IPアクセスルータ Si-Rシリーズ

Web設定事例集 V33



はじめに

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

> 2007年 7月初版 2007年11月第2版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。 従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。 Microsoft Corporationのガイドラインに従って画面写真を使用しています。 All rights reserved, Copyright© 富士通株式会社 2007

目次

目次

	はじと	かに	2
	本書の	D構成と使いかた	7
		本書の読者と前提知識	7
		本書の構成	7
		本書における商標の表記について	8
		本装置のマニュアルの構成	9
第 1	章	導入例	10
	1.1	「かんたん設定メニュー」で設定する	.11
		1.1.1 プライベート LAN を構築する	11
		1.1.2 セグメント接続/分割する	.15
		1.1.3 PPPoE 接続する	.19
		1.1.4 CATV インターネットに接続する	.23
		1.1.5 インターネットへ ISDN 接続する	.25
		1.1.6 インターネットへ専用線接続する	.30
		1.1.7 オフィスへ ISDN 接続する	.34
		1.1.8 オフィスへ専用線接続する	.39
	1.2	LAN をネットワーク間接続する	.42
	1.3	IPv4 のネットワークに IPv6 ネットワークを追加する	.50
	1.4	プライベート LAN を構築する	.55
	1.5	インターネットへ専用線で接続する	.61
	1.6	インターネットへ PPPoE で接続する	.67
	1.7	インターネットヘデータ通信カードを使用して接続する	.76
	1.8	無線 I AN とデータ通信カードで仮設店舗を構築する	.86
	19		97
	1 10		103 103
	1.10		100
	1.11		109
	1.12		115
	1.13	復数の事業所 LAN を IP-VPN 網を利用して接続 9 る	127
		1.13.1 ADSL モナムを使用して IP-VPN 網と接続9 る	128
	1 1 1	1.13.2 「高迷ナインツル専用線を使用してIP-VPN 約と技続9 る	130
	1.14		45
		1.14.1 NAI を併用しない回走 IP アトレスでの VPN(自動鍵父授)	145
		1.14.2 NATと併用した回応IPアドレスCのVPN(日朝鍵文揆)	150
	1 1 5		109
	1.15	IPv6の事業所 LAN を IPv6 トンネルで接続する	190
**			
第2	早	沽用例	01
	2.1	RIPの経路を制御する(IPv4)2	205
		2.1.1 特定の経路情報の送信を許可する	207
		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	209
		2.1.3 特定の経路情報の受信を許可する	211
		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	213
		2.1.5 行正の経路情報の必信を禁止する	216
	2.0	2.1.0 対定の経路に 対応の経路 対応の <	218
	Z.Z	NIF VI在昭位前御9 る(IFVO)	<u>2</u> 20

		2.2.1	特定の経路情報の送信を許可する	222
		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	224
		2.2.3	特定の経路情報の受信を許可する	226
		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	
		2.2.5	特定の経路情報の送信を禁止する	231
		2.2.6	特定の経路情報の受信を禁止する	233
2.	.3	OSPFv2	を使用したネットワークを構築する(IPv4)	235
		2.3.1	バーチャルリンクを使う	
		2.3.2	スタブエリアを使う	
2.	.4	OSPF の)経路を制御する(IPv4)	
		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	
		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	
		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	
2.	5	OSPF 機	能を使う(IPv6)	
		251	OSPE ネットワークを構築する	273
		2.5.2	てして境界ルータでエリア内部経路を集約する	278
		253	エリア境界ルータで不要な経路情報を遮断する	280
2	6	E.G.P の紙	⁻ YBFA1111 - CC	282
۷.	.0	261		202 ງຊາ
		2.0.1		202
		2.0.2		286
		2.0.3		200 200
r	7	2.0.4 車業所問	「120円成の過回柱町を使用する」 また MDI c 培結サービフ を利用して 培結する	200 າດາ
Ζ.	. /		Jで MFLS 接続サービスで利用して接続する	202
		2.7.1	トンネルエンドホインドをインタフェースアドレスにして MPLS LSP を使用する トンネルエンドポイントをインタフェーフアドレフトは別のアドレフにして	
		2.1.2	トンネルエンドボインドをインタンエースンドレスとは別のシドレスにして MPLS LSP を使用する	302
2	8	MPISな	-使用したレイヤ 2VPN(FoMPLS)を構築する	313
2	9	MPLSA	- 使用したレイヤ 3\/PN(BGP/MPI S \/PN)を構築する	321
۷.	.0	291		322
		2.3.1		333
n	10	2.5.2 マルチレ	MFL3 枘と守用板を使用して按続する	
Ζ.	.10	2101	ノノ 版 肥 と ぼ ノ	
		2.10.1	ISDN ビマルナリノク機能を使う	
		2.10.2	復数専用線 ビマルナリノク 機能を 使う	
~	1 1	2.10.3		
Ζ.	.	マルティ	- ヤスト械能を使う	
		2.11.1	マルチキャスト機能 (PIM-DM) を使っ	
		2.11.2	マルナキャスト機能 (PIM-SM) を使っ	
		2.11.3	マルチキャスト機能(スタティックルーティンク)を使っ	
2.	.12	VLAN 機	能を使う	372
2.	.13	IP フィル	レタリング機能を使う	376
		2.13.1	外部の特定サービスへのアクセスだけ許可する	
		2.13.2	外部から特定サーバへのアクセスだけ許可する	
		2.13.3	外部から特定サーバへのアクセスだけ許可して SPI を併用する	409
		2.13.4	外部の特定サービスへのアクセスだけ許可する(IPv6 フィルタリング)	
		2.13.5	外部の特定サーバへのアクセスだけを禁止する	
		2.13.6	利用者が意図しない発信を防ぐ	
		2.13.7	回線が接続しているときだけ許可する	
		2.13.8	外部から特定サーバへの ping だけを禁止する	
2.	.14	IPsec 機	能を使う	452
		2.14.1	IPv4 over IPv4 で固定 IP アドレスでの VPN(手動鍵交換)	456
		2.14.2	IPv4 over IPv6 で固定 IP アドレスでの VPN(自動鍵交換)	
		2.14.3	IPv4 over IPv6 で可変 IP アドレスでの VPN(自動鍵交換)	472
		2.14.4	IPv6 over IPv4 で固定 IP アドレスでの VPN(自動鍵交換)	

目次

	2.14.5	IPv6 over IPv4 で可変 IP アドレスでの VPN(自動鍵交換)	489
	2.14.6	IPv6 over IPv6 で固定 IP アドレスでの VPN(自動鍵交換)	500
	2.14.7	IPv6 over IPv6 で可変 IP アドレスでの VPN(自動鍵交換)	510
	2.14.8	IPv4 over IPv4 で1つの IKE セッションに複数の IPsec トンネル構成での VPN(白動鍵交換)	520
	2 14 9	VIN (日初錠ス)() IPsec 機能と他機能との併田	532
	2.14.0	IPv4 over IPv4 で固定 IP アドレスでバックアップ田に使田する VPN (自動鍵交換)	552
	2.14.10		569
	2.14.11		578
	2.14.12	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	588
	2.14.10	アンプレート着信機能 (IADIUS 認証) を使用した可変 IP アドレスでの VPN	599
	2.14.14	テンプレート着信機能(MADIOG LLL) を使用した IPv4 over IPv4 で固定 IP アドレスでの	
	211 11 0		611
	2.14.16	テンプレート着信機能(動的 VPN)を使用した	C 22
	0 1 4 1 7	IPV4 OVER IPV4 C回足 IP アドレスCO VPN (儿女柄成)	
	2.14.17	テノフレート宿信機能(動的 VPN)を使用した IPV6 OVER IPV6 で回走 IP ゲトレスでの	
	2.14.18	NAT トラバーサルを使用した可変 IP アドレスでの VPN	663
	2.14.19	テンプレート着信機能(AAA 認証)および NAT トラバーサルを使用した	
		可変 IP アドレスでの VPN	671
	2.14.20	接続先情報(動的 VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	680
2.15	システム	ログを採取する	712
2.16	マルチN	IAT 機能(アドレス変換機能)を使う	715
	2.16.1	プライベート LAN 接続でサーバを公開する	716
	2.16.2	PPPoE 接続でサーバを公開する	718
	2.16.3	ネットワーク型接続でサーバを公開する	721
	2.16.4	サーバ以外のアドレス変換をしないで、プライベート LAN 接続でサーバを公開する	724
	2.16.5	複数の NAT トラバーサル機能を使用した IPsec クライアントを 同じ IPsec サーバに接続する	726
	2.16.6	NAT あて先変換で双方向のアドレスを変換する	728
2.17	VoIP NA	T トラバーサル機能を使う	730
2.18	TOS/Tra	ffic Class 値書き換え機能を使う	732
2.19	VIANブ	?ライオリティマッピング機能を使う	735
2 20	·=/	ッ (************************************	737
2.20		- ノノ 100 ㎡ と	יסי רפר
	2.20.1	何たのイフタフェーへてフェーロフフ悈形を使う	737 סמד
2 21	2.20.2 データロ	広向元ことにフェービアフ級形で戻り	730 742
2.21	ノノノロ		74Z
2.22	市場前個	J(WFQ)	744
2.23	DHCP 榜		/48
	2.23.1	DHCP サーバ機能を使っ	749
	2.23.2	DHCP 人タティック機能を使う	752
	2.23.3	DHCP クライアント機能を使う	
	2.23.4	UHCP リレーエーシェント機能を使う	
0 0 4	2.23.5	IPV6 DHCP クライアノト械能を使う	760
2.24	DNS U-	- 八機能を使う(ProxyDNS)	/64
	2.24.1	DNS サーバの自動切り替え機能(順引き)を使う	764
	2.24.2	UNS リーハの日期切り台ん (成形 () どうさ) を () この に いっか いう い に せい ご つ に い つ の に 新 印 得 燃 火 ち た こ	
	2.24.3	UNS リーハア トレスの日期収存機能を使う	
	2.24.4	UNS リーハア トレスを UHUF リーハから取得して使う	//
	2.24.5	UND 回いロクビン イノノイルン 成形を定し	//3
ງງ⊏	2.24.0 時空の・	- DN3 y ^一 ハ悈彤で戻し	ל/ / ררר
Z.ZD	村止りし	INL ^ VJ/ ノヒヘで示エ 9 る(UNL ノ 1 ルグ	////

目次

	2.28	VRRP 機能を使う	817
		2.28.1 簡易ホットスタンバイ機能を使う	
		2.28.2 クラスタリング機能を使う	
	2.29	ポリシールーティング機能を使う	827
		2.29.1 Ingress ポリシールーティング機能を使う	
		2.29.2 マルチルーティング機能を使う	
	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)	835
		2.30.1 リモートパワーオン情報を設定する	
		2.30.2 リモートパワーオン機能を使う	
	2.31	スケジュール機能を使う	837
		2.31.1 スケジュールを予約する	838
		2.31.2 電話番号変更を予約する	
		2.31.3 構成定義情報の切り替えを予約する	
	2.32	通信料金を節約する(課金制御機能)	
		2.32.1 課金単位時間を設定する	
		2.32.2 課金制御機能(発信抑止)を設定する	
	2.33	ノリッシ/ SIP 機能を使う	
		2.33.1 フリッジで FNA をつないで STP 機能を使う	
		2.33.2 ノリッンクルーヒンク機能を使う	855
	0.04	2.33.3 IP トノイルで事業所向をノリッン接続9 る(Ethernet over IP ノリッン)	
	2.34	後数の LAN ホートをスイッテンク HUB のように使う	
	2.35		
		2.35.1 事美所ごとに別の VPC を使用する	
	2.20	2.35.2 VPU と VUU の回時ンエービノクを使用9 る	
	2.30	ISDN 按税で突破こした通信バックアッフを使う	
	2.37	外部のハンコンから PIAFS 接続 9 る	
	2.38	アナロクモデムで通信バックアッフをする	
	2.39	データ通信カードで通信バックアップをする	913
	2.40	外部のパソコンから着信接続する(リモートアクセスサーバ)	919
		2.40.1 1 台の装置でリモートアクセスサーバを構成する	
		2.40.2 複数台の装置でリモートアクセスサーバを構成する	
		2.40.3 リモートアクセスサーバが使用する RADIUS サーバを多重化する	
	2.41	スイッチボートを使う	
		2.41.1 スイッチポートを HUB として使用する	
		2.41.2 VLAN 透過モードを使用する	
		2.41.3 スイッチボートを独立ボートとして使用する	
	0.40	2.41.4 人イツナホートを分割して使用する	
	2.42		
	2.43	SIP-SIP ケートワェイ機能を使っ	
	2.44	IEEE802.1X 認証機能を使う	
		2.44.1 有線 LAN と無線 LAN で IEEE802.1X 認証機能を使う	
	2.45	个止端末アクセス防止機能(MAC アドレス認証)を使う	
	2.46	ARP 認証機能を使う	
索引			986

本書の構成と使いかた

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

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

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。 本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

本書の構成

以下に、本書の構成と各章の内容を示します。

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

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

☆ ヒント 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。

補足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。

● 参照 操作方法など関連事項を説明している箇所を示します。

適用機種 本装置の機能を使用する際に、対象となる機種名を示します。



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

本書における商標の表記について

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

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

UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。

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

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

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

本装置のマニュアルの構成

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

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



この章では、本装置の代表的な接続形態を紹介します。

1.1 「かんたん設定メニュー」で設定する

適用機種 Si-R180,180B,220B,220C

[設定] タブをクリックすると、[かんたん設定メニュー] ボタンと [詳細設定メニュー] ボタンの2つが表示されます。

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

1.1.1 プライベートLANを構築する



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

本装置のIPアドレスを変更しない場合

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

Si-R180、180Bは、本装置の電源を投入するだけで通信することができます。ただし、インタフェースは、以下の図とは逆になります(LAN0→LAN1、LAN1→LAN0)。Si-R180、180Bでは、スイッチポート(SW1~4)が 有効になります。



● 設定条件

[事務所側]

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

[会議室側]

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

[その他の条件]

 パスワードを設定する パスワード

: himitu

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

こんな事に気をつけて

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

本装置のIPアドレスを変更する場合

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

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



こんな事に気をつけて

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

● 参照 Si-Rシリーズ Webユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P19)

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

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

「プライベート LAN 構築かんたん設定」ページが表示されます。

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

2. 「必須設定」で以下の項目を指定します。

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

■必須設定				
グローバル側IPアドレス	 ● DHCPで自動的に取得する ● 指定する IPアドレス ネットマスク 2 (192.0.0) 			
ブライベート側IPアドレス	IPアドレス 192.168.2.1 ネットマスク 24 (255.255.255.0) ▼			

3. 「オプション設定」で以下の項目を指定します。

- DHCPサーバ デフォルトルータ広報 DNSサーバ広報
- → 192.168.2.1

→使用する

- →192.168.2.1
- UPnP 機能
 → UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は "使用する"を選択します。

● 参照「2.17 VoIP NAT トラバーサル機能を使う」(P.730)

	○使用しない ◎使用する	
DHCPサーバ	デフォルトルータ広 報	192.168.2.1
	DNSサーバ広報	192.168.2.1
	ドメイン名広報	
UPnP機能	●使用しない●使	用する

4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に通信できる状態になります。

こんな事に気をつけて

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

☆ヒント——

◆ 省略値について

プライベートLAN構築かんたん設定に適用される主な省略値を示します。

○:変更可能、×:変更不可

	項目	適用される省略値	かんたん設定 での設定変更
グローバル側 IPアドレス		DHCPクライアント機能により自動的に取得する	0
	ネットマスク	DHCP クライアント機能により自動的に取得する	0
	セカンダリIPアドレス	なし	×
	デフォルトルータ	DHCP クライアント機能により自動的に取得する	0
	DNSサーバアドレス	DHCPクライアント機能により自動的に取得する	0
	DHCPサーバ機能	使用しない	×
	NAT機能	マルチNATを使用する	×
		・アドレス個数:1個	
		・アドレス割り当てタイマ:5分	
	RIP機能		×
	・RIP送信	ルーティングプロトコルを使用しない	
	・RIP受信	RIP-V1を使用する	
	インタフェース	Si-R180、180B:LAN0、Si-R180、180B以外:LAN1	○ (※)
	転送レート	自動認識	0
プライベート側	IPアドレス	192.168.1.1	0
	ネットマスク	24 (255.255.255.0)	0
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能	使用する	0
	・割り当て先頭IPアドレス	本装置のプライベートLAN 側の IP アドレス、ネットマ	×
		スクから求めたネットワークアドレス+2	×
	・割り当てアドレス数	253	
	デフォルトルータ広報	192.168.1.1	0
	DNS サーバ広報	192.168.1.1	\bigcirc
	ドメイン名広報	なし	0
	RIP機能		×
	・RIP送信	RIP-V1を使用する	
	・RIP受信	RIP-V1を使用する	
	転送レート	自動認識	0
IPv6 経路		使用しない	×
ブリッジ		使用しない	×
UPnP機能		使用しない	0

※) Si-R180、180Bは変更できません。

1.1.2 セグメント接続/分割する

<u>適用機種</u> Si-R180,180B,220B,220C

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

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

本装置のIPアドレスを変更しない場合

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

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



● 設定条件

[LAN-A側]

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

[LAN-B側]

転送レートは自動認識

ネットワークアドレス/ネットマスク

● IPアドレス

- : 192.168.0.1
- : 192.168.0.0/24

[その他の条件]

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

こんな事に気をつけて

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

- かんたん設定メニューでLAN間接続の「セグメント接続/分割」をクリックします。
 「セグメント接続/分割かんたん設定」ページが表示されます。
- 2. [設定終了] ボタンをクリックします。

再起動後に通信できる状態となります。

本装置のIPアドレスを変更する場合

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

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



こんな事に気をつけて

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

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

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

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

「セグメント接続/分割かんたん設定」ページが表示されます。

2. [LAN0] で以下の項目を指定します。

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

LAN0		
IPアドレス	192.168.3.1	
ネットマスク	24 (255.255.255.0)	

3. [LAN1] で以下の項目を指定します。

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

LAN1(スイッチ)	3
IPアドレス	192.168.2.1
ネットマスク	24 (255.255.255.0)

Si-R180、180Bでは、表示が上記の画面とは異なります。

4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に通信できる状態になります。

こんな事に気をつけて

- 本装置のIPアドレスを変更した場合、以下に示す2つの操作が必要です。
- 本装置に接続しているパソコンのIPアドレスも合わせて変更する必要があります。
- 再起動後に本装置にアクセスするためには、URLで指定するIPアドレスに変更後のIPアドレスを指定する必要があります。

どとント

◆ 省略値について

セグメント接続/分割かんたん設定時に適用される主な省略値を示します。

〇:変更可能、×:変更不可

	項目	適用される省略値	かんたん設定 での設定変更
LAN0	IPアドレス	192.168.1.1	0
	ネットマスク	24 (255.255.255.0)	0
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能	使用しない	×
	NAT機能	使用しない	×
	RIP機能		×
	・RIP送信	RIP-V1を使用する	
	・RIP受信	RIP-V1を使用する	
	転送レート	自動認識	0
LAN1	IPアドレス	192.168.0.1	0
	ネットマスク	24 (255.255.255.0)	0
	セカンダリIPアドレス	なし	×
	DHCP サーバ機能	使用しない	×
	NAT機能	使用しない	×
	RIP機能		×
	・RIP送信	RIP-V1を使用する	
	・RIP受信	RIP-V1を使用する	
	転送レート	自動認識	0

1.1.3 PPPoE 接続する

適用機種 Si-R180,180B,220B,220C

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

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

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



● 設定条件

[通信事業者側]

- ユーザ認証 ID
- ユーザ認証パスワード
- LANOポートを使用する

[プライベートLAN側]

- 本装置のIPアドレス
- ネットワークアドレス/ネットマスク

[その他の条件]

 パスワードを設定する パスワード : userid(プロバイダから提示された内容)

:userpass(プロバイダから提示された内容)

- : 192.168.1.1
- : 192.168.1.0/24

この例の場合、本装置がご購入時の状態の場合、まず、かんたん設定でインターネットへの「PPPoE 接続」をク

: himitu

リックし、「PPPoEかんたん設定」画面でユーザ認証IDとユーザ認証パスワードを入力します。次に、[設定終 了] ボタンをクリックすると、通信できます(Si-R180、180Bでは購入時の状態の場合、インタフェースは、上 の図とは逆になります(LAN0→LAN1、LAN1→LAN0)。)。

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

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

こんな事に気をつけて

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

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

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

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

「PPPoEかんたん設定」ページが表示されます。

2. 「必須設定」で以下の項目を指定します。

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

■必須設定	3
ユーザ認証ID	userid
ユーザ認証バスワード	

3. 必要に応じて、「オプション設定」で以下の項目を指定します。

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

UPnP 機能

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

■オプション設定	3
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
DNSサーバ	▼自動取得
接続ネットワーク名	internet
接続先名	ISP-1
PPPoEで使用するインタフ ェース	⊙ LAN0 ◯ LAN1
常時接続機能	 ● 使用する ● 使用しない 無通信監視タイマ ● 秒
アドレス変換	 ○ 使用しない ③ マルチNAT UPnP機能 ●使用しない ○使用する
LAN0転送レート	自動認識 💙
LAN1転送レート	自動認識 💙

Si-R180、180Bでは、表示が上記の画面とは異なります。

4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。

こんな事に気をつけて

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

*** ****

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○:変更可能、×:変更不可

項目	適用される省略値	かんたん設定 での設定変更
プライベート側 IP アドレス	192.168.1.1	0
ネットマスク	24 (255.255.255.0)	0
DNSサーバアドレス	なし(自動取得)	0
自動接続	する	×
常時接続	使用する	0
無通信監視	しない	0
接続ネットワーク名	internet	0
接続先名	ISP-1	0
DHCP サーバ機能	使用する	×
・割り当て先頭IPアドレス	本装置のプライベート側IPアドレス、ネットマスクから求めたネット	
	ワークアドレス+2	
・割り当てアドレス数	253	
・DNSサーバのIPアドレス	「自動取得(※ 1)」指定時は、本装置のプライベート側 IP アドレス	
アドレス変換	マルチ NAT を使用	0
	アドレス割り当てタイマ:5分	
UPnP機能	使用しない	0
RIP機能		×
・RIP送信(LAN側)	送信しない	
・RIP 受信(LAN 側)	受信しない	
・RIP送信(PPPoE側)	送信しない	
・RIP 受信(PPPoE側)	受信しない	
スタティック経路		×
・LAN側	なし	
・PPPoE側	デフォルトルートを設定する(メトリック値:1)	
LAN0転送レート	自動認識	0
LAN1転送レート	自動認識	0
インタフェース	Si-R180、180B:LAN0、Si-R180、180B以外:LAN1	○ (※2)
ヘッダ圧縮	VJ-Compression:使用しない	×
MTUサイズ	1454	×
MSS書き換え	使用する(1414バイト)	×

※1) DNS サーバの IP アドレスを「自動取得」にした場合は、ProxyDNS 情報が以下のように設定されます。 「順引き情報一覧」

1.000		
•	優先順位	: 1
•	ドメイン	: *
	タイプ	:すべて
	送信元IPアドレス/マスク	: any
•	動作	:接続先のDNSサーバへ問い合わせる
•	ネットワーク名	: internet
「逆	引き情報一覧」	
•	優先順位	: 1
•	ネットワークアドレス	: any
•	動作	:接続先のDNSサーバへ問い合わせる
•	ネットワーク名	: internet
Si_P	180 180B は変更できません	

※2) Si-R180、180Bは変更できません。

1.1.4 CATV インターネットに接続する

適用機種 Si-R180,180B,220B,220C

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

※ヒント —

◆ ケーブルモデムとは?

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

本装置を使った CATV インターネット接続は、CATV 事業者が提供するインターネット接続サービスをプライ ベート LAN 上の複数のパソコンから利用するための接続形態です。本装置と CATV 事業者が提供するケーブルモ デムを接続することで、プライベート LAN 上のパソコンからインターネット接続サービスを利用できます。 本装置のアドレス変換機能が CATV 事業者側のネットワークと利用者側のプライベート LAN との間で動作し、プ ライベート LAN 側の IP アドレスを外部から隠すため、セキュリティが確保できます。

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

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



● 設定条件

[CATV 事業者側]

- LAN1 ポートを使用する
- IPアドレス

DNSサーバ

- ネットワークアドレス/ネットマスク
- デフォルトルータ

: 172.16.184.0/24 : 172.16.184.100

: 172.16.184.33

: 192.10.10.10

【プライベートLAN側】

• IPアドレス

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

こんな事に気をつけて

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

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

- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- 1. かんたん設定メニューでLAN間接続の「プライベートLAN構築」をクリックします。

→ 192.168.1.1

→24 (255.255.255.0)

「プライベートLAN構築かんたん設定」ページが表示されます。

2. 「必須設定」で以下の項目を指定します。

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

■必須設定	3
グローバル側IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 172.16.184.33 ネットマスク 24 (255.255.255.0)
ブライベート側IPアドレス	IPアドレス 192.168.1.1 ネットマスク 24 (255.255.25.0) マ
グローバル側インタフェース	⊙LAN0 ○LAN1

3. 「オプション設定」で以下の項目を指定します。

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

■オプション設定		3
デフォルトルータ	172.16.184.100	
DNSサーバアドレス	192.10.10.10	
DHCPサーバ	●使用しない●使	用する
	デフォルトルータ広 報	192.168.1.1
	DNSサーバ広報	192.10.10.10
	ドメイン名広報	

4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。

1.1.5 インターネットへ ISDN 接続する

適用機種 Si-R220B,220C

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

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

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



● 設定条件

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

こんな事に気をつけて

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

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

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

• IPアドレス

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

「インターネットへISDN接続かんたん設定」ページが表示されます。

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

2. 「必須設定」で以下の項目を指定します。

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

■必須設定	
接続先の電話番号	03-1234-5678
ユーザ認証ID	userid
ユーザ認証バスワード	•••••

3. 必要に応じて、「オプション設定」で以下の項目を指定します。

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

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

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

補足 0を指定した場合、回線の自動切断は行いません。

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

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

- ・ 接続ネットワーク名
 ・ internet(接続するネットワークの名称を半角英数字8文字以内で入力
 します。接続先を区別するための任意の名称を指定します。)
- 接続先名 → ISP-1 (プロバイダの名称を半角英数字8文字以内で入力します。接続先 を区別するための任意の名称を指定します。)
- アドレス変換 →1つのグローバルアドレスを使って、複数台のパソコンからネット ワークにアクセスする場合は、"マルチ NAT"を選択します。
 WPnP機能 →アドレス変換で"マルチ NAT"を選択した場合だけ設定します。UPnP 対応装置やUPnP対応アプリケーションプログラムを使用する場合に

"使用する"を選択します。

• MP

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

こんな事に気をつけて

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

• かんたんフィルタ →初期値は"使用しない"。

■オプション設定	3
IPアトレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
DNSサーバ	☑自動取得
接続先の電話番号2	
接続先の電話番号3	
常時接続機能	 使用する 使用しない 無通信監視タイマ 60 秒 課金単位時間 0
接続先ネットワーク名	internet
接続先名	ISP-1
アドレス変換	 ● 使用しない ● マルチNAT ■ UPnP機能 ● 使用しない ● 使用しない
MP	○使用する ④使用しない
かんたんフィルタ	○使用する ④使用しない

4. 設定が終了したら、[設定終了] ボタンをクリックします。 再起動後に、通信できる状態になります。

<u>▲</u>注意・

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

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

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

インターネットに接続できた場合は、弊社のページが表示されます。

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

どとント

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○:変更可能、×:変更不可

項目	適用される省略値	オプション設定 での設定変更
自動ダイヤル	使用する	×
すべてのデータ通信の着信	許可しない	×
常時接続機能	使用しない	0
無通信監視タイマ	60秒	0
課金単位時間	なし	0
接続ネットワーク名	internet	0
接続先名	ISP-1	0
接続先のサブアドレス	なし	×
DHCPサーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数 ・DNS サーバの IP アドレス	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス+ 2 64 「自動取得(※1)」指定時は、本装置のIPアドレス	×
アドレス変換	マルチNATを使用 アドレス割り当てタイマ:5分	0
UPnP機能		0
MP機能(※2)	使用しない	0
かんたんフィルタ(※3)	使用する	0
RIP機能 ・RIP送信(LAN側) ・RIP受信(LAN側) ・RIP送信(WAN側) ・RIP受信(WAN側)	送信しない 受信しない 送信しない 受信しない	X
スタティック経路 ・LAN 側 ・WAN 側	なし デフォルトルートを設定する(メトリック値:1)	×
データ圧縮	LZS:なし	×
ヘッダ圧縮	VJ-Compression:使用する IP ヘッダ圧縮:使用しない	×
IPv6 経路	使用しない	×
ブリッジ	使用しない	×
課金制御	上限 3,000円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

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

[順]	引き情報一覧」	
•	優先順位	: 1
•	ドメイン	: *
	タイプ	:すべて
	送信元IPアドレス/マスク	: any
•	動作	:接続先のDNSサーバへ問い合わせる
•	ネットワーク名	: internet

「逆引き情報一覧」

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

:1

- ネットワーク名 : internet
- ※2) MP機能を「使用する(自動)」にした場合は、以下のように設定されます。
 - :する トラフィックによる増減
 - 回線増加条件 :回線使用率(90%)、猶予時間(10秒)
 - 回線削除条件 :回線使用率(40%)、猶予時間(60秒)
- ※3)かんたんフィルタを「使用する」にした場合は、以下のように設定されます。
 - :する トラフィックによる増減
 - Windows[®] 95 / 98 / Me / 2000、Windows NT[®]で Microsoft Network を使用する場合に、NetBIOS over TCPが使用する TCP および UDP のサービスポート 137 から 139 を遮断するフィルタを設定しま す。
 - ping (ICMP echo) や syslog、time、SNTP で使用するプロトコルを抑止するフィルタを設定します。 なお、回線が接続状態の場合はそれぞれのパケットを通過させます。
 - Windows[®] 2000 から本装置を経由してインターネットへ接続する場合、Windows[®] 2000 が送信する予 期しないDNSパケットによって自動発信してしまう場合があります。この問題を回避するために、 ProxyDNS 情報に問い合わせタイプが SOA(6)、SRV(33)のDNS パケットを破棄するフィルタ、お よびホストデータベース情報にIPアドレス「127.0.0.1」でホスト名「localhost」の情報を設定します。

1.1.6 インターネットへ専用線接続する

適用機種 Si-R220B,220C

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

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

ここでは、以下の条件でOCNエコノミーを利用する場合を例に説明します。



● 設定条件

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

こんな事に気をつけて ―

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

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

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

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

「インターネットへ専用線接続かんたん設定」ページが表示されます。

2. 「必須設定」で以下の項目を指定します。

- IPアドレス → 172.16.184.33 (割り当てられたホストアドレスの先頭)
- ネットマスク →29 (255.255.258)
- 使用する回線速度 → 128Kbps
- DNS サーバ → 192.10.10.10 (OCN から提示された IP アドレス)

■必須設定	3
IPアドレス	172.16.184.33
ネットマスク	29 (255.255.255.248) 🗸
使用する回線速度	O64Kbps ⊙128Kbps
DNSサーバ	192.10.10.10

3. 必要に応じて、「オプション設定」で以下の項目を指定します。

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

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

UPnP 機能

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

■オプション設定	オプション設定	
接続ネットワーク名	internet	
接続先名	ISP-1	
ドメイン名	domain.ocn.ne.jp	
アドレス変換	 ● 使用しない ● マルチNAT グローバルアドレス アドレス個数 1 個 UPnP機能 ●使用しない ●使用する 	

4. 設定が終了したら、[設定終了] ボタンをクリックします。 再起動後に、通信できる状態になります。

心 ヒント —

◆ OCN エコノミーなら「マルチ NAT」機能が便利

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

◆ マルチ NAT

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

NAT機能は、プライベートアドレスとグローバルアドレスを1対1に対応付けるもので、NAT機能を介して通信できるパソコンの台数は割り当てられるIPアドレスと同じになります。このため、プロバイダと端末型ダイ ヤルアップ契約の場合、1つしかIPアドレスが割り当てられないので、同時接続台数が1台に制限されます。 マルチNATは、この問題を解決するために1対1の対応付けから、多対1の対応付けを実現した機能です。IP アドレスとポート番号を組み合わせたIP情報の割り当てを行うことによって、プライベートアドレスとグ ローバルアドレスとを多対1に対応付け、同時に複数のパソコンからの利用が可能となります。

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

インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

WWW ブラウザで URL 「http://www.fujitsu.com」を入力します。
 インターネットに接続できた場合は、弊社のページが表示されます。

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

〇:変更可能、×:変更不可

項目	適用される省略値	オプション設定 での設定変更
ブロードキャストアドレス	ネットワークドレス+オール1	×
接続ネットワーク名	internet	\bigcirc
DHCPサーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数	使用する 本装置の IP アドレス、ネットマスクから求めたネットワークアドレス+ 2 64	×
NAT機能	使用しない(※ 1)	0
UPnP機能	使用しない	0
かんたんフィルタ	使用しない	×
RIP機能 ・RIP送信(LAN側) ・RIP受信(LAN側) ・RIP送信(WAN側) ・RIP受信(WAN側)	送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN 側 ・WAN 側	なし デフォルトルートを設定する(メトリック値:1)	×
データ圧縮	LZS:なし	×
ヘッダ圧縮 	VJ-Compression:使用する IP ヘッダ圧縮:使用しない	×
IPv6 経路	使用しない	×
ブリッジ	使用しない	×

※1)マルチNAT使用時のアドレス割り当てタイマは5分を設定します。

1.1.7 オフィスへ ISDN 接続する

適用機種 Si-R220B,220C

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

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

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





● 設定条件

• DHCPサーバ機能は使用しない

[東京事業所]

•	電話番号	: 03-7777-7777
•	ユーザ認証 ID とユーザ認証パスワード	
	発信	: tokyo、tokyopass
	着信	: kawasaki, kawapass
•	LAN 側のネットワークアドレス/ネットマスク	:192.168.1.0/24(本装置のIPアドレス:192.168.1.1)
[]	崎事業所]	
•	電話番号	: 044-999-9999
•	ユーザ認証 ID とユーザ認証パスワード	
	発信	: kawasaki, kawapass
	着信	: tokyo, tokyopass
•	LAN 側のネットワークアドレス/ネットマスク	:192.168.2.0/24(本装置のIPアドレス:192.168.2.1)

こんな事に気をつけて

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

■ 参照 Si-Rシリーズ Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P19)

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

東京事業所の本装置を設定する

1. かんたん設定でオフィスへの「ISDN 接続」をクリックします。

「オフィスへISDN接続かんたん設定」ページが表示されます。

2. 「必須設定」で以下の項目を指定します。

- 接続先の電話番号 →044-999-9999
 - ユーザ認証ID(発信) → tokyo
 - → tokyopass
 - ユーザ認証パスワード(発信)
- ユーザ認証ID(着信) → kawasaki
- ユーザ認証パスワード(着信) → kawapass
 - → 192.168.1.1(既存の LAN につなぐときは適宜変更)
 - →24(255.255.255.0)(既存のLANにつなぐときは適宜変更)

→192.168.2.1 (接続先となる本装置のネットワークアドレス)

相手ルータのIPアドレス

IPアドレス

ネットマスク

- 相手ルータのネットマスク →24(255.255.255.0)(接続先となる本装置のネットマスク)
- ■必須設定 3 接続先の電話番号 044-999-9999 ユーザ認証ID(発信) tokyo ユーザ認証バスワード(発信) •••••••• ユーザ認証ID(着信) kawasaki ユーザ認証バスワード(着信) ••••••• IPアドレス 192.168.1.1 ネットマスク 24 (255,255,255,0) ~ 相手ルータのIPアトレス 192.168.2.1 相手ルータのネットマスク 24 (255.255.255.0) ¥

3. 「オプション設定」で以下の項目を指定します。

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

ます。接続先を区別するため任意の名称を指定します。)

オプション設定	
DHCPサーバ	 ● 使用しない ● 使用する DNSサーバ広報
常時接続機能	 ○ 使用する ③ 使用しない 無通信監視タイマ 0 秒 課金単位時間 0
接続ネットワーク名	kaisya
接続先名	kawasaki

4. 設定が終了したら、[設定終了] ボタンをクリックします。 再起動後に、通信できる状態になります。

川崎事業所の本装置を設定する

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

補足 設定が終わったら、[設定終了] ボタンをクリックします。

「必須設定」

- 接続先の電話番号 →03-7777-7777
- ユーザ認証 ID(発信) → kawasaki
- ユーザ認証パスワード(発信) → kawapass
- · ユーザ認証ID(着信) → tokyo
- ユーザ認証パスワード(着信) →tokyopass
- IPアドレスネットマスク
- →24 (255.255.255.0)

→ tokyo

→192.168.1.1(接続先となる本装置のネットワークアドレス)

→192.168.2.1 (本装置のLAN側のIPアドレス)

→24(255.255.255.0)(接続先となる本装置のネットマスク)

「オプション設定」

• 接続ネットワーク名

• 相手ルータのIPアドレス

相手ルータのネットマスク

- →kaisya(接続するネットワークの名称)
- 接続先名
通信する

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

▲注意 -

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



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

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

〇:**変更可能、×:変更不可**

項目	適用される省略値	オプション設定 での設定変更
自動ダイヤル	使用する	×
サブアドレス	なし	×
不特定相手着信	許可しない	×
常時接続機能	使用しない	0
無通信監視タイマ	60秒	0
課金単位時間	なし	0
接続ネットワーク名	localnet	0
接続先名	OFFICE-1	0
該当接続先への着信許可	許可する	×
DHCP サーバ機能	使用する	0
・割り当て先頭IPアドレス	本装置の IP アドレス、ネットマスクから求めたネットワークアドレス+	
・割り当てアドレス数	2	
	64	
NAT 機能	使用しない	×
MP機能	使用しない	0
かんたんフィルタ	使用しない	×
RIP機能		×
・RIP送信(LAN側)	送信しない	
・RIP 受信(LAN 側)	受信しない	
・RIP送信(WAN側)	送信しない	
・RIP 受信(WAN側)	受信しない	
スタティック経路		×
・LAN 側	なし	
・WAN 側	相手ルータのIPアドレス、ネットマスクを元にスタティックルートを設 定する	
データ圧縮	LZS:なし	0
ヘッダ圧縮	VJ-Compression:使用する IP ヘッダ圧縮:使用しない	0
IPv6 経路	使用しない	×
ブリッジ	使用しない	×
課金制御	上限 3,000円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

1.1.8 オフィスへ専用線接続する

適用機種 Si-R220B,220C

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

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

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

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



● 設定条件

[本社]

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

[支社]

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

こんな事に気をつけて

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

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

本社の本装置を設定する

かんたん設定でオフィスへの「専用線接続」をクリックします。
 「オフィスへ専用線接続かんたん設定」ページが表示されます。

2. 「必須設定」で以下の項目を指定します。

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

→ 192.168.2.1 (接続先となる本装置の IP アドレス)

■必須設定	3
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
相手ルータのIPアドレス	192.168.2.1
相手ルータのネットマスク	24 (255.255.255.0)
使用する回線速度	◯64Kbps ⊙128Kbps

3. 「オプション設定」で以下の項目を指定します。

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

■オプション設定	3
接続ネットワーク名	kaisya
接続先名	kawasaki
DHCPサーバ	 ● 使用しない ● 使用する DNSサーバ広報

4. 設定が終了したら、[設定終了] ボタンをクリックします。 再起動後に、通信できる状態になります。

支社の本装置を設定する

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

補足 設定が終わったら、[設定終了] ボタンをクリックします。

「必須設定」

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

→128Kbps

「オプション設定」

• ネットマスク

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

◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○:変更可能、×:変更不可

項目	適用される省略値	オプション設定 での設定変更
接続ネットワーク名	localnet	0
DHCPサーバ機能 ・割り当て先頭アドレス ・割り当てアドレス数	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス+ 2 64	0
NAT機能	使用しない	×
かんたんフィルタ	使用しない	×
RIP機能 ・RIP送信(LAN側) ・RIP受信(LAN側) ・RIP送信(WAN側) ・RIP受信(WAN側)	送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・LAN 側 ・WAN 側	なし 相手ルータのIPアドレス、ネットマスクを元にスタティックルートを設 定する	×
データ圧縮	LZS:なし	\bigcirc
ヘッダ圧縮	VJ-Compression:使用する IPヘッダ圧縮:使用しない	0
IPv6 経路	使用しない	x
ブリッジ	使用しない	×

1.2 LAN をネットワーク間接続する

適用機種 全機種

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

こんな事に気をつけて

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

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



[その他の条件]

:使用する
:設定する
:TIMEプロトコル
: 192.168.0.20

☆ ヒント ───

◆ TIMEプロトコル、SNTPとは?

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

こんな事に気をつけて

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

LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →192.168.0.1
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報 🥑				
IPv4	●使用する●使用しない			
	 ○ DHCPで自動的に取得す ○ 指定する 	5		
IPアドレス		192.168.0.1		
		24 (255.255.255.0)		
	フロートキャストアトレス	ネットワークアドレス+オール1 💌		

- 5. [保存] ボタンをクリックします。
- 6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

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

RIP情報		3		
RIP送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する			
RIP受信	●受信しない ● V1で受信する ● V2、V2(Multicast)で受信する			
《 RIP 送信時は加算するメトリック値を設定してください。》 メトリック値				

- 8. [保存] ボタンをクリックします。
- 9. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

10. 以下の項目を指定します。

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

<スタティック経路情報入力フィールド>						
	◎ デフォルトルート					
ネ		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 192.168.0.5 			
ット	0	ネットワーク指定				
י <mark>ר</mark>		あて先IPアドレス				
ーク		あて先アドレスマス ク	0 (0.0.0)			
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 			
メトリック値 厚	1	v				
曖 先 度	0					

11. [追加] ボタンをクリックします。

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

<スタティック経路情報入力フィールド>						
	○デフォルトルート					
ネ		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 192.168.0.5 			
ット	•	ネットワーク指定				
ר כ		あて先IPアドレス	192.168.2.0			
ー ク		あて先アドレスマス ク	24 (255.255.255.0)			
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 192.168.0.10 			
メトリック値	1	v				
優先度	0					

- 13. [追加] ボタンをクリックします。
- **14.** IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP 情報」が表示されます。

DHCP機能 →使用しない

■DHCP情報						
	⊙ 使用しない					
	0	ルー機能を使用する				
		DHCPサーバIPアドレ		,ス1		
		DHCPサーバIPアドL		,ス2		
		MACアドレスチェック		,	 □ホストデータベース □ AAA 参照するAAA情報 	
	0	サーバ機	能を使用す	る	·	
		割当て先 ス	頭IPアドレ			
		割当てア	ドレス数	32		
		リース期		1	8 💌	
	デフォル 報 DNSサ ーバ広 報 ドメイン名	トルータ広				
DHCP		DNSサ	プライマリ			
機能		報	セカンダリ			
		ドメイン者	る広報			
		TIMEサー	-バ広報			
		NTPサー	バ広報	R		
		WINSサ	プライマリ			
		1	報	セカンダリ		
		SIPサー バ広報	記述形式	⊙ト [*]	メイン名 OIPアドレス	
			ブライマリ			
			セカンダリ			
		MACアドレスチェッ ク		□ 7	マストデータベース	
				ΠA	AA 参照するAAA情報	
		※"割当で ークアドレ	て先頭アドレ ,ス内である	ス"カ ことを	「本装置のIPアドレスと同じネットワ 「確認してください。	

16. 【保存】ボタンをクリックします。

LAN1 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

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

■IPアドレス情報									
IPv4	●使用する ●使用しない								
IP アド レス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 								

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

7. 以下の項目を指定します。

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

RIP情報	3
RIP送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する
RIP受信	○受信しない ●V1で受信する ●V2、V2(Multicast)で受信する
《 RIP 送信時は加算する <mark>メトリック値</mark>	るメトリック値を設定してください。》 □ ▼

8. [保存] ボタンをクリックします。

9. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

10. 以下の項目を指定します。

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

DHC	P情報		3					
	○使用しない							
	⊙リレー機i	能を使用する	3					
	DHCPサ	ーバIPアドレ	,ス1					
	DHCPサ	ーバIPアドレ	,72					
	MAC7H	レスチェック	□ホストデータベース □ AAA 参照するAAA情報					
	⊙ サーバ機	能を使用す	3					
	割当て芽 ス	・頭IPアドレ	192.168.1.2					
	割当てア	ドレス数	253					
	リース期	間	1 •					
	デフォル 報	トルータ広	192.168.1.1					
DHCP	DNSサ	プライマリ	192.168.1.1					
機能	報	セカンダリ						
	ドメインキ	名広報						
	TIMEサ-	ーバ広報						
	NTPサー	バ広報						
	WINSサ	プライマリ						
	報	セカンダリ						
		記述形式	●ドメイン名 ○IPアドレス					
	SIPサー バ広報	プライマリ						
	- 1/2-5TK	セカンダリ						
	MACZE	レスチェッ	□ホストデータベース					
	ク		□AAA 参照するAAA情報					
	※"割当 ークアドレ	て先頭アドレ ノス内である	ス"が本装置のIPアドレスと同じネットワ ことを確認してください。					

11. 【保存】ボタンをクリックします。

自動時刻を設定する

- **1. 設定メニューの基本設定で「装置情報」をクリックします**。 「装置情報」ページが表示されます。
- 「タイムサーバ情報」をクリックします。
 「タイムサーバ情報」が表示されます。
- 3. 以下の項目を指定します。
 - タイムサーバ機能 →使用する
 - サーバ設定 →設定する
 プロトコル → TIME プロトコル
 - タイムサーバIPアドレス → 192.168.0.20



- 4. [保存] ボタンをクリックします。
- 5. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

LAN をネットワーク間接続する

1.3 IPv4のネットワークに IPv6 ネットワークを追加する

適用機種 全機種

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



● 設定条件

[LAN-A側]

プレフィックス/プレフィックス長

[LAN-B側]

プレフィックス/プレフィックス長

: 2001:db8:1111:1000::/64

: 2001:db8:1111:1001::/64

こんな事に気をつけて

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

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

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

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

IP	√6基	本情報											3
IPv6	0	使用しない⊙使用	する										
インタフェースID	 ● 自動 ○ 指定する 												
	アド	レスまたはプレフ	ィックス		Valid 期限	Life 有	time ‡	無期	限	Pref. Life 期限有	etime ∄	無期限	フラ グ
IPv6	200	1:db8:1111:1000::			30		Β	*		7	B	*	c0
アトレス					30		Β	¥		7	B	¥ 🗌	c0
					30		Β	*		7	B	*	c0
					30		Β	۷		7	B	¥ 🗌	c0
	0 0	送信しない 送信する											
		最大送信間隔	600	Ŧ	少								
		最小送信間隔	200	Ŧ	少								
ルー		Router Lifetime	1800	Ŧ	少								
タ広報		MTU]									
		Reachable Time	0	3	ジ秒								
		Retrans Timer	0	3	ジ秒								
		Cur Hop Limit	64]									
		フラグ	00										

- 5. [保存] ボタンをクリックします。
- **6.** IPv6 関連の設定項目の「IPv6 RIP 情報」をクリックします。 「IPv6 RIP 情報」が表示されます。

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

■IPv6 RIP情報		3
RIP送信	 ○ 送信しない ○ 送信する メトリック値 ○ ▼ 	
RIP受信	○受信しない⊙受信する	
	集約経路	破棄経路 設定
	 ○デフォルトルート ◎ネットワーク指定 	☑設定す る
集約経路送信		■ 設定する
		■ 設定す る
		■ 設定する
サイトローカルブレ フィックス	○交換しない ◎交換する	

8. [保存] ボタンをクリックします。

LAN1 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。
 「LAN1 情報(物理 LAN)」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、
 「LAN1 情報(VLAN)」ページが表示されます。
- 3. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

- IPv6
- インタフェースID →自動
- IPv6アドレス アドレスまたはプレフィックス →2001:db8:1111:1001::

→使用する

ルータ広報 →送信する

IP	Pv6基本情報 3												
IPv6	01	使用しない⊙使用	する										
インタフェースID	 ● 自動 ● 指定する 												
	アド	レスまたはプレフ	ィックス		Valid 期限 ³	Life [:] 有	time ჭ	無期	限	Pref. Life 期限有	etime 魚	₩期限	フラ グ
IPv6	200	1:db8:1111:1001::			30		Β	۷		7	B	*	c0
アトレス					30		Β	*		7	B	~	c0
					30		Β	۷		7	В	v	c0
					30		Β	*		7	B	¥ 🗌	c0
	0 0	送信しない 送信する											
		最大送信間隔	600	私	<u>ل</u>								
		最小送信間隔	200	利	<u>ل</u>								
ルー		Router Lifetime	1800	利	り								
タム報		MTU											
in a		Reachable Time	0	3	り秒								
		Retrans Timer	0	2	り秒								
		Cur Hop Limit	64]									
		フラグ	00]									

- 5. [保存] ボタンをクリックします。
- **6.** IPv6 **関連の設定項目の「IPv6 RIP 情報」をクリックします**。 「IPv6 RIP 情報」が表示されます。

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

■IPv6 RIP情報		3
RIP送信	 ○ 送信しない ○ 送信する メトリック値 ○ ▼ 	
RIP受信	○受信しない ⊙受信する	
	集約経路	破棄経路 設定
	 ●デフォルトルート ●ネットワーク指定 	☑ 設定す る
集約経路送信		☑設定す る
		☑設定す る
		☑設定す る
サイトローカルブレ フィックス	○交換しない●交換する	

- 8. [保存] ボタンをクリックします。
- 9. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

1.4 プライベートLANを構築する

適用機種 全機種

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

こんな事に気をつけて

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

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



: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

● 設定条件

[事務所側 LAN]

転送レート

- LANOポートを使用する
- :自動認識

: 1

:5分

- 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 アドレス個数 アドレス割当てタイマ

[会議室側 LAN]

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

こんな事に気をつけて

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

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

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 4. 以下の項目を指定します。
 - IPv4

- →使用する
- IPアドレス → DHCPで自動的に取得する

■IPアドレス情報 []					
IPv4	⊙使用する○使用しない				
IP アド レス	 ● DHCPで自動的に取得する ● 指定する IPアドレス ネットマスク 2 (192.0.0) ブロードキャストアドレ ス 				

- 5. [保存] ボタンをクリックします。
- **6.** IP 関連の設定項目の「RIP 情報」をクリックします。 「RIP 情報」が表示されます。

プライベート LAN を構築する

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

RIP情報	3
RIP送信	 ●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する
RIP受信	●受信しない ●V1で受信する ●V2、V2(Multicast)で受信する
《 RIP 送信時は加算する メトリック値	るメトリック値を設定してください。》

- 8. [保存] ボタンをクリックします。
- 9. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

10. 以下の項目を指定します。

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

■NAT情報	3
NATの使用	○使用しない ○NAT ⊙マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません
クローバルアドレス	
アトレス個数	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
アトレス割当てタイマ	5 分 💙
NATセキュリティ	○通常 ⊙ 高い

こんな事に気をつけて

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

11. [保存] ボタンをクリックします。

プライベート LAN を構築する

LAN1 情報を設定する

こんな事に気をつけて

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

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

2. 以下の項目を指定します。

• インタフェース

	<lan情報追加フィールド></lan情報追加フィールド>
インタフェース	物理LAN 🗸

→物理LAN

3. [追加] ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

4. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

5. 以下の項目を指定します。

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

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス 		

- 6. [保存] ボタンをクリックします。
- **7. IP 関連の設定項目の「DHCP 情報」をクリックします**。 「DHCP 情報」が表示されます。

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

■DHCP情報				
	○ 使用しない			
	○リレー機能を	リレー機能を使用する		
	DHCPサーバ	NPアドレス1		
	DHCPサーバ	NPアドレス2		
	MACアドレス	チェック	 □ホストデータベース □ AAA 参照するAAA情報 	
	⊙ サーバ機能を	使用する		
	割当て先頭 ス	Pアドレ 192.	168.1.2	
	割当てアドレ	ス数 253		
	リース期間	1		
	デフォルトル・ 報	一夕広 192.	168.1.1	
DHCP	DNSサ ブラ	ライマリ 192.	168.1.1	
機能	報 セ	<u> ウンダリ</u>		
	ドメイン名広	報		
	TIMEサーバ	広報		
	NTPサーバル	な報		
	WINSサ ブラ	ライマリ 📃		
	報 セ	<u> ウンダリ</u>		
	記	述形式 ⊙ト	メイン名 OIPアドレス	
	SIPサー ブラ バ広報	ライマリ 📃		
	セ	<u> ケンダリ</u>		
	MACアドレス	Fry 🗖	ホストデータベース	
	ク	□ A	AAA 参照するAAA情報	
	※"割当て先」 ークアドレスP	頭アドレス"た りであることで	『本装置のIPアドレスと同じネットワー を確認してください。	

- 9. [保存] ボタンをクリックします。
- 10. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

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

RIP情報	3	
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する 	
RIP受信	●受信しない ●V1で受信する ●V2、V2(Multicast)で受信する	
《 RIP 送信時は加算するメトリック値を設定してください。》 <mark>メトリック値</mark>		

12. 【保存】ボタンをクリックします。

13. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

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

こんな事に気をつけて

本装置のDHCPサーバ機能を使用する場合は、以下の点に注意してください。

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

1.5 インターネットへ専用線で接続する

適用機種 Si-R220B,220C,370,570

ここでは、以下の設定条件で専用線を利用する場合を例に説明します。

こんな事に気をつけて

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

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



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート(Si-R220B、220C の場合) で OCN エコノミー専用線(128Kbps)を使用する
- LAN0を使用して、新規にLANを構築する
- OCN 側の DNS サーバを使用 : 192.10.10.10
- OCN より提示されたドメイン名 : domain.ocn.ne.jp
- 接続するパソコンの台数はOCNから割り当てられたIPアドレスよりも少ない
- 割り当てIPアドレス
 ネットワークアドレス/ネットマスク
 ホストアドレス
 ブロードキャストアドレス
 エ72.16.184.32/29
 エ72.16.184.33~172.16.184.38
 ブロードキャストアドレス
 エ72.16.184.39
 本装置のLAN側のIPアドレス
 172.16.184.33
 internet

こんな事に気をつけて

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

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

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

WAN0 情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →専用線
 <WAN情報追加フィールド>
 回線インタフェース 専用線 ▼
- 【追加】ボタンをクリックします。
 「WAN0 情報(専用線)」ページが表示されます。
- **4. 「基本情報」をクリックします。** 「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - ポート →スロット0-0
 - 回線速度 → 128Kbps

■基本情報	3
ボート	スロット 0-0 💌
回線速度	128Kbps 💙

Si-R220B、220Cでは、ポートは固定です。

6. [保存] ボタンをクリックします。

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →172.16.184.33
 ネットマスク →29 (255.255.248)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
IPアドレス	 O DHCPで自動的に取得する 指定する IPアドレス オットマスク 29 (255.255.245) ブロードキャストアドレ ス ネットワークアドレス 	8) 、 +オール1 、	

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

7. 以下の項目を指定します。

● DHCP機能		→サーバ機能を使用する
割当て先頭IP	アドレス	→ 172.16.184.34
割当てアドレ	ス数	→ 6
リース期間		→1日
デフォルトル・	ータ広報	→ 172.16.184.33
DNSサーバ広	報	
プライマリ		→ 192.10.10.10
セカンダリ		→指定しない
ドメイン名広	報	→domain.ocn.ne.jp
TIMEサーバ広	云報	→指定しない
NTPサーバ広	報	→指定しない
WINSサーバ』	広報	→指定しない
SIPサーバ広幸	艮	→指定しない
MACアドレス	チェック	→指定しない

■DHCP情報					2		
	○ 使用しない			-			
	0	リレー機能	能を使用する	5			
		DHCPサ	ーバIPアドレ	,ス1			
		DHCPサ	ーバIPアドレ	,ス2			
		мас7۴	レスチェック	,	 □ホストデータベース □ AAA 参照するAAA情報 		
	0	サーバ機	能を使用す	3			
		割当て先 ス	頭IPアドレ	172.1	6.184.34		
		割当てア	ドレス数	6			
		リース期		1			
		デフォル 報	~ルータ広	172.1	6.184.33		
DHCP		DNSサ	ブライマリ	192.1	0.10.10		
機能			報	セカンダリ			
		ドメイン者	広報	doma	in.ocn.ne.jp		
		TIMEサー	-バ広報				
		NTPサー	バ広報				
		WINSサ	プライマリ				
			報	セカンダリ			
			記述形式	<u>⊛</u> ۲.	メイン名 OIPアドレス		
		SIPサー バ広報	プライマリ				
			セカンダリ				
		мастн	レスチェッ	□ 7	マストデータベース		
		ク ク		ΠA	AA 参照するAAA情報		
		※ [•] 割当で ークアドレ	「先頭アドレ ス内である	ス"カ ことを	「本装置のIPアドレスと同じネットワ 「確認してください。		

8. [保存] ボタンをクリックします。

相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - • ネットワーク名
 → internet

<ネットワーク情報追加フィールド>		
ネットワーク名	internet	

4. [追加] ボタンをクリックします。

「ネットワーク情報(internet)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →デフォルトルート **→**1
 - メトリック値
 - 優先度

→0



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。 「接続先情報」が表示されます。
- 10. 以下の項目を指定します。
 - 接続先名 →ISP-1
 - 接続先種別 →専用線接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

使用インタフェース	WAND 💌		
DNSサーバ	192.10.10.10		

- 13. 【保存】ボタンをクリックします。
- 14. 画面左側の [再起動] ボタンをクリックします。

設定した内容が有効になります。

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

1.6 インターネットへ PPPoE で接続する

適用機種 全機種

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

こんな事に気をつけて

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

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



● 設定条件

[通信事業者側]

- ユーザ認証 ID
- ユーザ認証パスワード
- LANOポートを使用する

[プライベートLAN側]

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

: userid (プロバイダから提示された内容)

:userpass(プロバイダから提示された内容)

こんな事に気をつけて

- ・ 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。
- 参照 Si-Rシリーズ Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.19)
- ・ 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- PPPoE で利用する相手情報のMTU値は、接続先から指定されたMTU値を設定します。一般的には、1454を設定すれば問題ありません。

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

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 2. 「LAN 情報」でインタフェースがLAN0の[削除] ボタンをクリックします。 メッセージボックスに「削除していいですか?」というメッセージが表示されます。
- 3. [OK] ボタンをクリックします。

インタフェースが LAN0の定義が削除されます。

- 4. 以下の項目を指定します。
 - インタフェース

→物理LAN

	<lan情報追加フィールド></lan情報追加フィールド>
インタフェース	物理LAN 🗸

5. [追加] ボタンをクリックします。

「LAN0 情報(物理 LAN)」ページが表示されます。

6. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

7. 以下の項目を指定します。

ポート番号
 master
 backup

→基本0 →バックアップなし(Si-R180、180B以外の機種だけ指定)

転送レート →自動認識

■基本情報		
		基本 0 🖌
小「闺ち	backup	バックアップなし 💌
優先使用ボート		 ⊙ master ○ 先にリンクアップしたボート
転送レート		自動認識 💟

8. [保存] ボタンをクリックします。

LAN1 情報を設定する

こんな事に気をつけて

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

1. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 以下の項目を指定します。

• インタフェース

<lan情報追加フィールド></lan情報追加フィールド>	
インタフェース	物理LAN 🖌

→物理LAN

3. [追加] ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

4. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

5. 以下の項目を指定します。

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

■IPアドレス情報		
IPv4	⊙使用する○使用しない	
IP アド レス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.0) ▼ ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼]

- 6. [保存] ボタンをクリックします。
- **7. IP 関連の設定項目の「DHCP 情報」をクリックします**。 「DHCP 情報」が表示されます。

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

■DHCP情報		
	 ○ 使用しない ○ リレー機能を使用する 	
	MACアドレスチェック □ホストデータベース □AAA 参照するAAA情報	
	⊙ 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	
DHCP	DNSサ プライマリ 192.168.1.1	
機能	マイバム セカンダリ	
	ドメイン名広報	
	TIMEサーバ広報	
	NTPサーバ広報	
	WINSサ プライマリ	
	報 セカンダリ	
	記述形式 OFメイン名 OIPアドレス	
	SIPサー プライマリ	
	MACアドレスチェッ	
	ク □ AAA 参照するAAA情報 □	
	※"割当て先頭アドレス"が本装置のIPアドレスと同じネットワ ークアドレス内であることを確認してください。	

9. [保存] ボタンをクリックします。

相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → internet

<ネットワーク情報追加フィールド>	
ネットワーク名	internet

4. [追加] ボタンをクリックします。

「ネットワーク情報 (internet)」ページが表示されます。

5. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - MTU サイズ → 1454
 自動接続 → する
 - MTUサイズ 1454 バイト 自動接続 ●する ○しない
- 7. [保存] ボタンをクリックします。
- 8. 「PPP 関連」をクリックします。

PPP関連の設定項目と「圧縮情報」が表示されます。

9. 以下の項目を指定します。

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

■圧縮情報	3
ヘッダ圧縮 (IPCP)	■VJ ■IPヘッダ圧縮
ヘッタ圧縮 (IPV6CP)	■IPヘッダ圧縮

Si-R180、180B、260Bでは、"データ圧縮"の項目はありません。

- 10. [保存] ボタンをクリックします。
- **11.** 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

12. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

ネットワーク →デフォルトルート
 メトリック値 →1
 優先度 →0

<スタティック経路情報入力フィールド>		
ネットワーク	 ● デフォルトルート ● ネットワーク指定 あて先IPアドレス あて先アドレスマスク 0 (0.0.0) 	
メトリック値	1 •	
優先度	0	

14. [追加] ボタンをクリックします。

15. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT情報」が表示されます。

16. 以下の項目を指定します。

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

NAT情報	3
NATの使用	●使用しない●NAT●マルチNAT●静的NATのみ
グローバルアドレス	
アトレス個数	1 1個
アドレス割当てタイマ	5 分 🗸
NATセキュリティ	○通常 ⊙ 高い

こんな事に気をつけて

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

- 17. [保存] ボタンをクリックします。
- 18. IP 関連の設定項目の「IP 基本情報」をクリックします。

「IP基本情報」が表示されます。

- 19. 以下の項目を指定します。
 - MSS書き換え →使用する 書き換えサイズ → 1414

MSS書き換え	 ○ 使用しない ③ 使用する
	書き換えサイズ 1414 バイト

20. [保存] ボタンをクリックします。
21. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

22. 以下の項目を指定します。

- 接続先名
- →ISP-1
- 接続先種別 → PPPoE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

23. [追加] ボタンをクリックします。

PPPoE 接続の設定項目と「基本情報」が表示されます。

24. 以下の項目を指定します。

- 使用インタフェース → LANO
- DNSサーバ →指定しない

使用インタフェース	
DNSサーバ	

25. [保存] ボタンをクリックします。

26. PPPoE 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

•	送信認証情	報		
	認証ID		→userid	
	認証パスワード		→ userpass	
Γ	PPP情報			3
送信認証情報	認証ID	userid		
	达1668进1月节	認証バスワード	•••••	7

28. [保存] ボタンをクリックします。

ProxyDNS情報、URLフィルタ情報を設定する

- **1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- **2. 「順引き情報」をクリックします**。 「順引き情報」が表示されます。
- 3. 以下の項目を指定します。
 - ドメイン名
 - タイプ →すべて
 - 送信元IPアドレス →指定しない
 - 動作 →接続先のDNS サーバへ問い合わせる

→ *

ネットワーク名 → internet



- 4. [追加] ボタンをクリックします。
- **5. 「逆引き情報」をクリックします**。 「逆引き情報」が表示されます。

動作

6. 以下の項目を指定します。

• ネットワークアドレス

→すべて →接続先のDNS サーバへ問い合わせる

ネットワーク名

→internet



- 7. [追加] ボタンをクリックします。
- 8. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

1.7 インターネットヘデータ通信カードを使用して 接続する

適用機種 Si-R240,240B

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

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

こんな事に気をつけて

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

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



● 設定条件

[Internet 側]

- データ通信カード装着 SLOT
- 認証ID
- 認証パスワード
- 電話番号
- 無通信監視タイマ
- 強制切断

[プライベートLAN側]

- : SLOT0
- : 通信事業者から提示された内容
- : 通信事業者から提示された内容
- :通信事業者から提示された内容
- :無通信監視時間を1分とする
- : 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
- 本装置のIPアドレス : 192.168.1.1
- ネットワークアドレス/マスク : 192.168.1.0/24

こんな事に気をつけて

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

● 参照 Si-Rシリーズ Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P19)

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

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

● 参照 Si-Rシリーズ メッセージ集「課金制御機能による強制切断」

課金制御機能(強制切断)により切断した場合、以降の手動および自動発信を禁止します。

接続するにはデータ通信カードのアカウント情報のクリア(clear cardmodem account)を実行する必要があります。 ・ パケット数による強制切断のパケット数は、累計送受信バイト数(PPPパケット長)を128で割った値を用います。

パケット数による強制切断のパケット数は目安であり、通信事業者でのパケット数と異なる場合があります。

WAN0 情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →データ通信カード

<wan情報追加フィールド></wan情報追加フィールド>		
回線インタフェース	データ通信カード 🔽	

3. [追加] ボタンをクリックします。

「WAN 情報(データ通信カード)」ページが表示されます。

- 4. 以下の項目を指定します。
 - ポート →スロット0-0

■基本情報	報	3
ボート	スロットロー0 💌	

5. [保存] ボタンをクリックします。

こんな事に気をつけて

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

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →192.168.1.1
 ネットマスク →24 (255.255.255.0)

ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
IP アド レス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス IPアドレス 192.168.1.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 		

- 5. [保存] ボタンをクリックします。
- **6.** IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP 情報」が表示されます。

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

DHC	情報
	○ 使用しない
	○リレー機能を使用する
	□AAA 参照するAAA情報
	⊙ サーバ機能を使用する
	割当て先頭IPアドレ ス
	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
DHCP	DNSサ プライマリ 192.168.1.1
機能	報セカンダリー
	ドメイン名広報
	TIMEサーバ広報
	NTPサーバ広報
	WINSサ プライマリ
	報セカンダリー
	cuptte 記述形式 ●ドメイン名 ● IPアドレス
	バ広報 プライマリ
	セカンダリ
	MACアドレスチェッ
	ク DAAA 参照するAAA情報
	※"割当て先頭アドレス"が本装置のIPアドレスと同じネットワ ークアドレス内であることを確認してください。

8. [保存] ボタンをクリックします。

相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。 1. 「相手情報」ページが表示されます。 「ネットワーク情報」をクリックします。 2. 「ネットワーク情報」が表示されます。 3. 以下の項目を指定します。 ネットワーク名 → internet <ネットワーク情報追加フィールド> ネットワーク名 internet [追加] ボタンをクリックします。 4. 「ネットワーク情報(internet)」ページが表示されます。 「共通情報」をクリックします。 5. 共通情報の設定項目と「基本情報」が表示されます。 以下の項目を指定します。 6. 自動接続 →する 自動接続 ●する ○しない 7. [保存] ボタンをクリックします。 8. 「PPP 関連」をクリックします。 PPP 関連の設定項目と「圧縮情報」が表示されます。 9. 以下の項目を指定します。 ヘッダ圧縮(IPCP) →チェックしない ヘッダ圧縮(IPV6CP) →チェックしない ■圧縮情報 3 ヘッタ圧縮 (IPCP) ■VJ ■IPヘッダ圧縮 ヘッダ圧縮 (IPV6CP) ■IPヘッダ圧縮
- 10. [保存] ボタンをクリックします。
- 11. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

12. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

ネットワーク →デフォルトルート
 メトリック値 →1
 優先度 →0

	<スタティック経路情報入力フィールド>
ネットワーク	 ● デフォルトルート ● ネットワーク指定 あて先IPアドレス あて先アドレスマスク 0 (0.0.0)
メトリック値 優先度	

14. [追加] ボタンをクリックします。

15. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

16. 以下の項目を指定します。

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

NAT情報	3
NATの使用	●使用しない●NAT●マルチNAT●静的NATのみ
クローバルアドレス	
アトレス個数	1 18
アドレス割当てタイマ	5 分 🗸
NATセキュリティ	○通常 ⊙ 高い

こんな事に気をつけて

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

17. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

- 接続先名 → ISP-1
 接続先種別 →データ通信カード接続
 - ダイヤル1 電話番号 → (通信

→(通信事業者から提示された内容)

	<接続先情報追加フィールド>
接続先名	ISP-1
接続先種別	 データ通信カード接続 ダイヤル1 電話番号 PPPoE接続 IPトンネル接続 IPsec/IKE接続 別インタフェースから送出 MPLSトンネル接続 パケット破棄

19. [追加] ボタンをクリックします。

「接続先情報(ISP-1)」が表示されます。

- **20.** データ通信カード接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 21. 以下の項目を指定します。
 - 無通信監視タイマ →送受信パケットについて60秒
 - 強制切断 指定したパケット数を超えたら切断する

累計

→チェックする
 → 100000パケット

■接続制	御情報
無通信監 視タイマ	送受信パケット 🔽 について 60 秒
課金単位 時間	 昼間(月~金) (08:00~19:00) 0秒 夜間(土日の昼間) (19:00~23:00) 0秒 深夜・早朝 (23:00~08:00) 0秒
強制切断	 □指定した時間を超えたら切断する 累計: 時間 ▼ □指定したパケット数を超えたら切断する 累計: 100000 パケット(128バイト換算)

- 22. [保存] ボタンをクリックします。
- **23.** データ通信カード接続の設定項目の「PPP 情報」をクリックします。 「PPP 情報」が表示されます。

,	 送信認証情報 	報		
認証ID			→ (通信事業者から提示された内容)	容)
	認証パスワー	ード	→(通信事業者から提示された内容)	容)
	PPP情報		3	
	`¥/===n= ⊤ ▲≢±0	認証ID		
1	达估论证用牧	認証バスワード		

25. [保存] ボタンをクリックします。



各通信事業者の認証ID、認証パスワード、電話番号を以下に示します。

詳細については、各通信事業者にお問い合わせください。

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

ProxyDNS 情報、URL フィルタ情報を設定する

- **1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- 「順引き情報」をクリックします。
 「順引き情報」が表示されます。

• ドメイン名

タイプ

- 送信元 IP アドレス

→指定しない

動作 →接続先のDNSサーバへ問い合わせる
 ネットワーク名 → internet

→ *

→すべて

<順引き情報入力フィールド>				
ドメイン 名	*			
タイプ	すべて ▼(番号指定 "その他"を選択時のみ有効で す。)			
送信元 IPアドレ ス	※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。			
動作	 ○ 廃棄する ③ 接続先のDNSサーバへ問い合わせる ネットワーク名 internet ▼ 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 rmt0 ▼ 解決したホストへのホスト経路自動作成 ●しばい ○する DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 使用できるインタフェースが存在しません ▼ 設定したDNSサーバへ問い合わせる DNSサーバへ下しス DNSサーバアドレス 			

- 4. [追加] ボタンをクリックします。
- **5. 「逆引き情報」をクリックします**。 「逆引き情報」が表示されます。
- 6. 以下の項目を指定します。
 - ネットワークアドレス →すべて
 - 動作 →接続先のDNSサーバへ問い合わせる ネットワーク名 → internet



7. [追加] ボタンをクリックします。

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

1.8 無線 LAN とデータ通信カードで仮設店舗を構築 する

適用機種 Si-R240,240B

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

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

こんな事に気をつけて

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

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



● 設定条件

有線 LAN を使ってローカルサーバに接続する

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

無線 LAN を使ってアクセスポイントを構築する

•	利用するポート	: slot1
•	利用する論理定義	: lan1
•	利用する回線定義	: wlan0
•	通信モード	: IEEE802.11b/g
•	チャネル	: 10
•	SSID	: samplenet
•	認証モード	: WPA2-PSK
•	暗号化モード	: AES
•	事前共有キー(PSK)	:テキストで"abcdefghijklmnopqrstuvwxyz"
•	IPアドレス	: 192.168.2.1/24
•	その他	:接続端末のアドレスは DHCP 機能を利用する
デ	ータ通信カードを使ってインターネ	ットへ接続する
•	利用するポート	: slot0

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

端末を設定する

無線 LAN アダプタの設定マニュアルを参考に設定を行ってください。

本装置を設定する

有線LANを使ってローカルサーバに接続する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

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

■IPアドレス情報 🦉			
IPv4	⊙使用する○使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 		

5. [保存] ボタンをクリックします。

無線LAN情報(無線LAN情報)を設定する

1. 設定メニューのルータ設定で「無線 LAN 情報」をクリックします。

「無線 LAN 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - ポート →スロット1-0

<無線LAN情報追加フィールド>		
ボート スロット1-0 🗸		

3. [追加]ボタンをクリックします。

無線 LAN0 情報の設定項目と「回線情報」が表示されます。

- 4. 以下の項目を指定します。
 - ポート →スロット1-0
 通信モード → 11b/g
 - チャネル →10
 - SSID → samplenet

■回線情報	3
ボート	スロット1-0 💌
通信モート	11b/g 🗸
チャネル	10 🗸
SSID	samplenet

- 5. [保存] ボタンをクリックします。
- **6. 「認証/暗号化情報」をクリックします**。 「認証/暗号化情報」が表示されます。

- 認証モード
- →wpa2-psk

● WPA暗号化モード → AES

WPA事前共有キー →テキスト

→ abcdefghijklmnopqrstuvwxyz

■認証/暗号化情報		
認証モート	wpa2-psk 💌	
WPA暗号化モート	○TKIP/AES自動判別○TKIP ④AES	
WPA事前共有キー		

8. [保存] ボタンをクリックします。

無線 LAN を使ってアクセスポイントを構築する

LAN (無線LAN) 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - インタフェース →無線LAN

<lan情報追加フィールド></lan情報追加フィールド>		
インタフェース 無線LAN マ		

- **3. [追加] ボタンをクリックします**。 「LAN1 情報(無線 LAN)」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - 無線LAN定義
 →無線LAN0



- 6. [保存] ボタンをクリックします。
- 7. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

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

■IPアドレス情報			
IPv4	●使用する●使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.2.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 		

9. [保存] ボタンをクリックします。

10. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

11. 以下の項目を指定します。

•	DHCP機能	→サーバ機能を使用する
	割当て先頭 IP アドレス	→ 192.168.2.10
	割当てアドレス数	→ 10
	リース期間	→1日
	デフォルトルータ広報	→192.168.2.1
	DNSサーバ広報	
	プライマリ	→192.168.2.1
	ドメイン名広報	→wlan.com

■DHCP情報					
	○使用しない				
○リレー機能を使用する					
		DHCPサ	ーバIPアドレ	,ス1	
		DHCPサ	ーバIPアドレ	,ス2	
		мастк	レスチェック	,	 □ホストデータベース □ AAA 参照するAAA情報
	۲	サーバ機	能を使用す	3	·
		割当て先 ス	頭IPアドレ	192.1	68.2.10
		割当てア	ドレス数	10	
		リース期	1	1	
		デフォル 報	トルータ広	192.1	68.2.1
DHCP	P	DNSサ	ブライマリ	192.1	68.2.1
機能		報	セカンダリ		
		ドメイン名	3広報	wlan.	com
		TIMEサー	-バ広報		
		NTPサー	バ広報		
		WINSサ	ブライマリ		
		報	セカンダリ		
			記述形式	<u>الا</u>	メイン名 OIPアドレス
		SIPサー バ広報	プライマリ		
			セカンダリ		
		MACアドレスチェッ		□ヵ	マストデータベース
		<u>ک</u>		ΠA	AA 参照するAAA情報
		※"割当で ークアドレ	て先頭アドレ ・ス内である	ス"カ ことを	「本装置のIPアドレスと同じネットワ」 「確認してください。

12. [保存] ボタンをクリックします。

データ通信カードを使ってインターネットへ接続する

WAN 情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →データ通信カード

<wan情報追加フィールド></wan情報追加フィールド>		
回線インタフェース		データ通信カード 🖌

3. [追加] ボタンをクリックします。

「WAN 情報(データ通信カード)」ページが表示されます。

- 4. 以下の項目を指定します。
 - ポート →スロット0-0

■基本情報	報	3
ボート		

5. [保存] ボタンをクリックします。

相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → internet

<ネットワーク情報追加フィールド>		
ネットワーク名	internet	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (internet)」ページが表示されます。

5. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - 自動接続 →する

<mark>自動接続</mark> ⊙する ○しない

- 7. [保存] ボタンをクリックします。
- 8. 「PPP 関連」をクリックします。

PPP関連の設定項目と「圧縮情報」が表示されます。

- 9. 以下の項目を指定します。
 - ヘッダ圧縮(IPCP) →チェックしない
 - ヘッダ圧縮 (IPV6CP) →チェックしない

■圧縮情報	3
ヘッダ圧縮 (IPCP)	■VJ ■IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	■IPヘッダ圧縮

- 10. [保存] ボタンをクリックします。
- 11. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

12. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

ネットワーク →デフォルトルート
 メトリック値 →1
 優先度 →0

	<スタティック経路情報入力フィールド>				
ネットワーク	 ● デフォルトルート ● ネットワーク指定 あて先IPアドレス あて先アドレスマスク 0 (0.0.0) 				
メトリック値 優先度					

14. [追加] ボタンをクリックします。

15. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

16. 以下の項目を指定します。

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

NAT情報	3
NATの使用	○使用しない○NAT ⊙マルチNAT ○静的NATのみ
クローバルアドレス	
アトレス個数	1 1 1 個
アドレス割当てタイマ	5 分 🗸
NATセキュリティ	○通常 ⊙ 高い

こんな事に気をつけて

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

- 17. [保存] ボタンをクリックします。
- **18. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

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

<接続先情報追加フィールド>			
接続先名	ISP-1		
接続先種別	 データ通信カード接続 ダイヤル1 電話番号 PPPoE接続 IPトンネル接続 IPsec/IKE接続 別インタフェースから送出 MPLSトンネル接続 パケット破棄 		

20. [追加] ボタンをクリックします。

「接続先情報(ISP-1)」が表示されます。

- **21. データ通信カード接続の設定項目の「接続制御情報」をクリックします**。 「接続制御情報」が表示されます。
- 22. 以下の項目を指定します。
 - 無通信監視タイマ →送受信パケットについて60秒

■接続制御情報	3
 無通信監 視タイマ 送受信パケット ▼ (こついて 60 秒) 	

- 23. [保存] ボタンをクリックします。
- 24. データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

- 25. 以下の項目を指定します。
 - ・ 送信認証情報
 認証 ID → (通信事業者から提示された内容)
 認証パスワード → (通信事業者から提示された内容)

PPP情報		3
	認証ID	
达后路证用报	認証バスワード	

26. [保存] ボタンをクリックします。

ProxyDNS情報、URLフィルタ情報を設定する

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

「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

3. 以下の項目を指定します。

ドメイン名

- **→** *
- タイプ →すべて
- 送信元IPアドレス

ネットワーク名

→指定しない

• 動作

→接続先のDNSサーバへ問い合わせる →internet

- <順引き情報入力フィールド> ドメイン 名 その他"を選択時のみ有効で すべて <mark>▼(番号指定</mark> タイプ す。) 送信元 IPアドレ ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィッ ス クス長形式で入力してください。 ○ 廃棄する ● 接続先のDNSサーバへ問い合わせる ネットワーク名 internet 🔽 接続先のDNSサーバへ指定ネットワークを経由して問い合
 わせる ネットワーク名 rmt0 💌 動作 解決したホストへのホスト経路自動作成 ●しない ●する ○ DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 使用できるインタフェースが存在しません 💌 ○ 設定したDNSサーバへ問い合わせる DNSサーバアドレス
- 4. [追加] ボタンをクリックします。
- 5. 「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

動作

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

ネットワーク名



7. [追加] ボタンをクリックします。

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。



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

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

こんな事に気をつけて

無線LAN インタフェース上では、以下の機能は利用できません。

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

1.9 事業所 LAN を ISDN で接続する

適用機種 Si-R220B,220C,370,570

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

こんな事に気をつけて

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

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

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



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート(Si-R220B、220Cの場合) で ISDN 回線(64Kbps)を使用する
- スタティック経路機能を使用する

•	接続ネットワーク名	: intranet
•	無通信監視時間を1分とする	
[5	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
[]	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 着信
- : kawasaki, kawapass
- : tokyo、tokyopass

こんな事に気をつけて

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

東京事業所を設定する

WAN0 情報を設定する

設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 回線インタフェース → ISDN

<wan情報追加了< th=""><th>フィールド></th></wan情報追加了<>	フィールド>
回線インタフェース	ISDN 👻

3. [追加] ボタンをクリックします。

「WAN0 情報 (ISDN)」ページが表示されます。

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 4. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する
 IPアドレス → 192.168.1.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	●使用する●使用しない	
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス I92.168.1.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ネットワークアドレス+オール1 	

5. [保存] ボタンをクリックします。

相手情報を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名

→ intranet

<ネットワーク情報追加フィールド>		
ネットワーク名	intranet	

4. [追加] ボタンをクリックします。

「ネットワーク情報(intranet)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7. 以下の項目を指定します。

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

● 優先度 →0



- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

• 接続先名

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

→kawasaki



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

12. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

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

■PPP情報 [7]				
認証方式				
送信認証 情報	認証ID 認証バスワー ド	tokyo		
受諾認証 情報	認証ID 認証バスワー ド	kawasaki		

14. [保存] ボタンをクリックします。

15. ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

16. 以下の項目を指定します。

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

■接続制御情報		3
常時接続 機能	⊙使用しない○使用する	
無通信監 視タイマ	送受信パケット 🗸 について 60 秒	

こんな事に気をつけて

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

- 一方の装置で着信接続を優先する。
- 一方の装置で接続優先制御を行わない。
- 17. [保存] ボタンをクリックします。
- **18. 画面左側の [再起動] ボタンをクリックします。** 設定した内容が有効になります。

川崎事業所を設定する

「東京事業所を設定する」を参考に、川崎事業所を設定します。				
「WAN0 情報」				
• 回線インタフェース	→ISDN			
「LAN0情報」-「IP関連」				
「IPアドレス情報」				
• IPv4	→使用する			
• IPアドレス	→指定する			
IPアドレス	→ 192.168.2.1			
ネットマスク	→24 (255.255.255.0)			
ブロードキャストアドレス	→ネットワークアドレス+オール1			
「相手情報」-「ネットワーク情	報」			
 ネットワーク名 	→intranet			
「ネットワーク情報」- 「IP 関連」				
「スタティック経路情報」				
• ネットワーク	→ネットワーク指定			
あて先 IP アドレス	→ 192.168.1.0			
あて先アドレスマスク	→24 (255.255.255.0)			
• メトリック値	→ 1			
● 優先度	→ 0			
「接続先情報」				
● 接続先名	→tokyo			
• 接続先種別	→ISDN接続			
	→通常接続			
ダイヤル1				
電話番号	→ 03-7777-7777			
	→指定しない			
接続无情報」- ISDN 接続」				
PPP 情報」				
● 認証方式	→ PAP、CHAP			
 送信認証情報 				
認証 ID	→ kawasaki			
認証ハスワート	→ kawapass			
 受諾認証情報 	. telu a			
認証 ルフロード	→ tokyo			
	· LONYOPASS			
 市时按杭ົ市和 毎、済行を知らく一 	→(沢用しない)			
 ・ ・ ・	→达党信ハケットについく60秒			

1.10 事業所 LAN を専用線で接続する

適用機種 Si-R220B,220C,370,570

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

こんな事に気をつけて

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

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



● 設定条件

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

[本社]

 接続ネットワーク名 	: honsya
• 接続先名	: honsya-1
 ネットワークアドレス/ネットマスク 	: 192.168.1.0/24
• 本装置のLAN側のIPアドレス	: 192.168.1.1
 DNS サーバ 	: 192.168.1.2
 基幹ネットワーク側ルータIPアドレス 	: 192.168.1.3
[支社]	
• 接続ネットワーク名	: shisya1
• 接続先名	: shisya-1
 ネットワークアドレス/ネットマスク 	: 192.168.2.0/24
 本装置のLAN側のIPアドレス 	: 192.168.2.1



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

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

■ 参照 Si-Rシリーズ Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P19)

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

本社を設定する

WAN0 情報を設定する

- **1. 設定メニューのルータ設定で「WAN 情報」をクリックします**。 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →専用線

<wan情報設造力dフィールド></wan情報設造力dフィールド>	
回線インタフェース	専用線

- 【追加】ボタンをクリックします。
 「WAN0情報(専用線)」ページが表示されます。
- **4. 「基本情報」をクリックします。** 「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - ポート →スロット0-0
 - 回線速度 → 1.5Mbps

■基本情報	3
ポート	고ㅁット 0-0 💌
回線速度	1.5Mbps 💌

Si-R220B、220Cでは、ポートは固定です。

6. [保存] ボタンをクリックします。

LAN0 情報を設定する

- 1. 設定メニューのルータ設定で「LAN情報」をクリックします。

 「LAN情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

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

■IPアドレス情報		
IPv4	●使用する●使用しない	
ז ואדמו	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス I92.168.1.1 	
	ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス	

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7. 以下の項目を指定します。

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

<スタティック経路情報入力フィールド>				
◎ デフォルトルート				
ネ	0	中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 192.168.1.3 	
ット		ネットワーク指定		
ヮ		あて先IPアドレス		
こク		あて先アドレスマス ク	0 (0.0.0)	
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 	
メトリック値	メ × リ ッ ク 値			
優先度	0			

8. [追加] ボタンをクリックします。

相手情報を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名

→shisya1

<ネットワーク情報追加フィールド>		
ネットワーク名	shisya1	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (shisya1)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7. 以下の項目を指定します。

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

● 優先度 →0



- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

- 接続先名 → shisya-1
- 接続先種別 →専用線接続

機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

使用インタフェース	WANO 💌	
DNSサーバ	192.10.10.10	

13. [保存] ボタンをクリックします。

14. 画面左側の [再起動] ボタンをクリックします。 設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。

「WAN0 情報」

- 回線インタフェース →専用線
 「専用線」-「基本情報」
 ポート →スロット0-0
- 回線速度 → 1.5Mbps

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

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

「相手情報」-「ネットワーク情報」

 ネットワーク名 	→ honsya		
「ネットワーク情報」-「IP 関連」			
「スタティック経路情報」			
• ネットワーク	→デフォルトルート		
• メトリック値	→ 1		
● 優先度	→ 0		
「接続先情報」			
● 接続先名	→honsya-1		
• 接続先種別	→専用線接続		
1.11 複数の事業所 LAN をフレームリレーで接続する

適用機種 Si-R220B,220C,370,570

ここでは、フレームリレーで複数の事業所を接続する場合を例に説明します。

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

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

こんな事に気をつけて

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

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



● 設定条件

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

[センタ1と接続する条件]

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

[センタ2と接続する条件]

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

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

WAN0 情報を設定する

1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 回線インタフェース →フレームリレー

<wan情報追加フィールド></wan情報追加フィールド>	
回線インタフェース	フレームリレー 💌

- 【追加】ボタンをクリックします。
 「WAN0情報(フレームリレー)」ページが表示されます。
- 4. 「基本情報」をクリックします。

「基本情報」が表示されます。

5. 以下の項目を指定します。

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

■基本情報	3
ボート	スロットロー0 💙
回線速度	128Kbps 💌
PVC状態確認手順	○使用しない⊙使用する
CLLMメッセージ	○使用しない⊙使用する
輻輳通知ヒット	FECN BECN

6. [保存] ボタンをクリックします。

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

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

■IPアドレス情報		
IPv4	●使用する●使用しない	
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 10.100.87.3 ネットマスク 24 (255.255.255.0) ▼ ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 	

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

7. 以下の項目を指定します。

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

RIP情報	3	
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する 	
RIP受信	○受信しない ●V1で受信する ●V2、V2(Multicast)で受信する	
《 RIP 送信時は加算するメトリック値を設定してください。》 <mark>メトリック値 </mark>		

8. [保存] ボタンをクリックします。

接続先(センタ1)の情報を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → center1

<ネットワーク情報追加フィールド>		
ネットワーク名	center1	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (center1)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. 以下の項目を指定します。

•	IPアドレス
	相手側IPアドレス
	自側IPアドレス

→設定する →10.200.3.1 →10.200.3.18

■IP基本情報		
10751.7	 ○ 設定してい ● 設定する 	=1
	相手側IPアドレス 10.200.3.1	
	自側IPアドレス 10.200.3.18	

7. [保存] ボタンをクリックします。

IP 関連の設定項目の「RIP 情報」をクリックします。 「RIP 情報」が表示されます。

- 9. 以下の項目を指定します。
 - RIP送信 → V1 で送信する
 - RIP受信 → V1 で受信する
 - メトリック値 →0

■RIP情報	3	
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する 	
RIP受信	●受信しない ● V1で受信する ● V2、V2(Multicast)で受信する	
《 RIP 送信時は加算するメトリック値を設定してください。》 <mark>メトリック値</mark>		

- 10. [保存] ボタンをクリックします。
- **11. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 12. 以下の項目を指定します。
 - 接続先名

DLCI

• 接続先種別

→ap1 →フレームリレー接続 →16



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

13. [追加] ボタンをクリックします。

フレームリレー接続の設定項目と「基本情報」が表示されます。

•	使用インタフェース	→WAN0
•		→ 16

• DLC	→ 16

• CIR →64Kbps

使用インタフェース	WANO 🛩
DLCI	16
CIR	64Kbps 💟

15. [保存] ボタンをクリックします。

接続先(センタ2)の情報を設定する

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

「相手情報」-「ネットワーク情	報」
 ネットワーク名 	→center2
「ネットワーク情報」-「IP 関連」	
「IP基本情報」	
• IPアドレス	→設定する
相手側IPアドレス	→ 10.200.103.1
自側IPアドレス	→10.200.103.18
「RIP情報」	
● RIP送信	→V1 で送信する
● RIP受信	→V1 で受信する
 メトリック値 	→0
「接続先情報」	
● 接続先名	→ap2
● 接続先種別	→フレームリレー接続
DLCI	→ 17
「接続先情報」-「フレームリレー	接続」
「基本情報」	
• 使用インタフェース	→WAN0
• DLCI	→ 17

• CIR →64Kbps

1.12 複数の事業所 LAN を ATM で接続する

適用機種 Si-R260B,370,570

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

こんな事に気をつけて -

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

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



● 設定条件

[本社]

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

[事業所A]

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

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

[事業所B]

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

こんな事に気をつけて

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

本社を設定する

WAN0情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース → ATM

<WAN情報追加フィールド> 回線インタフェース ATM ▼

3. [追加] ボタンをクリックします。

「WANO情報(ATM)」ページが表示されます。

4. 「基本情報」をクリックします。

「基本情報」が表示されます。

- 5. 以下の項目を指定します。
 - ポート →スロット0-0
 - VPI →0
 - VP速度 →指定しない
 - OAM (F4) →受け付けない

■基本情報	3
ボート	スロット0-0 V
VPI	0
VP速度	 ● 指定しばい ● 指定する Mbps ▼
OAM(F4)	●受け付けない●受け付ける

6. [保存] ボタンをクリックします。

LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →10.200.87.3
 ネットマスク →24 (255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報 []		
IPv4	⊙使用する○使用しない	
IP アド レス	 ○ DHCPで自動的に取得する ○ 指定する □Pアドレス 10.200.87.3 ネットマスク 24 025.255.255. ブロードキャストアドレ ネットワークアドレ 	0) ▼ ス+オール1 ▼

5. [保存] ボタンをクリックします。

事業所A向けの相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名

→JigyoA

<ネットワーク情報追加フィールド>		
ネットワーク名		Jigyo A

4. [追加] ボタンをクリックします。

「ネットワーク情報(JigyoA)」ページが表示されます。

- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

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

	<スタティック経路情報入力フィールド>	
 ○ デフォルトルート ③ ネットワーク指定 		
ネットワーク	あて先IPアドレス 10.200.81.0	
	あて先アドレスマスク 24 (255.255.2) 🗸	
メトリック値	1 💌	
優先度	0	

- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

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



Si-R260Bでは、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

ATM接続の設定項目と「基本情報」が表示されます。

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

使用インタフェース	WANO 🗸
VCI	80
VC速度	6 Mbps 💙
サービスタイプ	 ◇ CBR ◇ VBR 平均速度値 Kbps ▼ 最大バースト長 ○ UBR+ 最低速度値 Kbps ▼ GFR+ (保証速度値 Kbps ▼
OAM(F5)	⊙受け付けない ○受け付ける

13. [保存] ボタンをクリックします。

事業所B向けの相手情報を設定する

- 画面上部の「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → JigyoB

<ネットワーク情報追加フィールド>	
ネットワーク名	Jigyo B

- 【追加】ボタンをクリックします。
 「ネットワーク情報(JigyoB)」ページが表示されます。
- 5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

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

● 優先度

→0

<スタティック経路情報入力フィールド>	
 ○ デフォルトルート ③ ネットワーク指定 	
ネットワーク	あて先IPアドレス 10.200.82.0
	あて先アドレスマスク 24 (255.255.255.0) 🔽
メトリック値	1
優先度	0

- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

接続先名 → jigyo-b
 接続先種別 → ATM 接続

→81

VCI



Si-R260Bでは、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

ATM接続の設定項目と「基本情報」が表示されます。

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

使用インタフェース	WANO 🔽
VCI	81
VC速度	4 Mbps 🕶
サービスタイプ	 ● CBR ● VBR 平均速度値 ▲大バースト長 ● UBR+ 最低速度値 Kbps ♥ ● GFR+ 保証速度値 Kbps ♥
OAM(F5)	●受け付けない ●受け付ける

13. 【保存】ボタンをクリックします。

14. 画面左側の [再起動] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

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

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

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

事務所Aを設定する

「本社を設定する」を参考に、事業所Aを設定します。

「WAN0 情報」- 「ATM」 「基本情報」

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

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

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

「相手情報」-「ネットワーク情報」

•	ネットワーク名	→Honsya
[7	ネットワーク情報」-「IP 関連」	
۲2	スタティック経路情報」	
•	ネットワーク	→デフォルトルート
•	メトリック値	→ 1
•	優先度	→ 0
Γŧ	接続先情報」	
•	接続先名	→honsya-1
•	接続先種別	→ ATM 接続
	VCI	→81
Γŧ	妾続先情報」-「ATM 接続」	
٢ł	基本情報」	
•	使用インタフェース	→WAN0
•	VCI	→81
•	VC速度	→6Mbps
•	サービスタイプ	→CBR
•	OAM (F5)	→受け付けない

事務所Bを設定する

「本社を設定する」を参考に、事業所Bを設定します。

「WANO情報」-「ATM」 「基本情報」 ・ ポート →スロット0-0 ・ VPI →0 ・ VP速度 →1

• OAM (F4) →受け付けない

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

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

「相手情報」-「ネットワーク情報」

• ネッ	トワーク名	→Honsya
「ネット	ヽワーク情報」-「IP 関連」	
「スタラ	「ィック経路情報」	
• ネッ	トワーク	→デフォルトルート
• ×+	トリック値	→ 1
• 優先	度	→0
「接続先	に情報」	
 接続 	洗名	→honsya-2
 接続 	先種別	→ ATM 接続
VCI		→82
「接続労	た情報」-「ATM 接続」	
「基本情	青報」	
• 使用	ヨインタフェース	→WAN0
• VCI		→82
• VCì	速度	→4Mbps
• サー	-ビスタイプ	→CBR
• OAN	VI (F5)	→受け付けない

1.13 複数の事業所 LAN を IP-VPN 網を利用して接続する

適用機種 全機種

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

こんな事に気をつけて

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

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

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

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

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

1.13.1 ADSL モデムを使用して IP-VPN 網と接続する

適用機種 全機種



● 設定条件

• LANOポートをADSLモデムに接続する

[IP-VPN網]

- 東京営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。また、グレースフルリスタートを使用する。
- 横浜営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 大阪営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。グレースフルリスタートは使用しない。

•	東京営業所向けIPアドレス	: 172.16.1.2
•	横浜営業所向け IP アドレス	: 172.16.2.2
•	大阪営業所向けIPアドレス	: 172.16.3.2
•	AS番号	: 1
[5	東京営業所]	
•	IP-VPN 網側ポート	: LANO
•	LAN0側IPアドレス	: 192.168.1.1
•	LAN0 側ネットワークアドレス/ネットマスク	: 192.168.1.0/24
•	LAN1 側 IP アドレス	: 10.10.10.1
•	LAN1 側ネットワークアドレス/ネットマスク	: 10.10.10.0/24
•	AS番号	: 65000
•	BGPグレースフルリスタート	:使用する
•	営業所内のルーティングプロトコル	: RIPv2

[横浜営業所]

•	IP-VPN 網側ポート	: LANO
•	LAN0 側 IP アドレス	: 192.168.2.1
•	LAN0 側ネットワークアドレス/ネットマスク	: 192.168.2.0/24
•	LAN1 側 IP アドレス	: 10.20.10.1
•	LAN1 側ネットワークアドレス/ネットマスク	: 10.20.10.0/24
•	AS番号	: 65001
•	BGPグレースフルリスタート	:使用しない
[7	、阪営業所]	
•	IP-VPN 網側ポート	: LANO
•	IP-VPN 網側ポート LAN0 側 IP アドレス	: LAN0 : 192.168.3.1
•	IP-VPN 網側ポート LAN0 側 IP アドレス LAN0 側ネットワークアドレス / ネットマスク	: LAN0 : 192.168.3.1 : 192.168.3.0/24
• • •	IP-VPN 網側ポート LAN0 側 IP アドレス LAN0 側ネットワークアドレス / ネットマスク LAN1 側 IP アドレス	: LAN0 : 192.168.3.1 : 192.168.3.0/24 : 10.30.10.1
• • • •	IP-VPN 網側ポート LAN0 側 IP アドレス LAN0 側ネットワークアドレス/ネットマスク LAN1 側 IP アドレス LAN1 側ネットワークアドレス/ネットマスク	: LAN0 : 192.168.3.1 : 192.168.3.0/24 : 10.30.10.1 : 10.30.10.0/24
• • • • •	IP-VPN 網側ポート LAN0 側 IP アドレス LAN0 側ネットワークアドレス/ネットマスク LAN1 側 IP アドレス LAN1 側ネットワークアドレス/ネットマスク AS 番号	: LAN0 : 192.168.3.1 : 192.168.3.0/24 : 10.30.10.1 : 10.30.10.0/24 : 65002

東京営業所を設定する

LAN0情報を設定する

- 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 - IP \mathcal{P} F \mathcal{V} \rightarrow 192.168.1.1

 $\hat{\mathcal{A}}$ \mathcal{V} F \mathcal{V} \rightarrow 24 (255.255.255.0)

 \mathcal{J} \mathcal{U} \mathcal{V} \mathcal{V} \mathcal{V} \mathcal{V} \mathcal{V}

IPアドレス情報		
IPv4	●使用する●使用しない	
IP アド レス	 DHCPで自動的に取得する 指定する IPアドレス ネットマスク ブロードキャストアドレ マロードキャストアドレ 	5 192.168.1.1 24 (255.255.255.0) ・ ネットワークアドレス+オール1 ・

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT情報」が表示されます。

7. 以下の項目を指定します。

• NATの使用

→使用しない

■NAT情報	3
NATの使用	●使用しない ○NAT ○マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

8. [保存] ボタンをクリックします。

9. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 10. 以下の項目を指定します。
 - ネットワーク
 ネットワーク指定
 あて先IPアドレス
 →172.16.1.0
 →24 (255.255.255.0)
 中継ルータアドレス
 →指定する
 IPアドレス
 →192.168.1.2
 メトリック値
 →1

→0

優先度

<スタティック経路情報入力フィールド>			
	0	デフォルトルート	
×		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス
ット	0	ネットワーク指定	
ワ		あて先IPアドレス	172.16.1.0
ーク		あて先アドレスマス ク	24 (255.255.255.0)
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 192.168.1.2
メトリック値 優先度	メトリック値 優先 0		

11. [追加] ボタンをクリックします。

LAN1情報を設定する

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

1. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →10.10.10.1
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

IPアドレス情報
IPv4 ●使用する●使用しない
① DHCPで自動的に取得する
● 指定する
IPアドレス 10.10.10.1
ス 24 (255.255.255.0) ▼
ブロードキャストアドレ ネットワークアドレス+オール1 ▼

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

- 7. 以下の項目を指定します。
 - RIP送信 →V2 (Multicast) で送信する
 - RIP受信 → V2、V2 (Multicast) で受信する

RIP情報	3
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ⊙V2(Multicast)で送信する
RIP受信	 ○受信しない ○ V1で受信する ⊙ V2、V2(Multicast)で受信する

8. [保存] ボタンをクリックします。

ルーティングプロトコル情報を設定する

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

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

- 3. 以下の項目を指定します。
 - RIP
 BGP 経路情報 →
 - →再配布する
 - BGP
 RIP 経路情報

```
→再配布する
```

■再配	再配布情報		
	インタフェース経路情報	○再配布しない⊙再配布する	
	スタティック経路情報	○再配布しない⊙再配布する	
DID	BGP経路情報	○再配布しない ③再配布する メトリック値: 0 ▼	
κιΡ	OSPF経路情報	●再配布しない ○再配布する メトリック値: ○ ▼	
	DNS経路情報	●再配布しない ○再配布する メトリック値: ○ ▼	
	インタフェース経路情報	●再配布しない●再配布する	
	スタティック経路情報	⊙再配布しない○再配布する	
BGP	RIP経路情報	○再配布しない⊙再配布する	
	OSPF経路情報	●再配布しない●再配布する	
	DNS経路情報	● 再配布しない ● 再配布する	

- 4. [保存] ボタンをクリックします。
- 5. 「BGP 関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

- 6. 以下の項目を指定します。
 - BGP機能 →使用する
 - 自AS番号 →65000

■BGP情報	3
BGP機能	○使用しない ●使用する
自AS番号	65000

- 7. [保存] ボタンをクリックします。
- **8.** BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。 「BGP ネットワーク情報」が表示されます。

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

<bgpネットワーク情報入力フィールド></bgpネットワーク情報入力フィールド>	
あて先IPアドレス	10.10.10.0
あて先アドレスマスク	24 (255.255.255.0) 🗸

- 10. [追加] ボタンをクリックします。
- **11.** BGP 関連の設定項目の「BGP 相手情報」をクリックします。 「BGP 相手情報」が表示されます。
- 12. [追加] ボタンをクリックします。

BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。

13. 以下の項目を指定します。

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

■BGP相手基本情報	
相手側IPアト レス	172.16.1.2
相手AS番号	1
自側IPアドレ ス	
KeepAliveタ イマ	30 秒 🗸
Holdタイマ	90 秒 🗸
MEDメトリッ ク値	0
ASバスブリ ベンド	0
EBGP MULTIHOP	2

必要に応じて上記以外の項目を指定します。

- 14. [保存] ボタンをクリックします。
- **15. 「**BGP **拡張機能情報」をクリックします**。 「BGP 拡張機能情報」が表示されます。
- 16. 以下の項目を指定します。
 - グレースフルリスタート アドレスファミリ

→IPv4ユニキャスト

グレースフルリスタート	アドレスファミリ	<mark>ァミリ</mark> ☑IPv4ユニキャスト	
JU-XJUJXX-F	staleタイマ	360 秒 💌	

- 17. [保存] ボタンをクリックします。
- **18. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

「東京営業所を設定する」を参考に、	横浜営業所を設定します。
「LAN0情報」-「IP 関連」	
「IPアドレス情報」	
• IPv4	→使用する
 IPアドレス 	→指定する
IPアドレス	→ 192.168.2.1
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「NAT情報」	
 NATの使用 	→使用しない
「スタティック経路情報」	
 ネットワーク 	→ネットワーク指定
あて先IPアドレス	→ 172.16.2.0
あて先アドレスマスク	→24 (255.255.255.0)
中継ルータアドレス	→指定する
IPアドレス	→ 192.168.2.2
• メトリック値	→ 1
● 優先度	→ 0
「LAN1情報」-「IP関連」	
「IPアドレス情報」	
• IPv4	→使用する
• IPアドレス	→指定する
IPアドレス	→ 10.20.10.1
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「ルーティングプロトコル情報」	- 「BGP関連」
「BGP情報」	
• BGP機能	→使用する
● 自AS番号	→65001
「BGP ネットワーク情報」	

あて先IPアドレス → 10.20.10.0
 あて先アドレスマスク → 24 (255.255.25)

「BGP相手情報」-「BGP相手基本情報」

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

「東京営業所を設定する」を参考に、	大阪営業所を設定します。
「LAN0情報」-「IP関連」	
「IPアドレス情報」	
• IPv4	→使用する
• IPアドレス	→指定する
IPアドレス	→ 192.168.3.1
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「NAT 情報」	
● NATの使用	→使用しない
「スタティック経路情報」	
• ネットワーク	→ネットワーク指定
あて先IPアドレス	→ 172.16.3.0
あて先アドレスマスク	→24 (255.255.255.0)
中継ルータアドレス	→指定する
	→ 192.168.3.2
● メトリック値	→ 1
● 優先度	→ 0
「LAN1情報」-「IP関連」	
「IPアドレス情報」	
• IPv4	→使用する
• IPアドレス	→指定する
IPアドレス	→ 10.30.10.1
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「ルーティングプロトコル情報	- 「BGP関連」
「BGP情報」	

•	BGP機能	→使用する

• 自AS番号 →65002

「BGPネットワーク情報」

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

「BGP相手情報」-「BGP相手基本情報」

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

1.13.2 高速ディジタル専用線を使用して IP-VPN 網と接続する

適用機種 Si-R220B,220C,370,570



● 設定条件

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

[IP-VPN網]

- 東京営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。また、グレースフルリスタートを使用する。
- 横浜営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 大阪営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。グレースフルリスタートは使用しない。

: 1

: RIPv2

: 65000

: 172.16.1.1

- 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

[東京営業所]

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

[横浜営業所]

• LAN 側の IP アドレス : 192.168.2.1 • LAN側のネットワークアドレス/ネットマスク : 192.168.2.0/24 • WAN 側の IP アドレス : 172.16.2.1 • AS番号 : 65001 BGP グレースフルリスタート :使用しない [大阪営業所] LAN側のIPアドレス : 192.168.3.1 • LAN 側のネットワークアドレス/ネットマスク : 192.168.3.0/24 • WAN 側の IP アドレス : 172.16.3.1 • AS番号 : 65002 • BGP グレースフルリスタート :使用しない

東京営業所を設定する

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

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

■IPアドレス情報		
IPv4	⊙使用する○使用しない	
	 ○ DHCPで自動的に取得する ○ 指定する 	
	IPアドレス 192.168.1.1	
	ネットマスク 24 (255.255.255.0) 🗸	
	ブロードキャストアドレ ス ネットワークアドレス+オール1	

5. [保存] ボタンをクリックします。

6. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

• NATの使用

→使用しない

	■NAT情報	3
	NATの使用	●使用しない ○NAT ○マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

8. [保存] ボタンをクリックします。

9. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

10. 以下の項目を指定します。

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

RIP情報	3
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ⊙V2(Multicast)で送信する
RIP受信	●受信しない ● V1で受信する ● V2、V2(Multicast)で受信する

11. [保存] ボタンをクリックします。

IP-VPN 網と接続する相手情報を設定する

- 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →専用線

<WAN情報追加フィールド>
回線インタフェース 専用線 ▼

3. [追加] ボタンをクリックします。

「WAN0 情報(専用線)」ページが表示されます。

4. 「基本情報」をクリックします。

「基本情報」が表示されます。

- 5. 以下の項目を指定します。
 - ポート →スロット0-0
 - 回線速度 → 128Kbps

■基本情報	3
ボート	スロット 0-0 🔽
回線速度	128Kbps 💙

Si-R220B、220Cでは、ポートは固定です。

- 6. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 9. 以下の項目を指定します。
 - ネットワーク名 → IP-VPN

<ネットワーク情報追加フィールド>	
ネットワーク名 IP-VPN	

10. [追加] ボタンをクリックします。

「ネットワーク情報 (IP-VPN)」ページが表示されます。

11. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

- 12. 以下の項目を指定します。
 - 接続先名

- →ip-vpn →専用線接続
- 接続先種別
- <接続先情報追加フィールド> 接続先名 ip-vpn ◯ ATM接続 VCI 専用線接続 ⊙ 通常接続 使用インタフェース WAN1 V ○ 論理リンクにバンドルする 使用インタフェー WAN1 V 2 バンドル先 選択できる定義がありません 🔽 ○ ISDN接続 ⊙ 通常接続 使用インタフェース すべて 🗸 接続先種 ダイヤル1 電話番号 サブアドレス 別 ○ 論理リンクにバンドルする 使用インタフェー すべて 🗸 ス バンドル先 選択できる定義がありません 🗸 ○ フレームリレー接続 DLCI ○ PPPoE接続 ○ IPトンネル接続 ○ IPsec/IKE接続 ○ 別インタフェースから送出 ○ MPLSトンネル接続 ○ バケット破棄
- Si-R220B、220Cでは、接続先種別の表示が上記の画面とは異なります。

- **13.** [追加] ボタンをクリックします。 専用線接続の設定項目と「基本情報」が表示されます。
- 14. 以下の項目を指定します。
 - 使用インタフェース → WAN0

使用インタフェース WANO 🗸

- 15. [保存] ボタンをクリックします。
- **16. 画面上部の「ネットワーク情報(IP-VPN)」をクリックします。**

「ネットワーク情報(IP-VPN)」が表示されます。

17. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

- 18. 以下の項目を指定します。
 - IPアドレス →設定する
 相手側IPアドレス → 172.16.1.2
 自側IPアドレス → 172.16.1.1

■IP基本情報		3
IP アド レス	 ○ 設定しない ● 設定する 相手側IPアドレス 172.16.1.2 自側IPアドレス 172.16.1.1 	

19. [保存] ボタンをクリックします。

ルーティングプロトコル情報を設定する

- **1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 「ルーティングマネージャ情報」をクリックします。
 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

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

■再配布情報		
RIP	インタフェース経路情報	○再配布しない⊙再配布する
	スタティック経路情報	○再配布しない⊙再配布する
	BGP経路情報	○再配布しない ③再配布する メトリック値: □ ▼
	OSPF経路情報	 ● 再配布しばい ○ 再配布する メトリック値: 0 ▼
	DNS経路情報	●再配布しない ○再配布する メトリック値: ○ ▼
BGP	インタフェース経路情報	●再配布しない●再配布する
	スタティック経路情報	●再配布しない●再配布する
	RIP経路情報	○再配布しない⊙再配布する
	OSPF経路情報	● 再配布しない ● 再配布する
	DNS経路情報	●再配布しない●再配布する

4. [保存] ボタンをクリックします。

5. 「BGP 関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

6. 以下の項目を指定します。

- BGP機能 →使用する
- 自AS番号 →65000

■BGP情報	3
BGP機能	○使用しない ⊙使用する
自AS番号	65000

- 7. [保存] ボタンをクリックします。
- BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。
 「BGP ネットワーク情報」が表示されます。
- 9. 以下の項目を指定します。
 - あて先IPアドレス → 192.168.1.0
 - あて先アドレスマスク →24 (255.255.255.0)

<bgpネットワーク情報入力フィールド></bgpネットワーク情報入力フィールド>	
あて先IPアドレス	192.168.1.0
あて先アドレスマスク	24 (255.255.255.0) 🗸

- 10. [追加] ボタンをクリックします。
- 11. BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP相手情報」が表示されます。

12. [追加] ボタンをクリックします。

BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。

13. 以下の項目を指定します。

- 相手側 IP アドレス → 172.16.1.2
- 相手AS番号

BGP相手基	上本情報 [3]
相手側IPアト レス	172.16.1.2
相手AS番号	1

→1

必要に応じて上記以外の項目を指定します。

- 14. [保存] ボタンをクリックします。
- **15. 「**BGP **拡張機能情報」をクリックします**。 「BGP 拡張機能情報」が表示されます。
- 16. 以下の項目を指定します。
 - グレースフルリスタート アドレスファミリ → IPv4

→IPv4ユニキャスト

グレースフルリスタート	アドレスファミリ ☑IPv4ユニキャスト	
	staleタイマ	360 秒 💌

- 17. [保存] ボタンをクリックします。
- **18. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

横浜営業所を設定する

「東京営業所を設定する」を参考に、横浜営業所を設定します。

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

• IPv4	→使用する
• IPアドレス	→指定する
IPアドレス	→ 192.168.2.1
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「NAT情報」	
 NATの使用 	→使用しない
「WAN0 情報」	
• 回線インタフェース	→専用線

- ポート →スロット0-0
- 回線速度 → 128Kbps

「相手情報」-「ネットワーク情報」 ネットワーク名 →IP-VPN 「接続先情報」 • 接続先名 →ip-vpn • 接続先種別 →専用線接続 「接続先情報」-「専用線接続」 「基本情報」 • 使用インタフェース → WAN0 「ネットワーク情報」-「IP 関連」 「IP 基本情報」 • IPアドレス →設定する 相手側IPアドレス → 172.16.2.2 自側IPアドレス → 172.16.2.1 「ルーティングプロトコル情報」-「BGP関連」 「BGP情報」 • BGP機能 →使用する • 自AS番号 →65001 「BGPネットワーク情報」 • あて先IPアドレス → 192.168.2.0 あて先アドレスマスク →24 (255.255.255.0) 「BGP相手情報」-「BGP相手基本情報」 • 相手側 IP アドレス → 172.16.2.2 • 相手 AS 番号 **→**1

大阪営業所を設定する

「東京営業所を設定する」を参考に、大阪営業所を設定します。

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

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

NATの使用 →使用しない

「WAN0情報」

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

1

「相手情報」-「ネットワーク情報」 ネットワーク名 →IP-VPN 「接続先情報」 • 接続先名 →ip-vpn • 接続先種別 →専用線接続 「接続先情報」-「専用線接続」 「基本情報」 使用インタフェース → WAN0 「ネットワーク情報」-「IP 関連」 「IP 基本情報」 IPアドレス →設定する 相手側IPアドレス → 172.16.3.2 自側IPアドレス → 172.16.3.1 「ルーティングプロトコル情報」-「BGP関連」 「BGP情報」 • BGP機能 →使用する • 自AS番号 →65002 [BGP ネットワーク情報] • あて先IPアドレス → 192.168.3.0 あて先アドレスマスク →24 (255.255.255.0)

「BGP相手情報」-「BGP相手基本情報」

- 相手側IPアドレス → 172.16.3.2
- 相手AS番号 →1

<u>▲</u>注意

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

適用機種 全機種

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

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

適用機種 全機種

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

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

● 前提条件

【支社A(PPPoE常時接続)】

- ローカルネットワーク IP アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス
- PPPoEユーザ認証 ID
 PPPoEユーザ認証パスワード
 userpass1 (プロバイダから提示された内容)
 PPPoE LAN ポート
 ILAN0 ポート使用
 I支社B (PPPoE常時接続)]
 ローカルネットワークIPアドレス
 192.168.3.1/24
 - インターネットプロバイダから割り当てられた固定 IP アドレス
- : 202.168.3.66/24

 PPPoE ユーザ認証 ID
 : userid3 (プロバイダから提示された内容)

 PPPoE ユーザ認証パスワード
 : userpass3 (プロバイダから提示された内容)

 PPPoE LAN ポート
 : LAN0 ポート使用

[本社]

- ローカルネットワーク IP アドレス
- 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

: 192.168.2.1/24



● 設定条件

[支社A]

- ネットワーク名
- 接続先名
- IPsec/IKE区間
- IPsec対象範囲

[支社B]

- ネットワーク名
- 接続先名
- IPsec/IKE区間
- IPsec対象範囲

[本社]

- ネットワーク名
- 接続先名
- IPsec/IKE区間
- IPsec対象範囲
- ネットワーク名
- 接続先名

- : vpn-hon
- : honsya
- : 202.168.1.66 202.168.2.66
- : 192.168.1.0/24-any4
- : vpn-hon
- : honsya
- : 202.168.3.66 202.168.2.66
- : 192.168.3.0/24-any4
- : vpn-shiA
- : shisyaA
- : 202.168.2.66 202.168.1.66
- : any4-192.168.1.0/24
- : vpn-shiB
- : shisyaB

● IPsec/IKE区間	: 202.168.2.66 - 202.168.3.66
• IPsec対象範囲	: any4-192.168.3.0/24
[共通A]	
 鍵交換タイプ 	:Main Mode 使用
• IPsecプトロコル	esp
• IPsec暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
● IPsec DH グループ	:なし
● IKE 認証鍵	:abcdefghijkImnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: des-cbc
● IKE 認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768
[共通B]	
 鍵交換タイプ 	:Main Mode 使用
• IPsecプトロコル	: esp
● IPsec暗号アルゴリズム	: 3des-cbc
• IPsec認証アルゴリズム	: hmac-sha1
● IPsec DH グループ	:なし
● IKE 認証鍵	:ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321(文字列)
● IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: 3des-cbc
• IKE認証アルゴリズム	: hmac-sha1
● IKE DH グループ	: modp1024

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

♦ IKE とは? 自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社AのIPsec/IKEを設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続

機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

	⊙ Main Mode使用
建交換モ	相手側エンドボイ 202168266
-r-	ント 202.100.2.00
	自側エンドポイン 202.168.1.66

- 13. [保存] ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

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

	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc I des-cbc null	
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
	SA有効時間	8 時間 🗸	
	SA有効データ 量	0 GByte 💌	

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 鍵

→文字列

→ abcdefghijklmnopqrstuvwxyz1234567890

•	SAの 設定	
	暗号アルゴリズム	→des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-md5
	DHグループ	→modp768 (グループ1)

■IKE情報		3
IKE認証鍵	鍵識別	○16進数 ⊙文字列
	鍵	••••••
IKE認証方式	C,	shared
ポート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🖌

- 19. 【保存】ボタンをクリックします。
- 20. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

支社BのIPsec/IKEを設定する

「支社AのIPsec/IKEを設定する」を参考に、支社Bを設定します。

「相手情報」-「ネットワーク情報」 ネットワーク名 →vpn-hon 「ネットワーク情報」-「IP 関連」 「スタティック経路情報」 • ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.3.0 あて先アドレスマスク →24 (255.255.255.0) • メトリック値 **→**1 優先度 →0 「接続先情報」 • 接続先名 → honsya • 接続先種別 →IPsec/IKE 接続 「接続先情報」-「IPsec/IKE 接続」 「基本情報」 鍵交換モード → Main Mode 使用 相手側エンドポイント →202.168.2.66 自側エンドポイント →202.168.3.66 [IPsec 情報] • SAの設定 暗号アルゴリズム →3des-cbc 認証アルゴリズム →hmac-sha1 「IKE情報」 • IKE 認証鍵 鍵識別 →文字列 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321 • SAの設定 暗号アルゴリズム → 3des-cbc 認証(ハッシュ)アルゴリズム →hmac-sha1 DHグループ →modp1024

本社の IPsec/IKE を設定する

支社A向けの設定をする

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 -

<ネットワーク情報追加フィールド>		
ネットワーク名		vpn-shiA

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7. 以下の項目を指定します。

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

● 優先度 →0



- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

• 接続先名

- → shisyaA
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

	● Main Mode使用
鍵交換モ −ト	相手側エンドボイ 202.168.1.66
	自側エンドボイン 202.168.2.66

- 13. [保存] ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

 SAの設定 暗号アルゴリズム → des-cbc 認証アルゴリズム → hmac-md5
 暗号アルゴリ □aes-cbc-256 □aes-cbc-192 □aes-cbc-128 ズム □3docacho □docacho □ null

	ズム	🔲 3des-cbc 🗹 des-cbc 🗌 null		
SA	認証アルゴリ ズム	♥hmac-md5 □hmac-sha1 □認証なし 使用しない		
の設 定	PFS時のDHグ ルーブ			
	SA有効時間	8 時間 🖌		
SA有効データ 量		0 GByte 💌		

16. [保存] ボタンをクリックします。

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

「IKE情報」が表示されます。

18. 以下の項目を指定します。

 IKE 認証鍵 鍵識別

鍵

→文字列 →abcdefghijklmnopqrstuvwxyz1234567890

SAの設定
 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768 (グループ 1)

■IKE情報		3
IKE認証鍵	<mark>键</mark> 識別	○16進数 ⊙文字列
	鏈	••••••
IKE認証方式	C C	shared
ボート番号		500
SAの設定	暗号アルゴリズ ム	des-cbc 💌
	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🗸

- 19. [保存] ボタンをクリックします。
- **20.** 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

支社B向けの設定をする

「支社A向けを設定する」を参考に、支社B向けを設定します。			
「相手情報」-「ネットワーク情報」			
• ネットワーク名	→vpn-shiB		
「ネットワーク情報 - 「IP 関連」			
「スタティック経路情報」			
• ネットワーク	→ネットワーク指定		
あて先IPアドレス	→ 192.168.3.0		
あて先アドレスマスク	→24 (255.255.255.0)		
• メトリック値	→ 1		
● 優先度	$\rightarrow 0$		
「接続先情報」			
● 接続先名	→ shisyaB		
● 接続先種別	→IPsec/IKE 接続		
「接続先情報」-「IPsec/IKE接続」			
「基本情報」			
 鍵交換モード 	→ Main Mode 使用		
相手側エンドポイント	→202.168.3.66		
自側エンドポイント	→202.168.2.66		
「IPsec情報」			
• SAの設定			
暗号アルゴリズム	→3des-cbc		
認証アルゴリズム	→hmac-sha1		
「IKE情報」			
• IKE 認証鍵			
鍵識別	→文字列		
鍵	→ ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321		
 SAの設定 			
暗号アルゴリズム	→ 3des-cbc		
認証(ハッシュ)アルコリスム	→hmac-sha1		
DHシルーノ	→ moup 1024		

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

適用機種 全機種

IPsec機能を使って自動鍵交換でVPNを構築する場合の設定方法を説明します。
 ここでは以下の条件によって、支社Aおよび支社BはPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。
 ● 前提条件
[支社A]
 ・ ローカルネットワークIPアドレス
 : 192.168.1.1/24

インターネットプロバイダから割り当てられた固定 IP アドレス

: 202.168.1.66/24

- グローバルネットワーク IP アドレス : 10.0.1.1/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE LAN ポート : LANO ポート使用

[支社B]

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

[本社]

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



● 設定条件

[支社A]

- ネットワーク名
- 接続先名
- IPsec/IKE 区間
- IPsec対象範囲 ٠

[支社B]

- ネットワーク名 .
- 接続先名
- IPsec/IKE 区間 •
- IPsec 対象範囲 •

[本社]

- ネットワーク名
- 接続先名
- IPsec/IKE 区間
- IPsec対象範囲
- ネットワーク名
- 接続先名 •

- : vpn-hon
- : honsya
- : 10.0.1.1 202.168.2.66
- : 192.168.1.0/24-any4
- : vpn-hon
- : honsya
- : 10.0.3.1 202.168.2.66
- : 192.168.3.0/24-any4
- : vpn-shiA
- ∶ shisyaA
- : 202.168.2.66 10.0.1.1
- : any4-192.168.1.0/24
- : vpn-shiB
- : shisyaB
 - 157

● IPsec/IKE区間	: 202.168.2.66 - 10.0.3.1
• IPsec対象範囲	: any4-192.168.3.0/24
[共通A]	
 鍵交換タイプ 	:Main Mode 使用
• IPsecプトロコル	: esp
● IPsec 暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
● IPsec DH グループ	:なし
● IKE 認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: des-cbc
• IKE 認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768
[共通B]	
 鍵交換タイプ 	:Main Mode 使用
• IPsecプトロコル	: esp
● IPsec 暗号アルゴリズム	: 3des-cbc
● IPsec認証アルゴリズム	: hmac-sha1
● IPsec DHグループ	:なし
● IKE 認証鍵	:ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321(文字列)
● IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: 3des-cbc
• IKE認証アルゴリズム	: hmac-sha1
● IKE DH グループ	: modp1024

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

◆ IKE とは? 自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社Aを設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。

→ 10.0.1.1

→isakmp

→udp

4. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 202.168.1.66
 ポート番号 → isakmp

 グローバルIP情報
 - IPアドレス ポート番号
- プロトコル

<静的NAT情報入力フィールド>		
IPアト プライベート レス		202.168.1.66
IP情報 ボ· 番·	ボート 番号	isakmp ▼(番号指定: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
グローバル IP情報	IPアド レス	10.0.1.1
	ボート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
プロトコル		udp ✓(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

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

9. 画面上部の「相手情報」をクリックします。

 「相手情報」ページが表示されます。

10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

- 11. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

12. [追加]ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

13. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

14. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 15. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先 IP アドレス
 → 192.168.2.0
 → 24 (255.255.255.0)

→0

- メトリック値 →1
- 優先度

<スタティック経路情報入力フィールド>			
ネットワーク	 ○デフォルトルート ③ネットワーク指定 あて先IPアドレス 192.168.2.0 あて先アドレスマスク 24 (255.255.2) 		
メトリック値	1 💌		
優先度	0		

16. [追加] ボタンをクリックします。

17. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

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

	⊙ Main Mode使用	
鍵交換モ →ト	相手側エンドボイント	
	自側エンドポイン ト 202.168.1.66	

- 21. [保存] ボタンをクリックします。
- **22.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

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

暗号アルゴリ ズム ③des-cbc- ③des-cbc- ③des-cbc- ③des-cbc- ③des-cbc- ◎des-cbc- ◎des-cb	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ⊻des-cbc null
	▼hmac-md5 □hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない 🗸
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 💌

24. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

26. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 鍵

→文字列

鍵 → abcdefghijklmnopqrstuvwxyz1234567890 • SAの設定

暗号アルゴリズム	→des-cbc
認証(ハッシュ)アルゴリズム	→hmac-md5
DHグループ	→modp768(グループ 1)

■IKE情報		3
	鏈識別	○16進数 ⊙文字列
IKE認証規	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグルーブ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🖌

- 27. 【保存】ボタンをクリックします。
- 28. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

支社Bを設定する

「支社Aを設定する」を参考に、支社Bを設定します。

「朴	目手情報」-「ネットワーク情報	员」
۲Ż	、ットワーク情報」-「IP 関連」	
「靔	的NAT情報」	
•	プライベートIP情報	
	IPアドレス	→202.168.3.66
	ポート番号	→isakmp
•	グローバル IP 情報	
	IPアドレス	→10.0.3.1
	ポート番号	→isakmp
•	プロトコル	→udp
•	プライベートIP情報	
	IPアドレス	→202.168.3.66
	ポート番号	→すべて
•	グローバル IP 情報	
	IPアドレス	→10.0.3.1
	ポート番号	→すべて
•	プロトコル	→esp
「朻	目手情報」-「ネットワーク情報	员」
•	ネットワーク名	→vpn-hon
「ネ	ヽットワーク情報」-「IP 関連」	
۲Z	マンジョン マンション マンション マンション マンシン マンション マンシン マンシ	
•	ネットワーク	→ネットワーク指定
	あて先 IP アドレス	→192.168.2.0
	あて先アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→ 1
•	優先度	→0
「挼	続先情報」	
•	接続先名	→honshya
•	接続先種別	→IPsec/IKE 接続
「挼	続先情報」-「IPsec/IKE接続」	
「基	基本情報」	
•	鍵交換モード	→ Main Mode 使用
	相手側エンドポイント	→202.168.2.66
	自側エンドポイント	→202.168.3.66
ΓIF	Psec情報」	
•	SAの 設定	
	暗号アルゴリズム	→3des-cbc

認証アルゴリズム →hmac-sha1

「IKE情報」

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

→ modp1024

本社の IPsec/IKE を設定する

支社A向けの設定をする

DHグループ

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shiA

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shiA

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先 IP アドレス → 192.168.1.0
 あて先アドレスマスク → 24 (255.255.255.0)
 - メトリック値 →1
 優先度 →0



8. [追加] ボタンをクリックします。

9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

10. 以下の項目を指定します。

• 接続先名

- → shisyaA
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

- 12. 以下の項目を指定します。
 - 鍵交換モード 相手側エンドポイント 自側エンドポイント

→ Main Mode 使用 → 10.0.1.1 → 202.168.2.66

	◎ Main Mode使用
鍵交換モ ート	相手側エンドボイ 10.0.1.1
	自側エンドポイン 202.168.2.66

13. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

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

IPs	■IPsec情報(自動鍵)		
対象	自側IPアドレ ス/マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/ブレフィックス長形式で入力してください。	
ット	相手側IPアド レス/マスク	指定する べ"指定する"を選択時のみ有効です。) 192.168.1.0 ※IPv4アドレス/マスクビット形式もしく(はIPv6アドレ ス/プレフィックス長形式で入力してください。	
	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
	SA有効時間	8 時間 🖌	
	SA有効データ 量	0 GByte 🗸	

- 16. [保存] ボタンをクリックします。
- **17.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

166

٠	IKE 認証鍵	
	鍵識別	→文字列
	鍵	→abcdefghijklmnopqrstuvwxyz1234567890
•	SAの設定	

暗号アルゴリズム	→des-cbc
認証(ハッシュ)アルゴリズム	→hmac-md5
DHグループ	→modp768(グループ 1)

■IKE情報		3
	<mark>键</mark> 識別	◎16進数 ④文字列
IKE認証規	键	••••••
IKE認証方式	¢.	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🗸

- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

支社B向けの設定をする

「支社A向けを設定する」を参考に、支社Bを設定します。

「相手情報」-「ネットワーク情報」

•	ネットワーク名	→vpn-shiB
۲đ	ネットワーク情報」-「IP 関連」	
۲2	スタティック経路情報」	
•	ネットワーク	→ネットワーク指定
	あて先 IP アドレス	→192.168.3.0
	あて先アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→ 1
•	優先度	→ 0
旧招	接続先情報」	
•	接続先名	→shisyaB
•	接続先種別	→IPsec/IKE 接続
旧招	接続先情報」-「IPsec/IKE接続」	
围	基本情報」	
•	鍵交換モード	→ Main Mode 使用
	相手側エンドポイント	→ 10.0.3.1
	自側エンドポイント	→202.168.2.66

「IPsec情報」

•	対象パケット	
	自側 IP アドレス/マスク	→IPv4すべて
	相手側IPアドレス/マスク	→指定する
		→ 192.168.3.0/24

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

「IKE情報」

IKE 認証鍵
 鍵識別 →文字列
 鍵 →ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321

•	SAの 設定	
	暗号アルゴリズム	→3des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-sha1
	DHグループ	→modp1024

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

適用機種 全機種

接続するたびにIPアドレスが変わる環境でVPNを構築する場合の設定方法を説明します。 ここでは、以下の条件によって、支社Aおよび支社BはPPPoEでインターネットに接続され、本社はグローバル アドレス空間のVPN 終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社A (PPPoE 接続)]

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

【支社B(PPPoE 接続)】

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

[本社]

ローカルネットワーク IP アドレス

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



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 ٠
- IKE (UDP: 500番ポート) のプライベートアドレス ٠
 - : 192.168.3.1
- ESPのプライベートアドレス : 192.168.3.1

[本社]

• ネットワーク名	: vpn-shiA
● 接続先名	: shisyaA
● IPsec/IKE区間	:202.168.2.66 - 支社A
● IPsec 対象範囲	: any4-192.168.1.0/24
• ネットワーク名	: vpn-shiB
• 接続先名	: shisyaB
● IPsec/IKE区間	:202.168.2.66 - 支社 B
● IPsec対象範囲	: any4-192.168.3.0/24
[共通A]	
 鍵交換タイプ 	: Aggressive Mode
• IPsecプトロコル	: esp
• IPsec 暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
● IPsec DH グループ	:なし
● IKE支社AID/IDタイプ	:shisyaA(自装置名)/FQDN
● IKE認証鍵	:abcdefghijkImnopqrstuvwxyz1234567890(文字列)
● IKE 認証方法	: shared
• IKE 暗号アルゴリズム	: des-cbc
• IKE認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768
[共通B]	
 鍵交換タイプ 	: Aggressive Mode
• IPsecプトロコル	: esp
• IPsec 暗号アルゴリズム	: 3des-cbc
• IPsec認証アルゴリズム	: hmac-sha1
● IPsec DHグループ	:なし
● IKE支社BID/IDタイプ	:shisyaB(自装置名)/FQDN
● IKE認証鍵	:ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321(文字列)
● IKE認証方法	: shared
● IKE暗号アルゴリズム	: 3des-cbc
• IKE認証アルゴリズム	: hmac-sha1
● IKE DH グループ	: modp1024

☆ ヒント

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

♦ ID タイプとは?

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

こんな事に気をつけて

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社A(Initiator)を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3.** 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 192.168.1.1
 ポート番号 → isakmp

 グローバルIP情報
- ・ ノロ ハの市 備報
 IPアドレス →指定しない
 ポート番号 → isakmp
- プロトコル → udp



7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

•	プライベート IP 情報	
	IPアドレス	→ 192.168.1.1
	ポート番号	→すべて
•	グローバル IP 情報	
	IPアドレス	→指定しない

- ポート番号 →すべて • プロトコル → esp
- 画面上部の「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- **10. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 11. 以下の項目を指定します。

● ネットワーク名	→ vpn-hon
<ネットワー:	ク情報追加フィールド>
ネットワーク名	vpn-hon

12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

13. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

- **14.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 15. 以下の項目を指定します。

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

● 優先度

	<スタティック経路情報入力フィールド>
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先IPアドレス 192.168.2.0 あて先アドレスマスク 24 (255.255.2)
メトリック値 優先度	

→0

- 16. [追加] ボタンをクリックします。
- **17. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント 自装置識別情報

→ Aggressive Mode (Initiator) 使用 → 202.168.2.66 → shisyaA

	⊙ Aggressive Mode(Ir	nitiator)使用
	自側エンドボイン ト	
鍵交換モ ート	相手側エンドポイ ント	202.168.2.66
	自装置識別情報	shisyaA
	IDタイプ	⊙ FQDN ◯ User-FQDN

21. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

23. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5



24. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

26. 以下の項目を指定します。

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

■IKE情報		3
14 다르지르지 수례	鏈識別	○16進数 ⊙文字列
INERGIERE	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🖌

27. [保存] ボタンをクリックします。

28. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

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

支社B(Initiator)を設定する

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

「相手情報」-「ネットワーク情報」 「ネットワーク情報」-「IP 関連」 「静的NAT情報」 • プライベート IP 情報 IPアドレス → 192.168.3.1 ポート番号 →isakmp • グローバル IP 情報 IPアドレス →指定しない ポート番号 →isakmp • プロトコル → udp • プライベート IP 情報 IPアドレス → 192.168.3.1 →すべて ポート番号 • グローバル IP 情報 IPアドレス →指定しない ポート番号 →すべて プロトコル →esp 「相手情報」-「ネットワーク情報」 ネットワーク名 →vpn-hon 「ネットワーク情報」-「IP 関連」 「スタティック経路情報」 ネットワーク →ネットワーク指定 あて先 IP アドレス → 192.168.2.0 あて先アドレスマスク →24 (255.255.255.0) メトリック値 →1 優先度 →0 「接続先情報」 • 接続先名 → honshya • 接続先種別 →IPsec/IKE 接続 「接続先情報」-「IPsec/IKE接続」 「基本情報」 鍵交換モード → Aggresive Mode (Initiator) 使用 相手側エンドポイント →202.168.2.66 自装置識別情報 → shisyaB 「IPsec情報」 • SAの設定 暗号アルゴリズム → 3des-cbc 認証アルゴリズム →hmac-sha1

「IKE情報」

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

本社(Responder)を設定する

支社A向けの設定をする

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shiA

<ネットワーク情報	<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-shiA		

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先 IP アドレス
 → 192.168.1.0
 → 24 (255.255.255.0)
 - メトリック値 →1
 - 優先度 →0
 <スタティック経路情報入力フィールド>
 ○デフォルトルート
 ③ネットワーク指定

÷ – –	۰	ネットワーク指定		
ネットワーク		あて先IPアドレス	192.168.1.0	
		あて先アドレスマスク	24 (255.255.255.0)	~
メトリック値	1	~		
偏先度	n			

8. [追加] ボタンをクリックします。

9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

10. 以下の項目を指定します。

● 接続先名

- → shisyaA
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

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

→shisyaA

→des-cbc

→hmac-md5

	⊙ Aggressive Mode(Responder)使用
	自側エンドボイン 202.168.2.66
鍵交換モ ート	相手側エンドボイ ノト
	相手装置識別情 報
	IDタイプ O FQDN O User-FQDN

- 13. 【保存】ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

• 対象パケット	
自側 IP アドレス/マスク	→IPv4すべて
相手側IPアドレス/マスク	→指定する
	→192.168.1.0/24

SAの設定
 暗号アルゴリズム
 認証アルゴリズム

	IPsec情報(自動鍵)				
対象 バケ ット	自側IPアドレ ス/マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしく(はIPv6アドレ ス/プレフィックス長形式で入力してください。			
	/ 1 <i>)</i> ット	相手側IPアド レス/マスク	指定する 「指定する"を選択時のみ有効です。) 192.168.1.0 ※IPv4アドレス/マスクビット形式もしく(ゴIPv6アドレ ス/プレフィックス長形式で入力してください。		
		暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null		
SA の設 定	SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし		
	の設 定	PFS時のDHグ ルーブ	使用しない		
		SA有効時間	8 時間 🖌		
		SA有効データ 量	0 GByte 💌		

- 16. 【保存】ボタンをクリックします。
- **17.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

٠	IKE 認証鍵	
	鍵識別	→文字列
	鍵	→abcdefghijklmnopqrstuvwxyz1234567890
•	SAの設定	

暗号アルゴリズム	→des-cbc
認証(ハッシュ)アルゴリズム	→hmac-md5
DHグループ	→modp768(グループ 1)

■IKE情報		3
	<mark>键</mark> 識別	○16進数 ⊙文字列
IKE認証援	鍵	••••••
IKE認証方式		shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 💙

- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

支社B向けの設定をする

「支社A向けを設定する」を参考に、支社B向けを設定します。

「相手情報」-「ネットワーク情報」

 ネットワーク名 →vpn-shiB 「ネットワーク情報」-「IP 関連」 「スタティック経路情報」 • ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.3.0 あて先アドレスマスク →24 (255.255.255.0) • メトリック値 **→**1 **→**0 優先度 「ネットワーク情報」-「接続先情報」 • 接続先名 →shisyaB • 接続先種別 →IPsec/IKE 接続 「接続先情報」-「IPsec/IKE接続」 「基本情報」 鍵交換モード → Aggresive Mode (Responder) 使用 自側エンドポイント →202.168.2.66 相手装置識別情報 → shisyaB
「IPsec情報」

٠	対象パケット	
	自側 IP アドレス/マスク	→IPv4すべて
	相手側IPアドレス/マスク	→指定する
		→ 192.168.3.0/24

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

「IKE情報」

•	IKE 認証鍵	
	鍵識別	→文字列
	鍵	→ABCDEFGHI
	鍵	→ABCDEFGH

→ X 字列 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321

•	SAの 設定	
	暗号アルゴリズム	→3des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-sha1
	DHグループ	→modp1024S

1.15 IPv6の事業所LANをISDNで接続する

適用機種 Si-R220B,220C,370,570

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

こんな事に気をつけて

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

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

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



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート(Si-R220B、220Cの場合) で ISDN(64Kbps)を使用する
- IPv6を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名 : kaisya 無通信監視時間を1分とする [東京事業所] ネットワークアドレス/プレフィックス長 : 2001:db8:1111:1000::/64 接続先名 : tokyo • 電話番号 : 03-7777-7777 ユーザ認証 ID とユーザ認証パスワード 発信 : tokyo, tokyopass 着信 : kawasaki, kawapass
- IPv6 の事業所 LAN を ISDN で接続する

[川崎事業所]

- ネットワークアドレス/プレフィックス長
- 接続先名
- 電話番号
- ユーザ認証 ID とユーザ認証パスワード 発信 着信
- こんな事に気をつけて

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

: kawasaki

: 044-999-9999

: 2001:db8:1111:1001::/64

: kawasaki, kawapass

: tokyo、 tokyopass

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

東京事業所を設定する

WAN0 情報を設定する

- **1. 設定メニューのルータ設定で「WAN 情報」をクリックします**。 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース → ISDN

【追加】ボタンをクリックします。
 「WAN0情報(ISDN)」ページが表示されます。

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- IPv6 →使用する
 インタフェースID →自動
 IPv6アドレス アドレスまたはプレフィックス →2001:db8:1111:1000::
- Valid Lifetime
 → 30日

 Pref. Lifetime
 → 7日

 フラグ
 → c0

 ・
 ルータ広報

	■IPv6基本情報												
IF	<mark>v6</mark>	○使用しない●使用する											
イタェス	シーフー」	0 0	 ● 自動 ○ 指定する 										
		アド	レスまたはプレフ	ィックス		Valid Life <mark>期限有</mark>	time <u>‡</u>	無期限	Pref. Life 期限有	time 魚	無期限	フラ グ	
IF	IPv6	2001:db8:1111:1000::				30	Β	¥ 🗌	7	B	¥ 🗌	cO	
V	トス					30	Β	¥ 🗌	7	Β	¥ 🗌	cO	
						30	Β	¥ 🗆	7	Β	¥ 🗌	c0	
						30	Β	¥ 🗌	7	В	¥ 🗌	cO	
		0 0	送信しない 送信する										
			最大送信間隔	600	利	少							
			最小送信間隔	200	Į₹	少							
л	,		Router Lifetime	1800	利	少							
タ転	広		MTU]								
TP	`		Reachable Time	0	3	り秒							
			Retrans Timer	0	3	り秒							
			Cur Hop Limit	64]								
			フラグ	00]								

5. [保存] ボタンをクリックします。

相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。

ネットワーク名 → kaisya

<ネットワーク情報追加フィールド>						
ネットワーク名	kaisya					

4. [追加] ボタンをクリックします。

「ネットワーク情報(kaisya)」ページが表示されます。

5. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

6. 以下の項目を指定します。

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



機種により、接続先種別の表示が上記の画面とは異なります。

7. [追加] ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

ISDN 接続の設定項目の「PPP 情報」をクリックします。
 「PPP 情報」が表示されます。

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

PPP情報	報	3
認証方式		P
送信認証 情報	認証ID 認証バスワー ド	tokyo
受諾認証 情報	認証ID 認証バスワー ド	kawasaki

10. [保存] ボタンをクリックします。

11. ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

12. 以下の項目を指定します。

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

■接続制御	印情報	3
常時接続 機能	⊙使用しない○使用する	
無通信監 視タイマ	送受信パケット 🗸 について 60 秒	

13. [保存] ボタンをクリックします。

14. 画面上部の「ネットワーク情報 (kaisya)」をクリックします。

「ネットワーク情報(kaisya)」ページが表示されます。

15. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

•	IPv6	→使用する
•	インタフェースID	→自動
•	IPv6アドレス	→指定しない

ルータ広報 →送信しない

■IPv6基本情報													
IPv6	○使用しない◎使用する												
インフェフレス	0	 ● 自動 ○ 指定する 											
	איק	レスまたはプレフ		Valic 期限	I Life 【有	time £	無期	限	Pref. Lifetime 期限有 無期限			フラ グ	
IPv6					30		Β	*		7	В	~	c0
アトレス				30		В	*		7	B	¥	c0	
					30		B	¥		7	B	*	c0
					30		В	*		7	B	×	c0
	 	送信しない 送信する											
		最大送信間隔	600	Į₹	少								
		最小送信間隔	200	Ŧ	少								
ルー		Router Lifetime	1800]₹	少								
タ広報		MTU]									
тк		Reachable Time	0	3	り秒								
		Retrans Timer	0	3	り 秒								
		Cur Hop Limit	64]									
		フラグ	00]									

こんな事に気をつけて

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

- 一方の装置で着信接続を優先する。
- 一方の装置で接続優先制御を行わない。
- 17. [保存] ボタンをクリックします。

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

「IPv6スタティック経路情報」が表示されます。

- ネットワーク あて先ネットワーク/プレフィックス長
- メトリック値

- →ネットワーク指定 → 2001:db8:1111:1001::/64
- **→** 1 →0

優先度

- <IPv6スタティック経路情報入力フィールド> ○デフォルトルート ⊙ ネットワーク指定 ネットワーク あて先ブレフィ ックス/ブレフ ィックス長 64 メトリック値 1 🔽 優先度 0
- [追加] ボタンをクリックします。 20.
- 21. 画面左側の [再起動] ボタンをクリックします。

設定した内容が有効になります。

▲注意 -

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

川崎事業所を設定する

「東京事業所を設定する」を参考に、川崎事業所を設定します。

「WAN0 情報」

 回線インタフェース → ISDN

「LAN0 情報」-「IPv6 関連」

「IPv6基本情報」

•	IPv6	→使用する
•	インタフェースID	→自動
•	IPv6アドレス	
	アドレスまたはプレフィックス	→2001:db8:1111:1001
	Valid Lifetime	→30日
	Pref. Lifetime	→7日
	フラグ	→c0
•	ルータ広報	→送信する
Гŧ	目手情報」-「ネットワーク情報」	

ネットワーク名

→ tokyo

		+
接続	无情	報目

•	接続先名	→tokyo
•	接続先種別	→ISDN 接続
		→通常接続
	ダイヤル1	
	電話番号	→03-7777-7777
	サブアドレス	→指定しない
「接	続先情報」-「ISDN 接続」	
ΓPF	P情報」	
•	認証方式	→ PAP、CHAP
•	送信認証情報	
	認証ID	→kawasaki
	認証パスワード	→kawapass
•	受諾認証情報	
	認証ID	→ tokyo
	認証パスワード	→ tokyopass
「接	続制御情報」	
•	常時接続情報	→使用しない
•	無通信監視タイマ	→送受信パケットについて60秒
「相	手情報」-「IPv6関連」	
ΓΙΡν	v6基本情報」	
•	IPv6	→使用する
•	インタフェースID	→自動
•	IPv6アドレス	→指定しない
•	ルータ広報	→送信しない
ΓIΡν	v6スタティック経路情報」	
•	ネットワーク	→ネットワーク指定
	あて先ネットワーク/プレフィックス長	→ 2001:db8:1111:1000::/64
•	メトリック値	→1
•	優先度	→ 0

1.16 IPv6の事業所LAN を IPv6 トンネルで接続する

適用機種 全機種

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



● 設定条件

[東京事業所]

- ダイナミックルーティングを使用する
- LAN0 側の IPv4 アドレス
- LAN1 側の IPv4 アドレス
- LAN1 側の IPv6 プレフィックス / プレフィックス長

[川崎事業所]

- ダイナミックルーティングを使用する
- LAN0 側の IPv4 アドレス
- LAN1 側の IPv4 アドレス
- LAN1 側の IPv6 プレフィックス/プレフィックス長
- ※) この例では、プライベートアドレス(IPv4)/ドキュメント記述用アドレス(IPv6)を使用しています。

こんな事に気をつけて

- ・ 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。
 - 参照 Si-Rシリーズ Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.19)
- IPv6 over IPv4 トンネルを利用する場合は、カプセル化された IPv4 パケットのフラグメントを防ぐため、トンネルに 利用する相手情報の MTU に 1280 を設定してください。
- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

- : 172.16.184.1
- : 172.16.185.1

: 2001:db8:1111:10b9::/64 (※)

- : 172.16.21.1
- : 172.16.22.1
- : 2001:db8:1111:1016::/64 (※)

東京事業所の本装置を設定する

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →172.16.184.1
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報								
IPv4	⊙使用する○使用しない							
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 172.16.184.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 							

- 5. [保存] ボタンをクリックします。
- 6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

- 7. 以下の項目を指定します。
 - RIP送信 → V1 で送信する
 - • RIP受信
 → V1 で受信する

RIP情報	3
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する
RIP受信	○受信しない ● V1で受信する ● V2、V2(Multicast)で受信する

- 8. [保存] ボタンをクリックします。
- 9. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

DHCP機能
 →使用しない

DHC	P帽	報			3
	۲	使用しない	1		
	0	リレー機能	能を使用する	5	
		DHCPサ	ーバIPアドレ	,ス1	
		DHCPサ	ーバIPアドレ	,ス2	
		мастк	レスチェック		 □ホストデータベース □ AAA 参照するAAA情報
	0	サーバ機	能を使用す	3	
		割当て先 ス	頭IPアドレ		
		割当てア	ドレス数	32	
		リース期	38	1	
		デフォルトルータ広 報			
DHCP		DNSサ ーバ広 報	プライマリ		
機能			セカンダリ		
		ドメイン名	。 広報		
		TIMEサーバ広報			
		NTPサーバ広報			
		WINSサ	プライマリ		
		報	セカンダリ		
		NK SIPサー バ広報	記述形式	<u>الا</u>	メイン名 OIPアドレス
			プライマリ		
			セカンダリ		
		MACアドレスチェッ ク		∎∄	マストデータベース
				□ AAA 参照するAAA情報	
		※"割当で ークアドレ	「先頭アドレ ス内である	ス"カ ことを	「本装置のIPアドレスと同じネットワ」 「確認してください。

11. [保存] ボタンをクリックします。

12. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

13. 以下の項目を指定します。

NATの使用 →使用しない

■NAT情報	3
NATの使用	●使用しない ○NAT ○マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

14. [保存] ボタンをクリックします。

LAN1情報を設定する

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

1. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 172.16.185.1
 ネットマスク → 24 (255.255.255.0)

ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報								
IPv4	●使用する ○使用しない							
IP アド レス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス I72.16.185.1 ネットマスク 24 (255.255.0) 							
	ブロードキャストアドレ ス ネットワークアドレス+オール1							

- 5. [保存] ボタンをクリックします。
- **6.** IP **関連の設定項目の「RIP 情報」をクリックします**。 「RIP 情報」が表示されます。
- 7. 以下の項目を指定します。
 - RIP送信 → V1 で送信する
 - • RIP受信
 → V1 で受信する

R	IP情報	3
RIP	送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する
RIP	受信	○受信しない ●V1で受信する ●V2、V2(Multicast)で受信する

- 8. [保存] ボタンをクリックします。
- **9.** IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP 情報」が表示されます。

DHCP機能
 →使用しない

DHC	P情	報			3	
	۲	使用しない	1			
	0	リレー機能	能を使用する	5		
		DHCPサ	ーバIPアドレ	,ス1		
		DHCPサ	ーバIPアドレ	、ス2		
		MACアドレスチェック		,	 □ホストデータベース □ AAA 参照するAAA情報 	
	0	サーバ機	能を使用す	る		
		割当て先頭IPアドレ ス				
		割当てア	ドレス数	32		
		リース期	8	1		
		デフォルトルータ広 報				
DHCP		DNSサ	プライマリ			
機能		報	セカンダリ			
		ドメイン名	站広報			
		TIMEサーバ広報				
		NTPサーバ広報				
		WINSサ	プライマリ			
		ーハム 報	セカンダリ			
			記述形式	<u>ا</u> ۲	メイン名 OIPアドレス	
		SIPサー バ広報	プライマリ			
		/ 1 <u>/</u> 24ŦIX	セカンダリ			
		MACZH	レスチェッ	∎≉	マントデータベース	
		かいり FUX J エッ		□ AAA 参照するAAA情報		
		※"割当で ークアドレ	「先頭アドレ ス内である	ス"カ ことを	「本装置のIPアドレスと同じネットワ 確認してください。	

11. 【保存】ボタンをクリックします。

12. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

13. 以下の項目を指定します。

NATの使用 →使用しない

■NAT情報	3
NATの使用	●使用しない ○NAT ○マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

14. [保存] ボタンをクリックします。

LAN情報(東京事業所)を設定する

設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. 以下の項目を指定します。

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

	■IPv6基本情報											
]	IPv6	0	○使用しない●使用する									
-	インタフェースID	 ● 自動 ○ 指定する 										
		アドレスまたはプレフィックス				Valid Lifetime Pref. Lifetime 期限有 無期限 期限有 無				無期限	フラ グ	
]	IPv6	2001:db8:1111:10b9::				30	Β	¥ 🗌	7	Β	¥ 🗌	c0
	アトレス					30	Β	¥ 🗌	7	B	*	cO
						30	B	*	7	B	*	cO
						30	Β	¥ 🗌	7	В	¥ 🗌	c0
		0 0	送信しない 送信する									
			最大送信間隔	600	秒							
			最小送信間隔	200	秒							
	ルー		Router Lifetime	1800	秒							
	タ広 報		MTU]							
			Reachable Time	0]₹!	飏						
			Retrans Timer	0]₹!	飏						
			Cur Hop Limit	64]							
			フラグ	00]							

5. [保存] ボタンをクリックします。

IP トンネル接続の情報(川崎事業所)を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。

「ネットワーク情報」が表示されます。

- 2. 以下を指定します。
 - ネットワーク名

→v6kawasa (接続するネットワークの名称)

<ネットワーク情報追加フィールド>		
ネットワーク名	v6kawasa	

3. [追加] ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

- 4. 「共通情報」をクリックします。 共通情報の設定項目と「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - MTUサイズ →1280

MTUサイズ 1280 バイト

- 6. [保存] ボタンをクリックします。
- 7. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

- 8. 以下を指定します。
 - 接続先名 →tun-kawa
 - 接続先種別 → IP トンネル接続

<接続先情報追加フィールド>				
接続先名	tun-kawa			
接続先種別	 ATM接続 マ可用線接続 ・ 通常接続			

機種により、接続先種別の表示が上記の画面とは異なります。

9. [追加] ボタンをクリックします。

IP トンネル接続の設定項目と「基本情報」が表示されます。

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

自側エントポイント	172.16.184.1	
相手側エントボイント	172.16.21.1	

- 11. [保存] ボタンをクリックします。
- **12. 画面上部の「ネットワーク情報」をクリックします**。 「ネットワーク情報」ページが表示されます。
- 13. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

- 14. 以下の項目を指定します。
 - IPv6 →使用する

IP√	6基本情報
IPv6	○使用しない ◎使用する

- 15. [保存] ボタンをクリックします。
- **16.** IPv6 **関連の設定項目の「IPv6 スタティック経路情報」をクリックします**。 「IPv6 スタティック経路情報」が表示されます。
- 17. 以下の項目を指定します。
 - ネットワーク → あて先ネットワーク/プレフィックス長 →
 - メトリック値

→ネットワーク指定 →2001:db8:1111:1016::/64

→1

3

- <IPv6スタティック経路情報入力フィールド>
 デフォルトルート
 ネットワーク指定
 あて先ブレフィーックス/ブレフィックス/ブレフィックス人、
 メトリック値 1
- 18. [追加] ボタンをクリックします。
- **19. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

川崎事業所の本装置を設定する

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

LAN情報(川崎事業所)を設定する

「LAN0 情報」-「IP 関連」

「IPアドレス情報」

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

「LAN1情報」-「IP関連」

「IPアドレス情報」

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

「LAN1情報」-「IPv6 関連」

「IPv6基本情報」

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

IP トンネル接続の情報(東京事業所)を設定する

「相手情報」-「ネットワーク情報」 • ネットワーク名	→v6tokyo(接続するネットワークの名称)
「ネットワーク情報」-「共通情報」 「基本情報」	
• MTUサイズ	→ 1280
「ネットワーク情報」-「Pv6 関連」	
「IPv6基本情報」	
• IPv6	→使用する
「IPv6スタティック経路情報」	
 ネットワーク 	→ネットワーク指定
あて先ネットワーク/プレフィックス長	→2001:db8:1111:10b9::/64
 メトリック値 	→ 1

「接続先情報」

•	接続先名	→ tun-tkyo			
•	接続先種別	→ IP トンネル接続			
「授	「接続先情報」- 「IP トンネル接続」				
「基	「基本情報」				
•	自側エンドポイント	→ 172.16.21.1			
•	相手側エンドポイント	→ 172.16.184.1			

₩Ŷ**Ĕ**

◆ NATとIPv6 over IPv4 トンネルを併用する

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

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

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

具体例を以下に示します。

条件:

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

IPv6 over IPv4 トンネル接続:

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

静的 NAT 設定:

• プライベートIP情報				
IPアドレス	192.168.1.1			
ポート番号	すべて			
 グローバル IP 情報 				
IPアドレス	172.16.0.1			
ポート番号	すべて			
・ プロトコル	IPv6 over IPv4			
なお、この具体例で、相手ト	ヽンネル GW の設定は、以下のとおりです。			
172.16.0.1と172.31.0.1の間でトンネル通信を行うことを前提とします。				
相手トンネル GW に Si-R シ	リーズ(NAT 未使用)を利用する場合は、相手側の Si-R に以下を設定します。			
自側エンドポイント	172.31.0.1			
相手側エンドポイント	172.16.0.1			



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)		205	
	2.1.1	特定の経路情報の送信を許可する.................................	207
	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.............	209
	2.1.3	特定の経路情報の受信を許可する....................................	211
	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.............	213
	2.1.5	特定の経路情報の送信を禁止する....................................	216
	2.1.6	特定の経路情報の受信を禁止する....................................	218
2.2	RIP の	経路を制御する (IPv6)	220
	2.2.1	特定の経路情報の送信を許可する..................................	222
	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............	224
	2.2.3	特定の経路情報の受信を許可する...................................	226
	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.............	228
	2.2.5	特定の経路情報の送信を禁止する.................................	231
	2.2.6	特定の経路情報の受信を禁止する..................................	233
2.3	OSPF\	v2を使用したネットワークを構築する(IPv4)	235
	2.3.1	バーチャルリンクを使う	243
	2.3.2	スタブエリアを使う	251
2.4	OSPF	の経路を制御する (IPv4)	263
	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	263
	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	266
	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	269
2.5	OSPF	: 機能を使う(IPv6)	273
	2.5.1	OSPF ネットワークを構築する	
	2.5.2	エリア境界ルータでエリア内部経路を集約する	
	2.5.3	エリア境界ルータで不要な経路情報を遮断する	
2.6	BGP 0	D経路を制御する (IPv4)	
	2.6.1	特定の経路情報の受信を透過させる	
	2.6.2	特定のASからの経路情報の受信を遮断する	
	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	
	2.6.4	冗長構成の通信経路を使用する	
2.7	事業所		
	2.7.1	トンネルエンドポイントをインタフェースアドレスにして MPLS LSP を使用する	
	2.7.2	トンネルエンドポイントをインタフェースアドレスとは別のアドレスにして MPLS LSPを値	使用する.302
2.8	MPLS	を使用したレイヤ2VPN(EoMPLS)を構築する	

2.9	MPLS 경	を使用したレイヤ 3VPN(BGP/MPLS VPN)を構築する	. 321
	2.9.1	MPLS網とLANを使用して接続する	. 322
	2.9.2	MPLS網と専用線を使用して接続する	. 333
2.10	マルチリ	リンク機能を使う	. 343
	2.10.1	ISDN でマルチリンク機能を使う	. 343
	2.10.2	複数専用線でマルチリンク機能を使う	. 346
	2.10.3	専用線とISDN 回線でマルチリンク機能を使う	. 352
2.11	マルチョ	キャスト機能を使う	359
	2 11 1	マルチキャスト操能(PIM_DM)を使う	359
	2.11.1	マルチュャスト機能 (PIM_SM) を使う	363
	2 11 3	マルチェッスト機能(スタティックルーティング)を使う	368
2 1 2	2.11.5 VIΔN档	、 ルノ キャスト 100 ビ (スノノ キノノル・ノ キノノ) を ビ フ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	372
2.12		。 加セレング機能を使う	376
2.10	2 13 1	りょうしょう。 「外部の特定サービスへのアクセスだけ許可する	380
	2.10.1	りつめれたり ビス (の) ノビスにり 計写する	301
	2.10.2	りつかりしれたり、ハベックノンスにり計りする・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	409
	2.13.0	ノロックマンクロング (Dys フィルタリング)	. 4 03 121
	2.13.4	りつめ特定サービス、のアクセスだけ計画する(11000年かりラフラ)	421
	2.13.5	「「中の存足」「ハベのノノビスに」を示正する	/38
	2.13.0	利用省が急回しない元后と向く、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、	. 430
	2.13.7	四秋が安航していることにに計りする	. 443
2 4 4	2.13.0 IDeee 档	「Yren/ごう存在り」///、のping/こりを示正する	. 440
2.14	2 4 4 4	SILではフ	. 452
	2.14.1	IF V4 OVELIF V4 C回とIF アドレスCO VFN(于到鍵文傑)	. 450
	2.14.2	IF V4 OVER IF V0 C回とIF アドレスCO VFN(日勤雑文傑)	. 404
	2.14.3	IPv4 over IPv6 C可変IPアドレスCのVPN(日朝鍵文換)	. 472
	2.14.4	IPv6 over IPv4 で回走 IP アトレス Cの VPN(日朝鍵交換)	. 480
	2.14.5	IPv6 over IPv4 で可変IPアトレスでのVPN(自動鍵交換)	. 489
	2.14.6	IPv6 over IPv6 で固定 IP アトレス での VPN(日勤鍵交換)	. 500
	2.14.7	IPv6 over IPv6 で可変 IP アトレス Cの VPN(日朝鍵交換)	. 510
	2.14.8	IPv4 over IPv4 で1つのIKE セッションに復数のIPsec トンネル構成でのVPN(自動鍵交換)	. 520
	2.14.9	IPSeC機能と他機能との併用	. 532
	2.14.10	IPv4 over IPv4 で固定 IP アトレスでハックアッフ用に使用する VPN(自動鍵父換)	. 552
	2.14.11	テンフレート看信機能(AAA 認証)を使用した固定 IP アトレスでの VPN	. 569
	2.14.12	テンフレート看信機能(AAA 認証)を使用した可変 IP アドレスでの VPN	. 578
	2.14.13	テンプレート看信機能(RADIUS 認証)を使用した固定 IP アドレスでの VPN	. 588
	2.14.14	テンフレート看信機能(RADIUS 認証)を使用した可変 IP アドレスでの VPN	. 599
	2.14.15	テンプレート看信機能(動的 VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	. 611
	2.14.16	テンプレート看信機能(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)	633
	2.14.17	テンプレート看信機能(動的 VPN)を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN	. 642
	2.14.18	NAT トラバーサルを使用した可変 IP アドレスでの VPN	. 663
	2.14.19	テンプレート着信機能(AAA 認証)およびNAT トラバーサルを使用した可変IP アドレスでの VPN	. 671
	2.14.20	接続先情報(動的 VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	. 680
2.15	システム	ムログを採取する	. 712
2.16	マルチト	NAT機能(アドレス変換機能)を使う	. 715
	2.16.1	プライベート LAN 接続でサーバを公開する	. 716
	2.16.2	PPPoE 接続でサーバを公開する	. 718
	2.16.3	ネットワーク型接続でサーバを公開する	. 721
	2.16.4	サーバ以外のアドレス変換をしないで、プライベート LAN 接続でサーバを公開する	. 724
	2.16.5	複数のNAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する	. 726
	2.16.6	NAT あて先変換で双方向のアドレスを変換する	. 728
2.17	VoIP NA	AT トラバーサル機能を使う	. 730
2.18	TOS/Tra	affic Class 値書き換え機能を使う	. 732
2.19	VLAN 7	プライオリティマッピング機能を使う....................................	. 735

2.20	シェーピング機能を使う737			
	2.20.1 特定のインタフェースでシェーピング機能を使う	737		
	2.20.2 送信先ごとにシェーピング機能を使う	738		
2.21	データ圧縮/ヘッダ圧縮機能を使う....................................	742		
2.22	帯域制御(WFQ)機能を使う	744		
2.23	DHCP機能を使う	748		
	2.23.1 DHCP サーバ機能を使う	749		
	2.23.2 DHCP スタティック機能を使う	752		
	2.23.3 DHCP クライアント機能を使う	754		
	2.23.4 DHCP リレーエージェント機能を使う	756		
	2.23.5 IPv6 DHCP クライアント機能を使う	760		
2.24	DNS サーバ機能を使う(ProxyDNS)	764		
	2.24.1 DNSサーバの自動切り替え機能(順引き)を使う	764		
	2.24.2 DNSサーバの自動切り替え機能(逆引き)を使う	766		
	2.24.3 DNS サーバアドレスの自動取得機能を使う	768		
	2.24.4 DNS サーバア ドレスを DHCP サーバから取得して使う	771		
	2.24.5 DNS問い合わせタイプフィルタ機能を使う	773		
	2.24.6 DNSサーバ機能を使う	775		
2.25	ーー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	777		
2.26	NMP エージェント機能を使う	779		
2.27		782		
2.28		817		
	2.28.1 簡易ホットスタンバイ機能を使う	818		
		822		
2.29		827		
	2.29.1 Ingress ポリシールーティング機能を使う	827		
		832		
2 30	注意に、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、、	835		
2.50	2 1 1 1 1 1 - トパワーオン信報を設定する	836		
	2.00.1 ノビードパン タン情報を使う	836		
2 31	てたジュール機能を使う	837		
2.01	ステレー 70歳前にになっていた。 2311 スケジュールを予約する	838		
	2.01.1 ステンユ ルビアボリック····································	840		
	2.01.2 电前面与交叉で July 2	841		
2 32	通信料全を筋約する(理全判測機能)	842		
2.52	過估行並で即約990(床並附卸機能)	843		
	2.32.1 訴並半位時間で設定する	94J 9//		
2 22	2.52.2 「尿亚附峰機能(元向沖止)を改定す。9 · · · · · · · · · · · · · · · · · · ·	846		
2.55	フラフラク 511 100 m 200 J	846		
	2.33.1 ノリソノと「れんとうゆいとう」「成配と使う	855		
	2.00.2 クラブフラル ビンフ機能を使う	862		
2 34	2.33.5 「「リアルビ事業が間とソリノン没続する(Luternet over II フリノノ) 海教のI AN ポートをフィッチングHUBのように使う	868		
2.34	2000 LAN ホートセストリフラフラ 100 000 Jに使う	871		
2.55	2111 禍之ぼり	971 971		
	2.55.7 事業所にこに別めいでを使用する 2.35.2 VPCとVCCの同時シェーピングを使用する	881		
2 36	2.002 ・1 0 C 100 の Party エービンフ で C の 9 つ · · · · · · · · · · · · · · · · · ·	802		
2.00	のJN Jn モデ派 こうに起信 ハノンアノン で 戻う ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	900		
2 3 2	アナログモディア通信バックアップをする	300		
2 30	、、ニュ こ、ユミニロハノン、ノンモッツ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	912		
2.00	シーン温温の「こ温温ハンシンシンション・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	910		
2.70	2 40 1 1台の装置でリモートアクヤスサーバを堪成する	910		
	2.1.2. 複数台の装置でリモートアクセスサーバを構成する	924		
	2.40.3 リモートアクセスサーバが使用する RADIUS サーバを多重化する	933		

2.41	スイッチポートを使う	. 939
	2.41.1 スイッチポートを HUB として使用する	. 940
	2.41.2 VLAN 透過モードを使用する	. 944
	2.41.3 スイッチポートを独立ポートとして使用する	. 947
	2.41.4 スイッチポートを分割して使用する	. 952
2.42	アプリケーションフィルタ機能を使う	. 957
2.43	SIP-SIP ゲートウェイ機能を使う	. 960
2.44	IEEE802.1X 認証機能を使う	. 963
	2.44.1 有線 LAN と無線 LAN で IEEE802.1X 認証機能を使う	. 963
2.45	不正端末アクセス防止機能(MACアドレス認証)を使う	. 978
2.46	ARP認証機能を使う	. 983

RIPの経路を制御する(IPv4) 2.1

適用機種 全機種

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

経路情報のフィルタリング条件

対象となる経路情報

• RIP による経路情報

指定条件

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

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

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

∛∑·ヒント =

◆ IP アドレスとアドレスマスクの決め方

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

例) 指定値 : 172.21.0.0/16の場合

> 経路情報 : 172.21.0.0/16は制御対象となる

172.21.0.0/24 は制御対象とならない

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

指定値	:172.21.0.0/16 の場合
経路情報	:172.21.0.0/24は制御対象となる
	172.21.10.0/24は制御対象となる

こんな事に気をつけて

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

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A.特定の条件の経路情報だけを透過させ、その他はすべて遮断する。
- B.特定の条件の経路情報だけを遮断し、その他はすべて透過させる。

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する
- また、設計方針 B の例として、以下の設定例について説明します。
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

こんな事に気をつけて

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

2.1.1 特定の経路情報の送信を許可する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。
 「RIP フィルタリング情報」が表示されます。

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



- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を指定します。
 - 動作 →遮断
 - 方向 →送信
 - フィルタリング条件 →すべて
 - メトリック値 →指定しない
- 8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.1.2 特定の経路情報のメトリック値を変更して送信する

適用機種 全機種

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

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。
 「LAN1 情報(物理LAN)」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、 「LAN1 情報(VLAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

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

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	⊙透過 ○遮断		
方向	○受信⊙送信		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ⑦完全に一致 マスクレた結果が一致 IPアドレス 192.168.10.0 アドレスマスク 24 (255.255.255.0) 		
メトリック値	1		

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて -

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

2.1.3 特定の経路情報の受信を許可する

適用機種 全機種

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



● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。
 「RIP フィルタリング情報」が表示されます。

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

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	⊙透過 ○遮断		
方向	⊙受信○送信		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ○完全に一致 ○マスクした結果が一致 IPアドレス アドレスマスク 0 0.0.0) 		
メトリック値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

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

8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.1.4 特定の経路情報のメトリック値を変更して受信する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP関連」をクリックします。
 IP関連の設定項目と「IPアドレス情報」が表示されます。
- **4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。** 「RIP フィルタリング情報」が表示されます。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件	→経路情報指定
	快楽余件 IP アドレス	→元全に一致 → 192,168,10,0
	アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→ 1

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	 ●透過 ○遮断 		
方向	⊙受信○送信		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ⑦完全に一致 マスクレた結果が一致 IPアドレス 192.168.10.0 アドレスマスク 24 (255.255.255.0) 		
メトリック値	1		

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

10. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

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

「RIPフィルタリング情報」が表示されます。

12. 手順5.~6.を参考に、以下の項目を指定します。

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

13. 手順5.~6.を参考に、以下の項目を指定します。

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

14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

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

2.1.5 特定の経路情報の送信を禁止する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。 「RIP フィルタリング情報」が表示されます。
| • | 動作 | →遮断 |
|---|-----------|---------------------|
| • | 方向 | →送信 |
| • | フィルタリング条件 | →経路情報指定 |
| | 検索条件 | →完全に一致 |
| | IPアドレス | → 10.20.30.0 |
| | アドレスマスク | →24 (255.255.255.0) |
| • | メトリック値 | →指定しない |

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	○透過 ⊙遮断		
方向	○受信⊙送信		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ○完全に一致 ○マスクした結果が一致 IPアドレス 10.20.30.0 アドレスマスク 24 (255.255.255.0) 		
メトリック値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

2.1.6 特定の経路情報の受信を禁止する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。 「RIP フィルタリング情報」が表示されます。

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

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	○透過 ③遮断		
方向	⊙受信○送信		
フィルタリング条件	 文信 ○ 送信 すべて デフォルトルート 経路情報指定 検索条件 ○完全に一致 ○マスクレた結果が一致 IPアドレス 10.20.30.0 アドレスマスク 24 (255.255.0) 		
メトリック値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

RIPの経路を制御する(IPv6) 2.2

適用機種 全機種

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

経路情報のフィルタリング条件

対象となる経路情報

RIPによる経路情報(IPv6)

指定条件

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

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



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

∛**:**とント=

◆ プレフィックスとプレフィックス長の決め方

経路情報

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

: 2001:db8:1111::/32は制御対象となる

2001:db8:1111::/64は制御対象とはならない

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

指定値	:2001:db8::/16 の場合
経路情報	:2001:db8::/32は制御対象となる
	2001:db8:1111::/32は制御対象となる

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A.特定の条件の経路情報だけを透過させ、その他はすべて遮断する。
- B.特定の条件の経路情報だけを遮断し、その他はすべて透過させる。

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する
- また、設計方針 Bの例として、以下の設定例について説明します。
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

こんな事に気をつけて

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

2.2.1 特定の経路情報の送信を許可する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

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

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



- 6. [追加] ボタンをクリックします。
- 7. 手順5.~6.を参考に、以下の項目を指定します。
 - 動作 →遮断
 - 方向 →送信
 - フィルタリング条件 →すべて
 - メトリック値 →指定しない
- 8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.2.2 特定の経路情報のメトリック値を変更して送信する

適用機種 全機種

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

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

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



6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

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

→1

2.2.3 特定の経路情報の受信を許可する

適用機種 全機種

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



● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **3. 「**IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

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

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

<ripフィルタリング情報入力フィールド></ripフィルタリング情報入力フィールド>			
動作	⊙透過 ○遮断		
方向	⊙受信○送信		
フィルタリング条件	 すべて デフォルトルート 経路情報指定 検索条件 ○完全に一致 ○マスクした結果が一致 IPアドレス アドレスマスク 0 (0.0.0) 		
メトリック値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

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

8. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.2.4 特定の経路情報のメトリック値を変更して受信する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- 4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

•

5. 以下の項目を指定します。

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



6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

→透過

→受信

→ 1

10. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

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

「IPv6 RIPフィルタリング情報」が表示されます。

12. 手順5.~6.を参考に、以下の項目を指定します。

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

13. 手順5.~6.を参考に、以下の項目を指定します。

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

14. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

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

2.2.5 特定の経路情報の送信を禁止する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN情報」をクリックします**。 「LAN情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- 4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

- 動作
- 方向
 フィルタリング条件 検索条件 プレフィックス/プレフィックス長
- メトリック値

→送信
 →経路情報指定
 →完全に一致
 → 2001:db8:1111::/64
 →指定しない

→遮断

<ipv6 ripフィルタリング情報入力フィールド=""></ipv6>			
動作	○透過 ⊙遮断		
方向	○受信⊙送信		
フィルタ リング条 件	 ○ すべて ○ デフォルトルート ● 経路情報指定 検索条件 ● 完全に一致 ○ マスクした結果が一致 ブレフィックス ブレフィック ス長 		
メトリック 値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

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

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.2.6 特定の経路情報の受信を禁止する

適用機種 全機種

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



● フィルタリング設計

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

上記のフィルタリング設計に従って設定する場合の例を示します。

- **1. 設定メニューのルータ設定で「LAN情報」をクリックします**。 「LAN情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4.** IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。 「IPv6 RIP フィルタリング情報」が表示されます。

- 動作
- 方向
- フィルタリング条件 検索条件 プレフィックス/プレフィックス長
- メトリック値

→受信
 →経路情報指定
 →完全に一致
 → 2001:db8:1111::/64
 →指定しない

→遮断

<ipv6 ripフィルタリング情報入力フィールド=""></ipv6>			
動作	○透過 ⊙遮断		
方向	⊙受信○送信		
フィルタ リング条 件	 すべて デフォルトルート 経路情報指定 検索条件 マスクした結果が一致 ブレフィックス ノブレフィックス ス長 2001:db8:1111: 64 		
メトリック 値			

6. [追加] ボタンをクリックします。

7. 手順5.~6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない
- 8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.3 OSPFv2を使用したネットワークを構築する (IPv4)

適用機種 全機種

ここでは、OSPFv2を使用したダイナミックルーティングのネットワークの設定方法について説明します。 OSPFを使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。 エリアには、エリアごとにエリアIDを設定します。バックボーンエリアには必ず0.0.0.0のエリアIDを設定し、 ほかのエリアには重複しないように0.0.0.0以外のエリアIDを設定します。

エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

● 参照 Si-Rシリーズ 機能説明書「2.5 OSPF機能」(P.37)

こんな事に気をつけて

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

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



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

● 前提条件

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

● 設定条件

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

[ルータ1でのルーティングプロトコル情報]

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.0
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN1 でのルータ優先度	: 0
•	エリア 0.0.0.1 への集約経路設定	: 10.20.0.0/16
[]	レータ2でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN0でのルータ優先度	: 1
•	LAN1 での passive-interface 設定	:設定する
[]	レータ3でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	LAN0 でのルータ優先度	: 255
•	LAN1でのpassive-interface 設定	:設定する

[ルータ4でのルーティングプロトコル情報]

• LAN0でのルーティングプロトコル	: OSPF		
• LAN1でのルーティングプロトコル	: OSPF		
 LAN0でのOSPFエリアID 	: 0.0.0.1		
・ LAN1でのOSPFエリアID	: 0.0.0.1		
• LAN1でのpassive-interface設定	:設定する		
• LAN0でのルータ優先度	: 1		
[ルータ5でのルーティングプロトコル情報]			
• LANOでのルーティングプロトコル	: OSPF		
 remote 定義でのルーティングプロトコル 	: OSPF		
 LAN0でのOSPFエリアID 	: 0.0.0.0		
 remote 定義でのOSPFエリアID 	: 0.0.0.2		
• エリア0.0.0.2への集約経路設定	: 10.30.0.0/16		
[ルータ6でのルーティングプロトコル情報]			
• LAN0でのルーティングプロトコル	: OSPF		
 remote 定義でのルーティングプロトコル 	: OSPF		
 LAN0でのOSPFエリアID 	: 0.0.0.2		
 remote 定義での OSPF エリア ID 	: 0.0.0.2		
• LAN0でのpassive-interface設定	:設定する		

上記の設定条件に従って設定を行う場合の設定例を示します。

ルータ1を設定する

LAN情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「OSPF 情報」をクリックします。
 「OSPF 情報」が表示されます。

- OSPF機能 →使用する
- エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ⊙使用する
エリア定義番号	0

- 6. [保存] ボタンをクリックします。
- 7. 手順2.~6.を参考に、「LAN1情報(物理LAN)」で以下の項目を指定します。

「LAN1情報(物理LAN)」-「IP関連」 「OSPF情報」

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

OSPF 関連を設定する

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

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- **10.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- **11.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアID

→0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	

- 13. 【保存】ボタンをクリックします。
- **14. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- **15.** 手順 11. ~ 13. を参考に、以下の項目を指定します。 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 - エリアID →0.0.0.1
- **16.** OSPF **エリア情報(1)の「経路集約情報」をクリックします**。 「経路集約情報」が表示されます。

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

<経路集約情報入力フィールド>		
ネットワークアドレス	10.20.0.0	
ネットマスク	16 (255.255.0.0)	

- 18. [追加] ボタンをクリックします。
- 19. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

ルータ2を設定する

「ルータ1を設定する」を参考に、ルータ2を設定します。

「LAN0 情報」-「IP 関連」 「OSPF 情報」		
• OSPF機能	→使用する	
 エリア定義番号 	→ 0	
• 指定ルータ優先度	→ 1	
「LAN1情報」-「IP 関連」		
「OSPF情報」		
• OSPF機能	→使用する	
 エリア定義番号 	→ 0	
• パケット送信	→抑止する	
「ルーティングプロトコル情報」-「OSPF 関連」 「OSPF エリア情報(0)」-「OSPF エリア基本情報」		

エリアID →0.0.0.1

ルータ3を設定する

「ルータ1を設定する」を参考に、ルータ3を設定します。

「LAN0 情報」-「IP 関連」 「OSPF 情報」

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

「LAN1情報」-「IP 関連」 「OSPF 情報」

•	OSPF機能	→使田する
•	USFF 1 成 R	マぼ用する

- エリア定義番号 →0
- パケット送信 →抑止する

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

エリアID → 0.0.0.1

ルータ4を設定する

「ルータ1を設定する」を参考に、ルータ4を設定します。

「LAN0 情報」-「IP 関連」 「OSPF 情報」		
● OSPF機能	→使用する	
 エリア定義番号 	→ 0	
• 指定ルータ優先度	→ 1	
「LAN1情報」-「IP 関連」 「OSPF情報」		
• OSPF機能	→使用する	
 エリア定義番号 	→ 0	
• パケット送信	→抑止する	
「ルーティングプロトコル情報」-「OSPF 関連」 「OSPFエリア情報(0)」-「OSPFエリア基本情報」		

エリアID →0.0.0.1

ルータ5を設定する

「ルータ1を設定する」を参考に、ルータ5を設定します。

「LAN0 情報」 - 「IP 関連」 「OSPF 情報」 OSPF 機能 →使用する エリア定義番号 →0 「ルーティングプロトコル情報」 - 「OSPF 関連」

「OSPFエリア情報(0)」-「OSPFエリア基本情報」

エリアID → 0.0.0.0

「OSPF エリア情報(1)」-「OSPF エリア基本情報」

- エリアID → 0.0.0.2
 経路集約情報
- ネットワークアドレス
 → 10.30.0.0

 ネットマスク
 → 16 (255.0.0.0)

ルータ6と接続する remote 定義に OSPF 機能を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3.** OSPF 機能を設定するネットワーク欄の [修正] ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- **「IP 関連」をクリックします**。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- 5. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

- 6. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →1

■OSPF情報	3
OSPF機能	○使用しない ⊙使用する
エリア定義番号	1

- 7. [保存] ボタンをクリックします。
- 8. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

ルータ6を設定する

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

「LAN0 情報」-「IP 関連」

「OSPF情報」

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

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

エリアID →0.0.0.2

「相手情報」-「IP 関連」

「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →0

こんな事に気をつけて

remote定義で使用する場合は、IPアドレスを必ず設定してください。

<u>∧</u>注意

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

2.3.1 バーチャルリンクを使う

適用機種 全機種

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

こんな事に気をつけて

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



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

● 前提条件

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

● 設定条件

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

[ルータ1でのルーティングプロトコル情報]

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

[ルータ2でのルーティングプロトコル情報]

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
[]	レータ3でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.0
•	LAN1 でのOSPFエリア ID	: 0.0.0.2
•	OSPF ルータ ID	: 10.30.10.1
•	バーチャルリンク接続先 OSPF ルータ ID	: 10.40.10.1
[]	レータ4でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	remote 定義でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.2
•	remote定義でのOSPFエリアID	: 0.0.0.3
•	OSPF ルータ ID	: 10.40.10.1
•	バーチャルリンク接続先 OSPF ルータ ID	: 10.30.10.1
[]	レータ5でのルーティングプロトコル情報]	
•	LAN0でのルーティングプロトコル	: OSPF
•	remote定義でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.3
•	remote 定義での OSPF エリア ID	: 0.0.0.3

上記の設定条件に従って設定を行う場合の設定例を示します。

ルータ1を設定する

LAN0情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「OSPF 情報」をクリックします。 「OSPF 情報」が表示されます。

- OSPF機能 →使用する
- エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

- 6. [保存] ボタンをクリックします。
- 7. 手順2.~6.を参考に、「LAN1情報(物理LAN)」で以下の項目を指定します。

「LAN1情報(物理LAN)」-「IP関連」 「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →1

OSPF 関連を設定する

- 8. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。 「ルーティングプロトコル情報」ページが表示されます。
- **9.** 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- **10.** OSPF **関連の設定項目の「OSPF エリア情報」をクリックします**。 「OSPF エリア情報」が表示されます。
- **11. [追加] ボタンをクリックします**。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアID

→0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	

- 13. [保存] ボタンをクリックします。
- **14. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
- 15. 手順 11. ~ 13. を参考に、以下の項目を指定します。
 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.1
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ルータ2を設定する

「ルータ1を設定する」を参考に、ルータ2を設定します。

「LAN0情報」-「IP 関連」
 「OSPF情報」
 →使用する
 エリア定義番号
 →0
 「LAN1情報」-「IP 関連」
 「OSPF情報」
 OSPF機能
 →使用する
 エリア定義番号
 →0

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

エリアID →0.0.0.1

ルータ3を設定する

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **3**. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- **4.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ⊙使用する
エリア定義番号	0

6. [保存] ボタンをクリックします。

7. 手順2.~6.を参考に、以下の項目を指定します。

「LAN1 情報」-「IP 関連」 「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →1

OSPF 関連を設定する

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

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- 10. 以下の項目を指定します。
 - ルータID → 10.30.10.1

■ルータID情報		3
ルータID	10.30.10.1	

- 11. 【保存】ボタンをクリックします。
- **12.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- 13. [追加] ボタンをクリックします。

OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。

- 14. 以下の項目を指定します。
 - エリアID

→0.0.0.0

■OSPFエリア基本	情報	3
エリアID	0.0.0.0	

- 15. [保存] ボタンをクリックします。
- **16. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
- 17. 手順 13. ~ 15. を参考に、以下の項目を指定します。
 「OSPFエリア情報 (1)」-「OSPFエリア基本情報」
 ・ エリアID → 0.0.0.2
- **18.** OSPF **エリア情報(1)の設定項目の「バーチャルリンク情報」をクリックします**。 「バーチャルリンク情報」が表示されます。
- 19. 以下の項目を指定します。
 - 接続先ルータID → 10.40.10.1

<バーチャルリンク情報入力フィールド>		/ールド>
接続先ルータID	10.40.10.1	

- 20. [追加] ボタンをクリックします。
- **21. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ルータ4を設定する

LAN0情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「OSPF 情報」をクリックします。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報		3
OSPF機能	○使用しない⊙使用する	
エリア定義番号	0	

6. [保存] ボタンをクリックします。

ルータ5と接続する remote 定義に OSPF 機能を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **9.** OSPF 機能を設定するネットワーク欄の [修正] ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- 10.
 「IP 関連」をクリックします。

 IP 関連の設定項目と「IP 基本情報」が表示されます。
- **11.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。

- OSPF機能 →使用する
- エリア定義番号 →1

■OSPF情報		3
OSPF機能	○使用しない ●使用する	
エリア定義番号	1	

13. [保存] ボタンをクリックします。

OSPF 関連を設定する

- **14. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **15.** 「OSPF 関連」をクリックします。 OSPF 関連の設定項目と「ルータID 情報」が表示されます。
- 16. 以下の項目を指定します。
 - ルータID

→ 10.40.10.1

■ルータID情報		3
ルータID	10.40.10.1	

- 17. [保存] ボタンをクリックします。
- **18.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- **19. [追加] ボタンをクリックします**。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 20. 以下の項目を指定します。
 - エリアロ

→0.0.0.2

■OSPFエリア基本情報		3
エリアID	0.0.0.2	

- 21. [保存] ボタンをクリックします。
- **22.** OSPF エリア情報(0)の「バーチャルリンク情報」をクリックします。 「バーチャルリンク情報」が表示されます。
- 23. 以下の項目を指定します。
 - 接続先ルータID → 10.30.10.1



- 24. [追加] ボタンをクリックします。
- **25. 画面上部の「ルーティングプロトコル情報」をクリックします**。 OSPF 関連の設定項目と「OSPF エリア基本情報」が表示されます。

- 26. 手順 19. ~ 21. を参考に、以下の項目を指定します。
 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
 ・ エリアID → 0.0.0.3
- **27. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ルータ5を設定する

「ルータ1を設定する」を参考に、ルータ5を設定します。

「LAN0 情報」-「IP 関連」 「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0

「相手情報」-「IP 関連」 「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0

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

エリアID → 0.0.0.3

2.3.2 スタブエリアを使う

適用機種 全機種

OSPF以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。 OSPFは、RIPまたはBGPで受信した経路情報、スタティック経路情報およびインタフェース経路情報をOSPF ネットワークに取り入れることができます。また、OSPFの経路情報をRIPおよびBGPで広報することができます。 OSPF以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPFネットワーク外の経路とし てデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアから OSPF以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア(NSSA) として運用します。

こんな事に気をつけて

OSPF以外のネットワークと接続する場合、OSPF以外のネットワークで使用するインタフェース経路情報をOSPF ネットワークに取り入れるように設定する必要があります。



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

● 前提条件

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

● 設定条件

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

[東京営業所]

【ルータ1でのルーティングプロト:	コル情報]
-------------------	-------

•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.0
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	エリア ID 0.0.0.1 のエリアタイプ	: stub
[]	レータ2でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN1でのOSPFエリアID	: 0.0.0.1
•	エリア ID 0.0.0.1 のエリアタイプ	: stub
[]	レータ3でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LAN0でのOSPFエリアID	: 0.0.0.0
•	LAN1 での OSPF エリア ID	: 0.0.0.2
•	エリア ID 0.0.0.2のエリアタイプ	: nssa
[]	レータ4でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	:RIP V2、OSPF
•	LANOでのOSPFエリアID	: 0.0.0.2
•	LAN1でのpassive-interface 設定	:設定する
•	エリア ID0.0.0.2のエリアタイプ	: nssa
•	OSPF 経路の RIP での広報	:再配布する
•	RIP 経路の OSPF での広報	:再配布する
[]	レータ5でのルーティングプロトコル情報]	
•	LAN0 でのルーティングプロトコル	: OSPF
•	remote定義でのルーティングプロトコル	: BGP
•	LANOでのOSPFエリアID	: 0.0.0.0
•	BGP経路のOSPFでの広報	:再配布する
•	BGP AS 番号	: 65000
•	BGPネットワークのIGPとの同期	:同期させる
•	BGPネットワーク	: 10.10.10.0/24
•	BGP集約経路	: 10.0.0/8
•	AS外部経路の集約	: 20.10.0.0/16
[横浜営業所]

[ルータ6でのルーティングプロトコル情報]

● BGP AS 番号

: 65001

- BGPネットワークのIGPとの同期
- : 同期させる
- BGPネットワーク

: 20.10.10.0/24、20.10.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

東京営業所を設定する

ルータ1を設定する

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3	
OSPF機能	○使用しない ●使用する	
エリア定義番号	0	

- 6. [保存] ボタンをクリックします。
- **7.** 手順2.~6.を参考に、以下の項目を指定します。

「LAN1情報」	-	「IP関連」	
「OSPF情報」			

- OSPF機能 →使用する
- エリア定義番号 →1

OSPF 関連を設定する

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

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

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

「OSPFエリア情報」が表示されます。

11. [追加]ボタンをクリックします。

OSPF エリア情報(0)の「OSPF エリア基本情報」が表示されます。

- 12. 以下の項目を指定します。
 - エリアID →0.0.0.0

OSPFエリア基本	情報	3
エリアID	0.0.0.0	

- 13. [保存] ボタンをクリックします。
- **14. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

15. 手順 11.~13.を参考に、以下の項目を指定します。

OSPFエリア情報(1)の「OSPFエリア基本情報」

- エリアID →0.0.0.1
- エリア種別 →スタブエリア
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ルータ2を設定する

「ルータ1を設定する」を参考に、ルータ2を設定します。

「LAN0 情報」-「IP 関連」 「OSPF 情報」	
● OSPF機能	→使用する
 エリア定義番号 	→ 0
「LAN1 情報」-「IP 関連」 「OSPF 情報」 • OSPF 機能	→使用する
 エリア定義番号 	→ 0
「ルーティングプロトコル情 「OSPF エリア情報(0)」- 「(青報」-「OSPF 関連」 DSPF エリア基本情報」
• エリアル	→0.0.0.1

エリア種別 →スタブエリア

ルータ3を設定する

「ルータ1を設定する」を参考に、ルータ3を設定します。

「LAN0情報」-「IP 関連」

「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →0

「LAN1情報」-「IP 関連」 「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →1

「ルーティングプロトコル情報」-「OSPF 関連」 「OSPF エリア情報(0)」-「OSPF エリア基本情報」 • エリアID → 0.0.0.0

- 「OSPF エリア情報(1)」-「OSPF エリア基本情報」
- エリアID →0.0.0.2
- エリア種別 →準スタブエリア

ルータ4を設定する

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4. IP 関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

6. [保存] ボタンをクリックします。

LAN1情報を設定する

設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。

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

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

- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 10. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

11. 以下の項目を指定します。

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

■RIP情報	
RIP送信	○送信しない ○V1で送信する ○V2で送信する ⊙V2(Multicast)で送信する
RIP受信	○受信しない ○V1で受信する ⊙V2、V2(Multicast)で受信する

- 12. [保存] ボタンをクリックします。
- **13.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。

14. 以下の項目を指定します。

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

OSPF情報		
OSPF機能	○使用しない ⊙使用する	
エリア定義番号	0	
出力コスト	10	
指定ルータ優先度	1	
Helloバケット送信間隔	10 秒 🗸	
隣接ルータ停止確認間隔	40 秒 🗸	
バケット再送間隔	5 秒 🗸	
LSUバケット送信遅延時間	1 秒 🗸	
認証方式	 ● 認証を行わない ● テキスト認証 鍵種別 ● 文字列 ● 16進数 認証鍵 ● MD5認証 MD5認証 MD5認証 	
パケット送信	⊙抑止する○抑止しない	

15. [保存] ボタンをクリックします。

OSPF 関連を設定する

- **16. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **17.** 「OSPF 関連」をクリックします。 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- **18.** OSPF **関連の設定項目の「OSPF エリア情報」をクリックします**。 「OSPF エリア情報」が表示されます。
- **19. [追加] ボタンをクリックします**。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。

20. 以下の項目を指定します。

- エリアID →0.0.0.2
- エリア種別 →準スタブエリア

■OSPFエリア基本情報	
エリアID	0.0.0.2
エリア種別	 ●通常エリア ●スタブエリア ●準スタブエリア

21. [保存] ボタンをクリックします。

ルーティングマネージャ情報を設定する

- **22. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **23.** 「ルーティングマネージャ情報」をクリックします。 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

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

■再配布情報 [2]		
	インタフェース経路情報	○再配布しない⊙再配布する
	スタティック経路情報	○再配布しない⊙再配布する
RIP	BGP経路情報	 ● 再配布しない ○ 再配布する メトリック値: ○ ▼
	OSPF経路情報	○再配布しない ⊙再配布する メトリック値: 0 ▼
	DNS経路情報	 ● 再配布しない ○ 再配布する メトリック値:
	インタフェース経路情報	⊙再配布しない○再配布する
	スタティック経路情報	⊙再配布しない○再配布する
BGP	RIP経路情報	⊙再配布しない○再配布する
	OSPF経路情報	⊙再配布しない○再配布する
	DNS経路情報	⊙再配布しない○再配布する
	インタフェース経路情報	 ● 再配布しばい ● 再配布する メトリック値 20 メトリックタイブ type2 ▼
OSPF	スタティック経路情報	 ● 再配布しばい ● 再配布する メトリック値 20 メトリックタイブ type2 ▼
	RIP経路情報	 ○ 再配布しない ● 再配布する メトリック値 20 メトリックタイプ type2 ▼

- 25. [保存] ボタンをクリックします。
- **26. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

ルータ5を設定する

LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

- 5. 以下の項目を指定します。
 - OSPF機能
 →使用する
 - エリア定義番号 →0

■OSPF情報	5	9
OSPF機能	○使用しない ●使用する	-
エリア定義番号	0	-

6. [保存] ボタンをクリックします。

ルーティングマネージャ情報を設定する

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」ページが表示されます。
- 「ルーティングマネージャ情報」をクリックします。
 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
- 9. 以下の項目を指定します。
 - OSPF

BGP経路情報

→再配布する

	 ○ 再配布しない ● 再配布する 	
OSPF BGP轻路情報	メトリック値 20 メトリックタイプ type2 👻	

10. [保存] ボタンをクリックします。

BGP関連を設定する

- **11.** ルーティングプロトコル情報の設定項目の「BGP 関連」をクリックします。 BGP 関連の設定項目と「BGP 情報」が表示されます。
- 12. 以下の項目を指定します。
 - BGP機能 →使用する
 - 自AS番号 →65000
 - BGPネットワーク →チェックしない

BGP情報	3
BGP機能	○使用しない ◎使用する
自AS番号	65000
自ID番号	0.0.0.0
BGPネットワーク	□常に広報する

- 13. [保存] ボタンをクリックします。
- **14.** BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。 「BGP ネットワーク情報」が表示されます。

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

<bgpネットワーク情報入力フィールド></bgpネットワーク情報入力フィールド>		
あて先IPアドレス	10.10.10.0	
あて先アドレスマスク	24 (255.255.255.0)	

16. [追加] ボタンをクリックします。

17. BGP 関連の設定項目の「BGP 集約経路情報」をクリックします。

「BGP集約経路情報」が表示されます。

18. 以下の項目を指定します。

- 集約IPアドレス → 10.0.0.0
- 集約アドレスマスク →8(255.0.0.0)
- 集約対象経路
 →広報しない

<bgp集約経路情報入力フィールド></bgp集約経路情報入力フィールド>		
集約IPアドレス	10.0.0.0	
集約アドレスマスク	8 (255.0.0.0)	
集約対象経路	○広報する ⊙広報しない	

- 19. [追加] ボタンをクリックします。
- **20.** BGP **関連の設定項目の「**BGP **相手情報」をクリックします**。 「BGP 相手情報」が表示されます。
- 21. [追加] ボタンをクリックします。

BGP相手情報(0)の設定項目と「BGP相手基本情報」が表示されます。

→1

- 22. 以下の項目を指定します。
 - 相手側IPアドレス →172.16.1.2
 - 相手 AS 番号

BGP相手基本情報	
相手側IPアト レス	172.16.1.2
相手AS番号	1

必要に応じて上記以外の項目を指定します。

23. [保存] ボタンをクリックします。

OSPF 関連を設定する

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

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

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

「OSPF エリア情報」が表示されます。

- **27.** [追加] ボタンをクリックします。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 28. 以下の項目を指定します。
 - エリアID →0.0.0.0
 - エリア種別 →通常エリア

■OSPFエリア基本情報	
エリアID	0.0.0.0
エリア種別	 ●通常エリア ○スタブエリア ○準スタブエリア

- 29. [保存] ボタンをクリックします。
- **30. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
- 31. 「AS外部経路集約情報」をクリックします。

「AS外部経路集約情報」が表示されます。

32. 以下の項目を指定します。

- ネットワークアドレス → 20.10.0.0
- ネットマスク → 16 (255.255.0.0)

<as外部経路集約情報入力フィールド></as外部経路集約情報入力フィールド>		
ネットワークアドレス	20.10.0.0	
ネットマスク	16 (255.255.0.0)	

- 33. [追加] ボタンをクリックします。
- **34. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

横浜営業所を設定する

ルータ6を設定する

「ルータ5を設定する」を参考に、ルータ6を設定します。

「ルーティングプロトコル情報」-「BGP 関連」 「BGP 情報」

- BGP機能 →使用する
- 自AS番号 →65001
- BGPネットワーク →チェックしない

「BGPネットワーク情報」

- あて先IPアドレス → 20.10.10.0
- あて先アドレスマスク →24 (255.255.255.0)
- あて先IPアドレス → 20.10.20.0
- あて先アドレスマスク →24 (255.255.255.0)

「BGP相手情報」-「BGP相手基本情報」

- 相手側IPアドレス →172.16.2.2
- 相手AS番号 →1

2.4 OSPFの経路を制御する(IPv4)

適用機種 全機種

本装置で、ほかのルータから受信する経路情報(LSA)に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

2.4.1 OSPF ネットワークでエリアの経路情報(LSA)を集約する

適用機種 全機種

エリア内のLSAを、本装置(エリア境界ルータ)で集約して、バックボーンエリアへ取り込む場合の設定方法を 説明します。



● 経路情報の設計

• エリア内のLSAを、本装置(エリア境界ルータ)で集約してバックボーンエリアに取り込む

● 設定条件

٠	LAN0でのルーティングプロトコル	: OSPF
•	LAN1 でのルーティングプロトコル	: OSPF
•	LANOでのエリアID	: 0.0.0.0
•	LAN1 でのエリア ID	: 0.0.0.1
•	バックボーンエリアへの集約経路設定	: 10.20.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN情報を設定する

- 1. 設定メニューのルータ設定で「LAN情報」をクリックします。

 「LAN情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。

- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「OSPF 情報」をクリックします。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ⊙使用する
エリア定義番号	0

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、「LAN1情報(物理LAN)」で以下の項目を指定します。

「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →1

OSPF 関連を設定する

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

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

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

「OSPFエリア情報」が表示されます。

- **11.** [追加] ボタンをクリックします。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 12. 以下の項目を指定します。
 - エリアID → 0.0.0.0

- 13. [保存] ボタンをクリックします。
- **14. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- **15. 手順 11.~13.を参考に、以下の項目を指定します**。 OSPFエリア情報(1)の「OSPFエリア基本情報」
 - エリアID →0.0.0.1
- **16.** OSPF **エリア情報(1)の「経路集約情報」をクリックします**。 「経路集約情報」が表示されます。

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

<経路集約情報入力フィールド>		
ネットワークアドレス	10.20.0.0	
ネットマスク	16 (255.255.0.0) 💌	

- 18. [追加] ボタンをクリックします。
- 19. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.4.2 AS 外部経路を集約して OSPF ネットワークに広報する

適用機種 全機種

AS 外部(OSPF 以外)のネットワークの経路情報を本装置(AS 境界ルータ)で集約して、バックボーンエリア に広報する場合の設定方法を説明します。



● 経路情報の設計

• AS外部経路情報を本装置(AS境界ルータ)で集約して OSPF ネットワーク(バックボーンエリア)に広報する

● 設定条件

•	LAN0 でのルーティングプロトコル	: OSPF
•	remote0 でのルーティングプロトコル	: BGP
•	LANOでのエリアID	: 0.0.0.0

• バックボーンエリアへの集約経路設定 : 20.10.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP **関連の設定項目の「**OSPF **情報」をクリックします**。 「OSPF 情報」が表示されます。

- OSPF機能 →使用する
- エリア定義番号 →0

OSPF情報	<u>[</u>	3
OSPF機能	○使用しない ⊙使用する	
エリア定義番号	0	

6. [保存] ボタンをクリックします。

OSPF 関連を設定する

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」ページが表示されます。
- **6.** 「OSPF 関連」をクリックします。
 OSPF 関連の設定項目と「ルータID 情報」が表示されます。
- OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。
 「OSPF エリア情報」が表示されます。
- **10. [追加] ボタンをクリックします**。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 11. 以下の項目を指定します。
 - エリアID →0.0.0.0

■OSPFエリア基本情報		?
エリアID	0.0.0.0	

12. [保存] ボタンをクリックします。

ルーティングマネージャ情報を設定する

- **13. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **14.** 「ルーティングマネージャ情報」をクリックします。 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
- 15. 以下の項目を指定します。
 - OSPF BGP 経路情報

→再配布する

	○ 再配布しない● 再配布する	
OSPF	BGP轻路情報	メトリック値 20 メトリックタイブ type2 💙

16. [保存] ボタンをクリックします。

OSPF 関連を設定する

- **17. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **18.** 「OSPF 関連」をクリックします。 OSPF 関連の設定項目と「ルータID 情報」が表示されます。
- 19. 「AS外部経路集約情報」をクリックします。

「AS外部経路集約情報」が表示されます。

- 20. 以下の項目を指定します。
 - ネットワークアドレス → 20.10.0.0
 - ネットマスク → 16 (255.255.0.0)

<as外部経路集約情報入力フィールド></as外部経路集約情報入力フィールド>	
ネットワークアドレス	20.10.0.0
ネットマスク	16 (255.255.0.0)

- 21. [追加] ボタンをクリックします。
- 22. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.4.3 エリア境界ルータで不要な経路情報(LSA)を遮断する

適用機種 全機種

エリア境界ルータで、通信に使用しないTYPE3 サマリLSAの経路情報を遮断する設定方法を説明します。



● 経路情報の設計

- エリア1の10.0.0/8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、10.0.0/8の経路 情報を遮断する
- その他はすべて透過させる

● 前提条件

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

本装置およびルータ1~4までのすべての装置で、使用するすべてのインタフェースにIPアドレスが設定されている

● 設定条件

- LANOでのルーティングプロトコル : OSPF
- remote0 でのルーティングプロトコル : OSPF
- LANOでのエリアID : 0.0.0.0
- remote0でのエリアID : 0.0.0.2
- 10.0.0.0/8のLSAを遮断

上記の経路情報に従って設定する場合の設定例を示します。

LAN情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。

- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「OSPF 情報」をクリックします。 「OSPF 情報」が表示されます。
- 5. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ◎使用する
エリア定義番号	0

6. [保存] ボタンをクリックします。

相手情報を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **9. 「相手情報」でネットワーク名がrmt0の【修正】ボタンをクリックします**。 「ネットワーク情報 (rmt0)」ページが表示されます。
- **10. 「IP 関連」をクリックします**。 IP 関連の設定項目と「IP 基本情報」が表示されます。
- **11.** IP 関連の設定項目の「OSPF 情報」をクリックします。 「OSPF 情報」が表示されます。
- 12. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →1

■OSPF情報	[*	3
OSPF機能	○使用しない ⊙使用する	
エリア定義番号	1	

13. [保存] ボタンをクリックします。

OSPF 関連を設定する

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

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

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

「OSPF エリア情報」が表示されます。

17. [追加] ボタンをクリックします。

OSPF エリア情報(0)の「OSPF エリア基本情報」が表示されます。

- 18. 以下の項目を指定します。
 - エリアID →0.0.0.0

OSPFエリア基本情報 エリアID 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0 0.0.0

- 19. [保存] ボタンをクリックします。
- **20. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- 21. 手順17.~19.を参考に、以下の項目を指定します。
 OSPFエリア情報(1)の「OSPFエリア基本情報」
 ・エリアID →0.0.0.2
- **22. 画面上部のルーティングプロトコル情報をクリックします**。 OSPF 関連項目と「OSPF エリア情報」が表示されます。
- **23. エリア定義番号(1)の[修正]ボタンをクリックします。** OSPFエリア情報(1)関連項目と「OSPFエリア基本情報」が表示されます。
- **24.** OSPF エリア情報(1) 関連項目の「サマリLSA入出力可否情報」をクリックします。 「サマリLSA入出力可否情報」が表示されます。

25. 以下の項目を指定します。

- 動作 →遮断
 方向 →入力
 対象経路情報 →経路情報指定
 - 検索条件 IP アドレス

→ 一 一 一 社 品 前 報 指 ん 一 致 一 致 一 致 一 3 、 一 3 、 10.0.0.0

アドレスマスク →8 (255.0.0.0)

<サマリLSA入出力可否情報入力フィールド>		
動作	○透過 ④遮断	
方向	◎入力○出力	
対象経路情報	 ○ すべて ③ 経路情報指定 検索条件 ◎ 完全に一致 ○ マスクレた結果が一致 	
	IPアドレス 10.0.0 アドレスマスク 8 055.0.0) ▼	

- 26. [追加] ボタンをクリックします。
- 27. 手順25.~26.を参考に、以下の項目を指定します。
 - 動作 →透過
 - 方向 →入力
 - 対象経路情報 →すべて

28. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.5 OSPF機能を使う(IPv6)

適用機種 Si-R180B, 220C, 240B, 570

2.5.1 OSPF ネットワークを構築する

適用機種 Si-R180B, 220C, 240B, 570

OSPF (IPv6)を使用したネットワークの構築について説明します。

▲注意

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

こんな事に気をつけて

- ・ ルータは、各エリアに 30 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合 は、2つ以上のエリアの指定ルータ(DR: Designated Router)とならないように設定してください。
- ・ LANを使用した隣接OSPFルータとMTU値が一致しない場合は、隣接関係を構築できません。
- ・ 経路情報を最大値まで保持した場合、OSPF以外の経路情報の減少によって経路情報に空きができても、OSPFの経路は、経路情報に反映されません。
- 本装置で保有できるLSA数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません(LSDBオーバフロー)。
 また、LSA生成元のルータの停止などによって、LSA数が本装置の上限値以下まで減少した場合、本装置の電源を再投入したり、[設定反映] ボタンや [再起動] ボタンをクリックしたりしても、正常に通信できるまでに最大60分かかることがあります。
- ・ OSPFで使用するインタフェースは、以下の条件で使用してください。

	本装置が DR を兼務する場合	本装置がDRを兼務しない場合
Si-R180B、220C、240B	(10000÷本装置保有LSA数)未満	(20000÷本装置保有LSA数)未満
Si-R570	(15000÷本装置保有LSA数)未満	(30000÷本装置保有LSA数)未満

また、通信速度15Kbps以上の通信帯域を確保する必要があります。

• OSPF (IPv6) 機能を Si-R570 で使用する場合は、拡張用 512M メモリモジュールが必要です。



● 前提条件

- 本装置1、2のすべてのインタフェースでIPv6機能を利用する設定がされている
- 本装置1のLAN1には、グローバルアドレスが設定されている
- 本装置1のLAN2には、OSPF外ネットワークへの経路がスタティック設定されている

● 設定条件

- 本装置1はバックボーンエリアと通常エリアのエリア境界ルータであり、かつ、OSPF外ネットワークへ到達 するためのAS境界ルータとして運用する
- 本装置2はバックボーンエリアとスタブエリアのエリア境界ルータとして運用する。また、バックボーンエリアでは指定ルータとして運用する
- 各エリアIDは、以下のとおり バックボーンエリア : 0.0.0.0 通常エリア : 0.0.0.1 スタブエリア : 0.0.0.2

[本装置1]

- LANOはバックボーンエリアに属する
- LAN1 は通常エリアに属し、ほかにルータが接続されていないため、Passive-interface として OSPF パケット を送信しないようにする
- OSPFルータIDは 100.0.0.1とする
- スタティック経路をOSPFに再配布する

[本装置2]

- LAN0はバックボーンエリアに属し、バックボーンエリアの指定ルータとするため、指定ルータ優先度に255 を設定する
- LAN1はスタブエリアとする
- OSPFルータIDは 100.0.2とする

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

LAN情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
- **4. IPv6 関連の設定項目の「IPv6 OSPF 情報」をクリックします**。 「IPv6 OSPF 情報」が表示されます。

- OSPF機能 →使用する
- エリア定義番号 →0

■IPv6 OSPF情報	3
OSPF機能	○使用しない⊙使用する
エリア定義番号	0
出力コスト	10
指定ルータ優先度	1
Helloパケット送信間隔	10 秒 🔽
隣接ルータ停止確認間隔	40 秒 🔽
バケット再送間隔	5 秒 🗸
LSUバケット送信遅延時間	1 秒 🗸
バケット送信	○抑止する ⊙抑止しない

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、「LAN1情報(物理LAN)」で以下の項目を指定します。

「LAN1 情報(物理 LAN)」-「IPv6 関連」-「IPv6 OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →1
- パケット送信 →抑止する

IPv6 OSPF 関連を設定する

- **8. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 9. 「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

- 10. 以下の項目を指定します。
 - ルータID

→100.0.0.1

■IPv6 ルータID情報		3
ルータID	100.0.0.1	

- 11. [保存] ボタンをクリックします。
- **12.** IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。 「IPv6 OSPF エリア情報」が表示されます。
- **13.** [追加] ボタンをクリックします。 IPv6 OSPF エリア情報(0)の「IPv6 OSPF エリア基本情報」が表示されます。

- エリアID
- エリア種別 →通常エリア

■IPv6 OSPFエリア基本情報	
エリアID	0.0.0.0
エリア種別	 ●通常エリア ●スタブエリア

- 15. [保存] ボタンをクリックします。
- **16. 画面上部のルーティングプロトコル情報をクリックします**。 IPv6 OSPF 関連項目と「IPv6 OSPF エリア情報」が表示されます。
- 17. 手順 13.~15.を参考に、以下の項目を指定します。
 - エリアID → 0.0.0.1
 - エリア種別 →通常エリア

ルーティングマネージャ情報を設定する

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

→0.0.0.0

19. 「IPv6 ルーティングマネージャ情報」をクリックします。

IPv6ルーティングマネージャ情報の設定項目と「IPv6再配布情報」が表示されます。

- 20. 以下の項目を指定します。
 - OSPF

```
スタティック経路情報
```

→再配布する



- 21. [保存] ボタンをクリックします。
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

→ 使用する

「LAN0情報」- 「IPv6 関連」 「IPv6 OSPF 情報」 • OSPF機能

- エリア定義番号 →0
- 指定ルータ優先度 → 255

「LAN1情報」- 「IPv6 関連」 「IPv6 OSPF 情報」

- OSPF機能 → 使用する
- エリア定義番号 →1

「ルーティングプロトコル情報」 - 「IPv6 OSPF 関連」 「IPv6 ルータID情報」 • ルータID → 100.0.0.2

- 「IPv6 OSPF エリア情報(0)」- 「IPv6 OSPF 基本情報」
- エリアID → 0.0.0.0
- エリア種別 →通常エリア
- 「IPv6 OSPF エリア情報(1)」- 「IPv6 OSPF 基本情報」
- エリアID →0.0.0.2
- エリア種別 →スタブエリア

2.5.2 エリア境界ルータでエリア内部経路を集約する

<u>適用機種</u> Si-R180B,220C,240B,570

エリア境界ルータで、エリア内経路を集約してほかのエリアに広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを 使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり バックボーンエリア : 0.0.0.0 (エリア定義番号0)
 エリア1 : 0.0.0.1 (エリア定義番号1)
- 各インタフェースのIPアドレスは、以下のとおり LAN1 : 2001:db8:10::1/64 LAN2 : 2001:db8:20::1/64

● 設定条件

 エリア1のエリア内部経路(2001:db8:10::/64、2001:db8:20::/64)は、集約経路(2001:db8::/32、コスト 100)としてバックボーンエリアに広報する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

IPv6 OSPF 関連を設定する

- **1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **「IPv6 OSPF 関連」をクリックします。** IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。
- **3.** IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。 「IPv6 OSPF エリア情報」が表示されます。

4. エリア定義番号1の [修正] ボタンをクリックします。

IPv6 OSPF エリア情報(1)の「IPv6 OSPF エリア基本情報」が表示されます。

5. 「IPv6 経路集約情報」をクリックします。

「IPv6経路集約情報」が表示されます。

- 6. 以下の項目を指定します。
 - • プレフィックス/プレフィックス長
 →2001:db8::/32



- 7. [追加] ボタンをクリックします。
- 8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.5.3 エリア境界ルータで不要な経路情報を遮断する

<u>適用機種</u> Si-R180B,220C,240B,570

エリア境界ルータで、ほかのエリアに対し特定のエリア内経路(エリア間プレフィックスLSA)を遮断して広報 する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを 使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり バックボーンエリア : 0.0.0.0 (エリア定義番号0) エリア1 : 0.0.0.1 (エリア定義番号1)
- 各インタフェースのIPアドレスは、以下のとおり LAN1 : 2001:db8:10::1/64 LAN2 : 2001:db8:20::1/64

● 設定条件

• エリア1からバックボーンエリアへの広報で、2001:db8:20::/64は破棄し、その他のエリア内部経路は透過させる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」ページが表示されます。
- [IPv6 OSPF 関連]をクリックします。
 IPv6 OSPF 関連の設定項目と「IPv6ルータID 情報」が表示されます。
- **3.** IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。 「IPv6 OSPF エリア情報」が表示されます。
- **4. エリア定義番号1の[修正]ボタンをクリックします。** IPv6 OSPF エリア情報(1)の「IPv6 OSPF エリア基本情報」が表示されます。

5. 「IPv6エリア間プレフィックスLSA入出力可否情報」をクリックします。

「IPv6エリア間プレフィックスLSA入出力可否情報」が表示されます。

- 6. 以下の項目を指定します。
 - 動作 →遮断
 方向 →出力
 対象経路情報 →程路情報指定 検索条件 →完全に一致
 プレフィックス/プレフィックス長 →2001:db8:20::/64

<ipv6 エリア間ブレフィックスlsa入出力可否情報入力フィールド=""></ipv6>			
動作	○透過 ③遮断		
方向	○入力 ⊙出力		
	 ○ すべて ● 経路情報指定 		
対象経 路情報	検索条件 ◎ 完全に一致 ○ マスクした結果が一致		
	ブレフィックス/ ブレフィックス長 2001:db8:20:: 64		

- 7. [追加] ボタンをクリックします。
- 8. 手順6.~7.を参考に、以下の項目を指定します。
 - 動作 →透過
 - 方向 →出力
 - 対象経路情報 →すべて
- 9. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.6 BGPの経路を制御する(IPv4)

適用機種 全機種

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

● 参照 Si-Rシリーズ 機能説明書「2.4 BGP4機能」(P.33)

2.6.1 特定の経路情報の受信を透過させる

適用機種 全機種

通信が必要なネットワークに限定して経路を透過させる場合の設定方法を説明します。



● 経路情報の設計

- 10.0.0.0/8のネットワークの経路情報を透過
- 11.0.0.0/8のネットワークの経路情報を透過
- その他はすべてを遮断

上記の経路情報に従って設定する場合の設定例を示します。

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」のページが表示されます。
- **FBGP 関連」をクリックします。** BGP 関連の設定項目と「BGP 情報」が表示されます。
- **3.** BGP **関連の設定項目の「BGP 相手情報」をクリックします**。 「BGP 相手情報」が表示されます。
- **4.** フィルタリング設定を行うBGP相手情報の【修正】ボタンまたは【追加】ボタンをクリックします。 BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。
- **5.** BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。 「BGP フィルタリング情報」が表示されます。

•	動作	→透過
•	方向	→受信
•	フィルタリング条件	→経路情報指定
	検索条件	→完全に一致
	IPアドレス	→10.0.0.0
	アドレスマスク	→8 (255.0.0.0)

<bgpフィルタリング情報入力フィールド></bgpフィルタリング情報入力フィールド>		
動作	⊙透過 ○遮断	
方向	⊙受信○送信	
	 AS番号指定 AS番号 すべて すべて 	
フィルタリング条件	 ● 経路情報指定 	
	検索条件 ◎ 完全に一致 ○ マスクした結果が一致	
	IPアドレス 10.0.0	
	アドレスマスク 8 (255.0.0.0)	

7. [追加] ボタンをクリックします。

優先順位1の定義が追加されます。

- 8. 手順6.~7.を参考に、以下の項目を優先順位2の定義として指定します。
 - 動作 →透過
 - 方向 →受信
 - フィルタリング条件 →経路情報指定 検索条件 →完全に一致
 IPアドレス → 11.0.0.0
 アドレスマスク → 8 (255.0.0.0)

9. 手順6.~7.を参考に、以下の項目を優先順位3の定義として指定します。

- 動作 →遮断
- 方向 →受信
- フィルタリング条件 →すべて
- 10. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.6.2 特定のASからの経路情報の受信を遮断する

適用機種 全機種

フルルートを受信するネットワーク(トランジット)に接続されている場合、特定の経路情報を遮断する場合の設定方法を説明します。



● 経路情報の設計

- AS4からの経路情報を遮断
- その他はすべて透過

上記の経路情報に従って設定する場合の設定例を示します。

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」のページが表示されます。
- [BGP 関連]をクリックします。
 BGP 関連の設定項目と「BGP 情報」が表示されます。
- **3.** BGP 関連の設定項目の「BGP 相手情報」をクリックします。 「BGP 相手情報」が表示されます。
- **4.** フィルタリング設定を行うBGP相手情報の[修正]ボタンまたは[追加]ボタンをクリックします。 BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。
- **5.** BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。 「BGP フィルタリング情報」が表示されます。

- 動作 →遮断
- 方向 →受信
- フィルタリング条件 → AS 番号指定
 AS 番号 → 4

<bgpフィルタリング情報入力フィールド></bgpフィルタリング情報入力フィールド>		
動作	○透過 ◉遮断	
方向	⊙受信○送信	
 AS番 AS番 すべ デフ: デフ: 経路 IPア アド 	 AS番号指定 AS番号 4 すべて デフォルトルート 経路情報指定 	
	検索条件 ● 完全に一致 ● マスクした結果が一致 IPアドレス アドレスマスク 0 00.0.0)	

- 「追加」ボタンをクリックします。
 優先順位1の定義が追加されます。
- 8. 手順6.~7.を参考に、以下の項目を優先順位2の定義として指定します。
 - 動作 →透過
 - 方向 →受信
 - フィルタリング条件 →すべて
- 9. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.6.3 IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する

適用機種 全機種

異なる IP-VPN 網を使用し、冗長化ネットワークを構成する場合、IP-VPN 網1から受信した経路情報の IP-VPN 網2への送信を遮断、および IP-VPN 網2から受信した経路情報の IP-VPN 網1への送信を遮断する場合の設定方法を 説明します。



● 経路情報の設計

- AS2からAS3への経路情報を遮断
- AS3からAS2への経路情報を遮断

上記の経路情報に従って設定する場合の設定例を示します。

AS2への広報時のBGPフィルタリングを設定する

- **1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」のページが表示されます。
- **7** [BGP 関連]をクリックします。
 BGP 関連の設定項目と「BGP 情報」が表示されます。
- **3.** BGP 関連の設定項目の「BGP 相手情報」をクリックします。 「BGP 相手情報」が表示されます。
- **4.** フィルタリング設定を行うBGP相手情報の【修正】ボタンまたは【追加】ボタンをクリックします。 BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。
- **5.** BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。 「BGP フィルタリング情報」が表示されます。

- 動作 →遮断
- 方向 →送信
- フィルタリング条件 → AS 番号指定
 AS 番号 → 3

<bgpフィルタリング情報入力フィールド></bgpフィルタリング情報入力フィールド>	
動作	○透過 ⊙遮断
方向	○受信⊙送信
フィルタリング条件	 AS番号指定 AS番号 3 すべて デフォルトルート 経路情報指定 検索条件 完全に一致
	 ○ マスクした結果が一致 IPアドレス

「追加」ボタンをクリックします。
 優先順位1の定義が追加されます。

8. 手順6.~7.を参考に、以下の項目を指定します。

BGP相手情報(0)の優先順位2の定義

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて

AS3への広報時のBGPフィルタリングを設定する

9. 「AS2への広報時のBGPフィルタリングを設定する」を参考に、以下の項目を指定します。

BGP相手情報(1)の優先順位1の定義

- 動作 →遮断
- 方向 →送信
- フィルタリング条件 → AS 番号指定
 AS 番号 → 2

BGP相手情報(1)の優先順位2の定義

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて

10. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.6.4 冗長構成の通信経路を使用する

適用機種 全機種

IP-VPN網に接続する経路を2つ使用した冗長構成で、通信の負荷分散および通信網異常による経路切り替えを行う場合の設定方法を説明します。



● 経路情報の設計

- OSPFネットワークである AS1 で IP-VPN 網を経由した AS2 への通信経路を冗長化する
- 10/8 への通信は経路1を優先経路とし、11/8 への通信経路は経路2を優先経路とする。それぞれの経路で異常が発生した場合、異常が発生していない経路に切り替わる。優先順位を設定するときは MED メトリック値を使用する
- AS1内のOSPFネットワークでの経路変更はBGPでAS2に広報する

上記の経路情報に従って設定する場合の設定例を示します。

本装置1を設定する

ルーティングプロトコル情報を設定する

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。
 「ルーティングプロトコル情報」のページが表示されます。
- [BGP 関連]をクリックします。
 BGP 関連の設定項目と「BGP 情報」が表示されます。
- **3.** BGP **関連の設定項目の「**BGP **相手情報」をクリックします**。 「BGP 相手情報」が表示されます。
- **4.** フィルタリング設定を行うBGP相手情報の【修正】ボタンまたは【追加】ボタンをクリックします。 BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。
- **5.** BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。 「BGP フィルタリング情報」が表示されます。
| • | 動作 | →透過 |
|---|-------------------|------------------------------------|
| • | 方向 | →送信 |
| • | フィルタリング条件
検索条件 | →経路情報指定
→ == 仝 に ー み |
| | 快来来け
IPアドレス | → <u>元主に一</u> <u></u>
→10.0.0.0 |
| | アドレスマスク | →8 (255.0.0.0) |
| • | MED メトリック値 | → 0 |

<bgpフィルタリング情報入力フィールド></bgpフィルタリング情報入力フィールド>		
動作	 ●透過 ○遮断 	
方向	○受信⊙送信	
	○ AS番号指定	
フィルタリング条件	AS番号 ○ すべて ○ デフォルトルート ③ 経路情報指定	
	 検索条件 ◎ 完全に一致 ○ マスクした結果が一致 	
	IPアドレス 10.0.0	
	アドレスマスク 8 (255.0.0.0)	
MEDメトリック値	0	

7. [追加] ボタンをクリックします。

優先順位1の定義が追加されます。

8. 手順6.~7.を参考に、以下の項目を優先順位2の定義として指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →経路情報指定 検索条件 →完全に一致
 IPアドレス → 11.0.0.0
 アドレスマスク → 8 (255.0.0.0)
- MEDメトリック値 →10

9. 手順6.~7.を参考に、以下の項目を優先順位3の定義として指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて

10. 画面上部の「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

11. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

• BGP OSPF 経路情報

→再配布する

	インタフェース経路情報	⊙再配布しない○再配布する
	スタティック経路情報	●再配布しない●再配布する
BGP	RIP経路情報	⊙再配布しない○再配布する
	OSPF経路情報	○再配布しない⊙再配布する
	DNS経路情報	⊙再配布しない○再配布する

- 13. [保存] ボタンをクリックします。
- **14. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ルーティングプロトコル情報」-「BGP 関連」 「BGP フィルタリング情報」 BGP 相手情報(0)の優先順位1の定義 ・動作 →透過 ・方向 →送信

- フィルタリング条件
 →経路情報指定
 検索条件
 →完全に一致
 IPアドレス
 アドレスマスク
 →8 (255.0.0.0)
- MEDメトリック値 →10

BGP相手情報(0)の優先順位2の定義

- 動作 →透過
 方向 →送信
 フィルタリング条件 →経路情報指定 検索条件 →完全に一致
 IPアドレス →11.0.00
 アドレスマスク →8 (255.0.00)
- MEDメトリック値 →0

BGP相手情報(0)の優先順位3の定義

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」 「再配布情報」

BGP
 OSPF 経路情報
 →再配布する

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- BGP/MPLS VPN 機能では、BGP フィルタリング情報は無効となります。
- 送信時のフィルタを設定した場合、相手装置に広報する MED メトリック値、AS パスプリペンドはフィルタの設定値 が使用されます。
- MEDメトリック値の設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- ASパスプリペンドの設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- BGP使用中に[設定反映]をクリックした場合、接続中のセッションが一度切断されることがあります。

2.7 事業所間を MPLS 接続サービスを利用して接続する

適用機種 全機種

本装置ではMPLSのLSP(label Switching Path:トンネルラベルスイッチングパス)をトンネルとしてインタフェースに対応させるため、シェーピングや帯域制御などの機能をLSPごとに使用することができます(MPLS LSPトンネル)。

ここでは、MPLS 接続サービス(キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送 サービスを想定しています)と本装置の MPLS LSP トンネルを使用して、事業所の間を接続する場合の設定方法 を説明します。

こんな事に気をつけて

- ・ 隣接 LSR は、ダイナミックルーティングを用いて最適経路から決定することはできません。MPLS LSP の送出先の 設定と MPLS LSP での次ホップのラベルスイッチルータの設定で静的に指定する必要があります。
- MPLS LSP トンネルでは、IPv4、IPv6のプロトコルだけをサポートしています。ブリッジは使用できません。MPLS LSP トンネル上にさらにラベルをスタックできるのは、BGP/MPLS VPN 機能だけです。LDP over LDPの形態はサ ポートしていません。MPLS LSP トンネルを使用するインタフェースでは、MPLSを利用しないように設定してくだ さい。
- MPLS LSP トンネルで IPv6 通信を行う場合は、2 層目のラベルスタックに IPv6 Explicit NULL ラベルを用いた多重ス タックとなります。また、MPLS TTL 伝達の設定で指定した値に関係なく、TTL の継承は行われません。
- ・ 複数の MPLS LSP トンネルを使用する場合は、それぞれ別の自側トンネルエンドポイントアドレスと相手側トンネル エンドポイントアドレスを設定してください。同じ自側トンネルエンドポイントアドレスが複数設定されている場合 は、それぞれのLSP で受信したパケットが期待したLSP のインタフェースとは別のインタフェースで受信されてし まうため、受信インタフェースに依存して動作する IP フィルタリング機能、TOS 値書き換え機能、NAT 機能、マル チキャスト機能、ダイナミックルーティング(RIP、OSPF)機能などは正しく動作しません。
- 複数の MPLS LSP トンネルで相手側トンネルエンドポイントアドレスの設定が同じアドレスであった場合は、MPLS LSP の送出先の設定と MPLS LSP での次ホップのラベルスイッチルータは同じ値を設定してください。違う値を設定 した場合、どれかの値だけが使用されます。
- MPLS 通信で、優先制御機能、EXP 値書き換え機能、およびシェーピング機能を利用する場合は、MPLS LSP トンネルを使用してください。

2.7.1 トンネルエンドポイントをインタフェースアドレスにして MPLS LSP を使用する

適用機種 全機種



● 前提条件

[本装置1]

- LAN0がMPLS網、LAN1が事業所内LANとする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS網とのラベル交換はインタフェースアドレスに対して行う
- 本装置1と本装置2の間は、EBGPでループバックインタフェースどうしで経路情報を交換する

[本装置2]

- LAN0が MPLS 網、LAN1 が事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS網とのラベル交換は、インタフェースアドレスに対して行う
- 本装置2と本装置1の間は、EBGPでループバックインタフェースどうしで経路情報を交換する

● 設定条件

[本装置1]

• LAN0 (MPLS 網側) の IP アドレス	: 10.1.101.2
 接続する MPLS 網の次ホップ LSR の)IPアドレス :10.1.101.1
 LAN1(事業所内側)のIPアドレス 	: 192.168.101.1
• ループバックインタフェースのIPア	'ドレス :10.0.0.101
 本装置1の属するAS番号 	: 101
 本装置2の属するAS番号 	: 201
[本装置2]	
[本装置 2] • LANO(MPLS網側)のIPアドレス	: 10.1.201.2
 【本装置 2】 LAN0 (MPLS 網側)のIPアドレス 接続する MPLS 網の次ホップLSR の 	:10.1.201.2 NPアドレス :10.1.201.1
 【本装置 2】 LAN0(MPLS 網側)のIPアドレス 接続する MPLS 網の次ホップLSRの LAN1(事業所内側)のIPアドレス 	:10.1.201.2 NPアドレス :10.1.201.1 :192.168.201.1
 【本装置 2】 LAN0(MPLS 網側)のIPアドレス 接続する MPLS 網の次ホップLSRの LAN1(事業所内側)のIPアドレス ループバックインタフェースのIPア 	:10.1.201.2 DIPアドレス :10.1.201.1 :192.168.201.1 ごドレス :10.0.0.201

本装置1の属するAS番号 : 101

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

MPLS網との接続情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 10.1.101.2
 ネットマスク → 24 (255.255.255.0)

ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報 []			
IPv4	●使用する●使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 10.1.101.2 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 		

5. [保存] ボタンをクリックします。

6. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

- 7. 以下の項目を指定します。
 - MPLS機能 →使用する
 - ラベル配布プロトコル → LDP

■MPLS基本情報	3
MPLS機能	○使用しない ●使用する
ラベル配布ブロトコル	LDP 🗸

- 8. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「MPLS 情報」をクリックします。
 「MPLS 情報」ページが表示されます。
- **10. 「基本情報」をクリックします。** 「基本情報」が表示されます。

•	MPLS TTL 伝達	→しない
•	LDP	
	router ID	→ 10.1.101.2
	制御方式	→ independent
	IPv4 Transportアドレス	→ 10.1.101.2

■基本情報 (1)		3	
MPLS TTL伝達		⊙しない ○する	
	router ID	10.1.101.2	
LDP	制御方式	⊙independent ○ordered	
	IPv4 Transport アドレス	10.1.101.2	

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 14. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

- 15. 以下の項目を指定します。
 - LDP

インタフェース経路情報	→再配布しない
RIP経路情報	→再配布しない
OSPF 経路情報	→再配布しない

	インタフェース経路情報	⊙再配布しない○再配布する
	スタティック経路情報	⊙再配布しない○再配布する
LDP	RIP経路情報	● 再配布しない ● 再配布する
	BGP経路情報	⊙再配布しない○再配布する
	OSPF経路情報	●再配布しない ○再配布する

16. [保存] ボタンをクリックします。

MPLS トンネルを設定する

- **17. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **18. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- 19. 以下の項目を指定します。
 - ネットワーク名 → tokyo

<ネットワーク情報追加フィールド>	
ネットワーク名	tokyo

20. [追加] ボタンをクリックします。

「ネットワーク情報(tokyo)」ページが表示されます。

21. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

22. 以下の項目を指定します。

- 接続先名
- →lsp1
- 接続先種別 → MPLS トンネル接続



機種により、接続先種別の表示が上記の画面とは異なります。

23. [追加] ボタンをクリックします。

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

24. 以下の項目を指定します。

- 送出先インタフェース → LANO
- IPv4 転送先ルータ → 10.1.101.1
- 自側エンドポイント → 10.1.101.2
- 相手側エンドポイント → 10.1.201.2

送出先インタフェース	LANO
IPv4転送先ルータ	10.1.101.1
自側エントポイント	10.1.101.2
相手側エントボイント	10.1.201.2

- 25. [保存] ボタンをクリックします。
- ループバックインタフェースを設定する
- **26. 設定メニューの基本設定で「装置情報」をクリックします**。 「装置情報」ページが表示されます。
- **27. 「ループバック情報」をクリックします**。 「ループバック情報」が表示されます。
- 28. 以下の項目を指定します。
 - IPアドレス → 10.0.0.101

■ループバック情	報	3
IPアドレス	10.0.0.101	

29. [保存] ボタンをクリックします。

LAN1情報を設定する

- **30. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 31. 以下の項目を指定します。
 - インタフェース →物理LAN

<lan情報追加フィールド></lan情報追加フィールド>		
インタフェース	物理	ELAN 🔽

32. [追加] ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

33. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

34. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 192.168.101.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス → ネットワークアドレス+オール1

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
IP アド レス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス I92.168.101.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ 		
	ス ネットワークアドレス+オール1 ▼		

35. [保存] ボタンをクリックします。

本装置1との間で経路交換を設定する

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

37. 「BGP 関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

38. 以下の項目を指定します。

- BGP機能 →使用する
- 自AS番号 → 101
- BGPネットワーク →チェックしない

■BGP情報	
BGP機能	○使用しない ⊙使用する
自AS番号	101
自ID番号	0.0.0.0
BGPネットワーク	□常に広報する

- 39. [保存] ボタンをクリックします。
- **40.** BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP相手情報」が表示されます。

41. [追加] ボタンをクリックします。

BGP相手情報(0)の設定項目と「BGP相手基本情報」が表示されます。

42. 以下の項目を指定します。

- 相手側IPアドレス → 10.0.0.201
- 相手AS番号 →201
- 自側IPアドレス → 10.0.0.101

こんな事に気をつけて

- ルートリフレクタのIPアドレスを相手側IPアドレスに設定してください。
- ・ 自側 IP アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

BGP相手表	基本情報 []
相手側IPアト レス	10.0.201
相手AS番号	201
自側IPアドレ ス	10.0.0.101

- 43. [保存] ボタンをクリックします。
- **44.** BGP 関連の設定項目の「BGP ネットワーク情報」をクリックします。 「BGPネットワーク情報」が表示されます。

- あて先IPアドレス → 192.168.101.0
- あて先アドレスマスク →24 (255.255.255.0)

<bgpネットワーク情報入力フィールド></bgpネットワーク情報入力フィールド>		
あて先IPアドレス	192.168.101.0	
あて先アドレスマスク	24 (255.255.255.0) 💌	

- 46. [追加] ボタンをクリックします。
- **47.** BGP 相手情報(0)の設定項目の「BGP 拡張機能情報」をクリックします。 「BGP 拡張機能情報」が表示されます。
- 48. 以下の項目を指定します。
 - エンフォースマルチホップ →使用する
 エンフォースマルチホップ ○使用しない ○使用する
- 49. [保存] ボタンをクリックします。
- **50. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **51.** 「ネットワーク情報」で相手定義番号が0の [修正] ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- **52.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP 基本情報」が表示されます。
- 53. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 54. 以下の項目を指定します。
 - ネットワーク あて先IPアドレス あて先アドレスマスク

→ネットワーク指定
 → 10.0.0.201
 → 32 (255.255.255.255)



- 55. [追加] ボタンをクリックします。
- **56. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する | を参考に、本装置2を設定します。

MPLS網との接続情報を設定する

「LAN0情報(物理LAN)」-「IP 関連」 「IPアドレス情報」

• IPv4 →使用する →指定する • IPアドレス IPアドレス → 10.1.201.2 ネットマスク →24 (255.255.255.0) →ネットワークアドレス+オール1 ブロードキャストアドレス

「LAN0情報(物理LAN)」-「MPLS 関連」 「MPLS基本情報」

•	MPLS 機能	→使用する
	ラベル配布プロトコル	→LDP

「MPLS情報」

•	MPLS TTL 伝達	→しない
	router ID	→ 10.1.201.2
	制御方式	→ independent
	IPv4 Transportアドレス	→ 10.1.201.2

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」 「再配布情報」

•	LDP	
	インタフェース経路情報	→再配布しない
	RIP経路情報	→再配布しない
	OSPF 経路情報	→再配布しない

MPLS トンネルを設定する

「相手情報」-「ネットワーク情報」			
 ネットワーク名 	→kawasaki		
「ネットワーク情報」-「接続先	情報」		
● 接続先名	→lsp1		
● 接続先種別	→ MPLS トンネル接続		
「接続先情報」-「MPLS トンネル接続」			
「基本情報」			
• 送出先インタフェース	→ LAN0		
 IPv4 転送先ルータ 	→ 10.1.201.1		
• 自側エンドポイント	→ 10.1.201.2		
• 相手側エンドポイント	→ 10.1.101.2		

ループバックインタフェースを設定する

「装置情報」-「ループバック情報」

IPアドレス → 10.0.0.201

LAN1情報を設定する

「LAN1 情報(物理 LAN)」-「IP 関連」 「IP アドレス情報」

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →192.168.201.1
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

「LAN1情報(物理LAN)」-「MPLS関連」

「MPLS基本情報」

•	MPLS 機能	→使用する
	ラベル配布プロトコル	→LDP

本装置1との間で経路交換を設定する

「ルーティングプロトコル情報」 「BGP情報」	- 「BGP関連」
● BGP機能	→使用する
● 自AS番号	→ 201
「BGP相手情報」	
「BGP相手基本情報」	
• 相手側 IP アドレス	→ 10.0.0.101
● 相手AS番号	→ 101
• 自側IPアドレス	→ 10.0.0.201
「BGP 拡張機能情報」	
 エンフォースマルチホップ 	→使用する
「ルーティングプロトコル情報」 「再配布情報」 • BGP インタフェース経路情報	- 「ルーティングマネージャ情報」 →再配布する
「相手情報」-「ネットワーク情報」-「IP 関連」 「ネットワーク情報」-「IP 関連」 「スタティック経路情報」	程」

 ネットワーク指定 あて先IPアドレス → 10.0.0.101
 あて先アドレスマスク → 32 (255.255.255)

2.7.2 トンネルエンドポイントをインタフェースアドレスとは 別のアドレスにして MPLS LSP を使用する





● 前提条件

[本装置1]

- LAN0が MPLS 網、LAN1 が事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置1と本装置2の間は、LSP上でOSPFを用いて経路情報を交換する
- MPLS 網を使用した LSP 上の通信は 5 Mbps に帯域を制限する
- LSPでセッション監視を行い、セッションの切断を検知する

[本装置2]

- LAN0が MPLS 網、LAN1 が事業所内 LAN とする
- 接続する MPLS 網の次ホップ LSR とは、インタフェースアドレスでコネクションを確立する
- MPLS網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置1と本装置2の間は、LSP上でOSPFを用いて経路情報を交換する
- MPLS 網を使用した LSP 上の通信は 5 Mbps に帯域を制限する
- LSPでセッション監視を行い、セッションの切断を検知する

● 設定条件

[本装置1]

•	LANO(MPLS網側)のIPアドレス	: 10.1.101.2
•	接続する MPLS 網の次ホップ LSRの IP アドレス	: 10.1.101.1
•	LAN1(事業所内側)の IP アドレス	: 192.168.101.1
•	MPLS トンネルの自側 IP アドレス	: 10.0.0.101
•	MPLS トンネルの相手側 IP アドレス	: 10.0.0.201
[才	装置2]	
•	LANO(MPLS網側)のIPアドレス	: 10.1.201.2
•	接続する MPLS 網の次ホップ LSR の IP アドレス	: 10.1.201.1

• LAN1(事業所内側)のIPアドレス : 192.168.201.1

MPLSトンネルの自側IPアドレス : 10.0.0.101
 MPLSトンネルの相手側IPアドレス : 10.0.0.201

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

MPLS網との接続情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 10.1.101.2
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		9
IPv4	●使用する●使用しない	
IPアトレス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 10.1.101.2 ネットマフク 24 (255 255 0) 	
	ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼	

5. [保存] ボタンをクリックします。

6. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

7. 以下の項目を指定します。

- MPLS機能 →使用する
- ラベル配布プロトコル →LDP

MPLS基本情報	3
MPLS機能	○使用しない ⊙使用する
ラベル配布ブロトコル	LDP 💌

8. [保存] ボタンをクリックします。

9. 設定メニューのルータ設定で「MPLS情報」をクリックします。

「MPLS情報」ページが表示されます。

10. 「基本情報」をクリックします。

「基本情報」が表示されます。

11. 以下の項目を指定します。

 MPLS TTL 伝達 →しない
 LDP router ID → 10.1.101.2
 制御方式 → independent IPv4 Transport アドレス → 10.1.101.2

■基	本情報	3
MPL	.S TTL伝達	⊙しない ○する
	router ID	10.1.101.2
LDP	制御方式	⊙independent ⊙ordered
	IPv4 Transport アドレス	10.1.101.2

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- 14. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

- 15. 以下の項目を指定します。
 - LDP

インタフェース経路情報	→再配布しない
RIP経路情報	→再配布しない
OSPF 経路情報	→再配布しない

	インタフェース経路情報	⊙再配布しない○再配布する
	スタティック経路情報	● 再配布しない ● 再配布する
LDP	RIP経路情報	● 再配布しない ● 再配布する
	BGP経路情報	● 再配布しない ● 再配布する
	OSPF経路情報	● 再配布しない ● 再配布する

16. 【保存】ボタンをクリックします。

MPLS トンネルを設定する

- **17. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **18. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。

ネットワーク名

→tokyo

<ネットワーク情報追加フィールド>	
ネットワーク名	tokyo

20. [追加] ボタンをクリックします。

「ネットワーク情報(tokyo)」ページが表示されます。

21. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

22. 以下の項目を指定します。

• 接続先名

→lsp1

• 接続先種別

→ MPLS トンネル接続

機種により、接続先種別の表示が上記の画面とは異なります。

23. [追加] ボタンをクリックします。

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

- 送出先インタフェース → LANO
- IPv4 転送先ルータ → 10.1.101.1
- 自側エンドポイント → 10.0.0.101
- 相手側エンドポイント → 10.0.0.201

送出先インタフェース	
IPv4転送先ルータ	10.1.101.1
自側エンドボイント	10.0.0.101
相手側エントポイント	10.0.201

- 25. [保存] ボタンをクリックします。
- **26. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **27.** 「ネットワーク情報」で相手定義番号が0の【修正】ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- 28. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

29. 以下の項目を指定します。

•	IPアドレス	→設定する
	相手側IPアドレス	→ 10.0.0.201
	自側 IP アドレス	→ 10.0.0.101

■IP基本情報		?
IP アド レス	 ○ 設定しない ● 設定する 	
	相手側IPアドレス 10.0.0.201	
	自側IPアドレス 10.0.0.101	

30. [保存] ボタンをクリックします。

MPLS トンネルでシェーピングを設定する

31. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

32. 以下の項目を指定します。

•	シェーピング	→使用する
	最大送信レート	→5Mbps

シェービング	 ○ 使用しない ③ 使用する 	
	最大送信レート 5 Mbps 🗸	

33. [保存] ボタンをクリックします。

MPLS トンネルでセッション監視を設定する

- **34. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **35. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- **36.** 「ネットワーク情報」で相手定義番号が0の [修正] ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- **37. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 38. 「接続先情報」で接続先定義番号が0の[修正]ボタンをクリックします。 MPLSトンネル接続の設定項目と「基本情報」が表示されます。
- **39.** MPLS トンネル接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。

40. 以下の項目を指定します。

時接続機能	→使用する
続先監視	→使用する
信元 IP アドレス	→ 10.0.0.101
て先IPアドレス	→ 10.0.0.201
常時送信間隔	→10秒
送間隔	→1秒
イムアウト時間	→5秒
常時送信間隔	→1分
信TTL/HopLimit	→ 1
	時接続機能 続先監視 信元 IP アドレス て先 IP アドレス 常時送信間隔 送間隔 イムアウト時間 常時送信間隔 信 TTL/HopLimit

■接続	御情報
	○使用しない ●使用する
	送信元IPアトレス 10.0.0101
	あて先IPアドレス 10.0.201
	正常時送信間隔 10 秒 🖌
接続	再送間隔 1 秒 🗸
元監 視	タイムアウト時間 5 秒 🗸
	異常時送信間隔 1 分 ▼
	送信 TTL/HopLimit 1
	連続応答受信回数 1
	異常時送信開始待ち時間 0 秒 💌
	監視方式 ○常時監視○無通信時監視

41. 【保存】ボタンをクリックします。

LAN1情報を設定する

42. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

43. 以下の項目を指定します。

•	インタフェース	→物理LAN
	<lan<sup>M</lan<sup>	報追加フィールド>
-	インタフェース	物理LAN 🖌

44. [追加]ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

45. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

46. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 192.168.101.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
	 ○ DHCPで自動的に取得する ● 指定する 		
	IPアドレス 192.168.101.1		
	ネットマスク 24 (255.255.255.0) 🗸		
	ブロードキャストアドレ ス ネットワークアドレス+オール1 マ		

47. [保存] ボタンをクリックします。

本装置2との間で経路交換を設定する

- **48. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **49. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- **50.** 「ネットワーク情報」で相手定義番号が0の【修正】ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- **51.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP 基本情報」が表示されます。
- **52.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。

OSPF機能 →使用する



- 54. [保存] ボタンをクリックします。
- **55. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 56. 「LAN 情報」でインタフェースがLAN1の[修正] ボタンをクリックします。

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

- **57.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 58. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

59. 以下の項目を指定します。

- OSPF機能 →使用する
- パケット送信 →抑止する

■OSPF情報	3	
OSPF機能	○使用しない ●使用する	
エリア定義番号	0	
出力コスト	10	
Helloバケット送信間隔	10 秒 💙	
隣接ルータ停止確認間隔	40 秒 💌	
バケット再送間隔	5 秒 💌	
LSUバケット送信遅延時間	1 秒 💌	
認証方式	 ● 認証を行わない ● テキスト認証 鍵種別 ● 文字列 ● 16進数 認証鍵 ● MD5認証 MD5認証鍵 ● MD5認証鍵 	
パケット送信	⊙抑止する○抑止しない	

- 60. [保存] ボタンをクリックします。
- **61. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **62.** 「ルーティングマネージャ情報」をクリックします。 ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
- 63. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

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

「OSPFエリア情報」が表示されます。

- **65.** [追加] ボタンをクリックします。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 66. 以下の項目を指定します。
 - エリアID → 0.0.0.0

OSPFエリア基本	「「「」	3
エリアID	0.0.0.0	

- 67. [保存] ボタンをクリックします。
- **68. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

MPLS網との接続情報を設定する

「LAN0 情報(物理 LAN)」- 「IP 「IP アドレス情報」	関連」
• IPv4	→使用する
 IPアドレス 	→指定する
IPアドレス	→ 10.1.201.2
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「LAN0 情報(物理LAN)」-「MI 「MPLS基本情報」	PLS関連」
● MPLS 機能	→使用する
ラベル配布プロトコル	→LDP
「MPLS情報」	
「基本情報」	
• MPLS TTL 伝達	→しない
router ID	→ 10.1.201.2
制御方式	→independent
IPv4 Transportアドレス	→ 10.1.201.2
「ルーティングプロトコル情報」 「再配布情報」 • LDP	- 「ルーティングマネージャ情報」
インタフェース経路情報	→再配布しない

MPLS トンネルを設定する

「相手情報」-「ネットワーク情報」 ネットワーク名 → kawasaki 「ネットワーク情報」-「接続先情報」 接続先名 →lsp1 • 接続先種別 → MPLS トンネル接続 「接続先情報」-「MPLS トンネル接続」 「基本情報」 送出先インタフェース →LAN0 • IPv4 転送先ルータ → 10.1.201.1 自側エンドポイント → 10.0.0.201 • 相手側エンドポイント → 10.0.0.101 「ネットワーク情報」-「IP 関連」

•	IPアドレス	→設定する
	相手側IPアドレス	→ 10.0.0.101
	自側IPアドレス	→ 10.0.0.201

MPLS トンネルでシェーピングを設定する

「相手情報」-「ネットワーク情報」 「ネットワーク情報」-「共通情報」

•	シェーピング	→使用する
	最大送信レート	→5Mbps

MPLS トンネルでセッション監視を設定する

「相手情報」-「ネットワーク情報」 「接続先情報」-「MPLS トンネル接続」

「接続制御情報」

•	接続先監視	→使用する
	送信元IPアドレス	→10.0.0.201
	あて先IPアドレス	→ 10.0.0.101
	正常時送信間隔	→10秒
	再送間隔	→1秒
	タイムアウト時間	→5秒
	異常時送信間隔	→1分
	送信 TTL/Hoplimit	→ 1

LAN1情報を設定する

「LAN1情報	(物理LAN)」	-	「IP関連」
「IPアドレス情	青報」		
• IPv4			→使月

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 192.168.201.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

本装置1との間で経路交換を設定する

「相手情報」-「ネットワーク情報」
 「ネットワーク情報」-「IP 関連」
 「OSPF 情報」
 ● OSPF 機能 →使用する

「LAN1 **情報(物理**LAN)」-「IP 関連」 「OSPF 情報」

- OSPF機能 →使用する
- パケット送信 →抑止する

「ルーティングプロトコル情報」-「OSPF 関連」 「OSPF エリア情報」

エリアID →0.0.0.0

2.8 MPLSを使用したレイヤ2VPN(EoMPLS)を 構築する

適用機種 全機種

本装置では、MPLS網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク(閉 域網)を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用するこ とができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

● 参照 Si-Rシリーズ 機能説明書「2.8.1 MPLSを使用したレイヤ2VPN (EoMPLS)」(P.45)

ここでは、MPLS 接続サービス(キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送 サービスを想定しています)と、MPLS LSP トンネルを使用して事業所でレイヤ 2VPN を EoMPLS で構築する事 例を紹介します。

こんな事に気をつけて

- 複数のインタフェースを同一のVCに含めることはできません。
- ・ トンネルLSPを使用するインタフェースでは、MPLSを利用する設定にしてください。
- ・ VCインタフェースでは、シェーピング機能、LAN ポートバックアップ機能および VLAN 機能を併用して動作させる ことができます。IP機能、IPv6機能、ブリッジ機能(MAC フィルタ機能を含む)、VRRP機能は動作できません。
- EoMPLS通信を行う場合は、MAC学習やSTPのサポートを行わないため、パケットのループが発生しないように構成してください。Ethernetフレームがループし続けて通信できなくなります。また、EoMPLS通信を用いて冗長構成を行う場合も、LANインタフェース側に、STPなどを使用できるスイッチ装置を設置し、Ethernetフレームがループしないように設定してください。
- VLAN Tag が異なる VLAN インタフェースどうしで VC を構成し、LAN 側で STP を使用する場合は、VLAN Tag の値 をそろえてください。



● 前提条件

[本装置1]

- LAN0はMPLS網とし、LAN1、LAN2は事業所内LANとする
- 接続する MPLS 網の次ホップLSR とは、ループバックアドレスでコネクションを確立する
- MPLS 網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

[本装置2]

- LAN0はMPLS網とし、LAN1は事業所内LANとする
- 接続する MPLS 網の次ホップLSR とは、ループバックアドレスでコネクションを確立する
- MPLS網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

[本装置3]

- LAN0はMPLS網とし、LAN1は事業所内LANとする
- 接続する MPLS 網の次ホップ LSR とは、ループバックアドレスでコネクションを確立する
- MPLS網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

● 設定条件

[本装置1]

- LAN0 (MPLS網側)のIPアドレス: 10.1.104.2
- ループバックのIPアドレス : 10.0.0.104
- LAN1のVC番号 : 10
- LAN2のVC番号 : 20

[本装置2]

- LAN0 (MPLS 網側) の IP アドレス: 10.1.204.2
- ループバックのIPアドレス : 10.0.0.204
- LAN1のVC番号 : 10

[本装置3]

- LAN0 (MPLS 網側) の IP アドレス: 10.1.214.2
- ループバックのIPアドレス : 10.0.0.214
- LAN1のVC番号 :20

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

MPLS網との接続情報を設定する

- 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 10.1.104.2
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	●使用する●使用しない	
IPアドレス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス I0.1.104.2 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス 	

- 5. [保存] ボタンをクリックします。
- 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」ページが表示されます。

7. 以下の項目を指定します。

 ネットワーク 	→ネットワーク指定
あて先 IP アドレス	→ 10.0.0.204
あて先アドレスマスク	→32 (255.255.255.255)
中継ルータアドレス	→指定する
IPアドレス	→ 10.1.104.1
• メトリック値	→ 1
● 優先度	→ 0

<スタティック経路情報入力フィールド>				
	○ デフォルトルート			
ネ		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 	
ット	۲	ネットワーク指定		
5		あて先IPアドレス	10.0.0.204	
ーク		あて先アドレスマス ク	32 (255.255.255.255) 💌	
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 10.1.104.1 	
メトリック値 優先度	1	✓		

8. [追加] ボタンをクリックします。

9. 手順7.~8.を参考に、以下の項目を指定します。

٠	ネットワーク	→ネットワーク指定
	あて先IPアドレス	→ 10.0.0.214
	あて先アドレスマスク	→32 (255.255.255.255)
	中継ルータアドレス	→指定する
	IPアドレス	→ 10.1.104.1
•	メトリック値	→ 1
•	優先度	→0

10. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

11. 以下の項目を指定します。

- MPLS機能 →使用する
- ラベル配布プロトコル → LDP

MPLS基本情報	[3
MPLS機能	○使用しない ⊙使用する
ラベル配布ブロトコル	LDP 💌

12. [保存] ボタンをクリックします。

13. 設定メニューのルータ設定で「MPLS情報」をクリックします。

「MPLS情報」ページが表示されます。

14. 「基本情報」をクリックします。

「基本情報」が表示されます。

15. 以下の項目を指定します。

- MPLS TTL伝達 →する

こんな事に気をつけて

router IDとIPv4 Transportアドレスには、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■基	本情報	3
MPL:	S TTL伝達	●しない ●する
	router ID	10.0.0.104
LDP	制御方式	⊙independent Oordered
	IPv4 Transport アドレス	10.0.0.104

- 16. [保存] ボタンをクリックします。
- **17. 設定メニューの基本設定で「装置情報」をクリックします**。 「装置情報」ページが表示されます。

18. 「ループバック情報」をクリックします。

「ループバック情報」が表示されます。

19. 以下の項目を指定します。

- IPアドレス → 10.0.0.104
- OSPF機能
 →使用しない
- PHP機能 →使用しない

■ループバック情	報 [2]	
IPアドレス	10.0.0.104	
OSPF機能 使用しない 使用する エリア定義番号 ロ <liロ< li=""> ロ <liロ< li=""> <li< th=""></li<></liロ<></liロ<>		
PHP機能	○使用する ●使用しない	

20. [保存] ボタンをクリックします。

各拠点へのVCを設定する

- **21. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 22. 以下の項目を指定します。
 - インタフェース →物理LAN

	<lan情報追力< th=""><th>]フィールド></th></lan情報追力<>]フィールド>
インタフェース		物理LAN 🖌

- **23. [追加] ボタンをクリックします**。 「LAN1 情報(物理 LAN)」ページが表示されます。
- **24.** 「MPLS 関連」をクリックします。 MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。
- **25.** MPLS 関連の設定項目の「EoMPLS 情報」をクリックします。 「EoMPLS 情報」が表示されます。

- EoMPLS機能 →使用する
 VC ID → 10
 相手装置のIPv4アドレス → 10.0.0.204
 VC タイプ → auto
- EXP 値書き換え → 固定値 0

■EoMPLS情報	3
EoMPLS機能	○使用しない ⊙使用する
VC ID	10
相手装置のIPv4アトレス	10.0.204
VCタイプ	auto 🗸
EXP値書き換え	 ● 固定値 ● VLANタグのプライオリティを使用する

- 27. [保存] ボタンをクリックします。
- 28. 手順21.~27.を参考に、以下の項目を指定します。

「LAN2情報(物理LAN)」

- EoMPLS機能 →使用する
- VC ID →20
- 相手装置のIPv4アドレス → 10.0.0.214
- VCタイプ →auto
- EXP 値書き換え →固定値 0
- 29. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

MPLS網との接続情報を設定する

「LAN0 情報(物理LAN)」-「IP 関連」 「IP アドレス情報」

• IPv4

→使用する

IPアドレス IPアドレス ネットマスク ブロードキャストアドレス -

→指定する
 → 10.1.204.2
 → 24 (255.255.255.0)
 →ネットワークアドレス+オール1

「スタティック経路情報」

ネットワーク
 ネットワーク指定
 あて先IPアドレス
 → 10.0.0.104
 → 32 (255.255.255.0)
 中継ルータアドレス
 →指定する
 IPアドレス
 → 10.1.204.1

• メトリック値	→ 1			
● 優先度	→ 0			
「LAN0 情報」-「MPLS 関連」 「MPLS基本情報」				
• MPLS 機能	→使用する			
 ラベル配布プロトコル 	→LDP			
「MPLS情報」-「MPLS関連」				
 MPLS TTL 伝達 	→する			
• LDP				
router ID	→10.0.0.204			
制御方式	→independent			
IPv4 Transportアドレス	→ 10.0.0.204			

「ループバック情報」

•	IPアドレス	→ 10.0.0.204
•	OSPF機能	→使用しない
•	PHP機能	→使用しない

各拠点へのVCを設定する

ΓL	「LAN情報」-「MPLS関連」		
٢N	「MPLS基本情報」-「EoMPLS情報」		
•	EoMPLS 機能	→使用する	
•	VC ID	→ 10	
•	相手装置のIPv4アドレス	→ 10.0.0.104	
•	VCタイプ	→auto	
•	EXP値書き換え	→固定値0	

本装置3を設定する

「本装置2を設定する」を参考に、本装置3を設定します。

MPLS網との接続情報を設定する

「LAN0情報(物理LAN)」-「IP関連」

「IPアドレス情報」

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 10.1.214.2
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

筆	2	音	活田例
为	2	14	/ロ/ロ/リ

「スタティック経路情報」

•	ネットワーク	→ネットワーク指定
	あて先IPアドレス	→ 10.0.0.104
	あて先アドレスマスク	→32 (255.255.255.0)
	中継ルータアドレス	→指定する
	IPアドレス	→ 10.1.214.1
•	メトリック値	→ 1
•	優先度	→ 0
٢L	AN0情報」-「MPLS関連」	
٢N	IPLS基本情報」	
•	MPLS機能	→使用する
•	ラベル配布プロトコル	→LDP
٢N	/IPLS情報」-「MPLS関連」	
围	基本情報」	
•	MPLS TTL 伝達	→する
•	LDP	
	router ID	→ 10.0.0.214
	制御方式	→ independent

「装置情報」

「ループバック情報」

IPv4 Transportアドレス

•	IPアドレス	→10.0.0.214
•	OSPF機能	→使用しない
•	PHP機能	→使用しない

→ 10.0.0.214

各拠点への VC を設定する

「LAN 情報」-「MPLS 関連」 「MPLS基本情報」-「EoMPLS 情報」		
•	EoMPLS機能	→使用する
•	VC ID	→ 10
•	相手装置のIPv4アドレス	→ 10.0.0.104
•	VCタイプ	→auto
•	EXP値書き換え	→固定値0

2.9 MPLSを使用したレイヤ3VPN(BGP/MPLS VPN)を構築する

適用機種 全機種

本装置では、MPLS網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク(閉 域網)を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用するこ とができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

● 参照 Si-Rシリーズ 機能説明書「2.8.2 MPLSを使用したレイヤ3VPN (BGP/MPLS VPN)」(P.47)

ここでは、MPLSを使用した VPN ネットワークを構築する場合の設定方法を説明します。

東京事業所と川崎事業所がMPLS網に接続し、業務ごとに異なるVPNネットワークを構築します。このとき、本 装置1、2がそれぞれの前提条件を満たしていることを前提とします。

こんな事に気をつけて

- BGP/MPLS VPN 機能は IPv4 の場合だけ利用できます。 IPv6 では使用できません。
- BGPで接続できる相手は1セッションだけです。このため、ルートリフレクタと接続する必要があります。
- ・ IP-VPN 接続と併用することはできません。
- ・ BGPネットワーク、BGP集約経路およびBGPフィルタリングの機能は使用できません。
- BGP/MPLS VPN 機能とNAT 機能を併用することはできません。
- ・ 本装置は、LERとしてだけ動作します。
- ・ BGP/MPLS VPN で構成された VPN ネットワーク内では、EBGP、OSPF および RIP は使用できません。
- 異なる VPN を収容する場合、VPN のインタフェースに設定した IP アドレスおよび属するネットワークアドレスを他 VPN インタフェースに設定できません。必ず異なるネットワークアドレスを設定してください。
- MPLS網と接続するインタフェースで RIP を使用する場合、VPN で使用するインタフェース経路を RIP で広報しま す。MPLS への広報に対してフィルタリングを行ってください。
- LERでは、受信したIPパケットをIP処理層を通さずにラベルを付加します。IPフィルタリング機能、TOS値書き換え機能およびソートフラグメント機能は、VPNに設定したインタフェースへの入力に限り動作します。ただし、VPN からの入力をIPsecによって暗号化し、対向ルータに送信する運用や帯域制御(WFQ)機能、イコールコストマルチパスなどの他IP機能を使用した運用は行うことはできません。
- VRRPと併用する場合は、トリガとしてインタフェースダウントリガまたはルートダウントリガ(VPN内経路は対象 外)が利用できます。ノードダウントリガは利用できません。
- BGP/MPLS VPN構成では、LERはMTU長の設定にかかわらず、IPパケットのフラグメント処理を行いません。受 信したパケットはそのままラベルを付加して送信します。このため、MTU長を調整する必要がある運用(VoIP通信 でのインターリーブなど)はできません。
- ・ ループバックインタフェースで設定した IP アドレスを BGP の自側 IP アドレスとして使用しなければいけません。
- IP アドレスが設定されていないインタフェースでは MPLS は使用できません。隣接 MPLS 装置間で LDP セッション を構築する際、インタフェースのアドレスを用いる場合があります。
- BRIなどの低速回線での高負荷時や装置の転送能力を超える高負荷が発生する場合、LDPセッションが切断されることがあります。LDPのHelloホールドタイマを長め(例:30秒)に設定してください。
- MPLSを利用すると、Ethernetフレームに4バイトのシムヘッダが最大2つ付加されます。最大1526バイトの Ethernetフレームが送出されることになります。通常のEthernetフレームの最大サイズは1518バイトです。1526バ イトのフレームに対応していない機器と接続する場合は、MPLSを利用するインタフェースのMTUサイズを初期値 の1500バイトから1492バイトに変更することで通信することができます。
- VPN 通信で使用するネットワークアドレスと、本装置に設定するすべてのネットワークアドレスが重複しないように 設定してください。たとえば、本装置の MPLS ドメイン側 IP アドレスが 10.1.1.1/24 のとき、10.1.1.0/24 のネット ワークを VPN として収容することはできません。
- ・ VPN 以外の SNMP マネージャは VPN 内の装置を管理することはできません。
- BGP セッションの通信に使用するループバックインタフェースに設定したアドレスへの経路は集約しないでください。集約すると、トンネルLSP が正しく生成されません。

2.9.1 MPLS 網とLAN を使用して接続する

適用機種 全機種



LSR(Label Switching Router):MPLSコアルータ RR(Route Reflector) :ルートリフレクタ

● 前提条件

[本装置1]

- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける VLAN ID:2 ネットワークアドレス: 10.10.10.0/24 VLAN ID:3 ネットワークアドレス: 10.20.10.0/24
- LAN1はVLAN出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN1とする
- LAN0のIPアドレス : 172.16.2.2
- LAN2のIPアドレス : 10.10.10.1
- LAN3のIPアドレス : 10.20.10.1
- LAN0~3では、NAT機能およびDHCPクライアント機能は使用しない

[本装置2]

- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける
 - VLAN ID:2 ネットワークアドレス:10.10.20.0/24

```
VLAN ID:3 ネットワークアドレス:10.20.20.0/24
```

- LAN1はVLAN出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN1とする
- LAN0のIPアドレス : 172.16.1.2
- LAN2のIPアドレス : 10.10.20.1
- LAN3のIPアドレス : 10.20.20.1
- LAN0~3では、NAT機能およびDHCPクライアント機能は使用しない

● 設定条件

 MPLS 網の使用条件 	
BGP AS番号	: 10
RRのIPアドレス	: 172.16.100.1
MPLS網で使用する IPv4 ネットワーク	: OSPF
	: バックボーンエリア
 VPN-Aの使用条件 	
ルート識別子	: 10:1
使用するネットワーク	:10.10.10/24 川崎事業所
	:10.10.20/24 東京事業所
	:10.10.21/24 東京事業所
● VPN-Bの使用条件	
ルート識別子	: 10:2
使用するネットワーク	:10.20.10/24 川崎事業所
	:10.20.20/24 東京事業所
	:10.20.21/24 東京事業所

[本装置1]

•	ループバックインタフェースのIPアドレス	: 10.1.1.1
•	ループバックインタフェースでのルーティングプロトコル	: OSPF
•	ループバックインタフェースでの OSPF エリア ID	: 0.0.0.1
•	LAN0 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.1
•	LAN2 で使用する VPN	: VPN-A
•	LAN3 で使用する VPN	: VPN-B
[4	「装置2]	
•	ループバックインタフェースのIPアドレス	: 10.2.1.1
•	ループバックインタフェースでのルーティングプロトコル	: OSPF
•	ループバックインタフェースでの OSPF エリア ID	: 0.0.0.2
•	LAN0 でのルーティングプロトコル	: OSPF
•	LANOでのOSPFエリアID	: 0.0.0.2
•	LAN2 で使用する VPN	: VPN-A
•	LAN2 で使用する BGP/MPLS VPN スタティック経路情報	
	あて先IPアドレス	: 10.10.21.0/24
	中継ルータアドレス	: 10.10.20.2
•	LAN3 で使用する VPN	: VPN-B
•	LAN3 で使用する BGP/MPLS VPN スタティック経路情報	
	あて先IPアドレス	: 10.20.21.0/24
	中継ルータアドレス	: 10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置2を設定する

ループバック情報を設定する

- 設定メニューの基本設定で「装置情報」をクリックします。
 「装置情報」ページが表示されます。
- 「ループバック情報」をクリックします。
 「ループバック情報」が表示されます。
- 3. 以下の項目を指定します。
 - IPアドレス → 10.2.1.1
 OSPF機能 →使用する エリア定義番号 → 0

こんな事に気をつけて

エリア定義は、ルータ設定の「ルーティングプロトコル情報」-「OSPFエリア情報」で設定します。

■ループバック情報 2		
IPアトレス	10.2.1.1	
OSPF機能	 ○ 使用しない ③ 使用する エリア定義番号 □ 	

4. [保存] ボタンをクリックします。

MPLS 網と接続する LAN0 に OSPF 機能を設定する

- 5. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN 情報」ページが表示されます。
- 6. 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 7. 「IP 関連」をクリックします。IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **8.** IP **関連の設定項目の「OSPF 情報」をクリックします**。 「OSPF 情報」が表示されます。
- 9. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ⊙使用する
エリア定義番号	0

10. [保存] ボタンをクリックします。
OSPF 関連を設定する

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

→0.0.0.2

- **12.** 「OSPF 関連」をクリックします。 OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
- **13.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- **14.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 15. 以下の項目を指定します。
 - エリアID

■OSPFエリア基本情報		3
エリアID	0.0.0.2	

16. [保存] ボタンをクリックします。

MPLS 網と接続する LAN0 に MPLS 機能を設定する

- **17. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **18.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **19.** 「MPLS 関連」をクリックします。

MPLS関連の設定項目と「MPLS基本情報」が表示されます。

- 20. 以下の項目を指定します。
 - MPLS機能 →使用する
 - ラベル配布プロトコル → LDP

MPLS基本情報	3
MPLS機能	○使用しない ●使用する
ラベル配布ブロトコル	LDP 💌

- 21. [保存] ボタンをクリックします。
- **22. 設定メニューのルータ設定で「MPLS 情報」をクリックします**。 「MPLS 情報」ページが表示されます。
- **23. 「基本情報」をクリックします。** 「基本情報」が表示されます。

● MPLS TTL 伝達

LDP	
router ID	→ 10.2.1.1
制御方式	→ independent
IPv4 Transportアドレス	→ 10.2.1.1

こんな事に気をつけて

router IDとIPv4 Transportアドレスには、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■基	本情報	3
MPLS TTL伝達		⊙しない ⊙する
	router ID	10.2.1.1
LDP	制御方式	⊙independent Oordered
	IPv4 Transport アドレス	10.2.1.1

25. [保存] ボタンをクリックします。

ルートリフレクタの接続情報を設定する

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

→する

27. 「BGP 関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

- 28. 以下の項目を指定します。
 - BGP機能 →使用する
 - 自AS番号 →10
 - 自ID番号 →10.2.1.1

こんな事に気をつけて

自ID番号には、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■BGP情報	3
BGP機能	○使用しない ●使用する
自AS番号	10
自ID番号	10.2.1.1

- 29. [保存] ボタンをクリックします。
- **30.** BGP **関連の設定項目の「**BGP **相手情報」をクリックします**。 「BGP 相手情報」が表示されます。
- **31. [追加] ボタンをクリックします。** BGP相手情報(0)の設定項目と「BGP相手基本情報」が表示されます。

- 相手側 IP アドレス → 172.16.100.1
- 相手AS番号 →10
- 自側IPアドレス → 10.2.1.1

こんな事に気をつけて

- ルートリフレクタのIPアドレスを相手側IPアドレスに設定してください。
- ・ 自側 IP アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

■BGP相手基本情報	
相手側IPアト レス	172.16.100.1
相手AS番号	10
自側IPアFレ ス	10.2.1.1

- 33. [保存] ボタンをクリックします。
- **34.** BGP 相手情報(0)の設定項目の「BGP 拡張機能情報」をクリックします。 「BGP 拡張機能情報」が表示されます。
- 35. 以下の項目を指定します。
 - アドレスファミリ情報 → VPN IPv4ユニキャスト

■BGP拡張機能情報	3
アドレスファミリ情報	VPN IPv4ユニキャスト 💌

36. [保存] ボタンをクリックします。

VPN-AおよびVPN-B情報としてVRF情報を設定する

- **37. 画面上部の「ルーティングプロトコル情報」をクリックします。** 「ルーティングプロトコル情報」のページが表示されます。
- **38. 「**BGP 関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

39. BGP **関連の設定項目の「VRF 情報」をクリックします**。 「VRF 情報」が表示されます。

•	ルート識別子	
	AS番号	→ 10
	識別番号	→ 1
•	BGP/MPLS VPN 広報	
	スタティック経路情報	→再配布する
	インタフェース経路情報	→再配布する

<vrf情報入力フィールド></vrf情報入力フィールド>			
山山大港明之	AS番号	10	
ノレー「10戦力」」	識別番号 <mark></mark>	1	
BGP/MPLS VPN広 報	スタティック経路情報	○再配布しない ③再配布する	
	インタフェース経路情 報	○再配布しない ③ 再配布する	

- 41. [追加] ボタンをクリックします。
- 42. 手順40.~41.を参考に、以下の項目を指定します。

•	ルート識別子	
	AS番号	→ 10
	識別番号	→ 2
•	BGP/MPLS VPN 広報	
	スタティック経路情報	→再配布する
	インタフェース経路情報	→再配布する

LAN2情報を設定する

- **43. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **44.** 「LAN 情報」でインタフェースがLAN2の【修正】ボタンをクリックします。 「LAN2 情報(物理LAN)」ページが表示されます。
- **45.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 46. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する
 IPアドレス → 10.10.20.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報				
IPv4	●使用する●使用しない			
IPアドレス	 DHCPで自動的に取得する 指定する IPアドレス 10.10.20.1 ネットマスク 24 (255.255.255.0 ブロードキャストアドレ ス) マ ス+オール1 マ		

47. [保存] ボタンをクリックします。

48. IP 関連の設定項目の「BGP/MPLS VPN 情報」をクリックします。

「BGP/MPLS VPN 情報」が表示されます。

49. 以下の項目を指定します。

- BGP/MPLS VPN 機能 →使用する
- VRF 定義番号 →0

■BGP/MPLS VPN情報		3
BGP/MPLS VPN機能	○使用しない⊙使用する	
VRF定義番号	0	

- 50. [保存] ボタンをクリックします。
- 51. IP 関連の設定項目の「BGP/MPLS VPNスタティック経路情報」をクリックします。

「BGP/MPLS VPN スタティック経路情報」が表示されます。

- 52. 以下の項目を指定します。
 - ネットワーク あて先IPアドレス あて先アドレスマスク 中継ルータアドレス

→ネットワーク指定
 → 10.10.21.0
 → 24 (255.255.255.0)
 → 10.10.20.2



53. [追加] ボタンをクリックします。

54. 手順43.~53.を参考に、「LAN3情報(物理LAN)」で以下の項目を指定します。

LAN3情報を設定する

「LAN 情報3 情報	(物理LAN)」-	「IP関連」
「IPアドレス情報」		

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 10.20.20.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 →使用する
- VRF定義番号 →1

「BGP/MPLS VPN スタティック経路情報」

 ネットワーク あて先IPアドレス あて先アドレスマスク 中継ルータアドレス →ネットワーク指定
→ 10.20.21.0
→ 24 (255.255.255.0)
→ 10.20.20.2

55. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

本装置1を設定する

「本装置2を設定する」を参考に、本装置1を設定します。

ループバック情報を設定する

「装置情報」-「ループバック情報」

- IPアドレス → 10.1.1.1
 OSPF機能 →使用する
- エリア定義番号 →0

MPLS 網と接続する LAN0 に OSPF 機能を設定する

「LAN0 情報」-「IP 関連」 「OSPF 情報」

- OSPF機能 →使用する
- エリア定義番号 →0

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

エリアID → 0.0.0.1

MPLS 網と接続する LAN0 に MPLS 機能を設定する

「LAN0情報」-「MPLS関連」 -

「MPLS基本情報」

- MPLS機能 →使用する
- ラベル配布プロトコル → LDP

「MPLS情報-「基本情報」

- MPLS TTL 伝達 →する

ルートリフレクタの接続情報を設定する

1	「 <mark>ルーティングプロトコル情報」</mark> 「BGP 情報」	- 「BGP関連」
•	BGP機能	→使用する
	自AS番号	→ 10
•	• 自ID番号	→ 10.1.1.1
[BGP相手情報」-「BGP相手基本情	青報」
•	• 相手側IPアドレス	→ 172.16.100.1
•	• 相手AS番号	→ 10
•	● 自側IPアドレス	→ 10.1.1.1
I	BGP相手情報」-「BGP拡張機能情	青報」
•	 アドレスファミリ情報 	→VPN IPv4ユニキャスト
VPN-/	Aおよび VPN-B 情報として V	RF情報を設定する
	ー ルーティングプロトコル情報」	- 「BGP関連」
1		
	AS番号	→ 10
	識別番号	→ 1
•	● BGP/MPLS VPN 広報	
	スタティック経路情報	→再配布しない
	インタフェース経路情報	→冉配布する
I		
•		. 10
	AS街勺 	\rightarrow 10 \rightarrow 2
-		· Z
•		

LAN2情報を設定する

「LAN2情報」-「IP 関連」 「IP アドレス情報」

スタティック経路情報

インタフェース経路情報

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

「LAN2情報」-「BGP関連」

「BGP/MPLS VPN 情報」

• BGP/MPLS VPN 榜	能 →使用する
------------------	---------

• VRF定義番号 →0

→再配布しない

→再配布する

LAN3情報を設定する

「LAN3 情報」-「IP 関連」 「IP アドレス情報」

• IPv4

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

「LAN3情報」-「BGP関連」 「BGP/MPLS VPN情報」

- BGP/MPLS VPN 機能 →使用する
- VRF定義番号 →1

2.9.2 MPLS 網と専用線を使用して接続する

適用機種 Si-R220B,220C,370,570



LSR(Label Switching Router):MPLSコアルータ RR(Route Reflector) :ルートリフレクタ

● 前提条件

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

● 設定条件

- MPLS 網の使用条件 BGP AS 番号 RRの IP アドレス MPLS 網で使用する IPv4 ネットワーク
- VPN-Aの使用条件 ルート識別子 使用するネットワーク
- VPN-Bの使用条件 ルート識別子 使用するネットワーク

: 10 : 172.16.100.1 : OSPF : バックボーンエリア : 10:1 : 10.10.10/24 川崎事業所 : 10.10.20/24 東京事業所 : 10.10.21/24 東京事業所

: 10:2

- :10.20.10/24 川崎事業所
- :10.20.20/24 東京事業所
- : 10.20.21/24 東京事業所

[本装置1(川崎事業所)]

ループバックインタフェースのIPアドレス : 10.1.1.1
 ループバックインタフェースでのルーティングプロトコル : OSPF
 ループバックインタフェースでのOSPFエリアID : 0.0.0.1
 rmt0でのルーティングプロトコル : OSPF
 rmt0でのOSPFエリアID : 0.0.0.1

٠	LAN0 で使用する VPN	: VPN-A
٠	LAN1 で使用する VPN	: VPN-B
[7	\$装置2(東京事業所)]	
•	ループバックインタフェースのIPアドレス	: 10.2.1.1
•	ループバックインタフェースでのルーティングプロトコル	: OSPF
•	ループバックインタフェースでのOSPFエリアID	: 0.0.0.2
•	rmt0 でのルーティングプロトコル	: OSPF
•	rmt0でのOSPFエリアID	: 0.0.0.2
•	LAN0 で使用する VPN	: VPN-A
•	LAN0で使用する BGP/MPLS VPN スタティック経路情報	
	あて先IPアドレス	: 10.10.21.0/24
	中継ルータアドレス	: 10.10.20.2
•	LAN1 で使用する VPN	: VPN-B
٠	LAN1 で使用する BGP/MPLS VPN スタティック経路情報	
	あて先IPアドレス	: 10.20.21.0/24
	中継ルータアドレス	: 10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置2を設定する

ループバック情報を設定する

- 設定メニューの基本設定で「装置情報」をクリックします。
 「装置情報」ページが表示されます。
- 「ループバック情報」をクリックします。
 「ループバック情報」が表示されます。
- 3. 以下の項目を指定します。
 - IPアドレス → 10.2.1.1
 OSPF機能 →使用する エリア定義番号 → 0

こんな事に気をつけて

```
エリア定義は、ルータ設定の「ルーティングプロトコル情報」-「OSPFエリア情報」で設定します。
```

■ループバック情報 [
IPアドレス	10.2.1.1
OSPF機能	 ○ 使用しない ③ 使用する エリア定義番号 □

4. [保存] ボタンをクリックします。

MPLS 網と接続するインタフェースに OSPF 機能を設定する

- 5. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- OSPF 機能を設定するネットワーク欄の [修正] ボタンをクリックします。
 「ネットワーク情報」ページが表示されます。
- **6.** 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- IP 関連の設定項目の「OSPF 情報」をクリックします。
 「OSPF 情報」が表示されます。
- 10. 以下の項目を指定します。
 - OSPF機能 →使用する
 - エリア定義番号 →0

■OSPF情報	3
OSPF機能	○使用しない ●使用する
エリア定義番号	0

- 11. [保存] ボタンをクリックします。
- **12. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **13.** 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- **14.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- **15.** 【追加】ボタンをクリックします。 OSPFエリア情報(0)の「OSPFエリア基本情報」が表示されます。
- 16. 以下の項目を指定します。

• エリアID

→	0.	0.	0	.2

335

■OSPFエリア基本情報		3
エリアID	0.0.0.2	

17. [保存] ボタンをクリックします。

MPLS 網と接続するインタフェースに MPLS 機能を設定する

- **18. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **19. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。

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

「ネットワーク情報」ページが表示されます。

21. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

- 22. 以下の項目を指定します。
 - MPLS機能 →使用する
 - ラベル配布プロトコル → LDP

MPLS基本情報	3
MPLS機能	○使用しない ●使用する
ラベル配布ブロトコル	LDP 💌

- 23. [保存] ボタンをクリックします。
- **24.** 設定メニューのルータ設定で「MPLS情報」をクリックします。

「MPLS 情報」ページが表示されます。

25. 「基本情報」をクリックします。

「基本情報」が表示されます。

26. 以下の項目を指定します。

•	MPLS TTL 伝達	→する
•	LDP	
	router ID	→ 10.2.1.1
	制御方式	→ independent
	IPv4 Transportアドレス	→ 10.2.1.1

こんな事に気をつけて

router IDとIPv4 Transportアドレスには、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■基本情報		3	
MPL:	S TTL伝達	⊙しない ⊙する	
	router ID	10.2.1.1	
LDP	制御方式	⊙independent ⊙ordered	
	IPv4 Transport アドレス	10.2.1.1	

27. [保存] ボタンをクリックします。

ルートリフレクタへの接続情報を設定する

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

336

29. 「BGP 関連」をクリックします。 BGP 関連の設定項目と「BGP 情報」が表示されます。

- BGP機能 →使用する
- 自AS番号 →10
- 自ID番号 → 10.2.1.1

こんな事に気をつけて

自ID番号には、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

BGP情報	
BGP機能	○使用しない ●使用する
自AS番号	10
自ID番号	10.2.1.1

- 31. [保存] ボタンをクリックします。
- **32.** BGP 関連の設定項目の「BGP 相手情報」をクリックします。

「BGP相手情報」が表示されます。

33. [追加] ボタンをクリックします。

BGP相手情報(0)の設定項目と「BGP相手基本情報」が表示されます。

34. 以下の項目を指定します。

- 相手側IPアドレス →172.16.100.1
- 相手AS番号 →10
- 自側IPアドレス → 10.2.1.1

こんな事に気をつけて

- ルートリフレクタのIPアドレスを相手側IPアドレスに設定してください。
- ・ 自側 IP アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

■BGP相手基本情報	
相手側IPアト レス	172.16.100.1
相手AS番号	10
自側IPアドレ ス	10.2.1.1

- 35. [保存] ボタンをクリックします。
- **36.** BGP 相手情報(0)の設定項目の「BGP 拡張機能情報」をクリックします。 「BGP 拡張機能情報」が表示されます。
- 37. 以下の項目を指定します。
 - アドレスファミリ情報 → VPN IPv4 ユニキャスト

■BGP拡張機能情報	3
アドレスファミリ情報	IPv4그二キャスト ♥

38. [保存] ボタンをクリックします。

VPN-AおよびVPN-B情報としてVRF情報を設定する

- **39. 画面上部の「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」のページが表示されます。
- **40.** 「BGP 関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

41. BGP 関連の設定項目の「VRF 情報」をクリックします。

「VRF 情報」が表示されます。

42. 以下の項目を指定します。

- ルート識別子
 AS番号 → 10
 識別番号 → 1
- BGP/MPLS VPN 広報
 スタティック経路情報 →再配布する
 インタフェース経路情報 →再配布する

<vrf情報入力フィールド></vrf情報入力フィールド>		
비 드니 沖미고	AS番号	10
リレード諸戦力リナ	識別番号	1
BGP/MPLS VPN広	スタティック経路情報	○再配布しない ⊙ 再配布す る
幸反	インタフェース経路情 報	○再配布しない ③ 再配布する

43. [追加] ボタンをクリックします。

44. 手順42.~43.を参考に、以下の項目を指定します。

- ルート識別子
 AS番号 → 10
 識別番号 → 2
 BGP/MPLS VPN 広報
- スタティック経路情報 →再配布する インタフェース経路情報 →再配布する

LAN0 情報を設定する

- **45. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **46.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **47.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。

•	IPv4	→使用する
•	IPアドレス	→指定する
	IPアドレス	→ 10.10.20.1
	ネットマスク	→24 (255.255.255.0)
	ブロードキャストアドレス	→ネットワークアドレス+オール1

■IPアドレス情報 🥑			
IPv4	⊙使用する○使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 10.10.20.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 		

- 49. [保存] ボタンをクリックします。
- **50**. IP 関連の設定項目の「BGP/MPLS VPN 情報」をクリックします。

「BGP/MPLS VPN 情報」が表示されます。

- 51. 以下の項目を指定します。
 - BGP/MPLS VPN 機能 →使用する
 - VRF定義番号 →0

BGP/MPLS VPN情報		3
BGP/MPLS VPN機能	○使用しない ⊙使用する	
VRF定義番号	0	

- 52. [保存] ボタンをクリックします。
- **53.** IP 関連の設定項目の「BGP/MPLS VPN スタティック経路情報」をクリックします。 「BGP/MPLS VPN スタティック経路情報」が表示されます。
- 54. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →10.10.21.0
 →24 (255.255.255.0)
 中継ルータアドレス
 →10.10.20.2

<bgp mpls="" vpnスタティック経路情報入力フィールド=""></bgp>			
ネットワーク	 デフォルトルート 中継ルータアドレス ・ホットワーク指定 あて先IPアドレス 10.10.21.0 あて先アドレスマスク 24 (255.255.255.0) 中継ルータアドレス 10.10.20.2 		

55. [追加] ボタンをクリックします。

56. 手順45.~55.を参考に、「LAN1情報(物理LAN)」で以下の項目を指定します。

LAN1情報を設定する

```
    「LAN1情報(物理LAN)」-「IP関連」
    「IPアドレス情報」
    ・ IPv4 →使用する
    ・ IPアドレス →指定する
    ۱Pアドレス →10.20.20.1
    ネットマスク →24 (255.255.255.0)
    ブロードキャストアドレス →ネットワークアドレス+オール1
```

「LAN1情報(物理LAN)」-「BGP関連」

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 →使用する
- VRF 定義番号 → 1

「BGP/MPLS VPN スタティック経路情報」

- ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →10.20.21.0
 →24 (255.255.255.0)
 中継ルータアドレス
 →10.20.20.2
- 57. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

本装置1を設定する

「本装置2を設定する」を参考に、本装置1を設定します。

ループバック情報を設定する

「装置情報」-「ループバック情報」

•	IPアドレス	→ 10.1.1.1
•	OSPF機能	→使用する
	エリア定義番号	→ 0

MPLS 網と接続するインタフェースに OSPF 機能を設定する

「LAN 情報」-「IP 関連」 「OSPF 情報」			
• OSPF機能			
 エリア定義番号 			

「ルーティングプロトコル情報」-「OSPF 関連」

「OSPF エリア情報(0)」-「OSPF エリア基本情報」

エリアID →0.0.0.1

→使用する

 $\rightarrow 0$

MPLS 網と接続するインタフェースに MPLS 機能を設定する

「相手情報」-「ネットワーク情報」 「ネットワーク情報」-「MPLS 関連」 「MPLS 基本情報」		
• MPLS 機能	→使用する	
 ラベル配布プロトコル 	→LDP	
「MPLS情報」-「基本情報」		
• MPLS TTL 伝達	→する	
• LDP		
router ID	→ 10.1.1.1	
制御方式	→ independent	
IPv4 Transportアドレス	→ 10.1.1.1	
ルートリフレクタへの接続情報を	設定する	
「ルーティングプロトコル情報」 「BGP情報」	- 「BGP関連」	
● BGP機能	→使用する	
• 自AS番号	→ 10	
• 自ID番号	→ 10.1.1.1	
「BGP相手情報」-「BGP相手基本	「情報」	
• 相手側 IP アドレス	→ 172.16.100.1	
● 相手AS番号	→ 10	
• 自側IPアドレス	→ 10.1.1.1	
「BGP相手情報」-「BGP拡張機能	行報」	
 アドレスファミリ情報 	→VPN IPv4ユニキャスト	

VPN-AおよびVPN-B情報としてVRF情報を設定する

「ルーティングプロトコル情報」-「BGP 関連」 「VRF 情報(0)」		
• ,	ルート識別子 AS 番号 識別番号	\rightarrow 10 \rightarrow 1
•	BGP/MPLS VPN 広報 スタティック経路情報 インタフェース経路情報	→再配布しない →再配布する
ΓVR	RF情報(1)」	
• ,	ルート識別子 AS 番号 識別番号	\rightarrow 10 \rightarrow 2
•	BGP/MPLS VPN 広報 スタティック経路情報 インタフェース経路情報	 →再配布しない →再配布する

LAN0 情報を設定する

「LAN0 情報」- 「IP 関連」 「IP アドレス情報」	
• IPv4	→使用する
• IPアドレス	→指定する
IPアドレス	→ 10.10.10.1
ネットマスク	→24 (255.255.255.0)
ブロードキャストアドレス	→ネットワークアドレス+オール1
「BGP/MPLS VPN 情報」	

- BGP/MPLS VPN 機能 →使用する
- VRF定義番号 →0

LAN1情報を設定する

「LAN1情報」	-	ΓIΡ	関連」	
「IPアドレス情	報	L		

•	IPv4	

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

→使用する

→1

「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 →使用する
- VRF 定義番号

こんな事に気をつけて

サポートインタフェースは PRI(ISDN、HSD)、BRI(ISDN、HSD)、ATMとLAN です。モデムや FR には対応していません。

▲注意 -

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

2.10 マルチリンク機能を使う

適用機種 Si-R220B,220C,370,570

2.10.1 ISDN でマルチリンク機能を使う

適用機種 Si-R220B,220C,370,570

ISDNによって相手装置と接続するときに、マルチリンク機能を使用することができます。マルチリンク機能では、Bチャネル(64Kbps)を論理的に複数本束ねることによって、最大1472Kbpsで通信できます。また、回線 使用率によって動的にチャネル数を増減することができ、回線を効率良く利用することができます。

● 参照 Si-Rシリーズ 機能説明書「2.9 マルチリンク機能」(P.50)

ここでは、ISDN 接続をネットワーク情報(intranet)で定義してある環境に対してマルチリンクを行う場合の設定方法を説明します。

● 設定条件

- ネットワーク情報 (intranet) で ISDN による通信環境が設定済み
- 接続直後のリンク数は2チャンネル
- 最大リンク数は4チャネル(2本のINSネット64回線を利用する)
- チャネルの使用率90%以上が10秒以上続いたら、チャネルを増加する
- チャネルの使用率40%以下が60秒以上続いたら、チャネルを減少する
- 受信順序制御機能(MP)を使用する

上記の設定条件に従ってマルチリンクを行う場合の設定例を示します。

回線情報を設定する

- 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

 「WAN 情報」ページが表示されます。
- インタフェースがWAN0の【修正】ボタンをクリックします。
 「基本情報」ページが表示されます。
- 3. 以下の項目を指定します。
 - 自局番号チェック
 チェックする番号1

→する →電話番号を指定 →03-7777-7777 (回線自局電話番号)

	 ○ しない ○ する 	
自局番号チェ ック	チェックする番 号1	 電話番号を指定 ● 03-7777-7777 サブアドレス
	チェックする番 号2	電話番号を指定 サブアドレス
	グローバル着 信	○利用しない●利用する

- 4. [保存] ボタンをクリックします。
- 5. 手順1.~4.を参考に、WAN1情報を設定します。

相手情報を設定する

- **6. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- ネットワーク名がintranetの[修正] ボタンをクリックします。
 「ネットワーク情報 (intranet)」ページが表示されます。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。
- **10. 「接続先情報」でマルチリンクを設定する接続先の[修正] ボタンをクリックします**。 ISDN 接続の設定項目と「基本情報」が表示されます。
- 11. 以下の項目を指定します。
 - 使用インタフェース →すべて

使用インタフェース すべて 🗸

- 12. [保存] ボタンをクリックします。
- **13.** ISDN 接続の設定項目の「PPP 情報」をクリックします。 「PPP 情報」が表示されます。
- 14. 以下の項目を指定します。
 - MP接続 →する
 BAP/BACP利用 →する



15. [保存] ボタンをクリックします。

PPP 関連を設定する

- **16. 画面上部の「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- **17.** 「PPP 関連」をクリックします。 PPP 関連の設定項目と「圧縮情報」が表示されます。
- 18. PPP関連の設定項目の「MP情報」をクリックします。

- MP回線初期リンク数 →2
- MP回線最大リンク数 →4

•	トラフィックによる増減	→する
	回線増加条件	
	回線使用率	→90
	猶予時間	→ 10
	回線削除条件	
	回線使用率	→40
	猶予時間	→60
		. –

● 受信パケット順序制御 →する

MP情報		3
MP回線初回リンク数	2	
MP回線最大リンク数	4	
最小分割長		
トラフィックによる増減	 ● しない ● する ● 同線使用率 猶予時間 ● 回線増加条件 90 % 10 秒 ● 同線削減条件 40 % 60 秒 	
受信バケット順序制御	○しない ⊙する	

- 20. [保存] ボタンをクリックします。
- 21. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- ・ 複数の ISDN 回線を利用してマルチリンク機能を利用する場合は、以下のどちらかが必要です。
 - 着信側回線で代表取り扱いサービスを契約し、同じ番号でどちらの回線でも着信できるようにする。
 - 装置に自局電話番号を正しく設定したうえで、BAPを利用する。
- 初期接続時はすべて同じ電話番号に発信するため、相手側が電話番号の異なる複数の回線で構成される場合は、指定 された初期接続回線数まで増やせないことがあります。この場合は着信側回線で代表取り扱いサービスを契約し、同 じ番号でどちらの回線でも着信できるようにしてください。

2.10.2 複数専用線でマルチリンク機能を使う

適用機種 Si-R370,570

複数の専用線によって単一の論理リンクを構成することができます。この場合、定義上は1つの専用線を主たる 回線(マスタ回線)として定義し、残りの専用線は補助回線(バンドル回線)として定義します。 ここでは、論理リンクを介して2つの事業所(本店、支店)のネットワークを接続する場合について説明します。

● 参照 Si-Rシリーズ 機能説明書「2.9 マルチリンク機能」(P.50)

こんな事に気をつけて 速度の異なる回線を論理回線として結合した場合、期待する速度が出ない場合があります。また、専用線だけで論理リ ンクを構成した場合は、PPP最大接続チャネル数および初期接続チャネル数は無視されます。



● 設定条件

- マスタ回線として、スロット0に実装されたBRI拡張モジュールL2で専用線(128Kbps)を使用する
- バンドル回線として、スロット1に実装された BRI 拡張モジュール L2 で専用線(128Kbps)を使用する

[本店]

•	接続ネットワーク名	: honten
•	接続先名	: honten-1
•	本装置の IP アドレス / ネットマスク	: 192.168.1.1/24
•	マルチリンクのためのユーザ認証 ID とユーザ認	証パスワード
	発信	: honten hontenpasswd
	着信	: shiten shitenpasswd
[3	5店]	
•	接続ネットワーク名	: shiten
•	接続先名	: shiten-1
•	本装置のIPアドレス/ネットマスク	: 192.168.2.1/24

マルチリンクのためのユーザ認証 ID とユーザ認証パスワード
 発信
 注 shiten shitenpasswd
 着信
 注 honten hontenpasswd

上記の設定条件に従って本店の論理リンクの設定例を示します。

回線情報を設定する

スロット 0-0:WAN0 スロット 1-0:WAN1 として以下の手順で設定します。

1. 設定メニューのルータ設定で「WAN 情報」をクリックします。 「WAN 情報」ページが表示されます。

2. 以下の項目を指定します。

• 回線インタフェース →専用線

<want情報追加フィールド></want情報追加フィールド>		
回線インタフェース	専用線 🔽	

- 【追加】ボタンをクリックします。
 「WAN0情報(専用線)」ページが表示されます。
- **4. 「基本情報」をクリックします**。 「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - ポート →スロット0-0
 - 回線速度 → 128kbps
 - フラグ監視 →無効にする

■基本情報	3
ボート	지미ット 0-0 🗸
回線速度	128Kbps 💌
フラグ監視	●無効にする ○有効にする

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、WAN1情報を設定します。

相手情報を設定する

- 設定メニューのルータ情報で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。

ネットワーク名

→ honten

<ネットワーク情報追加フィールド>		
ネットワーク名	honten	

11. [追加] ボタンをクリックします。

「ネットワーク情報(honten)」ページが表示されます。

12. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

13. 以下の項目を指定します。

• 接続先種別

→専用線接続



14. [追加] ボタンをクリックします。 専用線接続の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

- 接続先名 → honten-1
- 使用インタフェース → WANO

■基本情報	3
接続先名	honten-1
使用インタフェース	WANO 💌

- 16. [保存] ボタンをクリックします。
- **17. 設定項目の「PPP 情報」をクリックします**。 「PPP 情報」が表示されます。

- MP接続 →する
 認証方式 → PAP、CHAP
 送信認証情報
 認証パスワード → honten

 受諾認証情報
 認証ID → hontenpasswd

 受諾認証情報
 認証ID → shiten
 認証パスワード → shitenpasswd
- BAP/BACP利用



→しない

- 19. [保存] ボタンをクリックします。
- **20. 画面上部の「ネットワーク情報(honten)」をクリックします**。 「ネットワーク情報(honten)」ページが表示されます。
- **21. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先種別		→専用線接続 →論理リンクにバンドルする
使用インタ	フェース	→WAN1
バンドル先		→honten-1 (0)



23. [追加] ボタンをクリックします。

専用線接続(バンドル)の設定項目と「基本情報」が表示されます。

24. [保存] ボタンをクリックします。

PPP 関連を設定する

- **25. 画面上部の「ネットワーク情報(honten)」をクリックします**。 「ネットワーク情報(honten)」ページが表示されます。
- 26.
 「PPP 関連」をクリックします。

 PPP 関連の設定項目と「圧縮情報」が表示されます。
- **27. 「MP 情報」をクリックします**。 「MP 情報」が表示されます。
- 28. 以下の項目を指定します。
 - 受信パケット順序制御 → する

受信バケット順序制御 ○しない ⊙する

- 29. [保存] ボタンをクリックします。
- 30. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

専用線だけで論理リンクを構成した場合、少なくとも1つの専用線で接続が可能であれば通信が維持されます。

- セッション監視機能は、論理リンクに対して機能します。マスタ回線で通信できない場合は、論理リンク内の通信可能な回線を探し、監視を継続します。
- 自動復旧モードは、論理リンクに対して機能します。自動復旧しない設定の場合でも、論理リンク内の少なくとも1 つの回線が接続中であれば通信を維持します。
- ・ 論理リンクを構成した場合、対向する装置間で正しく認証情報を設定するか、認証をoffに設定してください。

2.10.3 専用線と ISDN 回線でマルチリンク機能を使う

適用機種 Si-R370,570

こんな事に気をつけて

専用線とISDNによって単一の論理リンクを構成することができます。この場合、ISDNでのマルチリンク機能と同様、回線使用率により動的に接続チャネル数を増減することができます。

論理リンクを構成する場合、主に使用する回線として専用線を設定します。これをマスタ回線と呼びます。 ISDNは補助回線として設定します。これをバンドル回線と呼びます。

論理リンクの接続情報は、ISDNの接続情報を含めマスタ回線定義にすべて設定します。

速度の異なる回線を論理回線として結合した場合、期待する速度が出ない場合があります。

● 参照 Si-Rシリーズ機能説明書「2.9 マルチリンク機能」(P.50)

ここでは、論理リンクを介して2つの事業所(本店、支店)のネットワークを接続する場合について説明します。



● 設定条件

- マスタ回線として、スロット0に実装された BRI 拡張モジュール L2 で専用線(128Kbps)を使用する
- バンドル回線として、スロット1に実装されたBRI拡張モジュールL2でISDN回線を使用する
- 最大リンク数は3チャネル
- ISDN 回線はマルチリンク機能を使用する
- 回線使用率90%以上が10秒以上続いたら、チャネルを増加する
- 回線使用率40%以下が60秒以上続いたら、チャネルを減少する
- 無通信監視時間をしない

[本店]

•	接続ネットワーク名	: honten
•	接続先名	: honten-1
•	本装置のIPアドレス/ネットマスク	: 192.168.1.1/24
•	電話番号	: 03-7777-7777

- ユーザ認証 ID とユーザ認証パスワード 発信 : honten, hontenpass 着信 : shiten, shitenpass [支店] 接続ネットワーク名 : shiten 接続先名 : shiten-1 • 本装置のIPアドレス/ネットマスク : 192.168.2.1/24 電話番号 : 044-999-9999 ユーザ認証 ID とユーザ認証パスワード 発信 : shiten, shitenpass
 - honten, hontenpass

上記の設定条件に従って本店の論理リンクの設定例を示します。

回線情報を設定する

着信

スロット 0-0: WAN0、専用線 スロット 1-0: WAN1、ISDN として以下の手順で設定します。

1. 設定メニューのルータ設定で「WAN 情報」をクリックします。 「WAN 情報」ページが表示されます。

2. 以下の項目を指定します。

• 回線インタフェース →専用線

<wan情報追加フィールドン< th=""></wan情報追加フィールドン<>	
回線インタフェース	専用線 🖌

3. [追加] ボタンをクリックします。

「WAN0 情報(専用線)」ページが表示されます。

4. 「基本情報」をクリックします。

「基本情報」が表示されます。

5. 以下の項目を指定します。

- ポート →スロット0-0
- 回線速度 → 128kbps
- フラグ監視 →無効にする

■基本情報	3
ボート	지미ット 0-0 💌
回線速度	128Kbps 💌
フラグ監視	●無効にする ○有効にする

- 6. [保存] ボタンをクリックします。
- 7. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

回線インタフェース → ISDN

<wan情報追加t< th=""><th>フィールド></th><th></th></wan情報追加t<>	フィールド>	
回線インタフェース	ISDN	~

9. [追加] ボタンをクリックします。

「WAN1 情報(ISDN)」ページが表示されます。

10. 「基本情報」をクリックします。

「基本情報」が表示されます。

11. 以下の項目を指定します。

- ポート →スロット1-0
 自局番号チェック →する
- f チェックする番号1 → 03-7777-7777

■基本情報		
ボート	지미ット 1-0 💌	
自動接続	○すべて禁止 ⊙相手毎に設定	
着信動作	○すべて禁止 ⊙相手毎に設定	
自局番号チェ ック	 ● しばい ● する チェックする番 電話番号を指定 ♥ 03-7777-7777 号1 チェックする番 電話番号を指定 ♥ サブアドレス チェックする番 (電話番号を指定 ♥) サブアドレス ダローバル者 信 ● 利用しない ●利用する 	

12. [保存] ボタンをクリックします。

相手情報を設定する

- **13. 設定メニューのルータ情報で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **14. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 15. 以下の項目を指定します。
 - ネットワーク名 → honten

<ネットワーク情報	暖追加フィールド>
ネットワーク名	honten

16. [追加]ボタンをクリックします。

「ネットワーク情報(honten)」ページが表示されます。

17. 「接続先情報」をクリックします。 「接続先情報」が表示されます。

- →専用線接続 • 接続先種別 ○ ATM接続 VCI ⊙ 専用線接続 ⊙ 通常接続 使用インタフェース WAN1 V ○ 論理リンクにバンドルする 使用インタフェース WAN1 🗸 バンドル先 ap0-2 (2) 🗸 ◯ ISDN接続 ⊙ 通常接続 使用インタフェース すべて 🗸 接続先種別 電話番号 ダイヤル1 サブアドレス ○ 論理リンクにバンドルする 使用インタフェース すべて 💙 バンドル先 ap0-2 (2) 🗸 ○ フレームリレー接続 DLCI ○ PPP₀E接続 ○ IPトンネル接続 ○ IPsec/IKE接続 ○ 別インタフェースから送出 ○ MPLSトンネル接続 ○ バケット破棄
- 19. [追加]ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

- 接続先名 → honten-1
- 使用インタフェース → WAN0
- ダイヤル1
 電話番号 →044-999-9999

■基本情報		3	
接続先名		honten-1	
使用インタフェ	ース	WANO 💌	
DNSサーバ			
▲ ISDN回線を含む論理リンクを構成する場合、以下の情報を設定してください。			≛ເາ。
ダイセル 1	電話番号	044-999-9999	
	サブアドレス	ζ	

- 21. [保存] ボタンをクリックします。
- **22. 設定項目の「PPP 情報」をクリックします**。 「PPP 情報」が表示されます。

•	MP接続	→する
•	認証方式	→ PAP、CHAP
•	送信認証情報 認証 ID 認証パスワード	→honten →hontenpasswd
•	受諾認証情報 認証 ID 認証パスワード	→ shiten → shitenpasswd
•	BAP/BACP利用	→する

■PPP情報 [2]			3
▲ 論理リンクを構成する場合、MP接続の設定>は必ず"する"を選択して 下さい。			
MP接続	⊙しない	⊙する	
→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→→			
認証方式)	
`¥∕≕≡ग≑∓∔≢≭₽	認証ID	honten	
达信器证件牧	認証バスワード	•••••	
产品会社会和会计本主主题	認証ID	shiten	
文祐認進相報	認証バスワード	•••••	
BAP/BACP利用 Oしない @する			

- 24. [保存] ボタンをクリックします。
- **25. 画面上部の「ネットワーク情報 (honten)」をクリックします**。 「ネットワーク情報 (honten)」ページが表示されます。
- **26. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

٠	接続先種別	→ISDN 接続
		→論理リンクにバンドルする
	使用インタフェース	→WAN1
	バンドル先	→honten-1 (0)



28. [追加] ボタンをクリックします。

ISDN 接続(バンドル)の設定項目と「基本情報」が表示されます。

29. [保存] ボタンをクリックします。

PPP 関連を設定する

- **30. 画面上部の「ネットワーク情報(honten)」をクリックします**。 「ネットワーク情報(honten)」ページが表示されます。
- **31.** 「PPP 関連」をクリックします。 PPP 関連の設定項目と「圧縮情報」が表示されます。
- **32. 「MP情報」をクリックします**。 「MP情報」が表示されます。

MP回線初回リンク数 →1

•	MP回線最大リンク数	→ 3
•	トラフィックによる増減 回線増加条件	→する
	回線使用率	→90
	猶予時間	→ 10
	回線削減条件	
	回線使用率	→40
	猶予時間	→60
•	受信パケット順序制御	→する

■MP情報	
いの自然が同じて力数	1

MP回線初回リンク数	1
MP回線最大リンク数	3
最小分割長	
トラフィックによる増減	 ● しない ● する ● 同線使用率 猶予時間 ● 回線増加条件 90 % 10 秒 ● 回線削減条件 40 % 60 秒
受信バケット順序制御	●しない ●する

34. [保存] ボタンをクリックします。

35. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

専用線の通信障害を検出した場合、ISDN接続だけでも論理リンクの維持を試みます。ISDN接続だけで、論理リンクを 維持する場合は、以下の点に注意してください。

3

- ・ 常時接続が有効の場合は、即時 ISDN 接続を行います。
- 常時接続が無効の場合は、発信契機により ISDN 接続を行います。 ただし、ほかの設定によっては無通信時に ISDN は切断されます。
- セッション監視が有効な場合、発信契機がセッション監視パケットだけの期間は、接続・切断が繰り返されることが あります。このような場合は、常時接続設定を有効にしてください。
- 対向する両装置で着番認証を無効に設定すると、ISDN 接続ができないことがあります。着番認証を無効にする場合 は、相手局の認証を無効に設定してください。
- 専用線とISDN 接続での論理リンク構成時に、専用線が通信障害などで使用できない場合、ISDN 接続が切断されない ことがあります。専用線とISDN 接続での論理リンク構成時には、必ず回線使用率によるチャネル制御を設定してく ださい。

2.11 マルチキャスト機能を使う

適用機種 全機種

本装置には、マルチキャスト機能を動作させるために以下の2種類のプロトコルがあります。

- PIM-DMプロトコル
- PIM-SM プロトコル

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

● 参照 Si-Rシリーズ 機能説明書「2.10 マルチキャスト機能」(P.52)

2.11.1 マルチキャスト機能 (PIM-DM)を使う

適用機種 全機種

マルチキャスト機能(PIM-DM)を使用すると、会社などのLAN内で、動画や音声などを配送することができます。

こんな事に気をつけて

- マルチキャストでパケットを配送するルータは、すべて PIM-DM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- IPアドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側IPアドレスと相手側IPアドレスの両方を正しく設定する必要があります。



ここでは、PIM-DMを利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。 本装置1、本装置2、本装置3が以下のとおり設定されていることを前提とします。

● 前提条件

 VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける VLAN ID:2 ネットワークアドレス: 192.168.2.0/24
 VLAN ID:3 ネットワークアドレス: 192.168.3.0/24

[本装置1]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1のIPアドレス : 192.168.1.1/24
- LAN2のIPアドレス : 192.168.2.1/24
- LAN3のIPアドレス : 192.168.3.1/24

[本装置2]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1のIPアドレス : 192.168.4.1/24
- LAN2のIPアドレス : 192.168.2.2/24

[本装置3]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN1のIPアドレス : 192.168.5.1/24
- LAN2のIPアドレス : 192.168.3.2/24

● 設定条件

• マルチキャスト・ルーティングプロトコルには PIM-DM を利用する

[本装置1]

マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2、LAN3を使用する

[本装置2]

• マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する

[本装置3]

• マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。
本装置1を設定する

LAN1情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。
 「LAN1 情報(物理LAN)」ページが表示されます。Si-R180、180B でスイッチポートを利用している場合は、 「LAN1 情報(VLAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「マルチキャスト情報」をクリックします。 「マルチキャスト情報」が表示されます。
- 5. 以下の項目を指定します。
 - マルチキャスト機能 → PIM-DM

■マルチキャスト情報 マルチキャスト機能 ○使用しない Ostatic ⊙PIM-DM ○PIM-SM

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を指定します。

「LAN2情報(VLAN)」

マルチキャスト機能 → PIM-DM

「LAN3情報 (VLAN)」

- マルチキャスト機能 → PIM-DM
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

LAN1情報を設定する

「LAN1情報」-「IP関連」

「マルチキャスト情報」

マルチキャスト機能 → PIM-DM

LAN2情報を設定する

「LAN2情報」-「IP関連」 「マルチキャスト情報」

マルチキャスト機能 → PIM-DM

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。

LAN1情報を設定する

「LAN1情報」-「IP関連」	
「マルチキャスト情報」	

マルチキャスト機能 → PIM-DM

LAN2情報を設定する

「LAN2情報」-「IP 関連」

「マルチキャスト情報」

マルチキャスト機能 → PIM-DM

2.11.2 マルチキャスト機能 (PIM-SM)を使う

適用機種 全機種

マルチキャスト機能(PIM-SM)を使用すると、インターネットなど、十分な帯域を保証されないネットワーク 上で、マルチキャスト・パケットを配送することができます。

こんな事に気をつけて

- マルチキャスト・パケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- IPアドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側IPアドレスと相手側IPアドレスの両方を正しく設定する必要があります。
- ネットワーク内にBSR(Bootstrap Router:ブートストラップルータ)として動作するルータを1台以上置く必要が あります。BSRはRP(Rendezvous Point:ランデブーポイント)の情報を広報します。
- ネットワーク内に RP として動作するルータを1台以上置く必要があります。パケットの配送は、RP を配送樹の頂点として開始され、その後、最短経路(SPT: Shortest Path Tree)に切り替わります。
- PIM-SMではマルチキャスト・パケットの配送を RP を配送樹の頂点として開始するため、RP はネットワークの中心 付近に置くことをお勧めします。
- SPTへの切り替えは、マルチキャスト・パケットの受信者の直前のルータ(lasthop router)が行います。lasthop router で設定することで SPT への切り替えを無効にすることができます。



ここでは、PIM-SM を利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

この設定例では、VLANを利用して、上図のネットワークを仮想的に構築します。

マルチキャスト・パケットは、はじめは RPである本装置2を経由して、本装置1→本装置2→本装置3→本装置 4の順に配送されます(一度、本装置1から本装置2に送られ、本装置2を配送樹の頂点として配送されます)。 本装置4へのパケット転送開始直後に、本装置4はSPTへの切り替えを開始します。切り替えが行われると、本 装置1→本装置3→本装置4のように、最短経路を利用して配送されます(本装置1を配送樹の頂点として配送 されます)。同様の切り替えが本装置5でも行われます。

ここでは、本装置1、本装置2、本装置3、本装置4、本装置5が以下のとおりに設定されていることを前提とします。

● 前提条件

- VLAN ID とネットワークアドレスを以下のように対応付ける
 - VLAN ID:2 ネットワークアドレス:192.168.2.0/24
 - VLAN ID:3 ネットワークアドレス:192.168.3.0/24
 - VLAN ID:11 ネットワークアドレス:192.168.11.0/24
 - VLAN ID: 12 ネットワークアドレス: 192.168.12.0/24
 - VLAN ID: 13 ネットワークアドレス: 192.168.13.0/24
- ユニキャストのルーティングテーブルの作成に RIP を使用する

[本装置1]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス : 192.168.10.1/24
- LAN2のIPアドレス : 192.168.11.1/24
- LAN3のIPアドレス : 192.168.12.1/24

[本装置2]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN1、LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス : 192.168.12.2/24
- LAN2のIPアドレス : 192.168.13.1/24

[本装置3]

- LAN0、LAN1はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN4、LAN5はVLANとし、出力先の物理インタフェースはLAN1とする
- LAN2のIPアドレス : 192.168.11.2/24
- LAN3のIPアドレス : 192.168.13.2/24
- LAN4のIPアドレス : 192.168.2.1/24
- LAN5のIPアドレス : 192.168.3.1/24

[本装置4]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス : 192.168.4.1/24
- LAN2のIPアドレス : 192.168.2.2/24

[本装置5]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス : 192.168.5.1/24
- LAN2のIPアドレス : 192.168.3.2/24

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-SM を利用する
- RP、BSRは本装置2が行う
- SPTへの切り替えを行う(初期値)

[本装置1]

• マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2、LAN3を使用する

[本装置2]

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する
- RP : 192.168.12.2
- BSR : 192.168.12.2

[本装置3]

• マルチキャスト・パケットを転送するインタフェースとしてLAN2~5を使用する

[本装置4]

• マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する

[本装置5]

• マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 2. 「LAN 情報」でインタフェースがLAN1の[修正]ボタンをクリックします。

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

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- **4.** IP 関連の設定項目の「マルチキャスト情報」をクリックします。 「マルチキャスト情報」が表示されます。
- 5. 以下の項目を指定します。
 - マルチキャスト機能 → PIM-SM

■マルチキャスト情報		Ş
マルチキャスト機能	○使用しない ○static ○PIM-DM ⊙PIM-SM	

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を指定します。

「LAN2情報 (VLAN)」

マルチキャスト機能 → PIM-SM

「LAN3情報 (VLAN)」

- マルチキャスト機能 → PIM-SM
- 8. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

1. 「本装置1を設定する」を参考に、以下の項目を指定します。

「LAN1情報 (VLAN)」

マルチキャスト機能 → PIM-SM

「LAN2情報 (VLAN)」

- マルチキャスト機能 → PIM-SM
- 設定メニューのルータ設定で「マルチキャスト情報」をクリックします。
 「マルチキャスト情報」ページが表示されます。
- **3.** 「IPマルチキャスト情報」をクリックします。 「IPマルチキャスト情報」が表示されます。

4. 以下の項目を指定します。

PIM-SM
 RP候補 →する
 IPアドレス → 192.168.12.2
 BSR候補 →する
 IPアドレス → 192.168.12.2

■IPマル	■IPマルチキャスト情報		
	RP候補	 ○ しばい ● する IPアドレス 192.168.12.2 ブライオリティ 0 	
PIM-2M	BSR候補	 ○ しばい ● する IPアドレス 192.168.12.2 ブライオリティ 0 	

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。

「LAN2 (VLAN) 情報」-「IP 関連」 「マルチキャスト情報」 マルチキャスト機能 → PIM-SM 「LAN3 (VLAN) 情報」-「IP 関連」 「マルチキャスト情報」 マルチキャスト機能 → PIM-SM 「LAN4 (VLAN) 情報」-「IP 関連」 「マルチキャスト情報」 マルチキャスト機能 → PIM-SM 「LAN5 (VLAN) 情報」-「IP 関連」 「マルチキャスト情報」 マルチキャスト機能 → PIM-SM

本装置4を設定する

「本装置1を設定する」を参考に、本装置4を設定します。

「LAN1 (VLAN) 情報」-「IP 関連」
 「マルチキャスト情報」
 ● マルチキャスト機能 → PIM-SM
 「LAN2 (VLAN) 情報」-「IP 関連」

「マルチキャスト情報」

マルチキャスト機能 → PIM-SM

本装置5を設定する

「本装置1を設定する」を参考に、本装置5を設定します。

「LAN1 (VLAN) 情報」-「IP 関連」 「マルチキャスト情報」 ● マルチキャスト機能 → PIM-SM

「LAN2(VLAN)情報」-「IP 関連」 「マルチキャスト情報」

マルチキャスト機能 → PIM-SM

2.11.3 マルチキャスト機能(スタティックルーティング)を使う

適用機種 全機種

マルチキャスト機能(スタティックルーティング)を使用すると、マルチキャストパケットが配送される経路を 静的に設定することができます。

こんな事に気をつけて

マルチキャスト・スタティックルーティングでは、入力インタフェースでのIGMP グループ参加を指定することができます。

上流側に PIM-DM などの IGMP 参加要求を受け付けるマルチキャスト・ルータが存在する場合は、入力インタフェース で IGMP グループ参加を行うことで、パケットを強制的に転送させることができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。 本装置1、本装置2、本装置3が以下のとおり設定されていることを前提とします。

● 前提条件

- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける
 - VLAN ID:2 ネットワークアドレス:192.168.2.0/24
- VLAN ID:3 ネットワークアドレス:192.168.3.0/24

[本装置1]

- LANO は VLAN の出力先としてだけ使用し、通常の LAN としては使用しない
- LAN2、LAN3 は VLAN とし、出力先の物理インタフェースは LAN0 とする
- LAN1のIPアドレス : 192.168.1.1/24
- LAN2のIPアドレス : 192.168.2.1/24
- LAN3のIPアドレス : 192.168.3.1/24

[本装置2]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス : 192.168.4.2/24
- LAN2のIPアドレス : 192.168.2.1/24

[本装置3]

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN4、LAN5はVLANとし、出力先の物理インタフェースはLAN1とする
- LAN1のIPアドレス : 192.168.5.2/24
- LAN2のIPアドレス : 192.168.3.2/24

● 設定条件

- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする
- 入力インタフェースでのIGMP グループ参加は行わない

[本装置1]

• マルチキャストパケットを転送するインタフェースとして LAN1、LAN2、LAN3 を使用する

[本装置2]

• マルチキャストパケットを転送するインタフェースとしてLAN1、LAN2を使用する

[本装置3]

• マルチキャストパケットを転送するインタフェースとしてLAN1、LAN2を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

1. 設定メニューのルータ設定で「LAN情報」をクリックします。 「LAN情報」ページが表示されます。

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

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

- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP 関連の設定項目の「マルチキャスト情報」をクリックします。 「マルチキャスト情報」が表示されます。

5. 以下の項目を指定します。

• マルチキャスト機能 → static

■マルチキャスト情報 マルチキャスト機能 ○使用しない ⊙ static ○ PIM-DM ○ PIM-SM

- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考に、以下の項目を指定します。

「LAN2情報(VLAN)」

マルチキャスト機能 → static

「LAN3情報 (VLAN)」

- マルチキャスト機能 → static
- **8. 設定メニューのルータ設定で「マルチキャスト情報」をクリックします**。 「マルチキャスト情報」ページが表示されます。

9. 「IP マルチキャストスタティック経路情報」をクリックします。

「IPマルチキャストスタティック経路情報」ページが表示されます。

10. 以下の項目を指定します。

- 配送元ホストアドレス → 192.168.1.2
- マルチキャストグループアドレス → 239.255.1.1
- 入力インタフェース → LAN1
- ・ 出力インタフェース → lan2-lan3
- グループ参加 → しない

<ipマルチキャストスタティック経路情報入力フィールド></ipマルチキャストスタティック経路情報入力フィールド>	
配送元ホストアドレス	192.168.1.2
マルチキャストグループアドレス	239.255.1.1
入力インタフェース	LAN1 💌
出力インタフェース	lan2-lan3
グループ参加	⊙しない ○する

- 11. [追加] ボタンをクリックします。
- **12. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。 「LAN1情報」-「IP 関連」 「マルチキャスト情報」 マルチキャスト機能 → static 「LAN2情報」-「IP 関連」 「マルチキャスト情報」 マルチキャスト機能 → static 「マルチキャスト情報」-「IPマルチキャストスタティック経路情報」 配送元ホストアドレス → 192.168.1.2 配送元ホストアドレス → 192.168.1.2 配送元ホストアドレス → 192.168.1.2

- 配送元ホストアドレス → 192.168.1.2
- グループ参加 → しない

本装置3を設定する

「本装置1を設定する」を参考に、本装置3を設定します。

「LAN1情報」-「IP関連」

「マルチキャスト情報」

- マルチキャスト機能 → static
- 「LAN2情報」-「IP関連」

「マルチキャスト情報」

マルチキャスト機能 → static

「マルチキャスト情報」-「IPマルチキャストスタティック経路情報」

- 配送元ホストアドレス → 192.168.1.2
- マルチキャストグループアドレス → 192.168.1.1
- 入力インタフェース → LAN2
- 出力インタフェース → lan1
- グループ参加 → しない

2.12 VLAN 機能を使う

適用機種 全機種

ここでは、VLAN機能を利用して、1つの物理ポートで3つのネットワークを組む場合を例に説明します。



● 参照 Si-Rシリーズ 機能説明書「2.11 VLAN機能」(P.55)

● 設定条件

- LAN0 ポートを使用する
- VLAN IDとして2、3、4を使用する
- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける
 - VLAN ID:2 ネットワークアドレス:192.168.20.0/24
 - VLAN ID:3 ネットワークアドレス:192.168.30.0/24
 - VLAN ID:4 ネットワークアドレス:192.168.40.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - インタフェース → VLAN
 <LAN情報追加フィールド>
 インタフェース VLAN ▼
- 3. [追加] ボタンをクリックします。

「LAN1 情報(VLAN)」ページが表示されます。

「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。

5. 以下の項目を指定します。

- 出力先 → LAN0
- VLAN ID →2
- プライオリティ →0

■基本情報	3
出力先	LANO 🗸
VLAN ID	2
ブライオリティ	0

6. [保存] ボタンをクリックします。

7. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

8. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 192.168.20.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

IPアドレス情報		
IPv4	⊙使用する○使用しない	
	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス I92.168.20.1 	
IPアドレス	ネットマスク 24 (255.255.255.0) ▼ ブロートドキャストアドレ ス ネットワークアドレス+オール1 ▼	

9. [保存] ボタンをクリックします。

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

|RIP1||報」が衣小されます。

11. 以下の項目を指定します。

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

■RIP情報	[*	3
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ○V2(Multicast)で送信する 	
RIP受信	 ○受信しない ○ V1で受信する ○ V2、V2(Multicast)で受信する 	
《 RIP 送信時は加算するメトリック値を設定してください。》 <mark>メトリック値</mark>		

12. [保存] ボタンをクリックします。

13. 手順1.~12.を参考に、以下の項目を指定します。

[192.168.30.0/24のネットワーク]

•	インタフェース情報	→ VLAN
	出力先	→lan0
	VLAN ID	→ 3
	プライオリティ	→ 0
•	IPアドレス	→指定する
	IPアドレス	→ 192.168.30.1
	ネットマスク	→24 (255.255.255.0)
	ブロードキャストアドレス	→ネットワークアドレス+オール1
•	RIP送信	→V1 で送信する

- RIP受信 → V1 で受信する
- メトリック値 →0

14. 手順1.~12.を参考に、以下の項目を指定します。

[192.168.40.0/24のネットワーク]

•	インタフェース情報	→ VLAN
	出力先	→lan0
	VLAN ID	→ 4
	プライオリティ	→ 0
•	IPアドレス	→指定する
	IPアドレス	→ 192.168.40.1
	ネットマスク	→24 (255.255.255.0)
	ブロードキャストアドレス	→ネットワークアドレス+オール1
•	RIP送信	→V1 で送信する
•	RIP受信	→V1 で受信する
•	メトリック値	→0

15. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- VLAN 機能を利用すると、Ethernet フレームに4バイトのVLAN タグが付加され、最大1522バイトのEthernet フレームが送出されることになります。通常のEthernet フレームの最大サイズは1518バイトです。そのため、その状態では1522バイトのフレームに対応していない機器とは接続することはできません。1522バイトのフレームに対応していない機器とは接続することはできません。1522バイトのフレームに対応していない機器とは接続することはできません。1522バイトのフレームに対応
- ・ VLANの物理インタフェースに、VLANインタフェースを使用することはできません。
- 同じ物理インタフェースを使用する複数の VLAN インタフェース上で、重複する VLAN ID を使用することはできません。
- VLAN対応スイッチングHUBやルータ製品の中には、VLANが設定されていないLANポートで、VLANタグ付きフレームを受信してしまう装置があります。
 このような装置と接続する際には、スイッチングHUB(またはルータ)の設定を「VLANあり」から「VLANなし」に設定を変更してください。
 また、フレームを送信するPCのarpエントリが本装置に残っていると、arpエントリの生存時間中だけ通信するという現象が発生する場合があります。これを防ぐために、設定後に本装置の[設定反映] ボタンをクリックしてください。

- VLANを利用する物理LANインタフェースの情報として、以下の手順で「ポート番号」と「転送レート」を必ず設定してください。「LAN情報(物理LAN)」を設定しない場合、VLANを利用するLAN情報は設定できません。以下に手順を示します。
 - 1.設定メニューのルータ設定で「LAN 情報」をクリックします。
- 2.インタフェースに"物理インタフェース"を指定して、[追加] ボタンをクリックします。
- 3.「共通情報」-「基本情報」で、ポート番号と転送レートを選択して、[保存] ボタンをクリックします。
- ・ VLAN インタフェースを追加する場合は、先に物理 LAN インタフェースを設定してください。

2.13 IP フィルタリング機能を使う

適用機種 全機種

● 参照 Si-Rシリーズ 機能説明書「2.12 IPフィルタリング機能」(P.56)

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。



IP フィルタリングの条件

本装置では、以下の条件を指定することによって、データの流れを制御できます。

- 動作
- プロトコル
- 送信元情報(IPアドレス/アドレスマスク/ポート番号)
- あて先情報(IPアドレス/アドレスマスク/ポート番号)
- TCP 接続要求
- TOS 値
- 方向

· ☆ ヒント —

◆ TCP 接続要求とは

TCPプロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうか指定するものです。 フィルタリングの動作に透過、プロトコルにTCPを指定した場合に有効です。TCPプロトコルはコネクショ ン型であるため、コネクション確立要求を発行し、それに対する応答を受信することによって、コネクション を開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断 し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

次に、TCPパケットとフラグ設定について説明します。TCPパケット内にはSYNフラグとACKフラグの2つの制御フラグがあります。このフラグの組み合わせによって、TCPパケットの内容が分かります。以下に、対応表を示します。

制御フラグ		TCDパケットの内容
SYN	ACK	TCP// 9 POMA
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

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

☆ヒント゠

◆ アドレス変換(NAT)機能利用時の IP フィルタリングのかかるタイミング

内部LANから外部LANに向かう場合は、アドレス変換でアドレスが変更される前にIPフィルタリング処理を 通過します。また、外部LANから内部LANに向かう場合は、アドレス変換でアドレスが変更されたあとで、 IPフィルタリング処理を通過します。つまり、IPフィルタリングは「プライベートアドレス」を対象に行い ます。

本装置のIPフィルタリングとアドレス変換の位置付けは以下のとおりです。



IP フィルタリングの設計方針

IPフィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる。
- B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する。

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけ許可して SPIを併用する
- 外部の特定サービスへのアクセスだけを許可する (IPv6 フィルタリング)

また、設計方針 Bの例として、以下の設定例について説明します。

- 外部の特定サーバへのアクセスだけを禁止する
- 利用者が意図しない発信を防ぐ
- 回線が接続しているときだけ許可する

補足

TCP接続要求の設定は、プロトコルにTCPまたはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

こんな事に気をつけて

- IP フィルタリングでWWW(ポート番号80)でのアクセスを制限する設定を行った場合、外部のWWWブラウザから設定ができなくなる場合があります。
- IP フィルタリングでDHCP(ポート番号67、68)でのアクセスを制限する設定を行った場合、DHCP機能が使用できなくなる場合があります。
- IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用 されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。 PPPoE の場合は、remote 側にフィルタをかけるようにしてください。
- ・ IP フィルタリングの方向に「reverse」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象に なります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
 - 送信元IPアドレス/アドレスマスクとあて先IPアドレス/アドレスマスク
 - 送信元ポート番号とあて先ポート番号

2.13.1 外部の特定サービスへのアクセスだけ許可する

適用機種 全機種

LAN定義の場合

ここでは、一時的にLANを作成し、外部LANのすべてのFTPサーバに対してアクセスすることだけを許可し、 ほかのサーバ(WWWサーバなど)へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ 名を解決するために、DNSサーバへのアクセスは許可します。

補足

 ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要 があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定した場合も DNSサーバへの発信が発生します。あらかじめ接続するFTPサーバが決まっている場合は、本装置のDNSサーバ機 能を利用することによって、DNSサーバへの発信を抑止することができます。

•本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



● フィルタリング設計

- 内部 LAN のホスト(192.168.1.0/24)から外部 LAN の FTP サーバへのアクセスを許可
- 内部LANのホスト(192.168.1.0/24)から外部LANへのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- 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

```
捕足 このルールでは、ftp passive モードによるデータ転送はできません。
```

上記のフィルタリングルールの設定を行う場合の設定例を示します。

任意のFTPサーバのポート21へのTCPパケットを透過させる(内部LAN→外部LAN)

→ ACL0

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名



3. [追加] ボタンをクリックします。 「ACL定義情報(ACL0)|ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

- プロトコル → tcp
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.2)
- あて先情報
 IPアドレス →指定しない
 アドレスマスク →指定しない
 公式
 ①
 ④
 ①
 ①
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ③
 ④
 ⑤
 ③
 ⑤
 ⑤
 ⑤
 ○
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 ⑦
 10
 11
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
 12
- ■IP定義情報 3 tep ブロトコル (番号指定: "その他"を選択時のみ有効です 送信元情 IPアドレス
 192.168.1.0 アドレスマ 報 24 (255.255.255.0) ¥ スク IPアドレス あて先情 アドレスマ 報 0 (0.0.0.0) ~ スク 指定なし 💊 TOS、または、DSCPを選択時に値を入力してくだ QoS さい
- 6. [保存] ボタンをクリックします。

7. 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

- 8. 以下の項目を指定します。
 - 送信元ポート番号 →指定しない
 - あて先ポート番号 →21 (ftpのポート番号)
 - TCP接続要求 →対象

■TCP定義情報	3
送信元ポート番号	
あて先ボート番号	21
TCP接続要求	⊙対象○対象外

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「LAN情報」をクリックします**。 「LAN情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **12.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- **13.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。
- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>	
動作	◎透過○遮断
方向	入出力 💌
ACL定義番号	0 参照

15. [追加] ボタンをクリックします。

FTP サーバからの応答パケットを透過させる(外部 LAN → 内部 LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」	
• 定義名	→ACL1
「ACL定義情報(ACL1)」-「IP定	2義情報」
• プロトコル	→tcp
 送信元情報 IPアドレス アドレスマスク 	→指定しない →指定しない
 あて先情報 IPアドレス アドレスマスク 	→ 192.168.1.0 → 24 (255.255.255.0)
• QoS	→指定なし
「ACL定義情報(ACL1)」-「TCF	っ定義情報」
• 送信元ポート番号	→21(ftpのポート番号)
• あて先ポート番号	→指定しない
● TCP 接続要求	→対象外
「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」	
• 動作	→透過
• 方向	→入出力

• ACL定義番号 → 1

DNS サーバのポート 53 への UDP パケットを透過させる(内部 LAN → 外部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL2
ΓA	CL定義情報(ACL2)」-「IP定義	情報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.0.10 → 32 (255.255.255.255)
•	QoS	→指定なし

18. 「UDP定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
 - あて先ポート番号 → 53 (domainのポート番号)

■UDP定義情報		3
送信元ポート番号		
あて先ポート番号	53	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(外部 LAN → 内部 LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL3
ΓA	CL定義情報(ACL3)」-「IP定義	情報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.0.10 → 32 (255.255.255.255)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	QoS	→指定なし

23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報(ACL3)」-「UDP定義情報」

- ・ 送信元ポート番号 →53 (domainのポート番号)
- あて先ポート番号 →指定しない

24. 手順10.~15.を参考に、以下の項目を指定します。

「LAN情報」-「IP関連」	
「IP フィルタリング情報」	

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →3

ICMP のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

 ● 定義名 	→ACL4
「ACL定義情報(ACL4)」-「IP定義	鳧情報」
• プロトコル	→icmp
 送信元情報 IPアドレス アドレスマスク 	→指定しない →指定しない
 あて先情報 IPアドレス アドレスマスク 	→指定しない →指定しない

• QoS →指定なし

26. 「ICMP定義情報」をクリックします。

「ICMP定義情報」ページが表示されます。

27. 以下の項目を指定します。

•	ICMP	
	タイプ	→指定しない
	コード	→指定しない

	定義情報	R 🕄
	タイブ	
ICMP	コード	

- 28. [保存] ボタンをクリックします。
- 29. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →4

残りのパケットをすべて遮断する

30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ ACL5

「ACL定義情報(ACL5)」-「IP 定義情報」

• プロトコル	→すべて
 送信元情報 IPアドレス アドレスマスク 	→指定しない →指定しない
 あて先情報 IPアドレス アドレスマスク 	→指定しない →指定しない

- QoS →指定なし
- 31. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →5
- **32. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

リモート定義の場合

ここでは、LAN上のパソコンからインターネット上のすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ(WWWサーバなど)へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するために、DNSサーバへのアクセスは許可します。

- ・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の設定を行う場合の設定例を示します。

任意のFTP サーバのポート21へのTCPパケットを透過させる(LAN→インターネット)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - ・ 定義名 → ACL0
 <ACL情報追加フィールド>
 定義名 ACL0
- 3. [追加] ボタンをクリックします。

「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

- プロトコル → tcp
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス →指定しない
 アドレスマスク →指定しない
- QoS →指定なし

■IP定義情報		
プロトコル		tcp ▼ (番号指定: ^{"そ} の他"を選択時のみ有効です)
送信元情	IPアドレス	192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	
報	アトレスマ スク	0 (0.0.0.0)
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

補足 このルールでは ftp passive モードによるデータ転送はできません。

8. 以下の項目を指定します。

- ・ 送信元ポート番号 →指定しない
- あて先ポート番号 →21 (ftpのポート番号)
- TCP 接続要求 →対象

■TCP定義情報		?
送信元ポート番号		
あて先ボート番号	21	
TCP接続要求	●対象○対象外	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします。** 「相手情報」ページが表示されます。
- **11. フィルタリングを行うネットワーク情報の [修正] ボタンをクリックします**。 「ネットワーク情報」が表示されます。
- **12. 「IP 関連」をクリックします**。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<if< th=""><th>フィルタリング情報入力フィールド></th></if<>	フィルタリング情報入力フィールド>
動作	●透過 ○透過(接続中のみ) ○遮断
方向	入出力 🔽
ACL定義番号	0 参照

15. [追加] ボタンをクリックします。

FTP サーバからの応答パケットを透過させる(インターネット→LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ ACL1

「ACL定義情報(ACL1)」-「IP定義情報」

- プロトコル → tcp
 送信元情報

 ドアドレス →指定しない

 アドレスマスク →指定しない
 あて先情報
- め C 2.164X

 IPアドレス

 → 192.168.1.0

 アドレスマスク

 → 24 (255.255.255.0)
- QoS →指定なし

「ACL定義情報(ACL1)」-「TCP定義情報」

- ・ 送信元ポート番号 →21 (ftpのポート番号)
- あて先ポート番号 →指定しない
- TCP接続要求 →対象外

「相手情報」-「IP 関連」

「IP フィルタリング情報」

動作 →透過
 方向 →入出力
 ACL定義番号 →1

DNS サーバのポート 53 への UDP パケットを透過させる(LAN → インターネット)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL2
ΓA	CL定義情報(ACL2)」-「IP定義	情報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.0.10 → 32 (255.255.255.255)
•	QoS	→指定なし

18. 「UDP 定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
 - あて先ポート番号 →53 (domainのポート番号)

■UDP定義情報		?
送信元ポート番号		
あて先ポート番号	53	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(インターネット→LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL3
ΓA	CL定義情報(ACL3)」-「IP定義	情報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.0.10 → 32 (255.255.255.255)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	QoS	→指定なし

23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報(ACL3)」-「UDP定義情報」

- ・ 送信元ポート番号 →53 (domainのポート番号)
- あて先ポート番号 →指定しない

24. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」		
「IP フィルタリング情報」		
• 動作		

- →透過
- 方向 →入出力
- ACL定義番号 →3

ICMP のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL4
ΓA	CL定義情報(ACL4)」-「IP定義	情報」
•	プロトコル	→icmp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし

26. 「ICMP定義情報」をクリックします。

「ICMP定義情報」ページが表示されます。

27. 以下の項目を指定します。

•	ICMP	
	タイプ	→指定しない
	コード	→指定しない

定義情報	R 3
タイブ	
コード	

- 28. [保存] ボタンをクリックします。
- 29. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →4

残りのパケットをすべて遮断する

30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ACL5

「ACL定義情報(ACL5)」-「IP定義情報」

•	プロトコル	→すべて
•	送信元情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない

- QoS →指定なし
- 31. 手順 10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP関連」

「IP フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →5
- **32. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.13.2 外部から特定サーバへのアクセスだけ許可する

適用機種 全機種

LAN定義の場合

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の 設定方法を説明します。ただし、FTPサーバ名を解決するために DNS サーバへのアクセスは許可します。



 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

- ICMPの通信を許可するためには (1)ICMPパケットを透過させる

その他をすべて遮断するには

(1)すべてのパケットを遮断する

補足 このルールでは、ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

内部LANのホストのポート21へのTCPパケットを透過させる(外部LAN→内部LAN)

設定メニューのルータ設定で「ACL情報」をクリックします。 1.

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名 → ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

3. [追加] ボタンをクリックします。

「ACL定義情報(ACL0)|ページが表示されます。

4. 「IP定義情報」をクリックします。

「IP定義情報」ページが表示されます。

以下の項目を指定します。 5.

- プロトコル → tcp 送信元情報 IPアドレス → 192.168.0.0 アドレスマスク →24 (255.255.255.0) あて先情報
- IPアドレス アドレスマスク • QoS
- → 192.168.1.5 → 32 (255.255.255.255) →指定なし
- ■IP定義情報 3 top ブロトコル (番号指定: ~その他~を選択時のみ有効です) 送信元情 IPアドレス
 192.168.0.0 アトレスマ 24 (255.255.255.0) 報 ¥ IPアドレス 192.168.1.5 あて先情 アトレスマ 報 32 (255.255.255.255) 🔽 スク 指定なし TOS、または、DSCPを選択時に値を入力してくだ QoS さい
- 6. [保存] ボタンをクリックします。

7. 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

- 8. 以下の項目を指定します。
 - 送信元ポート番号 →指定しない
 - あて先ポート番号 →21 (ftpのポート番号)
 - TCP接続要求 →対象

■TCP定義情報	3
送信元ポート番号	
あて先ボート番号	21
TCP接続要求	●対象○対象外

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 12. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- **13.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。
- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	⊙透過○遮断	
方向	入出力 💌	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。
内部LANのホストからの応答パケットを透過させる(内部LAN→外部LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」	
• 定義名	→ACL1
「ACL定義情報(ACL1)」-「IP5	定義情報」
• プロトコル	→tcp
 送信元情報 IPアドレス 	→ 192.168.1.5
アドレスマスク	→32 (255.255.255.255)
 あて先情報 IPアドレス アドレスマスク 	→ 192.168.0.0 → 24 (255.255.255.0)
• QoS	→指定なし
「ACL定義情報(ACL1)」-「TCI	P定義情報」
• 送信元ポート番号	→21(ftpのポート番号)
• あて先ポート番号	→指定しない
● TCP 接続要求	→対象外
「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」	
• 動作	→透過
• 方向	→入出力
• ACL定義番号	→ 1

DNS サーバのポート 53 への UDP パケットを透過させる(外部 LAN → 内部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL2
ΓA	CL定義情報(ACL2)」-「IP定義	情報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.0.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.1.10 → 32 (255.255.255.255)
•	QoS	→指定なし

18. 「UDP 定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →53 (domainのポート番号)

■UDP定義情報		?
送信元ポート番号		
あて先ポート番号	53	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(内部 LAN → 外部 LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ ACL3
ΓA	CL定義情報(ACL3)」-「IP定義	情報」
•	プロトコル	→udp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.1.10 → 32 (255 255 255 255)
•	あて先情報 IPアドレス	→ 192.168.0.0
	アドレスマスク	→24 (255.255.255.0)
•	QoS	→指定なし

23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報(ACL3)」-「UDP定義情報」

- ・ 送信元ポート番号 →53 (domainのポート番号)
- あて先ポート番号 →指定しない

24. 手順10.~15.を参考に、以下の項目を指定します。

「LAN情報」-「IP関連」	
「IPフィルタリング情報」	

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →3

ICMP のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL4
٢A	ACL定義情報(ACL4)」-「IP定義	情報」
•	プロトコル	→icmp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IP アドレス アドレスマスク	→指定しない →指定しない

• QoS →指定なし

26. 「ICMP定義情報」をクリックします。

「ICMP定義情報」ページが表示されます。

27. 以下の項目を指定します。

•	ICMP	
	タイプ	→指定しない
	コード	→指定しない

	定義情報	
ICMP	タイブ	
	コード	

- 28. [保存] ボタンをクリックします。
- 29. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →4

残りのパケットをすべて遮断する

30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ ACL5

「ACL定義情報(ACL5)」-「IP定義情報」

• プロトコル	→すべて
 送信元情報 IPアドレス アドレスマスク 	→指定しない →指定しない
 あて先情報 IPアドレス アドレスマスク 	→指定しない →指定しない

- QoS →指定なし
- 31. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →5
- **32. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

リモート定義の場合

ここでは、LAN上のWWWサーバに対する外部のパソコンからのアクセスを許可し、LAN上のほかのパソコン へのアクセスは禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上の WWWサーバに対してアクセスすると想定されるため、そのアクセスには制限をつけません。



● フィルタリング設計

- LAN上のホスト(192.168.1.2/32)をWWWサーバとして利用することを許可
- LAN上のホスト(192.168.1.3/32)から任意のWWWサーバへのアクセスを許可
- LAN 上のホスト(192.168.1.0/24)から WAN の先の DNS サーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断
- こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- LAN上のホストのWWWサーバとしての利用を許可するには
 - (1)192.168.1.2/32のポート80 (www-http) へのパケットを透過させる
 - (2)(1)の応答パケットを透過させる
- 任意のWWW サーバへのアクセスを許可するには
 - (1)192.168.1.3/32の任意のポートから任意のWWWサーバのポート80(www-http)へのパケットを透過させる
 - (2)(1)の応答パケットを透過させる
- ICMPの通信を許可するためには (1)ICMPパケットを透過させる
- その他をすべて遮断するには

 (1)すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

LAN上のホストのポート80へのパケットを透過させる(インターネット→LAN)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

• 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

3. [追加] ボタンをクリックします。

「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

٠	プロトコル	→tcp
•	送信元情報 IP アドレス	→指定しない
	アドレスマスク	→指定しない
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.1.2 → 32(255.255.255.2

• QoS

→32(255.255.255.255) →指定なし

ブロトコル		tep ▼ (番号指定: ["] その他"を選択時のみ有効です)
送信元情	IPアトレス	
報	アドレスマ スク	0 (0.0.0)
あて先情	IPアドレス	192.168.1.2
報	アドレスマ スク	32 (255.255.255.265) 💌
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

- ・ 送信元ポート番号 →指定しない
- あて先ポート番号 →80 (www-httpのポート番号)
- TCP 接続要求

→対象

TCP定義情報	3
送信元ポート番号	
あて先ポート番号	80
TCP接続要求	⊙対象○対象外

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **11. フィルタリングを行うネットワーク情報の [修正] ボタンをクリックします**。 「ネットワーク情報」が表示されます。
- **12. 「IP 関連」をクリックします**。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>	
動作	●透過 ●透過(接続中のみ) ●遮断
方向	入出力 💌
ACL定義番号	0 参照

15. [追加] ボタンをクリックします。

LAN上のホストからの応答パケットを透過させる(LAN→インターネット)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」		
• 定義名	→ ACL1	
「ACL定義情報(ACL1)」-「IP定詞	奏情報」	
• プロトコル	→ tcp	
 送信元情報 IPアドレス アドレスマスク 	→ 192.168.1.2 → 32(255.255.255.255)	
 あて先情報 IPアドレス アドレスマスク 	→指定しない →指定しない	
• QoS	→指定なし	
「ACL定義情報(ACL1)」-「TCPS	定義情報」	
• 送信元ポート番号	→80(www-httpのポート番号)	
• あて先ポート番号	→指定しない	
● TCP接続要求	→対象外	
「相手情報」- 「IP 関連」 「IP フィルタリング情報」		
● 動作	→透過	
• 方向	→入出力	
● ACL定義番号	→ 1	

任意のWWWサーバのポート80へのパケットを透過させる(LAN→インターネット)

17. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ ACL2
٢A	ACL定義情報(ACL2)」-「IP定義	情報」
•	プロトコル	→tcp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.1.3 → 32 (255.255.255.255)
•	あて先情報 IP アドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし
٢A	ACL定義情報(ACL2)」-「TCP定	2義情報」
•	送信元ポート番号	→指定しない
•	あて先ポート番号	→80(www-httpのポート番号)
•	TCP接続要求	→対象

「相手情報」-「IP 関連」

「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →2

任意のWWWサーバからの応答パケットを透過させる(インターネット→LAN)

18. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ ACL3

「ACL定義情報(ACL3)」-「IP定義情報」

•	プロトコル	→tcp
•	送信元情報	
	IP アトレス アドレスマスク	→指定しない →指定しない
	ちて仕はむ	

- あて先情報
 IPアドレス → 192.168.1.3
 アドレスマスク → 32 (255.255.255.255)
- QoS →指定なし

「ACL定義情報(ACL3)」-「TCP定義情報」

- ・ 送信元ポート番号 →80 (www-httpのポート番号)
- あて先ポート番号 →指定しない
- TCP接続要求 →対象外

「相手情報」-「IP 関連」

「IP フィルタリング情報」

- 動作 →透過
 う向 →入出力
- ACL定義番号 →3

DNS サーバのポート 53 への UDP パケットを透過させる(LAN → インターネット)

19. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL4	
ΓА	CL定義情報	(ACL4)」-「IP定義情報」	

•	プロトコル	→udp
•	送信元情報	
	IPアドレス	→ 192.168.1.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報	

- IPアドレス
 →指定しない

 アドレスマスク
 →指定しない
- QoS →指定なし

IP フィルタリング機能を使う

20. 「UDP 定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

21. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
 - あて先ポート番号 →53 (domain のポート番号)

■UDP定義情報	3
送信元ボート番号	
あて先ボート番号	53

- 22. [保存] ボタンをクリックします。
- 23. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」

「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →4

DNS サーバからの応答パケットを透過させる(インターネット→LAN)

24. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → ACL5

「ACL定義情報(ACL5)」-「IP定義情報」

- プロトコル → udp
 送信元情報

 ドアドレス →指定しない
 アドレスマスク →指定しない

 あて先情報

 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- QoS →指定なし

25. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報(ACL5)」-「UDP定義情報」

- ・ 送信元ポート番号 →53 (domainのポート番号)
- あて先ポート番号 →指定しない
- 26. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →5

ICMP のパケットを透過させる

27. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL6
ΓA	CL定義情報(ACL6)」-「IP定義	情報」
•	プロトコル	→icmp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし

28. 「ICMP 定義情報」をクリックします。

「ICMP定義情報」ページが表示されます。

29. 以下の項目を指定します。

•	ICMP	
	タイプ	→指定しない
	コード	→指定しない

	定義情報	R	3
	タイプ		
ICIVIP	コード		

- 30. [保存] ボタンをクリックします。
- 31. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →6

残りのパケットをすべて遮断する

32. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ACL7

「ACL定義情報(ACL7)」-「IP定義情報」

• プロトコル	→すべて
 送信元情報 IPアドレス アドレスマスク 	→指定しない →指定しない
 あて先情報 IPアドレス 	→指定しない
アドレスマスク	→指定しない

- QoS →指定なし
- 33. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP関連」

「IP フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →7
- **34. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.13.3 外部から特定サーバへのアクセスだけ許可して SPI を併用する

適用機種 全機種

LAN定義の場合

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止し、SPIを 利用して外部へアクセスする場合の設定方法を説明します。ただし、FTPサーバ名を解決するためにDNSサーバ へのアクセスは許可します。



 ・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
- ICMPの通信を許可するためには (1)ICMPパケットを透過させる
- 内部LANから外部へ開始するアクセスは許可し、その他をすべて遮断するには
 (1)残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルールの設定を行う場合の設定例を示します。

内部LANのホストのポート21へのTCPパケットを透過させる(外部LAN→内部LAN)

- **1. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名

→ ACL0

 <ACL情報追加フィールド>

 定義名
 ACL0

- 【追加】ボタンをクリックします。
 「ACL定義情報(ACL0)」ページが表示されます。
- **4. 「IP 定義情報」をクリックします**。 「IP 定義情報」ページが表示されます。

アドレスマスク

• QoS

•	プロトコル	→tcp
•	送信元情報	
	IPアドレス	→ 192.168.0.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報 IP アドレス	→ 192.168.1.5

→ 192.168.1.5
→32 (255.255.255.255)
→指定なし

■IP定義			
ブロトコル		tcp ▼ (番号指定: 7その他"を選択時のみ有効です)	
送信元情	IPアドレス	192.168.0.0	
報	アトレスマ スク	24 (255.255.255.0)	
あて先情	IPアドレス	192.168.1.5	
報	アドレスマ スク	32 (255.255.255.255) 💌	
QoS		指定なし <mark>→</mark> TOS、または、DSCPを選択時に値を入力してくだ さい	

6. [保存] ボタンをクリックします。

7. 「TCP 定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

8. 以下の項目を指定します。

- ・ 送信元ポート番号 →指定しない
- あて先ポート番号 →21(ftpのポート番号)
- TCP接続要求 →対象

■TCP定義情報	3
送信元ポート番号	
あて先ボート番号	21
TCP接続要求	◎対象○対象外

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「LAN情報」をクリックします**。 「LAN情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **12. 「**IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

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

「IPフィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →0

fACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	◎透過○遮断	
方向	入出力 👻	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

内部LANのホストからの応答パケットを透過させる(内部LAN→外部LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」

 ● 定義名 	→ACL1		
「ACL定義情報(ACL1)」-「IP定義情報」			
• プロトコル	→tcp		
 送信元情報 IPアドレス アドレスマスク 	→ 192.168.1.5 → 32 (255.255.255.255)		
 あて先情報 IPアドレス アドレスマスク 	→192.168.0.0 →24 (255.255.255.0)		
• QoS	→指定なし		
「ACL定義情報(ACL1)」-「TCP5	官義情報」		
• 送信元ポート番号	→21(ftpのポート番号)		
• あて先ポート番号	→指定しない		
 TCP 接続要求 	→対象外		

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

•	動作	→透過
•	方向	→入出力
•	ACL定義番号	→ 1

DNS サーバのポート 53 への UDP パケットを透過させる(外部 LAN → 内部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

- 定義名 →ACL2
 FACL定義情報 (ACL2) 「IP定義情報」
 プロトコル → udp
 送信元情報
 IPアドレス → 192.168.0.0 アドレスマスク → 24 (255.255.255.0)

 あて先情報
- IPアドレス → 192.168.1.10
 アドレスマスク → 32 (255.255.255)
 OoS →指定なし
- 18. 「UDP定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →53 (domainのポート番号)

UDP定義情報		3
送信元ボート番号		
あて先ボート番号	53	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →2

DNS サーバからの応答パケットを透過させる(内部 LAN → 外部 LAN)

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → ACL3

「ACL定義情報(ACL3)」-「IP定義情報」

- プロトコル → udp
 送信元情報
 IPアドレス → 192.168.1.10
 アドレスマスク → 32 (255.255.255.255)
- あて先情報
 IPアドレス → 192.168.0.0
 アドレスマスク → 24 (255.255.255.0)
- QoS →指定なし
- 23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報(ACL3)」-「UDP定義情報」

- ・ 送信元ポート番号 →53 (domainのポート番号)
- あて先ポート番号 →指定しない
- 24. 手順10.~15.を参考に、以下の項目を指定します。

「LAN情報」-「IP関連」

「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →3

ICMP のパケットを透過させる

25. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

定義名

→ACL4

「ACL定義情報(ACL4)」-「IP定義情報」

- プロトコル → icmp
 送信元情報
- IPアドレス →指定しない
 アドレスマスク →指定しない
 あて先情報
- IPアドレス
 →指定しない

 アドレスマスク
 →指定しない
- QoS →指定なし

26. 「ICMP定義情報」をクリックします。

「ICMP定義情報」ページが表示されます。

•	ICMF	C			
	タイ	プ		→指定しない	
	$\Box -$	ド		→指定しない	
	ICMP	定義情報	報		3
		タイブ			
1	GMP	コード			

- 28. [保存] ボタンをクリックします。
- 29. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →4

残りのパケットに SPIを利用して IP フィルタリングを行う

30. 条件にあてはまらない場合の [修正] ボタンをクリックします。

「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。

- 31. 以下の項目を指定します。
 - 動作

→SPI

<ipフィルタリング情報入力フィールド(条件にあてはまらない場合)></ipフィルタリング情報入力フィールド(条件にあてはまらない場合)>				
動作	 ○ 透過 ○ 遮断 ③ SPI 			
	情報保持タイマ 5 分 🗸			

- 32. [保存] ボタンをクリックします。
- **33. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

リモート定義の場合

ここでは、外部からLAN上のWWWサーバに対するアクセスを許可し、ほかのLAN上のパソコンへのアクセスを禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のサーバに対してアクセスしますが、これらのアクセスに対してはSPIによるIPフィルタリングの対象とします。



● フィルタリング設計

- LAN上のホスト(192.168.1.2/32)をWWWサーバとして利用を許可
- ICMPの通信を許可
- 内部 LAN から外部へ開始するアクセスは許可し、その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- ICMPの通信を許可するためには (1)ICMPパケットを透過させる
- 内部LANから外部へ開始するアクセスは許可し、その他をすべて遮断するには
 (1)残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルールの設定を行う場合の設定例を示します。

LAN上のホストのポート80へのパケットを透過させる(インターネット→LAN)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

• 定義名	→ ACL0
	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ACLO

- 【追加】ボタンをクリックします。
 「ACL定義情報(ACL0)」ページが表示されます。
- **「IP定義情報」をクリックします。** 「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

- プロトコル → tcp
 送信元情報
 IPアドレス →指定しない
 アドレスマスク →指定しない

 あて先情報
- IPアドレス → 192.168.1.2
 アドレスマスク → 32 (255.255.255)
 OoS →指定なし

■IP定義	■IP定義情報			
ブロトコル		tcp ▼ (番号指定:、その他″を選択時のみ有効です)		
送信元情	IPアドレス			
報	アドレスマ スク	0 (0.0.0.0)		
あて先情	IPアドレス	192.168.1.2		
報	アトレスマ スク	32 (255.255.255.255) 💌		
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい		

- 6. [保存] ボタンをクリックします。
- 「TCP 定義情報」をクリックします。
 「TCP 定義情報」ページが表示されます。

- ・ 送信元ポート番号 →指定しない
- あて先ポート番号 → 80 (www-httpのポート番号)
- TCP 接続要求

→対象

■TCP定義情報		3
送信元ポート番号		
あて先ボート番号	80	
TCP接続要求	●対象○対象外	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **11. フィルタリングを設定するネットワークの欄の [修正] ボタンをクリックします**。 「ネットワーク情報」ページが表示されます。
- **12. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- 13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	●透過 ○透過(接続中のみ) ○遮断	
方向	入出力 🗸	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

LAN上のホストからの応答パケットを透過させる(LAN→インターネット)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」	
• 定義名	→ACL1
「ACL定義情報(ACL1)」-「IP定義	情報」
• プロトコル	→tcp
 送信元情報 IPアドレス 	→ 192.168.1.2
アドレスマスク	→32 (255.255.255.255)
 あて先情報 IPアドレス アドレスマスク 	→指定しない →指定しない
• QoS	→指定なし
「ACL定義情報(ACL1)」-「TCP定	2義情報」
• 送信元ポート番号	→80(www-httpのポート番号)
• あて先ポート番号	→指定しない
• TCP 接続要求	→対象外
「相手情報」- 「IP 関連」 「IP フィルタリング情報」 • 動作	→漆冶

方向 →入出力
 ACL定義番号 →1

ICMP のパケットを透過させる

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL2
٢A	CL定義情報(ACL2)」-「IP定義	情報」
•	プロトコル	→icmp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし

18. 「ICMP定義情報」をクリックします。

「ICMP定義情報」ページが表示されます。

•	CMF タイゴ コー	っ プ ド		→指定しない →指定しない
	omp //P	定義情報 タイブ コード	R	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →2

残りのパケットに SPIを利用して IP フィルタリングを行う

22. 条件にあてはまらない場合の [修正] ボタンをクリックします。

「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。

- 23. 以下の項目を指定します。
 - 動作

→ SPI

<ip7< th=""><th>イルタリング情報入力フィールド(条件にあて(はまらない場合)></th></ip7<>	イルタリング情報入力フィールド(条件にあて(はまらない場合)>
動作	 ○ 透過 ○ 透過(接続中のみ) ○ 遮断 ③ SPI 情報保持タイマ 5 分 ▼

- 24. [保存] ボタンをクリックします。
- **25. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.13.4 **外部の特定サービスへのアクセスだけ許可する** (IPv6フィルタリング)

適用機種 全機種

LAN定義の場合

ここでは、IPv6 フィルタリングを使って、内部 LAN 上のパソコンから外部 LAN 上のすべての FTP サーバに対し てアクセスすることだけを許可し、ほかのサーバ(WWW サーバなど)へのアクセスを禁止する場合の設定方法 を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。



• 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。

- 内部LAN
 外部LAN

 LAN1
 LAN0

 透過
 DNSサ-バ

 IPフィルタリング
 FTPサ-バ

 透過
 FTPサ-バ

 遮断
 WWWサ-バ
- •本装置はftp-data転送に関するフィルタリングルールを自動的に作成します。

● フィルタリング設計

- 内部 LAN 上のホスト(2001:db8:1111:1000::/64)から任意の FTP サーバへのアクセスを許可
- 内部 LAN 上のホスト(2001:db8:1111:1000::/64)から外部 LAN の DNS サーバへのアクセスを許可
- ICMPv6の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6は、IPv6通信を行う際にさまざまな制御メッセージを交換します。ICMPv6の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6の通信を透過させる設定を行ってください。

● フィルタリングルール

• FTP サーバへのアクセスを許可するには

 (1)2001:db8:1111:1000::/64の任意のポートから、任意のアドレスのポート21(ftp)へのTCPパケットを透 過させる

- (2)(1)の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
 - (1)2001:db8:1111:1000::/64の任意のポートからDNS サーバのポート 53(domain)への UDP パケットを透 過させる
 - (2)(1)の応答パケットを透過させる
- ICMPv6の通信を許可するためには (1)ICMPv6パケットを透過させる
- その他をすべて遮断するには

 (1)すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

FTP サーバのポート21 (ftp) への TCP パケットを透過させる (内部 LAN → 外部 LAN)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名 → ACL0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ACLO

3. [追加] ボタンをクリックします。

「ACL定義情報(ACL0)」ページが表示されます。

4. 「IPv6定義情報」をクリックします。

「IPv6定義情報」ページが表示されます。

- 5. 以下の項目を指定します。
 - プロトコル

- → tcp
- 送信元 IPv6アドレス/プレフィックス長

→ 2001:db8:1111:1000::/64

- あて先 IPv6アドレス/プレフィックス長
- QoS

→指定しない→指定なし

tcp ✓ 番号指定: // ぞの他 ″を選択時のみ有効です)
2001:db8:1111:1000::
指定なし
1 2 1 1

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP 定義情報」をクリックします。 「TCP 定義情報」ページが表示されます。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →21(ftpのポート番号)
- TCP接続要求 →対象

■TCP定義情報	3
送信元ポート番号	
あて先ポート番号	21
TCP接続要求	●対象○対象外

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **12.** 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

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

「IPv6フィルタリング情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	●透過 ○透過(接続中のみ) ○遮断	
方向	入出力 👻	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

FTP サーバからの応答パケットを透過させる(外部 LAN →内部 LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」		
 定義名 	→ ACL1	
「ACL定義情報(ACL1)」-「IPv6定義情報」		
 プロトコル 	→tcp	
• 送信元 IPv6アドレス/プレフィックス長	→指定しない	
• あて先 IPv6アドレス/プレフィックス長	→2001:db8:1111:1000::/64	
• QoS	→指定なし	
「ACL定義情報(ACL1)」-「TCP定義情報」		
• 送信元ポート番号	→21(ftpのポート番号)	
• あて先ポート番号	→指定しない	
• TCP 接続要求	→対象外	
「LAN 情報」- 「IPv6 関連」 「IPv6 フィルタリング情報」		
• 動作	→透過	
• 方向	→入出力	
• ACL定義番号	→ 1	

DNS サーバのポート 53 への UDP パケットを透過させる(内部 LAN → 外部 LAN)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」 ・ 定義名 → ACL2 「ACL定義情報 (ACL2)」 - 「IPv6 定義情報」 ・ プロトコル → udp ・ 送信元 IPv6アドレス/プレフィックス長 → 2001:db8:1111:1000::/64 ・ あて先 IPv6アドレス/プレフィックス長 →指定しない ・ QoS →指定なし

18. 「UDP 定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号

→53(domainのポート番号)

■UDP定義情報	3
送信元ポート番号	
あて先ボート番号	53

20. [保存] ボタンをクリックします。

21. 手順10.~15.を参考に、以下の項目を指定します。

	「LAN情報」-「IPv6 関連」		
	「IPv6 フィルタリング情報」		
	 動作 	→透過	
		→入出力	
	 ACL 定義番号 	→ 2	
DNS	サーバからの応答パケットを透	5過させる	(外部LAN→内部LAN)
22.	手順1.~6.を参考に、以下の項目	を指定します	• •
	「ACL情報」		
	 ● 定義名 		→ ACL3
	「ACL定義情報(ACL3)」-「IPv6定	義情報」	
	• プロトコル		→udp
	• 送信元 IPv6アドレス/プレフィッ	クス長	→指定しない
	• あて先 IPv6アドレス/プレフィッ	クス長	→2001:db8:1111:1000::/64
	• QoS		→指定なし
23.	手順18.~20.を参考に、以下の項	目を指定しま	きす 。
	「ACL定義情報(ACL3)」-「UDP定	義情報」	
	• 送信元ポート番号	→53 (domai	inのポート番号)
	• あて先ポート番号	→指定しない	
24.	手順10.~15.を参考に、以下の項	目を指定しま	きす。
	「I AN 情報」- 「IPv6 関連」		
	「IPv6フィルタリング情報」		
	● 動作	→透過	
	• 方向	→入出力	
	• ACL定義番号	→ 3	
ICM	Pv6のパケットを透過させる		
25.	手順1.~6.を参考に、以下の項目	を指定します	- •
	「ACL情報」		
	 ● 定義名 		→ ACL4
	「ACL定義情報(ACL4)」-「IPv6定	義情報」	
	• プロトコル		→icmpv6
	• 送信元 IPv6アドレス/プレフィッ	クス長	→指定しない
	• あて先 IPv6アドレス/プレフィッ	クス長	→指定しない
	• QoS		→指定なし
26.	「ICMP定義情報」をクリックします	す。	
	「ICMP定義情報」ページが表示されま	す。	

•	ICM	Ρ		
	タイ	プ	→指定しない	
	$\Box -$	ド	→指定しない	
	ICMP	定義情報	R	3
T		タイプ		
L L	GMP	7-6		

- 28. [保存] ボタンをクリックします。
- 29. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」 「IPv6フィルタリング情報」

- 動作 →透過
- →入出力 方向
- ACL定義番号 →4

残りのパケットをすべて遮断する

30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名		→ ACL5				
٢A	「ACL定義情報(ACL5)」-「IPv6定義情報」						
•	プロトコ	עוב	→すべて				
•	送信元	IPv6 アドレス/プレフィックス長	→指定しない				
•	あて先	IPv6 アドレス/プレフィックス長	→指定しない				
•	QoS		→指定なし				

31. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IPv6 関連」 「IPv6フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →5
- 32. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、IPv6フィルタリングを使って、LAN上のパソコンからイントラネット上のすべてのFTPサーバに対し てアクセスすることだけを許可し、ほかのサーバ(WWWサーバなど)へのアクセスを禁止する場合の設定方法 を説明します。ただし、FTPサーバ名を解決するためにDNSサーバへのアクセスを許可する設定にします。



•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。

- DNSサーバ 透過 IPv6フィルタリング Internet 透過 WWWサーバ 遮断 ネットワークアドレス 2011.db8:1111:1000:/64
- •本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。

● フィルタリング設計

- LAN上のホスト(2001:db8:1111:1000::/64)から任意のFTPサーバへのアクセスを許可
- LAN 上のホスト(2001:db8:1111:1000::/64)からWAN の先のDNS サーバへのアクセスを許可
- ICMPv6の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6は、IPv6通信を行う際にさまざまな制御メッセージを交換します。ICMPv6の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6の通信を透過させる設定を行ってください。

● フィルタリングルール

- FTPサーバへのアクセスを許可するには
 - (1)2001:db8:1111:1000::/64の任意のポートから、任意のFTPサーバのポート21(ftp)へのTCPパケットを 透過させる
 - (2)(1)の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
 - (1)2001:db8:1111:1000::/64の任意のポートからDNSサーバのポート53(domain)へのUDPパケットを透 過させる
 - (2)(1)の応答パケットを透過させる
- ICMPv6の通信を許可するためには
 - (1)ICMPv6パケットを透過させる

その他をすべて遮断するには

 (1)すべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

任意のFTPサーバのポート21(ftp)へのTCPパケットを透過させる(LAN→イントラネット)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

定義名

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ACLO

- 【追加】ボタンをクリックします。
 「ACL 定義情報(ACL0)」ページが表示されます。
- **4.** 「IPv6定義情報」をクリックします。

「IPv6定義情報」ページが表示されます。

- 5. 以下の項目を指定します。
 - プロトコル

- → tcp
- 送信元 IPv6アドレス/プレフィックス長 →2001:db8:1111:1000::/64

→ ACL0

- あて先 IPv6アドレス/プレフィックス長 →指定しない
- QoS

→指定なし

■IPv6定義情報	3
プロトコル	tcp V (番号指定: Cの他"を選択時のみ有効です)
送信元IPv6アトレ ス/ブレフィックス	2001:db8:1111:1000::
あて先IPv6アドレ スノブレフィックス	
QoS	指定なし ▼ Traffic Class、または、DSCPを選択時に値を入力 してください

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

- ・ 送信元ポート番号 →指定しない
- あて先ポート番号 →21 (ftpのポート番号)
- TCP接続要求 →対象

■TCP定義情報	5
送信元ポート番号	
あて先ボート番号	21
TCP接続要求	●対象○対象外

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします。** 「相手情報」ページが表示されます。
- **11. フィルタリングを行うネットワーク情報の [修正] ボタンをクリックします**。 「ネットワーク情報」が表示されます。
- **12.** 「IPv6 関連」をクリックします。 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

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

「IPv6フィルタリング情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>			
動作	●透過 ○透過(接続中のみ) ○遮断		
方向	入出力 💌		
ACL定義番号	0 参照		

15. [追加] ボタンをクリックします。

FTP サーバからの応答パケットを透過させる(イントラネット→LAN)

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」				
 定義名 	→ ACL1			
「ACL定義情報(ACL1)」-「IPv6定義情報」				
 プロトコル 	→tcp			
• 送信元 IPv6アドレス/プレフィックス長	→指定しない			
• あて先 IPv6アドレス/プレフィックス長	→2001:db8:1111:1000::/64			
• QoS	→指定なし			
「ACL定義情報(ACL1)」-「TCP定義情報」				
• 送信元ポート番号	→21(ftpのポート番号)			
• あて先ポート番号	→指定しない			
• TCP 接続要求	→対象外			
「相手情報」-「IPv6関連」				
「IPv6 フィルタリング情報」				
● 動作	→透過			
• 方向	→入出力			
• ACL 定義番号	→ 1			

DNS サーバのポート53 への UDP パケットを透過させる(LAN →イントラネット)

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名	→ ACL2				
「ACL定義情報(ACL2)」-「IPv6定義情報」					
 プロトコル 	→udp				
• 送信元 IPv6アドレス/プレフィックス長	→2001:db8:1111:1000::/64				
• あて先 IPv6アドレス/プレフィックス長	→指定しない				
• QoS	→指定なし				
「UDP定義情報」をクリックします。					

18.

「UDP定義情報」ページが表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号

→53 (domainのポート番号)

■UDP定義情報	3
送信元ポート番号	
あて先ボート番号	53

20. [保存] ボタンをクリックします。

21. 手順10.~15.を参考に、以下の項目を指定します。

	「相手情報」-「IPv6関連」		
	IPV6 ノイルタリンク情報」	、`禾`□	
	 動1F 方向 	→返迥 →入出力	
	 ACL 定義番号 	→2	
DNS	サーハからの心谷ハケットを透	通させる	(イントラネット→LAN)
22.	手順1.~6.を参考に、以下の項目	を指定します	0
	「ACL情報」		
	• 定義名		→ ACL3
	「ACL定義情報(ACL3)」-「IPv6定	義情報」	
	• プロトコル		→udp
	• 送信元 IPv6アドレス/プレフィッ	クス長	→指定しない
	• あて先 IPv6アドレス/プレフィッ	クス長	→ 2001:db8:1111:1000::/64
	• QoS		→指定なし
23.	手順18.~20.を参考に、以下の項	目を指定しま	र す。
	「ACL定義情報(ACL3)」-「UDP定	義情報」	
	• 送信元ポート番号	→53 (domai	nのポート番号)
	• あて先ポート番号	→指定しない	
24.	手順10.~15.を参考に、以下の項	目を指定しま	र す。
	「相手情報」-「IPv6関連」		
	「IPv6フィルタリング情報」		
	● 動作	→透過	
	• 方向	→入出力	
	• ACL定義番号	→ 3	
ICM	Pv6のパケットを透過させる		
25.	手順1.~6.を参考に、以下の項目	を指定します	- 0
	「ACL情報」		
	 定義名 		→ ACL4
	「ACL定義情報(ACL4)」-「IPv6定	義情報」	
	• プロトコル		→icmpv6
	• 送信元 IPv6アドレス/プレフィッ	クス長	→指定しない
	• あて先 IPv6アドレス/プレフィッ	クス長	→指定しない
	• QoS		→指定なし
26.	「ICMP定義情報」をクリックします	す。	
	「ICMP定義情報」ページが表示されま	す。	

	ICM	D		
	タイ	プ	→指定しない	
	$\Box -$	ド	→指定しない	
	ICMP	定義情報	報	3
T		タイプ		
ľ	OMP	コード		

- 28. [保存] ボタンをクリックします。
- 29. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IPv6関連」

「IPv6 フィルタリング情報」

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →4

残りのパケットをすべて遮断する

30. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名		→ACL5
「ACL定義情報(ACL5)」-「IPv6定義情報」			
•	プロトコル		→すべて
•	送信元	IPv6アドレス/プレフィックス長	→指定しない
•	あて先	IPv6アドレス/プレフィックス長	→指定しない
•	QoS		→指定なし

31. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」- 「IPv6 関連」 「IPv6 フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →5
- 32. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。
2.13.5 外部の特定サーバへのアクセスだけを禁止する

適用機種 全機種

LAN定義の場合

ここでは、外部 LAN の FTP サーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設定

• 内部LANのホスト(192.168.1.0/24)から外部LANのFTPサーバ(192.168.0.5)へのアクセスを禁止

● フィルタリングルール

FTPサーバへのアクセスを禁止するには

 (1)192.168.1.0/24から192.168.0.5のポート21(ftp)へのTCPパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

FTP サーバ(192.168.0.5) への TCP パケットを遮断する(内部 LAN → 外部 LAN)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

3. [追加] ボタンをクリックします。

「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

アドレスマスク

• QoS

•	プロトコル	→tcp
•	送信元情報	
	IPアドレス	→ 192.168.1.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報 IP アドレス	→ 192.168.0.5

→ 32	(255.255.255.255)

■IP定義情報		
ブロトコル		tep ▼ (番号指定: 7その他"を選択時のみ有効です)
送信元情	IPアドレス	192.168.1.0
報	アドレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	192.168.0.5
報	アトレスマ スク	32 (255.255.255.255) 💌
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい

6. [保存] ボタンをクリックします。

7. 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →21 (ftpのポート番号)
- TCP接続要求 →対象

■TCP定義情報		5
送信元ポート番号		
あて先ボート番号	21	
TCP接続要求	●対象○対象外	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **11.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **12.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **13.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →0

▲ 「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	○透過 ⊙遮断	
方向	入出力 👻	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

16. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、インターネット上の特定のサーバに対するアクセスを禁止する場合の設定方法を説明します。



● フィルタリング設計

• LAN上のホスト(192.168.1.0/24)からアドレス100.100.100.00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 100.100.100.000 任意のポートへのすべてのパケットを遮断する

上記のフィルタリングルールの設定を行う場合の設定例を示します。

アドレス(100.100.100)へのすべてのパケットを遮断する(LAN→インターネット)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

• 定義名 → ACL0		
<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

- 【追加】ボタンをクリックします。
 「ACL定義情報(ACL0)」ページが表示されます。
- 「IP定義情報」をクリックします。
 「IP定義情報」ページが表示されます。

- プロトコル →すべて
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス → 100.100.100
 アドレスマスク → 32 (255.255.255)

 OoS →指定なし

■IP定義	情報	3
ブロトコル		すべて (番号指定:
_{送信元桂} IPアドレフ		192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	100.100.100.100
報	アドレスマ スク	32 (255.255.255.265) 💌
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **9. フィルタリングを設定するネットワークの欄の [修正] ボタンをクリックします**。 「ネットワーク情報」ページが表示されます。
- **10. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。

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

「IPフィルタリング情報」が表示されます。

- 12. 以下の項目を指定します。
 - 動作 →遮断
 - 方向 →入出力
 - ACL定義番号 →0

ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	○透過 ○透過(接続中のみ) ⊚遮断	
方向	入出力 👻	
ACL定義番号	0 参照	

- 13. [追加] ボタンをクリックします。
- **14. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.13.6 利用者が意図しない発信を防ぐ

適用機種 全機種

LAN 上のパソコンは、利用者の意志とは無関係に、実体のない NetBIOS サーバにアクセスすることがあります。 その際、回線が接続され、利用者が意識しないところで通信料金がかかってしまいます。 ここでは、上記のような、回線に対するむだな発信を抑止する場合のフィルタリング設定方法を説明します。



● フィルタリング設計

• ポート137~139 (NetBIOS サービス) へのアクセスを禁止

● フィルタリングルール

ポート137~139へのアクセスを禁止するには
 (1)ポート137~139へのすべてのパケットを遮断する
 (2)ポート137~139からのすべてのパケットを遮断する

Windows[®](TCP上のNetBIOS)環境のネットワークでは、セキュリティ上の問題とむだな課金を抑えるために、
 ポート番号 137~139の外向きの転送経路をふさいでおく必要があります。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

ポート137~139へのTCPパケットを遮断する

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

```
→ ACL0
```

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

- 【追加】ボタンをクリックします。
 「ACL定義情報(ACL0)」ページが表示されます。
- **4.** 「IP 定義情報」をクリックします。 「IP 定義情報」ページが表示されます。

•	プロトコル	→tcp
•	送信元情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし

■IP定義	■IP定義情報		
ブロトコル		tcp ▼ (番号指定: ["] その他"を選択時のみ有効です)	
洋信元情	IPアドレス		
報	アドレスマ スク	0 (0.0.0)	
あて失情	IPアドレス		
報	アドレスマ スク	0 (0.0.0)	
QoS		指定なし ▼ TOS、または、DSCPを選択時に値を入力してくだ さい	

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP 定義情報」をクリックします。 「TCP 定義情報」ページが表示されます。
- 8. 以下の項目を指定します。
 - ・ 送信元ポート番号 →指定しない
 - あて先ポート番号 → 137-139
 - TCP接続要求 →対象

■TCP定義情報		3
送信元ポート番号		
あて先ボート番号	137-139	
TCP接続要求	●対象○対象外	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **11. フィルタリングを行うネットワーク情報の [修正] ボタンをクリックします**。 「ネットワーク情報」が表示されます。
- **12. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **13.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →0

fACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	◎透過 ◎透過(接続中のみ) ⑧遮断	
方向	入出力 🔽	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

ポート137~139からのTCPパケットを遮断する

16. 手順1.~15.を参考に、以下の項目を指定します。

「ACL情報」

● 定義名	→ACL1
「ACL定義情報(ACL1)」-「IP定義	。情報」
• プロトコル	→tcp
 送信元情報 IPアドレス 	→指定しない
アドレスマスク	→指定しない
 あて先情報 IPアドレス アドレフマフク 	→指定しない
• QoS	・ 指定 なし
「ACL定義情報(ACL1)」-「TCP」	E義情報」
• 送信元ポート番号	→137-139
• あて先ポート番号	→指定しない
	+1.4

• TCP接続要求 →対象

「相手情報」-「IP 関連」

「IP フィルタリング情報」

•	動作	→遮断
•	方向	→入出力
•	ACL定義番号	→ 1

ポート137~139へのUDPパケットを遮断する

17. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

- ・ 定義名 →ACL2
 FACL定義情報 (ACL2)] 「IP定義情報」
 ・ プロトコル → udp
 ・ 送信元情報

 ・ ど信元情報
 ・ アドレスマスク
 ・ 指定しない
 ・ 方指定しない
 ・ 方指定しない
- QoS →指定なし

18. 「UDP定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

19. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号 → 137-139

UDP定義情報		3
送信元ボート番号		
あて先ボート番号	137-139	

- 20. [保存] ボタンをクリックします。
- 21. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」- 「IP 関連」 「IP フィルタリング情報」

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →2

ポート137~139からのUDPパケットを遮断する

22. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

 定義名 → ACL3 「ACL定義情報(ACL3)」-「IP定義情報」 • プロトコル →udp • 送信元情報 IPアドレス →指定しない アドレスマスク →指定しない あて先情報 →指定しない IPアドレス アドレスマスク →指定しない • QoS →指定なし

23. 手順18.~20.を参考に、以下の項目を指定します。

「ACL定義情報(ACL3)」-「UDP定義情報」

- 送信元ポート番号 →137-139
- あて先ポート番号 →指定しない
- 24. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」-「IP 関連」 「IP フィルタリング情報」

- 動作 → 遮断
- 方向 →入出力
- ACL定義番号 →3
- **25. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.13.7 回線が接続しているときだけ許可する

適用機種 全機種

ー部のパソコンでは、ネットワークの設定によって、ログイン時に自動的にPINGを発行してPPPoEまたは ISDN回線を接続してしまうものがあります。回線接続を必要とするICMPパケットを遮断することによって、 意図しないPINGによるむだな発信を抑止することができます。ここでは、回線が接続されているときにだけ ICMPパケットを透過させる場合の設定方法を説明します。



補足 IPアドレスを直接指定せず、DNSによる名前アドレス変換を利用した場合、発信を抑止することはできません。



● フィルタリング設計

• すでに回線が接続している場合にだけ PING を許可

● フィルタリングルール

すでに回線が接続している場合にだけ PING を許可するには
 (1)回線接続中だけ ICMP パケットを透過させる

上記のフィルタリングルールの設定を行う場合の設定例を示します。

回線が接続しているときだけICMPパケットを透過させる

- 設定メニューのルータ設定で「ACL情報」をクリックします。
 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。

• 定義名

→ ACL0

	<acl情報追加フィールト"></acl情報追加フィールト">
定義名	ACLO

3. [追加] ボタンをクリックします。 「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP定義情報」をクリックします。

「IP定義情報」ページが表示されます。

以下の項目を指定します。 5.

٠	プロトコル	→icmp
•	送信元情報 IPアドレス	→指定しない
	アドレスマスク	→指定しない
•	あて先情報	
	IPアドレス	→指定しない
	アドレスマスク	→指定しない

• QoS		→指定なし
■IP定義	養情報	3
ブロトコル		icmp (番号指定: ~ その他 ~ を選択時のみ有効です)
送信元報	IPアドレス	
報	7ドレスマ スク	0 (0.0.0)
あて先情	IPアドレス	
報	アドレスマ	0 (0.0.0)

指定なし 💙 TOS、または、DSCPを選択時に値を入力してくだ

[保存] ボタンをクリックします。 6.

えク

「ICMP定義情報」をクリックします。 7.

「ICMP定義情報」ページが表示されます。

さい

- 8. 以下の項目を指定します。
 - ICMP タイプ

コード

QoS

→指定しない
→指定しない

■ICMP定義情報		R	3
	タイプ		
ICIMP	コード		

- 9. [保存] ボタンをクリックします。
- 10. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- フィルタリングを行うネットワーク情報の[修正]ボタンをクリックします。 11. 「ネットワーク情報」が表示されます。
- 「IP関連」をクリックします。 12. IP関連の設定項目と「IPアドレス情報」が表示されます。
- IP関連の設定項目の「IPフィルタリング情報」をクリックします。 13. 「IPフィルタリング情報」が表示されます。

- 動作 →透過(接続中のみ)
- 方向 →入出力
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	○透過 ●透過(接続中のみ) ○遮断	
方向	入出力 🔽	
ACL定義番号	0 参照	

- 15. [追加] ボタンをクリックします。
- 16. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.13.8 外部から特定サーバへの ping だけを禁止する

適用機種 全機種

LAN定義の場合

ここでは、内部LANの特定のサーバに対するping(ICMP ECHO)を禁止し、この特定のサーバに対するほかの ICMPパケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の 設定方法を説明します。



● フィルタリング設定

- 内部 LAN のサーバ(192.168.1.5/32) に対して外部からの ping (ICMP ECHO)を禁止
- その他はすべて通過

● フィルタリングルール

- 内部LANのサーバ(192.168.1.5/32)に対して外部からのping(ICMP ECHO)を禁止するには (1)192.168.1.5/32へのICMP TYPE 8のICMPパケットを遮断する
- その他のパケットを許可する

 (1)すべてのパケットを透過させる

上記のフィルタリングルールの設定を行う場合の設定例を示します。

アドレス(192.168.1.5/32) への ICMP TYPE 8 の ICMP パケットを遮断する (外部 LAN → 内部 LAN)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>	
定義名	ACLO

3. [追加] ボタンをクリックします。

「ACL定義情報(ACL0)」ページが表示されます。

「IP定義情報」をクリックします。 4.

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

・プロ	コトコル	→icmp
• 送付	言元情報	
IP 🤇	アドレス	→指定しない
ア	ドレスマスク	→指定しない
• あ	て先情報	
IP 2	アドレス	→ 192.168.1.5

アドレスマスク →32 (255.255.255.255) .

•	QoS	

→指定なし

■IP定義情報		
ブロトコル		icmp (番号指定: ~ その他 ~ を選択時のみ有効です)
送信元情	IPアトレス	
報	アドレスマ スク	0 (0.0.0)
あて先情	IPアドレス	192.168.1.5
報	アドレスマ スク	32 (255.255.255.255) 💌
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- 7. 「ICMP定義情報」をクリックします。 「ICMP定義情報」ページが表示されます。
- 8. 以下の項目を指定します。
 - ICMP タイプ

コード

→8 →指定しない

	定義情報	R	3
	タイブ	8	
ICMP	コード		

- 9. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「LAN 情報」をクリックします。 10. 「LAN情報」ページが表示されます。
- 11. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0情報(物理LAN)」ページが表示されます。
- **12.** 「IP 関連」をクリックします。 IP関連の設定項目と「IPアドレス情報」が表示されます。

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

「IPフィルタリング情報」が表示されます。

- 14. 以下の項目を指定します。
 - 動作 →遮断
 - 方向 →入出力
 - ACL定義番号 →0

 [「]ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	○透過 ⊙遮断	
方向	入出力 👻	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

残りのパケットをすべて透過させる

16. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL1
٢A	ACL定義情報(ACL1)」-「IP	定義情報」
•	プロトコル	→すべて
•	送信元情報 IP アドレス	→指定しない
	アドレスマスク	→指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし

17. 手順10.~15.を参考に、以下の項目を指定します。

「LAN 情報」-「IP 関連」 「IP フィルタリング情報」

•	動作	→透過
•	方向	→入出力
•	ACL定義番号	→ 1

18. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

リモート定義の場合

ここでは、LAN上の特定のサーバに対する ping(ICMP ECHO)を禁止し、この特定のサーバに対するほかの ICMPパケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の 設定方法を説明します。



● フィルタリング設計

- LAN 上のサーバ(192.168.1.5/32)に対して外部からの ping(ICMP ECHO)を禁止
- その他はすべて通過

● フィルタリングルール

- LAN上のサーバ(192.168.1.5/32)に対して外部からのping(ICMP ECHO)を禁止するには (1)192.168.1.5/32のICMP TYPE 8のICMPパケットを遮断する
- その他のパケットを許可する

 (1)すべてのパケットを透過させる

アドレス(192.168.1.5/32)へのICMP TYPE 8のICMPパケットを遮断する (インターネット→LAN)

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

```
→ ACL0
```

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

3. [追加] ボタンをクリックします。

「ACL定義情報(ACLO)」ページが表示されます。

FIP定義情報」をクリックします。 「IP定義情報」ページが表示されます。

•	プロトコル	→icmp
•	送信元情報 IP アドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IP アドレス アドレスマスク	→ 192.168.1.5 → 32 (255.255.255.255)
•	QoS	→指定なし

■IP定義情報		
ブロトコル		icmp (番号指定: ~ その他 ~ を選択時のみ有効です)
、 送信二桂 IPアトレス		
報	アドレスマ スク	0 (0.0.0)
あて先情	IPアドレス	192.168.1.5
報	アドレスマ スク	32 (255.255.255.255) 💌
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- 「ICMP定義情報」をクリックします。
 「ICMP定義情報」ページが表示されます。
- 8. 以下の項目を指定します。
 - ICMP

タイプ	→8
コード	→指定しない

■ICMP定義情報		
	タイプ	8
IC IVIP	コード	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **11. フィルタリングを行うネットワーク情報の [修正] ボタンをクリックします**。 「ネットワーク情報」が表示されます。
- **12. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **13.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。

- 動作 →遮断
- 方向 →入出力
- ACL定義番号 →0

ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	○透過 ⊙ 遮断	
方向	入出力 💌	
ACL定義番号	0 参照	

15. [追加] ボタンをクリックします。

残りのパケットをすべて透過させる

- **16.** 手順1.~6.を参考に、以下の項目を指定します。
 - 「ACL情報」

 定義名 	→ ACL1
「ACL定義情報	(ACL1)」-「IP定義情報」

•	プロトコル	→すべて
•	送信元情報 IP アドレス アドレスマスク	→指定しない →指定しない
•	あて先情報 IP アドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし

17. 手順10.~15.を参考に、以下の項目を指定します。

「相手情報」- 「IP 関連」 「IP フィルタリング情報」

動作

方向 →入出力

→透過

• ACL定義番号 →1

18. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.14 IPsec機能を使う

適用機種 全機種

VPN(Virtual Private Network)は、インターネットを利用して遠隔地のLANをつなぐと、遠隔地のLAN上のア プリケーションやデータが、あたかも同じオフィスのLANのように利用できる機能です。また、認証情報や暗号 情報を設定することにより、インターネット上を流れるデータのセキュリティを確保することができます。 本装置では、VPNを実現するために IPsec というプロトコルを使用して、以下の接続形態が利用できます。

- 固定 IP アドレスでの VPN(手動鍵交換)
 固定 IP アドレスで送信元、送信先の IP アドレス範囲を指定して VPN 通信を行います。
 認証情報、暗号情報の鍵は手動で設定します。
- 固定 IP アドレスでの VPN(自動鍵交換)
 固定 IP アドレスで送信元、送信先の IP アドレス範囲を指定して VPN 通信を行います。
 認証情報、暗号情報の鍵は自動で交換します。
- 可変 IP アドレスでの VPN(自動鍵交換) 自側の IP アドレスが動的に割り当てられる環境で、経路情報(送信先の IP アドレス)に従って VPN 通信を行います。認証情報、暗号情報の鍵は自動で交換します。
- 1つのIKEセッションに複数のIPsecトンネル構成でのVPN(自動鍵交換) 複数のIPsec対象範囲が存在し、IPsec対象範囲をすべて(any)とすることができない環境で、IKEセッション(トンネル)を1つとしてVPN通信を行います。
 認証情報、暗号情報の鍵は自動で交換します。
- IPsec機能と他機能との併用 IPsec機能と他機能を併用する場合のいくつかの設定例を説明します。
- 固定 IP アドレスでバックアップ用に使用する VPN(自動鍵交換)(Si-R370、570)
 固定 IP アドレスでの VPN に加えて、異常を検出した場合に、自動でバックアップを行い、処理を引き継ぐことができます。
- テンプレート着信機能(AAA 認証)を使用した固定 IP アドレスでの VPN(自動鍵交換)
 IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用して VPN 通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能(AAA 認証)を使用した可変 IP アドレスでの VPN(自動鍵交換) 相手側の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使 用して VPN 通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能(RADIUS 認証)を使用した固定 IP アドレスでの VPN(自動鍵交換) IKE 不特定着信の IKE 認証鍵取得に RADIUS 認証機能を使用して VPN 通信を行います。認証情報および暗号 情報の鍵は自動で交換します。
- テンプレート着信機能(RADIUS 認証)を使用した可変 IP アドレスでの VPN(自動鍵交換) 相手側の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に RADIUS 認証機能 を使用して VPN 通信を行います。認証情報および暗号情報の鍵は自動で交換します。
- テンプレート着信機能(動的 VPN)を使用した固定 IP アドレスでの VPN(自動鍵交換) 動的 VPN 接続契機パケットを監視して動的に VPN 通信を行います。
 自装置の IPsec トンネル IP アドレス、IPsec 対象範囲、IPsec 経路情報および接続先監視アドレスは、動的 VPN 情報交換機能で自動に交換します。
- NAT トラバーサルを使用した可変 IP アドレスでの VPN(自動鍵交換) 自側の IP アドレスが動的に割り当てられる環境で、IKE 区間にある NAT を介した IPsec 通信を可能にするた めに、NAT トラバーサル機能を使用して VPN 通信を行います。

 テンプレート着信機能(AAA 認証)およびNATトラバーサルを使用した可変IPアドレスでのVPN(自動鍵 交換)

相手側のIPアドレスが動的に割り当てられる環境で、IKE不特定着信のIKE認証鍵取得にAAA認証機能を使用し、またIKE区間にあるNATを介したIPsec通信を可能にするために、NATトラバーサル機能を使用して VPN通信を行います。認証情報および暗号情報の鍵は自動で交換します。

● 参照 Si-Rシリーズ 機能説明書「2.14 IPsec機能」(P.67)

こんな事に気をつけて

- IPsecはIPv4、IPv6で使用できます。
- NAT 変換には、IPsecの前の変換とIPsecのあとの変換があります。IPsec前に変換する場合はIPsec用の「ネット ワーク情報」で設定します。IPsec後に変換する場合は、回線接続用の「ネットワーク情報」または「LAN 情報」で 設定します。
- インターネット VPN では、VPN 装置どうしがインターネットを介して通信する必要があるため、VPN 装置にはイン ターネット上で使用可能なグローバルな IP アドレスを使用してください(NAT を使用している場合は、マルチ NAT (静的 NAT)で IP アドレスを割り当てます)。
- ・ VPN相互接続するアドレスがプライベートアドレスの場合、重複しないように設計してください。
- ・ IPsec では、IPv4、IPv6 パケット通信だけをサポートしています。IPv4、IPv6 パケット以外は VPN の対象とならないため中継されません。
- 暗号パケットが多重に暗号化される形態で使用しないでください。暗号パケットが二重に暗号化され、復号処理が正常に行えないため通信異常となります。
- ・ IPsecとNAT機能を併用する場合は、マルチNATを使用してください。
- ・ IPsecとマルチNATを併用する場合は、静的NATの設定が必要となることがあります。
- ・ 経路情報を設定する場合、IPsec/IKEネゴシエーションパケットがVPNのトンネルに入らないように設定してください。
- ・ 複数の接続先情報定義に同じ IPsec トンネルアドレスを定義しないでください。
- IKE セッションに対して複数の IPsec トンネル構成を使用する場合は、同じ IPsec 対象範囲がないように設定してください。
- IPsec対象範囲が複数ネットワーク存在し、IPsec対象範囲にすべて(any)を設定できない環境の場合だけ、"IKE セッションに対して複数のIPsecトンネル構成"を使用することをお勧めします。ネットワークごとにIPsec SAを作 成する構成やIPsec対象範囲にすべて(any)を定義できない装置と接続する場合は、"IKE セッションに対して複数 のIPsecトンネル構成"を使用してください。
- ・ テンプレート着信機能(AAA 認証および RADIUS 認証)を使用した IPsec では、以下の点に注意してください。
 - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
 - 初回 IKE ネゴシエーションは Responder でのみ動作します。
 - 自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはで きません。
 - テンプレート定義の接続先監視アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することは できません。
 - AAA設定またはRADIUS認証サーバ側のユーザIDとユーザ認証パスワードを同じに設定してください。
- RADIUS および AAA の登録情報を変更して IPsec が接続できない場合は、手動切断を行い、再度テンプレート着信機能で接続してください。
- ・ 動的 VPN 情報交換機能を使用する場合、システム全体で一意となるユーザ ID を設定してください。
- テンプレート着信機能(動的 VPN)を使用した IPsec では、以下の点に注意してください。
 - IKEセッションに対して複数のIPsecトンネル構成を使用することはできません。
 - IKE モードは Main Mode で動作します。
 - 動的 VPN で作成されたインタフェースにスタティック経路情報が設定されるように動的 VPN 接続契機パケットを 監視するインタフェースの経路情報を設定してください。
 - V31以降のファームウェアとV30ファームウェアでIPsecを行う場合は、V31以降のファームウェアの動的VPN クライアント情報設定で交換情報のエンコードタイプを "off" に指定する必要があります。また、動的VPNサー バをV31以降のファームウェアにする必要があります。
- 動的 VPN で接続する自側ネットワークを異なるアドレスファミリで設定した場合、拡張 IPsec 対象範囲が1定義分追加されます。
- ・ 拡張 IPsec 対象範囲機能未対応版数(V30)の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネット ワークに異なるアドレスファミリを設定しないでください。

- 拡張 IPsec 対象範囲機能を使用して IPsec パケットを通過させた場合、IPsec 対象範囲をチェックする相手装置の場合は IPsec が遮断されます。この場合は、拡張 IPsec 対象範囲機能を使用することはできません。
- 拡張 IPsec 対象範囲を使用して双方向通信を行う場合、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合、片側通信のみ暗号化し、折り返しの通信は暗号化されない場合があります。
- NAT トラバーサル機能を利用するときは、以下の点に注意してください。
 - IKEを行う双方の装置で設定してください。片方の装置での利用やNATトラバーサルのバージョンが異なると、 NATトラバーサルはできません。
 - NAT トラバーサルは、以下のRFC、Internet Draftのバージョンをサポートします。
 - "Negotiation of NAT-Traversal in the IKE"
 - RFC3947
 - draft-ietf-ipsec-nat-t-ike-03 draft-ietf-ipsec-nat-t-ike-02
 - "UDP Encapsulation of IPsec ESP Packets"
 - RFC3948
 - IPsec トンネルに存在する NAT 装置の変換テーブルが解放されると、NAT トラバーサルは動作できなくなります。 変換テーブルを保持するために、接続先監視機能と併用することを推奨します。
 - IPsec通信プロトコルは暗号(ESP)を使用するように設定してください。IPsec通信プロトコルが認証(AH)の 場合は動作しません。
 - 自側トンネルエンドポイントアドレス、および相手側エンドポイントアドレスに IPv4 アドレスを設定してください。IPv6 アドレスを設定した場合は動作しません。
 - IKEを使用する設定をしてください。動的VPN(dvpn)および手動鍵(manual)を設定した場合は動作しません。 - 初回IKE ネゴシエーションが、initiator 装置側でNAT される環境でのみ動作します。
 - テンプレート着信機能(AAA 認証および RADIUS 認証)を使用した IPsec では、IKE モードを Aggressive Mode で 設定してください。Main Mode で設定した場合は動作しません。
- 接続優先制御の設定は、IKEネゴシエーションのすれ違いが頻発する場合にそれぞれ異なる優先方法を設定してください。同じ優先制御を行うと、競合した場合にIKEネゴシエーションが失敗します。この機能を利用する場合は、以下の設定を奨励します。
 - 一方の装置で Initiatorを優先し、一方の装置で Responderを優先する。

◆ VPN とは?

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPNを 使ってつないだルータ間の通信経路のことをトンネルと言います。

◆ 自動鍵交換とは?

IPsecの通信に使用される暗号化・認証用の鍵素材を、自動で作成・更新します。鍵素材を定期的に自動更新 させることにより、セキュリティの強度を高めることができます。自動鍵交換を使用しない場合は、手動で鍵 を設定する必要があります。

◆ NATとIPsecを併用する

IPsecで使用するグローバルアドレスでNATを使用している場合(IPsec後のNAT変換後)は、IPsecパケットがNATを通過できるように、「LAN情報」または「ネットワーク情報」で、以下の静的NATを設定します。

利用形態	設定内容		
固定 IP アドレスでの VPN (手動鍵交換)	 ESPパケットの受信を設定します。 プライベートIP情報 IPアドレス 自側エンドポイントに設定したアドレス ポート番号 すべて グローバルIP情報 IPアドレス 相手 VPN 装置に設定された本装置側のIPアドレス ポート番号 すべて プロトコル ESP 		

利用形態	設定内容	
固定 IP アドレスでの VPN (自動鍵交換)	設定内容 rットの受信を設定します。 イベートIP情報 ドレス 自側エンドポイントに設定したアドレス ト番号 500 ーバルIP情報 ドレス 相手 VPN装置に設定された本装置側のIP アドレス ト番号 500 トコル UDP ケットの受信を設定します。 イベートIP 情報 ドレス 自側エンドポイントに設定したアドレス ト番号 すべて ーバルIP情報 ドレス 相手 VPN装置に設定された本装置側のIP アドレス ト番号 すべて ーバルIP情報 ドレス 相手 VPN装置に設定された本装置側のIP アドレス ト番号 すべて ーバル ESP のWAN (ネットワーク情報)の自側 IP アドレスが202.168.1.66 (固定) であり、 8.1.66 (自側) と202.168.2.66 (相手側)の間で IP sec/IKE 通信を行う場合、 KE 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	
可変IPアドレスでのVPN (Initiator) 可変IPアドレスでのVPN (Initiator)	・ 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 ESPパケットの受信を設定します。 ・ プライベートIP情報	
	IPアドレス 本装置のLAN側IPアドレス ポート番号 すべて ・ グローバルIP情報 IPアドレス 指定しない ポート番号 すべて ・ プロトコル ESP	

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

適用機種 全機種

IPsec機能を使って手動鍵交換でVPNを構築する場合の設定方法を説明します。 ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間の VPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社(PPPoE 常時接続)]

- ローカルネットワークIPアドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス
 - : 202.168.1.66/24

:LAN0ポート使用

- :userid(プロバイダから提示された内容)
 - :userpass(プロバイダから提示された内容)

PPPoE LAN ポート

• PPPoEユーザ認証パスワード

• PPPoEユーザ認証ID

[本社]

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

● 設定条件

[支社]

•	IPsec区間	: 202.168.1.66 - 202.168.2.66
•	IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット
•	IPsec プロトコル	: esp
•	IPsec送信用SPI	:100(16進数)
•	IPsec 送信用 SA 暗号アルゴリズムと暗号秘密鍵	:des-cbc、0123456789(16進数)
•	IPsec 送信用 SA 認証アルゴリズムと認証秘密鍵	:hmac-md5、123456789a(16進数)
•	IPsec受信用SPI	:101(16進数)
•	IPsec 受信用 SA 暗号アルゴリズムと暗号秘密鍵	:des-cbc、23456789ab(16進数)
•	IPsec 受信用 SA 認証アルゴリズムと認証秘密鍵	:hmac-md5、3456789abc(16 進数)
[才	[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)

ジェント=

♦ 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 で弱い鍵として見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

des-cbc で弱い鍵として具体的に知られているものには以下のようなものがあります。本装置は、これらの文字列で 始まる鍵で通信できないようにしています。

0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、FEFE FEFE FEFE FEFE、01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、FE01 FE01 FE01 FE01、E01F E01F F10E F10E、E001 E001 F101 F101、1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、E0FE E0FE F1FE F1FE、FE1F FE1F FE0E FE0E、1F01 1F01 0E01 0E01、FEE0 FEE0 FEF1 FEF1

- ・ 暗号アルゴリズムに 3desを選択する場合は、以下のように鍵を16桁ごとに3つに分割し、鍵1≠鍵2≠鍵3となる ように鍵を設定してください。
 - 鍵: 1122334455667788 9900aabbccddeeff 1122334455667788 鍵1(16桁) 鍵2(16桁) 鍵3(16桁)

鍵1=鍵3のように鍵を設定すると、16バイトの鍵で暗号化するのと同じ結果になります。また、鍵1=鍵2、鍵2 =鍵3のように鍵を設定すると、それぞれ鍵3、鍵1のdes-cbc暗号と同じ結果になります(鍵1=鍵2=鍵3の場合 も同様です)。



上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度 →0



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

•	鍵交換モード	→手動鍵使用
	相手側エンドポイント	→202.168.2.66
	自側エンドポイント	→202.168.1.66

建六场工	⊙ 手動鍵使用
現文換で	相手側エンドポイント 202.168.2.66
	自側エンドボイント 202.168.1.66

- 13. 【保存】ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

IPsec 機能を使う

	5~の設定(洋信田)	
•		
	SPI值	→100
	暗号アルゴリズム	→des-cbc
	暗号鍵	
	鍵識別	→16進数
	鍵	→0123456789
	認証アルゴリズム	→hmac-md5
	認証鍵	
	鍵識別	→16進数
	鍵	→123456789a
•	SAの設定(受信用)	
•	SA の設定(受信用) SPI 値	→ 101
•	SAの設定(受信用) SPI 値 暗号アルゴリズム	→ 101 → des-cbc
•	SAの設定(受信用) SPI値 暗号アルゴリズム 暗号鍵	→ 101 → des-cbc
•	SAの設定(受信用) SPI 値 暗号アルゴリズム 暗号鍵 鍵識別	→ 101 → des-cbc → 16 進数
•	SA の設定(受信用) SPI 値 暗号アルゴリズム 暗号鍵 鍵識別 鍵	→ 101 → des-cbc → 16 進数 → 23456789ab
•	SA の設定(受信用) SPI 値 暗号アルゴリズム 暗号鍵 鍵識別 鍵 認証アルゴリズム	→ 101 → des-cbc → 16 進数 → 23456789ab → hmac-md5
•	SAの設定(受信用) SPI値 暗号アルゴリズム 暗号鍵 鍵識別 鍵 認証アルゴリズム 認証鍵	→ 101 → des-cbc → 16 進数 → 23456789ab → hmac-md5
•	SA の設定(受信用) SPI値 暗号アルゴリズム 暗号鍵 鍵識別 鍵 認証アルゴリズム 認証鍵 鍵識別	 → 101 → des-cbc → 16 進数 → 23456789ab → hmac-md5 → 16 進数

	SPI值		100 (16進数)
	暗号アルゴリズム		des-cbc 💌
	暗号鍵	键識別	⊙16進数 ○文字列
SAの設定 (送信田)		键	•••••
	認証アルゴリズム		hmac-md5 💌
	= ग =∓\$74	键識別	●16進数 ○文字列
	認証規	键	•••••
	相手側IPアトレス		
対象バケ	相手側アドレスマ スク		0 (0.0.0.0)
ット (受信用)	自側IPアトレス		
	自側アトレスマス ク		0 (0.0.0.0)
	SPI值		101 (16進数)
	暗号アルゴリズム		des-cbc 💌
	暗号鍵	<mark>键</mark> 識別	⊙16進数 ○文字列
SAの設定 (受信用)		鏈	•••••
	認証アル	ゴリズム	hmac-md5 💌
	ड्याइस २७%	键識別	⊙16進数 ○文字列
	^{認証規} 键		•••••

- 16. [保存] ボタンをクリックします。
- **17. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-shi	

4. [追加] ボタンをクリックします。

「ネットワーク情報(vpn-shi)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度 →0



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

•	鍵交換モード	→手動鍵使用
	相手側エンドポイント	→202.168.1.66
	自側エンドポイント	→202.168.2.66

键态摘开	⊙ 手動鍵使用
ᆕᅕ	相手側エンドポイント 202.168.1.66
	自側エンドポイント 202.168.2.66

- 13. 【保存】ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

•	SAの設定(送信用)	
	SPI值	→ 101
	暗号アルゴリズム	→des-cbc
	暗号鍵	
	鍵識別	→16進数
	鍵	→23456789ab
	認証アルゴリズム	→hmac-md5
	認証鍵	
	鍵識別	→16進数
	鍵	→3456789abc
•	SAの設定(受信用)	
	SPI值	→ 100
	暗号アルゴリズム	→des-cbc
	暗号鍵	
	鍵識別	→16進数
	鍵	→0123456789
	認証アルゴリズム	→hmac-md5
	認証鍵	
	鍵識別	→16進数
	鍵	→ 123456789a

	SPI值		101 (<mark>16進数)</mark>
	暗号アルゴリズム		des-cbc 💌
	暗号键	<mark>键</mark> 識別	●16進数 ○文字列
SAの設定 (送信田)		键	•••••
	認証アル	ゴリズム	hmac-md5 💌
	≡ग≑∓%क	键識別	●16進数 ○文字列
	認証規	键	•••••
	相手側IPアトレス		
対象バケ	相手側アトレスマスク		0 (0.0.0.0)
ット (受信用)	自側IPアトレス		
	自側アFI ク	ノスマス	0 (0.0.0.0)
	SPI值		100 (16進数)
	暗号アル	ゴリズム	des-cbc 💌
	마소 다 수행	键識別	●16進数 ○文字列
SAの設定 (受信用)	喧ち楚	鍵	•••••
	認証アルゴリズム		hmac-md5 💌
	 認証鍵 鍵識別 鍵 	键識別	⊙16進数 ○文字列
		•••••	

- 16. 【保存】ボタンをクリックします。
- **17. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

IPsec機能を使ってIPv4ローカルネットワーク間をIPv6インターネットで結び、自動鍵交換でVPNを構築する場合の設定方法を説明します。

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

● 前提条件

[支社(PPPoE常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス

202.168.1.66/24

:LAN0ポート使用

• 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

:userpass(プロバイダから提示された内容)

- 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
- PPPoE LAN ポート

[本社]

- ローカルネットワーク IPv4 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固定 IPv4 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固定 IPv6 アドレス
- 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



- : 192.168.2.1/24
- 202.168.2.66/24
- : 2001:db8:1111:2::66/64

● 設定条件	
[支社]	
• ネットワーク名	: vpn-hon
● 接続先名	: honsya
• IPsec/IKE区間	: 2001:db8:1111:1::66-2001:db8:1111:2::66
• IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット
[本社]	
 ネットワーク名 	: vpn-shi
● 接続先名	: shisya
• IPsec/IKE区間	: 2001:db8:1111:2::66-2001:db8:1111:1::66
• IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット
[共通]	
 鍵交換タイプ 	:Main Mode 使用
• IPsecプロトコル	esp
• IPsec暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
• IPsec DHグループ	:なし
• IKE 認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
• IKE 暗号アルゴリズム	: des-cbc
• IKE認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768
 塗 ヒント	

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度 →0



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

→ Main Mode 使用
→2001:db8:1111:2::66
→2001:db8:1111:1::66

	⊙ Main Mode使用
鍵交換モ ート	相手側エンドボイ ント 2001:db8:1111:2::66
	自側エンドボイン ト 2001:db8:1111:1::66

- 13. [保存] ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

,	• SA	4の設定	
	暗	号アルゴリズ	ム → des-cbc
	認	証アルゴリズ	ム → hmac-md5
		暗号アルコリ スム	□ aes-cbc-256 □ aes-cbc-192 □ aes-cbc-128 □ 3des-cbc ☑ des-cbc □ null
		記録マルール	

SA	認証アルゴリ ズム	☑hmac-md5 □hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
~	いちか時間		
	SA有X则时间	8 時間 📉	
	SA有効データ 量	0 GByte 💌	

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

 IKE 認証鍵 鍵識別

鍵

→文字列 →abcdefghijkImnopqrstuvwxyz1234567890

SAの設定
 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768 (グループ1)

■IKE情報	■IKE情報		
₩┍═╗═┰ᢓᡈ	鏈識別	○16進数 ⊙文字列	
INERGHUR	鍵	••••••	
IKE認証方式	7	shared	
ボート番号		500	
	暗号アルゴリズ ム	des-cbc 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌	
	DHグループ	modp768(ヴループ1) 💌	
	SA有効時間	24 時間 🖌	

- 19. [保存] ボタンをクリックします。
- 20. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。
本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi

<ネットワーク情	報追加フィールド>
ネットワーク名	vpn-shi

4. [追加] ボタンをクリックします。

「ネットワーク情報(vpn-shi)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度 →0



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

鍵交換モード	→ Main Mode 使用
相手側エンドポイント	→2001:db8:1111:1::66
自側エンドポイント	→2001:db8:1111:2::66
	鍵交換モード 相手側エンドポイント 自側エンドポイント



13. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5

	暗号アルゴリ ズム	☐aes-cbc-256 ☐aes-cbc-192 ☐aes-cbc-128 ☐3des-cbc ☑des-cbc ☐ null	
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □ 認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
	SA有効時間	8 時間 🗸	
	SA有効データ 量	0 GByte 💌	

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

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



- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

接続するたびにIPアドレスが変わる環境でVPNを構築する場合の設定方法を説明します。 IPv4ローカルネットワーク間をIPv6インターネットで結んでIPsecを行います。

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

: 192.168.1.1/24

● 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
- PPPoE ユーザ認証 ID
- PPPoE ユーザ認証パスワード

:userpass(プロバイダから提示された内容)

- PPPoE LAN ポート
- :LAN0ポート使用

:userid(プロバイダから提示された内容)

- [本社]
- ローカルネットワーク IPv4 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固定 IPv4 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固定 IPv6 アドレス
- 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



- : 192.168.2.1/24
- : 202.168.2.66/24
- : 2001:db8:1111:2::66/64

	設定条件	
[3	支社 (Initiator)]	
•	ネットワーク名	: vpn-hon
•	接続先名	: honsya
•	IPsec/IKE区間	:支社-2001:db8:1111:2::66
•	IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット
•	IKE(UDP:500番ポート)のプラ-	イベートアドレス
		:2001:db8:1111:1::66 (インターネットプロバイダから割り当てられた IPv6 アドレス)
•	ESPのプライベートアドレス	:2001:db8:1111:1::66 (インターネットプロバイダから割り当てられた IPv6 アドレス)
[7	本社]	
•	ネットワーク名	: vpn-shi
•	接続先名	: shisya
•	IPsec/IKE区間	:2001:db8:1111:2::66-支社
•	IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット
[;	共通]	
•	鍵交換タイプ	: Aggressive Mode
•	IPsecプロトコル	: esp
•	IPsec 暗号アルゴリズム	: des-cbc
٠	IPsec 認証アルゴリズム	: hmac-md5
•	IPsec DH グループ	:なし
٠	IKE 支社 ID/ID タイプ	:shisya(自装置名)/FQDN
٠	IKE認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
•	IKE 認証方法	: shared
٠	IKE 暗号アルゴリズム	: des-cbc
•	IKE認証アルゴリズム	: hmac-md5
•	IKE DH グループ	: modp768

☆ ヒント

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

♦ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社(Initiator)を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名		vpn-hon

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定
 あて先IPアドレス → 192.168.2.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 → 1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント 自装置識別情報

→Aggresive Mode(Initiator)使用 →2001:db8:1111:2::66

```
→ shisya
```

	⊙ Aggressive Mode(Ir	nitiator)使用
	自側エンドボイン ト	
鍵交換モ ート	相手側エンドポイ ント	2001:db8:1111:2::66
	自装置識別情報	shisya
	IDタイプ	⊙ FQDN O User-FQDN

13. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
	SA有効時間	8 時間 🗸	
	SA有効データ 量	0 GByte 💌	

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

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

■IKE情報		3
ルロヨロミンク語	鏈識別	○16進数 ⊙文字列
INEGGILHE	鍵	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグルーブ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🗸

- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社(Responder)を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0 あて先アドレスマスク →24 (255.255.255.0)
 メトリック値 →1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

鍵交換モード → Aggresive Mode (Responder) 使用 自側エンドポイント → 2001:db8:1111:2::66 → shisya

	⊙ Aggressive Mode(Responder)使用
	自側エンドボイン ト 2001:db8:1111:2::66
鍵交換モ ート	相手側エンドボイ
	相手装置識別情 報
	IDタイプ ● FQDN User-FQDN

13. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
の設 定	PFS時のDHグ ルーブ	使用しない
	SA有効時間	8 時間 🗸
	SA有効データ 量	0 GByte 💌

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

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



- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

IPsec機能を使ってIPv6ローカルネットワーク間をIPv4インターネットで結び、自動鍵交換でVPNを構築する場合の設定方法を説明します。

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

: 192.168.1.1/24

: 202.168.1.66/24

:LAN0ポート使用

:userid(プロバイダから提示された内容)

:userpass(プロバイダから提示された内容)

● 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
- 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
- PPPoE ユーザ認証 ID
- PPPoEユーザ認証パスワード
- PPPoE LAN ポート

[本社]

- ローカルネットワークIPv4アドレス
- ローカルネットワーク IPv6 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固定 IPv4 アドレス
- 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



- : 192.168.2.1/24
 - : 2001:db8:1111:2::1/64
 - 202.168.2.66/24

● 設定条件			
[支社]			
 ネットワーク名 	: vpn-hon		
● 接続先名	: honsya		
• IPsec/IKE区間	: 202.168.1.66-202.168.2.66		
• IPsec 対象範囲	:IPsec相手情報を使用するすべてのパケット		
[本社]			
 ネットワーク名 	: vpn-shi		
• 接続先名	: shisya		
• IPsec/IKE区間	: 202.168.2.66-202.168.1.66		
• IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット		
[共通]			
 鍵交換タイプ 	:Main Mode 使用		
• IPsecプロトコル	: esp		
• IPsec 暗号アルゴリズム	: des-cbc		
• IPsec認証アルゴリズム	: hmac-md5		
● IPsec DHグループ	:なし		
• IKE認証鍵	:abcdefghijkImnopqrstuvwxyz1234567890(文字列)		
• IKE 認証方法	: shared		
• IKE 暗号アルゴリズム	: des-cbc		
• IKE 認証アルゴリズム	: hmac-md5		
● IKE DH グループ	: modp768		
送上ント			

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - IPv6

→使用する

■IPv6基本情報		
IPv6	IPv6 ○使用しない ◎使用する	

- 7. [保存] ボタンをクリックします。
- **8.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。
- 9. 以下の項目を指定します。
 - ネットワーク あて先プレフィックス/プレフィックス長
 - メトリック値

→ネットワーク指定 →2001:db8:1111:2::/64

3

→1

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>			
ネットワーク	 デフォルトルート ネットワーク指定 あて先ブレフィ ックス/ブレフ ィックス長 2001:db8:1111:2:: 		
メトリック値	1 🗸		

- 10. [追加] ボタンをクリックします。
- **11. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

● 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>				
接続先名	honsya			
接続先種別	 ATM接続 マ可用線接続 ・ 通常接続			

機種により、接続先種別の表示が上記の画面とは異なります。

13. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

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

	◎ Main Mode使用
鍵交換モ −ト	相手側エンドボイ 202.168.2.66
	自側エンドポイン 202.168.1.66

15. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

17. 以下の項目を指定します。

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

IPs	■IPsec情報(自動鍵)		
	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。)	
対象 バケ		スパレマイントレンバマスシビット形式GOC(GIPV6)トレ スパリレフィックス長形式で入力してください。	
אש	相手側IPアト レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。)	
		※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/ブレフィックス長形式で入力してください。	
	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
SA	認証アルゴリ ズム	▼hmac-md5 □hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
	SA有効時間	8 時間 🗸	
	SA有効データ 量	0 GByte 💌	

18. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

•	IKE認証鍵	
	鍵識別	→文字列
	JUE 1997	→abcdefghijkImnopqrstuvwxyz1234567890
•	SAの 設定	
	暗号アルゴリズム	→des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-md5
	DHグループ	→modp768(グループ1)

■IKE情報		3
	鏈識別	○16進数 ⊙文字列
INE BOUT DE	鏈	••••••
IKE認証方式		shared
ポート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🖌

- 21. [保存] ボタンをクリックします。
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi

- 【追加】ボタンをクリックします。
 「ネットワーク情報(vpn-shi)」ページが表示されます。
- 5. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - IPv6 →使用する

■IPv6基本情報	3
IPv6 ○使用しない ⊙使用する	

- 7. [保存] ボタンをクリックします。
- IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。
 「IPv6 スタティック経路情報」が表示されます。

- ネットワーク あて先プレフィックス/プレフィックス長
- メトリック値

→ネットワーク指定 →2001:db8:1111:1::/64

→1

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>			
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先ブレフィ ックス/ブレフ ィックス長 2001:db8:1111:1 64 		
メトリック値	1 💌		

10. [追加] ボタンをクリックします。

11. 「接続先情報」をクリックします。 「接続先情報」が表示されます。

12. 以下の項目を指定します。

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



機種により、接続先種別の表示が上記の画面とは異なります。

13. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

	⊙ Main Mode使用
键交換モ →ト	相手側エンドボイント 202.168.1.66
	自側エンドポイン ト 202.168.2.66

15. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

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



- 18. [保存] ボタンをクリックします。
- **19.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

•	IKE 認証 鍵識別 鍵	鍵		→文字列 →abcdefghijklmnopqrstuvwxyz1234567890	
•	 SAの設定 暗号アルゴリズム 認証(ハッシュ)アルゴリズム DHグループ 		リズム	→des-cbc →hmac-md5 →modp768(グループ1)	
	■IKE情報				
	建識別 (2015) (201		◯16進数	☆●文字列	
	N⊏ni6all₩E	键	•••••	••••••	
IKE認証方式 shared		shared			

IKE認証方式	t	shared
ボート番号		500
	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🖌

- 21. [保存] ボタンをクリックします。
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

接続するたびにIPアドレスが変わる環境でVPNを構築する場合の設定方法を説明します。 IPv6ローカルネットワーク間をIPv4インターネットで結んでIPsecを行います。 ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間の

● 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
- ローカルネットワーク IPv6 アドレス
- PPPoEユーザ認証ID

PPPoE LAN ポート

- PPPoEユーザ認証パスワード
- : 192.168.1.1/24 : 2001:db8:1111:1::1/64
- : userid(プロバイダから提示された内容)
- : userpass(プロバイダから提示された内容)

: 192.168.2.1/24

: 202.168.2.66/24

: 2001:db8:1111:2::1/64

:LAN0 ポート使用

- [本社]
- ローカルネットワーク IPv4 アドレス
- ローカルネットワーク IPv6 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固定 IPv4 アドレス

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。

インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス: 202.168.2.65



● 設定条件	
【支社(Initiator)】	
 ネットワーク名 	: vpn-hon
• 接続先名	: honsya
• IPsec/IKE区間	:支社-202.168.2.66
• IPsec 対象範囲	:IPsec相手情報を使用するすべてのパケット
• IKE(UDP:500番ポート)のプライベートアドL	
	: 192.168.1.1
• ESPのプライベートアドレス	: 192.168.1.1
[本社]	
 ネットワーク名 	: vpn-shi
• 接続先名	: shisya
• IPsec/IKE区間	:202.168.2.66-支社
• IPsec 対象範囲	:IPsec相手情報を使用するすべてのパケット
[共通]	
 鍵交換タイプ 	: Aggressive Mode
• IPsecプロトコル	: esp
• IPsec暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
・ IPsec DHグループ	:なし
• IKE 支社 ID/ID タイプ	:shisya(自装置名)/FQDN
• IKE 認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: des-cbc
• IKE認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768

☆ヒント------

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

♦ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社(Initiator)を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。

→指定しない

→isakmp

→udp

4. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

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

<静的NAT情報入力フィールド>				
プライベート	IPアド レス	192.168.1.1		
IP情報 ポート 番号		isakmp · (番号指定: 7その他 を選択時の み有効です)		
グローバル	IPアド レス			
IP忭青報	ボート 番号	isakmp V(番号指定: 7その他 ~ を選択時の み有効です)		
プロトコル		udp ✓(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

•	プライベート IP 情報	
	IPアドレス	→ 192.168.1.1
	ポート番号	→すべて
•	グローバル IP 情報	
	IPアドレス	→指定しない
	ポート番号	→すべて

- プロトコル → esp
- 画面上部の「相手情報」をクリックします。
 「相手情報」ページが表示されます。

10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

- 11. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

13. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

14. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 15. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0
 あて先アドレスマスク → 24 (255.255.255.0)

→0

- メトリック値 →1
- 優先度

<スタティック経路情報入力フィールド>				
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先IPアドレス 192.168.2.0 あて先アドレスマスク 24 (255.255.255.0) 			
メトリック値				
優先度	0			

16. [追加] ボタンをクリックします。

17. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6基本情報」が表示されます。

- 18. 以下の項目を指定します。
 - IPv6

→使用する

■IPv6基本情報	3
IPv6 ○使用しない ◎使用する	

- 19. [保存] ボタンをクリックします。
- **20.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。

- ネットワーク あて先プレフィックス/プレフィックス長
- メトリック値

→ネットワーク指定 →2001:db8:1111:2::/64

→1



- 22. [追加] ボタンをクリックします。
- **23. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

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



機種により、接続先種別の表示が上記の画面とは異なります。

25. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

26. 以下の項目を指定します。

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



27. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

•	対象パケット	
	自側 IP アドレス/マスク	→IPv6すべて
	相手側IPアドレス/マスク	→IPv6すべて

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

■IPsec情報(自動鍵)		
自側IPアドレ ス/マスク オタ パケ パケ オタ オー オー		IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
אר אר	相手側IPアド レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
の設 定	PFS時のDHグ ループ	使用しない
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 🖌

- 30. [保存] ボタンをクリックします。
- **31.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

DHグループ

٠	IKE認証鍵	
	鍵識別	→文字列
	鍵	→abcdefghijklmnopqrstuvwxyz1234567890
•	SAの 設定	
	暗号アルゴリズム	→des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-md5

→hmac-md5 →modp768(グループ1)

■IKE情報	3	
1/ 드릴 문지 수정	键識別	○16進数 ⊙文字列
IKE認証規	鏈	••••••
IKE認証方式	ς.	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🗸

- 33. [保存] ボタンをクリックします。
- **34. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社(Responder)を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。



4. [追加]ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

IP 関連の設定項目の「スタティック経路情報」をクリックします。
 「スタティック経路情報」が表示されます。

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

- 8. [追加] ボタンをクリックします。
- 9. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 10. 以下の項目を指定します。
 - IPv6

→使用する

■IPv6基本情報	
IPv6 ○使用しない ●使用する	

- 11. 【保存】ボタンをクリックします。
- **12.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。
- 13. 以下の項目を指定します。
 - ネットワーク あて先プレフィックス/プレフィックス長
 - メトリック値

→ネットワーク指定 →2001:db8:1111:1::/64

	→	1

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>			
ネットワーク	 デフォルトルート ネットワーク指定 あて先プレフィ ックス/プレフ ィックス長 2001:db8:1111:1:: 		
メトリック値	1 💌		

- 14. [追加] ボタンをクリックします。
- **15. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>				
接続先名	shisya			
接続先種 別	 ATM接続 VCI 専用線接続 通常接続 (使用インタフェース WANI ♥ 論理リンクにバンドルする (使用インタフェー ス ボンドル先 選択できる定義がありません ♥ ISDN接続 通常接続 (使用インタフェース すべて ♥			

機種により、接続先種別の表示が上記の画面とは異なります。

17. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

18. 以下の項目を指定します。

 鍵交換モード 自側エンドポイント 相手装置識別情報

→Aggresive Mode(Responder)使用 →202.168.2.66

→ shisya

	⊙ Aggressive Mode(R	esponder)使用
	自側エンドボイン ト	202.168.2.66
鍵交換モ ート	相手側エンドポイ ント	
	相手装置識別情 報	shisya
	IDタイプ	⊙ FQDN O User-FQDN

19. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

21. 以下の項目を指定します。

- 対象パケット 自側IPアドレス/マスク →IPv6すべて 相手側IPアドレス/マスク →IPv6すべて
 SAの設定
 - 暗号アルゴリズム → des-cbc 認証アルゴリズム → hmac-md5

■IPsec情報(自動鍵)				
対象	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。		
ット	相手側IPアド レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。		
	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ☑ des-cbc □ null		
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □ 認証なし		
の設 定	PFS時のDHグ ループ	使用しない		
	SA有効時間	8 時間 💙		
	SA有効データ 量	0 GByte 💌		

22. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

•	 IKE 認証 鍵識別 鍵 	鍵	→文字列 →abcdefghijkImnopqrstuvwxyz1234567890
•	・ SAの設定 暗号アル 認証(ハ DHグル・	官 ,ゴリズム 、ッシュ)アルゴ ^ー ープ	→des-cbc リズム →hmac-md5 →modp768(グループ1)
ſ	IKE情報		3
	ルト記記録	鏈識別	◎16進数 ◎ 文字列
	IN E DIG OLL HE	鍵	••••••
	IKE認証方式 sh		shared
	<mark>ボート番号</mark> 50		500
		暗号アルコリズ ム	des-cbc 💌
	SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
		DHグループ	modp768(ヴループ1) 💌
		SA有効時間	24 時間 🖌

- 25. [保存] ボタンをクリックします。
- **26. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

IPsec機能を使ってIPv6で自動鍵交換でVPNを構築する場合の設定方法を説明します。

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

● 前提条件

[支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワーク IPv6 アドレス : 2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス

: 202.168.1.66/24

- インターネットプロバイダから割り当てられた固定 IPv6 アドレス
 - : 2001:db8:1111:1::66/64
- PPPoEユーザ認証ID :userid(プロバイダから提示された内容) :userpass(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

PPPoE LAN ポート

:LAN0ポート使用

[本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24 • ローカルネットワーク IPv6 アドレス : 2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24 • インターネットプロバイダから割り当てられた固定 IPv6 アドレス : 2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス:202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートのIPv6アドレス:2001:db8:1111:2::65



● 設定条件

[支社]

- ネットワーク名
- 接続先名
- IPsec/IKE 区間
- IPsec対象範囲

[本社]

- ネットワーク名 .
- 接続先名
- IPsec/IKE 区間
- IPsec 対象範囲

[共通]

- 鍵交換タイプ
- IPsecプロトコル
- IPsec 暗号アルゴリズム
- IPsec認証アルゴリズム
- IPsec DH グループ
- ٠ IKE認証鍵
- IKE 認証方法
- IKE 暗号アルゴリズム •
- IKE 認証アルゴリズム
- IKE DH グループ ٠

- : vpn-shi
- : shisya
- : 2001:db8:1111:2::66-2001:db8:1111:1::66
- : IPsec 相手情報を使用するすべてのパケット
- : Main Mode 使用
- : esp
- : des-cbc
- : hmac-md5
- :なし
 - : abcdefghijklmnopqrstuvwxyz1234567890(文字列)
- : shared
 - : des-cbc

501

- : hmac-md5
- : modp768

· 🏠 ヒント 🗕 🗕

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名

→vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名		vpn-hon

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - IPv6

→使用する

3

■IPv6基本情報 IPv6 ○使用しない ◎使用する

- 7. [保存] ボタンをクリックします。
- **8.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。

- ネットワーク あて先プレフィックス/プレフィックス長
- メトリック値

→ネットワーク指定 →2001:db8:1111:4::/64

→1

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>			
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先ブレフィ ックス/ブレフ ィックス長 2001:db8:1111:4:: 		
メトリック値	1 💌		

- 10. [追加] ボタンをクリックします。
- **11. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 12. 以下の項目を指定します。
 - 接続先名 → honsya
 - 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

13. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

鍵交換モード → Main Mode使用
 相手側エンドポイント → 2001:db8:1111:2::66
 自側エンドポイント → 2001:db8:1111:1::66

	⊙ Main Mode使用
鍵交換モ ート	相手側エンドボイ ント 2001:db8:1111:2::66
	自側エンドボイン ト 2001:db8:1111:1::66

15. [保存] ボタンをクリックします。

16. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

- 対象パケット 自側IPアドレス/マスク →IPv6すべて 相手側IPアドレス/マスク →IPv6すべて
- SAの設定
 暗号アルゴリズム → des-cbc
 認証アルゴリズム → hmac-md5

■IPsec情報(自動鍵)			
対象 バケ ット	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。	
	相手側IPアド レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。	
SA の設 定	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし	
	PFS時のDHグ ループ	使用しない	
	SA有効時間	8 時間 🗸	
	SA有効データ 量	0 GByte 🛩	

- 18. [保存] ボタンをクリックします。
- **19.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。
| • | IKE認証鍵 | |
|---|-----------|---|
| | 鍵識別
鍵 | →文字列
→abcdefghijklmnopqrstuvwxyz1234567890 |
| • | SAの
設定 | |
| | 暗号アルゴリズム | →des-cbc |

DHグループ		→modp768(グループ1)	
■IKE情報		3	
	<mark>键</mark> 識別	○16進数 ⊙文字列	
IKE認証規	鏈	••••••	
IKE認証方式		shared	
ポート番号		500	
暗号アルコリズ ム		des-cbc 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌	
	DHグループ	modp768(ヴループ1) 🗸	
	SA有効時間	24 時間 💙	

認証(ハッシュ)アルゴリズム →hmac-md5

- 21. [保存] ボタンをクリックします。
- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi



4. [追加]ボタンをクリックします。

「ネットワーク情報(vpn-shi)」ページが表示されます。

5. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - IPv6 →使用する

■IPv6基本情報	3
IPv6 ○使用しない ◎使用する	

- 7. [保存] ボタンをクリックします。
- 8. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6スタティック経路情報」が表示されます。

- 9. 以下の項目を指定します。
 - ネットワーク あて先プレフィックス/プレフィックス長
 - メトリック値

→ネットワーク指定 →2001:db8:1111:3::/64

→1



- 10. [追加] ボタンをクリックします。
- 11. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

13. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

•	鍵交換モード	→ Main Mode 使用
	相手側エンドポイント	→2001:db8:1111:1::66
	自側エンドポイント	→2001:db8:1111:2::66



15. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

17. 以下の項目を指定します。

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

■IPsec情報(自動鍵)		
対象	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしく(はIPv6アドレ ス/プレフィックス長形式で入力してください。
ット	相手側IPアト レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ☑ des-cbc □ null
SA	認証アルゴリ ズム	▼hmac-md5 □hmac-sha1 □認証なし
の設 定	PFS時のDHグ ルーブ	使用しない
	SA有効時間	8 時間 🗸
	SA有効データ 量	0 GByte 💌

- 18. [保存] ボタンをクリックします。
- **19.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

DHグループ

٠	IKE 認証鍵	
	鍵識別	→文字列
	鍵	→abcdefghijklmnopqrstuvwxyz1234567890
•	SAの 設定	
	暗号アルゴリズム	→des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-md5

→modp768 (グループ1)

■IKE情報		3	
	<mark>键</mark> 識別	○16進数 ⊙文字列	
IKE認証規	鏈	••••••	
IKE認証方式	C I	shared	
ボート番号		500	
	暗号アルゴリズ ム	des-cbc 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸	
	DHグループ	modp768(ヴループ1) 💌	
	SA有効時間	24 時間 🗸	

- 21. [保存] ボタンをクリックします。
- 22. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

接続するたびにIPv6アドレスが変わる環境でVPNを構築する場合の設定方法を説明します。 ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN終端装置として本装置が接続されていることを前提とします。

: 2001:db8:1111:3::1/64

:LAN0ポート使用

:userid(プロバイダから提示された内容)

:userpass(プロバイダから提示された内容)

● 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 .
- PPPoEユーザ認証ID •
- PPPoEユーザ認証パスワード •
- PPPoE LAN ポート

[本社]

- ローカルネットワークIPv4アドレス
- ローカルネットワーク IPv6 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固定 IPv4 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固定 IPv6 アドレス ٠
- 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 .
 - h 192 168 2 2 ファイルサーバ www ーバ 192.168.2.4 2001:db8:1111:4::2 192.168.2.3 2001:db8:1111:4::3 2001:db8:1111:4::4 ネットワークアドレス 本社 I AN1 192.168.2.1 192,168,2.0/24 2001:db8:1111:4::/64 2001:db8:1111:4::1 202.168.2.66 LAN0 2001:db8:1111:2::66 ネットワークアドレス 202.168.2.0/24 2001:db8:1111:2::/64 ルータ 202 168 2 65 2001:db8:1111:2::65 internet トンネル ADSLモデム PPPoE 192.168.1.1 LAN1 2001:db8:1111:3::1 ネットワークアドレス 支社 192.168.1.0/24 2001:db8:1111:3::/64 192.168.1.2 192.168.1.3 192.168.1.4 2001:db8:1111:3::2 2001:db8:1111:3::3 2001:db8:1111:3::4

- : 192.168.2.1/24
- : 2001:db8:1111:4::1/64
- : 202.168.2.66/24
- : 2001:db8:1111:2::66/64

● 設定条件				
【支社(Initiator)】				
 ネットワーク名 	: vpn-hon			
● 接続先名	: honsya			
● IPsec/IKE区間	:支社-2001:db8:1111:2::66			
● IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット			
• IKE(UDP:500番ポート)の	プライベートアドレス			
	: 2001:db8:1111:1::66			
	(インターネットプロバイダから割り当てられた IPv6 アドレス)			
• ESPのプライベートアドレス	: 2001:db8:1111:1::66			
	(インターネットプロバイダから割り当てられた IPv6 アドレス)			
[本社]				
 ネットワーク名 	: vpn-shi			
● 接続先名	: shisya			
● IPsec/IKE区間	:2001:db8:1111:2::66-支社			
● IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット			
[共通]				
 鍵交換タイプ 	: Aggressive Mode			
• IPsecプロトコル	: esp			
● IPsec暗号アルゴリズム	: des-cbc			
● IPsec認証アルゴリズム	: hmac-md5			
● IPsec DHグループ	:なし			
● IKE 支社 ID/ID タイプ	:shisya(自装置名)/FQDN			
● IKE 認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)			
● IKE 認証方法	: shared			
● IKE 暗号アルゴリズム	: des-cbc			
● IKE 認証アルゴリズム	: hmac-md5			
● IKE DH グループ	: modp768			

☆ ヒント ──

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

♦ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社(Initiator)を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 → 1
 - メトリック値 →1
 優先度 →0



- 8. [追加] ボタンをクリックします。
- 9. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 10. 以下の項目を指定します。
 - IPv6

→使用する

512

■IPv6基本情報 IPv6 ○使用しない ●使用する

- 11. [保存] ボタンをクリックします。
- **12.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。

3

- ネットワーク あて先プレフィックス/プレフィックス長
- メトリック値

→ネットワーク指定 →2001:db8:1111:4::/64

→1

	<ipv6人メディック#全路1月¥q人ノリフィールトン< th=""></ipv6人メディック#全路1月¥q人ノリフィールトン<>		
	○デフォルトルート		
ネットワーク	 マットワーク指定 あて先プレフィ 		
	ックス/ブレフ ィックス長		
メトリック値	1 🗸		

14. [追加] ボタンをクリックします。

15. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

16. 以下の項目を指定します。

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



機種により、接続先種別の表示が上記の画面とは異なります。

17. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

18. 以下の項目を指定します。

鍵交換モード → Aggressive Mode (Initiator)使用 相手側エンドポイント → 2001:db8:1111:2::66 → shisya

	Aggressive Mode(Res	ponder)使用
	自側エンドボイン ト	101:db8:1111:2::66
鍵交換モ ート	相手側エンドボイント	
	相手装置識別情 報	isya
	IDタイプ 🧿	FQDN OUser-FQDN

- 19. [保存] ボタンをクリックします。
- **20.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

21. 以下の項目を指定します。

•	対象パケット	
	自側 IP アドレス/マスク	→IPv6すべて
	相手側IPアドレス/マスク	→IPv6すべて
•	SAの 設定	
	暗号アルゴリズム	→des-cbc
	認証アルゴリズム	→hmac-md5



- 22. [保存] ボタンをクリックします。
- **23.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE情報」が表示されます。

以下の項目を指定します。 24.

DHグループ

•	IKE認証鍵	
	鍵識別	→文字列
	鍵	→abcdefghijklmnopqrstuvwxyz1234567890
•	SAの 設定	
	暗号アルゴリズム	→des-cbc

認証(ハッシュ)アルゴリズム →hmac-md5 →modp768 (グループ1)

■IKE情報		3
	键識別	○16進数 ⊙文字列
IKE認証要	键	••••••
IKE認証方式		shared
ポート番号		500
	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🗸

- [保存] ボタンをクリックします。 25.
- 26. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

本社(Responder)を設定する

- 1. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- 2. 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。
- 以下の項目を指定します。 3.



[追加] ボタンをクリックします。 4.

「ネットワーク情報 (vpn-shi)」ページが表示されます。

「IP関連」をクリックします。 5.

IP関連の設定項目と「IP基本情報」が表示されます。

IP関連の設定項目の「スタティック経路情報」をクリックします。 6. 「スタティック経路情報」が表示されます。

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

- <
 <tr>
 <スタティック経路情報入力フィールド>

 デフォルトルート

 ・デフォルトルート

 ・ネットワーク指定

 あて先IPアドレス

 192.168.1.0

 あて先アドレスマスク

 24 @255.255.255.0)

 メトリック値

 優先度
- 8. [追加] ボタンをクリックします。
- 9. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 10. 以下の項目を指定します。
 - IPv6

→使用する

■IPv6基本情報	
IPv6 ○使用しない ●使用する	

- 11. 【保存】ボタンをクリックします。
- **12.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。
- 13. 以下の項目を指定します。
 - ネットワーク あて先プレフィックス/プレフィックス長
 - メトリック値

→ネットワーク指定 →2001:db8:1111:3::/64

→1

	<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>
ネットワーク	 デフォルトルート ネットワーク指定 あて先ブレフィ ックス/ブレフ ィックス長 2001:db8:1111:3:: 64
メトリック値	1 💌

- 14. [追加] ボタンをクリックします。
- **15. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>		
接続先名	shisya	
接続先種別	 ATM接続 VCI 専用線接続 通常接続 (使用インタフェース WAN1 *) 論理リンクにバンドルする (使用インタフェー ス バンドルする (使用インタフェー	

機種により、接続先種別の表示が上記の画面とは異なります。

17. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

18. 以下の項目を指定します。

 鍵交換モード 自側エンドポイント

→Aggresive Mode(Responder)使用

→2001:db8:1111:2::66 →shisya



19. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

21. 以下の項目を指定します。

- 対象パケット 自側IPアドレス/マスク →IPv6すべて 相手側IPアドレス/マスク →IPv6すべて
 SAの設定
 - 暗号アルゴリズム → des-cbc 認証アルゴリズム → hmac-md5

■IPsec情報(自動鍵)		
対象	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/ブレフィックス長形式で入力してください。
ット	相手側IPアド レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ☑ des-cbc □ null
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
の設 定	PFS時のDHグ ループ	使用しない
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 💌

22. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

24. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 鍵 		→文字列 →abcdefghijkImnopqrstuvwxyz123456789	
 SAの設定 暗号アルゴリズム 認証(ハッシュ)アルゴ! DHグループ 		→des-cbc リズム →hmac-md5 →modp768(グループ1)	
■IKE情報			
ルロ刻計論	鍵識別	○16進数	
	键	•••••	
IKE認証方式	ς.	shared	
ポート番号		500	
	暗号アルコリズ ム	des-cbc 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌	
OFOTEER			
UNU DEC	DHグループ	modp768グループ1) 💌	

- 25. [保存] ボタンをクリックします。
- **26. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.14.8 IPv4 over IPv4 で1つの IKE セッションに複数の IPsec トンネル構成での VPN(自動鍵交換)

適用機種 全機種

IPsec機能を使って複数のネットワークにそれぞれの IPsec SA を作成する環境を構築する場合を例に説明します (自動鍵交換の固定 IP アドレスを使用した構成です)。

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

● 前提条件

[支社(PPPoE 常時接続)]

- ローカルネットワークIPアドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス

: 202.168.1.66/24

:LAN0ポート使用

- PPPoEユーザ認証ID
 userid (プロバイダから提示された内容)
- PPPoEユーザ認証パスワード
 userpass(プロバイダから提示された内容)
- PPPoE LANポート
- [本社]
- ローカルネットワークIPアドレス1 : LAN0 ポート使用
 ローカルネットワークIPアドレス2 : 192.168.3.1/24
 インターネットプロバイダから割り当てられた固定のIPアドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス : 202.168.2.65

● 設定条件

[支社]

• IPsec/IKE区間 : 202.168.1.66 - 202.168.2.66 • IPsec対象範囲(1) : any - 192.168.2.0/24 (マルチルーティングにも定義する) • IPsec対象範囲(2) : any - 192.168.3.0/24 [本社] • IPsec/IKE区間 : 202.168.2.66 - 202.168.1.66 • IPsec対象範囲(1) : 192.168.2.0/24 - any (マルチルーティングにも定義する) • IPsec 対象範囲(2) : 192.168.3.0/24 - any [共通] : Main Mode 使用 • IPsecプトロコル : esp • IPsec 暗号アルゴリズム : des-cbc IPsec PFS 時の DH グループ :なし • IKE 共有鍵 :abcdefghijklmnopqrstuvwxyz1234567890(文字列) • IKE 認証方式 : shared (事前共有鍵方式) • IKE 暗号アルゴリズム : des-cbc • IKE 認証 (ハッシュ) アルゴリズム : hmac-md5 IKE DH グループ :modp768 (グループ1)



上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

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

- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

- 10. 以下の項目を指定します。
 - 接続先名
 - 接続先種別

→IPsec/IKE 接続

→ honsya



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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



13. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

● 対象パケット	
相手側IPアドレス/マスク	→指定する
	→ 192.168.2.0/24

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

IPs	■IPsec情報(自動鍵)			
対象	自側IPアドレ ス/マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/ブレフィックス長形式で入力してください。		
ット	相手側IPアド レス/マスク	指定する 「指定する」を選択時のみ有効です。) 192.168.2.0 ※IPv4アドレス/マスクビット形式もしく(はIPv6アドレ ス/プレフィックス長形式で入力してください。		
	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ☑ des-cbc □ null		
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし		
の設 定	PFS時のDHグ ルーブ	使用しない		
	SA有効時間	8 時間 🗸		
	SA有効データ 量	0 GByte 💌		

- 16. 【保存】ボタンをクリックします。
- **17.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

- IKE 認証鍵 鍵識別 →文字列 鍵 → abcdefghijkImnopqrstuvwxyz1234567890
 SAの設定
 暗日マルブレブ () 」 は a c a base
- 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768(グループ1)

■IKE情報		3
	鏈識別	○16進数 ⊙文字列
IKE認証要	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🗸

- 19. [保存] ボタンをクリックします。
- **20.** IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。 「マルチルーティング情報」が表示されます。
- 21. 以下の項目を指定します。
 - あて先情報
 IPアドレス
 アドレスマスク

→ 192.168.2.0 → 24 (255.255.255.0)

	IPアドレ ス	192.168.2.0
あて先 情報	アドレス マスク	24 (255.255.255.0) 💌
	ボート番 号	

- **22. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。
- **23. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- →honsya2
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

25. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

26. 以下の項目を指定します。

- 鍵交換モード 接続先名
- → IKE は他の接続先情報を使用 → honsya

鍵交換モ	● IKEは他の接続先情報を使用
	接続先名 honsya 💌

- 27. [保存] ボタンをクリックします。
- **28.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec情報」が表示されます。

- 対象パケット 相手側IPアドレス/マスク →指定する → 192.168.3.0/24
- SAの設定
 暗号アルゴリズム → des-cbc
 認証アルゴリズム → hmac-md5



- 30. [保存] ボタンをクリックします。
- **31. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社の IPsec/IKE を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-shi	

4. [追加]ボタンをクリックします。

「ネットワーク情報(vpn-shi)」ページが表示されます。

「IP 関連」をクリックします。
 IP 関連の設定項目と「IP 基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度



→0

- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

10. 以下の項目を指定します。

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



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

- 12. 以下の項目を指定します。
 - 鍵交換モード → Main Mode使用 相手側エンドポイント → 202.168.1.66
 自側エンドポイント → 202.168.2.66

	⊙ Main Mode使用	
鍵交換モ ート	相手側エンドポイ ント 自側エンドポイン ト 202.168.2.66	

- 13. [保存] ボタンをクリックします。
- **14.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

- 対象パケット 自側IPアドレス/マスク →指定する → 192.168.2.0/24
- SAの設定
 暗号アルゴリズム → des-cbc
 認証アルゴリズム → hmac-md5



16. 【保存】ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 →文字列 鍵 → abcdefghijkImnopqrstuvwxyz1234567890
 SAの設定 暗号アルゴリズム → des-cbc 認証 (ハッシュ)アルゴリズム → hmac-md5 DH グループ → modp768 (グループ1)

IKE情報		<u>13</u>
	<mark>键</mark> 識別	○16進数 ⊙文字列
IKE認証題	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
<mark>SAの設定</mark>	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(ヴループ1) 🔽
	SA有効時間	24 時間 🛩

19. [保存] ボタンをクリックします。

20. IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。

「マルチルーティング情報」が表示されます。

21. 以下の項目を指定します。

送信元情報
 IPアドレス
 アドレスマスク

→ 192.168.2.0 → 24 (255.255.255.0)

	IPアドレ ス	192.168.2.0
送信元 情報	アドレス マスク	24 (255.255.255.0)
	ポート番 号	

- 22. [追加] ボタンをクリックします。
- **23. 「接続先情報」をクリックします。** 「接続先情報」が表示されます。
- 24. 以下の項目を指定します。
 - 接続先名 → shisya2
 - 接続先種別
- →IPsec/IKE 接続

<接続先情報追加フィールド>			
接続先名	sgusta2		
接続先種別	 ATM接続 VCI 専用線接続 使用インタフェース WANI × 論理リンクにバンドルする 使用インタフェー ス バンドル先 選択できる定義がありません × ISDN接続 通常接続 使用インタフェー		

機種により、接続先種別の表示が上記の画面とは異なります。

25. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

26. 以下の項目を指定します。

鍵交換モード → IKE は他の接続先情報を使用 接続先名 → shisya

鍵交換モ ート

● IKEは他の接続先情報を使用

接続先名 shisya 💟

- 27. [保存] ボタンをクリックします。
- **28.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec情報」が表示されます。

29. 以下の項目を指定します。

- 対象パケット 自側 IP アドレス/マスク →指定する → 192.168.3.0/24
- SAの設定
 暗号アルゴリズム → des-cbc
 認証アルゴリズム → hmac-md5

	IPs	IPsec情報(自動鍵)	
ţ	対象	自側IPアドレ ス/マスク	指定する 「指定する"を選択時のみ有効です。) 192.168.3.0 ※IPv4アドレス/マスクビット形式もしく(JIPv6アドレ ス/ブレフィックス長形式で入力してください。
	/ 1) ット	相手側IPアド レス/マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしく(はIPv6アドレ ス/プレフィックス長形式で入力してください。
		暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
	SA	A RATIONAL Contraction A Representation Representatio Representation Representation Representa	☑ hmac-md5 □ hmac-sha1 □認証なし
	の設 定	PFS時のDHグ ループ	使用しない
1		SA有効時間	8 時間 💙
		SA有効データ 量	0 GByte 🗸

- 30. [保存] ボタンをクリックします。
- **31. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.14.9 IPsec 機能と他機能との併用

```
適用機種 全機種
```

IPsec 機能と他機能を併用する場合のいくつかの設定例を、以下に説明します。

ここでは、「1.14 複数の事業所 LAN を VPN(IPsec)で接続する」(P.145)の設定が行われていることを前提とします。

- IPsec変換前のマルチNAT / IPフィルタリング / TOS 値書き換え機能
- IPsec変換前のシェーピング機能と帯域制御(WFQ)機能
- IPsec 変換前の MSS 書換え機能
- IPsec変換前のMTU分割機能
- 接続先監視機能
- IKE セッション監視機能
- 動的経路(RIP)機能



- 以下の機能については、IPv6アドレスで使用することはできません。
- IPsec変換前のマルチ NAT 機能
- IKE セッション監視機能

IPsec 変換前のマルチ NAT / IP フィルタリング / TOS 値書き換え機能との併用例

● 設定条件

[支社]

•	NAT の使用	:マルチ NAT を使用する
	グローバルアドレス	: 192.168.1.1
	アドレス個数	: 1
	アドレス割当てタイマ	:5分
•	IPフィルタリング	:支社 - 本社間の telnet / ftp 通信以外遮断
•	TOS値書き換え	:ftp通信を0xa0に変換

[本社]

- IPフィルタリング :支社 本社間の telnet / ftp 通信以外遮断
- TOS 値書き換え
 ttp 通信を 0xa0 に変換

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- **1. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名 → ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

【追加】ボタンをクリックします。 「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

- プロトコル → tcp
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス → 192.168.2.0
 アドレスマスク → 24 (255.255.255.0)
- QoS →指定なし

■IP定義	■IP定義情報 []	
ブロトコル		tcp ▼ (番号指定: ^{(*} その他 [*] を選択時のみ有効です)
送信元情	IPアドレス	192.168.1.0
報	アドレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	192.168.2.0
報	アドレスマ スク	24 (255.255.255.0)
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

8. 以下の項目を指定します。

- ・ 送信元ポート番号 →指定しない
- あて先ポート番号 →21 (ftpのポート番号)、23 (telnetのポート番号)
- TCP接続要求 →対象

■TCP定義情報	3
送信元ボート番号	
あて先ポート番号	21,23
TCP接続要求	●対象○対象外

9. [保存] ボタンをクリックします。

10. 手順1.~9.を参考に、以下の項目を指定します。

「ACL情報」	
• 定義名	→ACL1
「ACL定義情報(ACL1)」-「IP定	義情報」
• プロトコル	→tcp
 送信元情報 IPアドレス アドレスマスク 	→ 192.168.2.0 → 24 (255.255.255.0)
 あて先情報 IPアドレス アドレスマスク 	→ 192.168.1.0 → 24 (255.255.255.0)
• QoS	→指定なし
「ACL定義情報(ACL1)」-「TCP」	定義情報」
● 送信元ポート番号	→21(ftpのポート番号)、23(telnetのポート番号)
• あて先ポート番号	→指定しない
 TCP 接続要求 	→対象外

11. 手順1.~9.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ACL2
٢A	ACL定義情報(ACL2)」-「IP定義	情報」
•	プロトコル	→すべて
•	送信元情報 IPアドレス	→指定しない
	アドレスマスク	→指定しない
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない
•	QoS	→指定なし
٢A	ACL定義情報(ACL2)」-「TCP定	2義情報」
•	送信元ポート番号	→指定しない
•	あて先ポート番号	→指定しない
•	TCP接続要求	→対象

12. 手順1.~9.を参考に、以下の項目を指定します。

「ACL情報」

定義名	→ACL3
CL定義情報(ACL3)」-「IP定事	奏情報」
プロトコル	→tcp
送信元情報	
IPアドレス	→ 192.168.1.0
アドレスマスク	→24 (255.255.255.0)
	定義名 CCL定義情報(ACL3)」-「IP定 プロトコル 送信元情報 IPアドレス アドレスマスク

- あて先情報
 IPアドレス
 - → 192.168.2.0

→0

- アドレスマスク →24 (255.255.255.0)
- QoS →TOS
- 「ACL定義情報(ACL3)」-「TCP定義情報」
- 送信元ポート番号 →指定しない
- あて先ポート番号 →20 (ftp-dataのポート番号)、21 (ftpのポート番号)
- TCP接続要求 →対象
- **13. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **14. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- 15. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名が vpn-honの [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

16. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

17. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT情報」が表示されます。

- 18. 以下の項目を指定します。
 - NATの使用 →マルチNAT
 - グローバルアドレス → 192.168.1.1
 - アドレス個数 →1

■NAT情報	3
NATの使用	○使用しない○NAT ⊙マルチNAT ○静的NATのみ
クローバルアトレス	192.168.1.1
アトレス個数	1 (8

- 19. [保存] ボタンをクリックします。
- **20.** IP 関連の設定項目の「IP フィルタリング情報」をクリックします。 「IP フィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作 ③透過 〇遮断		
方向 入出力 💌		
ACL定義番号	0 参照	

22. [追加] ボタンをクリックします。

23. 手順20.~22.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →入出力
- ACL定義番号 →1
- 24. 手順20.~22.を参考に、以下の項目を指定します。
 - 動作 →遮断
 - 方向 →入出力
 - ACL定義番号 →2

25. IP 関連の設定項目の「TOS 値書き換え情報」をクリックします。

「TOS値書き換え情報」が表示されます。

26. 以下の項目を指定します。

- 新TOS →a0
- ACL定義番号 →3

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<tos値書き換え情報入力フィールド></tos値書き換え情報入力フィールド>		
新TOS a0		
ACL定義番号	3 参照	

- 27. [追加] ボタンをクリックします。
- 28. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

本社を設定する

- **1. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名 → ACL0
 <ACL情報追加フィールド>
 定義名 ACL0
- 【追加】ボタンをクリックします。
 「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

- プロトコル → tcp
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス → 192.168.2.0
 アドレスマスク → 24 (255.255.255.0)
- QoS →指定なし

■IP定義情報		
ブロトコル		tcp ▼ (番号指定: ["] その他"を選択時のみ有効です)
送信元情	IPアドレス	192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	192.168.2.0
報	アトレスマ スク	24 (255.255.255.0)
増 TO さし		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- 「TCP定義情報」をクリックします。
 「TCP定義情報」ページが表示されます。

- 送信元ポート番号 →指定しない
- あて先ポート番号
- TCP接続要求

→21 (ftpのポート番号)、23 (telnetのポート番号) →対象

-		
	TOD字美桂胡	

■TCP定義情報	3
送信元ポート番号	
あて先ボート番号	21,23
TCP接続要求	⊙対象○対象外

- 9. [保存] ボタンをクリックします。
- 10. 手順1.~9.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → ACL1

「ACL定義情報(ACL1)」-「IP定義情報」

- プロトコル → tcp
 送信元情報
 IPアドレス → 192.168.2.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- QoS →指定なし

「ACL定義情報(ACL1)」-「TCP定義情報」

・ 送信元ポート番号 → 21 (ftpのポート番号)、23 (telnetのポート番号)

- あて先ポート番号 →指定しない
- TCP接続要求 →対象外
- 11. 手順1.~9.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → ACL2

「ACL定義情報(ACL2)」-「IP定義情報」

- プロトコル →すべて
 送信元情報
 IPアドレス →指定しない
 アドレスマスク →指定しない

 あて先情報
- IPアドレス
 →指定しない

 アドレスマスク
 →指定しない
- QoS →指定なし

「ACL定義情報(ACL2)」-「TCP定義情報」

- ・ 送信元ポート番号 →指定しない
 ・ あて先ポート番号 →指定しない
- TCP 接続要求 →対象

手順1.~9.を参考に、以下の項目を指定します。 12.

「ACL情報」	
• 定義名	→ ACL3
「ACL定義情報(ACL3)」-「IF	っ定義情報」
• プロトコル	→tcp
 送信元情報 IPアドレス アドレスマスク 	→ 192.168.2.0 → 24 (255.255.255.0)
 あて先情報 IPアドレス アドレスマスク 	→ 192.168.1.0 → 24 (255.255.255.0)
• QoS	→ TOS → 0

「ACL定義情報(ACL3)」-「TCP定義情報」

- 送信元ポート番号 →20 (ftp-dataのポート番号)、21 (ftpのポート番号)
- あて先ポート番号 →指定しない
- TCP 接続要求 →対象
- 設定メニューのルータ設定で「相手情報」をクリックします。 13. 「相手情報」ページが表示されます。
- 14. 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。
- 15. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shiの [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-shi) |ページが表示されます。

16. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

17. IP関連の設定項目の「IPフィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

- 18. 以下の項目を指定します。
 - 動作 →透渦
 - 方向 →入出力
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>	
動作	◎透過 ○遮断
方向	入出力 💌
ACL定義番号	0 参照

19. [追加] ボタンをクリックします。

- 20. 手順 17.~ 19.を参考に、以下の項目を指定します。
 - 動作 →透過
 - 方向 →入出力
 - ACL定義番号 →1
- 21. 手順 17.~19.を参考に、以下の項目を指定します。
 - 動作 →遮断
 - 方向 →入出力
 - ACL定義番号 →2
- 22. IP 関連の設定項目の「TOS 値書き換え情報」をクリックします。

「TOS値書き換え情報」が表示されます。

- 23. 以下の項目を指定します。
 - 新TOS →a0
 - ACL定義番号 →3

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<tos値書き換え情報入力フィールド></tos値書き換え情報入力フィールド>		
新TOS	a0	
ACL定義番号	3 参照	

- 24. [追加] ボタンをクリックします。
- **25. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。
IPsec 変換前のシェーピング機能と帯域制御(WFQ)機能の併用例

● 設定条件

[本社]

- シェーピングレート :2Mbps
- 帯域制御対象送信元 IP アドレス : 192.168.2.0/24
- 帯域制御対象送信元ポート番号 : すべて
- 帯域制御対象あて先IPアドレス : 192.168.1.0/24
- 帯域制御対象あて先ポート番号 :すべて
- 帯域制御対象プロトコル : TCP
- 帯域制御対象 TOS 値 : すべて
- 割り当て帯域 : 最優先

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

【追加】ボタンをクリックします。
 「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

•	プロトコル	→tcp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.2.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)

• QoS →指定なし

■IP定義情報		
プロトコル		tcp ▼ (番号指定: ["] その他"を選択時のみ有効です)
送信元情	IPアドレス	192.168.2.0
報	アドレスマ スク	24 (255.255.255.0)
あて 先 情 報	IPアドレス	192.168.1.0
	アトレスマ スク	24 (255.255.255.0)
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してください

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

- 8. 以下の項目を指定します。
 - 送信元ポート番号 →指定しない
 - あて先ポート番号 →指定しない
 - TCP接続要求 →対象

■TCP定義情報		3
送信元ポート番号		
あて先ボート番号		
TCP接続要求	●対象○対象外	

- 9. [保存] ボタンをクリックします。
- **10. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **11. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 12. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の [修正] ボタンをクリック します。

「ネットワーク情報(vpn-shi)」ページが表示されます。

- **13. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。
- 14. 以下の項目を指定します。
 - シェーピング →使用する 最大送信レート →2Mbps

シェービング	 ○ 使用しない ③ 使用する
	最大送信レート 2 Mbps ¥

15. 【保存】ボタンをクリックします。

16. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

17. IP 関連の設定項目の「帯域制御(WFQ)情報」をクリックします。

「帯域制御(WFQ)情報」が表示されます。

- 18. 以下の項目を指定します。
 - 帯域 →最優先
 - ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択] ボタンをクリックして設定します。

<帯域制御(WFQ)情報入力フィールド>		
帯域	 ●最優先 ● ベストエフォート ● 使用率 ● 使用帯域 ● 依田帯域 ● 帯域を他と共有 共有できる定義が存在しません 	
ACL定義番号	0 参照	

- 19. [追加] ボタンをクリックします。
- 20. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

IPsec機能と帯域制御(WFQ)機能を併用する場合、IPsec前のパケットに対して帯域制御を行うときには、IPsec用の「相手情報」-「ネットワーク情報」で設定します。この場合、IPsec用の「ネットワーク情報」でシェーピングを行うか、または、実回線の「ネットワーク情報」でIPsec後のパケットに対して帯域制御を設定する必要があります。

IPsec 変換前の MSS 書き換え機能との併用例

[共通]

MSS書き換え値 : 1414Byte

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

[●] 設定条件

4. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

5. 以下の項目を指定します。

MSS書き換え →使用する
 書き換えサイズ → 1414

MSS書き換え	 ○ 使用しない ③ 使用する
	書き換えサイズ 1414 バイト

- 6. [保存] ボタンをクリックします。
- **一面方側の[設定反映]ボタンをクリックします**。

 設定した内容が有効になります。

本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

- **「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - MSS書き換え →使用する 書き換えサイズ → 1414



- 6. [保存] ボタンをクリックします。
- **一面方側の[設定反映]ボタンをクリックします**。

 設定した内容が有効になります。

IPsec変換前のMTU分割機能との併用例

● 設定条件 [共通]

• MTU長 :1460Byte

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名が vpn-honの [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - MTUサイズ → 1460

MTUサイズ 1460 バイト

- 6. [保存] ボタンをクリックします。
- **一面右側の[設定反映]ボタンをクリックします**。

 設定した内容が有効になります。

本社を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の [修正] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
- 5. 以下の項目を指定します。
 - MTUサイズ → 1460

MTUサイズ 1460 バイト

- 6. [保存] ボタンをクリックします。
- 7. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

接続先監視機能との併用例

● 設定条件

[支社]

- 送信元IPアドレス : 192.168.1.1
- あて先IPアドレス : 192.168.2.1
- タイムアウト時間 :5秒
- 正常時送信間隔 :10秒
- 異常時送信間隔
 1分

補足 監視対象装置は、本社側 VPN 装置を指定します。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名が vpn-honの[修正] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

- **4. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 5. 「接続先情報」でIPsec/IKE接続で接続先名がhonsyaの【修正】ボタンをクリックします。 IPsec/IKE接続の設定項目と「基本情報」が表示されます。
- IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。
 「接続制御情報」が表示されます。

•	接続先監視	→使用する
	送信元IPアドレス	→ 192.168.1.1
	あて先IPアドレス	→192.168.2.1
	正常時送信間隔	→10秒
	再送間隔	→1秒
	タイムアウト時間	→5秒
	異常時送信間隔	→1分

		使用しない 使用する	
		送信元IPアドレス	192.168.1.1
		あて先IPアドレス	192.168.2.1
		正常時送信間隔	10 秒 🗸
接続		再送間隔	1 秒 🗸
先監 視		タイムアウト時間	5 秒 🗸
		異常時送信間隔	1 分 🗸
		送信 TTL/HopLimit	255
		連続応答受信回数	1
		異常時送信開始待ち時間	0 秒 🖌
		監視方式	⊙常時監視 ○無通信時監視

- 8. [保存] ボタンをクリックします。
- 画面左側の [設定反映] ボタンをクリックします。
 設定した内容が有効になります。

IKEセッション監視機能との併用例

● 設定条件

[支社]

- あて先IPアドレス : 192.168.2.1
- タイムアウト時間 :5秒
- 正常時送信間隔 : 10秒
- 異常時送信間隔 :1分

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。

補足 監視対象装置は、本社側 VPN 装置を指定します。

3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

- **4. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- **5.** 「接続先情報」で IPsec/IKE 接続で接続先名が honsya の [修正] ボタンをクリックします。 IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

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

「IKE 情報」が表示されます。

7. 以下の項目を指定します。

IKE セッション監視
 あて先 IP アドレス → 192.168.2.1
 タイムアウト時間 → 5秒
 正常時送信間隔 → 10秒
 異常時送信間隔 → 1分

	あて先IPアドレス	192.168.2.1
IKEセッショ	タイムアウト時間	5 秒 🗸
ン監視	正常時送信間隔	10 秒 🗸
	異常時送信間隔	1 分 💙

- 8. [保存] ボタンをクリックします。
- 9. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

- こんな事に気をつけて
 - IKE セッション監視のあて先IPアドレスは、「IPsec 情報」の"対象パケット"に含まれるIPアドレスを指定してください。
 - ・ IKE セッション監視のあて先 IP アドレスに、常時運転している IPsec 対象の装置を指定してください。あて先 IP アドレスに相手 IKE サーバとは異なる装置を指定した場合、あて先 IP アドレスからの応答が受信できなくなります。その場合、相手 IKE サーバが生存していても IPsec/IKE SA は解放されます。そのため通信が不安定になることがあります。

動的経路(RIP)機能と併用する場合

● 設定条件

[共通]

- RIP送信 : v1
- RIP受信 : v1
- RIP送信時加算メトリック値 :0

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名が vpn-hon の [修正] ボタンをクリック します。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

- **「IP 関連」をクリックします**。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- 5. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 6. 【全削除】ボタンをクリックします。 「削除していいですか?」の確認画面が表示されます。
- [OK] ボタンをクリックします。
 「スタティック経路情報」が削除されます。
- **8. IP 関連の設定項目の「RIP 情報」をクリックします**。 「RIP 情報」が表示されます。

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

■RIP情報		
RIP送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する	
RIP受信	○受信しない ●V1で受信する ●V2、V2(Multicast)で受信する	
《 RIP 送信時は加算するメトリック値を設定してください。》		
メトリック値	0 🗸	

- 10. [保存] ボタンをクリックします。
- **11. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の [修正] ボタンをクリック します。

「ネットワーク情報(vpn-shi)」ページが表示されます。

- **「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- IP 関連の設定項目の「スタティック経路情報」をクリックします。
 「スタティック経路情報」が表示されます。
- 6. [全削除] ボタンをクリックします。 「削除していいですか?」の確認画面が表示されます。
- [OK] ボタンをクリックします。
 「スタティック経路情報」が削除されます。
- **8. IP 関連の設定項目の「RIP 情報」をクリックします**。 「RIP 情報」が表示されます。

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

■RIP情報		
RIP送信	●送信しない ●V1で送信する ●V2で送信する ●V2(Multicast)で送信する	
RIP受信	●受信しない ● V1で受信する ● V2、V2(Multicast)で受信する	
《 RIP 送信時は加算するメトリック値を設定してください。》		
メトリック値	0 🗸	

- 10. 【保存】ボタンをクリックします。
- 11. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.14.10 IPv4 over IPv4 で固定 IP アドレスでバックアップ用に使用する VPN(自動鍵交換)

<u>適用機種</u> Si-R220B,220C,370,570

専用線側の通信パスに障害が発生した場合にISDN回線を利用し、ISDN回線側ではIPsec機能を使って自動鍵交換でVPNを構築することによって通信をバックアップする場合の設定方法を説明します。 ここでは、以下のとおり支社と本社が専用線で接続されていることを前提とします。

● 前提条件

[支社]

- ローカルネットワークIPアドレス : 192.168.1.1/24
- 専用線使用スロット
 SLOTO
- 専用線回線速度 : 128K
- 専用線自側IPアドレス : 201.168.1.1
- ネットワーク名 :honsya
- 接続先名 : honsya

[本社]

- ローカルネットワークIPアドレス : 192.168.2.1/24
- 専用線使用スロット
 SLOTO
- 専用線回線速度 : 128K
- 専用線自側IPアドレス : 201.168.1.2
- ネットワーク名 :shisya
- 接続先名 · · · · · · · · · · · · · · · · · shisya



● 設定条件	
[支社]	
● 接続先名	: vpn-hon
[バックアップ回線(ISDN)]	
 ネットワーク名 	: hon-back
● 接続先名	: hon-back
 ISDN回線使用スロット 	: SLOT1
• ISP電話番号	: 123-4567-891
 ユーザ認証 ID 	:userid(プロバイダから提示された内容)
 ユーザ認証パスワード 	:userpass(プロバイダから提示された内容)
 ISDN 自側 IP アドレス 	: 202.168.1.1
• ISDN回線無通信監視	:5分
• IPsec/IKE区間	: 202.168.1.1 - 202.168.1.2
• IPsec 対象範囲	:IPsec 相手情報を使用するすべてのパケット
• 専用線(レギュラー回線)ダウン時動作	:ISDN 回線で IPsec/IKE を使用
• 接続先監視機能	:使用する
• 接続優先制御	:Initiatorを優先する
[本社]	
• 接続先名	: vpn-shi
[バックアップ回線(ISDN)]	
ネットワーク名	: shi-back
• 接続先名	: shi-back
 ISDN回線使用スロット 	: SLOT1
• ISP電話番号	: 123-4567-890
• ユーザ認証 ID	:userid(プロバイダから提示された内容)
 ユーザ認証パスワード 	:userpass(プロバイダから提示された内容)
 ISDN 自側 IP アドレス 	: 202.168.1.2
• 常時接続	:する
• IPsec/IKE区間	: 202.168.1.2 - 202.168.1.1
• IPsec 対象範囲	:IPsec 相手情報を使用するすべてのパケット
• 専用線(レギュラー回線)ダウン時動作	:ISDN回線でIPsec/IKEを使用
• 接続先監視機能	:使用する
• 接続優先制御	:Responderを優先する
[共通]	
 鍵交換モード 	:Main Mode 使用
• IPsecプトロコル	: esp
 IPsec暗号アルゴリズム 	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
• IPsec DHグループ	:なし
• IKE認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: des-cbc

• IKE 認証アルゴリズム

- : hmac-md5
- IKE DH グループ
 ™modp768 (グループ1)

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する

支社の VPN を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3.** 「ネットワーク情報」で専用線接続を行うネットワーク名がhonsyaの [修正] ボタンをクリックします。 「ネットワーク情報 (honsya)」ページが表示されます。
- **4. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 5. 「接続先情報」で専用線接続で接続先名がhonsyaの【修正】ボタンをクリックします。 専用線接続の設定項目と「基本情報」が表示されます。
- 6. 専用線接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。

•	接続先監視	→使用する
	送信元IPアドレス	→201.168.1.1
	あて先 IP アドレス	→201.168.1.2
	正常時送信間隔	→10秒
	再送間隔	→1秒
	タイムアウト時間	→5秒
	異常時送信間隔	→ 1分
	接続優先制御	→Initiatorを優先する

■接続	■接続制御情報		
	 ○ 使用しない ③ 使用する 		
	送信元IPアドレス 201.168.1.1		
	あて先IPアドレス 201.168.1.2		
	正常時送信間隔 10 秒 🗸		
接続	再送間隔 1 秒 🗸		
充監 視	タイムアウト時間 5 秒 🗸		
	異常時送信間隔 1 分 ▼		
	送信 TTL/HopLimit 255		
	連続応答受信回数 1		
	異常時送信開始待ち時間 0 秒 ▼		
	監視方式 ◎常時監視 ○無通信時監視		
接続 優先 制御	○使用しない ⊙Initiatorを優先する ○Responderを優先する		

- 8. [保存] ボタンをクリックします。
- 9. 画面上部の「ネットワーク情報(honsya)」をクリックします。 「ネットワーク情報(honsya)」ページが表示されます。
- 10. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →vpn-hon
- 接続先種別 → IPsec/IKE 接続



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

12. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

13. 以下の項目を指定します。

 鍵交換モード 	→ Main Mode 使用
相手側エンドポイント	→202.168.1.2
自側エンドポイント	→202.168.1.1

	⊙ Main Mode使用	
鍵交換モ ート	相手側エンドボイント 202.168.1.2	
	自側エンドボイン ト 202.168.1.1	

14. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

認証アルゴリズム

16. 以下の項目を指定します。

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

暗号アルゴリ ズム □aes-cbc-256 □aes-cbc-192 □aes □3des-cbc ☑des-cbc □null		aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ⊻des-cbc null	
SA	認証アルゴリ ズム	✔ hmac-md5 hmac-sha1 記証なし 使用しない	
の設 定	PFS時のDHグ ルーブ		
	SA有効時間	8 時間 🖌	
	SA有効データ 量	0 GByte 🗸	

17. 【保存】ボタンをクリックします。

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

「IKE 情報」が表示されます。

19. 以下の項目を指定します。

•	IKE 認証鍵 鍵識別 鍵	→文字列 →abcdefghijkImnopqrstuvwxyz1234567890
•	SAの設定 暗号アルゴリズム 認証(ハッシュ)アルゴリズム DH <i>グ</i> ループ	→des-cbc →hmac-md5 →modp768(グループ)

■IKE情報		3	
ルロヨロミンク語	鏈識別	○16進数 ⊙文字列	
INESSIL	鏈	••••••	
IKE認証方式	7	shared	
ボート番号		500	
	暗号アルゴリズ ム	des-cbc 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌	
	DHグルーブ	modp768(ヴループ1) 💌	
	SA有効時間	24 時間 🖌	

20. [保存] ボタンをクリックします。

支社のバックアップ回線を設定する

21. 設定メニューのルータ設定で「WAN 情報」をクリックします。 「WAN 情報」ページが表示されます。

22. 以下の項目を指定します。

• 回線インタフェース → ISDN



- **23. [追加] ボタンをクリックします**。 「WAN1 情報(ISDN)」ページが表示されます。
- **24. 「基本情報」をクリックします**。 「基本情報」が表示されます。
- 25. 以下の項目を指定します。

• ポート	→ ス	ペロット 1-0
■基本情報		3
ボート	スロット 1-0 🔽	

- 26. [保存] ボタンをクリックします。
- **27. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **28. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 29. 以下の項目を指定します。
 - ネットワーク名 → hon-back

<ネットワーク情報追加フィールド>	
ネットワーク名 hon-back hon-back	

30. [追加] ボタンをクリックします。

「ネットワーク情報(hon-back)」ページが表示されます。

31. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

32. 以下の項目を指定します。

IPアドレス	→設定する
相手側IPアドレス	→指定しない
自側IPアドレス	→202.168.1.1

■IP基本情報	3
IPアドレス	 設定しない 設定する 相手側IPアドレス
	自側IPアドレス 202.168.1.1

33. [保存] ボタンをクリックします。

IP 関連の設定項目の「スタティック経路情報」をクリックします。 34.

「スタティック経路情報」が表示されます。

35. 以下の項目を指定します。

- ネットワーク →ネットワーク指定 あて先 IP アドレス →202.168.1.2 あて先アドレスマスク →32 (255.255.255.255)
- メトリック値
- 優先度

→1

→0

<スタティック経路情報入力フィールド>			
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先IPアドレス 202.168.1.2 あて先アドレスマスク 32 (255.255.255.255) ▼ 		
メトリック値	1 💌		
優先度	0		

- [追加] ボタンをクリックします。 36.
- 37. 「ネットワーク情報(hon-back)」で「接続先情報」をクリックします。 「接続先情報」が表示されます。

接続先名接続先種別

→ hon-back
→ISDN接続
→通常接続

ダイヤル1 電話番号

→ 123-4567-891



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

- **39. [追加] ボタンをクリックします。** ISDN 接続の設定項目と「基本情報」が表示されます。
- 40. 以下の項目を指定します。
 - 使用インタフェース → WAN1

使用インタフェース WAN1 V

- 41. [保存] ボタンをクリックします。
- **42.** ISDN 接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。

• 常時接続機能 無通信監視タイマ →使用しない →送受信パケットについて300秒

■接続制御	即情報 []
常時接続 機能	⊙使用しない○使用する
無通信監 視タイマ	送受信パケット 🔽 について 300 秒

[保存] ボタンをクリックします。 44.

45. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

- 46. 以下の項目を指定します。
 - 認証方式 → PAP、 CHAP • 送信認証情報 認証ID → userid 認証パスワード → userpass

■PPP情報		
認証方式		>
送信题証	認証ID	userid
情報	認証バスワー ド	••••••

- 47. [保存] ボタンをクリックします。
- 48. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

本社を設定する

本社の VPN を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3.** 「ネットワーク情報」で専用線接続を行うネットワーク名が shisya の [修正] ボタンをクリックします。 「ネットワーク情報 (shisya)」ページが表示されます。
- **4. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 5. 「接続先情報」で専用線接続で接続先名が shisya の [修正] ボタンをクリックします。 専用線接続の設定項目と「基本情報」が表示されます。
- 6. 専用線接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 7. 以下の項目を指定します。

接続先監視	→使用する
送信元IPアドレス	→201.168.1.2
あて先IPアドレス	→201.168.1.1
正常時送信間隔	→10秒
再送間隔	→1秒
タイムアウト時間	→5秒
異常時送信間隔	→ 1分
接続優先制御	→ Responder を優先する



- 8. [保存] ボタンをクリックします。
- 9. 画面上部の「ネットワーク情報 (shisya)」をクリックします。

「ネットワーク情報(shisya)」ページが表示されます。

10. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

11. 以下の項目を指定します。

• 接続先名

- →vpn-shi
- 接続先種別 → IPsec/IKE 接続



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

12. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

13. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント 自側エンドポイント → Main Mode 使用 → 202.168.1.1 → 202.168.1.2

	⊙ Main Mode使用	
鍵交換モ ート	相手側エンドボイント 202.168.1.1	
	自側エンドボイン ト 202.168.1.2	

14. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

16. 以下の項目を指定します。

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

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null		
SA	認証アルゴリ ズム	☑hmac-md5 □hmac-sha1 □認証なし		
) の 定	PFS時のDHグ ルーブ	使用しない		
	SA有効時間	8 時間 🗸		
	SA有効データ 量	0 GByte 🗸		

17. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

19. 以下の項目を指定します。

,	● IKE 認証	鍵		
	鍵識別			→文字列
	鍵			→abcdefghijklmnopqrstuvwxyz1234567890
,	• SAの設知	定		
暗号アルゴリズム				→des-cbc
認証(ハッシュ)アルゴリズム			リズム	→hmac-md5
	DHグル	ープ		→modp768(グループ1)
	■IKE情報			3
		鏈識別	◯16進数	
	IKE認証键	鍵	•••••	••••••
	₩┎═╗╤┰╼╧═	P	- to a second	

键		••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 🔽
	SA有効時間	24 時間 🖌

20. [保存] ボタンをクリックします。

本社のバックアップ回線を設定する

21. 設定メニューのルータ設定で「WAN 情報」をクリックします。 「WAN 情報」ページが表示されます。

22. 以下の項目を指定します。

• 回線インタフェース → ISDN



- **23. [追加] ボタンをクリックします**。 「WAN1 情報(ISDN)」ページが表示されます。
- **24. 「基本情報」をクリックします**。 「基本情報」が表示されます。
- 25. 以下の項目を指定します。

• ポート	→スロ]ット1-0
■基本情報		3
ボート	スロット 1-0 💌	

- 26. [保存] ボタンをクリックします。
- **27. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **28. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 29. 以下の項目を指定します。
 - ネットワーク名 → shi-back

<ネットワーク情報追加フィールド>		
ネットワーク名	shi-back	

30. [追加] ボタンをクリックします。

「ネットワーク情報(shi-back)」ページが表示されます。

31. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

32. 以下の項目を指定します。

•	IPアドレス	→設定する
	相手側IPアドレス	→指定しない
	自側 IP アドレス	→202.168.1.2

■IP基本情報		3
	 ○ 設定しない ● 設定する 	
IPアドレス	相手側IPアドレス	
	自側IPアドレス 202.168.1.2	

33. [保存] ボタンをクリックします。

34. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

35. 以下の項目を指定します。

- ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →202.168.1.1
 →32 (255.255.255.255)
- メトリック値 →1
 優先度 →0
- 36. [追加] ボタンをクリックします。
- **37.** 「ネットワーク情報(shi-back)」で「接続先情報」をクリックします。 「接続先情報」が表示されます。

- 接続先名 接続先種別
- →shi-back →ISDN 接続
- →通常接続

ダイヤル1 電話番号

→123-4567-890



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

39. [追加]ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

- 40. 以下の項目を指定します。
 - 使用インタフェース → WAN1

使用インタフェース WAN1 V

- 41. 【保存】ボタンをクリックします。
- **42.** ISDN 接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。

● 常時接続機能		→使用する	
■接続	制御情報		3
常続能機	○使用しない◎使用する		

補足「常時接続機能」で"使用する"を選択すると、表示される「接続制御情報」画面が変わります。

- 44. [保存] ボタンをクリックします。
- **45.** ISDN 接続の設定項目の「PPP 情報」をクリックします。 「PPP 情報」が表示されます。
- 46. 以下の項目を指定します。
 - 認証方式 → PAP、CHAP
 - ・ 送信認証情報
 認証 ID → userid
 認証パスワード → userpass

■PPP情報			
認証方式			
送信题証	認証ID	userid	
情報	認証バスワー ド	•••••	

- 47. [保存] ボタンをクリックします。
- 48. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.14.11 テンプレート着信機能(AAA 認証)を使用した 固定 IP アドレスでの VPN

適用機種 全機種

IPsec機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。 ここでは以下の条件によって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

: 202.168.1.66/24

:LAN0ポート使用

● 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

• 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

PPPoEユーザ認証 ID

: userid(プロバイダから提示された内容)

:userpass(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
- PPPoE LAN ポート

[本社]

• ローカルネットワーク IPv4 アドレス

- : 192.168.2.1/24
- : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス: 202.168.2.65



● 設定条件	
[支社]	
• ネットワーク名	: vpn-hon
● 接続先名	: honsya
• IPsec/IKE区間	: 202.168.1.66 - 202.168.2.66
• IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット
[本社]	
• テンプレート名	: vpn-shi
• IPsec/IKE区間	: 202.168.2.66 - 202.168.1.66
• IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット
[共通]	
 鍵交換タイプ 	: Main Mode
• IPsecプロトコル	: esp
• IPsec暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
● IPsec DH グループ	:なし
● IKE認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
• IKE 暗号アルゴリズム	: des-cbc
● IKE 認証アルゴリズム	: hmac-md5
・ IKE DH グループ	: modp768

こんな事に気をつけて

- テンプレート着信機能(AAA 認証)を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに 設定してください。
- ユーザIDとユーザ認証パスワードは、テンプレート情報のIKE 情報の交換モードにより以下のように設定します。
 Main Modeの場合 : 相手側 IPsec トンネルアドレス
 Aggressive Modeの場合 : 相手側の装置識別情報

どとント

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(Initiator)

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名 vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 → 1
 - 優先度 →0



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>		
接続先名	honsya	
接続先種別	 ATM接続 VCI 専用線接続 ● 適常接続 (使用インタフェース WANI ▼) ● 論理リンクにバンドルする (使用インタフェー ス WANI ▼) ● 論理リンクにバンドルする (使用インタフェー ス バンドル先 避探できる定義がありません ▼) ISDN接続 ● 通常接続 (使用インタフェース すべて ▼) バクドル先 「選択できる定義がありません ▼) ISDN接続 ● 通常接続 (使用インタフェース すべて ▼) バンドル先 「選択できる定義がありません ▼) ISDN接続 ● フレームリレー接続 [DLCI] PPPoE接続 IPトンネル接続 ● IPsec/IKE接続 MPLSトンネル接続 	

機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

	⊙ Main Mode使用
鍵交換モ ート	相手側エンドボイント 202.168.2.66
	自側エンドボイン ト 202.168.1.66

13. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

認証アルゴリズム

15. 以下の項目を指定します。

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5

	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ⊻des-cbc null
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
の設 定	PFS時のDHグ ルーブ	使用しない V
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 🗸

16. 【保存】ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

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

■IKE情報		3
いて言わらい分類	鏈識別	○16進数 ⊙文字列
IVE 98 911 ##	鏈	•••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768グループ1) 💌
	SA有効時間	24 時間 🖌

- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する(Responder)

- 設定メニューのルータ設定で「テンプレート情報」をクリックします。
 「テンプレート情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - テンプレート名 → vpn-shi
 - 接続種別

→IPsec/IKE (RADIUS/AAA)

<テンプレート情報追加フィールド>		
テンプレート名 vpn-shi		
接続種別	 ○ ISDN ⊙ IPsec/IKE(RADIUS/AAA) ○ IPsec/IKE(動的VPN) 	

機種により、接続種別の表示が上記の画面とは異なります。

3. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shi)」と設定項目が表示されます。

4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5. 以下の項目を指定します。

- 使用するrmtインタフェース →rmt1から1インタフェースを予約
- 参照する AAA 情報 →0
- 鍵交換モード → Main Mode (Responder) 使用
 自側エンドポイント → 202.168.2.66

使用するrmtイン タフェース	rmt1から1インタフェースを予約	
MTUサイズ	1500 バイト	
無通信監視タイ マ	送受信バケットについて 🛛 🛛 🕸 🔽	
参照するAAA情 報	0	
鍵交換モート	 Aggressive Mode(Responder)使用 自側エンド ポイント IDタイプ ● FQDN ● User-FQDN Main Mode(Responder)使用 自側エンド 和イント 202.168.2.66 	

- 6. [保存] ボタンをクリックします。
- テンプレート情報 (vpn-shi) の設定項目の「IPsec/IKE 関連」をクリックします。
 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

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

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
SA	SA 認証アルゴリ ズム □ hmac-md5 □ hmac-sha1 □ 認証なし の設 定 PFS時のDHグ ループ 使用しない ▼	
の設 定		
	SA有効時間	8 時間 🗸
	SA有効テータ 量	0 GByte 🗸

- 9. [保存] ボタンをクリックします。
- **10.** IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

- 11. 以下の項目を指定します。
 - SAの設定
 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768 (グループ1)

	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 🗸
	SA有効時間	24 時間 🖌

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **14.** 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 15. 以下の項目を指定します。
 - グループ名

```
→vpn-shisya
```

<グループID情報追加フィールド>	
ブループ名	vpn-shisya

16. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

17. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

• ユーザID

→202.168.1.66

<aaaユーザ情報追加フィールド></aaaユーザ情報追加フィールド>	
ユーザID 202.168.1.66	

19. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と設定項目が表示されます。

20. 「認証情報」をクリックします。

「認証情報」が表示されます。

- 21. 以下の項目を指定します。
 - ユーザID →202.168.1.66
 - 認証パスワード → 202.168.1.66

■認証情報	3
ユーザID	202.168.1.66
認証バスワード	•••••

- 22. [保存] ボタンをクリックします。
- **23.** AAA ユーザ情報(0)の設定項目の「IP 関連」をクリックします。 IP 関連の設定項目と「IP 基本情報」が表示されます。
- **24.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 25. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →192.168.1.0
 →24 (255.255.255.0)

→1

→1

- メトリック値
- 優先度

<スタティック経路情報入力フィールド>		
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先IPアドレス 192.168.1.0 あて先アドレスマスク 24 (255.255.255.0) 	
メトリック値	1 💌	
優先度	1	

- 26. [追加] ボタンをクリックします。
- **27.** AAA ユーザ情報(0)の設定項目の「IPsec/IKE 関連」をクリックします。 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。
• 対象パケット 自側 IP アドレス/マスク →IPv4すべて 相手側IPアドレス/マスク →IPv4すべて



29. [保存] ボタンをクリックします。

30. IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE情報」が表示されます。

- 31. 以下の項目を指定します。
 - IKE 認証鍵

鍵識別 鍵

→文字列

→ abcdefghijklmnopqrstuvwxyz1234567890

■IKE情報		3
	<mark>键識別</mark>	○16進数 ⊙文字列
IKE認証規	键	••••••

- [保存] ボタンをクリックします。 32.
- 33. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

2.14.12 テンプレート着信機能(AAA 認証)を使用した 可変 IP アドレスでの VPN

適用機種 全機種

IPsec機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。 ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間の VPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 (PPPoE 常時接続)]

- ローカルネットワークIPv4アドレス
- PPPoE ユーザ認証 ID
- PPPoEユーザ認証パスワード
- PPPoE LAN ポート

- : 192.168.1.1/24
- : userid (プロバイダから提示された内容)
- :userpass(プロバイダから提示された内容)
- :LAN0ポート使用

[本社]

• ローカルネットワーク IPv4 アドレス

: 192.168.2.1/24

• インターネットプロバイダから割り当てられた固定 IPv4 アドレス

: 202.168.2.66/24

• インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス: 202.168.2.65



● 設定条件 [支社] ネットワーク名 : vpn-hon • 接続先名 : honsya :支社 - 202.168.2.66 • IPsec/IKE区間 IPsec対象範囲 :IPsec 相手情報を使用するすべてのパケット IKE (UDP:500番ポート)のプライベートアドレス : 192.168.1.1 • ESPのプライベートアドレス : 192.168.1.1 [本社] テンプレート名 : vpn-shi • IPsec/IKE区間 :202.168.2.66 - 支社 IPsec対象範囲 : IPsec 相手情報を使用するすべてのパケット [共通] 鍵交換タイプ : Aggressive Mode IPsec プロトコル : esp • IPsec 暗号アルゴリズム : des-cbc • IPsec認証アルゴリズム : hmac-md5 • IPsec DH グループ :なし • IKE 支社 ID / ID タイプ :shisya(自装置名)/FQDN • IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列) IKE 認証方法 : shared • IKE 暗号アルゴリズム : des-cbc • IKE 認証アルゴリズム : hmac-md5 IKE DH グループ : modp768

こんな事に気をつけて

- テンプレート着信機能(AAA 認証)を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに 設定してください。
- ユーザIDとユーザ認証パスワードは、テンプレート情報のIKE 情報の交換モードにより以下のように設定します。
 Main Mode の場合 : 相手側 IPsec トンネルアドレス
 Aggressive Mode の場合 : 相手側の装置識別情報

Ŵ**ヒント —**

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(Initiator)

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。

→指定しない

→ isakmp

→udp

4. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

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

<静的NAT情報入力フィールド>		
プライベート	IPアド レス	192.168.1.1
IP忭青報	ボート 番号	isakmp · (番号指定: 7その他 を選択時の み有効です)
グローバル	IPアド レス	
IP忭青報	ボート 番号	isakmp V(番号指定: 7その他 ~ を選択時の み有効です)
プロトコル		udp ✓(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

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

- プロトコル → esp
- 画面上部の「相手情報」をクリックします。
 「相手情報」ページが表示されます。

「ネットワーク情報」をクリックします。 10.

「ネットワーク情報」が表示されます。

- 11. 以下の項目を指定します。
 - ネットワーク名 →vpn-hon

<ネットワーク情	報追加フィールド>
ネットワーク名	vpn-hon

12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

13. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

14. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15. 以下の項目を指定します。

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

<スタティック経路情報入力フィールド>		
ネットワーク	 ○ デフォルトルート ③ ネットワーク指定 あて先IPアドレス 192.168.2.0 あて先アドレスマスク 24 (255.255.255.0) 	
メトリック値	1 💌	
優先度	0	

16. [追加] ボタンをクリックします。

17. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント 自装置識別情報

→ Aggressive Mode (Initiator) 使用 → 202.168.2.66 → shisya

	⊙ Aggressive Mode(Initiator)使用	
	自側エンドボイン ト	
鍵交換モ ート	相手側エンドボイ ント	202.168.2.66
	自装置識別情報	shisya
	IDタイプ	⊙ FQDN ◯ User-FQDN

21. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

23. 以下の項目を指定します。

認証アルゴリズム

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



24. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

•	IKE 認訨鍵 鍵識別 鍵	→文字列 →abcdefghijklmnopqrstuvwxyz1234567890
•	SAの設定 暗号アルゴリズム 認証(ハッシュ)アルゴリズム DH <i>グ</i> ループ	→des-cbc →hmac-md5 →modp768(グループ1)

IKE情報		3
レビニション	鏈識別	○16進数 ⊙文字列
17日16日開建	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🖌

- 27. [保存] ボタンをクリックします。
- **28. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する(Responder)

- 設定メニューのルータ設定で「テンプレート情報」をクリックします。
 「テンプレート情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - テンプレート名 → vpn-shi
 - 接続種別 → IPsec/IKE(RADIUS/AAA)

<テンプレート情報追加フィールド>		
テンプレート名 vpn-shi		
接続種別	● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN)	

機種により、接続種別の表示が上記の画面とは異なります。

【追加】ボタンをクリックします。
 「テンプレート情報(vpn-shi)」と設定項目が表示されます。

4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5. 以下の項目を指定します。

• 使用するrmtインタフェース →rmt1から1インタフェースを予約

→0

- 参照する AAA 情報
- 鍵交換モード 自側エンドポイント IDタイプ

→ Aggressive Mode(Responder)使用 → 202.168.2.66 → FQDN



- 6. [保存] ボタンをクリックします。
- テンプレート情報 (vpn-shi) の設定項目の「IPsec/IKE 関連」をクリックします。
 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

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

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
の設 定	PFS時のDHグ ループ	使用しない V
	SA有効時間	8 時間 🗸
	SA有効データ 量	0 GByte 💌

9. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

- 11. 以下の項目を指定します。
 - SAの設定
 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768 (グループ1)

	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 🗸
	SA有効時間	24 時間 🖌

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **14.** 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 15. 以下の項目を指定します。
 - グループ名

```
→vpn-shisya
```

<グループID情報追加フィールド>		
グループ名	vpn-shisya	

16. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

17. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

• ユーザID

→ shisya

<aaaユーザ情報追加フィールド></aaaユーザ情報追加フィールド>	
ユーザID	shisya

19. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と設定項目が表示されます。

20. 「認証情報」をクリックします。

「認証情報」が表示されます。

21. 以下の項目を指定します。

- ユーザID → shisya
- 認証パスワード → shisya

■認証情報	3
ユーザID	shisya
認証バスワード	•••••

- 22. [保存] ボタンをクリックします。
- **23.** AAA ユーザ情報(0)の設定項目の「IP 関連」をクリックします。 IP 関連の設定項目と「IP 基本情報」が表示されます。
- **24.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 25. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →192.168.1.0
 →24 (255.255.255.0)

→1

→1

- メトリック値
- 優先度

<スタティック経路情報入力フィールド>			
ネットワーク	 デフォルトルート ネットワーク指定 あて先IPアドレス 192.168.1.0 あて先アドレスマスク 24 (255.255.255.0) 		
メトリック値	1 💌		
優先度	1		

- 26. [追加] ボタンをクリックします。
- **27.** AAA ユーザ情報(0)の設定項目の「IPsec/IKE 関連」をクリックします。 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

● 対象パケット	
自側 IP アドレス/マスク	→IPv4すべて
相手側IPアドレス/マスク	→IPv4すべて

■IPsec情報		
自側F Fレス, マスク 対象	自側IPア ドレス/ マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/ プレフィックス長形式で入力してください。
ット	相手側IP アトレス ノマスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/ プレフィックス長形式で入力してください。

- 29. [保存] ボタンをクリックします。
- 30. IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

- 31. 以下の項目を指定します。
 - IKE 認証鍵 鍵識別 鍵

→文字列 →abcdefghijkImnopqrstuvwxyz1234567890

■IKE情報		3
ार ⊏≣ग≣ग≎वे	<mark>键識別</mark>	○16進数 ⊙文字列
INE認証題	鏈	•••••

- 32. [保存] ボタンをクリックします。
- **33. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.14.13 テンプレート着信機能(RADIUS 認証)を使用した 固定 IP アドレスでの VPN

適用機種 全機種

IPsec機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。 ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間の VPN終端装置として本装置が接続されていることを前提とします。

: 202.168.1.66/24

:LAN0ポート使用

● 前提条件

[本社]

[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
- PPPoEユーザ認証ID

- : userid(プロバイダから提示された内容)
- PPPoEユーザ認証パスワード
- :userpass(プロバイダから提示された内容)
- PPPoE LAN ポート

• 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



\bullet	設定条件	
[支	[社]	
٠	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]	
٠	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
		. 0
•	認証情報2(セカンタリ) サ 右 鍵	. 102 169 2 1
	六句疑 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	?U)
	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
		. U
•	アカワノティンク情報2(セカン5	· 192 168 2 1
	ナーバIPアドレス	: 192.168.2.6
	復旧待機時間	:30分
	優先度	: 100
[井	[通]	
•	鍵交換タイプ	: Main Mode
٠	IPsecプロトコル	: esp
•	IPsec暗号アルゴリズム	: des-cbc
•	IPsec認証アルゴリズム	: hmac-md5
•	IPsec DH グループ	:なし
•	IKE認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
•	IKE認証方法	: shared
•	IKE 暗号アルゴリズム	: des-cbc

• IKE 認証アルゴリズム : hmac-md5

● IKE DH グループ

[RADIUS サーバに登録する情報(プライマリ、セカンダリ共通)]

- 認証ユーザID : 202.168.1.66
- 認証ユーザパスワード : 202.168.1.66
- IPsec対象範囲 : any4 any4
- IKE 認証鍵 : abcdefghijkImnopqrstuvwxyz1234567890(文字列)

: modp768

• IPv4スタティック経路情報 : 192.168.1.0/24

こんな事に気をつけて

- テンプレート着信機能(RADIUS 認証)を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パス ワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
 Main Mode の場合 : 相手側 IPsec トンネルアドレス
 Aggressive Mode の場合 : 相手側の装置識別情報
- ※ビント ——
- ◆ DH グループとは?

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

◆ IKE とは? 自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(Initiator)

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド> ネットワーク名 vpn-hon

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- **6.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

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

- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

	⊙ Main Mode使用
鍵交換モ ート	相手側エンドボイ 202.168.2.66 202.168.2.66
	目側エンドボイン 202.168.1.66

13. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

認証アルゴリズム

15. 以下の項目を指定します。

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5

SA の設 定	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ⊻des-cbc null
	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
	PFS時のDHグ ループ	使用しない V
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 🗸

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

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

IKE情報		3
गर सहराहत देखे	鏈識別	○16進数 ⊙文字列
INE 68 all ##	鏈	••••••
IKE認証方式	7	shared
ポート番号		500
SAの設定	暗号アルコリズ ム	des-cbc 💌
	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🗸

- 19. 【保存】ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する(Responder)

- 設定メニューのルータ設定で「テンプレート情報」をクリックします。
 「テンプレート情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - テンプレート名 → vpn-shi
 - 接続種別
- →IPsec/IKE (RADIUS/AAA)

< テンプレート情報追加フィールド>		
テンプレート名 vpn-shi		
接続種別	 ○ ISDN ⊙ IPsec/IKE(RADIUS/AAA) ○ IPsec/IKE(動的VPN) 	

機種により、接続種別の表示が上記の画面とは異なります。

3. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shi)」と設定項目が表示されます。

4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 使用するrmtインタフェース →rmt1から1インタフェースを予約
- 参照する AAA 情報 →0
- 鍵交換モード → Main Mode (Responder) 使用
 自側エンドポイント → 202.168.2.66

使用するrmtイン タフェース	rmt1 から1 インタフェースを予約		
MTUサイズ	1500 / バイト		
無通信監視タイ マ	送受信バケットについて 🛛 🛛 🛛 🔽		
参照するAAA情 報	0		
鍵交換モード	 Aggressive Mode(Responder)使用 自側エンド ポイント IDタイプ ● FQDN ● User-FQDN Main Mode(Responder)使用 自側エンド 北イント 202.168.2.66		

- 6. [保存] ボタンをクリックします。
- テンプレート情報 (vpn-shi) の設定項目の「IPsec/IKE 関連」をクリックします。
 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

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

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし	
の設 PFS時のDHグ 定 ループ		使用しない	
	SA有効時間	8 時間 🗸	
	SA有効データ 量	0 GByte 💌	

- 9. [保存] ボタンをクリックします。
- **10.** IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

- 11. 以下の項目を指定します。
 - SAの設定
 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768 (グループ1)

	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 🗸
	SA有効時間	24 時間 🖌

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **14.** 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 15. 以下の項目を指定します。
 - グループ名

```
→vpn-shisya
```

<グループID情報追加フィールド>			
グループ名	vpn-shisya		

16. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

17. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

٠	RADIUSサービス	→クライアント機能
	認証	→チェックする
	アカウンティング	→チェックする
•	自側認証 IP アドレス	→ 192.168.2.1

• 自側アカウンティングIPアドレス → 192.168.2.1

■基本情報	
RADIUSサービス	クライアント機能 ▼ ■認証 ■アカウンティング (クライアント機能またはサーバ機能を選択した 場合にのみ有効となります)
自側認証IPアドレス	192.168.2.1
自側アカウンティンク IPアトレス	192.168.2.1

- 19. [保存] ボタンをクリックします。
- 20. RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」ページが表示されます。

21. 認証情報1の [修正] ボタンをクリックします。

22. 以下の項目を指定します。

認証情報1	
共有鍵	→192.168.2.1
サーバIPアドレス	→192.168.2.5
復旧待機時間	→30分
優先度	→ 0

	共有鍵	•••••
認証情報 1	サーバIPア ドレス	192.168.2.5
	サーバ UDPポート	⊙1812 ◯1645
	復旧待機 時間	30 分 🗸
	優先度	0
	自側認証 IPアドレス	

23. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

24. 認証情報2の[修正] ボタンをクリックします。

→ 192.168.2.1
→ 192.168.2.6
→30分
→ 100

認証件青春日 2	共有鍵	••••••
	サーバIPア ドレス	192.168.2.6
	サーバ UDPポート	⊙ 1812 ◯ 1645
	復旧待機 時間	30 分 🗸
	優先度	100
	自側認証 IPアドレス	

26. 認証情報2の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

27. アカウンティング情報1の [修正] ボタンをクリックします。

•	アカウンティング情報1	
	共有鍵	→192.168.2.1
	サーバIPアドレス	→192.168.2.5
	復旧待機時間	→30分
	優先度	→ 0

	共有鍵	••••••
	サーバIPア ドレス	192.168.2.5
	サーバ UDPポート	⊙1813 ◯1646
アカウンティング情報 1	復旧待機 時間	30 分 💌
	優先度	0
	自側アカウ ンティング IPアドレス	

- **29. アカウンティング情報1の[保存]ボタンをクリックします**。 「サーバ情報(クライアント機能)」に戻ります。
- 30. アカウンティング情報2の[修正]ボタンをクリックします。

アカウンティング情報2
 共有鍵 → 192.168.2.1
 サーバIPアドレス → 192.168.2.6
 復旧待機時間 → 30 分
 優先度 → 100

	共有鍵	•••••
	サーバIPア ドレス	192.168.2.6
	サーバ UDPポート	⊙1813 ◯1646
アカウンティング情報 2	復旧待機 時間	30 分 🗸
	優先度	100
	自側アカウ ンティング IPアドレス	

32. アカウンティング情報2の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

33. 画面左側の[設定反映]ボタンをクリックします。

設定した内容が有効になります。

2.14.14 テンプレート着信機能(RADIUS 認証)を使用した 可変 IP アドレスでの VPN

適用機種 全機種

IPsec機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。 ここでは以下の条件によって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間の VPN終端装置として本装置が接続されていることを前提とします。

● 前提条件

[支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス
- PPPoE ユーザ認証 ID
- PPPoEユーザ認証パスワード
- PPPoE LANポート

- : 192.168.1.1/24
- :userid(プロバイダから提示された内容)
- :userpass(プロバイダから提示された内容)
- :LAN0 ポート使用

[本社]

• ローカルネットワークIPv4アドレス

- : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス

: 202.168.2.66/24

• インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス: 202.168.2.65



● 設定条件 [支社]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE区間 : 支社 202.168.2.66
- IPsec 対象範囲
 IPsec 相手情報を使用するすべてのパケット
- IKE (UDP:500番ポート)のプライベートアドレス
- : 192.168.1.1
- ESPのプライベートアドレス : 192.168.1.1

[本社]

- テンプレート名 : vpn-shi
- IPsec/IKE区間 :202.168.2.66 支社
- IPsec 対象範囲
 IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス : クライアント機能
 - :認証、アカウンティング
- 自側認証 IP アドレス : 192.168.2.1
- 自側アカウンティングIPアドレス : 192.168.2.1
- 認証情報1(プライマリ) 共有鍵
 192.168.2.1
 サーバIPアドレス
 192.168.2.5
 復旧待機時間
 30分
 優先度
 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 : abcdefghijkImnopqrstuvwxyz1234567890 (文字列)

- IKE 認証方法
- IKE 暗号アルゴリズム
 ides-cbc
- IKE 認証アルゴリズム
 hmac-md5
- IKE DH グループ : modp768

[RADIUS サーバに登録する情報(プライマリ、セカンダリ共通)]

- 認証ユーザID :shisya
- 認証ユーザパスワード :shisya
- IPsec対象範囲 : any4 any4
- IKE 認証鍵 : abcdefghijkImnopqrstuvwxyz1234567890(文字列)

: shared

• IPv4スタティック経路情報 : 192.168.1.0/24

こんな事に気をつけて

- ・ テンプレート着信機能(RADIUS 認証)を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パス ワードを同じに設定してください。
- ユーザIDとユーザ認証パスワードは、テンプレート情報のIKE 情報の交換モードにより以下のように設定します。
 Main Modeの場合
 : 相手側 IPsec トンネルアドレス
 Aggressive Modeの場合: 相手側の装置識別情報

☆ ヒント ━

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(Initiator)

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。
- **「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

•	プライベートIP情報	
	IPアドレス	→192.168.1.1
	ポート番号	→isakmp
•	グローバル IP 情報	
	IPアドレス	→指定しない

- ポート番号 →isakmp • プロトコル
 - →udp

<静的NAT情報入力フィールド>		
ブライベート	IPアド レス	192.168.1.1
IP情報	ボート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
グローバル	IPアド レス	
IP竹青幸反	ポート 番号	isakmp ✓(番号指定: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
プロトコル		udp ✓(番号指定: ************************************

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

- プライベート IP 情報 IPアドレス → 192.168.1.1 →すべて ポート番号 • 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
- 画面上部の「相手情報」をクリックします。 9. 「相手情報」ページが表示されます。
- 10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

- 11. 以下の項目を指定します。
 - ネットワーク名 →vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

「IP関連」をクリックします。 13.

IP関連の設定項目と「IP基本情報」が表示されます。

IP関連の設定項目の「スタティック経路情報」をクリックします。 14.

「スタティック経路情報」が表示されます。

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

- <
 <tr>
 <スタティック経路情報入力フィールド>

 デフォルトルート

 ・デフォルトリート

 ・ネットワーク指定

 あて先IPアドレス

 がくりック値

 1

 優先度
- 16. [追加] ボタンをクリックします。
- **17. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント 自装置識別情報

→ Aggressive Mode (Initiator) 使用 → 202.168.2.66 → shisya

	● Aggressive Mode(Ir	nitiator)使用
	自側エンドポイン ト	
鍵交換モ ート	相手側エンドポイント	202.168.2.66
	自装置識別情報	shisya
	IDタイプ	⊙ FQDN ○ User-FQDN

21. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

23. 以下の項目を指定します。

認証アルゴリズム

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



24. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

26. 以下の項目を指定します。

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

C and L

■IKE情報		3
ルロ到記録	<mark>鏈識別</mark>	○16進数 ⊙文字列
INCK部理	键	••••••
IKE認証方式	7	shared
ポート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🗸

- 27. [保存] ボタンをクリックします。
- **28. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本社を設定する(Responder)

- 設定メニューのルータ設定で「テンプレート情報」をクリックします。
 「テンプレート情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - テンプレート名 → vpn-shi
 - 接続種別 → IPsec/IKE(RADIUS/AAA)

<テンプレート情報追加フィールド>		
テンプレート名 vpn-shi		
接続種別	● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN)	

機種により、接続種別の表示が上記の画面とは異なります。

3. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shi)」と設定項目が表示されます。

4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 使用するrmtインタフェース →rmt1から1インタフェースを予約
- 参照する AAA 情報 →0
- ・ 鍵交換モード
 ・ Aggressive Mode (Responder)使用
 自側エンドポイント
 ・ 202.168.2.66
 ・ FQDN



- 6. [保存] ボタンをクリックします。
- テンプレート情報 (vpn-shi) の設定項目の「IPsec/IKE 関連」をクリックします。
 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

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

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □ 認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない V	
	SA有効時間	8 時間 🖌	
	SA有効テータ 量	0 GByte 💌	

9. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

- 11. 以下の項目を指定します。
 - SAの設定
 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768 (グループ1)

	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🗸

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **14.** 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 15. 以下の項目を指定します。
 - グループ名

```
→vpn-shisya
```

<グループID情報追加フィールド>			
<mark>ブループ名 vpn-shisya </mark>			

16. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

17. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

٠	RADIUSサービス	→クライアント機能
	認証	→チェックする
	アカウンティング	→チェックする
•	自側認証 IP アドレス	→ 192.168.2.1

• 自側アカウンティングIPアドレス →192.168.2.1

■基本情報		
RADIUSサービス	クライアント機能 ▼ 図認証 マアカウンティング (クライアント機能また(はサーバ機能を選択した 場合にのみ有効となります)	
自側認証IPアトレス	192.168.2.1	
自側アカウンティンク IPアドレス	192.168.2.1	

- 19. [保存] ボタンをクリックします。
- 20. RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」が表示されます。

21. 認証情報1の [修正] ボタンをクリックします。

22. 以下の項目を指定します。

•

認証情報1	
共有鍵	→192.168.2.1
サーバIPアドレス	→192.168.2.5
復旧待機時間	→30分
優先度	→0

	共有鍵	•••••
	サーバIPア ドレス	192.168.2.5
	サーバ UDPポート	⊙1812 ◯1645
認証情報 1	復旧待機 時間	30 分 💙
	優先度	0
	自側認証 IPアドレス	

23. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

24. 認証情報2の[修正] ボタンをクリックします。

● 認証情報2	
共有鍵	→ 192.168.2.1
サーバIPアドレス	→ 192.168.2.6
復旧待機時間	→30分
優先度	→ 100
復旧待機時間 優先度	→30分 →100

	共有鍵	••••••
	サーバIPア ドレス	192.168.2.6
	サーバ UDPポート	⊙1812 ◯1645
認証情報 2	復旧待機 時間	30 分 🗸
	優先度	100
	自側認証 IPアドレス	

26. 認証情報2の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

27. アカウンティング情報1の [修正] ボタンをクリックします。

•	アカウンティング情報1	
	共有鍵	→192.168.2.1
	サーバIPアドレス	→192.168.2.5
	復旧待機時間	→30分
	優先度	→0

	共有鍵	••••••
アカウンティング情報 1	サーバIPア ドレス	192.168.2.5
	サーバ UDPポート	⊙1813 ◯1646
	復旧待機 時間	30 分 🗸
	優先度	0
	自側アカウ ンティング IPアドレス	

- **29. アカウンティング情報1の[保存]ボタンをクリックします**。 「サーバ情報(クライアント機能)」に戻ります。
- 30. アカウンティング情報2の [修正] ボタンをクリックします。

٠	アカウンティング情報2	
	共有鍵	→ 192.168.2.1
	サーバIPアドレス	→192.168.2.6
	復旧待機時間	→30分
	優先度	→ 100

	共有鍵	•••••
	サーバIPア ドレス	192.168.2.6
	サーバ UDPポート	⊙1813 ◯1646
アカウンティング情報 2	復旧待機 時間	30 分 🗸
	優先度	100
	自側アカウ ンティング IPアドレス	

32. アカウンティング情報2の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

33. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.14.15 テンプレート着信機能(動的 VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN

適用機種 全機種

IPsec機能、動的 VPN 情報交換機能およびテンプレート機能を使って、支社間を本社を経由しないで自動鍵交換で VPN を構築する場合の設定方法を説明します。

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

● 前提条件

[支社A (PPPoE常時接続)]

• ローカルネットワーク IPv4 アドレス	: 192.168.1.1/24
 PPPoEユーザ認証ID 	:userid1(プロバイダから提示された内容)
• PPPoEユーザ認証パスワード	:userpass1(プロバイダから提示された内容)
・ PPPoE LAN ポート	:LAN0ポート使用
• NAT機能	:マルチ NAT を使用する
 ネットワーク名 	: internet
● 接続先名	: ISP-1
[支社 B(PPPoE 常時接続)]	
 ローカルネットワーク IPv4 アドレス 	: 192.168.2.1/24
• PPPoEユーザ認証ID	:userid2(プロバイダから提示された内容)
● PPPoEユーザ認証パスワード	:userpass2(プロバイダから提示された内容)
・ PPPoE LANポート	:LAN0ポート使用
• NAT機能	:マルチNATを使用する
 ネットワーク名 	: internet
● 接続先名	: ISP-1
[本社]	

ローカルネットワーク IPv4 アドレス

: 192.168.0.1/24

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


[本社 (Responder)]

- ネットワーク名
- 接続先名
- IPsec/IKE区間
- IPsec対象範囲
- ネットワーク名
- 接続先名 •
- IPsec/IKE 区間 •
- IPsec対象範囲

[共通(本社-支社A、B)]

- 鍵交換タイプ •
- IPsec プロトコル
- IPsec 暗号アルゴリズム •
- IPsec認証アルゴリズム .
- IPsec DH グループ
- IKE 支社 A ID/ID タイプ
- IKE 支社 B ID/ID タイプ
- IKE 支社 A IKE 認証鍵
- IKE 支社 B IKE 認証鍵
- IKE 認証方法
- IKE 暗号アルゴリズム •
- IKE認証アルゴリズム •
- IKE DH グループ

● 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 :更新する セッション更新間隔 ٠ 時間 :5分 • クライアントIPアドレス : 192.168.1.1 ドメイン名 : example.com • VPN 通信 利用インタフェース : rmt0
- 動的 VPN クライアントの優先度 : 10
- 動的 VPN IPv4 経路情報の優先度 : 1

: shisyaA :202.168.2.66 - 支社A

: vpn-shiA

- : IPsec 相手情報を使用するすべてのパケット
- : vpn-shiB
- : shisyaB
- : 202.168.2.66 支社 B
- : IPsec 相手情報を使用するすべてのパケット
- : Aggressive Mode
- : esp
- : des-cbc
- : hmac-md5
- :なし
- :shisyaA(自装置識別情報)/FQDN
- :shisyaB(自装置識別情報)/FQDN
- : abcdefghijklmnopqrstuvwxyz1234567890
- : 1234567890abcdefghijklmnopqrstuvwxyz
- : shared
- : des-cbc
- : hmac-md5
- : modp768

[支社B]

- クライアント情報
- サーバ情報 : 192.168.0.1 アドレス ポート番号 : 5070 認証ID : shisyaBid 認証パスワード : shisyaBpass 有効期間 :1時間 セッション更新間隔 :更新する • 時間 :5分

:0

- 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]

٠

- サーバ機能 : 使用する
 ドメイン名 : example.com
 認証 : 行う
 AAA グループID : 0
- AAAユーザ情報(支社A認証情報) ユーザID : shisyaAid 認証パスワード : shisyaApass
- AAAユーザ情報(支社B認証情報) ユーザID : shisyaBid 認証パスワード : shisyaBpass

[共通(支社A-支社B)]

- IPsecプロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-128
- IPsec認証アルゴリズム :hmac-sha1
- IPsec DHグループ :modp768
- IKE 認証鍵 :ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE認証方法 : shared
 - IKE 暗号アルゴリズム :aes-cbc-128
- IKE 認証アルゴリズム :hmac-sha1
- IKE DH グループ :modp768

·⑦ ヒント ——

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

♦ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社Aを設定する(Initiator)

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3.** 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。
- **「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- **5.** IP **関連の設定項目の「静的 NAT 情報」をクリックします**。 「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

•	プライベートIP情報	
	IPアドレス	→ 192.168.1.1
	ポート番号	→isakmp
•	グローバルIP情報	
	IPアドレス	→指定しない
	ポート番号	→isakmp

プロトコル → udp

<静的NAT情報入力フィールド>			
プライベート	IPアド レス	192.168.1.1	
IP忭青報	ボート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
グローバル	IPアド レス		
IP忭青報	ボート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
プロトコル		udp ✓(番号指定: 7その他"を選択 時のみ有効です)	

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

- フライベートIP情報
 IPアドレス → 192.168.1.1
 ポート番号 → すべて

 グローバルIP情報
 IPアドレス →指定しない
 ポート番号 → すべて

 プロトコル → esp
- 画面上部の「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- **10. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- 11. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

13. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

14. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15. 以下の項目を指定します。

- ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.0.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
- 優先度 →0

<スタティック経路情報入力フィールド>			
ネットワーク	 デフォルトルート ネットワーク指定 あて先IPアドレス 192.168.0.0 あて先アドレスマスク 24 (255.255.255.0) 		
メトリック値 優先度			

16. [追加] ボタンをクリックします。

- 17. 手順 15.~16.を参考に、以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度 →2

18. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

19. 以下の項目を指定します。

● 接続先名

→honsya

• 接続先種別

→IPsec/IKE 接続

機種により、接続先種別の表示が上記の画面とは異なります。

20. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

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

	◎ Aggressive Mode(Initiator)使用	
	自側エンドボイン	
鍵交換モ −ト	相手側エンドボイント 202.168.2.66	
	自装置識別情報 shisyaA	
	IDタイプ O FQDN O User-FQDN	

22. [保存] ボタンをクリックします。

23. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

24. 以下の項目を指定します。

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

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null	
SA	認証アルゴリ ズム	☑hmac-md5 □hmac-sha1 □認証なし	
の設 定	PFS時のDHグ ルーブ	使用しない	
	SA有効時間	8 時間 🖌	
	SA有効データ 量	0 GByte 💌	

- 25. [保存] ボタンをクリックします。
- **26.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

- IKE認証鍵 鍵識別 →文字列 鍵 → abcdefghijkImnopqrstuvwxyz1234567890
 SAの設定
- 暗号アルゴリズム → des-cbc
 認証(ハッシュ)アルゴリズム → hmac-md5
 DHグループ → modp768(グループ1)

■IKE情報		3
11/10/2010/17/24	鏈識別	○16進数 ⊙文字列
INE 66 all 598	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🖌

- 28. [保存] ボタンをクリックします。
- **29. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- **30.** 「クライアント関連情報」をクリックします。 クライアント関連情報の設定項目と「基本情報」が表示されます。
- **31. クライアント関連情報の設定項目の「ドメイン情報」をクリックします**。 「ドメイン情報」が表示されます。
- 32. 以下の項目を指定します。
 - ドメイン名

→ example.com



- **33. [追加] ボタンをクリックします**。 「ドメイン情報(0)」ページが表示されます。
- **34. 「基本情報」をクリックします**。 「基本情報」が表示されます。

•	ドメイン名	→example.com
•	サーバ情報	
	アドレス	→192.168.0.1
	ポート番号	→ 5070
	認証ID	→shisyaAid
	認証パスワード	→ shisyaApass
•	有効期間	→1時間
•	優先度	→ 10
	わいション再新問題	、西ギオス

- セッション更新間隔 →更新する 時間 →5分
 クライアントIPアドレス →192.168.1.1
- VPN通信
 利用インタフェース → rmt0
- 経路情報の優先度
 IPv4 →1

■基本情報		
ドメイン名		example.com
	アドレス	192.168.0.1
	ボート番号	5070
サーバ情報	認証ID	shisyaAid
	認証バスワ ード	•••••
	アドレス	
わかいない	ボート番号	5070
サーバ情報	認証ID	
	認証バスワ ード	
有効期間		1 時間 🖌
優先度		10 🗸
セッション更新間隔		 ● 更新しない ● 更新する 時間 5 分 ▼
クライアントレ	Pアドレス	192.168.1.1
	利用インタフ ェース	rmt0 💌
VPN通信	中継ルータア ドレス	×LANインタフェース選択時のみ指定してく ださい
	終端クロー バルアトレス	
経路情報の	IPv4	1
優先度	更 IPv6	

- 36. [保存] ボタンをクリックします。
- **37. ドメイン情報(0)の設定項目の「自側ネットワーク情報」をクリックします**。 「自側ネットワーク情報」が表示されます。

• 動的 VPN で接続する自側ネットワーク → 192.168.1.0/24

<自側ネットワーク情報入力フィールド>		
動的VPNで接 続する自側ネッ トワーク	192.168.1.0 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/ プレフィックス長形式で入力してください。	

39. [追加] ボタンをクリックします。

40. 設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

41. 以下の項目を指定します。

- テンプレート名 → vpn-shiB
- 接続種別 → IPsec/IKE(動的 VPN)

<テンプレート情報追加フィールド>		
テンプレート名	vpn-shiB	
接続種別	 ○ ISDN ○ IPsec/IKE(RADIUS/AAA) ⊙ IPsec/IKE(動的VPN) 	

機種により、接続種別の表示が上記の画面とは異なります。

42. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shiB)」と設定項目が表示されます。

43. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

44. 以下の項目を指定します。

- 使用するrmtインタフェース →rmt10から10インタフェースを予約
- 自側エンドポイント → 192.168.1.1

使用するrmtインタフェース	rmt10 から10 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケットについて 🛛 🛛 🛛 🔽
自側エントボイント	192.168.1.1

45. [保存] ボタンをクリックします。

46. テンプレート情報 (vpn-shiB) の設定項目の「動的 VPN 関連」をクリックします。

動的 VPN 関連の設定項目と「基本情報」が表示されます。

47. 以下の項目を指定します。

• ドメイン情報 →使用する

"使用する"を選択すると、以下の項目が指定できます。

・ドメイン情報 →0 (example.com)

■基本情報	3
ドメイン情報	 ○ 使用しない ③ 使用する O(example.com) ▼

•

- 48. [保存] ボタンをクリックします。
- 49. テンプレート情報 (vpn-shiB) の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

50. 以下の項目を指定します。

SAの 設定	
暗号アルゴリズム	→aes-cbc-128
認証アルゴリズム	→hmac-sha1
PFS 時の DH グループ	→modp768(グループ1)

IPsec情報		3
暗·	暗号アルゴリズム	□aes-cbc-256 □aes-cbc-192 ☑aes- cbc-128 □3des-cbc □des-cbc □null
SAの設	認証アルゴリズム	□hmac-md5 ☑hmac-sha1 □認証なし
定	PFS時のDHグル ーブ	modp768(グルーブ1) 🔽
\$	SA有効時間	8 時間 🗸
	SA有効データ量	0 GByte 🗸

- 51. [保存] ボタンをクリックします。
- 52. IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

- 53. 以下の項目を指定します。
 - IKE 認証鍵
 鍵識別 →文字列
 鍵 →ABCDI
 - → ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890

 SAの設定 暗号アルゴリズム 認証(ハッシュ)アルゴリズム DHグループ

→aes-cbc-128 →hmac-sha1 →modp768(グループ1)

■IKE情報		3	
गर स्टब्स् इस्ट्रेस	建識別	◯16進数 ⊙文字列	
INERGILE	鍵	•••••	
IKE認証方式	C C	shared	
ポート番号		500	
	暗号アルゴリズ ム	aes-cbc-128 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-sha1 💌	
	DHグループ	modp768(グループ1) 💌	
	SA有効時間	24 時間 🖌	

- 54. [保存] ボタンをクリックします。
- **55.** IPsec/IKE **関連の設定項目の「接続制御情報」をクリックします**。 「接続制御情報」が表示されます。

• 接続先監視 送信元IPアドレス → 192.168.1.1

■接続制御情報		
位在生产组	送信元IP7トレス	192.168.1.1
1女約676561分	正常時送信間隔	▶ ▼

[保存] ボタンをクリックします。 57.

設定メニューのルータ設定で「ACL情報」をクリックします。 58.

「ACL情報」ページが表示されます。

59. 以下の項目を指定します。

定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

[追加] ボタンをクリックします。 60.

「ACL情報(ACL0)」ページが表示されます。

61. 「IP 定義情報」をクリックします。

「IP定義情報」が表示されます。

62. 以下の項目を指定します。

•	プロトコル	→すべて
•	送信元情報	
	IPアドレス	→ 192.168.1.0
	アドレスマスク	→24 (255.255.255.0)
	ナマナはお	

- あて先情報 IPアドレス →192.168.2.0 アドレスマスク →24 (255.255.255.0) →指定なし
- Qos

IP定義情報		3
ブロトコル		すべて (番号指定: ~ その他 ~ を選択時のみ有効です)
_{送信一情} IPアトレス		192.168.1.0
	アトレスマスク	24 (255.255.255.0)
あて失情	IPアドレス	192.168.2.0
おいてい アドレスマ スク		24 (255.255.255.0)
208		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

- 63. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「相手情報」をクリックします。 64. 「相手情報」ページが表示されます。

- 「ネットワーク情報」をクリックします。 65. 「ネットワーク情報」が表示されます。
- 「ネットワーク情報」でネットワーク名が vpn-honの [修正] ボタンをクリックします。 66. 「ネットワーク情報 (vpn-hon)」ページが表示されます。
- 67. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

68. 「動的VPN情報」をクリックします。

「動的 VPN 情報」が表示されます。

69. 以下の項目を指定します。

- 動的VPN 接続 →する 相手ネットマスク →24 (255.255.255.0) 利用するテンプレート情報 →vpn-shiB
- ACL 定義番号 →0



ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<動的VPN情報入力フィールド>			
	 ● する 		
動的VPN接続	相手ネットマスク 24 (255.255.255.0) 🗸		
	利用するテンプレート情報 vpn-shiB 🕶		
	o Utatı		
ACL定義番号	0 参照		

- [追加] ボタンをクリックします。 70.
- 71. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

支社Bを設定する(Initiator)

「支社Aを設定する」を参考に、支社Bを設定します。

「相手情報」-「ネットワーク情報」 「ネットワーク情報(internet)」-「IP 関連」 「静的 NAT 情報」		
• プライベート IP 情報		
IPアドレス	→ 192.168.2.1	
ポート番号	→isakmp	
● グローバル IP 情報		
IPアドレス	→指定しない	
ポート番号	→isakmp	
• プロトコル	→udp	
• プライベート IP 情報		
IPアドレス	→192.168.2.1	
ポート番号	→すべて	
● グローバル IP 情報		
IPアドレス	→指定しない	
ポート番号	→すべて	
• プロトコル	→esp	

「相手情報」-「ネットワーク情報」

•	ネットワーク名	→vpn-hon
۲đ	ネットワーク情報(vpn-hon)」-「	「IP関連」
[2	スタティック経路情報」	
•	ネットワーク	→ネットワーク指定
	あて先IPアドレス	→ 192.168.0.0
	あて先アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→ 1
•	優先度	→ 0
•	ネットワーク	→ネットワーク指定
	あて先IPアドレス	→ 192.168.1.0
	あて先アドレスマスク	→24 (255.255.255.0)
•	メトリック値	→1
•	優先度	→2
旧招	接続先情報」	
•	接続先名	→ honsya
•	接続先種別	→IPsec/IKE 接続
旧招	接続先情報」-「IPsec/IKE接続」	
围	基本情報」	
•	鍵交換モード	→Aggressive Mode(Initiator)使用
	相手側エンドポイント	→202.168.2.66
	自装置識別情報	→shisyaB

「IPsec情報」

•	いた。		
•		-tos obo	
		→ hmac-md5	
F		· IIIIac-IIIuo	
•	IKE認証鍵		
	鍵識別	→文字列	
	鍵	→ 123456789	0abcdefghijklmnopqrstuvwxyz
•	SAの 設定		
	暗号アルゴリズム	→des-cbc	
	認証(ハッシュ)アルゴリズム	→hmac-md5	
	DHグループ	→modp768	(グループ1)
Г≣	油的\/PN/情報 _「クライアン	ト関連情報	「ドメイン情報」
I≝ Ft≡			
1 전			
•		→ example.co	om
•	サーバ情報		
		→ 192.168.0.	1
		→ 5070	
	認証バスリート	→ shisyaBpas	SS
•	有効期間	→1時間	
•	優先度	→ 10	
•	セッション更新間隔	→ 更新する	
	時間	→5分	
•	クライアントIPアドレス	→ 192.168.2.	1
•	VPNI诵信		
	利用インタフェース	→ rmt0	
•			
•	IPv4	→ 1	
ге		,	
IE		4	. 100 100 0 0/04
•	動的 VPN で接続9 る日側ネットワ	-9	→ 192.168.2.0/24
•	動的VPNサーバ登録		→する
ΓĘ	テンプレート情報		
•	テンプレート名	→vpn-shiA	
•	培績和別	→ IPsoc/IKE	(動的VPN)
г-			
	「ノノレート情報(Vpn-sniA)」-	共進情報」	
垣			
•	使用するrmtインタフェース	→rmt10から	10インタフェースを予約
•	自側エンドポイント	→ 192.168.2.	1
F٦	テンプレート情報(vpn-shiA)」-	「動的VPN関連	重」
「基	基本情報」		

• ドメイン情報 →使用する

「テンプレート情報(vpn-shiA)」-	「IPsec/IKE 関連」
「IPsec情報」	
 SAの設定 	
暗号アルゴリズム	→aes-cbc-128
認証アルゴリズム	→hmac-sha1
PFS 時の DH グループ	→modp768(グループ1)
「IKE情報」	
● IKE認証鍵	
鍵識別	→文字列
鍵	→ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
 SAの設定 	
暗号アルゴリズム	→aes-cbc-128
認証(ハッシュ)アルゴリズム	→hmac-sha1
DHグループ	→modp768(グループ1)
「接続制御情報」	
● 接続先監視	
送信元IPアドレス	→ 192.168.2.1
「ACL情報」	
「ACL 情報」 • 定義名	→ ACL0
「ACL 情報」 ● 定義名 「ACL 定義情報(ACL0)」- 「IP 定言	→ ACL0 義情報」
「ACL 情報」 • 定義名 「ACL 定義情報 (ACL0)」-「IP 定語 • プロトコル	→ACL0 義情報」 →すべて
「ACL 情報」 定義名 「ACL 定義情報 (ACL0)」-「IP 定義 プロトコル 送信元情報 	→ ACL0 義 情報」 →すべて
 「ACL 情報」 定義名 「ACL 定義情報 (ACL0)」-「IP 定調 プロトコル 送信元情報 IP アドレス 	→ ACL0 義情報」 →すべて → 192.168.2.0
 「ACL 情報」 定義名 「ACL 定義情報 (ACL0)」-「IP 定義 プロトコル 送信元情報 IPアドレス アドレスマスク 	→ ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0)
 「ACL 情報」 定義名 「ACL 定義情報 (ACL0)」-「IP 定義 プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0)
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定: プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定書 プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0)
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定書 プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク のて先情報 IPアドレス アドレスマスク QoS	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0) → 指定なし
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定: プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク QoS 「相手情報」-「ネットワーク情報 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0) → 指定なし 報」
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定: プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク QoS 「相手情報」-「ネットワーク情 「ネットワーク情報 (vpn-hon)」- 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0) → 指定なし 報」 「IP 関連」
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定書 プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク GoS 「相手情報」-「ネットワーク情報 「ネットワーク情報 (vpn-hon)」- 「動的VPN情報」 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0) → 指定なし 報」 「IP 関連」
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定: プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク ④のS 「相手情報」-「ネットワーク情: 「ネットワーク情報 (vpn-hon)」- 「動的 VPN 情報」 動的 VPN 接続 	 → ACL0 義情報」 → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0) → 指定なし 報J 「IP 関連」 → する
 「ACL情報」 定義名 「ACL定義情報 (ACL0)」-「IP定: プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク のS 「相手情報」-「ネットワーク情: 「ネットワーク情報 (vpn-hon)」- 動的 VPN 情報」 動的 VPN 接続 相手ネットマスク 	 → ACL0 義情報J → すべて → 192.168.2.0 → 24 (255.255.255.0) → 192.168.1.0 → 24 (255.255.255.0) → 指定なし 報J 「IP 関連」 → する → 24 (255.255.255.0)

利用するテンプレート情報 → vpn-shiA • ACL定義番号 → 0

本社を設定する(Responder)

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shiA

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-shiA	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0 あて先アドレスマスク →24 (255.255.255.0)
 メトリック値 →1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → shisyaA
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

 鍵交換モード 自側エンドポイント

→ Aggressive Mode(Responder)使用 → 202.168.2.66



13. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5



16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

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



- 19. [保存] ボタンをクリックします。
- **20.** 手順1.~19.を参考に、支社Bを設定します。
- **21. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **22. 「グループID情報」をクリックします**。 「グループID情報」が表示されます。

グループ名

→ dvpnserver

<グループID情報追加フィールド>		~`>
グループ名	dvpnserver	

24. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

25. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

- 26. 以下の項目を指定します。
 - ユーザID

→ shisyaAid

<AAAユーザ情報追加フィールド>

- **27. [追加] ボタンをクリックします**。 「AAA ユーザ情報(0)」と設定項目が表示されます。
- **28. 「認証情報」をクリックします**。 「認証情報」が表示されます。
- 29. 以下の項目を指定します。
 - ● 認証パスワード
 → shisyaApass

認証情報		
ユーザID	shisyaApass	
認証バスワード	•••••	

- 30. [保存] ボタンをクリックします。
- 31. 手順21.~29.を参考に、支社Bを設定します。
- **32. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- **33. 「サーバ関連情報」をクリックします。** サーバ関連情報の設定項目と「基本情報」が表示されます。

→使用する
→ example.com
→行う
→0

■基本情報	R	3
	 ○ 使用しばい ● 使用する 	
サーバ機能	ドメイ ン名 example.com	
7 7 798 86	 ○ 行わない ◎ 行う AAAグループID 0 	

- 35. [保存] ボタンをクリックします。
- **36. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.14.16 テンプレート着信機能(動的VPN)を使用した IPv4 over IPv4で固定 IP アドレスでの VPN(冗長構成)

適用機種 全機種

IPsec機能、動的 VPN 情報交換機能およびテンプレート機能を使って、自動鍵交換で VPN を冗長構成で構築する 場合の設定方法を説明します。

ここでは「2.14.15 テンプレート着信機能(動的VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでのVPN」 (P611) で説明したネットワーク構成で、支社と本社が動的 VPN によって接続されていることを前提とします。 ただし、支社 A は VRRP による冗長構成の設定を行います。



● 設定条件(冗長構成)

[支社A (Si-R1)]

•	ローカルネットワーク IPv4 アドレス	: 192.168.1.10/24		
•	VRRP優先度	: 254		
•	動的 VPN クライアントの優先度	: 1		
•	ノードダウントリガ	: 202.168.2.66		
	[支社A(Si-R2)]			
[3	社A (Si-R2)]			
•	【社A(Si-R2)】 ローカルネットワーク IPv4 アドレス	: 192.168.1.11/24		
• •	社A(Si-R2)】 ローカルネットワークIPv4 アドレス VRRP 優先度	: 192.168.1.11/24 : 100		

[支社A (共通)]

•	VRRP仮想IPアドレス	: 192.168.1.1/24
•	VRRPグループID	: 10
•	OSPFエリアID	: 0.0.0.0

上記の設定条件に従って設定を行う場合の設定例を示します。

支社Aを設定する(Si-R1)

「2.14.15 テンプレート着信機能(動的 VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN」(P.611)を 参考に、動的 VPN での設定を事前に行います。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。
 「LAN1 情報(物理LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 192.168.1.10
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報				
IPv4	⊙使用する○使用しない			
IPアドレス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 192: ネットマスク 24 (0) ブロードキャストアドレ ス 	168.1.10 255.255.255.255.255.255.255.255.255.255		

- 5. [保存] ボタンをクリックします。
- 6. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます

7. 以下の項目を指定します。

OSPF機能 →使用する

■OSPF情報		3
OSPF機能	○使用しない⊙使用する	

8. [保存] ボタンをクリックします。

9. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

10. 以下の項目を指定します。

● VRRP機能

→使用する

VRRP機能	○ 使用しない③ 使用する
	バスワード

Si-R180、180Bでは、LANバックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

- 11. [保存] ボタンをクリックします。
- **12. 共通情報の設定項目の「VRRP グループ情報」をクリックします**。 「VRRP グループ情報」が表示されます。
- **13.** 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。 VRRP グループ情報の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

•	グループID	→ 10
•	プライオリティ	→優先度指定
	優先度	→254
	仮想IPアドレス	→192.168.1.1
•	プリエンプトモード	→OFF

■基本情報	3	
グループID	10	
	◎ 優先度指定	
	優先度 254	
ブライオリティ	254	
	○ 優先度固定(最優先)	
	優先度 255	
	仮想IPアドレス インタフェースアドレスを使用	
AD送信間隔	1 秒	
	O ON	
ブリエンブトモード	⊙ OFF	
	移行禁止時間 0 秒	

- 15. [保存] ボタンをクリックします。
- **16.** VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。

- 減算プライオリティ
- →254 →ノードダウントリガ (node) • トリガ種別 あて先IPアドレス →202.168.2.66 送出インタフェース →指定なし 再送間隔 →5 タイムアウト時間 →16 正常時送信間隔 **→** 17 異常時送信間隔 →30

<vrrpトリガ情報入力フィールド></vrrpトリガ情報入力フィールド>			
減算ブライ オリティ	254		
	○ インタフェースダウントリガ(ifdown)		
	インタフェース すべて 💌		
	○ ルートダウントリガ(route)		
トリガ種別	・デフォルトルート ネットワ ・経路を指定する あて先IPアド レス あて先アドレ スマスク インタフ 北定なし		
	 シートメリントリル(node) あて先IPアドレス 202.168.2.66 		
送出インタフェース 指定なし 🗸			
	再送間隔 5 秒		
タイムアウト時間 16 秒 正常時送信間隔 17 秒			
	異常時送信間隔 30 秒		

- [追加] ボタンをクリックします。 18.
- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。 19. 「ルーティングプロトコル情報」ページが表示されます。
- 「ルーティングマネージャ情報」をクリックします。 20.

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

- 21. 以下の項目を指定します。
 - OSPF スタティック経路情報 → 再配布する メトリック値 **→** 20 メトリックタイプ → type2

	○ 再配布しない● 再配布する
OSPF スタティック経路情報	メトリック値 20 メトリックタイプ type2 🗸

22. [保存] ボタンをクリックします。

23. 「OSPF関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

- **24.** OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。 「OSPF エリア情報」が表示されます。
- 25. [追加] ボタンをクリックします。
- 26. 以下の項目を指定します。
 - エリアID

→ 0.0.0.0

■OSPFエリア基本情報		3
エリアID	0.0.0.0	

- 27. [保存] ボタンをクリックします。
- **28. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- **29. 「クライアント関連情報」をクリックします。** クライアント関連情報の設定項目と「基本情報」が表示されます。
- **30.** クライアント関連情報の設定項目の「ドメイン情報」をクリックします。 「ドメイン情報」が表示されます。
- **31.** 「ドメイン情報」で定義番号が0の [修正] ボタンをクリックします。 「ドメイン情報(0)」ページが表示されます。
- 32. 以下の項目を指定します。
 - 優先度 →1 (最優先)
 - クライアントIPアドレス → 192.168.1.10

優先度	1(最優先) 🕶
セッション更新間隔	 ● 更新しない ● 更新する 時間 5 分 ▼
クライアントIPアトレス	192.168.1.10

- 33. [保存] ボタンをクリックします。
- **34. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **35. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- **36.** 「ネットワーク情報」でネットワーク名が internet の [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。
- **37. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。

38. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

39. 「静的NAT情報」でプライベートアドレスが192.168.1.1の【修正】ボタンをクリックします。

40. 以下の項目を指定します。

 プライベートIP情報 IPアドレス

→ 192.168.1.10



- 41. [保存] ボタンをクリックします。
- 42. 手順 39. ~ 41. を参考に、以下の項目を指定します。
 - プライベートIP情報
 IPアドレス → 192.168.1.10
- **43. 画面上部の「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **44.** 「ネットワーク情報」でネットワーク名が vpn-hon の [修正] ボタンをクリックします。 「ネットワーク情報 (vpn-hon)」ページが表示されます。
- **45. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- **46.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- **47.** 「スタティック経路情報」であて先IPアドレス/マスクが192.168.2.0/24の【修正】ボタンをクリックします。
- 48. 以下の項目を指定します。
 - 優先度 → 200
 優先度 200
- 49. [保存] ボタンをクリックします。
- **50. 設定メニューのルータ設定で「テンプレート情報」をクリックします**。 「テンプレート情報」ページが表示されます。
- **51.** 「テンプレート情報」でテンプレート名が vpn-shiB の [修正] ボタンをクリックします。 「テンプレート情報 (vpn-shiB)」ページが表示されます。
- **52. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。

- 53. 以下の項目を指定します。
 - 自側エンドポイント → 192.168.1.10

自側エンドボイント 192.168.1.10

- 54. [保存] ボタンをクリックします。
- **55.** 「IPsec/IKE 関連」をクリックします。 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。
- **56.** IPsec/IKE **関連の設定項目の「接続制御情報」をクリックします**。 「接続制御情報」が表示されます。
- 57. 以下の項目を指定します。
 - 接続先監視
 送信元IPアドレス → 192.168.1.10

■接続制御	青報	3
拉结开时间	送信元IPアトレス	192.168.1.10
1女称7.70亩代	正常時送信間隔	▶ ▼

- 58. [保存] ボタンをクリックします。
- **59. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

支社Aを設定する(Si-R2)

「支社Aを設定する(Si-R1)」を参考に、Si-R2を設定します。

LAN1情報を設定する

「LAN1 情報」-「IP 関連」	
「IPアドレス情報」	
 IPアドレス 	→192.168.1.11
「OSPF情報」	
• OSPF機能	→使用する
「LAN1 情報」-「共通情報」 「基本情報」 ・ VRRP機能 「VRRP グループ0 情報」 「基本情報」	→使用する
• グループID	→ 10
 プライオリティ 優先度 仮想 IP アドレス 	→優先度指定 →100 →192.168.1.1
• プリエンプトモード	→OFF

OSPF 情報を設定する

「ルーティングプロトコル情報」-「ルーティングマネージャ情報」 「再配布情報」

OSPF

スタティック経路情報	→再配布する
メトリック値	→20
メトリックタイプ	→type2

「ルーティングプロトコル情報」-「OSPF 関連」-「ルータ ID 情報」 「OSPF エリア情報」

エリアID → 0.0.0.0

動的VPN情報を設定する

「動的 VPN 情報」-「クライアント関連情報」-「ドメイン情報」 「基本情報」 • 優先度 →2

クライアントIPアドレス → 192.168.1.11

相手情報を設定する

「相手情報」-「ネットワーク情報(internet)」-「IP 関連」 「静的 NAT 情報」

プライベートIP情報
 IPアドレス → 192.168.1.11

「相手情報」-「ネットワーク情報(vpn-hon)」-「IP 関連」 「スタティック経路情報」

優先度 →200

テンプレート情報を設定する

「テンプレート情報」-「共通情報」 「基本情報」

● 自側エンドポイント → 192.168.1.11

「テンプレート情報」-「IPsec/IKE 関連」 「接続制御情報」 • 接続先監視

・ 接続元監祝 送信元 IP アドレス → 192.168.1.11

本社を設定する

「2.14.15 テンプレート着信機能(動的 VPN)を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN」(P.611)を 参考に、本社を設定します。 相手情報を設定する 「相手情報」-「ネットワーク情報 (vpn-shiA)」-「IP 関連」 「スタティック経路情報」 優先度 → 10 「相手情報」-「ネットワーク情報」 ネットワーク名 →vpn-shia 「ネットワーク情報 (vpn-shia)」-「IP 関連」 「スタティック経路情報」 ネットワーク →ネットワーク指定 あて先IP アドレス → 192.168.1.0 →24 (255.255.255.0) あて先アドレスマスク メトリック値 **→**1 優先度 →254 「接続先情報」 • 接続先名 → shisyaa 接続先種別 →IPsec/IKE 接続 「接続先情報」-「IPsec/IKE接続」 「基本情報」 鍵交換モード → Aggressive Mode (Responder) 使用 自側エンドポイント →202.168.2.66 相手装置識別情報 → shisyaa 「IPsec情報」 • SAの設定 暗号アルゴリズム → des-cbc 認証アルゴリズム →hmac-md5 「IKE情報」 • IKE 認証鍵 鍵識別 →文字列 鍵 → abcdefghijklmnopqrstuvwxyz1234567890 SAの設定 暗号アルゴリズム → des-cbc 認証(ハッシュ)アルゴリズム →hmac-md5 DHグループ →modp768 (グループ1)

2.14.17 テンプレート着信機能(動的 VPN)を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN

適用機種 全機種

IPsec機能、動的VPN 情報交換機能およびテンプレート機能を使って、支社間を本社を経由しないで自動鍵交換でVPN を構築する場合の設定方法を説明します。

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

● 前提条件

[支社A (PPPoE常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワーク IPv6 アドレス : 2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス

: 202.168.1.66/24

:LAN0ポート使用

: 2001:db8:1111:1::66/64

- 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
- PPPoEユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1(プロバイダから提示された内容)
 - PPPoE LAN ポート

[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
- 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)
 - :LAN0 ポート使用

[本社]

PPPoE LAN ポート

- ローカルネットワーク IPv4 アドレス : 192.168.0.1/24
 ローカルネットワーク IPv6 アドレス : 2001:db8:1111:4::1/64
 - インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス : 2001:db8:1111:2::66/64
 - インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス:202.168.2.65
 - インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス: 2001:db8:1111:2::65



● 設定条件(VPN 接続)

[支社A]

- ネットワーク名
- : vpn-hon

- 接続先名
- IPsec/IKE区間
- IPsec対象範囲
- テンプレート名
- IPsec/IKE 始点
- 接続先監視アドレス

[支社B]

- ネットワーク名
- 接続先名
- IPsec/IKE区間
- IPsec 対象範囲
- テンプレート名
- IPsec/IKE 始点

- : honsya
- : 2001:db8:1111:1::66 2001:db8:1111:2::66
- : IPsec 相手情報を使用するすべてのパケット
- ∶vpn-shiB
- : 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
- : 2001:db8:1111:3::1
- : vpn-hon
- : honsya
- : 2001:db8:1111:1::67 2001:db8:1111:2::66
- : IPsec 相手情報を使用するすべてのパケット
- ∶vpn-shiA
- : 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 •

接続先名

- : vpn-shiA
- : shisyaA
 - : 2001:db8:1111:2::66 2001:db8:1111:1::66
 - : IPsec 相手情報を使用するすべてのパケット

: 2001:db8:1111:2::66 - 2001:db8:1111:1::67 : IPsec 相手情報を使用するすべてのパケット

IPsec対象範囲 ネットワーク名

IPsec/IKE区間

- 接続先名
- IPsec/IKE区間
- IPsec対象範囲

[共通(本社-支社A、B)]

- 鍵交換タイプ
- IPsec プロトコル ٠
- IPsec 暗号アルゴリズム
- IPsec 認証アルゴリズム
- IPsec DH グループ
- IKE 支社 A IKE 認証鍵
- IKE 支社 B IKE 認証鍵
- IKE 認証方法
- IKE 暗号アルゴリズム
- IKE 認証アルゴリズム
- IKE DH グループ

● 設定条件(動的 VPN 接続)

[支社A]

٠

- クライアント情報
- サーバ情報 アドレス : 2001:db8:1111:4::1 ポート番号 : 5070 認証ID : shisyaAid 認証パスワード : shisyaApass
 - 有効期間 :1時間
- セッション更新間隔 :更新する ٠ 時間 :5分
- クライアントIPアドレス : 2001:db8:1111:3::1 ٠
- 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

- : Main Mode
- : esp
- : des-cbc

: vpn-shiB

: shisyaB

- : hmac-md5
- :なし
- : abcdefghijklmnopqrstuvwxyz1234567890
- : 1234567890abcdefghijklmnopqrstuvwxyz
- : shared
- : des-cbc
- : hmac-md5
- : modp768

:0

• -	サーバ情報	
-	アドレス	: 2001:db8:1111:4::1
5	ポート番号	: 5070
Ē	認証ID	: shisyaBid
Ē	認証パスワード	: shisyaBpass
• 7	有効期間	:1 時間
• -	セッション更新間隔 時間	: 更新する :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	
7	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	社]	
• -	サーバ機能	:使用する
	ドメイン名	: example.com
Ē		: 行う
/		. 0
• /	AAAユーザ情報(支社A認証情報) コーザID	
-	ユーリ レ 認証 パフ ロ ド	shisyaAld
г •		· SIIISyaApass
• /	AAA ユーリ 旧報(又社 D 認証 旧報) フ ― ザ ID	, shisvaBid
-	認証パスワード	: shisyaBia
[共j	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
•	KF 認証鍵	: ABCDEEGHUKI MNOPORSTUVWXY71234567890
•	IKE認証方法	: shared
•	IKF 暗号アルゴリズム	i aes-chc-128
• 1	IKF認証アルゴリズム	· hmac-sha1
- I		· mildesilat
•		· 1100h/08

ど
と
ント

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合の設定例を示します。

支社Aを設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-hon	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - IPv6

→使用する

■IPv6基本情報		3
IPv6	●使用しない●使用する	

- 7. [保存] ボタンをクリックします。
- **8.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。
- 9. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先プレフィックス/プレフィックス長
 → 2001:db8:1111:4::/64
 - メトリック値

優先度

- **→** 1

→0

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>				
ネットワーク	 デフォルトルート ネットワーク指定 あて先ブレフィ ックス/ブレフィ ィックス長 2001:db8:1111:4:: 			
メトリック値	1 💌			
優先度	0			

10. [追加] ボタンをクリックします。

- 11. 手順9.~10.を参考に、以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先プレフィックス/プレフィックス長
 → 2001:db8:1111:5::/64
 - メトリック値 →1
 - 優先度 →2
- 12. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

13. 以下の項目を指定します。

- 接続先名
- →honsya

→ IPsec/IKE 接続

- 接続先種別
- <接続先情報追加フィールド> <mark>接続先名</mark> honsya ○ ATM接続 VCI ○ 専用線接続 ⊙ 通常接続 使用インタフェース WAN1 🗸 ○ 論理リンクにバンドルする 使用インタフェー WAN1 🔽 2 バンドル先 選択できる定義がありません 🗸 ◯ ISDN接続 ⊙ 通常接続 使用インタフェース すべて 🗸 接続先種 電話番号 ダイヤル1 サブアドレス 別 ○ 論理リンクにバンドルする 使用インタフェー すべて 🗸 ス バンドル先 選択できる定義がありません 🔽 ○ フレームリレー接続 DLCI ○ PPP₀E接続 ○ IPトンネル接続 ⊙ IPsec/IKE接続 ○ 別インタフェースから送出 ○ MPLSトンネル接続 ○ バケット破棄

機種により、接続先種別の表示が上記の画面とは異なります。

14. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

•	鍵交換モード	→ Main Mode 使用
	相手側エンドポイント	→2001:db8:1111:2::66
	自側エンドポイント	→2001:db8:1111:1::66
	◎ Main Mode使用	

	◎ Main Model发用
建态换于	相手側て、バボイ
	2001:db8:1111:2:66
•	
	目側エンドボイン 0001/#0.1111.1/06
	•

16. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

18. 以下の項目を指定します。

- 対象パケット 自側IPアドレス/マスク →IPv6すべて 相手側IPアドレス/マスク →IPv6すべて
- SAの設定
 暗号アルゴリズム → des-cbc
 認証アルゴリズム → hmac-md5

■IPsec情報(自動鍵)		
対象 パケ ット	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしく(JIPv6アドレ ス/ブレフィックス長形式で入力してください。
	相手側IPアト レス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
SA の設 定	暗号アルゴリ ズム	aes-cbc-256 aes-cbc-192 aes-cbc-128 3des-cbc ✓ des-cbc null
	認証アルゴリ ズム	▼hmac-md5 □hmac-sha1 □認証なし
	PFS時のDHグ ループ	使用しない
	SA有効時間	8 時間 🗸
	SA有効データ 量	0 GByte 💌

- 19. [保存] ボタンをクリックします。
- **20.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。
| • | IKE 認証
鍵識別
鍵 | 鍵 | | →文字列
→abcdefghijkImnopqrstuvwxyz1234567890 |
|---|-------------------------------|------------------------------|-------|---|
| • | SAの設知
暗号アル
認証(ハ
DHグル | 定
/ゴリズム
\ッシュ)アルゴ
ープ | リズム | →des-cbc
→hmac-md5
→modp768(グループ1) |
| | IKE情報 | | | 3 |
| Т | KF認証鍵 | 键 識別 | ◯16進数 | ₹●文字列 |

いと言語言語会社	鏈識別	○16進数 ⊙文字列
INE認証要	鏈	••••••
IKE認証方式	7	shared
ボート番号		500
	暗号アルゴリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🖌

- 22. [保存] ボタンをクリックします。
- **23. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- **24. 「クライアント関連情報」をクリックします。** クライアント関連情報の設定項目と「基本情報」が表示されます。
- **25.** クライアント関連情報の設定項目の「ドメイン情報」をクリックします。 「ドメイン情報」が表示されます。
- 26. 以下の項目を指定します。
 - ドメイン名

→example.com



- **27. [追加] ボタンをクリックします。** 「ドメイン情報(0)」ページが表示されます。
- **28. 「基本情報」をクリックします**。 「基本情報」が表示されます。

ドメイン名 → example.com
 サーバ情報

 アドレス → 2001:db8:1111:4::1
 ポート番号 → 5070
 認証 ID → shisyaAid
 認証パスワード → shisyaApass

 有効期間 → 1 時間
 優先度 → 10

→更新する

→2001:db8:1111:3::1

→5分

→1

- セッション更新間隔
 時間
- クライアントIPアドレス
- VPN 通信
 利用インタフェース → rmt0
- 経路情報の優先度
 IPv6

■基本情報		
ドメイン名		example.com
	アドレス	2001:db8:1111:4::1
	ボート番号	5070
サーバ情報	認証ID	shisyaAid
	認証バスワ ード	••••••
	アトレス	
セカン (511	ボート番号	5070
サーバ情報	認証ID	
	認証バスワ ード	
有効期間		1 時間 🖌
優先度		10 💌
セッション更新問隔		 ● 更新しない ● 更新する ● 時間 5 分 ▼
クライアントロ	Pアドレス	2001:db8:1111:3::1
	利用インタフ ェース	rmt0 💌
VPN通信	中継ルータア ドレス	×LANインタフェース選択時のみ指定してく ださい
	終端クロー バルアドレス	
経路情報の	IPv4	
優先度	IPv6	1

- 30. [保存] ボタンをクリックします。
- **31. ドメイン情報(0)の設定項目の「自側ネットワーク情報」をクリックします**。 「自側ネットワーク情報」が表示されます。

• 動的 VPN で接続する自側ネットワーク → 2001:db8:1111:3::/64

<自側ネットワーク情報入力フィールド>		
動的VPNで接	2001:db8:1111:3::	
続する自側ネッ	※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/	
トワーク	ブレフィックス長形式で入力してください。	

- 33. [追加] ボタンをクリックします。
- 34. 設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

35. 以下の項目を指定します。

- テンプレート名 → vpn-shiB
- 接続種別 → IPsec/IKE (動的 VPN)

<テンプレート情報追加フィールド>		
テンプレート名	vpn-shiB	
接続種別	● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN)	

機種により、接続種別の表示が上記の画面とは異なります。

36. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shiB)」と設定項目が表示されます。

37. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

38. 以下の項目を指定します。

- 使用するrmtインタフェース →rmt10から10インタフェースを予約
- 自側エンドポイント →2001:db8:1111:1::66

使用するrmtインタフェース	rmt10 から10 インタフェースを予約
MTUサイズ	1500 / バイト
無通信監視タイマ	送受信パケットについて 0 秒 💌
自側エントポイント	2001:db8:1111:1::66

- 39. [保存] ボタンをクリックします。
- **40.** テンプレート情報(vpn-shiB)の設定項目の「動的 VPN 関連」をクリックします。 動的 VPN 関連の設定項目と「基本情報」が表示されます。

・ドメイン情報 →使用する
 "使用する"を選択すると、以下の項目が指定できます。

ドメイン情報 →0 (example.com)

■基本情報	3
ドメイン情報	 ○ 使用しばい ③ 使用する
	O(example.com) 💙

- 42. [保存] ボタンをクリックします。
- 43. テンプレート情報(vpn-shiB)の設定項目の「IPsec/IKE 関連」をクリックします。

IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

44. 以下の項目を指定します。

 SAの設定 暗号アルゴリズム → aes-cbc-128
 認証アルゴリズム → hmac-sha1
 PFS時のDHグループ → modp768 (グループ1)

■IPsec情報		
	暗号アルゴリズム	□aes-cbc-256 □aes-cbc-192 ☑aes- cbc-128 □3des-cbc □des-cbc □null
SAの設	認証アルゴリズム	□hmac-md5 ☑hmac-sha1 □認証なし
定	PFS時のDHグル ープ	modp768(グループ1) 🔽
	SA有効時間	8 時間 🗸
	SA有効データ量	0 GByte 🗸

45. [保存] ボタンをクリックします。

46. IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE情報」が表示されます。

47. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 →文字列 鍵 →ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
 SAの設定

暗号アルゴリズム → aes-cbc-128 認証(ハッシュ)アルゴリズム → hmac-sha1 DHグループ → modp768(グループ1)

IKE情	報	3
IKE認証	键識別	○16進数 ⊙文字列
键	鏈	•••••
IKE認証	方式	shared
 SAの設 定	暗号アルゴリズム	aes-cbc-128 💌
	認証(ハッシュ)アル ゴリズム	hmac-shal 💌
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🕶

- 48. [保存] ボタンをクリックします。
- **49.** IPsec/IKE **関連の設定項目の「接続制御情報」をクリックします**。 「接続制御情報」が表示されます。
- 50. 以下の項目を指定します。
 - 接続先監視
 送信元 IP アドレス

$\rightarrow 2001 \cdot dh R \cdot 1111 \cdot 2 \cdot 1$	
² 2001.000.1111.3.1	

■接続制御情報			3
位在生产组	送信元IP ア トレス	2001:db8:1111:3::1	
按称兀监祝	正常時送信間隔	秒 🗸	_

- 51. [保存] ボタンをクリックします。
- 52. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

- 53. 以下の項目を指定します。
 - IPv6 →使用する
 - インタフェースID →自動

■IPv6基本情報	3
IPv6	○使用しない ⊙使用する
インタフェースID	 ● 自動 ○ 指定する

- 54. [保存] ボタンをクリックします。
- **55. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 56. 以下の項目を指定します。
 - 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

- **57. [追加] ボタンをクリックします。** 「ACL定義情報(ACL0)」ページが表示されます。
- **58.** 「IPv6 定義情報」をクリックします。 「IPv6 定義情報」ページが表示されます。

- プロトコル
- 送信元 IPv6アドレス/プレフィックス長
- あて先 IPv6アドレス/プレフィックス長
- QoS

- →すべて
- →2001:db8:1111:3::/64
- →2001:db8:1111:5::/64
- →指定なし

■IPv6定義情報	3
プロトコル	すべて ▼ (番号指定:、その他″を選択時のみ有効です)
送信元IPv6アトレ ス/フレフィックス	2001:dv8:1111:3::
あて先IPv6アドレ スノブレフィックス	2001:dv8:1111:5:
QoS	指定なし ▼ Traffic Class、または、DSCPを選択時に値を入力 してください

- 60. [保存] ボタンをクリックします。
- **61. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **62. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- **63.** 「ネットワーク情報」でネットワーク名が vpn-hon の [修正] ボタンをクリックします。 「ネットワーク情報 (vpn-hon)」ページが表示されます。
- **64. 「**IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

65. 「IPv6動的VPN情報」をクリックします。

66. 以下の項目を指定します。

- 動的VPN接続 →する
 相手プレフィックス長 → 64
 利用するテンプレート情報 → vpn-shiB
- ACL定義番号 →0

「ACL定義番号」を指定する際は、[参照] ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<ipv6動的vpn情報入力フィールド></ipv6動的vpn情報入力フィールド>		
動的VPN接続	 ● する 相手ブレフィックス長 64 利用するテンプレート情報 vpn-shiB ▼ ● しびふい 	
ACL定義番号	0 参照	

- 67. [追加] ボタンをクリックします。
- 68. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

支社Bを設定する

「支社Aを設定する」を参考に、支社Bを設定します。

「朴	「相手情報」-「ネットワーク情報」		
•	ネットワーク名	→vpn-hon	
「ネ	、ットワーク情報」-「IPv6 関連」		
ΓIF	Pv6基本情報」		
•	IPv6	→使用する	
ΓIF	₽v6スタティック経路情報」		
•	ネットワーク あて先プレフィックス/プレフィッ	ックス長	→ネットワーク指定 →2001:db8:1111:4::/64
•	メトリック値		→ 1
•	優先度		→ 0
•	ネットワーク あて先プレフィックス/プレフィ	ックス長	→ネットワーク指定 →2001:db8:1111:3::/64
•	メトリック値		→ 1
•	優先度		→2
「授	続先情報」		
•	接続先名	→honsya	
•	接続先種別	→IPsec/IKE	接続
「挼	続先情報」-「IPsec/IKE接続」		
「基	「本情報」		
•	鍵交換モード	→ Main Mod	e使用
	相手側エンドポイント	→2001:db8:1	1111:2::66
	自側エンドポイント	→2001:db8:1	1111:1::67
ΓIF	Psec情報」		
•	対象パケット 自側IPアドレス/マスク 相手側IPアドレス/マスク	→IPv6すべて →IPv6すべて	-
•	SAの設定 暗号アルゴリズム 認証アルゴリズム	→des-cbc →hmac-md5	
۲IK	KE 情報」		
•	IKE 認証鍵 鍵識別 鍵	→文字列 →123456789	90abcdefghijklmnopqrstuvwxyz
•	SA い設定 暗号アルゴリズム 認証(ハッシュ)アルゴリズム DH グループ	→ des-cbc → hmac-md5 → modp768	(グループ1)

「動的 VPN 情報」-「クライアン 「基本情報」	ト関連情報」-「ドメイン情報」
• ドメイン名	→ example.com
 サーバ情報 	
アドレス	→ 2001:db8:1111:4::1
ポート番号	→ 5070
認証ID 詞言パコロード	→ shisyaBid
認証ハスワート	→ shisyaBpass
• 有効期間	
● 優先皮	$\rightarrow 10$
 セッション更新間隔 	→ 更新する
 クライアントIPアドレス 	→ 2001:db8:1111:5::1
• VPN 通信	
利用インタフェース	→ rmtu
 経路情報の優先度 IPv6 	→ 1
	1-ク → 2001·db8·1111·5··/24
	→ オろ
	$\rightarrow 9$ w
「テンプレート情報」	
• テンプレート名	→ vpn-shiA
● 接続種別	→IPsec/IKE(動的VPN)
「テンプレート情報(vpn-shiA)」-	「共通情報」
「基本情報」	
 使用するrmtインタフェース 	→rmt10から10インタフェースを予約
• 自側エンドポイント	→2001:db8:1111:1::67
「テンプレート情報(vpn-shiA)」-	「動的VPN関連」
「基本情報」	
• ドメイン情報	→使用する
「テンプレート情報(vpn-shiA)」-	「IPsec/IKE 関連」
「IPsec情報」	
• SAの設定	
暗号アルゴリズム	→aes-cbc-128
認証アルゴリズム	→ hmac-sha1
PFS時のDH クルーフ	→modp768 (クルーフ1)
• IKE 認証鍵	
避 識 別	→又字列 → ABCDEECHLIKI MNOPORSTUVA/XV71234567890
₩ • \$^0;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2;2	
 SAU 設定 暗号アルゴリズム 	→aes-cbc-128
認証 (ハッシュ) アルゴリズム	→hmac-sha1
DHグループ	→modp768(グループ1)

「接続制御情報」

1.13	באד כון ישוניויטעויא		
•	接続先監視 送信元 IP アドレス	→2001:db8:	1111:5::1
٢E	テンプレート情報(vpn-shiA)」-	「IPv6関連」	
ГП	Pv6基本情報」		
•	IPv6	→使用する	
•	インタフェースID	→自動	
٢A	ACL情報」		
•	定義名	→ ACL0	
٢A	CL定義情報(ACL0)」-「IPv65	È義情報」	
•	プロトコル		→すべて
•	送信元 IPv6アドレス/プレフィ	ックス長	→2001:db8:1111:5::/64
•	あて先 IPv6アドレス/プレフィ	ックス長	→2001:db8:1111:3::/64
•	QoS		→指定なし
Гŧ	目手情報」-「ネットワーク情報	段」	
[7	ネットワーク(vpn-hon)情報」-	「IPv6関連」	
ГП	Pv6動的VPN情報」		
•	動的VPN接続	→する	

 動的 VPN 接続 → する 相手プレフィックス長 → 64 利用するテンプレート情報 → vpn-shiA
 ACL 定義番号 → 0

本社を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shiA

<ネットワーク情報追加フィールド> ネットワーク名 vpn-shiA

- 【追加】ボタンをクリックします。
 「ネットワーク情報 (vpn-shiA)」ページが表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 6. 以下の項目を指定します。
 - IPv6 →使用する

■IPv6基本情報		3
IPv6	○使用しない ⊙使用する	

- 7. [保存] ボタンをクリックします。
- **8.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。
- 9. 以下の項目を指定します。
 - ネットワーク あて先プレフィックス/プレフィックス長
 - →ネットワーク指定 →2001:db8:1111:3::/64

- メトリック値
- 優先度

→0

→1

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>			
ネットワーク	 デフォルトルート ネットワーク指定 あて先ブレフィ ックス/ブレフィ ィックス長 2001:db8:1111:3:: 		
メトリック値	1 💌		
優先度	0		

- 10. [追加] ボタンをクリックします。
- **11. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- → shisyaA
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

13. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

鍵交換モード	→ Main Mode 使用
相手側エンドポイント	→2001:db8:1111:1::66
自側エンドポイント	→2001:db8:1111:2::66
	鍵交換モード 相手側エンドポイント 自側エンドポイント

	◎ Main Mode使用		
鍵交換モ ート	相手側エンドボイ ント 2001:db8:1111:1::66		
	自側エンドポイン ト 2001:db8:1111:2::66		

- 15. [保存] ボタンをクリックします。
- **16.** IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。 「IPsec 情報」が表示されます。

•	対象パケット	
	自側 IP アドレス/マスク	→IPv6すべて
	相手側IPアドレス/マスク	→IPv6すべて
•	SAの 設定	

暗号アルゴリズム→ des-cbc認証アルゴリズム→ hmac-md5

■IPsec情報(自動鍵)				
対象	自側IPアドレ ス/マスク	IPv6すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしく(JIPv6アドレ ス/プレフィックス長形式で入力してください。		
ット	相手側IPアド レス/マスク	Pv6すべて ▼ "指定する"を選択時のみ有効です。) メロマンクロンクロンクロンクロンクロンクロンクロンクロンクロンクロンクロンクロンクロン		
	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null		
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし		
の設 定	PFS時のDHグ ループ	使用しない		
	SA有効時間	8 時間 🖌		
	SA有効データ 量	0 GByte 🗸		

- 18. [保存] ボタンをクリックします。
- **19.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

20. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 →文字列 鍵 → abcdefghijkImnopqrstuvwxyz1234567890
 SAの設定 暗号アルゴリズム → des-cbc 認証 (ハッシュ)アルゴリズム → hmac-md5 DH グループ → modp768 (グループ1)

■IKE情報		
गर स्ट्रन्स् अ	<mark>键</mark> 識別	○16進数 ⊙文字列
IKE認証要	鏈	••••••
IKE認証方式		shared
ポート番号		500
	暗号アルコリズ ム	des-cbc 💌
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(ヴループ1) 💌
	SA有効時間	24 時間 🖌

- 21. [保存] ボタンをクリックします。
- **22.** 手順1.~21.を参考に、支社Bを設定します。

23. 設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA情報」ページが表示されます。

24. 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 25. 以下の項目を指定します。
 - グループ名 → dvpnserver



26. [追加]ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

27. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

- 28. 以下の項目を指定します。
 - ユーザID

→ shisyaAid



29. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と設定項目が表示されます。

- **30. 「認証情報」をクリックします**。 「認証情報」が表示されます。
- 31. 以下の項目を指定します。
 - 認証パスワード → shisyaApass

■認証情報		
ユーザID	shisyaApass	
認証バスワード	•••••	

- 32. [保存] ボタンをクリックします。
- **33.** 手順23.~31.を参考に、支社Bを設定します。
- **34. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- 35. 「サーバ関連情報」をクリックします。

サーバ関連情報の設定項目と「基本情報」が表示されます。

→使用する
→ example.com
→行う
→0

■基本情報		3
	 ○ 使用した ● 使用する 	มี
サーバ機能	ドメイ ン名	example.com
/ /WHE	認証	 ○行わない ◎行う AAAグループID □

- 37. [保存] ボタンをクリックします。
- **38. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

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

適用機種 全機種

接続するたびにIPアドレスが変わる環境でNATトラバーサルを使って、VPNを構築する場合の設定方法を説明します。

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

: 192.168.1.1/24

:LAN0ポート使用

:userid(プロバイダから提示された内容)

:userpass(プロバイダから提示された内容)

● 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
- PPPoE ユーザ認証 ID
- PPPoEユーザ認証パスワード
- PPPoE LAN ポート

[本社]

• ローカルネットワーク IPv4 アドレス

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



● 設定条件	
[支社]	
 ネットワーク名 	: vpn-hon
● 接続先名	: honsya
● IPsec/IKE区間	:支社 - 202.168.2.66
• IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット
[本社]	
 ネットワーク名 	: vpn-shi
● 接続先名	: shisya
● IPsec/IKE区間	:202.168.2.66 - 支社
• IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット
[共通]	
 鍵交換タイプ 	Aggressive Mode
• IPsecプロトコル	esp
● IPsec 暗号アルゴリズム	: des-cbc
• IPsec認証アルゴリズム	: hmac-md5
● IPsec DHグループ	:なし
● IKE支社ID/IDタイプ	:shisya(自装置名)/FQDN
● IKE認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
• IKE 暗号アルゴリズム	: des-cbc
• IKE認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768
● IKE NAT トラバーサル機能	:使用する

資ヒント ———

◆ DH グループとは?

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

♦ IKE とは?

自動鍵交換を行うためのプロトコルです。

♦ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(Initiator)

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

● 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>			
接続先名	honsya		
接続先種別	 ATM接続 マロース WANI マ 通常接続 (使用インタフェース WANI マ 論理リンクにバンドルする (使用インタフェース WANI マ 論理リンクにバンドルする (使用インタフェー WANI マ バンドル先 選択できる定義がありません マ ISDN接続 「ISDN接続 使用インタフェース すべて マ ダイヤル1 電話番号 ダイヤル1 電話番号 ヴェイヤル1 電話番号 ヴェアドレス 論理リンクにバンドルする (使用インタフェー		

機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

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

→ shisya

	⊙ Aggressive Mode(Initiator)使用	
鍵交換モ ート	自側エンドボイン ト	
	相手側エンドポイ ント	202.168.2.66
	自装置識別情報	shisya
	IDタイプ	⊙ FQDN ○ User-FQDN

13. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5



16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

 IKE 認証鍵 鍵識別 鍵

→文字列 → abcdefghijkImnopqrstuvwxyz1234567890

 SAの設定 暗号アルゴリズム
 認証(ハッシュ)アルゴリズム
 DHグループ

→ des-cbc → hmac-md5 → modp768(グループ1) → 使田すろ

• NAT トラバーサル機能		バーサル機能	→使用する
■IKE情報			3
	ルビ言和言正分割	鍵識別	○16進数 ⊙文字列
	IKE認証挺	鍵	•••••
IKE認証方式		t	shared
ポート番号			500
		暗号アルコリズ ム	des-cbc 💌
	SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 🗸
	DHグループ	modp768(グループ1) 🔽	

24

時間 🖌

19. [保存] ボタンをクリックします。

SA有効時間

20. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

本社を設定する(Responder)

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-shi	

4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0 あて先アドレスマスク →24 (255.255.255.0)
 メトリック値 →1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- → shisya
- 接続先種別 → IPsec/IKE 接続

機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

 鍵交換モード 自側エンドポイント

→ Aggressive Mode(Responder)使用 → 202.168.2.66

- 13. 【保存】ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→ des-cbc → hmac-md5

SA の設 定	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
	PFS時のDHグ ルーブ	使用しない V
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 💌

16. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

 IKE 認証鍵 鍵識別

鍵

→文字列

→ abcdefghijklmnopqrstuvwxyz1234567890

 SAの設定 暗号アルゴリズム
 認証(ハッシュ)アルゴリズム
 DHグループ

• NAT トラバーサル機能

→ des-cbc → hmac-md5 → modp768(グループ1) →使用する

- IKE情報 3 ○16進数 ⊙文字列 键識別 IKE認証鍵 键 IKE認証方式 shared ボート番号 500 暗号アルコリズ des-cbc ~ L 認証(ハッシュ)ア hmac-md5 💌 SAの 設定 ルゴリズム DHグループ modp768(グループ1) 🔽 SA有効時間 時間 🗸 24 初回再送時間 10 秒 🗸 再送回数 3 対象バケット送信契機 IKEネゴシエーション開始動作 ○対象回線接続契機 NATトラバーサル機能 ○使用しない ⊙使用する
- 19. [保存] ボタンをクリックします。
- **20. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.14.19 テンプレート着信機能(AAA 認証)および NAT トラバーサル を使用した可変 IP アドレスでの VPN

適用機種 全機種

IPsec機能、テンプレート機能および NAT トラバーサルを使って、自動鍵交換で VPN を構築する場合の設定方法 を説明します。

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

● 前提条件

[支社 (PPPoE 常時接続)]

- ローカルネットワークIPv4アドレス
- PPPoE ユーザ認証 ID
- PPPoEユーザ認証パスワード
- PPPoE LANポート

: userpass(プロバイダから提示された内容)

: userid (プロバイダから提示された内容)

:LAN0 ポート使用

: 192.168.1.1/24

[本社]

• ローカルネットワーク IPv4 アドレス

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



● 設定条件	
[支社]	
 ネットワーク名 	: vpn-hon
● 接続先名	: honsya
● IPsec/IKE区間	:支社 - 202.168.2.66
• IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット
[本社]	
 テンプレート名 	: vpn-shi
• IPsec/IKE区間	:202.168.2.66 - 支社
• IPsec対象範囲	:IPsec相手情報を使用するすべてのパケット
[共通]	
 鍵交換タイプ 	: Aggressive Mode
• IPsecプロトコル	esp
● IPsec 暗号アルゴリズム	: des-cbc
● IPsec認証アルゴリズム	: hmac-md5
● IPsec DH グループ	:なし
● IKE支社ID / ID タイプ	:shisya(自装置名)/FQDN
● IKE 認証鍵	:abcdefghijklmnopqrstuvwxyz1234567890(文字列)
• IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: des-cbc
• IKE 認証アルゴリズム	: hmac-md5
● IKE DH グループ	: modp768
● IKE NAT トラバーサル機能	:使用する

こんな事に気をつけて

- テンプレート着信機能(AAA 認証)を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに 設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。
 Main Mode の場合
 :相手側 IPsec トンネルアドレス
 Aggressive Mode の場合:相手側の装置識別情報

◆ DH グループとは?

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

♦ IKEとは?

自動鍵交換を行うためのプロトコルです。

◆ ID タイプとは?

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

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(Initiator)

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>		
ネットワーク名 vpn-hon vpn-hon		

4. [追加] ボタンをクリックします。

「ネットワーク情報(vpn-hon)」ページが表示されます。

5. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 7. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 → 1

→0

● 優先度



- 8. [追加] ボタンをクリックします。
- 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>			
接続先名	honsya		
接続先種 別	 ATM接続 VCI 専用線接続 通常接続 (使用インタフェース WANI * 論理リンクにバンドルする (使用インタフェー ス バンドルする (使用インタフェー ス バンドル・ 選択できる定義がありません * ISDN接続 通常接続 (使用インタフェース ずべて * ダイヤル1 電話番号 ダイヤル1 電話番号 ダイヤル1 電話番号 ダイヤル1 電話番号 ダイヤル1 電話番号 ダイヤル1		

機種により、接続先種別の表示が上記の画面とは異なります。

11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

12. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント 自装置識別情報

→ Aggressive Mode(Initiator)使用 → 202.168.2.66 → shisya

	⊙ Aggressive Mode(Initiator)使用		
鍵交換モ ート	自側エンドボイン ト		
	相手側エンドポイ ント	202.168.2.66	
	自装置識別情報	shisya	
	IDタイプ	⊙ FQDN ○ User-FQDN	

13. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

15. 以下の項目を指定します。

認証アルゴリズム

• SAの設定 暗号アルゴリズム

→ des-cbc →hmac-md5



16. [保存] ボタンをクリックします。

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

「IKE情報」が表示されます。

18. 以下の項目を指定します。

• IKE 認証鍵 鍵識別

鍵

→文字列

- → abcdefghijklmnopqrstuvwxyz1234567890 • SAの設定 暗号アルゴリズム → des-cbc
- 認証(ハッシュ)アルゴリズム →hmac-md5 DHグループ →modp768 (グループ1) • NAT トラバーサル機能 →使用する

■IKE情報			
1/ 도쿄지문지수례	键識別	○16進数 ⊙文字列	
IKE認証規	键	••••••	
IKE認証方式	ς.	shared	
ボート番号		500	
	暗号アルゴリズ ム	des-cbc 💌	
SAの設定	認証(ハッシュ)ア ルゴリズム	hmac-md5 💌	
	DHグループ	modp768(ヴループ1) 💌	
	SA有効時間	24 時間 🖌	
初回再送時	88 8]	10 秒 🗸	
再送回数		3 0	
IKEネゴシエ	ーション開始動作	●対象バケット送信契機○対象回線接続契機	
NATトラバー	サル機能	●使用しない●使用する	

- [保存] ボタンをクリックします。 19.
- 20. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

本社を設定する(Responder)

- 設定メニューのルータ設定で「テンプレート情報」をクリックします。
 「テンプレート情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - テンプレート名 → vpn-shi
 - 接続種別
- →IPsec/IKE (RADIUS/AAA)

<テンプレート情報追加フィールド>	
テンプレート名 vpn-shi	
接続種別	 ○ ISDN ⊙ IPsec/IKE(RADIUS/AAA) ○ IPsec/IKE(動的VPN)

機種により、接続先種別の表示が上記の画面とは異なります。

3. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shi)」ページが表示されます。

4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

5. 以下の項目を指定します。

- 使用するrmtインタフェース →rmt1から1インタフェースを予約
- 参照する AAA 情報 → 0
- ・ 鍵交換モード

 ・ Aggressive Mode (Responder)使用
 ・ 202.168.2.66
 ・ FQDN



- 6. [保存] ボタンをクリックします。
- テンプレート情報 (vpn-shi) の設定項目の「IPsec/IKE 関連」をクリックします。
 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

 SAの 暗号 認証 	設定 アルゴリズム アルゴリズム	→des-cbc →hmac-md5
IPsec	情報	5
	暗号アルゴリズム	□aes-cbc-256 □aes-cbc-192 □aes- cbc-128 □3des-cbc ☑des-cbc □null
SAの設	認証アルゴリズム	☑ hmac-md5 □ hmac-sha1 □認証なし
定	PFS時のDHグル ーブ	使用しない
	SA有効時間	8 時間 🗸

9. [保存] ボタンをクリックします。

SA有効データ量 0

10. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

GByte 🔽

11. 以下の項目を指定します。

•	SAの設定	
	暗号アルゴリズム	→des-cbc
	認証(ハッシュ)アルゴリズム	→hmac-md5
	DHグループ	→modp768(グループ1)

NATトラバーサル機能 →使用する

■IKE情報		
	暗号アルコリズム	des-cbc 💌
いの沙中	認証(ハッシュ)アルゴリズム	hmac-md5 💌
SAUJE	DHグループ	modp768(グループ1) 🔽
	SA有効時間	24 時間 🖌
初回再送時間		10 秒 🖌
再送回数		3 🛛
NATトラバーサル機能		○使用しない⊙使用する

- 12. [保存] ボタンをクリックします。
- **13. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **14. 「**グループ ID 情報」をクリックします。

「グループID情報」が表示されます。

- 15. 以下の項目を指定します。
 - グループ名

<グループID情報追加フィールド>		
グループ名 vpn-shisya		

16. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

→vpn-shisya

17. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

- 18. 以下の項目を指定します。
 - ユーザID → shisya



19. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と設定項目が表示されます。

- **20. 「認証情報」をクリックします。** 「認証情報」が表示されます。
- 21. 以下の項目を指定します。
 - ユーザID → shisya

 認証パスワード → shisya

■認証情報		3
ユーザID	shisya	
認証バスワード		

- 22. [追加] ボタンをクリックします。
- **23.** AAA ユーザ情報(0)の設定項目の「IP 関連」をクリックします。 IP 関連の設定項目と「IP 基本情報」が表示されます。
- 24. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

25. 以下の項目を指定します。

٠	ネットワーク	→ネットワーク指定		
	あて先IPアドレス	→ 192.168.1.0		
	あて先アドレスマスク	→24 (255.255.255.0)		

- メトリック値 →1
- 優先度 →1

<スタティック経路情報入力フィールド>		
ネットワーク	 デフォルトルート ネットワーク指定 あて先IPアドレス 192.168.1.0 あて先アドレスマスク 24 (255.255.255.0) 	
メトリック値	1 🗸	
優先度	1	

- 26. [追加] ボタンをクリックします。
- **27.** AAA ユーザ情報(0)の設定項目の「IPsec/IKE 関連」をクリックします。 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

● 対象パケット	
自側 IP アドレス/マスク	→IPv4すべて
相手側IPアドレス/マスク	→IPv4すべて

IPs	ec情報	3
対象	自側IPア ドレス/ マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/ プレフィックス長形式で入力してください。
ット	相手側IP アドレス /マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/ ブレフィックス長形式で入力してください。

- 29. [保存] ボタンをクリックします。
- **30.** IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE情報」が表示されます。

- 31. 以下の項目を指定します。
 - IKE 認証鍵 鍵識別 鍵

→文字列 →abcdefghijkImnopqrstuvwxyz1234567890

■IKE情報		3
тис≡ग≑т≎а	<mark>键識別</mark>	○16進数 ⊙文字列
INE認証援	键	••••••

- 32. [保存] ボタンをクリックします。
- **33. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.14.20 接続先情報(動的 VPN)を使用した IPv4 over IPv4で 固定 IP アドレスでの VPN

適用機種 全機種

IPsec機能、動的 VPN 情報交換機能、接続先およびテンプレート機能を使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

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

● 前提条件

【本社(PPPoE 常時接続)】

 ローカルネットワーク IPv4 アドレス 	: 192.168.0.1/24
• PPPoEユーザ認証ID	:userid0(プロバイダから提示された内容)
● PPPoEユーザ認証パスワード	:userpass0(プロバイダから提示された内容)
・ PPPoE LANポート	:LAN0ポート使用
● NAT機能	:マルチ NAT を使用する
 ネットワーク名 	: internet
● 接続先名	: ISP-1
【支社A(PPPoE 常時接続)】	
 ローカルネットワーク IPv4 アドレス 	: 192.168.1.1/24
• PPPoEユーザ認証ID	:userid1(プロバイダから提示された内容)
• PPPoEユーザ認証パスワード	:userpass1(プロバイダから提示された内容)
● PPPoE LANポート	:LAN0ポート使用
● NAT機能	:マルチ NAT を使用する
 ネットワーク名 	: internet
● 接続先名	: ISP-1
[支社 B(PPPoE 常時接続)]	
 ローカルネットワークIPv4アドレス 	: 192.168.2.1/24
• PPPoEユーザ認証ID	:userid2(プロバイダから提示された内容)
● PPPoEユーザ認証パスワード	:userpass2(プロバイダから提示された内容)
• PPPoE LANポート	: LAN0 ポート使用
● NAT機能	:マルチ NAT を使用する
• ネットワーク名	: internet
● 接続先名	: ISP-1
【動的 VPN サーバ】	
● ローカルネットワークIPv4アドレス	: 192.168.10.1/24
 インターネットプロバイダから割り当てられた 	固定 IPv4 アドレス : 202.168.2.66/24

インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス:202.168.2.65



•	● 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		
[重	カ的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		
٠	ネットワーク名	: vpn-shiB		
•	接続先名	: shisyaB		
٠	IPsec/IKE区間	:202.168.2.66 - 支社 B		
٠	IPsec対象範囲	:IPsec 相手情報を使用するすべてのパケット		
[‡	ŧ通(本社、支社A、B-動的 VPN サーバ)]			
٠	鍵交換タイプ	: Aggressive Mode		
٠	IPsecプロトコル	: esp		
٠	IPsec暗号アルゴリズム	: des-cbc		
٠	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		
٠	IKE 支社 B ID/ID タイプ	:shisyaB(自装置識別情報)/FQDN		
٠	IKE本社 IKE認証鍵	: 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ		
•	IKE支社AIKE認証鍵	: abcdefghijkImnopqrstuvwxyz1234567890		
٠	IKE 支社 B IKE 認証鍵	: 1234567890abcdefghijklmnopqrstuvwxyz		
٠	IKE 認証方法	: shared		
٠	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)			
[7	[社]			
•	テンプレート名	: vpn-shi		
•	IKE(UDP:500番ポート)のプライベートアド	レス		
		: 192.168.0.1		

- ESPのプライベートアドレス : 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.0.1

[支社A]

 ネットワーク名 	: vpn-hon
● 接続先名	: honsya
• テンプレート名	: vpn-shiB
• IKE(UDP:500番ポート)のプライベー	トアドレス
	: 192.168.1.1
• ESPのプライベートアドレス	: 192.168.1.1
 接続先監視アドレス 	: 192.168.1.1-192.168.0.1
 テンプレート接続先監視アドレス 	: 192.168.1.1
[支社 B]	
 ネットワーク名 	: vpn-hon
● 接続先名	: honsya
 テンプレート名 	: vpn-shiA
• IKE(UDP:500番ポート)のプライベー	トアドレス
	: 192.168.2.1
• ESPのプライベートアドレス	: 192.168.2.1
 接続先監視アドレス 	: 192.168.2.1-192.168.0.1
 テンプレート接続先監視アドレス 	: 192.168.2.1
● 設定条件(動的 VPN 接続)	
[本社 - 支社 A/B 間の動的 VPN 共通設定]	
• クライアント情報	: 0
 サーバ情報 	
アドレス	: 192.168.10.1
ポート番号	: 5070
• 有効期間	:1時間
• セッション更新間隔	:5分
 ドメイン名 	: example.com
● VPN 通信	
利用インタフェース	: rmt0
 動的 VPN クライアントの優先度 	: 10
 動的 VPN IPv4 経路情報の優先度 	: 1
• IPsecプロトコル	: esp
• IPsec暗号アルゴリズム	: aes-cbc-128
• IPsec認証アルゴリズム	: hmac-sha1
● IPsecDHグループ	: modp768
● IKE認証鍵	: ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
• IKE 認証方法	: shared
● IKE 暗号アルゴリズム	: aes-cbc-128
• IKE 認証アルゴリズム	: hmac-sha1
● IKE DH グループ	: modp768

[本社の動的 VPN 設定]

٠	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
[3	5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
[3	5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
[重	b的 VPN サーバ設定]	
•	サーバ機能	:使用する
	ドメイン名	: example.com
	認証	:行う
	AAA グループ ID	: 0
•	AAAユーザ情報(本社認証情報)	
	ユーザID	: honsyaid
	認証パスワード	: honsyapass
•	AAAユーザ情報(支社A認証情報)	
	ユーザID	: shisyaAid
	認証パスワード	: shisyaApass
•	AAAユーザ情報(支社B認証情報)	
	ユーザID	: shisyaBid
	認証パスワード	: shisyaBpass

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でネットワーク名がinternet の [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。
- **「IP 関連」をクリックします**。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
5. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

• プロトコル

- プライベートIP情報
 IPアドレス → 192.168.0.1
 ポート番号 → isakmp

 グローバルIP情報
- IPアドレス →指定しない ポート番号 →isakmp

→udp

<静的NAT情報入力フィールド>		
プライベート	IPアド レス	192.168.0.1
IP情報	ボート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
グローバル	IPアド レス	
IP竹青報	ボート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
プロトコル		udp ✓(番号指定: ************************************

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 192.168.0.1
 ポート番号 → すべて

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

画面上部の「相手情報」をクリックします。 「相手情報」ページが表示されます。

10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

- 以下の項目を指定します。
 ネットワーク名
 - →vpn-srv

<ネットワーク情報追加フィールド>		
ネットワーク名	vpn-srv	

12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-srv)」ページが表示されます。

13. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

14. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

15. 以下の項目を指定します。

 ネットワーク 	→ネットワーク指定
あて先IPアドレス	→ 192.168.10.0
あて先アドレスマスク	→24 (255.255.255.0)
• メトリック値	→ 1

● 優先度



→0

- 16. [追加] ボタンをクリックします。
- 17. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →dvpn-srv
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

 鍵交換モード 相手側エンドポイント

自装置識別情報

→Aggressive Mode(Initiator)使用 →202.168.2.66

→honsya

	⊙ Aggressive Mode(Initiator)使用		
鍵交換モ ート	自側エンドボイン ト		
	相手側エンドポイ ント	202.168.2.66	
	自装置識別情報	honsya	
	IDタイプ	⊙ FQDN O User-FQDN	

21. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

23. 以下の項目を指定します。

認証アルゴリズム

SAの設定
 暗号アルゴリズム

→des-cbc →hmac-md5

	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ☑des-cbc □null
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし
の設 定 し	PFS時のDHグ ルーブ	使用しない V
	SA有効時間	8 時間 🖌
	SA有効データ 量	0 GByte 💌

24. [保存] ボタンをクリックします。

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

「IKE 情報」が表示されます。

26. 以下の項目を指定します。

IKE認証鍵	
鍵識別	→文字列
鍵	→ 1234567890ABCDEFGHIJKLMNOPQRSTUVWXYZ
SAの 設定	
暗号アルゴリズム	→des-cbc
認証(ハッシュ)アルゴリズム	→hmac-md5
DHグループ	→modp768 (グループ1)
	IKE 認証鍵 鍵識別 鍵 SAの設定 暗号アルゴリズム 認証 (ハッシュ)アルゴリズム DH グループ



- 27. [保存] ボタンをクリックします。
- **28. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- **29. 「クライアント関連情報」をクリックします**。 クライアント関連情報の設定項目と「基本情報」が表示されます。
- **30.** クライアント関連情報の設定項目の「ドメイン情報」をクリックします。 「ドメイン情報」が表示されます。

• ドメイン名

→ example.com

	<ドメイン情報追加フィールド>
ドメイン 名	example.com

32. [追加] ボタンをクリックします。

「ドメイン情報(0)」ページが表示されます。

33. 「基本情報」をクリックします。

「基本情報」が表示されます。

34. 以下の項目を指定します。

•	ドメイン名	→ example.com
•	サーバ情報	
	アドレス	→192.168.10.1
	ポート番号	→5070
	認証ID	→ honsyaid
	認証パスワード	→honsyapass
•	有効期間	→1時間
•	優先度	→ 10
•	セッション更新間隔 時間	→ 更新する →5分
•	クライアントIPアドレス	→192.168.0.1
•	VPN通信	
	利用インタフェース	→rmt0
•	経路情報の優先度	
	IPv4	→ 1
	IPv6	→ 1
•	自側ユーザID	→ honsya

■基本情報 2			
ドメイン名		example.com	
サーバ情報	アドレス	192.168.0.1	
	ボート番号	5070	
	認証ID	honsyaid	
	認証バスワ ート	•••••	
	アドレス		
セカンダリ	ボート番号	5070	
サーバ情報	認証ID		
	認証バスワ ード		
有効期間		1 時間 🖌	
優先度		10 🗸	
セッション更新間隔		 ● 更新しばい ● 更新する 時間 5 分 ▼ 	
クライアントロ	Pアトレス	192.168.0.1	
利用インタフ ェース		rmt0 💌	
VPN通信	中継ルータア ドレス	※LANインタフェース選択時のみ指定してく ださい	
	終端クロー バルアドレス		
経路情報の	IPv4	1	
優先度	IPv6	1	
自側ユーザID		honsya	

- 35. [保存] ボタンをクリックします。
- **36.** ドメイン情報(0)の設定項目の「自側ネットワーク情報」をクリックします。 「自側ネットワーク情報」が表示されます。
- 37. 以下の項目を指定します。
 - 動的 VPN で接続する自側ネットワーク → 192.168.0.0/24

<自側ネットワーク情報入力フィールド>		
動的VPNで接	192.168.0.0	
続する自側ネッ	※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/	
トワーク	ブレフィックス長形式で入力してください。	

- 38. [追加] ボタンをクリックします。
- 39. 設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

- テンプレート名 → vpn-shi
- 接続種別 → IPsec/IKE(動的 VPN)

<テンプレート情報追加フィールド>		
テンプレート名	vpn-shi	
接続種別	 ○ ISDN ○ IPsec/IKE(RADIUS/AAA) ⊙ IPsec/IKE(動的VPN) 	

機種により、接続先種別の表示が上記の画面とは異なります。

41. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shi)」ページが表示されます。

42. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 43. 以下の項目を指定します。
 - 使用するrmtインタフェース →rmt10から10インタフェースを予約
 - 自側エンドポイント → 192.168.0.1

使用するrmtインタフェース	rmt10 から10 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケットについて 0 秒 💌
自側エントボイント	192.168.0.1

- 44. [保存] ボタンをクリックします。
- **45.** テンプレート情報(vpn-shi)の設定項目の「動的 VPN 関連」をクリックします。 動的 VPN 関連の設定項目と「基本情報」が表示されます。
- 46. 以下の項目を指定します。
 - ドメイン情報 →使用する
 "使用する"を選択すると、以下の項目が指定できます。
 - ・ドメイン情報 →0 (example.com)

■基本情報	3
ドメイン情報	○ 使用しない ⊙ 使用する O(example.com) ▼

- 47. [保存] ボタンをクリックします。
- **48.** テンプレート情報 (vpn-shi) の設定項目の「IPsec/IKE 関連」をクリックします。 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

	IPsec情報 暗号アルゴリズム	☐ aes-cbc-256 ☐ aes-cbc-192 ☑ aes- cbc-128
	PFS 時の DH グループ	→modp768(グループ1)
	認証アルゴリズム	→hmac-sha1
	暗号アルゴリズム	→aes-cbc-128
•	SA の 設定	

SAの設	認証アルゴリズム	□hmac-md5 ☑hmac-sha1 □認証なし
定	PFS時のDHグル ーブ	modp768(ヴループ1) 🔽
	SA有効時間	8 時間 🖌
	SA有効データ量	0 GByte 💌

50. [保存] ボタンをクリックします。

51. IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE情報」が表示されます。

52. 以下の項目を指定します。

IKE 認証鍵
 鍵識別 →文字列
 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
 SAの設定
 暗号アルゴリズム → aes-cbc-128
 認証 (ハッシュ)アルゴリズム → hmac-sha1
 DH グループ → modp768 (グループ1)

IKE認証	键識別	○16進数 ⊙文字列	
键	鍵	••••••	
IKE認証	方式	shared	
SAの設 定	暗号アルコリズム	aes-cbc-128 💌	
	認証(ハッシュ)アル ゴリズム	hmac-shal 💌	
	DHグループ	modp768(ヴループ1) 💌	
	SA有効時間	24 時間 🖌	

53. [保存] ボタンをクリックします。

54. IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

- 55. 以下の項目を指定します。
 - 接続先監視
 送信元IPアドレス → 192.168.0.1

■接続制御情報		
接続先監視	送信元IPアドレス	192.168.0.1
	正常時送信間隔	▶ ▼

56. [保存] ボタンをクリックします。

57. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 58. 以下の項目を指定します。
 - 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>			
定義名	ACLO		

59. [追加] ボタンをクリックします。

「ACL情報(ACL0)」ページが表示されます。

60. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

61. 以下の項目を指定します。

- プロトコル →すべて
 送信元情報
 IPアドレス → 192.168.0.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報 IPアドレス アドレスマスク

• Qos

- → 192.168.1.0
- →24 (255.255.255.0)
- →指定なし

■IP定義	■ IP定義情報 [9]		
プロトコル		すべて ▼ (番号指定: 7その他"を選択時のみ有効です)	
送信元情	IPアドレス	192.168.0.0	
報	アトレスマ スク	24 (255.255.255.0)	
あて先情	IPアドレス	192.168.1.0	
報 アトレスマ スク		24 (255.255.255.0)	
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい	

62. [保存] ボタンをクリックします。

63. 手順61.~62.を参考に、以下の項目を指定します。

•	プロトコル	→すべて
•	送信元情報	
	IPアドレス	→ 192.168.0.0
	アドレスマスク	→24 (255.255.255.0)
•	あて先情報	
		100 100 0 0

- IPアドレス
 → 192.168.2.0

 アドレスマスク
 → 24 (255.255.255.0)
- Qos →指定なし

- 設定メニューのルータ設定で「相手情報」をクリックします。 64. 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。 65. 「ネットワーク情報」が表示されます。
- 「ネットワーク情報」でネットワーク名がinternetの「修正」ボタンをクリックします。 66. 「ネットワーク情報(internet)」ページが表示されます。
- 「IP関連」をクリックします。 67. IP関連の設定項目と「IP基本情報」が表示されます。
- 「動的VPN情報」をクリックします。 68.

「動的 VPN 情報 | が表示されます。

- 以下の項目を指定します。 69.
 - 動的VPN 接続 →する →24 (255.255.255.0) 相手ネットマスク 利用するテンプレート情報 →vpn-shi • ACL定義番号 →0



ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<動的VPN情報入力フィールド>			
動的VPN接続	 ● する 相手ネットマスク 24 (255.255.255.0) 利用するテンプレート情報 vpn-shi マ ○しばい 		
ACL定義番号	0 参照		

[追加] ボタンをクリックします。 70.

71. 手順69.~70.を参考に、以下の項目を指定します。

- 動的VPN接続 →する 相手ネットマスク →24 (255.255.255.0) 利用するテンプレート情報 →vpn-shi ACL 定義番号 **→**1
- 画面左側の「設定反映」ボタンをクリックします。 72. 設定した内容が有効になります。

支社Aを設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」でネットワーク名がinternetの [修正] ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。

→指定しない

→isakmp

→udp

4. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

6. 以下の項目を指定します。

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

<静的NAT情報入力フィールド>		
ゴライベート	IPアド レス	192.168.1.1
IP情報 ボート 番号		isakmp V(番号指定: 7その他 ~ を選択時の み有効です)
グローバル IP情報	IPアド レス	
	ボート 番号	isakmp V(番号指定: 7その他 ~ を選択時の み有効です)
プロトコル		udp ✓(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

7. [追加] ボタンをクリックします。

8. 手順6.~7.を参考に、以下の項目を指定します。

•	プライベートIP情報	
	IPアドレス	→ 192.168.1.1
	ポート番号	→すべて
•	グローバル IP 情報	
	IPアドレス	→指定しない
	ポート番号	→すべて

プロトコル → esp

9. 「本社を設定する」の手順9.~27.を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」 ネットワーク名 →vpn-srv 「ネットワーク情報 (vpn-srv)」-「IP 関連」 「スタティック経路情報」 ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.10.0 あて先アドレスマスク →24 (255.255.255.0) メトリック値 **→**1 優先度 →0 「接続先情報」 • 接続先名 → dvpn-srv • 接続先種別 → IPsec/IKE 接続 「接続先情報」-「IPsec/IKE 接続」 「基本情報」 鍵交換モード → Aggressive Mode (Initiator) 使用 相手側エンドポイント →202.168.2.66 自装置識別情報 → shisyaA 「IPsec情報」 SAの設定 暗号アルゴリズム → des-cbc 認証アルゴリズム →hmac-md5 「IKE情報」 • IKE 認証鍵 鍵識別 →文字列 鍵 → abcdefghijklmnopqrstuvwxyz1234567890 • SAの設定 暗号アルゴリズム →des-cbc 認証(ハッシュ)アルゴリズム →hmac-md5 DHグループ →modp768 (グループ1)

10. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします。

「動的 VPN 情報」ページが表示されます。

11. 「クライアント関連情報」をクリックします。 クライアント関連情報の設定項目と「基本情報」が表示されます。

12. クライアント関連情報の設定項目の「ドメイン情報」をクリックします。 「ドメイン情報」が表示されます。

- 13. 以下の項目を指定します。
 - ドメイン名 → example.com

	<ドメイン情報追加フィールド>	1
ドメイン 名	example.com	

14. [追加] ボタンをクリックします。

「ドメイン情報(0)」ページが表示されます。

15. 「基本情報」をクリックします。

「基本情報」が表示されます。

16. 以下の項目を指定します。

٠	ドメイン名	→example.com
•	サーバ情報	
	アドレス	→ 192.168.10.1
	ポート番号	→5070
	認証ID	→shisyaAid
	認証パスワード	→ shisyaApass
•	有効期間	→1時間
•	優先度	→ 10
•	セッション更新間隔 時間	→更新する →5分
•	クライアントIPアドレス	→ 192.168.1.1
•	VPN 通信 利用インタフェース	→rmt0
•	経路情報の優先度	
	IPv4	→ 1
	IPv6	→ 1

■基本情報 []		
ドメイン名		example.com
	アドレス	192.168.10.1
	ボート番号	5070
サーバ情報	認証ID	shisyaAid
	認証バスワ ード	•••••
	アドレス	
わかいない	ボート番号	5070
サーバ情報	認証ID	
	認証バスワ ード	
有効期間		1 時間 🖌
優先度		10 💌
セッション更新間隔		 ● 更新しない ● 更新する ● 時間 5 分 ▼
クライアントロ	Pアドレス	192.168.1.1
	利用インタフ ェース	rmt0 💌
VPN通信	中継ルータア ドレス	×LANインタフェース選択時のみ指定してく ださい
	終端クロー バルアドレス	
経路情報の	IPv4	1
優先度	IPv6	1

17. [保存] ボタンをクリックします。

18. ドメイン情報(0)の設定項目の「自側ネットワーク情報」をクリックします。

「自側ネットワーク情報」が表示されます。

- 19. 以下の項目を指定します。
 - 動的 VPN で接続する自側ネットワーク → 192.168.1.0/24



- 20. [追加] ボタンをクリックします。
- **21. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **22. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。

.....

- 23. 以下の項目を指定します。
 - ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

24. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

25. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

26. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

27. 以下の項目を指定します。

- ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.0.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 → 1
- 優先度 → 0



28. [追加] ボタンをクリックします。

29. 手順27.~28.を参考に、以下の項目を指定します。

- ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.2.0 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 → 1
- 優先度 → 2

30. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

31. 以下の項目を指定します。

● 接続先名

→honsya

• 接続種別

→IPsec/IKE 接続

機種により、接続先種別の表示が上記の画面とは異なります。

32. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

•	鍵交換モード	→動的 VPN 接続
	自側エンドポイント	→ 192.168.1.1
~		

建交換モ	⊙ 動的VPN接続
'∕ 	自側エンドポイント 192.168.1.1

- 34. [保存] ボタンをクリックします。
- 35. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec情報(動的VPN)」が表示されます。

36. 以下の項目を指定します。

		[will
	PFS 時の DH グループ	→modp768(グループ1)
	認証アルゴリズム	→hmac-sha1
	暗号アルゴリズム	→aes-cbc-128
•	SAの 設定	

■IPsec情報		13	
	暗号アルゴリズム	□aes-cbc-256 □aes-cbc-192 ☑aes- cbc-128 □3des-cbc □des-cbc □null	
SAの設	認証アルゴリズム	□hmac-md5 ☑hmac-sha1 □認証なし	
定	PFS時のDHグル ーブ	modp768(ヴループ1) 💌	
	SA有効時間	8 時間 🖌	
	SA有効データ量	0 GByte 💌	

37. [保存] ボタンをクリックします。

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

500

aes-cbc-128 💌

hmac-sha1 💌

24 時間 🛩

modp768(グループ1) 🔽

暗号アルコリズ

認証(ハッシュ)ア

ルゴリズム DHグルーブ

SA有効時間

ム

「IKE 情報」が表示されます。

39. 以下の項目を指定します。

ボート番号

SAの設定

•	• IKE 認証	鍵				
	鍵識別			→文字列		
	鍵			→ABCDEFGHIJKLMN	OPQRSTUVWXYZ1234567890	
•	。 SAの設定	Ē				
	暗号アル	ゴリズム		→aes-cbc-128		
	認証(ハ	、ッシュ)アルゴ	リズム	→hmac-sha1		
	DHグル・	ープ		→modp768(グループ	1)	
Γ	IKE情報			13	1	
		键識別	○16谁数	□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		
	IKE認証鍵	23				
	IKE認証方式	6	shared			

- 40. [保存] ボタンをクリックします。
- **41.** IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

- 42. 以下の項目を指定します。
 - 接続先監視 →使用する
 送信元IPアドレス → 192.168.1.1
 あて先IPアドレス → 192.168.0.1

	0 0	使用しない 使用する	
		送信元IPアドレス	192.168.1.1
		あて先IPアドレス	192.168.0.1
		正常時送信間隔	10 秒 🖌
接続		再送間隔	1 秒 🖌
先監 視		タイムアウト時間	5 秒 🖌
		異常時送信間隔	1 分 💌
		送信 TTL/HopLimit	255
		連続応答受信回数	1
		異常時送信開始待ち時間	0 秒 🗸
		監視方式	⊙ 常時監視 ○無通信時監視

- 43. [保存] ボタンをクリックします。
- **44.** IPsec/IKE 接続の設定項目の「動的 VPN 関連」をクリックします。 「基本情報」が表示されます。
- 45. 以下の項目を指定します。
 - ・ドメイン情報 →0 (example.com)
 - 相手側ユーザID

→honsya

■基本情報	3
ドメイン情報	O(example.com) 💌
相手側ユーザID	honsya

- 46. [保存] ボタンをクリックします。
- 47. 動的 VPN 関連の設定項目の「相手側ネットワーク情報」をクリックします。

「相手側ネットワーク情報」が表示されます。

- 48. 以下の項目を指定します。
 - 動的 VPN で接続する相手側ネットワーク → 192.168.0.0/24
 - テンプレートを使用して接続要求

→しない

<	相手側ネットワーク情報入力フィールド>
動的VPNで接続 する相手側ネッ トワーク	192.168.0.0 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/ ブレフィックス長形式で入力してください。
テンプレートを 使用して接続要 求	⊙しない○する

49. [追加] ボタンをクリックします。

50. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 51. 以下の項目を指定します。
 - 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名 ACLO		

52. [追加] ボタンをクリックします。

「ACL情報 (ACL0)」ページが表示されます。

53. 「IP 定義情報」をクリックします。

「IP定義情報」が表示されます。

54. 以下の項目を指定します。

- プロトコル →すべて
 送信元情報
 IPアドレス → 192.168.1.0
 アドレスマスク → 24 (255.255.255.0)
- あて先情報
 IPアドレス
 アドレスマスク

• Qos

→24(255.255.255.0) →指定なし

→ 192.168.2.0

■IP定義情報		
ブロトコル		すべて (番号指定:
送信元情	IPアドレス	192.168.1.0
報 アドレスマ スク		24 (255.255.255.0)
あて先情	IPアドレス	192.168.2.0
報	アトレスマスク	24 (255.255.255.0)
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい

- 55. [保存] ボタンをクリックします。
- **56. 設定メニューのルータ設定で「テンプレート情報」をクリックします**。 「テンプレート情報」ページが表示されます。

- テンプレート名 → vpn-shiB
- 接続種別 → IPsec/IKE(動的 VPN)

<テンプレート情報追加フィールド>		
テンプレート名 vpn-shiB		
接続種別	● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN)	

機種により、接続先種別の表示が上記の画面とは異なります。

58. [追加] ボタンをクリックします。

「テンプレート情報 (vpn-shiB)」と設定項目が表示されます。

59. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 60. 以下の項目を指定します。
 - 使用するrmt インタフェース →rmt10から10インタフェースを予約
 - 自側エンドポイント → 192.168.1.1

使用するrmtインタフェース	rmt10 から10 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケットについて 🛛 🛛 🕸 💌
自側エンドボイント	192.168.1.1

- 61. [保存] ボタンをクリックします。
- **62.** テンプレート情報(vpn-shiB)の設定項目の「動的 VPN 関連」をクリックします。 動的 VPN 関連の設定項目と「基本情報」が表示されます。

63. 以下の項目を指定します。

- ドメイン情報 →使用する
 "使用する"を選択すると、以下の項目が指定できます。
- ドメイン情報 →0 (example.com)

■基本情報	3
ドメイン情報	○ 使用しない ④ 使用する O(example.com) ▼

- 64. [保存] ボタンをクリックします。
- **65.** テンプレート情報 (vpn-shiB) の設定項目の「IPsec/IKE 関連」をクリックします。 IPsec/IKE 関連の設定項目と「IPsec 情報」が表示されます。

• SAの	設定	
暗号フ	ァルゴリズム	→aes-cbc-128
認証アルゴリズム		→hmac-sha1
PFS₿	寺の DH グループ	→modp768(グループ1)
	k+ ±0	10
IPsec	肩 鞭	3
	暗号アルゴリズム	□aes-cbc-256 □aes-cbc-192 ☑aes- cbc-128
		3des-cbc des-cbc null

SAの設	認証アルゴリスム	□hmac-md5 ☑hmac-sha1 □認証なし
定	PFS時のDHグル ーブ	modp768(ヴループ1) 🔽
	SA有効時間	8 時間 🕶
	SA有効データ量	0 GByte 🗸

67. [保存] ボタンをクリックします。

68. IPsec/IKE 関連の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

69. 以下の項目を指定します。

IKE 認証鍵
 鍵 →文字列
 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
 SAの設定
 暗号アルゴリズム → aes-cbc-128
 認証 (ハッシュ)アルゴリズム → hmac-sha1
 DH グループ → modp768 (グループ1)

IKE認証	键識別	○16進数 ⊙文字列
鍵	鍵	•••••
IKE認証	方式	shared
	暗号アルコリズム	aes-cbc-128 💌
SAの設	認証(ハッシュ)アル ゴリズム	hmac-shal 💌
疋	DHグループ	modp768(グループ1) 💌
	SA有効時間	24 時間 🖌

70. [保存] ボタンをクリックします。

71. IPsec/IKE 関連の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

72. 以下の項目を指定します。

接続先監視
 送信元IPアドレス → 192.168.1.1

■接続制御	青報	3
按结生防闭	送信元IPアドレス	192.168.1.1
1女初775亩1光	正常時送信間隔	● 秒 ♥

73. [保存] ボタンをクリックします。

- 設定メニューのルータ設定で「相手情報」をクリックします。 74. 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。 75. 「ネットワーク情報」が表示されます。
- 「ネットワーク情報」でネットワーク名が vpn-honの[修正] ボタンをクリックします。 76. 「ネットワーク情報 (vpn-hon)」ページが表示されます。
- 「IP関連」をクリックします。 77. IP関連の設定項目と「IP基本情報」が表示されます。
- 「動的VPN情報」をクリックします。 78.

「動的 VPN 情報」が表示されます。

- 79. 以下の項目を指定します。
 - 動的VPN 接続 →する 相手ネットマスク →24 (255.255.255.0) 利用するテンプレート情報 →vpn-shiB • ACL定義番号 →0



ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の [選択] ボタンをクリックして設定します。

<動的VPN情報入力フィールド>		
動的VDN接結	 ● する 相手ネットマスク 	24 (255.255.255.0)
	利用するテンプレート情報 ○しない	vpn-shiB 🔽
ACL定義番号	0 参照	

- [追加] ボタンをクリックします。 80.
- 81. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

支社Bを設定する

「支社Aを設定する」を参考に、支社Bを設定します。

「相手情報」-「ネットワーク 「ネットワーク情報(internet)」 「静的 NAT 情報」	>情報」 」-「IP 関連」
• プライベート IP 情報	
IPアドレス	→ 192.168.2.1
ポート番号	→ isakmp
 グローバル IP 情報 	
IPアドレス	→指定しない
ポート番号	→ isakmp
• プロトコル	→ udp
 プライベートIP情報 	
IPアドレス	→ 192.168.2.1
ポート番号	→すべて
 グローバルIP情報 	
IPアドレス	→指定しない
ポート番号	→すべて
• プロトコル	→ esp

「相手情報」-「ネットワーク情報」

•	ネットワーク名	→vpn-srv			
۲ł	「ネットワーク情報(vpn-srv)」-「IP 関連」				
[7	スタティック経路情報」				
•	ネットワーク あて先IPアドレス	→ネットワーク指定 →192 168 10 0			
	あて先アドレスマスク	→24 (255.255.255.0)			
•	メトリック値	$\rightarrow 1$			
•	優先度	→0			
F授	ē続先情報」				
•	接続先名	→dvpn-srv			
•	接続先種別	→IPsec/IKE接続			
F授	衰続先情報」-「IPsec/IKE接続」				
「砉	基本情報」				
•	鍵交換モード	→Aggressive Mode(Initiator)使用			
	相手側エンドポイント	→202.168.2.66			
	自装置識別情報	→shisyaB			
ΓIF	Psec情報」				
•	SAの 設定				
	暗号アルゴリズム	→des-cbc			
	認証アルゴリズム	→hmac-md5			

「IKE情報」

 IKE 認証鍵 鍵識別 鍵 SAの設定 暗号アルゴリズム 認証(ハッシュ)アルゴリズム DH グループ 	→文字列 → 1234567890abcdefghijklmnopqrstuvwxyz → des-cbc → hmac-md5 → modp768 (グループ1)
「動的 VPN 情報」-「クライアン	'卜関連情報」
「ドメイン情報」 ・ ドメイン名 「ドメイン情報(0)」-「基本情報」	→ example.com
Ⅰ基本情報」● ドメイン名	→ example.com
 サーバ情報 アドレス ポート番号 認証ID 認証パスワード 有効期間 	→ 202.168.2.66 → 5070 → shisyaBid → shisyaBpass → 1 時間
● 優先度	→ 10
 セッション更新間隔 時間 クライアントIPアドレス 	→ 更新する → 5分 → 192.168.2.1
 VPN 通信 利用インタフェース 経路情報の優先度 IPv4 IPv6 	\rightarrow rmt0 \rightarrow 1 \rightarrow 1
「相手情報」-「ネットワーク情報	報」
 ネットワーク名 	→ vpn-hon
「ネットワーク情報(vpn-hon)」-	「IP関連」
「スタティック経路情報」	
 ネットワーク ホートローフ 	→ネットワーク指定

•	* / * / * /	
	あて先IPアドレス	→ 192.168.0.0
	あて先アドレスマスク	→ 24 (255.255.255.0)
•	メトリック値	→ 1
•	優先度	→ 0
•	ネットワーク あて先 IP アドレス	→ネットワーク指定 → 192.168.1.0
	あて先アドレスマスク	→ 24 (255.255.255.0)
•	メトリック値	→ 1
•	優先度	→ 2

「接続先情報」

1.13	女心ノし「月干以」	
•	接続先名	→ honsya
•	接続先種別	→ IPsec/IKE 接続
Γŧ	接続先情報」-「IPsec/IKE 接続」	
٢ł	基本情報」	
•	鍵交換モード	→動的VPN 接続
	自側エンドポイント	→ 192.168.2.1
ГП	Psec情報(動的VPN)」	
•	SAの 設定	
	暗号アルゴリズム	→ aes-cbc-128
	認証アルゴリズム	→ hmac-sha1
	PFS 時の DH グループ	→ modp768(グループ1)
ΓI	KE情報(動的 VPN)」	
٠	IKE認証鍵	
	鍵識別	→文字列
	鍵	→ ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
•	SAの 設定	
	暗号アルゴリズム	→ aes-cbc-128
	認証(ハッシュ)アルゴリズム	→ hmac-sha1
	DHクループ	→modp768 (クルーフ1)
Γŧ	妾続制御情報」	
٠	接続先監視	→使用する
	送信元IPアドレス	→ 192.168.2.1
		→ 192.168.0.1
1	動的VPN関連」- 基本情報」	
13		
•	ドメイン情報	$\rightarrow 0$ (example.com)
•	相手側ユーザID	→ honsya
Гt	目手側ネットワーク情報」	
٠	動的VPNで接続する相手側ネット	ワーク → 192.168.0.0/24
•	テンプレートを使用して接続要求	→ しない
٢A	ACL情報」	
•	定義名	→ ACL0
ΓA	ACL 情報(ACL0)」-「IP 定義情報	艮」
•	プロトコル	→すべて
•	送信元情報	
	IPアドレス	→ 192.168.2.0
	アドレスマスク	→ 24 (255.255.255.0)
•	あて先情報	
	IPアドレス	→ 192.168.1.0
	アドレスマスク	→ 24 (255.255.255.0)
	_	

• Qos →指定なし

「相手情報」-「ネットワーク情報」			
「ネットワーク情報(vpn-hon)」-「IP 関連」			
「動的VPN情報」			
● 動的VPN 接続	→する		
相手ネットマスク	→ 24 (255.255.255.0)		
利用するテンプレート情報	→ vpn-shiB		
• ACL 定義番号	$\rightarrow 0$		
「テンプレート情報」			
 テンプレート名 	→ vpn-shiA		
● 接続種別	→ IPsec/IKE(動的 VPN)		
「テンプレート情報(vpn-shiA)」-	「共通情報」		
「基本情報」			
 使用するrmtインタフェース 	→ rmt10から10インタフェースを予約		
• 自側エンドポイント	→ 192.168.2.1		
「テンプレート情報(vpn-shiA)」-	「動的VPN関連」		
「基本情報」			
• ドメイン情報	→使用する		
「テンプレート情報(vpn-shiA)」-	「IPsec/IKE 関連」		
「IPsec情報」			
• SAの設定			
暗号アルゴリズム	→ aes-cbc-128		
認証アルゴリズム	→ hmac-sha1		
PFS 時の DH グループ	→modp768(グループ1)		
「IKE情報」			
● IKE 認証鍵			
鍵識別	→文字列		
鍵	→ ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890		
 SAの設定 			
暗号アルゴリズム	→ aes-cbc-128		
認証(ハッシュ)アルゴリズム	\rightarrow hmac-sha1		
DHクルーフ	→modp768 (クルーフ1)		
「接続制御情報」			
 接続先監視 ※信= IP コードレコー 			
达信元 IP アトレ人	→ 192.168.2.1		

動的 VPN サーバを設定する

- **1. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **2. 「グループID情報」をクリックします**。 「グループID情報」が表示されます。
- 3. 以下の項目を指定します。
 - グループ名 → dvpnserver

<グループID情報追加フィールド>		
ブループ名	dvpnserver	

4. [追加]ボタンをクリックします。

「グループID 情報(0)」と設定項目が表示されます。

5. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

- 6. 以下の項目を指定します。
 - ユーザID

→ honsyaid

→ honsyaid



7. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と設定項目が表示されます。

8. 「認証情報」をクリックします。

「認証情報」が表示されます。

- **9.** 以下の項目を指定します。
 - ユーザID
 - 認証パスワード → honsyapass

■認証情報	
ユーザID	honsyaid
認証バスワード	

- 10. [保存] ボタンをクリックします。
- 11. 手順2.~ 10.を参考に、支社Aを設定します。
- **12.** 手順2.~10.を参考に、支社Bを設定します。
- **13. 設定メニューのルータ設定で「動的 VPN 情報」をクリックします**。 「動的 VPN 情報」ページが表示されます。
- **14. 「サーバ関連情報」をクリックします**。 「サーバ関連情報」ページが表示されます。

→使用する
→ example.com
→行う
→ 0

■基本情報		3
	 ○ 使用した ③ 使用する 	มี 1 วี
サーバ機能	ドメイ ン名	example.com
2 / 10% BE	認証	 ○ 行わない ● 行う AAAグループID □

- 16. [保存]ボタンをクリックします。
- **17. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.15 システムログを採取する

適用機種 全機種

本装置では、各種システムログ(回線の接続/切断など)をネットワーク上のシステムログサーバに送信するこ とができます。また、セキュリティログとして以下のログを採取することができます。

- PPP (着信拒否)
- IPフィルタ(遮断したパケット)
- URLフィルタ(遮断したパケット)
- NAT (遮断したパケット、変換テーブル作成)
- DHCP(配布したIPv4アドレス、IPv6プレフィックス)
- IDS(検出されたパケット)
- IEEE802.1X 認証(不正端末の MAC アドレス)
- MACアドレス認証(不正端末のMACアドレス)
- ARP 認証(不正端末の MAC アドレス)

ここでは、採取したログをサーバに送信する場合の設定方法を説明します。



● 設定条件

- 以下のセキュリティログを採取する
 - PPP
 - IPフィルタ
 - URLフィルタ
 - NAT
 - DHCP
 - IDS
 - IEEE802.1X認証
 - MAC アドレス認証
 - ARP認証
- ログ受信用サーバのIPアドレス : 192.168.1.10

上記の設定条件に従って設定を行う場合の設定例を示します。

システムログ情報を設定する

- **1. 設定メニューの基本設定で「装置情報」をクリックします**。 「装置情報」ページが表示されます。
- 「システムログ情報」をクリックします。
 「システムログ情報」が表示されます。
- 3. 以下の項目を指定します。
 - システムログ送信 サーバ1 送信先ホスト
- →送信する →192.168.1.10
- セキュリティログ

→ PPP、IP フィルタ、URL フィルタ、NAT、DHCP、IDS、 IEEE802.1X 認証、MAC アドレス認証、ARP 認証



Si-R240、240B以外では、セキュリティログの表示が上記の画面とは異なります。

- 4. [保存] ボタンをクリックします。
- 5. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。 ここでは、本装置で確認する方法を説明します。

1. 表示メニューの「システム関連」の「システムログ情報」をクリックします。

「システムログ情報」ページが表示されます。

【システムログ情報】
システムログ情報を初期状態に戻す場合は、システムログ情報クリアをクリックしてください。
システムログ情報クリア
Jan 01 09:00:10 10.35.156.170 Si-R570: init: system startup now.
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: wan 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 0 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 2 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 3 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 4 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 5 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 5 ap 1 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 6 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 7 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 8 ap 0 is not attached: lack of co
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 8 ap 1 is not attached: lack of co
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 8 ap 2 is not attached: lack of co
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 9 ap 0 is not attached: lack of co
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 9 ap 1 is not attached: lack of co
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 10 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: remote 12 ap 0 is not attached: no line
Jan 01 09:00:10 10.35.156.170 Si-R570: sshd: generating public/private host key pair.
Jan 01 09:00:10 10.35.156.170 Si-R570: Idpd: ipv4 trans addr not found: LDP on interface I
Jan 01 09:00:10 10.35.156.170 Si-R570: Idpd: ipv4 trans addr not found: LDP on interface I
Jan 01 09:00:10 10.35.156.170 Si-R570: protocol: [mb/0] lan port link up
Jan 01 09:00:11 10.35.156.170 Si-R570: sshd: generated public/private host key pair.

2.16 マルチ NAT 機能(アドレス変換機能)を使う

適用機種 全機種

本装置のマルチNAT機能を使用すると、通信発生のたびにあいているグローバルアドレスを割り当てるので、限られた数のグローバルアドレスでそれ以上のパソコンを接続できます。

ここでは、静的 NAT を使って、サーバを公開する場合を例に説明します。静的 NAT は、特定のパソコンやアプリケーションに同じ IP アドレス、ポート番号を割り当てます。そのために Web を公開するような場合に適しています。

● 参照 Si-Rシリーズ 機能説明書「2.15 マルチ NAT 機能」(P.77)

◆ 同時に接続できる台数

機能	同時接続台数およびセッション数	備考	
基本NAT	グローバルアドレス数 セッション数制限なし	割り当て時間内は外部からの通信もできる 基本 NAT と静的 NAT で同一グローバルアドレスを 使用しないでください	
動的NAT	Si-R180、180B、260Bは最大1024セッション、 Si-R220B、220C、240、240Bは最大2000セッション、 Si-R370は最大3000セッション、 Si-R570は最大5000セッションまで	外部からの通信はできない	
静的NAT	Si-R180、180B、260Bは最大64個、 Si-R220B、220C、240、240Bは最大200個、 Si-R370は最大300個、 Si-R570は最大500個まで割り当て可能	プライベートアドレスとポートをグローバルアドレ スとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの 通信もできる	
あて先変換	Si-R180、180B、260Bは最大64個、 Si-R220B、220C、240、240Bは最大200個、 Si-R370は最大300個、 Si-R570は最大500個まで割り当て可能	グローバルアドレスをプライベートアドレスに割り 当てできる	

こんな事に気をつけて

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

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

2.16.1 プライベートLAN 接続でサーバを公開する



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。



上記の設定条件に従って設定を行う場合の設定例を示します。

静的NAT情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「NAT 情報」をクリックします。
 「NAT 情報」が表示されます。

• NATの使用

→マルチ NAT

NAT情報	3
NATの使用	●使用しない ○NAT ●マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

6. [保存] ボタンをクリックします。

7. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

こんな事に気をつけて

動的NATと静的NATが混在する場合、動的NATで使用するIPアドレスと静的NATで使用するIPアドレスは重複しない ように設定してください。

8. 以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 172.16.1.2
 ポート番号 → ftp
- グローバルIP情報
 IPアドレス → 192.168.0.1
 ポート番号 → ftp

 プロトコル → tcp

<静的NAT情報入力フィールド>		
プライベート	IPアド レス	172.16.1.2
IP忭青報	ボート 番号	ttp ▼(番号指定: "その他"を選択時の み有効です)
グローバル	IPアド レス	192.168.0.1
IP竹青幸G	ボート 番号	ttp ▼(番号指定: "その他"を選択時の み有効です)
プロトコル		tcp (番号指定: ************************************

9. [追加] ボタンをクリックします。

10. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

NAT セキュリティは、"高い"が初期値として選択されています。ftp や dns の要求した相手からの応答時には"高い" を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には"通常"を選択 してください。

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

2.16.2 PPPoE 接続でサーバを公開する

適用機種 Si-R180,180B

PPPoE を使ってインターネットへ接続している場合の例です。

ここでは、PPPoE 接続時に静的 NATを使ってサーバを公開する場合の設定方法を説明します。



既存のLANを使用する

•	ユーザ認証 ID	: userid
•	ユーザ認証パスワード	userpass
•	ネットワークアドレス/ネットマスク	: 192.168.1.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

かんたん設定で PPPoE 接続の情報を設定する

1. かんたん設定メニューで「PPPoE 接続」をクリックします。

「PPPoEかんたん設定」ページが表示されます。

2. [必須設定] で以下の項目を指定します。

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

■必須設定	3
ユーザ <mark>認</mark> 証ID	userid
ユーザ認証バスワード	•••••

3. [設定終了] ボタンをクリックします。 再起動後に、通信できる状態になります。

アドレス変換情報を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 「ネットワーク情報」で登録したネットワークの欄の [修正] ボタンをクリックします。 「ネットワーク情報」ページが表示されます。
- **「IP 関連」をクリックします**。
 IP 関連の設定項目と「IP 基本情報」が表示されます。
- IP 関連の設定項目の「NAT 情報」をクリックします。
 「NAT 情報」が表示されます。
- 6. 以下の項目を指定します。
 - NATの使用 →マルチNAT

林戸 NAT セキュリティで "高い"を選択した場合、ftp や DNS が要求した相手からの応答かどうかをチェックします。相手
 サーバが NAT を使用している場合など、要求先とは別のアドレスから応答する場合は、"通常"を選択してください。

こんな事に気をつけて

ネットワーク型接続でマルチNATを使用する際、グローバルアドレスの設定が必須となります。なお、端末型接続では、 接続時にグローバルアドレスが割り当てられるため、設定は不要です。

■NAT情報 3 NATの使用 ○使用しない ○NAT ○マルチNAT ○静的NATのみ

- 7. [保存] ボタンをクリックします。
- 8. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

•	プライベートIP情報	
	IPアドレス	→192.168.1.2
	ポート番号	→www,http
•	グローバル IP 情報	
	IPアドレス	→指定しない
	ポート番号	→www,http

こんな事に気をつけて

動的NATと静的NATが混在する場合、動的NATで使用するIPアドレスと静的NATで使用するIPアドレスは重複しないようにしてください。

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

<静的NAT情報入力フィールド>				
プライベート	IPアド レス	192.168.1.2		
IP忭春報	ポート 番号	www.http v(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
グローバル	IPアド レス			
IP忭青幸G	ポート 番号	www.http V(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

10. [追加] ボタンをクリックします。

11. 手順9.~10.を参考に、以下の項目を指定します。

プライベートIP情報
 IPアドレス → 192.168.1.3
 ポート番号 → ftp

 グローバルIP情報
 IPアドレス → 指定しない
 ポート番号 → ftp

12. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。
2.16.3 ネットワーク型接続でサーバを公開する

<u>適用機種</u> Si-R220B,220C,370,570

ここでは、静的 NAT を使ってサーバを公開する場合の設定方法を説明します。



● 設定条件

- slot0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート(Si-R220B、220C の場合)で ISDN でインターネットに接続する
- ISDNに接続する

•	ユーザ認証 ID	: userid
•	ユーザ認証パスワード	: userpass
•	ネットワーク型接続を行う	
•	既存のLANを使用する	
•	割り当てネットワークアドレス	: 10.10.10.96/29
•	wwwに割り当てる IP アドレス	: 10.10.10.98
•	ftpに割り当てるIPアドレス	: 10.10.10.99
•	動的 NAT で使用する IP アドレス	: 10.10.10.100~102
•	ネットワークアドレス/ネットマスク	: 192.168.1.0/24
•	ブロードキャストアドレス	: 192.168.1.255

ここでは、設定条件に従って、ISDN 接続する設定が行われていることを前提として、設定例を示します。

NAT情報を設定する

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3.** NAT 情報を行うネットワーク情報の【修正】ボタンをクリックします。 「ネットワーク情報 (internet)」ページが表示されます。
- **4. 「**IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

- IP 関連の設定項目の「NAT 情報」をクリックします。
 「NAT 情報」が表示されます。
- 6. 以下の項目を指定します。
 - NATの使用 →マルチNAT
 - グローバルアドレス → 10.10.10.100
 - アドレス個数 →3
 - アドレス割当てタイマ →5分
 - NATセキュリティ →高い

NAT情報	3
NATの使用	●使用しない●NAT●マルチNAT●静的NATのみ
クローバルアドレス	10.10.100
アトレス個数	3 1個
アトレス割当てタイマ	5 分 🗸
NATセキュリティ	○通常 ⊙ 高い

- 7. [保存] ボタンをクリックします。
- IP 関連の設定項目の「静的 NAT 情報」をクリックします。
 「静的 NAT 情報」が表示されます。

9. 以下の項目を指定します。

•	プライベートIP情報	
	IPアドレス	→ 192.168.1.2
	ポート番号	→www,http
•	グローバル IP 情報	
	IPアドレス	→ 10.10.10.98
	ポート番号	→www,http

プロトコル →すべて

<静的NAT情報入力フィールド>		
ブライベート	IPアド レス	192.168.1.2
IP竹青報	ボート 番号	www.http V番号指定: COM で選択時の み有効です)
グローバル IP情報	IPアド レス	10.10.10.98
	ポート 番号	www.http V(番号指定: COM で選択時の み有効です)
プロトコル		すべて ▼(番号指定: [*] その他 [*] を選択 時のみ有効です)

10. [追加] ボタンをクリックします。

11. 手順 10.~11.を参考に、以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 192.168.1.3
 ポート番号 → ftp (21)
- グローバルIP情報
 IPアドレス → 10.10.10.99
 ポート番号 → ftp (21)

 プロトコル →すべて

12. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

NATでは、FTPやDNSが要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している 場合など、要求先とは別のアドレスから応答するときには、「相手情報」-「ネットワーク情報」-「IP関連」-「NAT 情報」で、「NATセキュリティ」を"通常"に設定してください。 また、アドレス変換ルールが存在する場合、「NATセキュリティ」は画面から設定できない場合があります。

2.16.4 サーバ以外のアドレス変換をしないで、プライベートLAN 接続でサーバを公開する

適用機種 全機種

ここでは、静的NATだけを使って、サーバ以外のアドレス変換をしないで、FTPサーバを公開する場合の設定方法を説明します。



● 設定条件

[事務所A側]

- LANOポートを使用する
- 静的 NAT だけを使用する

[グループ LAN 側]

٠	IPアドレス	: 172.16.1.1
•	ネットワークアドレス/ネットマスク	: 172.16.1.0/24
•	FTPサーバのIPアドレス	: 172.16.1.2

上記の設定条件に従って設定を行う場合の設定例を示します。

静的NAT情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **4.** IP **関連の設定項目の「NAT 情報」をクリックします**。 「NAT 情報」が表示されます。

5. 以下の項目を指定します。

• NATの使用

→静的NATのみ

NAT情報	3
NATの使用	●使用しない ●NAT ●マルチNAT ●静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

- 6. [保存] ボタンをクリックします。
- 7. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

8. 以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 172.16.1.2
 ポート番号 → ftp

 グローバルIP情報
 IPアドレス → 192.168.0.1
 ポート番号 → ftp
- プロトコル → tcp

<静的NAT情報入力フィールド>		
ブライベート	IPアド レス	172.16.1.2
IP情報	ボート 番号	★(番号指定: "その他"を選択時の み有効です) (番号指定: (番号# (番号# (番母# (番母# (毎) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕) (⊕)
グローバル IP情報 番号	IPアド レス	192.168.0.1
	ボート 番号	★ ★ ● (番号指定: ************************************
ブロトコル		tcp (番号指定: 7その他"を選択時のみ有効です)

9. [追加] ボタンをクリックします。

10. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

NAT セキュリティは、"高い"が初期値として選択されています。ftpやdnsの要求した相手からの応答時には"高い" を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には"通常"を選択 してください。 また、アドレス変換ルールが存在する場合、「NAT セキュリティ」は画面から設定できない場合があります。

2.16.5 複数の NAT トラバーサル機能を使用した IPsec クライアントを 同じ IPsec サーバに接続する

適用機種 全機種

ここでは、静的NATを使って、複数のNATトラバーサル機能を使用したIPsecクライアントを同じIPsecサーバに接続する場合の設定方法を説明します。



● 設定条件

[IPsec サーバ側]

- LANOポートを使用する
- マルチ NAT を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

NAT情報を設定する

- 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「NAT 情報」をクリックします。
 「NAT 情報」が表示されます。

5. 以下の項目を指定します。

- NATの使用 →マルチNAT
- IPsecパススルー →無効

■NAT情報	3
NATの使用	●使用しない ● NAT ● マルチ NAT ● 静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません
グローバルアドレス	
アトレス個数	1
アトレス割当てタイマ	5 分 🗸
NATセキュリティ	○通常 ⊙ 高い
IPsecバススルー	○有効⊙無効

- こんな事に気をつけて
 - NAT セキュリティは、"高い"が初期値として選択されています。ftpやdnsの要求した相手からの応答時には"高い"を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には"通常"を選択してください。

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

- IPsec クライアントが NAT トラバーサル機能を使用する場合は、IPsec パススルーを"無効"に設定します。IPsec パススルーを"有効"に設定すると、相手ごとに 1 つの IPsec パスしか接続することができません。
- 6. [保存] ボタンをクリックします。
- 7. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.16.6 NAT あて先変換で双方向のアドレスを変換する

適用機種 全機種

ここでは、NATあて先変換を使って、双方向のIPアドレスを変換する場合の設定方法を説明します。 この機能を使用して異なるアドレス体系をもつA社とB社を接続した場合、同じアドレス体系であるかのように 見せることができます。



: 172.16.1.1

● 設定条件

[A社]

- IPアドレス
- ネットワークアドレス/ネットマスク : 172.16.1.0/24

[B社]

- LAN0ポートを使用する
- マルチ NAT を使用する
- NAT あて先変換を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

NATあて先変換情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- IP 関連の設定項目の「NAT 情報」をクリックします。
 「NAT 情報」が表示されます。

5. 以下の項目を指定します。

• NATの使用

→マルチNAT

	INAT情報	3
N	ATの使用	●使用しない ●NAT ●マルチNAT ●静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

6. [保存] ボタンをクリックします。

7. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的NAT情報」が表示されます。

8. 以下の項目を指定します。

- プライベートIP情報
 IPアドレス → 172.16.1.2
 ポート番号 →すべて
- グローバルIP情報
 IPアドレス → 192.168.100.2-192.168.100.254
 ポート番号 →すべて

<静的NAT情報入力フィールド>			
プライベート	IPアド レス	172.16.1.2	
IP情報	ボート 番号	すべて ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
グローバル	IPアド レス	192.168.100.2-192.168.100.254	
IP情報	ボート 番号	すべて ▼(番号指定: 「その他"を選択時の み有効です)	

9. [追加] ボタンをクリックします。

10. IP 関連の設定項目の「NAT あて先変換情報」をクリックします。

「NATあて先変換情報」が表示されます。

11. 以下の項目を指定します。

- プライベートアドレス →172.16.100.2
- グローバルアドレス → 192.168.1.2-192.168.1.254

<natbox< td=""></natbox<>	変換情報入力フィールド>
ブライベートアドレス	172.16.100.2
グローバルアドレス	192.168.1.2-192.168.1.254

- 12. [追加]ボタンをクリックします。
- **13. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.17 VoIP NAT トラバーサル機能を使う

適用機種 全機種

マルチ NAT機能を使用すると動作しない VoIP アダプタが UPnP に対応している場合、本装置の VoIP NAT トラ バーサル機能を使用することによって動作できるようになることがあります。同様に、UPnPに対応した装置や アプリケーションプログラムもマルチNAT機能を使用しても動作できるようになることがあります。

参照 Si-Rシリーズ 機能説明書 [2.16 VoIP NAT トラバーサル機能」(P.81)

ここでは、UPnP対応VoIPアダプタやUPnP対応アプリケーションプログラムを使用する設定方法を説明します。



● 設定条件

[インターネット側LAN]

- LAN0ポートを使用する
- 転送レート :自動認識
- IPアドレス :DHCPサーバから自動的に取得
- マルチ NAT を使用する グローバルアドレス アドレス個数
- :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 : 1
- アドレス割り当てタイマ :5分
- NATでのSIPアプリ対応を無効にする

[UPnP対応装置(プライベートLAN)側]

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

こんな事に気をつけて

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

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

ここでは、設定条件に従って、LANの設定が行われていることを前提とします。 上記の設定条件に従って設定を行う場合の設定例を示します。

→使用する

UPnP 情報を設定する

- 設定メニューのルータ設定で「UPnP情報」をクリックします。
 「UPnP情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - UPnP 機能



- 3. [保存] ボタンをクリックします。
- **4. 画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.18 TOS/Traffic Class 値書き換え機能を使う

適用機種 全機種

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットをIPアドレスとポート 番号の組み合わせでTOS/Traffic Class 値を変更することにより、ポリシーベースネットワークのポリシーに合わ せることができます。

● 参照 Si-Rシリーズ 機能説明書「2.17 TOS/Traffic Class 値書き換え機能」(P.84)

TOS/Traffic Class 値書き換え機能の条件

本装置では、以下の条件を指定することによって、ポリシーベースネットワークのポリシーに合ったTOS/Traffic Class 値に書き換えることができます。

- プロトコル
- 送信元情報(IPアドレス/アドレスマスク/ポート番号)
- あて先情報(IPアドレス/アドレスマスク/ポート番号)
- IPパケットのTOS値またはIPv6パケットのTraffic Class値
- 新TOSまたはTraffic Class

ここではネットワークが以下のポリシーをもつ場合の設定方法を説明します。

- FTP(TOS値a0)を最優先とする
- その他はなし



● 設定条件

- 送信元IPアドレス/アドレスマスク
- 送信元ポート番号
- あて先IPアドレス/アドレスマスク
- あて先ポート番号
- プロトコル

: 192.168.1.0/24

- :指定しない
- :指定しない
- :20 (ftp-dataのポート番号)、21 (ftpのポート番号)
- : TCP

•	TOS值	:00
•	新TOS值	: a0

上記の設定条件に従って設定を行う場合の設定例を示します。

FTP サーバのアクセスで TOS 値を00からa0に変更する

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ ACL0

<acl情報追加フィールド></acl情報追加フィールド>		
定義名	ACLO	

3. [追加] ボタンをクリックします。 「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

• QoS

•	プロトコル	→tcp
•	送信元情報 IPアドレス アドレスマスク	→ 192.168.1.0 → 24 (255.255.255.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →指定しない

- →指定しない →TOS
- **→**0

■IP定義情報		
ブロトコル		tcp ▼ (番号指定: [*] その他 [*] を選択時のみ有効です)
送信元情	IPアドレス	192.168.1.0
報	アトレスマ スク	24 (255.255.255.0)
あて先情	IPアドレス	
報	アトレスマスク	0 (0.0.0)
QoS		TOS TOS、または、DSCPを選択時に値を入力してくだ さい 0

- 6. [保存] ボタンをクリックします。
- **7.** 「TCP定義情報」をクリックします。

「TCP定義情報」ページが表示されます。

8. 以下の項目を指定します。

- 送信元ポート番号 →指定しない
- あて先ポート番号 →20 (ftp-dataのポート番号)、21 (ftpのポート番号)
- TCP 接続要求

→対象

TCP定義情報	3
送信元ポート番号	
あて先ボート番号	20,21
TCP接続要求	⊙対象○対象外

- [保存] ボタンをクリックします。 9.
- 設定メニューのルータ設定で「相手情報」をクリックします。 10. 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。 11. 「ネットワーク情報」が表示されます。
- 12. 「ネットワーク情報」でTOS 値書き換えの設定を行うネットワーク名の [修正] ボタンをクリックし ます。

「ネットワーク情報」が表示されます。

- 「IP関連」をクリックします。 13. IP関連の設定項目と「IPアドレス情報」が表示されます。
- 「TOS値書き換え情報」をクリックします。 14. 「TOS 値書き換え情報」が表示されます。
- 15. 以下の項目を指定します。
 - 新TOS →a0
 - ACL 定義番号 **→**0



「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<tos値書き換え情報入力フィールド></tos値書き換え情報入力フィールド>		
新TOS	a0	
ACL定義番号	0 参照	

- 16. [追加] ボタンをクリックします。
- 画面左側の [設定反映] ボタンをクリックします。 17. 設定した内容が有効になります。

2.19 VLAN プライオリティマッピング機能を使う

適用機種 全機種

VLAN プライオリティマッピング機能を使用して、レイヤ2スイッチなどでQoS制御を行うことができます。 本装置から送信される VLAN パケットの VLAN のプライオリティ値を、IP パケットの TOS フィールドおよび IPv6 パケットのトラフィッククラスフィールドの値から設定します。

● 参照 Si-Rシリーズ 機能説明書「2.18 VLAN プライオリティマッピング機能」(P.86)

本装置では、以下の条件を指定することによって、VLANのプライオリティフィールドを設定することができます。

- プロトコル
- TOS/Traffic Class
- プライオリティ

ここでは、本装置が以下の音声データを転送する場合の設定方法を説明します。

- 音声(IPでTOS値がa0)を最優先とする(プライオリティ値が7)
- その他は初期値(プライオリティ値が0)



● 設定条件

- プロトコル
 : IPv4
- TOS値 :a0
- プライオリティ値 :7

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

- 2. 「LAN 情報」で VLAN プライオリティマッピングの設定を行う LAN の [修正] ボタンをクリックします。 「LAN 情報(VLAN)」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。

4. 共通情報の設定項目の「VLAN プライオリティマッピング情報」をクリックします。

「VLANプライオリティマッピング情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル → IPv4
- TOS/Traffic Class → a0
- プライオリティ →7

<vlanプライオリティマッピング情報入力フィールド></vlanプライオリティマッピング情報入力フィールド>		
プロトコル ◎IPv4 ○IPv6		
TOS/Traffic Class	a0	
ブライオリティ	7	

- 6. [追加] ボタンをクリックします。
- 7. **画面左側の【設定反映】ボタンをクリックします**。 設定した内容が有効になります。

2.20 シェーピング機能を使う

適用機種 全機種

シェーピング機能を使用すると、LANおよびWAN回線に送出するデータ量を制限することができます。

2.20.1 特定のインタフェースでシェーピング機能を使う



ここでは、Ethernet回線の送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約帯域は 5Mbps

上記の設定条件に設定を行う場合の設定例を示します。

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

4. 以下の項目を指定します。

 シェーピング →使用する 最大送信レート → 5Mbps

シェービング	 ○ 使用しない ● 使用する 	
	最大送信レート 5 Mbps ⊻	

Si-R180、180Bでは、LANバックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.20.2 送信先ごとにシェーピング機能を使う

適用機種 全機種

ここでは、各拠点に送出するデータ量を制限する場合の設定方法を説明します。



● 設定条件

- 広域 Ethernet をアクセスラインとする。L2-VPN 網を利用して本社と各拠点を接続する
- 本社から拠点Aへの送信データは、最大3Mbpsに制限する
- 本社から拠点Bへの送信データは、最大3Mbpsに制限する
- 本社から拠点Aと拠点Bへの送信データの合計は、最大5Mbpsに制限する
- 本社の本装置はLAN ポートのアドレス設定ができた状態から設定を始める

上記の設定条件に設定を行う場合の設定例を示します。

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

- 4. 以下の項目を指定します。
 - シェーピング →使用する 最大送信レート → 5Mbps

シェービング	○ 使用しない③ 使用する
	最大送信レート 5 Mbps ✔

Si-R180、180Bでは、LANバックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

- 5. [保存] ボタンをクリックします。
- 6. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 8. 以下の項目を指定します。
 - ネットワーク名

<ネットワーク情報追加フィールド>		
ネットワーク名	kyotenA	

→ kyotenA

9. [追加] ボタンをクリックします。

「ネットワーク情報(kyotenA)」が表示されます。

10. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 11. 以下の項目を指定します。
 - シェーピング →使用する
 最大送信レート → 3Mbps

シェービング	○ 使用しない ◎ 使用する		
	最大送信レート 3 Mbps V		

- 12. [保存] ボタンをクリックします。
- 13. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

14. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 15. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →192.168.128.0
 →24 (255.255.255.0)



- 16. [追加] ボタンをクリックします。
- 17. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

18. 以下の項目を指定します。

• 接続先名

→OV-A

• 接続先種別 →別インタフェースから送出

機種により、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

別インタフェースから送出の設定項目と「基本情報」が表示されます。

20. 以下の項目を指定します。

- 送出先インタフェース → LAN1
- 転送先ルータ
 IPv4ルータ → 172.16.0.128

送出先インタフェース		LAN1 💌
転送先ルータ	IPv4ルータ	172.16.0.128
	IPv6ルータ	

21. [保存] ボタンをクリックします。

22. 手順6.~21.を参考にして、拠点Bを設定します。

「ネットワーク情報」

 ネットワーク名 	→kyotenB
「共通情報」	
• シェーピング	→使用する
最大送信レート	→3Mbps
「スタティック経路情報」	
 ネットワーク 	→ネットワーク指定
あて先IPアドレス	→192.168.192.0
あて先アドレスマスク	→24 (255.255.255.0)
「接続先情報」	
● 接続先名	→ OV-B
● 接続先種別	→別インタフェースから送出
「基本情報」	
• 送出先インタフェース	→LAN1
 転送先ルータ 	
IPv4ルータ	→ 172.16.0.192

23. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.21 データ圧縮/ヘッダ圧縮機能を使う

適用機種 全機種

PPPを使った相手装置との接続時に、データ圧縮およびヘッダ圧縮機能によって回線の利用効率を高めることができます。

データ圧縮は、ISDN 接続、専用線接続、およびモデム接続をサポートしています。

データ圧縮およびヘッダ圧縮機能を利用する場合、接続する相手装置側でも同じ圧縮機能をサポートしている必要があります。以下に、サポートしている圧縮機能を示します。

- データ圧縮(Si-R220B、220C、370、570)
 - LZS
- ヘッダ圧縮
- VJ : : VJ へッダ圧縮(RFC1144 に準拠)の利用
- IPHC : IP ヘッダ圧縮(圧縮方法:RFC2507/RFC2508、ネゴシエーション方法:RFC2509) に準拠)の利用

ヘッダ圧縮の場合

ここでは、PPPoE 接続をネットワーク0(rmt0)で定義している環境に対して、ヘッダ圧縮を行う場合の設定方法を説明します。

3

● 設定条件

- ネットーク情報(rmt0)で PPPoE による通信環境が設定済み
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってヘッダ圧縮を行う場合の設定例を示します。

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- **3. 「**PPP 関連」をクリックします。

PPP 関連に関する項目と「圧縮情報」が表示されます。

- 4. 以下の項目を指定します。
 - ヘッダ圧縮(IPCP) → VJ、IPヘッダ圧縮

■
圧縮情報 ヘッダ圧縮 (IPCP) 図VJ 図IPヘッダ圧縮

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

こんな事に気をつけて

ヘッダ圧縮機能は、シェーピングによって通信速度が低速の場合に効果があります。高速回線で使用した場合は、処理 のオーバーヘッドによって回線の利用効率が低くなることがあります。

ISDN、専用線、モデム接続の場合

ここでは、ISDN 接続、専用線接続、およびモデム接続をネットワーク0(remote0)で定義している環境に対し てデータ圧縮およびヘッダ圧縮を併用する場合の設定方法を説明します。

● 設定条件

- ネットーク情報(rmt0)でISDNによる通信環境が設定済み
- データ圧縮機能を使用する
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってデータ圧縮およびヘッダ圧縮を行う場合の設定例を示します。

- **1. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- ネットワーク名がrmt0の[修正]ボタンをクリックします。
 「ネットワーク情報 (rmt0)」ページが表示されます。
- 「PPP 関連」をクリックします。
 PPP 関連の設定項目と「圧縮情報」が表示されます。
- 5. 以下の項目を指定します。
 - ヘッダ圧縮(IPCP) → VJ、IPヘッダ圧縮
 - データ圧縮(CCP) → LZS

■圧縮情報	3
ヘッダ圧縮 (IPCP)	✓VJ ☑IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	□IPヘッダ圧縮
テータ圧縮 (CCP)	▼LZS

- 6. [保存] ボタンをクリックします。
- 7. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて MPと併用する場合は、「相手情報」-「ネットワーク情報」-「PPP 関連」-「MP 情報」-「受信パケット順序制御」 を"する"に設定してください。

2.22 帯域制御 (WFQ) 機能を使う

適用機種 全機種

本装置の帯域制御(WFQ)機能では、IPアドレスやポート番号の組み合わせで帯域を割り当てることによって、 特定のデータを優先的に通すことができます。

● 参照 Si-R シリーズ 機能説明書「2.20 帯域制御(WFQ)機能」(P.88)

帯域制御 (WFQ) 機能の条件

本装置では、以下の条件を指定することによって、優先的にデータを通すように帯域を割り当てることができます。

- プロトコル
- IPアドレス
- ポート番号
- IPパケットのTOS値またはIPv6パケットのTraffic Class値

ここでは、広域 Ethernet による拠点間の接続がすでに設定されている場合を例に帯域制御を利用する設定方法を 説明します。



● 設定条件

- LAN0インタフェースで広域 Ethernet を利用する通信環境が設定済み
- 広域 Ethernet の契約速度は 1 Mbps
- 音声データ(TOS値:a0)を最優先で透過させる

上記の設定条件に従って帯域制御する場合の設定例を示します。

東京事業所を設定する

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

• 定義名

→ ACL0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ACLO

【追加】ボタンをクリックします。 「ACL定義情報(ACL0)」ページが表示されます。

4. 「IP 定義情報」をクリックします。 「IP 定義情報」ページが表示されます。

5. 以下の項目を指定します。

•	プロトコル	→すべて
•	送信元情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)

	アドレスマスク	→0 (0.0.0
•	QoS	→TOS
		→a0

IP定義	情報	3
ブロトコル		すべて (番号指定: ~ その他 ″ を選択時のみ有効です)
送信元情	IPアドレス	
報	アドレスマ スク	0 (0.0.0)
あて先情	IPアドレス	
報	アドレスマ スク	0 (0.0.0)
QoS		TOS

- 6. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 8. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報に関する設定項目と「基本情報」が表示されます。

10. 以下の項目を指定します。

 シェーピング	→使用する
最大送信レート	→1Mbps
シェービング	 ○ 使用しない ● 使用する 最大送信レート 1 Mbps ▼

Si-R180、180Bでは、LAN バックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

11. [保存] ボタンをクリックします。

12. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

13. IP 関連の設定項目の「帯域制御(WFQ)情報」をクリックします。

「帯域制御(WFQ)情報」が表示されます。

14. 以下の項目を指定します。

- 帯域 →最優先
- ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<帯域制御(WFQ)情報入力フィールド>		
帯域	 ●最優先 ● ベストエフォート ● 使用率 ● 使用帯域 Kbps ▼ ● 帯域を他と共有 共有できる定義が存在しません ▼ 	
ACL定義番号	0 参照	

- 15. [追加] ボタンをクリックします。
- **16. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

大阪事業所を設定する

「東京事業所を設定する」を参考に、大阪事業所を設定します。

「ACL情報」

 定義名 → ACL0

「ACL定義情報(ACL0)」-「IP定義情報」

- プロトコル →すべて 送信元情報 IPアドレス →指定しない アドレスマスク →0 (0.0.0)
- あて先情報 IPアドレス →指定しない アドレスマスク →0 (0.0.0)
- → TOS • QoS →a0

「LAN0 情報」-「共通情報」 「基本情報」

• インタフェース情報 →物理インタフェース シェーピング →使用する 最大送信レート →1Mbps

「LAN0情報」-「IP 関連」 「帯域制御(WFQ)情報」

- 帯域 →最優先 • ACL定義番号
 - →0

2.23 DHCP機能を使う

適用機種 全機種

本装置のIPv4 DHCPには、以下の機能があります。

- DHCP サーバ機能
- DHCPスタティック機能
- DHCP クライアント機能
- DHCPリレーエージェント機能

● 参照 Si-R シリーズ 機能説明書「2.21.1 IPv4 DHCP機能」(P.91)

本装置では、それぞれのインタフェースでDHCP機能が使用できます。

こんな事に気をつけて

- ・ 1つのインタフェースでは、1つの機能だけ動作します。同時に複数の機能を動作することはできません。
- ・ 本装置のDHCPサーバは、リレーエージェントを経由して運用することはできません。

本装置のIPv6 DHCPには、以下の機能があります。ここでは、IPv6 DHCPクライアント機能を使用する場合について説明しています。

- IPv6 DHCP サーバ機能
- IPv6 DHCP クライアント機能

● 参照 Si-Rシリーズ 機能説明書「2.21.2 IPv6 DHCP機能」(P.94)

2.23.1 DHCP サーバ機能を使う

適用機種 全機種

DHCPサーバ機能は、ネットワークに接続されているパソコンに対して、IPアドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびにIPアドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCPクライアント機能を持つパソコンはIPアドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- ドメイン名
- NTPサーバのIPアドレス
- TIMEサーバの IP アドレス
- WINSサーバのIPアドレス
- SIPサーバのドメイン名または IP アドレス

こんな事に気をつけて

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

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

・ 本装置のDHCPサーバ機能は、DHCPリレーエージェントのサーバにはなれません。

ここでは、DHCP サーバ機能を使用する場合の設定方法説明します。



● 設定条件

- 本装置のIPアドレス
- ブロードキャストアドレス
- パソコンに割り当てる IP アドレス
- パソコンに割り当て可能IPアドレス数
- ネットワークアドレス/ネットマスク
- DHCPサーバ機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP サーバ機能を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN 情報」ページが表示されます。

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

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

3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

IPアドレス

ネットマスク

- IPv4 →使用する
- IPアドレス →指定する
 - → 192.168.2.1
 - →24 (255.255.255.0)

ブロードキャストアドレス →ネットワークアドレス+オール1



- 5. [保存] ボタンをクリックします。
- **6.** IP 関連の設定項目の「DHCP 情報」をクリックします。 「DHCP 情報」が表示されます。

- : 192.168.2.1 : 3 (ネットワークアドレス+オール1)
- : 192.168.2.2~192.168.2.33
- : 32
- : 192.168.2.0/24

7. 以下の項目を指定します。

- DHCP機能 →サーバ機能を使用する 割当て先頭IPアドレス → 192.168.2.2
 割当てアドレス数 → 32
- ★ DHCPサーバ機能で割り当てることのできる最大数は253です。

DHC	P情報
	 ○使用しない ○リレー機能を使用する
	DHCPサーバIPアドレス2
	MACアドレスチェック □ホストデータベース □AAA 参照するAAA情報
	● サーバ機能を使用する
	割当て先頭IPアドレ ス 192.168.2.2
	割当てアドレス数 32
	リース期間 1 日 💌
	デフォルトルータ広報
DHCP	DNSサ プライマリ
機能	報セカンダリ
	ドメイン名広報
	TIMEサーバ広報
	NTPサーバ広報
	WINSサ プライマリ
	報やカンダリー
	arptt 記述形式 ●ドメイン名 ●IPアドレス
	SIP プライマリ
	セカンダリ
	MACアドレスチェッ
	ク DAAA 参照するAAA情報 D
	※"割当て先頭アドレス"が本装置のIPアドレスと同じネットワ ークアドレス内であることを確認してください。

必要に応じて上記以外の項目を指定します。

- 8. [保存] ボタンをクリックします。
- 9. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.23.2 DHCPスタティック機能を使う

適用機種 全機種

DHCPサーバは、使用していないIPアドレスを一定期間(またはパソコンがIPアドレスを返却するまで)割り当 てます。不要になったIPアドレスは自動的に再利用されるため、パソコンのIPアドレスが変わることがあります。 本装置では、IPアドレスとMACアドレスを対応付けることによって、登録されたパソコンからDHCP要求が発行 されると、常に同じIPアドレスを割り当てることができます。これをDHCPスタティック機能と言います。 DHCPスタティック機能を利用する場合は、ホストデータベース情報にIPアドレスとMACアドレスを設定して ください。

MACアドレスとは、LAN機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。 本装置がサポートしている「IPフィルタリング機能」、「マルチルーティング機能」などはパソコンのIPアドレスが固定されていないと使いにくい場合があります。これらの機能とDHCPサーバ機能の併用を実現するために、本装置では「DHCPスタティック機能」をサポートしています。

こんな事に気をつけて

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

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

 アドレス 192.168.2.1
 192.168.2.1

 キットワークアドレス 192.168.2.024
 キットワークアドレス 192.168.2.024

ここでは、DHCPスタティック機能を使用する場合の設定方法を説明します。

● 設定条件

- ネットワークアドレス/ネットマスク : 192.168.2.0/24
- IPアドレスを固定するパソコンのMACアドレス: 00:00:0e:12:34:56
- 割り当てIPアドレス : 192.168.2.2
- DHCPサーバ機能を使用する

こんな事に気をつけて

設定の「LAN0 情報」、「LAN1 情報」でDHCP サーバ機能を使用する設定をしていない場合は、DHCP スタティック機能 の設定は有効になりません。

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCPスタティック機能を設定する

- **1. 設定メニューのルータ設定で「ホストデータベース情報」をクリックします**。 「ホストデータベース情報」ページが表示されます。
- 2. 未設定の欄の [修正] ボタンをクリックします。
- 3. 以下の項目を指定します。
 - IPv4アドレス → 192.168.2.2
 - MACアドレス → 00:00:0e:12:34:56

載記
ホストデータベース情報は「リモートパワーオン機能」、「DHCPスタティック機能」、「DNSサーバ機能」で使われて
おり、それぞれ必要な項目だけを設定します。

	ホスト名	
	IPv4アドレス	192.168.2.2
	IPv6アドレス	
'	MACアドレス	00:00:0e:12:34:56
	リモート電源制御	⊙対象○対象外

必要に応じて上記以外の項目を指定します。

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

権足 DHCPスタティック機能で設定できるホストの最大数は64です。

2.23.3 DHCP クライアント機能を使う

適用機種 全機種

DHCP クライアント機能は、DHCP サーバから IP アドレスなどの情報を取得する機能です。使用する場合は、 DHCP サーバが動作している LAN に接続する必要があります。利用者は、IP アドレスを意識することなくネット ワークを利用できます。

本装置のDHCPクライアント機能は、以下の情報を受け取って動作します。

- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- TIMEサーバのIPアドレス
- NTPサーバのIPアドレス
- ドメイン名
- リース更新時間

こんな事に気をつけて

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

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

ここでは、DHCP クライアント機能を使用する場合の設定方法を説明します。



● 設定条件

本装置のIPアドレス :[

:DHCPサーバから取得する

上記の設定条件に従って設定を行う場合の設定例を示します。

DHCP クライアント機能を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4
- →使用する
- IPアドレス → DHCPで自動的に取得する

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
IP アド レス	 ● DHCPで自動的に取得する ● 指定する IPアドレス ネットマスク 2 (192.0.0) ブロードキャストアドレ ス 		

- 5. [保存] ボタンをクリックします。
- IP 関連の設定項目の「NAT 情報」をクリックします。
 「NAT 情報」が表示されます。
- 7. 以下の項目を指定します。
 - NATの使用

→フルチNAT	

■NAT情報	3
NATの使用	○使用しない○NAT ○マルチNAT ○静的 NATのみ ※NATの使用とDHCPリレーサービスの併 用はできません

- 8. [保存] ボタンをクリックします。
- 9. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.23.4 DHCP リレーエージェント機能を使う

適用機種 全機種

DHCPクライアントは、同じネットワーク上にあるサーバから、IPアドレスなどの情報を獲得することができます。 DHCPリレーエージェントは、遠隔地にあるDHCPクライアントの要求をDHCPサーバが配布する情報を中継す る機能です。この機能を利用することで、遠隔地の別のネットワークにDHCPサーバが存在する場合も同様に情 報を獲得することができます。

こんな事に気をつけて

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

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

ここでは、DHCPリレーエージェント機能を使用する場合の設定方法を説明します。

LAN接続の場合



上記の設定条件に従って設定を行う場合の設定例を示します。
DHCPリレーエージェント機能を設定する

ここでは、LAN1を使用した場合を例に説明します。LAN0の場合も同様の手順で設定できます。

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

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

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

3. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

- 以下の項目を指定します。 5.
 - DHCP機能 →リレー機能を使用する DHCPサーバIPアドレス1 → 192.168.0.10

DHC	HCP情報 []						
	○使用しない						
	● リレー機能を使用する						
	DHCPサーバIPアドレス1 192.168.0.10						
	MACアドレスチェック □ホストデータベース □AAA 参照するAAA情報						
	○ サーバ機能を使用する						
	割当て先頭IPアドレ ス						
	割当てアドレス数 32						
	リース期間 1 日 💌						
	デフォルトルータ広報						
DHCP							
機能	報セカンダリ						
	ドメイン名広報						
	TIMEサーバ広報						
	NTPサーバ広報						
	WINSサ プライマリ						
	報 セカンダリ						
	記述形式 ●ドメイン名 OIPアドレス						
	SIPサー プライマリ						
	「「「「」」 セカンダリ						
	MACアドレスチェッ						
	ク □ AAA 参照するAAA情報 □						
	※"割当て先頭アドレス"が本装置のIPアドレスと同じネッ ークアドレス内であることを確認してください。	トワ					

- 6. [保存] ボタンをクリックします。
- 画面左側の [設定反映] ボタンをクリックします。 7. 設定した内容が有効になります。

リモート接続の場合

適用機種 Si-R220B,220C,260B,370,570



● 設定条件

- DHCPリレーエージェント機能を使用する
- 支社に DHCP クライアントが存在する
- 本社にDHCPサーバが存在する

[本社]

•	ルータのIPアドレス	: 192.168.2.1
•	ネットワークアドレス/ネットマスク	: 192.168.2.0/24
•	DHCPサーバのIPアドレス	: 192.168.2.10
[3	5社]	
•	2社] 本装置のIPアドレス	: 192.168.1.1

ここでは、本社、支社のネットワークがすでに専用線接続されていることを前提としています。

● 参照「1.10事業所LANを専用線で接続する」(P.103)

上記の設定条件に従って設定を行う場合の設定例を示します。

支社を設定する(DHCP リレーエージェント機能を設定する)

ここでは、LAN0を使用した場合を例に説明します。LAN1の場合も同様の手順で設定できます。

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の [修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **3.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

- 5. 以下の項目を指定します。
 - DHCP機能 →リレー機能を使用する
 DHCPサーバIPアドレス1 → 192.168.0.10

DHCP"情報							
	0						
	۲	リレー機能	能を使用する	5			
		DHCPサ	ーバIPアドレ	ス1 192.168.0.10			
		DHCPサ	ーバIPアドレ	,72			
MAC		мас75	レスチェック	 □ホストデータベース □AAA 参照するAAA情報 			
	0	サーバ機	能を使用す	3			
		割当て先 ス	頭IPアドレ				
		割当てア	ドレス数	32			
		リース期	8	1 🛛 💌			
		デフォル 報	トルータ広				
DHCP		DNSサ	プライマリ				
機能		報	セカンダリ				
		ドメイン名	広報				
		TIMEサー	-バ広報				
		NTPサー	バ広報				
		WINSサ	プライマリ				
		報	セカンダリ				
			記述形式	●ドメイン名 ○IPアドレス			
		SIPサー バ広報	プライマリ				
	7 1)2471	/ 1/2-A+IX	セカンダリ				
		MACZH	レスチェッ	□ホストデータベース			
		ク		■AAA 参照するAAA情報			
		」 ※"割当?	「先頭アドレ	ス"が本装置のIPアドレスと同じネットワ			
		ークアドレ	ス内である	ことを確認してください。			

- 6. [保存] ボタンをクリックします。
- **一面方側の[設定反映]ボタンをクリックします**。

 設定した内容が有効になります。

2.23.5 IPv6 DHCP クライアント機能を使う

適用機種 全機種

IPv6 DHCP クライアント機能は、プロバイダの IPv6 DHCP サーバから IPv6 プレフィックスなどの情報を取得する 機能です。この機能を利用すると、プロバイダから取得した IPv6 プレフィックスをサブネット化して、Router Advertisement Message (RA)で下流ネットワークに 64 ビットの IPv6 プレフィックスを配布することができます。 ここでは、PPPoE でインターネットに接続して、IPv6 DHCP クライアント機能を使用する場合の設定方法を説明 します。



: userpass

:48ビット

: LAN1 ポート

● 設定条件

- PPPoEで使用するLANポート : LAN0ポート
 ユーザ認証ID : userid
- ユーザ認証パスワード
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長
- IPv6 プレフィックスを配布する LAN ポート
- RAで配布する IPv6 プレフィックスのサブネット ID : 0001

上記の設定条件に従って設定を行う場合の設定例を示します。

IPv6 DHCP クライアントを設定する

- 1. 「1.6 インターネットへ PPPoE で接続する」(P.67)を参考に、PPPoE での接続を設定します。
- **2. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **3.** クライアントの設定を行うネットワーク情報の [修正] ボタンをクリックします。 「ネットワーク情報」が表示されます。
- 「IPv6 関連」をクリックします。
 IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

- 5. 以下の項目を指定します。
 - IPv6

→使用する

■IPv6基本情報 IPv6 ○使用しない ◎使用する

- 6. [保存] ボタンをクリックします。
- **7. IPv6 関連の設定項目の「IPv6 DHCP 情報」をクリックします**。 「IPv6 DHCP 情報」が表示されます。
- 8. 以下の項目を指定します。
 - DHCP機能

→クライアント機能を使用する

3

■IPv6 DHCP情報	3
DHCP機能	 ●使用しない ● クライアント機能を使用する ● サーバ機能を使用する

9. [保存] ボタンをクリックします。

LAN情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - インタフェース →物理LAN



- **3. [追加] ボタンをクリックします**。 「LAN1 情報(物理 LAN)」ページが表示されます。
- **「IPv6 関連」をクリックします。** IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

• IPv6

→使用する

- IPv6アドレス アドレスまたはプレフィックス → dhcp@rmt0:1::
- ルータ広報 →送信する

■IPv6基本情報 []													
IPv6	/6 ○使用しない ●使用する												
インタフェースID	 ● 自動 ○ 指定する 												
	איק	レスまた(はプレフ	ィックス		Valic 期限	Life 有	time ș	無期	限	Pref. Life 期限有	time 魚	無期限	フラ グ
IPv6	dhc	p@rmt0:1::			30		Β	*		7	Β	¥ 🗌	c0
アトレス					30		B	*		7	В	¥	c0
					30		B	*		7	Β	~	c0
					30		B	*		7	В	v	c0
	0 0	送信しない 送信する											
		最大送信間隔	600	Ŧ	沙								
		最小送信間隔	200	Ŧ	沙								
ルー		Router Lifetime	1800	Ŧ	沙								
タ広報		MTU]									
тк		Reachable Time	0	3	り 秒								
		Retrans Timer	0	3	ジ秒								
		Cur Hop Limit	64]									
		フラグ	00										

6. [保存] ボタンをクリックします。

ProxyDNS を設定する

1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。

→*

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

- 3. 以下の項目を指定します。
 - ドメイン名
 - 動作

→接続先のDNS サーバへ指定ネットワークを経由して問い合わせる

	< 順引き情報入力フィールド>						
ドメイン 名	*						
タイプ	すべて ▼(番号指定 "その他"を選択時のみ有効で す。)						
送信元 IPアドレ ス	※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。						
動作	 ○ 廃棄する ○ 接続先のDNSサーバへ問い合わせる ネットワーク名 rmt0 ※ 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 rmt0 解決したホストへのホスト経路自動作成 ●しない ○する ○ DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 使用できるインタフェースが存在しません 設定したDNSサーバへ問い合わせる DNSサーバアドレス 						

- 4. [追加] ボタンをクリックします。
- 「逆引き情報」をクリックします。
 「逆引き情報」が表示されます。
- 6. 以下の項目を指定します。
 - 動作

- →接続先のDNS サーバへ指定ネットワークを経由して問い合わせる
- 7. [追加] ボタンをクリックします。
- 8. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.24 DNSサーバ機能を使う (ProxyDNS)

適用機種 全機種

本装置のProxyDNSには、以下の機能があります。

- DNSサーバの自動切り替え機能
- DNSサーバアドレスの自動取得機能
- DNS問い合わせタイプフィルタ機能
- DNS サーバ機能

● 参照 Si-Rシリーズ 機能説明書「2.22 DNS サーバ機能」(P.96)

2.24.1 DNSサーバの自動切り替え機能(順引き)を使う

適用機種 全機種

ProxyDNSは、パソコン側で本装置のIPアドレスをDNSサーバのIPアドレスとして登録するだけで、ドメイン ごとに使用するDNSサーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社のDNSサーバを使用する場合 使用するドメイン : honsya.co.jp DNSサーバのIPアドレス : 192.168.2.2
- インターネット上のDNSサーバを使用する場合 使用するドメイン
 honsya.co.jp以外 DNSサーバのIPアドレス
 100.100.100

パソコン側の設定を確認する

1. パソコン側が DHCP クライアントかどうか確認します。

DHCPクライアントでない場合は設定します。

こんな事に気をつけて

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

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

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS 情報を設定する

- 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。
 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- **2. 「順引き情報」をクリックします**。 「順引き情報」が表示されます。
- 3. 以下の項目を指定します。
 - ドメイン名 →* .honsya.co.jp
 - 動作 →設定したDNSサーバへ問い合わせる
 DNSサーバアドレス → 192.168.2.2



4. [追加] ボタンをクリックします。

5. 手順3.~4.を参考に、以下の項目を指定します。

ドメイン名

DNSサーバアドレス

動作 →設定したDNS サーバへ問い合わせる

→ *****

→ 100.100.100.100

6. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.24.2 DNS サーバの自動切り替え機能(逆引き)を使う

適用機種 全機種

ProxyDNSは、先に説明した順引きとは逆に、IPアドレスごとに使用するDNSサーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

•	会社のDNSサーバを使用する場合	
	逆引き対象のネットワークアドレス	: 192.168.0.0
	DNSサーバのIPアドレス	: 192.168.2.2
•	インターネット上のDNSサーバを使用する場合	
	逆引き対象のネットワークアドレス	: 192,168,0,0以

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

パソコン側の設定を確認する

1. パソコン側がDHCPクライアントかどうか確認します。

DHCPクライアントでない場合は設定します。

こんな事に気をつけて

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

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

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS情報を設定する

- **1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- 2. 「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

3. 以下の項目を指定します。

• ネットワークアドレス

→指定する →192.168.0.0/24

動作
 DNS サーバアドレス

→設定したDNSサーバへ問い合わせる →192.168.2.2



4. [追加] ボタンをクリックします。

5. 手順3.~4.を参考に、以下の項目を指定します。

ネットワークアドレス →すべて
 動作 →設定したDNSサーバへ問い合わせる DNSサーバアドレス → 100.100.100

6. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.24.3 DNS サーバアドレスの自動取得機能を使う

適用機種 全機種

この機能を利用すると、ProxyDNSがDNSサーバのアドレスを、回線接続時に接続先から自動的に取得します。 そのため、DNSサーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、接続先がDNSサーバアドレスの配布機能(RFC1877)に対応している場合にだけ利用できます。

● 設定条件

- ドメイン名
 :*
- 動作 : 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる

こんな事に気をつけて

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

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

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

- **1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- 「順引き情報」をクリックします。
 「順引き情報」が表示されます。

• ドメイン名

```
→*
```

動作 →接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 → internet(DNSサーバを使用するネットワーク名)

<順引き情報入力フィールド>							
ドメイン 名	*						
タイプ	すべて ▼【番号指定 【1000】"その他"を選択時のみ有効です。)						
送信元 IPアドレ ス	×IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィッ ウス長形式で入力してください。						
動作	 ○ 廃棄する ○ 接続先のDNSサーバへ問い合わせる ネットワーク名 rmt0 ▼ 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 internet ▼ 解決したホストへのホスト経路自動作成 ●しばい ●する ○ DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 使用できるインタフェースが存在しません ▼ ● 設定したDNSサーバへ問い合わせる DNSサーバアドレス 						

- 4. [追加] ボタンをクリックします。
- 5. **画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

パソコン側の設定を行う

ここでは、Windows[®] 2000の場合を例に説明します。

- [コントロールパネル]ウィンドウで [ネットワークとダイヤルアップ接続] アイコンをダブルク リックします。
- 2. [ローカルエリア接続] アイコンを右クリックし、プロパティを選択します。 [ローカルエリア接続のプロパティ] ダイアログボックスが表示されます。
- 3. 一覧から「インターネットプロトコル (TCP/IP)」をクリックして選択します。
- 4. [プロパティ] ボタンをクリックします。
- 5. 「次のDNSサーバーのアドレスを使う」を選択します。
- 6. 「優先 DNS サーバー」に、本装置の IP アドレスを入力します。
- 7. [OK] ボタンをクリックします。
- 8. [はい] ボタンをクリックし、パソコンを再起動します。 再起動後に、設定した内容が有効になります。

· ☆ ヒント —

◆本装置の「DHCPサーバ機能」を使わない場合の設定は?

パソコン側の「DNS 設定」で本装置のIPアドレスを指定すると、ProxyDNS機能だけ使用できます。また、 本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとし て本装置のIPアドレスを指定するとProxyDNS機能を使用できます。

◆ DNS 解決したホストへのホスト経路を自動で作成する設定は?

「ProxyDNS 情報 URL フィルタ情報」-「順引き情報」の動作に"接続先のDNS サーバへ指定ネットワーク を経由して問い合わせる"を指定した場合は、「解決したホストへのホスト経路自動作成」に"する"を指定 することにより、DNS 解決したホストへのホスト経路を自動で作成することができます。

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは?

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わ せるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視し て指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.24.4 DNS サーバアドレスを DHCP サーバから取得して使う

幾種

この機能を利用すると、ProxyDNSがDNSサーバのアドレスを、DHCPサーバから自動的に取得します。そのた め、DNSサーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、DHCP サーバが DNS サーバのアドレスを広報している場合にだけ利用できます。

: *

● 設定条件

- ドメイン名
- 動作

: lan0の DNS サーバへ問い合わせる

こんな事に気をつけて

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

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

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

- 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。 1. 「ProxyDNS 情報/URLフィルタ情報」ページが表示されます。
- 2. 「順引き情報」をクリックします。 「順引き情報」が表示されます。
- 以下の項目を指定します。 3.
 - ドメイン名

動作

→ *

→ DHCP クライアントが取得した DNS サーバへ問い合わせる インタフェース名

→ LAN0 (DNS サーバのアドレスを取得しているインタフェース)

	<順引き情報入力フィールド>
ドメイン 名	×
タイプ	すべて ▼(番号指定 "その他"を選択時のみ有効で す。)
送信元 IPアドレ ス	※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	 ○ 廃棄する ○ 接続先のDNSサーバへ問い合わせる ネットワーク名 rmt0 ▼ 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 rmt0 ▼ 解決したホストへのホスト経路自動作成 ●しばい ●する ● DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 LAN0 ▼ ● 設定したDNSサーバへ問い合わせる DNSサーバアドレス

- 4. [追加] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

パソコン側の設定を行う

ここでは、Windows[®] 2000の場合を例に説明します。

- [コントロールパネル]ウィンドウで [ネットワークとダイヤルアップ接続] アイコンをダブルク リックします。
- 2. [ローカルエリア接続] アイコンを右クリックし、プロパティを選択します。 [ローカルエリア接続のプロパティ] ダイアログボックスが表示されます。
- 3. 一覧から「インターネットプロトコル (TCP/IP)」をクリックして選択します。
- 4. [プロパティ] ボタンをクリックします。
- 5. 「次のDNSサーバーのアドレスを使う」を選択します。
- 6. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
- 7. [OK] ボタンをクリックします。
- 8. [はい] ボタンをクリックし、パソコンを再起動します。 再起動後に、設定した内容が有効になります。

心 ヒント —

◆ 本装置の「DHCP サーバ機能」を使わない場合の設定は?

パソコン側の「DNS 設定」で本装置の IP アドレスを指定すると、ProxyDNS 機能だけ使用できます。また、 本装置以外の DHCP サーバを使用している場合でも、DHCP サーバで広報する DNS サーバの IP アドレスとし て本装置の IP アドレスを指定すると ProxyDNS 機能を使用できます。

◆ DNS 解決したホストへのホスト経路を自動で作成する設定は?

「ProxyDNS 情報 URL フィルタ情報」 - 「順引き情報」の動作に "接続先のDNS サーバへ指定ネットワーク を経由して問い合わせる"を指定した場合は、「解決したホストへのホスト経路自動作成」に"する"を指定 することにより、DNS 解決したホストへのホスト経路を自動で作成することができます。

◆「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは?

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わ せるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視し て指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。

2.24.5 DNS 問い合わせタイプフィルタ機能を使う

適用機種 全機種

端末が送信する DNS パケットのうち、特定の問い合わせタイプ (QTYPE) のパケットを破棄することができます。

たとえば、Windows[®] 2000が送信する予期しないDNSパケットによって、自動発信する問題を回避するために、かんたん設定のかんたんフィルタを「使用する」に設定します。このとき、問い合わせタイプが SOA(6)とSRV(33)のパケットを破棄する場合の設定方法を説明します。

こんな事に気をつけて

ProxyDNS機能を使用する場合、問い合わせタイプがA(1)のDNS問い合わせパケットを破棄するように指定にする と、正常な通信が行えなくなります。

● 設定条件

- ドメイン名 : *
- 問い合わせタイプ : SOA (6)
- 動作
 ご破棄する

こんな事に気をつけて

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

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

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

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

「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

- ・ドメイン名 →*
- タイプ → SOA
- 動作 →廃棄する

	<順引き情報入力フィールド>
ドメイン 名	*
タイプ	SOA ▼(番号指定 "その他"を選択時のみ有効で す。)
送信元 IPアドレ ス	XIPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	 ● 廃棄する ● 接続先のDNSサーバへ問い合わせる ネットワーク名 rmt0 ● 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 rmt0 ● 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 ○ わせる アットワーク名 rmt0 ● 同日の日の日の日の日の日の日の日の日の日の日の日の日の日の日の日の日の日の日の

- 4. [追加] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「2.24.3 DNS サーバアドレスの自動取得機能を使う」(P.768)の「パソコン側の設定を行う」(P.769)を参照してください。

2.24.6 DNS サーバ機能を使う

適用機種 全機種

本装置のホストデータベースにホスト名とIPアドレスを登録します。登録したホストに対してDNS要求があった場合は、ProxyDNSがDNSサーバの代わりに応答します。LAN内の情報をホストデータベースにあらかじめ登録しておくと、LAN内のホストのDNS要求によって回線が接続されるといったトラブルを防止できます。

● 設定条件

- ホスト名
 host.com
- IPv4アドレス : 192.168.1.2
- IPv6アドレス : 2001:db8::2

こんな事に気をつけて

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

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

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1. 設定メニューのルータ設定で「ホストデータベース情報」をクリックします。 「ホストデータベース情報」ページが表示されます。

2. 未設定の欄の [修正] ボタンをクリックします。

3. 以下の項目を指定します。

- ホスト名 → host.com (パソコンの名前)
- IPv4アドレス → 192.168.1.2 (パソコンのIPアドレス)
- リモート電源制御 →対象外

麻豆 ホストデータベース情報は「リモートパワーオン機能」、「DHCPスタティック機能」、「DNS サーバ機能」で使われて おり、それぞれ必要な項目だけを設定します。

	ホスト名	host.com
	IPv4アドレス	192.168.1.2
	IPv6アドレス	
1	MACアドレス	
	リモート電源制御	○対象 ⊙対象外

- 4. [保存] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「2.24.3 DNS サーバアドレスの自動取得機能を使う」(P.768)の「パソコン側の設定を行う」(P.769)を参照してください。

2.25 特定のURLへのアクセスを禁止する (URLフィルタ機能)

適用機種 全機種

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、 ProxyDNS 情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



● 参照 Si-Rシリーズ 機能説明書「2.22 DNSサーバ機能」(P.96)

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

● 設定条件

アクセスを禁止するドメイン名 :www.danger.com

こんな事に気をつけて

- URL フィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。
- ・ 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

ぶとント ――

◆「*」は使えるの?

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「*.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合の設定例を示します。

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

URLフィルタの情報を設定する

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

「ProxyDNS 情報/URLフィルタ情報」ページが表示されます。

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

- 3. 以下の項目を指定します
 - ・ドメイン名 → www.danger.com
 - 動作 →廃棄する



- 4. [追加] ボタンをクリックします。
- 5. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.26 SNMPエージェント機能を使う

適用機種 全機種

本装置は、SNMP(Simple Network Management Protocol)エージェント機能をサポートしています。 ここでは、Si-R370がSNMPホストに対して MIB 情報を通知する場合の設定方法を説明します。



 ・参照 Si-R シリーズ 機能説明書
 「2.23 SNMP 機能」
 (P.98)

Ŵ゙**と**ント゠

♦ SNMPとは?

SNMP (Simple Network Management Protocol)は、ネットワーク管理用のプロトコルです。SNMPホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMPエージェントは、SNMPホストの要求に対してMIB (Management Information Base)という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMPエージェントからSNMPホストに対して 非同期通知を行うことができます。

● 参照 Si-Rシリーズ 仕様一覧「3.1 標準 MIB 定義」(P.50)、「3.2 富士通拡張 MIB」(P.79)、「3.3 Trap 一覧」(P83)

こんな事に気をつけて

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

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

● 設定条件

• SNMPエージェント機能を使用する

• í	き理者 しんしん しんしん しんしん しんしん しんしん しんしん しんしん しん	:	suzuki
-----	---	---	--------

- 機器名称 : Si-R370
- 機器設置場所 :1F(1階)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMPホストアドレス : 192.168.1.100
- コミュニティ名 : public00 (SNMPv1/SNMPv2c時)
- ユーザ名
 : user00 (SNMPv3時)

上記の設定条件に従って設定を行う場合の設定例を示します。

SNMP 情報を設定する

1. 設定メニューの詳細設定で「SNMP情報」をクリックします。

「SNMP情報」ページが表示されます。

2. 以下の項目を指定します。

- SNMPエージェント機能 →使用する
- 機器管理者 → suzuki
 機器名称 →指定する
- 機器名称 → Si-R370
- 機器設置場所 →1F
- エージェントアドレス → 192.168.1.1

■基本情報	3
SNMPエージェント機 能	 ○使用しない ●使用する ○使用する(IBバージョン互換MIBモード)
機器管理者	suzuki
機器名称	装置名称を使用する (装置名称情報が設定されていないため選択できません) ③ 指定する 機器名称 Si-R370
機器設置場所	1F
エージェントアドレス	192.168.1.1

3. [保存] ボタンをクリックします。

SNMPv1 または SNMPv2c でアクセスする場合

SNMPv1またはSNMPv2cでアクセスする場合は、以下の情報を設定します。

- **4. 設定メニューの詳細設定で「SNMP情報」をクリックします**。 「SNMP情報」ページが表示されます。
- **5. 「SNMPv1/v2c情報」をクリックします**。 「SNMPv1/v2c情報」が表示されます。

•	SNMPホスト1	→指定する
	コミュニティ名	→ public00
	IPアドレス	→ 192.168.1.100

SNMPホスト2以降 →指定しない

SNMPv1/v2c情報		
	 ○ publicとする(任意のホストを対象とする) ● 指定する 	
	コミュニティ名 public00	
SNMP/0.2F1	IPアドレス 192.168.1.100	
	トラップ ●送信しない ○ V1 ○ V2	
	書き込み要求 ⊙許可しない○許可する	
	 ● 指定しない 	

7. [保存] ボタンをクリックします。

SNMPv3でアクセスする場合

SNMPv3でアクセスする場合は、以下の情報を設定します。

- **8. 設定メニューの詳細設定で「SNMP情報」をクリックします**。 「SNMP情報」ページが表示されます。
- **9. 「SNMPv3 情報」をクリックします**。 「SNMPv3 情報」が表示されます。
- 10. SNMPv3情報リストの [修正] ボタンをクリックします。

11. 以下の項目を指定します。

- ユーザ名 → user00
- SNMPホスト → 192.168.1.100

ユーザ名	user00	
ホフトアドレ	SNMPホスト	トラップ通知ホスト
ス ス	192.168.1.100	

- 12. [保存] ボタンをクリックします。
- 13. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

- エージェントアドレスには、本装置に設定されたどれかのインタフェースのIPアドレスを設定します。誤ったIPアドレスを設定した場合は、SNMPホストとの通信ができなくなります。
- ATM 網によっては、物理リンクが確立してから通信ができるようになるまでに時間がかかるものがあります。装置起動時に、ATM 網の先の SNMP ホストに送信した trap が、相手に正常に届かない場合があります。

2.27 ECMP機能を使う

適用機種 全機種

ここでは、ECMP機能を利用した負荷分散通信を行う場合の設定方法を説明します。

ADSLでは、受信速度は高速ですが、送信速度はそれほど高速ではありません。この例では、ADSLを2本利用して負荷を分散することで、送信速度の向上をはかります。さらに、片方のトンネルに障害が発生した場合に、通信可能なトンネルを利用して通信のバックアップを実現します。



● 参照 Si-Rシリーズ 機能説明書「2.24 ECMP機能」(P.104)

● 設定条件

- 拠点では、センタへの通信は、トンネル1とトンネル2を利用して負荷分散して送信します。どちらかのトンネルで通信障害が発生した場合は、通信可能なトンネルだけを利用して送信します。
- センタでは、拠点への通信は、トンネル1だけを利用して送信します。トンネル1で通信障害が発生した場合は、トンネル2を利用して送信します。
- トンネル1の通信障害は、両端の本装置が接続先監視で検出します。
 この監視は、ISP Aの通信障害およびセンタ側本装置(左)の故障を検出します。
- トンネル2の通信障害は、両端の本装置が接続先監視で検出します。
 この監視は、ISP Bの通信障害およびセンタ側本装置(右)の故障を検出します。

上記の設定条件に従って設定を行う場合の設定例を示します。

センタ側本装置(左)を設定する

IPsecに関するACLを設定する

- 設定メニューのルータ設定で「ACL情報」をクリックします。
 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 定義名

→IKE

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	IKE

3. [追加] ボタンをクリックします。 「ACL定義情報(IKE)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

5. 以下の項目を指定します。

プロトコル	→udp
送信元情報 IPアドレス アドレスマスク	→202.168.1.66 →32 (255.255.255.255)
あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
	プロトコル 送信元情報 IPアドレス アドレスマスク あて先情報 IPアドレス アドレスマスク

• QoS →指定なし

■IP定義情報				
ブロトコル		udp		
送信元情	IPアドレス	202.168.1.66		
報	アドレスマ スク	32 (255.255.255.255) 💌		
あて先情	IPアトレス			
報	アドレスマ スク	0 (0.0.0)		
QoS		^{指定なし} ▼ TOS、または、DSCPを選択時に値を入力してくだ さい		

- 6. [保存] ボタンをクリックします。
- **7.** 「UDP 定義情報」をクリックします。 「UDP 定義情報」ページが表示されます。

- 送信元ポート番号 →500
- あて先ポート番号 → 500

■UDP定義情報	3
送信元ポート番号	500
あて先ボート番号	500

- 9. [保存] ボタンをクリックします。
- 10. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

•	定義名	→ESP
ΓA	CL定義情報(ESP)」-「IP定義	青報」
•	プロトコル	→その他(50)
•	送信元情報 IPアドレス アドレスマスク	→202.168.1.66 →32 (255.255.255.255)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0)
•	QoS	→指定なし

LAN1側を設定する

- **11. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 12. 以下の項目を指定します。
 - インタフェース →物理LAN

<LAN情報追加フィールド> インタフェース 物理LAN ▼

- **13. [追加] ボタンをクリックします**。 「LAN1 情報(物理 LAN)」ページが表示されます。
- **14.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →202.168.1.66
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

I Pアドレ	■IPアドレス情報			
IPv4	●使用する●使用しない			
IPアドレス	 DHCPで自動的に取得する 指定する IPアドレス 202.168.1.66 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス キットワークアドレス 	× + オ−ル1 ×		

- 16. [保存] ボタンをクリックします。
- 17. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

18. 以下の項目を指定します。

•	ネットワーク	→デフォルトルート
	中継ルータアドレス	→指定する
	IPアドレス	→202.168.1.65
•	メトリック値	→ 1
•	優先度	→ 0

<スタティック経路情報入力フィールド>			
◎ デフォルトルート			
ネ		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 202.168.1.65
ット	0)ネットワーク指定	
5		あて先IPアドレス	
ー ク		あて先アドレスマス ク	0 (0.0.0)
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス
メトリック値 優先度	1	v	

19. [追加] ボタンをクリックします。

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

「IPフィルタリング情報」が表示されます。

- 21. 以下の項目を指定します。
 - 動作 →透過
 - 方向 →リバース
 - ACL定義番号 →0

 [「]ACL定義番号」を指定する際は、[参照]ボタンをクリックして、表示された画面から設定する定義番号欄の[選択]
 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>		
動作	⊙透過○遮断	
方向	リバース 💌	
ACL定義番号	0 参照	

- 22. [追加] ボタンをクリックします。
- 23. 手順20.~22.を参考に、以下の項目を指定します。
 - 動作 →透過
 - 方向 →リバース
 - ACL定義番号 →1
- 24. 条件にあてはまらない場合の [修正] ボタンをクリックします。

「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。

- 25. 以下の項目を指定します。
 - 動作 →遮断



26. [保存] ボタンをクリックします。

トンネルを設定する

- **27. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **28. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 29. 以下の項目を指定します。
 - ネットワーク名 → RMTbyA

<ネットワーク情報追加フィールド>		
ネットワーク名	RMTbyA	

- **30. [追加] ボタンをクリックします**。 「ネットワーク情報(RMTbyA)」が表示されます。
- 31. 「共通情報」をクリックします。 共通情報の設定項目と「基本情報」が表示されます。
- 32. 以下の項目を指定します。
 - MTUサイズ →1400

MTUサイズ

- 33. [保存] ボタンをクリックします。
- 34. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

1400 バイト

- 35. 以下の項目を指定します。
 - MSS書き換え →使用する 書き換えサイズ → 1360

MSS書き換え	 ○ 使用しない ③ 使用する
	書き換えサイズ 1360 バイト

- 36. [保存] ボタンをクリックします。
- 37. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

- 38. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 192.168.1.0
 あて先アドレスマスク → 24 (255.255.255.0)
 メトリック値 →1
 - 優先度

	<スタティック経路情報入力フィールド>
ネットワーク	 デフォルトルート ネットワーク指定 あて先IPアドレス 192.168.1.0 あて先アドレスマスク 24 (255.255.0)
メトリック値	1 💌
優先度	0

 $\rightarrow 0$

- 39. [追加] ボタンをクリックします。
- **40. 「接続先情報」をクリックします**。

「接続先情報」が表示されます。

● 接続先名

- →IPsecbyA
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>		
接続先名	IPsecbyA	
接続先種 別	 ATM接続 VCI 専用線接続 通常接続 (使用インタフェース WAN1 ♥) 論理リンクにバンドルする (使用インタフェー ス バンドル先 運択できる定義がありません ♥ ISDN接続 通常接続 (使用インタフェース すべて ♥) バンドル先 運択できる定義がありません ♥ ISDN接続 通常接続 (使用インタフェース すべて ♥) デンドル先 運転番号 ダイヤル1 電話番号 ダイヤル1 すべて ♥ パンドル先 運択できる定義がありません ♥ フレームリレー接続 DLCI PPPoE接続 IPsec/IKE接続 別インタフェースから送出 MPLSトンネル接続 バケット破棄 	

機種により、接続先種別の表示が上記の画面とは異なります。

42. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

43. 以下の項目を指定します。

- 鍵交換モード
 - 自側エンドポイント 相手装置識別情報 ID*タイプ*

→ Aggressive Mode(Responder)使用 → 202.168.1.66 → RMTbyA

→FQDN

	O Aggressive Mode(R	'esponder)使用
	自側エンドボイン ト	202.168.1.66
<u>鍵交換</u> モ ート	相手側エンドポイ ント	
	相手装置識別情 報	RMTbyA
	IDタイプ	⊙ FQDN ○ User-FQDN

44. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

46. 以下の項目を指定します。

- 対象パケット 自側IPアドレス/マスク → IPv4 すべて 相手側IPアドレス/マスク → IPv4 すべて
- SAの設定 暗号アルゴリズム
 認証アルゴリズム
 PFS時のDHグループ
 SA有効時間
- → des-cbc → hmac-md5 → modp1536(グループ5) → 8 時間
- SA更新
 Responder時 →更新する
 時間 → 30



- 47. [保存] ボタンをクリックします。
- **48.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

 IKE 認証鍵 鍵識別 鍵

→文字列
→12345678-A

■IKE情報		
	<mark>键識別</mark>	◎16進数 ⑧文字列
INE認知	键	•••••

- 50. [保存] ボタンをクリックします。
- **51.** IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 52. 以下の項目を指定します。

•	接続先監視	→使用する
	送信元IPアドレス	→ 172.16.1.252
	あて先IPアドレス	→ 192.168.1.1
	正常時送信間隔	→5秒
	再送間隔	→1秒
	タイムアウト時間	→5秒
	異常時送信間隔	→1分

	○ 使用しない● 使用する
	送信元IPアドレス 172.16.1.252
	あて先IPアドレス 192.168.1.1
	正常時送信間隔 5 秒 🗸
接続	再送間隔 1 秒 🗸
充監 視	タイムアウト時間 5 秒 🗸
	異常時送信間隔 1 分 ▼
	送信 TTL/HopLimit 255
	連続応答受信回数 1
	異常時送信開始待ち時間 0 秒 🗸
	監視方式 ◎常時監視○無通信時監視

53. [保存] ボタンをクリックします。

LAN0 側を設定する

54. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

- **55.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **56. 「共通情報」をクリックします。** 共通情報に関する設定項目と「基本情報」が表示されます。

VRRP機能

→使用する

VRRP機能	 ○ 使用しない ● 使用する
	バスワード

Si-R180、180Bでは、LANバックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

58. [保存] ボタンをクリックします。

- **59. 共通情報の設定項目の「VRRP グループ情報」をクリックします**。 「VRRP グループ情報」が表示されます。
- **60.** 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。 VRRP グループ情報の設定項目と「基本情報」が表示されます。

→10

61. 以下の項目を指定します。

- グループID
- ・ プライオリティ →優先度指定 優先度 → 254
 仮想 IP アドレス → 172.16.1.254

■基本情報	3
グループID	10
ブライオリティ	⊙ 優先度指定
	優先度 254
	仮想IPアドレス
	○ 優先度固定(最優先)
	優先度 255
	仮想IPアドレス インタフェースアドレスを使用

- 62. [保存] ボタンをクリックします。
- **63.** VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。
- 64. 以下の項目を指定します。
 - 減算プライオリティ → 254
 - トリガ種別
 →インタフェースダウントリガ (ifdown)

 インタフェース → RMTbyA

	<vrrpトリガ情報入力フィールド></vrrpトリガ情報入力フィールド>
減算ブライ オリティ	254
	● インタフェースダウントリガ(ifdown)
トリガ種別	インタフェース RMTbyA 💌

65. [追加] ボタンをクリックします。

66. 画面上部の「LAN0 情報」をクリックします。

「LAN0情報(物理LAN)」ページが表示されます。

67. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 68. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →172.16.1.252
 ネットマスク →24 (255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		3
IPv4	⊙使用する○使用しない	
IPアドレス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス I72.16.1.252 	
	ネットマスク 24 (255.255.255.0) ブロードギャストアドレ ス	

- 69. [保存] ボタンをクリックします。
- **70. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

センタ側本装置(右)を設定する

IPsecに関するACLを設定する

- 設定メニューのルータ設定で「ACL情報」をクリックします。
 「ACL情報」ページが表示されます。
- 2. 以下の項目を指定します。
- 【追加】ボタンをクリックします。
 「ACL定義情報(IKE)」ページが表示されます。
- **4. 「IP 定義情報」をクリックします**。 「IP 定義情報」ページが表示されます。
| • | プロトコル | →udp |
|---|---------|-----------------------|
| • | 送信元情報 | |
| | IPアドレス | →202.168.1.67 |
| | アドレスマスク | →32 (255.255.255.255) |
| • | あて先情報 | |
| | IPアドレス | →指定しない |

アドレスマスク	→0 (0.0.0)

ブロトコル		udp (番号指定:
送信元情	IPアドレス	202.168.1.67
報	アドレスマ スク	32 (255.255.255.255) 💌
あて先情	IPアドレス	
報	アドレスマ スク	0 (0.0.0)
QoS		指定なし ♥ TOS、または、DSCPを選択時に値を入力してくだ さい

6. [保存] ボタンをクリックします。

7. 「UDP 定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

8. 以下の項目を指定します。

- 送信元ポート番号 →500
- あて先ポート番号 → 500

UDP定義情報	3
送信元ボート番号	500
あて先ポート番号	500

- 9. [保存] ボタンをクリックします。
- 10. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名	→ESP
「ACL定義情報(ESP)」-「IPを	定義情報」
• プロトコル	→その他(50)
 送信元情報 IPアドレス アドレスマスク 	→202.168.1.67 →32 (255.255.255.255)
 あて先情報 IPアドレス アドレスマスク 	→指定しない →0 (0.0.0.0)

QoS →指定なし

LAN1側を設定する

11. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

12. 以下の項目を指定します。

•	• インタフェース	→物理LAN
ĺ	<lan情幸< th=""><th>段追加フィールド></th></lan情幸<>	段追加フィールド>
I	インタフェース	物理LAN ❤

13. [追加]ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

14. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 15. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する
 IPアドレス →202.168.1.67
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	⊙使用する○使用しない	
IPアドレス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 202.168.1.67 ネットマスク 24 (255.255.255.0) ▼ ブロードキャストアドレ ネットワークアドレス+オール1 ▼ 	

- 16. [保存] ボタンをクリックします。
- **17.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

- ネットワーク →デフォルトルート 中継ルータアドレス →指定する
 IPアドレス → 202.168.1.65
 メトリック値 →1
- 優先度

	<スタティック経路情報入力フィールド>		
	۲	デフォルトルート	
ネ		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス 202.168.1.65
ット	0	ネットワーク指定	
トワ		あて先IPアドレス	
ー ク		あて先アドレスマス ク	0 (0.0.0)
		中継ルータアドレス	 DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 指定する IPアドレス
メトリック値	1	v	
優先度	0		

→0

19. [追加] ボタンをクリックします。

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

「IPフィルタリング情報」が表示されます。

21. 以下の項目を指定します。

- 動作 →透過
- 方向 →リバース
- ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>	
動作	⊙透過 ○遮断
方向	リバース 🗸
ACL定義番号	0 参照

22. [追加] ボタンをクリックします。

- 23. 手順20.~22.を参考に、以下の項目を指定します。
 - 動作 →透過
 - 方向 →リバース
 - ACL定義番号 →1
- 24. 条件にあてはまらない場合の [修正] ボタンをクリックします。

「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。

- 25. 以下の項目を指定します。
 - 動作

→遮断

CIP7	<ipフィルタリング情報入力フィールド(条件にあて(はまらない場合)></ipフィルタリング情報入力フィールド(条件にあて(はまらない場合)>	
動作	 ○ 透過 ③ 遮断 ○ SPI 	
	情報保持タイマ 5 分 🗸	

26. [保存] ボタンをクリックします。

トンネルを設定する

- **27. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **28. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- 29. 以下の項目を指定します。
 - ネットワーク名 → RMTbyB



30. [追加]ボタンをクリックします。

「ネットワーク情報(RMTbyB)」が表示されます。

- **31. 「共通情報」をクリックします**。 共通情報の設定項目と「基本情報」が表示されます。
- 32. 以下の項目を指定します。
 - MTUサイズ → 1400

```
MTUサイズ 1400 バイト
```

- 33. [保存] ボタンをクリックします。
- **34. 「IP 関連」をクリックします**。

IP関連の設定項目と「IP基本情報」が表示されます。

 MSS 書き	奥え	→使用する	
書き換えた	トイズ	→1360	
MSS書き換え	 ○ 使用しない ③ 使用する 書き換えサイズ 1360 	バイト	

[保存] ボタンをクリックします。 36.

37. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

38. 以下の項目を指定します。

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



- [追加] ボタンをクリックします。 39.
- 「接続先情報」をクリックします。 40. 「接続先情報」が表示されます。

● 接続先名

- →IPsecbyB
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>		
接続先名	IPsecbyB	
接続先種別	 ATM接続 VCI 専用線接続 通常接続 (使用インタフェース WAN1 ♥ 論理リンクにバンドルする (使用インタフェー ス バンドル先 運択できる定義がありません ♥ ISDN接続 通常接続 (使用インタフェース すべて ♥	

機種により、接続先種別の表示が上記の画面とは異なります。

42. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

43. 以下の項目を指定します。

- 鍵交換モード
 - 自側エンドポイント 相手装置識別情報 ID*タイプ*

→ 202.168.1.67 → RMTbyB → FQDN

→ Aggressive Mode (Responder) 使用

-		
	⊙ Aggressive Mode(Responder)使用	
	自側エンドボイン ト	202.168.1.67
鍵交換モ ート	相手側エンドポイ ント	
	相手装置識別情 報	RMTbyB
	IDタイプ	⊙ FQDN O User-FQDN

44. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

46. 以下の項目を指定します。

- 対象パケット 自側IPアドレス/マスク → IPv4 すべて 相手側IPアドレス/マスク → IPv4 すべて
- SAの設定 暗号アルゴリズム 認証アルゴリズム
 PFS時のDHグループ
 SA有効時間
- → des-cbc → hmac-md5 → modp1536(グループ5) → 8 時間
- SA更新
 Responder時 →更新する
 時間 → 30



- 47. [保存] ボタンをクリックします。
- **48.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

 IKE 認証鍵 鍵識別 鍵

→文字列
→12345678-B

IKE認証鍵	键	•••••
	键識別	○16進数 ⊙文字列
■IKE情報		3

- 50. [保存] ボタンをクリックします。
- **51.** IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 52. 以下の項目を指定します。

•	接続先監視	→使用する
	送信元IPアドレス	→ 172.16.1.253
	あて先IPアドレス	→ 192.168.1.1
	正常時送信間隔	→5秒
	再送間隔	→1秒
	タイムアウト時間	→5秒
	異常時送信間隔	→1分

	○ 使用しない
	⊙ 使用する
	送信元IPアドレス 172.16.1.253
	あて先IPアドレス 192.168.1.1
	正常時送信間隔 5 秒 🗸
接続	再送間隔 1 秒 🗸
允監 視	タイムアウト時間 5 秒 🗸
	異常時送信間隔
	送信 TTL/HopLimit 255
	連続応答受信回数 1
	異常時送信開始待ち時間 0 秒 🗸
	監視方式 ○常時監視○無通信時監視

53. [保存] ボタンをクリックします。

LAN0 側を設定する

54. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

- **55.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **56. 「共通情報」をクリックします。** 共通情報に関する設定項目と「基本情報」が表示されます。

VRRP機能

→使用する

	○ 使用しない
VRRP機能	⊙ 使用する
	バスワード

Si-R180、180Bでは、LAN バックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

58. [保存] ボタンをクリックします。

- **59. 共通情報の設定項目の「VRRP グループ情報」をクリックします**。 「VRRP グループ情報」が表示されます。
- **60.** 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。 VRRP グループ情報の設定項目と「基本情報」が表示されます。

→10

61. 以下の項目を指定します。

- グループID
- プライオリティ →優先度指定 優先度 → 100
 仮想 IP アドレス → 172.16.1.254

■基本情報	3
グループID	10
 ● 優先度指定 	
	優先度 100
ブライオリティ	仮想IPアドレス
	○ 優先度固定(最優先)
	優先度 255
	仮想IPアドレス インタフェースアドレスを使用

- 62. [保存] ボタンをクリックします。
- **63.** VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。
- 64. 以下の項目を指定します。
 - 減算プライオリティ → 254
 - トリガ種別 →インタフェースダウントリガ (ifdown)
 インタフェース → RMTbyB

<vrrpトリガ情報入力フィールド></vrrpトリガ情報入力フィールド>		
減算ブライ オリティ	254	
	⊙ インタフェースダウントリガ(ifdown)	
トリガ種別	インタフェース РМТьуВ 💌	

65. [追加] ボタンをクリックします。

66. 画面上部の「LANO情報」をクリックします。

「LAN0 情報(物理 LAN)」ページが表示されます。

67. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 68. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →172.16.1.253
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレ	·ス情報	3
IPv4	⊙使用する○使用しない	
IP アド レス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 172.16.1.253 ネットマスク 24 (255.255.0) ▼ ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 	

- 69. [保存] ボタンをクリックします。
- **70. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

拠点側本装置を設定する

PPPoE で利用する LAN を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - インタフェース →物理LAN
 <LAN情報追加フィールド>
 インタフェース 物理LAN ▼
- 3. [追加] ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

4. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

- 5. 以下の項目を指定します。
 - インタフェース → VLAN

	<lan情報追加フィールド></lan情報追加フィールド>	
インタフェース	VLAN 💌	

- **6. [追加] ボタンをクリックします**。 「LAN2 情報(VLAN)」ページが表示されます。
- 7. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 8. 以下の項目を指定します。
 - 出力先 → LAN1
 - VLAN ID $\rightarrow 10$

■基本情報	3
出力先	LAN1 🗸
VLAN ID	10

- 9. [保存] ボタンをクリックします。
- 10. 手順4.~9.を参考に、以下の項目を指定します。

「LAN3情報(VLAN)」—「共通情報」

- 出力先 → LAN1
- VLAN ID →20

IPsecに関するACLを設定する

- **11. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 12. 以下の項目を指定します。
 - 定義名 → IKE-A

<acl情報追加フィールトド></acl情報追加フィールトド>		
定義名	IKE-A	

13. [追加] ボタンをクリックします。

「ACL定義情報(IKE-A)」ページが表示されます。

14. 「IP 定義情報」をクリックします。

「IP定義情報」ページが表示されます。

→udp
→202.168.1.66
→32 (255.255.255.255)
→指定しない

	アドレスマスク	→0 (0.0.0)
•	QoS	→指定なし

■IP定義	■IP定義情報	
ブロトコル		udp (番号指定:
送信元情	IPアドレス	202.168.1.66
報	アドレスマ スク	32 (255.255.255.255) 💌
あて先情	IPアドレス	
報	アドレスマ スク	0 (0.0.0)
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

16. [保存] ボタンをクリックします。

17. 「UDP 定義情報」をクリックします。

「UDP定義情報」ページが表示されます。

18. 以下の項目を指定します。

- 送信元ポート番号 →500
- あて先ポート番号 → 500

UDP定義情報		3
送信元ポート番号	500	
あて先ボート番号	500	

- 19. [保存] ボタンをクリックします。
- 20. 手順 11.~16.を参考に、以下の項目を指定します。

「ACL情報」

٠	定義名	→ESP-A	
ΓA	CL定義情報(ESP-A)」-「IP定義情報」	

•	プロトコル	→その他(50)
•	送信元情報 IPアドレス アドレスマスク	→202.168.1.66 →32 (255.255.255.255)
•	あて先情報 IPアドレス アドレスマスク	→指定しない →0(0.0.0.0)
•	QoS	→指定なし

21. 手順 11.~19.を参考に、以下の項目を指定します。

	「ACL情報」	
	• 定義名	→IKE-B
	「ACL定義情報(IKE-B)」-「IP定	義情報」
	• プロトコル	→udp
	 送信元情報 IPアドレス アドレスマスク 	→202.168.1.67 →32 (255.255.255.255)
	 あて先情報 IPアドレス アドレスマスク OoS 	→指定しない →0(0.0.0) →指定なし
	「ACI 定義情報(IKE-B)」-「UDP	定義情報
	 ・ 送信元ポート番号 	→ 500
	 あて先ポート番号 	→ 500
22.	手順11.~16.を参考に、以下の3	項目を指定します。
	「ACL情報」	
	• 定義名	→ESP-B
	「ACL定義情報(ESP-B)」-「IP定	2義情報」
	• プロトコル	→その他 (50)
	 送信元情報 IPアドレス 	→202.168.1.67
	アドレスマスク	→32 (255.255.255.255)
	 あて先情報 IPアドレス アドレスマスク 	→指定しない →0(0.0.0)
	• QoS	→指定なし

プロバイダAを利用する PPPoE 接続を設定する

- **23. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **24. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 25. 以下の項目を指定します。
 - ネットワーク名 → INTER-A

<ネットワーク情報追加フィールド>	
ネットワーク名 INTER-A	

26. [追加] ボタンをクリックします。

「ネットワーク情報(INTER-A)」が表示されます。

27. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 28. 以下の項目を指定します。
 - MTUサイズ → 1454

MTUサイズ 1454 バイト

- 29. [保存] ボタンをクリックします。
- **30. 「**IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

- 31. 以下の項目を指定します。
 - MSS書き換え →使用する 書き換えサイズ → 1414



- 32. [保存] ボタンをクリックします。
- 33. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

34. 以下の項目を指定します。

ネットワーク →ネットワーク指定
 あて先IPアドレス → 202.168.1.66
 あて先アドレスマスク → 32 (255.255.255)
 メトリック値 →1

→0

● 優先度



- 35. [追加] ボタンをクリックします。
- 36. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →リバース
- ACL定義番号 →0

「ACL定義番号」を指定する際は、「参照」ボタンをクリックして、表示された画面から設定する定義番号欄の「選択」 ボタンをクリックして設定します。

<ipフィルタリング情報入力フィールド></ipフィルタリング情報入力フィールド>	
動作	⊙透過 ○ 遮断
方向	リバース 💌
ACL定義番号	0 参照

38. [追加] ボタンをクリックします。

39. 手順 36.~38.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →リバース
- ACL定義番号 →1

40. 条件にあてはまらない場合の [修正] ボタンをクリックします。

「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。

41. 以下の項目を指定します。

動作

→遮断



- 42. [保存] ボタンをクリックします。
- 43. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

- 44. 以下の項目を指定します。
 - NATの使用 →マルチNAT

■NAT情報	3
NATの使用	○使用しない○NAT ⊙マルチNAT ○静的NATのみ

- 45. [保存] ボタンをクリックします。
- **46.** IP **関連の設定項目の「静的 NAT 情報」をクリックします**。 「静的 NAT 情報」が表示されます。

•	プライベートIP情報	
	IPアドレス	→192.168.1.1
	ポート番号	→isakmp
•	グローバル IP 情報	
	IPアドレス	→指定しない

- ポート番号 →isakmp • プロトコル
 - →udp

<静的NAT情報入力フィールド>		
ブライベート	IPアド レス	192.168.1.1
IP情報	ポート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
グローバル	IPアド レス	
IP竹青幸反	ポート 番号	isakmp ▼(番号指定: ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
プロトコル		udp ✓(番号指定: ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

48. [追加] ボタンをクリックします。

手順46.~48.を参考に、以下の項目を指定します。 49.

- プライベートIP情報 IPアドレス → 192.168.1.1 ポート番号 →すべて • グローバル IP 情報 IPアドレス →指定しない ポート番号 →すべて • プロトコル →esp
- 50. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

• 接続先名

- →ISP-A
- 接続先種別 → PPPoE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

52. [追加] ボタンをクリックします。

PPPoE 接続の設定項目と「基本情報」が表示されます。

- 53. 以下の項目を指定します。
 - ・ 使用インタフェース → LAN2
 使用インタフェース LAN2 ▼
- 54. [保存] ボタンをクリックします。
- **55.** PPPoE 接続の設定項目の「PPP 情報」をクリックします。 「PPP 情報」が表示されます。

 送信認証情報 認証 ID 認証パフロード 		報 ド	\rightarrow UIDtoA \rightarrow PASStoA
ſ	■PPP情報		
	送信認証情報	認証ID 認証バスワード	UIDto A

57. [保存] ボタンをクリックします。

プロバイダBを利用する PPPoE 接続を設定する

58. 手順23.~58.を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」				
 ネットワーク名 	→INTER-B			
「ネットワーク情報」-「IP 関連」				
「スタティック経路情報」				
• ネットワーク	→ネットワーク指定			
あて先IPアドレス	→202.168.1.67			
あて先アドレスマスク	→32 (255.255.255.255)			
• メトリック値	→ 1			
● 優先度	→ 0			
「IP フィルタリング情報」				
• 動作	→透過			
• 方向	→リバース			
• ACL 定義番号	→2			
● 動作	→透過			
• 方向	→リバース			
• ACL 定義番号	→ 3			
「IP フィルタリング情報」-「条件にあてはまらない場合の動作」				
● 動作	→遮断			
「ネットワーク情報」-「接続先情報	报 」			
• 接続先名	→ISP-B			
「基本情報」				
• 使用インタフェース	→LAN3			
「PPP 情報」				
• 送信認証情報				
認証ID	→UIDtoB			
認証パスワード	→ PASStoB			

センタ側本装置(左)とのトンネルを設定する

- **59. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **60. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 61. 以下の項目を指定します。
 - ネットワーク名 → CENTER-A

<ネットワーク情報追加フィールド>		
ネットワーク名	CENTER-A	

62. [追加] ボタンをクリックします。

「ネットワーク情報(CENTER-A)」が表示されます。

63. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

64. 以下の項目を指定します。

• MTUサイズ →1400

MTUサイズ 1400 バイト

- 65. [保存] ボタンをクリックします。
- 66. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

- 67. 以下の項目を指定します。
 - MSS書き換え →使用する 書き換えサイズ → 1360



- 68. [保存] ボタンをクリックします。
- 69. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

• ネットワーク	→ネットワーク指定
あて先IPアドレス	→ 172.16.1.0
あて先アドレスマスク	→24 (255.255.255.0)
• メトリック値	→ 1
● 優先度	→ 1

<スタティック経路情報入力フィールド>		
 デフォルトルート ネットワーク指定 あて先IPアドレス 172.16.10 あて先アドレスマスク 24 (255.255.0) 		
メトリック値	1 💌	
優先度	1	

- 71. [追加] ボタンをクリックします。
- **72. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。

• 接続先名

- →IPsecbyA
- 接続先種別 → IPsec/IKE 接続



機種により、接続先種別の表示が上記の画面とは異なります。

74. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

75. 以下の項目を指定します。

- 鍵交換モード
 - 相手側エンドポイント 自装置識別情報 IDタイプ

→ 202.168.1.66 → RMTbyA → FQDN

→ Aggressive Mode (Initiator) 使用

	⊙ Aggressive Mode(Initiator)使用		
	自側エンドポイン ト		
鍵交換モ ート	相手側エンドボイ ント	202.168.1.66	
	自装置識別情報	RMTbyA	
	IDタイプ	⊙ FQDN O User-FQDN	

76. [保存] ボタンをクリックします。

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

「IPsec情報」が表示されます。

78. 以下の項目を指定します。

•	対象パケット		
	自側 IP アドレス/マスク	→IPv4すべて	
	相手側IPアドレス/マスク	→IPv4すべて	
•	SAの設定		

→ des-cbc → hmac-md5

→8時間

→modp1536 (グループ5)

暗号アルゴリズム
認証アルゴリズム
PFS時のDHグループ
SA有効時間

SA更新	
Initiator時	
時間	→ 90
Responder 時	→更新する
時間	→ 90
	SA 更新 Initiator 時 時間 Responder 時 時間

IPs	IPsec情報(自動鍵)			
対象 パケ ット	自側IPアドレ ス/マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。		
	相手側IPアト レス/マスク	IPv4すべて ▼ ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。		
	暗号アルゴリ ズム	□aes-cbc-256 □aes-cbc-192 □aes-cbc-128 □3des-cbc ♥des-cbc □null		
SA	認証アルゴリ ズム	☑ hmac-md5 □ hmac-sha1 □認証なし		
の設 定	PFS時のDHグ ルーブ	modp1536(ヴループ5) 💌		
	SA有効時間	8 時間 🗸		
	SA有効データ 量	0 GByte 💌		
C A	Initiator 時 一タ 量	90 秒少 0 MByte 🗸		
更新	Responder 時	 ● 更新しない ● 更新する 時間 90 秒 データ量 0 MByte ▼ 		

- 79. [保存] ボタンをクリックします。
- **80.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。 「IKE 情報」が表示されます。

 IKE 認証鍵 鍵識別 鍵

→文字列
→12345678-A

■IKE情報		3
レビジョン	鏈識別	○16進数 ⊙文字列
INE認証 現	鍵	•••••

- 82. [保存] ボタンをクリックします。
- **83.** IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 84. 以下の項目を指定します。

•	接続先監視	→使用する
	送信元IPアドレス	→ 192.168.1.1
	あて先IPアドレス	→ 172.16.1.252
	正常時送信間隔	→5秒
	再送間隔	→1秒
	タイムアウト時間	→5秒
	異常時送信間隔	→1分

	 ○ 使用しない ③ 使用する
	送信元IPアドレス 192.168.1.1
	正常時送信間隔 5 秒 ▼
接続 先監 俎	再送間隔 1 秒 ▼ タイムアウト時間 5 秒 ▼
тла	
	这信TTL/HopLimit 255 連続応答受信回数 1
	異常時送信開始待ち時間 □ 秒 ▼ 転視方式 ○ 常時転視 ○ 無通信時転視

85. [保存] ボタンをクリックします。

センタ側本装置(右)とのトンネルを設定する

86. 手順60.~86.を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」			
• ネットワーク名	→CENTER-B		
「ネットワーク情報」-「接続先情報	L		
● 接続先名	→IPsecbyB		
「接続先情報」-「IPsec/IKE接続」			
「基本情報」			
• 相手側エンドポイント	→202.168.1.67		
• 自装置識別情報	→RMTbyB		
「IKE情報」			
• 鍵	→12345678-B		
「接続制御情報」			
• あて先IPアドレス	→ 172.16.1.253		

ECMP を設定する

- **87. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします**。 「ルーティングプロトコル情報」ページが表示されます。
- **88.** 「ルーティングマネージャ情報」をクリックします ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
- **89.** ルーティングマネージャ情報の設定項目の「ECMP 情報」をクリックします。 「ECMP 情報」が表示されます。
- 90. 以下の項目を指定します。
 - ECMP機能 →ハッシュ方式

■ECMP情報	3
ECMP機能	 ○使用しない ○ラウンドロビン方式 ③ハッシュ方式

- 91. 【保存】ボタンをクリックします。
- **92. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.28 VRRP機能を使う

適用機種 全機種

VRRP機能は2つ以上のルータがグループを形成し、1台のルータ(仮想ルータ)のように動作します。グループ 内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ(実際にルーティングを行う装 置)とバックアップルータ(マスタルータで異常を検出したときにルーティング処理を引き継ぐ装置)を決定し ます。

本装置には、以下のVRRP機能があります。

- ・ 簡易ホットスタンバイ機能
 動的に経路制御(RIPなど)できない端末から、別のネットワークへの通信に使用しているルータがなんらか
 の理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能 VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、2台のルー タを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

● 参照 Si-Rシリーズ 機能説明書「2.25 VRRP機能」(P.107)

こんな事に気をつけて

- 本装置の電源の投入、マスタルータでの動的定義変更、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。プリエンプトモードがonの場合は自動で切り戻りますが、プリエンプトモードがoffの場合は、操作メニューの「VRRP手動切り戻し」で切り戻しを行う必要があります。
- 優先度の値が大きい方が優先的にマスタルータとなります。
- LANに接続される装置はデフォルトルートとして仮想IPアドレスを設定してください。
- ルータに設定されるIPアドレスと仮想IPアドレスを同じにした場合、そのIPアドレスで装置にアクセスすることはできなくなることがありますので、異なるIPアドレスを設定することをお勧めします。なお、ルータに設定されるIPアドレスと仮想IPアドレスを同じにする場合は、必ず、そのルータの優先度を優先度固定(最優先)に設定してください(優先度として優先度固定(最優先)を設定した場合、仮想IPアドレスは設定できません)。
- 優先度に "優先度固定(最優先)"を定義した場合は、プリエンプトモードの on/off にかかわらず、プリエンプトモードが on のときと同様に動作します。
- VRRP機能では、VRRP-ADメッセージに以下のパケットを使用します。IPフィルタ設定時には、このパケットを遮断しないように設定する必要があります。
 あて先IPアドレス : 224.0.0.18
 プロトコル番号 : 112
- ・ トリガ機能を使用する場合は VRRP グループの優先度に "優先度固定(最優先)"を指定しないでください。

2.28.1 簡易ホットスタンバイ機能を使う

適用機種 全機種

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現できます。2台のルータを PPPoE でインターネットに接続して、ホットスタンバイを構成する場合の設定方法を説明します。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータはWAN側経路をノードダウントリガによって監視する
- [マスタルータ]

 PPPoEで使用する LAN ポート 	:LANOポート
 本装置のIPアドレス/ネットマスク 	: 192.168.1.10/24
● ユーザ認証 ID	: userid
 ユーザ認証パスワード 	: userpass
 ノードダウントリガの監視IPアドレス 	:202.168.2.1(プロバイダ側のDNSサーバアドレスなど)
[バックアップルータ]	
 PPPoEで使用するLANポート 	:LANOポート
 本装置のIPアドレス/ネットマスク 	: 192.168.1.11/24
• ユーザ認証 ID	: userid2
 ユーザ認証パスワード 	: userpass2

上記の設定条件に従って設定を行う場合の設定例を示します。

マスタルータを設定する

1. 「1.6 インターネットへPPPoE で接続する」(P.67)を参考に、PPPoE での接続を設定します。

2. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

3. 「LAN 情報」でLAN1の[修正] ボタンをクリックします。

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

4. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

- 5. 以下の項目を指定します。
 - VRRP機能

→使用する

VRRP機能	 ○ 使用しない ③ 使用する
	バスワード

Si-R180、180Bでは、LANバックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

6. [保存] ボタンをクリックします。

7. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

「VRRPグループ情報」が表示されます。

8. 「VRRP グループ情報」でグループ番号が0の[修正] ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

9. 以下の項目を指定します。

•	グループID	→ 10
•	プライオリティ	→優先度指定
	優先度	→254
	仮想IPアドレス	→ 192.168.1.1

• プリエンプトモード → OFF

■基本情報 ?			
グルーブID	10		
	⊙ 優先度指定		
	優先度 254		
ブライオリティ	仮想IPアドレス		
	○ 優先度固定(最優先)		
	優先度 255 仮想IPアドレス インタフェースアドレスを使用		
AD送信間隔	1 秒		
ブリエンプトモード	 ○ ON ⊙ OFF 移行禁止時間 		

- 10. 【保存】ボタンをクリックします。
- **11.** VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。

- 減算プライオリティ
- →254 • トリガ種別 →ノードダウントリガ (node) あて先IPアドレス →202.168.2.1 送出インタフェース →指定なし 再送間隔 →5 タイムアウト時間 →16 正常時送信間隔 → 17 異常時送信間隔 →30

<vrrpトリガ情報入力フィールド></vrrpトリガ情報入力フィールド>		
減算ブライ オリティ	254	
トリガ種別	254 ● インタフェースダウントリガ インタフェース ● ルートダウントリガ(route ・ パートダウントリガ(route ● デフォルト ● ジブフォルト ● 経路を指 ● 経路を指 ● あて先F レス あて先F フィマスク 1 **** **** **** ● ノードダウントリガ(node) あてた」Pアドレス 送出インタフェース 再送間隔 タイムアウト時間 正常時送信間隔	ガ(ifdown) すべて ▼) ・ルート 定する 「アド 0 0.0.0) ▼ 16 秒 17 秒
	止常時送信間隔 異常時送信間隔	17_秒 30_秒

- 13. [追加] ボタンをクリックします。
- 画面左側の [設定反映] ボタンをクリックします。 14. 設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

LAN1情報を設定する

「LAN1情報」-「共通情報」			
「基本情報」			
→使用する			
「VRRP グループ0 情報」			
「基本情報」			
→ 10			
→優先度指定			
→ 100			
→192.168.1.1			

• プリエンプトモード → OFF

手順12.の設定例で、インタフェースダウントリガを使用してWAN側(PPPoE)インタフェース状態を監視する場合は、マスタルータ側に以下の設定を追加します。

LAN1情報を設定する

「LAN1 情報」-「共通情報」 「VRRP グループ0 情報」-「VRRP トリガ情報」

- VRRP機能 →使用する
- 減算プライオリティ → 254
- トリガ種別 →インタフェースダウントリガ (ifdown)
 インタフェース → rmt0

2.28.2 クラスタリング機能を使う

適用機種 全機種

本装置では、2台のルータに複数のグループIDを設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。2台のルータをPPPoEでインターネットに接続する場合の設定方法を説明します。



- 設定条件
- 故障発生後の切り戻しは手動で行う
- マスタルータは PPPoE 側のインタフェースをインタフェースダウントリガにより監視する

[グループ A]	

● グループID	: 10		
 仮想 IP アドレス 	: 192.168.1.1		
[グループ B]			
・ グループID	: 11		
 仮想IPアドレス 	: 192.168.1.2		
[マスタルータ]			
 PPPoEで使用するLANポート 	: LAN0ポート		
 本装置のIPアドレス/ネットマスク 	: 192.168.1.10/24		
• ユーザ認証 ID	userid		
• ユーザ認証パスワード	userpass		
[バックアップルータ]			
 PPPoE で使用する LAN ポート 	: LAN0ポート		
 本装置のIPアドレス/ネットマスク 	: 192.168.1.11/24		
• ユーザ認証 ID	: userid2		
• ユーザ認証パスワード	: userpass2		

こんな事に気をつけて

クラスタリング機能を有効に利用するには、PCからのトラフィック量に応じて、PC側で設定するデフォルトルートの 定義を適切に分散する必要があります。

上記の設定条件に従って設定を行う場合の設定例を示します。

ここでは、インターネットへPPPoEで接続されていることを前提とします。

● 参照「1.6 インターネットへ PPPoE で接続する」(P.67)

マスタルータを設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 以下の項目を指定します。
 インタフェース
 - →物理LAN

<LAN情報追加フィールド> インタフェース 物理LAN ✔

- 【追加】ボタンをクリックします。
 「LAN1情報(物理LAN)」ページが表示されます。
- 4. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

- 5. 以下の項目を指定します。
 - VRRP機能

→使用する

VRRP機能	 ○ 使用しない ③ 使用する
	バスワード

Si-R180、180Bでは、LANバックアップ機能をサポートしていないため、 "優先使用ポート"の項目はありません。また、 "ポート番号"の表示内容が異なります。

- 6. [保存] ボタンをクリックします。
- **7. 共通情報の設定項目の「VRRPグループ情報」をクリックします**。 「VRRPグループ情報」が表示されます。
- **8.** 「VRRP グループ情報」でグループ番号が0の[修正]ボタンをクリックします。 VRRP グループ情報の設定項目と「基本情報」が表示されます。

• プライオリティ

仮想IPアドレス

• グループID

優先度

→ 10
→優先度指定 →254
→ 192.168.1.1

● プリエンプトモード → OFF

■基本情報	3
グループID	10
ブライオリティ	 ● 優先度指定
	1変元度 仮想IPアドレス 192.168.1.1
	 ○ 優先度固定(最優先) 優先度 255 仮想IPアドレス インタフェースアドレスを使用
AD送信間隔	1 秒
ブリエンブトモード	 ○ ON ⊙ OFF 移行禁止時間 □ 秒

- 10. 【保存】ボタンをクリックします。
- **11.** VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。 「VRRP トリガ情報」が表示されます。
- 12. 以下の項目を指定します。
 - 減算プライオリティ → 254
 - トリガ種別 →インタフェースダウントリガ (ifdown)
 インタフェース → rmt0

<vrrpトリガ情報入力フィールド></vrrpトリガ情報入力フィールド>		
減算ブライ オリティ	254	
	⊙ インタフェースダウントリガ(ifdown)	
トリノリ権力リ	インタフェース rmt0 v	

- 13. [追加] ボタンをクリックします。
- **14. 画面上部の「LAN1情報(物理LAN)」をクリックします**。 「LAN1情報(物理LAN)」ページが表示されます。
- **15. 共通情報の設定項目の「VRRP グループ情報」をクリックします**。 「VRRP グループ情報」が表示されます。
- **16.** 「VRRP グループ情報」でグループ番号が1の [修正] ボタンをクリックします。 VRRP グループ情報の設定項目と「基本情報」が表示されます。

• プライオリティ

仮想IPアドレス

• グループID

優先度

→ 11
→優先度指定 → 100
→ 192.168.1.2

プリエンプトモード → ON

■基本情報	3
グルーブID	11
ブライオリティ	 ● 優先度指定 ////////////////////////////////////
	100 仮想IPアドレス 192.168.1.2
	 ● 優先度固定(最優先) 優先度 255 仮想IPアドレス インタフェースアドレスを使用
AD送信間隔	1 秒
ブリエンブトモード	 ON OFF 移行禁止時間 ● 秒

- 18. [保存] ボタンをクリックします。
- **19. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

LAN1情報を設定する

「LAN1情報」-「共通情報」	
「基本情報」	
• VRRP機能	→使用する
「VRRP グループ 0 情報」	
「基本情報」	
● グループID	→ 10
• プライオリティ	→優先度指定
優先度	→ 100
仮想IPアドレス	→ 192.168.1.1
• プリエンプトモード	→ON
「VRRP グループ 1 情報」	
「基本情報」	
• グループ ID	→ 11
• プライオリティ	→優先度指定
優先度	→ 254
仮想IPアドレス	→ 192.168.1.2
• プリエンプトモード	→OFF
「VRRP トリガ情報」	
• 減算プライオリティ	→254
● トリガ種別	→インタフェースダウントリガ(ifdown)
インタフェース	→rmt0

2.29 ポリシールーティング機能を使う

適用機種 全機種

本装置では、入力側でポリシールーティングを行う Ingress ポリシールーティングと、出力側でポリシールーティングを行うマルチルーティングの2つを設定することができます。

2.29.1 Ingress ポリシールーティング機能を使う

適用機種 全機種

Ingress ポリシールーティング機能とは、ルーティングによる経路情報の参照前に、入力パケットのあて先IPア ドレスだけではなく、送信元IPアドレスやポート番号などの情報も利用して、設定した送出先へパケットを転送 する機能です。この機能を利用することによって、受信インタフェースごとに経路情報に従わないパケット転送 を行うことができます。ここでは、支社←→本社は本社ネットワークのファイアウォールを通さずに通信し、支 社←→インターネットは本社ネットワークのファイアウォールを通して通信する場合の設定方法を説明します。



● 前提条件

- 本社←→インターネットの通信パス(①の通信パス)
- 本社の本装置にインターネットへの通信が設定済み(lan 0)
- 支社←→本社の通信パス(②の通信パス)
- 本社の本装置に IPsec を利用した VPN 通信が設定済み (remote 0 ap 0)

● 設定条件

- 支社←→インターネットの通信は、本社のファイアウォールを経由する(③の通信パス)
- Ian 0インタフェースに、本装置あてパケット以外を Ian1 の 192.168.4.1(ファイアウォール)に転送する Ingress ポリシールーティングを設定する
- remote 0インタフェースに、本装置あてパケット以外を lan2 の 192.168.2.1 に転送する lngress ポリシー ルーティングを設定する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置あてIPv4パケットに一致するACL定義を設定する

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名 → ACL0
 <ACL情報追加フィールドン
 定義名 ACL0
- **3. [追加] ボタンをクリックします**。 「ACL定義情報(ACL0)」ページが表示されます。
- **4.** 「IP 定義情報」をクリックします。 「IP 定義情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル →すべて
 送信元情報
 IPアドレス →指定しない
 アドレスマスク →指定しない

 あて先情報
 - IPアドレス
 → 202.168.2.66

 アドレスマスク
 → 32 (255.255.255)
- QoS →指定なし



6. [保存] ボタンをクリックします。
すべてのIPv4パケットに一致するACL定義を設定する

7. 手順1.~6.を参考に、以下の項目を指定します。

「ACL情報」

 定義名 →ACL1 「ACL定義情報(ACL1)」-「IP定義情報」 • プロトコル →すべて 送信元情報 IPアドレス →指定しない アドレスマスク →指定しない あて先情報 IPアドレス →指定しない アドレスマスク →指定しない QoS →指定なし

本装置あてパケット以外を lan1 の 192.168.4.1 に転送するポリシーグループを設 定する

- 8. 設定メニューのルータ設定で「ポリシーグループ情報」をクリックします。 「ポリシーグループ情報」ページが表示されます。
- [追加] ボタンをクリックします。
 「ポリシーグループ定義情報(0)」ページが表示されます。
- **10.** 「パターン定義情報」をクリックします。 「パターン定義情報」が表示されます。
- 11. 以下の項目を指定します。
 - 動作 →使用しない
 - ACL定義番号 →0

<バターン定義情報入力フィールド>

 動作
 ●使用する ●使用しばい ●バックアップとして使用する

 ACL定義番号
 ●

12. [追加] ボタンをクリックします。

「パターン定義情報」が表示されます。

- 13. 手順 11. ~ 12. を参考に、以下の項目を指定します。
 - 動作 →使用する
 - ACL定義番号 →1
- **14. 「送出先定義情報」をクリックします**。 「送出先定義情報」が表示されます。

• 送出インタフェース	→LAN1
 転送先ルータ 	
IPv4ルータ	→ 192.168.4.1
IPv6ルータ	→指定しない
■送出先定義情報	

■送出先定義情	青報	3
送出先インタフェ	ース	LAN1 💌
起送生正一句	IPv4ルータ	192.168.4.1
FAIZ/U/U ×	IPv6ルータ	

16. [保存] ボタンをクリックします。

本装置あてパケット以外を lan2の192.168.2.1 に転送するポリシーグループを設定する

17. 手順8.~16.を参考に、以下の項目を指定します。

「ポリシーグループ情報」
「パリシーグループ定義情報(1)」-「パターン定義情報」
優先順位0
● 動作 →使用しない
ACL定義番号 →0
優先順位1
● 動作 →使用する
ACL定義番号 →1
「ポリシーグループ定義情報(1)」-「送出先定義情報」
● 送出インタフェース → LAN2

転送先ルータ
 IPv4ルータ → 192.168.2.1
 IPv6ルータ →指定しない

Ian 0インタフェースに Ingress ポリシールーティングを設定する

- **18. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **19.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **20.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **21.** IP 関連の設定項目の「Ingress ポリシールーティング情報」をクリックします。 「Ingress ポリシールーティング情報」が表示されます。

• ポリシーグループ定義番号 →0

<ingressポリシールーティング情報入力< th=""><th>Jフィールド></th></ingressポリシールーティング情報入力<>	Jフィールド>
ポリシーグループ定義番号	0 参照

23. [追加]ボタンをクリックします。

「Ingress ポリシールーティング情報」が表示されます。

remote 0インタフェースに Ingress ポリシールーティングを設定する

- **24. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **25.** VPN 接続をしているネットワーク情報(vpn-shiA)の [修正] ボタンをクリックします。 「ネットワーク情報(vpn-shiA)」ページが表示されます。
- **26.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- **27.** IP 関連の設定項目の「Ingress ポリシールーティング情報」をクリックします。 「Ingress ポリシールーティング情報」が表示されます。
- 28. 以下の項目を指定します。
 - ポリシーグループ定義番号 →1

<Ingressポリシールーティング情報入力フィールド> ポリシーグループ定義番号 1 参照

29. [追加] ボタンをクリックします。

「Ingress ポリシールーティング情報」が表示されます。

30. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

Ingress ポリシールーティング機能は、ポリシーに一致した場合、ブロードキャストパケットやマルチキャストパケット、本装置あてパケットも転送します。

2.29.2 マルチルーティング機能を使う

適用機種 全機種

マルチルーティング機能を使用すると、同じあて先ネットワークへの送信データを、別の通信パスを利用して送信することができます。



● 設定条件

- IPsecを利用した VPN 通信が設定済み (remote 0 ap 0)
- 参照
 「1.14.1 NATを併用しない固定 IP アドレスでの VPN (自動鍵交換)」(P.145)、
 「1.14.2 NATと併用した固定 IP アドレスでの VPN (自動鍵交換)」(P.156)
- 新規に音声データ用の専用線(BRI:128Kbps)を追加する
- 通常、音声データ(TOS 値:a0)は専用線を利用する
- 通常、その他のデータは IP-VPN を利用する
- 専用線(音声用)がダウンした場合は、音声データも IP-VPN を使用する
- IP-VPN(データ用)がダウンした場合は、その他のデータも専用線を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

- **1. 設定メニューのルータ設定で「WAN 情報」をクリックします**。 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →専用線

		<wan情報追加t< th=""><th>フィールド></th><th></th></wan情報追加t<>	フィールド>	
回線イン	/タフェース		専用線	~

3. [追加] ボタンをクリックします。

「WAN0 情報(専用線)」ページが表示されます。

4. 「基本情報」をクリックします。 「基本情報」が表示されます。

 ポート →ス 	ベロット0-0
----------------------------	---------

• 回線速度 → 128Kbps

■基本情報	3
ボート	スロット 0-0 💌
回線速度	128Kbps 🗸

Si-R220B、220Cでは、ポートは固定です。

- 6. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 8. 「ネットワーク情報」でマルチルーティングを設定するネットワーク名の [修正] ボタンをクリック します。

「ネットワーク情報」が表示されます。

- **9. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 10. 「接続先情報」でIP-VPNを使用している接続先名の[修正]ボタンをクリックします。 IPsec/IKE接続の設定項目と「基本情報」が表示されます。
- **11.** IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。 「マルチルーティング情報」が表示されます。

→a0

- 12. 以下の項目を指定します。
 - 動作 →バックアップとして使用する
 - TOS



- 13. [追加] ボタンをクリックします。
- 14. 手順 12.~13.を参考に、以下の項目を指定します。
 - 動作 →使用する

15. 画面上部の「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

- **16. 「接続先情報」をクリックします**。 「接続先情報」が表示されます。
- 17. 以下の項目を指定します。
 - 接続先名

- →HSD
- 接続先種別 →専用線接続



機種により、接続先種別の表示が上記の画面とは異なります。

18. [追加] ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

19. 画面左側の [再起動] ボタンをクリックします。 設定した内容が有効になります。

2.30 遠隔地のパソコンを起動させる (リモートパワーオン機能)

適用機種 全機種

リモートパワーオン機能は、本装置につながっている離れた所にあるパソコンを、WWW ブラウザから Wakeup on LAN 機能を使用して起動させることができます。

本機能は、WWW ブラウザで本装置のトップページが表示できる環境で利用できます。

ここでは、1階の事務所のパソコンから6階の事務所のパソコンを起動する場合の設定方法を説明します。



● 設定条件

[本社側]

- 起動するパソコンのホスト名
- 起動するパソコンのMACアドレス

: host1 : 00:00:0e:12:34:56

☆ ヒント =

◆ Wakeup on LAN 機能とは?

AMD社が開発したネットワーク上の電源OFF状態のパソコンを遠隔操作で起動する機能です。起動は Magic Packet と呼ばれるパケットを送付して行います。なお、Wakeup on LAN 機能はパソコンを起動するだけで電源 OFF は行いません。

電源OFF する場合は、別途、電源制御用ソフトウェアが必要になります。

こんな事に気をつけて

- 本機能は、Wakeup on LAN に対応したパソコンだけで利用できます。Wakeup on LAN 対応機種については、パソコンのメーカーにお問い合わせください。
- ・ 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。

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



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。

リモートパワーオン情報を設定する 2.30.1

適用機種 全機種

- 設定メニューのルータ設定で「ホストデータベース情報」をクリックします。 1. 「ホストデータベース情報」ページが表示されます。
- 2. 未設定の欄の[修正]ボタンをクリックします。
- 3. 以下の項目を指定します。
 - ホスト名 →host1
 - MACアドレス →00:00:0e:12:34:56
 - リモート電源制御 →対象

・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 補足 おり、それぞれ必要な項目だけを設定します。

[•] ホスト名は必須の設定項目ではありませんが、実際にリモートパワーオンを実行する場合にホスト情報一覧から目標 とするパソコンを選択するのに有効な情報になります。

	ホスト名	host1
	IPv4アドレス	
	IPv6アドレス	
1	MACアドレス	00:00:0e:12:34:56
	リモート電源制御	⊙対象○対象外

- 4. [保存] ボタンをクリックします。
- 5. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

2.30.2 リモートパワーオン機能を使う

適用機種 全機種

- 1. パソコン上のWWW ブラウザで、起動させるパソコンがつながっている本装置のトップページを表示 します。
- 2. 操作メニューで「リモートパワーオン」をクリックします。 「リモートパワーオン」ページが表示されます。
- 起動させるパソコンの [オン] ボタンをクリックします。 3. 本装置が、該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。



「「アインンが Magic Packet を受信してから起動が完了するまで、数十秒から数分かかります(お使いの機種やOS に よって異なります)。

2.31 スケジュール機能を使う

適用機種 全機種

本装置のスケジュール機能には、以下のとおりです。

- スケジュール予約 特定の動作とそれを行う時間をスケジュール予約情報として登録できます。スケジュール予約情報を登録し ておくと、特定時間帯のデータの発着信を制限したり、定期的に課金情報をクリアしたりする作業を、本装 置が自動的に行います。スケジュール予約情報は、最大16件まで登録できます。
- 電話番号変更予約(Si-R220B、220C、370、570) 指定した日時に構成定義情報の電話番号を一括して変更することができます。電話番号変更予約情報は、最 大4件まで登録できます。電話番号は、予約情報1件に対して4つまで登録することができます。
- 構成定義情報切り替え予約
 本装置は、内部に2つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

● 参照 Si-Rシリーズ Web ユーザーズガイド「1.5 時刻を設定する」(P.14)

2.31.1 スケジュールを予約する

適用機種 全機種

発信抑止を予約する

ここでは、毎日午後11時から午前8時までの発信を抑止する場合の設定方法を説明します。

- 設定条件
- 動作
 :発信抑止
- 日/曜日
 :毎日
- 開始時刻 : 23:00
- 終了時刻 : 08:00

上記の設定条件に従ってスケジュールを予約する場合の設定例を示します。

- 設定メニューの基本設定で「スケジュール情報」をクリックします。
 「スケジュール情報」ページが表示されます。
- 「月間/週間予約情報」をクリックします。
 「月間/週間予約情報」が表示されます。
- 3. 「月間/週間予約情報」で未設定の欄の[修正]ボタンをクリックします。

4. 以下の項目を指定します。

- 動作 →発信抑止
- 予約時刻 →23:00
- →毎日
 終了時刻
 →08:00

	動作	発信抑止	
1	予約時刻	23 : 00	 ●毎日 ●毎週 □日曜日 □月曜日 □火曜日 □水曜日 □木曜日 □金曜日 □土曜日 ●毎月 □日
	<mark>終了時刻</mark>	08 : 00	

回線接続中に、発信抑止または着信抑止が実行されても、回線は切断されません。

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

こんな事に気をつけて

リモートパワーオンを予約する

ここでは、毎朝8時に特定のパソコンを起動する場合を例に説明します。

- **1. 設定メニューの基本設定で「スケジュール情報」をクリックします**。 「スケジュール情報」ページが表示されます。
- **2. 「月間/週間予約情報」をクリックします**。 「月間/週間予約情報」が表示されます。
- 3. 未設定の欄の[修正]ボタンをクリックします。

4. 以下の項目を指定します。

- 動作
- →リモートパワーオン
- 予約時刻 → 08:00

```
→毎日
```

	動作	リモートバワ・	-オン 💌
1	予約時刻	08 : 00	 ● 毎日 ● 毎週 □ 日曜日 □ 月曜日 □ 火曜日 □ 水曜日 □ 土曜日 ○ 毎月 □ 日
	終了時刻		

Si-R180、180B、260Bでは、表示内容が上記の画面とは異なります。

こんな事に気をつけて

リモートパワーオン機能を利用するには、あらかじめ利用するパソコンを「ホストデータベース情報」-「リモート電 源制御」を「対象」として登録しておく必要があります。また、スケジュール機能を使ってリモートパワーオンする場 合、「リモート電源制御」が「対象」となっているすべてのパソコンが起動します。

● 参照「2.30 遠隔地のパソコンを起動させる(リモートパワーオン機能)」(P.835)

- 5. [保存] ボタンをクリックします。
- 6. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.31.2 電話番号変更を予約する

適用機種 Si-R220B,220C,240,240B,370,570

ここでは、2004年7月1日午前2時に電話番号を「06-123-4567」から「06-6123-4567」に変更する場合の設定 方法を説明します。

● 設定条件

- 実行日時 : 2004年7月1日 2時00分
- 電話番号変更前情報 : 06-123-4567
- 電話番号変更後情報 : 06-6123-4567

上記の設定条件に従って電話番号変更を予約する場合の設定例を示します。

- 設定メニューの基本設定で「スケジュール情報」をクリックします。
 「スケジュール情報」ページが表示されます。
- **2. 「電話番号変更予約情報」をクリックします**。 「電話番号変更予約情報」が表示されます。
- 3. 「電話番号変更予約情報」で未設定の欄の[修正]ボタンをクリックします。

4. 以下の項目を指定します。

• 実行日時

→2004年7月1日2時00分

電話番号変更情報
 変更前1 → 06-123-4567
 変更後1 → 06-6123-4567

	実行 日時	20 04	年7月1日2時00分
1	電話 番変 情報	変更 前1 変更 前2	06-123-4567 後1 変更 後2
		変更 前3	资更 後3
		変更 前4	変更 後4

5. [保存] ボタンをクリックします。

6. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて 指定時刻になると自動的に本装置が再起動され、電話番号が更新されます。その際、データ通信中の場合は、回線が切 断されます。

2.31.3 構成定義情報の切り替えを予約する

適用機種 全機種

本装置は、構成定義情報を内部に2つ持つことができます。

ここでは、2004年7月1日6時30分に構成定義情報を1から2に切り替える場合の設定方法を説明します。

● 設定条件

- 実行日時 : 2004年7月1日 6時30分
- 構成定義情報切り替え :構成定義情報1→構成定義情報2

上記の設定条件に従って構成定義情報を切り替える場合の設定例を示します。

- 設定メニューの基本設定で「スケジュール情報」をクリックします。
 「スケジュール情報」ページが表示されます。
- 2. 「構成定義切り替え予約情報」をクリックします。 「構成定義切り替え予約情報」が表示されます。
- 3. 「構成定義切り替え予約情報」で未設定の欄の[修正]ボタンをクリックします。
- 4. 以下の項目を指定します。
 - 実行日時 →2004年7月1日6時30分
 - 動作 →構成定義情報2で再起動

 実行日時
 20 04 年7 月1 日6 時30 分

 1 動作
 構成定義情報2で再起動 ▼

- 5. [保存] ボタンをクリックします。
- 6. **画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

2.32 通信料金を節約する (課金制御機能)

適用機種 Si-R220B,220C,240,240B,370,570

本装置は通信料金を節約するための機能をサポートしています。この機能は、通信料金のむだ、使い過ぎを防ぐことができます。以下に、各機能について説明します。

● 課金単位時間

ISDN 回線やプロバイダの多くは、一定時間単位で料金を算定する従量課金制度を採用して料金を決めています。 通信料金が3分10円で計算される場合、3分の中で何度も切断/接続を繰り返すと、料金額はその回数×10円に なります。

そこで課金単位時間(通信料金が計算されるときの単位時間)を設定し、無通信監視タイマ(初期値:60秒)と 連動することで、単位時間内は回線を切断させないようにします。無通信監視タイマとは、設定した時間を超え てアクセスがなければ自動的に切断するという機能です。

課金単位時間に3分間を指定した場合、以下のようになります。



● 課金制御機能(発信抑止/強制切断)

データ通信に費やした通信時間や通信料金が一定の値を超えた場合、接続を禁止したり、ログにアラームを出し たりする課金制御機能(発信抑止)もあります。また、Si-R240、240Bのデータ通信カード接続では、通信時間 や送受信パケット数の累計が一定の値を超えた場合、接続中の回線を切断し、以降の手動および自動発信を禁止 する課金制御機能(強制切断)もあります。無意識のうちに通信料金を使いすぎるのを防ぐことができます。

こんな事に気をつけて

- ・ 設定前に本装置の内部時刻を正しくセットしてください。
- 課金制御機能(発信抑止)は、指定された料金を超えた場合に発信を制御する機能であり、運用中の回線を切断する 機能ではありません。回線の接続中に指定された料金を超えても、回線を接続したままだと料金がかかり続けます。 その結果、通信料金が指定した金額を超えてしまうのでご注意ください。
- モデムでは、回線の切断に時間がかかるため、課金単位を超えて切断される場合があります。
- 通信料金による課金制御機能(発信抑止)は、ISDN 接続の場合のみ有効です。

課金単位時間を設定する 2.32.1

適用機種 Si-R220B,220C,240,240B,370,570

ここでは、相手情報としてremote0、接続先情報としてap0がすでに登録済みであることを前提とします。

● 設定条件

- 無通信監視タイマ :60秒
- 課金単位時間 昼間(08:00~19:00) :180秒 夜間(19:00~23:00) :180秒 深夜·早朝(23:00~08:00) :240秒

上記の設定条件に従って課金単位時間を設定する場合の設定例を示します。

- 設定メニューのルータ設定で「相手情報」をクリックします。 1. 「相手情報」ページが表示されます。
- 2. 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。
- 「ネットワーク情報」でネットワーク名が「rmt0」の[修正] ボタンをクリックします。 3. 「ネットワーク情報(rmt0)」が表示されます。
- 「接続先情報」をクリックします。 4. 「接続先情報」が表示されます。
- 「接続先情報」で接続先名が「ap0」の[修正] ボタンをクリックします。 5. ISDN 接続の設定項目と「基本情報」が表示されます。

6. ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

- 無通信監視タイマ →送受信パケットについて60秒
- 課金単位時間

深夜·早朝

昼間 夜間 → 180 →180

深夜・	早朝	→240
無通信監 視タイマ	送受信バケット 🔽	について 60 秒
	昼間(月~金) (08:00~19:00)	180 0 秒
課金単位 時間	夜間(土日の昼間) (19:00~23:00)	180 . 0 秒
	深夜·早朝	and a file

240 0 秒

7. [保存] ボタンをクリックします。

(23:00~08:00)

8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.32.2 課金制御機能(発信抑止)を設定する

<u>適用機種</u> Si-R220B,220C,370,570

ここでは、接続累計時間が50時間、または通信料金の合計が10,000円になると接続要求を抑止する場合の設定 方法を説明します。

● 設定条件

- 通信時間累計の上限時間
 50時間
- 通信料金の上限金額
 10,000円

上記の設定条件に従って設定を行う場合の設定例を示します。

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 回線インタフェースがISDNの[修正]ボタンをクリックします。
 「WAN 情報(ISDN)」ページが表示されます。
- 3. 「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

4. 以下の項目を指定します。

•	通信時間による発信抑止 上限時間	→する →50 時間
•	課金金額による発信抑止	→する > 10000
	上阪並領	-10000

■接続制御情報	3
通信時間による発信 抑止	 ● しない ● する 上限時 間 制御動 ●発信抑止 ●システムログ出力 作
課金額による発信抑 止	 ● しない ● する 上限金 10000 円 額 0 発信抑止 ○システムログ出力 作 のみ

5. [保存] ボタンをクリックします。

画面左側の「設定反映」ボタンをクリックします。 6.

設定した内容が有効になります。



課金情報をクリアすることで、再度、発信ができるようになります。課金情報をクリアするには、表示メニューの 「課金情報」から行います。

こんな事に気をつけて

- ・ 本書の表記で使われる通信料金とは、INSネット64基本サービスの「料金情報通知」をもとに、本装置のソフトウェ アが算出した値です。算出される値は、お客様の契約や回線利用状況によって異なりますので、請求金額とは必ずし も一致しません。
 - たとえば以下のような場合があります。
 - INS テレホーダイサービス利用時
 - 各種料金割り引きサービス利用時
- 本装置の電源を切ると、課金情報(通信時間累計、通信料金累計など)はすべてクリアされます。

2.33 ブリッジ/STP機能を使う



ここでは、ブリッジで FNA をつないで STP 機能を使用する場合、ブリッジグルーピング機能を使用する場合お よび IP トンネルでブリッジ通信を行う場合の設定方法を説明します。

こんな事に気をつけて

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

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

- ・ STP機能は、グループ0でだけ動作します。VLANインタフェースでは、STPを使用できません。
- WAN インタフェースでブリッジを利用する場合は、1つの相手情報(remote)に対して、1つの接続先情報(ap)となるように設計してください。
- 本装置では、ファームウェアの更新やSNMPでの監視などの目的でIPv4のIPアドレスを使用します。そのため、 IPv4のIPアドレスを設定しないで運用することはできません。IPv6およびブリッジだけを使用しているネットワー クで運用する場合でも、どれかのLANインタフェースに必ずIPv4のIPアドレスを設定してください。
- ・ VLAN でバインドされたインタフェースでブリッジを行うことはできません。
- 本装置のブリッジMAC学習は、異なるVLAN上で同一のMACアドレスを学習することはできません。本装置は、唯 一装置がもつ学習テーブルを各VLANが共有するSVL(Shared VLAN Learning)と呼ばれる方式で学習を行ってい ます。VLANインタフェースでブリッジを行う場合は、異なるVLAN上に同一のMACアドレスを持つネットワークと 接続しないでください。
- 設定を間違えてループ構成を構成し、ブロードキャストストームが発生してコンソールなどが反応しなくなった場合は、ブリッジが有効なWANやLANのケーブルを抜くとブロードキャストストームが収まります。ブロードキャストストームが収まったところで設定を修正してください。

2.33.1 ブリッジで FNA をつないで STP 機能を使う

適用機種 全機種

ブリッジ機能を使用すると、離れたLANどうしを1つのサブネットワークとして使用することができます。また、STP機能を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

● 参照 Si-Rシリーズ 機能説明書「2.25 VRRP機能」(P.107)

LAN接続の場合

適用機種 全機種

ここでは、離れたLAN(FNA)をブリッジでつなぐ場合を例に説明します。



● 設定条件

- 本社へFNAのデータだけをブリッジする
- STP 機能を使用する

ブリッジ機能によりネットワークを接続する場合は、ブリッジ通信をするパケット以外をフィルタリングする設定にしてください。フィルタリングしないと不要なトラフィックが発生するだけでなく、IP 通信できなくなる場合があります。

上記の設定条件に従って設定を行う場合の設定例を示します。

ブリッジ情報を設定する(LAN1)

1. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN 情報」ページが表示されます。

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

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

3. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

こんな事に気をつけて

- ブリッジ機能 →使用する
- STP機能 →使用する

■ブリッジ情報		3
フリッジ機能	○使用しない ●使用する	
クループ識別子	0	
	 ○ 使用しばい ③ 使用する 	
STP機能	バスコスト ○ 自動決定 ○ 指定する	
	インタフェース優先度 128	

5. [保存] ボタンをクリックします。

ブリッジ情報を設定する(LAN0)

- 6. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN 情報」ページが表示されます。
- 7.
 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「ブリッジ関連」をクリックします。
 ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。
- 9. 以下の項目を指定します。
 - ブリッジ機能 →使用する
 - STP機能 →使用する

■ブリッジ情報	[2
フリッジ機能	○使用しない ⊙使用する	
クルーブ識別子	0	
	 ○ 使用しない ● 使用する 	
STP機能	バスコスト ○自動決定 ○指定する	
	インタフェース優先度 128	

10. 【保存】ボタンをクリックします。

フィルタリング情報でFNAを透過させる(支社→本社)

- **11. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 12. 以下の項目を指定します。
 - ◆ 定義名 → ACL0

< ACLI育税15加フィールト >		
定義名	ACLO	

13. [追加] ボタンをクリックします。

「ACL 定義情報(ACL0)」ページが表示されます。

14. 「MAC定義情報」クリックします。

「MAC定義情報」ページが表示されます。

15. 以下の項目を指定します。

- ・ 送信元 MAC アドレス → すべて
- あて先 MAC アドレス →指定する
 アドレス指定 → 00:00:0e:0a:12:34
- フォーマット種別 → LLC形式
 LSAP → 8080

→しない

VLAN タグ解析

MAC定義情報	3
送信元MACアドレス	すべて ▼ アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	指定する アドレス指定(″指定する″を選択時のみ有効です) 00:00:0e:0a12:34
フォーマット種別	 すべて LLC形式 LSAP 8080 VLANタグ解析 ●しばい ●する SNAP形式 type値 VLANタグ解析 ●しばい ●する Ethernet形式 type値 VLANタグ解析 ●しばい ●する

- 16. 【保存】ボタンをクリックします。
- **17. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **18.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- **19. 「ブリッジ関連」をクリックします。** ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。
- **20. ブリッジ関連の設定項目の「MAC フィルタリング情報」をクリックします**。 「MAC フィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →リバース
- ACL定義番号 →0

<macフィルタリング情報入力フィールド></macフィルタリング情報入力フィールド>	
動作 💿 透過 🔾 遮断	
方向	リバース 💌
ACL定義番号	0 参照

22. [保存] ボタンをクリックします。

フィルタリング情報でSTPを透過させる

23. 手順 11.~22.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → ACL1

	, IOET	
「ACL情報(ACL1)」-「MAC定義情報」		
 送信元 MAC アドレス 	→すべて	
● あて先 MAC アドレス	→指定する	
アドレス指定	→ 01:80:c2:00:00:00	
• フォーマット種別	→LLC形式	
LSAP	→ 4242	
VLAN タグ解析	→しない	
「LAN 情報」-「ブリッジ関連」		

「MAC フィルタリング情報」

•	動作	→透過
•	方向	→リバース
•	ACL定義番号	→ 1

残りの通信をすべて遮断する

24. 手順 11.~22.を参考に、以下の項目を指定します。

「ACL情報」

 定義名 →ACL2 「ACL情報(ACL2)」-「MAC定義情報」 • 送信元 MAC アドレス →すべて • あて先 MAC アドレス →すべて • フォーマット種別 →すべて 「LAN 情報」-「ブリッジ関連」 「MAC フィルタリング情報」 動作 →遮断 方向 →入出力 • ACL 定義番号 →2

25. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

リモート接続の場合

適用機種 Si-R220B,220C,260B,370,570

ここでは、専用線をはさんで離れたLAN(FNA)をブリッジでつなぐ場合の設定方法を説明します。WANイン タフェースの種類によって設定が異なりますので、使用するWANインタフェースに応じてWAN関連定義を 行ってください。



● 設定条件

- SLOT0 に実装された BRI 拡張モジュール L2 または基本ボード上の ISDN ポート(Si-R220B、220Cの場合) で専用線(128kbps)を使用する
- 本社へFNAのデータだけをブリッジする
- STP 機能を使用する

こんな事に気をつけて

ブリッジ機能を使用すると定期的に発信するため、超過課金が発生します。ISDN 回線やモデム接続で STP 機能を使用 しないでください。

この例では、本社と支社がすでに専用線接続されていることを前提としています。

● 参照「1.10事業所LANを専用線で接続する」(P.103)

上記の設定条件に従って設定を行う場合の設定例を示します。

ブリッジ情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。
- 「ブリッジ関連」をクリックします。
 ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

- ブリッジ機能 →使用する
- STP機能 →使用する

■ブリッジ情報		3
ブリッジ機能	○使用しない ◎使用する	
グループ識別子	0	
	 ○ 使用しない ③ 使用する 	
STP機能	バスコスト ○自動決定 ○指定する	
	インタフェース優先度 128	

- 5. [保存] ボタンをクリックします。
- 6. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- 7. 「ネットワーク情報」でブリッジ設定を行うネットワーク名の [修正] ボタンをクリックします。 「ネットワーク情報」が表示されます。
- 「ブリッジ関連」をクリックします。
 ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

9. 以下の項目を指定します。

- ブリッジ機能 →使用する
- STP機能 →使用する

■ブリッジ情報		3
ブリッジ機能	○使用しない ⊙使用する)
グループ識別子	0	
STP機能	 ○ 使用しない ● 使用する 	
	パスコスト	 ●自動決定 ○指定する
	インタフェース優先度	128

- 10. [保存] ボタンをクリックします。
- フィルタリング情報でFNAを透過させる(支社→本社)
- **11. 設定メニューのルータ設定で「ACL情報」をクリックします**。 「ACL情報」ページが表示されます。
- 12. 以下の項目を指定します。
 - 定義名

→ ACL0

	<acl情報追加フィールド></acl情報追加フィールド>
定義名	ACLO

13. [追加] ボタンをクリックします。 「ACL 定義情報(ACL0)」ページが表示されます。

ブリッジ/ STP 機能を使う

14. 「MAC定義情報」クリックします。

「MAC 定義情報」ページが表示されます。

15. 以下の項目を指定します。

- ・送信元MACアドレス →すべて
 ・あて先MACアドレス →指定する アドレス指定 → 00:00:0e:0a:12:34
 ・フォーマット種別 → LLC形式
 - LSAP → 8080 VLANタグ解析 → しない

■MAC定義情報		
送信元MACアドレス	すべて アドレス指定("指定する"を選択時のみ有効です)	
あて先MACアドレス	指定する アドレス指定(‴指定する″を選択時のみ有効です) 00:00:0e:0a:12:34	
フォーマット種別	 すべて LLC形式 LSAP 8080 VLANタグ解析 ●しない ○する SNAP形式 type値 VLANタグ解析 ●しない ○する Ethernet形式 type値 VLANタグ解析 ●しない ○する 	

- 16. [保存] ボタンをクリックします。
- **17. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **18.** 「ネットワーク情報」でブリッジ設定を行うネットワーク名の [修正] ボタンをクリックします。 「ネットワーク情報」が表示されます。
- **19. 「ブリッジ関連」をクリックします。** ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。
- **20. ブリッジ関連の設定項目の「MAC フィルタリング情報」をクリックします**。 「MAC フィルタリング情報」が表示されます。

- 動作 →透過
- 方向 →リバース
- ACL定義番号 →0

<macフィルタリング情報入力フィールド></macフィルタリング情報入力フィールド>	
動作	⊙透過 ○遮断
方向	リバース 💌
ACL定義番号	0 参照

22. [保存] ボタンをクリックします。

フィルタリング情報でSTPを透過させる

23. 手順 11.~22.を参考に、以下の項目を指定します。

「ACL情報」

• 定義名 → ACL1

	ACLI
「ACL情報(ACL1)」-「MAC定義	遠情報」
 送信元 MAC アドレス 	→すべて
● あて先 MAC アドレス	→指定する
アドレス指定	→ 01:80:c2:00:00:00
• フォーマット種別	→LLC形式
LSAP	→ 4242
VLAN タグ解析	→しない
「LAN 情報」-「ブリッジ関連」	
「MAC フィルタリング情報」	

٠	動作	→透過
•	方向	→リバース
•	ACL定義番号	→ 1

残りの通信をすべて遮断する

24. 手順 11.~22.を参考に、以下の項目を指定します。

「ACL情報」

・ 定義名 → ACL2
 「ACL情報 (ACL2)」 - 「MAC定義情報」
 ・ 送信元 MAC アドレス → すべて
 ・ あて先 MAC アドレス → すべて
 ・ フォーマット種別 → すべて
 「相手情報」 - 「ブリッジ関連」
 「MAC フィルタリング情報」
 ・ 動作 → 遮断
 ・ 方向 → 入出力

ACL定義番号 →2

25. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.33.2 ブリッジグルーピング機能を使う

適用機種 全機種

ブリッジグルーピング機能とは、各インタフェースにグループ識別子を設定し、それぞれのインタフェースにグ ループを割り当てることによって、ブリッジ転送が、そのグループ内に閉じた形で行われるようにする機能で す。グループを分けることで、ブリッジ通信を各グループに分離することができます。

こんな事に気をつけて

- ・ ブリッジ学習テーブル生存時間は、グループ0に設定した値がすべてのグループで使用されます。
- ・ VLAN インタフェースをブリッジグループに含める場合は、1つまたは複数のリモートインタフェースとVLAN イン タフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数のLAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さいLAN インタフェースでだけ以下の機能を利用できます。
 - FTP(ファームアップデートなど)
 - telnet
 - Web ブラウザによる設定
 - syslogの送信
 - SNMPエージェント、Trap送信
 - ダイナミックルーティング
- IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が 行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使 用してください。
- ブリッジグループを複数定義する場合は、グループ識別子を0から順番に、間をあけないで設定してください。
- STPはグループ0でだけ動作するため、グループ0以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ0でループを構成するブリッジ構成を行う場合は、必ずSTPを有効にしてください。
- IPをブリッジする場合、WAN側にはブリッジで中継されるフレームだけが転送され、直接WAN側に Ethernet フレームではない IPパケットを送受信することはできません。よって、IPをブリッジする運用形態では、IPに関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- ・ WAN 経由で IP をブリッジし、ブリッジ転送を許す場合(転送ポリシが Loose)、たとえ WAN の先に存在するネット ワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジに よって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題な く WAN の先に存在するあて先ネットワークにブリッジで転送されて到達します。

ここでは、ブリッジグルーピング機能を使用して、本社と特定の支社との間で業務ごとに異なる通信を分離して 実現する場合の設定方法を説明します。

本社のLAN0と支社のLAN0との間はA業務関連だけを通信し、本社のLAN1と支社のLAN1との間はB業務関連だけを通信します。互いの通信はIPも含めて完全に分離します。



すでにATM 網を利用して、本社と支社の間でVPCを2つ接続し、以下のとおりに設定されていることを前提とします。

● 参照「2.35 ATM 網を使う」(P.871)

● 前提条件

[本社、支社共通]

• ATM 網を利用して、本社と支社の間で VPC を2つ接続している

[本社]

- LAN0のIPv4アドレス : 192.168.1.1/24
- LAN1のIPv4アドレス : 192.168.2.1/24

[支社]

- LAN0のIPv4アドレス : 192.168.1.2/24
- LAN1のIPv4アドレス : 192.168.2.2/24

● 設定条件

[本社、支社共通]

- ブリッジグループ数 : 2 グループ(A業務用とB業務用)
- IPv4の転送方式 : ブリッジで転送
- 転送ポリシ
 strict (完全に IPv4 通信を分離)

本社を設定する

ブリッジグループ0に属するインタフェースを設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **3. 「IP 関連」をクリックします**。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →192.168.1.1
 ネットマスク →24 (255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレ	ス情報	3
IPv4	●使用する●使用しない	
IP7ŀレス	 ○ DHCPで自動的に取得す。 ● 指定する IPアドレス ネットマスク ブロードキャストアドレス ス 	る 192.168.1.1 24 (255.255.255.0) ▼ ネットワークアドレス+オール1 ▼

5. [保存] ボタンをクリックします。

6. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

7. 以下の項目を指定します。

- ブリッジ機能 →使用する
- グループ識別子 →0
- STP機能 →使用しない

■ブリッジ情報		3
ブリッジ機能	○使用しない ⊙使用する	
グループ識別子	0	
	 ● 使用しない ● 使用する 	
STP機能	バスコスト	 ●自動決定 ●指定する
	インタフェース優先度	128

- 8. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。

- **10. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 「ネットワーク情報」でブリッジグループ0に属する(A業務用VPC)ネットワーク名の[修正]ボ タンをクリックします。
 「ネットワーク情報」ページが表示されます。
- **12. 「IP 関連」をクリックします**。

IP関連の設定項目と「IP基本情報」が表示されます。

- 13. 以下の項目を指定します。
 - IPアドレス

→設定しない

■IP基本情報	3
IPアドレス	 設定しない 設定する 相手側IPアドレス 自側IPアドレス

- 14. [保存] ボタンをクリックします。
- 15. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

16. 以下の項目を指定します。

- ブリッジ機能 →使用する
- グループ識別子 →0
- STP機能 →使用しない

■ブリッジ情報		3	
フリッジ機能	○使用しない ●使用する		
クループ識別子	0		
	 ● 使用しない ○ 使用する 		
STP機能	パスコスト ○ 自動決定 ○ 指定する		
	インタフェース優先度 128		

17. [保存] ボタンをクリックします。

ブリッジグループ0を設定する

- **18. 設定メニューのルータ設定で「ブリッジ情報」をクリックします。** 「ブリッジ情報」ページが表示されます。
- **19. 「ブリッジグループ情報」をクリックします**。 「ブリッジグループ情報」が表示されます。
- 20. 「ブリッジグループ情報」でグループ識別子が0の[修正]ボタンをクリックします。

IPv4ルーティング機能 →使用しない
 転送ポリシ → strict

	 ○ 使用する ③ 使用しない
0 IPv4ルーティンク機能	転送ポリシ の loose

22. [保存] ボタンをクリックします。

ブリッジグループ1に属するインタフェースを設定する

- **23. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 24. 以下の項目を指定します。
 - インタフェース →物理LAN

	<lan情報追加フィールド></lan情報追加フィールド>	
インタフェース	物理LAN 🛩	

25. [追加] ボタンをクリックします。

「LAN1情報(物理LAN)」ページが表示されます。

- **26.** 「IP 関連」をクリックします。 IP 関連の設定項目と「IP アドレス情報」が表示されます。
- 27. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する
 IPアドレス → 192.168.2.1
 ネットマスク → 24 (255.255)
 ブロードキャストアドレス → ネットワーク

→ 192.168.2.1 → 24(255.255.255.0) →ネットワークアドレス+オール1

ブ	ドキャ	ストア	ドレス	

IP アドレ	ス情報	3
IPv4	⊙使用する○使用しない	
	 ○ DHCPで自動的に取得する ○ 指定する 	
	IPアドレス	192.168.2.1
	ネットマスク	24 (255.255.255.0) 🔽
	ブロードキャストアドレ ス	ネットワークアドレス+オール1 💌

- 28. [保存] ボタンをクリックします。
- 29. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

- ブリッジ機能 →使用する
- グループ識別子 →1
- STP 機能 →使用しない

■ブリッジ情報		3	
ブリッジ機能	○使用しない ◎使用する		
クループ識別子	1		
	 ● 使用しない ○ 使用する 		
STP機能	バスコスト ○自動決定 ○指定する		
	インタフェース優先度 128		

- [保存] ボタンをクリックします。 31.
- 設定メニューのルータ設定で「相手情報」をクリックします。 32. 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。 33. 「ネットワーク情報」が表示されます。
- 34. 「ネットワーク情報」でブリッジグループ1に属する(B業務用VPC)ネットワーク名の[修正]ボ タンをクリックします。

「ネットワーク情報」ページが表示されます。

- 「IP関連」をクリックします。 35. IP関連の設定項目と「IP基本情報」が表示されます。
- 36. 以下の項目を指定します。
 - IPアドレス →設定しない

■IP基本情報	3
IPアドレス	 設定しない 設定する 相手側IPアドレス 自側IPアドレス

37. [保存] ボタンをクリックします。

38. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

- ブリッジ機能 →使用する
- グループ識別子 →1
- STP機能 →使用しない

■ブリッジ情報		3
フリッジ機能	○使用しない ⊙使用する	
クループ識別子	1	
	 ● 使用しばい ○ 使用する 	
STP機能	バスコスト ○自動決定 ○指定する	
	インタフェース優先度 128	

40. [保存] ボタンをクリックします。

ブリッジグループ1を設定する

- **41. 設定メニューのルータ設定で「ブリッジ情報」をクリックします**。 「ブリッジ情報」ページが表示されます。
- **42. 「ブリッジグループ情報」をクリックします**。 「ブリッジグループ情報」が表示されます。
- 43. 「ブリッジグループ情報」でグループ識別子が1の[修正]ボタンをクリックします。
- 44. 以下の項目を指定します。
 - IPv4 ルーティング機能
 転送ポリシ

→使用しない → strict



- 45. [保存] ボタンをクリックします。
- **46. 画面左側の[設定反映]ボタンをクリックします**。 設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。 この例では、LAN側のIPアドレス以外は、本社とすべて同じです。

2.33.3 IP トンネルで事業所間をブリッジ接続する (Ethernet over IP ブリッジ)

適用機種 Si-R220B,220C,260B,370,570

IP トンネル上でブリッジ機能を使用することにより、IP 通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

こんな事に気をつけて

- ・ ブリッジ学習テーブル生存時間は、グループ0に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1つまたは複数のリモートインタフェースとVLAN イン タフェースでだけグルーピングできます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数のLAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で定義番号がもっとも小さいLAN インタフェースでだけ以下の機能を利用できます。
 - FTP(ファームアップデートなど)
 - telnet
 - Web ブラウザによる設定
 - syslogの送信
 - SNMPエージェント、Trap送信
 - ダイナミックルーティング
- IP フレームをブリッジする場合に、転送ポリシを loose に設定したときだけ、ブリッジグループ外とルーティングが 行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使 用してください。
- ブリッジグループを複数定義する場合は、グループ識別子を0から順番に、間をあけないで設定してください。
- STPはグループ0でだけ動作するため、グループ0以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ0でループを構成するブリッジ構成を行う場合は、必ずSTPを有効にしてください。
- IPをブリッジする場合、WAN側にはブリッジで中継されるフレームだけが転送され、直接WAN側に Ethernet フレームではない IPパケットを送受信することはできません。よって、IPをブリッジする運用形態では、IPに関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- ・WAN 経由でIPをブリッジし、ルーティングを許す場合(転送ポリシがLoose)、たとえWANの先に存在するネット ワークに対する経路であっても、すべての静的経路の設定はLANインタフェース側で定義してください。ブリッジに よって相手装置のLANと本装置のLANがWAN経由で接続されているため、LAN側に経路設定を定義すれば、問題な くWANの先に存在するあて先ネットワークにブリッジで転送されて到達します。
- Ethernet over IP ブリッジの接続先に対して接続先監視を行うことができません。接続先監視の設定は行わないでください。

ここでは、本社と特定の支社との間で、IP網を経由し、IPv4以外のフレームに対してブリッジ通信を行う場合の 設定方法を説明します。



● 前提条件

• IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG(Closed Users Group)サービ スを利用する

[本社 (PPPoE 常時接続)]

- 払い出される IPv4 アドレス(LAN0 ポートに設定)
 - : 192.168.10.1/24
- PPPoEユーザ認証ID
 userid1@groupname
- PPPoE ユーザ認証パスワード : userpass1
- PPPoE LAN ポート
 LAN1 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

[支社 (PPPoE 常時接続)]

- 払い出される IPv4 アドレス(LAN0 ポートに設定)
 - : 192.168.20.1/24
- PPPoEユーザ認証 ID : userid2@groupname
- PPPoE ユーザ認証パスワード :userpass2
- PPPoE LAN ポート : LAN1 ポート使用
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

- 接続ネットワーク名 :honsya
- 接続先名 : honsya1
- 自側エンドポイントアドレス : 192.168.10.1
- 相手側エンドポイントアドレス : 192.168.20.1

[支社]

- 接続ネットワーク名 : shisya
- 接続先名 : shisya1

- ・ 自側エンドポイントアドレス
 :192.168.20.1
- 相手側エンドポイントアドレス : 192.168.10.1

[本社、支社共通]

- ブリッジ対象インタフェース : LANO ポートと IP トンネル
- IPv4の転送方式 : ルーティングで転送
- IPv6の転送方式
 ブリッジで転送

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

PPPoE 接続を設定する

1. 「1.6 インターネットへPPPoEで接続する」(P.67)を参考に、PPPoEでの接続を設定します。

IPv4 トンネルを設定する

- **2. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 4. 以下の項目を指定します。
 - ネットワーク名 → shisya

<ネットワーク情報追加フィールド>			
ネットワーク名	shisya		

- 5. 【追加】ボタンをクリックします。 「ネットワーク情報(shisya)」ページが表示されます。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

こんな事に気をつけて 「1.6 インターネットへ PPPoE で接続する」(P.67)の設定例と本設定例は、PPPoE で使用する拠点ネットワークの LAN が逆になっています。
• 接続先名

→shisya1

接続先種別 → IP トンネル接続



機種により、接続先種別の表示が上記の画面とは異なります。

8. [追加] ボタンをクリックします。

IP トンネル接続の設定項目と「基本情報」が表示されます。

9. 以下の項目を指定します。

- 自側エンドポイント → 192.168.10.1
- 相手側エンドポイント → 192.168.20.1

自側エンドボイント	192.168.10.1
相手側エンドボイント	192.168.20.1

10. [保存] ボタンをクリックします。

ブリッジグループ0に属するインタフェースを設定する

- **11. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **12.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。

13. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

14. 以下の項目を指定します。

- ブリッジ機能 →使用する
- グループ識別子 →0
- STP機能 →使用しない

■ブリッジ情報		3	
ブリッジ機能	○使用しない ●使用する		
グループ識別子	0		
	 ● 使用しない ● 使用する 		
STP機能	バスコスト ○自動決定 ○指定する		
	インタフェース優先度 128		

- 15. [保存] ボタンをクリックします。
- **16. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **17. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- **18.** 「ネットワーク情報」でIP トンネルを設定したネットワーク名(shisya)の[修正]ボタンをクリックします。

「ネットワーク情報(shisya)」ページが表示されます。

19. 「ブリッジ関連」をクリックします。 ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

- ブリッジ機能 →使用する
- グループ識別子 →0
- STP機能 →使用しない

■ブリッジ情報		?	
ブリッジ機能	○使用しない ●使用する		
グループ識別子	0		
	 ● 使用しない ● 使用する 		
STP機能	バスコスト ○ 自動決定 ○ 指定する		
	インタフェース優先度 128		

21. [保存] ボタンをクリックします。

ブリッジグループ0を設定する

- **22. 設定メニューのルータ設定で「ブリッジ情報」をクリックします**。 「ブリッジ情報」ページが表示されます。
- **23. 「ブリッジグループ情報」をクリックします**。 「ブリッジグループ情報」が表示されます。
- 24. 「ブリッジグループ情報」でグループ識別子が0の[修正]ボタンをクリックします。
- 25. 以下の項目を指定します。
 - IPv4ルーティング機能 →使用する
 - IPv6ルーティング機能 →使用しない
 転送ポリシ → strict



- 26. [保存] ボタンをクリックします。
- **27. 画面左側の [再起動] ボタンをクリックします。** 設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。 この例では、LAN側のIPアドレス、PPPoEの接続先情報(認証情報)、IPv4 トンネルのエンドポイントアドレス 以外は、本社とすべて同じです。

2.34 複数のLAN ポートをスイッチング HUBのように 使う

適用機種 Si-R220B,220C,260B,370,570

ここでは、1つのLANポートをPPPoEで使用し、残りのLANポートをスイッチングHUBのように設定してプライベートLANを構築し、インターネットを利用する例を説明します。

まず、この機能を使用する前に Si-R シリーズ 機能説明書「2.26 ブリッジ機能」(P.112)を参照して、ブリッジ グルーピングの機能と注意事項を理解してから設定してください。



こんな事に気をつけて

- パソコンのLANインタフェースと本装置の切り替えスイッチのないLANポートを接続する場合は、クロスケーブル を使って接続してください。
- IPv4やIPv6をブリッジする場合、IP 関連の定義は、ブリッジグループ内で定義番号がもっとも小さいLAN インタフェース(レイヤ3代表インタフェース)を設定してください。ブリッジグループ内では、レイヤ3代表インタフェースでだけ、レイヤ3の機能が有効になります。
- LAN ポートのリンク状態によって動作する機能(例:OSPFやVRRPなど)は、これらの機能が定義されたレイヤ3 代表インタフェースのリンク状態だけを監視して動作しています。レイヤ3代表インタェースが同期はずれを起こし、 これ機能が代表インタフェースへの出力を止めた場合、同じグループ内のほかのポートからも、これの機能が出力す るパケットが出なくなります。よって、リンク状態をみて動作する機能は、レイヤ3代表インタフェースのLAN ポー トだけを使用してください。

「1.6 インターネットへ PPPoE で接続する」(P.67)の設定が終了し、以下のとおりに設定されていることを前提 とします。

● 参照 Si-Rシリーズ 機能説明書「2.26 ブリッジ機能」(P.112)

● 前提条件

- プライベートLAN側のネットワーク : 192.168.1.0/24
- レイヤ3代表インタフェース : LAN1

● 設定条件

- LAN1、LAN2、LAN3をグルーピングして、スイッチングHUBのように利用して、プライベートLAN側に使用する
- IPv4をブリッジ対象とする
- プライベートLAN側のブリッジグループとインターネット側の間のルーティングを許可する

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチング HUB のように利用する LAN インタフェースを設定する

1. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 以下の項目を指定します。

インタフェース →物理LAN

<lan情報追加フィールド></lan情報追加フィールド>	
インタフェース	物理LAN 🖌

3. [追加] ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

- 「ブリッジ関連」をクリックします。
 ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。
- 5. 以下の項目を指定します。
 - ブリッジ機能 →使用する
 - グループ識別子 →0
 - STP機能 →使用しない



- 6. [保存] ボタンをクリックします。
- 7. 手順1.~6.を参考にして、LAN2、LAN3を設定します。

ブリッジグループ0を設定する

- 8. 設定メニューのルータ設定で「ブリッジ情報」をクリックします。 「ブリッジ情報」ページが表示されます。
- 「ブリッジグループ情報」をクリックします。
 「ブリッジグループ情報」が表示されます。
- 10. 「ブリッジグループ情報」でグループ識別子が0の[修正]ボタンをクリックします。

11. 以下の項目を指定します。

- IPv4ルーティング機能 →使用しない 転送ポリシ → loose
 IPv6ルーティング機能 →使用しない
- 転送ポリシ → loose

	IPv4ルーティング機能	 ● 使用する ● 使用けない 転送ポリシ ○strict ● loose
U	IPv6ルーティング機能	 ○ 使用する ● 使用しない 転送ボリシ ○strict ● loose

- 12. [保存] ボタンをクリックします。
- **13. 画面左側の [再起動] ボタンをクリックします**。 設定した内容が有効になります。

2.35 ATM 網を使う

適用機種 Si-R260B,370,570

ここでは、ATM 網を利用して複数の事業所のネットワークを接続し、複数の VPC を使用する場合と VPC と VCC の同時シェーピングを使用する場合の設定方法を説明します。

2.35.1 事業所ごとに別の VPC を使用する

適用機種 Si-R260B,370,570



● 設定条件

[本社]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース (Si-R260B の場合) で ATM 網を使用する
- LAN側のIPアドレス : 192.168.1.1/24 (LAN0)
- 事業所A向けネットワーク名 : JigyoA
- 事業所A向け接続先名
 jigyo-a
- 事業所A向けVPI/VCI : 0/80
- 事業所A向けVP速度 :6Mbps
- 事業所B向けネットワーク名 : JigyoB
- 事業所B向け接続先名
 jigyo-b
- 事業所B向けVPI/VCI : 1/81
- 事業所B向けVP速度 :4Mbps

[事業所A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース (Si-R260B の場合) で ATM 網を使用する
- LAN側のIPアドレス : 192.168.101.1/24 (LAN0)
- ネットワーク名 :Honsya
- 接続先名 : : honsya-1
- VPI/VCI : 0/81
- VP速度 :6Mbps

[事業所 B]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース (Si-R260B の場合) で ATM 網を使用する
- LAN側IPアドレス : 192.168.102.1/24 (LAN0)
- ネットワーク名
 Honsya
- 接続先名 : honsya-2
- VPI/VCI : 0/82
- VP速度 :4Mbps

こんな事に気をつけて

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

拡張モジュール	注意点	
ATM25M / ATM155M 拡張モジュール12	 VP / VC 速度を設定する場合は、64Kbps ~ 25Mbps の範囲で8Kbps または50Kbps 刻み で指定します。 	
	 VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 VPCが 1VPCの場合にだけ、VP シェーピングとVC シェーピングを同時に利用することができます。 VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モンド・サークアンドに利用するエントはエキナサイ 	
	 ・ 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 ・ 複数 VPCで VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるように ネットワークを設計してください。このとき、16VPC まで利用することができます。 - VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービ スタイプを CBR に設定してください。 	
	 VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 	
	 VP シェーピング時は、VC 速度(CBR、GFR+)、平均速度(SCR)および最低速度(UBR+)の総和がVP 速度を超えないようにように設定してください。 VC シェーピング時は、VC 速度(CBR、GFR+)、平均速度(SCR)および最低速度(UBR+)の総和が25Mbpsを超えないようにように設定してください。 	
ATM25M 拡張モジュールH1	 VP / VC速度を設定する場合は、以下の設定範囲で設定してください。 64Kbps ~ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 VP シェービングを前提とした運用を本装置で行う場合は、以下のように設定してください。 VP 速度の総和を 25Mbps 以下に設定してください。 1-VPC での VP / VC シェービング時以外で、サービスタイブUBR+ は設定できません。複数 VPC での VP / VC シェーピング時は VBR を設定してください。 サービスタイブが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 サービスタイブが CBR の場合は、VC速度の総和が VP 速度を超えないように設定してください。 サービスタイブが UBR+の場合は、最低速度の総和が VP 速度を超えないように設定してください。 サービスタイブが GFR+の場合は、VC速度の総和が VP 速度を超えないように設定してください。 VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュールので同時に利用することはできません。 	

拡張モジュール	注意点
ATM155M	VP / VC 速度を設定する場合は、以下の設定範囲で設定してください。
拡張モジュールH1	- VP速度は、200Kbps~50Mbpsの範囲で8Kbpsまたは50Kbps刻みで指定できます。
	- VC速度は、64Kbps~100Mbpsの範囲で8Kbpsまたは50Kbps刻みで指定できます。
	・ VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。
	- VP速度の総和を 50Mbps 以下に設定してください。
	- 1-VPCでのVP/VCシェーピング時以外ではサービスタイプUBR+は設定できませ
	ん。複数 VPC での VP / VC シェーピング時は VBR を設定してください。
	- サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定し
	てください。
	- サービスタイプがCBRの場合は、VC速度の総和がVP速度を超えないように設定して
	ください。
	- サービスタイプが UBR+の場合は、最低速度の総和が VP 速度を超えないように設定し
	てください。
	- サービスタイフがGFR+の場合は、VC速度の総和がVP速度を超えないように設定し
	しくにさい。
	- VPジェービングを行うVPCとVPジェービングを行わないVPCは、同一払張モ
	ジュール内で同時に利用することはできません。
	 DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にして
	ください。
	atm <slot> send clock recovery</slot>

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

VPCの情報を設定する

設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 回線インタフェース → ATM

<wan情報追加フィールド></wan情報追加フィールド>			
回線インタフェース		ATM	~

- 【追加】ボタンをクリックします。
 「WAN0情報(ATM)」ページが表示されます。
- **4. 「基本情報」をクリックします。** 「基本情報」が表示されます。

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

■基本情報	3	
ボート	スロット0-0 🗸	
VPI	0	
VP速度	 ● 指定しない ● 指定する Mbps ▼ 	
OAM(F4)	●受け付けない●受け付ける	

6. [保存] ボタンをクリックします。

- 7. 手順1.~6.を参考に、以下の項目を指定します。
 - 回線インタフェース →ATM
 - 「WAN1情報 (ATM)」-「基本情報」
 - ポート →スロット0-0
 - VPI **→**0
 - VP 速度 →指定しない
 - OAM (F4) →受け付けない

本装置のIPアドレスを設定する

- 8. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN情報」ページが表示されます。
- 9. 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP関連」をクリックします。 10. IP関連の設定項目と「IPアドレス情報」が表示されます。
- 11. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する IPアドレス → 192.168.1.1 ネットマスク →24 (255.255.255.0) ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレ	レス情報	3	
IPv4	●使用する●使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス I92.168.1.1 ネットマスク 24 (255.255.255.0 ブロードキャストアドレ ス ネットワークアドレン) 、 ス+オール1 、	

12. [保存] ボタンをクリックします。

事業所A向けの情報を設定する

- **13. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **14. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 15. 以下の項目を指定します。
 - ネットワーク名

<ネットワーク情報追加フィールド>		
ネットワーク名		Jigyo A

→ JigyoA

- **16. [追加] ボタンをクリックします**。 「ネットワーク情報(JigyoA)」ページが表示されます。
- 17. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

- 18. 以下の項目を指定します。
 - 接続先名 接続先種別
 - VCI

→ATM 接続 →80

→jigyo-a



Si-R260Bでは、接続先種別の表示が上記の画面とは異なります。

19. [追加] ボタンをクリックします。

ATM接続の設定項目と「基本情報」が表示されます。

○別インタフェースから送出
 ○MPLSトンネル接続
 ○パケット破棄

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

使用インタフェース	WANO 🕶	
VCI	80	
VC速度	6 Mbps 🗸	
サービスタイプ	 ● CBR ● VBR 平均速度値 ▲大パースト長 ● UBR+ 最低速度値 Kbps ♥ ● GFR+ 保証速度値 Kbps ♥ 	
OAM(F5)	●受け付けない ●受け付ける	

- 21. [保存] ボタンをクリックします。
- **22. 画面上部の「ネットワーク情報(JigyoA)をクリックします**。 「ネットワーク情報(JigyoA)」が表示されます。
- **23.** 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

24. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

25. 以下の項目を指定します。

- ネットワーク
 →ネットワーク指定
 あて先IPアドレス
 →192.168.101.0
 →24 (255.255.255.0)
- メトリック値 →1
- 優先度 →0



26. [追加] ボタンをクリックします。

事業所B向けの情報を設定する

27. 手順 13.~26.を参考に、以下の項目を指定します。

「ネッ	トワ-	ーク情報」
-----	-----	-------

 ネットワーク名 	→JigyoB
「接続先情報」	
● 接続先名	→ jigyo-b
● 接続先種別	→ ATM 接続
VCI	→81
「基本情報」	
• 使用インタフェース	→WAN1
• VCI	→81
• VC 速度	→4Mbps
 サービスタイプ 	→CBR
• OAM (F5)	→受け付けない
「スタティック経路情報」	
• ネットワーク	→ネットワーク指定
あて先 IP アドレス	→192.168.102.0
あて先アドレスマスク	→24 (255.255.255.0)
• メトリック値	→1
• 優先度	→0

28. 画面左側の [再起動] ボタンをクリックします。

設定した内容が有効になります。

事業所Aを設定する

「本社を設定する」を参考に、事業所Aを設定します。

VPCの情報を設定する

「WAN0 情報」

•	回線インタフェース	→ATM
۲ł	基本情報」	
•	ポート	→スロット0-0
•	VPI	→ 0
•	VP速度	→指定しない
•	OAM (F4)	→受け付けない

本装置のIPアドレスを設定する

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

•	IPv4	→使用する
•	IPアドレス	→指定する
	IPアドレス	→ 192.168.101.1
	ネットマスク	→24 (255.255.255.0)
	ブロードキャストアドレス	→ネットワークアドレス+オール1

本社向けの情報を設定する

邤框	「相手情報」-「ネットワーク情報」			
•	ネットワーク名	→Honsya		
「ネ	、ットワーク情報」-「接続先情報」	J		
•	接続先名	→honsya-1		
•	接続先種別	→ ATM 接続		
	VCI	→81		
「接	そ続先情報」-「ATM 接続」			
「基	「本情報」			
•	使用インタフェース	→WAN0		
•	VCI	→81		
•	VC速度	→6Mbps		
•	サービスタイプ	→CBR		
•	OAM (F5)	→受け付けない		
「ネ	、ットワーク情報」-「IP 関連」			
「ス	、タティック経路情報」			
•	ネットワーク	→デフォルトルート		
•	メトリック値	→ 1		
•	優先度	→ 0		

事業所Bを設定する

「本社を設定する」を参考に、事業所Bを設定します。

VPCの情報を設定する

「WAN0 情報」

•	回線インタフェース	→ATM
۲ł	基本情報」	
•	ポート	→スロット0-0
•	VPI	→ 0
•	VP速度	→指定しない
•	OAM (F4)	→受け付けない

本装置のIPアドレスを設定する

「LAN0 情報」-「IP 関連」 「IP アドレス情報」

•	IPv4	→使用する
•	IPアドレス	→指定する
	IPアドレス	→192.168.102.1
	ネットマスク	→24 (255.255.255.0)
	ブロードキャストアドレス	→ネットワークアドレス+オール1

本社向けの情報を設定する

「相手情報」-「ネットワーク情報」		
• ネット	フーク名	→Honsya
「ネットワ	ーク情報」-「接続先情報」	J
● 接続先年	名	→honsya-1
 接続先和 	重別	→ ATM 接続
VCI		→82
「接続先情報	報」-「ATM 接続」	
「基本情報」	J	
• 使用イン	ンタフェース	→WAN0
• VCI		→ 82
• VC 速度	-	→4Mbps
 サービス 	スタイプ	→CBR
• OAM ((F5)	→受け付けない
「ネットワ	ーク情報」-「IP 関連」	
「スタティ	ック経路情報」	
• ネット!	フーク	→デフォルトルート
 メトリ 	ック値	→ 1
• 優先度		→ 0

2.35.2 VPCとVCCの同時シェーピングを使用する

適用機種

Si-R260B,370,570



● 設定条件

[本社]

•	slot0に実装されたATM25MまたはATM155M拡張モジュールL2、	または本装置に内蔵の ATM インタフェー
	ス(Si-R260Bの場合)でATM 網を使用する	

- IPv4アドレス :192.168.1.1/24(LAN0)
- IPv4通信向けネットワーク名 : JigyoA1
- IPv4 通信向け接続先名 ijigyoa-1
- IPv4通信向けVPI/VCI : 0/80
- IPv6アドレス :2001:db8:1111:1000::/64(LAN0)
- IPv6通信向けネットワーク名 : JigyoA2
- IPv6 通信向け接続先名 : jigyoa-2
- IPv6通信向けVPI/VCI : 0/81
- VP速度 :8Mbps
- IPv4 通信向けサービスタイプ :VBR(VC 速度:6Mbps、平均速度:5Mbps)
- IPv6通信向けサービスタイプ : UBR+ (VC速度:5Mbps、最低速度:3Mbps)

[事業所A]

- slot0 に実装された ATM25M または ATM155M 拡張モジュール L2、または本装置に内蔵の ATM インタフェース (Si-R260B の場合) で ATM 網を使用する
- IPv4アドレス : 192.168.2.1/24 (LAN0)
- IPv4 通信向けネットワーク名 :Honsya1
- IPv4 通信向け接続先名 : honsya-1
- IPv4 通信向け VPI/VCI : 0/82
- IPv6アドレス : 2001:db8:1111:1001::/64 (LAN0)
- IPv6 通信向けネットワーク名 :Honsya2
- IPv6通信向け接続先名 : honsya-2
- IPv6通信向けVPI/VCI : 0/83
- VP速度 :8Mbps

- IPv4 通信向けサービスタイプ
- :VBR(VC速度:6Mbps、平均速度:5Mbps)
- IPv6通信向けサービスタイプ : UBR+(VC速度:5Mbps、最低速度:3Mbps)

こんな事に気をつけて

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

拡張モジュール	注意点
<mark>拡張モジュール</mark> ATM25M ∕ ATM155M 拡張モジュールL2	 注意点 VP / VC速度を設定する場合は、64Kbps ~ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。 VPC が 1VPC の場合にだけ、VP シェーピングとVC シェーピングを同時に利用することができます。 VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPCまで利用することができます。 VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。 VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。 VP シェーピング時は、VC 速度(CBR、GFR+)、平均速度(SCR) および最低速度
	(UBR+)の総和がVP速度を超えないようにように設定してください。 ・ VCシェーピング時は、VC速度(CBR、GFR+)、平均速度(SCR)および最低速度 (UBR+)の総和が25Mbpsを超えないようにように設定してください。
ATM25M 拡張モジュールH1	 VP / VC速度を設定する場合は、以下の設定範囲で設定してください。 64Kbps ~ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。 VP シェービングを前提とした運用を本装置で行う場合は、以下のように設定してください。 VP 速度の総和を 25Mbps 以下に設定してください。 1-VPCでの VP / VC シェービング時以外で、サービスタイプUBR+は設定できません。複数 VPCでの VP / VC シェーピング時は VBRを設定してください。 サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。 サービスタイプが CBR の場合は、VC速度の総和が VP 速度を超えないように設定してください。 サービスタイプが UBR+の場合は、最低速度の総和が VP 速度を超えないように設定してください。 サービスタイプが GFR+の場合は、VC速度の総和が VP 速度を超えないように設定してください。 ソービスタイプが GFR+の場合は、VC速度の総和が VP 速度を超えないように設定してください。 マイださい。 ソービスタイプが GFR+の場合は、VC速度の総和が VP 速度を超えないように設定してください。

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

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

VPCの情報を設定する

設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 回線インタフェース → ATM

<wan情報追加フィールド></wan情報追加フィールド>			
回線インタフェース		ATM	~

- 【追加】ボタンをクリックします。
 「WAN0情報(ATM)」ページが表示されます。
- **4. 「基本情報」をクリックします。** 「基本情報」が表示されます。

• OAM (F4)

ポート →スロット0-0
 VPI →0
 VP速度 →1指定する →8Mbps

■基本情報	3
ボート	スロット0-0 🖌
VPI	0
VP速度	 ● 指定しない ● 指定する 8 Mbps ▼
OAM(F4)	●受け付けない●受け付ける

→受け付けない

6. [保存] ボタンをクリックします。

LAN情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。
 「LAN 情報」ページが表示されます。
- 8. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 9. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

10. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス
 IPアドレス
 ネットマスク
 ブロードキャストアドレス
- →指定する →192.168.1.1 →24(255.255.255.0)

ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報							
IPv4	⊙使用する○使用しない						
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス I92.168.1.1 ネットマスク 24 0255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 						

- 11. 【保存】ボタンをクリックします。
- 12. 「IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

• ルータ広報

- IPv6 →使用する
 インタフェースID →自動
 IPv6アドレス
 アドレスまたはプレフィックス → 2001:db8:1111:1000::
 Valid Lifetime → 30 日
 Pref. Lifetime → 7 日
 フラグ → c0
- IP√6基本情報 3 IPv6 ○使用しない ⊙使用する **イノ** ⊙自動 タフ ○指定する ı-スID Valid Lifetime Pref. Lifetime ne フラ 無期限 グ アドレスまたはプレフィックス 無期限 期限有 期限有 IPv6 2001:db8:1111:1000:: 8 🖌 🗖 7 🗄 🔽 🗖 c0 30 アド 8 🖌 🗌 7 🗄 🔽 🖸 c0 30 レス 30 8 🖌 🗖 7 🗄 🔽 🗖 c0 8 💌 🗖 7 8 🔽 🗖 c0 30 ○送信しない 送信する 最大送信間隔 600 秒 最小送信間隔 200 秒 Router Lifetime 1800 秒 ルー タ広 MTU 報 ミリ秒 Reachable Time 0 ミリ秒 Retrans Timer 0 Cur Hop Limit 64 フラグ 00

→送信する

14. [保存] ボタンをクリックします。

IPv4の相手情報を設定する

- **15. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **16. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 17. 以下の項目を指定します。

ネットワーク名 → JigyoA-1

<ネットワーク情報追加フィールド>					
ネットワーク名	Jigyo A-1				

18. [追加] ボタンをクリックします。

「ネットワーク情報(JigyoA-1)」ページが表示されます。

19. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

20. 以下の項目を指定します。

- 接続先名 →jigyoa-1
- 接続先種別 → ATM 接続
 VCI → 80



Si-R260Bでは、接続先種別の表示が上記の画面とは異なります。

21. [追加] ボタンをクリックします。

ATM接続の設定項目と「基本情報」が表示されます。

22. 以下の項目を指定します。

- 使用インタフェース → WAN0
 VCI → 80
 VC速度 → 6Mbps
 サービスタイプ → VBR 平均速度値 → 5Mbps
- 最大バースト長 → 32
- OAM (F5) →受け付けない

使用インタフェース	WAND V					
VCI	80					
VC速度	6 Mbps 🗸					
サービスタイプ	 ○ CBR ○ VBR 平均速度値 5 Mbps ♥ 最大バースト長 32 ○ UBR+ 最低速度値 Kbps ♥ ○ GFR+ 保証速度値 Kbps ♥ 					
OAM(F5)	⊙受け付けない ○受け付ける					

- 23. [保存] ボタンをクリックします。
- **24. 画面上部の「ネットワーク情報(JigyoA-1)をクリックします**。 「ネットワーク情報(JigyoA-1)」が表示されます。
- **25.** 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

26. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

27. 以下の項目を指定します。

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

● 優先度 →0



28. [追加] ボタンをクリックします。

IPv6の相手情報を設定する

- **29. 画面上部の「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **30.** 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。

ネットワーク名

→ JigyoA-2

<ネットワーク情報追加フィールド>					
ネットワーク名	Jigyo A-2				

32. [追加] ボタンをクリックします。

「ネットワーク情報(JigyoA-2)」ページが表示されます。

33. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

34. 以下の項目を指定します。

- 接続先名 →jigyoa-2
- 接続先種別 → ATM 接続
 VCI → 81

Si-R260Bでは、接続先種別の表示が上記の画面とは異なります。

35. [追加] ボタンをクリックします。

ATM接続の設定項目と「基本情報」が表示されます。

- 使用インタフェース → WAN0
 VCI → 81
 VC速度 → 5Mbps
- サービスタイプ → UBR+ 最低速度値 → 3Mbps
- OAM (F5) →受け付けない

使用インタフェース	WANO 💌
VCI	81
VC速度	5 Mbps 🕶
サービスタイプ	 ○ CBR ○ VBR 平均速度値 ▲大バースト長 ④ UBR+ 最低速度値 3 Mbps ♥ ○ GFR+ (保証速度値 Kbps ♥)
OAM(F5)	●受け付けない ●受け付ける

- 37. [保存] ボタンをクリックします。
- **38. 画面上部の「ネットワーク情報(JigyoA-2)をクリックします**。 「ネットワーク情報(JigyoA-2)」が表示されます。
- **39. 「**IPv6 関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

•	IPv6	→使用する
•	インタフェースID	→自動
•	IPv6アドレス	→指定しない

ルータ広報 →送信しない

■IPv6基本情報													
IPv6	○使用しない ◎使用する												
インタフェースID	 ● 自動 ○ 指定する 												
	אק	レスまたはプレフ	ィックス		Valic 期限	l Life 阴	time ‡	無期	限	Pref. Life 期限有	etime 魚	無期限	フラ グ
IPv6					30		Β	*		7	B	~	c0
アトレス					30		8	۷		7	B	v	c0
					30		Β	۷		7	B	~	c0
					30		Β	¥		7	B	¥	cO
	() ()	送信しない 送信する											
		最大送信間隔	600	Ŧ	沙								
		最小送信間隔	200	Į₹	少								
ルー		Router Lifetime	1800	Ŧ	沙								
タ広報		MTU]									
тк		Reachable Time	0	3	ジシションションションションションションションションションションションションション								
		Retrans Timer	0	3	ジシションションションションションションションションションションションションション								
		Cur Hop Limit	64										
		フラグ	00										

- 41. [保存] ボタンをクリックします。
- **42.** IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。 「IPv6 スタティック経路情報」が表示されます。
- 43. 以下の項目を指定します。
 - ネットワーク
 →ネットワーク指定
 あて先プレフィックス/プレフィックス長
 →2001:db8:1111:1001::/64
 - メトリック値

→ 1

<ipv6スタティック経路情報入力フィールド></ipv6スタティック経路情報入力フィールド>						
ネットワーク	 デフォルトルート ネットワーク指定 あて先プレフィ ックス/ブレフ ィックス長 64 					
メトリック値	1 💌					

- 44. [追加] ボタンをクリックします。
- **45. 画面左側の [再起動] ボタンをクリックします**。 設定した内容が有効になります。

事業所Aを設定する

「本社を設定する」を参考に、事業所Aを設定します。

VPCの情報を設定する

「WAN0 情報」

٠	回線インタフェース	→ATM						
۲ł	「基本情報」							
•	ポート	→スロット0-0						
•	VPI	→ 0						
•	VP速度	→8Mbps						
•	OAM (F4)	→受け付けない						

LAN情報を設定する

「LAN0情報」-「IP 関連」 「IPアドレス情報」 • IPv4 →使用する

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

「LAN0情報」-「IPv6関連」 「IPv6基本情報」

IPv6

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

IPv4の相手情報を設定する

「相手情報」-「ネットワーク情報」

•	ネットワーク名	→Honsya-1			
۲đ	「ネットワーク情報」-「接続先情報」				
•	接続先名	→honsya-1			
•	接続先種別	→ATM 接続			
	VCI	→82			

「接続先情報」-「ATM 接続」

「基本情報」	
• 使用インタフェース	→WAN0
• VCI	→ 82
• VC 速度	→6Mbps
• サービスタイプ	→VBR
平均速度值	→5Mbps
最大バースト長	→ 32
• OAM (F5)	→受け付けない
「ネットワーク情報」-「IP 関連」	
「スタティック経路情報」	
• ネットワーク	→ネットワーク指定
あて先IPアドレス	→ 192.168.1.0
あて先アドレスマスク	→24 (255.255.255.0)
• メトリック値	→ 1
● 優先度	→0

IPv6の相手情報を設定する

「相手情報」-「ネットワーク情報」				
 ネットワーク名 	→Honsya-2			
「ネットワーク情報」-「接続先情報」	I			
● 接続先名	→honsya-2			
● 接続先種別	→ ATM 接続			
VCI	→83			
「接続先情報」-「ATM接続」				
「基本情報」				
• 使用インタフェース	→WAN0			
• VCI	→83			
• VC 速度	→5Mbps			
• サービスタイプ	→UBR+			
最低速度值	→3Mbps			
• OAM (F5)	→受け付けない			
「ネットワーク情報」-「IPv6関連」				
「IPv6基本情報」				
• IPv6	→使用する			
• インタフェースID	→自動			
・ IPv6アドレス	→指定しない			
• ルータ広報	→送信しない			
「IPv6スタティック経路情報」				
• ネットワーク	→ネットワーク指定			
 あて先プレフィックス/プレフィ 	ックス長 →2001:db8:1111:1000::/64			
• メトリック値	→ 1			

2.36 ISDN 接続を契機とした通信バックアップを使う

適用機種 Si-R220B,220C,370,570

マスタ回線側で経路制御ができなくても、バックアップ回線である ISDN 回線の接続状態によって、通信をバックアップ側に切り替えることができます。



- 設定条件
- センタ側は、本装置以外の装置は設定が完了済み
- センタ側の 192.168.254.0/24 に接続されたそれぞれのルータは、本装置が広報する経路が選択されるように 設定されている
- センタから拠点への発信は行わない
- 拠点側本装置は、ISDN 接続の設定以外は設定が完了済み

上記の設定条件に従って設定を行う場合の設定例を示します。

センタ側本装置を設定する

- **1. 設定メニューのルータ設定で「WAN 情報」をクリックします**。 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース → ISDN

 <WAN情報追加フィールド>

 回線インタフェース

3. [追加]ボタンをクリックします。

「WAN0 情報(ISDN)」ページが表示されます。

4. 「基本情報」をクリックします。 「基本情報」が表示されます。

- ポート →スロット0-0

■基本情報	3
ボート	スロット 0-0 💌
自動接続	⊙すべて禁止 ○相手毎に設定

- 6. [保存] ボタンをクリックします。
- 7. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

- 8. 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 9. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

10. 以下の項目を指定します。

• IPv4

→使用する

IPアドレス
 IPアドレス
 ネットマスク
 ブロードキャストアドレス

→指定する →192.168.254.128 →24(255.255.255.0) →ネットワークアドレス+オール1

3

IPアドレス 情報	
v4	●使用する ○使用しない

IPv4	⊙使用する○使用しない
	 ○ DHCPで自動的に取得する ○ 指定する
ד, ואקסז	IPアドレス 192.168.254.128
	ネットマスク 24 (255.255.2) マ
	ブロードキャストアドレ ス ネットワークアドレス+オール1

11. [保存] ボタンをクリックします。

12. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP情報」が表示されます。

- 13. 以下の項目を指定します。
 - RIP送信

→V2(Multicast)で送信する

● RIP受信 → V2、V2 (Multicast) で受信する

RIP情報	3
RIP送信	 ○送信しない ○V1で送信する ○V2で送信する ⊙V2(Multicast)で送信する
RIP受信	○受信しない ○V1で受信する ⊙V2、V2(Multicast)で受信する

14. [保存] ボタンをクリックします。

15. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

- **16.** 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。
- 17. 以下の項目を指定します。・ ネットワーク名

```
<ネットワーク情報追加フィールド>
ネットワーク名 kyoten
```

→ kyoten

18. [追加] ボタンをクリックします。

「ネットワーク情報(kyoten)」ページが表示されます。

- **19. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- **20.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 21. 以下の項目を指定します。
 - ネットワーク あて先IPアドレス あて先アドレスマスク

→ネットワーク指定
→ 192.168.1.0
→ 24 (255.255.255.0)

<スタティック経路情報入力フィールド>			
ナットローク	 ○ デフォルトルート ③ ネットワーク指定 		
ホットワーク	あて先IPアドレス 192.168.1.0 あて先アドレスマスク 24 (255.255.255.0) V		

- 22. [追加] ボタンをクリックします。
- 23. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

 接続先名 → kyoten
 接続先種別 → ISDN 接続 →通常接続

電話番号

→1234



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

25. [追加] ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

26. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

27. 以下の項目を指定します。

● 受諾認証情報
 認証 ID → kyoten
 認証パスワード → kyotenpass

受諾國証	認証ID	kyoten	
情報	認証バスワー ド	•••••	

- 28. [保存] ボタンをクリックします。
- **29. 画面左側の [再起動] ボタンをクリックします**。 設定した内容が有効になります。

拠点側本装置を設定する

- 設定メニューのルータ設定で「相手情報」をクリックします。
 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 3. 以下の項目を指定します。
 - ネットワーク名 → center



- **4. [追加] ボタンをクリックします**。 「ネットワーク情報 (center)」ページが表示されます。
- 5. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

- 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 7. 以下の項目を指定します。
 - ネットワーク

→デフォルトルート



- 8. [追加] ボタンをクリックします。
- 「接続先情報」をクリックします。
 「接続先情報」が表示されます。

接続先名 → center
 接続先種別 → ISDN 接続
 →通常接続

ダイヤル1 電話番号

→5678



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

11. [追加] ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

12. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

13. 以下の項目を指定します。

・ 送信認証情報
 認証 ID
 → kyoten
 認証パスワード
 → kyotenpass

送信國証	認証ID	kyoten	
情報	認証バスワー ド	••••••	

- 14. [保存] ボタンをクリックします。
- **15.** ISDN 接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 16. 以下の項目を指定します。
 - 無通信監視タイマ →送信パケットのみについて60秒

無通信監 視タイマ 送信パケットのみ ▼ について 60 秒

- 17. [保存] ボタンをクリックします。
- **18. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.37 外部のパソコンから PIAFS 接続する

適用機種 Si-R220B,220C,370

ここでは、PIAFS対応のPHSを使用して外部のパソコンから本装置へ着信接続する例を説明します。接続先のパ ソコンの設定に関する説明は省略しています。

こんな事に気をつけて

- ・ 本装置の PIAFS 接続は PIAFS 1.0/2.0/2.1 に対応します。
- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順 どおり設定しても通信できないことがあります。
 - 参照 Si-R シリーズ トラブルシューティング [5 ご購入時の状態に戻すには」(P.52)
- ・ 文字入力フィールドでは、半角文字(0~9、A~Z、a~z、および記号)だけを使用してください。ただし、空白 文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。
 - 参照 Si-Rシリーズ Web ユーザーズガイド「1.7 文字入力フィールドで入力できる文字一覧」(P.19)

本装置のLAN側のネットワークと同じネットワークアドレスを別ネットワークのパソコンに割り当てること によって、Proxy ARPが自動的に動作し、ISDN回線経由で接続されたパソコンがLAN上に存在するように扱 えます。



◆ Proxy ARP とは

Ethernet上で通信する場合、相手を識別するためにMACアドレスが使用されます。このとき、IPアドレスと MACアドレスの対応付けを行う手段としてARP(Address Resolution Protocol)が使用されます。

ブロードキャストでARP要求を発行すると、LAN上で自分のIPアドレスに関連するARP要求であると認識したパソコンは、自分のMACアドレスを送り返します。

Proxy ARPとは、パソコンから送られてくる ARP 要求に対して、実際のパソコンの代わりに応答する機能です。


● 設定条件

- SLOT0に装着したBRI拡張モジュールL2(Si-R370)またはISDNUポート(Si-R220B、220C)を使用して ISDN回線に接続する
- 本装置のLAN側のネットワークアドレス/ネットマスク

: 192.168.1.0/24

[PC0 (ノートパソコン+ PHS) と接続する条件]

- 接続先ネットワーク名 : pc0
- 接続先名 : phs0
- 割り当てIPアドレス : 192.168.1.34
- 電話番号 : 070-1234-5678
- 受諾認証 ID : mobileid
- 受諾認証パスワード : mobilepass

[PC1 (ノートパソコン+ PHS) と接続する条件]

- 接続先ネットワーク名 :pc1
- 接続先名 : phs1
- 割り当てIPアドレス : 192.168.1.35
- 電話番号 : 070-1234-5679
- 受諾認証 ID : mobileid
- 受諾認証パスワード : mobilepass

上記の設定条件に従って設定を行う場合の設定例を示します。

回線情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース → ISDN

 <WAN情報追加フィールド>

 回線インタフェース

 ISDN

【追加】ボタンをクリックします。
 「WAN0情報(ISDN)」ページが表示されます。

LAN情報を設定する

- **4. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 5. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。

6. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

7. 以下の項目を指定します。

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

■IPアドレス情報			
IPv4	●使用する●使用しない		
IP アド レス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス I92.168.1.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オ 	-161 🗸	

8. [保存] ボタンをクリックします。

接続先情報(PC0)を設定する

- **9. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **10. 「ネットワーク情報」をクリックします**。 「ネットワーク情報」が表示されます。
- 11. 以下の項目を指定します。
 - ネットワーク名 → pc0

<ネットワーク情報追加フィールド>		
ネットワーク名	pc0	

12. [追加] ボタンをクリックします。

「ネットワーク情報 (pc0)」ページが表示されます。

- **13. 「共通情報」をクリックします。** 共通情報の設定項目と「基本情報」が表示されます。
- 14. 以下の項目を指定します。

自動接続 ○する ●しない

必要に応じて上記以外の項目を指定します。

- 15. [保存] ボタンをクリックします。
- **16. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。

•	IPアドレス	→設定する
	相手側IPアドレス	→ 192.168.1.34
	自側IPアドレス	→ 192.168.1.1

■IP基本情報		3
IPアドレス	 ○ 設定しない ○ 設定する 	1

18. [保存] ボタンをクリックします。

19. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

20. 以下の項目を指定します。

- 接続先名 → phs0
- 接続先種別 → ISDN 接続 ダイヤル1 電話番号 → 070-1234-5678

<接続先情報追加フィールド>		
接続先名	phs0	
接続先種別	 専用線接続 ISDN接続 ダイヤル1 電話番号 070-1234-5678 サブアドレス フレームリレー接続 DLCI モデム接続 ダイヤル1 電話番号 PPPoE接続 IPトンネル接続 IPsec/IKE接続 別インタフェースから送出 MPLSトンネル接続 バケット破棄 	

Si-R370では、接続先種別の表示が上記の画面とは異なります。

21. [追加] ボタンをクリックします。

ISDN 接続の設定項目と「基本情報」が表示されます。

22. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

•	認証方式	→ PAP、CHAP
•	送信認証情報	→設定しない
•	受諾認証情報 認証 ID	→mobileid
	認証パスワード	→ mobilepass
•	MP接続	→しない

PPP情:	報	
認証方式		
送信認証 情報	 認証ID 認証バスワード 	
受諾認証 情報	認証ID mobileid 認証バスワー ド ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	
MP接続	 ● しない ● する BAP/BACP利用 ●しない ● する ※ 発信者番号による識別で番号をチェックしない場合は着信相手識別 情報の設定が有効 	

24. [保存] ボタンをクリックします。

接続先情報(PC1)を設定する

サブアドレス

25. 「接続先情報 (PC0) を設定する」を参考に、以下の項目を指定します。

「相手情報」-「ネットワーク情報」

```
    ネットワーク名

                      →pc1
「ネットワーク情報」-「共通情報」
「基本情報」
• 自動接続
                      →しない
「ネットワーク情報」-「IP 関連」
「IP 基本情報」
• IPアドレス
                      →設定する
  相手側IPアドレス
                      → 192.168.1.35
 自側IPアドレス
                      → 192.168.1.1
  必要に応じて上記以外の項目を設定します。
「ネットワーク情報」-「接続先情報」

    接続先名

                      →phs1
• 接続先種別
                      →ISDN 接続
 ダイヤル1
  電話番号
                      →070-1234-5679
```

→設定しない

「接続先情報」-「ISDN接続」 「PPP情報」

- 認証方式 → PAP、CHAP
- 送信認証情報 →設定しない
- 受諾認証情報
 認証 ID → mobileid
 認証パスワード → mobilepass
- MP接続 →しない

26. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.38 アナログモデムで通信バックアップをする

適用機種 Si-R220B,220C

本装置の COM ポートに外付けのアナログモデムを接続することによって、アナログ回線を使用して通信することができます。

ここでは、営業所間をIP-VPN網で接続し、IP-VPN網側の通信が通信不能になった場合にアナログ回線側で通信 バックアップする場合を例に説明します。

この例では、BGP 経路よって優先度の低いスタティックルートをバックアップ回線側に設定します。メインの IP-VPN 側が通信不能になって BGP セッションが切断され、相手拠点の BGP 経路が消えた際に、バックアップ回 線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



本装置に接続できるモデムの条件は、以下のとおりです。

- COM ポート側の通信速度が 9600/19200/38400/57600/115200/230400bps のどれかの速度で通信できる
- 工場出荷時の設定で、RS/CS 信号によるハードフロー制御が有効になっている
- 通信中に`+++`をCOMポートから受信することによってエスケープモードになる
- 以下のATコマンドに対応している

カテゴリ	サポートコマンド
ソフトリセット	ATZ
リザルトコードを文字列にする	ATV1
エコーバックを抑止する	ATE0
CONNECTリザルトコードにDCE速度を付加する	ATW2
切断	ATH
応答	ATA
コマンド送出時先行文字	AT
電話番号送出時先行文字	ATD
パルス	Ρ
トーン	Т

カテゴリ	サポートコマンド
ダイヤルトーン検知なし	X3
ダイヤルトーン検知あり	X4
スピーカを OFF にする	M0
発呼時だけスピーカを ON にする	M1
スピーカをONにする	M2
スピーカをダイヤル終了からキャリア検出まで ON にする	M3
音量LOW	LO
音量Midium	L2
音量High	L3

以下のリザルトコードを返す

カテゴリ	サポートコマンド
正常実行	ОК
接続完了	CONNECT <回線速度>(※)
コマンドエラー	ERROR、+FCERROR、+FCON、+F4、FAX、DATA、VOICE
回線接続	NO CARRIER
ダイヤルトーン未検出	NO DIALTONE, NO DIAL TONE
話し中音検出	BUSY、PHONE IN USE、HAND SET IN USE
無音未検出	NO ANSWER
呼び出し検出	RING

※)回線速度:接続した回線速度

0-9の数字文字列の場合だけ回線速度として扱います。

0-9以外の文字が含まれる場合は、無視するため、回線速度を取得できません。

動作確認済みのアナログモデムは、以下のとおりです。

会社名	製品名
(株)アイ・オー・データ機器	DFML-560EL
(株)バッファロー	IGM-B56KS
オムロン(株)	ME5614E2

こんな事に気をつけて

- アナログモデムは、COMポートに接続してください。コンソールポートは、コンソール専用ですので、モデム接続 はできません。
- モデムの不揮発性メモリ(プロファイル)を工場出荷時設定にしてからモデムを接続してください。
- モデムでは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。
- アナログモデム接続では、以下の機能は動作しません。
 - 電話番号による相手識別機能
 - 金額による課金制御機能
 - 常時接続機能
 - シェーピング機能
- ・ モデムで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- アナログモデムによる発信は超過課金が発生するため、課金情報(アカウント情報)を監視して超過課金が発生していないか、こまめに確認してください。
- また、超過課金を防止する場合は、課金制御機能の接続時間制限を設定してください。
- アナログモデムでの通信速度は56Kbpsとみなして動作しますが、モデムの接続完了リザルトコードから速度を取得 できた場合は取得した速度を採用して動作します。

ここでは、以下を参照して、IP-VPN網接続が設定されていることを前提とします。

参照「1.13 複数の事業所LANをIP-VPN網を利用して接続する」(P.127)

•	設定条件	
•	ADSLモデムを使用して IP-VPN 網と接続する	
[亰	東京営業所]	
<	橫浜営業所とモデムで接続する条件>	
•	ネットワーク名	: backup
•	接続先名	: yokohama
•	WANの自側IPアドレス	: 172.17.1.1
•	WANの相手側 IP アドレス	: 172.17.1.2
•	電話番号	: 044-999-9999
•	無通信監視	:1分
•	ユーザ認証 ID とユーザ認証パスワード	
	発信	: tokyo, tokyopass
	着信	: kawasaki, kawapass
•	ダイヤル方式	:トーン
•	バックアップ用のスタティックルート	:10.20.0.0/16(優先度30)
[樟	黃浜営業所]	
</th <th>東京営業所とモデムで接続する条件></th> <th></th>	東京営業所とモデムで接続する条件>	
•	ネットワーク名	: backup
•	接続先名	: tokyo
•	WANの自側IPアドレス	: 172.17.1.2
•	WANの相手側IPアドレス	: 172.17.1.1
•	電話番号	: 033-999-9999
•	無通信監視	:1分
•	ユーザ認証 ID とユーザ認証パスワード	
	発信	: kawasaki, kawapass
	着信	: tokyo, tokyopass
•	ダイヤル方式	:トーン
•	バックアップ用のスタティックルート	:10.10.0.0/16(優先度30)

上記の設定条件に従って設定を行う場合の設定例を示します。

東京営業所の設定する

COMポートを設定する

- 設定メニューのルータ設定で「シリアル情報」をクリックします。
 「シリアル情報」ページが表示されます。
- **2. 「共通情報」をクリックします**。 「共通情報」が表示されます。
- 3. 以下の項目を指定します。
 - COMポート →使用する
 - COMポート通信速度 → 115200

■共通情報	3
COM#	○使用しない ●使用する
COMボート通信速度	115200 🗸

4. [保存] ボタンをクリックします。

バックアップ回線を設定する

- 5. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 7. 以下の項目を指定します。
 - ネットワーク名 → backup

<ネットワーク情報追加フィールド>		
ネットワーク名		backup

8. [追加] ボタンをクリックします。

「ネットワーク情報(backup)」ページが表示されます。

9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

電話番号

- 接続先名 → yokohama
- ・ 接続先種別
 →モデム接続
 ダイヤル1
 - →044-999-9999

<接続先情報追加フィールド>		
接続先名	yokohama	
接続先種別	 専用線接続 ISDN接続 ISDN接続 ダイヤル1 電話番号 フレームリレー接続 DLCI モデム接続 ダイヤル1 電話番号 044-999-9999 PPPoE接続 IPトンネル接続 IPsec/IKE接続 別インタフェースから送出 MPLSトンネル接続 パケット破棄 	

11. [追加] ボタンをクリックします。

「接続先情報(yokohama)」ページが表示されます。

- **12. モデム接続の設定項目の「接続制御情報」をクリックします**。 「接続制御情報」が表示されます。
- 13. 以下の項目を指定します。
 - 無通信監視タイマ →送受信パケットについて60秒



- 14. 【保存】ボタンをクリックします。
- **15. モデム接続の設定項目の「PPP 情報」をクリックします**。 「PPP 情報」が表示されます。

• 送信認証情報	
認証ID	→ yokohama
認証パスワード	→ yokopass
• 受諾認証情報	
認証ID	→tokyo
認証パスワード	→ tokyopass

■PPP情報		3
送信認証情報	認証ID	yokohama
	認証バスワード	••••••
四世司にはまれ	認証ID	tokyo
	認証バスワード	•••••

17. [保存] ボタンをクリックします。

着信デフォルト情報を設定する

- **18. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **19. 「着信相手識別情報」をクリックします**。 「着信相手識別情報」が表示されます。
- 20. 以下の項目を指定します。
 - 着信許可 →する
 着信相手識別情報 (?)
 着信許可 ○しない ⊙する
- 21. [保存] ボタンをクリックします。
- BGPより優先度の低いスタティックルートを設定する
- **22. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **23.** 「ネットワーク情報」をクリックします。 「ネットワーク情報」が表示されます。
- **24.** ネットワーク名が backupの [修正] ボタンをクリックします。 「ネットワーク情報(backup)」ページが表示されます。
- **25. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- **26.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

 ネットワーク 	→ネットワーク指定
あて先 IP アドレス	→ 10.20.0.0
あて先アドレスマスク	→16 (255.255.0.0)
• メトリック値	→ 1
● 優先度	→ 30

- <スタティック経路情報入力フィールド> ・ デフォルトルート ・ ネットワーク指定 あて先JPアドレス 10.20.00 あて先アドレスマスク 16 0255.255.0.0) ・ メトリック値 1 ・ 優先度 30
- 28. [追加] ボタンをクリックします。
- 29. 画面左側の [設定反映] ボタンをクリックします。

横浜営業所を設定する

「東京営業所を設定する」を参考に、横浜営業所を設定します。

2.39 データ通信カードで通信バックアップをする

適用機種 Si-R240,240B

本装置に PIAFS 着信対応のデータ通信カードを装着することによって、 PHS 回線を使用して通信することができます。

ここでは、営業所間をIP-VPN網で接続し、IP-VPN網側の通信が通信不能になった場合にウィルコムのPHS回線 側で通信バックアップする場合を例に説明します。

参照
 動作検証済みのデータ通信カード(富士通ホームページ)
 Si-R240

 http://fenics.fujitsu.com/products/sir/sir240/#supportcard
 Si-R240B

 http://fenics.fujitsu.com/products/sir/sir240b/#supportcard

この例では、BGP 経路よって優先度の低いスタティックルートをバックアップ回線側に設定します。メインの IP-VPN 側が通信不能になって BGP セッションが切断され、相手拠点の BGP 経路が消えた際に、バックアップ回 線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



こんな事に気をつけて

- データ通信カードの不揮発性メモリ(プロファイル)を工場出荷時設定にしてからデータ通信カードを装着してください。
- データ通信カードでは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。
- ・ データ通信カード接続では、以下の機能は動作しません。
 - 電話番号による相手識別機能
 - コールバック機能
 - 金額による課金制御機能
 - 常時接続機能
 - 回線接続保持タイマ機能
- ・ データ通信カードで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信カードによる発信は従量課金が発生するため、データ通信カード統計情報を監視して異常課金が発生していないか、こまめに確認してください。また、異常課金を防止する場合は、課金制御機能や強制切断機能の接続時間制限を設定してください。

- ・ データ通信カードの通信速度は64Kbpsとみなして動作します。
- ・ ウィルコム、FENICS、NTTコミュニケーションズのPHS 接続時には、通信方式に応じて、以下の番号を電話番号に 付加してください。

通信方式	電話番号に付加する番号
32kPIAFS方式	##3
64kPIAFS(ベストエフォート)方式	##4
1xパケット方式	##61
4xパケット方式または8xパケット方式	##64
フレックスチェンジ方式	##7

ここでは、以下を参照して、IP-VPN網接続が設定されていることを前提とします。

● 参照「1.13 複数の事業所LANをIP-VPN網を利用して接続する」(P.127)

● 設定条件

- ADSLモデムを使用して IP-VPN 網と接続する
- データ通信カードは SLOT0 に装着する

[東京営業所]

<横浜営業所とデータ通信カードで接続する条件>

 ネットワーク名 	: backup
● 接続先名	: yokohama
• WANの自側 IP アドレス	: 172.17.1.1
• WANの相手側 IP アドレス	: 172.17.1.2
● 電話番号	: 070-8888-8888
• 通信方式	:64kPIAFS(ベストエフォート)方式
● 無通信監視	:1分
 ユーザ認証 ID とユーザ認証パスワード 	
発信	: tokyo, tokyopass
着信	: kawasaki, kawapass
 バックアップ用のスタティックルート 	:10.20.0.0/16(優先度30)
[構近学業所]	
<東京営業所とデータ通信カードで接続する条件>	
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 	: : backup
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 	: : backup : tokyo
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側 IP アドレス 	: : backup : tokyo : 172.17.1.2
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 	: : backup : tokyo : 172.17.1.2 : 172.17.1.1
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 電話番号 	: : backup : tokyo : 172.17.1.2 : 172.17.1.1 : 070-9999-9999
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 電話番号 通信方式 	: : backup : tokyo : 172.17.1.2 : 172.17.1.1 : 070-9999-9999 : 64kPIAFS(ベストエフォート)方式
マ東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 電話番号 通信方式 無通信監視 	: : backup : tokyo : 172.17.1.2 : 172.17.1.1 : 070-9999-9999 : 64kPIAFS(ベストエフォート)方式 : 1分
く東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 電話番号 通信方式 無通信監視 ユーザ認証IDとユーザ認証パスワード 	: : backup : tokyo : 172.17.1.2 : 172.17.1.1 : 070-9999-9999 : 64kPIAFS(ベストエフォート)方式 : 1分
 <東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 電話番号 通信方式 無通信監視 ユーザ認証IDとユーザ認証パスワード 発信 	: backup : tokyo : 172.17.1.2 : 172.17.1.1 : 070-9999-9999 : 64kPIAFS(ベストエフォート)方式 : 1分 : kawasaki、kawapass
 <東京営業所とデータ通信カードで接続する条件> ネットワーク名 接続先名 WANの自側IPアドレス WANの相手側IPアドレス 電話番号 通信方式 無通信監視 ユーザ認証IDとユーザ認証パスワード 発信 着信 	: backup : tokyo : 172.17.1.2 : 172.17.1.1 : 070-9999-9999 : 64kPIAFS (ベストエフォート) 方式 : 1分 : kawasaki、kawapass : tokyo、tokyopass

上記の設定条件に従って設定を行う場合の設定例を示します。

東京営業所のバックアップ回線を設定する

WAN0 情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 2. 以下の項目を指定します。
 - 回線インタフェース →データ通信カード

WAN情報	追加フィールド>
回線インタフェース	データ通信カード 🔽

- **3.** 【追加】ボタンをクリックします。 「WAN 情報(データ通信カード)」ページが表示されます。
- 4. 以下の項目を指定します。
 - ポート →スロット0-0

```
■基本情報
ポート スロット0-0 ▼
```

5. [保存] ボタンをクリックします。

こんな事に気をつけて

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

3

バックアップ回線を設定する

- 6. 設定メニューのルータ設定で「相手情報」をクリックします。 「相手情報」ページが表示されます。
- 「ネットワーク情報」をクリックします。
 「ネットワーク情報」が表示されます。
- 8. 以下の項目を指定します。

ネットワーク名 → backup

<ネットワーク情報追加フィールド>		
ネットワーク名	backup	

9. [追加] ボタンをクリックします。

「ネットワーク情報(backup)」ページが表示されます。

10. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

 接続先名 → yokohama
 接続先種別 →データ通信カード接続 ダイヤル1 電話番号 → 070-8888-8888##4

<接続先情報追加フィールド>		
接続先名	yokohama	
	⊙ データ通信カート 接続	
	ダイヤル1 電話番号 070-8888-8888##4	
	○ PPP₀E接続	
接続先種別	○ IPトンネル接続	
	○ IPsec/IKE接続	
	○ 別インタフェースから送出	
	○ MPLSトンネル接続	
	○ パケット破棄	

12. [追加] ボタンをクリックします。

「接続先情報(yokohama)」ページが表示されます。

- **13.** データ通信カード接続の設定項目の「接続制御情報」をクリックします。 「接続制御情報」が表示されます。
- 14. 以下の項目を指定します。
 - 無通信監視タイマ →送受信パケットについて60秒

■接続制	御情報	3
無通信監 視タイマ	送受信パケット 🗸 について 60 秒	

- 15. [保存] ボタンをクリックします。
- 16. データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

- 17. 以下の項目を指定します。
 - ・ 送信認証情報
 認証 ID → yokohama
 認証パスワード → yokopass
 - 受諾認証情報
 認証 ID → tokyo
 認証パスワード → tokyopass

PPP情報		3
送信認証情報	認証ID	yokohama
	認証バスワード	••••••
受諾認証情報	認証ID	tokyo
	認証バスワード	

18. [保存] ボタンをクリックします。

着信デフォルト情報を設定する

- **19. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **20. 「着信相手識別情報」をクリックします**。 「着信相手識別情報」が表示されます。
- 21. 以下の項目を指定します。
 - 着信許可

■着信相手識別情報	3
着信許可	⊙しない⊙する

- 22. [保存] ボタンをクリックします。
- BGPより優先度の低いスタティックルートを設定する
- **23. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **24. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- **25.** ネットワーク名がbackupの [修正] ボタンをクリックします。 「ネットワーク情報(backup)」ページが表示されます。
- **26. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- **27.** IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。
- 28. 以下の項目を指定します。
 - ネットワーク →ネットワーク指定 あて先IPアドレス → 10.20.0.0 → 16 (255.255.0.0)
 メトリック値 → 1
 - 優先度 → 30

	<スタティック経路情報入力フィールド>
ネットワーク	 デフォルトルート ネットワーク指定 あて先IPアドレス 10.20.0.0 あて先アドレスマスク 16 255.255.0.0)
メトリック値	1 🗸
優先度	30

- 29. [追加] ボタンをクリックします。
- 30. 画面左側の [設定反映] ボタンをクリックします。

横浜営業所のバックアップ回線を設定する

「東京営業所のバックアップ回線を設定する」を参考に、横浜営業所を設定します。

2.40 外部のパソコンから着信接続する (リモートアクセスサーバ)

適用機種 Si-R220B,220C,370,570

ISDN 回線を使用して、外部のパソコンから本装置に着信接続する場合、本装置をリモートアクセスサーバとして使用することができます。以下の環境の場合に、リモートアクセスを行うことができます。

- デスクトップパソコン+TA→(ISDN)→本装置
- ノート型パソコン+ISDN カード→(ISDN)→本装置
- ノート型パソコン+PIAFS通信カード+PHS→(PHS網)→(ISDN)→本装置
- 本装置→(ISDN)→本装置

本装置では、テンプレート着信機能を使用した不特定着信と、AAAによる認証(ローカル認証、RADIUS認証) を組み合わせることで、リモートアクセスサーバを実現することができます。

● 参照 Si-R シリーズ 機能説明書 [2.28 テンプレート着信機能」(P.139)

2.40.1 1台の装置でリモートアクセスサーバを構成する

適用機種 Si-R220B,220C,370,570

ここでは、ノートパソコンに PHS を繋いで外出先から本社のネットワークに接続する場合を例に説明します。



着信時にプール内で使用していないIPアドレスが割り当てられる

● 設定条件

- SLOTOに装着した BRI 拡張モジュール L2(Si-R220B、220C以外)または ISDN Uポート(Si-R220B、220C)を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース

• 以下からの着信を許可する

[PC0 <ノートパソコン+ PHS >で外出先から接続]

- 受諾認証 ID
- 受諾認証パスワード
- PHSの電話番号は未登録

- : mobile-a
- : mobilepass-a

:rmt30から2個

[PC1 < ノートパソコン+ PHS > で外出先から接続]

- 受諾認証 ID
- 受諾認証パスワード
- PHSの電話番号は未登録
- 本社のLAN側のネットワークアドレス/ネットマスク
- 外部のパソコンに割り当てる IP アドレス

こんな事に気をつけて

- テンプレート着信機能をサポートする回線はISDNです(MP接続はできません)。
- テンプレート着信で使用するインタフェースはテンプレート専用になります。テンプレート用に予約されたrmtイン タフェースには、remote 定義を設定しないでください。 たとえば、rmt30~47インタフェースをテンプレート用に予約した場合、remote 30~47までのremote 定義を設定 しないでください。

: mobile-b

: mobilepass-b

: 192.168.1.0/24

: 192.168.1.34、192.168.1.35

- テンプレート情報を定義する場合(IPフィルタリングなど)、定義数は「テンプレート情報で設定した定義数×テンプレートで使用するrmtインタフェース数」で計算されるため、それを含めて装置最大定義数の範囲に収まるように定義してください。装置最大定義数を超えたときは、資源不足により該当機能が動作しない場合があります。
- 接続先情報を設定する場合、テンプレート用のインタフェースの個数分は設定しないでください。
 たとえば、接続先定義を最大48定義可能な装置で、10インタフェースをテンプレート用に使用する場合、接続先定 義の定義数は38となります。
- ・ テンプレート情報とAAA 情報のユーザ側の設定に同じ項目がある場合は、個人情報である AAA 情報が適用されます。 AAA 情報の未登録の項目に対しては、テンプレート情報の設定値が適用されます。
- 発信者番号による識別(CLID相手判定)をAAA 情報に設定していない場合は、発信者番号による相手判定は行いません(PPPのユーザ認証の結果だけで接続できるかどうかが決まります)。
- AAA 情報に同一ユーザ(パスワードも同一)が存在するときには、定義番号が小さいAAA ユーザ情報が優先されます。定義番号が大きいユーザ情報に発信者番号が一致する定義があり、定義番号が小さいユーザ情報に発信番号で識別を行わない定義がある場合も、定義番号の小さいユーザで着信が行われます。
- ・ 共通IDで複数の着信を行う場合は、AAA 情報のユーザ定義に、ID とパスワードだけを定義してください(個別情報 を定義しないで、ID とパスワードだけのユーザ情報を定義すると共有ID として扱われます)。

上記の設定条件に従って設定を行う場合の設定例を示します。

LAN0 情報を設定する

- 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理 LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

)
マ+オール1

■IPアドレス情報		3	
IPv4	 ●使用する ○使用しない 		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 		

5. [保存] ボタンをクリックします。

WAN0 情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。
 「WAN 情報」ページが表示されます。
- 7. 以下の項目を指定します。
 - 回線インタフェース → ISDN



- 【追加】ボタンをクリックします。
 「WAN1 情報(ISDN)」ページが表示されます。
- 9. [保存] ボタンをクリックします。

テンプレート情報を設定する

- **10. 設定メニューのルータ設定で「テンプレート情報」をクリックします**。 「テンプレート情報」ページが表示されます。
- 11. 以下の項目を指定します。
 - テンプレート名 → mobile
 - 接続先種別 → ISDN

<テンプレート情報追加フィールド>		
テンプレート名	mobile	
接続種別	 ● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN) 	

機種により、接続先種別の表示が上記の画面とは異なります。

12. [追加] ボタンをクリックします。

「テンプレート情報(mobile)」ページが表示されます。

13. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

- 使用インタフェース →WAN0
- 使用する rmt インタフェース →rmt30から2インタフェースを予約
- →指定する 参照する AAA 情報 AAA グループ ID **→**0

使用インタフェース	WAND 🗸
使用するrmtインタフェース	rmt30 から2 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケット 💟 について 🛛 🛛 🏼 💌
参照するAAA情報	 ○ 指定しない ③ 指定する AAAグループID □

[保存] ボタンをクリックします。 15.

「IP関連」をクリックします。 16.

IP 関連の設定項目と「IP 基本情報」が表示されます。

- 17. 以下の項目を指定します。
 - →設定する • 割当て IP アドレス 先頭IPアドレス アドレス数

→ 192.168.1.34	
→ 2	



- 18. [保存] ボタンをクリックします。
- 設定メニューのルータ設定で「AAA情報」をクリックします。 19. 「AAA情報」ページが表示されます。
- 「グループID情報」をクリックします。 20.

「グループID情報」が表示されます。

- 21. 以下の項目を指定します。
 - グループ名 → mobile



22. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

23. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

- 24. 以下の項目を指定します。
 - ユーザID → mobile-a



25. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と「認証情報」が表示されます。

- 26. 以下の項目を指定します。
 - ユーザID → mobile-a
 - ● 認証パスワード
 → mobilepass-a
 - 発信者番号による識別 →番号チェックしない

ユーザID	mobile-a	
認証バスワード	••••••	
発信者番号による識 別	 番号チェックしない 番号チェックする 相手電話番号 相手サブアドレ ス 	

- 27. [保存] ボタンをクリックします。
- 28. 手順26.~27.を参考に、以下の項目を指定します。
 - ユーザID → mobile-b
 - 認証パスワード → mobilepass-b
- **29. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.40.2 複数台の装置でリモートアクセスサーバを構成する

<u>適用機種</u> Si-R220B,220C,370,570

RADIUS機能を用いることで、アクセスユーザの情報をRADIUSサーバで一元管理し、複数のリモートアクセスサーバから同一のアクセスユーザ情報を利用できるようにすることができます。

ここでは、「2.40.1 1台の装置でリモートアクセスサーバを構成する」(P.919)の構成から、さらにリモートアクセスサーバを増設し着信可能な回線数を増やす場合を例に説明します。



● 設定条件

[本装置1]

- SLOT0 に装着した BRI 拡張モジュール L2 (Si-R220B、220C 以外) または ISDN U ポート (Si-R220B、220C) を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース
- 以下からの着信を許可する

[PC0 <ノートパソコン+ PHS >で外出先から接続]

- 受諾認証 ID
- 受諾認証パスワード
- PHSの電話番号は未登録

[PC1 < ノートパソコン+ PHS >で外出先から接続]

- 受諾認証 ID
- 受諾認証パスワード
- PHSの電話番号は未登録
- 本社のLAN側のネットワークアドレス/ネットマスク
- 本社のLAN側のIPアドレス
- 外部のパソコンに割り当てる IP アドレス
- 本装置に接続する RADIUS クライアントの IP アドレス
- RADIUS 共有鍵

: mobile-b

: mobile-a

: mobilepass-a

: mobilepass-b

:rmt30から2個

- : 192.168.1.0/24
- : 192.168.1.1
- : 192.168.1.34、192.168.1.35
- : 192.168.1.2
 - : rassharepass

[本装置2]

- SLOT0に装着したBRI 拡張モジュールL2(Si-R220B、220C以外)またはISDN Uポート(Si-R220B、220C)を使用してISDN 回線に接続する
- テンプレートで使用するインタフェース :rmt30から2個
- RADIUSサーバに問い合わせて着信を許可する
- 本社のLAN側のネットワークアドレス/ネットマスク
 ・本社のLAN側のIPアドレス
 ・外部のパソコンに割り当てるIPアドレス
 ・本装置が問い合わせるRADIUSサーバのIPアドレス
 ・RADIUS共有鍵
 ・rassharepass

こんな事に気をつけて

- ・ 1台の本装置上で、RADIUS サーバ機能と RADIUS クライアント機能を併用することはできません。
- 1台の本装置上で、RADIUSサーバ機能を複数設定することはできません。
- RADIUS プロトコルの制約で、同時に認証およびアカウンティングが行える数は 256 です。同時に 257 以上の認証と アカウンティングを行った場合は、両方とも失敗します。
- 本装置のRADIUS機能は4096バイトを超えるRADIUSのパケットを扱えません。RADIUSサーバ機能を用いる場合 は、経路情報を大量に設定すると(たとえばAAA 情報のスタティック経路情報だけの場合は約130個)この上限を超 えてしまい、パケットが送出できずRADIUSクライアント側で認証が失敗します。
- ・「AAA 情報」-「グループ ID 情報」-「AAA ユーザ情報」-「IP 関連」(「IPv6 関連」)-「スタティック経路情報」 (「IPv6 スタティック経路情報」) で設定した優先度は RADIUS サーバ機能では伝達することはできません。
- ・「AAA 情報」-「グループID 情報」-「AAA ユーザ情報」-「IP 関連」-「IP 基本情報」で設定した自側 IP アドレス は RADIUS サーバ機能では伝達することはできません。
- ・ RADIUS クライアント機能で受信した Framed-Route、Framed-IPv6-Route の情報は、優先度 100 の経路情報として 扱われます。また、これらの経路情報を受け入れた結果、装置の経路数の上限を超えてしまう場合は回線は切断され ます。
- ・ RADIUS クライアント機能を定義しても、同じグループのユーザ情報は利用されます。AAA グループに RADIUS ク ライアント機能とユーザ情報の両方を定義した場合、まず RADIUS で認証が行われます。RADIUS での認証が成功し た場合はのユーザ情報は利用されませんが、RADIUS で認証に失敗した場合は、次にユーザ情報で認証を行います。

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

• IF	Pv4	→使用する
• IF	Pアドレス	→指定する
IF	Pアドレス	→ 192.168.1.1
オイ	ネットマスク	→24 (255.255.255.0)
7	ブロードキャストアドレス	→ネットワークアドレス+オール1

■IPアドレス情報		3
IPv4	●使用する●使用しない	_
IP7Fレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.0) ブロードキャストアドレ ス 	

5. [保存] ボタンをクリックします。

WAN0 情報を設定する

6. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - 回線インタフェース → ISDN

 <wantf報追加フィールド>

 回線インタフェース

 ISDN

- 【追加】ボタンをクリックします。
 「WAN1 情報(ISDN)」ページが表示されます。
- 9. [保存] ボタンをクリックします。

テンプレート情報を設定する

- **10. 設定メニューのルータ設定で「テンプレート情報」をクリックします**。 「テンプレート情報」ページが表示されます。
- 11. 以下の項目を指定します。
 - テンプレート名 → mobile
 - 接続先種別 → ISDN

<テンプレート情報追加フィールド>		
テンプレート名	mobile	
接続種別	 ● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN) 	

機種により、接続先種別の表示が上記の画面とは異なります。

12. [追加] ボタンをクリックします。

「テンプレート情報(mobile)」ページが表示されます。

13. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

- 使用インタフェース → WAN0
- 使用するrmtインタフェース →rmt30から2インタフェースを予約
- 参照する AAA 情報
 AAA グループ ID
- →指定する→0

使用インタフェース	WAND V
使用するrmtインタフェース	rmt30 から2 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケット 💙 について 0 秒 💌
参照するAAA情報	 ○ 指定しない ③ 指定する
	AAAグループID 🛛

15. [保存] ボタンをクリックします。

16. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

17. 以下の項目を指定します。

割当てIPアドレス →設定する
 先頭IPアドレス → 192.168.1.34
 アドレス数 → 2

割当てIPアドレス	 ○ 設定しない ● 設定する
	先頭IPアドレス 192.168.1.34
	アドレス数 2

- 18. [保存] ボタンをクリックします。
- **19. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **20.** 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 21. 以下の項目を指定します。
 - グループ名

→mobile

</th <th>ブループID情報追加フィールド></th>	ブループID情報追加フィールド>
グループ名	mobile

22. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

23. 「AAA ユーザ情報」をクリックします。

「AAAユーザ情報」が表示されます。

• ユーザID

→ mobile-a



25. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と「認証情報」が表示されます。

26. 以下の項目を指定します。

- ユーザID → mobile-a
- 認証パスワード → mobilepass-a
- 発信者番号による識別 →番号チェックしない

■認証情報		
ユーザID	mobile-a	
認証バスワード	•••••	
発信者番号による識 別	 ● 番号チェックしばい ● 番号チェックする 	
	相手電話番号 相手サブアドレ ス	

27. [保存] ボタンをクリックします。

28. 手順26.~27.を参考に、以下の項目を指定します。

- ユーザID → mobile-b
- 認証パスワード → mobilepass-b

RADIUSサーバを設定する

- **29. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **30. 「グループID 情報」をクリックします**。 「グループID 情報」が表示されます。
- **31.** 「グループID 情報」でグループID が0の [修正] ボタンをクリックします。 「グループID 情報(0)」と設定項目が表示されます。
- 32. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

33. 以下の項目を指定します。

•	RADIUSサービス	→サーバ機能
	認証	→チェックする
	アカウンティング	→チェックする

■基本情報	3
RADIUSサービス	サーバ機能 マ マ アカウンティング (クライアント機能またはサーバ機能を選択した 場合にのみ有効となります)

- 34. [保存] ボタンをクリックします。
- **35. 「クライアント情報」をクリックします。** 「クライアント情報(サーバ機能)」ページが表示されます。
- 36. 以下の項目を指定します。
 - 共有鍵

- → rassharepass
- クライアントIPアドレス →アドレス指定

→ 192.168.1.2

<クライアント情報(サーバ機能)入力フィールド>		
共有鍵	••••••	
クライアン トIPアドレ ス	 ○ すべて ● アドレス指定 192.168.1.2 	

- 37. [追加] ボタンをクリックします。
- **38. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

本装置2を設定する

LAN0情報を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 3. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 192.168.1.2
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレ	ス情報	3
IPv4	⊙使用する○使用しない	
IPアドレス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス IPマドレス 192 ネットマスク 24 	.168.1.2 (255.255.255.0)
	ブロードキャストアドレス	トワークアドレス+オール1 💌

5. [保存] ボタンをクリックします。

WAN0情報を設定する

6. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - 回線インタフェース → ISDN



- **8. [追加] ボタンをクリックします**。 「WAN1 情報(ISDN)」ページが表示されます。
- 9. [保存] ボタンをクリックします。

テンプレート情報を設定する

- **10. 設定メニューのルータ設定で「テンプレート情報」をクリックします**。 「テンプレート情報」ページが表示されます。
- 11. 以下の項目を指定します。
 - テンプレート名 → mobile
 - 接続先種別 → ISDN

<テンプレート情報追加フィールド>		
テンプレート名	mobile	
接続種別	 ● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN) 	

機種により、接続先種別の表示が上記の画面とは異なります。

12. [追加] ボタンをクリックします。

「テンプレート情報(mobile)」ページが表示されます。

13. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

- 使用インタフェース → WAN0
- 使用するrmtインタフェース →rmt30から2インタフェースを予約
- 参照する AAA 情報 →指定する
 AAA グループID →0

使用インタフェース	WANO 💌
使用するrmtインタフェース	rmt30 から2 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケット 💙 について 0 秒 💌
参照するAAA情報	 指定しない 指定する AAAグループID 0

割

- 15. [保存] ボタンをクリックします。
- **16. 「IP 関連」をクリックします。** IP 関連の設定項目と「IP 基本情報」が表示されます。
- 17. 以下の項目を指定します。
 - 割当てIPアドレス →設定する
 先頭IPアドレス → 192.168.1.36
 アドレス数 → 2

	 ○ 設定しない ● 設定する 	
当てIPアドレス	先頭IPアドレス 192.168.1.36	
	アドレス数 2	

18. [保存] ボタンをクリックします。

RADIUS クライアントを設定する

- **19. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **20. 「グループID情報」をクリックします**。 「グループID情報」が表示されます。
- **21.** 「グループID 情報」でグループID が0の [修正] ボタンをクリックします。 「グループID 情報(0)」と設定項目が表示されます。
- **22.** 「RADIUS 関連」をクリックします。 RADIUS 関連の設定項目と「基本情報」が表示されます。
- 23. 以下の項目を指定します。
 - RADIUSサービス →クライアント機能
 認証 →チェックする
 アカウンティング →チェックする

■基本情報	3
RADIUSサービス	クライアント機能 ▼ 図認証 図アカウンティング (クライアント機能また(はサーバ機能を選択した 場合にのみ有効となります)

- 24. [保存] ボタンをクリックします。
- 25. 「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」が表示されます。

26. 認証情報1の[修正]ボタンをクリックします。

 認証情報1 	
共有鍵	→ rassharepass
サーバIPアドレス	→ 192.168.1.2

	共有鍵	••••••
	サーバIPア ドレス	192.168.1.2
	サーバ UDPポート	⊙1812 ◯1645
認証情報 1	復旧待機 時間	0 秒 💙
優 自 IP	優先度	0
	自側認証 IPアドレス	

28. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

29. アカウンティング情報1の [修正] ボタンをクリックします。

30. 以下の項目を指定します。

 アカウンティング情報1 共有鍵 → rassharepass サーバIPアドレス → 192.168.1.2

	共有鍵	••••••
アカウンティング情報 1	サーバIPア ドレス	192.168.1.2
	サーバ UDPポート	⊙ 1813 ◯ 1646
	復旧待機 時間	0 秒 💙
	優先度	0
	自側アカウ	
	シティンク IPアドレス	

31. アカウンティング情報1の[保存]ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

32. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.40.3 リモートアクセスサーバが使用する RADIUS サーバを多重化する

適用機種 Si-R220B,220C,370,570

RADIUS 機能を用いて、複数台の RADIUS サーバを使用することで、RADIUS サーバの信頼性を向上させることができます

ここでは、「2.40.11台の装置でリモートアクセスサーバを構成する」(P.919)の構成から、さらにリモートアクセスサーバを増設し着信可能な回線数を増やす場合を例に説明します。



着信時にプール内で使用していないIPアドレスが割り当てられる

● 設定条件

[本装置]

- SLOT0 に装着した BRI 拡張モジュール L2 (Si-R220B、220C 以外) または ISDN U ポート (Si-R220B、220C) を使用して ISDN 回線に接続する
- テンプレートで使用するインタフェース :rmt30から2個 本社のLAN 側のネットワークアドレス/ネットマスク : 192.168.1.0/24 本社のLAN側のIPアドレス : 192.168.1.1 • RADIUS 認証サーバ(プライマリ)のIPアドレス : 192.168.1.2 • RADIUS 認証サーバ(プライマリ)の共有鍵 : rassharepass • RADIUS 認証サーバ(セカンダリ)のIPアドレス : 192.168.1.3 RADIUS 認証サーバ(セカンダリ)の共有鍵 : rassharepass RADIUSアカウンティングサーバ(プライマリ)のIPアドレス: 192.168.1.2 RADIUSアカウンティングサーバ(プライマリ)の共有鍵 : rassharepass • RADIUS アカウンティングサーバ(セカンダリ)のIP アドレス: 192.168.1.3 • RADIUS アカウンティングサーバ(セカンダリ)の共有鍵 : rassharepass RADIUSサーバに登録する情報(プライマリ、セカンダリ共、共通) [PC0<ノートパソコン+PHS>で外出先から接続]
 - 認証ユーザID mobile-a 認証ユーザパスワード mobilepass-a

[PC1<ノートパソコン+PHS>で外出先から接続]

- 認証ユーザID

- 認証ユーザパスワード

mobile-b

mobilepass-b

- こんな事に気をつけて
 - テンプレート着信で使用するインタフェースはテンプレート専用になりますので、範囲に含まれるrmtインタフェースには remote 定義を設定しないでください。
 例:rmt30からrmt47をテンプレートで予約した場合、remote 30から remote 47までの remote 定義に対して設定を行わないでください。
 - テンプレート着信で使用するインタフェースの個数分、接続先情報定義をあけておく必要があります。
 例:接続先定義を最大48定義可能な装置で、10インタフェースをテンプレートで使用する場合、接続先定義の定義数は38定義までにしてください。
 - テンプレート情報内で設定されている定義の中で、RADIUS サーバのユーザ側にも同じ項目の定義が存在する場合は、RADIUS サーバでの設定値が適用されます。
 RADIUS サーバで未登録の項目に対しては、テンプレート情報の設定値が適用されます。

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

LAN0 情報を設定する

- **1. 設定メニューのルータ設定で「LAN情報」をクリックします**。 「LAN情報」ページが表示されます。
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 4. 以下の項目を指定します。
 - IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →192.168.1.1
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレ	ス情報 []	
IPv4	⊙使用する○使用しない	
ΙΡ ΓΓυλ	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.0) ▼ ブロードキャストアドレ ス 	

5. [保存] ボタンをクリックします。

WAN0情報を設定する

6. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - 回線インタフェース → ISDN

<	N情報追加フィールド>	
回線インタフェース ISDN V		

- **8. [追加] ボタンをクリックします**。 「WAN1 情報(ISDN)」ページが表示されます。
- 9. [保存] ボタンをクリックします。

テンプレート情報を設定する

- **10. 設定メニューのルータ設定で「テンプレート情報」をクリックします**。 「テンプレート情報」ページが表示されます。
- 11. 以下の項目を指定します。
 - テンプレート名 → mobile
 - 接続先種別 → ISDN

<テンプレート情報追加フィールド>		
テンプレート名	mobile	
接続種別	 ● ISDN ● IPsec/IKE(RADIUS/AAA) ● IPsec/IKE(動的VPN) 	

機種により、接続先種別の表示が上記の画面とは異なります。

12. [追加] ボタンをクリックします。

「テンプレート情報(mobile)」ページが表示されます。

13. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

- 使用インタフェース → WAN0
- 使用するrmtインタフェース →rmt30から2インタフェースを予約
- 参照する AAA 情報 →指定する
 AAA グループID →0

使用インタフェース	WAND 💌
使用するrmtインタフェース	rmt30 から2 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信バケット 💙 について 0 秒 💌
参照するAAA情報	 ○ 指定しない ③ 指定する AAAグルーブID □

- 15. [保存] ボタンをクリックします。
- **16. 「**IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

- 17. 以下の項目を指定します。
 - 割当てIPアドレス →設定する
 先頭IPアドレス → 192.168.1.34
 アドレス数 → 2

	 ○ 設定しない ○ 設定する 	
割当てIPアドレス	先頭IPアドレス 192.168.1.34	
	アドレス数 2	

- 18. [保存] ボタンをクリックします。
- **19. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **20.** 「グループID 情報」をクリックします。

「グループID情報」が表示されます。

- 21. 以下の項目を指定します。
 - グループ名

<グルーブID情報追加フィールド> グルーブ名 mobile

→ mobile

22. [追加] ボタンをクリックします。 「グループID情報(0)」と設定項目が表示されます。

RADIUSサーバを設定する

- **23.** グループIDの設定項目の「RADIUS 関連」をクリックします。 「RADIUS 基本情報」項目と「RADIUS 情報」項目が表示されます。
- **24.** RADIUS 関連の設定項目の「基本情報」をクリックします。 「RADIUS 基本情報」ページが表示されます。
- 25. 以下の項目を指定します。

 RADIUS サービス 	→クライント機能
認証	→チェックする
アカウンティング	→ チェックする

■基本情報	3
RADIUSサービス	クライアント機能 ✓ ✓ 認証 ☑ アカウンティング (クライアント機能また(はサーバ機能を選択した 場合(このみ有効となります)

26. [保存] ボタンをクリックします。
27. 「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」が表示されます。

28. 認証情報1の[修正]ボタンをクリックします。

29. 以下の項目を指定します。

 認証情報1 共有鍵

共有鍵	→ 192.168.2.1
サーバIPアドレス	→ 192.168.1.2
復旧待機時間	→30分
優先度	→ 0

	共有鍵	•••••
	サーバIPア ドレス	192.168.1.2
	サーバ UDPポート	⊙1812 ◯1645
認証情報 1	復旧待機 時間	30 分 💙
	優先度	0
	自側認証 IPアドレス	

30. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

31. 認証情報2の[修正] ボタンをクリックします。

32. 以下の項目を指定します。

•

認証情報2	
共有鍵	→ 192.168.2.1
サーバIPアドレス	→192.168.1.3
復旧待機時間	→30分
優先度	→ 100

	共有鍵	•••••
	サーバIPア ドレス	192.168.1.3
	サーバ UDPポート	⊙ 1812 ◯ 1645
認証情報 2	復旧待機 時間	30 分 🗸
	優先度	100
	自側認証 IPアドレス	

33. 認証情報2の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)に戻ります。

34. アカウンティング情報1の [修正] ボタンをクリックします。

アカウンティング情報1
 共有鍵 → 192.168.2.1
 サーバIPアドレス → 192.168.1.2
 復旧待機時間 → 30分
 優先度 → 0

	共有鍵	••••••
アカウンティング情報 1	サーバIPア ドレス	192.168.1.2
	サーバ UDPポート	⊙1813 ◯1646
	復旧待機 時間	30 分 💙
	優先度	0
	自側アカウ ンティング	
	IPアドレス	

36. アカウンティング情報1の[保存]ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

37. アカウンティング情報2の [修正] ボタンをクリックします。

38. 以下の項目を指定します。

•	アカウンティング情報2	
	共有鍵	→ 192.168.2.1
	サーバIPアドレス	→ 192.168.1.3
	復旧待機時間	→30分
	優先度	→ 100

	共有鍵	•••••
	サーバIPア ドレス	192.168.1.3
	サーバ UDPポート	⊙ 1813 ◯ 1646
アカウンティング情報 2	復旧待機 時間	30 分 🔽
	優先度	100
	自側アカウ ンティング IPアドレス	

39. アカウンティング情報2の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

40. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。

2.41 スイッチポートを使う

適用機種 Si-R180,180B

本装置ではLAN1側のポートをスイッチングHUBとして使用するか、従来の単独ポートとして使用するかを構成 定義により選択できます。また、スイッチングHUBとして使用する場合はVLAN機能を併用することでスイッ チポート(SW1~4)を独立ポートとして使用することもできます。

本装置のスイッチポートでは以下のような形態が利用できます。

- スイッチポートをHUBとして使用する 以下の2つ方法で使用できます。
 - VLAN ヘッダを含む場合は、一致する VLAN ID のみ転送を行う VLAN を使用しない場合、または VLAN を使用する場合で VLAN ID に応じた転送を行うときに選択します。

● 参照「2.41.1 スイッチポートをHUBとして使用する」(P.940)

VLAN ヘッダに依存しないで、MAC アドレスのみでスイッチポート間の転送を行う
 VLAN を使用していて VLAN ヘッダごと転送する場合、またはブリッジ機能を VLAN タグ転送モードで使用する場合に選択します。

参照「2.41.2 VLAN 透過モードを使用する」(P.944)

スイッチポートを独立した4ポートとして使用する
 スイッチポートをすべて別のインタフェースとして使用する場合に選択します。

● 参照「2.41.3 スイッチポートを独立ポートとして使用する」(P.947)

スイッチポートを独立した2ポートずつに分割して使用する
 スイッチポートをすべて別のインタフェースとして使用する場合に選択します。

● 参照「2.41.4 スイッチポートを分割して使用する」(P.952)

こんな事に気をつけて

- 本装置のスイッチポートのMTUは1532バイトです。EoMPLSなどのトンネルプロトコルを利用する場合はMTUを スイッチポートのMTUサイズ以下になるように設定するか、スイッチポートを無効にし、使用するパケットの最大 長の転送が可能な外付けのスイッチを使用してください。
- スイッチポートを使用しかつ VLAN 透過モードを使用しない場合は、LAN 定義を VLAN として定義します。そのため、VLANを使用した場合と同じ注意事項が適用されます。スイッチポートを使用する前に必ず「VLAN 機能」に関する記述を確認してください。

● 参照「2.12 VLAN機能を使う」(P.372)

2.41.1 スイッチポートをHUBとして使用する

適用機種 Si-R180,180B

接続するスイッチポートをHUBとしてインターネットに接続する場合の設定方法を説明します。



ここでは以下の条件によって、PPPoEを利用したインターネットとの接続が設定されていることを前提とします。

● 参照「1.6 インターネットへ PPPoE で接続する」(P.67)

● 前提条件

- LAN0 側の PPPoE 設定は完了している
- LAN1 設定がない

● 設定条件

[通信事業者側]

- ユーザ認証 ID
- ユーザ認証パスワード

- :userid(プロバイダから提示された内容)
- :userpass(プロバイダから提示された内容)

• LAN0 ポートを使用する

【プライベートLAN 側】

- LAN1 側をスイッチポートとして使用する
- ローカルネットワークではVLANは使用しない
- ローカルネットワークではDHCPサーバを使用し、パソコンに割り当てるアドレスは192.168.1.2から64個 用意する
- 本装置のIPアドレス : 192.168.1.1
- ネットワークアドレス/ネットマスク : 192.168.1.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

設定メニューのルータ設定で「スイッチ情報」をクリックします。

「スイッチ情報」ページが表示されます。

2. 「基本情報」をクリックします。 「基本情報」が表示されます。

|本本情報] 5 私がとれるす。

3. 以下の項目を指定します。

• スイッチ	→使用する
■基本情報	5
スイッチ	○使用しない <>>> ●使用しない <>>>

- 4. [保存] ボタンをクリックします。
- **5. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 6. 以下の項目を指定します。
 - インタフェース → VLAN



- 7.
 [追加] ボタンをクリックします。

 「LAN1 情報(VLAN)」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
- 9. 以下の項目を指定します。
 - ・ 出力先
 →スイッチ

```
■基本情報
出力先 スイッチ ▼
```

- 10. [保存] ボタンをクリックします。
- **11.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 12. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する
 IPアドレス → 192.168.1.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレ	■IPアドレス情報				
IPv4	⊙使用する○使用しない				
IPアドレス	 DHCPで自動的に取得す 指定する IPアドレス ネットマスク ブロードキャストアドレ ス 	る 192.168.1.1 24 (255.255.255.0) ・ ネットワークアドレス+オール1 ・			

13. [保存] ボタンをクリックします。

3

14. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

15. 以下の項目を指定します。

•	DHCP機能	→サーバ機能を使用する
	割当て先頭IPアドレス	→ 192.168.1.2
	割り当てアドレス数	→64
	リース期間	→1日
	デフォルトルータ広報	→ 192.168.1.1
	DNSサーバ広報	
	プライマリ	→ 192.168.1.1
	セカンダリ	→指定しない



備記 DHCPサーバ機能で割り当てることのできる最大数は253です。

■DHCP情報						
	0 0	使用しない リレー機能を使用する				
		DHCPサ	ーバIPアドレ	/ス1		
		DHCPサ	ーバIPアドレ	,ス2		
		MACアドレスチェック		,	□ホストデータベース □AAA 参照するAAA情報	
	۲	サーバ機	能を使用す	3		
		割当て先 ス	頭IPアドレ	192.1	68.1.2	
		割当てア	ドレス数	64		
		リース期		1		
			デフォルトルータ広 報		192.168.1.1	
DHCP		DNSサ	ブライマリ	192.1	68.1.1	
機能		報	セカンダリ			
	ドメイン名広		名広報			
		ΠMEサ-	-バ広報			
		NTPサー	バ広報			
		WINSサ ーバ広	ブライマリ			
		報	セカンダリ			
			記述形式	<u>۰</u> ۲.	メイン名 OIPアドレス	
		SIPU- バ広報	ブライマリ			
			セカンダリ			
		MAC7F	レスチェッ	口巾	ストデータベース	
		ク		ΠA	AA 参照するAAA情報	
		※"割当っ ークアドレ	て先頭アドレ , ス内である	ス"が ことを	海装置のIPアドレスと同じネットワー 確認してください。	

- 16. [保存] ボタンをクリックします。
- 17. 画面左側の[再起動]ボタンをクリックします。 設定した内容が有効になります。

こんな事に気をつけて

- ・ 本装置では VLAN IDの設定を省略した場合、VLAN ID として1が設定されたものとして動作します。
- 設定されたタグなし VLAN ID と同じ VLAN タグが付加されたパケットは、タグなし VLAN からパケットを受信したものとして処理されます。タグなし VLAN ID とネットワークで使用しているタグ付き VLAN ID が一致しないよう VLAN ID を設定してください。詳細については、「Si-R シリーズ Web リファレンス」を参照してください。

2.41.2 VLAN 透過モードを使用する

適用機種 Si-R180,180B

VLAN 透過モードを使用すると、VLAN を使用しているネットワークで VLAN ヘッダも含めてスイッチングする ことができます。

VLAN透過モードを使用する場合の設定方法を説明します。



● 前提条件

• IP網は、PPPoE 接続でLAN型払い出しによりアドレス割り当てを行う CUG(Closed Users Group)サービスを利用する

[本社 (PPPoE 常時接続)]

- 払い出される IPv4 アドレス(LAN1 ポートに設定)
- PPPoE ユーザ認証 ID
- PPPoEユーザ認証パスワード
- PPPoE LAN ポート
- NAT 機能を使用しない
- 常時接続機能を使用する

【支社(PPPoE常時接続)】

- 払い出される IPv4 アドレス(LAN1 ポートに設定)
- PPPoEユーザ認証ID
- PPPoEユーザ認証パスワード
- PPPoE LAN ポート
- NAT 機能を使用しない
- 常時接続機能を使用する

● 設定条件

[本社]

・ 自側エンドポイントアドレス : 192.168.10.1
 ・ 相手側エンドポイントアドレス : 192.168.20.1
 「支社】
 ・ 自側エンドポイントアドレス : 192.168.20.1
 ・ 相手側エンドポイントアドレス : 192.168.20.1
 ・ 相手側エンドポイントアドレス : 192.168.10.1

- : 192.168.10.1/24
- : userid1@groupname
- : userpass1
- :LAN0ポート使用
- : 192.168.20.1/24
- : userid2@groupname
- : userpass2
- :LAN0ポート使用

[本社、支社共通]

- ブリッジ対象インタフェース
- IPv4 の転送方式
- IPv6の転送方式

:LAN0ポートとIPトンネル

- :ルーティングで転送
- :ブリッジで転送

上記の設定条件に従って設定を行う場合の設定例を示します。

本社を設定する

- 設定メニューのルータ設定で「スイッチ情報」をクリックします。
 「スイッチ情報」ページが表示されます。
- 「基本情報」をクリックします。
 「基本情報」が表示されます。
- 3. 以下の項目を指定します。
 - スイッチ →使用する
 - VLAN tag →透過する

■基本情報		3
スイッチ	●使用しない●使用する	
VLAN tag	○透過しない⊙透過する	

- 4. [保存] ボタンをクリックします。
- **5.** [2.33.3 IP トンネルで事業所間をブリッジ接続する(Ethernet over IP ブリッジ)」(P.862)の手順1. ~10.を参考に、PPPoE および IPv4 トンネルを設定します。
- 6. 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - インタフェース →物理LAN

<lan情報追加フィールド></lan情報追加フィールド>	
インタフェース	物理LAN 🖌

- 【追加】ボタンをクリックします。
 「LAN1情報(物理LAN)」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
- 10. 以下の項目を指定します。
 - ポート番号 →スイッチ

■基本情報	3
ポート番号	スイッチ 💌

11. 【保存】ボタンをクリックします。

- **12.** [2.33.3 IP トンネルで事業所間をブリッジ接続する(Ethernet over IP ブリッジ)」(P.862)の手順 13.~26.を参考に、ブリッジ情報を設定します。
- **13. 画面左側の [再起動] ボタンをクリックします**。 設定した内容が有効になります。

支社を設定する

「本社を設定する」を参考に、支社を設定します。

この例では、LAN側のIPアドレス、PPPoEの接続先情報(認証情報)、IPv4トンネルのエンドポイントアドレス以外は、本社とすべて同じです。

2.41.3 スイッチポートを独立ポートとして使用する

適用機種 Si-R180,180B

スイッチポートをそれぞれ独立したLANポートとして使用する場合の設定方法を説明します。



● 設定条件

[基幹ネットワーク側]

- 本装置のIPアドレス : 10.200.100.1
- 本装置のネットワークアドレス/ネットマスク : 10.200.100.0/24
- ルーティング制御として RIP (Version2)を使う

[ネットワーク1~4側]

本装置のIPアドレスは以下のとおり	
ネットワーク1	: 192.168.1.1
ネットワーク2	: 192.168.2.1
ネットワーク3	: 192.168.3.1
ネットワーク4	: 192.168.4.1

- 本装置のネットワークアドレスおよびネットマスクは以下のとおり ネットワーク1 : 192.168.1.0/24 ネットワーク2 : 192.168.2.0/24 ネットワーク3 : 192.168.3.0/24 ネットワーク4 : 192.168.4.0/24
- ネットワーク1~4ではVLANタグは使用しない
- ネットワーク1~4に対して、タグなし VLAN ID としてそれぞれ 10~13を割り当てる
- ネットワーク1~4ではDHCPサーバ機能を使用する
- ネットワーク1~4はそれぞれSW1~SW4ポートを使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

- 設定メニューのルータ設定で「スイッチ情報」をクリックします。
 「スイッチ情報」ページが表示されます。
- **2. 「基本情報」をクリックします。** 「基本情報」が表示されます。
- 3. 以下の項目を指定します。

• スイッチ	→使用する	
■基本情報		3
スイッチ	○使用しない⊙使用する	

- 4. [保存] ボタンをクリックします。
- 5. スイッチ情報の設定項目の「ポート情報」をクリックします。 「ポート情報」が表示されます。
- ポート1の【修正】ボタンをクリックします。
 「ポート情報」ページが表示されます。
- 7. 以下の項目を指定します。
 - VLAN ID
 Untagged

→10

			<ポート情報入力フィールド>
	スイッチポート		●使用する●使用しない
	転送レート		自動認識 💙
	MDI		●自動 ○ MDI ○ MDI-X
1	フロー制御機能		⊙使用する○使用しない
	VLAN ID	Tagged	
		Untagged	10

- 8. [保存] ボタンをクリックします。
- 9. 手順6.~8.を参考に、ポート2~4をそれぞれ VLAN ID 11~13 に設定します。
- **10.** 設定メニューのルータ設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

- **11.** 「LAN 情報」でインタフェースがLAN0の [修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- **12. 「IP 関連」をクリックします**。 IP 関連の設定項目と「IP アドレス情報」が表示されます。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 10.200.100.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報			
IPv4	⊙使用する○使用しない		
IPアドレス	 ○ DHCPで自動的に取得す ● 指定する IPアドレス ネットマスク ブロードキャストアドレ ス 	る 10.200.100.1 24 (255.255.255.0) ▼ ネットワークアドレス+オール1 ▼	

- 14. [保存] ボタンをクリックします。
- **15. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 16. 以下の項目を指定します。
 - インタフェース

→ VLAN

<l< th=""><th>AN情報追加フィールド></th></l<>	AN情報追加フィールド>
インタフェース	VLAN 💌

17. [追加] ボタンをクリックします。

「LAN1 情報(VLAN)」ページが表示されます。

18. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 19. 以下の項目を指定します。
 - ・ 出力先
 →スイッチ
 - VLAN ID → 10

■基本情報	3
出力先	スイッチ 🗸
VLAN ID	10

- 20. [保存] ボタンをクリックします。
- **21.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

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

■IPアドレス情報			
IPv4	●使用する●使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.1.1 ネットマスク 24 (255.255.0) ▼ ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 		

23. [保存] ボタンをクリックします。

24. 「2.41.1 スイッチポートを HUB として使用する」(P.940)の手順 14. ~ 16. を参考に、以下の項目を設定します。

- DHCP機能 →サーバ機能
 割当て先頭IPアドレス → 192.168.130.2
 割当てアドレス数 → 64
 リース期間 →1日
- デフォルトルータ広報 → 192.168.130.1
- DNSサーバ広報 → 10.200.100.10

25. 手順 15.~23.を参考に、以下の項目を設定します。

「LAN2情報		(VLAN)]	-	「共通情	報」
「基	基本情報」				
•	出力先				→スイッチ

• VLAN ID → 11

「LAN2 情報(VLAN)」-「IP 関連」 「IP アドレス情報」

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

「LAN3情報(VLAN)」-「共通情報」

「基本情報」

- ・ 出力先
 →スイッチ
- VLAN ID → 12

「LAN3 情報(VLAN)」-「IP 関連」 「IP アドレス情報」

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

「LAN4 情報(VLAN)」-「共通情報」 「基本情報」

- ・ 出力先 →スイッチ
- VLAN ID → 13

「LAN4 情報(VLAN)」-「IP 関連」 「IP アドレス情報」

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 192.168.4.1
 ネットマスク → 24 (255.255.255.0)

26. 画面左側の [再起動] ボタンをクリックします。

設定した内容が有効になります。

スイッチポートを分割して使用する 2.41.4



4つのスイッチポートを2ポートずつに分割して使用する場合の設定方法を説明します。



LSR (Label Switching Router): MPLSコアルータ RR (Route Reflector) :ルートリフレクタ

● 設定条件

- MPLS 網の使用条件 BGP AS 番号 RRのIPアドレス MPLS網で使用する IPv4 ネットワーク
- VPN-Aの使用条件 ルート識別子 使用するネットワーク
- VPN-Bの使用条件 ルート識別子 使用するネットワーク

: 10 : 172.16.100.1 : OSPF : バックボーンエリア : 10:1 :10.10.10/24 川崎事業所 : 10.10.20/24 東京事業所 : 10.10.21/24 東京事業所

: 10:2 : 10.20.10/24 川崎事業所 : 10.20.20/24 東京事業所 : 10.20.21/24 東京事業所

[本装置1]

- スイッチポートを事業所内ネットワークの接続ポートとして使用する
- 川崎事業所のネットワークでは VLAN タグを使用しない
- スイッチポートの2ポートずつを異なるネットワークとし、VLAN ID、LAN 定義およびネットワークアドレ ٠ スを以下のように対応付ける

-	SW1、SW2		
	VLAN ID 2	LAN 定義:LAN1	ネットワークアドレス:10.10.10.0/24
-	SW3、SW4		
	VLAN ID: 3	LAN定義:LAN2	ネットワークアドレス: 10.20.10.0/24

設定事例集(/33)	第2章	活用的
• LAN	0のIPアドレス	: 172.16.2.2	
• LAN	1のIPアドレス	: 10.10.10.1	
• LAN	2のIPアドレス	: 10.20.10.1	
• LAN	0~2では、NAT機能および[OHCP クライアント機能は使用しない	
• ルー	プバックインタフェースのIP	アドレス : 10.1.1.1	
• ルー	プバックインタフェースでの	ルーティングプロトコル :OSPF	
• ルー	プバックインタフェースでの	OSPFエリアID : 0.0.0.1	
• LAN	0でのルーティングプロトコル	L : OSPF	
• LAN	0でのOSPFエリアID	: 0.0.0.1	
• LAN	2で使用するVPN	: VPN-A	
• LAN	3で使用する VPN	: VPN-B	
[本装置	2]		
• スイ	ッチポートを事業所内ネット	ワークの接続ポートとして使用する	
● 川崎	事業所のネットワークではVL	_AN タグを使用しない	
- SV VL - SV VL	V1、SW2 AN ID:2 LAN 定義:L V3、SW4 AN ID:3 LAN 定義:L	AN1 ネットワークアドレス:10.10.20.0/24 AN2 ネットワークアドレス:10.20.20.0/24	
• I AN	0のIPアドレス	: 172 16 1 2	
• LAN	1のIPアドレス	: 10.10.20.1	
• I AN	2のIPアドレス	: 10 20 20 1	
• LAN	- ~2では、NAT機能および[OHCPサーバ/クライアント機能は使用しない	
 ルー 	プバックインタフェースのIP	アドレス : 10.2.1.1	
 ルー 	プバックインタフェースでの	ルーティングプロトコル :OSPF	
 ルー 	プバックインタフェースでの	OSPFエリアID : 0.0.0.2	
• LAN	0でのルーティングプロトコル	レ : OSPF	
• LAN	0でのOSPFエリアID	: 0.0.0.2	
• LAN	1で使用するVPN	: VPN-A	
• LAN	1で使用する BGP/MPLS VPN	Iスタティック経路情報	
あて	先IPアドレス	: 10.10.21.0/24	
中継	ルータアドレス	: 10.10.20.2	
• LAN	2で使用するVPN	: VPN-B	
• LAN	2で使用する BGP/MPLS VPN	Iスタティック経路情報	
あて	先IPアドレス	: 10.20.21.0/24	

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

- 1. 設定メニューのルータ設定で「スイッチ情報」をクリックします。 「スイッチ情報」ページが表示されます。
- 2. 「基本情報」をクリックします。 「基本情報」が表示されます。
- 3. 以下の項目を指定します。
 - スイッチ →使用する

120112	

■本午1月報	L	3
スイッチ	○使用しない ⊙使用する	

- [保存] ボタンをクリックします。 4.
- スイッチ情報の設定項目の「ポート情報」をクリックします。 5. 「ポート情報」が表示されます。
- ポート1の [修正] ボタンをクリックします。 6.

「ポート情報」ページが表示されます。

- 7. 以下の項目を指定します。
 - VLAN ID Untagged

→2

<ポート情報入力フィールド>			<ポート情報入力フィールド>
	スイッチポート		⊙使用する○使用しない
	転送レート		自動認識 🖌
	MDI		●自動 ○ MDI ○ MDI-X
1	フロー制御機能		⊙使用する○使用しない
		Tagged	
	VEAN ID	Untagged	2

- 8. [保存] ボタンをクリックします。
- 9. 手順6.~8.を参考に、ポート2、3をVLAN ID 2に、ポート4をVLAN ID 3に設定します。
- 10. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN 情報 | ページが表示されます。
- 11. 「LAN 情報」でインタフェースがLAN0の [修正] ボタンをクリックします。 「LAN0情報(物理LAN)」ページが表示されます。
- 「IP関連」をクリックします。 12. IP関連の設定項目と「IPアドレス情報」が表示されます。

•	IPv4	→使用する
•	IPアドレス	→指定する
	IPアドレス	→172.16.2.2
	ネットマスク	→24 (255.255.255.0)
	ブロードキャストアドレス	→ネットワークアドレス+オール1

I IPアドレ	IPアドレス情報		
IPv4	⊙使用する○使用しない		
IPアドレス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 172.16.2.2 ネットマスク 24 (255.255.255.0) ブロードギャストアドレ ス ネットワークアドレス+オール1 		

- 14. [保存] ボタンをクリックします。
- **15. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 16. 以下の項目を指定します。
 - インタフェース

→ VLAN

	<lan情報追加フィールド></lan情報追加フィールド>
インタフェース	VLAN V

17. [追加] ボタンをクリックします。

「LAN1 情報(VLAN)」ページが表示されます。

18. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- 19. 以下の項目を指定します。
 - ・ 出力先 →スイッチ
 - VLAN ID →2

■基本情報	3
出力先	スイッチ 🗸
VLAN ID	2

20. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

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

■IPアドレス情報			
IPv4	●使用する●使用しない		
IP アド レス	 ○ DHCPで自動的に取得する ○ 指定する IPアドレス 10.10.10.1 ネットマスク 24 (255.255.0) ▼ ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

- 22. [保存] ボタンをクリックします。
- 23. 手順 15.~22.を参考に、以下の項目を設定します。

「LAN2情報	(VLAN)] -	「共通情報」
「基本情報」		
• 出力先		→スイッチ

VLAN ID →3

「LAN2 情報(VLAN)」-「IP 関連」 「IP アドレス情報」

- IPv4 →使用する
- IPアドレス →指定する
 IPアドレス → 10.20.10.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1
- **24.** 「2.9.1 MPLS 網とLAN を使用して接続する」(P.322)を参考に、ループバック情報、OSPF 機能、 MPLS 機能、ルートリフレクタ機能、VRF 情報を設定します。
- **25. 画面左側の [再起動] ボタンをクリックします**。 設定した内容が有効になります。

2.42 アプリケーションフィルタ機能を使う

適用機種 全機種

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させる ことができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト(192.168.1.100)からのみHTTP/TELNET/FTP/SSHサーバ機能へのアクセスを許可する。
- 内部LANのホスト(192.168.1.0/24)からのみTIMEサーバ機能へのアクセスを許可する。
- その他のサーバ機能は制限しない。

こんな事に気をつけて

IP フィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行っていてもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合の設定例を示します。

メンテナンス用のサーバ機能(TELNET/FTP/SSH)にアクセスできる PC を制限する

1. 設定メニューのルータ設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

- 2. 以下の項目を指定します。
 - 定義名

→ ACL0

<acli情報追加フィールド></acli情報追加フィールド>			
定義名	ACLO		

- **3. [追加] ボタンをクリックします**。 「ACL 定義情報(ACL0)」ページが表示されます。
- **4. 「IP 定義情報」をクリックします**。 「IP 定義情報」ページが表示されます。

5. 以下の項目を指定します。

- プロトコル →すべて
 送信元情報
 IP アドレス → 192.168.1.100
 アドレスマスク → 32 (255.255.255)
- あて先情報
 IP アドレス →指定しない
 アドレスマスク →指定しない
- QoS →指定なし

■IP定義情報		
ブロトコル		すべて ▼ (番号指定: ~ その他 ~ を選択時のみ有効です)
送信元時 IPアトレス		192.168.1.100
報	アトレスマ スク	32 (255.255.255.255) 💌
ホア生き IPアトレス		
報	アトレスマ スク	0 (0.0.0.0)
QoS		指定なし ✓ TOS、または、DSCPを選択時に値を入力してくだ さい

- 6. [保存] ボタンをクリックします。
- 設定メニューの基本設定で「装置情報」をクリックします。
 「装置情報」ページが表示されます。
- 8. 「サーバ機能情報」をクリックします。 「サーバ機能情報」ページが表示されます。
- 「FTP サーバ機能」のアプリケーションフィルタ機能に対する[設定]ボタンをクリックします。
 「アプリケーションフィルタ情報」ページが表示されます。
- 10. 「条件にあてはまらない場合の動作」の [修正] ボタンをクリックします。

動作

→ 遮断

<アプリケーションフィルタ情報入力フィールド(条件にあてはまらない場合)>		
動作	 ○ 透過 ○ 遮断 	

12. [保存] ボタンをクリックします。

「アプリケーションフィルタ情報」ページが表示されます。

- 13. 以下の項目を指定します。
 - 動作
 - ACL定義番号 →0

<アプリケーションフィルタ情報入力フィールド>		
動作	⊙透過 ◯ 遮断	
ACL定義番号	0 参照	

→透過

- 14. [追加] ボタンをクリックします。
- **15.** 手順 7. ~ 15. を参考に、TELNET サーバ機能、SSH サーバ機能、HTTP サーバ機能に対しても同様の設定を行います。

TIME サーバ機能を使用できる PC を 192.168.1.0/24 のネットワークに制限する

16. 手順 1.~ 15. を参考に、以下の項目を指定します。

「ACL情報」● 定義名

→ACL1

「ACL定義情報(ACL1)」-「IP 定義情報」

- ・ プロトコル →すべて
 ・ 送信元情報 IP アドレス → 192.168.1.0
- アドレスマスク →24 (255.255.255.0)
- あて先情報
 IP アドレス →指定しない
 アドレスマスク →指定しない
- QoS →指定なし

「サーバ機能情報」- 「アプリケーションフィルタ情報(TIME)」条件にあてはまらない場合の動作

- 動作 →遮断
- アプリケーションフィルタ情報
- 動作 →透過
- ACL定義番号 →1
- 17. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.43 SIP-SIP ゲートウェイ機能を使う

適用機種 全機種

本装置は、SIP電話サービス間の相互接続を行う SIP-SIP ゲートウェイ機能をサポートしています。

こんな事に気をつけて

- ・ 動的 VPN 機能と併用することはできません。
- ・ ゲートウェイのIPアドレスには、本装置に設定されたどれかのインタフェースのIPアドレスを設定します。誤った IPアドレスを設定した場合は、SIP-SIPゲートウェイ機能は正常に動作しません。
- データ通信の負荷が高い場合、音声品質が低下する場合があります。



ここでは、IP Pathfinder および CL シリーズで構成された IP 電話サービスからひかり電話ビジネスタイプへ接続 するゲートウェイ装置として、利用する場合の設定方法を説明します。

● 前提条件

- 内線側は IP Pathfinder および CL シリーズによる IP 電話網が構築されているものとする。
- 外線側はひかり電話ビジネスタイプに接続されているものとする。

● 設定条件

[内線側 (IP Pathfinder および CL シリーズ)]

- ゲートウェイのIPアドレス : 192.168.1.200
- SIPサーバ : 192.168.1.100
- SIPドメイン : voip.fujitsu.com
- ゲートウェイ番号 :9000
- 着信転送先ユーザ名 : 2000

[外線側(ひかり電話ビジネスタイプ)]

- ゲートウェイのIPアドレス : 192.168.3.222
- 網アドレス : 10.200.100.4
- IP電話番号 :0123456789
- ユーザID
 userid
- パスワード : userpass

上記の設定条件に従って設定を行う場合の設定例を示します。

SIP-SIP ゲートウェイ機能を設定する

- **1. 設定メニューのルータ設定で「SIP-SIP ゲートウェイ情報」をクリックします**。 「SIP-SIP ゲートウェイ情報」ページが表示されます。
- 2. 「基本情報」をクリックします。

「基本情報」が表示されます。

- 3. 以下の項目を指定します。
 - SIP-SIPゲートウェイ情報 →使用する

■基本情報	3
SIP-SIPゲートウェイ機能	○使用しない⊙使用する

- 4. [保存] ボタンをクリックします。
- 5. 「内線情報」をクリックします。

「内線情報」が表示されます。

6. 以下の項目を指定します。

- サービス情報
 ユーザ名 → 9000
 着信転送先ユーザ名 → 2000

 プライマリ Proxy サーバ情報
- IPアドレス → 192.168.1.100
 ユーザエージェント情報 自IPアドレス → 192.168.1.200

サービスドメイン名	→voip.fujitsu.com
■内線情報	

	サービス種別	IP PathfinderおよびCLシリーズ	
	ユーザ名	9000	
サービス情報	認証ユーザ名		
	認証バスワード		
	着信転送先ユーザ名	2000	
ブライマリ	IPアドレス	192.168.1.100	
Proxyサーバ情報	ボート番号	5060	
セカンダリ	IPアドレス		
Proxyサーバ情報	ボート番号	5060	
バックアップ	IPアドレス		
Proxyサーバ情報	ボート番号	5060	
フーザエージェント情報	自IPアトレス	192.168.1.200	
ユーリエーノエノド旧牧	サーヒストメイン名	voip.fujitsu.com	

[3]

7. [保存] ボタンをクリックします。

8. 「外線情報」をクリックします。

「外線情報」が表示されます。

•	サービス情報	
	ユーザ名	→0123456789
	認証ユーザ名	→userid
	認証パスワード	→userpass
•	プライマリ Proxy サーバ情報	
	IPアドレス	→ 10.200.100.4
•	ユーザエージェント情報	

▶ ユーサエーシェント情報	
自IPアドレス	→ 192.168.3.222
サービスドメイン名	→ 10.200.100.4

■外線情報			
	サーヒス種別	ひかり電話ビジネスタイプ	
	ユーザ名	0123456789	
サービス情報	認証ユーザ名	userid	
	認証バスワード		
Registrar	IPアトレス		
サーバ情報	ポート番号	5060	
ブライマリ	IPアトレス	10.200.100.4	
Proxyサーバ情報	ポート番号	5060	
セカンダリ	IPアトレス		
Proxyサーバ情報	ポート番号	5060	
バックアップ	IPアドレス		
Proxyサーバ情報	ポート番号	5060	
フーザエージェント情報	自IPアドレス	192.168.3.222	
ユーリエーノエンド情報	サービストメイン名	10.200.100.4	

10. [保存] ボタンをクリックします。

11. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

2.44 IEEE802.1X 認証機能を使う

適用機種 Si-R240,240B

IEEE802.1X認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権限を持っているか を検証することができます。

● 参照 Si-Rシリーズ 機能説明書「2.30 IEEE802.1X 認証機能」(P.146)

2.44.1 有線 LAN と無線 LAN で IEEE802.1X 認証機能を使う



ここでは、有線LANおよび無線LANインタフェースでIEEE802.1X認証を行う場合の設定方法を説明します。

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

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



	設定条件	
有	線 LAN を使ってローカルサーバに	接続する
•	利用するポート	: lan0
•	IPアドレス	: 192.168.0.1/24
有	線LAN でIEEE802.1X 認証を行って	C端末を収容する
•	利用するポート	: lan1
•	IPアドレス	: 192.168.10.1/24
•	IEEE802.1X認証	:有効
•	IEEE802.1X 認証(認証サーバ)	: aaa1
•	その他	:接続端末のアドレスは DHCP 機能を利用する
無	線LAN でIEEE802.1X 認証を行って	C端末を収容する
•	利用するポート	: slot1
•	利用する論理定義	: lan2
•	利用する回線定義	: wlan0
•	通信モード	: IEEE802.11g
•	チャネル	: 10
•	SSID	: samplenet
•	認証モード	:WPA/WPA2 自動判別認証
•	IEEE802.1X認証	:有効
•	IEEE802.1X 認証(認証サーバ)	: aaa1
•	IPアドレス	: 192.168.20.1/24
•	その他	:接続端末のアドレスは DHCP 機能を利用する
デ	ータ通信カードを使ってインターネ	ットへ接続する
•	利用するポート	: slot0
•	認証ID	:通信事業者から提示された内容
•	認証パスワード	:通信事業者から提示された内容
•	電話番号	:通信事業者から提示された内容
•	無通信監視タイマ	:無通信監視時間を1分とする
認	証/課金サーバを AAA 定義で指定	する
•	aaa定義番号	: aaa1
•	認証サーバIPアドレス	: 192.168.0.100
•	認証サーバシークレットキー	: passwd
•	課金サーバIPアドレス	: 192.168.0.100

• 課金サーバシークレットキー : passwd

上記の設定条件に従って設定を行う場合の設定例を示します。

端末を設定する

無線 LAN アダプタの設定マニュアルを参考に設定を行ってください。

本装置を設定する

有線LANを使ってローカルサーバに接続する

- **1. 設定メニューのルータ設定で「LAN情報」をクリックします**。 「LAN情報」ページが表示されます
- **2.** 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

4. 以下の項目を指定します。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス →192.168.0.1
 ネットマスク →24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報				
IPv4	⊙使用する○使用しない			
IP アド レス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス 192.168.0.1 ネットマスク 24 (255.255.255.0) ブロードキャストアドレ ス ネットワークアドレス+オール1 			

5. [保存] ボタンをクリックします。

有線LANでIEEE802.1X認証を行って端末を収容する

- 6. 設定メニューのルータ設定で「認証情報」をクリックします。 「認証情報」ページが表示されます。
- 「IEEE802.1X 認証情報」をクリックします。
 「IEEE802.1X 認証情報」が表示されます。
- 8. 以下の項目を指定します。
 - IEEE802.1X認証 →使用する
 - 認証方式 → MAC アドレスごと

■IEEE802.1X認証情報		3
IEEE802.1X認証	○使用しない ⊙使用する	
認証方式	⊙ MACアドレスごと ○ボートごと	

9. [保存] ボタンをクリックします。

10. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

11. 以下の項目を指定します。

インタフェース →物理LAN
 <LAN情報追加フィールド>
 インタフェース 物理LAN

12. [追加] ボタンをクリックします。

「LAN1 情報(物理 LAN)」ページが表示されます。

13. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

- 14. 以下の項目を指定します。
 - IPv4 →使用する
 - IPアドレス →指定する
 IPアドレス → 192.168.10.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	⊙使用する○使用しない	
IP アド レス	 ○ DHCPで自動的に取得する ● 指定する IPアドレス IPアドレス 192.168.10.1 ネットマスク 24 (255.255.255.0) マ ブロードキャストアドレ ス ネットワークアドレス+オール1 ▼ 	

- 15. [保存] ボタンをクリックします。
- 16. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

17. 「IEEE802.1X 認証情報」をクリックします。 「IEEE802.1X 認証情報」が表示されます。

•	認証動作モード	→使用する
"伢	使用する"を選択すると、以下の項目	目が指定できます。
•	認証方式	→デフォルト
•	ポート認証制御	→自動
•	認証失敗時再認証抑止時間	→1分
•	認証開始送信間隔	→30秒
•	EAP応答待ち時間	→30秒
•	EAP再送回数	→ 2
•	再認証間隔	→時間指定 1時間
•	参照する AAA 情報	→ 0

■IEEE802.1X認証情報	3
認証動作モート	○使用しない ⊙使用する
認証方式	◎デフォルト ○ MACアドレスごと ○ポート ごと
ボート認証制御	●自動○認証拒否○認証許容
認証失敗時再認証抑止時 間	1 分 🗸
認証開始送信間隔	30 秒 💙
EAP応答待ち時間	30 秒 🗸
EAP再送回数	2 0
再認証間隔	 ●時間指定 1 時間 ▼ ● 再認証しない
参照するAAA情報	0

- 19. [保存] ボタンをクリックします。
- **20.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

21. 「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

DHCP情報					
	0	使用しない	١		
	0	リレー機能	能を使用する	5	
		DHCPサ	ーバIPアドレ	,ス1	
		DHCPサ	ーバIPアドレ	,ス2	
		мастк	レスチェック	,	 ロホストデータベース ロAAA 参照するAAA情報
	۲	」 サーバ機	能を使用す	3	
		割当て先 ス	頭IPアドレ	192.1	68.10.10
		割当てア	ドレス数	10	
		リース期		1	
		デフォルトルータ広 報		192.1	68.10.1
DHCP		DNSサ	ブライマリ	192.1	68.10.1
機能		報	セカンダリ		
		ドメイン名	広報	lan.co	om
		TIMEサー	-バ広報		
		NTPサー	バ広報		
		WINSサ	ブライマリ		
		報	セカンダリ		
			記述形式	٥ŀ	メイン名 OIPアドレス
		ISIPサー バ広報	ブライマリ		
		セカンダリ			
		MACアドレスチェッ ク		∎≉	マストデータベース
				A	AA 参照するAAA情報
		※"割当で ークアドレ	「先頭アドレ ス内である	ス"カ ことを	「本装置のIPアドレスと同じネットワ」 「確認してください。

23. [保存] ボタンをクリックします。

無線LANでIEEE802.1X認証を行って端末を収容する

無線 LAN 情報を設定する

- **24. 設定メニューのルータ設定で「無線 LAN 情報」をクリックします**。 「無線 LAN 情報」ページが表示されます。
- 25. 以下の項目を指定します。
 - ポート

→スロット1-0

<海	無線LAN情報追加フィールト">
₩ - ►	スロット1-0 💌

26. [追加] ボタンをクリックします。

無線 LAN0 情報の設定項目と「回線情報」が表示されます。

27. 以下の項目を指定します。

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

■回線情報	3
ボート	고ㅁット1-0 🗸
通信モート	11g 🔽
チャネル	10 🗸
SSID	samplenet

- 28. [保存] ボタンをクリックします。
- 「認証/暗号化情報」をクリックします。 29. 「認証/暗号化情報」が表示されます。

30. 以下の項目を指定します。

- 認証モード →wpa/wpa2
- WPA 暗号化モード →TKIP/AES自動判別
- キー更新間隔(GTK) →10分
- MIC エラー検出 →使用しない

■認証/暗号化情報		3
認証モート	wpa/wpa2 🗸	
WPA暗号化モート	◎ TKIP/AES自動判別 ○ TKIP ○ AES	
キー更新間隔(GTK)	10 分 💌	
MICエラー検出	●使用しない●使用する	

31. [保存] ボタンをクリックします。

LAN (無線 LAN) 情報を設定する

- 設定メニューのルータ設定で「LAN情報」をクリックします。 32. 「LAN情報」ページが表示されます。
- 33. 以下の項目を指定します。
 - インタフェース →無線LAN

	<lan情報追加フィールド></lan情報追加フィールド>	
インタフェース	無線LAN 🗸	

[追加] ボタンをクリックします。 34.

「LAN2情報(無線LAN)」ページが表示されます。

「共通情報」をクリックします。 35. 共通情報の設定項目と「基本情報」が表示されます。

● 無線 LAN 定義
 →無線 LAN0

■基本情報	3
無線LAN定義	無線LAN 0 💙

[es]

- 37. [保存] ボタンをクリックします。
- **38.** 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

39. 以下の項目を指定します。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 192.168.20.1
 ネットマスク → 24 (255.255.255.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報			
IPv4	●使用する●使用しない		
IP アド レス	 ● 指定する IPアドレス ネットマスク ブロードキャストアドレス ス 	192.168.20.1 24 (255.255.255.0) ・ ネットワークアドレス+オール1 ・	

- 40. [保存] ボタンをクリックします。
- **41. 「共通情報」をクリックします**。 共通情報の設定項目と「基本情報」が表示されます。
- **42.** 「IEEE802.1X 認証情報」をクリックします。

「IEEE802.1X 認証情報」が表示されます。

43. 以下の項目を指定します。

認証動作モード →使用する
 "使用する"を選択すると、以下の項目が指定できます。

参照する AAA 情報

IEEE802.1X認証情報		3
認証動作モート	○使用しない ⊙使用する	
参照するAAA情報	0	

→0

44. [保存] ボタンをクリックします。

45. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

46. 「DHCP 情報」をクリックします。

「DHCP情報」が表示されます。

47. 以下の項目を指定します。

■DHCP情報 []								
	○使用しない							
	○リレ-	ルー機能を使用する						
DHCP 機能	DHC	DHCPサーバIPアドレ						
	DHC	DHCPサーバIPアドレ						
	МАС	MACアドレスチェック			□ホストデータベース			
					■AAA 参照するAAA情報			
	●サー	サーバ機能を使用す						
	割当 ス	割当て先頭IPアドレ ス			68.20.10			
	割当	割当てアドレス数						
	リーン	リース期間			8 💌			
	デフ 報	デフォルトルータ広 報		192.1	68.20.1			
	DNS	サ	ブライマリ	192.168.20.1				
	報	報	セカンダリ					
	ドメー	ドメイン名広報		wlan.	com			
	TIME	TIMEサーバ広報						
	NTP	NTPサーバ広報						
	WINS	WINSサ	ブライマリ					
	報	114	セカンダリ					
		SIPサー バ広報	記述形式	<u>ار</u>	メイン名 OIPアドレス			
	SIPt バ広		ブライマリ					
			セカンダリ					
	MAC	MACアドレスチェッ ク		∎≉	マストデータベース			
	ク			ΠA	AA 参照するAAA情報			
	※"割当て先頭アドレス"が本装置のIPアドレスと同じネットワ ークアドレス内であることを確認してください。							

48. [保存] ボタンをクリックします。

データ通信カードを使ってインターネットへ接続する

WAN情報を設定する

49. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

50. 以下の項目を指定します。

 回線インタフェース 	→データ通信カード				
<wan情報追加フィールド></wan情報追加フィールド>					
回線インタフェース	データ通信カード 🖌				

- **51.** 【追加】ボタンをクリックします。 「WAN 情報(データ通信カード)」ページが表示されます。
- 52. 以下の項目を指定します。
 - ポート →スロット0-0
 基本情報 ジョ
 ボート スロット0-0 マ
- 53. [保存] ボタンをクリックします。

相手情報を設定する

- **54. 設定メニューのルータ設定で「相手情報」をクリックします**。 「相手情報」ページが表示されます。
- **55. 「ネットワーク情報」をクリックします。** 「ネットワーク情報」が表示されます。
- 56. 以下の項目を指定します。
 - ネットワーク名 → internet

<ネットワーク情報追加フィールド>					
ネットワーク名	internet				

57. [追加] ボタンをクリックします。

「ネットワーク情報 (internet)」ページが表示されます。

- 58. 「共通情報」をクリックします。 共通情報の設定項目と「基本情報」が表示されます。
- 59. 以下の項目を指定します。
 - 自動接続

自動接続 ●する Oしない

)

→する

- 60. [保存] ボタンをクリックします。
- **61**. 「PPP 関連」をクリックします。

PPP関連の設定項目と「圧縮情報」が表示されます。
- ヘッダ圧縮(IPCP) →チェックしない
- ヘッダ圧縮(IPV6CP) →チェックしない

■圧縮情報	3
ヘッダ圧縮 (IPCP)	□VJ □IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	□IPヘッダ圧縮

63. [保存] ボタンをクリックします。

64. 「IP 関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

65. IP 関連の設定項目の「スタティック経路情報」をクリックします。 「スタティック経路情報」が表示されます。

66. 以下の項目を指定します。

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

	<スタティック経路情報入力フィールド>
ネットワーク	 ● デフォルトルート ● ネットワーク指定 あて先IPアドレス あて先アドレスマスク 0 0.0.0.0)
メトリック値	1 💌
優先度	0

67. [追加] ボタンをクリックします。

68. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

69. 以下の項目を指定します。

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

NAT情報	3
NATの使用	●使用しない●NAT●マルチNAT●静的NATのみ
グローバルアドレス	
アトレス個数	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
アドレス割当てタイマ	5 分 🗸
NATセキュリティ	○通常 ⊙ 高い

- 70. [保存] ボタンをクリックします。
- 71. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

- 接続先名
- 接続先種別 →データ通信カード接続

→ISP-1

<接続先情報追加フィールド>			
接続先名	ISP-1		
接続先種別	 データ通信カード接続 ダイヤル1 電話番号 PPPoE接続 IPトンネル接続 IPsec/IKE接続 別インタフェースから送出 MPLSトンネル接続 パケット破棄 		

73. [追加] ボタンをクリックします。

「接続先情報(ISP-1)」ページが表示されます。

- **74. データ通信カード接続の設定項目の「接続制御情報」をクリックします**。 「接続制御情報」が表示されます。
- 75. 以下の項目を指定します。
 - 無通信監視タイマ →送受信パケットについて60秒

■接続制	御情報	3
無通信監 視タイマ	送受信パケット 🗸 について 60 秒	

- 76. [保存] ボタンをクリックします。
- 77. データ通信カード接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

- 78. 以下の項目を指定します。
 - ・ 送信認証情報
 認証 ID → (通信事業者から提示された内容)
 認証パスワード → (通信事業者から提示された内容)

PPP情報		3
	認証ID	
达后路延用牧	認証バスワード	

79. [保存] ボタンをクリックします。

ProxyDNS情報、URLフィルタ情報を設定する

- **80. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします**。 「ProxyDNS 情報/URL フィルタ情報」ページが表示されます。
- **81. 「順引き情報」をクリックします**。 「順引き情報」が表示されます。

- ドメイン名
- タイプ
- 送信元 IP アドレス

→指定しない

動作 →接続先のDNSサーバへ問い合わせる
 ネットワーク名 → internet

→ *

→すべて

- <順引き情報入力フィールド> ドメイン 名 "その他"を選択時のみ有効で すべて <mark>∨(</mark>番号指定 タイプ す。) 送信元 IPアドレ ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィッ スクス長形式で入力してください。 ○ 廃棄する ⊙ 接続先のDNSサーバへ問い合わせる ネットワーク名 internet 💌 ■ 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 りわせる ネットワーク名 rmt0 🔽 動作 解決したホストへのホスト経路自動作成 のしない のする ○ DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 使用できるインタフェースが存在しません 🔽 ○ 設定したDNSサーバへ問い合わせる DNSサーバアドレス
- 83. [追加] ボタンをクリックします。
- **84. 「逆引き情報」をクリックします**。 「逆引き情報」が表示されます。
- 85. 以下の項目を指定します。
 - ネットワークアドレス →すべて
 - 動作 →接続先のDNSサーバへ問い合わせる
 ネットワーク名 → internet



86. [追加] ボタンをクリックします。

認証/課金サーバをAAA定義で指定する

87. 設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA情報」ページが表示されます。

88. 以下の項目を指定します。

	グループ名	→aaasvr
ſ		<グループID情報追加フィールド>
	グループ名	aaasvr

89. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

90. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

91. 以下の項目を指定します。

- RADIUSサービス →クライアント機能
 認証 →チェックする
 アカウンティング →チェックする
- Message-Authenticator →使用しない

■基本情報	3
RADIUSサービス	クライアント機能 ▼ 図認証 マアカウンティング (クライアント機能また(はサーバ機能を選択した 場合(このみ有効となります)
自側認証IPアドレス	
自側アカウンティンク IPアトレス	
Message- Authenticator	○使用する ◎使用しない

92. [保存] ボタンをクリックします。

93. RADIUS **関連の設定項目の「サーバ情報」をクリックします**。 「サーバ情報(クライアント機能)」が表示されます。

94. 認証情報1の[修正]ボタンをクリックします。

以下の項目を指定します。 95.

•	認証情報1	
	共有鍵	→passwd
	サーバIPアドレス	→ 192.168.0.100
	サーバUDPポート	→ 1812
	復旧待機時間	→0秒
	優先度	→ 0
	自側認証IPアドレス	→ 192.168.0.1

	共有鍵	
	サーバIPア ドレス	192.168.0.100
	サーバ UDPポート	⊙1812 ◯1645
認証情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側認証 IPアドレス	192.168.0.1

96. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

97. アカウンティング情報1の[修正]ボタンをクリックします。

98. 以下の項目を指定します。

• アカウンティング情報1 共有鍵 →passwd サーバIPアドレス → 192.168.0.100 サーバ UDP ポート →1813 復旧待機時間 →0秒 優先度 →0 自側アカウンティングIPアドレス →192.168.0.1

	共有鍵	•••••
	サーバIPア ドレス	192.168.0.100
	サーバ UDPポート	⊙1813 ◯1646
アカウンティング情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側アカウ ンティング IPアドレス	192.168.0.1

99. アカウンティング情報1の[保存]ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

100. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。



データ通信カードの認証 ID、パスワード、電話番号については、「1.7 インターネットへデータ通信カードを使用して 補記
テーク週间
月一日の回回にし、
たいれば、
たい

2.45 不正端末アクセス防止機能(MAC アドレス認証) を使う

適用機種 全機種

不正端末アクセス防止機能(MACアドレス認証)を使用すると、本装置のローカルLANに接続する端末がリモートネットワークへのアクセス権限を持っているかを認証することができます。

こんな事に気をつけて

MAC アドレス認証で利用する AAA のグループ ID を正しく設定してください。



ここでは、リモートネットワークへの接続がすでに設定されている場合を例にMACアドレス認証機能を利用する設定方法を説明します。

● 設定条件

- LAN0、LAN1 ポートで MAC アドレス認証を使用する
- LAN0、LAN1 ポートで利用する認証データベース LAN0 ポート
 : RADIUS サーバ
 LAN1 ポート
 : ローカルで設定した認証情報

: 0

: 1

- AAA グループID
 LAN0 ポート
 LAN1 ポート
- ローカル LAN-B で利用可能なユーザは以下のとおり

ユーザ	MACアドレス
PC11	00:11:11:00:00:01
PC12	00:22:22:00:00:02

• リモートネットワークへの接続定義は設定済み

- RADIUS サーバはリモートネットワークに接続
- RADIUSサーバのIPアドレス : 172.16.1.100
- RADIUS サーバのシークレット : radius-secret

上記の設定条件に従って設定を行う場合の設定例を示します。

MACアドレス認証で使用するパスワードを設定する

- 設定メニューのルータ設定で「認証情報」をクリックします。
 「認証情報」ページが表示されます。
- 「MACアドレス認証情報」をクリックします。
 「MACアドレス認証情報」が表示されます。
- 3. 以下の項目を指定します。
 - パスワード → macauth-pass
 - パスワードの確認 → macauth-pass

MACアドレス認証情報		3
バスワード	•••••	
バスワードの確認	•••••	

4. [保存] ボタンをクリックします。

MACアドレス認証を使用する

- 5. 設定メニューのルータ設定で「LAN 情報」をクリックします。 「LAN 情報」ページが表示されます。
- 6. 「LAN 情報」でインタフェースがLAN0の[修正] ボタンをクリックします。 「LAN0 情報(物理LAN)」ページが表示されます。
- 「共通情報」をクリックします。
 共通情報の設定項目と「基本情報」が表示されます。
- 8.
 「MAC アドレス認証情報」をクリックします。

 「MAC アドレス認証情報」が表示されます。
- 9. 以下の項目を指定します。

MACアドレ	ス認証情報	3
	 ○ 使用しない ③ 使用する 	
	参照するAAA情報 0	
認証機能	認証成功保持時間 20 分 🗸	
	認証失敗保持時間 5 分 💌	
	認証セキュリティ ●高い ●通常	

10. [保存] ボタンをクリックします。

11. 手順5.~10.を参考に、LAN1ポートを指定します。

「LAN1 情報(物理 LAN)」-「共通情報」 「MAC アドレス認証情報」

- 認証機能 →使用する
- 参照する AAA 情報 → 1

RADIUS サーバを利用する AAA グループ情報を設定する

- **12. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **13. 「グループ ID 情報」をクリックします**。 「グループ ID 情報」が表示されます。

14. 以下の項目を指定します。

グループ名 → localAuth

<グループID情報追加フィールド> グループ名 localAuth

- **15. [追加] ボタンをクリックします**。 「グループID情報(0)」と設定項目が表示されます。
- 16. 手順 12.~15.を参考に、グループ名を追加します。
 - グループ名 → radiusAuth
- **17. [追加] ボタンをクリックします**。 「グループID情報(1)」と設定項目が表示されます。

18. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

19. 以下の項目を指定します。

- RADIUSサービス →クライアント機能
 認証 →チェックする
 アカウンティング →チェックしない
- 自側認証 IP アドレス → 172.16.1.101

■基本情報	3
RADIUSサービス	クライアント機能 ✓ ✓ ✓ ✓ ✓ ✓ Ø認証□アカウンティング 〈クライアント機能またはサーバ機能を選択した 場合にのみ有効となります)
自側認証IPアトレス	172.16.1.101

- 20. [保存] ボタンをクリックします。
- **21.** RADIUS **関連の設定項目の「サーバ情報」をクリックします**。 「サーバ情報(クライアント機能)」が表示されます。
- 22. 認証情報1の[修正]ボタンをクリックします。

 認証情報1 共有鍵 サーバIPアドレス

→ radius-secret → 172.16.1.100

	共有鍵	•••••
	サーバIPア ドレス	172.16.1.100
	サーバ UDPポート	⊙ 1812 ◯ 1645
認証情報 1	復旧待機 時間	0 秒 🗸
	優先度	0
	自側認証 IPアドレス	

24. 認証情報1の[保存] ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

ローカル認証情報を利用する AAA グループ情報を設定する

- **25. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **26. 「グループID 情報」をクリックします**。 「グループID 情報」が表示されます。
- **27.** 「グループID 情報」でグループID が0の [修正] ボタンをクリックします。 「グループID 情報(0)」と設定項目が表示されます。
- **28. 「AAA ユーザ情報」をクリックします**。 「AAA ユーザ情報」が表示されます。
- 29. 以下の項目を指定します。
 - ユーザID

→001111000001

<AAAユーザ情報追加フィールド> ユーザID 001111000001

30. [追加] ボタンをクリックします。

「AAAユーザ情報(0)」と設定項目が表示されます。

31. 「認証情報」をクリックします。

「認証情報」が表示されます。

- 32. 以下の項目を設定します。
 - ユーザID →001111000001
 - ● 認証パスワード
 → macauth-pass

■認証情報		3
ユーザID	001111000001	
認証バスワード		

- 33. [保存] ボタンをクリックします。
- 34. 手順25.~33.を参考に、以下の項目を指定します。

「AAA ユーザ情報(0)」-「認証情報」 「認証情報」

- ユーザID →002222000002
- ● 認証パスワード
 → macauth-pass
- **35. 画面左側の [設定反映] ボタンをクリックします**。 設定した内容が有効になります。

2.46 ARP 認証機能を使う

適用機種 全機種

ここでは、既存のネットワークに本装置を追加して、ARP 認証を行う場合の設定方法を説明します。

こんな事に気をつけて

ARP認証で利用するAAAのグループIDを正しく設定してください。



: 172.16.1.100

● 設定条件

- LAN0でARP認証を使用する
- ARP認証で利用する認証データベース : RADIUS サーバ
- AAA グループのID : 0
- RADIUSサーバのIPアドレス
- RADIUSサーバはLAN1に接続されている
- RADIUSサーバのシークレット :radius-secret
- 認証失敗時の通信妨害を行う

上記の設定条件に従って設定を行う場合の設定例を示します。

RADIUS サーバの LAN を設定する

- **1. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。
 「LAN1 情報(物理LAN)」ページが表示されます。
- 「IP 関連」をクリックします。
 IP 関連の設定項目と「IP アドレス情報」が表示されます。

IPv4 →使用する
 IPアドレス →指定する
 IPアドレス → 172.16.1.200
 ネットマスク → 16 (255.255.0.0)
 ブロードキャストアドレス →ネットワークアドレス+オール1

I IPアドレ	ス情報	3
IPv4	●使用する●使用しない	
IPアドレス	 ○ DHCPで自動的に取得す ○ 指定する IPアドレス ネットマスク ブロードキャストアドレス ス 	る 172.16.1.200 16 (255.255.0.0) ・ ネットワークアドレス+オール1 ・

5. [保存] ボタンをクリックします。

ARP 認証を設定する

- **6. 設定メニューのルータ設定で「LAN 情報」をクリックします**。 「LAN 情報」ページが表示されます。
- 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。
 「LAN0 情報(物理LAN)」ページが表示されます。
- 8. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

- **9. 「ARP 認証情報」をクリックします**。 「ARP 認証情報」が表示されます。
- 10. 以下の項目を指定します。
 - ARP認証情報 →使用する
 "使用する"を選択すると、以下の項目が指定できます。
 - 参照する AAA 情報 →0
 - 通信妨害
 →する

ARP認証情報	3
ARP認証情報	○使用しない ⊙使用する
参照するAAA情報	0
通信妨害	⊖ರರು ⊙ ಕನ

11. 【保存】ボタンをクリックします。

RADIUS サーバを利用する AAA グループ情報を設定する

- **12. 設定メニューのルータ設定で「AAA 情報」をクリックします**。 「AAA 情報」ページが表示されます。
- **13. 「グループID 情報」をクリックします**。 「グループID 情報」が表示されます。

グループ名

→RADIUS

<	ブルーブID情報追加フィール	ド>
グループ名	RADIUS	

15. [追加] ボタンをクリックします。

「グループID情報(0)」と設定項目が表示されます。

16. 「RADIUS 関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

17. 以下の項目を指定します。

• RADIUSサービス	→クライアント機能
認証	→チェックする
アカウンティング	→チェックしない

● 自側認証 IP アドレス → 172.16.1.200

■基本情報	3
RADIUSサービス	クライアント機能 ▼ 図認証 □ アカウンティング 〈クライアント機能また(はサーバ機能を選択した 場合(このみ有効)となります)
自側認証IPアトレス	172.16.1.200

- 18. [保存] ボタンをクリックします。
- **19.** RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報(クライアント機能)」が表示されます。

- 20. 「認証情報1」の[修正] ボタンをクリックします。
- 21. 以下の項目を指定します。
 - 認証情報1 共有鍵 サーバIPアドレス

→ radius-secret → 172.16.1.100

	共有鍵	••••••
認証情報 1	サーバIPア ドレス	172.16.1.100
	サーバ UDPポート	⊙1812 ◯1645
	復旧待機 時間	0 秒 🗸
	優先度	0
	自側認証 IPアドレス	

22. 認証情報1の[保存]ボタンをクリックします。

「サーバ情報(クライアント機能)」に戻ります。

23. 画面左側の [設定反映] ボタンをクリックします。 設定した内容が有効になります。



Α

AAA 認証	
ADSL 回線	21
ADSL モデム	
arp エントリ	
ARP 認証機能	
AS 外部経路	
AS 境界ルータ	
ATM 接続	
ATM 網	

arp エントリ	
ARP 認証機能	
AS 外部経路	
AS 境界ルータ	
ATM 接続	
ATM 網	87´
В	

	.8/1
3	
GP/MPLS VPN	.321
GP4	.127
GP 経路の制御(IPv4)	.282
	000

I (IPv4)		
トラップルータ)		I
	343	I
		I
		I
		1

С

Ε

F

BGP4	127
BGP 経路の制御(IPv4)	
BSR(ブートストラップルータ)	
B チャネル	
0	

DHCP クライアント機能754

DHCP サーバ機能749

DHCP スタティック機能752

DH グループ147, 158

DNS サーバ機能775

DNS サーバの自動切り替え機能(逆引き)......766

DNS サーバの自動切り替え機能(順引き)......764

DNS 問い合わせタイプフィルタ機能773

Ethernet over IP ブリッジ862

В

CATV インターネット接続(かんたん設定)23 COM ポート	IP フィルタリングの ISDN 接続(IPv6) ISDN 接続(LAN)
D	L

Μ

ID タイプ	
IEEE802.1X 認証機能	
IKE	147, 158
IKE セッション監視機能	
Ingress ポリシールーティング機能	É 827
IPsec 機能	
IPsec クライアント	726
IPsec サーバ	726
IPv6	
IPv6 DHCP クライアント機能	
IPv6 over IPv4 トンネル	
IPv6 トンネル	
IPv6 ネットワークの追加	50
IPv6 フィルタリング	
IP-VPN 接続	
IP アドレス	205, 377, 744
IP アドレスの自動割り当て	749
IP トンネル	
IP フィルタリング機能	
IP フィルタリングの条件	
IP フィルタリングの設計方針	
ISDN 接続(IPv6)	
ISDN 接続(LAN)	

LAN のネットワーク間接続42

LSP(トンネルラベルスイッチングパス)....... 292

MAC アドレス752

MPLS LSP トンネル292 MPLS 接続サービス 292

MSS 書き換え機能543

MTU 分割機能545

I

986

NAT	
NAT トラバーサル機能	
NetBIOS サーバ	

N I

IN	
NAT	
NAT トラバーサル機能	
	400

Ο

索引

987

	_
URL フィルタ機能	 77

U

Т TOS/Traffic Class735

SIP-SIP ゲートウェイ機能	.960
SNMP	.779
SNMP エージェント機能	.779
SNTP	43
SPI409,	457
SPT(最短経路)	.363
STP	.846
_	

S

RADIUS 機能924, 9	33
RADIUS 認証452, 5	88
RFC18777	68
RIP 経路の制御(IPv4)2	05
RIP 経路の制御(IPv6)2	20
RP(ランデブーポイント)3	63
•	

R

PIAFS 接続	900
PIM-DM	359
PIM-SM	
PING	443
PPPoE 接続	67
PPPoE 接続(かんたん設定)	19
PPPoE プロトコル	19
Proxy ARP	900
ProxyDNS	764

Ρ

OCN エコノミー	32
OSPFv2 (IPv4)	235
OSPF 機能(IP v 6)	273
OSPF 経路の制御(IPv4)	263

V

W

あ

い

え

お

か

VCC	871, 881
VLAN ID	
VLAN 機能	
VLAN パケット	
VLAN プライオリティマッピング機能	
VoIP NAT トラバーサル機能	
VPC	871, 881
VPN	452, 454
VRRP 機能	

インターネットへ ISDN 接続(かんたん設定)..25 インターネットへ専用線接続(かんたん設定).30

オフィスへ ISDN 接続(かんたん設定)............34

課金単位時間設定843

可変 IP アドレス169 かんたん設定メニュー11

き

既存のネットワーク	16
基本 NAT	715
逆引き	766

<

クラスタリング機能	
グループ ID	
グループ識別子	
グローバルアドレス	

け

経路制御	
ケーブルモデム	23
ケーブルモデム接続	23

こ

構成定義情報切り替え予約	
高速ディジタル専用線	
固定 IP アドレス	145, 156, 456, 552
コネクション確立要求	

さ

サーバの公開	(PPPoE 接続)	718
サーバの公開	(ネットワーク型接続)	721
サーバの公開	(プライベート LAN 接続)	
		724

し

シェーピング	
シェーピング機能	
システムログ	712
システムログの確認	714
自動鍵交換	145, 156, 452, 454, 552
手動鍵交換	
準スタブエリア	
順引き	
冗長化ネットワーク	
冗長構成の通信経路	
省略値	
新 TOS	

す

スイッチポート	
スイッチング HUB	372, 868, 939
スケジュール機能	
スケジュール予約	
スタティックルーティング	
スタブエリア	251

せ

制御	
静的 NAT	
セキュリティ	
セグメント接続/分割(かんたん設定)	15
接続先監視機能	546
専用線接続	61
専用線接続(LAN)	103

そ

送信元情報	 376,	732

た

帯域制御機能	541,	744
ダイヤルアップ接続		23

ち

招调理全	376
吃吃杯亚	

つ

通信の負荷分散 …	 	288
通信バックアップ	 906,	913

τ

データ圧縮機能	742
データ通信カード	
データ通信カード接続	
テンプレート着信機能	
電話番号変更予約	

と

動画 · 音声	
動的 NAT	715
動的 VPN	611, 633
動的経路(RIP)機能	
ドメイン	
トラフィックの制御	
トランジット	
トンネリング	
トンネルエンドポイント	

に

認証情報4

ね

ネットワーク	97, 103
ネットワーク分割	15

は

バックアップ	
バックアップルータ	817
バックボーンエリア	
発信抑止	
発信抑止予約	

ßı

フィルタリング条件(ルーティング)	
フィルタリングの設計方針(ルーテ	ィング)…206
負荷分散通信	
不正端末アクセス防止機能	
プライオリティ	735
プライベート LAN 構築	55
プライベート LAN 構築(かんたん設	定)11
プライベートアドレス	
ブリッジ	
ブリッジグルーピング	
ブリッジグルーピング機能	
フレームリレー接続(LAN)	
フレッツ・ADSL	19, 21, 67
プロトコル	732, 735, 744

く

閉域ネットワーク	109
ヘッダ圧縮機能	742

ほ

方向	
ポート番号	744
ホストデータベース	775
ホストデータベース情報	752
ポリシーベースネットワーク	732
ポリシールーティング機能	

ま

マスタルータ	817
マニュアル構成	9
マルチ NAT	32
マルチ NAT 機能	532, 715
マルチキャスト機能	359
マルチキャスト・パケット	363
マルチダイヤル	25
マルチリンク機能	
マルチルーティング機能	

む

無線 LAN	. 86
無線通信	. 86
無通信監視タイマ	842

め

×	ЬΠ	いク値	205	220
\sim	פיו	ツノ呾	 200,	220

ø

優先順位	. 379
ユニキャスト	. 359

b

リモートアクセスサーバ	
リモートパワーオン機能	
リモートパワーオン予約	

れ

レイヤ 2VPN の構築	
レイヤ 3VPN の構築	

Si-Rシリーズ Web 設定事例集

P3NK-2652-02Z0 発行日 2007年11月

発行責任 富士通株式会社

本書の一部または全部を無断で他に転載しないよう、お願いいたします。

本書は、改善のために予告なしに変更することがあります。
 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、 損害については、弊社はその責を負いません。