および相手側トンネルエンドポイントアドレスにIPv6アドレスを設定した場合は動作しません。
  - IKEモードがAggressive Mode設定で、自側および相手側トンネルエンドポイントアドレスにIPv4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。
- RSAデジタル署名認証を使用した固定IPアドレスでのVPNを行う設定で、送信IDをIPアドレスにするには自装置識別情報の設定を削除してください。
- 自装置証明書および相手装置証明書の双方がない場合は、RSAデジタル署名認証は使用できません。
- テンプレート接続を使用したRADIUS/AAAでRSAデジタル署名認証は使用できません。
- 本装置は自装置証明書または相手装置証明書の有効期限が満了しても証明書を使用し続けます。有効期限が満了した場合は、証明書の更新（保存）を行ってください。
- RSAデジタル署名認証を使用したAggressive Modeの設定で、IKEセッション用Proposal定義を複数設定する場合、PFSと認証情報（auth-method）の設定はすべて同じ値を設定してください。
  これは、Aggressive ModeがDiffie-Hellmanグループと認証情報についてIKEネゴシエーションができないためです。
- 相手装置から送られて来た証明書の認証局情報が、自装置に設定している認証局情報と異なる場合は、IKEネゴシエーションが失敗し、通信を行うことができないときがあります。
- 自装置証明書のX.509v3オプションのサブジェクト代替名称にIPv6アドレスは使用できません。
- IDタイプがx501_sbjの場合は、Aggressiveモードを使用することはできません。
- 接続先情報の動的VPN接続を使用する場合、相手装置の自側ネットワーク設定（dvpn client localnet）と自装置の相手側ネットワーク設定（remote ap dvpn remotenet）が異なる場合は、以下に注意してください。
  - 双方の装置で自装置ID設定（dvpn client localid）を設定してください。
  - 接続先情報の動的VPN接続を使用する場合は、相手装置ID設定（remote ap dvpn remoteid）に相手装置の自装置ID（dvpn client localid）を設定してください。
  - 自装置の相手側ネットワーク設定（remote ap dvpn remotenet）に存在しないネットワーク情報を相手装置の自側ネットワーク設定（dvpn client localnet）に追加する場合は、必ず後ろの番号に追加してください。
  - 対向装置がテンプレート情報の動的VPN接続の場合、自装置の相手側ネットワーク設定（remote ap dvpn remotenet）に存在しないネットワークからの接続はできません。

- 接続先情報の動的 VPN 接続で INVITE 自動 ignore 機能を使用する場合は、以下に注意してください。
  - 相手装置側のネットワーク情報に all-0（0.0.0.0/0 または ::/0）が含まれている場合は、INVITE 自動 ignore ルール適用の対象外となります。
  - 動的 VPN が設定されている接続先情報にセッション監視定義があった場合は、セッション監視パケットも INVITE 自動 ignore 対象となります。
  - INVITE 自動 ignore 機能により作成された ignore ルールの自側アドレス範囲は、any（0.0.0.0/0 または ::/0）となります。
- IPsec Version3/IKE Version2 機能は、接続先情報のみサポートしています。
  テンプレート情報使用時は、IPsec Version2/IKE Version1 を使用してください。
- IPsec Version3 は IKE Version2 で動作します。
- IPsec Version3 を使用した手動鍵設定はサポートしていません。
- IPsec Version3/IKE Version2 を使用した動的 VPN はサポートしていません。
- IKE Version2 で設定した接続先情報で IKE Version1 を要求してきても接続はできません。
  また、その逆で IKE Version1 で設定した接続先情報で IKE Version2 を要求してきても接続はできません。
- 自側／相手側 ID タイプに設定する User-FQDN は、RFC822 に対応したチェックは行っていません。
  RFC822 に対応した対向装置と接続する場合は、正しい User-FQDN 値を設定してください。
- IPsec Version3 の拡張シーケンス番号（ESN）機能の設定は、IKE Version2 でネゴシエーションする両方の装置で設定してください。設定されていない場合は、IKE ネゴシエーションで接続に失敗します。
- IKE Version1 で Dead Peer Detection（DPD）機能を使用する場合、IKE でネゴシエーションする両方の装置で設定してください。設定されていない場合は、IKE ネゴシエーションで接続に失敗します。

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。

◆ IPsec Version3 とは？

拡張シーケンス番号（ESN）を使用することで、高速回線でのシーケンス番号の桁あふれが発生しにくくなります。

◆ NAT と IPsec を併用する

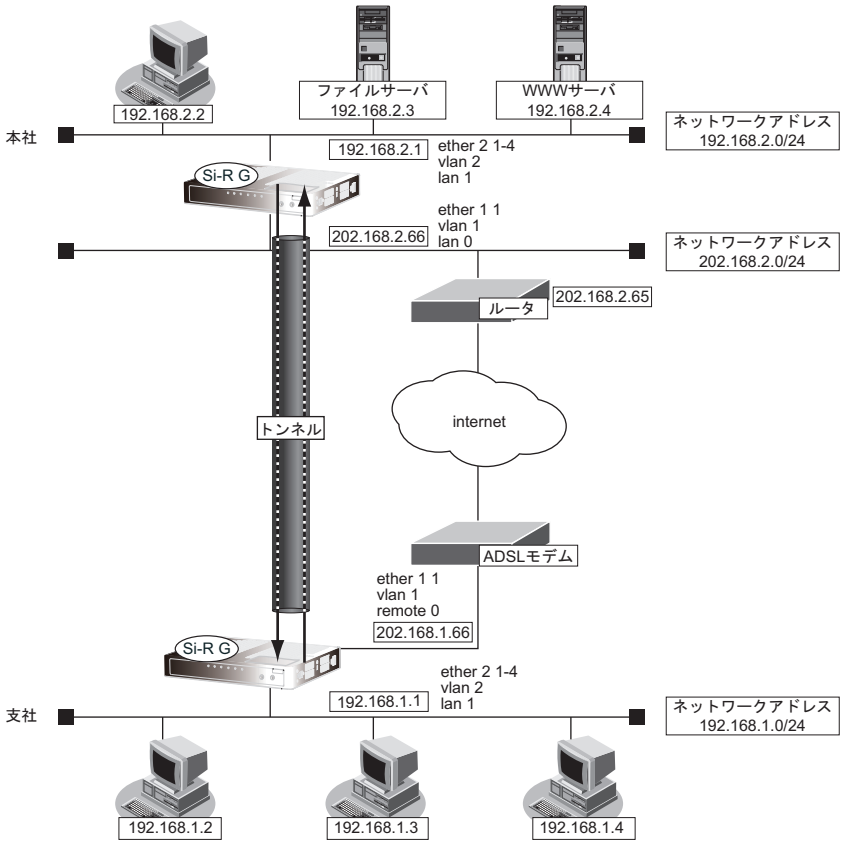
IPsec で使用するグローバルアドレスで NAT を使用している場合（IPsec 後の NAT 変換後）は、IPsec パケットが NAT を通過できるように、実回線の LAN または remote 定義で、以下の静的 NAT を設定します。

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
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 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、202.168.1.66 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

2.13.1　IPv4 over IPv4で固定IPアドレスでのVPN（手動鍵交換）

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。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1

[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

● 設定コマンド

[支社（PPPoE 常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

● 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コマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honten
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type manual

送信用 SA を設定する
# remote 1 ap 0 ipsec send protocol esp
# remote 1 ap 0 ipsec send spi 100
# remote 1 ap 0 ipsec send encrypt des-cbc hex 0123456789
# remote 1 ap 0 ipsec send auth hmac-md5 hex 123456789a

受信用 SA を設定する
# remote 1 ap 0 ipsec receive protocol esp
# remote 1 ap 0 ipsec receive spi 101
# remote 1 ap 0 ipsec receive encrypt des-cbc hex 23456789ab
# remote 1 ap 0 ipsec receive auth hmac-md5 hex 3456789abc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shiten
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type manual

送信用SAを設定する
# remote 0 ap 0 ipsec send protocol esp
# remote 0 ap 0 ipsec send spi 101
# remote 0 ap 0 ipsec send encrypt des-cbc hex 23456789ab
# remote 0 ap 0 ipsec send auth hmac-md5 hex 3456789abc

受信用SAを設定する
# remote 0 ap 0 ipsec receive protocol esp
# remote 0 ap 0 ipsec receive spi 100
# remote 0 ap 0 ipsec receive encrypt des-cbc hex 0123456789
# remote 0 ap 0 ipsec receive auth hmac-md5 hex 123456789a

設定終了
# save
# commit
```

2.13.2　IPv4 over IPv6で固定IPアドレスでのVPN（自動鍵交換）

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。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1

[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

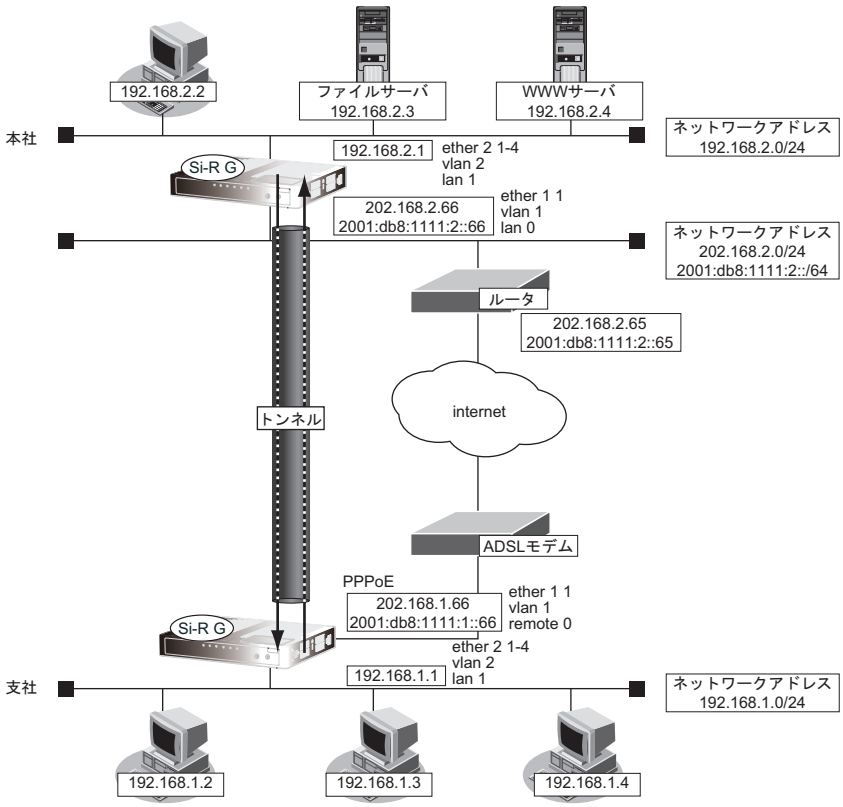
● 設定コマンド

[支社（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::66/64
# remote 0 ipv6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:2::66/64
# lan 0 ipv6 route 0 default 2001:db8:1111:2::65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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
- 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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

支社を設定する

● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.3　IPv6 over IPv4で固定IPアドレスでのVPN（自動鍵交換）

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。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1

[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

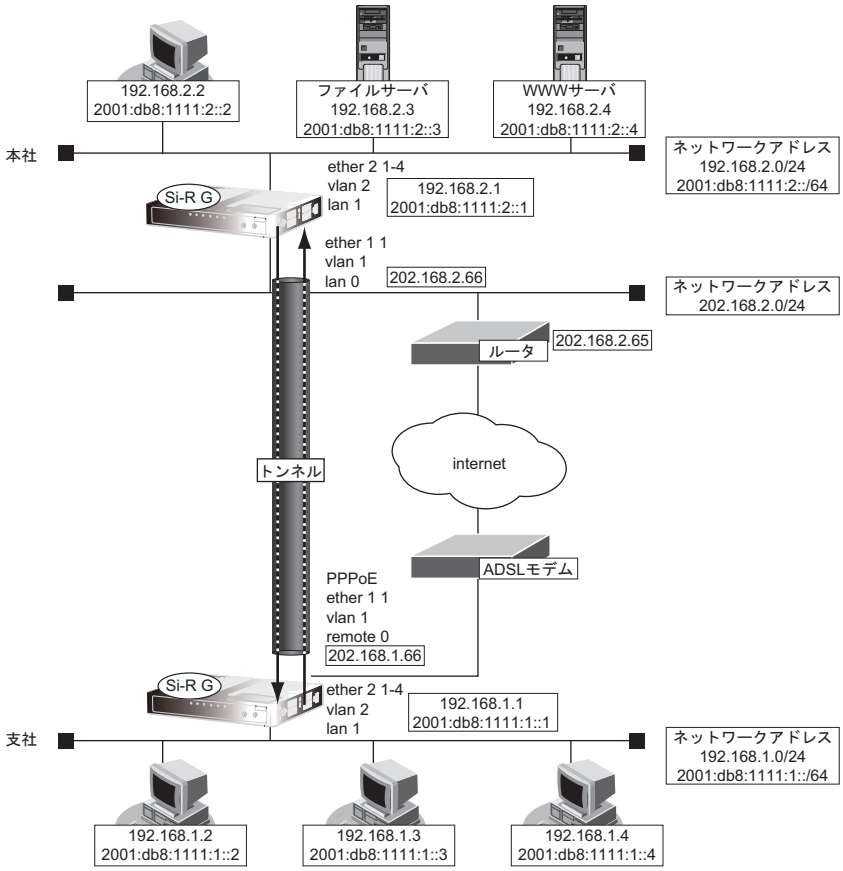
● 設定コマンド

[支社（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:1::1/64
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:2::1/64
# lan 1 vlan 2
```



● 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
- 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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.4　IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）

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。

ここでは以下のコマンドによって、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 ポート　：ETHER グループ 1 ポート 1

[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

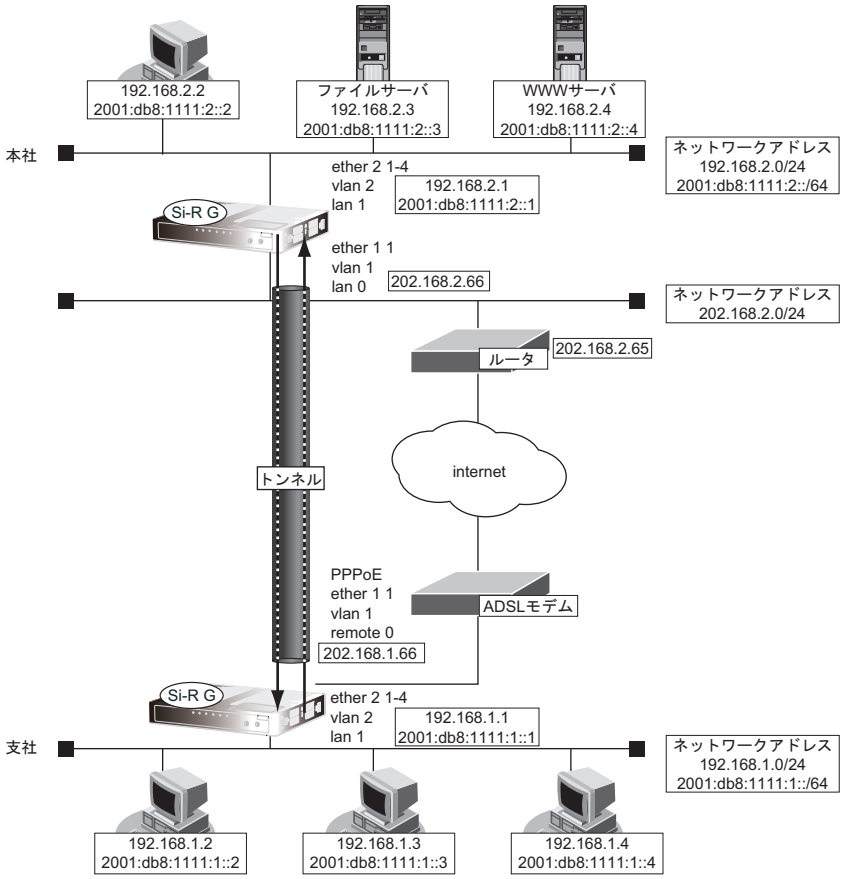
● 設定コマンド

[支社（PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 2001:db8:1111:1::1/64
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:2::1/64
# lan 1 vlan 2
```



● 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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPNを設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

本社（Responder）を設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.5　IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）

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。

ここでは以下のコマンドによって、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 ポート　：ETHER グループ 1 ポート 1

[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

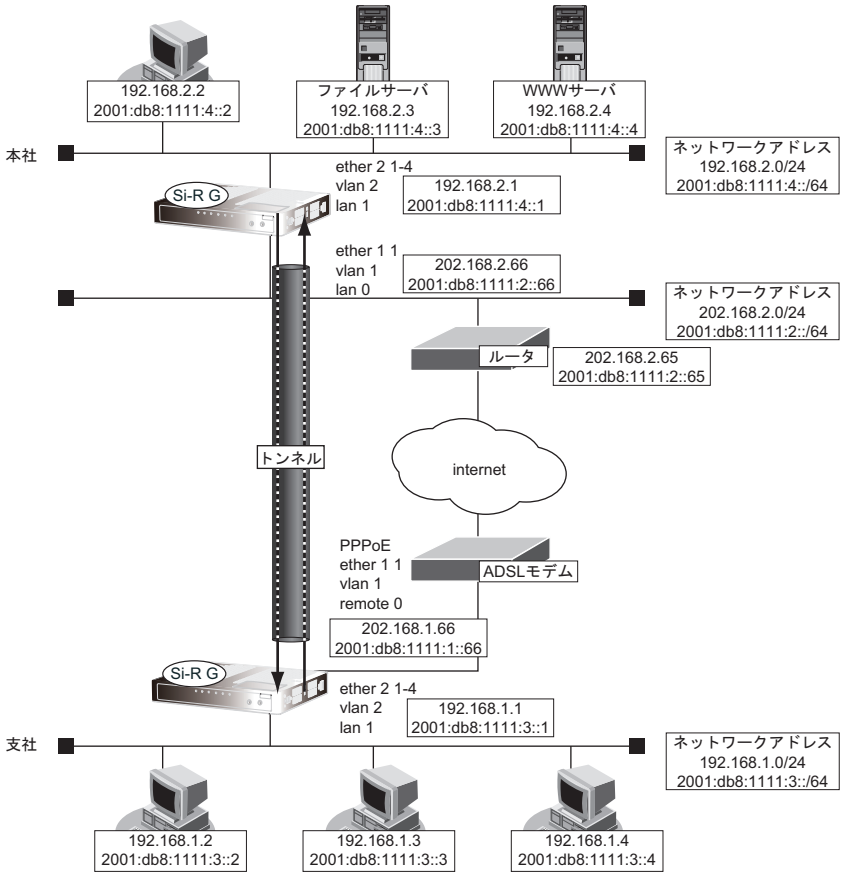
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ipv6 use on
# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:3::1/64
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::66/64
# remote 0 ipv6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:2::66/64
# lan 0 ipv6 route 0 default 2001:db8:1111:2::65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:4::1/64
# lan 1 vlan 2
```



● 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
- 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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

支社を設定する

● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
```

```
設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:3::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

2.13.6 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）

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）。

ここでは以下のコマンドにより、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ポート　：ETHERグループ1ポート1

[本社]

- ローカルネットワークIPアドレス1　：192.168.2.1/24
- 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

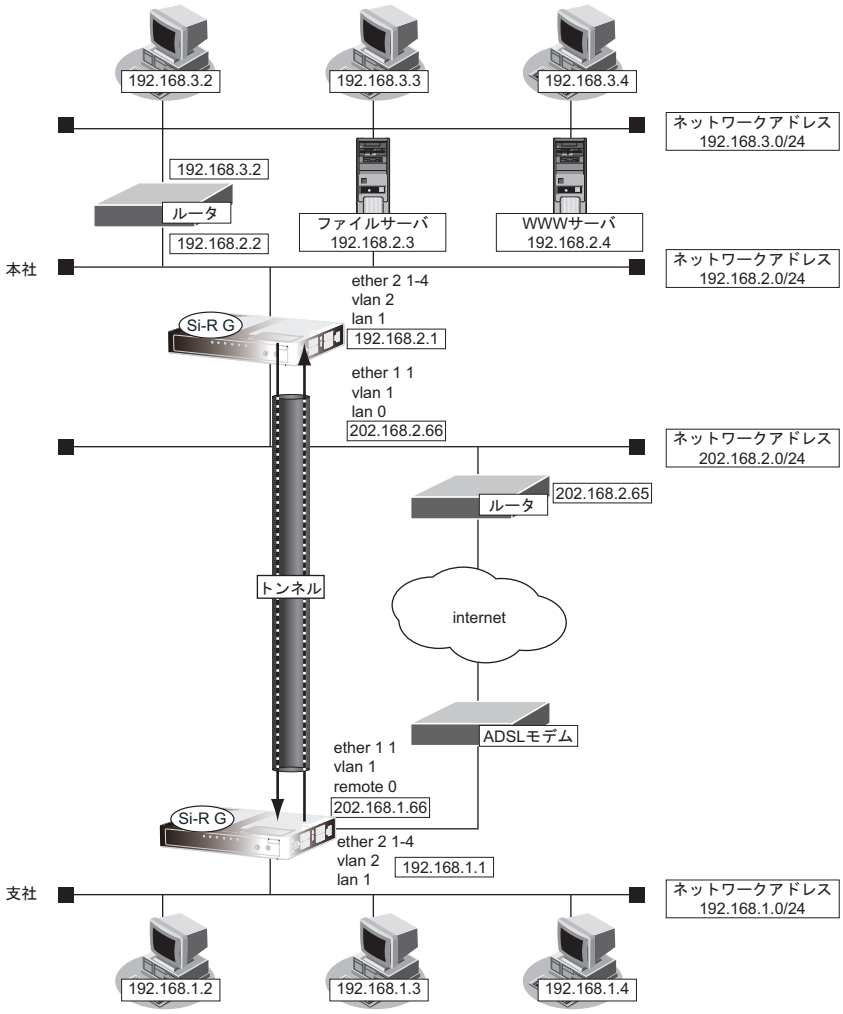
● 設定コマンド

[支社（PPPoE接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip route 0 192.168.3.0/24 192.168.2.2 1
# lan 1 vlan 2
```



● 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
- IPsec プロトコル　：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　：pre-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コマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ip route 1 192.168.3.0/24 1 1
# remote 1 ap 0 name honten1
# remote 1 ap 0 multiroute pattern 0 use any any 192.168.2.0/24 any 0 any
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.2.0/24
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 1 datalink type ipsec
# remote 1 ap 1 ipsec type ike
# remote 1 ap 1 ipsec ike protocol esp
# remote 1 ap 1 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 1 ipsec ike encrypt des-cbc
# remote 1 ap 1 ipsec ike auth hmac-md5
# remote 1 ap 1 ike bind ap 0

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shiten
# remote 0 ap 0 multiroute pattern 0 use 192.168.2.0/24 any any any 0 any
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 1 datalink type ipsec
# remote 0 ap 1 ipsec type ike
# remote 0 ap 1 ipsec ike protocol esp
# remote 0 ap 1 ipsec ike range 192.168.3.0/24 any4
# remote 0 ap 1 ipsec ike encrypt des-cbc
# remote 0 ap 1 ipsec ike auth hmac-md5
# remote 0 ap 1 ike bind ap 0

設定終了
# save
# commit
```

2.13.7　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、以下に説明します。

ここでは、「1.9 複数の事業所 LAN を VPN（IPsec）で接続する」（P.35）相当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 書き換え機能
- IPsec 変換前の MTU 分割機能
- 接続先監視機能
- 動的経路（RIP）機能
- IKE Dead Peer Detection（DPD）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

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コマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ip nat mode multi 192.168.1.1 1

# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 1 ip filter 0 pass acl 0 out
# remote 1 ip filter 1 pass acl 1 in
# remote 1 ip filter 2 reject acl 2 any
# remote 1 ip tos 0 acl 3 a0
```

本社を設定する

● コマンド

```
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 0 ip filter 0 pass acl 0 in
# remote 0 ip filter 1 pass acl 1 out
# remote 0 ip filter 2 reject acl 2 any
# remote 0 ip tos 0 acl 3 a0
```

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コマンド例を示します。

本社を設定する

● コマンド

```
# remote 0 shaping on 2m
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 6 any
# remote 0 ip priority 0 acl 0 express
```

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 remote で設定します。この場合、IPsec 用の remote でシェーピングを行うか、または、実回線の remote 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コマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ip msschange 1414
```

本社を設定する

● コマンド

```
# remote 0 ip msschange 1414
```

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コマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 mtu 1460
```

本社を設定する

● コマンド

```
# remote 0 mtu 1460
```

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コマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
```

こんな事に気をつけて

- 接続先監視のあて先IPアドレスは、remote ap ipsec ike rangeコマンドで設定するIPsec対象パケット範囲に含まれるIPアドレスを指定してください。
- 接続先監視のあて先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あることがあります。

動的経路（RIP）機能との併用例

● 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コマンド例を示します。

支社を設定する

● コマンド

```
# delete remote 1 ip route
# remote 1 ip rip use v1 v1 0 off
```

本社を設定する

● コマンド

```
# delete remote 0 ip route
# remote 0 ip rip use v1 v1 0 off
```

IKE Dead Peer Detection（DPD）機能との併用例

● 設定条件

[共通]

- 無通信監視時間　：10秒
- 再送時間　：1秒
- 再送回数　：3回

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
# remote 1 ap 0 ike dpd use on
# remote 1 ap 0 ike dpd idle 10s
# remote 1 ap 0 ike dpd retry 1s 3
```

本社を設定する

● コマンド

```
# remote 0 ap 0 ike dpd use on
# remote 0 ap 0 ike dpd idle 10s
# remote 0 ap 0 ike dpd retry 1s 3
```

こんな事に気をつけて

- DPDパケットの再送時間と再送回数は、「DPDパケット送信を開始するIPsec受信パケット無通信監視時間」より短い時間を設定してください。
  再送時間×（再送回数＋1）＜無通信監視時間
  その範囲を超えた場合は、定義反映時に設定エラーとなります。
- IKE Version1でDead Peer Detection（DPD）機能を使用する場合、IKEでネゴシエーションする両方の装置で設定してください。設定されていない場合は、IKEネゴシエーションで接続に失敗します。

2.13.8 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

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。

ここでは以下のコマンドによって、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 ポート　：ETHER グループ 1 ポート 1

[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

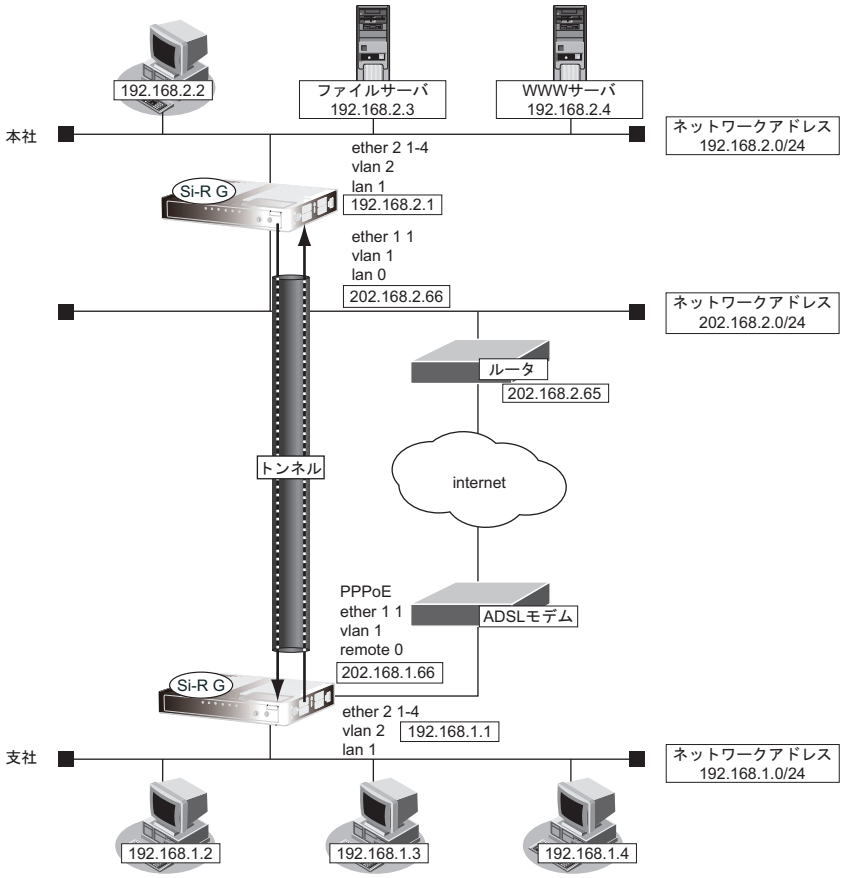
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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　：pre-shared（事前共有鍵方式）
- 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
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
```

```
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

本社（**Responder**）を設定する

● コマンド

```
VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode main
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name shisya
# aaa 0 user 0 id 202.168.1.66
# aaa 0 user 0 password 202.168.1.66
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 2

設定終了
# save
# reset
```

2.13.9 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

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。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1

[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

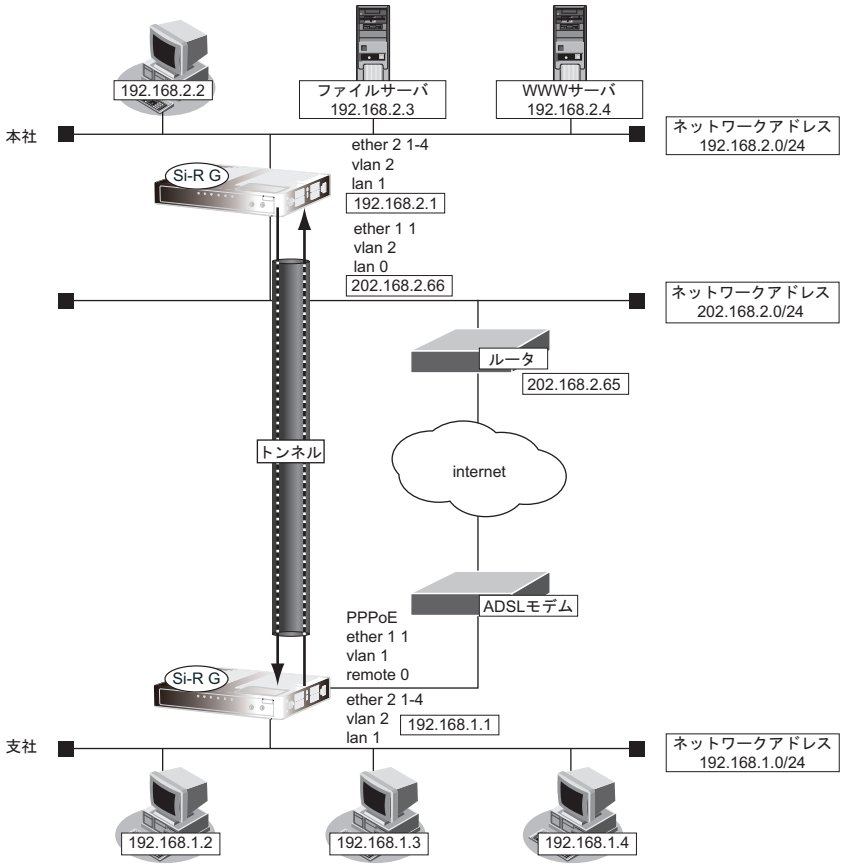
● 設定コマンド

[支社（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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　：pre-shared（事前共有鍵方式）
- 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
- テンプレート着信側からIKEネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0の設定を推奨します。

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
 # remote 0 ip nat static 0 192.168.1.1 500 any 500 17
 # remote 0 ip nat static 1 192.168.1.1 any any any 50
 # remote 0 ip nat static default reject

VPNを設定する
 # remote 1 name vpn-hon
 # remote 1 ap 0 name honsya
 # remote 1 ap 0 datalink type ipsec
 # remote 1 ap 0 ipsec type ike
 # remote 1 ap 0 ipsec ike protocol esp
 # remote 1 ap 0 ipsec ike range any4 any4
 # remote 1 ap 0 ipsec ike encrypt des-cbc
 # remote 1 ap 0 ipsec ike auth hmac-md5
 # remote 1 ap 0 ipsec ike pfs off
 # remote 1 ap 0 ipsec ike lifetime 8h
 # remote 1 ap 0 ipsec ike lifebyte 0
 # remote 1 ap 0 ipsec ike newsa initiator 90s 0
 # remote 1 ap 0 ipsec ike newsa responder 30s 0
 # remote 1 ap 0 ike mode aggressive
 # remote 1 ap 0 ike bind self
 # remote 1 ap 0 ike idtype fqdn
 # remote 1 ap 0 ike name local shisya
 # remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
 # remote 1 ap 0 ike proposal 0 encrypt des-cbc
 # remote 1 ap 0 ike proposal 0 hash hmac-md5
 # remote 1 ap 0 ike proposal 0 pfs modp768
 # remote 1 ap 0 ike proposal 0 lifetime 1d
 # remote 1 ap 0 ike retry 10s 3
 # remote 1 ap 0 ike release on
 # remote 1 ap 0 ike initial forward
 # remote 1 ap 0 tunnel remote 202.168.2.66
 # remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
 # save
 # reset
```

本社（**Responder**）を設定する

● コマンド

```
VPN（テンプレート）を設定する
 # template 0 name vpn-hon
 # template 0 combine use aaa
 # template 0 datalink type ipsec
 # template 0 interface pool 1 1
 # template 0 aaa 0
 # template 0 ipsec ike protocol esp
 # template 0 ipsec ike encrypt des-cbc
 # template 0 ipsec ike auth hmac-md5
 # template 0 ipsec ike pfs off
 # template 0 ipsec ike lifetime 8h
 # template 0 ipsec ike lifebyte 0
 # template 0 ipsec ike newsa initiator 90s 0
 # template 0 ipsec ike newsa responder off 0
 # template 0 ike mode aggressive
 # template 0 ike idtype fqdn
 # template 0 ike proposal 0 encrypt des-cbc
 # template 0 ike proposal 0 hash hmac-md5
 # template 0 ike proposal 0 pfs modp768
 # template 0 ike proposal 0 lifetime 1d
 # template 0 ike retry 10s 3
 # template 0 ike release on
 # template 0 tunnel local 202.168.2.66

AAA 情報を設定する
 # aaa 0 name shisya
 # aaa 0 user 0 id shisya
 # aaa 0 user 0 password shisya
 # aaa 0 user 0 ipsec ike range any4 any4
 # aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
 # aaa 0 user 0 ip route 0 192.168.1.0/24 1 2

設定終了
 # save
 # reset
```

2.13.10 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

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。

ここでは以下のコマンドによって、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 ポート　：ETHER グループ 1 ポート 1

[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

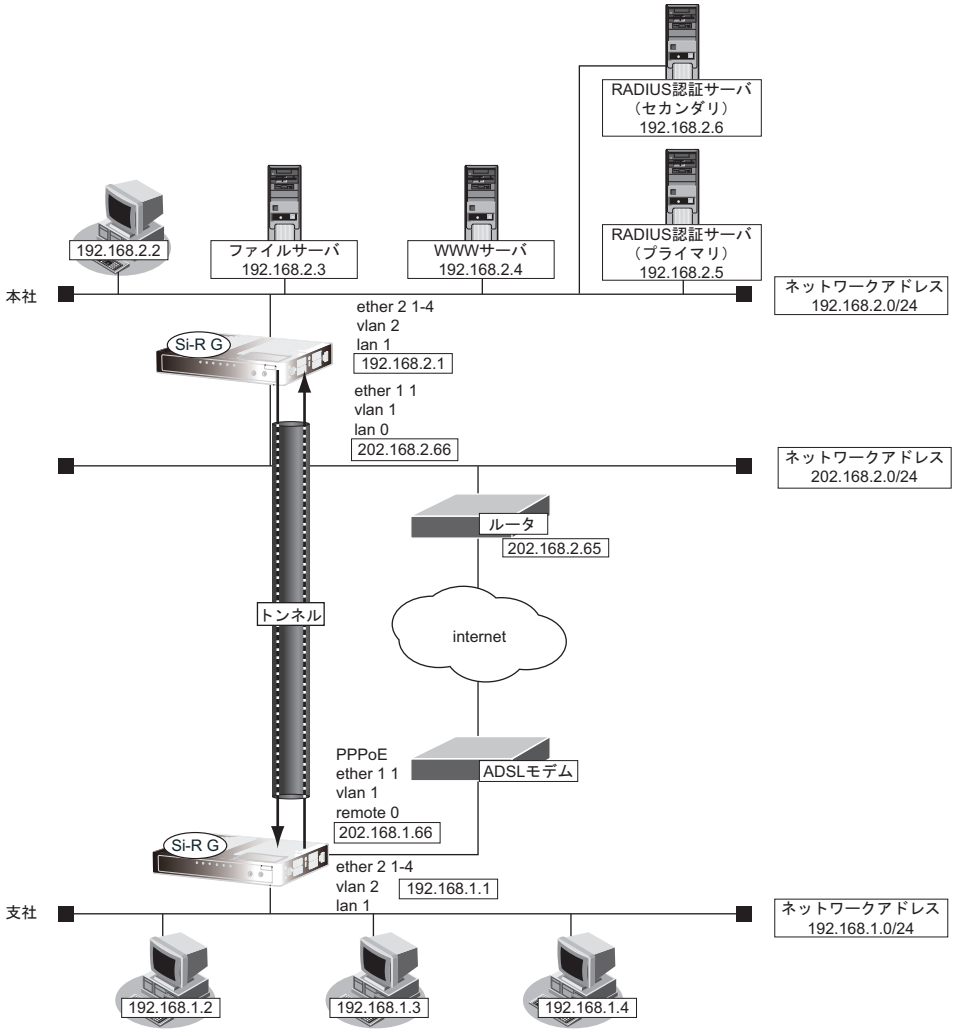
● 設定コマンド

[支社（PPPoE 常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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　：pre-shared（事前共有鍵方式）
- 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（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
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

本社（**Responder**）を設定する

● コマンド

```
VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode main
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name shisya

RADIUS クライアントに関する情報を設定する
# aaa 0 radius service client both
# aaa 0 radius auth source 192.168.2.1
# aaa 0 radius accounting source 192.168.2.1
# aaa 0 radius client server-info auth 0 secret 192.168.2.1
# aaa 0 radius client server-info auth 0 address 192.168.2.5
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret 192.168.2.1
# aaa 0 radius client server-info auth 1 address 192.168.2.6
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret 192.168.2.1
# aaa 0 radius client server-info accounting 0 address 192.168.2.5
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret 192.168.2.1
# aaa 0 radius client server-info accounting 1 address 192.168.2.6
# aaa 0 radius client server-info accounting 1 deadtime 30m
# aaa 0 radius client server-info accounting 1 priority 100

設定終了
# save
# reset
```

2.13.11 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

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。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1

[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

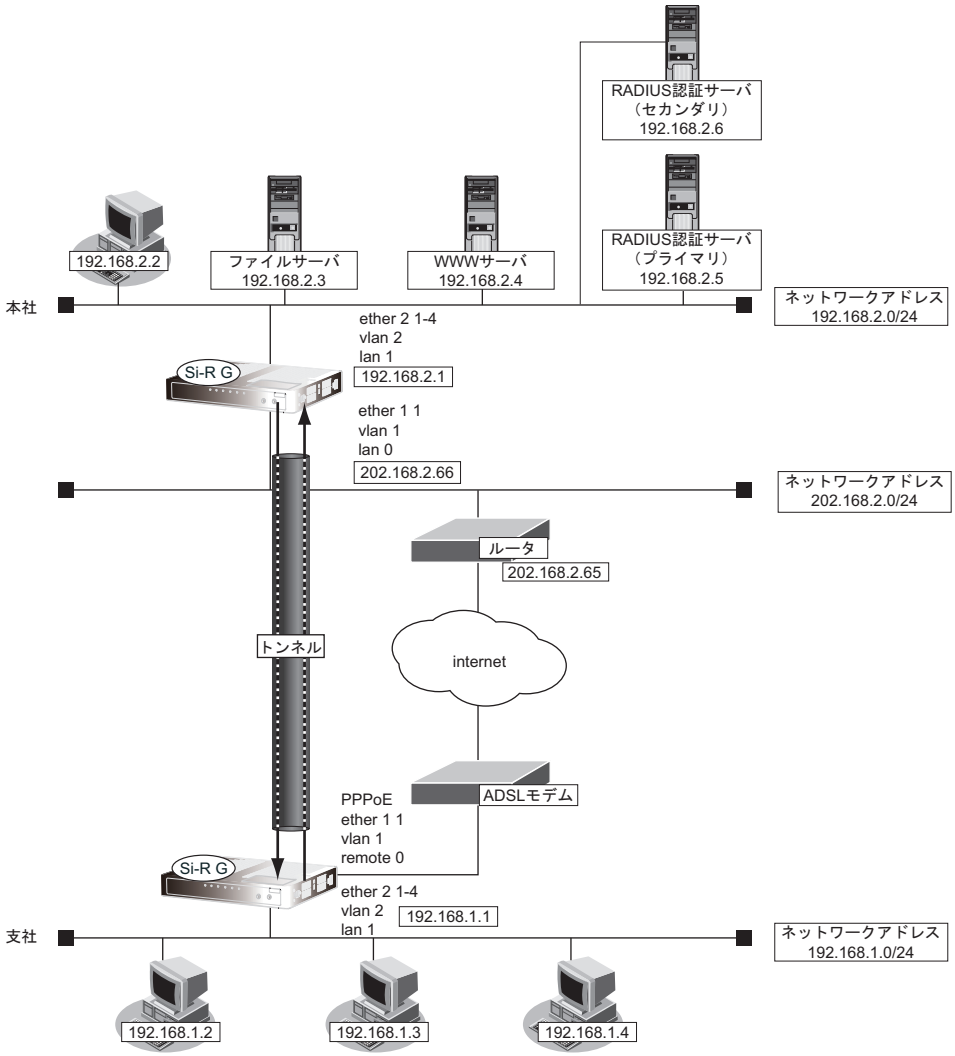
● 設定コマンド

[支社（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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
- 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　：pre-shared（事前共有鍵方式）
- 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（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
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、
  template ipsec ike newsa responder off 0 の設定を推奨します。

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
```

```
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

本社（**Responder**）を設定する

● コマンド

```
VPN（テンプレート）を設定する
# template 0 name vpn-hon
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA情報を設定する
# aaa 0 name shisya

RADIUSクライアントに関する情報を設定する
# aaa 0 radius service client both
# aaa 0 radius auth source 192.168.2.1
# aaa 0 radius accounting source 192.168.2.1
# aaa 0 radius client server-info auth 0 secret 192.168.2.1
# aaa 0 radius client server-info auth 0 address 192.168.2.5
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret 192.168.2.1
# aaa 0 radius client server-info auth 1 address 192.168.2.6
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret 192.168.2.1
# aaa 0 radius client server-info accounting 0 address 192.168.2.5
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret 192.168.2.1
# aaa 0 radius client server-info accounting 1 address 192.168.2.6
# aaa 0 radius client server-info accounting 1 deadtime 30m
```

```
# aaa 0 radius client server-info accounting 1 priority 100

設定終了
# save
# reset
```

2.13.12 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

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を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1
- 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ポート　：ETHERグループ1ポート1
- 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

● 設定コマンド

[支社Ａ（PPPoE常時接続）]

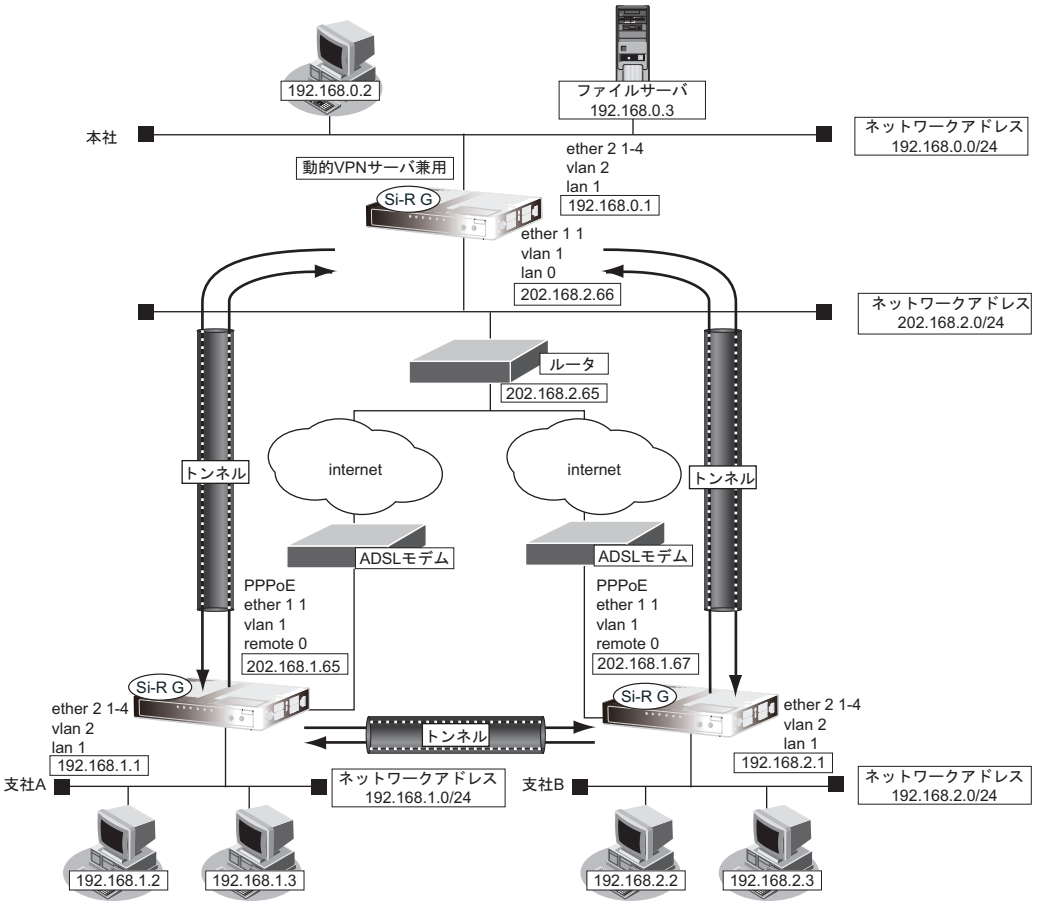
```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社Ｂ（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2
```



● 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 - 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 - 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　：pre-shared（事前共有鍵方式）
- 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　：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　：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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

支社 A（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 1
# remote 1 ip route 1 192.168.2.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any

動的 VPN 情報を定義する
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1
```

```
テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

設定終了
# save
# reset
```

支社 B（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
```

```
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 1
# remote 1 ip route 1 192.168.1.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

設定終了
# save
# reset
```

本社（**Responder**）を設定する

● コマンド

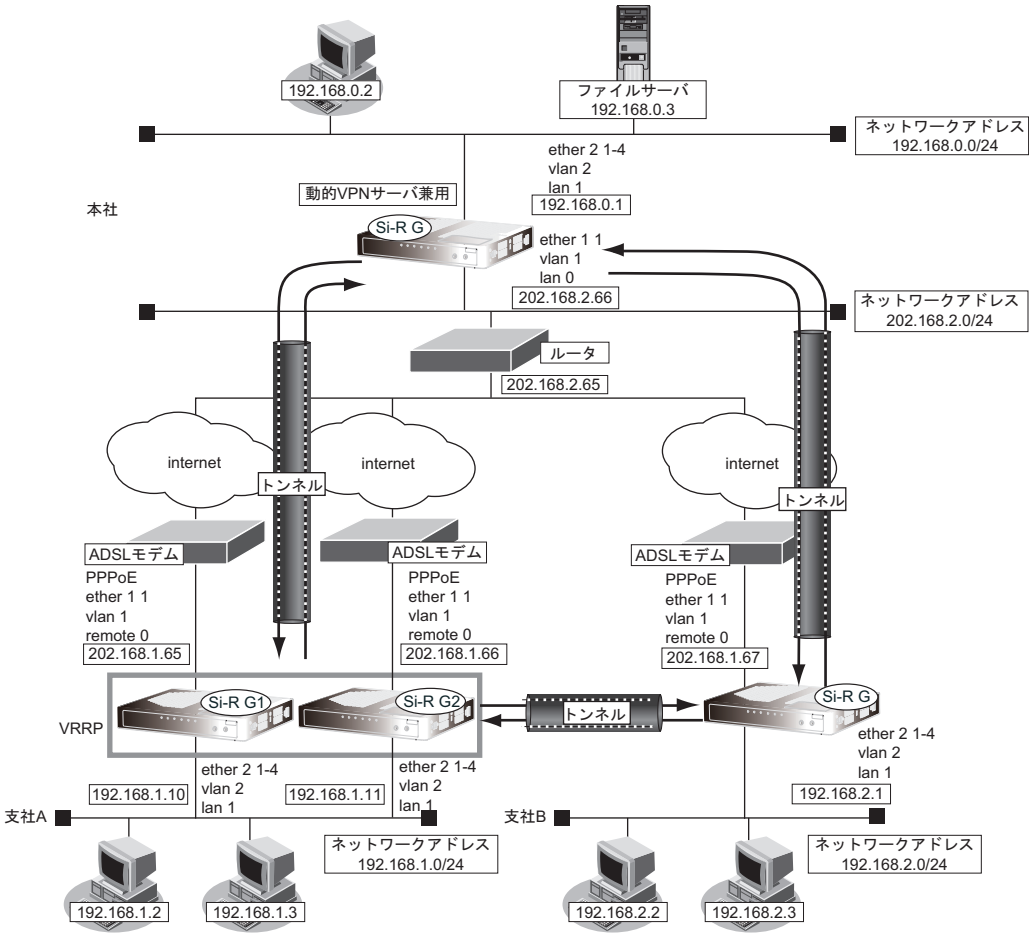
```
VPNを設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
```

```
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

動的VPNサーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass

設定終了
# save
# reset
```

2.13.13 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）

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「2.13.12 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.206）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。



● 設定コマンド

[支社A（Si-R G1）]

「2.13.12 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.206）で説明した支社Aの設定を事前に行います。

[支社A（Si-R G2）]

「2.13.12 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.206）で説明した支社Aの設定を事前に行います。

● 設定条件（冗長構成）

[支社 A（Si-R G1)]

- 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-R G2)]

- 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社 A（Si-R G1）を設定する

● コマンド

```
# lan 1 ip address 192.168.1.10/24 3
# remote 0 ip nat static 0 192.168.1.10 500 any 500 17
# remote 0 ip nat static 1 192.168.1.10 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 trigger 0 node 202.168.2.66 any

動的 VPN を設定する
# template 0 tunnel local 192.168.1.10
# template 0 sessionwatch address 192.168.1.10
# dvpn client 0 ua 192.168.1.10
# dvpn client priority 1

設定終了
# save
# reset
```

支社 A（Si-R G2）を設定する

● コマンド

```
# lan 1 ip address 192.168.1.11/24 3
# remote 0 ip nat static 0 192.168.1.11 500 any 500 17
# remote 0 ip nat static 1 192.168.1.11 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200
# remote 1 ap 0 ike name local shisyaa

VRRP を設定する
# lan 1 vrrp use on
```

```
# lan 1 vrrp group 0 id 10 100 192.168.1.1

OSPF を設定する
# lan 1 ip ospf use on 0
# routemanage ip redist ospf static on 20 type2
# ospf ip area 0 id 0.0.0.0

動的 VPN を設定する
# template 0 tunnel local 192.168.1.11
# template 0 sessionwatch address 192.168.1.11
# dvpn client 0 ua 192.168.1.11
# dvpn client priority 2

設定終了
# save
# reset
```

本社を設定する

● コマンド

```
# remote 0 ip route 0 192.168.1.0/24 1 10
# remote 0 ap 0 sessionwatch address 192.168.0.1 192.168.1.10
# remote 2 name vpn-shia
# remote 2 ap 0 name shisyaa
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaa
# remote 2 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.1.0/24 1 254

設定終了
# save
# reset
```

2.13.14 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

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を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート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
- 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ポート　：ETHERグループ1ポート1

[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

● 設定コマンド

[支社Ａ（PPPoE常時接続）]

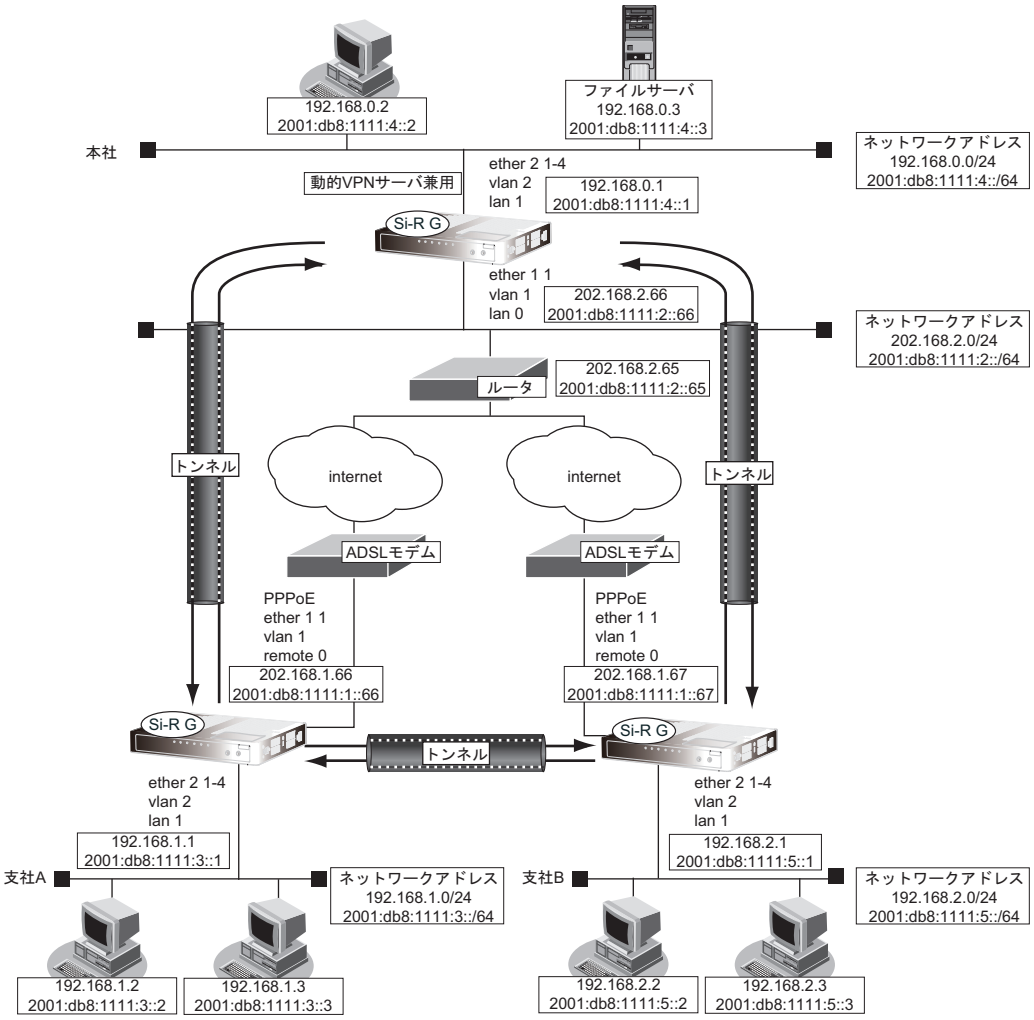
```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:3::1/64
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::66/64
# remote 0 ipv6 route 0 default 1 1
```

[支社Ｂ（PPPoE常時接続）]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:5::1/64
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::67/64
# remote 0 ipv6 route 0 default 1 1
```

[本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:2::66/64
# lan 0 ipv6 route 0 default 2001:db8:1111:2::65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:4::1/64
```



● 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　：pre-shared（事前共有鍵方式）
- 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　：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　：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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

支社Aを設定する

● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1 1
```

```
# remote 1 ipv6 route 1 2001:db8:1111:5::/64 1 2
# remote 1 ipv6 dvpn 0 invite acl 0 64 0
# acl 0 ipv6 2001:db8:1111:3::/64 2001:db8:1111:5::/64 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:3::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:3::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ipv6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipv6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::66
# template 0 sessionwatch address 2001:db8:1111:3::1

設定終了
# save
# reset
```

支社 B を設定する

● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
```

```
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::67
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1 1
# remote 1 ipv6 route 1 2001:db8:1111:3::/64 1 2
# remote 1 ipv6 dvpn 0 invite acl 0 64 0
# acl 0 ipv6 2001:db8:1111:5::/64 2001:db8:1111:3::/64 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:5::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:5::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ipv6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipv6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::67
# template 0 sessionwatch address 2001:db8:1111:5::1

設定終了
# save
# reset
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:3::/64 1 1
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:2::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:1::67
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:5::/64 1 1
```

動的VPNサーバを設定する
dvpn server use on
dvpn server domain example.com
dvpn server auth use on
dvpn server auth aaa 0
aaa name dvpnserver
aaa user 0 id shisyaAid
aaa user 0 password shisyaApass
aaa user 1 id shisyaBid
aaa user 1 password shisyaBpass

設定終了
save
reset

2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN

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。

ここでは以下のコマンドによって、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。

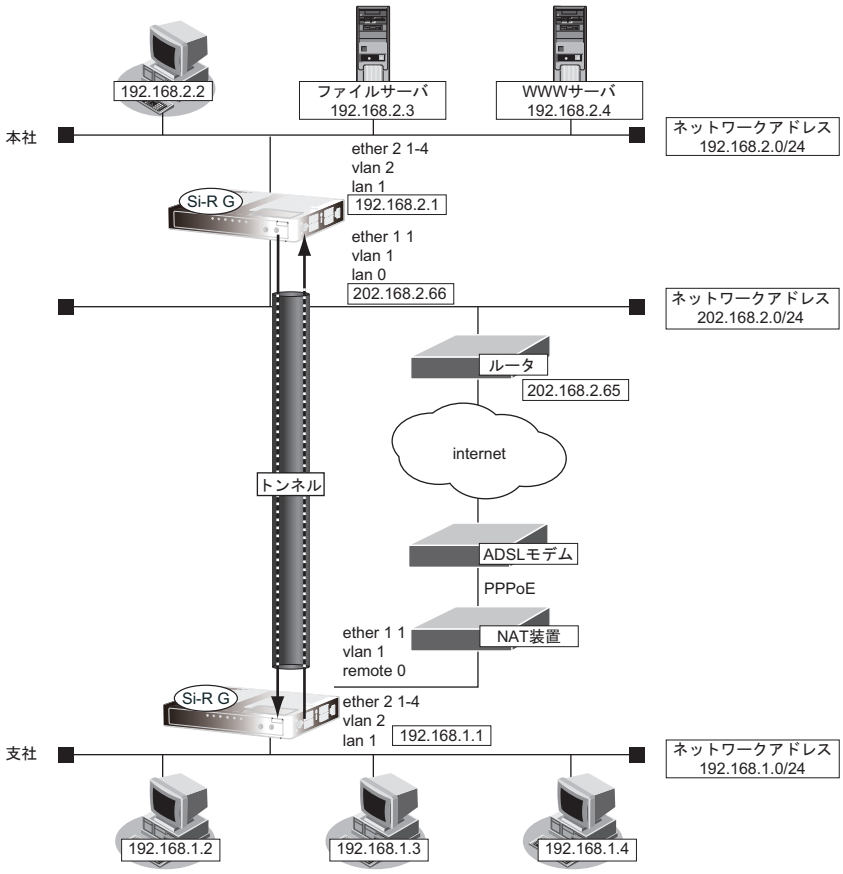
● 前提条件

[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 ポート　：ETHER グループ 1 ポート 1

[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　：aes-cbc-256
- IPsec認証アルゴリズム　：hmac-sha1
- 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　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：aes-cbc-256
- IKE認証アルゴリズム　：hmac-sha1
- 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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
PPPoE を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip msschange 1414

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# commit
```

本社（**Responder**）を設定する

● コマンド

```
LAN を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

VPN を設定する
# remote 0 name vpn-shi
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt aes-cbc-256
# remote 0 ap 0 ipsec ike auth hmac-sha1
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 0 ap 0 ike proposal 0 hash hmac-sha1
# remote 0 ap 0 ike nat-traversal use on
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# commit
```

2.13.16 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

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。

ここでは以下のコマンドによって、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。

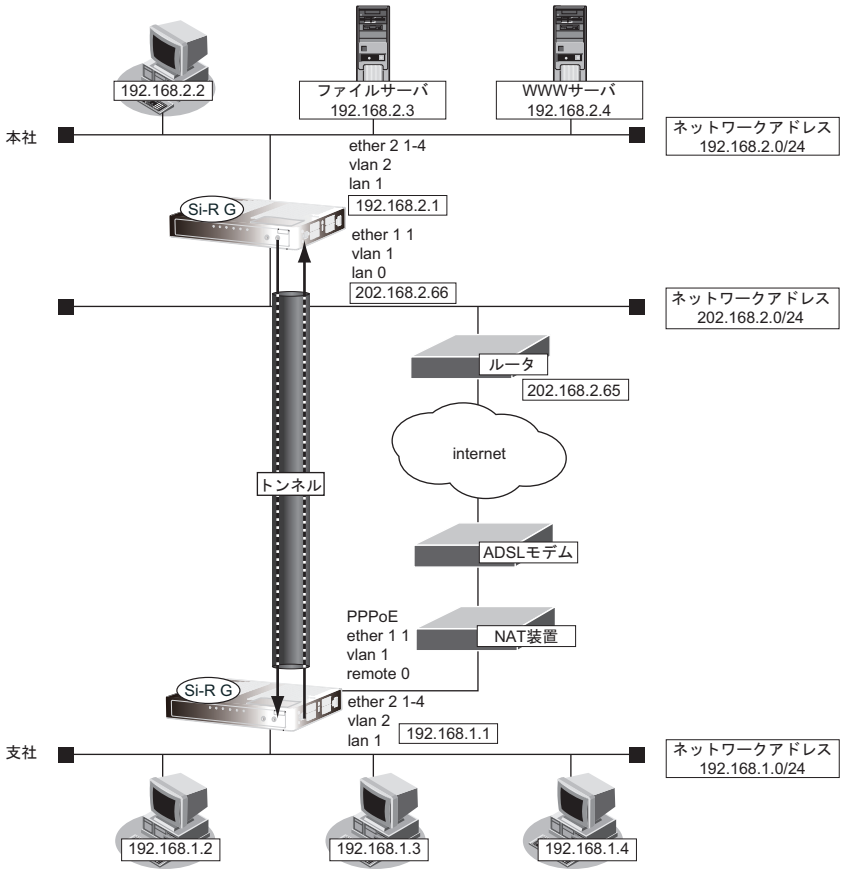
● 前提条件

[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 ポート　：ETHER グループ 1 ポート 1

[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　：aes-cbc-256
- IPsec認証アルゴリズム　：hmac-sha1
- 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　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：aes-cbc-256
- IKE認証アルゴリズム　：hmac-sha1
- 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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
PPPoE を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip msschange 1414

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# commit
```

本社（**Responder**）を設定する

● コマンド

```
LAN を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

VPN（テンプレート）を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-256
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt aes-cbc-256
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 ike nat-traversal use on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name vpn-shi
# aaa 0 user 0 id shisya
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 2

設定終了
# save
# commit
```

2.13.17 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

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。

ここでは以下のコマンドによって、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ポート　：ETHERグループ1ポート1
- 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ポート　：ETHERグループ1ポート1
- 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ポート　：ETHERグループ1ポート1
- 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
- ローカルネットワークETHERポート　：ETHERグループ2ポート1～4
- ローカルネットワークETHERポートVLAN　：2
- 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
- インターネット接続ETHERポート　：ETHERグループ1ポート1
- インターネット接続ETHERポートVLAN　：1

● 設定コマンド

[本社（PPPoE常時接続）]

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid0 userpass0
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社A（PPPoE常時接続）]

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

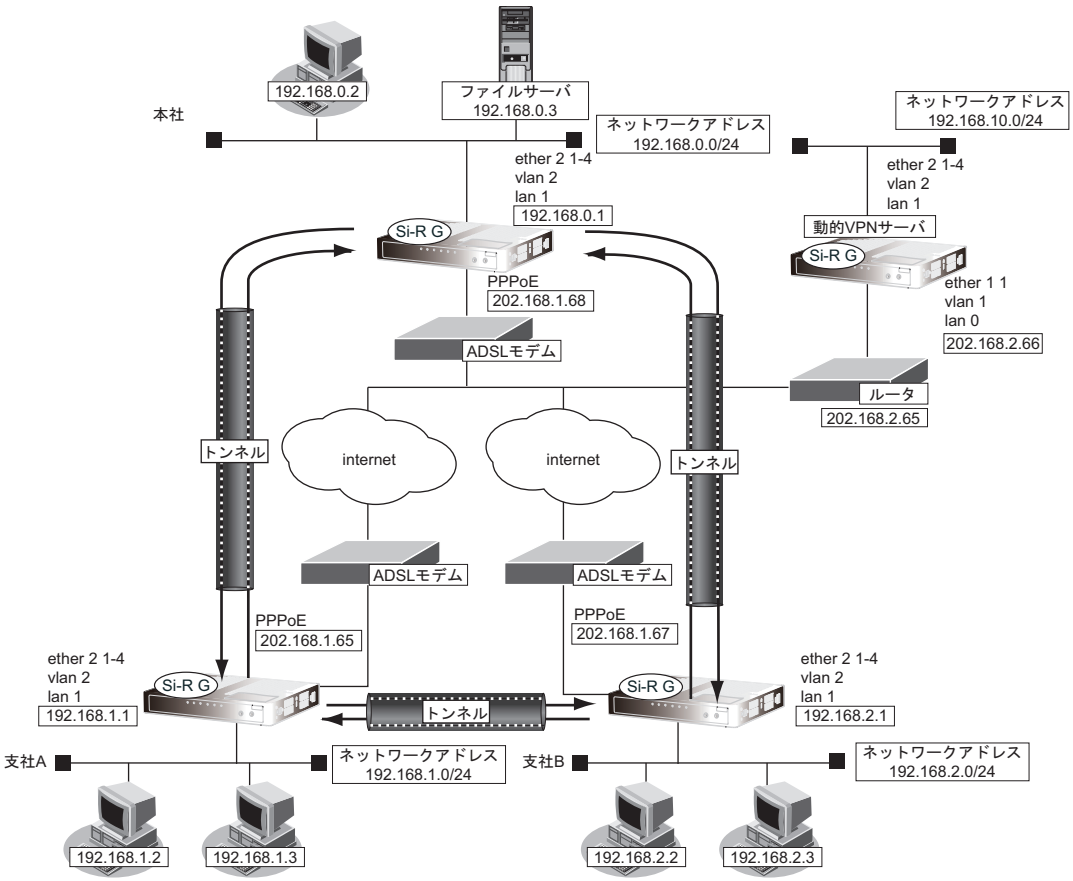
[支社B（PPPoE常時接続）]

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
```

```
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[動的VPNサーバ]

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.10.1/24 3
# lan 1 vlan 2
```



● 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 - 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 - 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 - 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　：pre-shared（事前共有鍵方式）
- 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
- INVITE自動ignore機能　：使用する
- 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　：pre-shared（事前共有鍵方式）
- 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コマンド例を示します。

本社を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
# remote 0 ip nat static 0 192.168.0.1 500 any 500 17
# remote 0 ip nat static 1 192.168.0.1 any any any 50
# remote 0 ip nat static default reject

本社-動的VPNサーバ間のVPNを設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local honsya
# remote 1 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1

本社-支社A/B間の動的VPNを設定する
# remote 0 ip dvpn 0 invite acl 0 24 0
# remote 0 ip dvpn 1 invite acl 1 24 0
# acl 0 ip 192.168.0.0/24 192.168.1.0/24 any any
# acl 1 ip 192.168.0.0/24 192.168.2.0/24 any any
# template 0 name vpn-shi
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.0.1
# template 0 sessionwatch address 192.168.0.1
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth honsyaid honsyapass
# dvpn client 0 ua 192.168.0.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.0.0/24 on
# dvpn client 0 localid honsya
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社 A を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

支社 A- 動的 VPN サーバ間の VPN を設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1

本社 - 支社 A 間の動的 VPN を設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.1.1
# remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.2.0/24 1 2

支社間の動的 VPN を設定する
# remote 2 ip dvpn 0 autoignore
# remote 2 ip dvpn 1 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
# template 0 name vpn-shiB
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
```

```
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社Bを設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

支社B-動的VPNサーバ間のVPNを設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1

本社-支社B間の動的VPNを設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.2.1
# remote 2 ap 0 sessionwatch address 192.168.2.1 192.168.0.1
```

```
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.1.0/24 1 2

支社間の動的VPN を設定する
# remote 2 ip dvpn 0 autoignore
# remote 2 ip dvpn 1 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
# template 0 name vpn-shiA
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

動的 VPN サーバを設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-hon
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote honsya
# remote 0 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.0.0/24 1 1
# remote 1 name vpn-shi
# remote 1 ap 0 name shisyaA
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1
# remote 2 name vpn-shiB
# remote 2 ap 0 name shisyaB
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaB
# remote 2 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.2.0/24 1 1

動的VPN サーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# aaa 0 name dvpnserver
# aaa 0 user 0 id honsyaid
# aaa 0 user 0 password honsyapass
# aaa 0 user 1 id shisyaAid
# aaa 0 user 1 password shisyaApass
# aaa 0 user 2 id shisyaBid
# aaa 0 user 2 password shisyaBpass

設定終了
# save
# reset
```

2.13.18 RSA デジタル署名認証を使用した固定 IP アドレスでの VPN（自動鍵交換）

RSA デジタル署名認証を使用した、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。

ここでは以下のコマンドによって、支店は 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。

また、事前に「2.41 PKI 機能を使う」（P.418）で証明書関連情報の設定が行われている必要があります。

● 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ポート　：ETHER グループ 2 ポート 1～4
- ローカルネットワークポート VLAN　：2
- 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 ポート　：ETHER グループ 1 ポート 1
- PPPoE ポート VLAN　：1

[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

● 設定コマンド

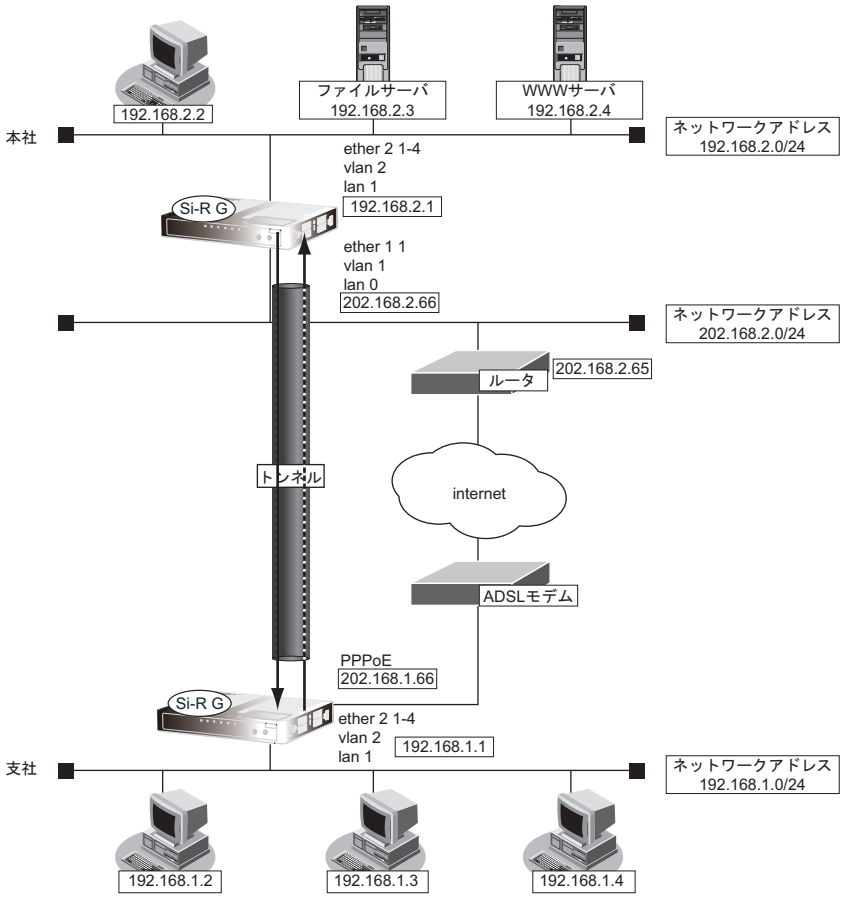
[支社（PPPoE 常時接続）]

```
# delete ether 1
# delete ether 2
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

[本社]

```
# delete ether 1
# delete ether 2
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
```

```
# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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
- 相手装置証明書識別番号　　：なし
- 自装置証明書識別番号　　：0
- 秘密識別番号　　：0

[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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[共通]

- 鍵交換タイプ　：Main Mode
- 自装置証明書情報の送信　：証明書要求ペイロード受信時
- 証明書要求　：送信する
- 認証局識別番号　：なし
- 有効期限切れ証明書　：使用する
- 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認証方法　：rsa-signature（RSAデジタル署名）
- 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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

本社（Responder）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.1.66
# remote 1 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# reset
```

2.13.19 RSAデジタル署名認証を使用した可変IPアドレスでのVPN（自動鍵交換）

RSAデジタル署名認証を使用した、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。

ここでは以下のコマンドによって、支店は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。

また、事前に「2.41 PKI機能を使う」（P.418）で証明書関連情報の設定が行われている必要があります。

● 前提条件

[支社（PPPoE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接続ポート　：ETHERグループ２ポート１～４
- ローカルネットワーク接続ポートVLAN　：2
- 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ポート　：ETHERグループ１ポート１
- PPPoEポートVLAN　：1

[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ポート　：ETHERグループ２ポート１～４
- ローカルネットワークポートVLAN　：2
- 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
- インターネット接続ポート　：ETHERグループ１ポート１
- インターネット接続ポートVLAN　：1

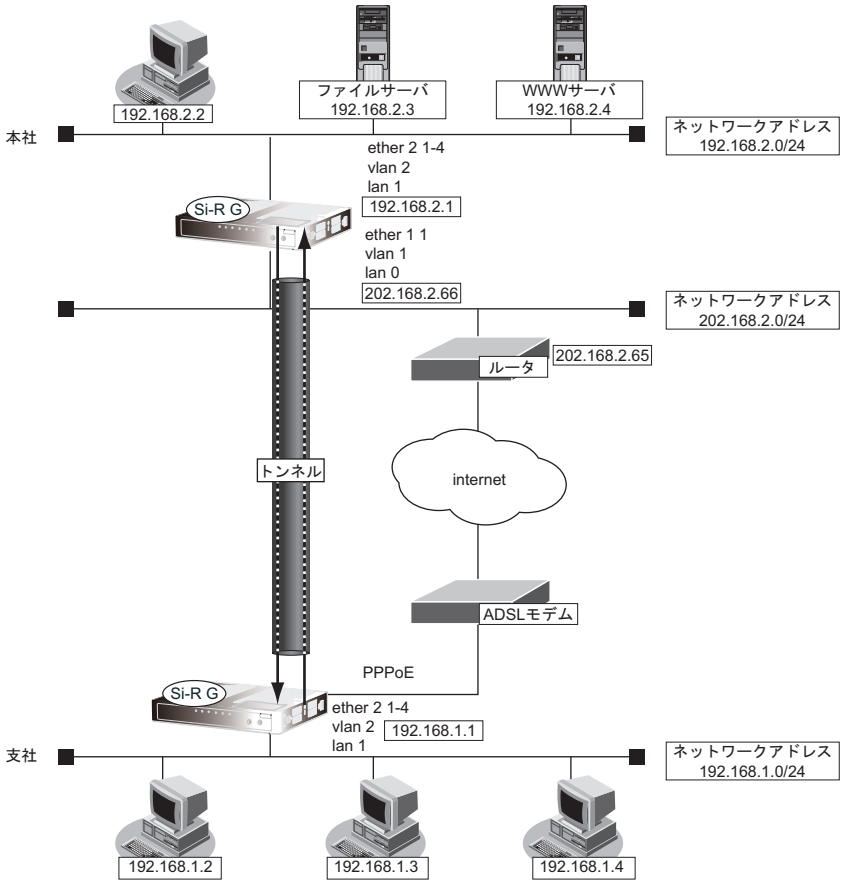
● 設定コマンド

[支社（PPPoE接続）]

```
# delete ether 1
# delete ether 2
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[本社]

```
# delete ether 1
# delete ether 2
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● 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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[共通]

- 鍵交換タイプ　：Aggressive Mode
- 自装置証明書情報の送信　：証明書要求ペイロード受信時
- 証明書要求　：送信する
- 認証局識別番号　：なし
- 有効期限切れ証明書　：使用する
- 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認証方法　：rsa-signature（RSAデジタル署名）
- 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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

本社（Responder）を設定する

● コマンド

```
VPNを設定する
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike name remote shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# reset
```

2.13.20 RSAデジタル署名認証で接続先情報（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN

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を構築し、RSAデジタル署名認証をする場合の設定方法を説明します。

ここでは以下のコマンドによって、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。

また、事前に「2.41 PKI機能を使う」（P.418）で証明書関連情報の設定が行われている必要があります。

● 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ポート　：ETHERグループ1ポート1
- 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ポート　：ETHERグループ1ポート1
- 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ポート　：ETHERグループ1ポート1
- 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
- ローカルネットワークETHERポート　：ETHERグループ2ポート1～4
- ローカルネットワークETHERポートVLAN　：2
- 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
- インターネット接続ETHERポート　：ETHERグループ1ポート1
- インターネット接続ETHERポートVLAN　：1

● 設定コマンド

[本社（PPPoE 常時接続）]

```
インターネットからIPsec/IKEパケットを受信する設定をする
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid0 userpass0
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社A（PPPoE 常時接続）]

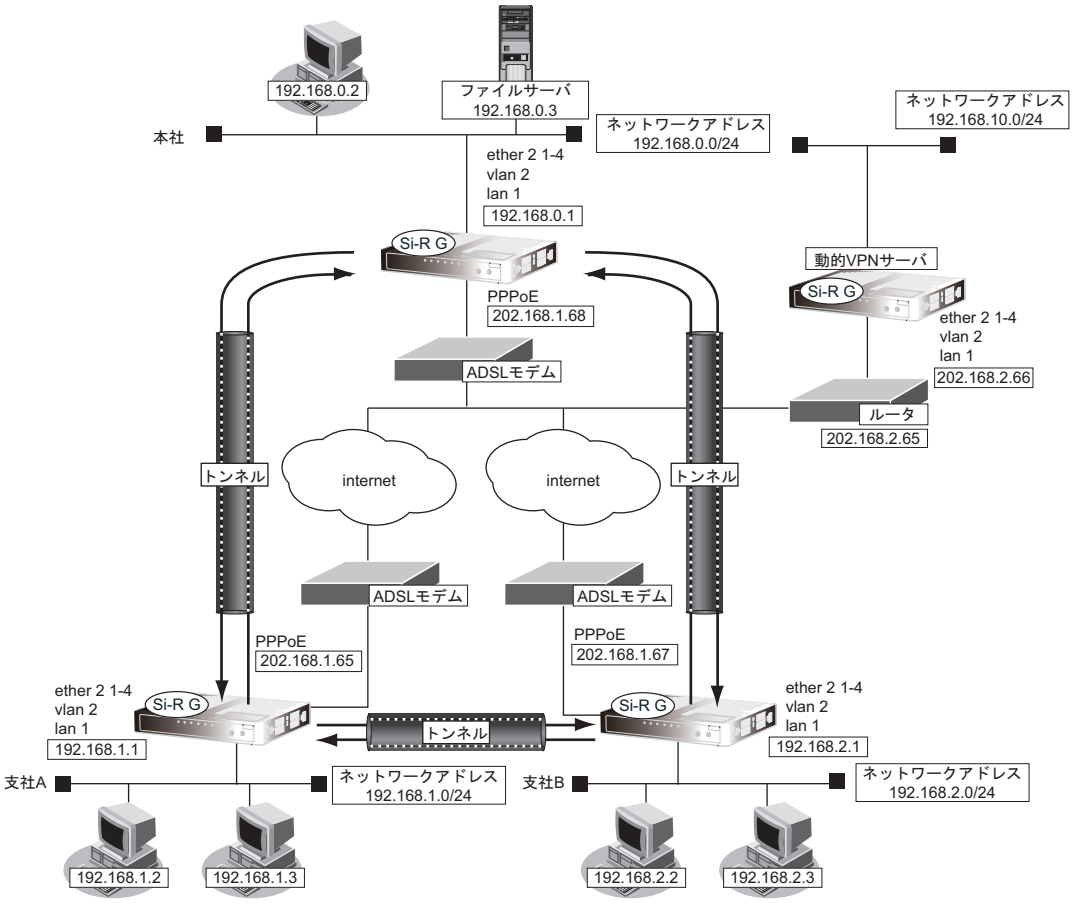
```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[支社 B（PPPoE 常時接続）]

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

[動的 VPN サーバ]

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.10.1/24 3
# lan 1 vlan 2
```



● 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 - 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 - 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 - 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認証方法　：rsa-signature
- 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
- 自装置証明書情報の送信　：証明書要求ペイロード受信時
- 証明書要求　：送信する
- 認証局識別番号　：なし
- 有効期限切れ証明書　：使用する
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

● 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

[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認証方法　：rsa-signature
- 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コマンド例を示します。

本社を設定する

● コマンド

```
インターネットからIPsec/IKEパケットを受信するように設定する
# remote 0 ip nat static 0 192.168.0.1 500 any 500 17
# remote 0 ip nat static 1 192.168.0.1 any any any 50
# remote 0 ip nat static default reject

本社-動的VPNサーバ間のVPNを設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local honsya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1

本社-支社A/B間の動的VPNを設定する
# remote 0 ip dvpn 0 invite acl 0 24 0
# remote 0 ip dvpn 1 invite acl 1 24 0
# acl 0 ip 192.168.0.0/24 192.168.1.0/24 any any
# acl 1 ip 192.168.0.0/24 192.168.2.0/24 any any
# template 0 name vpn-shi
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike proposal 0 auth-method rsa-signature
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike certificate local 0
# template 0 ike certificate key 0
# template 0 tunnel local 192.168.0.1
# template 0 sessionwatch address 192.168.0.1
# dvpn client 0 server 0 address 192.168.10.1 5070
```

```
# dvpn client 0 server 0 auth honsyaid honsyapass
# dvpn client 0 ua 192.168.0.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.0.0/24 on
# dvpn client 0 localid honsya
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

支社 A を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

支社 A- 動的 VPN サーバ間の VPN を設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1

本社 - 支社 A 間の動的 VPN を設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike proposal 0 auth-method rsa-signature
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 ike certificate local 0
# remote 2 ap 0 ike certificate key 0
# remote 2 ap 0 tunnel local 192.168.1.1
# remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.2.0/24 1 2
```

支社間の動的VPNを設定する
remote 2 ip dvpn 0 invite acl 0 24 0
acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
template 0 name vpn-shiB
template 0 interface pool 10 10
template 0 datalink type ipsec
template 0 combine use dvpn
template 0 dvpn client 0
template 0 ipsec ike protocol esp
template 0 ipsec ike encrypt aes-cbc-128
template 0 ipsec ike auth hmac-sha1
template 0 ipsec ike pfs modp768
template 0 ike proposal 0 auth-method rsa-signature
template 0 ike proposal 0 encrypt aes-cbc-128
template 0 ike proposal 0 hash hmac-sha1
template 0 ike proposal 0 pfs modp768
template 0 ike certificate local 0
template 0 ike certificate key 0
template 0 tunnel local 192.168.1.1
template 0 sessionwatch address 192.168.1.1

動的VPN（共通部分）を設定する
dvpn client 0 server 0 address 192.168.10.1 5070
dvpn client 0 server 0 auth shisyaAid shisyaApass
dvpn client 0 ua 192.168.1.1
dvpn client 0 domain example.com
dvpn client 0 localnet 0 192.168.1.0/24 on
dvpn client 0 interface rmt 0
dvpn client 0 priority 10
dvpn client 0 ip route distance 1

設定終了
save
reset

支社 B を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

支社 B- 動的 VPN サーバ間の VPN を設定する
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1

本社 - 支社 B 間の動的 VPN を設定する
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike proposal 0 auth-method rsa-signature
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 ike certificate local 0
# remote 2 ap 0 ike certificate key 0
# remote 2 ap 0 tunnel local 192.168.2.1
# remote 2 ap 0 sessionwatch address 192.168.2.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.1.0/24 1 2

支社間の動的 VPN を設定する
# remote 2 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
# template 0 name vpn-shiA
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike proposal 0 auth-method rsa-signature
```

```
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike certificate local 0
# template 0 ike certificate key 0
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

動的 VPN サーバを設定する

● コマンド

```
VPNを設定する
# remote 0 name vpn-hon
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote honsya
# remote 0 ap 0 ike proposal 0 auth-method rsa-signature
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike certificate local 0
# remote 0 ap 0 ike certificate key 0
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.0.0/24 1 1
# remote 1 name vpn-shi
# remote 1 ap 0 name shisyaA
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaA
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1
# remote 2 name vpn-shiB
# remote 2 ap 0 name shisyaB
# remote 2 ap 0 datalink type ipsec
```

```
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaB
# remote 2 ap 0 ike proposal 0 auth-method rsa-signature
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 ike certificate local 0
# remote 2 ap 0 ike certificate key 0
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.2.0/24 1 1

動的VPNサーバを設定する
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# aaa 0 name dvpnserver
# aaa 0 user 0 id honsyaid
# aaa 0 user 0 password honsyapass
# aaa 0 user 1 id shisyaAid
# aaa 0 user 1 password shisyaApass
# aaa 0 user 2 id shisyaBid
# aaa 0 user 2 password shisyaBpass

設定終了
# save
# reset
```

2.13.21 IPv4 over IPv4 で NAT と併用しない固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「1.9.1 NAT と併用しない固定 IP アドレスでの VPN（自動鍵交換）」（P.35）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「1.9.1 NAT と併用しない固定 IP アドレスでの VPN（自動鍵交換）」（P.35）と同じです。そちらを参照してください。

● 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]

- IKE Version　：ikev2
- 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
- IPsecV3 ESN　：あり
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- 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 PRF アルゴリズム　：hmac-md5

- IKE 支社 A ID タイプ　：address
- IKE 本社 ID タイプ　：address

[共通 B]

- IKE Version　：ikev2
- IPsec プロトコル　：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
- IPsecV3 ESN　：あり
- 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
- IKE PRF アルゴリズム　：hmac-sha1
- IKE 支社 B ID タイプ　：address
- IKE 本社 ID タイプ　：address

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コマンド例を示します。

支社 A を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

支社 B を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.3.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```

2.13.22 IPv4 over IPv4 で NAT と併用した可変 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「1.9.3 NAT と併用した可変 IP アドレスでの VPN（自動鍵交換）」（P.48）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「1.9.3 NAT と併用した可変 IP アドレスでの VPN（自動鍵交換）」（P.48）と同じです。そちらを参照してください。

● 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（Responder）]

- 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]

- IKE Version　：ikev2
- 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
- IPsecV3 ESN　：あり

- IKE支社A ID/IDタイプ　：shisyaA（自装置名）/FQDN
- IKE本社 IDタイプ　：address
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- 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 PRFアルゴリズム　：hmac-md5

[共通B]

- IKE Version　：ikev2
- IPsecプロトコル　：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
- IPsecV3 ESN　：あり
- IKE支社B ID/IDタイプ　：shisyaB（自装置名）/FQDN
- IKE本社 IDタイプ　：address
- 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
- IKE PRFアルゴリズム　：hmac-sha1

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？

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コマンド例を示します。

支社 A（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

支社 B（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.3.1 500 any 500 17
# remote 0 ip nat static 1 192.168.3.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```

本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype fqdn
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype fqdn
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```

2.13.23 IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）」（P.161）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）」（P.161）と同じです。そちらを参照してください。

● 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]

- IKE Version　：ikev2
- 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
- IPsecV3 ESN　：あり
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- 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 PRF アルゴリズム　：hmac-md5
- IKE 支社 ID タイプ　：address
- IKE 本社 ID タイプ　：address

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コマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

2.13.24 IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）」（P.165）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN（自動鍵交換）」（P.165）と同じです。そちらを参照してください。

● 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]

- IKE Version　：ikev2
- 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
- IPsecDH グループ　：なし
- IPsecV3 ESN　：あり
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- 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 PRF アルゴリズム　：hmac-md5
- IKE 支社 ID タイプ　：address
- IKE 本社 ID タイプ　：address

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コマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

2.13.25 IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「2.13.4 IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）」（P.169）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.4 IPv6 over IPv4 で可変 IP アドレスでの VPN（自動鍵交換）」（P.169）と同じです。そちらを参照してください。

● 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（Responder）]

- 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]

- IKE Version　：ikev2
- 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
- IPsecV3 ESN　：あり
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 本社 ID タイプ　：address
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- 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 PRF アルゴリズム　：hmac-md5

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？

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype fqdn
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

2.13.26 IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「2.13.5 IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）」（P.173）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.5 IPv6 over IPv6 で固定 IP アドレスでの VPN（自動鍵交換）」（P.173）と同じです。そちらを参照してください。

● 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]

- IKE Version　：ikev2
- 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
- IPsecV3 ESN　：あり
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- 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 PRF アルゴリズム　：hmac-md5
- IKE 支社 ID タイプ　：address
- IKE 本社 ID タイプ　：address

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コマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:3::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

2.13.27 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 IKE Version2）

「2.13.6 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）」（P.177）をIKE Version2を使ってVPNを構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.6 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）」（P.177）と同じです。そちらを参照してください。

● 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]

- IKE Version　：ikev2
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：des-cbc
- IPsec PFS時のDHグループ　：なし
- IPsecV3 ESN　：あり
- IKE共有鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方式　：pre-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）
- IKE PRFアルゴリズム　：hmac-md5
- IKE支社IDタイプ　：address
- IKE本社IDタイプ　：address

上記の設定条件に従って設定を行う場合のコマンド例を示します。

支社を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ip route 1 192.168.3.0/24 1 1
# remote 1 ap 0 name honten1
# remote 1 ap 0 multiroute pattern 0 use any any 192.168.2.0/24 any 0 any
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.2.0/24
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5
# remote 1 ap 1 datalink type ipsec
# remote 1 ap 1 ipsec type ikev2
# remote 1 ap 1 ipsec ike protocol esp
# remote 1 ap 1 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 1 ipsec ike encrypt des-cbc
# remote 1 ap 1 ipsec ike auth hmac-md5
# remote 1 ap 1 ike bind ap 0

設定終了
# save
# commit
```

本社を設定する

● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shiten
# remote 0 ap 0 multiroute pattern 0 use 192.168.2.0/24 any any any 0 any
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
# remote 0 ap 1 datalink type ipsec
# remote 0 ap 1 ipsec type ikev2
```

```
# remote 0 ap 1 ipsec ike protocol esp
# remote 0 ap 1 ipsec ike range 192.168.3.0/24 any4
# remote 0 ap 1 ipsec ike encrypt des-cbc
# remote 0 ap 1 ipsec ike auth hmac-md5
# remote 0 ap 1 ike bind ap 0

設定終了
# save
# commit
```

2.13.28 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 IKE Version2）

「2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN」（P.228）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN」（P.228）と同じです。そちらを参照してください。

● 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

[本社（Responder）]

- 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]

- IKE Version　：ikev2
- IPsec プロトコル　：esp
- IPsec 暗号アルゴリズム　：aes-cbc-256
- IPsec 認証アルゴリズム　：hmac-sha1
- IPsec DH グループ　：なし
- IPsecV3 ESN　：あり
- IKE 支社 ID/ID タイプ　：shisya（自装置名）/FQDN
- IKE 本社 ID タイプ　：address
- IKE 認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE 認証方法　：pre-shared（事前共有鍵方式）
- IKE 暗号アルゴリズム　：aes-cbc-256
- IKE 認証アルゴリズム　：hmac-sha1
- IKE DH グループ　：modp768
- IKE PRF アルゴリズム　：hmac-sha1
- 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？

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# delete remote 1
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike proposal 0 prf hmac-sha1
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# commit
```

本社（**Responder**）を設定する

● コマンド

```
LAN を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

VPN を設定する
# remote 0 name vpn-shi
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt aes-cbc-256
# remote 0 ap 0 ipsec ike auth hmac-sha1
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype fqdn
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 0 ap 0 ike proposal 0 hash hmac-sha1
# remote 0 ap 0 ike proposal 0 prf hmac-sha1
# remote 0 ap 0 ike nat-traversal use on
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# commit
```

2.13.29 RSA デジタル署名認証を使用した固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）

「2.13.18 RSA デジタル署名認証を使用した固定 IP アドレスでの VPN（自動鍵交換）」（P.247）を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.18 RSA デジタル署名認証を使用した固定 IP アドレスでの VPN（自動鍵交換）」（P.247）と同じです。そちらを参照してください。

また、事前に「2.41 PKI 機能を使う」（P.418）で証明書関連情報の設定が行われている必要があります。

● 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　：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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[本社（Responder）]

- 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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[共通]

- IKE Version　：ikev2
- 自装置証明書情報の送信　：証明書要求ペイロード受信時
- 証明書要求　：送信する
- 認証局識別番号　：なし
- 有効期限切れ証明書　：使用する
- 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 認証方法　：rsa-signature（RSA デジタル署名）
- 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 PRF アルゴリズム　：hmac-md5

- IKE 支社 ID タイプ　：address
- IKE 本社 ID タイプ　：address

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save

再起動
# reset
```

本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.1.66
# remote 1 ip route 0 192.168.1.0/24 1 1

設定終了
# save

再起動
# reset
```

2.13.30 RSAデジタル署名認証を使用した可変IPアドレスでのVPN（自動鍵交換 IKE Version2）

「2.13.19 RSAデジタル署名認証を使用した可変IPアドレスでのVPN（自動鍵交換）」（P.251）をIKE Version2を使ってVPNを構築する場合の設定方法を説明します。

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。

前提条件の設定および構成例は「2.13.19 RSAデジタル署名認証を使用した可変IPアドレスでのVPN（自動鍵交換）」（P.251）と同じです。そちらを参照してください。

また、事前に「2.41 PKI機能を使う」（P.418）で証明書関連情報の設定が行われている必要があります。

● 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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[本社（Responder）]

- 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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0

[共通]

- IKE Version　：ikev2
- 自装置証明書情報の送信　：証明書要求ペイロード受信時
- 証明書要求　：送信する
- 認証局識別番号　：なし
- 有効期限切れ証明書　：使用する
- 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
- IPsecV3 ESN　：あり
- IKE支社ID/IDタイプ　：shisya（自装置名）/FQDN
- IKE本社IDタイプ　：address
- IKE認証方法　：rsa-signature（RSAデジタル署名）
- 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 PRF アルゴリズム　：hmac-md5

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？

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save

再起動
# reset
```

本社（**Responder**）を設定する

● コマンド

```
VPN を設定する
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype fqdn
# remote 1 ap 0 ike name remote shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1

設定終了
# save

再起動
# reset
```

2.13.31　EAP 認証を使用した固定 IP アドレスでの VPN（自動鍵交換 IKE Version2）

EAP 認証機能を使用した、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。
ここでは以下のコマンドによって、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 終端装置が接続されていることを前提とします。
また、事前に「2.41.3 認証局証明書を設定する」（P.426）で相手装置から発行された証明書関連情報の設定が行われている必要があります。

● 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ポート　：ETHER グループ 2 ポート 1～4
- ローカルネットワークポート VLAN　：2
- 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 ユーザパスワード　：userpass（プロバイダから提示された内容）
- PPPoE ポート　：ETHER グループ 1 ポート 1
- PPPoE ポート VLAN　：1

[本社]

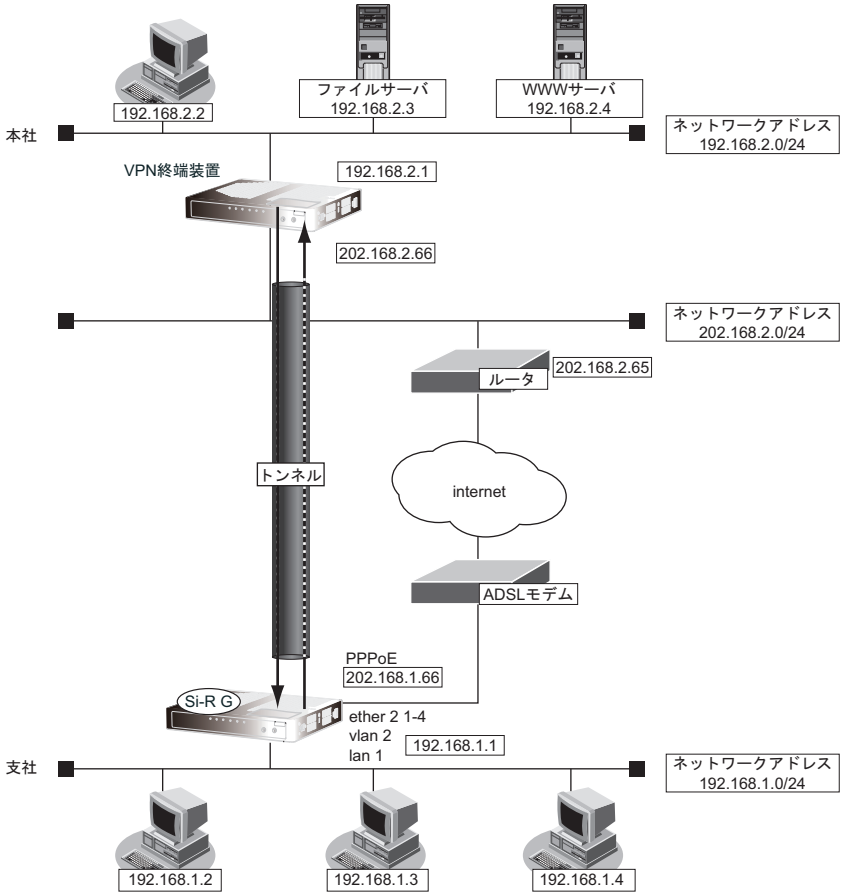
- ローカルネットワーク IPv4 アドレス　：192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス　：202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス　：202.168.2.65

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● 設定コマンド

```
支社（PPPoE 常時接続）を設定する
# delete ether 1
# delete ether 2
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
```

```
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```



● 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
- 相手装置証明書識別番号　：なし
- 自装置証明書識別番号　：0
- 秘密識別番号　：0
- IKE Version　：ikev2
- 証明書要求　：送信する
- 認証局識別番号　：0
- 有効期限切れ証明書　：使用する
- 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 タイプ　：FQDN
- IKE 本社 ID/ID タイプ　：honsya（自装置識別情報）/FQDN

- IKE 認証方法　：shared-key（事前共有鍵方式）
- 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 PRF アルゴリズム　：hmac-md5
- IKE EAP 認証 ID/PASSWORD　：shisya/shisyapass

こんな事に気をつけて

- EAP 認証機能を利用するときは、以下の点に注意してください。
  - IKE Version2 でのみ動作します。
  - 初回 IKE ネゴシエーションは Initiator でのみ動作します。
  - EAP 認証機能のユーザ ID とパスワードは対向装置と同一の設定となるよう設定してください。
    互いの装置で一致しないユーザ ID とパスワードが設定されていた場合、IKE ネゴシエーションで接続に失敗します。
  - EAP 認証機能を使用する場合、IDtype の設定は FQDN および USER_FQDN のみ有効となります。
    それ以外の設定の場合は、IKE ネゴシエーションで接続に失敗します。

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コマンド例を示します。

支社（Initiator）を設定する

● コマンド

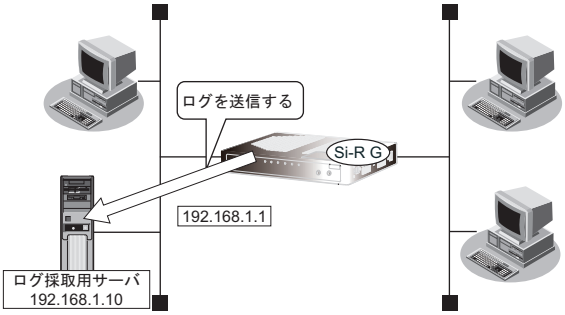
```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype fqdn
# remote 1 ap 0 ike name remote honsya
# remote 1 ap 0 ike proposal 0 auth-method shared-key
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate request enable 0
# remote 1 ap 0 ike eap auth send shisya shisyapass
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

2.14 システムログを採取する

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 syslog 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）

ここでは、システムログを採取する場合の設定方法を説明します。



● 設定条件

- 以下のプライオリティを設定する
  - プライオリティ LOG_ERROR
  - プライオリティ LOG_WARNING
  - プライオリティ LOG_NOTICE
  - プライオリティ LOG_INFO
- 以下のセキュリティログを採取する
  - IP フィルタ
  - NAT
  - PPP
  - DHCP
  - Proxy DNS
  - IDS
- 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システムログを採取する場合のコマンド例を示します。

● コマンド

```
# syslog server 0 address 192.168.1.10

システムログを設定する
# syslog pri error,warn,notice,info
# syslog security ipfilter,nat,ppp,dhcp,proxydns,ids

設定終了
# save
# commit
```

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。

2.15 マルチNAT機能（アドレス変換機能）を使う

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 マニュアル「機能説明書」

ヒント

◆ 同時に接続できる台数

機能	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	最大20000セッション	外部からの通信はできない
静的NAT	最大200個	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	最大200個	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

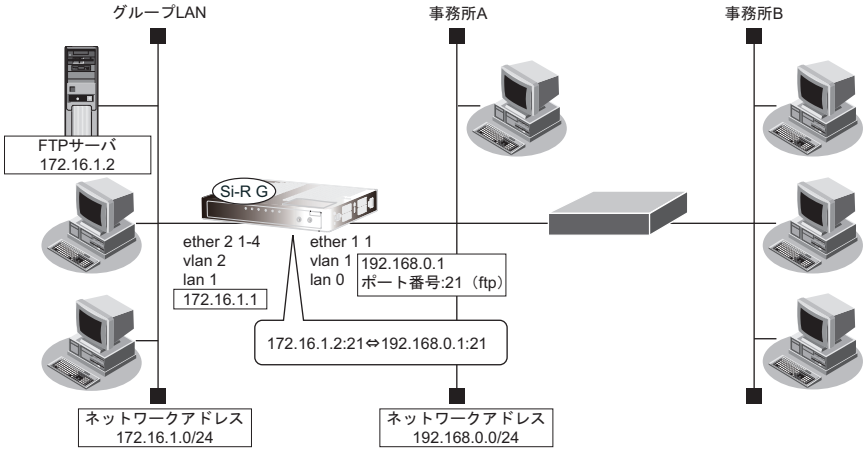
こんな事に気をつけて

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

2.15.1　プライベート LAN 接続でサーバを公開する

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]

- ETHER グループ 1 ポート 1 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コマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
```

こんな事に気をつけて

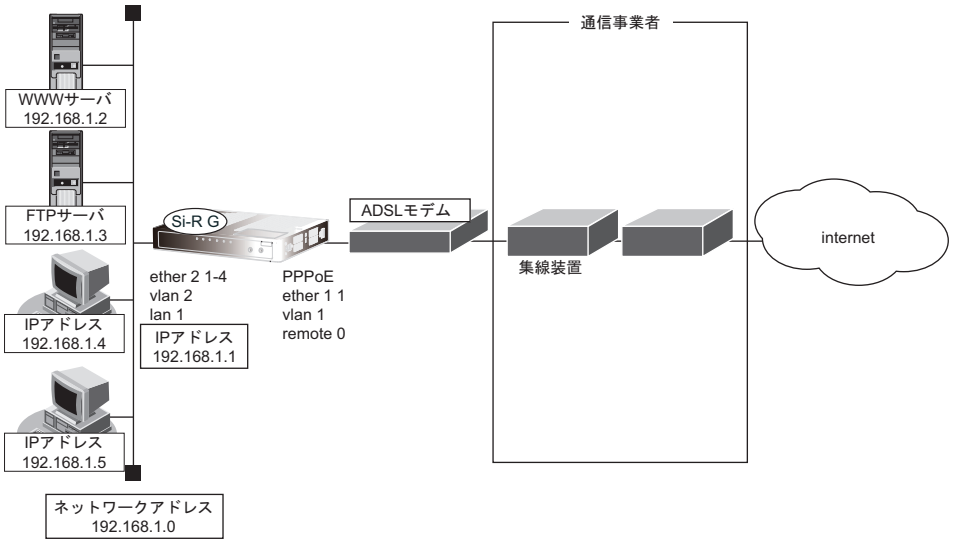
NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.15.2　PPPoE 接続でサーバを公開する

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
- ブロードキャストアドレス　：192.168.1.255

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
PPPoE でインターネットへ接続する環境を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414

# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0

NAT 情報を設定する
# remote 0 ip nat static 0 192.168.1.2 80 any 80 any
# remote 0 ip nat static 1 192.168.1.3 21 any 21 any

設定終了
# save

再起動
# reset
```

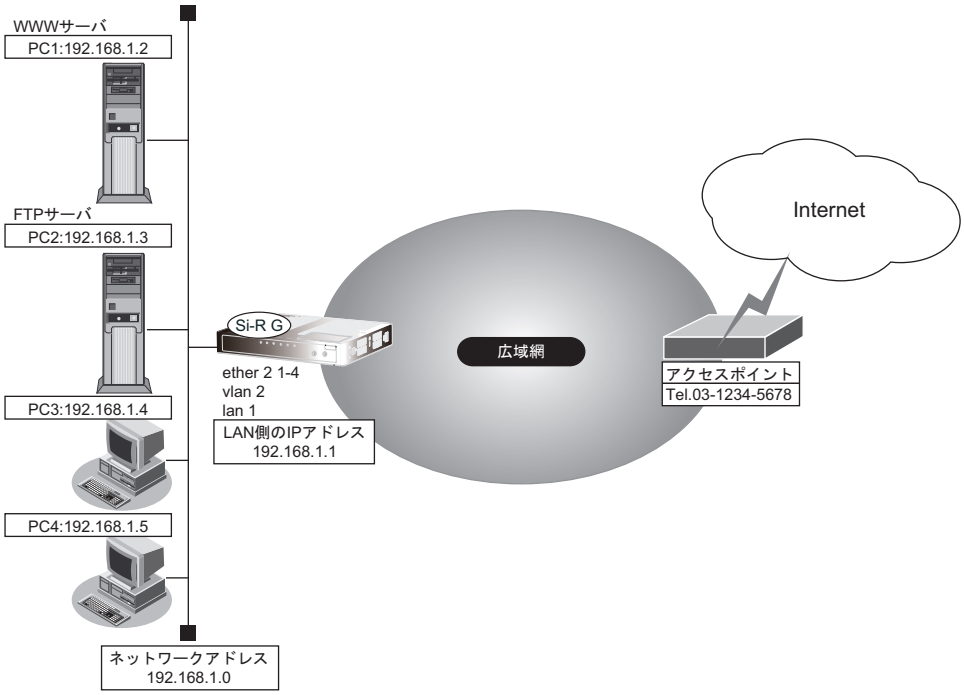
こんな事に気をつけて

- 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。
- 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。
- 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場合は、以下の設定を追加してください。

```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

2.15.3　ネットワーク型接続でサーバを公開する

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

- ネットワーク型接続を行う
- 広域網接続 ETHER ポート　：ETHERグループ 1 ポート 1
- 広域網接続 ETHER ポート VLAN　：1
- 広域網接続 lan インタフェース　：lan 0
- 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
- 既存の LAN を接続する ETHER ポート　：ETHERグループ 2 ポート 1～4
- 既存の LAN を接続する ETHER ポート VLAN　：2
- 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
広域網接続を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# lan 0 ip address 10.10.10.96/29 3

本装置のIP アドレスを設定する
# ether 2 1-4 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

NAT情報を設定する
# lan 0 ip nat mode multi 10.10.10.100 3 5m
# lan 0 ip nat static 0 192.168.1.2 80 10.10.10.98 80 any
# lan 0 ip nat static 1 192.168.1.3 21 10.10.10.99 21 any

設定終了
# save

再起動
# reset
```

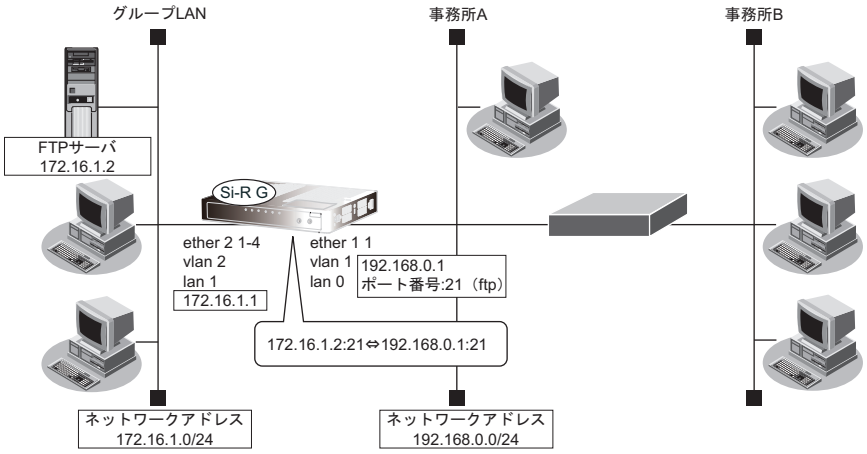
こんな事に気をつけて

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場合は、以下の設定を追加してください。

```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

2.15.4 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

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]

- ETHER グループ 1 ポート 1 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コマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode static any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
```

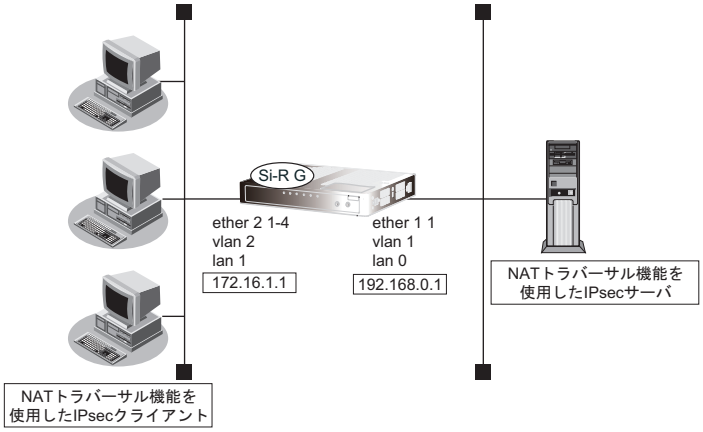
こんな事に気をつけて

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場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.15.5 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

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]

- ETHER グループ 1 ポート 1 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コマンド例を示します。

● コマンド

```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat wellknown 0 500 off

設定終了
# save
# commit
```

こんな事に気をつけて

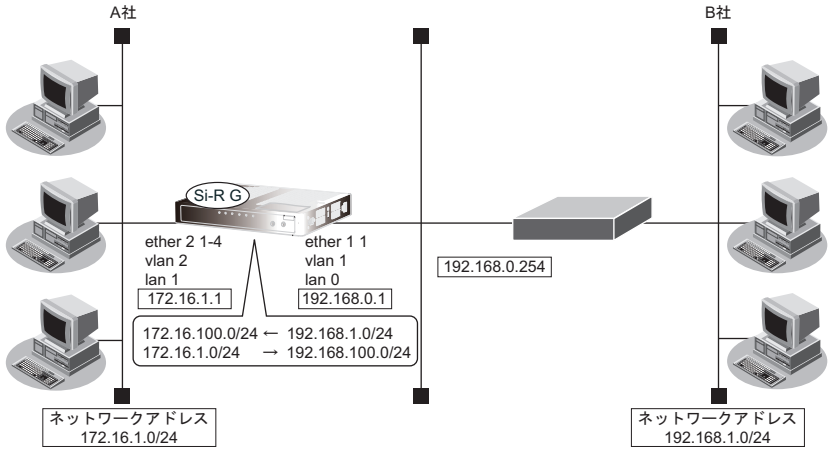
NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

2.15.6　NAT あて先変換で双方向のアドレスを変換する

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持つ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]

- ETHER グループ 1 ポート 1 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コマンド例を示します。

● コマンド

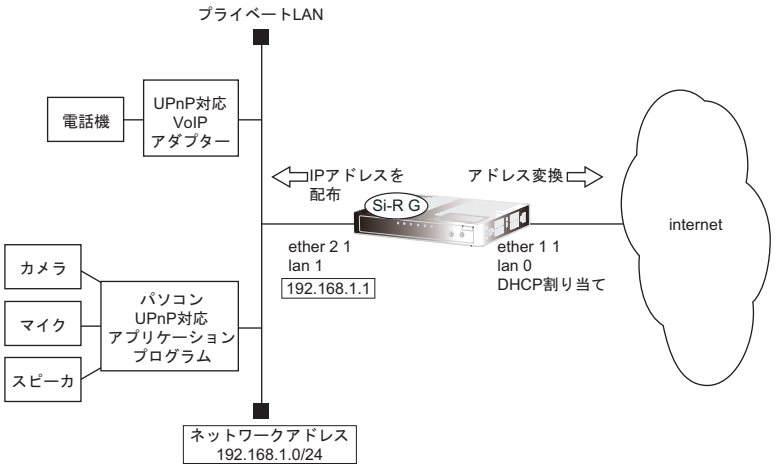
```
本装置の IP アドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

B 社 への経路を設定する
# lan 0 ip route 0 172.16.100.0/24 192.168.0.254

NAT 情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 any 192.168.100.2-192.168.100.254 any any
# lan 0 ip nat destination 0 172.16.100.2 192.168.1.2-192.168.1.254

設定終了
# save
# commit
```

2.16 VoIP NAT トラバーサル機能を使う

マルチNAT機能を使用すると動作しないVoIPアダプターが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 マニュアル「機能説明書」

ここでは、UPnP対応VoIPアダプターや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]

- ETHERグループ1ポート1を使用する
- 使用するVLAN ID　：1
- 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]

- ETHERグループ2ポート1を使用する
- 使用するVLAN ID　：2
- 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

こんな事に気をつけて

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

インターネット側のLAN情報を設定する
# lan 0 vlan 1
# lan 0 ip dhcp service client
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1
# lan 0 ip nat appli sip off

UPnP対応装置側のLAN情報を設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off

UPnP機能を設定する
# upnp use on

設定終了
# save

再起動
# reset
```

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、UPnP対応装置やパソコンの順に電源を投入します。

2.17 TOS/Traffic Class値書き換え機能を使う

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 マニュアル「機能説明書」

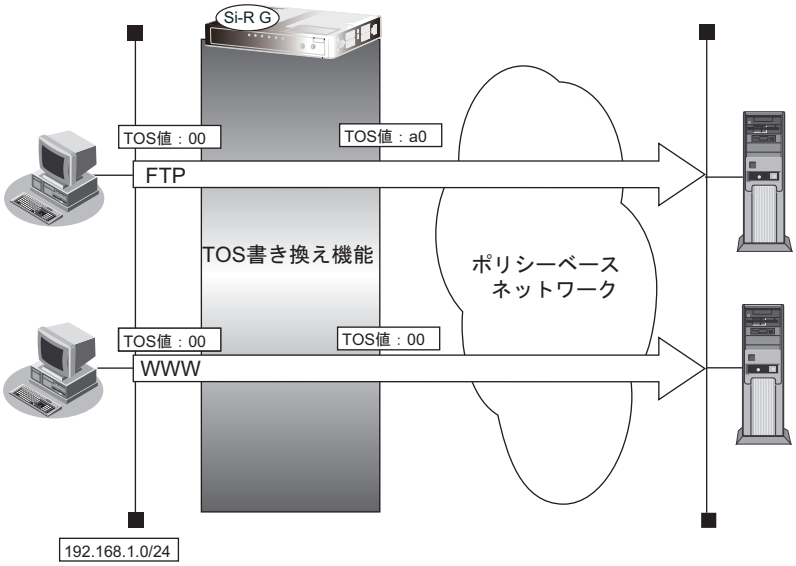
TOS/Traffic Class値書き換え機能の条件

本装置では、コマンドで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持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コマンド例を示します。

● コマンド

```
FTPサーバのアクセスでTOS値を00からa0に書き換える
# acl 0 ip 192.168.1.0/24 any 6 tos 0
# acl 0 tcp any 20,21 yes
# remote 0 ip tos 0 acl 0 a0

設定終了
# save
# commit
```

2.18 VLANプライオリティマッピング機能を使う

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、VLAN ID、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。

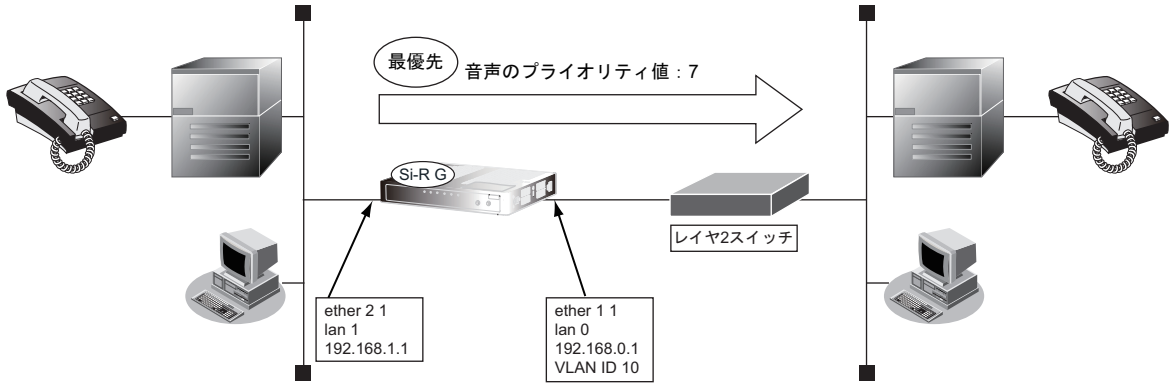
☛参照 マニュアル「機能説明書」

本装置では、コマンドで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。

- VLAN ID
- 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）



● 設定条件

- VLAN ID　：10
- 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コマンド例を示します。

● コマンド

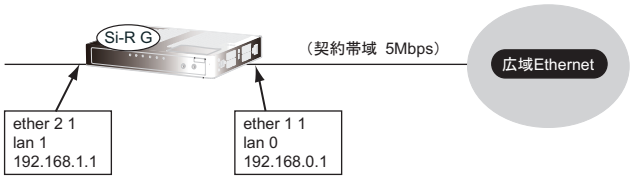
```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan tag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lanインタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

VLAN ID 10、TOS値 a0のパケットのプライオリティ値を7に設定する
# ether 1 1 vlan primap mode enable
# ether 1 1 vlan primap rule 0 10 ip a0 7

設定終了
# save
# commit
```

2.19 シェーピング機能を使う

シェーピング機能を使用すると、インタフェースから送出するデータ量を制限することができます。

2.19.1 特定のインタフェースでシェーピング機能を使う

ここでは、lan インタフェース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 側への送信データを、最大 5Mbps に制限する

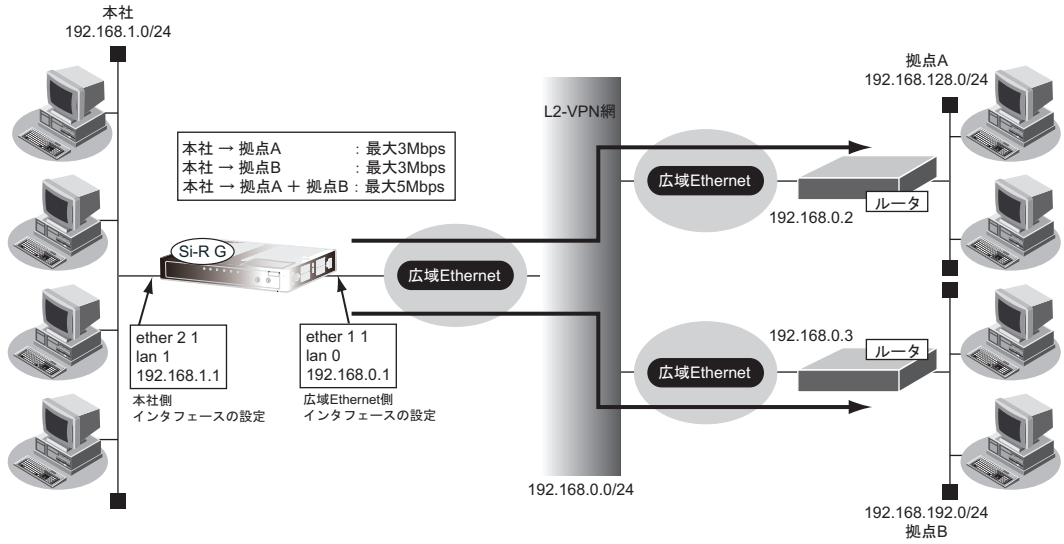
上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

lan 0 から送出するデータ量を 5Mbps に制限する
# lan 0 shaping on 5m

設定終了
# save
# commit
```

2.19.2　送信先ごとにシェーピング機能を使う

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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

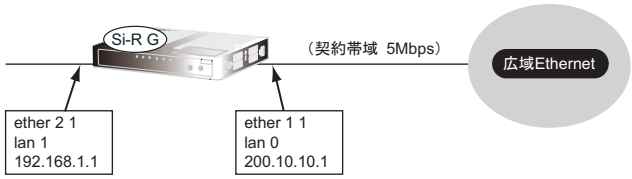
● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

lan 0 から送出するデータ量を 5Mbps に制限する
# lan 0 shaping on 5m

拠点 A の情報を設定する
# remote 0 name kyotenA
# remote 0 ip route 0 192.168.128.0/24 1 1
# remote 0 ap 0 name OV-A
# remote 0 ap 0 datalink type overlap
# remote 0 ap 0 overlap to lan 0
# remote 0 ap 0 overlap nexthop 192.168.0.2

拠点 B の情報を設定する
# remote 1 name kyotenB
```

```
# remote 1 ip route 0 192.168.192.0/24 1 1
# remote 1 ap 0 name OV-B
# remote 1 ap 0 datalink type overlap
# remote 1 ap 0 overlap to lan 0
# remote 1 ap 0 overlap nexthop 192.168.0.3

remote 0から送出するデータ量を3Mbpsに制限する
# remote 0 shaping on 3m

remote 1から送出するデータ量を3Mbpsに制限する
# remote 1 shaping on 3m

設定終了
# save
# commit
```

2.19.3　特定のポートでシェーピング機能を使う

ここでは、Ethernetポート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側への送信データを、最大5Mbpsに制限する

[広域Ethernet側]

- ポート　：ether 1 1を使う
- VLAN　：untag 10
- lan　：lan 0
- IPアドレス　：200.10.10.1/29

[LAN側]

- ポート　：ether 2 1を使う
- VLAN　：untag 20
- lan　：lan 1
- IPアドレス　：192.168.1.1/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 200.10.10.1/29 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

ether 1 1 から送出するデータ量を 5Mbps に制限する
# ether 1 1 shaping on 5m

設定終了
# save
# commit
```

2.20 ヘッダ圧縮機能を使う

PPP を使った相手装置との接続時に、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。

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。

- 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（remote 0）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

- ネットワーク 0（remote 0）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コマンド例を示します。

● コマンド

```
ヘッダ圧縮機能を設定する
# remote 0 ppp ipcp vjcomp enable
# remote 0 ppp ipcp iphc enable

設定終了
# save
# commit
```

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。

2.21 帯域制御（WFQ）機能を使う

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 マニュアル「機能説明書」

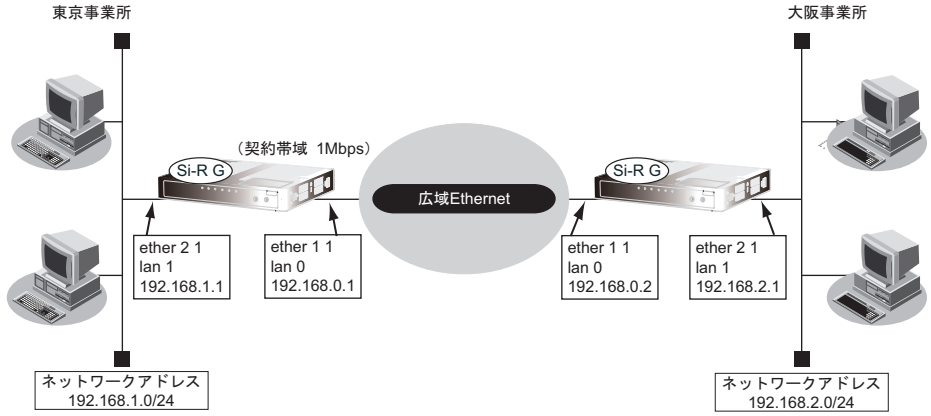
帯域制御（WFQ）機能の条件

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

2.21.1 特定のインタフェースで帯域制御（WFQ）機能を使う

ここでは、lanインタフェースから送出する音声データを最優先で透過させる場合の設定方法を説明します。



● 設定条件

- 広域Ethernet側への送信データを、最大1Mbpsに制限する
- 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コマンド例を示します。

● コマンド

東京事業所の設定

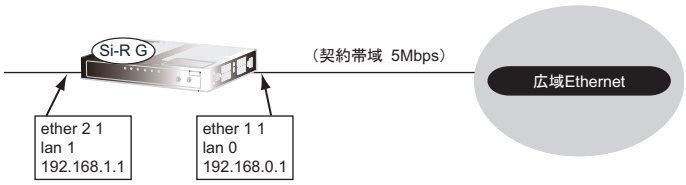
```
etherポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lanインタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 0 ip route 0 192.168.2.0/24 192.168.0.2 1
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

lan 0から送出するデータ量を1Mbpsに制限する
# lan 0 shaping on 1m

音声データを最優先で透過させる
# acl 0 ip any any any tos a0
# lan 0 ip priority 0 acl 0 express

設定終了
# save
# commit
```

大阪事業所の設定

```
etherポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lanインタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.2/24 3
# lan 0 ip route 0 192.168.1.0/24 192.168.0.1 1
# lan 1 vlan 20
# lan 1 ip address 192.168.2.1/24 3

lan 0から送出するデータ量を1Mbpsに制限する
# lan 0 shaping on 1m

音声データを最優先で透過させる
# acl 0 ip any any any tos a0
# lan 0 ip priority 0 acl 0 express

設定終了
# save
# commit
```

2.21.2 特定のポートで帯域制御（WFQ）機能を使う

ここでは、ether ポートから送出する音声データを最優先で透過させる場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet 側への送信データを、最大 5Mbps に制限する
- 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コマンド例を示します。

● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

ether 1 1 から送出するデータ量を 5Mbps に制限する
# ether 1 1 shaping on 5m

音声データを最優先で透過させる
# acl 0 ip any any any tos a0
# ether 1 1 priority ip 0 acl 0 express

設定終了
# save
# commit
```

2.22 DHCP機能を使う

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 マニュアル「機能説明書」

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。

- IPv6 DHCPサーバ機能
- IPv6 DHCPクライアント機能
- IPv6 DHCPリレーエージェント機能

☛参照 マニュアル「機能説明書」

2.22.1　DHCP サーバ機能を使う

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。

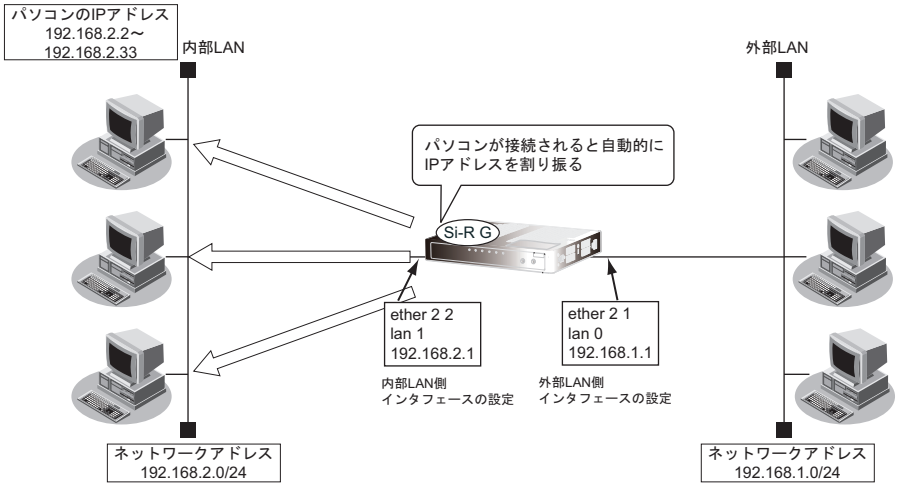
- IP アドレス
- ネットマスク
- リース期間
- デフォルトルータの IP アドレス
- DNS サーバの IP アドレス
- ドメイン名
- NTP サーバの IP アドレス
- TIME サーバの IP アドレス
- WINS サーバの IP アドレス
- SIP サーバのドメイン名または IP アドレス

こんな事に気をつけて

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を説明します。

補足 DHCP サーバ機能で割り当てることのできる IP アドレスの最大数は 253 個です。



● 設定条件

[外部 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

[内部 LAN 側]

- 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
- デフォルトルータの IP アドレス　：192.168.2.1
- リース期間　：1 日
- NTP サーバの IP アドレス　：192.168.2.1
- 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コマンド例を示します。

● コマンド

外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

内部側 LAN インタフェースの設定

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info ntpserver 192.168.2.1
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server
# lan 1 vlan 20

設定終了
# save
# commit
```

2.22.2 DHCPスタティック機能を使う

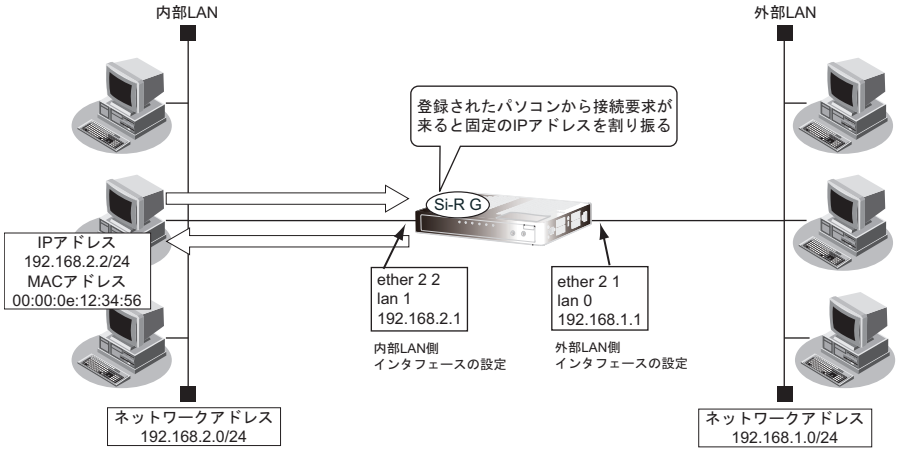
DHCPサーバは、使用していないIPアドレスを一定期間（またはパソコンがIPアドレスを返却するまで）割り当てます。不要になったIPアドレスは自動的に再利用されるため、パソコンのIPアドレスが変わることがあります。本装置では、IPアドレスとMACアドレスを対応付けることによって、登録されたパソコンからDHCP要求が発行されると、常に同じIPアドレスを割り当てることができます。これをDHCPスタティック機能と言います。

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。

補足
- ホストデータベース情報は「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。
- DHCPスタティック機能で設定できるホストの最大数は64個です。



● 設定条件

[外部LAN側]

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

[内部LAN側]

- IPアドレス／ネットマスク　：192.168.2.1/24
- 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
- デフォルトルータのIPアドレス　：192.168.2.1
- リース期間　：1日
- NTPサーバのIPアドレス　：192.168.2.1
- 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

DHCP サーバ機能を使用するコマンドを実行していない場合、DHCP スタティック機能の設定は無効となります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

内部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info ntpserver 192.168.2.1
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server
# lan 1 vlan 20

DHCP スタティック機能を設定する
# host 0 ip address 192.168.2.2
# host 0 mac 00:00:0e:12:34:56

設定終了
# save
# commit
```

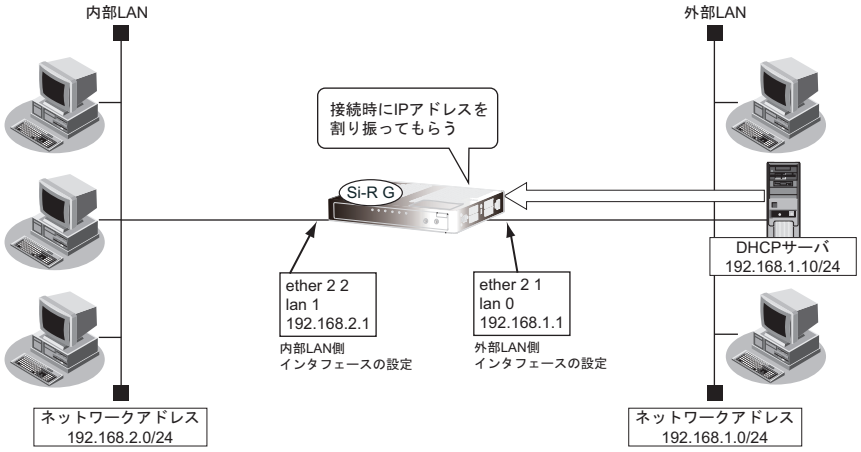
2.22.3　DHCP クライアント機能を使う

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

[外部 LAN 側]

- IP アドレス　：DHCP サーバから取得する

[内部 LAN 側]

- IP アドレス　：192.168.2.1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

DHCP クライアント機能を設定する
# lan 0 ip dhcp service client
# lan 0 vlan 10

マルチ NAT 機能を設定する
# lan 0 ip nat mode multi any 1

設定終了
# save
# commit
```

内部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

lan インタフェースを設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

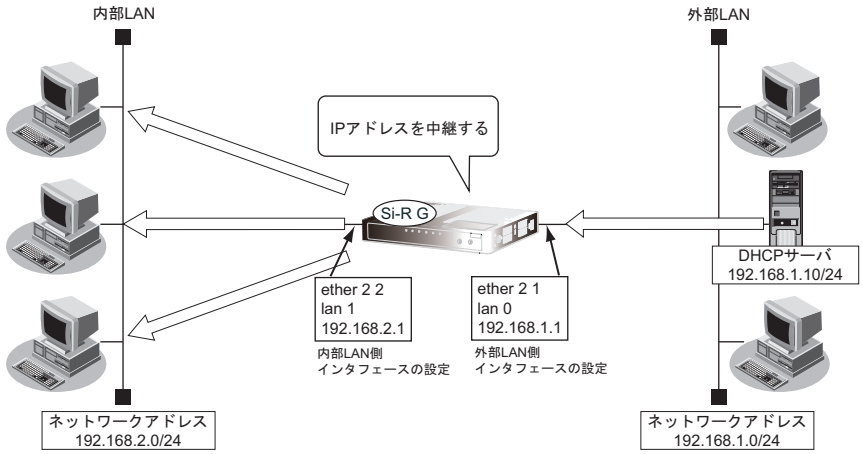
2.22.4　DHCP リレーエージェント機能を使う

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



● 設定条件

[外部 LAN 側]

- IP アドレス　：192.168.1.1
- DHCP サーバ　：192.168.1.10

[内部 LAN 側]

- IP アドレス　：192.168.2.1
- DHCP リレーエージェント機能を使用する

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コマンド例を示します。

● コマンド

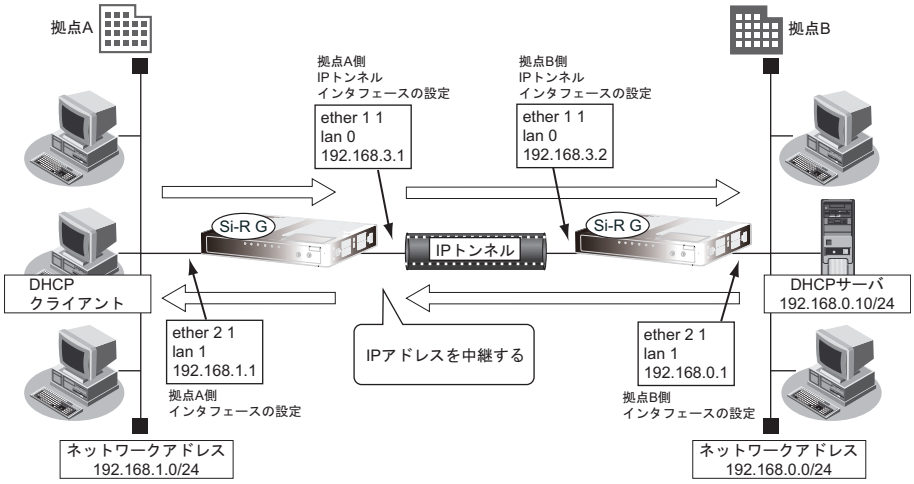
外部 LAN 側インタフェースの設定

```
etherポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lanインタフェースを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

内部 LAN 側インタフェースの設定

```
etherポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

lanインタフェースを設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 20

DHCPリレーエージェント機能を設定する
# lan 1 ip dhcp service relay 192.168.1.10

設定終了
# save
# commit
```

リモート接続の場合



● 設定条件

- DHCP リレーエージェント機能を使用する
- 拠点 A に DHCP クライアントが存在する
- 拠点 B に DHCP サーバが存在する

[拠点 A]

- 装置の IP アドレス　：192.168.1.1
- IP トンネル用インタフェース IP アドレス　：192.168.3.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24

[拠点 B]

- 装置の IP アドレス　：192.168.0.1
- IP トンネル用インタフェース IP アドレス　：192.168.3.2
- ネットワークアドレス／ネットマスク　：192.168.0.0/24
- DHCP サーバの IP アドレス　：192.168.0.10

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

拠点 A 側装置の設定

```
etherポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lanインタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.3.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

接続先の情報を設定する
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 192.168.3.1
# remote 0 ap 0 tunnel remote 192.168.3.2
# remote 0 ip route 0 default 1 1

リレーエージェントを設定する
# lan 1 ip dhcp service relay 192.168.0.10

設定終了
# save
# commit
```

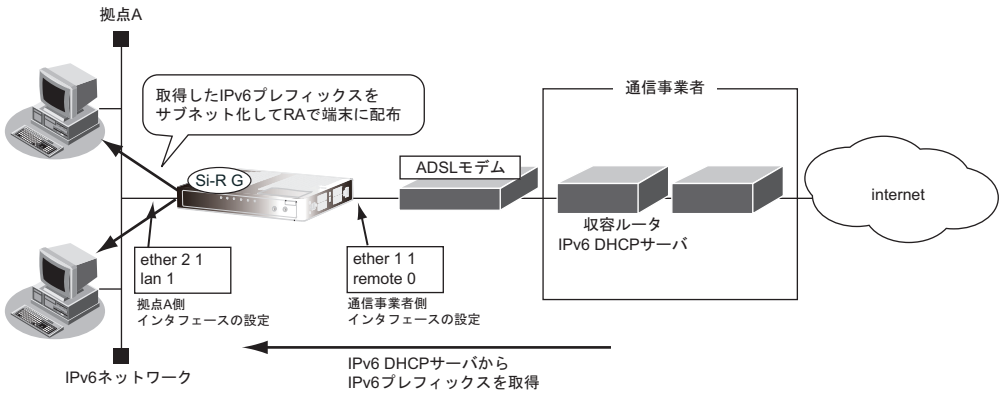
拠点 B 側装置の設定

```
etherポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lanインタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.3.2/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.0.1/24 3

接続先の情報を設定する
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 192.168.3.2
# remote 0 ap 0 tunnel remote 192.168.3.1
# remote 0 ip route 0 default 1 1

設定終了
# save
# commit
```

2.22.5　IPv6 DHCP クライアント機能を使う

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 で使用するポート　：ETHER グループ 1 ポート 1
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- IPv6 DHCP クライアントを有効にするインタフェース　：remote 0
- 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インタフェース　：lan 1
- 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コマンド例を示します。

● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 datalink type physical
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 default 1 1

IPv6 DHCP クライアントを設定する
# remote 0 ipv6 dhcp service client
# remote 0 ipv6 dhcp client option na off
# remote 0 ipv6 dhcp client option pd on

ProxyDNS を設定する
# proxydns domain 0 any * any on 0
# proxydns address 0 any on 0

lan 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@rmt0:1::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 vlan 20

設定終了
# save
# commit
```

2.22.6　IPv6 DHCP サーバ機能を使う

本装置の IPv6 DHCP サーバ機能は、以下の情報を広報することができます。

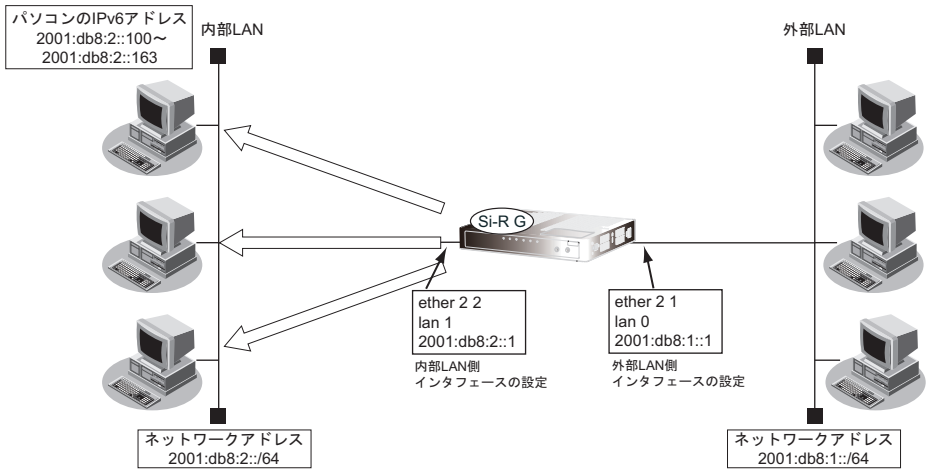
- IPv6 アドレス
- IPv6 プレフィックス
- DNS サーバの IPv6 アドレス
- DNS ドメイン名
- SIP サーバの IPv6 アドレス
- SIP ドメイン名
- SNTP サーバの IPv6 アドレス

こんな事に気をつけて

本装置の IPv6 DHCP サーバ機能は、IPv6 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、IPv6 DHCP サーバ機能を使用する場合の設定方法を説明します。

補足 IPv6 DHCP サーバ機能で割り当てることのできる IP アドレスの最大数は 300 個です。



● 設定条件

[外部 LAN 側]

- 本装置の IP アドレス　：2001:db8:1::1
- ネットワークアドレス／プレフィックス長　：2001:db8:1::/64

[内部 LAN 側]

- 本装置の IP アドレス　：2001:db8:2::1
- パソコンに割り当てる IPv6 アドレス　：2001:db8:2::100～2001:db8:2::163
- パソコンに割り当て可能 IPv6 アドレス数　：100
- ネットワークアドレス／プレフィックス長　：2001:db8:2::/64
- Valid Lifetime　：30 日
- Preferred Lifetime　：7 日
- DNS サーバの IPv6 アドレス　：2001:db8:2::1
- SNTP サーバの IPv6 アドレス　：2001:db8:2::1
- IPv6 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コマンド例を示します。

● コマンド

外部 LAN 側インタフェースの設定

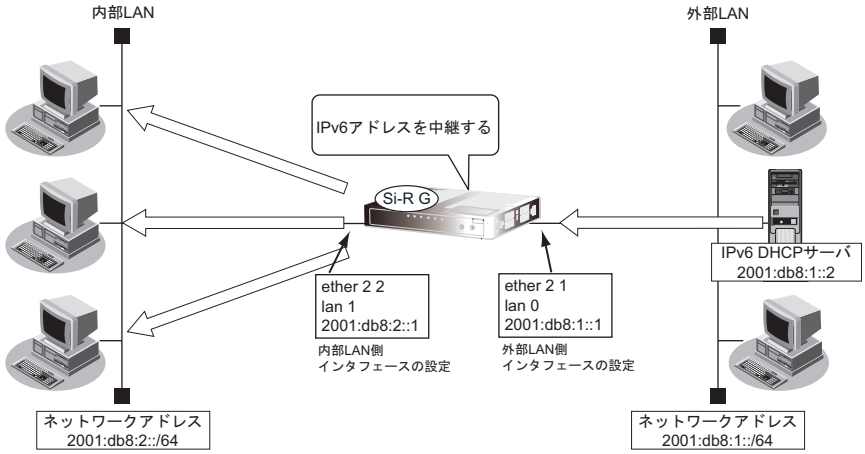
```
etherポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lanインタフェースを設定する
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1::1/64
# lan 0 vlan 10

設定終了
# save
# commit
```

内部 LAN 側インタフェースの設定

```
etherポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

IPv6 DHCPサーバの動作するインタフェースを設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:2::1/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 2001:db8:2::/64 infinity infinity c0
# lan 1 vlan 20

IPv6 DHCPサーバ機能を設定する
# lan 1 ipv6 dhcp service server
# lan 1 ipv6 dhcp server info address 2001:db8:2::100 100 30d 7d
# lan 1 ipv6 dhcp server info dns 2001:db8:2::1
# lan 1 ipv6 dhcp server info sntpserver 2001:db8:2::1

設定終了
# save
# commit
```

2.22.7　IPv6 DHCP リレーエージェント機能を使う

ここでは、IPv6 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。



● 設定条件

[外部 LAN 側]

- 本装置の IPv6 アドレス　：2001:db8:1::1
- IPv6 DHCP サーバアドレス　：2001:db8:1::2

[内部 LAN 側]

- 本装置の IPv6 アドレス　：2001:db8:2::1
- IPv6 DHCP リレーエージェント機能を使用する

こんな事に気をつけて

IPv6 DHCP リレーエージェント機能を使用するインタフェースには、ユニークローカルユニキャストアドレスのプレフィックス「fc00::/7」、またはグローバルユニキャストアドレスのプレフィックス「2000::/3」を持つ IPv6 アドレスが設定されている必要があります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1::1/64
# lan 0 vlan 10

設定終了
# save
# commit
```

内部 LAN インタフェースの設定

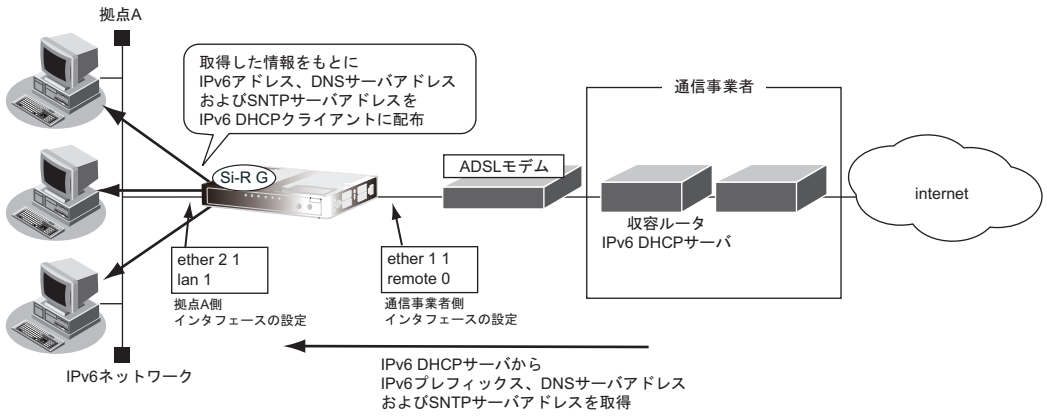
```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

lan インタフェースを設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:2::1/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 2001:db8:2::/64 infinity infinity c0
# lan 1 vlan 20

IPv6 DHCP リレーエージェント機能を設定する
# lan 1 ipv6 dhcp service relay
# lan 1 ipv6 dhcp relay interface lan0

設定終了
# save
# commit
```

2.22.8 IPv6 DHCP クライアント機能で取得した情報を IPv6 DHCP サーバ機能で配布する

ここでは、IPv6 DHCP クライアント機能と IPv6 DHCP サーバ機能を併用し、クライアントが取得した情報をサーバが配布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

クライアントが取得した情報のうち、IPv6 プレフィックス、DNS サーバアドレス以外の取得情報を自装置で使うことはできません。



● 設定条件

- PPPoE で使用するポート　：ETHER グループ 1 ポート 1
- 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 アドレスを配布する lan ポート　：lan 1 ポート
- パソコンに割り当てる IPv6 アドレスのサブネット ID　：0001
- パソコンに割り当てる IPv6 アドレスのインタフェース ID　：::100 ～ ::163
- パソコンに割り当て可能 IPv6 アドレス数　：100
- パソコンに配布する DNS サーバの IPv6 アドレス　：IPv6 DHCP クライアントが取得した DNS サーバアドレス
- パソコンに配布する SNTP サーバの IPv6 アドレス　：IPv6 DHCP クライアントが取得した SNTP サーバアドレス

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 default 1 1

IPv6 DHCP クライアントを設定する
# remote 0 ipv6 dhcp service client
# remote 0 ipv6 dhcp client option na off
# remote 0 ipv6 dhcp client option pd on

LAN 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@rmt0:1::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 vlan 20

IPv6 DHCP サーバを設定する
# lan 1 ipv6 dhcp service server
# lan 1 ipv6 dhcp server info address dhcp@rmt0:1::100 100 30d 7d
# lan 1 ipv6 dhcp server info dns dhcp@rmt0
# lan 1 ipv6 dhcp server info sntpserver dhcp@rmt0

設定終了
# save
# commit
```

2.22.9 通信事業者からの RA 情報と連携して IPv6 DHCP クライアント機能を使用する

通信事業者の収容ルータが広報する RA（Router Advertisement）と連携して、IPv6 DHCP クライアント機能を使用することができます。

受信した RA と連携できる IPv6 DHCP クライアントの機能は以下のとおりです。

- IPv6 DHCP サーバへの問い合わせ
  M または O フラグが設定された RA を受信した場合に、問い合わせを開始することができます。
- IPv6 アドレスの要求
  M フラグが設定された RA を受信した場合に、IPv6 DHCP サーバに IPv6 アドレスを要求することができます。
- IPv6 プレフィックスの要求
  M フラグが設定された RA を受信した場合に、IPv6 DHCP サーバに IPv6 プレフィックスを要求することができます。
- IPv6 アドレス、IPv6 プレフィックス以外の要求
  O フラグだけが設定された RA を受信した場合に、IPv6 アドレス、IPv6 プレフィックス以外の IPv6 DHCP サーバアドレスといったパラメタ情報だけを要求します。
  M フラグが設定された RA を受信した場合は、O フラグの設定に関係なく、IPv6 アドレス、IPv6 プレフィックスに加え、DNS サーバアドレスなどのパラメタ情報の要求を行います。

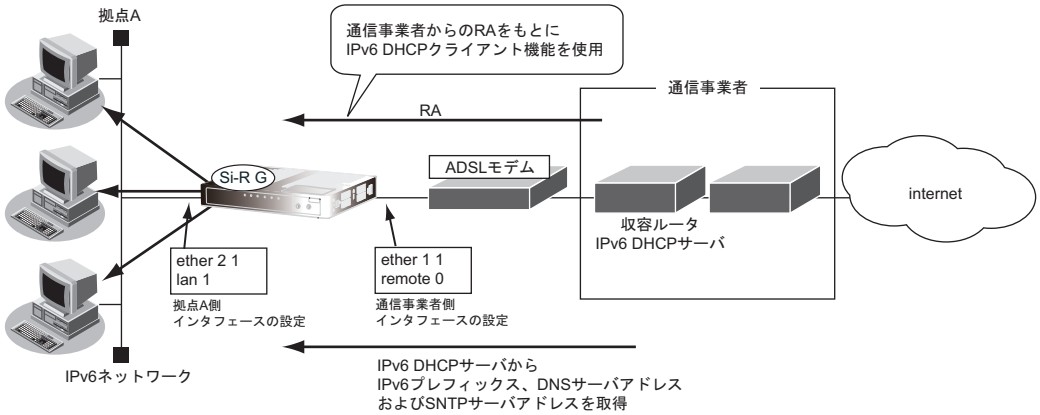
RA をもとに IPv6 DHCP クライアントが取得した情報は、以下の場合無効となります。

- RA のルータ有効期限（Router Lifetime）がタイムアウトした場合
- M および O フラグが設定されていない RA を受信した場合

こんな事に気をつけて

複数の通信事業者から RA を受信し、それぞれの RA で M フラグ、O フラグの設定が異なっている場合は、すべての RA のフラグの論理和の結果で判断します。たとえば、M フラグを設定する収容ルータが 1 台だけであっても、IPv6 DHCP クライアントは、M フラグが設定されている場合の動作となります。

ここでは、受信した RA をもとに IPv6 DHCP クライアント機能で通信事業者から情報を取得し、取得した情報を IPv6 DHCP サーバ機能で配布する方法について説明します。



● 設定条件

- PPPoE で使用するポート　：ETHER グループ 1 ポート 1
- ユーザ認証 ID　：userid
- ユーザ認証パスワード　：userpass
- 通信事業者からの RA　：受信
- IPv6 DHCP サーバへの問い合わせ　：M または O フラグが指定された RA を受信した場合に問い合わせを開始
- IPv6 DHCP サーバへの IPv6 アドレスの要求　：M フラグが指定された RA を受信した場合に要求
- IPv6 DHCP サーバへの IPv6 プレフィックスの要求　：M フラグが指定された RA を受信した場合に要求
- 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 アドレスを配布する lan ポート　：lan 1 ポート
- パソコンに割り当てる IPv6 アドレスのサブネット ID　：0001
- パソコンに割り当てる IPv6 アドレスのインタフェース ID　：::100 ～ ::163
- パソコンに割り当て可能 IPv6 アドレス数　：100
- パソコンに配布する DNS サーバの IPv6 アドレス　：IPv6 DHCP クライアントが取得した DNS サーバアドレス
- パソコンに配布する SNTP サーバの IPv6 アドレス　：IPv6 DHCP クライアントが取得した SNTP サーバアドレス

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ETHER ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ipv6 use on
# remote 0 ipv6 ra mode recv
# remote 0 ipv6 route 0 default 1 1

IPv6 DHCP クライアントを設定する
# remote 0 ipv6 dhcp service client auto
# remote 0 ipv6 dhcp client option na on
# remote 0 ipv6 dhcp client option pd on

LAN 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@rmt0:1::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 dhcp@rmt0:1::/64 infinity infinity
```

```
# lan 1 vlan 20

IPv6 DHCPサーバを設定する
# lan 1 ipv6 dhcp service server
# lan 1 ipv6 dhcp server info address dhcp@rmt0:1::100 100 30d 7d
# lan 1 ipv6 dhcp server info dns dhcp@rmt0
# lan 1 ipv6 dhcp server info sntpserver dhcp@rmt0

設定終了
# save
# commit
```

2.23 DNS サーバ機能を使う（ProxyDNS）

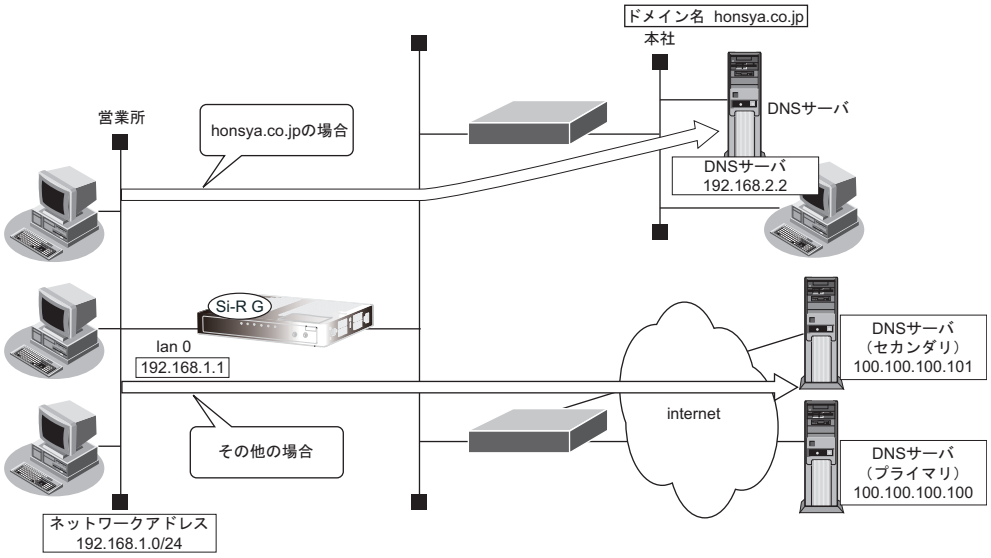
本装置の ProxyDNS には、以下の機能があります。

- 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 マニュアル「機能説明書」

2.23.1 DNS サーバの自動切り替え機能（順引き）を使う

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、100.100.100.101

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（順引き）を設定する
# proxydns domain 0 any *.honsya.co.jp any static 192.168.2.2
# proxydns domain 1 any * any static 100.100.100.100 100.100.100.101

設定終了
# save
# commit
```

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。

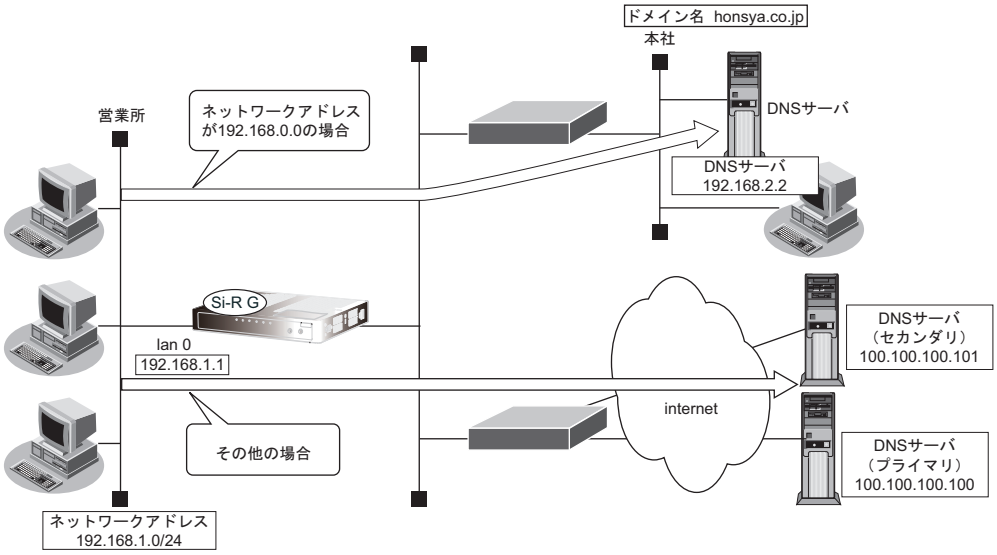
こんな事に気をつけて

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

2.23.2　DNS サーバの自動切り替え機能（逆引き）を使う

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、100.100.100.101

こんな事に気をつけて

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
DNS サーバ自動切り替え機能（逆引き）を設定する
# proxydns address 0 192.168.0.0/24 static 192.168.2.2
# proxydns address 1 any static 100.100.100.100 100.100.100.101

設定終了
# save
# commit
```

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。

2.23.3　DNS サーバアドレスの自動取得機能を使う

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 PPP IPCP（RFC1877）、DHCP（RFC2131）、IPv6 DHCP（RFC3361）のどれかによる DNS サーバアドレスの配布機能に対応している場合に利用できます。

● 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

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any on 0 off

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows 10の場合を例に説明します。

1. ［Windowsロゴ］ボタン、［Windowsシステムツール］、［コントロールパネル］の順にクリックします。
2. ［ネットワークとインターネット］をクリックします。
3. ［ネットワークと共有センター］をクリックします。
4. ［アダプターの設定の変更］をクリックします。
5. ［イーサネット］アイコンを右クリックし、［プロパティ］ボタンをクリックします。
   ［イーサネットのプロパティ］ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。
7. ［プロパティ］ボタンをクリックします。
   ［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。
8. 「次のDNSサーバーのアドレスを使う」を選択します。
9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
10. ［OK］ボタンをクリックします。
    ［イーサネットのプロパティ］ダイアログボックスに戻ります。
11. ［閉じる］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。

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？

以下のコマンドを設定することにより、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。

```
# proxydns domain 0 any * any on 0 on
```

◆「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。ただし、TCPによる問い合わせ時は「接続先のDNSサーバへ問い合わせる」と同様に経路情報に従います。

2.23.4　DNS サーバアドレスを DHCP サーバから取得して使う

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

コマンド入力時は、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　マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any dhcp lan0

設定終了
# save
# commit
```

パソコン側の設定を行う

ここでは、Windows 10の場合を例に説明します。

1. ［Windowsロゴ］ボタン、［Windowsシステムツール］、［コントロールパネル］の順にクリックします。
2. ［ネットワークとインターネット］をクリックします。
3. ［ネットワークと共有センター］をクリックします。
4. ［アダプターの設定の変更］をクリックします。
5. ［イーサネット］アイコンを右クリックし、［プロパティ］ボタンをクリックします。
   ［イーサネットのプロパティ］ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。
7. ［プロパティ］ボタンをクリックします。
   ［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。
8. 「次のDNSサーバーのアドレスを使う」を選択します。
9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
10. ［OK］ボタンをクリックします。
    ［イーサネットのプロパティ］ダイアログボックスに戻ります。
11. ［閉じる］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。

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。

2.23.5　DNS問い合わせタイプフィルタ機能を使う

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、パソコンからの予期しないDNSパケット送信によって、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

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
DNS問い合わせパケット破棄を設定する
# proxydns domain 0 6 * any reject

設定終了
# save
# commit
```

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、「2.23.3 DNSサーバアドレスの自動取得機能を使う」（P.353）の「パソコン側の設定を行う」（P.354）を参照してください。

2.23.6　DNS サーバ機能を使う

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

コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置側を設定する

● コマンド

```
ホストデータベース情報を設定する
# host 0 name host.com
# host 0 ip address 192.168.1.2
# host 0 ipv6 address 2001:db8::2

設定終了
# save
# commit
```

補足 ホストデータベース情報は「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。

パソコン側の設定を行う

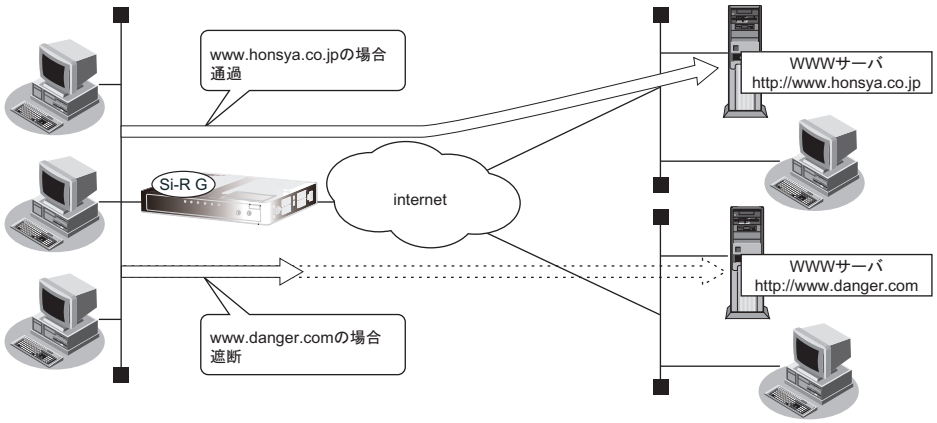
パソコン側の設定を行います。

設定方法は、「2.23.3 DNS サーバアドレスの自動取得機能を使う」(P.353) の「 パソコン側の設定を行う」(P.354) を参照してください。

2.24 特定のURLへのアクセスを禁止する（URLフィルタ機能）

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 マニュアル「機能説明書」

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。
- コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

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コマンド例を示します。

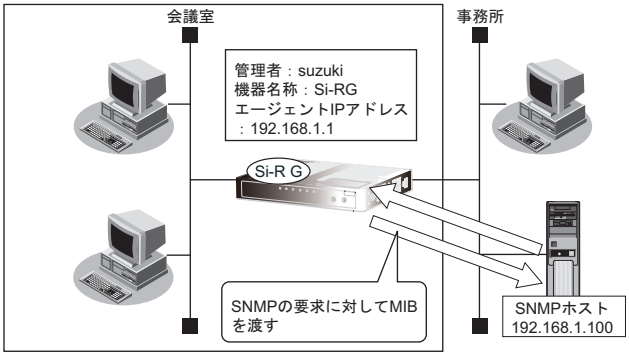
● コマンド

```
URL の情報を設定する
# proxydns domain 0 any www.danger.com any reject
# proxydns domain 1 any * any on 0

設定終了
# save
# commit
```

2.25 SNMP エージェント機能を使う

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、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 マニュアル「機能説明書」

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 マニュアル「仕様一覧」

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。
- 認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMP ホストの設定と同じにしてください。誤ったプロトコルとパスワードを設定した場合は、SNMP ホストとの通信ができなくなります。
- SNMPv3 で認証／暗号プロトコルを使用する場合、snmp 設定反映時の認証／暗号鍵生成に時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。

SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

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。

● 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-RG
- 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

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname Si-RG
# snmp agent location 1F
# snmp agent ip address 192.168.1.1

SNMP ホスト情報を設定する
# snmp manager 0 192.168.1.100 public00 off disable

SNMP エージェント機能を使用する
# snmp service enable

設定終了
# save
# commit
```

SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、以下の情報を設定します。

● 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-RG
- 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
- トラップ通知ホストアドレス　：192.168.1.100
- ユーザ名　：user00
- 認証プロトコル　：MD5
- 認証パスワード　：auth_password
- 暗号プロトコル　：DES
- 暗号パスワード　：priv_password
- MIB ビュー　：MIB 読み出しは system、interfaces グループのみ許可。
  トラップ通知は linkDown、linkUp トラップのみ許可。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

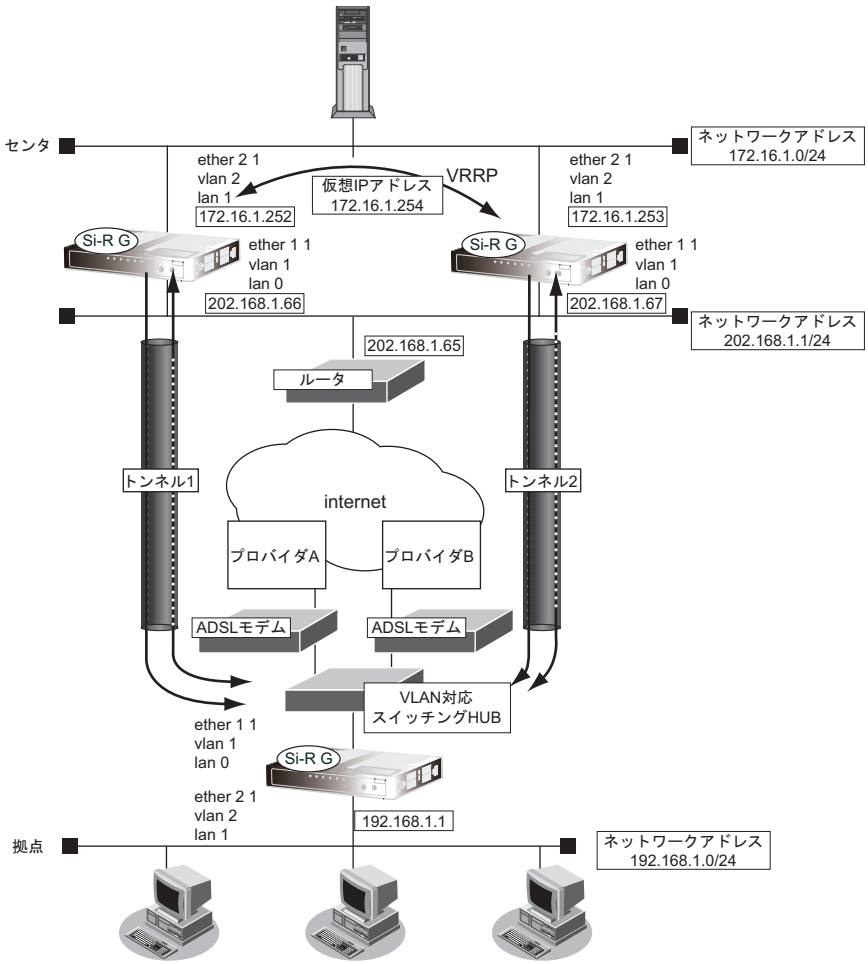
● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname Si-RG
# snmp agent location 1F
# snmp agent ip address 192.168.1.1

SNMPv3 情報を設定する
# snmp user 0 name user00
# snmp user 0 address 0 192.168.1.100
# snmp user 0 notification 0 192.168.1.100

認証・暗号プロトコルを設定する
# snmp user 0 auth md5 auth_password
# snmp user 0 priv des priv_password

MIB ビュー情報を設定する
# snmp user 0 read view 0
# snmp user 0 notify view 0
# snmp view 0 subtree 0 include system
# snmp view 0 subtree 1 include interfaces
# snmp view 0 subtree 2 include linkdown
# snmp view 0 subtree 3 include linkup

SNMP エージェント機能を使用する
# snmp service enable

設定終了
# save
# commit
```

2.26 ECMP機能を使う

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 マニュアル「機能説明書」

● 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コマンド例を示します。

● コマンド

[センタ側本装置（左）]

```
lan 定義を削除する
# delete lan

Ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

lan 0 側を設定する
# lan 0 ip address 202.168.1.66/24 3
# lan 0 ip route 0 default 202.168.1.65 1 1
# lan 0 ip filter 0 pass acl 0 reverse
# lan 0 ip filter 1 pass acl 1 reverse
# lan 0 ip filter default reject
# lan 0 vlan 1

lan 1 側を設定する
# lan 1 ip address 172.16.1.252/24 3
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 172.16.1.254
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
# lan 1 vlan 2

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.66/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.66/32 any 50 any

トンネルを設定する
# remote 0 name RMTbyA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyA
# remote 0 ap 0 ike shared key text 12345678-A
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.252 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

[センタ側本装置（右）]

```
lan定義を削除する
# delete lan

Etherポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

lan 0側を設定する
# lan 0 ip address 202.168.1.67/24 3
# lan 0 ip route 0 default 202.168.1.65 1 1
# lan 0 ip filter 0 pass acl 0 reverse
# lan 0 ip filter 1 pass acl 1 reverse
# lan 0 ip filter default reject
# lan 0 vlan 1

lan 1側を設定する
# lan 1 ip address 172.16.1.253/24 3
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 172.16.1.254
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
# lan 1 vlan 2

IPsecに関するACLを設定する
# acl 0 ip 202.168.1.67/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.67/32 any 50 any

トンネルを設定する
# remote 0 name RMTbyB
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyB
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.67
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyB
# remote 0 ap 0 ike shared key text 12345678-B
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.253 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

[拠点側本装置]

```
lan 定義を削除する
# delete lan

PPPoE で利用する Ether ポート LAN を設定する
# ether 1 1 use on
# ether 1 1 vlan tag 10,20

lan で使用する Ether ポートとアドレスを設定する
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 2

IPsec に関する ACL を設定する
# acl 0 ip any 202.168.1.66/32 17 any
# acl 0 udp 500 500
# acl 1 ip any 202.168.1.66/32 50 any
# acl 2 ip any 202.168.1.67/32 17 any
# acl 2 udp 500 500
# acl 3 ip any 202.168.1.67/32 50 any

プロバイダ A を利用する PPPoE 接続を設定する
# remote 0 name INTER-A
# remote 0 ip route 0 202.168.1.66/32 1 1
# remote 0 ip filter 0 pass acl 0 reverse
# remote 0 ip filter 1 pass acl 1 reverse
# remote 0 ip filter default reject
# remote 0 ip msschange 1414
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-A
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 ppp auth send UIDtoA PASStoA
# remote 0 ap 0 keep connect
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

プロバイダ B を利用する PPPoE 接続を設定する
# remote 1 name INTER-B
# remote 1 ip route 0 202.168.1.67/32 1 1
# remote 1 ip filter 0 pass acl 2 reverse
# remote 1 ip filter 1 pass acl 3 reverse
# remote 1 ip filter default reject
# remote 1 ip msschange 1414
# remote 1 mtu 1454
# remote 1 ap 0 name ISP-B
# remote 1 ap 0 datalink bind vlan 20
# remote 1 ap 0 ppp auth send UIDtoB PASStoB
# remote 1 ap 0 keep connect
# remote 1 ip nat mode multi any 1 5m
# remote 1 ip nat static 0 192.168.1.1 500 any 500 17
# remote 1 ip nat static 1 192.168.1.1 any any any 50
```

センタ側本装置（左）とのトンネルを設定する
remote 2 name CENTER-A
remote 2 ip route 0 172.16.1.0/24 1 2
remote 2 ip msschange 1360
remote 2 mtu 1400
remote 2 ap 0 name IPsecbyA
remote 2 ap 0 datalink type ipsec
remote 2 ap 0 tunnel remote 202.168.1.66
remote 2 ap 0 ipsec type ike
remote 2 ap 0 ipsec ike protocol esp
remote 2 ap 0 ipsec ike range any4 any4
remote 2 ap 0 ipsec ike encrypt des-cbc
remote 2 ap 0 ipsec ike auth hmac-md5
remote 2 ap 0 ipsec ike pfs modp768
remote 2 ap 0 ike name local RMTbyA
remote 2 ap 0 ike shared key text 12345678-A
remote 2 ap 0 ike proposal 0 encrypt des-cbc
remote 2 ap 0 sessionwatch address 192.168.1.1 172.16.1.252
remote 2 ap 0 sessionwatch interval 5s 1m 5s

センタ側本装置（右）とのトンネルを設定する
remote 3 name CENTER-B
remote 3 ip route 0 172.16.1.0/24 1 2
remote 3 ip msschange 1360
remote 3 mtu 1400
remote 3 ap 0 name IPsecbyB
remote 3 ap 0 datalink type ipsec
remote 3 ap 0 tunnel remote 202.168.1.67
remote 3 ap 0 ipsec type ike
remote 3 ap 0 ipsec ike protocol esp
remote 3 ap 0 ipsec ike range any4 any4
remote 3 ap 0 ipsec ike encrypt des-cbc
remote 3 ap 0 ipsec ike auth hmac-md5
remote 3 ap 0 ipsec ike pfs modp768
remote 3 ap 0 ike name local RMTbyB
remote 3 ap 0 ike shared key text 12345678-B
remote 3 ap 0 ike proposal 0 encrypt des-cbc
remote 3 ap 0 sessionwatch address 192.168.1.1 172.16.1.253
remote 3 ap 0 sessionwatch interval 5s 1m 5s

ECMP を設定する
routemanage ip ecmp mode hash

設定終了
save
commit

2.27 VRRP機能を使う

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（実際に経路情報を処理する装置）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経路情報の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。

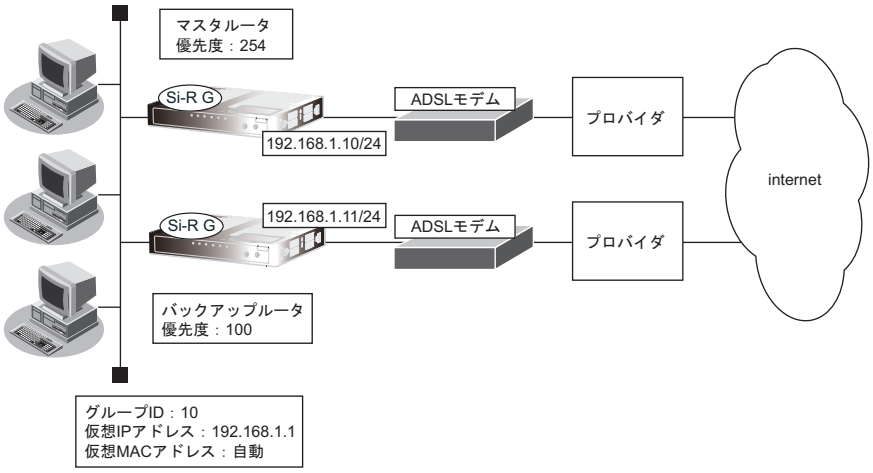
☛参照 マニュアル「機能説明書」

こんな事に気をつけて

- 本装置の電源の投入、マスタルータでの設定反映、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、vrrp preempt-permitコマンド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。
- ルータに設定するIPアドレスと仮想IPアドレスには、異なるIPアドレスを設定することをお勧めします。同じIPアドレスを設定した場合、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ります。同じにした場合、必ず、VRRPグループのVRRPルータの優先度を“master ip|ipv6”に設定してください（VRRPルータの優先度として“master ip|ipv6”を設定した場合、仮想IPアドレスは設定できません）。
- 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。
  IPv4-VRRP
  　あて先IPアドレス　：224.0.0.18
  　プロトコル番号　　：112
  IPv6-VRRP
  　あて先IPアドレス　：ff02::12
  　IPv6 Next Header　：112

2.27.1　簡易ホットスタンバイ機能を使う

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で使用するポート　：ETHERグループ1ポート1
- 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で使用するポート　：ETHERグループ1ポート1
- 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コマンド例を示します。

● コマンド

[マスタルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# ether 1 1 vlan untag 1

# delete lan 0

本装置の IP アドレスを設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 192.168.1.10/24 3
# lan 1 vlan 2

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する（ノードダウントリガを使用する）
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 node 202.168.2.1 any

設定終了
# save

再起動
# reset
```

[バックアップルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# ether 1 1 vlan untag 1

# delete lan 0

本装置の IP アドレスを設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 192.168.1.11/24 3
# lan 1 vlan 2

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 0 preempt on

設定終了
# save

再起動
# reset
```

上の設定例で、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、以下の設定を追加します。

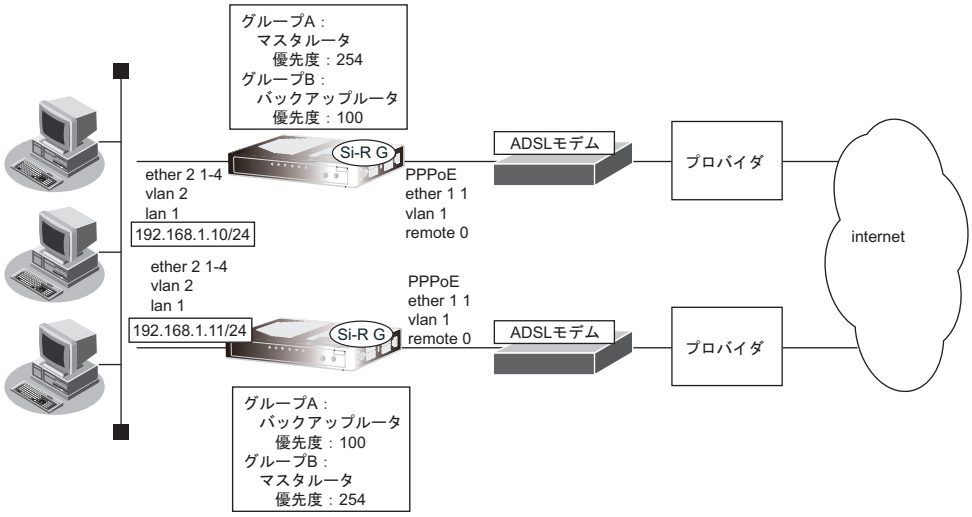
● コマンド

[マスタルータの設定]

```
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
```

2.27.2　クラスタリング機能を使う

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で使用するポート　：ETHERグループ1ポート1
- 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　：ETHERグループ1ポート1
- 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コマンド例を示します。

● コマンド

[マスタルータの設定]

```
ADSL モデムに接続するインタフェースを設定する
# delete lan

# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.10/24 3
# lan 1 vlan 2

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する（インタフェースダウントリガを使用する）
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 ifdown rmt0 254
# lan 1 vrrp group 1 id 11 100 192.168.1.2

設定終了
# save

再起動
# reset
```

[バックアップルータの設定]

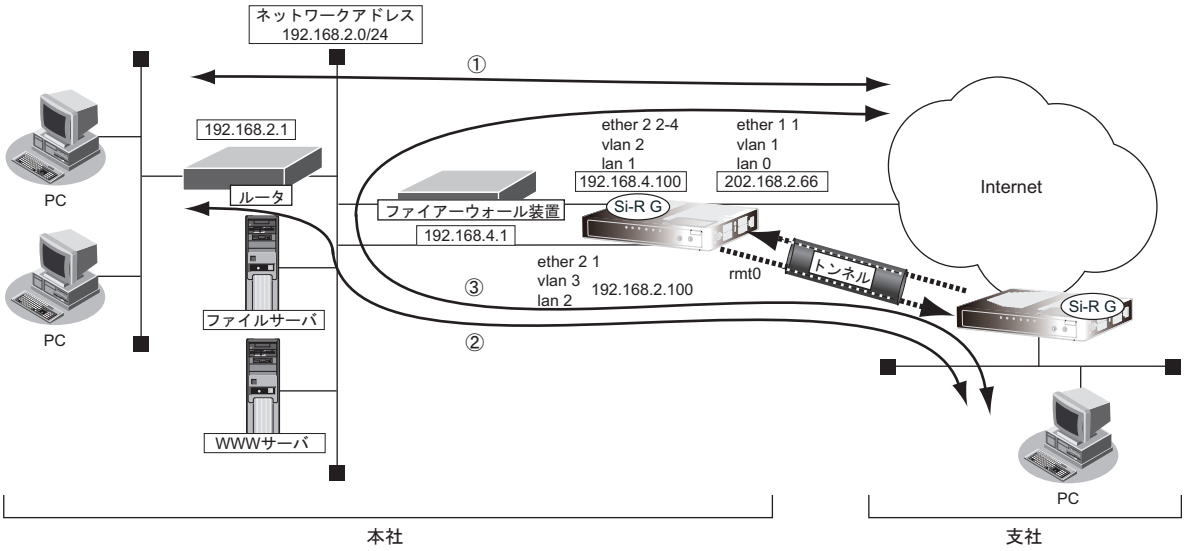
```
ADSL モデムに接続するインタフェースを設定する
# delete lan

# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.11/24 3
# lan 1 vlan 2

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2

VRRP を設定する
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
# lan 1 vrrp group 1 id 11 254 192.168.1.2
# lan 1 vrrp group 1 preempt off
# lan 1 vrrp group 1 trigger 0 ifdown rmt0 254

設定終了
# save

再起動
# reset
```

2.28 ポリシールーティング機能を使う

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。

2.28.1 Ingressポリシールーティング機能を使う

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ー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ー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

- 通信インタフェース
  - 本社の本装置の通信インタフェースが設定済み（ether、vlan、lan）
- 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、本社のファイアー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（ファイアーウォール）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コマンド例を示します。

● コマンド

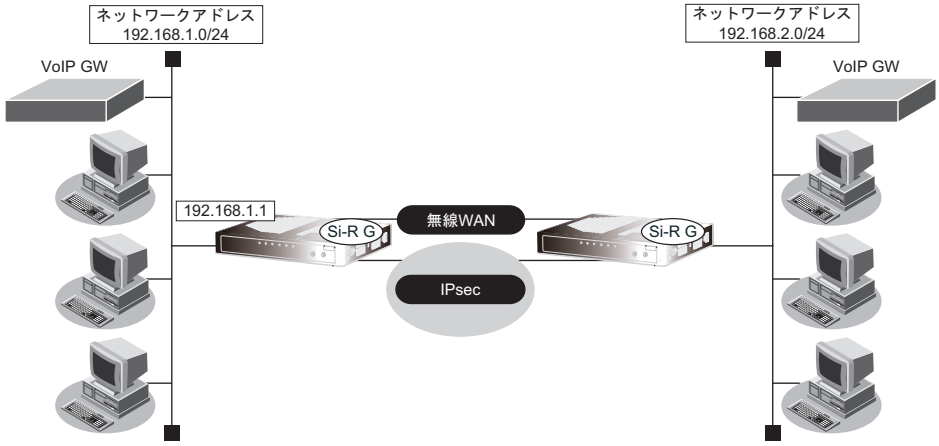
```
本装置あて IPv4 パケットに一致する ACL 定義を設定する
# acl 0 ip any 202.168.2.66/32 any

すべての IPv4 パケットに一致する ACL 定義を設定する
# acl 1 ip any any any

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
# policy-group 0 pattern 0 unmatch acl 0
# policy-group 0 pattern 1 match acl 1
# policy-group 0 interface lan1
# policy-group 0 nexthop 192.168.4.1

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
# policy-group 1 pattern 0 unmatch acl 0
# policy-group 1 pattern 1 match acl 1
# policy-group 1 interface lan2
# policy-group 1 nexthop 192.168.2.1

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
# lan 0 ip in-policy 0 policy-group 0

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
# remote 0 ip in-policy 0 policy-group 1

設定終了
# save
# commit
```

こんな事に気をつけて

Ingress ポリシールーティング機能は、パケット選択ルールに一致した場合、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。

2.28.2　マルチルーティング機能を使う

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 「2.13.1 IPv4 over IPv4で固定IPアドレスでのVPN（手動鍵交換）」（P.157）

- 新規に音声データ用の無線WAN（データ通信モジュール）を追加する
- 通常、音声データ（TOS値：a0）は無線WANを利用する
- 通常、その他のデータはIP-VPNを利用する
- 無線WAN（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、その他のデータも無線WANを使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

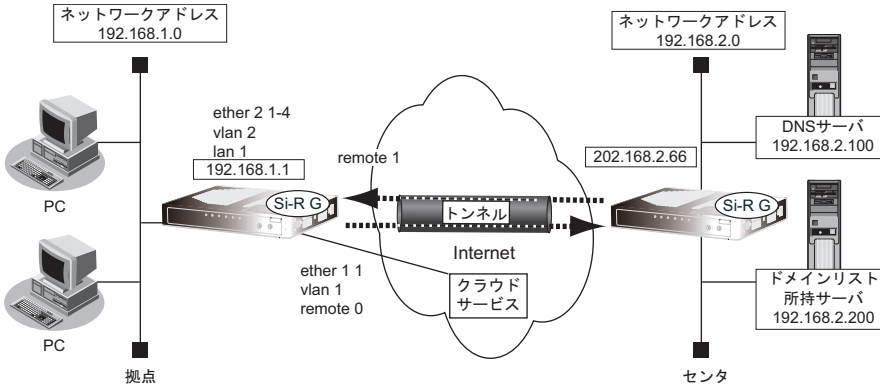
```
無線WAN設定する
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule

通常はIP-VPN を音声データで使用しないように設定する
# remote 0 ap 0 multiroute pattern 0 backup any any any any 0 a0
# remote 0 ap 0 multiroute pattern 1 use any any any any 0 any

無線WANの接続先を設定する
# remote 0 ap 1 name WWAN
# remote 0 ap 1 datalink bind wan 1
# remote 0 ap 1 ppp auth send userid  userpass
# remote 0 ap 1 dial 0 number *99***1#
# remote 0 ppp ipcp vjcomp disable

設定終了
# save
# commit
```

2.29 クラウドサービスゲートウェイ機能を使う

クラウドサービスゲートウェイ機能とは、通常の経路とは異なる経路を利用し、アクセス制御を行う機能です。

アクセス制御はドメイン名によって行います。ドメイン名は、ドメインリストで設定する方法と構成定義に設定する方法があります。

この例では、拠点とセンタ間をインターネットVPNのデフォルト経路として設定し、Windows Updateに関する通信は直接インターネットへむかう設定について説明します。



● 前提条件

PPPoE接続

- 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ポート　：ETHERグループポート1

拠点内ローカルネットワーク

- ローカルネットワークIPアドレス　：192.168.1.0/24

VPN接続

- ネットワーク名　：v-center
- 接続先名　：center
- IPsec/IKE区間　：拠点-202.168.2.66
- IPsec対象範囲　：any4-any4
- 鍵交換タイプ　：Aggressive Mode
- 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拠点ID/IDタイプ　：kyoten（自装置識別情報）/FQDN
- IKE認証鍵　：abcdefghijklmnopqrst
- IKE認証方法　：pre-shared（事前共有鍵方式）
- 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

● コマンド（共通部）

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

拠点内ローカルネットワークを設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

PPPoE接続を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip nat mode multi any 1 5m

VPN接続を設定する
# remote 1 name v-center
# remote 1 ip route 0 default 1 1
# remote 1 ap 0 name center
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt aes-cbc-128
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local kyoten
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrst
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike proposal 0 pfs modp768
```

パソコンの設定を確認する

DNSサーバのアドレスが本装置になっていることを確認してください。

2.29.1　ドメイン名をドメインリストで設定する

ドメイン名をセンタ側からドメインリストとして取得し、経路を制御します。経路制御方法としてProxyDNS機能およびIngressポリシールーティング機能を併用します。

● 設定条件

- ドメインリスト所持サーバのIPアドレス　：192.168.2.200
- ドメインリスト所持サーバのユーザ名　：user
- ドメインリスト所持サーバのパスワード　：password
- ドメインリストのパス名　：/list/domainlist
- ドメインリストで使用するドメインID番号　：0
- 動的IPアドレスを使用するACL定義番号　：0
- 動的IPアドレス保持時間　：1時間
- センタ内のDNSサーバアドレス　：192.168.2.100
- インターネット接続インタフェース　：remote 0
- 拠点内ローカルネットワークインタフェース　：lan 1

ヒント

◆ ドメインID番号とは？

本機能では経路ごとにドメインID番号を定義することができます。
ドメインID番号はドメインリストに記載し、対応したドメインだけが設定されます。

◆ 動的IPアドレスを使用するACLとは？

本機能ではドメインリストのドメインで得られたIPアドレスをACLに動的に反映させます。
使用する定義番号のACLのあて先IPアドレスに"dynamic"を記述し、ProxyDNS機能で設定するACL定義番号と対応させます。"dynamic"指定をしたACLはポリシーグループ設定以外に使用しないでください。

上記の設定条件に従って、クラウドサービスゲートウェイ設定を行う場合のコマンド例を示します。

● コマンド

```
ProxyDNSを設定する
# proxydns domain 0 domainlist 0 acl 0
# proxydns domain 0 any * any on 0 off
# proxydns domain 1 any * any static 192.168.2.100
# proxydns agetime 1h

ACLを設定する
# acl 0 ip any dynamic any

Ingressポリシールーティングを設定する
# policy-group 0 pattern 0 match acl 0
# policy-group 0 interface rmt0
# lan 1 ip in-policy 0 policy-group 0

ドメインリスト情報を設定する
# domainlistinfo 192.168.2.200 user password /list/domainlist

設定終了
# save
# commit
```

こんな事に気をつけて

- ドメインリストは、以下の方法で取得できます。
  - getdomainlist コマンド（domainlistinfo 設定必須）
  - スケジュール機能を使用する
- ドメインリストおよびそのリスト内ドメインの IP アドレスは本装置がリセットするとクリアされます。そのため装置再起動後、ドメインリストのドメインに対して通信ができなくなってしまうことがあります。
- ProxyDNS 機能で domainlist を指定する場合、proxydns domain コマンドで設定する <qname> は無視されます。
- 拠点で使用する端末（OS、インターネットブラウザなど）が設定した保持時間以上 IP アドレスを保持する場合は、通信ができなくなってしまうことがあります。
- ドメインリストの内容が変更された場合、ACL に含まれる動的 IP アドレスは、継続して使用するドメインの IP アドレスを含めてすべてクリアされます。
  ただし、ドメインリストにドメインを追記する場合に限り、それまでの IP アドレスは保持されて継続して通信を行うことができます。
- "dynamic" 指定をした ACL はポリシーグループ設定以外に使用しないでください。
- proxydns domain コマンドの構成定義の変更を反映させると、ドメインリストおよび動的あて先 IP アドレスはクリアされます。

参照 マニュアル「機能説明書」
マニュアル「コマンドユーザーズガイド」

2.29.2　ドメイン名を構成定義に設定する方法

ドメインリストを使用しないで、あらかじめドメイン名を設定しておき、そのドメイン名に対して経路を制御します。

経路制御方法としてはProxyDNS機能を使用します。

● 設定条件

- Windows Updateの際に通信を行うドメイン名

  以下のドメインは2012年4月現在のものです。最新はMicrosoft®のホームページでご確認ください。

  ドメイン1　：windowsupdate.microsoft.com
  ドメイン2　：*.windowsupdate.microsoft.com
  ドメイン3　：*.update.microsoft.com
  ドメイン4　：*.windowsupdate.com
  ドメイン5　：download.windowsupdate.com
  ドメイン6　：download.microsoft.com
  ドメイン7　：*.download.windowsupdate.com
  ドメイン8　：wustat.windows.com
  ドメイン9　：ntservicepack.microsoft.com

  (*は0文字以上複数文字列)
- 経路保持時間　：1時間

上記の設定条件に従って、クラウドサービスゲートウェイ設定を行う場合のコマンド例を示します。

● コマンド

```
ProxyDNSを設定する
# proxydns domain 0 any windowsupdate.microsoft.com any on 0 on
# proxydns domain 1 any *.windowsupdate.microsoft.com  any on 0 on
# proxydns domain 2 any *.update.microsoft.com any on 0 on
# proxydns domain 3 any *.windowsupdate.com any on 0 on
# proxydns domain 4 any download.windowsupdate.com any on 0 on
# proxydns domain 5 any download.microsoft.com any on 0 on
# proxydns domain 6 any *.download.windowsupdate.com any on 0 on
# proxydns domain 7 any wustat.windows.com any on 0 on
# proxydns domain 8 any ntservicepack.microsoft.com any on 0 on
# proxydns domain 9 any * any static 192.168.2.100
# proxydns agetime 1h

設定終了
# save
# commit
```

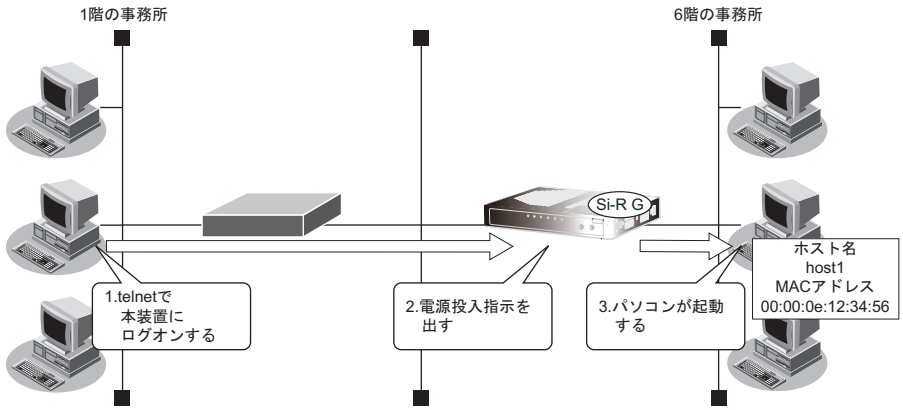
こんな事に気をつけて

- 経路保持時間を設定しない場合、保持時間はDNS回答パケットに含まれるTTL時間になります。
- 拠点で使用する端末（OS、インターネットブラウザなど）が設定した保持時間以上IPアドレスを保持する場合は、通信ができなくなってしまうことがあります。

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）

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、本装置からWakeup on LAN機能を使用して起動させることができます。

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。
- コマンド入力時は、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 マニュアル「コマンドユーザーズガイド」

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

● 設定コマンド

```
ホストデータベースへ登録する
# host 0 name host1
# host 0 mac 00:00:0e:12:34:56

設定終了
# save
# commit
```

2.30.2　リモートパワーオン機能を使う

1. パソコン上のtelnetクライアントから本装置にログインします。

2. 本装置からコマンドによって、Wakeup on LAN機能を使用します。

● コマンド

```
# rpon all
```

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

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20件まで登録できます。
- 電話番号変更予約
  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 マニュアル「コマンドユーザーズガイド」

2.31.1 スケジュールを予約する

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コマンド例を示します。

● コマンド

```
スケジュールを予約する
# schedule 0 in any 2300-0800 diallock

設定終了
# save
# commit
```

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。

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の設定方法を説明します。

● 設定条件

- 動作　：リモートパワーオン
- 予約時刻　：08:00
　：毎日

上記の設定条件に従ってリモートパワーオンを予約する場合のコマンド例を示します。

● コマンド

```
スケジュールを予約する
# schedule 0 at any 0800 rpon all

設定終了
# save
# commit
```

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場合は、あらかじめ対象とするパソコンの情報を本装置のホストデータベース情報に登録しておく必要があります。スケジュール機能を使ってリモートパワーオンを行うと、host rpon コマンドで off が指定されていない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.384）

2.31.2　電話番号変更を予約する

ここでは、2015年10月1日午前2時に電話番号を「*99***1#」から「*99***5#」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　：2015年10月1日　2時00分
- 電話番号変更前情報　：*99***1#
- 電話番号変更後情報　：*99***5#

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コマンド例を示します。

● コマンド

```
電話番号変更を予約する
# dnconvinfo 0 date 1510010200
# dnconvinfo 0 dial 0 *99***1# *99***5#

設定終了
# save
# commit
```

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

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、2015年2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　：2015年2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コマンド例を示します。

● コマンド

```
構成定義を切り替える
# addact 0 1502010630 reset config2

設定終了
# save
# commit
```

2.32 ブリッジグループ機能を使う

ブリッジグループ機能とは、各VLANインタフェースおよび相手接続情報にグループ識別子を設定し、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

- ブリッジグループ学習テーブル生存時間は、mac ageで設定した値がすべてのグループで使用されます。
- 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VLAN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VLAN IDがもっとも小さいVLANインタフェースに関連付けられたlanインタフェースでだけ以下の機能を利用できます。
  - FTP（ソフトウェア更新など）
  - telnet
  - 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。
- 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。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ます。
- コマンド入力時は、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。

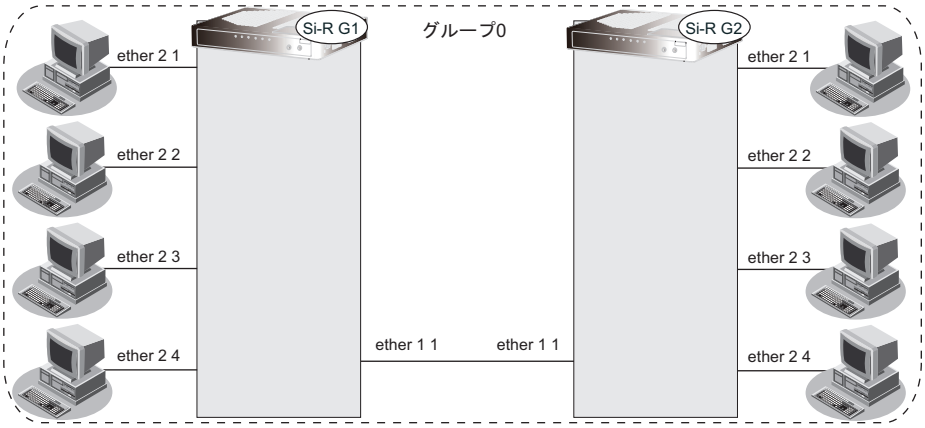
☛参照 マニュアル「コマンドユーザーズガイド」

2.32.1　異なるVLANをグルーピングする

ここでは、ブリッジグループ機能を使用して、異なるVLANを１つのブリッジセグメントとして運用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

- 異なるVLAN同士をグルーピングする場合、ブリッジ転送されると送出フレームには送出先のVLAN識別子が付与されます。
- 異なるVLAN同士をグルーピングする場合、IPセグメントは同一になるように構成する必要があります。



● 前提条件

- ETHERグループ１ポート１とETHERグループ２ポート１～４を同一ブリッジグループ０にする

[グループ0]

- ETHERポート

  ether 1 1　　：VLAN番号=1

  ether 2 1～4　　：VLAN番号=3

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

[本装置1][本装置2]

```
グループ0のETHERポート設定
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 3

VLANの設定
# vlan 1 bridgegroup use on
# vlan 1 bridgegroup group 0
# vlan 3 bridgegroup use on
# vlan 3 bridgegroup group 0

グループ0の設定
# bridgegroup 0 ip routing off
# bridgegroup 0 ipv6 routing off
# bridgegroup 0 ip policy strict
# bridgegroup 0 ipv6 policy strict

設定終了
# save
# commit
```

2.32.2 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）

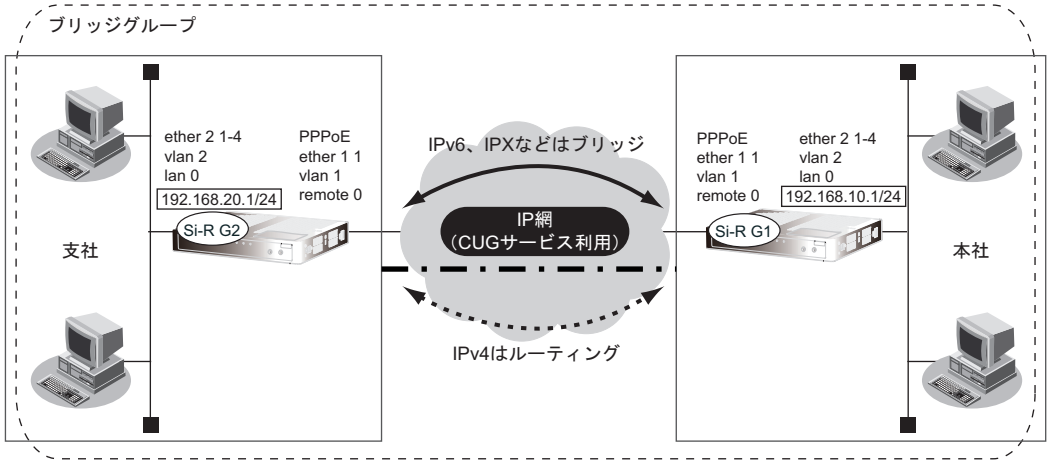
IP トンネル上でブリッジグループ機能を使用することにより、IP 通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

こんな事に気をつけて

- 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 VLAN 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 VLAN ID がもっとも小さい VLAN インタフェースに関連付けられた lan インタフェースでだけ以下の機能を利用できます。
  - FTP（ソフトウェア更新など）
  - telnet
  - 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。
- ブリッジグループ学習テーブル生存時間は、mac age に設定した値がすべてのグループで使用されます。
- 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。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。
- IPsec トンネル内で Ethernet over IP ブリッジ接続を行う際などで、パケットの複数回フラグメントを避けるため、送出先インタフェースの MTU をもとに、Ethernet over IP でカプセル化されたパケットのフラグメントサイズを調整しています。しかし、PPPoE によってインターネット接続されるなどで、PPPoE で利用する相手情報の MTU 値が送出先インタフェースの MTU 値より著しく下回った場合は、複数回フラグメントされる場合があります。

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）］

PPPoE 接続条件

- PPPoE ETHER ポート　：ETHER グループ 1 ポート 1
- PPPoE ETHER ポート VLAN 番号　：1
- PPPoE ユーザ認証 ID　：userid1@groupname
- PPPoE ユーザ認証パスワード　：userpass1
- NAT 機能を使用しない
- 常時接続機能を使用する

社内 LAN 接続条件

- ETHER ポート　：ETHER グループ 2 ポート 1～4
- VLAN 番号　：2
- lan 定義番号　：0
- 払い出される IPv4 アドレス（lan 0 インタフェースに設定）
  ：192.168.10.1/24

［支社（PPPoE 常時接続）］

PPPoE 接続条件

- PPPoE ETHER ポート　：ETHER グループ 1 ポート 1
- PPPoE ETHER ポート VLAN 番号　：1
- PPPoE ユーザ認証 ID　：userid2@groupname
- PPPoE ユーザ認証パスワード　：userpass2
- NAT 機能を使用しない
- 常時接続機能を使用する

社内LAN接続条件

- ETHERポート　：ETHERグループ2ポート1～4
- VLAN番号　：2
- lan定義番号　：0
- 払い出されるIPv4 アドレス（lan 0インタフェースに設定）
  ：192.168.20.1/24

● 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　：VLAN番号1のVLAN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コマンド例を示します。

● コマンド

[本装置1（本社側）]

```
# delete ether 1
# delete ether 2

# delete lan

CUGサービスに接続するPPPoEの接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1

# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0のIP アドレスを設定する
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 2
```

```
IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
# remote 1 ap 0 tunnel remote 192.168.20.1

ブリッジを行うインタフェースを設定する
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# vlan 2 bridgegroup use on
# vlan 2 bridgegroup group 0

ブリッジグループを設定する
# bridgegroup 0 ip routing on
# bridgegroup 0 ipv6 routing off

設定終了
# save
# commit
```

[本装置2（支社側）]

```
# delete ether 1
# delete ether 2

# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1

# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0 の IP アドレスを設定する
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# lan 0 ip address 192.168.20.1/24 3
# lan 0 vlan 2

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1

ブリッジを行うインタフェースを設定する
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# vlan 2 bridgegroup use on
# vlan 2 bridgegroup group 0
```

ブリッジグループを設定する
bridgegroup 0 ip routing on
bridgegroup 0 ipv6 routing off

設定終了
save
commit

2.33 透過モードを使う

透過モードとは、タグ付きVLANフレームおよびタグなしフレームをVLAN設定なしに転送可能とするモードです。

本装置ではVLAN設定を行い、設定に従った転送と、VLAN設定なしに全フレームを透過するモードをサポートします。

2.33.1 ブリッジグループ機能と併用する

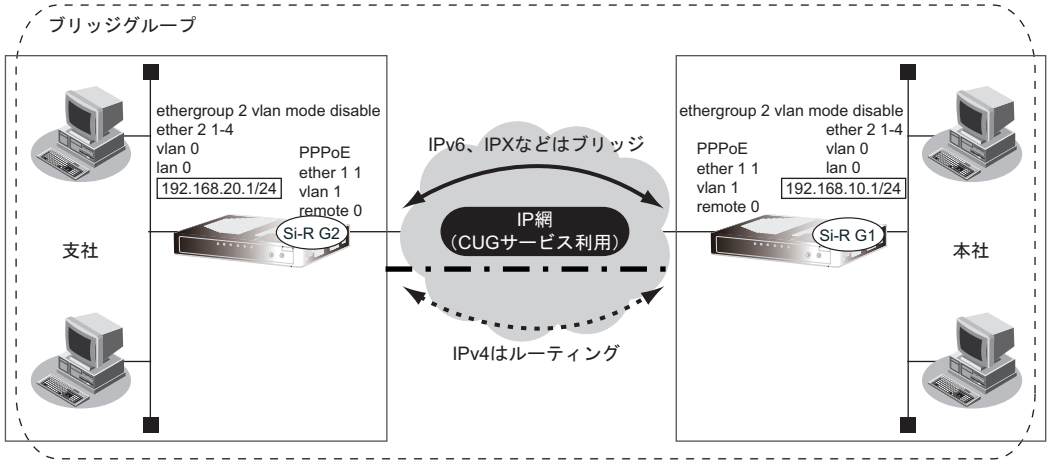
ETHERグループ２を透過モードで使用し、IPトンネル上でブリッジグループ機能を使用することにより、IP通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。また、透過モードを使用することで、ETHERグループ２配下に存在するすべてのVLANを相手拠点に転送することができます。

こんな事に気をつけて

- 透過モード設定時に、ブリッジグループを有効にすると、ETHERグループ２は各ポート単位でのブリッジグループ分けができません。全ポートが１つのブリッジグループにだけ属することができます。
- 透過モードとブリッジグループを併用する場合、VLANタグ透過モードを設定してください。
- 透過モード設定時は、タグなしフレームをlanインタフェースと括り付ける場合、VIDとして”0”を指定してください。
- 透過モード設定時は、ETHERグループ１に設定されていないVIDを、lanインタフェースで指定することができます。その場合、該当lanインタフェースはETHERグループ２の全ポートがリンクダウンまたは未使用状態になるまでup状態となります。
- 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VLAN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VLAN IDがもっとも小さいVLANインタフェースに関連付けられたlanインタフェースでだけ以下の機能を利用できます。
  - FTP（ソフトウェア更新など）
  - telnet
  - 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。
- ブリッジグループ学習テーブル生存時間は、mac ageに設定した値が、すべてのグループで使用されます。
- 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。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。
- Ethernet over IPと透過モードを併用する場合、タグ透過モード（bridgegroup vlan tag transmit on）を必ず設定してください。

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）］

PPPoE接続条件

- PPPoE ETHERポート　：ETHERグループ1ポート1
- PPPoE ETHERポートVLAN番号　：1
- PPPoEユーザ認証ID　：userid1@groupname
- PPPoEユーザ認証パスワード　：userpass1
- NAT機能を使用しない
- 常時接続機能を使用する

社内LAN接続条件

- ETHERグループ2　：透過モード
- ETHERポート　：ETHERグループ2ポート1～4
- VLAN番号　：0（タグなしフレーム）
- lan定義番号　：0
- 払い出されるIPv4アドレス（lan 0インタフェースに設定）　：192.168.10.1/24

［支社（PPPoE常時接続）］

PPPoE接続条件

- PPPoE ETHERポート　：ETHERグループ1ポート1
- PPPoE ETHERポートVLAN番号　：1
- PPPoEユーザ認証ID　：userid2@groupname
- PPPoEユーザ認証パスワード　：userpass2
- NAT機能を使用しない
- 常時接続機能を使用する

社内LAN接続条件

- ETHERグループ2　：透過モード
- ETHERポート　：ETHERグループ2ポート1～4
- VLAN番号　：0（タグなしフレーム）
- lan定義番号　：0
- 払い出されるIPv4アドレス（lan 0インタフェースに設定）　：192.168.20.1/24

● 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　：VLAN番号1のVLAN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コマンド例を示します。

● コマンド

[本装置1（本社側）]

```
# ether 1 1 use off
# ether 2 1-4 use off
# delete lan

CUGサービスに接続するPPPoEの接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0のIPアドレスを設定する
# ethergroup 2 vlan mode disable
# ether 2 1-4 use on
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 0

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
```

```
# remote 1 ap 0 tunnel remote 192.168.20.1

ブリッジを行うインタフェースを設定する
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# ethergroup 2 bridgegroup use on
# ethergroup 2 bridgegroup group 0

ブリッジグループを設定する
# bridgegroup 0 ip routing on
# bridgegroup 0 ipv6 routing off
# bridgegroup 0 vlan tag transmit on

設定終了
# save
# reset
```

[本装置2（支社側）]

```
# ether 1 1 use off
# ether 2 1-4 use off
# delete lan

CUGサービスに接続するPPPoE の接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0 のIP アドレスを設定する
# ethergroup 2 vlan mode disable
# ether 2 1-4 use on
# lan 0 ip address 192.168.20.1/24 3
# lan 0 vlan 0

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1

ブリッジを行うインタフェースを設定する
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# ethergroup 2 bridgegroup use on
# ethergroup 2 bridgegroup group 0

ブリッジグループを設定する
# bridgegroup 0 ip routing on
# bridgegroup 0 ipv6 routing off
# bridgegroup 0 vlan tag transmit on

設定終了
# save
# reset
```

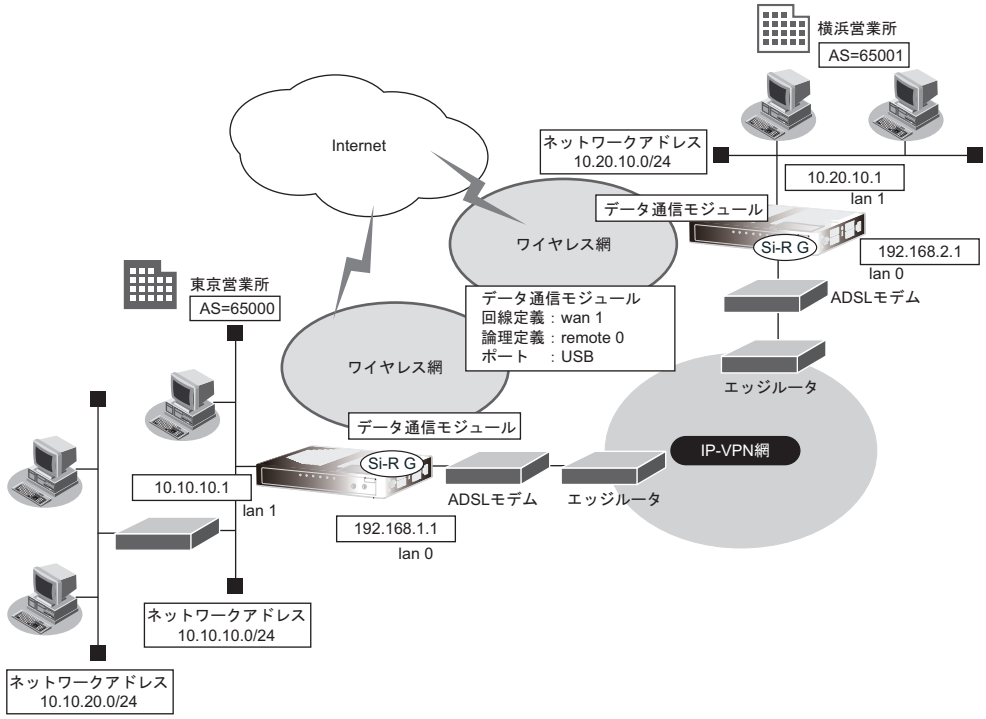
2.34 データ通信モジュールで通信バックアップをする

本装置にデータ通信モジュールを装着することで、ワイヤレス網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ワイヤレス網側で通信バックアップする場合を例に説明します。

参照 対応データ通信モジュール（富士通ホームページ）
http://www.fujitsu.com/jp/products/network/router/sir/sirg100b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg110b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg200b/#supportcard

この例では、BGP 経路に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 側が通信不能になり 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

- データ通信モジュールの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからデータ通信モジュールを装着してください。
- データ通信モジュールは、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。
- データ通信モジュール接続では、常時接続機能は動作しません。
- データ通信モジュールで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信モジュールによる発信は従量課金が発生するため、データ通信モジュール接続のアカウント情報を監視して不要な接続が行われていないか、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、強制切断を行う累計接続時間、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: {[USB]|[USB1]|[USB2]|[SLOT]} forced disconnection <target> <reason>
- データ通信モジュールの通信速度は 64Kbps とみなして動作します。

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 「1.8 複数の事業所LANをIP-VPN網を利用して接続する」（P.29）

● 設定条件

[東京営業所]

- 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
- 認証ID　：userid（通信事業者から提示された内容）
- 認証パスワード　：userpass（通信事業者から提示された内容）
- 電話番号　：*99***1#（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
- 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]

- 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
- 認証ID　：userid（通信事業者から提示された内容）
- 認証パスワード　：userpass（通信事業者から提示された内容）
- 電話番号　：*99***1#（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
- 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コマンド例を示します。

東京営業所のバックアップ回線を設定する

● コマンド

```
回線情報を設定する
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule
# wan 1 description L-03F

接続先の情報を設定する
# remote 0 description internet
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip route 0 default 1 1
# remote 0 ap 0 description ISP-1
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 dial 0 number *99***1#
# remote 0 ap 0 idle 1m

強制切断を行う累計パケット数を設定する
# remote 0 ap 0 disconnect packet 100000 per128
```

```
VPNを設定する
# remote 1 name tokyo
# remote 1 ip route 0 10.20.10.0/24 1 30
# remote 1 ap 0 name yokohama
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

インターネットからIPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 10.10.10.1 500 any 500 17
# remote 0 ip nat static 1 10.10.10.1 any any any 50

設定終了
# save
# commit
```

横浜営業所のバックアップ回線を設定する

● コマンド

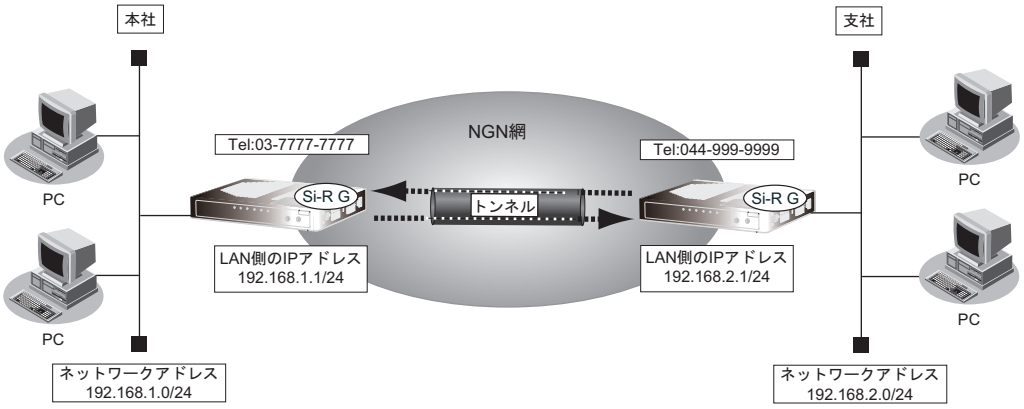
```
回線情報を設定する
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule
# wan 1 description L-03A

接続先の情報を設定する
# remote 0 description internet
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip route 0 default 1 1
# remote 0 ap 0 description ISP-1
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 dial 0 number *99***1#
# remote 0 ap 0 idle 1m

強制切断を行う累計パケット数を設定する
# remote 0 ap 0 disconnect packet 100000 per128

VPNを設定する
# remote 1 name yokohama
# remote 1 ip route 0 10.10.10.0/24 1 30
# remote 1 ap 0 name tokyo
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.1.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
```

```
# remote 1 ap 0 ike proposal encrypt des-cbc

インターネットからIPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 10.20.10.1 500 any 500 17
# remote 0 ip nat static 1 10.20.10.1 any any any 50

設定終了
# save
# commit
```

2.35 データコネクト機能を使う

本装置は、NGN回線（フレッツ光ネクストなど）が提供する帯域確保型データ通信サービス「データコネクト」に対応しています。

以下にデータコネクトを利用して接続する場合の設定方法を説明します。



● 前提条件

[本社（プライベートLAN側）]

- ETHERグループ２ポート１～４を使用する
- 使用するVLAN ID　：2
- LAN2インタフェースを使用する
- ローカルネットワークIPv4アドレス　：192.168.1.1/24

[支社（プライベートLAN側）]

- ETHERグループ２ポート１～４を使用する
- 使用するVLAN ID　：2
- LAN2インタフェースを使用する
- ローカルネットワークIPv4アドレス　：192.168.2.1/24

[共通（通信事業者網側）]

- ETHERグループ１ポート１を使用する
- 使用するVLAN ID　：1
- LAN1インタフェースを使用する
- DHCPクライアント機能を使用する
- DHCPv6クライアント機能を使用する
- IPv6デフォルトルート　：DHCPで取得

こんな事に気をつけて

- データコネクト機能を使用する場合、DHCPクライアント機能の設定をIPv4とIPv6両方で有効にしてください。
- データコネクトは従量課金制であるため、長時間通信を行うと超過課金の原因となります。ご使用する際は、通信料金に十分ご注意ください。
- データコネクトは、利用する帯域により通信料金が異なりますので、ご注意ください。
- データコネクト機能を使用する場合は、NATトラバーサル機能を使用する必要があります。
- 動的VPN機能と併用することはできません。

● 設定コマンド

[本社]

```
Etherポートを設定する
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

LAN情報を設定する
# delete lan
# lan 1 ip dhcp service client
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@lan1::/64
# lan 1 ipv6 route 0 default dhcp
# lan 1 ipv6 dhcp service client
# lan 1 ipv6 dhcp client option na off
# lan 1 ipv6 dhcp client option pd on
# lan 1 vlan 1
# lan 2 ip address 192.168.1.1/24 3
# lan 2 vlan 2
```

[支社]

```
Etherポートを設定する
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

LAN情報を設定する
# delete lan
# lan 1 ip dhcp service client
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@lan1::/64
# lan 1 ipv6 route 0 default dhcp
# lan 1 ipv6 dhcp service client
# lan 1 ipv6 dhcp client option na off
# lan 1 ipv6 dhcp client option pd on
# lan 1 vlan 1
# lan 2 ip address 192.168.2.1/24 3
# lan 2 vlan 2
```

● 設定条件

[本社]

- ネットワーク名　：dataconn
- 接続先　：shisya
- 支社電話番号　：044-999-9999
- IKE支社IDタイプ　：TEL-KEY-ID
- IKE支社ID　：044-999-9999
- IKE本社IDタイプ　：TEL-KEY-ID
- IKE本社ID　：03-7777-7777

[支社]

- ネットワーク名　：dataconn
- 接続先　：honsya
- 本社電話番号　：03-7777-7777
- IKE本社IDタイプ　：TEL-KEY-ID
- IKE本社ID　：03-7777-7777
- IKE支社IDタイプ　：TEL-KEY-ID
- IKE支社ID　：044-999-9999

[共通]

- データコネクトを使用する
- 通信速度　：64Kbps
- 無通信監視　：60秒
- IKE Version　：ikev2
- IPsecプロトコル　：esp
- IPsec暗号アルゴリズム　：aes-cbc-256
- IPsec認証アルゴリズム　：hmac-sha256
- IPsec DHグループ　：なし
- IPsecV3 ESN　：なし
- IKE認証鍵　：abcdefghijklmnopqrstuvwxyz1234567890（文字列）
- IKE認証方法　：pre-shared（事前共有鍵方式）
- IKE暗号アルゴリズム　：aes-cbc-256
- IKE認証アルゴリズム　：hmac-sha256
- IKE DHグループ　：modp1024
- IKE PRFアルゴリズム　：hmac-sha256
- IKE 相手装置ID送信　：送信する
- IKE NATトラバーサル　：使用する

本社を設定する

● コマンド

```
データコネクトを設定する
# ngn sip use on
# ngn sip bind lan 1

接続先の情報を設定する
# remote 1 name dataconn
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type dataconnect
# remote 1 ap 0 dial 0 number 0449999999
# remote 1 ap 0 dial 0 speed 64K
# remote 1 ap 0 idle 60s

VPNを設定する
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha256
# remote 1 ap 0 ipsec ike esn disable
# remote 1 ap 0 ike local-idtype tel_key_id
# remote 1 ap 0 ike remote-idtype tel_key_id
# remote 1 ap 0 ike name local 0377777777
# remote 1 ap 0 ike name remote 0449999999
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha256
# remote 1 ap 0 ike proposal 0 pfs modp1024
# remote 1 ap 0 ike proposal 0 prf hmac-sha256
# remote 1 ap 0 ike remote-id-send enable
# remote 1 ap 0 ike nat-traversal use on
```

```
# remote 1 ip route 0 192.168.2.0/24 1 1

網の通信帯域にあわせて送出するデータ量を制限する
# remote 1 shaping on 64k

設定終了
# save
# commit
```

支社を設定する

● コマンド

```
データコネクトを設定する
# ngn sip use on
# ngn sip bind lan 1

接続先の情報を設定する
# remote 1 name dataconn
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type dataconnect
# remote 1 ap 0 dial 0 number 0377777777
# remote 1 ap 0 dial 0 speed 64K
# remote 1 ap 0 idle 60s

VPN を設定する
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha256
# remote 1 ap 0 ipsec ike esn disable
# remote 1 ap 0 ike local-idtype tel_key_id
# remote 1 ap 0 ike remote-idtype tel_key_id
# remote 1 ap 0 ike name local 0449999999
# remote 1 ap 0 ike name remote 0377777777
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha256
# remote 1 ap 0 ike proposal 0 pfs modp1024
# remote 1 ap 0 ike proposal 0 prf hmac-sha256
# remote 1 ap 0 ike remote-id-send enable
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ip route 0 192.168.1.0/24 1 1

網の通信帯域にあわせて送出するデータ量を制限する
# remote 1 shaping on 64k

設定終了
# save
# commit
```

2.36 ISDN（INS-TA）で通信バックアップをする

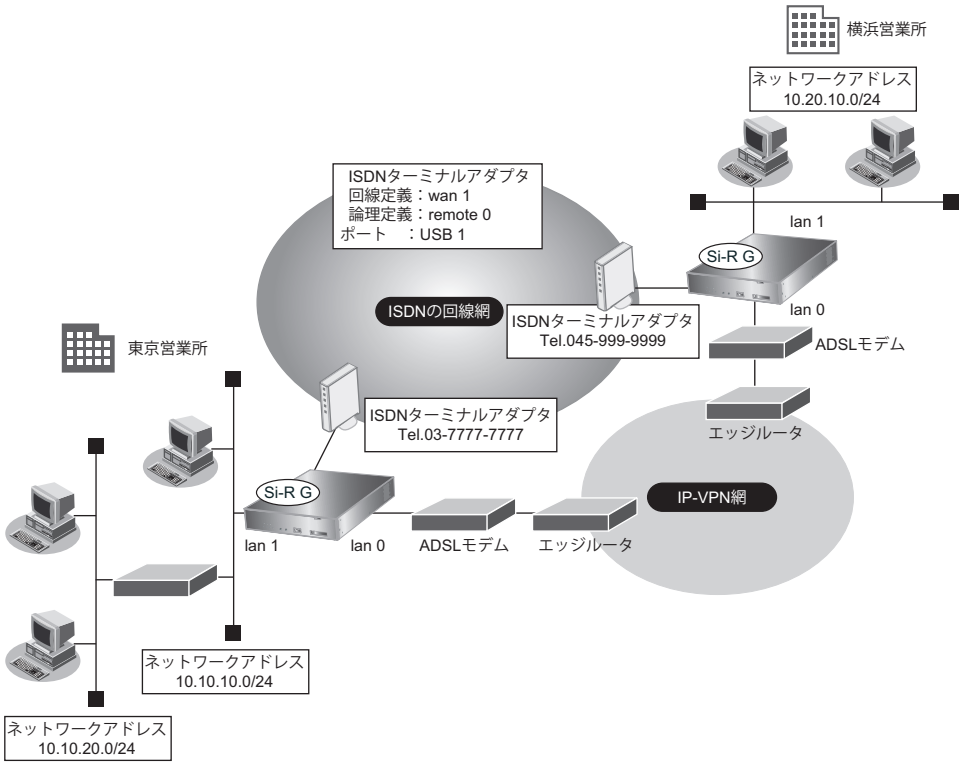
適用機種　***Si-R G200B, Si-R G100B***

本装置にデータ通信モジュールとしてISDNターミナルアダプタを装着することによって、ISDN網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ISDN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　対応データ通信モジュール（富士通ホームページ）
http://www.fujitsu.com/jp/products/network/router/sir/sirg200b/#supportcard
http://www.fujitsu.com/jp/products/network/router/sir/sirg100b/#supportcard

この例では、BGP経路に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

- ISDNターミナルアダプタの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからISDNターミナルアダプタを装着してください。
- データ通信モジュールでは、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。
- ISDNターミナルアダプタ接続では、以下の機能は動作しません。
  - コールバック機能
  - 常時接続機能
- ISDNターミナルアダプタで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- ISDNターミナルアダプタによる発信は従量課金が発生するため、ISDNターミナルアダプタ接続のアカウント情報を監視して不要な接続が行われていないか、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、強制切断を行う累計接続時間、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: {[USB]|[USB1]|[USB2]|[SLOT]} forced disconnection <target> <reason>
- ISDNターミナルアダプタの通信速度は64Kbpsとみなして動作します。

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 「1.8 複数の事業所 LAN を IP-VPN 網を利用して接続する」（P.29）

● 設定条件

- ISDN ターミナルアダプタ　：USB1
- 強制切断　：回線接続時間が 24 時間を超えた場合に回線を切断し、以降自動発信を行わない
- 発信者番号認証を有効にする

[東京営業所]

＜横浜営業所と ISDN ターミナルアダプタで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：yokohama
- 電話番号　：045-999-9999
- 無通信監視　：1 分（60 秒）
- ユーザ認証 ID とユーザ認証パスワード
  発信　：yokohama、yokopass
  着信　：tokyo、tokyopass
- 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 ISDN ターミナルアダプタで接続する条件＞

- ネットワーク名　：backup
- 接続先名　：tokyo
- 電話番号　：03-7777-7777
- 無通信監視　：1 分（60 秒）
- ユーザ認証 ID とユーザ認証パスワード
  発信　：tokyo、tokyopass
  着信　：yokohama、yokopass
- 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コマンド例を示します。
ここでは、Si-R G200B を例に説明します。

東京営業所のバックアップ回線を設定する

● コマンド

```
回線情報を設定する
# wan 1 use on
# wan 1 bind usb 1
# wan 1 line modemmodule
# wan 1 description V30slim

接続先の情報を設定する
# remote 0 name backup
# remote 0 ap 0 name yokohama
# remote 0 ap 0 datalink bind wan 1
```

```
# remote 0 ap 0 dial 0 number 045-999-9999
# remote 0 ap 0 ppp auth send yokohama yokopass
# remote 0 ap 0 ppp auth receive tokyo tokyopass
# remote 0 ap 0 idle 1m

強制切断を行う累計接続時間を設定する
# remote 0 ap 0 disconnect time 1d

BGP経路より優先度の低いスタティックルートを設定する
# remote 0 ip route 0 10.20.0.0/16 1 30

設定終了
# save
# commit
```

横浜営業所のバックアップ回線を設定する

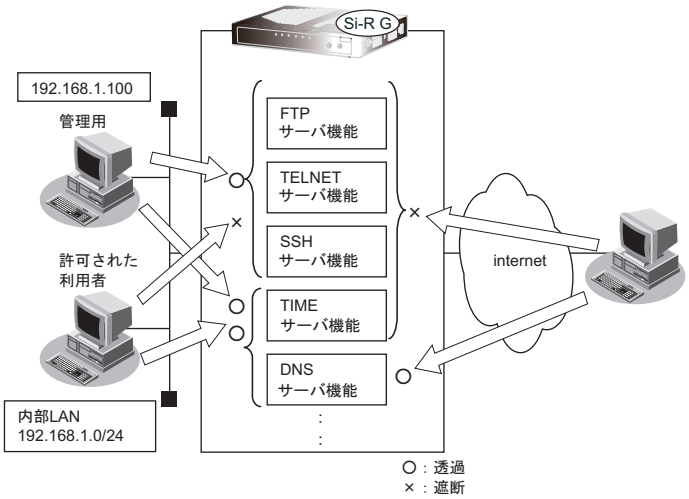
● コマンド

```
回線情報を設定する
# wan 1 use on
# wan 1 bind usb 1
# wan 1 line modemmodule
# wan 1 description V30slim

接続先の情報を設定する
# remote 0 name backup
# remote 0 ap 0 name tokyo
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 dial 0 number 03-7777-7777
# remote 0 ap 0 ppp auth send tokyo tokyopass
# remote 0 ap 0 ppp auth receive yokohama yokopass
# remote 0 ap 0 idle 1m

強制切断を行う累計接続時間を設定する
# remote 0 ap 0 disconnect time 1d

BGP経路より優先度の低いスタティックルートを設定する
# remote 0 ip route 0 10.10.0.0/16 1 30

設定終了
# save
# commit
```

2.37 アプリケーションフィルタ機能を使う

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。

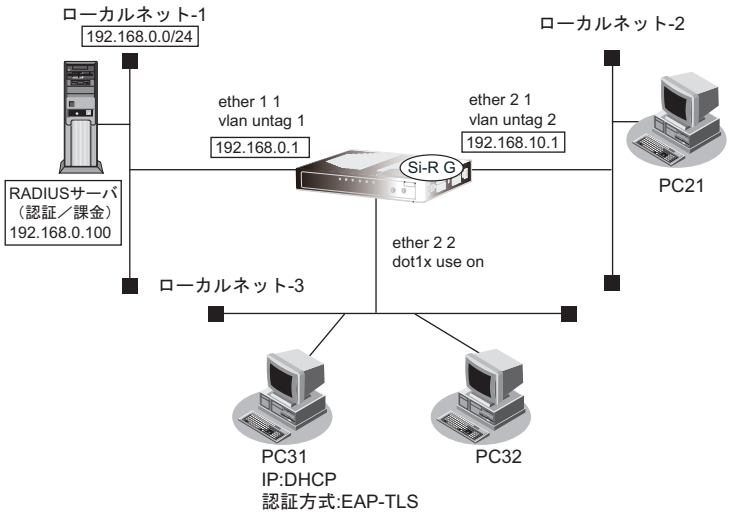
上記の設定条件に従ってアプリケーションフィルタを設定する場合のコマンド例を示します。

● コマンド

```
制限するサーバ機能に対し、デフォルトのアクセスを遮断する
# serverinfo ftp filter default reject
# serverinfo telnet filter default reject
# serverinfo ssh filter default reject
# serverinfo time filter default reject

管理用のホストからのFTP/TELNET/SSHサーバ機能へのアクセスを許可する
# acl 0 ip 192.168.1.100/32 any any any
# serverinfo ftp filter 0 accept acl 0
# serverinfo telnet filter 0 accept acl 0
# serverinfo ssh filter 0 accept acl 0

内部LANのホストからのTIMEサーバ機能へのアクセスを許可する
# acl 1 ip 192.168.1.0/24 any any any
# serverinfo time filter 0 accept acl 1

設定終了
# save
# commit
```

2.38 IEEE802.1X認証機能を使う

ここでは、etherポートで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

- 認証端末に割り当てるVLAN IDは、本装置のほかのetherポートまたは認証VLAN用予約VLANに設定されている必要があります。
- 本認証使用時は、etherポートの種別を通常ポート（ether type normal）設定にしてください。
- IEEE802.1X認証を使用するETHERポートでSTPを有効にした場合、ブロッキングからフォワーディングに復帰しても、再認証間隔の設定時間の間は通信が回復しないことがあります。
- MACアドレス認証と併用時に認証状態初期化操作を行う場合は、dot1xctl initialize port etherを実施してください。

● 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etherポート　：ether 1 1
- 利用するlanインタフェース　：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etherポート　：ether 2 2
- 利用するlanインタフェース　：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

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コマンド例を示します。

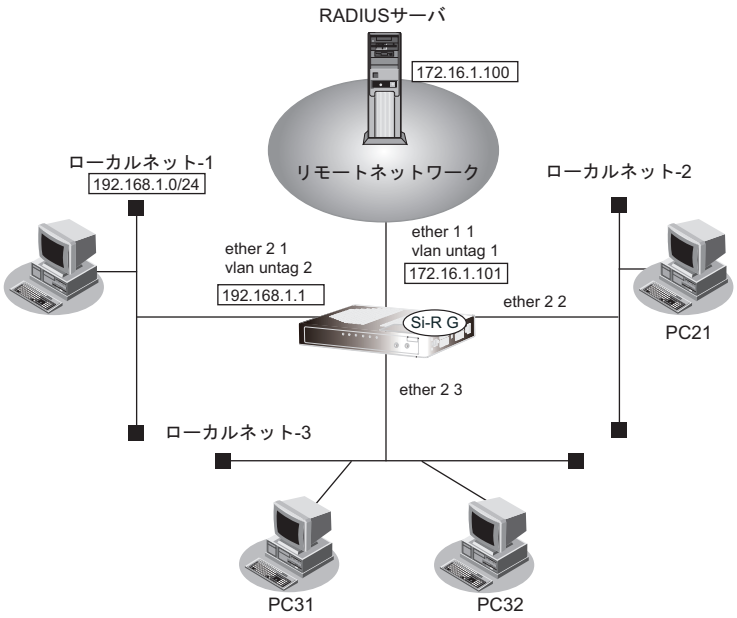
本装置を設定する

● コマンド

```
etherポートとlanインタフェースを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# lan 0 ip address 192.168.0.1/24 3
# lan 0 vlan 1

有線LANでIEEE802.1X 認証を行って端末を収容する
IEEE802.1X 機能を有効にする
# dot1x use on

etherポートとlanインタフェースを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 2
# lan 1 ip address 192.168.10.1/24 3
# lan 1 vlan 2

lanインタフェースにDHCPサーバを設定する
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.10.10/24 10
# lan 1 ip dhcp info gateway 192.168.10.1

etherポートでIEEE802.1X 認証を有効にする
# ether 2 2 dot1x use on

認証に利用するRADIUSサーバをAAA定義番号で指定する
# ether 2 2 dot1x aaa 1

認証／課金サーバをAAA定義で指定する
# aaa 1 name aaasvr
# aaa 1 radius service client both
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 192.168.0.100
# aaa 1 radius client server-info auth 0 source 192.168.0.1
# aaa 1 radius client server-info accounting 0 secret passwd
# aaa 1 radius client server-info accounting 0 address 192.168.0.100
# aaa 1 radius client server-info accounting 0 source 192.168.0.1

設定終了
# save
# commit
```

2.39 不正端末アクセス防止機能（MACアドレス認証）を使う

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。
- 認証端末に割り当てるVLAN IDは、本装置のほかのetherポートまたは認証VLAN用予約VLANに設定されている必要があります。
- 本認証使用時は、etherポートの種別を通常ポート（ether type normal）設定にしてください。
- IEEE802.1X認証と併用時に認証状態初期化操作を行う場合は、dot1xctl initialize port etherを実施してください。

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

- ether 1 1でWAN接続
- ether 2 1は固定VALNローカルネット
- ether 2 2、ether 2 3でMACアドレス認証機能を使う
- ether 2 2、ether 2 3で使用する認証データベース
  ether 2 2　：RADIUSサーバ
  ether 2 3　：ローカルで設定した認証情報
- AAAグループID
  ether 2 2　：0
  ether 2 3　：1

- ローカルネット -3 で利用可能なユーザは以下のとおり

ユーザ	MAC アドレス
PC31	00:11:11:00:00:01
PC32	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
- 認証成功時に割り当てる VID　：2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

本装置を設定する

● コマンド

```
MACアドレス認証を有効にする
# macauth use on

MACアドレス認証で使用するパスワードを設定する
# macauth password macauth-pass

固定VLANローカルネットを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 2
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

有線ポートでMACアドレス認証を使用する
# ether 2 2 use on
# ether 2 2 macauth use on
# ether 2 2 macauth aaa 0
# ether 2 3 use on
# ether 2 3 macauth use on
# ether 2 3 macauth aaa 1

RADIUSサーバを利用するAAAグループ情報を設定する
# aaa 0 name radiusAuth
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.101
# aaa 0 radius client server-info auth secret radius-secret
# aaa 0 radius client server-info auth address 172.16.1.100

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
# aaa 1 name localAuth
# aaa 1 user 0 id 001111000001
# aaa 1 user 0 password macauth-pass
# aaa 1 user 0 supplicant vid 2
# aaa 1 user 1 id 002222000002
# aaa 1 user 1 password macauth-pass
# aaa 1 user 1 supplicant vid 2

設定終了
# save
# commit
```

2.40 ARP 認証機能を使う

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。

Si-R G110B の場合を例にします。

● 設定条件

- 認証用パスワード　：abcd
- VLAN10 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 VLAN20 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
- 通信妨害のための ARP パケット送信間隔　：10 秒

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ARP 認証基本情報の設定
# arpauth use on
# arpauth password abcd

RADIUS サーバの VLAN を設定する
# ether 1 1 vlan untag 20
# lan 0 vlan 20
# lan 0 ip address 172.16.1.200/16 3

ARP 認証が動作する VLAN を設定する
# ether 2 1 vlan untag 10
# lan 1 vlan 10
# lan 1 ip address 172.17.1.100/16 3

ARP 認証を設定する
# vlan 10 arpauth use on
# vlan 10 arpauth aaa 0
# vlan 10 arpauth obstruction enable 10s

RADIUS サーバを利用する AAA グループ情報を設定する
# aaa 0 name RADIUS
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.200
# aaa 0 radius client server-info auth 0 secret radius-secret
# aaa 0 radius client server-info auth 0 address 172.16.1.100

設定終了
# save
# commit
```

2.41 PKI機能を使う

PKI機能とは、デジタル証明書の作成、登録、削除を行います。

証明書とは、ITU-T勧告のX.509に定義されており、本人情報、公開鍵、有効期限、シリアル番号、シグネチャなどが含まれています。

本装置はアプリケーションが、デジタル証明書を利用するために使用されます。

本装置のPKI機能では、以下の設定が利用できます。

- RSA鍵ペアの作成（証明書要求の作成）
- 自装置証明書の設定（認証局での証明書の発行）
- 自装置証明書の自己発行
- 相手装置証明書の設定
- 認証局証明書の設定

こんな事に気をつけて

- 本装置のPKI機能では、証明書について認証局（CA）に問い合わせることはできません。
- 認証局証明書は証明書の検証に利用されるため、設定した認証局証明書から発行されていない証明書の場合、検証に失敗することがあります。
  詳しくは、各アプリケーションの説明を参照してください。
- 自装置証明書の有効期限失効日付には、過去の日付や現在の日付を指定することはできません。

2.41.1 装置に証明書を登録する（自装置証明書を認証局（CA）で発行する）

RSA鍵ペア（証明書要求）を作成し、認証局（CA）で自装置証明書をBase64形式で受け取り（注）、登録する方法を説明します。また、相手装置証明書について登録する方法も説明します。

注）本装置では、認証局（CA）に問い合わせて証明書を取得することはできません。端末（パソコンなど）を使用して認証局（CA）に問い合わせて取得してください。

ここでは以下の条件によって、本装置のRSA鍵ペア（証明書要求）の作成、および自装置証明書と相手装置証明書を登録します。

● 設定条件

- 鍵ペア識別番号　：0
- 鍵長　：1024bit
- 証明書要求で使用するハッシュアルゴリズム　：md5
- 自装置証明書識別番号　：0
- 自装置証明書識別名　：my-cert0.pem
- 自装置証明書で使用するハッシュアルゴリズム　：md5
- 国名（C）　：JP
- 都道府県（ST）　：Kanagawa
- 市区町村（L）　：Kawasaki
- 組織または会社名（O）　：Fujitsu Limited
- 組織ユニットまたは部門（OU）　：Tech Div.
- ホスト名（CN）　：shisya.fujitsu.com

- メールアドレス　：shisya@fujitsu.com
- サブジェクト代替名称（IPアドレス）　：192.168.1.1
- サブジェクト代替名称（DNS名）　：shisya-A.fujitsu.com
- 相手装置証明書識別名　：rmt-cert0.pem

上記の設定条件に従って設定を行う場合のコマンド例を示します。

自装置証明書要求の作成（鍵ペアの作成）

● コマンド

```
自装置証明書要求（鍵ペア）の作成を行う
# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
Local certificate number[0-4] :
key bit(361-2048) :1024
certificate request hash(sha1 or md5) :md5
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
Common Name :shisya.fujitsu.com
Email Address :shisya@fujitsu.com
subjectAltName IP :192.168.1.1
subjectAltName DNS :shisya-A.fujitsu.com
以下のようなコマンドが表示され、自装置証明書要求（鍵ペア）の設定が行われます。
Please wait to create RSA private key and Certificate request.
certificate private 0 line 0 riUB@No/fTnpCpEt5EFOcClRdgTiDnB5n4DLemM5Lr1D8@zQQAL90cFFlcgzCY7P@W3ddbEokoMnHTc@6SP7VOy/isD2
certificate private 0 line 1 qC0dBKFQC1TpoWDZtplUkK5cU1YilubYxhA5V2dudYWb0xAcjflFvsNRzF/xcoi5FnKiOdZjzWxv75NjYMY@nzuVnL6
certificate private 0 line 2 w27xcCjoF1paovWVw1aA4rXXY2L4DGW30rs04sDWCnERcL855Mqw0@Xz0raGv@g8MfKGX3bnEaDImiyAlFflbxRVFsQU
certificate private 0 line 3 xM5/V6omhXp2WaRn6Xi/04wipg357HvboVnJKAiQpY6AbeAftpphz47KFPKnMDaMuxlPY2w@15Obr1KUM1VknoU/tYP
certificate private 0 line 4 cfsRgjZ8kEbsUEsNzfntKATltbtDSBqlZ5Bo46RwRlBkpakJ9dlVv30dJ7cdfnJi9hX@faJbpP3@F3NZP4yKAE3CWtqF
certificate private 0 line 5 jk31xZd75OHuAGNPWsWEVVMA6Kt@YpKpV9zwWGdImOKBs8XgTA8Y5hg8Ut@THKIRl0TgdM4avffQaYwwXWWCFxvUHz
certificate private 0 line 6 KsrHlSB2rYuTnCYCm2sYNdVXaVrMv6VqkNfYNrOwfweu0OqczYUZEDNOYSkP2tLDqBoO47nNWmJWObe2BOex1ujZktW/
certificate private 0 line 7 59UMtzcr44eZToKjXqU2JHi3ukoKHi4FEtYelj2ZMRMoz0DAflVspeddmCjmA0F7SvHh1egTyF0u9GfXW6kTlmBy6/lgc
certificate private 0 line 8 7VjmfcA4QXaAW4MROzijMMmT2kM0phwZ35MNeg977kXr2E2vzjnOh9Wlk4JmBYplxkw@OHo54sC9@HTYy8PNIJcP1nSs
certificate private 0 line 9 pn21UtTKuk7eVV7WHuxeEZnr0V7Wom0FA8Y0u0yQTX5Ebeft7DZMgNGrCxph@jIClmgstpyehofYQUc3KFvNmx2ujLJQ
certificate private 0 line 10 uittrerIb9m0oJxHmle91wPzGZqMwCy5HFL2lUIn/cuv0y1sh8qC20unS26tO0iv87dpWwcEqAlwt3PGZHm339YW7Cp
certificate private 0 line 11 i0q8WeYLk4sSb9vcsnicFdlNAyI9wrWBaZjQIV09vSleN26oTDNBxvmCbJmQyJjUIxcDntSiyrlyIUPthzziagC@SLet
certificate private 0 line 12 WbejnBFwGh/Y6RxCav38qx6@04Eb1bfVaubC/zDH9rLwgR10N/10RzlI0ZqzJ63oL
certificate request 0 line 0 MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaXRlZDESMBAG
certificate request 0 line 2 A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
certificate request 0 line 3 BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/l9yaAuR9ZB/TTlgkLUw7nHj
certificate request 0 line 5 Eu+i2RSudi7YhH70YOgMdBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
certificate request 0 line 6 fs/o1JIcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXl3CyHQ/x0LAgMBAAGg
certificate request 0 line 7 UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBAUA
certificate request 0 line 9 A4GBADod3PXDFWBJOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqO
certificate request 0 line 10 Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcL5xw0JKU79rlsyllGboCJa
certificate request 0 line 11 CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
Created RSA private key and Certificate request.
#

自装置証明書要求（鍵ペア）の作成終了
# save

自装置証明書要求（鍵ペア）の表示
# show crypto certificate base64 candidate
[Certificate Request]
```

```
[1]  Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaXRlZDESMBAG
A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
Eu+i2RSudi7YhH70YOgMdBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
fs/o1JIcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXl3CyHQ/x0LAgMBAAGg
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBAUA
A4GBADod3PXDFWBJOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqO
Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNaIR6IkDXcL5xw0JKU79rIsyllGboCJa
CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
-----END CERTIFICATE REQUEST-----
#
```

表示された自装置証明書要求の証明書部分「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」の最後の改行までをカット＆ペーストで端末（パソコンなど）に保存します。

保存した自装置証明書要求は端末で、FTP などで認証局（CA）と交換します。

次に認証局で発行された自装置証明書を FTP などで認証局から端末（パソコンなど）に保存します。

自装置証明書の取り込み

● コマンド

```
# crypto certificate local 0 name my-cert0.pem
Please input.
端末（パソコンなど）に保存した自装置証明書を貼り付けます。
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQEwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA1MDIyMjE1WhcNMDcwMTAxMDIyMjE1WjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAocGClVZtO1Tool3eIeItbmsOxhK3
KlOqwZhDM11sOGlQUvT6ImpyL25NcoQlJbN9mT31MWWpp1nfirBB3LenaT3X/MEo
vveD9FJ1VbnENjbuEmmjhvxnj7/MHDvQ1D3163BpsIkOlVs1dauO+uOZ6Rl1iM4G
Kypoad0ukW05f9ECAwEAATANBgkqhkiG9w0BAQQFAAOBgQBHokgsMEIT5CJbozH7
rX4u+dLwb0Y48rkfuTmITRfx+eVniPVCDaUxV0Ih361RaWtta/8I16OxHyImHCnt
LOLEsckcXxnU0ArYBNjyylrXwurBJYtlVZPOPqRDq7gSez4zp1lPkt14DrTRSgOh
3rQwOpmTcYT9UuD4iddD9CmUrA==
-----END CERTIFICATE-----
以下のようなコマンドが表示され、自装置証明書の設定が行われます。
certificate local 0 name my-cert0.pem
certificate local 0 line 0 MIICITCCAf4CAQAwDQYJKoZIhvcNAQEEBQAwgZIxCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIa2F3YXNha2kxEDAOBgNVBAoTB3NjYyBM
certificate local 0 line 2 dGQxDTALBgNVBAsTBGRhaTIxGDAWBgNVBAMTD0hpcm9mdW1pIEthc3VnYTEiMCAG
certificate local 0 line 3 CSqGSIb3DQEJARYTa2FzdWdAc2NjLWluYy5jby5qcDAeFw0wNjAxMDQwNzUwNTNa
certificate local 0 line 4 Fw0wNjAyMDMwNzUwNTNaMIGSMQswCQYDVQQGEwJKUDERMA8GA1UECBMIS2FuYWdh
certificate local 0 line 5 d2ExETAPBgNVBAcTCGthd2FzYWtpMRAwDgYDVQQKEwdzY2MgTHRkMQ0wCwYDVQQL
certificate local 0 line 6 EwRkYWkyMRgwFgYDVQQDEw9laXJvZnVtaSBLYXN1Z2ExIjAgBgkqhkiG9w0BCQEW
certificate local 0 line 7 E2thc3VnQHNjYy1pbmMuY28uanAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
certificate local 0 line 8 AM5sXoNnzM4FQrpYNf/ekLWYfH3w0yzI1qtGUpoWRZIGWiAs4rx/1RgGtnQnjNBc
certificate local 0 line 9 8tD9tG2Uo2ngiNsKNvRB39j7EGFIgdPJwwfAaKqA7rgRzQo7jyH7rE5CATVBAnYl
certificate local 0 line 10 HUOlhUAOzDy851u5p4ZjADdIcsPu+5FUqgMgVZ7/B/sdAgMBAAEwDQYJKoZIhvcN
certificate local 0 line 11 AQEEBQADgYEAwpvly/Ak6d1vMgdtclYY5S14jQKd2tnB9CtHz+byG4l75lgqh2uF
certificate local 0 line 12 xZIpbYuSGvVOS+zII1yilelxM5p7QPUs/BAWU1ePUmrLrasetEbgIFX0pXylWF8C
```

```
certificate local 0 line 13 bW08H9SMIDfkd6dindxpkA3VmVlPQKSwCkaAF2kA+LAao0lasskjm04=
#

自装置証明書の設定終了
# save
# reset
```

認証局や相手装置で発行された相手装置証明書をFTPなどで認証局から端末（パソコンなど）に保存します。

相手装置証明書の取り込み

● コマンド

```
# crypto certificate remote 0 name rmt-cert0.pem
Please input.
端末（パソコンなど）に保存した相手装置証明書を貼り付けます。
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwNQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZlYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMbIg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUlAxDrgSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GlkoN+tXc4Q==
-----END CERTIFICATE-----
以下のようなコマンドが表示され、相手装置証明書の設定が行われます。
certificate remote 0 name rmt-cert0.pem
certificate remote 0 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate remote 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate remote 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJob25zeWEu
certificate remote 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate remote 0 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSlAxETAP
certificate remote 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate remote 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEmhvbnN5
certificate remote 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate remote 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwNQay45L
certificate remote 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate remote 0 line 10 mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
certificate remote 0 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZlYiPujmlasvYvUw
certificate remote 0 line 12 /9AqZo3mV7b/uXDdljRMbIg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
certificate remote 0 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUlAxDrgSNM5zzg4AgIX+uE8XY5fE
certificate remote 0 line 14 VAupZ2q7za3Slq6GlkoN+tXc4Q==

相手装置証明書の設定終了
# save
# reset
```

2.41.2 装置に証明書を登録する（自装置証明書を自己発行する）

RSA鍵ペア（証明書要求）および自装置証明書を本装置で作成し登録する方法を説明します。
また、相手装置証明書について登録する方法も説明します。

ここでは以下の条件によって、本装置のRSA鍵ペア（証明書要求）、自装置証明書の作成および相手装置証明書を登録します。

● 設定条件

- 鍵ペア識別番号　：0
- 鍵長　：1024bit
- 証明書要求で使用するハッシュアルゴリズム　：md5
- 自装置証明書識別名　：my-cert0.pem
- 自装置証明書で使用するハッシュアルゴリズム　：md5
- 自装置証明書の有効期限
  失効日付　：2018年1月1日
- 国名（C）　：JP
- 都道府県（ST）　：Kanagawa
- 市区町村（L）　：Kawasaki
- 組織または会社名（O）　：Fujitsu Limited
- 組織ユニットまたは部門（OU）　：Tech Div.
- ホスト名（CN）　：shisya.fujitsu.com
- メールアドレス　：shisya@fujitsu.com
- サブジェクト代替名称（IPアドレス）　：192.168.1.1
- サブジェクト代替名称（DNS名）　：shisya-A.fujitsu.com
- 相手装置証明書識別名　：rmt-cert0.pem

上記の設定条件に従って設定を行う場合のコマンド例を示します。

自装置証明書の作成

● コマンド

```
自装置証明書の作成を行う
# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
Local certificate number[0-4] :0
key bit(361-2048) :1024
certificate request hash(sha1 or md5) :md5
local certificate name :my-cert0.pem
local certificate hash(sha1 or md5) :md5
expire date(YYYYMMDD) :20180101
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
```

Common Name :shisya.fujitsu.com
Email Address :shisya@fujitsu.com
subjectAltName IP :192.168.1.1
subjectAltName DNS :shisya-A.fujitsu.com
以下のようなコマンドが表示され、鍵ペアと自装置証明書の設定が行われます。

```
Please wait to create RSA private key and Certificate request.
certificate private 0 line 0 riUB@No/fTnpCpEt5EFOcClRdgTiDnB5n4DLemM5Lr1D8@zQQAL90cFFlcgzCY7P@W3ddbEokoMnHTc@6SP7VOy/isD2
certificate private 0 line 1 qC0dBKFQC1TpoWDZtplUkK5cU1YilubYxhA5V2dudYWb0xAcjflFvsNRzF/xcoi5FnKiOdZjzWxv75NjYMY@nzuVnL6
certificate private 0 line 2 w27xcCjoF1paovWVw1aA4rXXY2L4DGW30rs04sDWCnERcL855Mqw0@Xz0raGv@g8MfKGX3bnEaDImiyAlFflbxRVFsQU
certificate private 0 line 3 xM5/V6omhXp2WaRn6Xi/04wipg357HvboVnJKAiQpY6AbeAftpphz47KFPKnMDaMuxlPY2w@15Obr1KUM1VknoU/tYP
certificate private 0 line 4 cfsRgjZ8kEbsUEsNzfntKATltbtDSBqlZ5Bo46RwRIBkpakJ9dlVv30dJ7cdfnJi9hX@faJbpP3@F3NZP4yKAE3CWtqF
certificate private 0 line 5 jk31xZd75OHuAGNPWsWEVVMA6Kt@YpKpV9zwWGdImOKBs8XgTA8Y5hg8Ut@THKIRl0TgdM4avffQaYwwXWWCFxvUHz
certificate private 0 line 6 KsrHISB2rYuTnCYCm2sYNdVXaVrMv6VqkNfYNrOwfweu0OqczYUZEDNOYSkP2tLDqBoO47nNWmJWObe2BOex1ujZktW/
certificate private 0 line 7 59UMtzcr44eZToKjXqU2JHi3ukoKHi4FEtYelj2ZMRMoz0DAflVspeddmCjmA0F7SvHh1egTyF0u9GfXW6kTlmBy6/lgc
certificate private 0 line 8 7VjmfcA4QXaAW4MROzijMMmT2kM0phwZ35MNeg977kXr2E2vzjnOh9Wlk4JmBYplxkw@OHo54sC9@HTYy8PNlJcP1nSs
certificate private 0 line 9 pn21UtTKuk7eVV7WHuxeEZnr0V7Wom0FA8Y0u0yQTX5Ebeft7DZMgNGrCxph@jlClmgstpyehofYQUc3KFvNmx2ujLJQ
certificate private 0 line 10 uittrerIb9m0oJxHmle91wPzGZqMwCy5HFL2lUIn/cuv0y1sh8qC20unS26tO0iv87dpWwcEqAlwt3PGZHm339YW7Cp
certificate private 0 line 11 i0q8WeYLk4sSb9vcsnicFdlNAyI9wrWBaZjQIV09vSleN26oTDNBxvmCbJmQyJjUIxcDntSiyrlyIUPthzziagC@SLet
certificate private 0 line 12 WbejnBFwGh/Y6RxCav38qx6@04Eb1bfVaubC/zDH9rLwgR10N/10RzlI0ZqzJ63oL
certificate request 0 line 0 MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaXRlZDESMBAG
certificate request 0 line 2 A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
certificate request 0 line 3 BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
certificate request 0 line 5 Eu+i2RSudi7YhH70YOgMdBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
certificate request 0 line 6 fs/o1JIcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXl3CyHQ/x0LAgMBAAGg
certificate request 0 line 7 UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBAUA
certificate request 0 line 9 A4GBADod3PXDFWBJOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqO
certificate request 0 line 10 Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6IkDXcL5xw0JKU79rlsyllGboCJa
certificate request 0 line 11 CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
Created RSA private key and Certificate request.

Please wait to create Local certificate.
certificate local 0 name my-cert0.pem
certificate local 0 line 0 MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate local 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
certificate local 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate local 0 line 4 MDYxMDEwMDE1MDI5WhcNMDcwMTAxMDE1MDI5WjCBnzELMAkGA1UEBhMCSlAxETAP
certificate local 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate local 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
certificate local 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate local 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAnrnXhzgmp9MDVjjfGcSOLdTAY9v8
certificate local 0 line 9 j3JoC5H1kH9NMiCQtTDuceMS76LZFK52LtiEfvRg6Ax0EbzUK16WpXbM/7H/3k7u
certificate local 0 line 10 WqzljImQdjOrJLgTj4o4BAZ+z+jUkhykQ8PalCpbSuRcZWhxGM27E3sV2F8OLCxR
certificate local 0 line 11 Q0BdeXcLldD/HQsCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
certificate local 0 line 12 AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
certificate local 0 line 13 BgEB/wIBATANBgkqhkiG9w0BAQQFAAOBgQAAZ2LDxJ3a38HgT3el7FkXLWcfEEaK
certificate local 0 line 14 uIZNnV7/cjj9KimdSianZWdgEvDKQQOx41KtrWxxrHgrzRSbg4KpkjgUgthadJvq
certificate local 0 line 15 hKK1zeIemN7RnpFuuBODkxx4hM1vuzJRTVUWH+UJciFoMAQOnrjB8hoNyGfiQVji
certificate local 0 line 16 9OyuMYZvejGO5A==
Created Local certificate.
#
```

自装置証明書の作成終了

```
# save
```

自装置証明書の表示

```
# show crypto certificate base64 candidate
[Certificate Request]
[1]   Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGltaXRlZDESMBAG
A1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
Eu+i2RSudi7YhH70YOgMdBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
fs/o1JIcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXl3CyHQ/x0LAgMBAAGg
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAGhwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5YS1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBAUA
```

A4GBADod3PXDFWBJOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqO
Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcL5xw0JKU79rlsyllGboCJa
CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
-----END CERTIFICATE REQUEST-----

[Local Certificate]
[1]　Number : 0, Name : my-cert0.pem
-----BEGIN CERTIFICATE-----
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYxMDEwMDE1MDI5WhcNMDcwMTAxMDE1MDI5WjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAnrnXhzgmp9MDVjjfGcSOLdTAY9v8
j3JoC5H1kH9NMiCQtTDuceMS76LZFK52LtiEfvRg6Ax0EbzUK16WpXbM/7H/3k7u
WqzljImQdjOrJLgTj4o4BAZ+z+jUkhykQ8PaICpbSuRcZWhxGM27E3sV2F8OLCxR
Q0BdeXcLIdD/HQsCAwEAAaNVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBgwFoIUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAgw
BgEB/wIBATANBgkqhkiG9w0BAQQFAAOBgQAAZ2LDxJ3a38HgT3el7FkXLWcfEEaK
ulZNnV7/cjj9KimdSianZWdgEvDKQQOx41KtrWxxrHgrzRSbg4KpkjgUgthadJvq
hKK1zeIemN7RnpFuuBODkxx4hM1vuzJRTVUWH+UJciFoMAQOnrjB8hoNyGfiQVji
9OyuMYZvejGO5A==
-----END CERTIFICATE-----

表示された証明書要求と自装置証明書の証明書部分「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」の最後の改行までをカット＆ペーストで端末（パソコンなど）に保存します。

保存した自装置証明書は端末で、FTP などで相手装置と交換します。

設定終了
reset

認証局や相手装置で発行された相手装置証明書を FTP などで認証局から端末（パソコンなど）に保存します。

相手装置証明書の取り込み

● コマンド

```
# crypto certificate remote 0 name rmt-cert0.pem
Please input.
端末（パソコンなど）に保存した相手装置証明書を貼り付けます。
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwNQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZlYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMbIg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUlAxDrgSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GlkoN+tXc4Q==
-----END CERTIFICATE-----
以下のようなコマンドが表示され、相手装置証明書の設定が行われます。
certificate remote 0 name rmt-cert0.pem
certificate remote 0 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate remote 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate remote 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJob25zeWEu
certificate remote 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate remote 0 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSlAxETAP
certificate remote 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate remote 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEmhvbnN5
certificate remote 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate remote 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwNQay45L
certificate remote 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate remote 0 line 10 mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
certificate remote 0 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZlYiPujmlasvYvUw
certificate remote 0 line 12 /9AqZo3mV7b/uXDdljRMbIg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
certificate remote 0 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUlAxDrgSNM5zzg4AgIX+uE8XY5fE
certificate remote 0 line 14 VAupZ2q7za3Slq6GlkoN+tXc4Q==

相手装置証明書の設定終了
# save
# reset
```

2.41.3　認証局証明書を設定する

認証局証明書を使用する場合に認証局証明書を設定する方法を説明します。

「2.41.1 装置に証明書を登録する（自装置証明書を認証局（CA）で発行する）」（P.418）または「2.41.2 装置に証明書を登録する（自装置証明書を自己発行する）」（P.422）のどちらかで自装置証明書および相手装置証明書を登録してください。

ここでは以下の条件によって、本装置の認証局証明書を作成することを前提とします。

● 設定条件

- 認証局証明書識別名　：ca-cert0.pem

上記の設定条件に従って設定を行う場合のコマンド例を示します。

認証局証明書を交換し設定する

認証局で発行された認証局証明書をFTPなどで認証局から端末（パソコンなど）に保存します。

端末（パソコンなど）に保存した認証局証明書を貼り付けます。

● コマンド

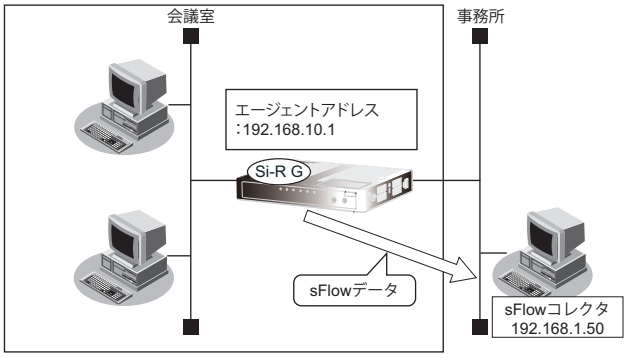
```
# crypto certificate ca 0 name ca-cert0.pem
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSlAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwNQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZIYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMbIg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUlAxDrgSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GlkoN+tXc4Q==
-----END CERTIFICATE-----
以下のようなコマンドが表示され、認証局証明書の設定が行われます。
certificate ca 0 name ca-cert0.pem
certificate ca 0 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwgZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 0 line 1 VQQIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate ca 0 line 2 c3UgTGltaXRlZDESMBAGA1UECxMJVGVjaCBEaXYuMRswGQYDVQQDExJob25zeWEu
certificate ca 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate ca 0 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSlAxETAP
certificate ca 0 line 5 BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEwhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate ca 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwlUZWNoIERpdi4xGzAZBgNVBAMTEmhvbnN5
certificate ca 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate ca 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwNQay45L
certificate ca 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate ca 0 line 10 mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
certificate ca 0 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZIYiPujmlasvYvUw
certificate ca 0 line 12 /9AqZo3mV7b/uXDdljRMbIg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
```

```
certificate ca 0 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUlAxDrgSNM5zzg4AgIX+uE8XY5fE
certificate ca 0 line 14 VAupZ2q7za3Slq6GlkoN+tXc4Q==

認証局証明書の設定終了
# save
# reset
```

2.42 sFlowエージェント機能を使う

本装置は、sFlowエージェント機能をサポートしています。

ここでは、sFlowコレクタに対してsFlow情報を通知する場合の設定方法を説明します。



☛参照 マニュアル「機能説明書」

ヒント

◆ sFlowとは？

sFlowは、トラフィックをリアルタイムにモニタリングするためのプロトコルです。

sFlow機能は、以下の役割を持つ装置で構成されます。

- sFlowエージェント
  トラフィックをモニターして、トラフィックに関する情報を送信する装置です。
- sFlowコレクタ
  トラフィック情報を受信して解析する装置です。

sFlowエージェントは、以下の機能をサポートしています。

- フローサンプル機能
  送受信パケットをユーザ指定の個数ごとにサンプリングし、sFlow情報に加工しコレクタに送信します。
- カウンタサンプル機能
  デバイスの統計情報をユーザ指定の間隔ごとにサンプリングし、sFlow情報に加工してコレクタに送信します。

本装置では、Ver.5のsFlowエージェント機能をサポートし、wan-lan間のパケットをサンプルの対象にしています。本機能を使用する場合、別途、sFlowコレクタが必要です。

☛参照 マニュアル「仕様一覧」

こんな事に気をつけて

- コレクタアドレスを設定していない場合、sFlowエージェント機能は停止した状態となります。
- エージェントアドレスが未設定、および自装置に存在しないアドレスを設定した場合、sFlowパケットの自局IPアドレスは、送出されるインタフェースに割り当てられたアドレスとなります。また、sFlowパケット内のエージェントアドレス には127.0.0.1が設定されます。

フローサンプルを設定する

フローサンプルをサンプリングする場合は、以下の情報を設定します。

● 設定条件

- sFlow エージェント機能を使用する
- エージェントアドレス　：192.168.10.1
- コレクタアドレス　：192.168.1.50
- 1000 パケット送信ごと、1000 パケット受信ごとにフローサンプルを行う

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
sFlow エージェント情報を設定する
#sflow agent 192.168.10.1
#sflow collector 192.168.1.50

サンプリングレートを設定する
#sflow sampling-rate 1000 1000

sFlow エージェント機能を使用する
#sflow service enable

設定終了
#save
#commit
```

カウンタサンプルを設定する

カウンタサンプルをサンプリングする場合は、以下の情報を設定します。

● 設定条件

- sFlow エージェント機能を使用する
- エージェントアドレス　：192.168.10.1
- コレクタアドレス　：192.168.1.50
- 60 秒ごとにカウンタサンプルを行う

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

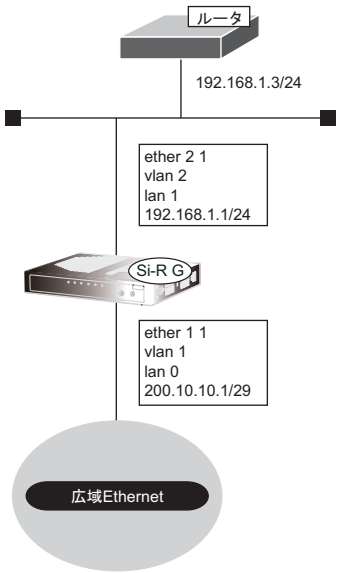
```
sFlow エージェント情報を設定する
#sflow agent 192.168.10.1
#sflow collector 192.168.1.50

カウンタサンプリングを設定する
#sflow polling-interval 60s

sFlow エージェント機能を使用する
#sflow service enable

設定終了
#save
#commit
```

2.43 トラッキング機能を使う

トラッキング機能を使用すると、トリガの状態が遷移した際にアクション（コマンド）を適用できます。
ここでは、トラッキング機能を使用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

- 適用するアクション（コマンド）として、カウンタ・ログ・統計・状態などの表示コマンド、および、トラッキング機能自身の設定・削除や統計情報表示・クリア操作コマンドを指定した場合、コマンドは実行されません。
- ノードトリガでの監視を行う場合、相手ノードにICMP ECHOパケットを定期的に送信します。そのため、定額制ではない回線を使用している場合は、超過課金の原因になることがあります。このような環境ではノードトリガを使わないでください。



● 設定条件

[広域Ethernet側]

- ポート　：ether 1 1 を使う
- VLAN　：untag 1
- lan　：lan 0
- IPアドレス　：200.10.10.1/29

[lan側]

- ポート　：ether 2 1 を使う
- VLAN　：untag 2
- lan　：lan 1
- IPアドレス　：192.168.1.1/24

[トラッキング]

- 監視先IPアドレス　：192.168.1.3
- 障害発生時のアクション　：ether 1 1 をofflineにする
- 復旧時のアクション　：ether 1 1 をonlineにする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

lan インタフェースを設定する
# lan 0 ip address 200.10.10.1/29 3
# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

トラッキング情報を設定する
# tracking 0 trigger 0 node 0
# tracking 0 action 0 down "offline ether group 1 port 1"
# tracking 0 action 1 up "online ether group 1 port 1"
# node-trigger 0 address 192.168.1.1 192.168.1.3

設定終了
# save
# commit
```

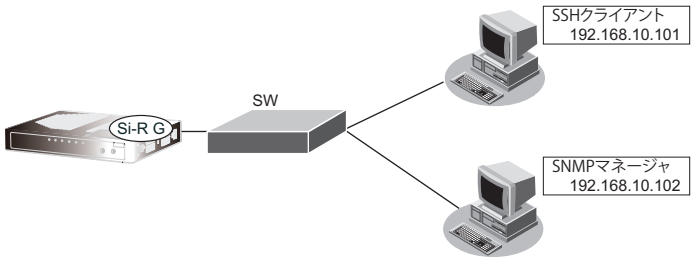
2.44 装置を保護する

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者(admin)用パスワードの設定
- オートログアウトの設定
- Telnet/SSHおよびSNMP接続に対するアクセス制限
- 不要なサービスの停止

2.44.1 設定例

以下にそれぞれの設定を行う場合の例を示します。



● 設定条件

- 管理者(admin) パスワード　：sirg_admin-2022
- IPアドレス　：192.168.10.100/24
- オートログアウトの設定（ログインしたままの状態で指定時間無操作だった際に自動切断を行う）
  コンソールのオートログアウト時間　：5分
  SSHのオートログアウト時間　：5分
  ※SSH のオートログアウト時間は ”telnetinfo autologout” と共通
- SNMP設定
  アクセス許可するSNMPマネージャ　：192.168.10.102
  コミュニティ名　：private
  マネージャからの書き込み　：許可しない
- SSH接続を許可するホストのIPアドレス　：192.168.10.101
- Telnet接続　：禁止
- 不要なサーバ機能はすべて停止
  # serverinfo <サーバ機能名> ip off
- IPv6アドレスをSi-R Gに付与した際には、IPv6に関する不要なサーバ機能はすべて停止
  # serverinfo <サーバ機能名> ipv6 off

```
adminパスワードをsirg_admin-2022に設定
# password admin set sirg_admin-2022

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m

Telnet/SSHのオートログアウトまでの無操作時間を5分に設定
# telnetinfo autologout 5m
```

```
自装置IPアドレスとVLANの設定
# lan 0 ip address 192.168.10.100/24 3
# lan 0 vlan 1

SNMPを有効、コミュニティ名をprivate、書き込み許可しない
# snmp service enable
# snmp manager 0 192.168.10.102 private v1 disable

許可するホストからのSSH接続のみ許可する
# acl 0 ip 192.168.10.101/32 any any any
# serverinfo ssh filter 0 accept acl 0
# serverinfo ssh filter default reject

Telnetサーバ機能を停止
# serverinfo telnet ip off

不要なサーバ機能はすべて停止
# serverinfo ftp ip off
# serverinfo sftp ip off
# serverinfo http ip off
# serverinfo dns ip off
# serverinfo sntp ip off
# serverinfo time ip tcp off
# serverinfo time ip udp off

設定終了
# save
# commit
```

索引

S

T

U

V

W

あ

え

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ふ

へ

ほ

ま

め

ゆ

り

Si-R Gシリーズ　コマンド設定事例集

P3NK-5712-05Z0

発行日　　2023年5月

発行責任　　富士通株式会社