

FUJITSU Network Si-R Si-Rシリーズ

Webリファレンス V35

FUJITSU

はじめに

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

2009年11月初版
2010年7月第2版
2012年11月第3版
2013年11月第4版
2014年6月第5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。
Copyright FUJITSU LIMITED 2009 - 2014

目次

はじめに	2
本書の使いかた	8
本書の読者と前提知識	8
本書における商標の表記について	9
本装置のマニュアルの構成	10
1 「設定メニュー」を表示する	11
2 「設定メニュー」の画面体系	12
2.1 かんたん設定メニュー	12
2.2 基本設定	13
2.3 ルータ設定	14
2.4 無線 LAN 管理設定	27
3 インターネットへ ISDN 接続かんたん設定	28
3.1 必須設定	28
3.2 オプション設定	29
4 インターネットへ専用線接続かんたん設定	31
4.1 必須設定	31
4.2 オプション設定	31
5 PPPoE かんたん設定	33
5.1 必須設定	33
5.2 オプション設定	33
6 オフィスへ ISDN 接続かんたん設定	35
6.1 必須設定	35
6.2 オプション設定	36
7 オフィスへ専用線接続かんたん設定	37
7.1 必須設定	37
7.2 オプション設定	37
8 プライベート LAN 構築かんたん設定	39
8.1 必須設定	39
8.2 オプション設定	40
9 セグメント接続／分割かんたん設定	41
9.1 LAN0	41
9.2 LAN1	41
10 パスワード情報	42
10.1 基本情報	42
10.2 ログインパスワード情報	43
10.3 ログインユーザ情報	44
11 装置情報	46
11.1 ルータ名称情報	46
11.2 タイムサーバ情報	47
11.3 システムログ情報	48
11.4 ファームウェア更新情報	50
11.5 異常時動作情報	51
11.6 IPv4 ループバック情報	52
11.7 IPv6 ループバック情報	53
11.8 サーバ機能情報	53
11.8.1 アプリケーションフィルタ情報	56
11.9 外部メディアスタート機能情報	57
12 スケジュール情報	58
12.1 月間／週間予約情報	58

12.2	電話番号変更予約情報	60
12.3	構成定義切り替え予約情報	61
13	WAN 情報	62
13.1	回線インターフェース：ISDN	63
13.1.1	基本情報	63
13.1.2	接続制御情報	65
13.2	回線インターフェース：専用線	66
13.2.1	基本情報	66
13.3	回線インターフェース：フレームリレー	67
13.3.1	基本情報	67
13.4	回線インターフェース：ATM	68
13.4.1	基本情報	68
13.5	回線インターフェース：データ通信カード	69
13.5.1	基本情報	69
14	無線 LAN 情報	70
14.1	回線情報	71
14.2	認証／暗号化情報	73
14.3	MAC フィルタリング情報	76
15	スイッチ情報	78
15.1	基本情報	78
15.2	ポート情報	79
16	LAN 情報	81
16.1	インターフェース：物理 LAN	82
16.1.1	共通情報	82
16.1.2	IP 関連	100
16.1.3	IPv6 関連	137
16.1.4	ブリッジ関連	169
16.1.5	MPLS 関連	177
16.2	インターフェース：VLAN	181
16.2.1	共通情報	181
16.3	インターフェース：無線 LAN	184
16.3.1	共通情報	184
17	シリアル情報	186
17.1	共通情報	186
17.2	モデム情報	187
18	相手情報	188
18.1	ネットワーク情報	188
18.1.1	共通情報	189
18.1.2	接続先情報	191
18.1.3	PPP 関連	252
18.1.4	IP 関連	254
18.1.5	IPv6 関連	296
18.1.6	ブリッジ関連	332
18.1.7	MPLS 関連	339
18.2	着信相手識別情報	342
19	テンプレート情報	343
19.1	接続種別：ISDN	344
19.1.1	共通情報	344
19.1.2	PPP 関連	346
19.1.3	IP 関連	348
19.1.4	IPv6 関連	369

19.2	接続種別 : IPsec/IKE (RADIUS/AAA)	386
19.2.1	共通情報	386
19.2.2	IPsec/IKE 関連	388
19.3	接続種別 : IPsec/IKE (動的 VPN 共有鍵認証方式)	394
19.3.1	共通情報	394
19.3.2	IPsec/IKE 関連	396
19.3.3	動的 VPN 関連	399
19.4	接続種別 : IPsec/IKE (動的 VPN 接続 RSA デジタル署名認証方式)	403
19.4.1	共通情報	403
19.4.2	IPsec/IKE 関連	405
20	LLDP 情報	407
20.1	基本情報	407
21	認証情報	409
21.1	IEEE802.1X 認証情報	409
21.2	MAC アドレス認証情報	410
22	AAA 情報	411
22.1	グループ ID 情報	411
22.1.1	共通情報	411
22.1.2	AAA ユーザ情報	412
22.1.3	RADIUS 関連	425
23	ACL 情報	433
23.1	ACL 定義情報	434
23.1.1	基本定義情報	434
23.1.2	IP 定義情報	435
23.1.3	TCP 定義情報	436
23.1.4	UDP 定義情報	436
23.1.5	ICMP 定義情報	437
23.1.6	IPv6 定義情報	438
23.1.7	MAC 定義情報	439
24	ポリシーグループ情報	440
24.1	ポリシーグループ定義情報	440
24.1.1	パターン定義情報	440
24.1.2	送出先定義情報	442
24.1.3	接続先監視定義情報	443
25	IP 情報	445
25.1	基本情報	445
26	ルーティングプロトコル情報	446
26.1	インターフェース情報	446
26.2	ルーティングマネージャ情報	446
26.2.1	再配布情報	447
26.2.2	優先度情報	450
26.2.3	ECMP 情報	451
26.3	RIP 関連	452
26.3.1	RIP タイマ情報	452
26.3.2	RIP マルチパス情報	453
26.3.3	RIP 再配布フィルタリング情報	453
26.3.4	RIP ユニキャスト送信情報	455
26.3.5	RIP 相手フィルタリング情報	456
26.4	BGP 関連	457
26.4.1	BGP 情報	457
26.4.2	IPv4 BGP ネットワーク情報	459
26.4.3	IPv6 BGP ネットワーク情報	460
26.4.4	IPv4 BGP 集約経路情報	461

26.4.5	IPv6 BGP 集約経路情報	462
26.4.6	BGP 相手情報	463
26.4.7	IPv4 BGP 再配布フィルタリング情報	471
26.4.8	IPv6 BGP 再配布フィルタリング情報	472
26.4.9	IPv4 VRF 情報	473
26.4.10	IPv4 MPLS 連携情報	474
26.5	OSPF 関連	475
26.5.1	ルータ ID 情報	475
26.5.2	OSPF エリア情報	476
26.5.3	AS 境界ルータ情報	482
26.5.4	AS 外部経路集約情報	482
26.5.5	OSPF 再配布フィルタリング情報	483
26.6	IPv6 ルーティングマネージャ情報	485
26.6.1	IPv6 再配布情報	485
26.6.2	IPv6 優先度情報	487
26.7	IPv6 RIP 関連	488
26.7.1	IPv6 RIP タイマ情報	488
26.7.2	IPv6 RIP マルチパス情報	489
26.7.3	IPv6 RIP 再配布フィルタリング情報	489
26.8	IPv6 OSPF 関連	491
26.8.1	IPv6 ルータ ID 情報	491
26.8.2	IPv6 OSPF エリア情報	492
26.8.3	IPv6 AS 境界ルータ情報	495
26.8.4	IPv6 OSPF 再配布フィルタリング情報	496
27	マルチキャスト情報	498
27.1	IP マルチキャスト情報	498
27.2	IP マルチキャストスタティック RP 情報	500
27.3	IP マルチキャストスタティック経路情報	501
28	UPnP 情報	502
28.1	基本情報	502
29	MPLS 情報	503
29.1	基本情報	503
30	ブリッジ情報	504
30.1	ブリッジグループ情報	504
30.1.1	ブリッジグループ情報（グループ識別子 0 の場合）	505
30.1.2	ブリッジグループ情報（グループ識別子 1 ~ 7 の場合）	507
31	動的 VPN 情報	508
31.1	サーバ関連情報	508
31.1.1	基本情報	508
31.2	クライアント関連情報	509
31.2.1	基本情報	509
31.2.2	ドメイン情報	509
32	SIP-SIP ゲートウェイ情報	514
32.1	基本情報	514
32.2	内線情報	515
32.3	外線情報	516
33	SNMP 情報	518
33.1	基本情報	518
33.2	SNMPv1/v2c 情報	520
33.3	SNMPv3 情報	522
33.3.1	ユーザ情報	522
33.3.2	MIB ビュー情報	525
33.4	トラップ情報	526

34	ProxyDNS 情報／URL フィルタ情報	527
34.1	共通情報	528
34.2	順引き情報	529
34.3	逆引き情報	531
35	ホストデータベース情報	533
36	証明書関連情報	535
36.1	自装置証明書情報	535
36.1.1	自装置証明書要求の作成（鍵ペアの作成）	535
36.1.2	自装置証明書の設定	537
36.2	相手装置証明書情報	539
36.2.1	相手装置証明書の設定	539
36.3	認証局証明書情報	540
36.3.1	認証局証明書の設定	540
37	無線 LAN 管理情報	541
37.1	管理グループ情報	541
37.2	管理機器情報	542
37.2.1	基本情報	543
37.3	管理外機器情報	544
38	MAC アドレスフィルタセット情報	545
38.1	MAC アドレスフィルタ情報	545
38.1.1	MAC アドレスフィルタ情報（一括設定）	546
38.1.2	MAC アドレスフィルタ情報（個別設定）	547
39	無線 LAN 管理パラメタ情報	548
39.1	無線 LAN 管理パラメタ	548
	索引.....	551

本書の使いかた

本書では、本装置の設定メニューで表示される画面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。

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

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。



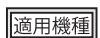
補足

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。



参考

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。



警告

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



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ブン・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。

なお、本文中では[®]を省略しています。

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 [®] 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	
Microsoft [®] Windows [®] 7 64bit Home Premium	Windows 7
Microsoft [®] Windows [®] 7 32bit Professional	

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-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-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-R220D ご利用にあたって	Si-R220D 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-R370B ご利用にあたって	Si-R370B 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-R570B ご利用にあたって	Si-R570B 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。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集	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。
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。
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。
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。
Web 設定事例集	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。
Web リファレンス (本書)	Web 画面の項目の詳細な情報を説明しています。

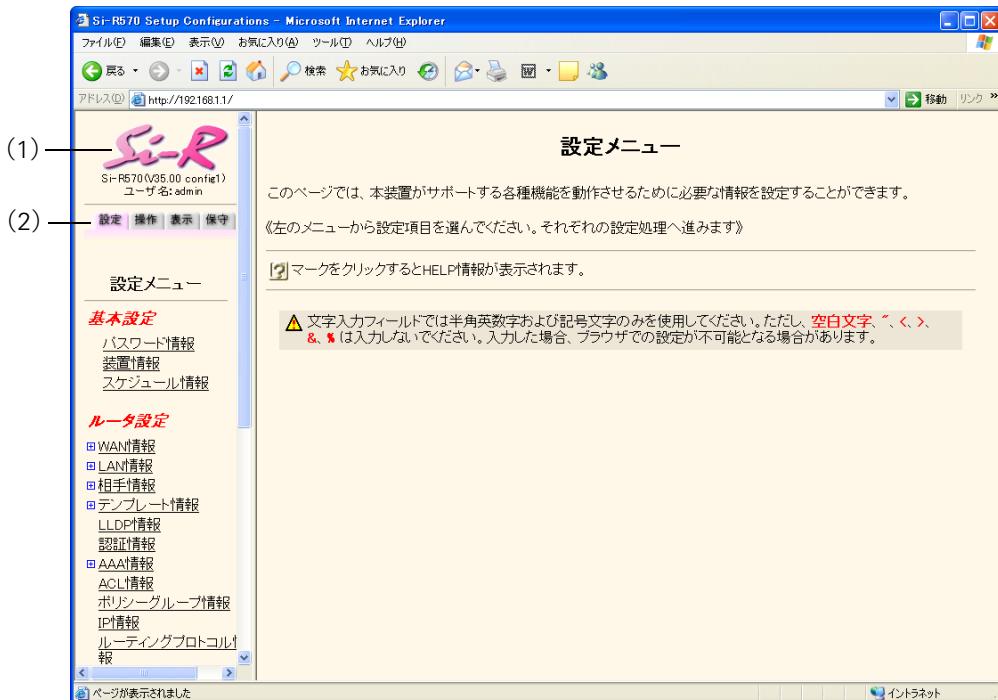
1 「設定メニュー」を表示する

「かんたん設定」をサポートしているかどうかで [設定] タブをクリックしたときに表示される画面が異なります。ここでは、Si-R570の場合を例に説明します。

こんな事に気をつけて

「設定メニュー」を表示するときは、管理者 (admin) でログインしてください。

 参照 Web ユーザーズガイド 「1.3 本装置にログインする」 (P.11)



画面左側に表示されるタブについて、以下に説明します。

(1) 本装置ロゴ : クリックすると、トップページが表示されます。

(2) [設定] タブ : Si-R180B、220C、220Dの場合

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」ボタンが表示されます。「詳細設定メニュー」ボタンをクリックすると、「基本設定」と「ルータ設定」が表示されます。

Si-R240B、260B、370、370B、570、570Bの場合

クリックすると、設定メニューが表示されます。設定メニューには「基本設定」、「ルータ設定」があります。

 参照 [操作] タブ、[表示] タブおよび [保守] タブについて

Web ユーザーズガイド 「2.1 操作メニューを使う」 (P.25)、「2.2 表示メニューを使う」 (P.45)、
「2.3 保守メニューを使う」 (P.49)

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 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.23)

2 「設定メニュー」の画面体系

[設定] タブをクリックして表示される設定用メニューの画面項目と体系について示します。

2.1 かんたん設定メニュー

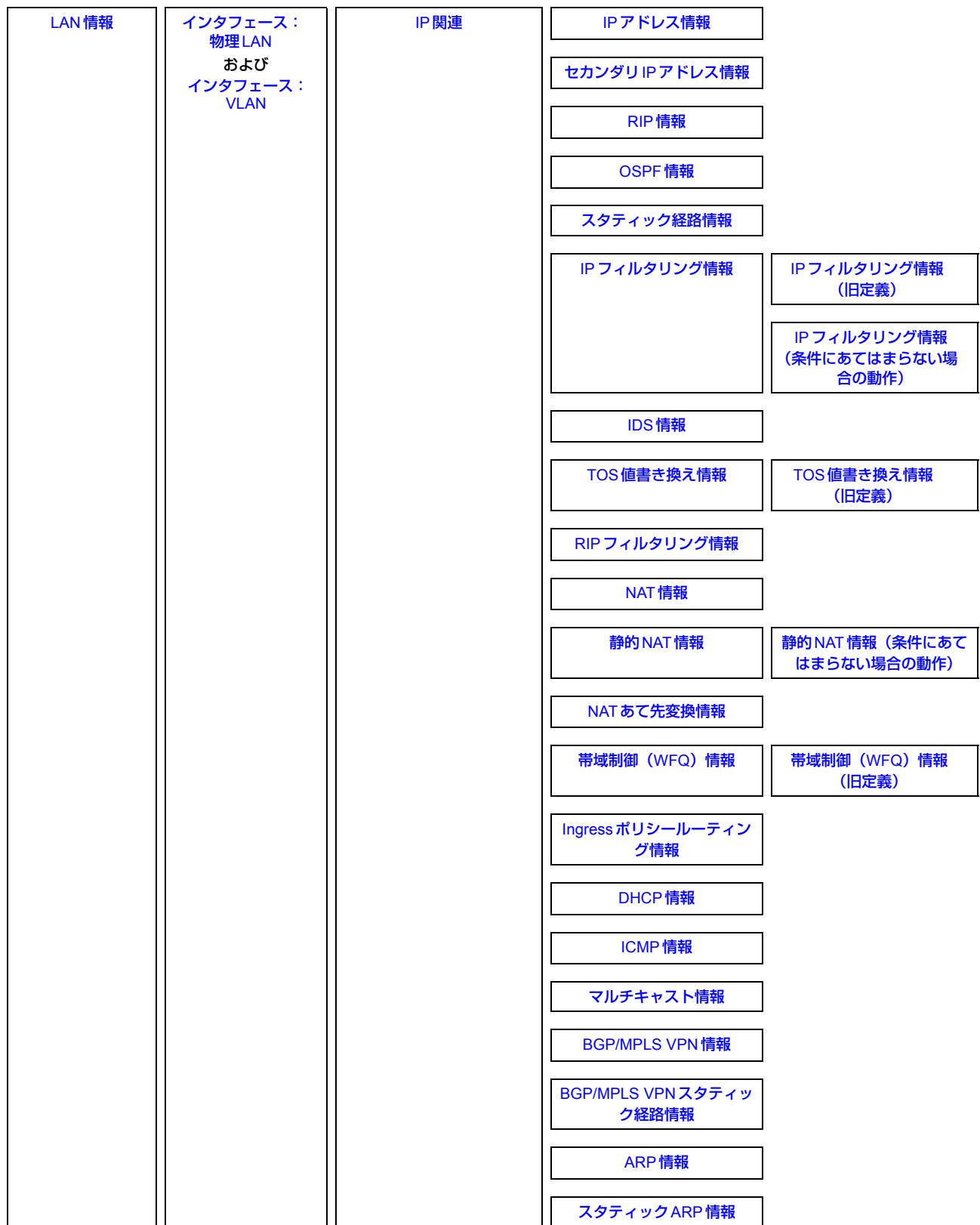
インターネットへISDN接続かんたん設定	必須設定 オプション設定
インターネットへ専用線接続かんたん設定	必須設定 オプション設定
PPPoEかんたん設定	必須設定 オプション設定
オフィスへISDN接続かんたん設定	必須設定 オプション設定
オフィスへ専用線接続かんたん設定	必須設定 オプション設定
プライベートLAN構築かんたん設定	必須設定 オプション設定
セグメント接続／分割かんたん設定	LAN0 LAN1

2.2 基本設定

パスワード情報	基本情報
	ログインパスワード情報
	ログインユーザ情報
装置情報	ルータ名称情報
	タイムサーバ情報
	システムログ情報
	ファームウェア更新情報
	異常時動作情報
	IPv4 ループバック情報
	IPv6 ループバック情報
	サーバ機能情報
	アプリケーションフィルタ情報
	外部メディアスタート機能情報
スケジュール情報	月間／週間予約情報
	電話番号変更予約情報
	構成定義切り替え予約情報

2.3 ルータ設定

WAN 情報	回線インターフェース : ISDN	基本情報
		接続制御情報
	回線インターフェース : 専用線	基本情報
	回線インターフェース : フレームリレー	基本情報
	回線インターフェース : ATM	基本情報
無線LAN 情報	回線情報	
	認証／暗号化情報	
	MAC フィルタリング情報	
スイッチ情報	基本情報	
	ポート情報	
LAN 情報	インターフェース : 物理 LAN	共通情報
		基本情報
		VRRP グループ情報
		基本情報
		VRRP トリガ情報
		VRRP アクション情報
		LLDP 情報
		IEEE802.1X 認証情報
		MAC アドレス認証情報
		ARP 認証関連
		基本情報
		認証不要端末情報
		トラップ情報



LAN 情報	インターフェース： 物理 LAN および インターフェース： VLAN	IPv6 関連	IPv6 基本情報 IPv6 RIP 情報 IPv6 OSPF 情報 IPv6 スタティック経路情報 IPv6 フィルタリング情報 IPv6 フィルタリング情報 (旧定義) IPv6 フィルタリング情報 (条件にあてはまらない場合の動作) IPv6 Traffic Class 値書き換え情報 IPv6 Traffic Class 値書き換え情報 (旧定義) IPv6 RIP フィルタリング情報 IPv6 帯域制御 (WFQ) 情報 IPv6 帯域制御 (WFQ) 情報 (旧定義) IPv6 Ingress ポリシールティング情報 IPv6 DHCP 情報
		ブリッジ関連	ブリッジ情報 MAC フィルタリング情報 MAC フィルタリング情報 (旧定義) 静的 MAC 学習テーブル情報 帯域制御 (WFQ) 情報
		MPLS 関連	MPLS 基本情報 LDP 情報 EoMPLS 情報
	インターフェース： VLAN	共通情報	基本情報 VLAN プライオリティマッピング情報 VRRP グループ情報 VRRP 基本情報 VRRP トリガ情報 VRRP アクション情報 MAC アドレス認証情報

LAN 情報	インターフェース : VLAN	共通情報	ARP 認証関連	基本情報
				認証不要端末情報
	インターフェース : 無線 LAN	共通情報	IEEE802.1X 認証情報	トラップ情報
				LLDP 情報
シリアル情報	共通情報	モデム情報	IEEE802.1X 認証情報	トラップ情報
				LLDP 情報
相手情報	ネットワーク情報	共通情報	IEEE802.1X 認証情報	トラップ情報
				基本情報
	接続先情報	接続先種別 : ATM 接続	IEEE802.1X 認証情報	トラップ情報
				基本情報
	接続先種別 : 専用線接続	接続先種別 : 専用線 (バンドル) 接続	IEEE802.1X 認証情報	接続制御情報
				マルチルーティング情報
	接続先種別 : 専用線 (バンドル) 接続	接続先種別 : ISDN 接続	IEEE802.1X 認証情報	トラップ情報
				基本情報
	接続先種別 : ISDN 接続		IEEE802.1X 認証情報	接続制御情報
				着信制御情報
			IEEE802.1X 認証情報	PPP 情報
				マルチルーティング情報
			IEEE802.1X 認証情報	トラップ情報
				基本情報

相手情報	ネットワーク情報	接続先情報	接続先種別：ISDN (バンドル) 接続	基本情報		
			接続先種別：フレームリ レー接続	基本情報		
				接続制御情報		
				マルチルーティング情報		
				トラップ情報		
			接続先種別：モデム接続	基本情報		
				接続制御情報		
				着信制御情報		
				PPP 情報		
				マルチルーティング情報		
				トラップ情報		
			接続先種別：データ通信 カード接続	基本情報		
				接続制御情報		
				着信制御情報		
				PPP 情報		
				マルチルーティング情報		
				トラップ情報		
			接続先種別：PPPoE 接続	基本情報		
				接続制御情報		
				PPP 情報		
				PPPoE 情報		
				マルチルーティング情報		
				トラップ情報		
			接続先種別：IP トンネル 接続	基本情報		
				接続制御情報		
				トラップ情報		

相手情報	ネットワーク情報	接続先情報	接続先種別 : IPsec/IKE 接続	基本情報				
				接続制御情報				
IPsec 情報 (自動鍵)								
IPsec 情報 (手動鍵)								
IPsec 情報 (動的VPN)								
IKE 情報 (IKEv1 共有鍵認証方式)								
IKE 情報 (IKEv2 共有鍵認証方式)								
IKE 情報 (IKEv1 RSA デジタル署名認証方式)								
IKE 情報 (IKEv2 RSA デジタル署名認証方式)								
IKE 情報 (動的VPN 接続 共有鍵認証方式)								
IKE 情報 (動的VPN 接続 RSA デジタル署名認証方式)								
拡張IPsec 対象範囲情報								
マルチルーティング情報								
動的VPN 関連 (基本情報)								
動的VPN 関連 (相手側ネットワーク情報)								
トラップ情報								
接続種別 : 別インターフェースから送出		<table border="1"> <tbody> <tr><td>基本情報</td></tr> <tr><td>接続制御情報</td></tr> <tr><td>マルチルーティング情報</td></tr> <tr><td>トラップ情報</td></tr> </tbody> </table>			基本情報	接続制御情報	マルチルーティング情報	トラップ情報
基本情報								
接続制御情報								
マルチルーティング情報								
トラップ情報								
接続先種別 : MPLS トンネル接続		<table border="1"> <tbody> <tr><td>基本情報</td></tr> <tr><td>接続制御情報</td></tr> <tr><td>マルチルーティング情報</td></tr> <tr><td>トラップ情報</td></tr> </tbody> </table>			基本情報	接続制御情報	マルチルーティング情報	トラップ情報
基本情報								
接続制御情報								
マルチルーティング情報								
トラップ情報								
接続先種別 : パケット破棄		<table border="1"> <tbody> <tr><td>基本情報</td></tr> </tbody> </table>			基本情報			
基本情報								

相手情報	ネットワーク情報	PPP 関連	圧縮情報
			MP 情報
IP 関連		IP 基本情報	
			RIP 情報
IP 関連		OSPF 情報	
			スタティック経路情報
IP 関連		IP フィルタリング情報	IP フィルタリング情報 (旧定義)
			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)
IP 関連		IDS 情報	
		TOS 値書き換え情報	TOS 値書き換え情報 (旧定義)
IP 関連		RIP フィルタリング情報	
		NAT 情報	
IP 関連		静的 NAT 情報	静的 NAT 情報 (条件にあて はまらない場合の動作)
		NAT あて先変換情報	
IP 関連		帯域制御 (WFQ) 情報	帯域制御 (WFQ) 情報 (旧定義)
IP 関連		Ingress ポリシールーティン グ情報	
		CLP 値設定情報	CLP 値設定情報 (旧定義)
IP 関連		マルチキャスト情報	
		EXP 値書き換え情報	EXP 値書き換え情報 (旧定義)
IP 関連		動的 VPN 情報	
IPv6 関連		IPv6 基本情報	
		IPv6 RIP 情報	
IPv6 関連		IPv6 OSPF 情報	
		IPv6 スタティック経路情報	

相手情報	ネットワーク情報	IPv6 関連	IPv6 フィルタリング情報	IPv6 フィルタリング情報 (旧定義)
			IPv6 フィルタリング情報 (条件にあてはまらない場合 の動作)	
			IPv6 Traffic Class 値書き換 え情報	IPv6 Traffic Class 値書き換 え情報 (旧定義)
			IPv6 RIP フィルタリング 情報	
			IPv6 帯域制御 (WFQ) 情報	IPv6 帯域制御 (WFQ) 情報 (旧定義)
			IPv6 Ingress ポリシールー ティング情報	
			IPv6 CLP 値設定情報	
			IPv6 DHCP 情報	
			IPv6 EXP 値書き換え情報	
			IPv6 動的 VPN 情報	
		ブリッジ関連	ブリッジ情報	
			MAC フィルタリング情報	MAC フィルタリング情報 (旧定義)
			静的 MAC 学習テーブル情報	
			帯域制御 (WFQ) 情報	
		MPLS 関連	MPLS 基本情報	
			LDP 情報	
	着信相手識別情報			
テンプレート情報	接続種別 : ISDN	共通情報	基本情報	
			トラップ情報	
		PPP 関連	認証情報	
			圧縮情報	

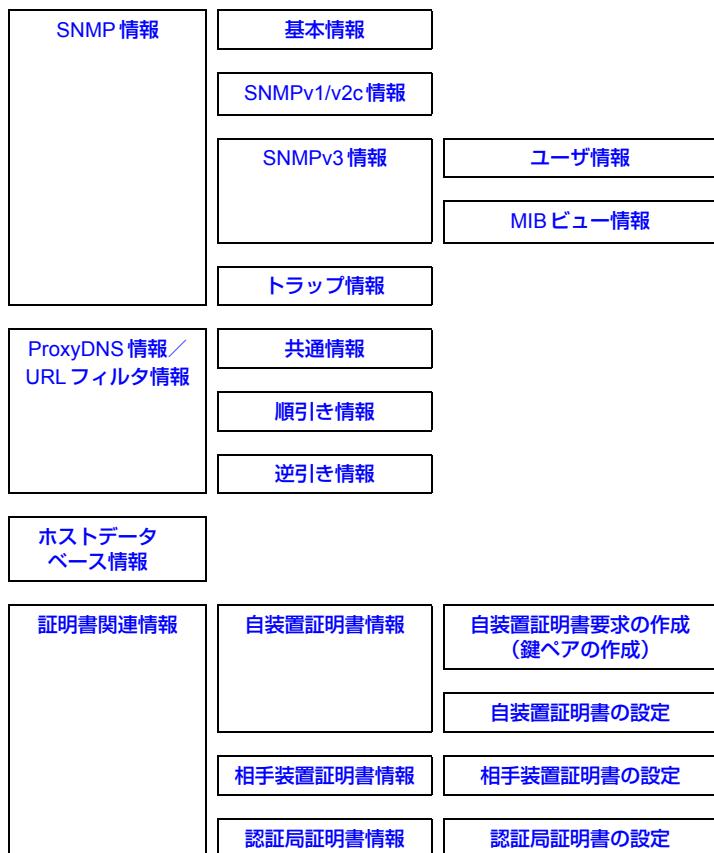
テンプレート情報	接続種別：ISDN、 接続種別：IPsec/IKE (RADIUS/AAA)、 接続種別：IPsec/IKE (動的VPN 共有鍵認 証方式) および 接続種別：IPsec/IKE (動的VPN接続 RSA デジタル署名認証方 式)	IP 関連	IP 基本情報
			IP フィルタリング情報
			IP フィルタリング情報 (旧定義)
			IP フィルタリング情報 (条件にあてはまらない 場合の動作)
			IDS 情報
			TOS 値書き換え情報
			TOS 値書き換え情報 (旧定義)
			NAT 情報
			静的NAT 情報
			静的NAT 情報 (条件にあて はまらない場合の動作)
			NAT あて先変換情報
			帯域制御 (WFQ) 情報
			帯域制御 (WFQ) 情報 (旧定義)
			Ingress ポリシールーティン グ情報
		IPv6 関連	IPv6 基本情報
			IPv6 フィルタリング情報
			IPv6 フィルタリング情報 (旧定義)
			IPv6 フィルタリング情報 (条件にあてはまらない場合 の動作)
			IPv6 Traffic Class 値書き換 え情報
			IPv6 Traffic Class 値書き換 え情報 (旧定義)
			IPv6 帯域制御 (WFQ) 情報
			IPv6 帯域制御 (WFQ) 情報 (旧定義)
			IPv6 Ingress ポリシールー ティング情報
	接続種別：IPsec/IKE (RADIUS/AAA)	共通情報	基本情報
			トラップ情報
		IPsec/IKE 関連	IPsec 情報
			IKE 情報 (IKEv1)
			接続制御情報

テンプレート情報	接続種別 : IPsec/IKE (動的VPN 共有鍵認証方式)	共通情報	基本情報
		IPsec/IKE 関連	IPsec 情報
接続種別 : IPsec/IKE (動的VPN 接続 RSA デジタル署名認証方式)	動的VPN 関連	IKE 情報 (動的VPN接続共有鍵認証方式)	接続制御情報
		基本情報	自側ネットワーク情報
LLDP 情報	IEEE802.1X 認証情報	共通情報	基本情報
		IPsec/IKE 関連	IPsec 情報
認証情報	MAC アドレス認証情報	IKE 情報 (動的VPN接続 RSA デジタル署名認証方式)	接続制御情報
		動的VPN 関連	基本情報
AAA 情報	グループID情報	自側ネットワーク情報	
		AAA ユーザ情報	認証情報
		IP 関連	IP 基本情報
			スタティック経路情報
		IPv6 関連	IPv6 基本情報
			IPv6 スタティック経路情報
		IPsec/IKE 関連	IPsec 情報
			IKE 情報
			拡張IPsec対象範囲情報
			接続制御情報
		サブリカント関連	サブリカント情報

AAA 情報	グループ ID 情報	RADIUS 関連	基本情報 サーバ情報 (クライアント機能) 送信情報 (クライアント機能) クライアント情報 (サーバ機能)
ACL 情報	ACL 定義情報	基本定義情報 IP 定義情報 TCP 定義情報 UDP 定義情報 ICMP 定義情報 IPv6 定義情報 MAC 定義情報	
ポリシーグループ 情報	ポリシーグループ 定義情報	パターン定義情報 送出先定義情報 接続先監視定義情報	
IP 情報	基本情報 インターフェース情報 ルーティングマネージャ情報 RIP 関連		
ルーティングプロトコル情報			



ルーティングプロトコル情報	IPv6 RIP 関連	IPv6 RIP タイマ情報	
		IPv6 RIP マルチパス情報	
IPv6 RIP 再配布フィルタリング情報			
IPv6 OSPF 関連	IPv6 OSPF エリア情報	IPv6 ルータ ID 情報	
		IPv6 OSPF エリア基本情報	
IPv6 経路集約情報			
IPv6 エリア間プレフィックス LSA 入出力可否情報			
IPv6 AS 境界ルータ情報			
IPv6 OSPF 再配布フィルタリング情報			
マルチキャスト情報	IP マルチキャスト情報		
	IP マルチキャストスイッチャティック RP 情報		
	IP マルチキャストスイッチャティック経路情報		
UPnP 情報	基本情報		
MPLS 情報	基本情報		
ブリッジ情報	ブリッジグループ情報	ブリッジグループ情報 (グループ識別子0の場合) ブリッジグループ情報 (グループ識別子1~7の場合)	
動的VPN情報	サーバ関連情報	基本情報	
	クライアント関連情報	基本情報	
		ドメイン情報	
		基本情報	
		自側ネットワーク情報	
SIP-SIPゲートウェイ情報	基本情報		
	内線情報		
	外線情報		



2.4 無線 LAN 管理設定



3 インターネットへ ISDN 接続かんたん設定

適用機種 Si-R220C, 220D

[操作] [かんたん設定メニュー] → インターネットへ「ISDN 接続」

インターネットへISDN接続かんたん設定

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■必須設定	
接続先の電話番号	<input type="text"/>
ユーザ認証ID	<input type="text"/>
ユーザ認証パスワード	<input type="password"/>
■オプション設定	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0) <input type="button" value="▼"/>
DNSサーバ	<input type="checkbox"/> 自動取得
接続先の電話番号2	<input type="text"/>
接続先の電話番号3	<input type="text"/>
常時接続機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない 無通信監視タイム <input type="text"/> 秒 課金単位時間 <input type="text"/> 0
接続先ネットワーク名	rmt0
接続先名	ap0-0
アドレス変換	<input type="radio"/> 使用しない <input checked="" type="radio"/> マルチNAT UPnP機能 <input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
MP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
かんたんフィルタ	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

3.1 必須設定

接続先の電話番号

半角数字32桁以内で指定します。-、(、)、が区切り文字として使用できます。

《指定例》

01-2345-6789

01(2345)6789

ユーザ認証ID

接続先より通知されたIDを半角英数字64文字以内で指定します。

ユーザ認証パスワード

接続先より通知されたパスワードを半角英数字64文字以内で指定します。

3.2 オプション設定

IP アドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

DNS サーバ

必要に応じて接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略、または0.0.0.0を指定する場合は、広報を行いません。また、“自動取得”をチェックする場合は、本装置のIPアドレスをDNSサーバアドレスとして広報します。実際のDNSサーバアドレスは回線接続時に相手システムより取得し、ProxyDNS機能が名前解決を行います。自動取得は相手システムがDNSサーバアドレスの広報機能(RFC1877)をサポートしている場合にだけ使用できます。

接続先の電話番号2／3

マルチダイヤルを行う場合に指定します。記述方法は、接続先の電話番号と同じです。

常時接続機能

インターネットへISDN接続機能を使用して常時接続する場合は“使用する”を選択します。

無通信監視タイマ

ISDN回線の無通信監視タイマを0～3600秒の範囲で指定します。その時間を超えても、通信が行われなかった場合は、ISDN回線を自動的に切断します。なお、0を指定した場合は、自動切断を行いません。

課金単位時間

課金単位時間を0.0～3600.0秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照され、同じ料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、0を指定した場合は、課金単位の調整を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

アドレス変換

1つのグローバル側IPアドレスを使用して、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

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。

MP

MP接続をする場合は、“使用する”を選択します。“使用する”を選択した場合は、データ通信量に応じて適宜増減します。

かんたんフィルタ

かんたんフィルタは、通常の使用方法で起こりやすい以下の問題を回避するためのIP フィルタを簡単に設定できます。

Windows NTなどによる Microsoft Network を使用している場合、お客様のネットワーク設定によっては、NetBIOS over TCP によって定期的に送出されるパケットにより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、NetBIOS over TCP が使用する TCP および UDP のサービスポートの 137～139 を遮断するフィルタを設定します。

ping (ICMP echo) などのコマンドにより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、ICMP プロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にあるときには、ICMP パケットを通過させます。

syslog、TIME、NTP (SNTP) により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、それぞれのプロトコルによる自動発信を抑止するフィルタを設定します。なお、回線が接続状態にあるときには、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 パケットにより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、ホストデータベース情報に IP アドレスが「127.0.0.1」のホスト名は「localhost」を設定します。

4 インターネットへ専用線接続かんたん設定

適用機種 **Si-R220C, 220D**

[操作] [かんたん設定メニュー] → インターネットへ「専用線接続」

インターネットへ専用線接続かんたん設定 [?]

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■必須設定	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0) ▼
使用する回線速度	<input type="radio"/> 64Kbps <input checked="" type="radio"/> 128Kbps
DNSサーバ	
■オプション設定	
接続ネットワーク名	rmt0
接続先名	ap0-0
ドメイン名	
アドレス変換	<input checked="" type="radio"/> 使用しない <input type="radio"/> マルチNAT グローバルアドレス: <input type="text"/> アドレス個数: <input type="text"/> 個 UPnP機能: <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。	
設定終了 キャンセル	

4.1 必須設定

IP アドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。マルチNATを使用する場合は、ローカルなIPアドレス、使用しない場合は、プロバイダから割り当てられたIPアドレスを指定します。

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

使用する回線速度

使用する回線速度を選択します。

DNS サーバ

接続先、またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。0.0.0.0を指定した場合は、広報を行いません。

4.2 オプション設定

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

ドメイン名

必要に応じて接続先、またはネットワーク管理者に指示されたドメイン名を半角英数字80文字以内で指定します。省略時は、DHCP サーバによる広報を行いません。

アドレス変換

マルチ NAT を使用すると、プロバイダから取得している IP アドレス個数以上の端末を利用できます。使用する場合は、“マルチ NAT”を選択します。WAN 側に固定のアドレスを1つ、または複数持っている場合は、“グローバルアドレス”と“アドレス個数”を設定します。

グローバルアドレス

グローバルアドレスを先頭とする“アドレス個数”分のアドレスが本装置の WAN IP アドレスとなります。

アドレス個数

1～16 の範囲で指定します。

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。

5 PPPoE かんたん設定

適用機種 Si-R180B, 220C, 220D

[操作] [かんたん設定メニュー] → インターネットへ「PPPoE 接続」
(Si-R180B の場合は [かんたん設定メニュー] → 「PPPoE 接続」)

PPPoE かんたん設定

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■ 必須設定	
ユーザ認証ID	<input type="text"/>
ユーザ認証パスワード	<input type="password"/>
■ オプション設定	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0) <input type="button" value="…"/>
DNSサーバ	<input checked="" type="checkbox"/> 自動取得
接続ネットワーク名	rmt0
接続先名	ap0-0
PPPoEで使用するインターフェース	<input checked="" type="radio"/> LAN0 <input type="radio"/> LAN1
常時接続機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 無通信監視タイム <input type="text" value="0"/> 秒
アドレス変換	<input type="radio"/> 使用しない <input checked="" type="radio"/> マルチNAT UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	自動認識 <input type="button" value="…"/>
LAN1転送レート	自動認識 <input type="button" value="…"/>

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

Si-R180B では、オプション設定の表示が、上記の画面とは異なります。

5.1 必須設定

ユーザ認証 ID／パスワード

PPPoE で接続する際に使用する、ユーザ認証 ID とパスワードを 64 行以内で指定します。

5.2 オプション設定

IP アドレス／ネットマスク

プライベート側の IP アドレスとネットマスクを指定します。本装置では、PPPoE で使用するように指定したインターフェースの反対側のインターフェースが自動的にプライベート側となります。Si-R180B では、LAN1（スイッチ）がプライベート側固定となります。

DNS サーバ

必要に応じて接続先またはネットワーク管理者に指示されたDNSサーバのIPアドレスを指定します。指定する値はDHCPサーバ機能により広報されます。省略または0.0.0.0を指定する場合は広報を行いません。また、“自動取得”を選択する場合は、本装置のIPアドレスをDNSサーバアドレスとして広報します。実際のDNSサーバアドレスは回線接続時に相手システムより取得し、ProxyDNS機能が名前解決を行います。自動取得は相手システムがDNSサーバアドレスの広報機能（RFC1877）をサポートしている場合にだけ使用できます。

接続ネットワーク名

ネットワークを識別する名称を8文字以内で指定します。

接続先名

接続先を識別する名称を8文字以内で指定します。

PPPoE で使用するインターフェース

PPPoEで使用するインターフェースを選択します。
Si-R180Bでは、LAN0（基本ポート0）固定となります。

常時接続機能

PPPoEを使用して常時接続を行う場合は“使用する”を選択します。

無通信監視タイマ

常時接続機能を使用しない場合の無通信監視タイマを0～3600秒の範囲で指定します。ここで指定した時間に通信が行われなかった場合、自動的に切断します。0を指定した場合は、自動的に切断しません。

アドレス変換

1つのグローバル側IPアドレスを使用して、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

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。

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。固定で指定する場合は、相手装置の仕様に合わせます。Si-R180B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（SW1～4）で有効になります。

こんな事に気をつけて

- “自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行います。
- Si-R180Bでは、LAN1（スイッチ）転送レートの設定が“自動認識”以外の場合は、MDIの設定はMDI-Xとして動作します。

6 オフィスへ ISDN 接続かんたん設定

適用機種 **Si-R220C, 220D**

[操作] [かんたん設定メニュー] → オフィスへ「ISDN 接続」

オフィスへISDN接続かんたん設定 

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■必須設定	
接続先の電話番号	<input type="text"/>
ユーザ認証ID(発信)	<input type="text"/>
ユーザ認証パスワード(発信)	<input type="text"/>
ユーザ認証ID(着信)	<input type="text"/>
ユーザ認証パスワード(着信)	<input type="text"/>
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0) <input type="button" value="▼"/>
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) <input type="button" value="▼"/>

■オプション設定	
DHCPサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する <input type="text"/> DNSサーバ広報
常時接続機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない <input type="text"/> 無通信監視タイム [0] 秒 <input type="text"/> 課金単位時間 [0]
接続ネットワーク名	rmt0
接続先名	ap0-0
MP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
ヘッダ圧縮	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
データ圧縮	<input type="checkbox"/> LZS

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

6.1 必須設定

接続先の電話番号

半角数字32桁以内で指定します。-、(、)、が区切り文字として使えます。

《指定例》

01-2345-6789

01(2345)6789

ユーザ認証ID／パスワード（発信）

本装置から発信接続するときに使用する認証IDとパスワードを半角英数字64文字以内で指定します。

ユーザ認証ID／パスワード（着信）

本装置から着信接続するときに使用する認証IDとパスワードを半角英数字64文字以内で指定します。

IP アドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。ただし、既存のネットワークに接続するのでなければ、修正は不要です。

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

相手ルータのIPアドレス／ネットマスク

相手ルータのIPアドレスとネットマスクを指定します。
本装置はこの指定で得られるネットワークに対してスタティックルートを指定します。

6.2 オプション設定

DHCP サーバ

DHCP サーバを使用する場合は、“使用する”を選択します。

DNS サーバ広報

必要に応じて接続先、またはネットワーク管理者に指示された DNS サーバの IP アドレスを指定します。指定する値は DHCP サーバ機能により広報されます。省略、または 0.0.0.0 を指定する場合は、広報を行いません。

常時接続機能

オフィスへ ISDN 接続機能を使用して常時接続を行う場合は“使用する”を選択します。

無通信監視タイマ

ISDN 回線の無通信監視タイマを 0～3600 秒の範囲で指定します。その時間を超えても、通信が行われない場合は、ISDN 回線を自動的に切断します。なお、0 を指定した場合は、自動切断を行いません。

課金単位時間

課金単位時間を 0.0～3600.0 秒の範囲で指定します。ここで指定する時間は無通信監視による回線切断のときに参照され、同じ料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、0 を指定した場合は、課金単位の調整を行いません。

接続ネットワーク名

ネットワークを識別する名称を半角英数字 8 文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字 8 文字以内で指定します。

MP

MP 接続をする場合は、“使用する”を選択します。“使用する”を選択した場合は、データ通信量に応じて適宜増減します。

ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJ ヘッダ圧縮 (RFC1144 に準拠) および IP ヘッダ圧縮 (RFC2507 / RFC2508 に準拠) をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZS をサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

7 オフィスへ専用線接続かんたん設定

適用機種 **Si-R220C, 220D**

[操作] [かんたん設定メニュー] → オフィスへ「専用線接続」

オフィスへ専用線接続かんたん設定

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■必須設定

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	<input type="radio"/> 64Kbps <input checked="" type="radio"/> 128Kbps

■オプション設定

接続ネットワーク名	rmt0
接続先名	ap0-0
DHCPサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する DNSサーバ広報
ヘッダ圧縮	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
データ圧縮	<input type="checkbox"/> LZS

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

設定終了 **キャンセル**

7.1 必須設定

IP アドレス／ネットマスク

本装置のIPアドレスとネットマスクを指定します。
IPアドレスに0.0.0.0を指定すると通信ができなくなります。

相手ルータのIP アドレス／ネットマスク

相手ルータのIPアドレスとネットマスクを指定します。
本装置は、この指定で得られるネットワークに対してストティックルートを指定します。

使用する回線速度

使用する回線速度を選択します。

7.2 オプション設定

接続ネットワーク名

ネットワークを識別する名称を半角英数字8文字以内で指定します。

接続先名

接続先を識別する名称を半角英数字8文字以内で指定します。

DHCP サーバ

DHCP サーバを使用する場合は、" 使用する " を選択します。

DNS サーバ広報

必要に応じて接続先、またはネットワーク管理者に指示された DNS サーバの IP アドレスを指定します。指定する値は DHCP サーバ機能により広報されます。省略、または 0.0.0.0 を指定する場合は、広報を行いません。

ヘッダ圧縮

送受信するヘッダを圧縮します。ヘッダ圧縮のアルゴリズムは、VJ ヘッダ圧縮 (RFC1144 に準拠) および IP ヘッダ圧縮 (RFC2507 / RFC2508 に準拠) をサポートします。使用する指定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

データ圧縮

送受信するデータを圧縮します。データ圧縮のアルゴリズムは、LZS をサポートします。使用する指定の場合も、実際にデータ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

8 プライベート LAN 構築かんたん設定

適用機種 **Si-R180B, 220C, 220D**

[操作] [かんたん設定メニュー] → LAN 間接続「プライベート LAN 接続」
(Si-R180B の場合は [かんたん設定メニュー] → 「プライベート LAN 接続」)

プライベート LAN 構築かんたん設定

⚠ 基本設定およびルータ設定で設定した情報は無効になります。

■必須設定	
グローバル側IPアドレス	<input checked="" type="radio"/> DHCPで自動的に取得する <input type="radio"/> 指定する IPアドレス: <input type="text"/> ネットマスク: <input type="text"/> 2 (192.0.0.0)
プライベート側IPアドレス	IPアドレス: <input type="text"/> 192.168.1.1 ネットマスク: <input type="text"/> 24 (255.255.255.0)
グローバル側インターフェース	<input type="radio"/> LAN0 <input checked="" type="radio"/> LAN1

■オプション設定	
デフォルトルータ	<input type="text"/>
DNSサーバアドレス	<input type="text"/>
DHCPサーバ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する デフォルトルータ広報: <input type="text"/> 192.168.1.1 DNSサーバ広報: <input type="text"/> 192.168.1.1 ドメイン名広報: <input type="text"/>
UPnP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	自動認識
LAN1転送レート	自動認識

“かんたん設定”では設定を終了すると、自動的に再起動され、通信を行うことができる状態になります。設定を元に戻す場合はキャンセルをクリックしてください。

設定終了 キャンセル

Si-R180B では、必須設定およびオプション設定の表示が、上記の画面とは異なります。

8.1 必須設定

グローバル側IPアドレス

このインターフェースのIPアドレスの取得方法を指定します。本装置をDHCPクライアントとして運用する場合は“DHCPで自動的に取得する”を選択します。IPアドレス、ネットマスクを指定する場合は“指定する”を選択し、以下の項目を設定します。

こんな事に気をつけて

- ・ 本装置をDHCPクライアントとして運用するには上流側にDHCPサーバが稼動している必要があります。
- ・ グローバル側IPアドレスで“指定する”で設定すると、RIP情報が流れていないネットワークではデフォルトルータとDNSサーバアドレスを設定する必要があります。

IPアドレス／ネットマスク

本装置のグローバル側のIPアドレスとネットマスクを指定します。

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

プライベート側IPアドレス／ネットマスク

本装置のプライベート側のIPアドレスとネットマスクを指定します。

グローバル側インターフェース

LAN0とLAN1のどちらをグローバル側のインターフェースにするか選択します。Si-R180Bでは、LAN0（基本ポート0）固定となります。

8.2 オプション設定

デフォルトルータ

本装置のデフォルトルータアドレスを指定します。ただし、グローバル側のIPアドレスを“DHCPで自動的に取得する”を選択している場合で、DHCPサーバがデフォルトルータを広報していれば自動的に取得するので指定する必要はありません。“指定する”を選択している場合はこの指定が優先されます。

DNSサーバアドレス

本装置を接続したネットワークの前に存在するDNSサーバアドレスを指定します。ただし、グローバル側のIPアドレスを“DHCPで自動的に取得する”を選択している場合で、DHCPサーバがDNSサーバアドレスを広報していれば自動的に取得するので指定する必要はありません。“指定する”を選択している場合はこの指定が優先されます。

DHCPサーバ

本装置をプライベート側ネットワークのDHCPサーバとして使用する場合は、“使用する”を選択します。

デフォルトルータ広報

DHCPサーバで広報するデフォルトルータのIPアドレスを指定します。省略するか0.0.0.0を指定するとDHCPサーバによる広報を行いません。

DNSサーバ広報

DNSサーバのIPアドレスを指定します。省略するか0.0.0.0を指定するとDHCPサーバによる広報を行いません。ProxyDNSを使用する場合は、本装置のIPアドレスを指定します。

ドメイン名広報

ドメイン名を80文字以内で指定します。省略するとDHCPサーバによる広報を行いません。RFC1034では英数字、”.”、”-”で指定することを推奨しています。

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。

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。固定で指定する場合は、相手装置の仕様に合わせます。Si-R180B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（SW1～4）で有効になります。

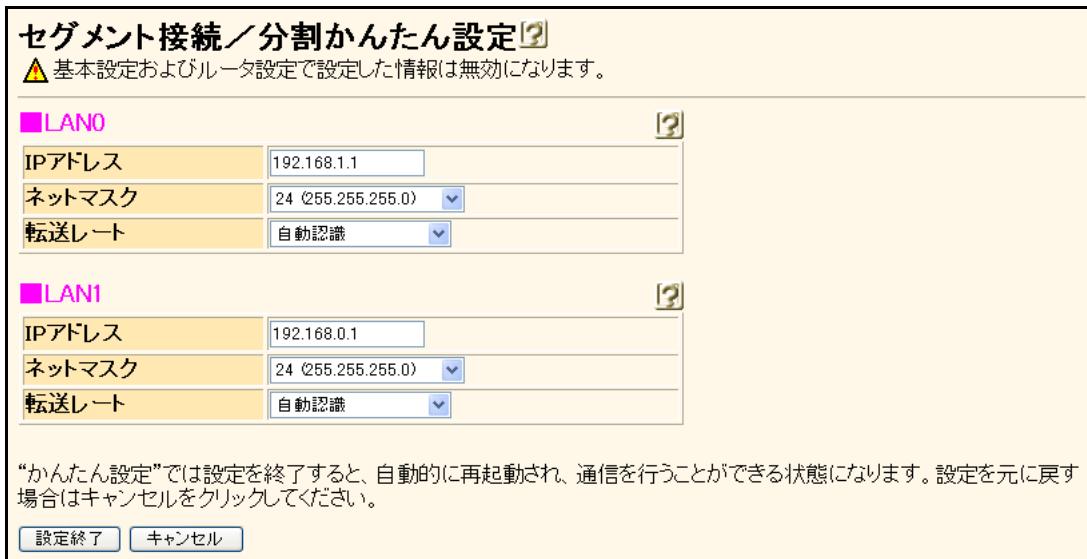
こんな事に気をつけて

- “自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。
その場合は“自動認識”ではなく固定の設定を行ってください。
- Si-R180Bでは、LAN1（スイッチ）転送レートの設定が“自動認識”以外の場合は、MDIの設定はMDI-Xとして動作します。

9 セグメント接続／分割かんたん設定

適用機種 Si-R180B, 220C, 220D

[操作] [かんたん設定メニュー] → LAN 間接続「セグメント接続／分割」
(Si-R180B の場合は [かんたん設定メニュー] → 「セグメント接続／分割」)



Si-R180B では、表示が上記の画面とは異なります。

9.1 LAN0

LAN0に接続するネットワークの設定を行います。

IP アドレス／ネットマスク

LAN0側のネットワークで使用する装置のIPアドレス／ネットマスクを指定します。

転送レート

LAN0側の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。固定で指定する場合は、相手装置の仕様に合わせます。

こんな事に気をつけて

“自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行ってください。

9.2 LAN1

Si-R180B の場合は、「LAN1 (スイッチ)」と表示されます。

LAN1に接続するネットワークの設定を行います。

IP アドレス／ネットマスク

LAN1側のネットワークで使用する装置のIPアドレス／ネットマスクを指定します。

転送レート

LAN1側の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。固定で指定する場合は、相手装置の仕様に合わせます。Si-R180B では、転送レートで選択した値は、スイッチポート (SW1～4) で有効になります。

こんな事に気をつけて

- “自動認識”は接続ネットワークの環境によって正しく動作しない場合があります。その場合は“自動認識”ではなく固定の設定を行ってください。
- Si-R180B では、転送レートの設定が“自動認識”以外の場合は、MDI の設定は MDI-X として動作します。

10 パスワード情報

適用機種 全機種

[操作] 基本設定「パスワード情報」

パスワード情報		
基本情報	ログインパスワード情報	ログインユーザ情報
このページでは、パスワードに関する情報についての設定ができます。		

10.1 基本情報

[操作] 基本設定「パスワード情報」→ [基本情報]

■ 基本情報	
<input checked="" type="checkbox"/> 暗号化パスワード形式	<input type="checkbox"/> 装置固有パスワード形式にする
※装置固有パスワード形式にする設定を更新するとそれ以降、暗号化パスワード形式の修正はできません。	
設定終了後、更新をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="更新"/> <input type="button" value="キャンセル"/>	

暗号化パスワード形式

本装置に設定する各種パスワード文字列は暗号化されて保存されます。

装置固有パスワード形式にしない場合は、保存した構成定義情報は他装置に復元することができます。

装置固有パスワード形式にした場合は、保存した構成定義情報は自装置にのみ復元することができ、他装置に復元することはできなくなります。装置固有パスワード形式にすることで、セキュリティを強化することができます。

なお、暗号化パスワード形式の設定は更新直後から有効になります。

こんな事に気をつけて

- “装置固有パスワード形式にする”を選択し更新するとそれ以降、暗号化パスワード形式の修正はできません。
- 装置固有パスワード形式を使用した構成定義は他装置には復元できません。

10.2 ログインパスワード情報

[操作] 基本設定「パスワード情報」→ [ログインパスワード情報]

この装置にログインするための「パスワード」を設定します。
管理者パスワードはログインユーザ名がadminの場合に使用するパスワード、一般ユーザパスワードはログインユーザ名がuserの場合に使用するパスワードです。

ログイン時のユーザによって権限クラスが決定され、権限クラスにより実行できる画面が異なります。adminでログインすると管理者クラス、userでログインすると一般ユーザクラスになります。

なお、コンソール、TELNET および SSH によるログイン時にもこの管理者パスワード および 一般ユーザパスワードを使用します。

また、FTP および SFTP によるログイン時には管理者パスワードを使用します。

■ログインパスワード情報	
管理者パスワード	<input type="text"/>
管理者パスワードの確認	<input type="text"/>
一般ユーザパスワード	<input type="text"/>
一般ユーザパスワードの確認	<input type="text"/>

設定終了後、更新をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置を操作するときのパスワードを設定します。

ログイン時のユーザによって権限クラスが決定され、権限クラスにより実行できる画面が異なります。パスワード入力によって操作できる時間は 10 分間です。それ以降の操作では再びパスワード入力して処理を行ってください。

なお、パスワードの設定は更新直後から有効になります。

管理者パスワード

ログインユーザ名がadminの場合に、8~64 文字でパスワードを指定します。adminでログインすると権限クラスが管理者クラスになります。

こんな事に気をつけて

7 文字以下、英字だけ、数字だけのパスワードを設定した場合、および、管理者パスワードの設定を削除した場合は、設定および削除は行われますが、脆弱である旨の警告メッセージが表示されます。

一般ユーザパスワード

ログインユーザ名がuserの場合に、8~64 文字でパスワードを指定します。userでログインすると権限クラスが一般ユーザクラスになります。

こんな事に気をつけて

7 文字以下、英字だけ、数字だけのパスワードを設定した場合、および、管理者パスワードの設定を削除した場合は、設定および削除は行われますが、脆弱である旨の警告メッセージが表示されます。

管理者パスワードの確認

上記で指定した管理者パスワードをもう一度指定します。

一般ユーザパスワードの確認

上記で指定した一般ユーザパスワードをもう一度指定します。

10.3 ログインユーザ情報

[操作] 基本設定「パスワード情報」→ [ログインユーザ情報]

この装置にログインする場合のユーザ認証で参照するAAA情報を設定できます。
権限クラスをAAAグループまたはRADIUSサーバに設定する方法と、認証時に参照するAAAグループを権限クラスによって分ける方法があります。この2つの方法を併用することはできません。

認証時に参照するAAAグループを分ける方法の場合、ユーザ認証は管理者、一般ユーザの順番に行い、管理者でユーザ認証に成功した場合は管理者クラス、一般ユーザでユーザ認証に成功した場合は一般ユーザクラスになります。

権限クラスにより実行できる画面が異なります。

ログインユーザ情報によるユーザ認証を行うには、ログインパスワード情報の管理者パスワードが設定されている必要があります。

なお、コンソール、TELNET、FTP および SSH によるログイン時にもログインユーザ情報を参照してユーザ認証を行います。

■ログインユーザ情報

<input checked="" type="radio"/> 権限クラスは AAA/RADIUS サーバで設定する	
参照するAAA情報	<input checked="" type="radio"/> 参照しない <input type="radio"/> 参照する AAAグループID <input type="text"/> 認証プロトコル <input checked="" type="radio"/> CHAP <input type="radio"/> PAP
	<input checked="" type="radio"/> 参照しない <input type="radio"/> 参照する AAAグループID <input type="text"/> 認証プロトコル <input checked="" type="radio"/> CHAP <input type="radio"/> PAP
<input type="radio"/> 権限クラスによって参照するAAAを分ける	
管理者で参照するAAA情報	<input checked="" type="radio"/> 参照しない <input type="radio"/> 参照する AAAグループID <input type="text"/> 認証プロトコル <input checked="" type="radio"/> CHAP <input type="radio"/> PAP
	<input checked="" type="radio"/> 参照しない <input type="radio"/> 参照する AAAグループID <input type="text"/> 認証プロトコル <input checked="" type="radio"/> CHAP <input type="radio"/> PAP
一般ユーザで参照するAAA情報	
一般ユーザで参照するAAA情報	<input checked="" type="radio"/> 参照しない <input type="radio"/> 参照する AAAグループID <input type="text"/> 認証プロトコル <input checked="" type="radio"/> CHAP <input type="radio"/> PAP
	<input checked="" type="radio"/> 参照しない <input type="radio"/> 参照する AAAグループID <input type="text"/> 認証プロトコル <input checked="" type="radio"/> CHAP <input type="radio"/> PAP

権限クラスによって参照するAAAを分ける方法では、管理者/一般ユーザが共にAAA情報を参照する場合、認証プロトコルは管理者で参照するAAA情報にて指定されたものになります。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

本装置にログインするときのユーザ認証で参照するAAA情報を設定します。

以下の2つの方法があり、どちらかを選択します。

- 権限クラスは AAA/RADIUS サーバで設定する
権限クラスを AAA グループまたは RADIUS サーバで設定する方法です。
- 権限クラスによって参照する AAA を分ける
認証時に参照する AAA グループを権限クラスによって分ける方法です。

認証時に参照する AAA グループを分ける方法の場合、ユーザ認証は、管理者、一般ユーザの順番に行い、ログイン時のユーザによって権限クラスが決定され、権限クラスにより実行できる画面が異なります。パスワード入力によって操作できる時間は10分間です。それ以降の操作では再びパスワード入力して処理を行ってください。

なお、ログインユーザ情報によるユーザ認証を行うには、ログインパスワード情報の管理者パスワードが設定されている必要があります。

参照する AAA 情報

“権限クラスは AAA/RADIUS サーバで設定する”を選択した場合に設定します。

AAA グループ ID

ユーザ認証を行う場合に参照する AAA のグループ ID を、10 未満の 10 進数で指定します。

認証プロトコル

ユーザ情報を RADIUS サーバに設定してユーザ認証を行う場合に使用する認証プロトコルを指定します。

管理者で参照する AAA 情報／ 一般ユーザで参照する AAA 情報

“権限クラスによって参照する AAA を分ける”を選択した場合に設定します。

管理者でユーザ認証を行う場合は、“管理者で参照する AAA 情報”を、一般ユーザでユーザ認証を行う場合は、“一般ユーザで参照する AAA 情報”を設定します。

AAA グループ ID

ユーザ認証を行う場合に参照する AAA のグループ ID を、10 未満の 10 進数で指定します。

認証プロトコル

ユーザ情報を RADIUS サーバに設定してユーザ認証を行う場合に使用する認証プロトコルを指定します。

11 装置情報

適用機種 全機種

[操作] 基本設定「装置情報」

装置情報		
ルータ名称情報	タイムサーバ情報	システムログ情報
ファームウェア更新情報	異常時動作情報	IPv4 ループバック情報
IPv6 ループバック情報	サーバ機能情報	外部メディアスタート機能情報
装置固有の機能についての設定ができます。		

11.1 ルータ名称情報

[操作] 基本設定「装置情報」 → [ルータ名称情報]

■ルータ名称情報	
ルータ名称	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/>	<input type="button" value="キャンセル"/>

ルータ名称

本装置の任意な名称を32文字以内で指定します。ルータ名称を設定すると、DHCP クライアント機能で DHCP サーバにルータ名称が広報されます。そのため、DHCP サーバからはこの名称で管理することができます。

こんな事に気をつけて

「SNMP 情報」の機器名称で“ルータ名称を使用する”を選択した場合、この名称が SNMP の機器名称として使用されます。

11.2 タイムサーバ情報

[操作] 基本設定「装置情報」→ [タイムサーバ情報]

■ タイムサーバ情報	
タイムサーバ機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
サーバ設定	<input checked="" type="radio"/> DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 <input type="radio"/> 設定する
	プロトコル <input checked="" type="radio"/> TIMEプロトコル <input type="radio"/> SNTPプロトコル タイムサーバIPアドレス <input type="text"/>
自動時刻設定間隔	<input type="text"/> 日 <input type="button" value="▼"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

タイムサーバ機能

ネットワーク上のタイムサーバから時刻情報を取得することによって、内部時刻を自動的に設定する場合は、“使用する”を選択します。

サーバ設定

使用するタイムサーバを指定します。“DHCPで取得する”を選択した場合は、DHCPクライアントの設定が必要です。直接IPアドレスで設定する場合は、“設定する”を選択し、プロトコルを選択して、タイムサーバIPアドレスを指定します。

プロトコル

タイムサーバから時刻情報を取得するときのプロトコルを選択します。

TIMEプロトコル

TIMEプロトコル(TCP)を使用する場合に指定します。

SNTPプロトコル

簡易NTPプロトコル(UDP)を使用する場合に指定します。

タイムサーバIPアドレス

タイムサーバのIPv4／IPv6アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

自動時刻設定間隔

タイムサーバから定期的に時刻情報を取得するときの取得周期を0～10日の範囲で指定します。省略または0を設定すると、起動(再起動)時だけ時刻情報を取得します。

11.3 システムログ情報

[操作] 基本設定「装置情報」→ [システムログ情報]

■システムログ情報		
システム ログ 送信	サーバ1	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 送信先ホスト <input type="text"/>
	サーバ2	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 送信先ホスト <input type="text"/>
	サーバ3	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 送信先ホスト <input type="text"/>
	ヘッダ部の追加	<input checked="" type="radio"/> しない <input type="radio"/> する 送信元IPアドレス <input type="text"/>
セキュリティログ		
<input type="checkbox"/> PPP <input type="checkbox"/> IPフィルタ <input type="checkbox"/> URLフィルタ <input type="checkbox"/> NAT <input type="checkbox"/> DHCP <input type="checkbox"/> IDS <input type="checkbox"/> IEEE802.1X認証 <input type="checkbox"/> MACアドレス認証 <input type="checkbox"/> ARP認証		
重複メッセージの出力	<input checked="" type="radio"/> する <input type="radio"/> しない	
コマンド履歴の出力	<input type="radio"/> する <input checked="" type="radio"/> しない	
対象 IEEE802.1X認証	<input checked="" type="checkbox"/> 認証成功 <input checked="" type="checkbox"/> 再認証成功 <input checked="" type="checkbox"/> 認証失敗 <input checked="" type="checkbox"/> 認証解除	
ARP認証	<input checked="" type="checkbox"/> 認証成功 <input checked="" type="checkbox"/> 認証失敗	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

接続切断、トラブルなどのさまざまな情報のシステムログをネットワーク上のsyslogサーバに対して送信することができます。その場合のファシリティ、プライオリティは以下のとおりです。

ファシリティ : local7 (23)

プライオリティ : error、warn、info、notice (※1)

※1) noticeはセキュリティログを使用する場合だけ出力されます。

 参照 プライオリティ、ファシリティの設定は、「[コマンドリファレンス-構成定義編-](#)」のsyslog priおよびsyslog facilityを参照してください。

システムログ送信

syslog 形式で syslog サーバにシステムログ情報を送信する場合は、" 送信する " を選択します。
送信先のサーバは3台まで定義できます。

サーバ1／2／3

送信先ホスト

送信先のIP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

ヘッダ部の追加

syslog サーバに送信するシステムログ情報にヘッダ部(タイムスタンプおよびホスト名)を追加する場合は、" する " を選択します。

送信元IP アドレス

ホスト名が未設定の場合に、ヘッダ部に設定する IP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

セキュリティログ

PPP の認証エラー情報、IP フィルタ、URL フィルタ、NAT により遮断されたパケットのログ情報、DHCP サーバが割り当てた IP アドレスログ、IDS により検出されたパケットのログ情報、IEEE802.1X 認証、MAC アドレス認証、ARP 認証のログ情報を採取します。

重複メッセージの出力

システムログにメッセージを出力するとき、直前に出力したメッセージと重複した場合に出力する場合は、" する " を選択します。

コマンド履歴の出力

コマンド実行履歴をシステムログに出力する場合は、" する " を選択します。

対象イベント

以下の機能ごとに出力対象とするイベントを設定します。

- IEEE802.1X 認証
- ARP 認証

11.4 ファームウェア更新情報

[操作] 基本設定「装置情報」→ [ファームウェア更新情報]

■ファームウェア更新情報

転送元ホスト名	<input type="text"/>
ログインID	<input type="text"/>
ログインパスワード	<input type="password"/>
ファイルロケーション	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ファームウェアを入れ替えたり、レベルアップを行うときに、転送元となるホストに接続するための情報を設定します。ファームウェアの更新操作は保守メニューから行うことができます。

転送元ホスト名

更新ファームウェアが存在するホスト名を128文字以内で指定します。IPv4/IPv6アドレスを指定することもできます。

こんな事に気をつけて

ProxyDNS 機能が設定されていない場合、ホスト名指定によるファームウェア更新は行えません。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff

ログインID

ファームウェア更新用のログインIDを16文字以内で指定します。

ログインパスワード

ファームウェア更新用のパスワードを32文字以内で指定します。

ファイルロケーション

更新用ファームウェアのロケーションを80文字以内で指定します。

11.5 異常時動作情報

[操作] 基本設定「装置情報」→ [異常時動作情報]

■異常時動作情報

CE保守ログイン	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
ウォッチドッグリセット機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
冷却ファン異常時の動作	<input checked="" type="radio"/> 運用継続 <input type="radio"/> システムダウン
温度異常時の動作	<input checked="" type="radio"/> 運用継続 <input type="radio"/> システムダウン
その他のハードエラー発生時の動作	<input checked="" type="radio"/> 運用継続 <input type="radio"/> システムダウン
システムダウン時の電源制御	<input checked="" type="radio"/> 切断する <input type="radio"/> 切断しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

本装置になんらかの異常が発生した場合の動作を設定します。

Si-R570、570B以外では、表示が上記の画面とは異なります。

CE保守ログイン

CEログインを許可する場合は、“許可する”を選択します。CEログインを許可することで、CEの保守作業を円滑に進めることができます。

ウォッチドッグリセット機能

ウォッチドッグリセット機能を使用する場合は、“使用する”を選択します。“使用する”を選択した場合、本装置がハングアップすると16～48秒以内にリセットがかかり再起動します。

冷却ファン異常時の動作 (Si-R240B、370、370B、570、570B)

冷却ファン異常を検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

温度異常時の動作 (Si-R180B 除く)

温度異常を検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

その他のハードエラー発生時の動作 (Si-R180B 除く)

冷却ファン、温度異常および電源異常以外のハードエラーを検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

ハードエラー発生時の動作 (Si-R180B)

ハードエラーを検出した場合にシステムダウンを行うか（縮退モードへ遷移）、そのまま運用を継続するかを選択します。

システムダウン時の電源制御 (Si-R570、570B)

冷却ファン異常または温度異常でシステムダウンを行う場合に、本装置の電源を切断する場合は、“切断する”を選択します。

11.6 IPv4 ループバック情報

[操作] 基本設定「装置情報」→ [IPv4 ループバック情報]

IP アドレス

ループバックインターフェースに割り当てる追加IPアドレスを指定します。ループバックインターフェースに割り当てたIPアドレスを通信に使用する場合は、以下の範囲の中で通信可能なアドレスを指定します。省略または0.0.0.0を設定した場合、ループバックアドレスを使用しないものとします。

有効範囲)

1.0.0.1-126.255.255.254
128.0.0.1-191.255.255.254
192.0.0.1-223.255.255.254

こんな事に気をつけて

- ほかのインターフェースと違うネットワークのIPアドレスを設定してください。
- 127.0.0.1はループバックインターフェースにすでに設定されています。ループバック情報として127.0.0.1を設定する必要はありません。

OSPF 機能

ループバックに割り当てるIPアドレスをOSPFで広報するかどうかを選択します。“使用する”を選択した場合、IPアドレスが設定されているときだけOSPFで広報します。広報するIPアドレスは、設定したIPアドレスだけです。すでに設定されているIPアドレス127.0.0.1は広報しません。

ループバックインターフェースも含めて、OSPFを使用できるインターフェースは、仕様一覧 [\[2.3 システム最大値一覧\]\(P.43\)](#) を参照してください。

エリア定義番号

広報を行うOSPFエリア情報の定義番号を指定します。指定する定義番号のOSPFエリア情報はあらかじめ設定しておく必要があります。OSPFエリア情報の設定は、「ルーティングプロトコル情報」の [OSPF 関連] にあります。

PHP 機能

ループバックインターフェースでのLSPのPHP機能を設定します。PHP機能を無効にする場合は、“使用しない”を選択します。PHP機能を有効にする場合は、“使用する”を選択します。MPLSトンネル接続を使用する場合に、自側エンドポイントとIPアドレスが同じとき、設定に関係なく“使用しない”が設定されます。

11.7 IPv6 ループバック情報

[操作] 基本設定「装置情報」→ [IPv6 ループバック情報]

■IPv6 ループバック情報

IPアドレス	<input type="text"/>
--------	----------------------

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IP アドレス

ループバックインターフェースに割り当てる追加IPv6 アドレスを 128ビットで指定します。本装置ではプレフィックス長は 128に固定となります。省略した場合、ループバックアドレスを使用しないものとします。

こんな事に気をつけて

- ・ ::1 はループバックインターフェースにすでに設定されています。ループバック情報として ::1 を設定する必要はありません。
- ・ リンクローカルアドレスは指定できません。

11.8 サーバ機能情報

[操作] 基本設定「装置情報」→ [サーバ機能情報]

■サーバ機能情報

※機能毎に利用端末を制限したい場合は、アプリケーションフィルタ機能の“設定”より設定してください。

機能名	動作	アプリケーションフィルタ機能
FTPサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
TELNETサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
SSHサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
SFTP	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
HTTPサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
DNSサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
SNTPサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
TIMEサーバ機能	<input checked="" type="radio"/> IPv4／IPv6 <input type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> 停止	<input type="button" value="設定"/>
	UDP	<input type="button" value="設定"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置の各サーバ機能を有効にするか停止するかを設定します。

FTP サーバ機能

FTP サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の [設定] ボタンをクリックして設定してください。

SFTP

SFTP サーバによる FTP 機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の [設定] ボタンをクリックして設定してください。

TELNET サーバ機能

TELNET サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の [設定] ボタンをクリックして設定してください。

HTTP サーバ機能

HTTP サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の [設定] ボタンをクリックして設定してください。

SSH サーバ機能

SSH

SSH サーバによるログイン機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

DNS サーバ機能

DNS サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の [設定] ボタンをクリックして設定してください。

SNTP サーバ機能

SNTP サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の【設定】ボタンをクリックして設定してください。

TIME サーバ機能

TCP

TCP による TIME サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

UDP

UDP による TIME サーバ機能を有効にするプロトコルを選択します。

- IPv4／IPv6
IPv4 と IPv6 プロトコルの両方で有効にする
- IPv4
IPv4 プロトコルだけ有効にする
- IPv6
IPv6 プロトコルだけ有効にする
- 停止
すべて停止する

利用端末を制限したい場合は、アプリケーションフィルタ機能の【設定】ボタンをクリックして設定してください。

11.8.1 アプリケーションフィルタ情報

[操作] 基本設定「装置情報」→「サーバ機能情報」→「アプリケーションフィルタ情報」

■アプリケーションフィルタ情報(FTP) [ACL定義参照](#)

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	ACL定義番号	操作
		ACL定義名	
条件にあてはまらない場合の動作		透過	修正 初期化
全削除			

<アプリケーションフィルタ情報入力フィールド>

動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
ACL定義番号	参照

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

こんな事に気をつけて

WWWに対するアクセスを制限する設定を行った場合、本装置に対しWWWブラウザからアクセスできなくなる場合があります。

動作

アプリケーションフィルタの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

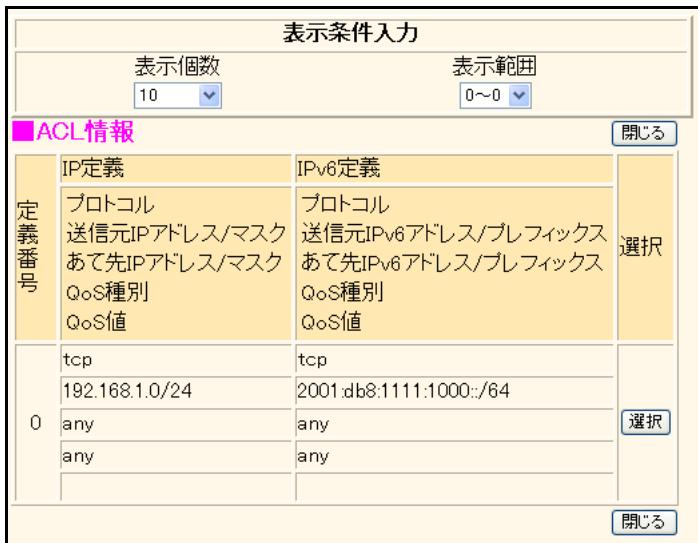
ACL 定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP 定義
- IPv6 定義

指定する定義番号欄の「[選択]」ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。
なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。「OK」ボタンをクリックして、設定をやり直してください。

[操作] 基本設定「装置情報」→[サーバ機能情報]→[アプリケーションフィルタ情報]
→「ACL 定義番号の [参照]」



「ACL情報」 - 「追加」／「修正」 - 「IP定義情報」および「IPv6定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

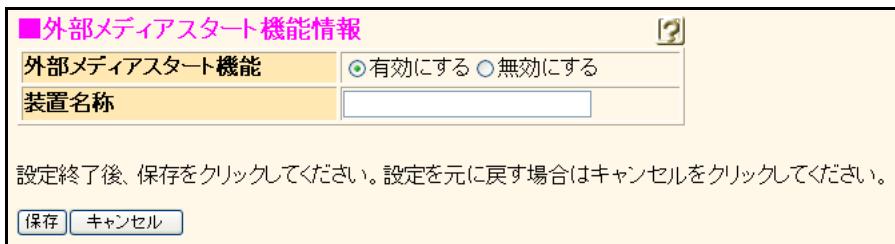
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報をだけを表示させることができます。

参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「アプリケーションフィルタ情報」のACL定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「アプリケーションフィルタ情報」にACL定義番号が設定され、画面が閉じます。[ACL定義参照]ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

11.9 外部メディアスタート機能情報

[操作] 基本設定「装置情報」→[外部メディアスタート機能情報]



外部メディアスタート機能

外部メディア（USBメモリ）を接続することで、PCレスでの設定変更／ファーム更新を可能にします。

装置名称

装置名称を32文字以内で指定します。省略時は初期値の装置名を利用します。

外部メディアスタート機能の有効時、ファームウェアおよび構成定義の退避／復旧の際のファイル名に付加します。

12 スケジュール情報

[操作] 基本設定「スケジュール情報」

スケジュール情報

月間／週間予約情報	電話番号変更予約情報	構成定義切り替え予約情報
-----------	------------	--------------

このページでは、スケジュール予約情報を設定できます。設定するスケジュール予約をクリックしてください。スケジュールの一覧が表示されますので、各予約で必要な処理のボタンをクリックしてください。

⚠️スケジュール機能を使用する際には、正しい時刻が設定されているか確認してください。現在の時刻は **Fri Dec 22 10:35:10 2006** です。

Si-R180B、260B では、「電話番号変更予約情報」は表示されません。

12.1 月間／週間予約情報

適用機種 全機種

[操作] 基本設定「スケジュール情報」 → [月間／週間予約情報]

■月間／週間予約情報

動作	予約時刻	終了時刻	周期	操作
1	-	-	-	修正 削除
2	-	-	-	修正 削除
3	-	-	-	修正 削除
4	-	-	-	修正 削除
5	-	-	-	修正 削除
6	-	-	-	修正 削除
7	-	-	-	修正 削除
8	-	-	-	修正 削除
9	-	-	-	修正 削除
10	-	-	-	修正 削除
11	-	-	-	修正 削除
12	-	-	-	修正 削除
13	-	-	-	修正 削除
14	-	-	-	修正 削除
15	-	-	-	修正 削除
16	-	-	-	修正 削除

全削除

保存した情報は、設定反映後に有効になります。

現在、設定されている月間または週間の予約が表示されています。処理するボタンをクリックし、次のページへ進みます。

Si-R180B、260B では、“終了時刻” の項目は表示されません。

[操作] 基本設定「スケジュール情報」→ [月間／週間予約情報] → [修正]

Si-R180B、260B では、"終了時刻" の設定項目は表示されません。

動作

発信抑止／着信抑止／ISDN課金情報クリア／モデム課金情報クリア／データ通信カード課金情報クリア／強制切断／リモートパワーオンの中から予約する処理動作を選択します。

Si-R180B、260B では、リモートパワーオンだけをサポートしています。

発信抑止

指定した時刻の間、自動発信を抑止します。

着信抑止

指定した時刻の間、自動着信を抑止します。

ISDN課金情報クリア

予約時刻に ISDN 課金情報をクリアします。

モデム課金情報クリア

予約時刻にモデム課金情報をクリアします。

データ通信カード課金情報クリア

予約時刻にデータ通信カード課金情報をクリアします。

強制切断

予約時刻に強制切断を実施します。

リモートパワーオン

予約時刻にホストデータベース情報で MAC アドレスが登録されている Wake up on LAN に対応したすべてのパソコンに対してリモートパワーオン処理を実施します。

予約時刻

選択した動作を実行（開始）する時刻と実行周期を指定します。

終了時刻 (Si-R220C、220D、240B、370、370B、570、570B)

選択した動作を終了する時刻を指定します。動作として発信抑止または着信抑止を選択した場合だけ設定できます。ここで予約時刻よりも早い時刻を指定した場合、実行は翌日の時刻になります。

12.2 電話番号変更予約情報

[適用機種] Si-R220C,220D,240B,370,370B,570,570B

[操作] 基本設定「スケジュール情報」→ [電話番号変更予約情報]

■電話番号変更予約情報

実行日時	電話番号変更情報	操作
1 -	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
2 -	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
3 -	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
4 -	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
<input type="button" value="全削除"/>		

保存した情報は、設定反映後に有効になります。

現在、設定されている電話番号変更予約が表示されています。処理するボタンをクリックし、次のページへ進みます。

[操作] 基本設定「スケジュール情報」→ [電話番号変更予約情報] → [修正]

1 電話番号変更情報	実行日時	20 <input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日 <input type="text"/> 時 <input type="text"/> 分		
	変更前1	<input type="text"/>	変更後1	<input type="text"/>
	変更前2	<input type="text"/>	変更後2	<input type="text"/>
	変更前3	<input type="text"/>	変更後3	<input type="text"/>
	変更前4	<input type="text"/>	変更後4	<input type="text"/>
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>				

実行日時

電話番号を変更する日時を西暦で2000～2036年の範囲で指定します。

電話番号変更情報

変更前と変更後の電話番号をそれぞれ32桁以内で指定します。

12.3 構成定義切り替え予約情報

[適用機種] 全機種

[操作] 基本設定「スケジュール情報」→ [構成定義切り替え予約情報]

実行日時		構成定義切り替え予約	操作
1	20 - -		修正 削除

保存した情報は、設定反映後に有効になります。

[操作] 基本設定「スケジュール情報」→ [構成定義切り替え予約情報] → [修正]

実行日時	20 <input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日 <input type="text"/> 時 <input type="text"/> 分
動作	構成定義情報1で再起動

保存 **キャンセル** **一覧へ戻る**

本装置は構成定義情報が2つ存在します。指定時刻に運用する構成定義情報を切り替えることができます。

なお、現在運用中の構成定義情報は保守メニューの「構成定義情報切り替え」で確認することができます。

こんな事に気をつけて

指定時刻になると、本装置は自動的に再起動され、構成定義情報が切り替わります。その際、データ通信中の場合は接続が切断されます。

実行日時

構成定義情報を切り替える日時を西暦で2000～2036年の範囲で指定します。

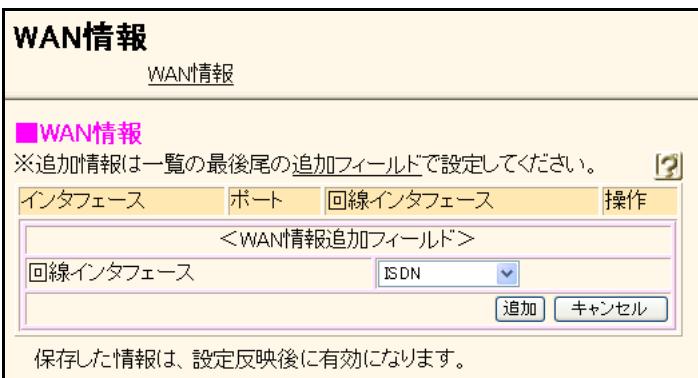
動作

切り替える構成定義情報を指定します。

13 WAN 情報

適用機種 Si-R220C, 220D, 240B, 260B, 370, 370B, 570, 570B

[操作] ルータ設定「WAN 情報」



現在、設定されている WAN インタフェースが表示されています。処理するボタンをクリックし、次のページへ進みます。本装置に接続する回線に関する物理的な情報（回線の種類や電話番号などの契約に関する情報）を設定します。Si-R220C、220D は 1 個、Si-R240B は 2 個、Si-R260B、370、370B は 16 個、Si-R570、570B は 132 個までを装置全体で設定できます。

回線インターフェース

本装置に接続する回線の種類を選択します。

- ISDN (Si-R220C、220D、370、370B、570、570B)
INS ネット 64 などの ISDN 回線交換接続を使用する場合に選択します。
- 専用線 (Si-R220C、220D、370、370B、570、570B)
ハイ・スーパー・デジタル (HSD) や DA64 などの専用線を使用する場合に選択します。
- フレームリレー
(Si-R220C、220D、370、370B、570、570B)
フレームリレー回線を使用する場合に選択します。
- ATM (Si-R260B、370、570)
ATM 回線を使用する場合に選択します。
- データ通信カード (Si-R240B)
データ通信カードを使用する場合に選択します。

13.1 回線インターフェース：ISDN

適用機種 Si-R220C, 220D, 370, 370B, 570, 570B

[操作] ルータ設定「WAN 情報 (ISDN)」→ [追加]

WAN0情報(ISDN)	
基本情報	接続制御情報

13.1.1 基本情報

[操作] ルータ設定「WAN 情報 (ISDN)」→ [追加] → [基本情報]

■ 基本情報															
ポート	スロット 0-0														
自動接続	<input type="radio"/> すべて禁止 <input checked="" type="radio"/> 相手毎に設定														
着信動作	<input type="radio"/> すべて禁止 <input checked="" type="radio"/> 相手毎に設定														
自局番号チェック	<input checked="" type="radio"/> しない <input type="radio"/> する <table border="1"> <tr> <td>チェックする番号1</td> <td>電話番号を指定</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>チェックする番号2</td> <td>電話番号を指定</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>グローバル着信</td> <td><input type="radio"/> 利用しない <input checked="" type="radio"/> 利用する</td> </tr> </table>	チェックする番号1	電話番号を指定	<input type="text"/>		サブアドレス	<input type="text"/>	チェックする番号2	電話番号を指定	<input type="text"/>		サブアドレス	<input type="text"/>	グローバル着信	<input type="radio"/> 利用しない <input checked="" type="radio"/> 利用する
チェックする番号1	電話番号を指定	<input type="text"/>													
	サブアドレス	<input type="text"/>													
チェックする番号2	電話番号を指定	<input type="text"/>													
	サブアドレス	<input type="text"/>													
グローバル着信	<input type="radio"/> 利用しない <input checked="" type="radio"/> 利用する														
発信者番号通知	<input checked="" type="radio"/> 網契約に従う <input type="radio"/> しない <input type="radio"/> する <table border="1"> <tr> <td>通知する電話番号</td> <td>電話番号を指定</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> </table>	通知する電話番号	電話番号を指定	<input type="text"/>		サブアドレス	<input type="text"/>								
通知する電話番号	電話番号を指定	<input type="text"/>													
	サブアドレス	<input type="text"/>													
レイヤ1起動種別	<input checked="" type="radio"/> 常時起動 <input type="radio"/> 呼毎起動 <table border="1"> <tr> <td>回線停止猶予時間</td> <td>60</td> <td>秒</td> </tr> </table>	回線停止猶予時間	60	秒											
回線停止猶予時間	60	秒													
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>															

ポート

回線を接続するスロットおよびポートを選択します。

自動接続

この回線に対する自動接続を装置全体で禁止するときに“すべて禁止”を選択します。“すべて禁止”を選択した場合は、いかなる通信データ発生時にも自動的に接続しません。“相手毎に設定”を選択した場合は、「相手情報」-「ネットワーク情報」-「接続先情報」で設定します。

着信動作

この回線に対する着信動作を装置全体で禁止するときに“すべて禁止”を選択します。“すべて禁止”を選択した場合は、すべてのデータ通信の着信を拒否し、発信専用となります。“相手毎に設定”を選択した場合は、「相手情報」-「ネットワーク情報」-「接続先情報」で設定します。

自局番号チェック

ダイヤルイン番号やi・ナンバー、サブアドレスを利用して着信機器識別するときに“する”を選択し、使用する番号を指定します。この番号は2つまで設定できます。

電話番号は、“電話番号を指定”、“i・ナンバー情報1（契約者回線番号）”、“i・ナンバー情報2/3（追加の番号）”のどれかを選択します。“電話番号を指定”を選択した場合は、その右の記入欄に電話番号を32桁まで指定します。また、どの場合にもサブアドレスは19桁まで指定できます。“電話番号を指定”を選択し、右の記入欄に電話番号を記述しないでサブアドレスだけを指定した場合は、電話番号は任意となります。

グローバル着信を行う場合は「グローバル着信」で“利用する”を選択します。

発信者番号通知

発信者番号通知の内容を変更する場合に設定します。通常は“網契約に従う”を選択します。“する”を選択した場合は、通知する電話番号とサブアドレスを指定します。電話番号は32桁まで、サブアドレスは19桁まで指定できます。

レイヤ1起動種別

回線同期確立手順の方式（レイヤ1起動種別）を選択します。

回線停止猶予時間

“呼毎起動”を指定した場合に、通信終了後の回線停止猶予時間を1～300秒の範囲で指定します。省略時は、60秒が設定されます。

13.1.2 接続制御情報

[操作] ルータ設定「WAN 情報 (ISDN)」→ [追加] → [接続制御情報]

■接続制御情報	
通信時間による発信抑止	<input checked="" type="radio"/> しない
	<input type="radio"/> する
上限時間	1 日
制御動作	<input checked="" type="checkbox"/> 発信抑止 <input type="checkbox"/> システムログ出力のみ
課金額による発信抑止	<input checked="" type="radio"/> しない
	<input type="radio"/> する
上限金額	3000 円
制御動作	<input checked="" type="checkbox"/> 発信抑止 <input type="checkbox"/> システムログ出力のみ

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

通信時間による発信抑止

この回線を使用した通信総時間の自動発信を抑止する場合は、“する”を選択します。

上限時間

制限を行う総通信時間を、1秒～999時間の範囲で指定します。省略はできません。

制限動作

制限時間に達したときに行う動作を選択します。“発信抑止”を選択した場合は、それ以降の自動発信の抑止とシステムログの出力を行います。“システムログ出力のみ”を選択した場合は、自動発信の抑止は行わずにシステムログの出力を行います。

制限動作

制限金額に達したときに行う動作を選択します。“発信抑止”を選択した場合は、それ以降の自動発信の抑止とシステムログの出力を行います。“システムログ出力のみ”を選択した場合は、自動発信の抑止は行わずにシステムログの出力を行います。

課金額による発信抑止

この回線を使用した課金合計金額の自動発信を抑止する場合は、“する”を選択します。

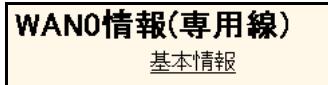
上限金額

制限を行う課金合計金額を、1～999999円の範囲で指定します。省略はできません。

13.2 回線インタフェース：専用線

適用機種 Si-R220C,220D,370,370B,570,570B

[操作] ルータ設定「WAN 情報（専用線）」→ [追加]



13.2.1 基本情報

[操作] ルータ設定「WAN 情報（専用線）」→ [追加] → [基本情報]

■ 基本情報

ポート	スロット 0-0
回線速度	64Kbps
フラグ監視	<input checked="" type="radio"/> 無効にする <input type="radio"/> 有効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

Si-R220C、220D では、ポートの表示が上記の画面とは異なります。

ポート

回線を接続するスロットおよびポートを選択します。

Si-R220C、220D では、ポートは固定です。

回線速度

接続する専用線の回線速度を選択します。

フラグ監視

フラグ監視機能を有効にする場合は、“有効にする”を選択します。

13.3 回線インタフェース：フレームリレー

適用機種 Si-R220C,220D,370,370B,570,570B

[操作] ルータ設定「WAN 情報（フレームリレー）」→ [追加]

WAN0情報(フレームリレー)
基本情報

13.3.1 基本情報

[操作] ルータ設定「WAN 情報（フレームリレー）」→ [追加] → [基本情報]

■ 基本情報	
ポート	スロット0-0
回線速度	64 Kbps
PVC状態確認手順	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
CLLMメッセージ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
輻輳通知ビット	<input checked="" type="checkbox"/> FECN <input checked="" type="checkbox"/> BECN

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

ポート

回線を接続するスロットおよびポートを選択します。

回線速度

接続するフレームリレーの回線速度を選択します。

PVC 状態確認手順

PVC 状態確認手順を使用する場合は、“使用する”を選択します。PVC 状態確認手順は以下の機能を持っています。

- ユーザ網間のリンクの正常性を確認する機能
- ユーザユーザ間の PVC 状態を通知する機能

こんな事に気をつけて

- この機能を使用するには通信事業者と契約する必要があります。
- 本装置は PVC 状態確認手順の双方向手順はサポートしておりません。

CLLM メッセージ

CLLM メッセージ受信時に輻輳制御を行う場合は、“使用する”を選択します。CLLM メッセージは、網が網状態（輻輳、故障）を通知するためにユーザに送出するメッセージです。本装置は通知内容に合わせて動作します。

こんな事に気をつけて

- この機能を使用するには通信事業者と契約する必要があります。

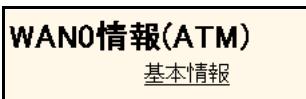
輻輳通知ビット

輻輳制御に利用するビットを選択します。選択したビットがセットされたパケットを受信した場合、本装置は網を正常な状態に戻すためにパケットの送信を抑制します。

13.4 回線インターフェース：ATM

適用機種 **Si-R260B, 370, 570**

[操作] ルータ設定「WAN 情報 (ATM)」→ [追加]



13.4.1 基本情報

[操作] ルータ設定「WAN 情報 (ATM)」→ [追加] → [基本情報]

A screenshot of the 'WAN0情報(ATM)' configuration window showing the 'Basic Information' tab. The window contains several input fields and radio buttons:

- ポート: ドロップダウンメニューで「スロット0-0」を選択。
- VPI: 数値入力欄に「0」を入力。
- VP速度: ラジオボタンで「指定しない」を選択。下部には「Mbps」の単位が示されている。
- OAM(F4): ラジオボタンで「受け付けない」を選択。

メッセージ: 「設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。」

ボタン: 「保存」、「キャンセル」。

ポート

回線を接続するスロットおよびポートを選択します。

VPI

契約時に割り当てられた、VPのVPI値を10進数を使用して、以下の範囲で指定します。

機種	拡張モジュール	VPI
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	0～127
	ATM25M 拡張モジュール H1 ATM155M 拡張モジュール H1	0～255
Si-R370	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	0～127
	-	
Si-R260B	-	

VP 速度

VPの契約速度を以下の範囲で指定します。

機種	拡張モジュール	VP
Si-R570	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64Kbps～25Mbps (8Kbps刻み、または50Kbps刻み)
	ATM25M 拡張モジュール H1	
Si-R370	ATM25M 拡張モジュール H1 ATM155M 拡張モジュール L2	200Kbps～50Mbps (8Kbps刻み、または50Kbps刻み)
	ATM25M 拡張モジュール L2 ATM155M 拡張モジュール L2	64Kbps～25Mbps (8Kbps刻み、または50Kbps刻み)
Si-R260B	-	

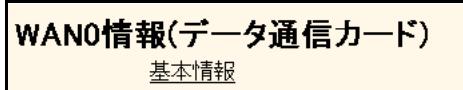
OAM (F4)

VP単位で故障管理を検出する必要がある場合に、“受け付ける”を有効にすることで、VP単位での故障を検出することができます。

13.5 回線インターフェース：データ通信カード

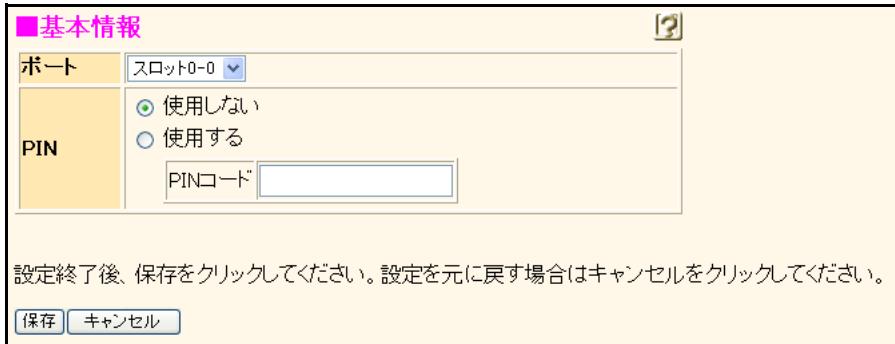
適用機種 **Si-R240B**

[操作] ルータ設定「WAN 情報（データ通信カード）」→ [追加]



13.5.1 基本情報

[操作] ルータ設定「WAN 情報（データ通信カード）」→ [追加] → [基本情報]



ポート

回線を接続するスロットおよびポートを選択します。

PIN

データ通信カードが盗難、紛失された場合に無断使用を防止するための PIN ロック機能を使用するかどうかを選択します。

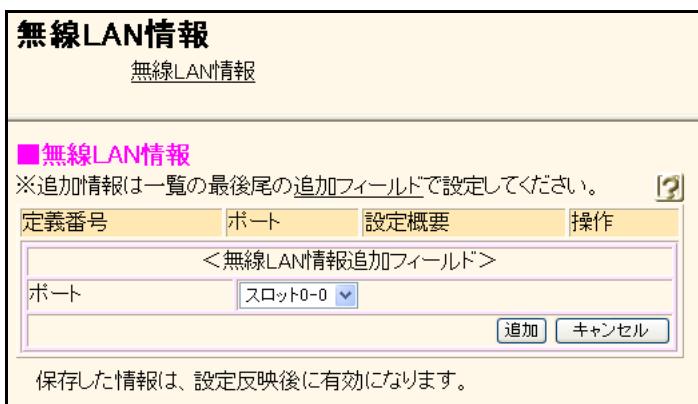
PIN コード

データ通信カードに設定されている PIN コードを設定します。

14 無線 LAN 情報

適用機種 *Si-R240B*

[操作] ルータ設定「無線 LAN 情報」

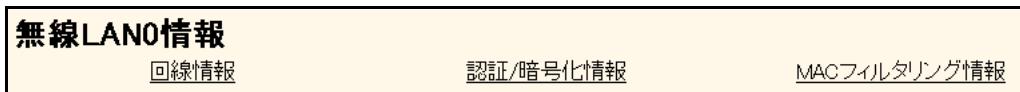


現在、設定されている無線 LAN 定義が表示されています。処理するボタンをクリックし、次のページへ進みます。
本装置に接続する無線 LAN カードに関する回線情報を設定できます。

ポート

回線を接続するスロットおよびポートを選択します。

[操作] ルータ設定「無線 LAN 情報」 → [追加]



14.1 回線情報

[操作] ルータ設定「無線 LAN 情報」→ [追加] → [回線情報]

■回線情報

ポート	スロット0-0
通信モード	11b
チャネル	自動選択
SSID	
SSID非通知	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
接続可能台数	5
無線送信出力	36(最大) ×0.5dBm
プロテクション	<input checked="" type="radio"/> 使用しない <input type="radio"/> CTSモード <input type="radio"/> RTS/CTSモード
RTSしきい値	2346 bytes
DTIM間隔	1
ビーコン送信間隔	100 ×1.024ミリ秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ポート

利用する無線 LAN カードが、どのスロットに挿入されているのかを選択します。

複数の無線 LAN 情報から同一のスロットを指定した場合は、一番定義番号の小さい LAN 情報からバインドされている無線 LAN 情報だけが有効となり、ほかの無線 LAN 定義は無効となります。

無線 LAN の利用には、本指定に加え、LAN 情報と無線 LAN 情報を関連付けする必要があります。

通信モード

無線通信モードを IEEE802.11b、11b/g、11g、11a から選択します。

チャネル

無線 LAN で使用するチャネルを選択します。
また、通信モードにより設定可能な値の範囲が異なります。

通信モード	設定可能な値の範囲
11b	自動選択および1～14
11b/g、11g	自動選択および1～13
11a	自動選択および36、40、44、48

SSID

無線 LAN アクセスポイントを識別する SSID を、32 文字以内の 0x21、0x23～0x7e のコードで構成される ASCII 文字列で指定します。

ビーコンフレームは電波が届く範囲の無線 LAN 端末にアクセスポイントの存在を知らせているため、ユーティリティソフトを使用すれば、第三者でも SSID を確認することができます。第三者が SSID を無断で設定し使用してしまう可能性があるため、必要に応じて SSID 非通知機能やセキュリティ機能を併用することを推奨します。

SSID 非通知

SSID 非通知を有効にすると、アクセスポイントは SSID を隠蔽したビーコンフレームを送信します。

それと同時に、無線 LAN 端末から SSID を指定しない ANY 接続に対して接続を拒否します。

- 使用しない
SSID 非通知を無効にすると同時に、ANY 接続を受け入れます。
- 使用する
SSID 非通知を有効にすると同時に、ANY 接続を拒否します。

接続可能台数

無線 LAN アクセスポイントに接続できる無線 LAN 端末台数の最大数を選択します。

ここで設定した接続可能台数を超えて無線 LAN 端末からの要求を受けると、アクセスポイントは無線 LAN 端末からのアソシエーション要求を失敗させます。

無線送信出力

フレーム送信で使用する無線送信出力を選択します。無線送信出力を 1～36（0.5dBm 単位）から選択します。設定値と送信出力との関係は、以下のようにになります。

設定値	送信出力	設定値	送信出力
1 (最小)	0.5 [dBm]	19	9.5 [dBm]
2	0.5 [dBm]	20	10.0 [dBm]
3	1.0 [dBm]	21	10.5 [dBm]
4	1.5 [dBm]	22	11.0 [dBm]
5	2.0 [dBm]	23	11.5 [dBm]
6	2.5 [dBm]	24	12.0 [dBm]
7	3.0 [dBm]	25	12.5 [dBm]
8	3.5 [dBm]	26	13.0 [dBm]
9	4.0 [dBm]	27	13.5 [dBm]
10	4.5 [dBm]	28	14.0 [dBm]
11	5.0 [dBm]	29	14.5 [dBm]
12	5.5 [dBm]	30	15.0 [dBm]
13	6.0 [dBm]	31	15.5 [dBm]
14	6.5 [dBm]	32	16.0 [dBm]
15	7.0 [dBm]	33	16.5 [dBm]
16	7.5 [dBm]	34	17.0 [dBm]
17	8.0 [dBm]	35	17.5 [dBm]
18	9.0 [dBm]	36 (最大)	18.0 [dBm]

RTS しきい値

RTS 制御フレームを送信するしきい値を 1～2346bytes の範囲の 10 進数で指定します。パケット長がしきい値を超える場合、RTS 制御フレームを送信します。

DTIM 間隔

ビーコンに DTIM を付加する間隔を 1～15 から選択します。1 を指定した場合、すべてのビーコンに DTIM を付加します。

ビーコン送信間隔

ビーコンの送出間隔を 20～1000（1.024ミリ秒単位）の範囲の 10 進数で指定します。

プロテクション

11b/11g 混在環境でのプロテクション（衝突回避）を指定します。

- 使用しない
衝突回避は行いません。
- CTS モード
CTS 制御フレームを使用して衝突回避します。
- RTS/CTS モード
RTS/CTS 制御フレームを使用して衝突回避します。

14.2 認証／暗号化情報

[操作] ルータ設定「無線 LAN 情報」→ [追加] → [認証／暗号化情報]

認証モードで、"open" および "shared" を選択した場合

■認証/暗号化情報

認証モード	<input type="button" value="open"/>
WEPの使用	<input checked="" type="radio"/> WEP不使用端末のみ接続可能 <input type="radio"/> WEP端末のみ接続可能
WEPキー[1]	テキスト <input type="button" value="…"/>
WEPキー[2]	テキスト <input type="button" value="…"/>
WEPキー[3]	テキスト <input type="button" value="…"/>
WEPキー[4]	テキスト <input type="button" value="…"/>
使用WEPキー	<input type="button" value="1"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

認証モードで、"wpa"、"wpa2" および "wpa/wpa2" を選択した場合

■認証/暗号化情報

wpa、wpa2、wpa/wpa2を使用するときは、バインドするLAN情報にIEEE802.1X設定が必須となります。

認証モード	<input type="button" value="wpa"/>
WPA暗号化モード	<input checked="" type="radio"/> TKIP/AES自動判別 <input type="radio"/> TKIP <input type="radio"/> AES
キー更新間隔(GTK)	10 分 <input type="button" value="…"/>
MICエラー検出	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

認証モードで、"wpa-psk"、"wpa2-psk" および "wpa/wpa2-psk" を選択した場合

■認証/暗号化情報

認証モード	<input type="button" value="wpa-psk"/>
WPA暗号化モード	<input checked="" type="radio"/> TKIP/AES自動判別 <input type="radio"/> TKIP <input type="radio"/> AES
WPA事前共有キー	テキスト <input type="button" value="…"/>
キー更新間隔(GTK)	10 分 <input type="button" value="…"/>
MICエラー検出	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

認証モード

IEEE802.11 の認証モードを選択します。

- open
IEEE802.11 のオープン認証を行います。
- shared
IEEE802.11 の共通鍵認証を行います。
- wpa
WPA を使った IEEE802.1X 認証を行います。
- wpa-psk
WPA を使った事前共有キー (PSK) 認証を行います。
- wpa2
WPA2 を使った IEEE802.1X 認証を行います。
- wpa2-psk
WPA2 を使った事前共有キー (PSK) 認証を行います。
- wpa/wpa2
WPA または WPA2 を自動判別して、IEEE802.1X 認証を行います。
- wpa/wpa2-psk
WPA または WPA2 を自動判別して、事前共有キー (PSK) 認証を行います。

shared を指定する場合は、WEP 定義が必須となります。

wpa-psk、wpa2-psk、wpa/wpa2-psk を指定する場合は、事前共有キー (PSK) 設定が必須となります。

wpa、wpa2、wpa/wpa2 を指定する場合は、バインドする LAN 情報に IEEE802.1X 設定が必須となります。

WEP の使用

無線 LAN 端末に無線ネットワークへの接続にあたって WEP を使用させるかどうかを指定します。

- WEP 不使用端末のみ接続可能
WEP を使用しない無線 LAN 端末との通信が可能になります。
- WEP 端末のみ接続可能
WEP を使用した無線 LAN 端末とだけ通信が可能になります。

WEP キー [1] ~ [4]

WEP 暗号に用いる WEP キーを指定します。

- 16 進数
16 進数でキーを指定します。
- テキスト
文字列でキーを指定します。

指定種別によって入力可能な文字数が異なります。

キー種別	16 進数キー	文字列キー
WEP キー長 (IV 除く)		
WEP 64-bit (40-bit)	10 衔	5 文字
WEP 128-bit (104-bit)	26 衔	13 文字
WEP 152-bit (128-bit)	10 衔	16 文字

指定した WEP キーが入力範囲未満の場合は、指定した WEP キー長を超えて近い WEP キー長と判断され、満たない部分は 0x0 でパディングされます。

文字列キーの場合、0x21、0x23～0x7e のコードで構成される ASCII 文字列で指定します。

使用 WEP キー

登録した WEP キーの中から実際に使用する WEP キーの識別番号を指定します。

WPA 暗号化モード

WPA/WPA2 で使用する暗号化モードを指定します。

ここで設定した暗号化モードは、認証モードに WPA/WPA2 に関する設定がされているときに有効です。

- TKIP
TKIP 暗号を行います。
- AES
AES (CCMP) 暗号を行います。
- TKIP/AES 自動判別
TKIP または AES で自動判別して暗号を行います。

WPA 事前共有キー

WPA認証に使用する事前共有キーを指定します

- 16進数
16進数でキーを指定します。
- テキスト
文字列でキーを指定します。

指定種別によって入力可能な文字数が異なります。

キー種別	16進数キー	文字列キー
事前共有キー	64 行	8～63 文字

文字列キーの場合、0x21、0x23～0x7eのコードで構成されるASCII文字列で指定します。16進数キーの場合、指定したキーの桁数が64桁に満たない部分は0x0でパディングされます。

キー更新間隔 (GTK)

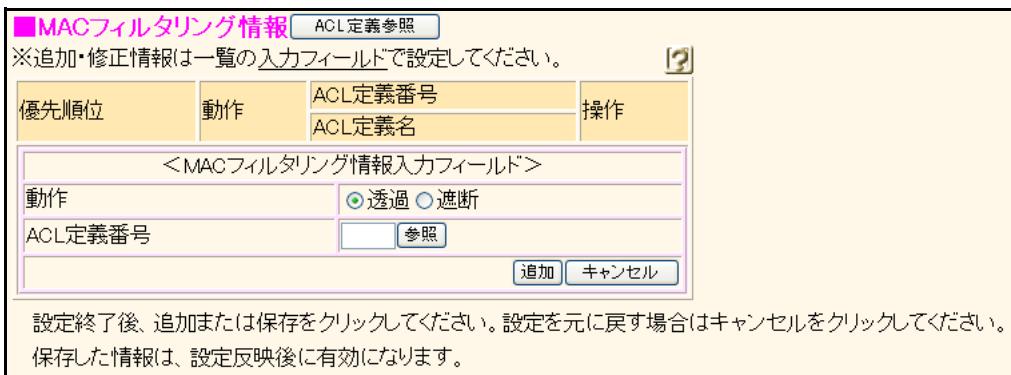
WPA/WPA2で使用するグループキー (GTK) の更新間隔を600（10分）～86400秒（1日）の範囲で指定します。単位は、d（日）、h（時）、m（分）、s（秒）のどれかを選択します。

MIC エラー検出

TKIP暗号化を使用する場合に、パケットの改ざんを防ぐためにMICエラーを検出するかどうかを選択します。60秒に2回以上のMICエラーを検出した場合、すべてのSTA（無線LAN端末）を切断します。さらに、無線LANの動作が保留状態となり、一定時間（60秒）の間、端末接続が行えない状態となります。保留状態が解除されたあとは、STA（無線LAN端末）が接続できる状態に戻ります。

14.3 MAC フィルタリング情報

[操作] ルータ設定「無線 LAN 情報」→ [追加] → [MAC フィルタリング情報]



現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

指定した ACL の送信元 MAC アドレスと一致した無線 LAN 端末の接続を、指定した動作に従って透過または遮断します。設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。

動作

フィルタリング条件に一致したときの MAC フィルタリングの動作を以下の 2 つから選択します。

- 透過
フィルタリング条件と一致する場合にフレームを透過します。
- 遮断
フィルタリング条件と一致する場合にフレームを遮断します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- MAC 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「無線 LAN 情報」→ [追加] → [MAC フィルタリング情報]
 → 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「MAC 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「MAC フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「MAC フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

15 スイッチ情報

適用機種 **Si-R180B**

[操作] ルータ設定「スイッチ情報」

スイッチ情報	
基本情報	ポート情報

15.1 基本情報

[操作] ルータ設定「スイッチ情報」→ [基本情報]

■ 基本情報	
スイッチ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
VLAN tag	<input type="radio"/> 透過しない <input checked="" type="radio"/> 透過する
スイッチの学習テーブル生存時間	288 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

スイッチ

LAN1 ポートのモードを設定します。

“使用する”を選択した場合、LAN1 ポートはスイッチポート (SW1～4) として利用できます。

こんな事に気をつけて

スイッチポートを利用し、複数のネットワークまたは Tagged VLAN を利用する場合は、必ずスイッチポートの VLAN ID と同じ VLAN ID を LAN 情報で設定してください。一致する ID が定義されていない場合は通信ができなくなります。

スイッチの学習テーブル生存時間

スイッチでのスイッチ学習テーブルの生存時間を 0～4080 秒の範囲で指定します。ただし、指定された値は指定値を超えない最大の 16 の倍数に設定されます。

VLAN tag

スイッチポートでの VLAN フレームの tag の扱いについて設定します。“透過する”を選択した場合、すべての VLAN tag は透過的に転送されます。

こんな事に気をつけて

“透過する”を選択した場合、ポート情報で定義された VLAN ID はすべて無視されます。

15.2 ポート情報

[操作] ルータ設定「スイッチ情報」→ [ポート情報]

■ポート情報			
ポート番号	スイッチポート	Tagged VLAN ID Untagged VLAN ID	操作
1	使用する		<input type="button" value="修正"/> <input type="button" value="初期化"/>
2	使用する		<input type="button" value="修正"/> <input type="button" value="初期化"/>
3	使用する		<input type="button" value="修正"/> <input type="button" value="初期化"/>
4	使用する		<input type="button" value="修正"/> <input type="button" value="初期化"/>
<input type="button" value="全初期化"/>			

保存した情報は、設定反映後に有効になります。

現在、設定されているポート情報が表示されています。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「スイッチ情報」→ [ポート情報] → [修正]

<ポート情報入力フィールド>	
スイッチポート	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
転送レート	自動認識
MDI	<input checked="" type="radio"/> 自動 <input type="radio"/> MDI <input type="radio"/> MDI-X
フロー制御機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
VLAN ID	Tagged <input type="text"/> Untagged <input type="text"/>
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>	

スイッチポート

スイッチポートを使用するかどうかを設定します。“使用しない”を選択した場合は、そのポートはリンクアップしません。

転送レート

ポートの転送レートを以下から選択します。

- 自動認識（通信速度を自動的に設定する場合）
- 100Mbps - 全二重
- 100Mbps - 半二重
- 10Mbps - 全二重
- 10Mbps - 半二重

MDI

MDIのモードを設定します。

“自動”を選択した場合、MDIを自動検出します。

こんな事に気をつけて

MDIの自動検出は、転送レートの設定が“自動認識”である場合にのみ有効となります。転送レートの設定が“自動認識”以外の場合は、MDIの自動検出を指定しても、MDI-Xとして動作します。また、転送レートが“自動認識”と設定されている場合は本設定にかかわらず、常に“自動認識”が指定されたものとみなされます。

フロー制御機能

フロー制御の動作を設定します。

“使用する”を選択した場合は、フロー制御機能を送受信ともに使用するとみなします。“使用しない”を選択した場合は、フロー制御機能を送受信ともに使用しないとみなします。

VLAN ID

VLAN ID を設定します。Tagged VLAN ID と Untagged VLAN ID で合わせて 10 組まで指定できます。

Tagged

Tagged VLAN ID を 1 ~ 4094 の範囲で指定します。

複数指定する場合は、"," で区切れます。範囲指定の場合は
"- -" で区切れます。

Untagged

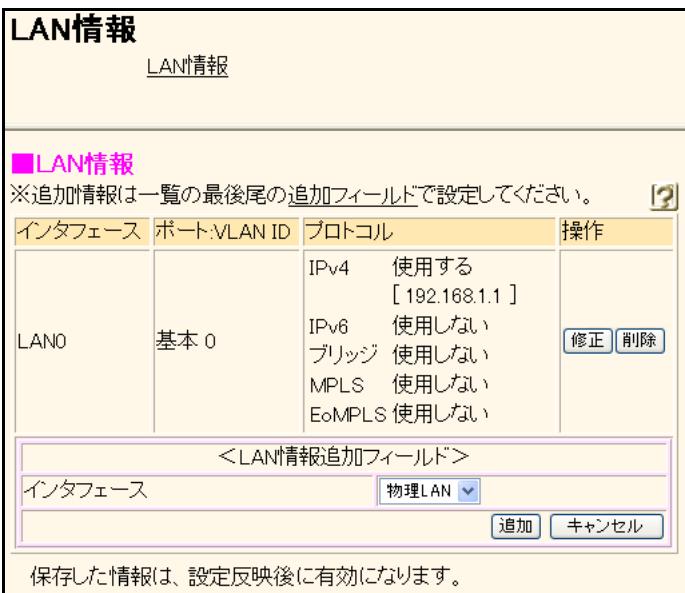
Untagged VLAN ID を 1 ~ 4094 の範囲で指定します。

複数指定することはできません。

16 LAN 情報

適用機種 全機種

[操作] ルータ設定「LAN 情報」



現在、設定されている LAN インタフェースの定義が表示されています。LAN インタフェースには、物理インターフェース、VLAN インタフェースおよび無線 LAN 用の論理インターフェースがあります。装置全体での LAN インタフェースの定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」 (P43) を参照してください。ただし、物理インターフェースの有効な定義は基本ボードおよび拡張スロットに存在する LAN ポートの数までです。処理するボタンをクリックし、次のページへ進みます。

インターフェース

設定する LAN インタフェースの種別を以下から選択します。

- 物理 LAN
物理的に接続された LAN を使用する場合に選択します。
- VLAN
物理 LAN 上に仮想的な LAN を使用する場合に選択します。
- 無線 LAN
無線 LAN 用の論理インターフェースとして使用する場合に選択します。

16.1 インタフェース：物理 LAN

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正]

LAN0情報(物理LAN)

共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
------	------	--------	--------	--------

このページではLAN情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

「LAN 情報」で選択するインターフェースによって表示が異なります。

16.1.1 共通情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報]

LAN0情報(物理LAN)

共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
------	------	--------	--------	--------

基本情報	VRRPグループ情報	LLDP情報
IEEE802.1X認証情報	MACアドレス認証情報	ARP認証関連
トラップ情報		

16.1.1.1 基本情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [基本情報]

■基本情報

ポート番号	master	基本	▼
	backup	バックアップなし	▼
優先使用ポート	<input checked="" type="radio"/> master <input type="radio"/> 先にリンクアップしたポート		
転送レート	自動認識 <input type="radio"/>		
シェーピング	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 最大送信レート <input type="text"/> Mbps <input type="radio"/>		
VRRP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する パスワード <input type="text"/> TRAPモード <input checked="" type="radio"/> 旧仕様 <input type="radio"/> 新仕様 <input type="radio"/>		
MTUサイズ	1500 バイト		
自動復旧	モード	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
	初期状態	<input checked="" type="radio"/> 非閉塞 <input type="radio"/> 閉塞	
MDI	<input checked="" type="radio"/> 自動 <input type="radio"/> MDI <input type="radio"/> MDI-X		
フロー制御機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない		
使用ポート	<input checked="" type="radio"/> 自動 <input type="radio"/> 通常 <input type="radio"/> ファイバ		

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

Si-R570、570B以外では、表示が上記の画面とは異なります。

ポート番号

master

起動時に使用する物理ポート番号を選択します。

backup

master で設定したポートで障害が発生した場合に、切り替えて使用する物理ポート番号を選択します。

こんな事に気をつけて

Si-R180B では、スイッチを選択する場合、対象となるスイッチポート (SW1~4) は、TAG 透過モードに設定してください。スイッチポートがTAG 透過モードでない場合は、通信ができません。

最大送信レート

最大送信レートを以下の範囲で指定します。Kbps は 1000bps を、Mbps は 1000Kbps を意味します。

機種	最大送信レート
Si-R570、570B 以外	1 ~ 100000Kbps
Si-R570、570B	1 ~ 1000000Kbps

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを“使用する”に設定してください。

優先使用ポート (Si-R180B 除く)

master ポートと backup ポートの両方が使用可能なときに使用するポートを選択します。

- master
master ポートを優先的に使用します。
- 先にリンクアップしたポート
master ポートと backup ポートのどちらか先にリンクアップして使用可能になったポートを使用します。

転送レート

接続する回線の転送レートを以下から選択します。

- 自動認識 (通信速度を自動的に設定する場合)
- 1000Mbps - 全二重 (Si-R570、570B)
- 100Mbps - 全二重
- 100Mbps - 半二重
- 10Mbps - 全二重
- 10Mbps - 半二重

シェーピング

シェーピング (リミッタ) 機能を設定します。シェーピング機能を使用する場合は“使用する”を選択し、最大送信レートを指定します。最大送信レートで設定したレートに送信を抑制します。

VRPP 機能

VRPP を使用する場合は、“使用する”を選択します。VRPP を使用するとルータの冗長構成を組むことができます。VRPP を使用しない場合は、以降の設定は無効になります。

パスワード

マスタが送信する Advertisement パケットに認証情報を含める場合に、パスワードを 8 文字以内で指定します。このインターフェースから送信されるすべての Advertisement パケットに適用されます。たとえば、同じネットワークでグループ ID を重複させて別グループとして扱う、などの特別な環境である場合に設定します。

なお、仮想 IP アドレスが IPv6 アドレスである VRPP グループは、パスワードを設定した場合であっても Advertisement パケットに認証情報は含まれません。

TRAP モード

IPv4 VRRP が送信する TRAP モードを選択します。

- 旧仕様
IPv4 VRRP が送信する TRAP モードとして旧仕様 (RFC2787) を使用します。
- 新仕様
IPv4 VRRP が送信する TRAP モードとして新仕様 (draft-ietf-vrrp-unified-mib-06) を使用します。

こんな事に気をつけて

仮想 IP アドレスが IPv6 アドレスである VRPP グループは、“旧仕様”を選択した場合であっても“新仕様”を使用します。

MTU サイズ

最大パケット送信サイズ (Maximum Transmission Unit) を 200～1500 バイトの範囲で指定します。

IPv6 通信で利用する場合は、1280 バイト以上 の値を指定します。

ブリッジを利用する場合は、1500 バイトを指定します。1500 バイト未満を指定すると正しくブリッジ通信できない場合があります。

RIP を利用する場合は、576 バイト以上を指定します。576 バイト未満を指定すると RIP パケットが送信されない場合があります。

自動復旧

LAN インタフェースに関する LAN 自動復旧の設定をします。

モード

LAN 故障時の自動復旧の動作モードを設定します。“しない”に設定した場合、LAN 故障が復旧してもオペレータ指示があるまで接続を復旧しません。

初期状態

初期状態を“閉塞”にすると、閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

MDI

MDI のモードを設定します。“自動”を選択した場合、MDI を自動検出します。

なお、Si-R180B、260B では、MDI の自動検出はサポートしていないため、“自動”がありません。

Si-R260B では LAN1～3 ポートで設定することができます。

Si-R260B では、LAN0 ポートは、to HUB to PC スイッチでだけ設定を変更することができます。

Si-R180B では、LAN0 ポートの設定だけ有効です。LAN1 ポートをスイッチポートとして使用しない場合は、LAN1 ポートは MDI として動作します。

こんな事に気をつけて

MDI の自動検出は、転送レートが“自動認識”である場合に有効です。

フロー制御機能 (Si-R220C、220D、240B、370、370B、570、570B)

フロー制御の動作を行う場合は、“使用する”を選択します。

使用ポート (Si-R570、570B)

基本ボード上の LAN0／1 ポート (RJ45) と LAN0／1 ファイバポートを排他利用することができます。LAN0／1 ポートを使用する場合は“通常”、LAN0／1 ファイバポートを使用する場合は“ファイバ”、ポートを自動で検出する場合は“自動”を選択します。

16.1.1.2 VRRP グループ情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [VRRP グループ情報]

グループ番号	グループID	プライオリティ	AD送信間隔	ブリエンプトモード	仮想IPアドレス	操作
0	-	-	-	-	-	修正 削除
1	-	-	-	-	-	修正 削除

保存した情報は、設定反映後に有効になります。

現在、設定されている VRRP グループ情報の定義が表示されています。VRRP グループは、それぞれのインターフェースで 2 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [VRRP グループ情報] → [修正]

LAN0情報 - VRRP グループ0情報

基本情報	VRRPトリガ情報	VRRPアクション情報
----------------------	---------------------------	-----------------------------

16.1.1.2.1 基本情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [VRRP グループ情報] → [修正] → [基本情報]

■ 基本情報

グループID	<input type="text"/>
プライオリティ	<input checked="" type="radio"/> 優先度指定 優先度 <input type="text"/> 仮想IPアドレス <input type="text"/> <small>※IPv6では一つしか設定できません</small>
	<input type="radio"/> 優先度固定(最優先) 優先度 <input type="text"/> 255 仮想IPアドレス <input type="checkbox"/> インタフェースアドレスを使用 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
AD送信間隔	1 <input type="text"/> 秒
ブリエンプトモード	<input checked="" type="radio"/> ON <input type="radio"/> OFF 移行禁止時間 <input type="text"/> 0 秒
仮想IPアドレス あて ICMP ECHO	<input checked="" type="radio"/> 応答しない <input type="radio"/> 応答する 応答送信元 <input checked="" type="radio"/> 仮想IPアドレス <input type="radio"/> IPアドレス <input type="radio"/> インタフェースアドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

グループ ID

VRRP グループのグループ ID を 1 ~ 255 の範囲で指定します。VRRP グループは、指定したグループ ID で識別（グループ化）されます。グループ ID は、装置内で重複しないように指定してください。

プライオリティ

優先度指定または優先度固定（最優先）を選択します。

- **優先度指定**
優先度および仮想 IP アドレスを設定します。VRRP グループ内で 1 番プライオリティが高いグループメンバーがマスターとなります。プライオリティは数値が大きいほど高くなります。
優先度は、なるべくグループ内で差をつけるように設定してください。トリガを使用する場合は、優先度に 1 を指定しないでください。また、トリガを使用する場合は、“優先度固定（最優先）”を選択すると該当グループがバックアップ状態となったときに VRRP が設定された LAN が通信不能となるため、“優先度指定”を選択してください。
- **優先度固定（最優先）**
プライオリティが 255 である VRRP グループメンバーとして動作します。また、仮想 IP アドレスはこのインターフェースの IP アドレスとなります。

優先度

プライオリティの優先度指定を選択した場合に、1 ~ 254 の範囲で指定します。

仮想 IP アドレス

プライオリティの優先度指定を選択した場合に、VRRP グループ内では、同じ仮想 IP アドレスを指定します。VRRP グループ内に優先度固定（最優先）と設定された VRRP グループメンバーが存在する場合は、そのメンバーに設定されたインターフェースの IP アドレスを指定します。自装置のインターフェースに設定された IP アドレスを指定しないでください。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

fe80::1 ~ fe80::ffff:ffff:ffff:ffff

AD 送信間隔

マスターが送信する Advertisement パケットの送信間隔を 1 ~ 255 秒の範囲で指定します。VRRP グループ内では同じ値を使用します。本装置と VRRP を構成する他装置にも同じ値を指定します。省略時は、1 秒が設定されます。

プリエンプトモード

通常は “ON” を選択します。

“OFF” を選択した場合、自装置 VRRP グループメンバの優先度が高くても、マスターである他装置の VRRP グループメンバがすでに存在すると、マスターになることはできません。“OFF” を選択した場合は、ネットワークの状態が不安定で、マスターの交代が頻繁に発生する場合に有効です。移行禁止時間秒は、マスターより前にバックアップのシステムが立ち上がり、本来マスターになるべき VRRP グループに制御が移らないのを防ぎます。

移行禁止時間

システム立ち上がりからプリエンプトモード OFF 状態を抑止する時間です。0 ~ 900 秒の範囲で指定します。省略時は、0 秒が設定されます。

仮想 IP アドレスあて ICMP ECHO

仮想 IP アドレスあて ICMP ECHO パケットに応答する場合は、“応答する” を選択します。

“応答する” を選択した場合は、応答パケットの送信元 IP アドレスを設定します。

応答送信元 IP アドレス

“仮想 IP アドレス” または “インターフェースアドレス” のどちらかを選択します。

16.1.1.2.2 VRRP トリガ情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [VRRP グループ情報] → [修正] → [VRRP トリガ情報]

■VRRPトリガ情報

※追加・修正情報は一覧ので設定してください。

トリガ定義番号	トリガ種別	減算プライオリティ	インターフェース	あて先IPアドレス	操作
<input type="button" value="全削除"/>					
<VRRPトリガ情報入力フィールド>					
トリガ種別	減算プライオリティ	254	<input checked="" type="radio"/> インタフェースダウントリガ(ifdown) インタフェース <input type="button" value="すべて"/> <input type="radio"/> ルートダウントリガ(route) ネットワーク <input checked="" type="radio"/> IPv4デフォルトルート <input type="radio"/> IPv6デフォルトルート <input type="radio"/> 経路を指定する インタフェース <input type="button" value="指定なし"/> <input type="radio"/> ノードダウントリガ(node)		
	あて先IPアドレス	<input type="text"/>			
	送出インターフェース	<input type="button" value="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				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているVRRP トリガ情報の定義が表示されています。VRRP トリガの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定した条件が発生した場合に、該当するVRRP グループメンバの優先度を下げます。条件にあてはまるすべてのトリガに適用されます。このインターフェースに異常が発生しない限り、減算されるプライオリティの最小は1です。

減算プライオリティ

設定した条件が発生した場合、「VRRP グループ情報」の [基本情報] で設定したプライオリティを減算する値を1～254の範囲で指定します（プライオリティ 1より低い値までは減算されません）。省略時は、254が設定されます。

トリガ種別

トリガとなる種別を以下の3つから選択します。

- インタフェースダウントリガ (ifdown)
指定されたインターフェースがダウンした場合にトリガを適用します。有効ではないインターフェースは動作上、無視されます。
- ルートダウントリガ (route)
指定された経路情報が存在しない、または中継インターフェースが変化した場合にトリガを適用します。
- ノードダウントリガ (node)
設定したノードに対して ICMP ECHO パケットを送信します。応答がタイムアウトした場合にトリガを適用します。あて先 IP アドレスが IPv4 アドレスである場合、ICMP ECHO パケット送信元 IP アドレスは、VRRP が設定された LAN インタフェースの IPv4 アドレスとなります。応答を受信するための経路情報が正しくない場合は、不当に異常を検出することがあります。あて先 IP アドレスが IPv6 アドレスである場合は、プロトコルが選択した本装置 IPv6 アドレスが送信元 IP アドレスとなります。

インターフェース

トリガの対象となるインターフェースを選択します。

インターフェースダウントリガ (ifdown) を指定する場合

“すべて”を選択した場合は、すべての LAN インタフェースが対象です。

ルートダウントリガ (route) を指定する場合

“指定なし”を選択した場合は、経路情報が存在すればトリガは適用されません。それ以外では経路情報によるパケット送出インターフェースが設定と異なる、または経路情報が存在しない場合にトリガが適用されます。

ネットワーク

“IPv4 デフォルトルート”、“IPv6 デフォルトルート”または“経路を指定する”を選択します。

“経路を指定する”を選択した場合は、IPv4 アドレス／マスクビット形式または IPv6 アドレス／プレフィックス長形式で指定します。

IPv4 アドレスを指定する場合

あて先または中継先ネットワークの IPv4 アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に有効な記述形式を示します。

IPv4 アドレス／マスクビット数

(例: 192.168.1.0/24)

IPv4 アドレス／マスク値

(例: 192.168.1.0/255.255.255.0)

また、0.0.0.0/0 (0.0.0.0/0.0.0.0) を指定した場合は、IPv4 デフォルトルートとなります。

IPv6 アドレスを指定する場合

あて先または中継先ネットワークの IPv6 アドレスとプレフィックス長の組み合わせを指定します。

マルチキャストアドレスやリンクローカルアドレスは指定できません。また、::/0 以外の組み合わせでの:: やプレフィックス長 0 も指定できません。

::/0 を指定した場合は、IPv6 デフォルトルートとなります。

あて先 IP アドレス

ICMP ECHO パケットの送出先 IP アドレスを指定します。IP アドレスは、以下の範囲で指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fe80:: ~ fe80::ffff:ffff:ffff:ffff

送出インターフェース

ICMP ECHO パケットを送出するインターフェースを指定します。“指定なし”的場合は送出時の経路情報によって決定されます。

こんな事に気をつけて

あて先 IP アドレスに IPv6 リンクローカルアドレスを設定した場合は、その IPv6 リンクローカルアドレスのインターフェースを指定してください。

再送間隔

ICMP ECHO パケットの応答が受信されない場合に、再送する時間を 1～60 秒の範囲で指定します。送信から指定した再送間隔まで応答がない場合に、ICMP ECHO パケットを再送します。省略時は、5 秒が設定されます。

タイムアウト時間

ICMP ECHO パケットの再送を繰り返しても応答が受信されず、タイムアウトするまでの時間を、([再送間隔 +1]～240) 秒の範囲で指定します。タイムアウトによって、トリガが適用されます。省略時は、(再送間隔 ×3+1) 秒が設定されます。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する時間を、([タイムアウト時間 +1]～255) 秒の範囲で指定します。正常に受信されている状態での周期送信間隔です。省略時は、タイムアウト時間 +1 秒が設定されます。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの、周期送信する間隔を 1～255 秒の範囲で指定します。応答が受信された場合は、トリガを適用しないで正常状態に戻ります。省略時は、30 秒が設定されます。

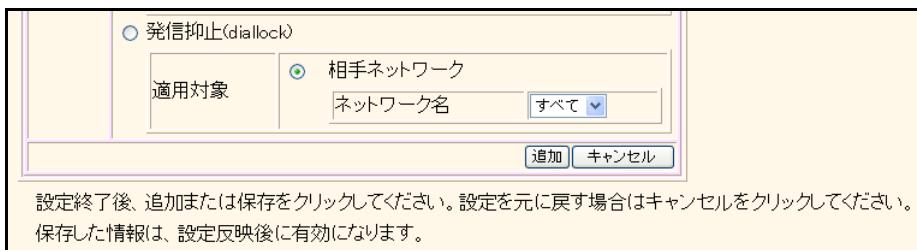
16.1.1.2.3 VRRP アクション情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [VRRP グループ情報] → [修正] → [VRRP アクション情報]

■VRRP アクション情報

※追加・修正情報は一覧の入力フィールドで設定してください。

定義番号	適用状態	動作	適用対象	操作
[全削除]				
<VRRP アクション情報入力フィールド>				
適用状態	<input checked="" type="radio"/> マスター(master) <input type="radio"/> バックアップおよびイニシャル(backup) <input checked="" type="radio"/> 接続/閉塞解除(online)			
	<input checked="" type="radio"/> スイッチ定義 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> スイッチポート ("ポート番号指定"を選択時のみ有効です。) </div> <input type="radio"/> LANインターフェース <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> インタフェース ("定義番号指定"を選択時のみ有効です。) </div> <input type="radio"/> 相手ネットワーク <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> ネットワーク接続先 ("定義番号指定"を選択時のみ有効です。) </div> <input type="radio"/> テンプレート定義 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> テンプレート名 テンプレート定義が存在しません ユーザID </div> <input type="radio"/> 切断/閉塞offline)			
動作	<input checked="" type="radio"/> スイッチ定義 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> スイッチポート ("ポート番号指定"を選択時のみ有効です。) </div> <input type="radio"/> LANインターフェース <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> インタフェース ("定義番号指定"を選択時のみ有効です。) </div> <input type="radio"/> 相手ネットワーク <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> ネットワーク接続先 ("定義番号指定"を選択時のみ有効です。) </div> <input type="radio"/> テンプレート定義 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> テンプレート名 テンプレート定義が存在しません ユーザID </div>			
	※接続ごとに認証ID、認証パスワードを変更する場合に設定します。			



現在、設定されている VRRP アクション情報の定義が表示されています。VRRP アクションの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

Si-R180B 以外では、“スイッチ定義”の設定項目は表示されません。

Si-R180B では、“着信抑止”的設定項目は表示されません。

適用状態

動作を適用する VRRP グループの状態を以下から選択します。

- マスター (master)
- バックアップおよびイニシャル (backup)

動作

アクションとなる種別を以下の 4 つから選択します。

- 接続/閉塞解除 (online)
適用状態に状態遷移した場合に対象を online にします。
- 切断/閉塞 (offline)
適用状態に状態遷移した場合に対象を offline にします。
- 発信抑止 (diallock)
適用状態の間、指定された相手ネットワークへの自動発信を抑止します。
- 着信抑止 (dialreject)
(Si-R220C、220D、240B、260B、370、370B、570、570B)
適用状態の間、指定された相手ネットワークからの自動着信を抑止します。

適用対象

アクションを適用する適用対象を選択します。

- スイッチ定義 (online、offline) (Si-R180B)
スイッチ定義を対象とする場合、選択します。
複数指定する場合は、”で区切って指定します。また、範囲指定する場合は、「2-4」のように “-” を使用して指定します。最大 5 組まで設定できます。
- LAN インタフェース (online、offline)
LAN インタフェースを対象とする場合、選択します。
複数指定する場合は、”で区切って指定します。ま

た、範囲指定する場合は、「2-4」のように “-” を使用して指定します。最大 5 組まで設定できます。

- 相手ネットワーク (online、offline)
ネットワーク名 接続先名を対象とする場合に選択します。複数指定する場合は、”で区切って指定します。また、範囲指定する場合は、「2-4」のように “-” を使用して指定します。相手定義番号、接続先定義番号それぞれ最大 5 組まで設定できます。
接続/閉塞解除 (online) の場合、接続時に接続先ごとに認証 ID および認証パスワードを変更する場合、ワンタイムパスワードを指定します。
 - 送信認証 ID
送信時に使用する認証 ID を 64 文字以内で指定します。
 - 送信認証パスワード
送信時に使用する認証パスワードを 64 文字以内で指定します。
- テンプレート定義 (online)
指定されたテンプレート定義で指定されたユーザ ID に接続する場合に選択します。ユーザ ID を 145 文字以内で指定します。
(有効範囲)
ユーザ名 (最大 64 文字) @ ドメイン名 (最大 80 文字)
- テンプレート定義 (offline)
指定されたテンプレート定義でテンプレート接続を切断する場合に選択します。ユーザ ID を 145 文字以内で指定します。ユーザ ID 省略時は、ユーザ ID を特定しないものとみなされます。
- 相手ネットワーク (diallock、dialreject)
発信抑止および着信抑止の対象となるネットワークを選択します。

16.1.1.3 LLDP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [追加] → [共通情報] → [LLDP 情報]

■LLDP情報

動作	<input checked="" type="radio"/> 送受信しない <input type="radio"/> 送受信する <input type="radio"/> 送信のみ <input type="radio"/> 受信のみ	
送信オプション情報	種別 情報名	
	IEEE802.1 情報	<input checked="" type="checkbox"/> ポート解説 (Port Description) <input checked="" type="checkbox"/> システム名 (System Name) <input checked="" type="checkbox"/> システム解説 (System Description) <input checked="" type="checkbox"/> システム機能 (System Capabilities) <input checked="" type="checkbox"/> 管理アドレス (Management Address) <input checked="" type="checkbox"/> ポートVLAN ID (Port VLAN ID) <input checked="" type="checkbox"/> プロトコルVLAN ID (Port And Protocol VLAN ID) <input checked="" type="checkbox"/> VLAN名 (VLAN Name) <input checked="" type="checkbox"/> プロトコルVLAN識別 (Protocol Identity)
	IEEE802.3 情報	<input checked="" type="checkbox"/> MAC/PHY定義/状態 (MAC/PHY Configuration/Status) <input checked="" type="checkbox"/> MDI給電 (Power Via MDI) <input checked="" type="checkbox"/> リンクアグリゲーション (Link Aggregation) <input checked="" type="checkbox"/> 最大フレーム長 (Maximum Frame Size)
送信VLAN情報	<input checked="" type="radio"/> すべて <input type="radio"/> VLAN ID 指定 _____	
受信情報更新通知	<input checked="" type="radio"/> しない <input type="radio"/> する	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

LLDP (Link Layer Discovery Protocol : 隣接探索プロトコル) のポートごとの設定を行います。

こんな事に気をつけて

LLDP 送信間隔時間などの装置全体に関する設定は、「設定メニュー」の「LLDP 情報」で行ってください。

動作

LLDP の動作を選択します。

- “送受信する”または“送信のみ”を選択した場合 本ポートに関する LLDP 情報を定期的に隣接装置に送信します。
- “送受信する”または“受信のみ”を選択した場合 隣接装置からの LLDP 情報を受信します。

受信した LLDP 情報は、LLDP 情報に含まれている有効時間が経過するまで保持します。

送信オプション情報

送信するオプション情報を選択します。

LLDP 情報には、常に送信する必須情報（装置識別、ポート識別、有効時間）と、送信するかどうかを選択できるオプション情報があります。

オプション情報をすべて送信しないようにしても、必須情報が常に送信されます。

送信する LLDP 情報は最大 1500 バイトに制限されるため、情報が 1500 バイトを超えるときは 1500 バイト以内に収まった情報だけを送信します。送信する情報が多いときは不要なオプション情報を送信しないように設定してください。

送信 VLAN 情報

送信オプション情報の“IEEE802.1 情報”で VLAN 情報を送信するように設定したとき、送信する VLAN 情報の VLAN ID を指定します。

- すべて
すべての VLAN の情報を送信します。
- VLAN ID 指定
送信する VLAN ID を 1～4094 の範囲の 10 進数で指定します。
VLAN ID を複数指定する場合は “,” で区切ります。
VLAN ID の範囲を指定する場合は “-” で区切ります。

受信情報更新通知

以下に示すような要因で LLDP 受信情報（隣接情報）が更新されたとき、SNMP トラップを送信して更新されたことを通知するかどうかを選択します。

- 新たな LLDP 情報を受信した
- 受信していた LLDP 情報の有効時間が経過して受信情報を破棄した
- 有効時間が 0 の LLDP 情報を受信して受信情報を破棄した
- LLDP 最大受信数を超えて LLDP 情報を受信したため受信情報を破棄した
- 「表示メニュー」 - 「LLDP 関連」 - 「隣接情報」の「隣接情報クリア」ボタンをクリックして受信情報を破棄した
- clear lldp neighbors コマンドを実行して受信情報を破棄した

こんな事に気をつけて

受信情報更新通知を“する”に設定した場合、「SNMP 情報」 - 「トランプ情報」の“lldpRemTablesChange”を“有効にする”に設定してください。

16.1.1.4 IEEE802.1X認証情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [追加] → [共通情報] → [IEEE802.1X認証情報]

認証動作モードで、“使用しない”を選択した場合

The screenshot shows a configuration dialog titled "IEEE802.1X認証情報". Under the "認証動作モード" section, the radio button for "使用しない" (Not used) is selected. Below the dialog, a note says: "設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。" At the bottom are "保存" (Save) and "キャンセル" (Cancel) buttons.

認証動作モードで、“使用する”を選択した場合

The screenshot shows a configuration dialog titled "IEEE802.1X認証情報". Under the "認証動作モード" section, the radio button for "使用する" (Used) is selected. The dialog includes fields for "認証方式" (Authentication method), "ポート認証制御" (Port authentication control), "認証失敗時再認証抑止時間" (Authentication failure when re-authentication is suppressed time), "認証開始送信間隔" (Authentication start transmission interval), "EAP応答待ち時間" (EAP response waiting time), "EAP再送回数" (EAP retransmission count), "再認証間隔" (Re-authentication interval), "参照するAAA情報" (AAA information to refer to), and "WOL転送モード" (WOL transfer mode). Below the dialog, a note says: "設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。" At the bottom are "保存" (Save) and "キャンセル" (Cancel) buttons.

認証動作モード

IEEE802.1X動作モードを選択します。

- 使用しない
IEEE802.1Xを使用しません。
- 使用する
IEEE802.1Xのオーセンティケータ動作を使用します。

こんな事に気をつけて

- IEEE802.1X認証を利用する場合は“IEEE802.1X認証情報”も設定してください。
- 同一LANインターフェースでMACアドレス認証機能との併用はできません。

認証方式

IEEE802.1X認証方式を選択します。“デフォルト”を選択した場合は、“IEEE802.1X認証機能定義”的設定を使用します。

こんな事に気をつけて

- 認証方式としてポートごとの認証を選択し、そのポートに接続される端末 (Supplicant) の一台が認証許容された場合、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。
- 同一LANインターフェースでMACアドレス認証を同時に有効とする場合は、認証方式が同じとなるように設定してください。

ポート認証制御

ポートの IEEE802.1X 認証状態を選択します。

- 自動
IEEE802.1X 認証機能によるポートアクセス制御機能を利用します。
- 認証拒否
常に認証が拒否されるポートとして利用します。
- 認証許容
常に認証成功となるポートとして利用します。

認証失敗時再認証抑止時間

認証が失敗したあと、認証を抑止する時間を 0 秒～600 秒の範囲で指定します。0 秒を指定した場合、認証に失敗した場合でも次の認証を抑止しません。省略時は、1 分が設定されます。

認証開始送信間隔

認証を開始するメッセージの送信間隔を 1 秒～600 秒の範囲で設定します。省略時は、30 秒が設定されます。

EAP 応答待ち時間

サブリカントからの応答を待ち合わせる時間を 1 秒～600 秒の範囲で指定します。省略時は、30 秒が設定されます。

EAP 再送回数

サブリカントからの応答が応答待ち時間内に受信できない場合に再送する回数を 1～10 の範囲で指定します。省略時は、2 回が設定されます。

再認証間隔

認証が成功したサブリカントを一定時間ごとに再認証するかについて指定します。再認証を行う場合、その間隔を 15 秒～18000 秒の範囲で指定します。省略時は、1 時間が設定されます。

参照する AAA 情報

IEEE802.1X 認証を行う場合に参照する AAA 情報のグループ ID を指定します。AAA のグループ ID を、10 未満の 10 進数で指定します。省略時は、0 が設定されます。

WOL 転送モード

WOL フレームの転送モードを指定します。端末の電源をリモートから制御する場合は “転送する” を選択します。

16.1.1.5 MACアドレス認証情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [MACアドレス認証情報]

The screenshot shows the 'MAC Address Authentication Information' configuration page. On the left, there's a sidebar labeled '認証機能' (Authentication Function) with two radio button options: '使用しない' (Not Used) and '使用する' (Used). The 'Used' option is selected. To its right, there are four input fields: '参照するAAA情報' (Reference AAA Information) with a dropdown menu, '認証成功保持時間' (Authentication Success Hold Time) set to 20 minutes, '認証失敗保持時間' (Authentication Failure Hold Time) set to 5 minutes, and '認証セキュリティ' (Authentication Security) with two radio button options: '高い' (High) and '通常' (Normal), where '高い' is selected. At the bottom, there are '保存' (Save) and 'キャンセル' (Cancel) buttons.

認証機能

MACアドレス認証を行うかどうかを選択します。

- 使用する
パケット送信元端末の MAC アドレス認証を行い、認められた MAC アドレスである場合に中継を行います。認められていなければパケット破棄します。
- 使用しない
MAC アドレス認証は行いません。

こんな事に気をつけて

MACアドレス認証を行うために、AAAユーザ情報、RADIUS情報を設定しておく必要があります。

認証セキュリティ

MACアドレス認証が正常に行えなかった場合（サーバ無応答、内部資源不足など）のセキュリティ動作について指定します。

- 高い パケット通過を遮断します。
- 通常 パケットを通過させます。

参考する AAA 情報

MACアドレス認証を行う場合に参考するAAAのグループIDを指定します。AAAのグループIDを、10未満の10進数で指定します。省略はできません。

認証成功保持時間

MACアドレス認証が成功した場合の保持時間を、60秒～86400秒の範囲で指定します。省略時は、20分が設定されます。

認証失敗保持時間

MACアドレス認証が失敗した場合の保持時間を、60秒～86400秒の範囲で指定します。省略時は、5分が設定されます。

16.1.1.6 ARP 認証関連

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [追加] → [共通情報] → [ARP 認証関連]

16.1.1.6.1 基本情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [追加] → [共通情報] → [ARP 認証関連] → [基本情報]
ARP 認証情報で、“使用しない”を選択した場合

ARP 認証情報で、“使用する”を選択した場合

ARP 認証情報

ARP パケットに対して、MAC アドレスの認証を行う場合は、“使用する”選択します。“使用する”を選択した場合は、ARP パケットに対して送信元端末の MAC アドレスの認証を行い、登録されていなければ syslog を表示します。

参照する AAA 情報

ARP 認証で使用する AAA 情報のグループ ID を指定します。AAA のグループ ID を、10 未満の 10 進数で指定します。省略はできません。

通信妨害

ARP 認証を行った結果、登録されていない MAC アドレスであった場合、その MAC アドレスに対して通信妨害を行うかどうかを選択します。

通信妨害を行う場合、通信妨害間隔を 0 秒および 10～43200 秒の範囲で指定します。省略時は、0 秒が設定されます。

ダミー MAC アドレス

通信妨害を行う場合に使用するダミーの MAC アドレスを指定します。省略時は、02:ff:ff:ff:ff:ff が設定されます。

こんな事に気をつけて

ネットワーク上に存在しない MAC アドレスを設定してください。存在する MAC アドレスを設定した場合、その MAC アドレスの装置が正常に通信できなくなります。

認証失敗保持時間

ARP 認証が失敗した場合の保持時間を、60～86400 秒の範囲で設定します。省略時は、20 分が設定されます。

端末数超過時動作

ARP 認証結果を保持可能な端末数を超えた場合の動作を選択します。

認証成功保持時間

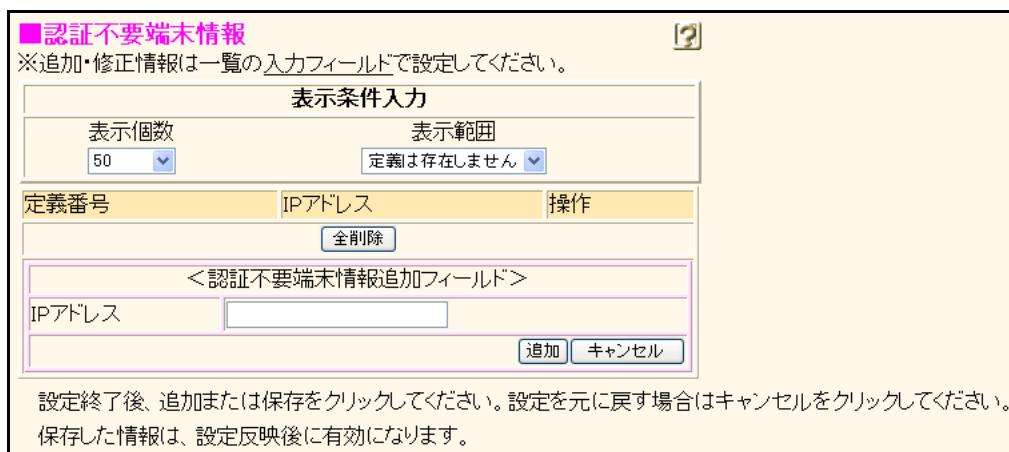
ARP 認証が成功した場合の保持時間を、60～86400 秒の範囲で設定します。省略時は、20 分が設定されます。

認証プロトコル

ARP 認証の認証プロトコルを設定します。

16.1.1.6.2 認証不要端末情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [追加] → [共通情報] → [ARP 認証関連]
→ [認証不要端末情報]



現在、設定されている認証不要端末情報の定義が表示されています。認証不要端末の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

IP アドレス

ARP パケットに対して、MAC アドレスの認証を行わないで通信を許可する端末の IP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

16.1.1.7 トラップ情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [共通情報] → [トラップ情報]

■トラップ情報	
linkDown	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
linkUp	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

トラップ情報

SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP 機能を利用しない場合、および旧バージョン互換 MIB モードで利用する場合は、この設定は意味を持ちません。

- linkDown
linkDown トラップを通知します。
- linkUp
linkUp トラップを通知します。

16.1.2 IP 関連

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連]

LAN0情報(物理LAN)			
共通情報	IP関連	IPv6関連	ブリッジ関連
IPアドレス情報	セカンダリIPアドレス情報		RIP情報
OSPF情報	スタティック経路情報		IPフィルタリング情報
IDS情報	TOS値書き換え情報		RIPフィルタリング情報
NAT情報	静的NAT情報		NATで先変換情報
帯域制御(WFO)情報	Ingressポリシールーティング情報		DHCP情報
ICMP情報	マルチキャスト情報		BGP/MPLS VPN情報
BGP/MPLS VPN	ARP情報		スタティックARP情報
スタティック経路情報			

16.1.2.1 IP アドレス情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [IP アドレス情報]

■IPアドレス情報

IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する
IPアドレス	IPアドレス: 192.168.1.1 ネットマスク: 2 (192.0.0.0) 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

※DHCPのサーバ機能使用時、IPアドレスを変更する場合は DHCP 機能の“割当て先頭アドレス”も確認してください。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

IPv4

IPv4 通信を行う場合は、“使用する”を選択します。

IP アドレス

このインターフェースのIPアドレス情報の取得方法を設定します。本装置をDHCPクライアントとして運用する場合は“DHCPで自動的に取得する”を選択します。IPアドレス、ネットマスク、ブロードキャストアドレスを指定する場合は“指定する”を選択します。

IP アドレス

本装置のIPアドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

こんな事に気をつけて

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

ネットマスク

本装置のネットマスクを指定します。

ブロードキャストアドレス

ブロードキャストアドレスを以下から選択します。通常は“ネットワークアドレス + オール1”を選択します。

- 0.0.0.0
- 255.255.255.255
- ネットワークアドレス + オール0
(ネットワークアドレスのホスト部をオール0にしたもの)
- ネットワークアドレス + オール1
(ネットワークアドレスのホスト部をオール1にしたもの)

16.1.2.2 セカンダリ IP アドレス情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [セカンダリ IP アドレス情報]

■セカンダリIPアドレス情報	
IPアドレス	<input type="text" value="192.0.0.0"/>
ネットマスク	255.255.255.254
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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

本装置は1つのインターフェースに複数のIPアドレスを持つことができます。複数のIPアドレスを使用する場合はここを指定します。

こんな事に気をつけて

セカンダリ IP アドレスの属するネットワークには、以下のサービスは行いません。

- RIP の送受信機能
- OSPF の送受信機能
- DHCP 機能

IP アドレス

セカンダリアドレスのIPアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

ネットマスク

セカンダリアドレスのネットマスクを指定します。

ブロードキャストアドレス

セカンダリアドレスのブロードキャストアドレスを以下から選択します。通常は“ネットワークアドレス + オール1”を選択します。

- 0.0.0.0
- 255.255.255.255
- ネットワークアドレス+オール0
(ネットワークアドレスのホスト部をオール0にしたもの)
- ネットワークアドレス+オール1
(ネットワークアドレスのホスト部をオール1にしたもの)

16.1.2.3 RIP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [RIP 情報]

RIP情報	
RIP送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input checked="" type="radio"/> 受信しない <input type="radio"/> V1で受信する <input type="radio"/> 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
《RIP V2使用時で認証パケットを破棄しない時はRIP V2のパスワードを設定してください。》	
認証パケット	<input type="radio"/> 破棄する <input checked="" type="radio"/> 破棄しない パスワード: <input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/>	<input type="button" value="キャンセル"/>

RIP を使用できるインターフェースの定義数は、仕様一覧 「2.3 システム最大値一覧」 (P.43) を参照してください。

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。

RIP 送信

RIP 情報を送信するかどうかを選択します。送信する設定にすると、RIP 情報を定期的に送信します。RIP 送信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、ブロードキャストで送信します。
- V2
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストで送信します。
- V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、マルチキャストで送信します。

RIP 受信

RIP 情報を受信するかどうかを選択します。RIP 受信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、受信します。
- V2、V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP 送信時に加算するメトリック値を選択します。

認証パケット

RIP V2 使用時にだけ有効な設定です。RIP V2 では、同じ パスワードグループでだけ RIP 情報の交換を行うことができます。パスワード認証による RIP 情報の交換を行う場合は、“破棄しない”を選択し、パスワードを 16 文字以内で指定します。“破棄する”を選択した場合は、パスワード認証による RIP 情報の交換は行いません。

16.1.2.4 OSPF 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [OSPF 情報]

■OSPF情報	
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 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
パケット再送間隔	5 秒
LSUパケット送信遅延時間	1 秒
認証方式	<input checked="" type="radio"/> 認証を行わない <input type="radio"/> テキスト認訂 鍵種別 <input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数 認証鍵 <input type="text"/> <input type="radio"/> MD5認訂 MD5認証鍵ID <input type="text"/> MD5認証鍵 <input type="text"/>
パケット送信	<input type="radio"/> 抑止する <input checked="" type="radio"/> 抑止しない
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

ループバックインターフェースも含めて、OSPF を使用できるインターフェースの定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P.43) を参照してください。

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 機能

OSPFを使用する場合は、“使用する”を選択します。

エリア定義番号

エリアの定義番号を 10 進数を使用して指定します。
OSPF エリア情報は、「ルーティングプロトコル情報」 – 「OSPF 関連」で設定することができます。省略時は、0 が設定されます。

出力コスト

OSPF 出力コストを 1 ~ 65535 の範囲で指定します。省略時は、10 が設定されます。

指定ルータ優先度

指定ルータおよび副指定ルータを決定するための優先度を 0 ~ 255 の範囲で指定します。値が大きいほど優先度は高くなります。省略時は、1 が設定されます。

こんな事に気をつけて

値が 0 の場合は、指定ルータおよび副指定ルータにはなりません。

Hello パケット送信間隔

OSPF 隣接関係の維持に使用する、Hello パケットの送信間隔を指定します。通常は、“10 秒”を指定します。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ Hello パケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Hello パケット送信間隔より大きな値を指定する必要があります。Hello パケット送信間隔の 4 倍を設定することをお薦めします。通常は “40 秒” を指定します。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を指定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
3 ~ 65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が “文字列” の場合は、8 文字以内で指定します。鍵種別が “16 進数” の場合は、16 進数を使用して 16 衔以内で指定します。16 衔未満の鍵を指定した場合、左詰めで設定され、残りは 16 衔になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

MD5 認証鍵 ID を 1 ~ 255 の範囲で指定します。

MD5 認証鍵

MD5 認証鍵を指定します。16 文字以内で指定します。

パケット送信

OSPF パケットの送信を抑止する場合は、" 抑止する " を選択します。

16.1.2.5 スタティック経路情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [スタティック経路情報]

■スタティック経路情報

※追加・修正情報は一覧ので設定してください。

操作	あて先IPアドレス/マスク	中継ルータアドレス	メトリック値	優先度	操作
<input type="button" value="全削除"/>					
<スタティック経路情報入力フィールド>					
ネットワーク	<input checked="" type="radio"/> デフォルトルート 中継ルータアドレス <input type="radio"/> DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 <input checked="" type="radio"/> 指定する <input type="text"/> IPアドレス				
	<input checked="" type="radio"/> ネットワーク指定 あて先IPアドレス <input type="text"/> あて先IPアドレス あて先アドレスマスク <input type="text"/> 0.0.0.0 中継ルータアドレス <input type="radio"/> DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 <input checked="" type="radio"/> 指定する <input type="text"/> IPアドレス				
メトリック値	<input type="text"/> 1				
優先度	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路情報の定義が表示されています。スタティック経路の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート

中継ルータアドレスを指定します。

- DHCPで取得する

受け取ったゲートウェイアドレスを中継ルータアドレスとして使用します。

- 指定する

中継ルータアドレスをIPアドレスで指定します。

- 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、中継ルータアドレスを指定します。

なお、あて先IPアドレスに0.0.0.0、あて先アドレスマスクに0 (0.0.0.0) を設定した場合、“デフォルトルート”を指定したものとして動作します。

優先度

スタティック経路情報の優先度を10進数で指定します。優先度は数値の小さい方がより高い優先度を示します。

- 中継ルータアドレスとして“指定する”を選択した場合
0～254の10進数で指定します。省略時は、0が指定されたものとみなされます。

- 中継ルータアドレスとして“DHCPで取得する”を選択した場合
1～254の10進数で指定します。省略時は、1が指定されたものとみなされます。

プロトコル	優先度
EBGP	20
OSPF	110
RIP	120
IBGP	200
DNS	15

複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じとなるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、「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」にあるECMP情報で、ECMPを使用するように設定します。ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
- 優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。

16.1.2.6 IP フィルタリング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [IP フィルタリング情報]

表示条件入力
表示定義内容
ACL対応定義

■IP フィルタリング情報 [ACL 定義参照](#)

※追加・修正情報は一覧ので設定してください。 [?](#)

優先順位	動作	方向	ACL定義番号	操作
			ACL定義名	
条件にあてはまらない場合の動作		透過		修正 初期化
全削除				

<IP フィルタリング情報入力フィールド>

動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
方向	入出力 ▼
ACL定義番号	参照

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IP フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IP フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下の2つ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入力パケットは、IPアドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とします。

ACL 定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

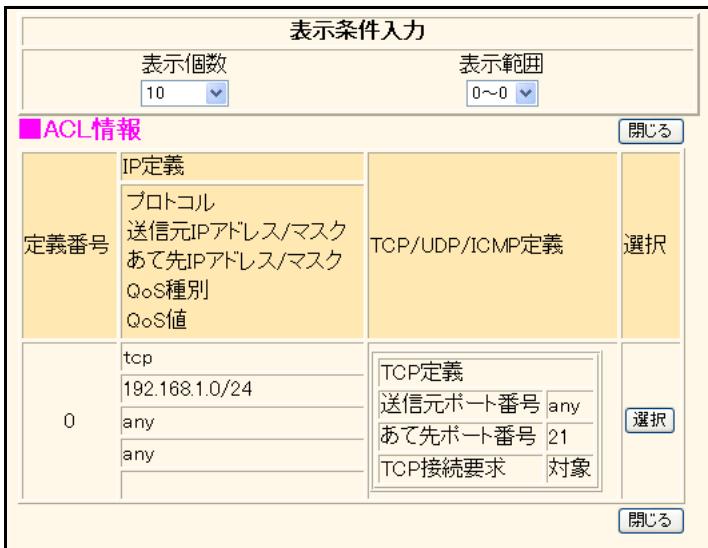
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の【選択】ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [IP フィルタリング情報]
 → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報を表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IP フィルタリング情報」の ACL 定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IP フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。「ACL 定義参照」ボタンをクリックした場合は、「選択」ボタンは表示されません。「閉じる」ボタンをクリックして、画面を閉じてください。

16.1.2.6.1 IP フィルタリング情報（旧定義）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [IP フィルタリング情報]
→ 「表示条件入力（旧定義）」

表示条件入力							
表示定義内容							
旧定義							
■IP フィルタリング情報							
※追加・修正情報は一覧の <input type="button" value="入力フィールド"/> で設定してください。							
優先順位	動作	プロトコル	送信元IPアドレス/マスク	TCP接続要求	TOS	方向	操作
			送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号 ICMPタイプ ICMPコード				
条件にあてはまらない場合の動作			透過	<input type="button" value="修正"/> <input type="button" value="初期化"/>			
<input type="button" value="全削除"/>							
<IP フィルタリング情報入力フィールド>							
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
プロトコル		すべて <input checked="" type="checkbox"/> 番号指定: <input type="text"/> “その他”を選択時のみ有効です					
送信元情報	IP アドレス	<input type="text"/>					
	アドレスマスク	<input type="text"/> 0.0.0.0					
	ポート番号	<input type="text"/>					
あて先情報	IP アドレス	<input type="text"/>					
	アドレスマスク	<input type="text"/> 0.0.0.0					
	ポート番号	<input type="text"/>					
ICMP	タイプ	<input type="text"/>					
	コード	<input type="text"/>					
TCP接続要求		<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外					
TOS		<input type="text"/>					
方向		<input type="button" value="入出力"/>					
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>							

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

表示条件入力に、“旧定義”を選択した場合に、IP フィルタリング情報の旧定義が表示されます。

動作

IP フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

フィルタリング条件としてのIP アドレスおよびアドレスマスクを指定します。チェック対象となったパケットのIP アドレスと定義したアドレスマスクの論理積と、定義したIP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は，“”で区切れます。範囲指定の場合は“-”で区切れます。送信元情報とあて先情報で合わせて10組まで指定できます。

ICMP

タイプ

フィルタリング条件としてICMPパケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPタイプ値を複数指定する場合は，“”で区切れます。範囲指定の場合は“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのICMPタイプ値がフィルタリングの対象になります。

コード

フィルタリング条件としてICMPパケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPコード値を複数指定する場合は，“”で区切れます。範囲指定の場合は“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのICMPコード値がフィルタリングの対象となります。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

TOS

フィルタリング条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は，“”で区切れます。範囲指定の場合は“-”で区切れます。10組まで指定できます。何も設定しない場合はすべてのTOSフィールド値をフィルタリングの対象とします。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下の2つ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
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とします。

入力パケットは、IPアドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。

16.1.2.6.2 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）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [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」[修正]

表示条件入力
表示定義内容
ACL 対応定義

■IP フィルタリング情報
ACL 定義参照

※追加・修正情報は一覧ので設定してください。

優先順位	動作	方向	ACL 定義番号	操作
			ACL 定義名	

<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	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 <input type="radio"/> SPI
情報保持タイム <input type="text" value="5"/> 分	

保存 キャンセル 一覧へ戻る
全削除

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている IP フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

こんな事に気をつけて

動作に遮断や SPI を指定し、IP フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IP フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPI セッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

16.1.2.7 IDS情報

[操作] ルータ設定「LAN情報（物理 LAN）」→ [修正] → [IP関連] → [IDS情報]

IDS機能 使用しない 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

IDS機能

侵入などのセキュリティに影響を与えるパケットを検知する場合は、“使用する”を選択します。

16.1.2.8 TOS値書き換え情報

[操作] ルータ設定「LAN情報（物理 LAN）」→ [修正] → [IP関連] → [TOS値書き換え情報]

表示条件入力			
表示定義内容 ACL対応定義			
TOS値書き換え情報 ACL定義参照			
※追加・修正情報は一覧の入力フィールドで設定してください。			
優先順位	ACL定義番号	新TOS	操作
ACL定義名			
全削除			
<TOS値書き換え情報入力フィールド>			
新TOS	<input type="text"/>		
ACL定義番号	<input type="text"/>	参照	
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているTOS値書き換え情報のACL定義が表示されています。処理は優先順位1から順に行われます。TOS値書き換えの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義されたTOS値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

新TOS

IPパケットに新しく指定するTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

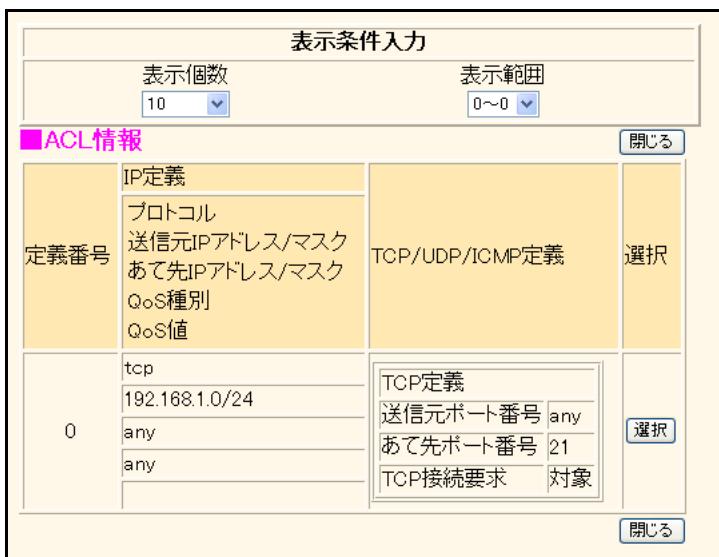
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [TOS 値書き換え情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「TOS 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「TOS 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.2.8.1 TOS 値書き換え情報（旧定義）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [TOS 値書き換え情報]
→ 「表示条件入力（旧定義）」

表示条件入力					
表示定義内容					
旧定義					
■TOS値書き換え情報					
※追加・修正情報は一覧の入力フィールドで設定してください。					
優先順位	プロトコル	送信元IPアドレス/マスク	TOS	操作	
		送信元ポート番号	新TOS		
あて先IPアドレス/マスク	あて先ポート番号				
全削除					
<TOS値書き換え情報入力フィールド>					
プロトコル すべて (番号指定: <input type="text"/> “その他”を選択時のみ有効です)					
送信元 情報	IPアレ ス	<input type="text"/>			
	アドレス マスク	<input type="text"/> 0 (0.0.0.0)			
	ポート番 号	<input type="text"/>			
あて先 情報	IPアレ ス	<input type="text"/>			
	アドレス マスク	<input type="text"/> 0 (0.0.0.0)			
	ポート番 号	<input type="text"/>			
TOS		<input type="text"/>			
新TOS		<input type="text"/>			
追加 キャンセル					
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。					

表示条件入力に、“旧定義”を選択した場合に、TOS 値書き換え情報の旧定義が表示されます。

プロトコル

TOS 値書き換えの条件としてプロトコルを以下の 6 つから選択します。（）内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255 の範囲で指定します。

送信元／あて先情報

TOS 値書き換え条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

TOS 値書き換え条件としての IP アドレスおよびアドレスマスクを指定します。

チェック対象となるパケットの IP アドレスと、定義する IP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定する場合は、すべてのポート番号が TOS 書き換えの対象となります。また、ポート番号を複数指定する場合は、 “,” で区切れます。範囲指定の場合は、 “-” で区切れます。送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0～ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、 “,” で区切れます。範囲指定の場合は、 “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値が書き換えの対象となります。

新 TOS

IP パケットに新しく指定する TOS フィールド値を 16 進数を使用して、0～ff の範囲で指定します。

16.1.2.9 RIP フィルタリング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [RIP フィルタリング情報]

■RIPフィルタリング情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<RIPフィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定				
	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致				
	IPアドレス	<input type="text"/>		アドレスマスク	<input type="text" value="0.0.0.0"/> ▼
メトリック値	<input type="text"/>				
追加 キャンセル					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

フィルタリング対象に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。
なお、IP アドレスに 0.0.0.0、アドレスマスクに 0 を指定した場合、デフォルトルートをフィルタリング対象とします。

方向

フィルタリング条件に該当するかチェックするタイミングを以下の 2 つから選択します。

- 受信
RIP パケット受信時に、フィルタリング条件に該当するかチェックします。
- 送信
RIP パケット送信時に、フィルタリング条件に該当するかチェックします。

検索条件

検索条件を選択します。

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、RIP経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更ができます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

16.1.2.10 NAT情報

[操作] ルータ設定「LAN情報（物理 LAN）」→ [修正] → [IP関連] → [NAT情報]

■NAT情報		
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 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	<input type="text"/>	
アドレス個数	1 個	
アドレス割当てタイム	5 分	
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い	
IPsecパスルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
アプリ対応	FTP	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	SIP	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	H.323	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	DNS	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	SNMP Trap	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	IRC	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	NTドメインログオン	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	各種ストリーミング	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
各種オンラインゲーム	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

NATの使用

“マルチNAT”を選択すると、複数の端末と併用できます。“静的NATのみ”を選択すると静的NAT情報の条件に一致しないパケットは変換されません。NATを使用しない場合は、以降の設定は無効です。

こんな事に気をつけて

本装置では「相手情報」、「LAN情報」および「テンプレート情報」の各インターフェースでアドレス変換機能を設定できます。ただし、使用する場合は、グローバルアドレスを使用するインターフェースだけで設定します。また、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。

グローバルアドレス

特定のグローバルアドレスを使用するときに指定します。指定しない場合は自動で割り当てられます。

アドレス個数

複数個のグローバルアドレスを使用する場合は、上述のグローバルアドレスを先頭とし連続した複数のアドレスを指定できます。その個数を1～16の範囲で指定します。なお、アドレス個数の設定はグローバルアドレスを指定した場合にだけ有効です。省略時は、1が設定されます。

アドレス割当てタイマ

アドレス変換情報は一定の時間、該当する通信が行われないと、自動的に解放されます。解放するための猶予時間を0～24時間の範囲で指定します。0を指定すると、タイマによる情報の解放は行われません。省略時は、5分が設定されます。

アプリ対応

使用するアプリケーションを選択し、それぞれに“有効”を設定します。

- FTP
- SIP
- H.323
- DNS
- SNMP Trap
- IRC
- NT ドメインログオン
- 各種ストリーミング
- 各種オンラインゲーム

NATセキュリティ

- 通常
相手サーバがNATを使用している際など、要求先とは別のアドレスから応答します。
- 高い
ftp や dns の要求する相手からの応答かどうかをチェックします。

IPsecパススルー

- 有効
相手ごとに1つのIPsecパスを接続することができます。
- 無効
IPsec クライアントがNAT トラバーサル機能を使用することができます。

こんな事に気をつけて

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 パスしか接続できません。

16.1.2.11 静的 NAT 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [静的 NAT 情報]

■静的NAT情報

※追加・修正情報は一覧ので設定してください。

プライベートアドレス	プライベートポート番号	プロトコル	操作
グローバルアドレス	グローバルポート番号		
条件にあてはまらない場合の動作		破棄	<input type="button" value="修正"/>
		<input type="button" value="初期化"/>	
<input type="button" value="全削除"/>			

<静的NAT情報入力フィールド>

プライベート IP 情報	IP アドレス	<input type="text"/>
ポート番号	すべて	(番号指定: <input type="text"/> "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	<input type="text"/>
ポート番号	すべて	(番号指定: <input type="text"/> "その他"を選択時の み有効です)
プロトコル	すべて	(番号指定: <input type="text"/> "その他"を選択 時のみ有効です)
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

NAT機能を使用すると、アドレス変換情報を固定で持つことができます。現在、設定されている固定のアドレス情報の定義が表示されています。静的NATの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

プライベート IP 情報

IP アドレス

固定でアドレス変換を行う場合にローカルネットワーク側のIPアドレスを指定します。省略はできません。

ポート番号

固定でアドレス変換を行う場合にローカルネットワーク側のポート番号を選択します。“その他”を選択し、ポート番号を指定する場合は、10進数を使用して1～65535の範囲で指定します。

なお、グローバルポート番号を範囲指定した場合、その範囲のグローバルポート番号は指定したプライベートポート番号を先頭とした範囲に変換されます。

例) プライベートポート番号: 1000

グローバルポート番号: 10000-11000

NAT変換後

プライベートポート番号: 1000-2000

グローバル IP 情報

IP アドレス

固定でアドレス変換を行う場合にリモートネットワーク側のIPアドレスを指定します。省略時は、先頭のグローバルアドレスに対して有効な指定となります。

IPアドレスを指定する場合は、“-”で区切った1組の範囲を指定します。

ポート番号

固定でアドレス変換を行う場合にリモートネットワーク側のポート番号を選択します。“その他”を選択し、ポート番号を指定する場合は、10進数を使用して1～65535の範囲から1つ、または“-”で区切った1組の範囲を指定します。

プロトコル

固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- esp (50)
- ah (51)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

16.1.2.11.1 静的NAT情報（条件にあてはまらない場合の動作）

[操作] ルータ設定「LAN情報（物理LAN）」→ [修正] → [IP関連] → [静的NAT情報]
→ 「条件にあてはまらない場合の動作」[修正]

■静的NAT情報

※追加・修正情報は一覧の入力フィールドで設定してください。

プライベートアドレス	プライベートポート番号	プロトコル	操作
グローバルアドレス	グローバルポート番号		

<静的NAT情報入力フィールド(条件にあてはまらない場合)>

動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 破棄
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>	
<input type="button" value="全削除"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている静的NAT定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。

動作

静的NAT定義のどれにも一致しない場合のIPフィルタリングの動作を以下の2つから選択します。

- 透過
静的NAT定義のどれにも一致しない場合にパケットを透過します。
- 破棄
静的NAT定義のどれにも一致しない場合にパケットを破棄します。

16.1.2.12 NAT あて先変換情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [NAT あて先変換情報]

■NAT あて先変換情報

※追加・修正情報は一覧の入力フィールドで設定してください。

プライベートアドレス	グローバルアドレス	操作
全削除		
<NAT あて先変換情報入力フィールド>		
プライベートアドレス	<input type="text"/>	
グローバルアドレス	<input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている NAT あて先変換情報の定義が表示されています。NAT あて先変換の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プライベートアドレス

ローカルネットワーク側の IP アドレスを指定します。

なお、グローバルアドレスを範囲指定した場合、その範囲のグローバルアドレスはここで指定したアドレスを先頭とした範囲に変換されます。

例) プライベートアドレス : 192.168.1.100

グローバルアドレス : 172.16.1.100-172.16.1.200

NAT あて先変換後

プライベートアドレス : 192.168.1.100-192.168.1.200

グローバルアドレス

リモートネットワーク側の IP アドレスを指定します。範囲指定する場合は、"-" で区切れます。範囲指定した場合、プライベートアドレスも自動的に範囲指定されます。

16.1.2.13 帯域制御 (WFQ) 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [帯域制御 (WFQ) 情報]

定義番号	ACL 定義番号	帯域	操作
	ACL 定義名		
	<input checked="" type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/>		
ACL 定義番号	<input type="button" value="参照"/>		<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報の ACL 定義が表示されています。帯域制御の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

表示条件入力は、“ACL 対応定義”または“旧定義”から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を 10 進数を使用して、1～99 の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが 100 を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbps または 1～100Mbps の範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

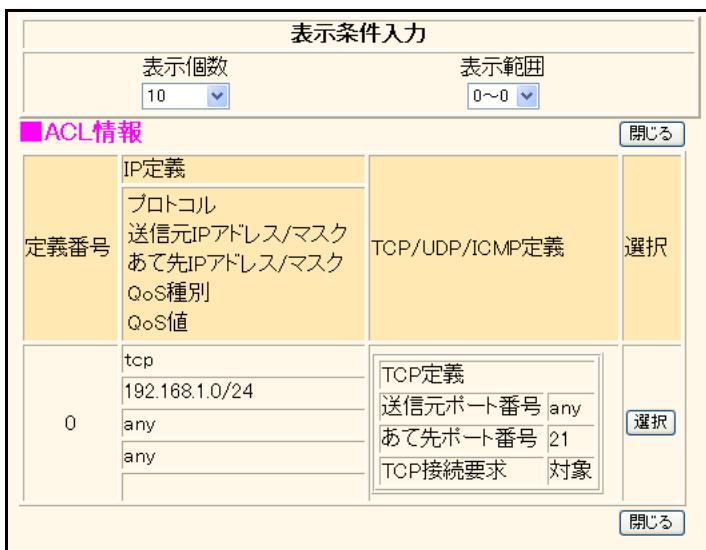
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [帯域制御 (WFQ) 情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「帯域制御 (WFQ) 情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「帯域制御 (WFQ) 情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.2.13.1 帯域制御 (WFQ) 情報 (旧定義)

[操作] ルータ設定「LAN 情報 (物理 LAN)」→ [修正] → [IP 関連] → [帯域制御 (WFQ) 情報]
→ 「表示条件入力 (旧定義)」

表示条件入力			
表示定義内容			
旧定義			
■帯域制御(WFQ)情報			
※追加・修正情報は一覧の入力フィールドで設定してください。			
定義番号	プロトコル	送信元IPアドレス／マスク	対象TOSフィールド値
		送信元ポート番号	操作
		あて先IPアドレス／マスク	帯域
		あて先ポート番号	
全削除			
<帯域制御(WFQ)情報入力フィールド>			
プロトコル		すべて (番号指定: <input type="text"/> "その他"を選択時のみ有効です)	
送信元情報	IPアドレス	<input type="text"/>	
	アドレスマスク	0 (0.0.0.0) <input type="button" value="▼"/>	
	ポート番号	<input type="text"/>	
あて先情報	IPアドレス	<input type="text"/>	
	アドレスマスク	0 (0.0.0.0) <input type="button" value="▼"/>	
	ポート番号	<input type="text"/>	
対象TOSフィールド値		<input type="text"/>	
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="button" value="▼"/> <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません <input type="button" value="▼"/>	
[追加] [キャンセル]			
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。			

表示条件入力に、“旧定義”を選択した場合に、帯域制御 (WFQ) 情報の旧定義が表示されます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IP アドレス／アドレスマスク

帯域制御の対象となる IP アドレスおよびアドレスマスクを指定します。対象となるパケットの IP アドレスと定義するアドレスマスクの論理積と、定義する IP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、”,”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 TOS フィールド値

帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのTOSフィールド値が帯域制御の対象となります。

帯域

帯域の使用率または帯域値を指定します。

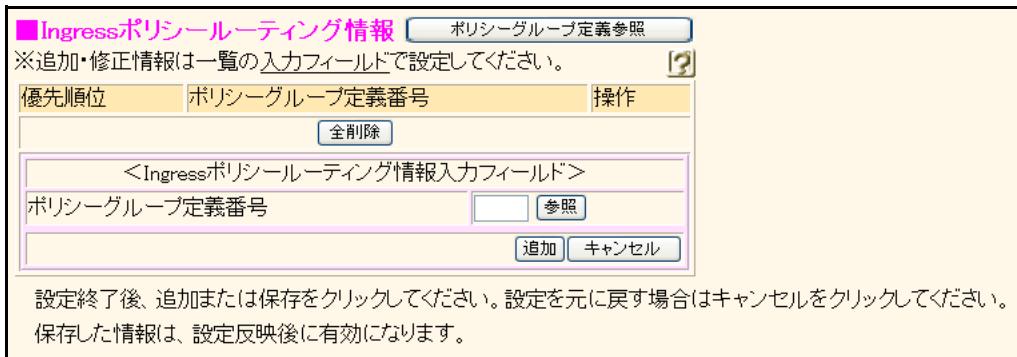
- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

16.1.2.14 Ingress ポリシールーティング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [Ingress ポリシールーティング情報]



現在、設定されている Ingress ポリシールーティング情報の定義が表示されています。処理は優先順位 1 から順に行われます。Ingress ポリシールーティング情報の定義数は、仕様一覧 「2.3 システム最大値一覧」 (P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に、指定されたポリシーグループに定義された送出先へパケットを送出します。

ポリシーグループ定義番号

[参照] ボタンをクリックして、ポリシーグループ定義番号を指定します。

別の画面に「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されます。指定する定義番号欄の [選択] ボタンをクリックし、ポリシーグループ定義番号を設定します。自動的に画面が閉じます。

なお、参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [Ingress ポリシールーティング情報] → 「ポリシーグループ定義番号の [参照]」



「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ポリシーグループ定義情報の一覧に見たい情報だけを表示させることができます。

参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「Ingress ポリシールーティング情報」のポリシーグループ定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「Ingress ポリシールーティング情報」にポリシーグループ定義番号が設定され、画面が閉じます。[ポリシーグループ定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.2.15 DHCP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [DHCP 情報]

DHCP機能

⚠ DHCPクライアントで運用する場合、設定はIPアドレス情報で行ってください。

DHCP情報

<input checked="" type="radio"/> 使用しない <input type="radio"/> リレー機能を使用する	<div style="border-bottom: 1px solid black; padding-bottom: 5px;">DHCPサーバIPアドレス1</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">DHCPサーバIPアドレス2</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">MACアドレスチェック</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">割当て先頭IPアドレス</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">割当て адрес数</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">リース期間</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">デフォルトルータ広報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">DNSサーバ広報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">TIMEサーバ広報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">NTPサーバ広報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">WINSサーバ広報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">SIPサーバ広報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">MACアドレスチェック</div>
	<input type="checkbox"/> ホストデータベース <input type="checkbox"/> AAA <div style="border-bottom: 1px solid black; padding-bottom: 5px;">参照するAAA情報</div> <div style="border-bottom: 1px solid black; padding-bottom: 5px;">認証プロトコル</div>
	<input type="radio"/> CHAP <input checked="" type="radio"/> PAP

※“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。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

DHCP 機能

それぞれのインターフェースの DHCP 機能を以下の 3つから選択します。

- 使用しない
DHCP 機能を使用しません。
- リレー機能を使用する
ほかのネットワークの DHCP サーバを、このネットワークの DHCP サーバとして使用し、利用する DHCP サーバの IP アドレスを指定します。
該当インターフェースを DHCP クライアントとして運用する場合は、IP アドレス情報の設定で “DHCP で自動的に取得する” を選択します。
- サーバ機能を使用する
本装置を該当インターフェースのネットワークの DHCP サーバとして使用します。

割当て先頭 IP アドレス

DHCP サーバ機能によって、割り当てる連続したアドレス群の先頭の IP アドレスを指定します。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

割当てアドレス数

DHCP サーバ機能で割り当てるアドレス数を 1～253 の範囲で指定します。省略時は、32 が設定されます。ホストデータベース機能を使用すると、特定の DHCP クライアントに対して固有の IP アドレスを割り当てるることができます。この場合の IP アドレスは、割当て先頭 IP アドレスと割当てアドレス数によって規定される動的割り当て範囲である必要はありません。

リース期間

DHCP サーバ機能によって割り当てた IP アドレスを貸し出す期間を、1 時間以上、365 日未満の範囲で指定します。0 を指定した場合は、無期限が設定されます。省略時は、1 日が設定されます。

デフォルトルータ広報

DHCP サーバで広報するデフォルトルータの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

DNS サーバ広報

DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。ProxyDNS を使用する場合は、本装置の IP アドレスを指定します。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

セカンダリ DNS サーバ広報

セカンダリ DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定すると DHCP サーバによる広報は行いません。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

ドメイン名広報

ドメイン名を 80 文字以内で指定します。省略時は、DHCP サーバによる広報は行いません。

TIME サーバ広報

TIME サーバの IP アドレスを設定します。省略するか 0.0.0.0 を設定すると DHCP サーバによる広報は行いません。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

NTP サーバ広報

NTP サーバの IP アドレスを設定します。省略するか 0.0.0.0 を設定すると DHCP サーバによる広報は行いません。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

WINS サーバ広報

WINS サーバの IP アドレスを指定します。プライマリ／セカンダリサーバ共に省略すると DHCP サーバによる広報は行いません。

有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

SIP サーバ広報

ドメイン名を使用して SIP サーバを広報する場合は、記述形式の “ドメイン名” を選択して 80 文字以内で指定します。なお、RFC1034 では英数字、“-”（ハイフン）、”.”（ピリオド）でドメイン名をつけることを推奨しています。また、IP アドレスを使用して SIP サーバを広報する場合は、記述形式の “IP アドレス” を選択して IP アドレスを指定します。ドメイン名と IP アドレスの混在指定はできません。プライマリ／セカンダリサーバ共に省略すると DHCP サーバによる広報を行いません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

MAC アドレスチェック

DHCP サーバおよび DHCP リレーエージェント機能を使用する際、DHCP クライアントの MAC アドレスチェックを行うかどうかを選択します。DHCP の要求の受付を許可する MAC アドレスの登録には、ホストデータベース情報および AAA 情報が使用できます。

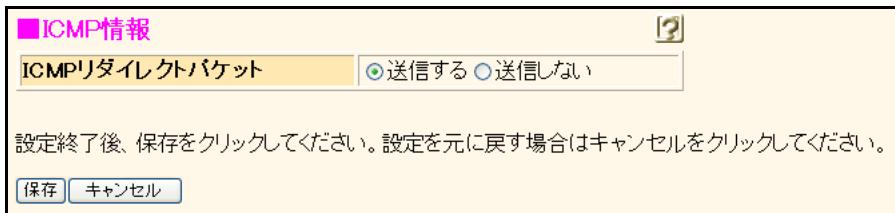
- ホストデータベース
ホストデータベース情報を使用します。
- AAA
AAA 情報を使用します。
参照する AAA 情報のグループ ID を 10 未満の 10 進数で指定します。
認証プロトコルを CHAP と PAP から選択します。

こんな事に気をつけて

MAC アドレスチェック機能を使用する場合、必要に応じて、ホストデータベース情報、AAA ユーザ情報、RADIUS 情報を設定してください。ホストデータベース情報と AAA 情報の両方を使用する場合、ホストデータベース情報が優先されます。

16.1.2.16 ICMP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」 → [修正] → [IP 関連] → [ICMP 情報]



ICMP リダイレクトパケット

ICMP リダイレクトパケットを送信する場合は、“送信する”を選択します。

16.1.2.17 マルチキャスト情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [マルチキャスト情報]

■マルチキャスト情報	
マルチキャスト機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> static <input type="radio"/> PIM-DM <input type="radio"/> PIM-SM
TTLしきい値	1
PIMプリファレンス値	1024
上流ルータの種類	<input checked="" type="radio"/> PIMルータのみ <input type="radio"/> すべて

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

マルチキャストを使用できるインターフェースの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。

マルチキャスト機能

LAN 上でマルチキャスト機能を使用する場合は、マルチキャスト・プロトコルを選択します。

こんな事に気をつけて

- マルチキャスト機能を使用するすべてのインターフェース上で、同じプロトコルを選択してください。同時に複数のプロトコルを使用することはできません。
- NAT 機能と併用することはできません。

PIM プリファレンス値

PIM の Assert メッセージに格納されるプリファレンス値を 10 進数を使用して 1 ~ 65535 の範囲で指定します。初期値は 1024 です。

並列な経路の存在のためにマルチキャスト・パケットが重複した場合は、PIM Assert メッセージによって、片側の転送経路が遮断されます。この際、プリファレンス値の小さい方の経路が有効になります。PIM Assert メッセージの発行時には、Assert 対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインターフェースのプリファレンス値を Assert メッセージに格納します。Assert メッセージが出力されるインターフェースのプリファレンス値が格納されるわけではありません。

TTL しきい値

LAN 上でマルチキャスト機能を使用するときの TTL しきい値を 10 進数を使用して 1 ~ 255 の範囲で指定します。初期値は 1 です。

PIM-SM の PIM Register パケットによりカプセル化されるマルチキャスト・パケットは、出力先インターフェースの TTL しきい値の設定にかかわらず出力されます。

上流ルータの種類

本装置より上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送される場合、どの種類のルータからのマルチキャストパケット転送を許可するかを指定します。

上流ルータが PIM ルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“すべて”を選択します。

こんな事に気をつけて

受信インターフェースと同一の IP セグメントから送信された（直接接続されたホストからの）マルチキャストパケットは、上流ルータの設定にかかわらず転送が行われます。

16.1.2.18 BGP/MPLS VPN 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [BGP/MPLS VPN 情報]

■BGP/MPLS VPN 情報	
BGP/MPLS VPN機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
VRF定義番号	0

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

BGP/MPLS VPN 機能

BGP/MPLS VPN を利用する場合は、“使用する”を選択します。

こんな事に気をつけて

- BGP/MPLS VPN で使用できる IBGP は 1 セッションだけです。
- IP-VPN 接続と併用することはできません。

VRF 定義番号

BGP/MPLS VPN 機能を利用する場合は、VRF を定義する必要があります。VRF の定義番号を 10 進数を使用して指定します。VRF 情報は「ルーティングプロトコル情報」 – [BGP 関連] – 「VRF 情報」で設定します。

こんな事に気をつけて

- BGP/MPLS VPN で構成された VPN ネットワーク内では EBGP/OSPF/RIP は使用できません。

16.1.2.19 BGP/MPLS VPN スタティック経路情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連]
 → [BGP/MPLS VPN スタティック経路情報]

■BGP/MPLS VPN スタティック経路情報

※追加・修正情報は一覧ので設定してください。

定義番号	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	操作
<input type="button" value="全削除"/>				

<BGP/MPLS VPN スタティック経路情報入力フィールド>

ネットワーク	<input checked="" type="radio"/> デフォルトルート	中継ルータアドレス	<input type="text"/>
	<input checked="" type="radio"/> ネットワーク指定	あて先IPアドレス	<input type="text"/>
	あて先アドレスマスク	<input type="text"/> 0.0.0.0	<input type="button" value="▼"/>
	中継ルータアドレス	<input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている BGP/MPLS VPN スタティック経路情報の定義が表示されています。スタティック経路の定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。ただし、デフォルトルートおよび同じ「あて先 IP アドレス」はインターフェースごとに 1 つだけ設定できます。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

- BGP/MPLS VPN スタティック経路情報で優先度は設定できません。優先度は 1 となります。
- デフォルトルートおよび同じ「あて先 IP アドレス」はインターフェースごとに 1 つだけ設定できます。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- 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、中継ルータアドレスを指定します。

16.1.2.20 ARP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [ARP 情報]

■ ARP 情報	
ARP定期送信機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 送信間隔 <input type="text"/> 分 ▾
Proxy ARP機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
ローカル Proxy ARP機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

ARP 定期送信機能

ARP を定期的に送信する機能です。ARP 定期送信機能を使用する場合は、“使用する”を選択し、送信間隔を設定します。

送信間隔

10進数を使用して、10～1200秒の範囲で指定します。

Proxy ARP 機能

本装置を経由して到達できる IPv4 アドレスに対する ARP 要求に対し代理応答する機能です。代理応答させない場合は“使用しない”を選択します。

ローカル Proxy ARP 機能

ARP 要求を受信したインターフェースの IPv4 ネットワーク範囲すべての要求に対し、代理応答する機能です。この機能は、端末間の直接通信が意図的に禁止されているネットワークでだけ使用してください。

16.1.2.21 スタティック ARP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IP 関連] → [スタティック ARP 情報]

■スタティックARP情報

※追加・修正情報は一覧ので設定してください。

定義番号	あて先IPアドレス	MACアドレス	操作
<input type="button" value="全削除"/>			
<スタティックARP情報入力フィールド>			
あて先IPアドレス	<input type="text"/>		<input type="button" value="追加"/>
MACアドレス	<input type="text"/>		<input type="button" value="キャンセル"/>
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。			

現在、設定されているスタティック ARP 情報の定義が表示されています。スタティック ARP の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

同じあて先へのスタティック ARP 情報を複数設定することはできません。

あて先 IP アドレス

スタティック ARP テーブルに登録するあて先 IP アドレスを指定します。

MAC アドレス

あて先 IP アドレスへパケットを送信する場合に使用する MAC アドレスを指定します。

16.1.3 IPv6 関連

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連]

LAN0情報(物理LAN)					
共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連	
IPv6基本情報	IPv6 RIP情報	IPv6 OSPF情報			
IPv6スティック経路情報	IPv6フィルタリング情報	IPv6 Traffic Class書き換え情報			
IPv6 RIPフィルタリング情報	IPv6帯域制御(WFO)情報	IPv6 Ingressポリシールーティング情報			
IPv6 DHCP情報					

16.1.3.1 IPv6 基本情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 基本情報]

■ IPv6基本情報	
IPv6 アド レス	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する インタフェースID <input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
	<input checked="" type="radio"/> ユニキャストアドレスを指定する <input type="text"/> アドレスまたはプレフィックス Valid Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 30 日 <input type="button" value="▼"/> Pref. Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 7 日 <input type="button" value="▼"/> フラグ <input type="text"/> c0
	<input type="radio"/> エニキャストアドレスを指定する <input type="text"/> アドレス
	<input checked="" type="radio"/> ユニキャストアドレスを指定する <input type="text"/> アドレスまたはプレフィックス Valid Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 30 日 <input type="button" value="▼"/> Pref. Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 7 日 <input type="button" value="▼"/> フラグ <input type="text"/> c0
	<input type="radio"/> エニキャストアドレスを指定する <input type="text"/> アドレス
	<input checked="" type="radio"/> ユニキャストアドレスを指定する <input type="text"/> アドレスまたはプレフィックス Valid Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 30 日 <input type="button" value="▼"/> Pref. Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 7 日 <input type="button" value="▼"/> フラグ <input type="text"/> c0

ルータ広報	<input type="radio"/> エニキャストアドレスを指定する	アドレス	<input type="text"/>
	<input checked="" type="radio"/> ユニキャストアドレスを指定する	アドレスまたはプレフィックス	<input type="text"/>
	Valid Lifetime	<input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 30 日 <input type="button" value="▼"/>	
	Pref. Lifetime	<input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 7 日 <input type="button" value="▼"/>	
フラグ	<input type="text"/> c0		
<input type="radio"/> エニキャストアドレスを指定する	アドレス	<input type="text"/>	
<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	最大送信間隔 <input type="text"/> 600 秒 最小送信間隔 <input type="text"/> 200 秒 Router Lifetime <input type="text"/> 1800 秒 MTU <input type="text"/> Reachable Time <input type="text"/> 0 ミリ秒 Retrans Timer <input type="text"/> 0 ミリ秒 Cur Hop Limit <input type="text"/> 64 フラグ <input type="text"/> 00		

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IPv6

IPv6通信を行う場合は、“使用する”を選択します。

インターフェース ID

インターフェース ID を設定します。

- 自動
装置のMACアドレスから自動生成されるインターフェースIDを使用します。通常は、“自動”を選択します。
- 指定する
16ビットごとに区切り文字 (:) を入れて、16進数を使用して16桁でインターフェースIDを指定します。このとき、他装置と同じインターフェースIDとならないような値を指定します。
記述例) 2001:db8:7654:3210

IPv6 アドレス

この装置で使用するユニキャストアドレスまたはエニキャストアドレスを4個まで設定できます。

- ユニキャストアドレスを指定する
ユニキャストアドレスを指定する場合に選択します。
- エニキャストアドレスを指定する
エニキャストアドレスを指定する場合に選択します。

アドレスまたはプレフィックス

本装置の LAN 側の IPv6 アドレスを標準的な IPv6 アドレス表記方式で指定します。本装置ではプレフィックス長は 64 に固定されます。インターフェース ID 部分がすべて 0 の場合、指定したアドレスはプレフィックスとして解釈され、実際に利用するアドレスはそのアドレスにインターフェース ID を付与したものとなります。リンクローカルアドレスは指定できません。

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場合は、上位を “dhcp@インターフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作している rmt インタフェースを指定します。

記述例)

2001:db8:1111:1000:1:2:3:4

完全な IPv6 アドレスとして解釈されます。

2001:db8:1111:1000::

プレフィックスとして解釈され、インターフェース ID 部分にはインターフェース ID が付与されます。

dhcp@rmt0:1000::1

rmt0 インタフェースで動作している IPv6 DHCP クライアントが取得したプレフィックスを使用して完全な IPv6 アドレスを指定します。

dhcp@rmt0:1000::

rmt0 インタフェースで動作している IPv6 DHCP クライアントが取得したプレフィックスを使用してプレフィックスを指定します。

Valid Lifetime

ルータ広報のプレフィックス情報ごとに設定する Valid Lifetime を指定します。通常は、“30 日” を指定します。

有効範囲)

0 ~ 365 日

0 ~ 8760 時間

0 ~ 525600 分

0 ~ 31536000 秒

IPv6 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指定をした場合は、IPv6 DHCP クライアントが取得した Valid Lifetime と比較して短い方が有効になります。

Pref. Lifetime

ルータ広報のプレフィックス情報ごとに設定する Preferred Lifetime を指定します。通常は、“7 日” を指定します。

有効範囲)

0 ~ 365 日

0 ~ 8760 時間

0 ~ 525600 分

0 ~ 31536000 秒

IPv6 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指定をした場合は、IPv6 DHCP クライアントが取得した Preferred Lifetime と比較して短い方が有効になります。

フラグ

ルータ広報のプレフィックス情報ごとに設定する フラグフィールドの内容を 16 進数を使用して 2 衔で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。

- on-link flag 80
- autonomous address-configuration flag 40

通常は “c0” を指定します。

アドレス

本装置のエニキャストアドレスを標準的な IPv6 アドレス表記方式で指定します。本装置ではプレフィックス長は 128 に固定されます。インターフェース ID によるアドレス生成は行われません。

ルータ広報

ルータ広報メッセージ (router advertisement message) を送信する場合は “送信する” を選択し、以下の項目を設定します。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。初期値は 600 秒です。省略はできません。

有効範囲) 4 ~ 1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。初期値は 200 秒です。省略はできません。

有効範囲) 3 ~ 最大送信間隔の 3 / 4

Router Lifetime

ルータ広報で送信する Router Lifetime を指定します。初期値は 1800 秒です。省略はできません。

有効範囲) 0 または最大送信間隔～9000

MTU

ルータ広報で送信する MTU option を指定します。省略時は、MTU option を含みません。

有効範囲) 1280～1500

Reachable Time

ルータ広報で送信する Reachable Time を指定します。省略値は 0 ミリ秒です。

有効範囲) 0～3600000

Retrans Timer

ルータ広報で送信する Retrans Timer を指定します。省略値は 0 ミリ秒です。

有効範囲) 0～4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit を指定します。省略値は 64 です。

有効範囲) 0～255

フラグ

ルータ広報の本体部分に設定する フラグフィールド の内容を 16進数を使用して 2 行で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。省略値は 00 です。

- Managed address configuration flag 80
- Other stateful configuration flag 40

16.1.3.2 IPv6 RIP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 RIP 情報]

■IPv6 RIP情報

RIP送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する メトリック値 <input type="text" value="0"/>	
RIP受信	<input checked="" type="radio"/> 受信しない <input type="radio"/> 受信する	
集約経路	破棄経路 設定	
集約経路送信	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定	<input checked="" type="checkbox"/> 設定する <input checked="" type="checkbox"/> 設定する <input checked="" type="checkbox"/> 設定する <input checked="" type="checkbox"/> 設定する
サイトローカルプレフィックス	<input type="radio"/> 交換しない <input checked="" type="radio"/> 交換する	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

RIP を使用できるインターフェースの定義数は、仕様一覧 「2.3 システム最大値一覧」 (P43) を参照してください。

RIP 送信

RIP を送信する場合は、“送信する”を選択します。

メトリック値

“送信する”を選択した場合に、加算するメトリック値を選択します。

RIP 受信

RIP を受信する場合は、“受信する”を選択します。

集約経路送信

RIP で集約経路を送信する場合に、集約して広報する経路を設定します。

集約経路

デフォルトルートまたはネットワーク指定を選択し、集約して広報する経路を指定します。

集約経路情報は、集約される経路情報がないときでも広報されます。また、同じあと先の経路情報がルーティングテーブルにないときでも広報され、ルーティングテーブルには設定されません。

- デフォルトルート
集約経路情報としてデフォルトルートだけを広報します。
- ネットワーク指定
集約経路情報をプレフィックス／プレフィックス長で指定します。指定した集約経路情報は広報され、集約経路情報に含まれる経路情報は広報されません。

破棄経路設定

広報した集約経路情報により本装置に送られた IP パケットをルーティングするための経路情報がないときに、そのあと先へは到達不能であることを ICMPv6 で通知することができます。チェックしないときは、そのあと先への経路がないことが ICMPv6 で通知されます。

チェックしたときは、集約経路情報と同じあと先の経路情報が破棄経路としてルーティングテーブルが設定されます。

サイトローカルプレフィックス

サイトローカルプレフィックスを交換する場合は、"交換する"を選択します。

16.1.3.3 IPv6 OSPF 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 OSPF 情報]

■ IPv6 OSPF情報

OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 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
パケット再送間隔	5 秒
LSUパケット送信遅延時間	1 秒
パケット送信	<input type="radio"/> 抑止する <input checked="" type="radio"/> 抑止しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

IPv6 OSPFを使用できるインターフェースの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。

OSPF 機能

OSPFを使用する場合は、"使用する"を選択します。

エリア定義番号

エリアの定義番号を10進数を使用して指定します。
OSPFエリア情報は、「ルーティングプロトコル情報」→「IPv6 OSPF関連」で設定することができます。省略時は、0が設定されます。

出力コスト

OSPF出力コストを1~65535の範囲で指定します。省略時は、10が設定されます。

指定ルータ優先度

指定ルータおよび副指定ルータを決定するための優先度を0~255の範囲で指定します。値が大きいほど優先度は高くなります。省略時は、1が設定されます。

こんな事に気をつけて

値が0の場合は、指定ルータおよび副指定ルータにはなりません。

Helloパケット送信間隔

OSPF隣接関係の維持に使用する、Helloパケットの送信間隔を指定します。省略時は、10秒が設定されます。

有効範囲)

1~18時間

1~1092分

1~65535秒

こんな事に気をつけて

OSPF隣接ルータ間で同じHelloパケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Hello パケット送信間隔より大きな値を指定する必要があります。Hello パケット送信間隔の 4 倍を設定することをお薦めします。省略時は、40 秒が設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

パケット送信

OSPF パケットの送信を抑止する場合は、“抑止する”を選択します。

こんな事に気をつけて

- OSPF 隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。
- 隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を指定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

3 ~ 65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

- LSA は生成されてから 1 時間が経過すると破棄されます。
- LSU 送信遅延時間に 1 時間以上を指定しないでください。
- 正しくルーティングできない場合があります。

16.1.3.4 IPv6 スタティック経路情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 スタティック経路情報]

■IPv6 スタティック経路情報

※追加・修正情報は一覧の入力フィールドで設定してください。

あて先プレフィックス／プレフィックス長	中継ルータアドレス	メトリック値	優先度	操作
<input type="button" value="全削除"/>				
<IPv6 スタティック経路情報入力フィールド>				
ネットワーク	<input checked="" type="radio"/> デフォルトルート 中継ルータアドレス <input type="text"/>			
	<input checked="" type="radio"/> 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 <input type="text"/> / <input type="text"/>			
	中継ルータアドレス <input type="text"/>			
	メトリック値 <input type="text" value="1"/>			
優先度 <input type="text" value="0"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 スタティック経路情報の定義が表示されています。IPv6 スタティック経路の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。
IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に1つしか設定できません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
中継ルータアドレスを指定します。
- 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、中継ルータアドレスを指定します。
あて先プレフィックスにリンクローカルアドレスは指定できません。ICMPv6 Redirect を正常に動作させるためには、中継ルータアドレスはリンクローカルアドレスで指定する必要があります。
なお、あて先プレフィックス／プレフィックス長に::/0を設定した場合、“デフォルトルート”を指定したものとして動作します。

優先度

このスタティック経路情報の優先度を、10進数を使用して0～254で指定します。省略時は、0が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度（省略時）
OSPF	110
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

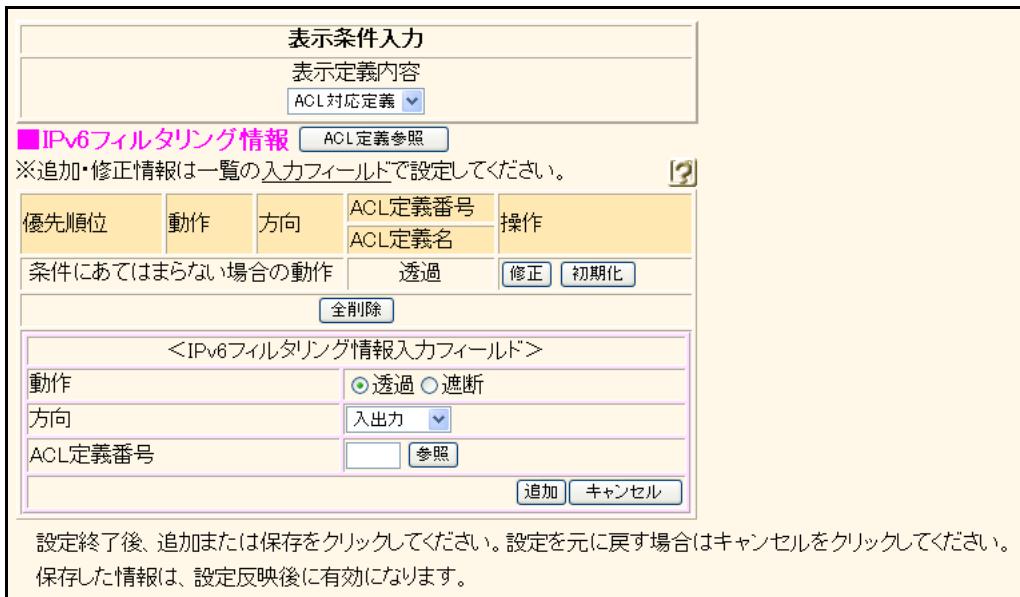
- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

メトリック値

このスタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

16.1.3.5 IPv6 フィルタリング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 フィルタリング情報]



表示条件入力
ACL 対応定義

■ IPv6 フィルタリング情報 [ACL 定義参照](#)

※ 追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	方向	ACL 定義番号	操作
			ACL 定義名	
条件にあてはまらない場合の動作	透過			修正 初期化
全削除				

<IPv6 フィルタリング情報入力フィールド>

動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
方向	入出力 参照
ACL 定義番号	参照

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく行えません。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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IPv6アドレス／プレフィックス長とあて先IPv6アドレス／プレフィックス長
 - 送信元ポート番号とあて先ポート番号リバースを指定した場合、入力パケットはIPv6アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL 定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

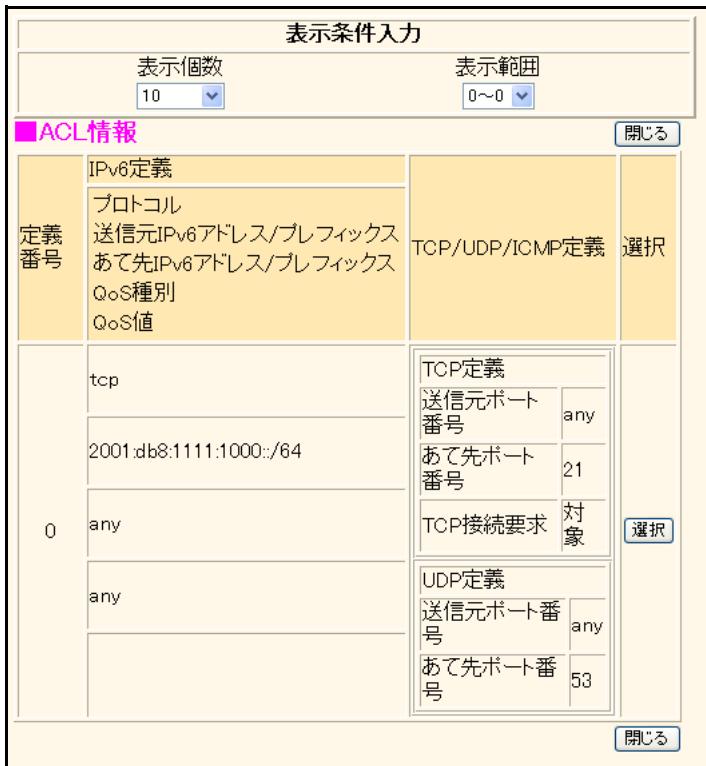
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の【選択】ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 フィルタリング情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.3.5.1 IPv6 フィルタリング情報（旧定義）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 フィルタリング情報]
→ 「表示条件入力（旧定義）」

表示条件入力								
表示定義内容								
旧定義								
■ IPv6 フィルタリング情報								
※追加・修正情報は一覧の <input type="text"/> で設定してください。 ?								
優先順位	動作	送信元IPv6アドレス/プレフィックス長	送信元ポート番号	あて先IPv6アドレス/プレフィックス長	TCP接続要求	Traffic Class	方向	
		あて先ポート番号						操作
		ICMPv6タイプ						
		ICMPv6コード						
条件にあてはまらない場合の動作				透過	修正	初期化		
全削除								
<IPv6 フィルタリング情報入力フィールド>								
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断						
プロトコル		すべて <input type="button" value="▼"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)						
送信元情報		IPv6アドレス/ プレフィック ス長 <input type="text"/> <input type="checkbox"/>						
あて先情報		IPv6アドレス/ プレフィック ス長 <input type="text"/> <input type="checkbox"/>						
ICMPv6		ポート番号 <input type="text"/> タイプ <input type="text"/> コード <input type="text"/>						
TCP接続要求		<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外						
Traffic Class		<input type="text"/>						
方向		入出力 <input type="button" value="▼"/>						
追加 キャンセル								
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。								

表示条件入力に、" 旧定義 " を選択した場合に、IPv6 フィルタリング情報の旧定義が表示されます。

動作

IPv6 フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の 5 つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、" その他 " を選択し、10 進数を使用して、0 ~ 254 の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

フィルタリング条件としての IPv6 アドレスおよびプレフィックス長を指定します。以下が等しい場合に条件に一致します。

- チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積
- 定義する IPv6 アドレスとプレフィックス長の論理積

ポート番号

フィルタリング条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、”,” で区切れます。範囲指定の場合は、”-” で区切れます。送信元情報とあて先情報を合わせて 10 組まで指定できます。

ICMPv6

タイプ

フィルタリング条件として ICMPv6 パケットのタイプ値を 10 進数を使用して 0～255 の範囲または “any” で指定します。ICMPv6 タイプ値を複数指定する場合は ”,” で区切れます。範囲指定の場合は ”-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての ICMPv6 タイプ値がフィルタリングの対象となります。

コード

フィルタリング条件として ICMPv6 パケットのコード値を 10 進数を使用して 0～255 の範囲または “any” で指定します。ICMPv6 コード値を複数指定する場合は ”,” で区切れます。範囲指定の場合は ”-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての ICMPv6 コード値がフィルタリングの対象となります。

TCP 接続要求

TCP プロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルに TCP を設定した場合だけ有効です。

Traffic Class

フィルタリング条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0～ff の範囲または “any” で指定します。Traffic Class 値を複数指定する場合は ”,” で区切れます。範囲指定の場合は ”-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての Traffic Class 値がフィルタリングの対象となります。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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 IPv6 アドレス／プレフィックス長とあて先 IPv6 アドレス／プレフィックス長
 - 送信元ポート番号とあて先ポート番号
 リバースを指定した場合、入力パケットは IPv6 アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対して TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

16.1.3.5.2 IPv6 フィルタリング情報（条件にあてはまらない場合の動作）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 フィルタリング情報]
→ 「条件にあてはまらない場合の動作」[修正]

The screenshot shows the 'IPv6 Filtering Rule' configuration interface. At the top, there's a header '表示条件入力' (Display Condition Input) and a dropdown '表示定義内容' (Display Definition Content) set to 'ACL 対応定義'. Below this is a section titled '■ IPv6 フィルタリング情報' (■ IPv6 Filtering Information) with a 'ACL 定義参照' (ACL Definition Reference) button. A note says '※ 追加・修正情報は一覧の入力フィールドで設定してください。' (Additional/modified information is set in the list input fields). The main area has tabs: '優先順位' (Priority), '動作' (Action), '方向' (Direction), 'ACL 定義番号' (ACL Definition Number), and '操作' (Operation). The '動作' tab is selected, showing three options: '透過' (Transparent), '遮断' (Block), and 'SPI'. Below these is a '情報保持タイム' (Information Hold Time) field set to '5 分'. At the bottom are '保存' (Save), 'キャンセル' (Cancel), and '一覧へ戻る' (Return to List) buttons, and a '全削除' (Delete All) button at the very bottom.

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断や SPI を指定し、IPv6 フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPv6 フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPI セッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

16.1.3.6 IPv6 Traffic Class 値書き換え情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連]
 → [IPv6 Traffic Class 値書き換え情報]

表示条件入力
表示定義内容
ACL対応定義

■IPv6 Traffic Class値書き換え情報 ACL定義参照

※追加・修正情報は一覧ので設定してください。

優先順位	ACL定義番号	新Traffic Class	操作
ACL定義名			

全削除

<IPv6 Traffic Class値書き換え情報入力フィールド>

新Traffic Class	<input type="text"/>
ACL定義番号	<input type="text"/> 参照

追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 Traffic Class 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Traffic Class 値書き換えの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義”または“旧定義”から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 Traffic Class

IPv6 パケットに新しく指定する IPv6 Traffic Class 値を 16 進数を使用して、0～ff の範囲で指定します。

ACL 定義番号

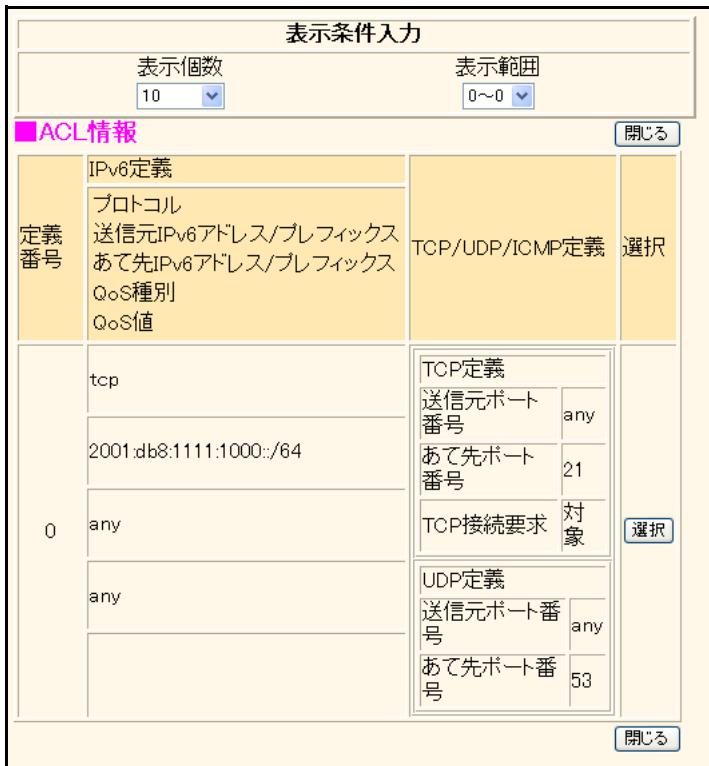
[参照] ボタンをクリックして、ACL 定義番号を指定します。別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連]
 → [IPv6 Traffic Class 値書き換え情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 Traffic Class 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 Traffic Class 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.3.6.1 IPv6 Traffic Class 値書き換え情報（旧定義）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連]
 → [IPv6 Traffic Class 値書き換え情報] → 「表示条件入力（旧定義）」

表示条件入力					
表示定義内容 旧定義					
■IPv6 Traffic Class値書き換え情報					
※追加・修正情報は一覧の <input type="text"/> で設定してください。					
優先順位	プロトコル	送信元IPv6アドレス/プレフィックス長	Traffic Class	操作	
		送信元ポート番号			
		あて先IPv6アドレス/プレフィックス長	新Traffic Class		
		あて先ポート番号			
<input type="button" value="全削除"/>					
<IPv6 Traffic Class書き換え情報入力フィールド>					
プロトコル		すべて <input type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)			
送信元情報	IPv6アドレス／ プレフィックス長	<input type="text"/> <input type="checkbox"/>			
	ポート番号	<input type="text"/>			
あて先情報	IPv6アドレス／ プレフィックス長	<input type="text"/> <input type="checkbox"/>			
	ポート番号	<input type="text"/>			
Traffic Class		<input type="text"/>			
新Traffic Class		<input type="text"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。					

表示条件入力に、“旧定義”を選択した場合に、IPv6 Traffic Class 値書き換え情報の旧定義が表示されます。

プロトコル

IPv6 Traffic Class 書き換え条件としてプロトコルを以下の5つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

IPv6 Traffic Class 値書き換え条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

IPv6 Traffic Class 値書き換え条件としてのIPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6 アドレスと定義するプレフィックス長の論理積、定義するIPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

IPv6 Traffic Class 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定する場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、”,” で区切れます。範囲指定の場合は “-” で区切れます。送信元情報とあて先情報を合わせて 10 組まで指定できます。

Traffic Class

IPv6 Traffic Class 値書き換え条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0～ff の範囲または “any” で指定します。Traffic Class フィールド値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての IPv6 Traffic Class 値が書き換えの対象となります。

新 Traffic Class

IPv6 パケットに新しく指定する IPv6 Traffic Class 値を 16 進数を使用して、0～ff の範囲で指定します。

16.1.3.7 IPv6 RIP フィルタリング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 RIP フィルタリング情報]

■ IPv6 RIP フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
<input type="button" value="全削除"/>					
<IPv6 RIP フィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信	フィルタリング条件	メトリック値
	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定			<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	
				プレフィックス / プレフィック ス長	
メトリック 値	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

RIP 受信（送信）時には、優先順位の高い定義から順に受信（送信）方向の条件を参照し、一致した条件があつた時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、受信（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。

動作

フィルタリング対象に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合に RIP 経路情報を透過します。
- 遮断
条件と一致した場合に RIP 経路情報を遮断します。

方向

フィルタリングを RIP 受信時に行うか、RIP 送信時に行うかを選択します。

- 受信
RIP 受信時に、フィルタリングを行います。
- 送信
RIP 送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を選択します。

- **すべて**
すべての経路情報をフィルタリング対象とします。
- **デフォルトルート**
デフォルトルートをフィルタリング対象とします。
- **経路情報指定**
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。
なお、プレフィックス／プレフィックス長に ::/0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

検索条件を選択します。

- **完全に一致**
指定したプレフィックスとプレフィックス長が完全に一致したRIP 経路情報をフィルタリング対象とします。
- **マスクした結果が一致**
指定したプレフィックスと、RIP 経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、そのRIP 経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP 経路情報のメトリック値を変更できます。送信時のRIP 経路にメトリック値を設定した場合、「RIP 情報」で設定した加算メトリック値は加算されません。省略または0 を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

16.1.3.8 IPv6 帯域制御 (WFQ) 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報]

表示条件入力
表示定義内容
ACL 対応定義

■ IPv6 帯域制御 (WFQ) 情報

※ 追加・修正情報は一覧の入力フィールドで設定してください。

定義番号	ACL 定義番号	帯域	操作
			<input type="button" value="全削除"/>
<IPv6 帯域制御 (WFQ) 情報入力フィールド>			
帯域	<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input style="width: 40px;" type="text"/> % <input type="radio"/> 使用帯域 <input style="width: 40px;" type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="button" value="共有できる定義が存在しません"/>	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	
	ACL 定義番号 <input type="text"/> <input type="button" value="参照"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報の ACL 定義が表示されています。帯域制御の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

表示条件入力は、「ACL 対応定義」または「旧定義」から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を 10 進数を使用して、1～99 の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが 100 を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbps または 1～100Mbps の範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

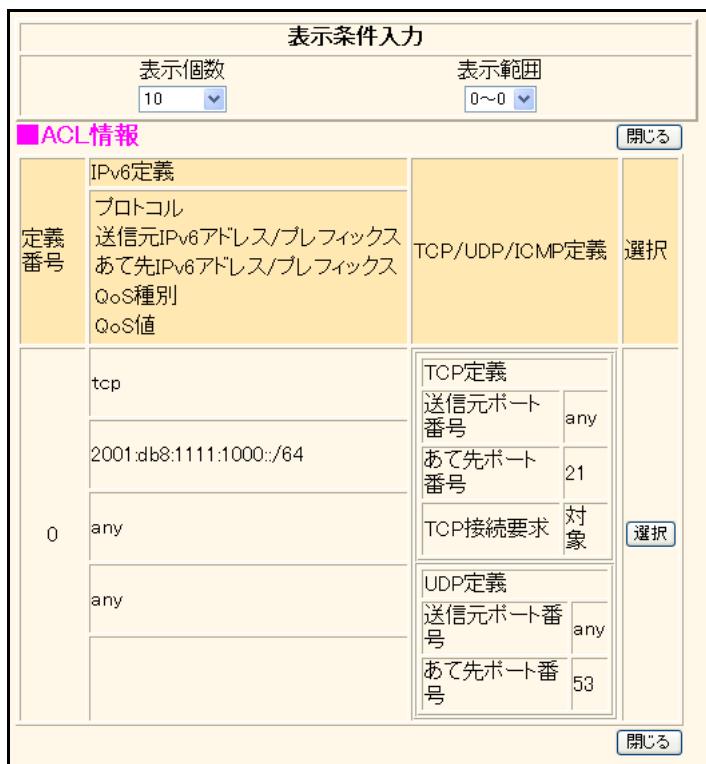
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」 / 「修正」 - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 帯域制御 (WFQ) 情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 帯域制御 (WFQ) 情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.3.8.1 IPv6 帯域制御 (WFQ) 情報 (旧定義)

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報]
→ 「表示条件入力 (旧定義)」

表示条件入力					
表示定義内容 <input type="button" value="旧定義"/>					
■ IPv6帯域制御(WFQ)情報					
※追加・修正情報は一覧の入力フィールドで設定してください。					
定義番号	プロトコル	送信元IPv6アドレス／プレフィックス長	対象Traffic Class値	操作	
		送信元ポート番号 あて先IPv6アドレス／プレフィックス長 あて先ポート番号			
<input type="button" value="全削除"/>					
<IPv6帯域制御(WFQ)情報入力フィールド>					
プロトコル		すべて (番号指定: <input type="text"/> “その他”を選択時のみ有効です)			
送信元情報	IPv6アドレス／プレフィックス長	<input type="text"/> <input type="button" value=""/>			
	ポート番号	<input type="text"/>			
あて先情報	IPv6アドレス／プレフィックス長	<input type="text"/> <input type="button" value=""/>			
	ポート番号	<input type="text"/>			
対象Traffic Class値		<input type="text"/>			
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="button" value="共有できる定義が存在しません"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。					

表示条件入力に、“旧定義”を選択した場合に、IPv6 帯域制御 (WFQ) 情報の旧定義が表示されます。

プロトコル

帯域制御の対象となるプロトコルを以下の5つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

帯域制御の対象となるIPv6 アドレスおよびプレフィックス長を指定します。対象となるパケットのIPv6 アドレスと定義するプレフィックス長の論理積と、定義するIPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 Traffic Class 値

帯域制御の対象となるIPv6パケットのTraffic Class値を16進数を使用して、0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのTraffic Class値が帯域制御の対象となります。

帯域

帯域の使用率または帯域値を指定します。

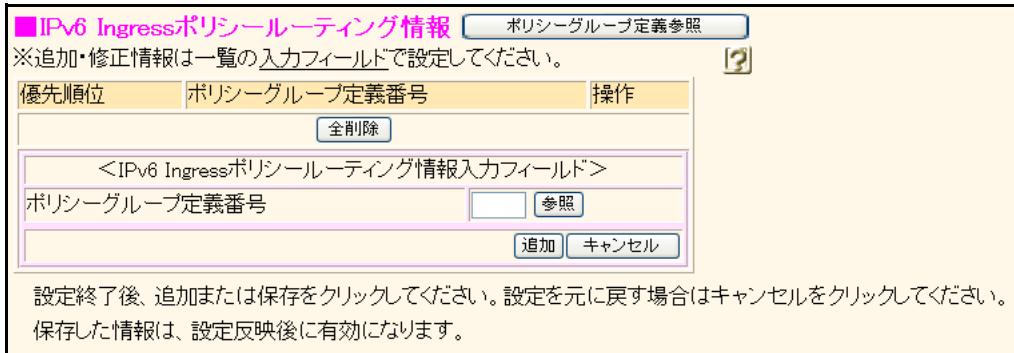
- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

16.1.3.9 IPv6 Ingress ポリシールーティング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連]
 → [IPv6 Ingress ポリシールーティング情報]



現在、設定されている IPv6 Ingress ポリシールーティング情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Ingress ポリシールーティング情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に、指定されたポリシーグループに定義された送出先へパケットを送出します。

ポリシーグループ定義番号

[参照] ボタンをクリックして、ポリシーグループ定義番号を指定します。

別の画面に「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されます。指定する定義番号欄の [選択] ボタンをクリックし、ポリシーグループ定義番号を設定します。自動的に画面が閉じます。

なお、参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連]
 → [IPv6 Ingress ポリシールーティング情報] → 「ポリシーグループ定義番号の [参照]」



「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ポリシーグループ定義情報の一覧に見たい情報を表示させることができます。

参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 Ingress ポリシールーティング情報」のポリシーグループ定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 Ingress ポリシールーティング情報」にポリシーグループ定義番号が設定され、画面が閉じます。[ポリシーグループ定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.3.10 IPv6 DHCP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [IPv6 関連] → [IPv6 DHCP 情報]

DHCP 機能で、" 使用しない " を選択した場合

■ IPv6 DHCP情報

DHCP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input type="radio"/> リレーエージェント機能を使用する <input type="radio"/> サーバ機能を使用する
---------------	---

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

DHCP 機能で、" クライアント機能を使用する " を選択した場合

■ IPv6 DHCP情報

DHCP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> クライアント機能を使用する <input type="radio"/> リレーエージェント機能を使用する <input type="radio"/> サーバ機能を使用する	
クライアント機能	DUID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
	IAID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
	プレフィックス要求	<input type="radio"/> しない <input checked="" type="radio"/> する <input type="checkbox"/> 「旧方式を使用する」 <small>※draft-troan-dhcpv6-opt-prefix-delegation-01.txtに準拠したサーバを使用する場合は、「旧方式を使用する」をチェックしてください。</small>
	DNSサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	DNSドメイン名要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	SIPサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	SIPドメイン名要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	SNTPサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない
リジェクト経路	<input checked="" type="radio"/> Blackhole <input type="radio"/> Reject	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

DHCP 機能で、"リレーエージェント機能を使用する"を選択した場合

■ IPv6 DHCP情報

DHCP機能		<input type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input checked="" type="radio"/> リレーエージェント機能を使用する <input type="radio"/> サーバ機能を使用する
リレー エージェント 機能	リレー先 インターフェース	lan0
	リレー先 サーバアドレス	
	送信元アドレ ス	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

DHCP 機能で、"サーバ機能を使用する"を選択した場合

■ IPv6 DHCP情報

DHCP機能		<input type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input type="radio"/> リレーエージェント機能を使用する <input checked="" type="radio"/> サーバ機能を使用する
サーバ機能	DUID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
	プリファレンス 値	<input type="text"/>
	アドレス配布	<input checked="" type="radio"/> しない <input type="radio"/> する 割当て開始アドレス <input type="text"/> 割当てアドレス数 <input type="text"/> Valid Lifetime <input checked="" type="radio"/> 期限なし <input type="radio"/> 期限あり <input type="text"/> 日 Pref. Lifetime <input checked="" type="radio"/> 期限なし <input type="radio"/> 期限あり <input type="text"/> 日
		<input checked="" type="radio"/> しない <input type="radio"/> する プレフィックス <input type="text"/> ✓ Valid Lifetime <input checked="" type="radio"/> 期限なし <input type="radio"/> 期限あり <input type="text"/> 日
		Pref. Lifetime <input checked="" type="radio"/> 期限なし <input type="radio"/> 期限あり <input type="text"/> 日 自動経路設定 <input checked="" type="radio"/> する <input type="radio"/> しない 配布先クライ アントDUID <input type="text"/>
		DNSサーバア ドレス配布 プライマリ <input type="text"/> セカンダリ <input type="text"/>
		DNSドメイン 名配布 <input type="text"/>
	SIPサーバア ドレス配布 プライマリ <input type="text"/> セカンダリ <input type="text"/>	
	SIPドメイン名 配布 プライマリ <input type="text"/> セカンダリ <input type="text"/>	

SNTPサーバ アドレス配布	プライマリ セカンダリ	<input type="text"/>	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。			
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>			

DHCP 機能

それぞれのインターフェースのIPv6 DHCP 機能を以下の4つから選択します。

- 使用しない
IPv6 DHCP 機能を使用しません。
- クライアント機能を使用する
本装置を該当インターフェースのIPv6 DHCP クライアントとして使用します。
- リレーエージェント機能を使用する
IPv6 DHCP リレーエージェントとして使用します。
- サーバ機能を使用する
本装置を該当インターフェースのネットワークのIPv6 DHCP サーバとして使用します。

クライアント機能

本装置を該当インターフェースのIPv6 DHCP クライアントとして使用する場合に設定します。

DUID

DUID を以下の2つから選択します。

- 自動
DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
260桁以内の16進数で表記した DUID を指定します。

IAID

IAID を以下の2つから選択します。

- 自動
自動生成される IAIID を使用します。通常は、この設定を使用します。
- 指定する
1～4294967295 の範囲の10進数で指定します。

プレフィックス要求

DHCP サーバにプレフィックスを要求するかどうかを設定します。DHCP サーバにプレフィックスを要求する場合は、“する”を選択します。“する”を選択した場合に、draft-troan-dhcpv6-opt-prefix-delegation-01.txt に準拠したサーバを利用するときは、“旧方式を使用する”をチェックします。

DNS サーバアドレス要求

DHCP サーバにDNS サーバアドレスを要求するかどうかを設定します。DHCP サーバにDNS サーバアドレスを要求する場合は、“する”を選択します。

DNS ドメイン名要求

DHCP サーバにDNS ドメイン名を要求するかどうかを設定します。DHCP サーバにDNS ドメイン名を要求する場合は、“する”を選択します。

SIP サーバアドレス要求

DHCP サーバにSIP サーバアドレスを要求するかどうかを設定します。DHCP サーバにSIP サーバアドレスを要求する場合は、“する”を選択します。

SIP ドメイン名要求

DHCP サーバにSIP ドメイン名を要求するかどうかを設定します。DHCP サーバにSIP ドメイン名を要求する場合は、“する”を選択します。

SNTP サーバアドレス要求

DHCP サーバにSNTP サーバアドレスを要求するかどうかを設定します。DHCP サーバにSNTP サーバアドレスを要求する場合は、“する”を選択します。

リジェクト経路

DHCP サーバから取得したプレフィックスのリジェクト経路を以下の2つから選択します。

- Blackhole
リジェクト経路あてのパケットを受信しても送信元にエラーを報告しません。
- Reject
リジェクト経路あてのパケットを受信した場合、送信元にエラーを報告します。

リレーエージェント機能

IPv6 DHCP リレーエージェントとして使用する場合に設定します。

リレー先インターフェース

IPv6 DHCP クライアントからの要求を中継し、送出するインターフェースを選択します。

リレー先サーバアドレス

リレー先サーバのIPv6 アドレスを設定します。

存在するリレー先インターフェースを指定してください。

送信元アドレス

サーバへのリレーパケットを送信する際の送信元アドレスとして、本装置に設定されている自側 IPv6 アドレスのどれかを指定します。

サーバ機能

本装置を該当インターフェースのネットワークのIPv6 DHCP サーバとして使用する場合に設定します。

DUID

- 自動
DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
260桁以内の 16進数で表記した DUID を指定します。

プリファレンス値

DHCP サーバのプリファレンス値を 0 ~ 255 の範囲の 10 進数で指定します。DHCP クライアントはこの値が大きい DHCP サーバを選択します。省略時は 0 が設定されます。

アドレス配布

DHCP クライアントに割り当てる IPv6 アドレスを設定します。クライアントに IPv6 アドレスを割り当てる場合は、“する”を選択し、以降の項目を設定します。

“しない”を選択した場合、ホストデータベース設定による静的なアドレス割り当てだけが行われます。

割当て開始アドレス

クライアントに割り当てる連続した IPv6 アドレス群の先頭の IPv6 アドレスを指定します。

有効範囲)

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

割当てアドレス数

クライアントに割り当てる IPv6 アドレス数を 0 ~ 300 の範囲で指定します。ホストデータベース機能を使用すると特定の IPv6 DHCP クライアントに対して固有の IPv6 アドレスを割り当てるることができます。この場合の IPv6 アドレスは、割り当て開始 IPv6 アドレスと割り当てアドレス数によって規定される動的割り当て範囲である必要はありません。

こんな事に気をつけて

割り当てアドレスとして 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場合は、上位を “dhcp@インターフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。

Valid Lifetime

割り当てる IPv6 アドレスの Valid Lifetime を指定します。

有効範囲)

0 ~ 365 日
0 ~ 8760 時間
0 ~ 525600 分
0 ~ 31536000 秒

Pref. Lifetime

割り当てる IPv6 アドレスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲)

0 ~ 365 日
0 ~ 8760 時間
0 ~ 525600 分
0 ~ 31536000 秒

プレフィックス配布

DHCP クライアントに割り当てるプレフィックスを設定します。クライアントにプレフィックスを割り当てる場合は、"する"を選択し、以降の項目を設定します。

プレフィックス

クライアントに割り当てるプレフィックスとプレフィックス長を設定します。プレフィックス長は 48～64 の範囲で指定します。

こんな事に気をつけて

配布するプレフィックスとして 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場合は、上位を "dhcp@インターフェース名" の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。

Valid Lifetime

割り当てるプレフィックスの Valid Lifetime を指定します。

有効範囲)

0～365 日

0～8760 時間

0～525600 分

0～31536000 秒

Pref. Lifetime

割り当てるプレフィックスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲)

0～365 日

0～8760 時間

0～525600 分

0～31536000 秒

自動経路設定

クライアントに割り当てたプレフィックスへの経路を自動で設定する場合は、"する"を選択します。

配布先クライアント DUID

配布先クライアントの DUID を、260 桁以内の 16 進数で指定します。

DNS サーバアドレス配布

配布する DNS サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する DNS サーバアドレスとして IPv6 DHCP クライアントが取得した DNS サーバアドレスを使用する場合は、"dhcp@インターフェース名" の形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ DNS サーバの指定はできません。

DNS ドメイン名配布

配布する DNS ドメイン名を設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する DNS ドメイン名として IPv6 DHCP クライアントが取得した DNS ドメイン名を使用する場合は、"dhcp@インターフェース名" の形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。

SIP サーバアドレス配布

配布する SIP サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SIP サーバアドレスとして IPv6 DHCP クライアントが取得した SIP サーバアドレスを使用する場合は、"dhcp@インターフェース名" の形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ SIP サーバの指定はできません。

SIP ドメイン名配布

配布する SIP ドメイン名を設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SIP ドメイン名として IPv6 DHCP クライアントが取得した SIP ドメイン名を使用する場合は、"dhcp@インターフェース名" の形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ SIP サーバの指定はできません。

SNTP サーバアドレス配布

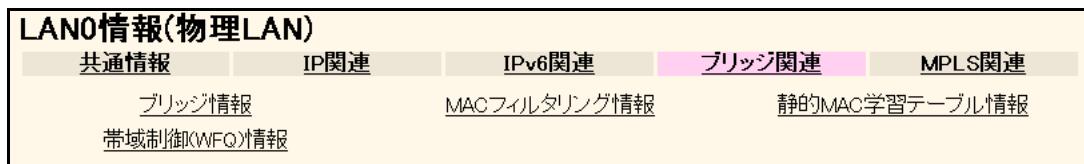
配布する SNTP サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SNTP サーバアドレスとして IPv6 DHCP クライアントが取得した SNTP サーバアドレスを使用する場合は、“dhcp@インターフェース名”の形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ SNTP サーバの指定はできません。

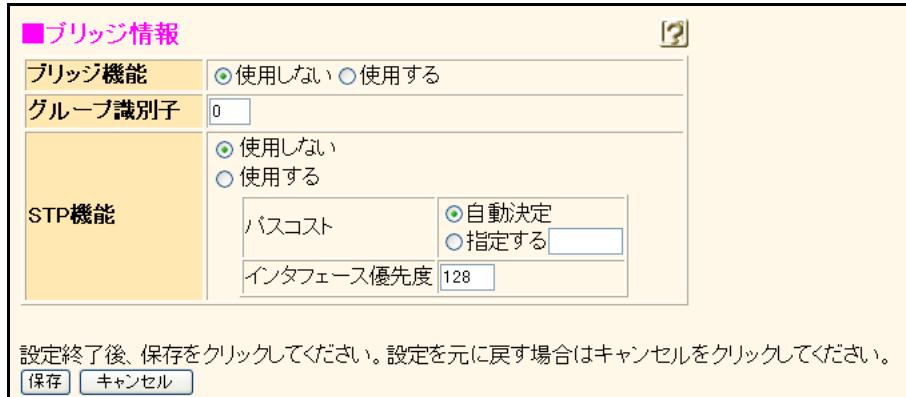
16.1.4 ブリッジ関連

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連]



16.1.4.1 ブリッジ情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [ブリッジ情報]



ブリッジ機能

接続相手とブリッジで通信する場合は、“使用する”を選択します。

インターフェース優先度

STPで使用するインターフェースごとの優先度を0～255の範囲で指定します。値が小さい方が優先となります。

グループ識別子

ブリッジのグループ識別子を10進数で指定します。0～7の範囲で指定します。省略時は0が設定されます。

STP 機能

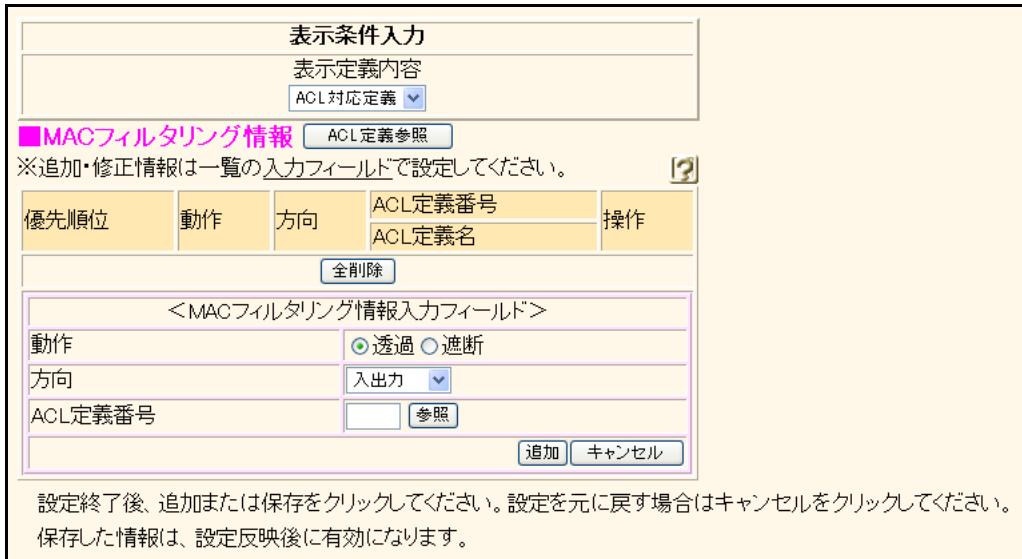
STP機能を利用して経路制御を行う場合は、“使用する”を選択して、以下の項目を設定します。グループ識別子に0を設定した場合だけ、STPを利用することができます。この設定項目はブリッジ機能を使用する場合だけ有効です。

パスコスト

STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

16.1.4.2 MAC フィルタリング情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [MAC フィルタリング情報]



現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

LAN モジュールで送受信する際にフィルタリング処理を行います。優先順位の高い定義から順にフレームのチェックを行い、フィルタリング条件が一致した場合に定義された動作を行います。

動作

フィルタリング条件に一致したときの MAC フィルタリングの動作を以下の 2 つから選択します。

- 透過
フィルタリング条件と一致する場合にフレームを透過します。
- 遮断
フィルタリング条件と一致する場合にフレームを遮断します。

方向

フィルタリングする方向を指定します。

- 入力
入力パケットのみをフィルタリング対象とする場合に指定します。
- 出力
出力パケットのみをフィルタリング対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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 MAC アドレスとあて先 MAC アドレス
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- MAC 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [MAC フィルタリング情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「MAC 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「MAC フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「MAC フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.4.2.1 MAC フィルタリング情報（旧定義）

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [MAC フィルタリング情報]
→ 「表示定義内容（旧定義）」

表示条件入力					
表示定義内容 <input type="button" value="旧定義"/>					
■MACフィルタリング情報					
※追加・修正情報は一覧の入力ファイルで設定してください。					
優先順位	動作	送信元MACアドレス	フォーマット種別	LSAP/type値	操作
動作	送信元MACアドレス あて先MACアドレス	フォーマット種別	VLANタグ解析	操作	
<input type="button" value="全削除"/>					
<MACフィルタリング情報入力フィールド>					
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 すべて <input type="button" value="…"/> アドレス指定（“指定する”を選択時のみ有効です）			
送信元MACアドレス					
あて先MACアドレス					
フォーマット種別		<input checked="" type="radio"/> すべて <input type="radio"/> LLC形式 LSAP <input type="button" value="…"/> VLANタグ解析 <input checked="" type="radio"/> しない <input type="radio"/> する <input type="radio"/> Ethernet形式 type値 <input type="button" value="…"/> VLANタグ解析 <input checked="" type="radio"/> しない <input type="radio"/> する			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

LAN モジュールで送受信する際にフィルタリング処理を行います。優先順位の高い定義から順にフレームのチェックを行い、フィルタリング条件が一致した場合に定義された動作を行います。

動作

フィルタリング条件に一致したときの動作を指定します。
MAC フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

送信元／あて先MACアドレス

MACアドレスを以下の項目から選択します。“指定する”を選択する場合は、アドレス指定にMACアドレスを16進数で指定します。

- すべて
すべてのMACアドレスを対象とします。
- ブロードキャスト
ブロードキャストMACアドレスを対象とします。
- マルチキャスト
ブロードキャストMACアドレスおよびマルチキャストMACアドレスを対象とします。
- 指定する
アドレス指定に指定するMACアドレスを対象とします。MACアドレスは、「xx:xx:xx:xx:xx:xx」(xxは2桁の16進数)の形式で指定します。

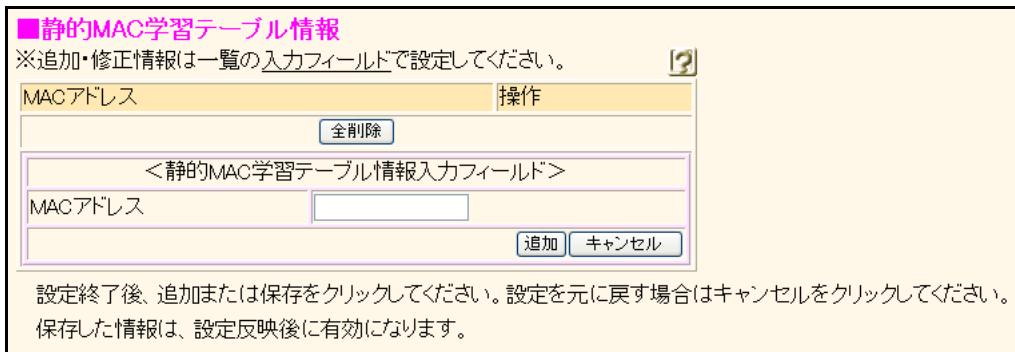
フォーマット種別

フィルタリング対象のフォーマットを以下の項目から選択します。“LLC形式”的場合は、LSAPを16進数を使用して、0～ffffの範囲で指定し、“Ethernet形式”的場合は、type値を16進数を使用して、5dd～ffffの範囲で指定します。未入力時にはすべての値が対象となります。また、VLANタグ付きパケットでVLANタグの先を解析するか選択します。“する”を指定した場合は、VLANタグ付きパケットでも正しく解析されます。

- LLC形式
LLC形式のパケットを対象とします。
- Ethernet形式
Ethernet形式のパケットを対象とします。
- すべて
すべてのパケットを対象とします。

16.1.4.3 静的 MAC 学習テーブル情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [静的 MAC 学習テーブル情報]



現在、設定されている静的 MAC 学習テーブルの定義が表示されています。静的 MAC 学習テーブル情報の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

MAC アドレス

MAC アドレスは、「xx:xx:xx:xx:xx:xx」（xx は 2 衔の 16 進数）の形式で指定します。

16.1.4.4 帯域制御 (WFQ) 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [帯域制御 (WFQ) 情報]

■帯域制御(WFQ)情報 ACL定義参照

※追加・修正情報は一覧の入力フィールドで設定してください。

定義番号	ACL定義番号	帯域	操作
	ACL定義名		
全削除			
<帯域制御(WFQ)情報入力フィールド>			
帯域	<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input style="width: 40px;" type="text"/> % <input type="radio"/> 使用帯域 <input style="width: 40px;" type="text"/> Kbps <input type="button" value="▼"/> <input type="radio"/> 帯域を他と共有 <input style="border: 1px solid blue; border-radius: 5px; padding: 2px 10px;" type="button" value="共有できる定義が存在しません"/>		
ACL定義番号	<input type="text"/>	参照	追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御の定義が表示されています。帯域制御の定義数は、仕様一覧 [\[2.3 システム最大値一覧\]](#) (P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱います。
- ベストエフォート
非優先（ベストエフォート）として扱います。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワーク中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有する場合に選択します。

こんな事に気をつけて

使用的回線が LAN の場合、シェーピングを使用しないと帯域制御機能は有効に動作しません。使用的回線が ATM の場合、適切な VC 速度を設定しないと帯域制御機能は有効に動作しません。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- MAC 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。
なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [ブリッジ関連] → [帯域制御 (WFO) 情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「MAC 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報をだけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「帯域制御 (WFO) 情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「帯域制御 (WFO) 情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

16.1.5 MPLS 関連

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [MPLS 関連]



16.1.5.1 MPLS 基本情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [MPLS 関連] → [MPLS 基本情報]

MPLS機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
ラベル配布プロトコル	LDP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

MPLS 機能

LAN 上で MPLS 機能を使用する場合は、“使用する”を選択します。

ラベル配布プロトコル

LAN 上で行うラベル配布プロトコルを選択します。

16.1.5.2 LDP 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [MPLS 関連] → [LDP 情報]

Hello タイマ	
interval	5 秒
HoldTime	<input checked="" type="radio"/> infinity <input checked="" type="radio"/> 指定する 15 秒
KeepAlive タイマ	
interval	1 分
timeout	3 分
LDP ラベル広報方式	
LDP ラベル保持方式	<input checked="" type="radio"/> DU <input type="radio"/> DoD
PHP 機能	<input checked="" type="radio"/> liberal <input type="radio"/> conservative
IPv4 Transport アドレス	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

Hello タイマ

interval

Hello の送信間隔のタイマを 1 ~ 65535 秒の範囲で指定します。初期値は 5 秒です。省略はできません。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

HoldTime

近隣関係の維持を判定するための HoldTime のタイマを 1 ~ 65534 秒の範囲で指定します。

近隣関係の維持を判定する場合は、HoldTime に infinity を選択します。初期値は 15 秒です。省略はできません。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65534 秒

こんな事に気をつけて

HoldTime の値は、interval の値より小さくすることはできません。HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

KeepAlive タイマ

interval

KeepAlive の送信間隔のタイマを 1 ~ 65535 秒の範囲で指定します。初期値は 1 分です。省略はできません。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

timeout

LDP セッションの維持を判定するための KeepAlive のタイマを 1 ~ 65535 秒の範囲で指定します。初期値は 3 分です。省略はできません。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

timeout の値は、interval の値より小さくすることはできません。timeout の値は interval の値の 3 倍以上を設定することを推奨します。

LDP ラベル広報方式

LDPのラベル広報方式を以下の2つから選択します。

- DU
Downstream Unsolicited を使用します。
- DoD
Downstream On Demand を使用します。

LDP ラベル保持方式

LDPのラベル保持方式を以下の2つから選択します。

- liberal
liberal を使用します。
- conservative
conservative を使用します。

PHP 機能

インターフェースでの LSP の PHP 機能を設定します。

- 使用しない
PHP 機能を無効にします。
- 使用する
PHP 機能を有効にします。

MPLS トンネル接続を使用する場合に、自側エンドポイントと IP アドレスが同じとき、設定に関係なく “使用しない” が設定されます。

IPv4 Transport アドレス

インターフェース単位で LDP が相手装置との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合、本装置に設定された IPv4 アドレスを指定します。0.0.0.0 を指定した場合は、「MPLS 情報」の IPv4 Transport Address の設定に従います。省略時は、0.0.0.0 を指定したものとみなします。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

こんな事に気をつけて

必ず本装置に存在するアドレスを指定してください。

本装置に存在しないアドレスをインターフェースに指定した場合は、そのインターフェースでは LDP を使用できません。

16.1.5.3 EoMPLS 情報

[操作] ルータ設定「LAN 情報（物理 LAN）」→ [修正] → [MPLS 関連] → [EoMPLS 情報]

■EoMPLS情報	
EoMPLS機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
VC ID	<input type="text"/>
相手装置のIPv4アドレス	<input type="text"/>
VCタイプ	auto
EXP値書き換え	<input checked="" type="radio"/> 固定値 0 <input type="radio"/> VLANタグのプライオリティを使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

EoMPLS 機能

EoMPLS機能を使用する場合は“使用する”を選択します。

VC ID

LAN 定義の VC ID を 10 進数を使用して 1 ~ 4294967295 で指定します。EoMPLS 通信の相手装置と同じ値を指定します。

相手装置の IPv4 アドレス

EoMPLS 通信の相手装置の IPv4 アドレスを指定します。相手装置で指定した IPv4 Transport Address 同じ値を指定します。0.0.0.0 および 255.255.255.255 は使用できません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

VC タイプ

相手装置で同じ VC ID を持つインターフェースと同じ値を指定します。

- auto
LAN 定義から、Ethernet または VLAN を自動的に識別します。
- ethernet
LAN 定義に関係なく VC Type を Ethernet に設定します。
- vlan
LAN 定義に関係なく VC Type を Ethernet VLAN に設定します。

EXP 値書き換え

固定の EXP 値を使用する場合、“固定値”を選択し、書き換える EXP 値を 10 進数を使用して 0 ~ 7 で指定します。

“固定値”を選択して、EXP 値を省略時は、0 が設定されます。VLAN タグのプライオリティを使用する場合は、“VLAN タグのプライオリティを使用する”を選択します。初期値は、EXP 値 0 です。

16.2 インタフェース : VLAN

[操作] ルータ設定「LAN 情報 (VLAN)」→ [追加]

LAN1情報(VLAN)

共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
------	------	--------	--------	--------

このページではLAN情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

「IP 関連」、「IPv6 関連」、「ブリッジ関連」および「MPLS 関連」は、「インターフェース：物理 LAN」を参照してください。

16.2.1 共通情報

[操作] ルータ設定「LAN 情報 (VLAN)」→ [追加] → [共通情報]

LAN1情報(VLAN)

共通情報	IP関連	IPv6関連	ブリッジ関連	MPLS関連
基本情報 MACアドレス認証情報	VLANプライオリティマッピング情報	VRRPグループ情報	ARP認証関連 トラップ情報	

「VRRP グループ情報」、「MAC アドレス認証情報」、「ARP 認証情報」および「トラップ情報」は、「インターフェース：物理 LAN」を参照してください。

16.2.1.1 基本情報

[操作] ルータ設定「LAN 情報 (VLAN)」→ [追加] → [共通情報] → [基本情報]

■ 基本情報

出力先	LAN0
VLAN ID	1
プライオリティ	0
シェーピング	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 最大送信レート <input type="text"/> Mbps
VRRP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する パスワード <input type="text"/> TRAPモード <input checked="" type="radio"/> 旧仕様 <input type="radio"/> 新仕様
MTUサイズ	1500 バイト

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

出力先

VLAN フレームの出力先インターフェースを選択します。すでに設定済みの物理インターフェースだけ選択できます。

VLAN ID

VLAN ID を 1～4094 の範囲で指定します。

こんな事に気をつけて

- Si-R180B では、以下の点にご注意ください。
- スイッチポートを使用する場合は、「スイッチ情報」 - [ポート情報] の Tagged VLAN ID または Untagged VLAN ID で設定されている必要があります。
 - スイッチポートをすべて同一のネットワークとして使用する場合は、設定は不要です。その場合、「スイッチ情報」 - [ポート情報] の VLAN ID の設定も不要です。
 - スイッチポートを使用する場合は、Ethernet 上に送出されるパケットのタグの有無はスイッチ情報で設定された内容に従います。VLAN ID が設定されている場合でも、スイッチ情報でタグなしと設定された場合は、タグなしのパケットとして Ethernet 上に送出されます。

プライオリティ

VLAN インタフェースのフレーム送出時に、VLAN タグのプライオリティフィールドに格納される値を 10 進数を使用して 0～7 の範囲で指定します。

シェーピング

シェーピング（リミッタ）機能の設定をします。シェーピング機能を使用する場合は “使用する” を選択し、最大送信レートを指定します。最大送信レートで設定したレートに送信を抑制します。

VRRP 機能

VRRP を使用する場合は、“使用する” を選択します。VRRP を使用するとルータの冗長構成を組むことができます。VRRP を使用しない場合は、以降の設定が無効になります。

パスワード

マスターが送信する Advertisement パケットに認証情報を含める場合に、パスワードを 8 文字以内で指定します。このインターフェースから送信されるすべての Advertisement パケットに適用されます。たとえば、同じネットワークでグループ ID を重複させて別グループとして扱う、などの特別な環境である場合に設定します。

なお、仮想 IP アドレスが IPv6 アドレスである VRRP グループは、パスワードを設定した場合であっても Advertisement パケットに認証情報は含まれません。

TRAP モード

IPv4 VRRP が送信する TRAP モードを選択します。

- 旧仕様
IPv4 VRRP が送信する TRAP モードとして旧仕様 (RFC2787) を使用します。
- 新仕様
IPv4 VRRP が送信する TRAP モードとして新仕様 (draft-ietf-vrrp-unified-mib-06) を使用します。

こんな事に気をつけて

仮想 IP アドレスが IPv6 アドレスである VRRP グループは、“旧仕様”を選択した場合であっても“新仕様”を使用します。

MTU サイズ

最大パケット送信サイズ (Maximum Transmission Unit) を 200～1500 バイトの範囲で指定します。

IPv6 通信で利用する場合は、1280 バイト以上の値を指定します。RIP を利用する場合は、576 バイト以上を指定します。576 バイト未満の MTU サイズを指定すると RIP パケットが送信されない場合があります。

こんな事に気をつけて

VLAN 機能を使用すると、Ethernet フレームに 4 バイトの VLAN タグが付加され、最大 1522 バイトの Ethernet フレームが送出されることになります。通常の Ethernet フレームの最大サイズは 1518 バイトです。そのため、その状態では 1522 バイトのフレームに対応していない機器とは接続することはできません。1522 バイトのフレームに対応していない機器と接続する場合は、VLAN インタフェースの MTU サイズを 1496 に変更してください。

16.2.1.2 VLAN プライオリティマッピング情報

[操作] ルータ設定「LAN 情報 (VLAN)」→ [追加] → [共通情報]
→ [VLAN プライオリティマッピング情報]

■VLANプライオリティマッピング情報

※追加・修正情報は一覧ので設定してください。

定義番号	プロトコル	TOS/Traffic Class	プライオリティ	操作
			<input type="button" value="全削除"/>	
<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	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	TOS/Traffic Class	<input type="text" value=""/>	
プライオリティ			<input type="text" value="0"/>	<input type="button" value="追加"/>
<input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているプライオリティマッピング情報の定義が表示されています。VLAN プライオリティマッピングの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プロトコル

プロトコルを以下の2つから選択します。

- IPv4
- IPv6

TOS/Traffic Class

IPのTOSフィールド値またはIPv6のTraffic Class フィールド値を“any”、または16進数を使用して、0～ffの範囲で指定します。複数の値を指定する場合は、”,”で区切ります。範囲指定の場合は、”-”で区切れます。10組まで指定できます。省略時は“any”が設定されます。

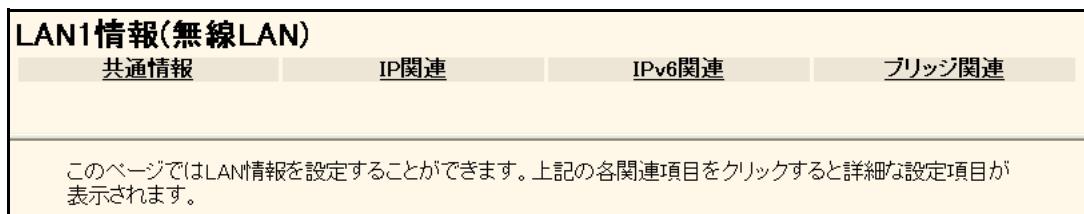
プライオリティ

設定するVLANのプライオリティを10進数を使用して、0～7の範囲で指定します。

16.3 インタフェース：無線 LAN

適用機種 **Si-R240B**

[操作] ルータ設定「LAN 情報（無線 LAN）」→ [追加]



「IP 関連」、「IPv6 関連」および「ブリッジ関連」は、「インターフェース：物理 LAN」を参照してください。

16.3.1 共通情報

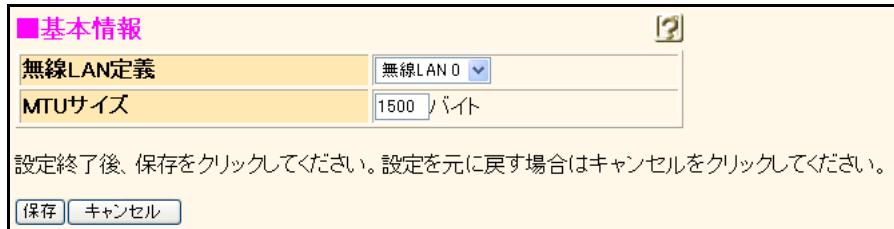
[操作] ルータ設定「LAN 情報（無線 LAN）」→ [追加] → [共通情報]



「LLDP 情報」および「トラップ情報」は、「インターフェース：物理 LAN」を参照してください。

16.3.1.1 基本情報

[操作] ルータ設定「LAN 情報（無線 LAN）」→ [追加] → [共通情報] → [基本情報]



無線 LAN 定義

無線 LAN の回線情報が定義されている無線 LAN 定義番号を選択します。

MTU サイズ

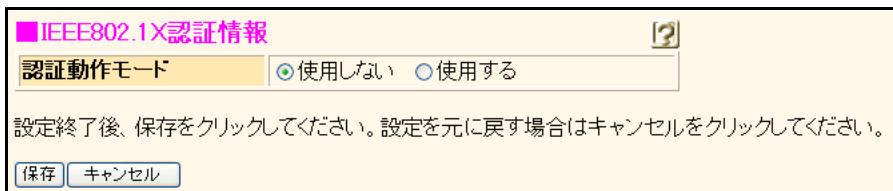
最大パケット送信サイズ (Maximum Transmission Unit) を 200～1500 バイトの範囲の 10 進数で指定します。

IPv6 通信で利用する場合は、1280 バイト以上の値を指定します。

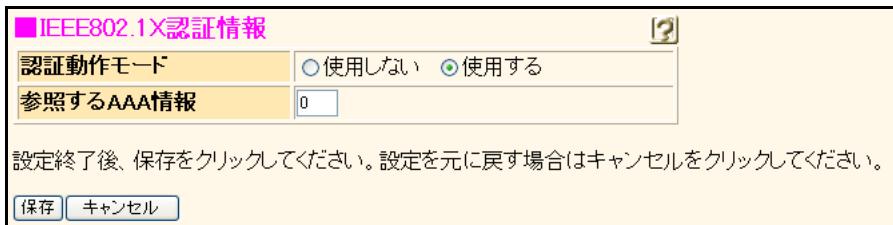
16.3.1.2 IEEE802.1X認証情報

[操作] ルータ設定「LAN 情報（無線 LAN）」→ [追加] → [共通情報] → [IEEE802.1X認証情報]

認証動作モードで、“使用しない”を選択した場合



認証動作モードで、“使用する”を選択した場合



認証動作モード

IEEE802.1X動作モードを選択します。

- 使用しない
IEEE802.1Xを使用しません。
- 使用する
IEEE802.1Xのオーセンティケータ動作を使用します。

こんな事に気をつけて

- IEEE802.1X認証を利用する場合は“IEEE802.1X認証情報”も設定してください。
- 同一LANインターフェースでMACアドレス認証機能との併用はできません。
- 無線LANでは、IEEE802.11認証モードがwpa、wpa2, wpa/wpa2と設定された場合のみIEEE802.1X認証機能が有効となります。その他のモードでは、IEEE802.1X認証機能は有効となりません。

参照する AAA 情報

IEEE802.1X認証を行う場合に参照する AAA 情報のグループIDを指定します。AAAのグループIDを、10未満の10進数で指定します。省略時は、0が設定されます。

17 シリアル情報

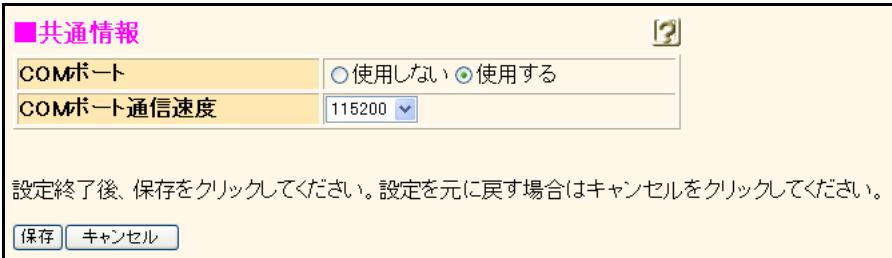
適用機種 **Si-R220C, 220D**

[操作] [詳細設定メニュー] → ルータ設定「シリアル情報」



17.1 共通情報

[操作] [詳細設定メニュー] → ルータ設定「シリアル情報」→ [共通情報]



COM ポート

本装置の COM ポートにモデムを接続して、モデム接続を利用する場合は、“使用する”を選択します。

COM ポート通信速度

COM ポートの通信速度を選択します。

17.2 モデム情報

[操作] [詳細設定メニュー] → ルータ設定「シリアル情報」→ [モデム情報]

■ モデム情報

ダイヤル方式	<input checked="" type="radio"/> トーン式 <input type="radio"/> パルス式	
ダイヤルトーンの検出	<input checked="" type="radio"/> する <input type="radio"/> しない	
スピーカ	モード	キャリア検出までONにする
音量	<input type="radio"/> 小 <input checked="" type="radio"/> 中 <input type="radio"/> 大	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ダイヤル方式

使用するアナログ回線のダイヤル方式を選択します。

ダイヤルトーンの検出

ダイヤルする前にダイヤルトーンを検出する場合は、“する”を選択します。

スピーカ

モード

モデムのスピーカの鳴り方を選択します。

音量

モデムのスピーカの音量を選択します。

18 相手情報

[操作] ルータ設定「相手情報」

相手情報	
ネットワーク情報	着信相手識別情報

Si-R180B、240B、260B では、「着信相手識別情報」は表示されません。

18.1 ネットワーク情報

[適用機種](#) 全機種

[操作] ルータ設定「相手情報」 → [ネットワーク情報]

表示条件入力			
接続先種別	表示個数	表示範囲	
<input type="button" value="全表示"/>	<input type="button" value="10"/>	<input type="button" value="▼"/>	
※ネットワーク情報の表示条件を設定してください。			
■ネットワーク情報			
※追加情報は一覧の最後尾の 追加フィールド で設定してください。 ?			
ネットワーク名 (相手定義番号)	プロトコル	接続先	操作
<input type="button" value="全削除"/>			
<ネットワーク情報追加フィールド>			
ネットワーク名	<input type="text" value="rmt0"/>	<input type="button" value="追加"/>	<input type="button" value="キャンセル"/>
保存した情報は、設定反映後に有効になります。			

現在、設定されている接続相手のネットワーク情報の定義が表示されています。ネットワークの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

表示条件入力

ネットワーク情報の表示条件を接続先種別、表示個数、および表示範囲によって指定することができます。設定することによって、ネットワーク情報の一覧に見たい情報だけを表示させることができます。

ネットワーク名

このネットワークを識別するための名称を8文字以内で指定します。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]

相手情報 - ネットワーク情報(rmt0)

共通情報 接続先情報 PPP関連 IP関連 IPv6関連 ブリッジ関連 MPLS関連

このページではネットワーク情報を設定することができます。
上記の各項目をクリックしてください。詳細な設定項目が表示されます。

18.1.1 共通情報

適用機種 全機種

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[共通情報]

相手情報 - ネットワーク情報(rmt0)

共通情報 接続先情報 PPP関連 IP関連 IPv6関連 ブリッジ関連 MPLS関連

基本情報 トランプ情報

18.1.1.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[共通情報]→[基本情報]

■ 基本情報	
ネットワーク名	rmt0
MTUサイズ	1500 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
シェーピング	最大送信レート <input type="text"/> Mbps

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ルーティングの対象となるネットワークの情報を設定します。

ネットワーク名

このネットワークを識別するための名称を8文字以内で指定します。

MTU サイズ

最大パケット送信サイズ (Maximum Transmission Unit) を 200～1500 バイトの範囲で指定します。IPv6 通信で利用する場合は、1280 バイト以上の値を指定します。

また、IPv6 トンネル (IPv6 over IPv4) を利用する場合は、1280 バイトを指定します。

PPPoE (PPP over Ethernet) を利用する場合は、1454 バイトを指定します。

ブリッジを利用する場合は、1500 バイトを指定します。1500 未満を指定すると、正しくブリッジ通信ができない場合があります。

RIP を利用する場合は、576 バイト以上を指定します。576 バイト未満の MTU を指定すると、RIP パケットが送信されない場合があります。

自動接続

データ通信発生時に自動的に接続する場合は、“使用する”を選択します。

こんな事に気をつけて

使用するインターフェースの設定 (WAN 接続) で自動接続をすべて禁止している場合は、自動接続を行うことができません。

シェーピング

シェーピング (リミッタ) 機能を設定します。シェーピング機能を使用する場合は“使用する”を選択し、最大送信レートを指定します。最大送信レートで設定したレートに送信を抑制します。

最大送信レート

最大送信レートを以下の範囲で指定します。Kbps は 1000bps を、Mbps は 1000Kbps を意味します。

機種	最大送信レート
Si-R570、570B 以外	1～100000Kbps
Si-R570、570B	1～1000000Kbps

こんな事に気をつけて

- ・ シェーピング機能は、以下の接続先種別では動作しません。
 - ISDN
 - フレームリレー
 - モデム
 - IP トンネル
 - データ通信カード
- ・ 回線に LAN を使用して、帯域制御機能を有効に動作させる場合は、シェーピングを“使用する”に設定してください。

18.1.1.2 トラップ情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [共通情報] → [トラップ情報]

■トラップ情報	
linkDown	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
linkUp	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

トラップ情報

SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP 機能を利用しない場合、および旧バージョン互換 MIB モードで利用する場合は、この設定は意味を持ちません。

- linkDown
linkDown トラップを通知します。
- linkUp
linkUp トラップを通知します。

18.1.2 接続先情報

適用機種 全機種

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]



[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]→[接続先情報]

《接続先は、各ネットワークの合計で 1000箇所まで設定できます。》

■接続先情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

優先順位	接続先名 (接続先定義番号)	種別	操作
全削除			
<接続先情報追加フィールド>			
接続先種別	ap0-0		
	<input type="radio"/> ATM接続 VCI <input type="text"/> <input type="radio"/> 専用線接続 <input checked="" type="radio"/> 通常接続 使用インターフェース <input type="button" value="WAN1"/> <input type="radio"/> 論理リンクにバンドルする 使用インターフェース <input type="button" value="WAN1"/> バンドル先 <input type="button" value="選択できる定義がありません"/> <input type="radio"/> ISDN接続 <input checked="" type="radio"/> 通常接続 使用インターフェース <input type="button" value="すべて"/> 電話番号 <input type="text"/> ダイヤル1 <input type="text"/> サブアドレス <input type="text"/> <input type="radio"/> 論理リンクにバンドルする 使用インターフェース <input type="button" value="すべて"/> バンドル先 <input type="button" value="選択できる定義がありません"/> <input type="radio"/> フレームリレー接続 DLCI <input type="text"/> <input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSトンネル接続 <input checked="" type="radio"/> パケット破棄		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

保存した情報は、設定反映後に有効になります。

現在、設定されている接続先情報の定義が表示されています。マルチルーティングを行う場合は、優先順位の1から順に評価され最初に条件が成立した接続先にデータが流れます。接続先の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

選択する接続種別によって、表示が異なります。

Si-R370、370B、570、570B 以外では、接続先種別の表示が、上記の画面とは異なります。

接続先名

この接続先を識別するための名称を8文字以内で指定します。

接続先種別

この接続先の種別を以下から選択します。

- ATM 接続 (Si-R260B、370、570)

ATM 回線を使用して接続する場合に選択します。使用するには WAN 情報で ATM 回線を設定してください。

VCI

契約時に割り当てられた VC の VCI 値を10進数を使用して指定します。指定可能な範囲は以下のとおりです。

有効範囲

ATM25M 拡張モジュール L2 (Si-R260B、370、570)
: 32 ~ 4095

ATM155M 拡張モジュール L2 (Si-R370、570)
: 32 ~ 2047

ATM25M 拡張モジュール H1 (Si-R570)
: 32 ~ 1023

ATM155M 拡張モジュール H1 (Si-R570)
: 32 ~ 1023

- 専用線接続 (Si-R220C、220D、370、370B、570、570B)
専用線回線を使用して接続する場合に選択します。使用するには WAN 情報で専用線回線を設定してください。
専用線の運用方法を“通常接続”または“論理リンクにバンドルする”から選択します。

通常接続

専用線を単独または論理リンクのマスタ回線で運用する場合に選択します。

論理リンクにバンドルする

専用線を論理リンクのバンドル回線として運用する場合に選択します。この場合、マスタ回線として運用する専用線をバンドル先として指定します。

使用インターフェース

専用線接続で使用する WAN インタフェースを選択します。

バンドル先

論理リンクにバンドルする回線として使用する場合にバンドル先の接続先を選択します。

- ISDN 接続 (Si-R220C、220D、370、370B、570、570B)
ISDN 回線を使用して接続する場合に選択します。使用するには WAN 情報で ISDN 回線を設定してください。
ISDN 接続の運用方法を“通常接続”または“論理リンクにバンドルする”から選択します。

通常接続

ISDN 回線を単独で運用する場合に選択します。

論理リンクにバンドルする

ISDN 回線を論理リンクのバンドル回線として運用する場合に選択します。この場合、マスタ回線として運用する専用線をバンドル先として指定します。

使用インターフェース

ISDN 接続で使用する WAN インタフェースを選択します。

ダイヤル1

接続に使用する電話番号を指定します。本装置では、複数の電話番号を指定できますが、それは「接続先情報」 - 「基本情報」で設定します。着信時には自動認識します。電話番号は32桁以内、サブアドレスは19桁以内で指定します。

バンドル先

論理リンクにバンドルする回線として使用する場合にバンドル先の接続先を選択します。

- フレームリレー接続
(Si-R220C、220D、370、370B、570、570B)
フレームリレー回線を使用して接続する場合に選択します。使用するには WAN 情報でフレームリレー回線を設定してください。

DLCI

DLCI を10進数を使用して16~991の範囲で指定します。DLCI を設定できるネットワーク数は、仕様一覧「[2.1 ソフトウェア仕様](#)」(P.34) を参照してください。DLCI は、フレームリレーを使用するときに1本の物理回線上に設定される複数の論理的な通信路（データリンク）を識別するための識別子です。

- モデム接続 (Si-R220C、220D)

モデムを使用して接続する場合に選択します。

- データ通信カード接続 (Si-R240B)
データ通信カードを使用して接続する場合に選択します。

ダイヤル1

接続に使用する電話番号を指定します。本装置では、複数の電話番号を指定できますが、それは「接続先情報」 - 「基本情報」で設定します。
電話番号は32桁以内で指定します。

- PPPoE 接続
PPPoE を使用して接続する場合に選択します。使用するには LAN 情報を設定してください。
- IP トンネル接続
IP トンネルを使用して接続する場合に選択します。IP トンネルに使用する IPv6 または IPv4 の設定は別の LAN 情報または相手情報で設定します。
- IPsec/IKE 接続
IPsec/IKE トンネルを使用して接続する場合に選択します。IPsec/IKE トンネルに使用する IPv4 と IPv6 の設定は別の相手情報で設定します。
- 別インターフェースから送出
パケット送出先として別インターフェースを使用して接続する場合に選択します。
- MPLS トンネル接続
MPLS トンネルを使用して接続する場合に選択します。
- パケット破棄
送信するパケットをすべて破棄する場合に選択します。

18.1.2.1 接続先種別：ATM 接続

適用機種 **Si-R260B, 370, 570**

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (ATM 接続)]→[追加]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-1)

ATM接続		
基本情報	接続制御情報	マルチルーティング情報
トラップ情報		

18.1.2.1.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (ATM 接続)]→[追加]→[基本情報]

■ 基本情報

接続先名	ap0-0
使用インターフェース	WAN0
VCI	32
VC速度	Kbps
サービスタイプ	<input checked="" type="radio"/> CBR <input type="radio"/> VBR 平均速度値 Kbps 最大バースト長 <input type="radio"/> UBR+ 最低速度値 Kbps <input type="radio"/> GFR+ 保証速度値 Kbps
OAM(F5)	<input checked="" type="radio"/> 受け付けない <input type="radio"/> 受け付ける
到達性監視	<input checked="" type="radio"/> 行わない <input type="radio"/> 行う 間隔 秒 再確認回数 回

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

Si-R260B、370では、“到達性監視”の設定項目は表示されません。

接続先名

この接続先を識別するための名称を8文字以内で指定します。

使用インターフェース

ATM接続で使用するWANインターフェースを選択します。
あらかじめWAN情報でATM回線インターフェースの設定をしておく必要があります。

VCI

契約時に割り当てられた、VC の VCI 値を 10 進数を使用して指定します。

指定可能な範囲は以下のとおりです。

有効範囲)

ATM25M (Si-R260B)

: 32 ~ 4095

ATM25M 拡張モジュール L2 (Si-R370、570)

: 32 ~ 4095

ATM155M 拡張モジュール L2 (Si-R370、570)

: 32 ~ 2047

ATM25M / ATM155M 拡張モジュール H1 (Si-R570)

: 32 ~ 1023

VC 速度

VC の契約速度を以下の範囲で指定します。

機種	拡張モジュール	VC 速度
Si-R570	ATM25M 拡張モジュール L2	64Kbps ~ 25Mbps (8Kbps 刻み、または 50Kbps 刻み)
	ATM155M 拡張モジュール L2	
	ATM25M 拡張モジュール H1	
Si-R370	ATM155M 拡張モジュール H1	64Kbps ~ 100Mbps (8Kbps 刻み、または 50Kbps 刻み)
	ATM25M 拡張モジュール L2	64Kbps ~ 25Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R260B	-	

サービスタイプ

VC のサービスタイプを以下の 4 つから選択します。

- CBR
速度保証契約または一部保証契約で最低速度保証の場合に選択します。
- VBR
平均的速度保証またはバースト長を指定する必要がある場合に選択します。
- UBR+
一部保証契約で最低速度保証の場合に選択します。
- GFR+
一部保証契約で最低速度保証の場合に選択します。

平均速度値

サービスタイプとして VBR を選択した場合、設定可能な速度は以下の範囲です。省略時は、VC 速度の範囲で自動設定されます。

機種	拡張モジュール	VC 速度
Si-R570	ATM25M 拡張モジュール L2	64Kbps ~ 25Mbps (8Kbps 刻み、または 50Kbps 刻み)
	ATM155M 拡張モジュール L2	
	ATM25M 拡張モジュール H1	
Si-R370	ATM155M 拡張モジュール H1	64Kbps ~ 100Mbps (8Kbps 刻み、または 50Kbps 刻み)
	ATM25M 拡張モジュール L2	64Kbps ~ 25Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R260B	-	

最大バースト長

サービスタイプとして VBR を選択した場合、連続送信を許可するセル数を最大バースト長として指定できます。最大バースト長は、1 ~ 1400 の範囲で指定できます。省略時は、自動的に設定されます。

最低速度値／保証速度値

サービスタイプとして UBR+ または GFR+ を選択した場合、設定可能な速度は以下の範囲です。省略時は、VC 速度の範囲で自動設定されます。

機種	拡張モジュール	VC 速度
Si-R570	ATM25M 拡張モジュール L2	64Kbps ~ 25Mbps (8Kbps 刻み、または 50Kbps 刻み)
	ATM155M 拡張モジュール L2	
	ATM25M 拡張モジュール H1	
Si-R370	ATM155M 拡張モジュール H1	64Kbps ~ 100Mbps (8Kbps 刻み、または 50Kbps 刻み)
	ATM25M 拡張モジュール L2	64Kbps ~ 25Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R260B	-	

こんな事に気をつけて

平均速度値、最低速度値および保証速度値は、VC 速度を超えない値を設定する必要があります。

OAM (F5)

VC 単位で故障を検出する必要がある場合に、“受け付ける”を選択することによって、VC 単位での故障が検出できます。

到達性監視 (Si-R570)

ATM レイヤで到達性監視を行う場合に、“行う”を選択します。到達性確認には、OAM (5) を使用します。“行う”を選択した場合は、間隔ごとに到達性を確認し、応答がなければ再確認します。再確認回数連続して応答がない場合は、応答が確認されるまで該当 VC を使用しない状態に移行します。“行う”を選択した場合、以降の項目を設定します。なお、到達性監視は、ATM25M 拡張モジュール H1 または ATM155M 拡張モジュール H1 に対してのみ有効です。

間隔

到達性を確認する間隔を 3～10 秒の範囲で指定します。
省略時は、3 秒が設定されます。

再確認回数

到達性確認に対して応答がなかった場合の再確認回数を 1～20 回の範囲で指定します。省略時、5 回が設定されます。

18.1.2.1.2 接続制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (ATM 接続)]→[追加]→[接続制御情報]

接続先監視

接続先の生存確認を行うための動作情報を選択します。指定したあて先IPアドレスにICMP ECHOパケットを送信します。タイムアウト時間までに応答がない場合に、この接続先を使用できない状態にします。その後、異常時送信間隔ごとにICMP ECHOパケットを送信し、接続先の復旧を待ち、復旧後にこの接続先を使用できる状態にします。

送信元IPアドレス

ICMP ECHOパケットの送信元IPアドレスとして、本装置に設定している自側IPv4/IPv6アドレスのどれかを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

あて先IPアドレス

監視対象となる接続先のIPv4/IPv6アドレスを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

正常時送信間隔

ICMP ECHOパケットの応答が正常に受信されている状態で、ICMP ECHOパケットを次に送信する間隔を、10進数を使用して1～60秒の範囲で指定します。

再送間隔

ICMP ECHOパケットの正常時の送信に対して応答がない場合、ICMP ECHOパケットを再送する間隔を、10進数を使用して1～(タイムアウト時間-1)秒の範囲で指定します。省略時は、1秒が設定されます。

タイムアウト時間

ICMP ECHOパケットの送信から生存確認失敗とするまでの時間を、10進数を使用して5～180秒の範囲で指定します。タイムアウト時間までに応答がない場合、監視対象との接続に障害が発生したとみなし、この接続先を使用できない状態にします。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから、接続先の障害が復旧し応答が受信されるまでの間、ICMP ECHO パケットを送信する間隔を、10進数を使用して 60 ~ 600 秒の範囲で指定します。

送信 TTL/HopLimit

ICMP ECHO パケットを送信するときの IP TTL 値を、1 ~ 255 の範囲で指定します。省略時は、255 が設定されます。

連続応答受信回数

異常状態から正常状態へ復旧するために必要な連続応答受信回数を、10進数を使用して 1 ~ 100 の範囲で指定します。省略時は、1 が設定されます。

異常時送信開始待ち時間

正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を指定します。0 秒を指定した場合は、待ち合わせをしません。省略時は、0 秒が設定されます。

有効範囲)

0 ~ 86400 秒

0 ~ 1440 分

0 ~ 24 時間

0 ~ 1 日

監視方式

監視方式を以下の 2 つから選択します。

- 常時監視

常時、監視を行います。

- 無通信時監視

無通信時に、監視を行います。

18.1.2.1.3 マルチルーティング情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (ATM 接続)] → [追加] → [マルチルーティング情報]

■マルチルーティング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	プロトコル	送信元IPアドレス/マスク 送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号	TOS	操作
<input type="button" value="全削除"/>					

<マルチルーティング情報入力フィールド>

動作	<input type="text" value="この接続先を使用する"/>
プロトコル	<input type="text" value="すべて (番号指定: 1~255)"/>
送信元情報	<input type="text" value="IPアドレス
マスク
ポート番号"/>
あて先情報	<input type="text" value="IPアドレス
マスク
ポート番号"/>
TOS	<input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているマルチルーティング情報の定義が表示されています。処理は優先順位1から順に行われます。マルチルーティングの定義は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。

動作

マルチルーティングの動作を以下の3つから選択します。

- 使用する
条件と一致した場合に、この接続先を使用します。
- 使用しない
条件と一致した場合に、この接続先を使用しません。
- バックアップとして使用する
条件と一致し、以降の接続先を使用することができない場合に、この接続先を使用します。

プロトコル

マルチルーティング条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1~255の範囲で指定します。

送信元／あて先情報

マルチルーティング条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

マルチルーティング条件としてのIP アドレスおよびアドレスマスクを指定します。チェック対象となったパケットのIP アドレスと定義したアドレスマスクの論理積と、定義したIP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

マルチルーティング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定した場合は、すべてのポート番号がマルチルーティングの対象となります。また、ポート番号を複数指定する場合は“,”で区切れます。範囲指定の場合は“-”で区切れます。送信元情報とあて先情報で合わせて10組まで指定できます。

18.1.2.1.4 トラップ情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (ATM 接続)] → [追加] → [トラップ情報]

■トラップ情報	
linkDown	<input type="radio"/> 有効にする <input checked="" type="radio"/> 無効にする
linkUp	<input type="radio"/> 有効にする <input checked="" type="radio"/> 無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

トラップ情報

SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP 機能を利用しない場合、および旧バージョン互換 MIB モードで利用する場合は、この設定は意味を持ちません。

- linkDown
linkDown トラップを通知します。
- linkUp
linkUp トラップを通知します。

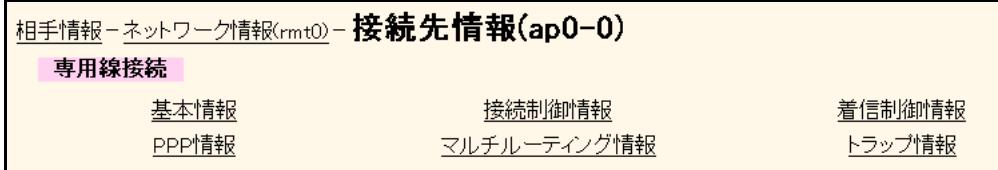
TOS

マルチルーティング条件としてIP パケットのTOS フィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOS フィールド値を複数指定する場合は“,”で区切れます。範囲指定の場合は“-”で区切れます。10組まで指定できます。何も設定しない場合はすべてのTOS フィールド値をマルチルーティングの対象とします。

18.1.2.2 接続先種別：専用線接続

適用機種 **Si-R220C, 220D, 370, 370B, 570, 570B**

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(専用線接続)]→[追加]

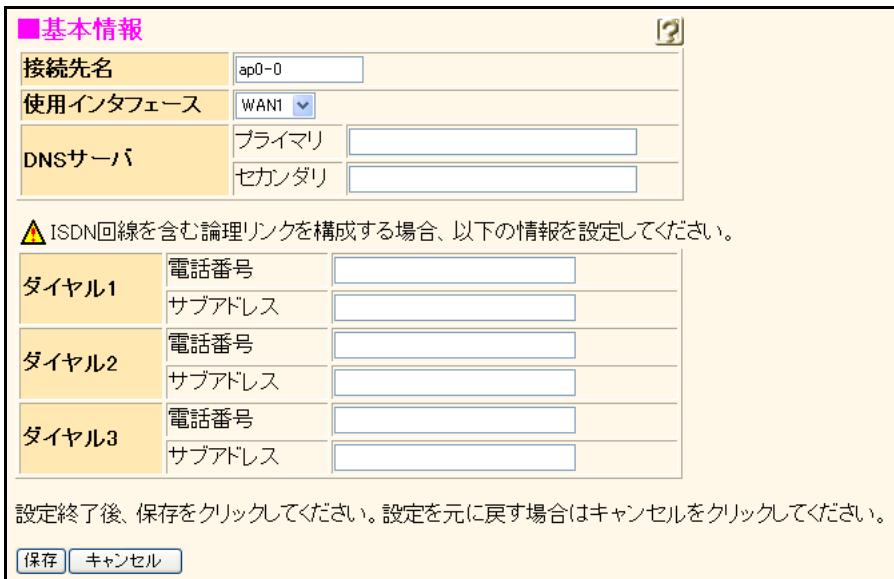


Si-R220C、220D では、「着信制御情報」は表示されません。

「マルチルーティング情報」および「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.2.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(専用線接続)]→[追加]→[基本情報]



Si-R220C、220D では、“ダイヤル1／2／3”的設定項目は表示されません。単回線のみの設定になります。

接続先名

この接続先を識別するための名称を8文字以内で指定します。

使用インターフェース

専用線接続で使用するWANインターフェースを選択します。あらかじめWAN情報で専用線インターフェースの設定をしておく必要があります。

DNS サーバ

接続の際に使用するDNSサーバのIPアドレスを指定します。ProxyDNS機能を使用する際に必要です。省略するか0.0.0.0を指定した場合は、自動取得となります。プライマリのみを省略することはできません。255.255.255.255を指定した場合は、DNSサーバは使用しません。また、このIPアドレスはPPPのネゴシエーションの中で相手から要求があった場合、相手に受け渡すDNSサーバアドレスとしても使用します。

ダイヤル1／2／3 (Si-R370、370B、570、570B)

接続に用いる電話番号は3つまで指定できます。ダイヤル1の電話番号にかかるときにはダイヤル2に、ダイヤル2がかかるときはダイヤル3の電話番号にダイヤルします。着信時には自動認識します。電話番号は32桁以内、サブアドレスは19桁以内で指定します

18.1.2.2.2 接続制御情報

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「接続先情報（専用線接続）」→「追加」→「接続制御情報」

常時接続機能で、“使用しない”を選択した場合

■接続制御情報		
接続 先監 視	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	送信元IPアドレス	<input type="text"/>
	あて先IPアドレス	<input type="text"/>
	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	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	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視	
△ 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。		
常時接続 機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
無通信監 視タイム	送受信パケット <input type="button"/> について 0 秒	
課金単位 時間	昼間(月～金) (08:00～19:00) <input type="text"/> 0 秒 夜間(土日の昼間) (19:00～23:00) <input type="text"/> 0 秒 深夜・早朝 (23:00～08:00) <input type="text"/> 0 秒	
発信抑止	<input type="checkbox"/> 指定した時間を超えて接続しない 累計: <input type="text"/> 時間 <input type="checkbox"/> 指定した課金を超えて接続しない 累計: <input type="text"/> 円	
接続優先 制御	<input checked="" type="radio"/> 使用しない <input type="radio"/> 発信を優先する <input type="radio"/> 着信を優先する	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button"/> 保存 <input type="button"/> キャンセル		

常時接続機能で、" 使用する " を選択した場合

The screenshot shows the 'Connection Control Information' configuration page. On the left, there's a vertical sidebar labeled '接続先監視' (Connection Target Monitoring). The main area has a title '■接続制御情報' (Connection Control Information) and contains several configuration fields:

- 送信元IPアドレス:** A text input field.
- あて先IPアドレス:** A text input field.
- 正常時送信間隔:** A dropdown menu set to '10 秒'.
- 再送間隔:** A dropdown menu set to '1 秒'.
- タイムアウト時間:** A dropdown menu set to '5 秒'.
- 異常時送信間隔:** A dropdown menu set to '1 分'.
- 送信 TTL/HopLimit:** A text input field set to '255'.
- 連続応答受信回数:** A text input field set to '1'.
- 異常時送信開始待ち時間:** A dropdown menu set to '0 秒'.
- 監視方式:** A radio button group with '常時監視' (Always Monitor) selected.

Below these fields, a note says: '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。' (When configuring logical links including ISDN lines, please set the following information.)

At the bottom, there are two radio buttons: '常時接続機能' (Always Connection Function) (selected) and '使用しない' (Do not use).

At the very bottom, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel).

Si-R220C、220D では、" 常時接続機能 " 以降の設定項目は表示されません。単独回線のみの設定になります。

接続先監視

接続先の生存確認を行うための動作情報を選択します。指定したあて先IPアドレスにICMP ECHOパケットを送信します。タイムアウト時間までに応答がない場合に、この接続先を使用できない状態にします。その後、異常時送信間隔ごとにICMP ECHOパケットを送信し、接続先の復旧を待ち、復旧後にこの接続先を使用できる状態にします。

送信元IPアドレス

ICMP ECHOパケットの送信元IPアドレスとして、本装置に設定している自側IPv4/IPv6アドレスのどれかを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

あて先IPアドレス

監視対象となる接続先のIPv4/IPv6アドレスを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

正常時送信間隔

ICMP ECHOパケットの応答が正常に受信されている状態で、ICMP ECHOパケットを次に送信する間隔を、10進数を使用して1～60秒の範囲で指定します。

再送間隔

ICMP ECHOパケットの正常時の送信に対して応答がない場合、ICMP ECHOパケットを再送する間隔を、10進数を使用して1～(タイムアウト時間-1)秒の範囲で指定します。省略時は、1秒が設定されます。

タイムアウト時間

ICMP ECHO パケットの送信から生存確認失敗とするまでの時間を、10進数を使用して 5～180 秒の範囲で指定します。タイムアウト時間までに応答がない場合、監視対象との接続に障害が発生したとみなし、この接続先を使用できない状態にします。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから、接続先の障害が復旧し応答が受信されるまでの間、ICMP ECHO パケットを送信する間隔を、10進数を使用して 60～600 秒の範囲で指定します。

送信 TTL/HopLimit

ICMP ECHO パケットを送信するときの IP TTL 値を、1～255 の範囲で指定します。省略時は、255 が設定されます。

連続応答受信回数

異常状態から正常状態へ復旧するために必要な連続応答受信回数を、10進数を使用して 1～100 の範囲で指定します。省略時は、1 が設定されます。

異常時送信開始待ち時間

正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を指定します。0 秒を指定した場合は、待ち合わせをしません。省略時は、0 秒が設定されます。

有効範囲)

0～86400 秒

0～1440 分

0～24 時間

0～1 日

監視方式

監視方式を以下の 2 つから選択します。

- 常時監視
常時、監視を行います。
- 無通信時監視
無通信時に、監視を行います。

常時接続機能

(Si-R370、370B、570、570B)

“使用する”を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。また、相手から切断された場合や回線エラーによる切断が行われた場合は、自動で再接続します。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。

無通信監視タイマ

(Si-R370、370B、570、570B)

無通信監視タイマを 0～3600 秒の範囲で指定します。ここで指定した時間、監視対象となるパケットが存在しなかつた場合は、自動的に切断します。なお、省略、または 0 を指定した場合、自動切断を行いません。

課金単位時間

(Si-R370、370B、570、570B)

各時間帯の課金単位時間を 0.0～3600.0 秒の範囲で指定してください。

ここで設定した時間は無通信監視による回線切断のときに参照され、同一料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、昼間時間帯に 0 を設定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に 0 を設定した場合、その前の時間帯の設定を利用します。

こんな事に気をつけて

この機能を使用するときは、操作メニューの時刻設定を用いて本装置の時刻を正しく設定してください。時刻が正しく設定されていない場合、課金単位時間は昼間の値のみが使われます。また、祝祭日には対応していません。

発信抑止

(Si-R370、370B、570、570B)

この接続先に対する発信抑制を接続時間と課金によって行うことができます。発信抑制を行う場合は、各行頭のチェックボックスをチェックし、時間は 1 秒～999 時間、金額は 1～999999 円の範囲で指定します。チェックボックスをチェックした場合、時間および金額の省略はできません。

接続優先制御 (Si-R370、370B、570、570B)

“発信を優先する”を選択すると、発信接続と着信接続が競合した場合に、発信接続を残し着信接続を切断します。“着信を優先する”を選択すると、発信接続と着信接続が競合した場合に、着信接続を残し発信接続を切断します。

こんな事に気をつけて

自装置と接続相手装置の両方で接続優先制御を行う場合は、それぞれ異なる優先方法を選択してください。同じ優先制御を行うと接続できない場合があります。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。

18.1.2.2.3 着信制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(専用線接続)]
→[追加]→[着信制御情報]

■着信制御情報 [?] ▲

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。

着信許可	<input type="radio"/> 許可しない <input checked="" type="radio"/> 許可する <input type="radio"/> 番号チェックしない <input checked="" type="radio"/> 接続先電話番号でチェックする <input type="radio"/> 指定する接続先電話番号でチェックする 相手電話番号: _____ 相手サブアドレス: _____
発信者番号による識別	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

着信許可

この接続先からの着信を許可する場合は、“許可する”を選択します。

発信者番号による識別

着信時の相手識別の方法には、発信者番号通知を用いる方法と、認証IDを用いる方法があります。

- 番号チェックをしない
発信者番号による相手識別は行いません。
- 接続先電話番号でチェックする
発信者番号通知を用いて相手を識別します。この場合「基本情報」で設定した電話番号で相手を識別します。
- 指定する接続先電話番号でチェックをする
相手識別のために相手電話番号および相手サブアドレスを指定します。電話番号は32桁以内、サブアドレスは19桁以内で指定します。

18.1.2.2.4 PPP情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (専用線接続)]
→ [追加] → [PPP情報]

MP接続	<input checked="" type="radio"/> しない <input type="radio"/> する
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。	
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
送信認証情報	認証ID 認証パスワード
受諾認証情報	認証ID 認証パスワード
BAP/BACP利用	<input checked="" type="radio"/> しない <input type="radio"/> する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

Si-R220C、220D では、“認証方式”以降の設定項目は表示されません。単独回線のみの設定になります。

MP接続

MP接続を行う場合は、“する”を選択します。

こんな事に気をつけて

Si-R370、370B、570、570B で論理リンクを構成する場合、MP接続の設定は必ず“する”を選択してください。

認証方式 (Si-R370、370B、570、570B)

着信時に利用する認証プロトコルを選択します。どちらも指定しない場合は、その相手からの着信は認証しません。ただし、発信者番号による識別が行われなかった相手からの着信については、「相手情報」 - 「着信相手識別情報」の設定が参照されます。発信者番号による識別は、「着信制御情報」で設定できます。

送信確認情報 (Si-R370、370B、570、570B)

発信時に使用する認証IDを64桁以内、認証パスワードを64桁以内で指定します。

受諾認証情報 (Si-R370、370B、570、570B)

着信時に受け付ける認証IDを64桁以内、認証パスワードを64桁以内で指定します。発信者番号による識別は「着信制御情報」で設定できます。

BAP/BACP利用 (Si-R370、370B、570、570B)

BAP/BACPを利用する場合は、“する”を選択します。ただし、発信者番号による識別が行われなかった相手からの着信については、「相手情報」 - 「着信相手識別情報」の設定が参照されます。発信者番号による識別は、「着信制御情報」で設定できます。

18.1.2.3 接続先種別：専用線（バンドル）接続

適用機種 Si-R370,370B,570,570B

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加]
→ [接続先情報（専用線接続、バンドル）] → [追加]

相手情報 - ネットワーク情報(rmt0) - **接続先情報(1)**

専用線接続(「バンドル」)

基本情報

18.1.2.3.1 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加]
→ [接続先情報（専用線接続、バンドル）] → [追加] → [基本情報]

■ 基本情報	
使用インターフェース	WAN1
バンドル先	ap0-0 (0)
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
保存	キャンセル

使用インターフェース

専用線接続で使用する WAN インタフェースを選択します。あらかじめ WAN 情報で専用線インターフェースの設定をしておく必要があります。

バンドル先

論理リンクにバンドルする回線として使用するバンドル先の接続先を選択します。

18.1.2.4 接続先種別：ISDN 接続

適用機種 **Si-R220C, 220D, 370, 370B, 5570, 570B**

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (ISDN 接続)]→[追加]



「マルチルーティング情報」、「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.4.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (ISDN 接続)]→[追加]→[基本情報]

接続先名	ap0-0
使用インターフェース	WAN0
ダイヤル1	電話番号 サブアドレス 相手種別 ISDN
ダイヤル2	電話番号 サブアドレス 相手種別 ISDN
ダイヤル3	電話番号 サブアドレス 相手種別 ISDN
DNSサーバ	プライマリ セカンダリ

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

Si-R370、370B、570、570B では、「相手種別」の設定項目は表示されません。

接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前は手動接続の際にも使用されます。

使用インターフェース

ISDN 接続で使用する WAN インタフェースを選択します。あらかじめ WAN 情報で ISDN 回線インターフェースの設定をしておく必要があります。

ダイヤル1／2／3

接続に使用する電話番号は3つまで指定できます。ダイヤル1の電話番号にかかるときにはダイヤル2に、ダイヤル2の電話番号にかかるときにはダイヤル3にダイヤルします。着信時には自動認識します。電話番号は32桁以内、サブアドレスは19桁以内で指定します。

相手種別は発信時にのみ参照されます。接続先の通信速度、および、通信手順を選択します。なお、64kPIAFS 着信時には、設定したサブアドレスは無視されます。

DNS サーバ

接続の際に使用する DNS サーバの IP アドレスを指定します。ProxyDNS 機能を使用する際に必要です。省略するか 0.0.0.0 を指定した場合は、自動取得となります。プライマリのみを省略することはできません。255.255.255.255 を指定した場合は、DNS サーバは使用しません。また、この IP アドレスは PPP のネゴシエーションの中で相手から要求があった場合、相手に受け渡す DNS サーバアドレスとしても使用します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

18.1.2.4.2 接続制御情報

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」 → 「接続先情報 (ISDN 接続)」 → 「追加」 → 「接続制御情報」

常時接続機能で、“使用しない”を選択した場合

■接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイム	送受信パケット <input type="button" value="▼"/> について <input type="text" value="0"/> 秒
課金単位時間	曜間(月～金) (08:00～19:00) <input type="text" value="0"/> 秒 夜間(土日の昼間) (19:00～23:00) <input type="text" value="0"/> 秒 深夜・早朝 (23:00～08:00) <input type="text" value="0"/> 秒
発信抑止	<input type="checkbox"/> 指定した時間を超えて接続しない、累計: <input type="text"/> 時間 <input type="button" value="▼"/> <input type="checkbox"/> 指定した課金を超えて接続しない、累計: <input type="text"/> 円
接続優先制御	<input checked="" type="radio"/> 使用しない <input type="radio"/> 発信を優先する <input type="radio"/> 着信を優先する
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

常時接続機能で、" 使用する " を選択した場合

■接続制御情報

常時接続機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
接続先監視	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
送信元IPアドレス <input type="text"/> あて先IPアドレス <input type="text"/> 正常時送信間隔 <input type="text"/> 秒 <input type="button" value="▼"/> 再送間隔 <input type="text"/> 秒 <input type="button" value="▼"/> タイムアウト時間 <input type="text"/> 秒 <input type="button" value="▼"> 異常時送信間隔 <input type="text"/> 分 <input type="button" value="▼"> 送信 TTL/HopLimit <input type="text"/> 255 連続応答受信回数 <input type="text"> 1 異常時送信開始待ち時間 <input type="text"/> 秒 <input type="button" value="▼"> 監視方式 <input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視 </input></input></input></input>	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

常時接続機能

" 使用する " を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。相手から切断された場合や回線エラーによって切断された場合は、自動で再接続します。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。

また、" 使用する " を選択すると、表示される画面が変わります。設定項目については、[ATM 接続] の「接続制御情報」を参考に設定します。使用しない場合は、以下の項目を設定します。

無通信監視タイマ

無通信監視タイマを0～3600秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または0を指定した場合、自動切断を行いません。

課金単位時間

各時間帯の課金単位時間を0.0～3600.0秒の範囲で指定します。ここで設定した時間は無通信監視による回線切断のときに参照され、同じ料金でもっとも接続時間が長くなるように回線切断タイミングを調整します。なお、昼間時間帯に0を設定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に0を設定した場合、その前の時間帯の設定を利用します。

こんな事に気をつけて

この機能を使用する場合は、操作メニューの時刻設定を使用して本装置の時刻を正しく設定してください。時刻が正しく設定されていない場合、課金単位時間は昼間の値だけが使用されます。祝祭日には対応していません。

発信抑止

この接続先に対する発信抑制を接続時間と課金によって行うことができます。

発信抑制を行う場合は、各行頭のチェックボックスをチェックし、時間は1秒～999時間、金額は1～999999円の範囲で指定します。チェックボックスをチェックした場合、時間および金額の省略はできません。

接続優先制御

- 使用しない
接続優先制御は行いません。
- 発信を優先する
発信接続と着信接続が競合した場合に、発信接続を残し着信接続を切断します。
- 着信を優先する
発信接続と着信接続が競合した場合に、着信接続を残し発信接続を切断します。

こんな事に気をつけて

自装置と接続相手装置の両方で接続優先制御を行う場合は、それぞれ異なる優先方法を選択してください。同じ優先制御を行うと接続できない場合があります。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。

18.1.2.4.3 着信制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (ISDN 接続)]→[追加]→[着信制御情報]

■着信制御情報	
発信者番号による識別	<input type="radio"/> 許可しない <input checked="" type="radio"/> 許可する
	<input type="radio"/> 番号チェックしない
	<input checked="" type="radio"/> 接続先電話番号でチェックする
	<input type="radio"/> 指定する接続先電話番号でチェックする
相手電話番号	<input type="text"/>
相手サブアドレス	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

着信許可

この接続先からの着信を許可する場合は、“許可する”を選択します。

発信者番号による識別

着信時の相手識別には、発信者番号通知を用いる方法と、認証IDを用いる方法があります。

- 番号チェックをしない
発信者番号による相手識別は行いません。
- 接続先電話番号でチェックする
発信者番号通知を用いて相手を識別します。この場合「基本情報」で設定した電話番号で相手を識別します。
- 指定する接続先電話番号でチェックをする
相手識別のために相手電話番号および相手サブアドレスを指定します。電話番号は32桁以内、サブアドレスは19桁以内で指定します。

18.1.2.4.4 PPP情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (ISDN接続)] → [追加] → [PPP情報]

■PPP情報

認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
送信認証情報	認証ID 認証パスワード
受諾認証情報	認証ID 認証パスワード
MP接続	<input checked="" type="radio"/> しない <input type="radio"/> する BAP/BACP利用 <input checked="" type="radio"/> しない <input type="radio"/> する <small>※ 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</small>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

認証方式

着信時に利用する認証プロトコルを選択します。どちらも指定しない場合は、その相手からの着信は認証しません。ただし、発信者番号による識別が行われなかった相手からの着信については、「相手情報」 - 「着信相手識別情報」の設定が参照されます。発信者番号による識別は、「着信制御情報」で設定できます。

送信確認情報

発信時に使用する認証IDを64桁以内、認証パスワードを64桁以内で指定します。

受諾認証情報

着信時に受け付ける認証IDを64桁以内、認証パスワードを64桁以内で指定します。発信者番号による識別は「着信制御情報」で設定できます。

MP接続

MP接続を行う場合は、「する」を選択します。

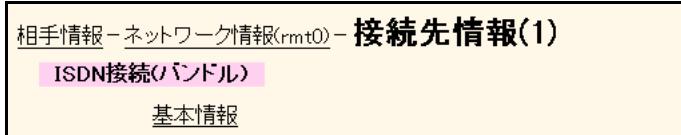
BAP/BACP利用

BAP/BACPを利用する場合は、「する」を選択します。ただし、発信者番号による識別が行われなかった相手からの着信については、「相手情報」 - 「着信相手識別情報」の設定が参照されます。発信者番号による識別は、「着信制御情報」で設定できます。

18.1.2.5 接続先種別：ISDN（バンドル）接続

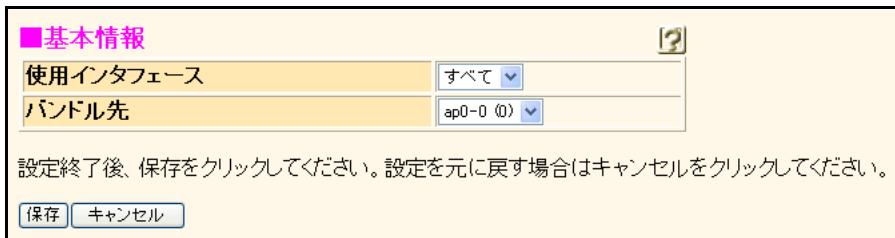
適用機種 Si-R370,370B,570,570B

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (ISDN、バンドル)]
→ [追加]



18.1.2.5.1 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (ISDN、バンドル)]
→ [追加] → [基本情報]



使用インターフェース

専用線接続で使用するWANインターフェースを選択します。あらかじめWAN情報で専用線インターフェースの設定をしておく必要があります。

バンドル先

論理リンクにバンドルする回線として使用するバンドル先の接続先を選択します。

18.1.2.6 接続先種別：フレームリレー接続

適用機種 Si-R220C, 220D, 370, 370B, 570, 570B

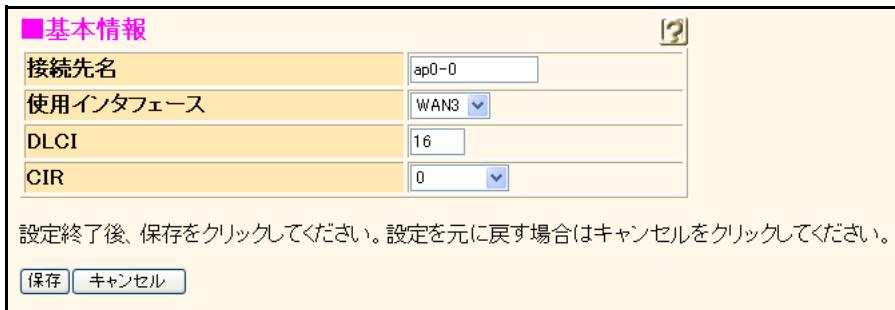
[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(フレームリレー接続)]→[追加]



「接続制御情報」、「マルチルーティング情報」および「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.6.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(フレームリレー接続)]→[追加]→[基本情報]



接続先名

この接続先を識別するための名称を8文字以内で指定します。

CIR

CIRを選択します。CIRは網が正常な状態で保証されるスループットです。本装置が輻輳制御動作を行う場合はCIRを基準としてスループットを制御します。

使用インターフェース

フレームリレー接続で使用するWANインターフェースを選択します。あらかじめWAN情報でフレームリレー回線インターフェースの設定をしておく必要があります。

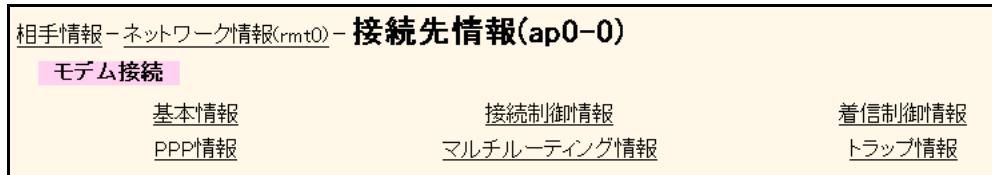
DLCI

DLCIを16～991の範囲で指定します。DLCIを設定できるネットワークは、仕様一覧「[2.1 ソフトウェア仕様\(P.34\)](#)」を参照してください。DLCIは、フレームリレーを使用する場合、一本の物理回線上に設定される複数の論理的な通信路（データリンク）を識別するための識別子です。

18.1.2.7 接続先種別：モデム接続

適用機種 Si-R220C, 220D

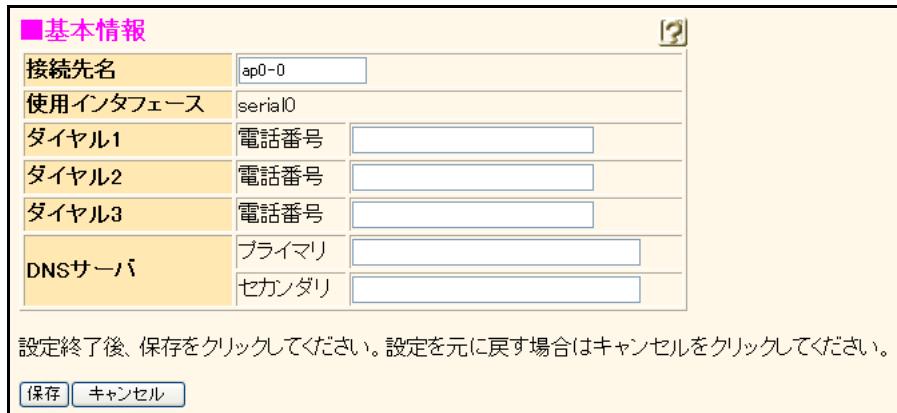
[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報（モデム接続）]→[追加]



「マルチルーティング情報」、「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.7.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報（モデム接続）]→[追加]→[基本情報]



設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前は手動接続の際にも使用されます。

使用インターフェース

本装置では、モデム接続で使用するインターフェースは固定です。

ダイヤル1／2／3

接続に用いる電話番号は3つまで指定できます。ダイヤル1の電話番号にかかるときにはダイヤル2に、ダイヤル2がかかるときはダイヤル3の電話番号にダイヤルします。着信時には自動認識します。電話番号は32桁以内で指定します。

DNS サーバ

接続の際に使用するDNSサーバのIPアドレスを指定します。ProxyDNS機能を使用する際に必要です。省略するか0.0.0.0を指定した場合は、自動取得となります。プライマリのみを省略することはできません。255.255.255.255を指定した場合、DNSサーバは使用しません。また、このIPアドレスはPPPのネゴシエーションの中で相手から要求があった場合、相手に受け渡すDNSサーバアドレスとしても使用します。

18.1.2.7.2 接続制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(モデム接続)]
→[追加]→[接続制御情報]

■接続制御情報	
無通信監視タイム	送受信パケット <input type="button" value="▼"/> について 0 秒
課金単位時間	日間(月～金) (08:00～19:00) <input type="text"/> 0 秒 夜間(土日の日間) (19:00～23:00) <input type="text"/> 0 秒 深夜・早朝 (23:00～08:00) <input type="text"/> 0 秒
発信抑止	<input type="checkbox"/> 指定した時間を超えて接続しない 累計: <input type="text"/> 時間 <input type="button" value="▼"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

無通信監視タイム

無通信監視タイムを0～3600秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または0を指定した場合、自動切断を行いません。

課金単位時間

各時間帯の課金単位時間を0.0～3600.0秒の範囲で指定します。ここで設定した時間は無通信監視による回線切断のときに参照され、同じ料金でもっとも接続時間が長くなるように回線切断タイミングを調整します。なお、昼間時間帯に0を設定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に0を設定した場合、その前の時間帯の設定を利用します。

こんな事に気をつけて

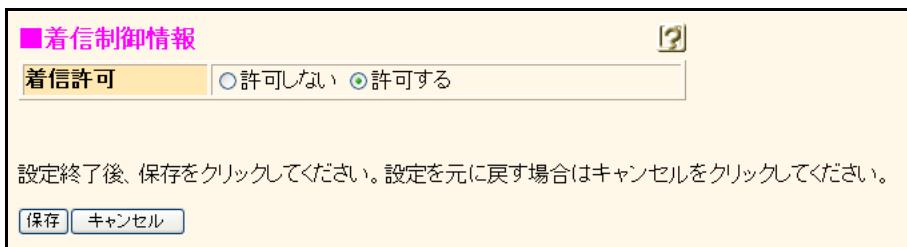
この機能を使用する場合は、操作メニューの時刻設定を使用して本装置の時刻を正しく設定してください。時刻が正しく設定されていない場合、課金単位時間は昼間の値だけが使用されます。祝祭日には対応していません。

発信抑止

この接続先に対する発信抑制を接続時間によって行うことができます。発信抑制を行う場合は、チェックボックスをチェックし、時間は1秒～999時間の範囲で指定します。チェックボックスをチェックした場合、時間の省略はできません。

18.1.2.7.3 着信制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報（モデム接続）]
→[追加]→[着信制御情報]



■着信制御情報

着信許可 許可しない 許可する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

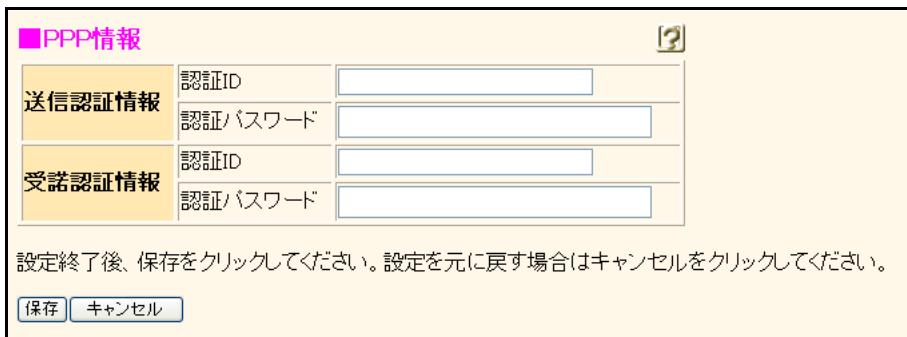
保存 **キャンセル**

着信許可

この接続先からの着信を許可する場合は、“許可する”を選択します。モデム接続では、発信者番号による識別はできません。

18.1.2.7.4 PPP 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報（モデム接続）]
→[追加]→[PPP 情報]



■PPP情報

送信認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
受諾認証情報	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

送信確認情報

発信時に使用する認証IDを64桁以内、認証パスワードを64桁以内で指定します。

受諾認証情報

着信時に受け付ける認証IDを64桁以内、認証パスワードを64桁以内で指定します。モデム接続では、発信者番号による識別はできません。

18.1.2.8 接続先種別：データ通信カード接続

適用機種 Si-R240B

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (データ通信カード接続)] → [追加]

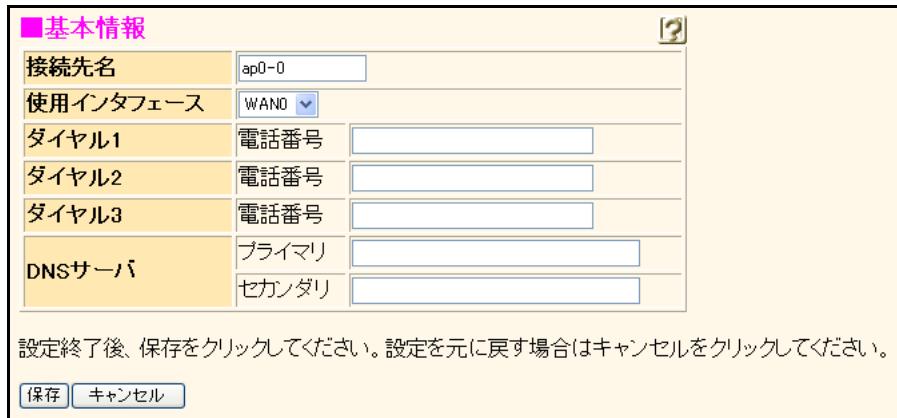


「着信制御情報」および「PPP情報」は、「接続先種別：モデム接続」を参照してください。

「マルチルーティング情報」、「トラップ情報」は、「接続先種別：ATM接続」を参照してください。

18.1.2.8.1 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (データ通信カード接続)] → [追加] → [基本情報]



接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前は手動接続の際にも使用されます。

使用インターフェース

データ通信カード接続で使用するWANインターフェースを選択します。あらかじめWAN情報でデータ通信カード回線インターフェースの設定をしておく必要があります。

ダイヤル1／2／3

接続に用いる電話番号は3つまで指定できます。ダイヤル1の電話番号にかかるときにはダイヤル2に、ダイヤル2にかかるときにはダイヤル3の電話番号にダイヤルします。電話番号は32桁以内で指定します。

DNSサーバ

接続の際に使用するDNSサーバのIPアドレスを指定します。ProxyDNS機能を使用する際に必要です。省略するか0.0.0.0を指定した場合は、自動取得となります。プライマリのみを省略することはできません。255.255.255.255を指定した場合は、DNSサーバは使用しません。また、このIPアドレスはPPPのネゴシエーションの中で相手から要求があった場合、相手に受け渡すDNSサーバアドレスとしても使用します。

18.1.2.8.2 接続制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報(データ通信カード接続)]→[追加]→[接続制御情報]

■接続制御情報

無通信監視タイム	送受信パケット <input type="button" value="▼"/> について 0 <input type="text"/> 秒
課金単位時間	昼間(月～金) (08:00～19:00) <input type="text"/> 0 <input type="text"/> 秒
	夜間(土日の昼間) (19:00～23:00) <input type="text"/> 0 <input type="text"/> 秒
	深夜・早朝 (23:00～08:00) <input type="text"/> 0 <input type="text"/> 秒
強制切断	<input type="checkbox"/> 指定した時間を超えたたら切断する 累計: <input type="text"/> 時間 <input type="button" value="▼"/> <input type="checkbox"/> 指定したパケット数を超えたたら切断する 累計: <input type="text"/> パケット(128バイト換算)
発信抑止	<input type="checkbox"/> 指定した時間を超えて接続しない 累計: <input type="text"/> 時間 <input type="button" value="▼"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

無通信監視タイム

無通信監視タイムを0～3600秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または0を指定した場合、自動切断を行いません。

課金単位時間

各時間帯の課金単位時間を0.0～3600.0秒の範囲で指定してください。

ここで設定した時間は無通信監視による回線切断のときに参照され、同一料金で最大の接続時間を得るよう回線切断タイミングを調整します。なお、昼間時間帯に0を設定した場合、課金単位の調整は行いません。また、夜間時間帯や深夜・早朝時間帯に0を設定した場合、その前の時間帯の設定を利用します。

こんな事に気をつけて

この機能を使用するときは、操作メニューの時刻設定を用いて本装置の時刻を正しく設定してください。時刻が正しく設定されていない場合、課金単位時間は昼間の値のみが使われます。また、祝祭日には対応していません。

強制切断

この接続先に対する強制切断を累計時間と累計パケット数によって行うことができます。

強制切断を行う場合は、各行頭のチェックボックスをチェックし、時間は1秒～999時間、パケット数は1～1000000000の範囲で指定します。なお、パケット数は送受信データバイト数(PPPパケット長)の累計を128で割った値を指定します。チェックボックスをチェックした場合、時間およびパケット数の省略はできません。

こんな事に気をつけて

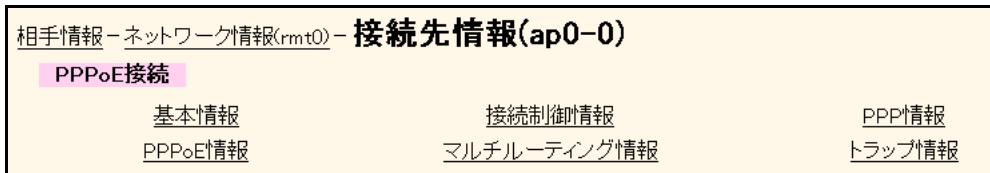
この接続先に対して強制切断が行われた場合は、以降の手動または自動発信を行いません。

発信抑止

この接続先に対する発信抑制を接続時間によって行うことができます。発信抑制を行う場合は、チェックボックスをチェックし、時間は1～999時間の範囲で指定します。チェックボックスをチェックした場合、時間の省略はできません。

18.1.2.9 接続先種別：PPPoE 接続

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (PPPoE 接続)]
→[追加]



「マルチルーティング情報」、「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.9.1 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (PPPoE 接続)]
→[追加]→[基本情報]

■ 基本情報	
接続先名	ap0-0
使用インターフェース	LAN0
DNSサーバ	プライマリ セカンダリ

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続先名

この接続先を識別するための名称を8文字以内で指定します。この名前は手動接続の場合にも使用されます。

使用インターフェース

通信を行なうインターフェースを選択します。

DNS サーバ

接続の際に使用するDNSサーバのIPアドレスを指定します。ProxyDNS機能を使用する際に必要です。省略するか0.0.0.0を指定した場合は、自動取得となります。プライマリのみを省略することはできません。255.255.255.255を指定した場合は、DNSサーバは使用しません。また、このIPアドレスはPPPのネゴシエーションの中で相手から要求があった場合、相手に受け渡すDNSサーバアドレスとしても使用します。

18.1.2.9.2 接続制御情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (PPPoE 接続)]
→[追加]→[接続制御情報]

■接続制御情報

常時接続機能 使用しない 使用する

無通信監視タイム 送受信パケットについて 0 秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

常時接続機能

“使用する”を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。相手から切断された場合や回線エラーによって切断された場合は、自動で再接続します。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。
また、“使用する”を選択すると、表示される画面が変わります。設定項目については、「接続先種別：ATM 接続」の「接続制御情報」を参考に設定します。使用しない場合は、以下の項目を設定します。

無通信監視タイム

無通信監視タイムを0～3600秒の範囲で指定します。ここで指定した時間の間に、監視対象となるパケットが存在しなかった場合は、自動的に切断します。なお、省略、または0を指定した場合、自動切断を行いません。

18.1.2.9.3 PPP 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (PPPoE 接続)]
→[追加]→[PPP 情報]

■PPP情報

送信認証情報 認証ID
認証パスワード

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

送信認証情報

認証 ID

送信時に使用する認証IDを64文字以内の文字列で指定します。

認証パスワード

送信時に使用する認証パスワードを64文字以内の文字列で指定します。

18.1.2.9.4 PPPoE 情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (PPPoE 接続)]
→ [追加] → [PPPoE 情報]

The screenshot shows a configuration page titled "PPPoE 情報". It contains two input fields: "アクセスコンセントレー タ名(AC-Name)" and "サービス名(Service-Name)". Below the fields is a note: "設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。" At the bottom are "保存" and "キャンセル" buttons.

アクセスコンセントレー タ名 (AC-Name)

アクセスコンセントレー タ名を 64 文字以内の文字列で指
定します。

サービス名 (Service-Name)

サービス名を 64 文字以内の文字列で指定します。

18.1.2.10 接続先種別：IP トンネル接続

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (IP トンネル接続)]
→ [追加]

相手情報 - ネットワーク情報(rmt2) - **接続先情報(ap0-0)**

IPトンネル接続	基本情報	接続制御情報	トラップ情報
-----------------	----------------------	------------------------	------------------------

「接続制御情報」、「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.10.1 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (IP トンネル接続)]
→ [追加] → [基本情報]

■ 基本情報

接続先名	ap0-0
自側エンドポイント	
相手側エンドポイント	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

接続先名

この接続先を識別するための名称を8文字以内で指定します。

自側／相手側エンドポイント

自側（相手側）のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.25.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

18.1.2.11 接続先種別：IPsec/IKE 接続

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
→ [追加]

「IPsec/IKE 接続」 - 「基本情報」の IPsec 動作モード、鍵交換モードと認証方式で、以下の設定を保存した場合

- IPsec/IKE (IKEv1)
 - Aggressive Mode (Initiator) 共有鍵認証方式
 - Aggressive Mode (Responder) 共有鍵認証方式
 - Main Mode 共有鍵認証方式
 - Aggressive Mode RSA デジタル署名認証方式
 - Main Mode RSA デジタル署名認証方式
- IPsec/IKE (IKEv2)
 - IKE_SA_INIT 共有鍵認証方式
 - IKE_SA_INIT RSA デジタル署名認証方式

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)

IPsec/IKE接続		
<u>基本情報</u>	<u>接続制御情報</u>	<u>IPsec情報</u>
IKE情報	拡張IPsec対象範囲情報	マルチルーティング情報
トラップ情報		

「IPsec/IKE 接続」 - 「基本情報」の IPsec 動作モードと鍵交換モードで、以下の設定を保存した場合

- IPsec/IKE (IKEv1)
 - IKE は他の接続先情報を使用
- IPsec/IKE (IKEv2)
 - IKE は他の接続先情報を使用
- 手動鍵設定

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)

IPsec/IKE接続		
<u>基本情報</u>	<u>接続制御情報</u>	<u>IPsec情報</u>
拡張IPsec対象範囲情報	マルチルーティング情報	トラップ情報

「IPsec/IKE 接続」 - 「基本情報」の IPsec 動作モードと認証方式で、以下の設定を保存した場合

- IPsec/IKE (動的VPN)
 - 共有鍵認証方式
 - RSA デジタル署名認証方式

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)

IPsec/IKE接続		
<u>基本情報</u>	<u>接続制御情報</u>	<u>IPsec情報</u>
IKE情報	拡張IPsec対象範囲情報	マルチルーティング情報
動的VPN関連	トラップ情報	

「マルチルーティング情報」および「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.11.1 基本情報

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
→ [追加] → [基本情報]

IPsec動作モード、鍵交換モード、認証方式、ID タイプの設定により、表示される画面が異なります。

ここでは、以下を選択した場合の画面例を示します。

- IPsec動作モード IPsec/IKE (IKEv1)
- 鍵交換モード Aggressive Mode (Initiator)
- 認証方式 共有鍵認証方式

■ 基本情報

接続先名	ap0-0
IPsec動作モード	<input checked="" type="radio"/> IPsec/IKE(IKEv1) <input type="radio"/> IPsec/IKE(IKEv2) <input type="radio"/> IPsec/IKE(動的VPN) <input type="radio"/> 手動鍵設定
鍵交換モード	Aggressive Mode(Initiator)
認証方式	<input checked="" type="radio"/> 共有鍵認証方式 <input type="radio"/> RSAデジタル署名認証方式
IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN
自側エンドポイント	
相手側エンドポイント	
自装置識別情報	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

接続先名

この接続先を識別するための名称を8文字以内で指定します。

IPsec動作モード

IPsecの動作モードを以下の4つから選択します。

- IPsec/IKE (IKEv1)
IPsec Version2/IKE Version1 を利用して通信する場合に選択します。
IPsec/IKE (IKEv1) を利用する場合、相手エンドポイント装置も IPsec/IKE (IKEv1) を利用する設定がされている必要があります。
- IPsec/IKE (IKEv2)
IPsec Version3/IKE Version2 を利用して通信する場合に選択します。
IPsec/IKE (IKEv2) を利用する場合、相手エンドポイント装置も IPsec/IKE (IKEv2) を利用する設定がされている必要があります。
- IPsec/IKE (動的VPN)
動的VPN機能を利用して通信をする場合に選択します。
動的VPN機能を利用する場合、相手エンドポイント装

置も動的VPN機能を利用する設定がされている必要があります。

- 手動鍵設定
手動鍵設定でのIPsecを利用して通信する場合に選択します。
手動鍵を利用する場合、相手エンドポイント装置に手動鍵の設定がされている必要があります。
手動鍵設定はIPsec Version2で動作します。

認証方式

IKEで使用する認証方式を選択します。

- 共有鍵認証方式
認証方式として共有鍵認証方式を利用したIKE通信をする場合に選択します。
共有鍵認証方式を利用する場合、相手エンドポイント装置に共有鍵認証方式の設定がされている必要があります。
- RSAデジタル署名認証方式
認証方式としてRSAデジタル署名認証方式を利用したIKE通信をする場合に選択します。
RSAデジタル署名認証方式を利用する場合、相手エンドポイント装置にRSAデジタル署名認証方式の設定がされている必要があります。

鍵交換モード

IPsec/IKE (IKEv1)

「IPsec/IKE (IKEv1)」で使用する認証方式を選択します。

- Main Mode
相手側／自側エンドポイントが固定IPアドレスでIPsec/IKEを利用して通信する場合に選択します。
Main Mode を利用する場合、相手エンドポイント装置に Main Mode の設定がされている必要があります。
- Aggressive Mode (Initiator)
自側エンドポイントが可変IPアドレスで認証方式として共有鍵認証方式IPsec/IKEを利用して通信をする場合に選択します。
Aggressive Mode (Initiator) を利用する場合、相手エンドポイント装置に Aggressive Mode (Responder) の設定がされている必要があります。
- Aggressive Mode (Responder)
相手側エンドポイントが可変IPアドレスで認証方式として共有鍵認証方式IPsec/IKEを利用して通信をする場合に選択します。
Aggressive Mode (Responder) を利用する場合、相手エンドポイント装置に Aggressive Mode (Initiator) の設定がされている必要があります。
- Aggressive Mode
Aggressive Mode RSA デジタル署名認証方式で IPsec/IKE を利用して通信をする場合に選択します。
 - Initiator として動作させる場合
相手側エンドポイントと自装置識別情報を指定します。
自側エンドポイントが固定IPアドレスで Aggressive Mode を使用する場合は、自側エンドポイントを指定します。
相手エンドポイント装置から自装置識別情報を受信する場合は、相手装置識別情報を指定します。
Initiator として動作させる場合、相手エンドポイント装置に Aggressive Mode RSA デジタル署名認証方式の Responder として動作させる設定がされている必要があります。
 - Responder として動作させる場合
自側エンドポイントと相手装置識別情報を指定します。
相手側エンドポイントが固定IPアドレスで Aggressive Mode を使用する場合は、相手側エンドポイントを指定します。
相手エンドポイント装置に自装置識別情報を送信する場合は、自装置識別情報を指定します。

Responder として動作させる場合、相手エンドポイント装置に Aggressive Mode RSA デジタル署名認証方式の Initiator として動作させる設定がされている必要があります。

こんな事に気をつけて

自側エンドポイント、相手側エンドポイント、自装置識別情報、相手装置識別情報のすべてに設定がされている場合、Initiator と Responder 両方の動作が可能です。

- IKE は他の接続先情報を使用する
同一エンドポイントアドレス間で IPsec SA を複数使用する場合に選択します。

IPsec/IKE (IKEv2)

「IPsec/IKE (IKEv2)」で使用する認証方式を選択します。

- IKE_SA_INIT
IKEv2 の初期交換を利用して通信をする場合に選択します。
- IKE は他の接続先情報を使用する
同一エンドポイントアドレス間で CHILD SA を複数使用する場合に選択します。

自側／相手側エンドポイント

IPv4 形式または IPv6 形式のアドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

自側エンドポイントとして 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場合は、上位を “dhcp@インターフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で入力します。インターフェース名には、IPv6 DHCP クライアント機能が動作している rmt インタフェースを指定します。

なお、IPv6 DHCP クライアントが取得したプレフィックスを使用できるのは、以下になります。

- IPsec/IKE (IKEv1) で Aggressive Mode (Initiator) 使用時
- IPsec/IKE (動的 VPN) 使用時
- IPsec/IKE (IKEv2) で自側トンネルエンドポイント不定アドレス使用時

RSA デジタル署名認証方式で、ID タイプが Address の場合は、IPv6 形式のアドレスは設定できません。

自装置識別情報

自装置識別情報を送信する場合に自装置を識別する情報
(名前) を 64 文字以内で指定します。

相手装置識別情報

相手装置識別情報を受信する場合に相手装置を識別する
情報 (名前) を 64 文字以内で指定します。

ID タイプ

IPsec/IKE (IKEv1) のネゴシエーションで使用する交換
ID タイプを選択します。

自装置／相手装置 ID タイプ

IPsec/IKE (IKEv2) のネゴシエーションで使用する自装置
／相手装置の交換 ID タイプを選択します。

接続先名

IKE 定義が設定されている接続先情報を選択します。

18.1.2.11.2 接続制御情報

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
→ [追加] → [接続制御情報]

■接続制御情報

常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
接続先監視	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	送信元IPアドレス	<input type="text"/>
	あて先IPアドレス	<input type="text"/>
	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	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	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視	
接続優先制御	<input checked="" type="radio"/> 使用しない <input type="radio"/> Initiatorを優先する <input type="radio"/> Responderを優先する	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続先監視の項目は、「接続先種別：ATM 接続」を参照してください。

常時接続機能

“使用する”を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。また、IKE ネゴシエーション失敗などによる IPsec SA ができない場合や IPsec SA が解放された場合は、自動で IKE ネゴシエーションによる再接続を行います。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。

接続優先制御

IKE SA を確立するための IKE ネゴシエーションが競合した場合の接続優先制御を以下の 3 つから選択します。

- 使用しない
そのまま IKE ネゴシエーションを続けます。
- Initiator を優先する
Initiator の要求を残し、Responder 要求を無視します。
- Responder を優先する
Responder の要求を残し、Initiator の要求を終了します。

こんな事に気をつけて

自装置と接続相手装置の両方で接続優先制御を行う場合は、それぞれ異なる優先方法を選択してください。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 接続を優先し、一方の装置で Responder 接続を優先する。

18.1.2.11.3 IPsec 情報（自動鍵）

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (IPsec/IKE 接続)]
→[追加]→[IPsec 情報（自動鍵）]

■ 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 <input checked="" type="checkbox"/> ("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	IPv4すべて <input checked="" type="checkbox"/> ("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	<input type="checkbox"/> aes-cbc-256 <input type="checkbox"/> aes-cbc-192 <input type="checkbox"/> aes-cbc-128 <input type="checkbox"/> 3des-cbc <input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> null
	認証アルゴリ ズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 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
SA 更新	Initiator 時	時間 90 秒 データ量 0 MByte
	Responder時	<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間 30 秒 データ量 0 MByte

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

この画面は、「IPsec/IKE 接続」－「基本情報」のIPsec動作モードで、“手動鍵設定”および“IPsec/IKE（動的VPN）”以外を選択した場合に表示されます。



◆ IPsec で 使用する プロトコル

IPsec で 使用する プロトコル は、IPsec の 設定 により 決定 します。プロトコル は AH と ESP が あり、1 つ の IPsec 情報 定義 に 暗号情報 と 認証情報 の 両方 を 指定 す ると 認証付き ESP と なります。

アルゴリズム の 組み合わせ は、以下のとおり です。

暗号情報	認証情報	プロトコル
暗号化しない	<input type="radio"/>	AH (認証)
<input type="radio"/>	認証なし	ESP (暗号)
<input type="radio"/>	<input type="radio"/>	ESP (認証+暗号)

暗号情報 : des-cbc、3des-cbc、null、aes-cbc-128、aes-cbc-192 または aes-cbc-256

認証情報 : hmac-md5 または hmac-sha1

※ 「暗号化しない」とは、暗号アルゴリズムを1つも選択しないことを指します。

「認証なし」とは、認証アルゴリズムで“認証なし”を選択または認証アルゴリズムを1つも選択しないことを指します。

対象パケット

自側／相手側 IP アドレス／マスク

IPsec を 適用する セッション の 送信元 IP アドレス および アドレスマスク と、あて先 IP アドレス および アドレスマスク を 以下 の 3 つ から 選択 します。アドレスを指定する場合は、“ 指定する ” を 指定 します。

- IPv4 すべて
IPv4 アドレス をすべて 選択 します。
- IPv6 すべて
IPv6 アドレス をすべて 選択 します。
- 指定する
IP アドレス／マスク を IPv4/IPv6 形式 で 指定 します。

SA の 設定

暗号アルゴリズム

トンネリングする パケット の 暗号アルゴリズム を 使用する 場合 に 選択 します。複数選択した 場合 、 aes-cbc-256、aes-cbc-192、aes-cbc-128、3des-cbc、des-cbc、null の 順 に 比較 されます。暗号アルゴリズム を 選択 しない 場合 は、パケット の 暗号化 を 行いません。

認証アルゴリズム

トンネリングする パケット の 認証アルゴリズム を 選択 し ます。複数選択した 場合 、 hmac-md5、hmac-sha1、認証なし の 順 に 比較 され ます。認証アルゴリズム を 選択 し ない 場合 および “ 認証なし ” だけ を 選択 した 場合 は、パケッ ト の 認証 を 行いません。

PFS 時の DH グループ

自動鍵交換 の 鍵 を 生成するため の 鍵素材 です。値 が 大きい 程 セキュリティ 強度 は 高く な ります。ただし、装置 の 負荷 が 高く な る 場合 が あります。使用 し ない 場合 は、“ 使用 し ない ” を 選択 し ます。

SA 有効時間

SA の 有効期限 を 以下 の 範囲 で 指定 し ます。指定 し た 時間 が 経過 し た 時点 で、SA の 有効期限 が 切れ、IKE によ って SA 情報 や 鍵情報 が 自動的 に 更新 さ れます。省略 し た 場合 は、8 時間 が 設定 さ れます。

有効範囲)

600～86400 秒

10～1440 分

1～24 時間

SA有効データ量

SAの有効期限をデータ量で指定します。指定したデータ量を経過した時点で、SAの有効期限が切れ、IKEによってSA情報や鍵情報が自動的に更新されます。省略時は、0が設定されデータ量によるSA更新が行われません。

有効範囲)

2400～110592000 キロバイト

3～108000 メガバイト

1～105 ギガバイト

SA 更新

SAの更新時間を設定します。

Initiator 時

自側が Initiator の場合に、IPsec SA の有効時間または有効データ量が満了になる前に IPsec で SA の更新を行うための時間とデータ量を指定します。また、IPsec SA 更新のデータ量は、IPsec SA の有効データ量が定義されていない場合は無効となります。

相手側の Responder 時の SA 更新時間とデータ量と同じにならないように設定してください。

時間

30～180 秒の範囲で指定します。省略時は、90 秒が設定されます。

データ量

120～230400 キロバイトの範囲で指定します。省略時は、0KByte が設定されます。

Responder 時

自側が Responder の場合に、IPsec SA の有効時間または有効データ量が満了になる前に IPsec SA の更新を行う場合は、“更新する”を選択します。“更新する”を選択した場合、更新を行う時間とデータ量を設定します。“更新しない”を選択した場合、Responder 側からの SA の更新は行いません。また、IPsec SA 更新のデータ量は、IPsec SA の有効データ量が定義されていない場合は無効となります。

相手側の Initiator 時の SA 更新時間とデータ量と同じにならないように指定してください。

時間

30～180 秒の範囲で指定します。省略時は、30 秒が設定されます。

データ量

120～230400 キロバイトの範囲で指定します。省略時は、0KByte が設定されます。

18.1.2.11.4 IPsec 情報（手動鍵）

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (IPsec/IKE 接続)]
→[追加]→[IPsec 情報（手動鍵）]

■ IPsec情報(手動鍵)

対象パケット (送信用)	自側IPアドレス	<input type="text"/>
	自側アドレスマスク	<input type="text"/> 0.0.0.0
	相手側IPアドレス	<input type="text"/>
	相手側アドレスマスク	<input type="text"/> 0.0.0.0
SAの設定 (送信用)	SPI値	<input type="text"/> (16進数)
	暗号アルゴリズム	<input type="text"/> des-cbc
	暗号鍵	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列 <input type="text"/>
	認証アルゴリズム	<input type="text"/> hmac-md5
	認証鍵	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列 <input type="text"/>
	相手側IPアドレス	<input type="text"/>
対象パケット (受信用)	相手側アドレスマスク	<input type="text"/> 0.0.0.0
	自側IPアドレス	<input type="text"/>
	自側アドレスマスク	<input type="text"/> 0.0.0.0
	SPI値	<input type="text"/> (16進数)
	暗号アルゴリズム	<input type="text"/> des-cbc
	暗号鍵	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列 <input type="text"/>
SAの設定 (受信用)	認証アルゴリズム	<input type="text"/> hmac-md5
	認証鍵	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列 <input type="text"/>
	相手側IPアドレス	<input type="text"/>
	相手側アドレスマスク	<input type="text"/> 0.0.0.0
	自側IPアドレス	<input type="text"/>
	自側アドレスマスク	<input type="text"/> 0.0.0.0

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

この画面は、「IPsec/IKE 接続」－「基本情報」のIPsec動作モードで、“手動鍵設定”を選択した場合に表示されます。
対象パケット（送信用）／（受信用）の項目は、「IPsec 情報（自動鍵）」を参照してください。

SA の設定（送信用）／（受信用）

SPI 値

SPI 値は、暗号情報や認証情報を定義したセキュリティパラメータインデックスです。相手装置の設定と同じ値を指定する必要があります。SPI 値を 100～ffffffff の 16 進数の範囲で指定します。

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを選択します。“暗号化しない”を選択した場合は、パケットの暗号化を行いません。

暗号鍵

- 鍵識別
鍵の識別を指定します。
- 鍵
暗号アルゴリズムで使用する暗号鍵を 16 進数および文字列を使用して、以下の範囲で指定します。

暗号アルゴリズム	入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
DES-CBC	1 ~ 16 衔	8 文字
3DES-CBC	1 ~ 48 衔	24 文字
AES-CBC-128	1 ~ 32 衔	16 文字
AES-CBC-192	1 ~ 48 衔	24 文字
AES-CBC-256	1 ~ 64 衔	32 文字

16 進数で 16 衔 (DES-CBC 指定時。3DES-CBC 指定時は 48 衔。AES-CBC-128 指定時は 32 衔。AES-CBC-192 指定時は 48 衔。AES-CBC-256 指定時は 64 衔。) 未満の鍵を指定した場合は、16 (64) 衔になるまで、自動的に "0" でパディングされます。

文字列で指定する場合は、8 文字 (DES-CBC 指定時。3DES-CBC 指定時は 24 文字。AES-CBC-128 指定時は 16 文字。AES-CBC-192 指定時は 24 文字。AES-CBC-256 指定時は 32 文字。) 固定の鍵長で指定してください。暗号情報のアルゴリズムに「暗号化しない」を選択した場合は、省略できます。

認証鍵

- 鍵識別
鍵の識別を指定します。
- 鍵
認証アルゴリズムで使用する認証鍵を 16 進数および文字列を使用して、以下の範囲で指定します。

暗号アルゴリズム	入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
HMAC-MD5	1 ~ 32 衔	16 文字
HMAC-SHA1	1 ~ 40 衔	20 文字

16 進数で 32 衔 (HMAC-MD5 指定時、HMAC-SHA1 指定時は 40 衔) 未満の鍵を指定した場合は、32 (40) 衔になるまで、自動的に "0" でパディングされます。

文字列で指定する場合は、16 文字 (HMAC-MD5 指定時、HMAC-SHA1 指定時は 20 文字) 固定の鍵長で指定します。認証情報のアルゴリズムに "認証なし" を選択した場合は、省略できます。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。“認証なし”を選択した場合、パケットの認証を行いません。

18.1.2.11.5 IPsec 情報（動的VPN）

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」 → 「接続先情報（IPsec/IKE 接続）」
 → 「追加」 → 「IPsec 情報（動的VPN）」

■ IPsec情報(動的VPN)

SAの設定	暗号アルゴリズム	<input type="checkbox"/> aes-cbc-256 <input type="checkbox"/> aes-cbc-192 <input checked="" type="checkbox"/> aes-cbc-128 <input type="checkbox"/> 3des-cbc <input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 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更新	Initiator時	時間 90 秒 データ量 0 MByte
	Responder時	<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間 30 秒 データ量 0 MByte

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

この画面は、「IPsec/IKE 接続」 – 「基本情報」のIPsec動作モードで、“IPsec/IKE（動的VPN）”を選択した場合に表示されます。

各項目の説明は、「IPsec情報（自動鍵）」を参照してください。

18.1.2.11.6 IKE 情報 (IKEv1 共有鍵認証方式)

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
→ [追加] → [IKE 情報 (IKEv1 共有鍵認証方式)]

IKE情報(IKEv1 共有鍵認証方式)

共有 鍵 認証	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	<input type="text"/>
ポート番号 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(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 回		
IKEネゴシエーション開始動作 <input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機		
NATトラバーサル機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する		
DPD 機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
	再送回数	3 回
IKE セッ ショ ン監 視	あて先IPアドレス	<input type="text"/>
	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	3 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

この画面は、「IPsec/IKE 接続」 – 「基本情報」の IPsec 動作モードで “IPsec/IKE (IKEv1)” を選択し、鍵交換モードと認証方式を以下の設定で保存した場合に表示されます。

- Aggressive Mode (Initiator) 共有鍵認証方式
- Aggressive Mode (Responder) 共有鍵認証方式
- Main Mode 共有鍵認証方式

共有鍵認証

IKE の認証に用いる鍵を設定します。本装置の IKE の認証には事前共有鍵認証と RSA デジタル証明認証方式があります。ここでは事前共有鍵 (Pre-shared key) の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
1 ~ 256 衔	1 ~ 128 文字

鍵識別

鍵の識別を選択します。

ポート番号

IKE プロトコルで使用する UDP のポート番号を 10 進数を使用して 1 ~ 65535 の範囲で指定します。IKE プロトコルでは通常ポート 500 番を使用しますので、通常は、“500”を指定します。省略時は、“500”が設定されます。

SA の設定

暗号アルゴリズム

IKE セッションの送受信パケットを暗号化／復号化するためのアルゴリズムを選択します。

認証（ハッシュ）アルゴリズム

IKE セッションのネゴシエーションパケットを認証するためのアルゴリズムを選択します。

DH グループ（Diffie-Hellman グループ）

自動鍵交換で鍵を生成するための鍵素材を選択します。値が大きい程セキュリティ強度は高くなります。ただし、鍵生成のための計算に時間がかかるため、装置の負荷が高くなる場合があります。

SA 有効時間

IKE SA の有効期限を以下の範囲で指定します。指定した時間が経過した時点で、SA の有効期限が切れ、IKE SA 情報や鍵情報が IKE によって自動的に更新されます。省略時は、24 時間が設定されます。

有効範囲)

600 ~ 86400 秒

10 ~ 1440 分

1 ~ 24 時間

初回再送時間

IKE の初回再送時間を 10 進数を使用して、1 ~ 60 秒の範囲で指定します。省略時は、10 秒が設定されます。

再送回数

IKE の再送回数を 10 進数を使用して、1 ~ 10 回の範囲で指定します。省略時は、3 回が設定されます。

IKE ネゴシエーション開始動作

IKE ネゴシエーション開始動作を選択します。対象回線接続契機を選択した場合は、対象パケット送信契機も含まれます。

NAT トラバーサル機能

IKE ネゴシエーションパケットや ESP パケットの送信元 IP アドレス、あて先 IP アドレスまたはポート番号が NAT 変換される環境では、“使用する”を選択します。

こんな事に気をつけて

- 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 情報（自動鍵）」画面の暗号アルゴリズムを設定してください。暗号アルゴリズム設定がない場合は動作しません。
- 「基本情報」画面の自側エンドポイント、および相手側エンドポイントに 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。

DPD 機能

DPD 機能を利用する場合は、“使用する”を選択します。

こんな事に気をつけて

無通信監視時間は再送時間 × (再送回数 + 1) 秒より大きくなるように指定してください。

IPsec 受信パケット無通信監視時間

DPD パケットの送信を開始する IPsec 受信パケット無通信監視時間を 10 進数を使用して、5 ~ 600 秒の範囲で指定します。省略時は、10 秒が設定されます。

再送時間

DPD パケットの再送時間を 10 進数を使用して、1~60 秒の範囲で指定します。省略時は、1 秒が設定されます。

こんな事に気をつけて

同時に接続先監視が設定されている場合、IKE セッション監視は動作せず、接続先監視だけが動作します。接続先監視は「接続制御情報」で設定できます。

再送回数

DPD パケットの再送回数を 10 進数を使用して、1~10 回の範囲で指定します。省略時は、3 回が設定されます。

IKE セッション監視

指定されたあて先 IP アドレスに対して ICMP ECHO パケットを送信します。タイムアウト時間までに応答がない場合に IPsec/IKE SA を解放します。

あて先 IP アドレス

ICMP ECHO パケットの送出先 IP アドレス指定します。
あて先 IP アドレスに 0.0.0.0、または省略時 IKE セッション監視をしません。また、正常時送信間隔、異常時送信間隔は初期値になります。

有効範囲)

1.0.0.1-126.255.255.254
128.0.0.1-191.255.255.254
192.0.0.1-223.255.255.254

タイムアウト時間

タイムアウト時間を、10 進数を使用して 5~180 秒の範囲で指定します。タイムアウト時間までに応答がない場合、監視対象ホストがダウンしたものとみなし、IPsec/IKE SA を解放します。省略時は、5 秒が設定されます。

正常時送信間隔

正常に受信されている状態での周期間隔です。ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を 10 進数を使用して 1~60 秒の範囲で指定します。省略時は、10 秒が設定されます。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの周期送信する間隔を、10 進数を使用して 60~600 秒の範囲で指定します。応答が受信された場合は正常時送信間隔状態に戻ります。省略時は、3 分が設定されます。

18.1.2.11.7 IKE 情報 (IKEv2 共有鍵認証方式)

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
→ [追加] → [IKE 情報 (IKEv2 共有鍵認証方式)]

■ IKE情報(IKEv2 共有鍵認証方式)		
共有鍵 認証	鍵識別	
	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列	
SAの設 定	鍵	<input type="text"/>
	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)
	擬似乱数関数(PRF)	hmac-md5
SA有効時間	24 時間	
相手装置ID送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	
初回再送時間	10 秒	
再送回数	3 回	
IKEネゴシエーション開始動作	<input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機	
拡張シーケンス番号	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
NATトラバーサル機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
DDP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
再送回数	3 回	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

この画面は、「IPsec/IKE 接続」－「基本情報」のIPsec動作モードで“IPsec/IKE (IKEv2)”を選択し、鍵交換モードと認証方式を以下の設定で保存した場合に表示されます。

- IKE_SA_INIT 共有鍵認証方式

共有鍵認証

IKE の認証に用いる鍵を設定します。本装置の IKE の認証には事前共有鍵認証と RSA デジタル証明認証方式があります。ここでは事前共有鍵 (Pre-shared key) の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵識別

鍵の識別を選択します。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
1～256 行	1～128 文字

SA の設定

暗号アルゴリズム

IKE セッションの送受信パケットを暗号化／復号化するためのアルゴリズムを選択します。

認証（ハッシュ）アルゴリズム

IKE セッションのネゴシエーションパケットを認証するためのアルゴリズムを選択します。

DH グループ (Diffie-Hellman グループ)

自動鍵交換で鍵を生成するための鍵素材を選択します。値が大きい程セキュリティ強度は高くなります。ただし、鍵生成のための計算に時間がかかるため、装置の負荷が高くなる場合があります。

擬似乱数関数 (PRF)

IKE の鍵生成で使用される擬似乱数関数のハッシュ関数 (PRF : Pseudo Random Function) を選択します。

SA 有効時間

IKE SA の有効期限を以下の範囲で指定します。指定した時間が経過した時点で、SA の有効期限が切れ、IKE SA 情報や鍵情報が IKE によって自動的に更新されます。省略時は、24 時間が設定されます。

有効範囲)

600 ~ 86400 秒

10 ~ 1440 分

1 ~ 24 時間

相手装置 ID 送信

IKE ネゴシエーションで相手装置 ID を含めて送信する場合は、“送信する”を選択します。

初回再送時間

IKE の初回再送時間を 10 進数を使用して、1 ~ 60 秒の範囲で指定します。省略時は、10 秒が設定されます。

再送回数

IKE の再送回数を 10 進数を使用して、1 ~ 10 回の範囲で指定します。省略時は、3 回が設定されます。

IKE ネゴシエーション開始動作

IKE ネゴシエーション開始動作を選択します。対象回線接続契機を選択した場合は、対象パケット送信契機も含まれます。

拡張シーケンス番号

IPsec バージョン 3 で定義されている拡張シーケンス番号 (ESN) を使用する場合は、“使用する”を選択します。

NAT トラバーサル機能

IKE ネゴシエーションパケットや ESP パケットの送信元 IP アドレス、あと先 IP アドレスまたはポート番号が NAT 変換される環境では、“使用する”を選択します。

こんな事に気をつけて

- 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。
- 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 情報（自動鍵）」画面の暗号アルゴリズムを設定してください。暗号アルゴリズム設定がない場合は動作しません。
- 「基本情報」画面の自側エンドポイント、および相手側エンドポイントに 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。

DPD 機能

DPD 機能を利用する場合は、“使用する”を選択します。

こんな事に気をつけて

無通信監視時間は再送時間 × (再送回数 + 1) 秒より大きくなるように指定してください。

IPsec 受信パケット無通信監視時間

DPD パケットの送信を開始する IPsec 受信パケット無通信監視時間を 10 進数を使用して、5 ~ 600 秒の範囲で指定します。省略時は、10 秒が設定されます。

再送時間

DPD パケットの再送時間を 10 進数を使用して、1 ~ 60 秒の範囲で指定します。省略時は、1 秒が設定されます。

再送回数

DPD パケットの再送回数を 10 進数を使用して、1 ~ 10 回の範囲で指定します。省略時は、3 回が設定されます。

18.1.2.11.8 IKE 情報 (IKEv1 RSA デジタル署名認証方式)

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (IPsec/IKE 接続)]
→[追加]→[IKE 情報 (IKEv1 RSA デジタル署名認証方式)]

■IKE情報(IKEv1 RSAデジタル署名認証方式)

RSA デジ タル 署 名 認 証	相手装置証明書識別番号	指定なし
	自装置証明書識別番号	使用できる自装置証明書が存在しません
	秘密鍵識別番号	使用できる秘密鍵が存在しません
	自装置証明書情報の送信	<input checked="" type="radio"/> 証明書要求ペイロード受信時 <input type="radio"/> 常時
証明書要求	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する 認証局識別番号 指定なし	
有効期限切れ証明書	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
ポート番号	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(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 回	
IKEネゴシエーション開始動作	<input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機	
NATトラバーサル機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
DPD 機 能	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
	再送回数	3 回
	あて先IPアドレス	
IKE セッ ショ ン監 視	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	3 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

この画面は、「IPsec/IKE 接続」 - 「基本情報」のIPsec動作モードで“IPsec/IKE (IKEv1)”を選択し、鍵交換モードと認証方式を以下の設定で保存した場合に表示されます。

- Aggressive Mode RSA デジタル署名認証方式
- Main Mode RSA デジタル署名認証方式

「RSA デジタル署名認証」以外の項目の説明は、「IKE 情報 (IKEv1 共有鍵認証方式)」を参照してください。

RSA デジタル署名認証

IKE の認証に用いる証明書を指定します。本装置の IKE の認証には事前共有鍵認証と RSA デジタル証明認証方式があります。ここでは RSA デジタル証明書の設定を行います。RSA デジタル証明書は、IKE を利用した IPsec 通信を行う相手ごとに設定する必要があります。

相手装置証明書識別番号

相手装置証明書の識別番号を選択します。

IKE の認証方式として RSA デジタル署名が設定されている場合、Main モードでは IKE ネゴシエーションで受信した ID (IP アドレスまたは FQDN) でサブジェクト代替名称 (IP アドレス、ドメイン名または 証明書対象者名) と一致する相手装置証明書を使用します。

Aggressive モードでは IKE ネゴシエーション内の ID (IP アドレスまたは FQDN) でサブジェクト代替名称 (IP アドレスまたはドメイン名) と一致する相手装置証明書を使用します。

自装置証明書識別番号

自装置証明書の識別番号を選択します。

認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

秘密鍵識別番号

秘密鍵の識別番号を選択します。

認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

自装置証明書情報の送信

自装置証明書の送信設定を選択します。

- 証明書要求ペイロード受信時
相手装置から証明書要求ペイロードを受信したときに、自装置証明書情報を送信します。
- 常時
相手装置から証明書要求ペイロードの受信の有無にかかわらず、常に自装置証明書情報を送信します。

証明書要求

証明書要求の送信設定を選択します。

- 送信しない
証明書要求を送信しません。
- 送信する
証明書要求を送信します。

認証局識別番号

証明書要求の送信設定を「送信する」に選択した場合に、使用する認証局情報の識別番号を選択します。選択した認証局情報を証明書要求に入れて送信します。

「指定なし」を選択した場合は、何も入れないで証明書要求を送信します。

有効期限切れ証明書

有効期限が切れている証明書を使用するかどうかを選択します。

- 使用する
有効期限が切れている証明書をそのまま使用します。
- 使用しない
有効期限が切れている証明書を使用しません。この場合、IKE ネゴシエーションに失敗します。

18.1.2.11.9 IKE 情報 (IKEv2 RSA デジタル署名認証方式)

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
 → [追加] → [IKE 情報 (IKEv2 RSA デジタル署名認証方式)]

■IKE情報(IKEv2 RSAデジタル署名認証方式)

RSAデジタル署名認証	相手装置証明書識別番号	指定なし
	自装置証明書識別番号	使用できる自装置証明書が存在しません
	秘密鍵識別番号	使用できる秘密鍵が存在しません
	自装置証明書情報の送信	<input checked="" type="radio"/> 証明書要求ペイロード受信時 <input type="radio"/> 常時 <input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する 認証局識別番号 指定なし
有効期限切れ証明書	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
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)
	擬似乱数関数(PRF)	hmac-md5
SA有効時間	24 時間	
相手装置ID送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する	
初回再送時間	10 秒	
再送回数	3 回	
IKEネゴシエーション開始動作	<input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機	
拡張シーケンス番号	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
NATトラバーサル機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
DPD機能	使用しない 使用する	
	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
	再送回数	3 回

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

この画面は、「IPsec/IKE 接続」 – 「基本情報」の IPsec 動作モードで “IPsec/IKE (IKEv2)” を選択し、鍵交換モードと認証方式を以下の設定で保存した場合に表示されます。

- IKE_SA_INIT RSA デジタル署名認証方式

「RSA デジタル署名認証」の項目の説明は、「IKE 情報 (IKEv1 RSA デジタル署名認証方式)」、「RSA デジタル署名認証」以外の項目の説明は、「IKE 情報 (IKEv2 共有鍵認証方式)」を参照してください。

18.1.2.11.10 IKE 情報（動的VPN接続 共有鍵認証方式）

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE接続)]
→ [追加] → [IKE情報（動的VPN接続 共有鍵認証方式）]

■ IKE情報(動的VPN接続 共有鍵認証方式)

共有 鍵 認証	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	<input type="text"/>
	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) SA有効時間 24 時間
		初回再送時間 10 秒
		再送回数 3 回
		IKEネゴシエーション開始動作 <input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機
	DDP 機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する IPsec受信パケット無通信監視時間 10 秒 再送時間 1 秒 再送回数 3 回
		設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
		保存 キャンセル

この画面は、「IPsec/IKE接続」 – 「基本情報」のIPsec動作モードで“IPsec/IKE（動的VPN）”を選択し、認証方式で“共有鍵認証方式”を設定保存した場合に表示されます。

各項目の説明は、「IKE情報（IKEv1 共有鍵認証方式）」を参照してください。

18.1.2.11.11 IKE 情報（動的VPN接続 RSA デジタル署名認証方式）

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE 接続)]
 → [追加] → [IKE 情報（動的VPN接続 RSA デジタル署名認証方式）]

IKE情報(動的VPN接続 RSAデジタル署名認証方式)

RSA デジ タル 署 名 認 証	相手装置証明書識別番号	指定なし
	自装置証明書識別番号	使用できる自装置証明書が存在しません
	秘密鍵識別番号	使用できる秘密鍵が存在しません
	自装置証明書情報の送信	<input checked="" type="radio"/> 証明書要求ペイロード受信時 <input type="radio"/> 常時
証明書要求	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する 認証局識別番号 指定なし	
	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
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)
	SA有効時間	24 時間
初回再送時間	10 秒	
再送回数	3 回	
IKEネゴシエーション開始動作	<input checked="" type="radio"/> 対象パケット送信契機 <input type="radio"/> 対象回線接続契機	
	<input checked="" type="radio"/> <input type="radio"/> 使用しない 使用する	
DPD 機能	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
	再送回数	3 回

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

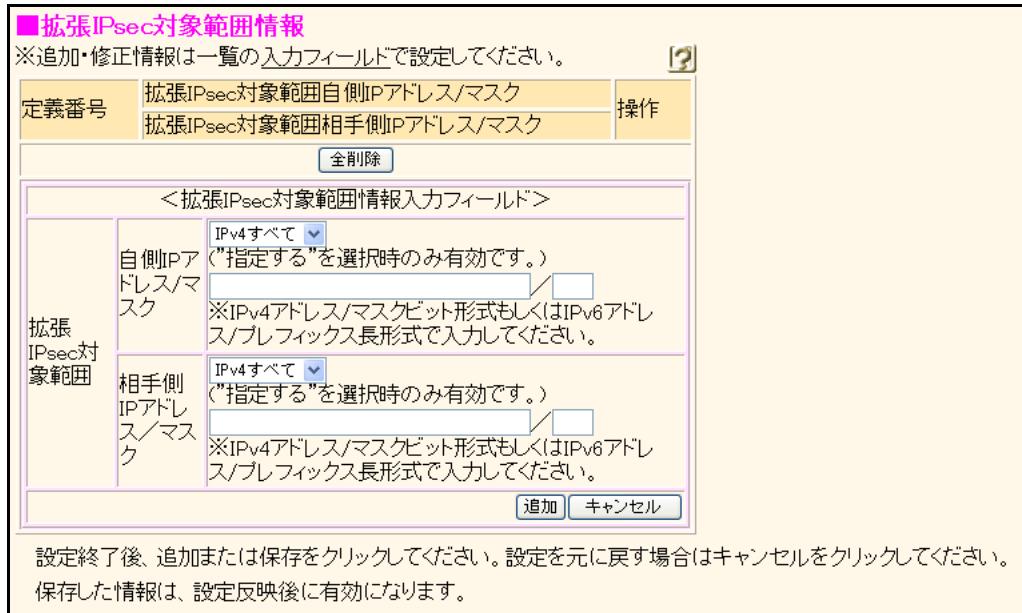
保存 **キャンセル**

この画面は、「IPsec/IKE 接続」 – 「基本情報」のIPsec動作モードで“IPsec/IKE（動的VPN）”を選択し、認証方式で“RSA デジタル署名認証方式”を設定保存した場合に表示されます。

各項目の説明は、「IKE 情報（IKEv1 RSA デジタル署名認証方式）」を参照してください。

18.1.2.11.12 拡張IPsec対象範囲情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報 (IPsec/IKE接続)]
→[追加]→[拡張IPsec対象範囲情報]



現在、設定されている拡張IPsec対象範囲情報の定義が表示されています。拡張IPsec対象範囲の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

拡張IPsec対象範囲設定は、自側（相手側）IPアドレス／アドレスマスクを複数定義することができます。

拡張IPsec対象範囲設定は、IPsec情報の対象パケットで定義した対象パケット以外を通過させる機能であるため、Security Policy Database (SPD) やIKEネゴシエーション（自動鍵設定のみ）には使用されません。

SPDやIKEネゴシエーションに使用するIDペイロードの設定（自動鍵設定のみ）は、IPsec情報の対象パケットで設定してください。

自側（相手側）IPアドレス／アドレスマスク

拡張IPsec対象範囲の送信元IPアドレスおよびアドレスマスクと、あて先IPアドレスおよびアドレスマスクを指定します。IPv4形式またはIPv6形式のアドレスを設定してください。

18.1.2.11.13 動的VPN関連

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE接続)]
 → [追加] → [基本情報 (鍵交換モード: 動的VPN接続)] → [保存] → [動的VPN関連]



18.1.2.11.14 動的VPN関連（基本情報）

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE接続)]
 → [追加] → [基本情報 (鍵交換モード: 動的VPN接続)] → [保存] → [動的VPN関連]
 → [基本情報]



ドメイン情報

動的VPN接続で使用するドメイン情報を選択します。

選択できない場合は、「動的VPN情報」 – 「クライアント
関連情報」 – 「ドメイン情報」を設定してください。

相手側ユーザID

動的VPN接続時に識別する相手側ユーザIDを50文字以内で指定します。

使用できる文字は、半角英数字、"-"、"_"、"_"です。

相手側ユーザIDは、ドメイン名と結合して動的VPN接続要求を受信したときに接続先情報を決定するために使用されます。

18.1.2.11.15 動的VPN関連（相手側ネットワーク情報）

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [接続先情報 (IPsec/IKE接続)]
 → [追加] → [基本情報（鍵交換モード：動的VPN接続）] → [保存] → [動的VPN関連]
 → [相手側ネットワーク情報]

■相手側ネットワーク情報

※追加・修正情報は一覧の入力フィールドで設定してください。

定義番号	動的VPNで接続する相手側ネットワーク	テンプレートを使用して接続要求	操作
全削除			
<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	<input type="text"/> <small>※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。</small>		
テンプレートを使用して接続要求	<input checked="" type="radio"/> しない <input type="radio"/> する		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている相手側ネットワーク情報の定義が表示されています。相手側ネットワークの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

動的VPNで接続する相手側ネットワーク

動的VPNで接続する相手側ネットワークをIPv4アドレスとマスクビット数（またはマスク値）またはIPv6アドレスとプレフィックス長で指定します。

- IPv4 アドレスを指定する場合
IPv4アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから1で連続した値にしてください。
デフォルトルートを設定する場合は、0.0.0.0/0 (0.0.0.0/0.0.0.0) を指定します。
- IPv6 アドレスを指定する場合
IPv6アドレスとプレフィックスの組み合わせで指定します。リンクローカルアドレスは指定できません。
デフォルトルートを設定する場合は、::/0を指定します。

テンプレートを使用して接続要求

指定した相手側ネットワークが動的VPNの接続契機となるIPv4/IPv6パケットの検出条件の設定でinvite条件に一致した場合に、テンプレートを使用して接続要求を発行するかどうかを選択します。

相手側ネットワークは、相手装置から動的VPN接続要求を受信したときに接続先を特定する条件として使用されます。

また、“しない”を選択した場合は、自装置からの動的VPN接続要求を発行するときにテンプレートを使用しないで、本接続先から動的VPN接続要求を発行します。接続先から動的VPN接続をするときは、通常“しない”を選択してください。

18.1.2.12 接続種別：別インタフェースから送出

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」
 → 「接続先情報（別インタフェースから送出）」 → 「追加」

相手情報 - ネットワーク情報(rmt0) - **接続先情報(ap0-0)**

別インタフェースから送出	基本情報	接続制御情報	マルチルーティング情報
	トラップ情報		

「接続制御情報」、「マルチルーティング情報」および「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。ただし、「接続制御情報」の監視方式は常時監視のみとなります。

18.1.2.12.1 基本情報

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」
 → 「接続先情報（別インタフェースから送出）」 → 「追加」 → 「基本情報」

■**基本情報**

接続先名	ap0-0
送出先インターフェース	LAN0
転送先ルータ	IPv4ルータ IPv6ルータ

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

接続先名

この接続先を識別するための名称を8文字以内で指定します。

送出先インターフェース

パケットを送出するインターフェースを選択します。

転送先ルータ（IPv4/IPv6 ルータ）

LAN インタフェースにパケットを送出するときの転送先ルータのIP アドレスを指定します。

送出先インターフェースが LAN インタフェースの場合は、必ず設定してください。転送ルータの IP アドレスは、利用する LAN インタフェースと同じセグメントにする必要があります。異なるセグメントの場合は、転送できません。

有効範囲)

1.0.0.1 ~ 126.255.255.254
 128.0.0.1 ~ 191.255.255.254
 192.0.0.1 ~ 223.255.255.254
 ::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

18.1.2.13 接続先種別：MPLS トンネル接続

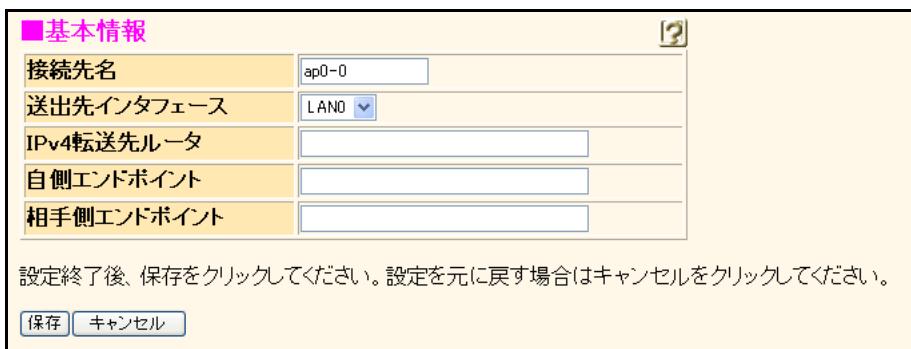
[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (MPLS トンネル接続)]
→ [追加]



「接続制御情報」、「マルチルーティング情報」および「トラップ情報」は、「接続先種別：ATM 接続」を参照してください。

18.1.2.13.1 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (MPLS トンネル接続)]
→ [追加] → [基本情報]



接続先名

この接続先を識別するための名称を8文字以内で指定します。

送出先インターフェース

パケットを送出するインターフェースを選択します。

IPv4 転送先ルータ

LAN インタフェースにパケットを送出する際の転送先ルータのアドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

自側エンドポイント

IPv4 形式のアドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

相手側エンドポイント

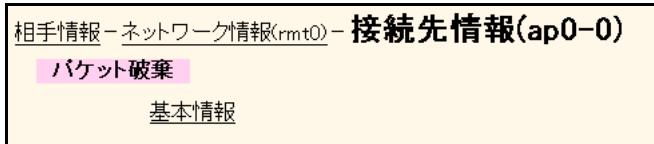
IPv4 形式のアドレスを指定します。送出先インターフェースが LAN インタフェースの場合は必ず設定してください。転送ルータのアドレスには利用する LAN インタフェースと同じセグメントにする必要があります。異なるセグメントの場合、転送は行えません。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

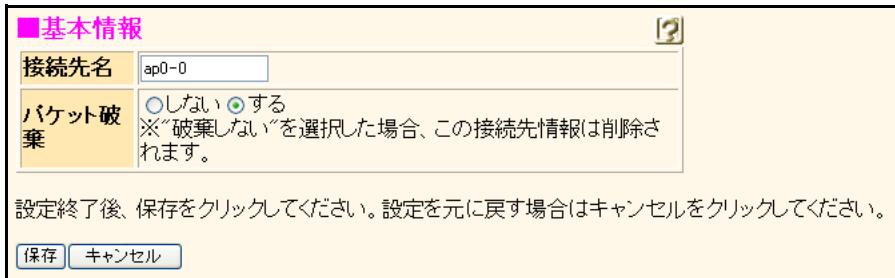
18.1.2.14 接続先種別：パケット破棄

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (パケット破棄)]
→ [追加]



18.1.2.14.1 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [接続先情報 (パケット破棄)]
→ [追加] → [基本情報]



接続先名

この接続先を識別するための名称を8文字以内で指定します。この接続先利用時には、すべてのパケットが破棄されます。

パケット破棄

送信するパケットをすべて破棄する場合は、“する”を選択します。

18.1.3 PPP 関連

適用機種 全機種

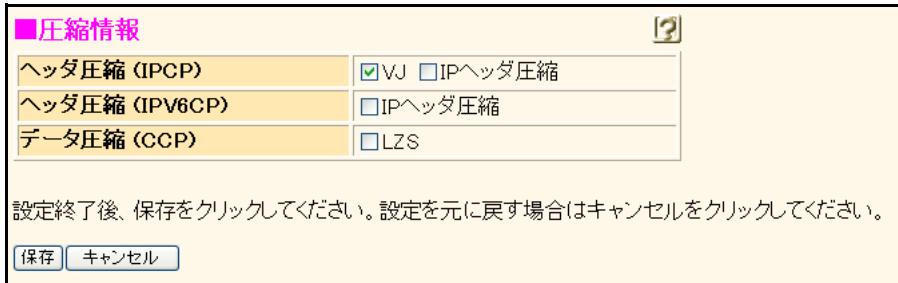
[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[PPP 関連]



Si-R180B、260B では、「MP 情報」は表示されません。

18.1.3.1 圧縮情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[PPP 関連]→[圧縮情報]



送信するパケットのヘッダ部分の圧縮を行う機能です。使用する設定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

Si-R180B、260B では、“データ圧縮 (CCP)” の設定項目は表示されません。

ヘッダ圧縮 (IPCP)

IPCP で使用する圧縮アルゴリズムを選択します。

- VJ
VJ ヘッダ圧縮 (RFC1144 準拠) を使用してヘッダ圧縮を行います。
- IP ヘッダ圧縮
IP ヘッダ圧縮 (RFC2507 / RFC2508 準拠) を使用してヘッダ圧縮を行います。

ヘッダ圧縮 (IPV6CP)

IPV6CP で使用する圧縮アルゴリズムを選択します。

- IP ヘッダ圧縮
IP ヘッダ圧縮 (RFC2507 / RFC2508 準拠) を使用してヘッダ圧縮を行います。

データ圧縮 (CCP) (Si-R220C、220D、240B、370、370B、570、570B)

CCP で使用するデータ圧縮アルゴリズムを選択します。

- LZS
LZS 圧縮 (RFC1974 準拠) を使用してデータ圧縮を行います。

こんな事に気をつけて

圧縮機能を MP で使用する場合、「ネットワーク情報」→「PPP 関連」→「MP 情報」の受信パケット順序制御で“する”を選択してください。受信パケット順序制御しないと圧縮機能が正しく動作しません。

18.1.3.2 MP 情報

適用機種 Si-R220C, 220D, 370, 370B, 570, 570B

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[PPP 関連]→[MP 情報]

■MP情報

MP回線初回リンク数

MP回線最大リンク数

最小分割長

しない
 する
 回線使用率 猶予時間
 回線増加条件 % 秒
 回線削減条件 % 秒

受信パケット順序制御 しない する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

Si-R220C、220D では、MP回線最大リンク数の項目は表示されません。

MP 回線初回リンク数

回線接続時に接続するチャネル数を以下の範囲で指定します。省略時は 1 が設定されます。

機種	リンク数
Si-R220C、220D	1～2
Si-R370、370B、570、570B	1～23

MP 回線最大リンク数 (Si-R370、370B、570、570B)

MP 通信の最大チャネル数を 2～23 の範囲で指定します。
省略時は 2 が設定されます。

最小分割長

送信データの最小分割長を 1～1524 の範囲で指定します。
最小分割単位に 128 バイトが設定されます。省略時は、最小分割長 256 バイト、最小分割単位 128 バイトが設定されたものとして動作します。

トラフィックによる増減

回線負荷に応じて帯域幅（1B、2B）を自動的にコントロールする機能を使用する場合は、“する”を選択し、回線増減の条件も指定します。

回線増加／削減条件

指定した回線使用率を超えた（削減の場合は下回った）状態が“猶予時間”以上続いた時点で、回線の接続（削減の場合は切断）を行います。回線使用率は 0～100%、猶予時間は 0～3600 秒の範囲で指定できます。

受信パケット順序制御

MP を使用すると、パケットの順序が入れ替って届く場合があります。正しい順序に並べ変えて受信する場合は“する”を選択します。

こんな事に気をつけて

- MP を使用する場合、受信パケット順序制御で“しない”を選択すると、以下の機能が正しく動作しません。
 - ・ ブリッジ機能
 - ・ ヘッダ圧縮機能
 - ・ データ圧縮機能

18.1.4 IP 関連

適用機種 全機種

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]

相手情報 - ネットワーク情報(rmt0)					
共通情報	接続先情報	PPP関連	IP関連	IPv6関連	ブリッジ関連
IP基本情報			RIP情報		OSPF情報
スタティック経路情報			IPフィルタリング情報		IDS情報
TOS値書き換え情報			RIPフィルタリング情報		NAT情報
静的NAT情報			NATあて先変換情報		帯域制御(WFO)情報
Ingressポリソールーティング情報			CLP値設定情報		マルチキャスト情報
EXP値書き換え情報			動的VPN情報		

Si-R260B、370、570以外では、「CLP値設定情報」は表示されません。

18.1.4.1 IP 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[IP 基本情報]

■IP基本情報

IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する 相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
MSS書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 書き換えサイズ <input type="text"/> バイト

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

IP アドレス

このネットワーク情報のIPアドレスを固定で使用する場合は“設定する”を選択します。“相手側IPアドレス”または“自側IPアドレス”的一方だけを指定し、他方を省略することもできます。動的に割り当てられる環境で、誤つてIPアドレスを設定した場合は、ルーティング動作は行いますが、ルータから通信できないことがあります。

また、RIPを使用する場合はどちらか一方を省略することはできません。両方とも指定するか“設定しない”を選択します。BGPまたはOSPFを使用する場合は、両方とも指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

こんな事に気をつけて

OSPFを使用するインター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を使用しないインターフェースとして扱われます。

MSS 書き換え

MSS書き換え機能の設定をします。MSS書き換え機能を使用する場合、“使用する”を選択し、書き換えサイズを0または160～1460の範囲で指定します。PPPoE (PPP over Ethernet) を利用する場合は、1414に設定します。0を指定した場合は、MSS書き換え機能が無効となります。

18.1.4.2 RIP 情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP 関連] → [RIP 情報]

The dialog box has a title bar 'RIP情報'. It contains two main sections: 'RIP送信' (RIP Transmission) and 'RIP受信' (RIP Reception). Under 'RIP送信', there are four options: '送信しない' (Not sending), 'V1で送信する' (Send via V1), 'V2で送信する' (Send via V2), and 'V2(Multicast)で送信する' (Send via V2 Multicast). Under 'RIP受信', there are three options: '受信しない' (Not receiving), 'V1で受信する' (Receive via V1), and 'V2、V2(Multicast)で受信する' (Receive via V2 or V2 Multicast). Below these sections is a note: «RIP 送信時は加算するメトリック値を設定してください。» (Please set the metric value to be added during RIP transmission). A dropdown menu shows '0'. Another note below says: «RIP V2使用時で認証パケットを破棄しない時はRIP V2のパスワードを設定してください。» (If you do not discard authentication packets during RIP V2 use, please set the RIP V2 password). A section for '認証パケット' (Authentication packet) has two options: '破棄する' (Discard) and '破棄しない' (Do not discard), with a password input field next to it. At the bottom, a note says: 「設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。」 (After setting is completed, click 'Save'. If you want to restore the original settings, click 'Cancel'). There are '保存' (Save) and 'キャンセル' (Cancel) buttons at the bottom.

RIP を使用できるインターフェースの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。

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。

RIP 送信

RIP 情報を送信するかどうかを選択します。送信する設定にすると、RIP 情報を定期的に送信します。RIP 送信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、ブロードキャストで送信します。
- V2
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストで送信します。
- V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、マルチキャストで送信します。

RIP 受信

RIP 情報を受信するかどうかを選択します。RIP 受信を行う場合は、RIP の種類を選択します。

- V1
ルーティングプロトコルに RIP V1 を使用し、受信します。
- V2、V2 (Multicast)
ルーティングプロトコルに RIP V2 を使用し、ブロードキャストおよびマルチキャストを受信します。

メトリック値

RIP 送信時に加算するメトリック値を選択します。

認証パケット

RIP V2 使用時にだけ有効な設定です。RIP V2 では、同じ パスワードグループでだけ RIP 情報の交換を行うことができます。パスワード認証による RIP 情報の交換を行う場合は、“破棄しない”を選択し、パスワードを 16 文字以内で設定します。“破棄する”を選択した場合は、パスワード認証による RIP 情報の交換は行いません。

18.1.4.3 OSPF 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[OSPF 情報]

■OSPF情報	
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
エリア定義番号	0
出力コスト	10
Helloパケット送信間隔	10 秒
隣接ルータ停止確認間隔	40 秒
パケット再送間隔	5 秒
LSUパケット送信遅延時間	1 秒
認証方式	<input checked="" type="radio"/> 認証を行わない <input type="radio"/> テキスト認証 鍵種別 <input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数 認証鍵 <input type="text"/> <input type="radio"/> MD5認証 MD5認証鍵ID <input type="text"/> MD5認証鍵 <input type="text"/>
パケット送信	<input type="radio"/> 抑止する <input checked="" type="radio"/> 抑止しない
送信方法	<input checked="" type="radio"/> マルチキャストで送信 <input type="radio"/> ユニキャストで送信
MTU値確認	<input checked="" type="radio"/> 確認する <input type="radio"/> 確認しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

ループバックインターフェースも含めて、OSPF を使用できるインターフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。

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 を使用できるインターフェースには上限があります。OSPF を使用するインターフェースの合計が本装置の上限を超えないように設定する必要があります。

OSPF機能

OSPFを使用するかどうかを選択します。

エリア定義番号

OSPFエリア情報のエリア定義番号を10進数を使用して指定します。OSPFエリア情報は、「ルーティングプロトコル情報」 - 「OSPF関連」で設定することができます。省略時は、0が設定されます。

出力コスト

OSPF出力コストを1～65535の範囲で指定します。省略時は、10が設定されます。

Helloパケット送信間隔

OSPF隣接関係の維持に使用する、Helloパケットの送信間隔を指定します。通常は、“10秒”を指定します。

有効範囲)

1～18時間

1～1092分

1～65535秒

こんな事に気をつけて

OSPF隣接ルータ間で同じHelloパケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Helloパケット送信間隔より大きな値を指定する必要があります。Helloパケット送信間隔の4倍を設定することをお薦めします。通常は“40秒”を指定します。

有効範囲)

1～18時間

1～1092分

1～65535秒

こんな事に気をつけて

OSPF隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。隣接ルータ停止確認間隔は、装置起動時に指定ルータおよび副指定ルータの選出を開始するまでの待機時間にも使用されます。大きな値を設定した場合は、経路交換の開始が遅れます。

パケット再送間隔

OSPFパケットを再送する間隔を指定します。省略時は、5秒が設定されます。

有効範囲)

1～18時間

1～1092分

3～65535秒

LSUパケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSUパケットでは、LSA(Link State Advertisement)を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1秒が設定されます。

有効範囲)

1～18時間

1～1092分

1～65535秒

こんな事に気をつけて

LSAは、生成されてから1時間が経過すると破棄されます。LSU送信遅延時間に1時間以上を指定しないでください。正しくルーティングできない場合があります。

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が“文字列”的場合は、8文字以内で指定します。鍵種別が“16進数”的場合は、16進数を使用して16桁以内で指定します。16桁未満の値を指定したときは左詰めで設定され、残りは16桁になるまで0x0でパディングされます。

MD5認証鍵ID

MD5認証鍵IDを1～255の範囲で指定します。

MD5認証鍵

MD5認証鍵を指定します。16文字以内で指定します。

パケット送信

OSPFパケットの送信を抑止するかどうかを選択します。

送信方法

OSPFパケットの送信方法を選択します。OSPFパケットをマルチキャストで受信できない装置と接続する場合は、“ユニキャストで送信”を選択します。

MTU値確認

隣接ルータとOSPFパケットのMTU値の確認を行うかどうかを選択します。隣接ルータの仕様により、MTU値の不整合が回避できないときは、“確認しない”を選択します。

18.1.4.4 スタティック経路情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP関連] → [スタティック経路情報]

■スタティック経路情報

※追加・修正情報は一覧の入力フィールドで設定してください。

あて先IPアドレス/マスク	メトリック値	優先度	操作
全削除			
<スタティック経路情報入力フィールド>			
<input type="radio"/> デフォルトルート <input checked="" type="radio"/> 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		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路の情報の定義が表示されています。仕様一覧 [\[2.3 システム最大値一覧\] \(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を指定した場合は、あて先IPアドレス／アドレスマスクを指定します。

メトリック値

このスタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して0～254の範囲で指定します。省略時は、0が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
EBGP	20
OSPF	110
RIP	120
IBGP	200
DNS	15

複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じになるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、「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」にある「ECMP情報」でECMPを使用するように設定します。ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。

こんな事に気をつけて

- 同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。
- 優先度が0のスタティック経路情報と、優先度が0以上のスタティック経路情報は同時に設定できません。
 - 優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。

18.1.4.5 IP フィルタリング情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP 関連] → [IP フィルタリング情報]

優先順位	動作	方向	ACL定義番号	操作
			ACL定義名	
条件にあてはまらない場合の動作		透過		<input type="button" value="修正"/> <input type="button" value="初期化"/>
<input type="button" value="全削除"/>				
<IP フィルタリング情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断			
方向	入出力 <input type="button" value="参照"/>			
ACL 定義番号	<input type="button" value="参照"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IP フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行います。IP フィルタリングの定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリングの動作を以下の 3 つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 透過（接続中のみ）
条件と一致する場合に、回線が接続しているときはパケット透過し、切断しているときは遮断します。
- 遮断
条件と一致する場合にパケットを遮断します。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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なお、入力パケットはIPアドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL定義番号を指定します。

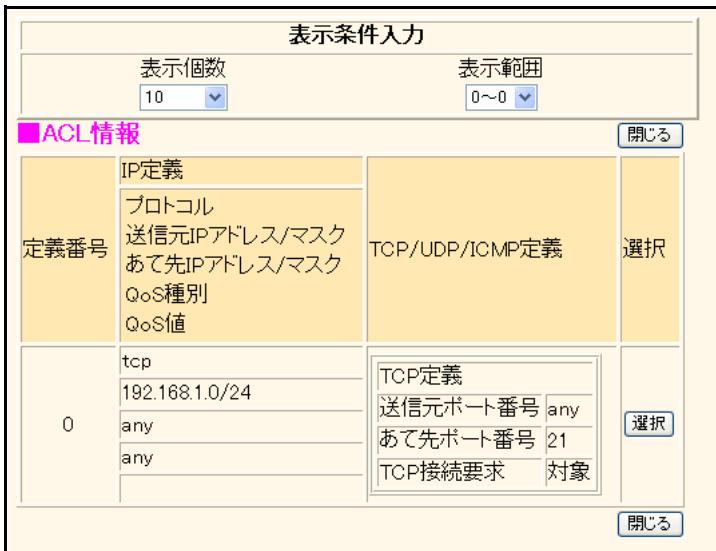
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の〔選択〕ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[IP フィルタリング情報]→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IP フィルタリング情報」の ACL 定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IP フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。「ACL 定義参照」ボタンをクリックした場合は、「選択」ボタンは表示されません。「閉じる」ボタンをクリックして、画面を閉じてください。

18.1.4.5.1 IP フィルタリング情報（旧定義）

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[IP フィルタリング情報]
→「表示条件入力（旧定義）」

表示条件入力							
表示定義内容							
旧定義							
■IP フィルタリング情報							
※追加・修正情報は一覧の入力フィールドで設定してください。 [?]							
優先順位	動作	プロトコル	送信元IPアドレス/マスク	TCP接続要求	TOS	方向	操作
			送信元ポート番号				
あて先IPアドレス/マスク	あて先ポート番号	ICMPタイプ	ICMPコード	透過	<input type="button" value="修正"/>	<input type="button" value="初期化"/>	
					条件にあてはまらない場合の動作		
<input type="button" value="全削除"/>							
<IP フィルタリング情報入力フィールド>							
動作 <input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断							
プロトコル <input type="checkbox"/> すべて <input type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)							
送信元情報	IP アドレス	<input type="text"/>					
	アドレスマスク	<input type="text"/> 0.0.0.0					
	ポート番号	<input type="text"/>					
あて先情報	IP アドレス	<input type="text"/>					
	アドレスマスク	<input type="text"/> 0.0.0.0					
	ポート番号	<input type="text"/>					
ICMP	タイプ	<input type="text"/>					
	コード	<input type="text"/>					
TCP 接続要求 <input checked="" type="radio"/> 対象 <input type="radio"/> 対象外							
TOS <input type="text"/>							
方向 <input type="text"/> 入出力							
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>							

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

表示条件入力に、「旧定義」を選択した場合に、IP フィルタリング情報の旧定義が表示されます。

動作

IP フィルタリングの動作を以下の3つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 透過（接続中のみ）
条件と一致する場合に、回線が接続しているときはパケット透過し、切断しているときは遮断します。
- 遮断
条件と一致する場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

フィルタリング条件としてのIP アドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIP アドレスと定義するアドレスマスクの論理積、定義するIP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号をフィルタリングの対象とします。また、ポート番号を複数指定する場合は、“”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMP

タイプ

フィルタリング条件として ICMP パケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMP タイプ値を複数指定する場合は、“”で区切れます。範囲指定の場合は “-” で区切れます。10組まで指定できます。省略時は “any” が設定され、すべての ICMP タイプ値がフィルタリングの対象となります。

コード

フィルタリング条件として ICMP パケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMP コード値を複数指定する場合は、“”で区切れます。範囲指定の場合は “-” で区切れます。10組まで指定できます。省略時は “any” が設定され、すべての ICMP コード値がフィルタリングの対象となります。

TCP 接続要求

TCP プロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

TOS

フィルタリング条件として IP パケットの TOS フィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOS フィールド値を複数指定する場合は、“”で区切れます。範囲指定の場合は、“-” で区切れます。10組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値がフィルタリングの対象となります。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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なお、入力パケットはIPアドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

18.1.4.5.2 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）

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連] → [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」[修正]

※追加・修正情報は一覧ので設定してください。

優先順位 動作 方向 ACL 定義番号 操作
ACL 対応定義

<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
 透過(接続中のみ)
 遮断
 SPI

情報保持タイム 5 分

保存 キャンセル 一覧へ戻る

全削除

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されているIP フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断や SPI を指定し、IP フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリング定義のどれにも一致しない場合の動作を以下の4つから選択します。

- 透過
IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 透過（接続中のみ）
IP フィルタリング定義のどれにも一致しない場合に、回線が接続しているときはパケットを透過し、切断しているときは遮断します。
- 遮断
IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。

SPI

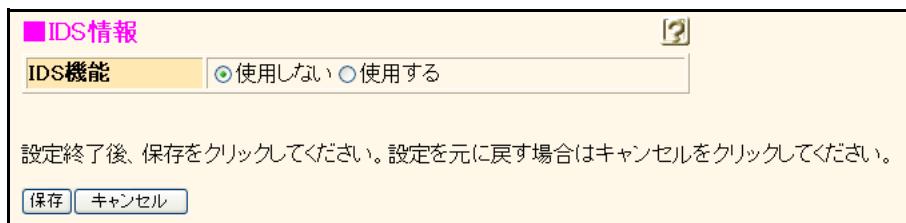
IP フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPI セッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

18.1.4.6 IDS情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP関連] → [IDS情報]



IDS機能

侵入などのセキュリティに影響を与えるパケットを検知する場合は、“使用する”を選択します。

18.1.4.7 TOS 値書き換え情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[TOS 値書き換え情報]

優先順位	ACL 定義番号	新TOS	操作
	ACL 定義名		

新TOS

新TOS:

ACL 定義番号: [参照]

[追加] [キャンセル]

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている TOS 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行います。TOS 値書き換えの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された TOS 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義”または“旧定義”から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 TOS

IP パケットに新しく指定する TOS フィールド値を 16 進数を使用して、0～ff の範囲で指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

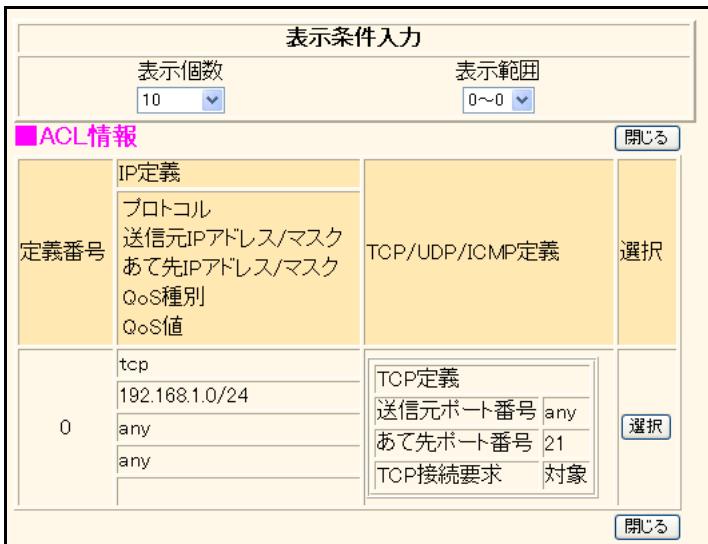
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[TOS 値書き換え情報]→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「TOS 値書き換え情報」の ACL 定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「TOS 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。「ACL 定義参照」ボタンをクリックした場合は、「選択」ボタンは表示されません。「閉じる」ボタンをクリックして、画面を閉じてください。

18.1.4.7.1 TOS値書き換え情報（旧定義）

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]→[TOS値書き換え情報]
→「表示条件入力（旧定義）」

表示条件入力				
表示定義内容				
旧定義				
■TOS値書き換え情報				
※追加・修正情報は一覧の入力フィールドで設定してください。				
優先順位	プロトコル	送信元IPアドレス/マスク	TOS	操作
		送信元ポート番号	新TOS	
あて先IPアドレス/マスク				
あて先ポート番号				
全削除				
<TOS値書き換え情報入力フィールド>				
プロトコル		<input type="button" value="すべて"/> (番号指定: <input type="text"/> "その他"を選択時の み有効です)		
送信元 情報	IPアレ ス	<input type="text"/>		
	アドレス マスク	<input type="text"/> 0.0.0.0		
	ポート番 号	<input type="text"/>		
あて先 情報	IPアレ ス	<input type="text"/>		
	アドレス マスク	<input type="text"/> 0.0.0.0		
	ポート番 号	<input type="text"/>		
TOS		<input type="text"/>		
新TOS		<input type="text"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。				

表示条件入力に、“旧定義”を選択した場合に、TOS値書き換え情報の旧定義が表示されます。

プロトコル

TOS値書き換えの条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

TOS値書き換え条件としてのアドレス情報を設定します。

IPアドレス／アドレスマスク

TOS値書き換え条件としてのIPアドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIPアドレスと、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定する場合は、すべてのポート番号が TOS 書き換えの対象となります。また、ポート番号を複数指定する場合は、 “,” で区切れます。範囲指定の場合は、 “-” で区切れます。送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0～ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、 “,” で区切れます。範囲指定の場合は、 “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値が書き換えの対象となります。

新 TOS

IP パケットに新しく指定する TOS フィールド値を 16 進数を使用して、0～ff の範囲で指定します。

18.1.4.8 RIP フィルタリング情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP 関連]
 → [RIP フィルタリング情報]

RIP フィルタリング情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
全削除					
<RIP フィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 <input checked="" type="radio"/> 受信 <input type="radio"/> 送信 <input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定				
フィルタリング条件	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 IP アドレス <input type="text"/> アドレスマスク <input type="text"/> 0.0.0.0				
メトリック値	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、(送信方向／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。

動作

フィルタリング条件に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかどうかをチェックします。RIP パケット受信時にチェックするか、送信時にチェックするかを選択します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定します。
経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致” または、“マスクした結果が一致” を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、RIP経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

18.1.4.9 NAT情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]→[NAT情報]

■NAT情報	
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ
グローバルアドレス	<input type="text"/>
アドレス個数	1 個
アドレス割当てタイマ	5 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパスルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
FTP	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SIP	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
H.323	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
DNS	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP Trap	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
IRC	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
NTDメインログオン	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
各種ストリーミング	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
各種オンラインゲーム	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

NATの使用

“マルチNAT”を選択すると、複数の端末と併用できます。“静的NATのみ”を選択すると静的NAT情報の条件に一致しないパケットは変換されません。NATを使用しない場合は、以降の設定は無効です。

こんな事に気をつけて

本装置では「相手情報」、「LAN情報」および「テンプレート情報」のインターフェースでアドレス変換機能を設定できます。ただし、使用する場合は、グローバルアドレスを使用するインターフェースだけで設定します。また、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。

アドレス個数

複数個のグローバルアドレスを使用する場合は、上述のグローバルアドレスを先頭とし、連続した複数のアドレスを指定します。その個数を1～16の範囲で指定します。なお、アドレス個数の設定は、グローバルアドレスを指定した場合にだけ有効です。省略時は、1が設定されます。

アドレス割当てタイマ

アドレス変換情報は一定の時間、該当する通信が行われないと、自動的に解放されます。解放するための猶予時間を0～24時間の範囲で指定します。0を指定すると、タイマによる情報の解放は行われません。省略時は、5分が設定されます。

グローバルアドレス

特定のグローバルアドレスを使用するときに指定します。指定しない場合は自動で割り当てられます。

NAT セキュリティ

- 通常
相手サーバがNATを使用している際など、要求先とは別のアドレスから応答します。
- 高い
ftpやdnsの要求する相手からの応答かどうかをチェックします。

IPsec パススルー

- 有効
相手ごとに1つのIPsecパスを接続することができます。
- 無効
IPsecクライアントがNATトランザル機能を使用することができます。

こんな事に気をつけて

IPsecクライアントがNATトランザ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パスしか接続できません。

アプリ対応

使用するアプリケーションを選択し、それぞれに“有効”を設定します。

- FTP
- SIP
- H.323
- DNS
- SNMP Trap
- IRC
- NT ドメインログオン
- 各種ストリーミング
- 各種オンラインゲーム

18.1.4.10 静的NAT情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]→[静的NAT情報]

■静的NAT情報

※追加・修正情報は一覧ので設定してください。

プライベートアドレス	プライベートポート番号	プロトコル	操作																		
グローバルアドレス	グローバルポート番号																				
条件にあてはまらない場合の動作		破棄	<input type="button" value="修正"/>																		
<input type="button" value="初期化"/>																					
<input type="button" value="全削除"/>																					
<静的NAT情報入力フィールド> <table border="1"> <tr> <td>プライベート IP情報</td> <td>IPアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>ポート番号</td> <td>すべて</td> <td>(番号指定:<input type="text"/> "その他"を選択時の み有効です)</td> </tr> <tr> <td>グローバル IP情報</td> <td>IPアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>ポート番号</td> <td>すべて</td> <td>(番号指定:<input type="text"/> "その他"を選択時の み有効です)</td> </tr> <tr> <td>プロトコル</td> <td>すべて</td> <td>(番号指定:<input type="text"/> "その他"を選択 時のみ有効です)</td> </tr> <tr> <td colspan="3"> <input type="button" value="追加"/> <input type="button" value="キャンセル"/> </td> </tr> </table>				プライベート IP情報	IPアドレス	<input type="text"/>	ポート番号	すべて	(番号指定: <input type="text"/> "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	<input type="text"/>	ポート番号	すべて	(番号指定: <input type="text"/> "その他"を選択時の み有効です)	プロトコル	すべて	(番号指定: <input type="text"/> "その他"を選択 時のみ有効です)	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		
プライベート IP情報	IPアドレス	<input type="text"/>																			
ポート番号	すべて	(番号指定: <input type="text"/> "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	<input type="text"/>																			
ポート番号	すべて	(番号指定: <input type="text"/> "その他"を選択時の み有効です)																			
プロトコル	すべて	(番号指定: <input type="text"/> "その他"を選択 時のみ有効です)																			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>																					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

マルチNATを使用すると、アドレス変換情報を固定で持つことができます。現在、設定されている固定のアドレス変換情報の定義が表示されています。静的NATの定義の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プライベートIP情報

IPアドレス

固定でアドレス変換を行う場合に、ローカルネットワーク側のIPアドレスを指定します。省略はできません。

ポート番号

固定でアドレス変換を行う場合に、ローカルネットワーク側のポート番号を選択します。“その他”を選択して、ポート番号を指定する場合は、10進数を使用して1～65535の範囲で指定します。

なお、グローバルポート番号を範囲指定する場合は、その範囲のグローバルポート番号は、指定したプライベートポート番号を先頭とした範囲へ変換されます。

例) プライベートポート番号: 1000

グローバルポート番号: 10000-11000

NAT変換後

プライベートポート番号: 1000-2000

グローバルIP情報

IPアドレス

固定でアドレス変換を行う場合にリモートネットワーク側のIPアドレスを指定します。省略時は、先頭のグローバルアドレスに対して有効な指定となります。

IPアドレスを指定する場合は、“-”で区切った1組の範囲を指定します。

ポート番号

固定でアドレス変換を行う場合にリモートネットワーク側のポート番号を選択します。“その他”を選択して、ポート番号を指定する場合は、10進数を使用して1～65535の範囲から1つ、または“-”で区切った1組の範囲を指定します。

プロトコル

固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- esp (50)
- ah (51)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

18.1.4.10.1 静的NAT情報（条件にあてはまらない場合の動作）

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP関連] → [静的NAT情報] → 「条件にあてはまらない場合の動作」[修正]

■静的NAT情報

※追加・修正情報は一覧の入力フィールドで設定してください。

プライベートアドレス	プライベートポート番号	プロトコル	操作
グローバルアドレス	グローバルポート番号		
<静的NAT情報入力フィールド(条件にあてはまらない場合)>			
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 破棄		
保存 <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>			
<input type="button" value="全削除"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている静的NAT定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。

動作

静的NAT定義のどれにも一致しない場合のIPフィルタリングの動作を以下の2つから選択します。

- 透過
静的NAT定義のどれにも一致しない場合にパケットを透過します。
- 破棄
静的NAT定義のどれにも一致しない場合にパケットを破棄します。

18.1.4.11 NAT あて先変換情報

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「IP 関連」→「NAT あて先変換情報」

■NAT あて先変換情報

※追加・修正情報は一覧の入力フィールドで設定してください。

プライベートアドレス	グローバルアドレス	操作
全削除		
<NAT あて先変換情報入力フィールド>		
プライベートアドレス	<input type="text"/>	
グローバルアドレス	<input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている NAT あて先変換情報の定義が表示されています。NAT あて先変換の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プライベートアドレス

ローカルネットワーク側の IP アドレスを指定します。

なお、グローバルアドレスを範囲指定した場合、その範囲のグローバルアドレスはここで指定したアドレスを先頭とした範囲に変換されます。

例) プライベートアドレス : 192.168.1.100

グローバルアドレス : 172.16.1.100-172.16.1.200

NAT あて先変換後

プライベートアドレス : 192.168.1.100-192.168.1.200

グローバルアドレス

リモートネットワーク側の IP アドレスを指定します。範囲指定する場合は、"-" で区切れます。範囲指定した場合、プライベートアドレスも自動的に範囲指定されます。

18.1.4.12 帯域制御 (WFQ) 情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP関連] → [帯域制御 (WFQ) 情報]

定義番号	ACL定義番号	帯域	操作
			<input type="button" value="全削除"/>

<帯域制御(WFQ)情報入力フィールド>

帯域	<input type="radio"/> 最優先	
	<input type="radio"/> ベストエフォート	
	<input checked="" type="radio"/> 使用率	<input type="text"/> %
	<input type="radio"/> 使用帯域	<input type="text"/> Kbps
	<input type="radio"/> 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

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報の ACL 定義が表示されています。帯域制御の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を 10 進数を使用して、1～99 の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが 100 を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbps または 1～100Mbps の範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

- 回線に LAN を使用して、帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。
- 回線に ATM を使用して、帯域制御機能を有効に動作させる場合は、適切な VC 速度を設定してください。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

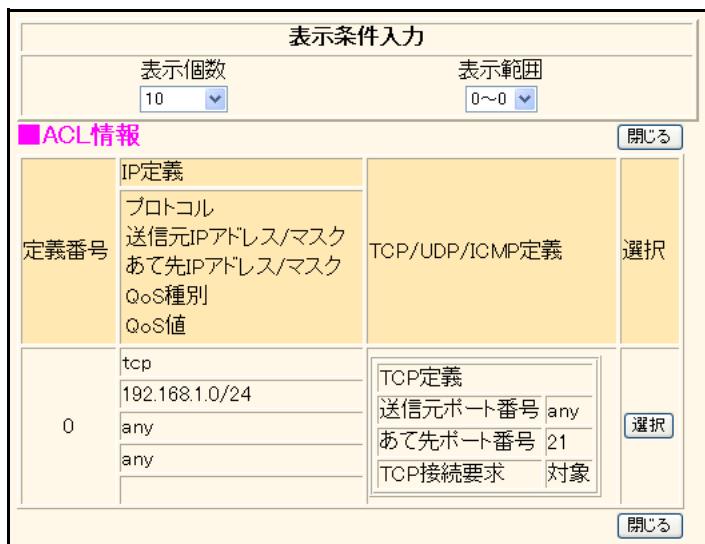
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP 関連] → [帯域制御 (WFQ) 情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「帯域制御 (WFQ) 情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「帯域制御 (WFQ) 情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.4.12.1 帯域制御 (WFQ) 情報 (旧定義)

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP関連] → [帯域制御 (WFQ) 情報]
→ 「表示条件入力 (旧定義)」

表示条件入力			
表示定義内容			
[旧定義]			
■帯域制御(WFQ)情報			
※追加・修正情報は一覧の <input type="text"/> で設定してください。 [?] <input type="button" value="全削除"/>			
定義番号	送信元IPアドレス/マスク	対象TOSフィールド値	操作
プロトコル	送信元ポート番号	あて先IPアドレス/マスク	帯域
	あて先ポート番号		
<input type="button" value="全削除"/>			
<帯域制御WFQ情報入力フィールド>			
プロトコル	すべて (番号指定: <input type="text"/> "その他"を選択時の み有効です)		
送信元 情報	IPアドレ ス	<input type="text"/>	
	アドレス マスク	0 0.0.0.0 <input type="button" value=""/>	
	ポート番 号	<input type="text"/>	
あて先 情報	IPアドレ ス	<input type="text"/>	
	アドレス マスク	0 0.0.0.0 <input type="button" value=""/>	
	ポート番 号	<input type="text"/>	
対象TOSフィール ド値	<input type="text"/>		
帯域	<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="button" value=""/> <input type="radio"/> 帯域を他と共有 <input type="text"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。			

表示条件入力に、“旧定義”を選択した場合に、帯域制御 (WFQ) 情報の旧定義が表示されます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IP アドレス／アドレスマスク

帯域制御の対象となるIPアドレスおよびアドレスマスクを指定します。対象となるパケットのIPアドレスと定義するアドレスマスクの論理積と、定義するIPアドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 TOS フィールド値

帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのTOSフィールド値が帯域制御の対象となります。

帯域

帯域の使用率または帯域値を指定します。

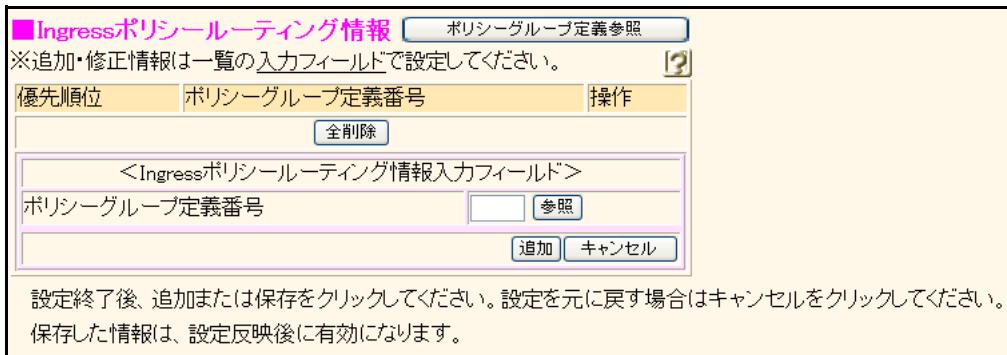
- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

回線にLANを使用して、帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。
回線にATMを使用して、帯域制御機能を有効に動作させる場合は、適切なVC速度を設定してください。

18.1.4.13 Ingress ポリシールーティング情報

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連]
 → [Ingress ポリシールーティング情報]



現在、設定されている Ingress ポリシールーティング情報の定義が表示されています。処理は優先順位 1 から順に行われます。Ingress ポリシールーティング情報の定義数は、仕様一覧 「2.3 システム最大値一覧」 (P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に、指定されたポリシーグループに定義された送出先へパケットを送出します。

ポリシーグループ定義番号

[参照] ボタンをクリックして、ポリシーグループ定義番号を指定します。

別の画面に「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されます。指定する定義番号欄の「選択」ボタンをクリックし、ポリシーグループ定義番号を設定します。自動的に画面が閉じます。

なお、参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連]
 → [Ingress ポリシールーティング情報] → 「ポリシーグループ定義番号の [参照]」

The screenshot shows a 'Policy Group Information' dialog box with the following details:

表示条件入力		
表示個数 10	表示範囲 0~0	
■ポリシーグループ情報		
定義番号	定義内容	
0	パターン定義	
	バックアップとして使用	acl0
	使用する	acl0
	使用しない	acl1
送出先定義		
lan0	192.168.100.10	

Buttons at the bottom: [閉じる] (Close) and [選択] (Select).

「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ポリシーグループ定義情報の一覧に見たい情報だけを表示させることができます。

参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「Ingress ポリシールーティング情報」のポリシーグループ定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「Ingress ポリシールーティング情報」にポリシーグループ定義番号が設定され、画面が閉じます。[ポリシーグループ定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.4.14 CLP 値設定情報

適用機種 **Si-R260B,370,570**

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連] → [CLP 値設定情報]

優先順位	CLP値	ACL定義番号	操作
		ACL定義名	

CLP値設定情報 [ACL定義参照](#)

※追加・修正情報は一覧ので設定してください。

CLP値 0を設定する 1を設定する

ACL定義番号 [参照](#)

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている CLP 値設定情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。CLP 値設定の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された CLP 値設定を行います。ただし、分割されたパケットに対しては正しく行えません。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

CLP 値

条件に一致した場合に CLP 値に設定する値を以下の 2 つから選択します。

- 0 を設定する
- 1 を設定する

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

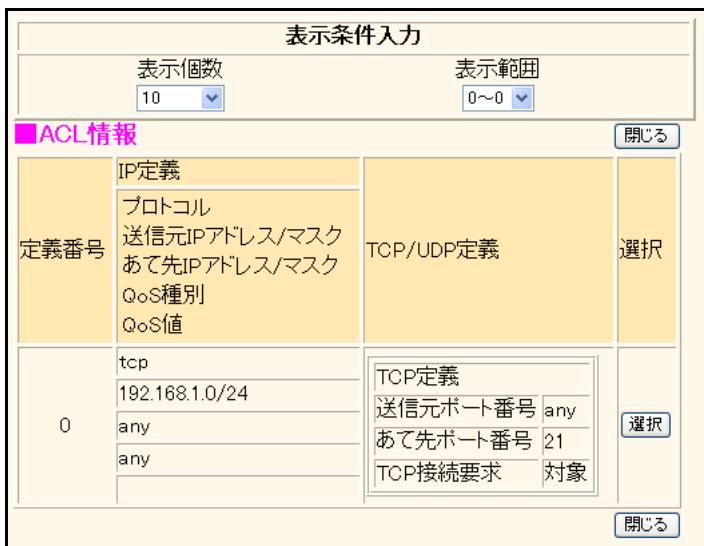
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「IP 関連」→「CLP 値設定情報」→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「CLP 値設定情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「CLP 値設定情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.4.14.1 CLP 値設定情報（旧定義）

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[CLP 値設定情報]
→「表示条件入力（旧定義）」

表示条件入力					
表示定義内容 旧定義					
■CLP値設定情報 ※追加・修正情報は一覧の <input type="text"/> で設定してください。					
優先順位	CLP値	プロトコル	送信元IPアドレス/マスク あて先IPアドレス/マスク あて先ポート番号	TOS	操作
<input type="button" value="全削除"/>					
<CLP値設定情報入力フィールド>					
CLP値	<input checked="" type="radio"/> 0を設定する <input type="radio"/> 1を設定する				
プロトコル	すべて <input type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)				
送信元情報	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text"/> 0.0.0.0			
	ポート番号	<input type="text"/>			
あて先情報	IPアドレス	<input type="text"/>			
	アドレスマスク	<input type="text"/> 0.0.0.0			
	ポート番号	<input type="text"/>			
TOS	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。					

表示条件入力に、“旧定義”を選択した場合に、CLP 値設定情報の旧定義が表示されます。

CLP 値

条件に一致した場合に CLP 値に設定する値を以下の 2 つから選択します。

- 0 を設定する
- 1 を設定する

プロトコル

CLP 値設定条件としてプロトコルを以下の 6 つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255 の範囲で指定します。

送信元／あて先情報

CLP 値設定条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

CLP 値設定条件としての IP アドレスおよびアドレスマスクを指定します。チェック対象となったパケットの IP アドレスと定義したアドレスマスクの論理積と、定義した IP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。省略時は、すべての IP アドレス／アドレスマスクが CLP 値設定の対象となります。

ポート番号

CLP 値設定条件としてポート番号を 10 進数を使用して、1～65535 の範囲または "any" で指定します。省略時、または "any" を指定した場合は、すべてのポート番号が CLP 値設定の対象となります。また、ポート番号を複数指定する場合は、"-" で区切れます。範囲指定の場合は "--" で区切れます。ポート番号は、送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

CLP 値設定条件として IP パケットの TOS フィールド値を 16 進数を使用して 0～ff の範囲または "any" で指定します。TOS フィールド値を複数指定する場合は "—" で区切れます。範囲指定の場合は "--" で区切れます。10 組まで指定できます。省略時は、すべての TOS フィールド値が CLP 値設定の対象となります。

18.1.4.15 マルチキャスト情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IP 関連] → [マルチキャスト情報]

■マルチキャスト情報	
マルチキャスト機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> static <input type="radio"/> PIM-DM <input type="radio"/> PIM-SM
TTLしきい値	1
PIMプリファレンス値	1024
上流ルータの種類	<input checked="" type="radio"/> PIMルータのみ <input type="radio"/> すべて

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

マルチキャスト機能

リモートインターフェース上でマルチキャスト機能を使用する場合は、どれかのマルチキャスト・プロトコルを選択します。マルチキャストを利用する場合は、インターフェースにIPアドレスを手動で割り当てます。IPアドレスが設定されていないインターフェースでの動作はサポートしていません。

こんな事に気をつけて

- マルチキャスト機能を使用するすべてのインターフェース上で、同じプロトコルを選択してください。同時に複数のプロトコルを利用することはできません。
- NAT機能と併用することはできません。

PIM プリファレンス値

PIMのAssertメッセージに格納されるプリファレンス値を10進数を使用して1～65535の範囲で指定します。初期値は1024です。

並列な経路の存在のためにマルチキャスト・パケットが重複した場合は、PIM Assertメッセージによって、片側の転送経路が遮断されます。この際、プリファレンス値の小さい方の経路が有効になります。PIM Assertメッセージの発行時には、Assert対象となるパケットの発信元へのユニキャスト経路を参照し、発信元へ向かうインターフェースのプリファレンス値をAssertメッセージに格納します。Assertメッセージが出力されるインターフェースのプリファレンス値が格納されるわけではありません。

TTL しきい値

LAN上でマルチキャスト機能を使用するときのTTLしきい値を10進数を使用して1～255の範囲で指定します。初期値は1です。

PIM-SMのPIM Registerパケットによりカプセル化されるマルチキャスト・パケットは、出力先インターフェースのTTLしきい値の設定にかかわらず出力されます。

上流ルータの種類

本装置から上流にルータが存在し、そのルータを経由してマルチキャストパケットが転送される場合、どの種類のルータからのマルチキャストパケット転送を許可するかを設定します。

上流ルータがPIMルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“すべて”を選択します。

こんな事に気をつけて

受信インターフェースと同一のIPセグメントから送信された（直接接続されたホストからの）マルチキャストパケットは、上流ルータの設定にかかわらず転送が行われます。

18.1.4.16 EXP 値書き換え情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[EXP 値書き換え情報]

優先順位	ACL定義番号	EXP	操作
	ACL定義名		

EXP値書き換え情報 [ACL定義参照](#) [?](#)

※追加・修正情報は一覧ので設定してください。

[全削除](#)

<EXP値書き換え情報入力フィールド>

EXP	<input type="text"/>
ACL定義番号	<input type="text"/> 参照

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている EXP 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。EXP 値書き換えの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された EXP 値を書き換えます。ただし、分割されたパケットに対しては正しく行えません。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

EXP

書き換える EXP 値を、0～7 の範囲で指定します。省略時は 0 が設定されます。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

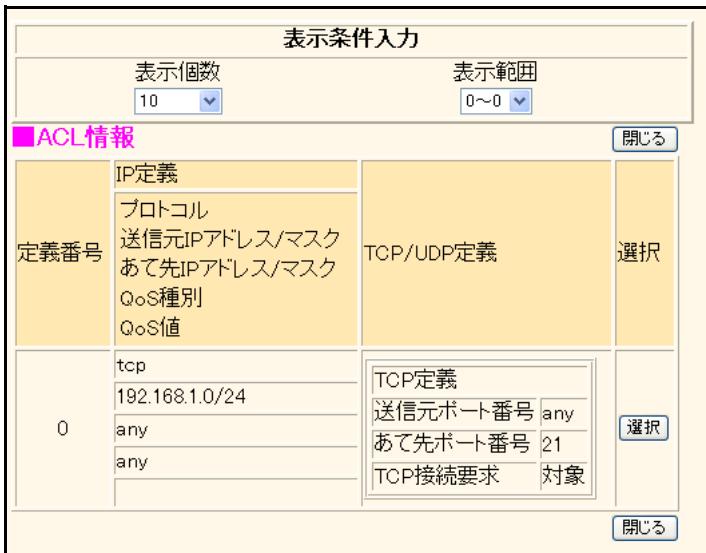
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[EXP 値書き換え情報]→「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「EXP 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「EXP 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.4.16.1 EXP 値書き換え情報（旧定義）

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP 関連]→[EXP 値書き換え情報]
→「表示条件入力（旧定義）」

表示条件入力				
表示定義内容				
旧定義				
■ EXP 値書き換え情報				
※追加・修正情報は一覧の入力フィールドで設定してください。				
優先順位	プロトコル	送信元IPアドレス/マスク	TOS	操作
		送信元ポート番号		
あて先IPアドレス/マスク		EXP		
		あて先ポート番号		
全削除				
<EXP 値書き換え情報入力フィールド>				
プロトコル <input style="border: none; border-radius: 2px; padding: 2px 10px;" type="button" value="すべて"/> (番号指定: <input style="width: 100px;" type="text"/> “その他”を選択時の み有効です)				
送信元 情報	IPアレ ス	<input type="text"/>		
	アドレス マスク	<input type="text" value="0.0.0.0"/>		
	ポート番 号	<input type="text"/>		
あて先 情報	IPアレ ス	<input type="text"/>		
	アドレス マスク	<input type="text" value="0.0.0.0"/>		
	ポート番 号	<input type="text"/>		
TOS <input type="text"/>				
EXP <input type="text"/>				
追加 キャンセル				
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。				

表示条件入力に、“旧定義”を選択した場合に、EXP 値書き換え情報の旧定義が表示されます。

プロトコル

EXP 値書き換え条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

EXP 値書き換え条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

EXP 値書き換え条件としてのIP アドレスおよびアドレスマスクを指定します。チェック対象となったパケットのIP アドレスと定義したアドレスマスクの論理積と、定義したIP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

EXP 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、 “,” で区切れます。範囲指定の場合は “-” で区切れます。ポート番号は、送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

EXP 値書き換え条件として IP パケットの TOS フィールド値を 16 進数を使用して 0～ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値を書き換えの対象となります。

EXP

書き換える EXP 値を、0～7 の範囲で指定します。省略時は 0 が設定されます。

18.1.4.17 動的VPN情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IP関連]→[動的VPN情報]

現在、設定されている動的VPN接続契機パケットのACL定義が表示されています。処理は優先順位1から順に行われます。動的VPN接続契機パケットの検出条件の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43)を参照してください。処理するボタンをクリックし、次のページへ進みます。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報を表示させることができます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動的VPN接続契機パケットの検出を行います。ただし、分割されたパケットに対しては正しく行えません。

動的VPN接続

動的VPN接続を行う場合は、“する”を選択します。

“しない（ネットワーク情報自動取得）”は、相手情報に接続先情報の動的VPN接続定義が行われている必要があります。また、相手情報ごとに1つしか選択できません。

相手ネットマスク

動的VPN接続を開始する場合に、相手を識別するための情報として相手ネットマスクを0~32から選択します。

利用するテンプレート情報

動的VPN接続に利用するテンプレート情報を選択します。

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

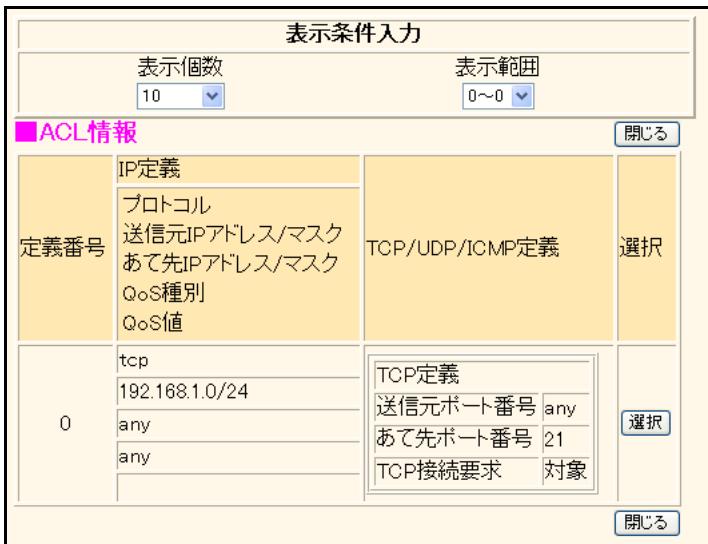
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の「[選択]」ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IP 関連] → [動的VPN情報]
→ 「ACL 定義番号の [参照]」



「ACL情報」 - 「追加」／「修正」 - 「IP定義情報」および「TCP定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報だけを表示させることができます。

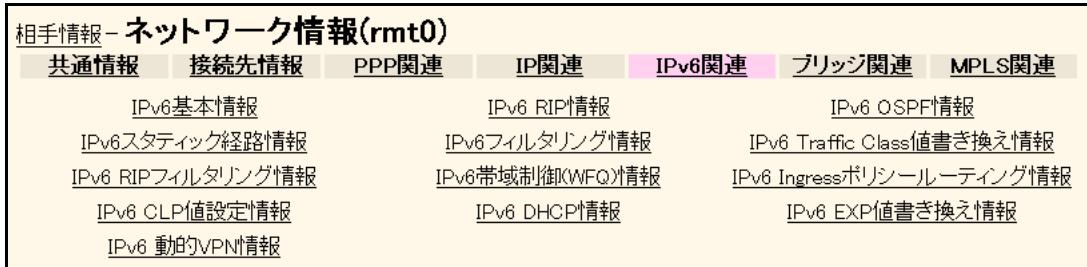
参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「動的VPN情報」のACL定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「動的VPN情報」にACL定義番号が設定され、画面が閉じます。[ACL定義参照]ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

18.1.5 IPv6 関連

適用機種 全機種

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]



Si-R260B、370、570以外では、「IPv6 CLP 値設定情報」は表示されません。

18.1.5.1 IPv6 基本情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 基本情報]

IPv6	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
<input checked="" type="radio"/> ユニキャストアドレスを指定する アドレスまたはプレフィックス <input type="text"/> Valid Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 日 <input type="button" value="▼"/> Pref. Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 日 <input type="button" value="▼"/> フラグ <input type="text"/> c0	
<input type="radio"/> エニキャストアドレスを指定する アドレス <input type="text"/>	
<input checked="" type="radio"/> ユニキャストアドレスを指定する アドレスまたはプレフィックス <input type="text"/> Valid Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 日 <input type="button" value="▼"/> Pref. Lifetime <input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり <input type="text"/> 日 <input type="button" value="▼"/> フラグ <input type="text"/> c0	
<input type="radio"/> エニキャストアドレスを指定する アドレス <input type="text"/>	
<input checked="" type="radio"/> ユニキャストアドレスを指定する アドレスまたはプレフィックス <input type="text"/>	

ルータ広報	Valid Lifetime	<input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり 30 日
	Pref. Lifetime	<input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり 7 日
	フラグ	c0
	<input type="radio"/> エニキャストアドレスを指定する アドレス	
	<input checked="" type="radio"/> ユニキャストアドレスを指定する アドレスまたはプレフィックス	
	Valid Lifetime	<input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり 30 日
	Pref. Lifetime	<input type="radio"/> 期限なし <input checked="" type="radio"/> 期限あり 7 日
	フラグ	c0
	<input type="radio"/> エニキャストアドレスを指定する アドレス	
	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 最大送信間隔 600 秒 最小送信間隔 200 秒 Router Lifetime 1800 秒 MTU Reachable Time 0 ミリ秒 Retrans Timer 0 ミリ秒 Cur Hop Limit 64 フラグ 00	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

IPv6

IPv6 通信を行う場合は、“使用する”を選択します。

インターフェース ID

インターフェース ID を設定します。

- 自動
装置の MAC アドレスから自動生成されるインターフェース ID を使用します。通常は、“自動”を選択します。
- 指定する
16 ビットごとに区切り文字 (:) を入れて、16 進数を使用して 16 行でインターフェース ID を指定します。このとき、他装置と同じインターフェース ID とならないような値を指定します。
記述例) 2001:db8:7654:3210

IPv6 アドレス

この装置で使用するユニキャストアドレスまたはエニキャストアドレスを4個まで設定できます。

- ユニキャストアドレスを指定する
ユニキャストアドレスを指定する場合に選択します。
- エニキャストアドレスを指定する
エニキャストアドレスを指定する場合に選択します。

アドレスまたはプレフィックス

本装置のLAN側のIPv6アドレスを標準的なIPv6アドレス表記方式で指定します。本装置ではプレフィックス長は64に固定されます。インターフェースID部分がすべて0の場合、指定したアドレスはプレフィックスとして解釈され、実際に利用するアドレスはそのアドレスにインターフェースIDを付与したものとなります。リンクローカルアドレスは指定できません。

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場合は、上位を “dhcp@インターフェース名” の形式で指定し、下位80ビット分を標準的なIPv6アドレス表記方式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているrmtインターフェースを指定します。

記述例)

2001:db8:1111:1000:1:2:3:4

完全なIPv6アドレスとして解釈されます。

2001:db8:1111:1000::

プレフィックスとして解釈され、インターフェースID部分にはインターフェースIDが付与されます。

dhcp@rmt0:1000::1

rmt0インターフェースで動作しているIPv6 DHCP クライアントが取得したプレフィックスを使用して完全なIPv6アドレスを指定します。

dhcp@rmt0:1000::

rmt0インターフェースで動作しているIPv6 DHCP クライアントが取得したプレフィックスを使用してプレフィックスを指定します。

Valid Lifetime

ルータ広報のプレフィックス情報ごとに設定するValid Lifetimeを指定します。通常は、“30日”を指定します。

有効範囲)

0～365日

0～8760時間

0～525600分

0～31536000秒

IPv6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指定をした場合は、IPv6 DHCP クライアントが取得したValid Lifetimeと比較して短い方が有効になります。

Pref. Lifetime

ルータ広報のプレフィックス情報ごとに設定するPreferred Lifetimeを指定します。通常は、“7日”を指定します。

有効範囲)

0～365日

0～8760時間

0～525600分

0～31536000秒

IPv6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指定をした場合は、IPv6 DHCP クライアントが取得したPreferred Lifetimeと比較して短い方が有効になります。

フラグ

ルータ広報のプレフィックス情報ごとに設定するフラグフィールドの内容を16進数を使用して2桁で指定します。この領域の値として、RFC2461で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。

- on-link flag 80
- autonomous address-configuration flag 40

通常は“c0”を指定します。

アドレス

本装置のエニキャストアドレスを標準的なIPv6アドレス表記方式で指定します。本装置ではプレフィックス長は128に固定されます。インターフェースIDによるアドレス生成は行われません。

ルータ広報

ルータ広報メッセージ (router advertisement message) を送信する場合は “送信する” を選択し、以下の項目を設定します。

最大送信間隔

ルータ広報メッセージの最大送信間隔を指定します。初期値は 600 秒です。省略はできません。

有効範囲) 4 ~ 1800

最小送信間隔

ルータ広報メッセージの最小送信間隔を指定します。初期値は 200 秒です。省略はできません。

有効範囲) 3 ~ 最大送信間隔の 3 / 4

Router Lifetime

ルータ広報で送信する Router Lifetime を指定します。初期値は 1800 秒です。省略はできません。

有効範囲) 0 または最大送信間隔 ~ 9000

MTU

ルータ広報で送信する MTU option を指定します。省略時は、MTU option を含みません。

有効範囲) 1280 ~ 1500

Reachable Time

ルータ広報で送信する Reachable Time を指定します。省略値は 0 ミリ秒です。

有効範囲) 0 ~ 3600000

Retrans Timer

ルータ広報で送信する Retrans Timer を指定します。省略値は 0 ミリ秒です。

有効範囲) 0 ~ 4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit を指定します。省略値は 64 です。

有効範囲) 0 ~ 255

フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を 16 進数を使用して 2 衔で指定します。この領域の値として、RFC2461 で以下の値が定義されています。必要に応じて以下の値の論理和を設定します。省略値は 00 です。

- Managed address configuration flag 80
- Other stateful configuration flag 40

18.1.5.2 IPv6 RIP 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 RIP 情報]

IPv6 RIP情報		
RIP送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する メトリック値 <input type="text" value="0"/>	
RIP受信	<input checked="" type="radio"/> 受信しない <input type="radio"/> 受信する	
集約経路送信	集約経路	破棄経路設定
	<input type="radio"/> デフォルトルート	<input checked="" type="checkbox"/> 設定する
	<input checked="" type="radio"/> ネットワーク指定	<input checked="" type="checkbox"/> 設定する
	<input type="text"/>	<input checked="" type="checkbox"/> 設定する
	<input type="text"/>	<input checked="" type="checkbox"/> 設定する
サイトローカルプレフィックス	<input type="radio"/> 交換しない <input checked="" type="radio"/> 交換する	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

RIPを使用できるインターフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。

RIP 送信

RIPを送信する場合は、“送信する”を選択します。

メトリック値

“送信する”を選択した場合に、加算するメトリック値を選択します。

RIP 受信

RIPを受信する場合は、“受信する”を選択します。

集約経路送信

RIPで集約経路を送信する場合に、集約して広報する経路を設定します。

集約経路

デフォルトルートまたはネットワーク指定を選択し、集約して広報する経路を指定します。

集約経路情報は、集約される経路情報がないときでも広報されます。また、同じあと先の経路情報がルーティングテーブルにないときでも広報され、ルーティングテーブルには設定されません。

- デフォルトルート
集約経路情報としてデフォルトルートだけを広報します。
- ネットワーク指定
集約経路情報をプレフィックス／プレフィックス長で指定します。指定した集約経路情報は広報され、集約経路情報に含まれる経路情報は広報されません。

破棄経路設定

広報した集約経路情報により本装置に送られたIPv6パケットをルーティングするための経路情報がないときに、そのあと先へは到達不能であることをICMPv6で通知することができます。チェックしないときは、そのあと先への経路がないことがICMPv6で通知されます。

チェック時は、集約経路情報と同じあと先の経路情報が破棄経路としてルーティングテーブルに設定されます。

18.1.5.3 IPv6 OSPF 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6関連]→[IPv6 OSPF情報]

■ IPv6 OSPF情報	
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
エリア定義番号	0
出力コスト	10
Helloパケット送信間隔	10 秒
隣接ルータ停止確認間隔	40 秒
パケット再送間隔	5 秒
LSUパケット送信遅延時間	1 秒
パケット送信	<input type="radio"/> 抑止する <input checked="" type="radio"/> 抑止しない
MTU値確認	<input checked="" type="radio"/> 確認する <input type="radio"/> 確認しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

IPv6 OSPFを使用できるインターフェースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

OSPF機能

OSPFを使用する場合は、“使用する”を選択します。

エリア定義番号

エリアの定義番号を10進数を使用して指定します。OSPFエリア情報は、「ルーティングプロトコル情報」→「IPv6 OSPF関連」で設定することができます。省略時は、0が設定されます。

出力コスト

OSPF出力コストを1～65535の範囲で指定します。省略時は、10が設定されます。

サイトローカルプレフィックス

サイトローカルプレフィックスを交換する場合は、“交換する”を選択します。

Helloパケット送信間隔

OSPF隣接関係の維持に使用する、Helloパケットの送信間隔を指定します。省略時は、10秒が設定されます。

有効範囲)

1～18時間

1～1092分

1～65535秒

こんな事に気をつけて

OSPF隣接ルータ間で同じHelloパケットの送信間隔を指定してください。

隣接ルータ停止確認間隔

OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。隣接ルータ停止確認間隔は、Hello パケット送信間隔より大きな値を指定する必要があります。Hello パケット送信間隔の 4 倍を設定することをお薦めします。省略時は、40 秒が設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

OSPF 隣接ルータ間で同じ隣接ルータ停止確認間隔を指定してください。

パケット送信

OSPF パケットの送信を抑止する場合は、“抑止する”を選択します。

MTU 値確認

隣接ルータと OSPF パケットの MTU 値の確認を行う場合は、“確認する”を選択します。

隣接ルータの仕様により、MTU 値の不整合が回避できないときは、“確認しない”を選択します。

パケット再送間隔

OSPF パケットを再送する間隔を指定します。省略時は、5 秒が設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

3 ~ 65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。省略時は、1 秒が設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

18.1.5.4 IPv6 スタティック経路情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IPv6 関連]
→ [IPv6 スタティック経路情報]

■ IPv6 スタティック経路情報

※追加・修正情報は一覧の入力フィールドで設定してください。

あて先プレフィックス／プレフィックス長	メトリック値	優先度	操作
全削除			
<IPv6 スタティック経路情報入力フィールド>			
<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定			
ネットワーク	あて先プレフィックス／プレフィックス長	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	
メトリック値	1		
優先度	0		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 スタティック経路情報の定義が表示されています。IPv6 スタティック経路の定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に1つしか設定できません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を選択した場合は、あて先プレフィックスとプレフィックス長を指定します。あて先プレフィックスにリンクローカルアドレスは指定できません。なお、あて先プレフィックス／プレフィックス長に ::/0 を設定した場合、“デフォルトルート”を指定したものとして動作します。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1～15 から選択します。RIP に再配布したときは、設定した RIP メトリック値 +1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して 0～254 の範囲で指定します。省略時は、0 が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
OSPF	110
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定するときは、以下の点に注意してください。

- 優先度が 0 のスタティック経路情報と、優先度が 0 以上のスタティック経路情報は同時に設定できません。
- 優先度が同じスタティック経路情報は同時に設定できません。

18.1.5.5 IPv6 フィルタリング情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]
→[IPv6 フィルタリング情報]

優先順位	動作	方向	ACL定義番号	操作
			ACL定義名	
条件にあてはまらない場合の動作		透過		<input type="button" value="修正"/> <input type="button" value="初期化"/>
<input type="button" value="全削除"/>				
<IPv6 フィルタリング情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断 方向 <input type="button" value="入出力"/> ACL定義番号 <input type="button" value="参照"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行います。IPv6 フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく行えません。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

表示条件入力は、“ACL 対応定義”または“旧定義”から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリングの動作を以下の 3 つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 透過（接続中のみ）
条件と一致する場合に、回線が接続されていればパケットを透過し、切断されていれば遮断します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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IPv6アドレス／プレフィックス長とあて先IPv6アドレス／プレフィックス長
 - 送信元ポート番号とあて先ポート番号
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL 定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

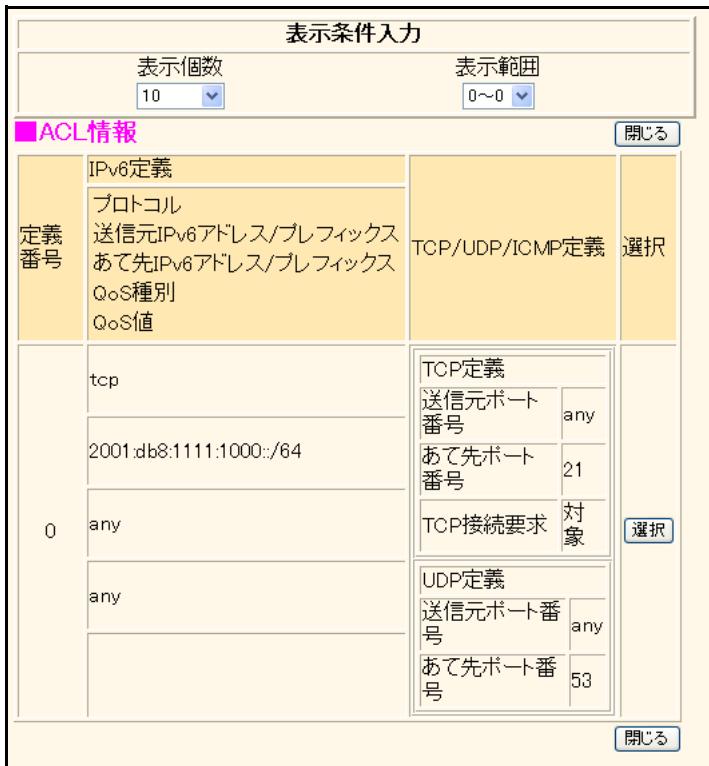
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の【選択】ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「IPv6 関連」
 →「IPv6 フィルタリング情報」→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.5.5.1 IPv6 フィルタリング情報（旧定義）

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「IPv6 関連」
 →「IPv6 フィルタリング情報」→「表示条件入力（旧定義）」

表示条件入力								
表示定義内容								
旧定義								
■ IPv6 フィルタリング情報								
※追加・修正情報は一覧の <input type="text"/> で設定してください。								
優先順位	動作	送信元IPv6アドレス/プレフィックス長	TCP接続要求	Traffic Class	方向	操作	<input type="button" value="修正"/> <input type="button" value="初期化"/>	
		送信元ポート番号						
		あて先IPv6アドレス/プレフィックス長						
		あて先ポート番号						
		ICMPv6タイプ						
ICMPv6コード								
条件にあてはまらない場合の動作		透過						
<input type="button" value="全削除"/>								
<IPv6 フィルタリング情報入力フィールド>								
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断						
プロトコル		すべて <input checked="" type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)						
送信元情報	IPv6アドレス/プレフィックス長	<input type="text"/> <input checked="" type="checkbox"/>						
	ポート番号	<input type="text"/>						
あて先情報	IPv6アドレス/プレフィックス長	<input type="text"/> <input checked="" type="checkbox"/>						
	ポート番号	<input type="text"/>						
ICMPv6	タイプ	<input type="text"/>						
	コード	<input type="text"/>						
TCP接続要求		<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外						
Traffic Class		<input type="text"/>						
方向		<input type="text"/> <input type="button" value="追加"/> <input type="button" value="キャンセル"/>						

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

表示条件入力に、"旧定義"を選択した場合に、IPv6 フィルタリング情報の旧定義が表示されます。

動作

IPv6 フィルタリングの動作を以下の3つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 透過（接続中のみ）
条件と一致する場合に、回線が接続されていればパケットを透過し、切断されていれば遮断します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の5つから選択します。（）内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、"その他"を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

フィルタリング条件としての IPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積、定義する IPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件として、ポート番号を 10 進数を使用して、1～65535 の範囲または "any" で指定します。"any" を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、"-" で区切れます。範囲指定の場合は、"~" で区切れます。送信元情報とあて先情報を合わせて 10 組まで指定できます。

ICMPv6

タイプ

フィルタリング条件として ICMPv6 パケットのタイプ値を 10 進数を使用して 0～255 の範囲または "any" で指定します。ICMPv6 タイプ値を複数指定する場合は "—" で区切れます。範囲指定の場合は "~" で区切れます。10 組まで指定できます。省略時は "any" が設定され、すべての ICMPv6 タイプ値がフィルタリングの対象となります。

コード

フィルタリング条件として ICMPv6 パケットのコード値を 10 進数を使用して 0～255 の範囲または "any" で指定します。ICMPv6 コード値を複数指定する場合は "—" で区切れます。範囲指定の場合は "~" で区切れます。10 組まで指定できます。省略時は "any" が設定され、すべての ICMPv6 コード値がフィルタリングの対象となります。

TCP 接続要求

TCP プロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、" 対象 " を選択します。プロトコルに TCP を設定した場合だけ有効です。

Traffic Class

フィルタリング条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0～ff の範囲または "any" で指定します。Traffic Class 値を複数指定する場合は "—" で区切れます。範囲指定の場合は "~" で区切れます。10 組まで指定できます。省略時は "any" が設定され、すべての Traffic Class 値がフィルタリングの対象となります。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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 IPv6 アドレス／プレフィックス長とあて先 IPv6 アドレス／プレフィックス長
 - 送信元ポート番号とあて先ポート番号
 なお、リバースを指定した場合は、入力パケットは IPv6 アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

18.1.5.5.2 IPv6 フィルタリング情報（条件にあてはまらない場合の動作）

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」 → 「IPv6 関連」
 → 「IPv6 フィルタリング情報」 → 「条件にあてはまらない場合の動作」 [修正]

表示条件入力
表示定義内容
ACL 対応定義

■ IPv6 フィルタリング情報 [ACL 定義参照](#)

※ 追加・修正情報は一覧ので設定してください。

優先順位	動作	方向	ACL 定義番号	操作
			ACL 定義名	
<IPv6 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	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断 <input type="radio"/> SPI 情報保持タイム <input type="text" value="5"/> 分			
	<input type="button" value="保存"/>	<input type="button" value="キャンセル"/>	<input type="button" value="一覧へ戻る"/>	<input type="button" value="全削除"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このネットワークに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断や SPI を指定し、IPv6 フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の4つから選択します。

- 透過
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 透過（接続中のみ）
条件と一致する場合に、回線が接続されていればパケットを透過し、切断されていれば遮断します。
- 遮断
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPv6 フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPI セッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

18.1.5.6 IPv6 Traffic Class 値書き換え情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]
→[IPv6 Traffic Class 値書き換え情報]

表示条件入力
表示定義内容
ACL対応定義

■ IPv6 Traffic Class 値書き換え情報 [ACL定義参照](#)

※追加・修正情報は一覧ので設定してください。

優先順位	ACL定義番号	新Traffic Class	操作
	ACL定義名		<input type="button" value="全削除"/>

<IPv6 Traffic Class 値書き換え情報入力フィールド>

新Traffic Class	<input type="text"/>
ACL定義番号	<input type="text"/> 参照

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 Traffic Class 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Traffic Class 値書き換えの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義”または“旧定義”から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 Traffic Class

IPv6 パケットに新しく指定する IPv6 Traffic Class 値を 16 進数を使用して、0～ff の範囲で指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

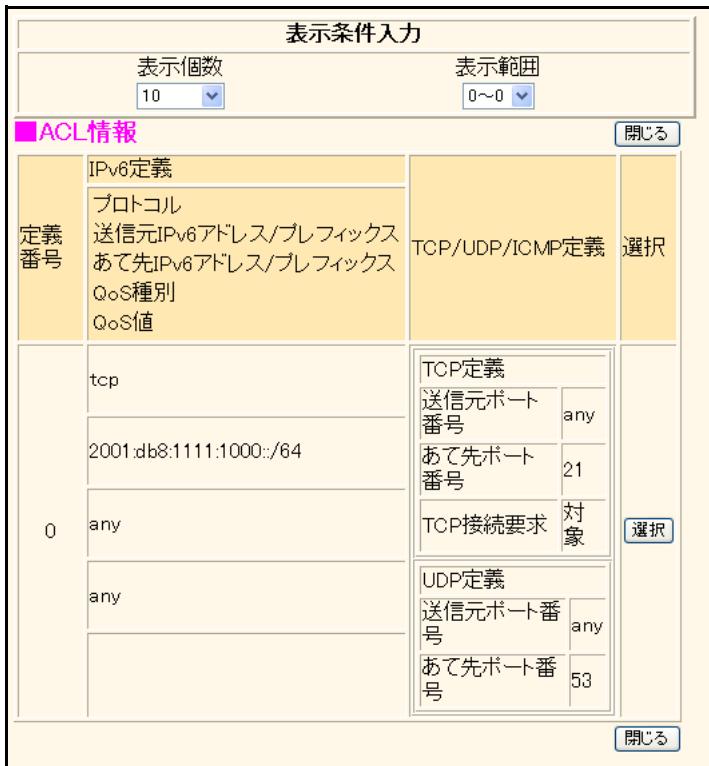
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」 → 「IPv6 関連」
 → 「IPv6 Traffic Class 値書き換え情報」 → 「ACL 定義番号の [参照]」



「ACL情報」 - 「追加」／「修正」 - 「IPv6定義情報」、「TCP定義情報」および「UDP定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

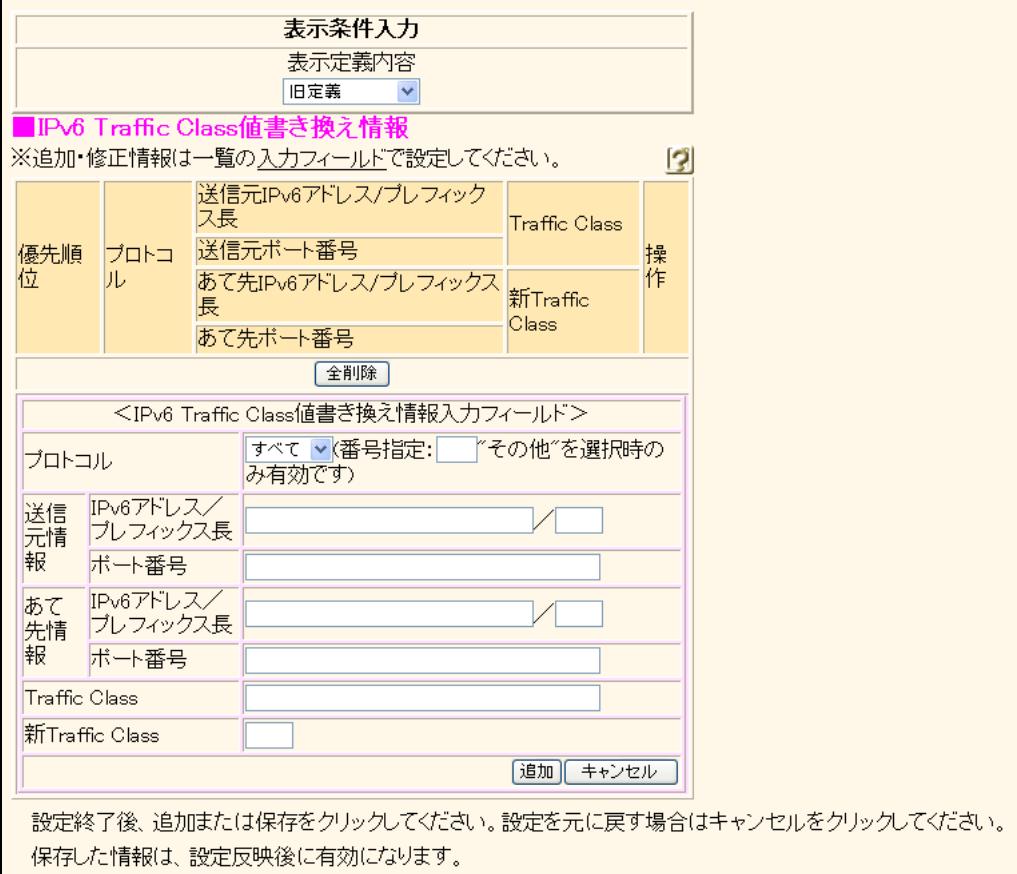
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報だけを表示させることができます。

参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「IPv6 Traffic Class 値書き換え情報」のACL定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IPv6 Traffic Class 値書き換え情報」にACL定義番号が設定され、画面が閉じます。[ACL定義参照]ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

18.1.5.6.1 IPv6 Traffic Class 値書き換え情報（旧定義）

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連]
 → [IPv6 Traffic Class 値書き換え情報] → 「表示条件入力（旧定義）」



The screenshot shows the 'IPv6 Traffic Class 値書き換え情報' configuration screen. At the top, there is a dropdown menu set to 'Old Definition'. Below it, a section titled 'IPv6 Traffic Class 値書き換え情報' contains a table for defining traffic classes. The table has columns for 'Priority' (優先順位), 'Protocol' (プロトコル), 'Source Address/Prefix Length' (送信元IPv6アドレス/プレフィックス長), 'Traffic Class' (Traffic Class), and 'Operation' (操作). There are four rows in the table, each corresponding to a different traffic class definition. Below the table is a button labeled 'Delete All' (全削除). A large input field labeled '<IPv6 Traffic Class 値書き換え情報入力フィールド>' follows, containing several sub-fields for protocol, source address, destination address, traffic class, and new traffic class. At the bottom of the input field is a 'Add' (追加) button and a 'Cancel' (キャンセル) button. A note at the bottom of the screen says: 'After setting is completed, click the "Save" button. If you want to restore the original settings, click the "Cancel" button. The saved information becomes effective after the setting is reflected.' (設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。)

表示条件入力に、“旧定義”を選択した場合に、IPv6 Traffic Class 値書き換え情報の旧定義が表示されます。

プロトコル

IPv6 Traffic Class 書き換え条件としてプロトコルを以下の5つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

IPv6 Traffic Class 値書き換え条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

IPv6 Traffic Class 値書き換え条件としてのIPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6 アドレスと定義するプレフィックス長の論理積、定義するIPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

IPv6 Traffic Class 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、”,” で区切れます。範囲指定の場合は “-” で区切れます。送信元情報とあて先情報を合わせて 10 組まで指定できます。

Traffic Class

IPv6 Traffic Class 値書き換え条件として IPv6 パケットの IPv6 Traffic Class 値を 16 進数を使用して 0～ff の範囲または “any” で指定します。Traffic Class フィールド値を複数指定する場合は ”,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての IPv6 Traffic Class 値が書き換えの対象となります。

新 Traffic Class

IPv6 パケットに新しく指定する IPv6 Traffic Class 値を 16 進数を使用して、0～ff の範囲で指定します。

18.1.5.7 IPv6 RIP フィルタリング情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IPv6 関連]
→ [IPv6 RIP フィルタリング情報]

■ IPv6 RIP フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	方向	フィルタリング条件	メトリック値	操作
<input type="button" value="全削除"/>					
<IPv6 RIP フィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input checked="" type="radio"/> すべて				
	<input type="radio"/> デフォルトルート				
	<input type="radio"/> 経路情報指定				
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致				
プレフィックス /プレフィック ス長	<input type="text"/> <input type="checkbox"/>				
メトリック 値	<input type="text"/>				
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

RIP 受信（送信）時には、優先順位の高い定義から順に受信（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。なお、一致した以降の条件は参照されません。また、受信（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。

動作

フィルタリング対象に該当する RIP 経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合に RIP 経路情報を透過します。
- 遮断
条件と一致した場合に RIP 経路情報を遮断します。

方向

フィルタリングを RIP 受信時に行うか、RIP 送信時に行うかを選択します。

- 受信
RIP 受信時に、フィルタリングを行います。
- 送信
RIP 送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、RIP 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、RIP経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

フィルタリング条件で“すべて”を選択したときは、メトリック値を設定しても無効となります。

18.1.5.8 IPv6帯域制御 (WFQ) 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6関連]
→[IPv6帯域制御 (WFQ) 情報]

表示条件入力			
表示定義内容			
ACL対応定義			
■ IPv6帯域制御(WFQ)情報			
ACL定義参照			
※追加・修正情報は一覧の <input type="text"/> で設定してください。			
定義番号	ACL定義番号	帯域	操作
全削除			
<IPv6帯域制御(WFQ)情報入力フィールド>			
帯域	<input type="radio"/> 最優先		
	<input type="radio"/> ベストエフォート		
	<input checked="" type="radio"/> 使用率	<input type="text"/> %	
	<input type="radio"/> 使用帯域	<input type="text"/> Kbps	
	<input type="radio"/> 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	<input type="text"/>	参照	<input type="button" value="追加"/>
<input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報のACL定義が表示されています。帯域制御の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IPv6アドレス、ポート番号、IPv6 Traffic Class値の条件を元に帯域を割り当てます。

表示条件入力は、“ACL対応定義”または“旧定義”から選択します。初期値は、ACL対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

回線に LAN を使用して、帯域制御機能を有効に動作させる

場合は、シェーピングを使用してください。

回線に ATM を使用して、帯域制御機能を有効に動作させ

る場合は、適切な VC 速度を設定してください。

ACL 定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

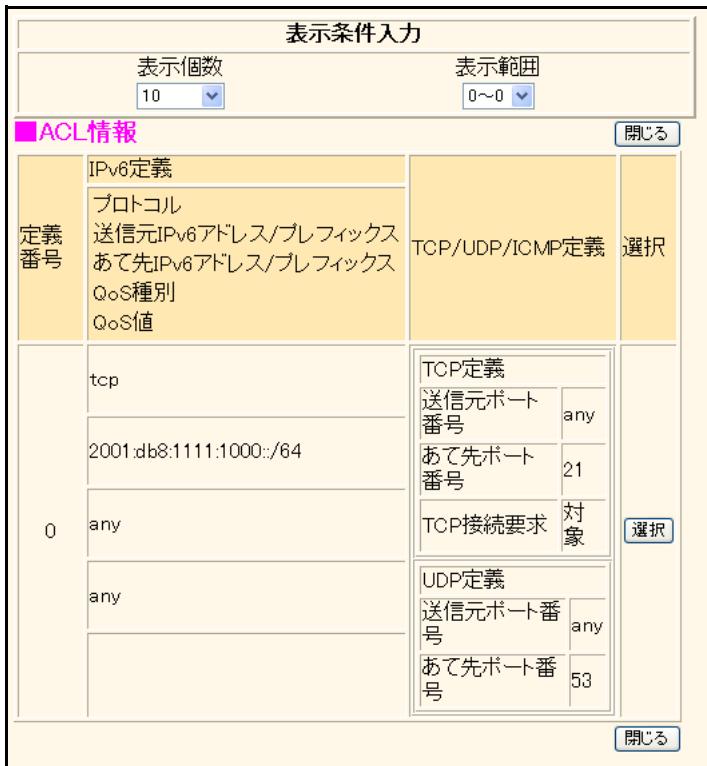
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の「選択」ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6関連]
 →[IPv6帯域制御(WFQ)情報]→「ACL定義番号の[参照]」



「ACL情報」 - [追加] / [修正] - 「IPv6定義情報」、「TCP定義情報」および「UDP定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報だけを表示させることができます。

参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「IPv6帯域制御(WFQ)情報」のACL定義番号に設定する定義番号欄の[選択]ボタンをクリックすると、「IPv6帯域制御(WFQ)情報」にACL定義番号が設定され、画面が閉じます。[ACL定義参照]ボタンをクリックした場合は、[選択]ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

18.1.5.8.1 IPv6 帯域制御 (WFQ) 情報 (旧定義)

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IPv6 関連]
 → [IPv6 帯域制御 (WFQ) 情報] → 「表示条件入力 (旧定義)」

表示条件入力					
表示定義内容					
旧定義					
■ IPv6帯域制御(WFQ)情報					
※追加・修正情報は一覧の <input type="text"/> で設定してください。					
定義番号	プロトコル	送信元IPv6アドレス／プレフィックス長	対象Traffic Class値	操作	
		送信元ポート番号			
		あて先IPv6アドレス／プレフィックス長 あて先ポート番号			
<input type="button" value="全削除"/>					
<IPv6帯域制御(WFQ)情報入力フィールド>					
プロトコル <input checked="" type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)					
送信元情報	IPv6アドレス／プレフィックス長	<input type="text"/>	<input type="button" value=""/>		
	ポート番号	<input type="text"/>	<input type="button" value=""/>		
あて先情報	IPv6アドレス／プレフィックス長	<input type="text"/>	<input type="button" value=""/>		
	ポート番号	<input type="text"/>	<input type="button" value=""/>		
対象Traffic Class値					
帯域	<input type="radio"/> 最優先	<input type="text"/>	<input type="button" value=""/>		
	<input type="radio"/> ベストエフォート	<input type="text"/>	<input type="button" value=""/>		
	<input checked="" type="radio"/> 使用率	<input type="text"/> %	<input type="button" value=""/>		
	<input type="radio"/> 使用帯域	<input type="text"/> Kbps	<input type="button" value=""/>		
<input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません					
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。					

表示条件入力に、“旧定義”を選択した場合に、IPv6 帯域制御 (WFQ) 情報の旧定義が表示されます。

プロトコル

帯域制御の対象となるプロトコルを以下の5つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

帯域制御の対象となるIPv6アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積と、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 Traffic Class 値

帯域制御の対象となるIPv6パケットのTraffic Class値を16進数を使用して、0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのTraffic Class値が帯域制御の対象となります。

帯域

帯域の使用率または帯域値を指定します。

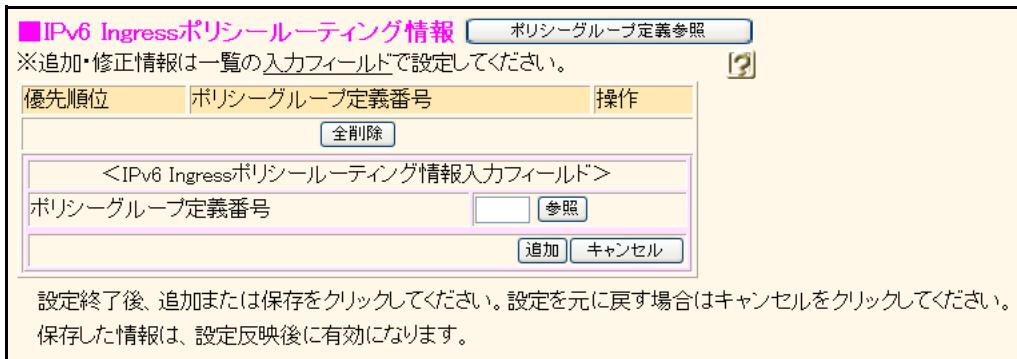
- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

回線にLANを使用して、帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。
回線にATMを使用して、帯域制御機能を有効に動作させる場合は、適切なVC速度を設定してください。

18.1.5.9 IPv6 Ingress ポリシールーティング情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IPv6 関連]
 → [IPv6 Ingress ポリシールーティング情報]



現在、設定されている IPv6 Ingress ポリシールーティング情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Ingress ポリシールーティング情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」 (P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に、指定されたポリシーグループに定義された送出先へパケットを送出します。

ポリシーグループ定義番号

[参照] ボタンをクリックして、ポリシーグループ定義番号を指定します。

別の画面に「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されます。指定する定義番号欄の [選択] ボタンをクリックし、ポリシーグループ定義番号を設定します。自動的に画面が閉じます。

なお、参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [IPv6 関連]
 → [IPv6 Ingress ポリシールーティング情報] → 「ポリシーグループ定義番号の [参照]」



「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ポリシーグループ定義情報の一覧に見たい情報を表示させることができます。

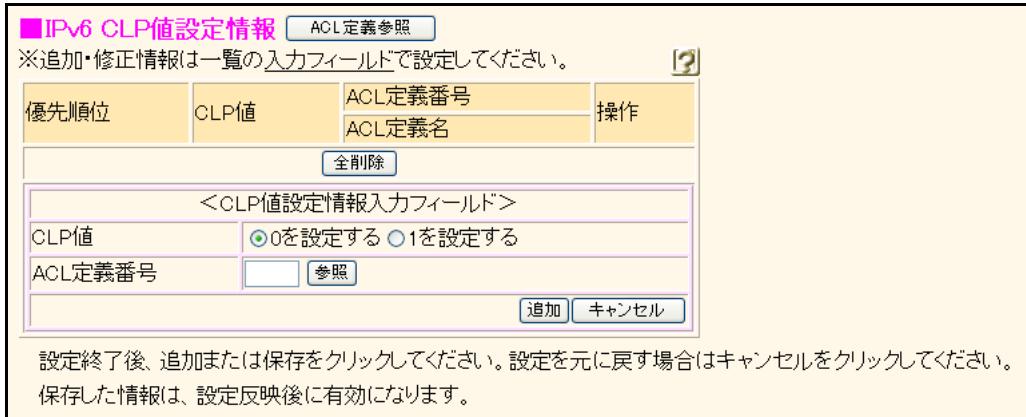
参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 Ingress ポリシールーティング情報」のポリシーグループ定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IPv6 Ingress ポリシールーティング情報」にポリシーグループ定義番号が設定され、画面が閉じます。[ポリシーグループ定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.5.10 IPv6 CLP 値設定情報

適用機種 Si-R260B,370,570

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [IPv6 関連] → [IPv6 CLP 値設定情報]



現在、設定されている IPv6 CLP 値設定情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 CLP 値設定の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」 (P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された IPv6 CLP 値設定を行います。ただし、分割されたパケットに対しては正しく行えません。

CLP 値

条件に一致した場合に IPv6 CLP 値に設定する値を以下の 2 つから選択します。

- 0 を設定する
- 1 を設定する

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

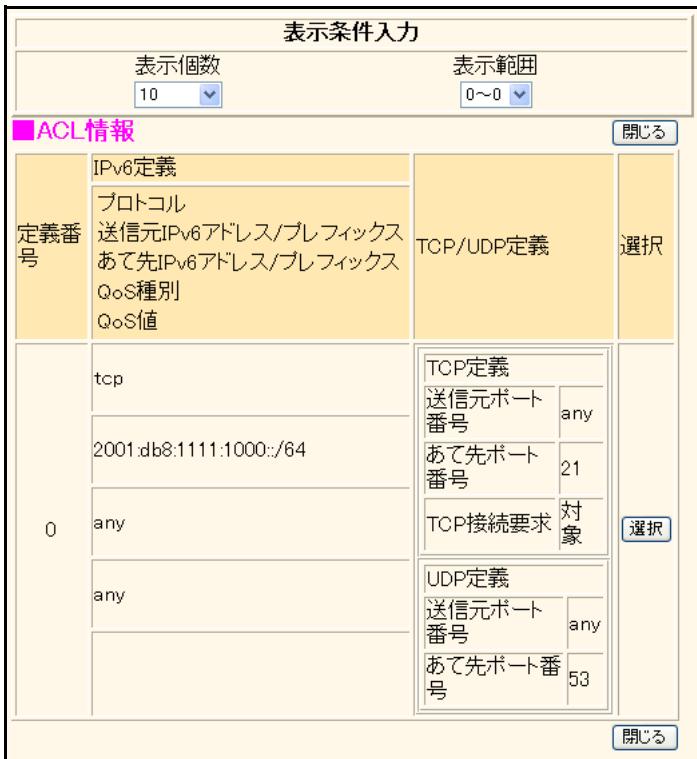
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 CLP 値設定情報]→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IPv6 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 CLP 値設定情報」の ACL 定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IPv6 CLP 値設定情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.5.11 IPv6 DHCP 情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 DHCP 情報]

DHCP 機能で、" 使用しない " を選択した場合

■ IPv6 DHCP情報

DHCP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input type="radio"/> リレーエージェント機能を使用する <input type="radio"/> サーバ機能を使用する
---------------	---

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

DHCP 機能で、" クライアント機能を使用する " を選択した場合

■ IPv6 DHCP情報

DHCP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> クライアント機能を使用する <input type="radio"/> リレーエージェント機能を使用する <input type="radio"/> サーバ機能を使用する	
クライアント機能	DUID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
	IAID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>
	プレフィックス要求	<input type="radio"/> しない <input checked="" type="radio"/> する <input type="checkbox"/> 旧方式を使用する <small>※draft-troan-dhcpv6-opt-prefix-delegation-01.txtに準拠したサーバを使用する場合は、“旧方式を使用する”をチェックしてください。</small>
	DNSサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	DNSドメイン名要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	SIPサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	SIPドメイン名要求	<input checked="" type="radio"/> する <input type="radio"/> しない
	SNTPサーバアドレス要求	<input checked="" type="radio"/> する <input type="radio"/> しない
リジェクト経路	<input checked="" type="radio"/> Blackhole <input type="radio"/> Reject	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

DHCP 機能で、"リレーエージェント機能を使用する"を選択した場合

■ IPv6 DHCP情報

DHCP機能		<input type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input checked="" type="radio"/> リレーエージェント機能を使用する <input type="radio"/> サーバ機能を使用する
リレー エージェント 機能	リレー先 インターフェース	lan0
	リレー先 サーバアドレス	
	送信元アドレ ス	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

DHCP 機能で、"サーバ機能を使用する"を選択した場合

■ IPv6 DHCP情報

DHCP機能		<input type="radio"/> 使用しない <input type="radio"/> クライアント機能を使用する <input type="radio"/> リレーエージェント機能を使用する <input checked="" type="radio"/> サーバ機能を使用する	
サーバ機能	DUID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>	
	プリファレンス 値	<input type="text"/>	
	プレフィックス 配布	<input checked="" type="radio"/> しない <input type="radio"/> する プレフィックス <input type="text"/> ✓ Valid Lifetime <input type="radio"/> 期限なし <input type="radio"/> 期限あり <input type="text"/> 日	
		Pref. Lifetime <input type="radio"/> 期限なし <input type="radio"/> 期限あり <input type="text"/> 日	
		自動経路設定 <input checked="" type="radio"/> する <input checked="" type="radio"/> しない 配布先 <input type="radio"/> 限定期間ない <input type="radio"/> 限定期間する クライアントDUID <input type="text"/>	
		DNSサーバア ドレス配布	プライマリ <input type="text"/> セカンダリ <input type="text"/>
		DNSドメイン 名配布	<input type="text"/>
	SIPサーバア ドレス配布	プライマリ <input type="text"/> セカンダリ <input type="text"/>	
	SIPドメイン名 配布	プライマリ <input type="text"/> セカンダリ <input type="text"/>	
	SNTPサーバ アドレス配布	プライマリ <input type="text"/> セカンダリ <input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>			

DHCP 機能

それぞれのインターフェースのIPv6 DHCP 機能を以下の4つから選択します。

- 使用しない
IPv6 DHCP 機能を使用しません。
- クライアント機能を使用する
本装置を該当インターフェースのIPv6 DHCP クライアントとして使用します。
- リレーエージェント機能を使用する
IPv6 DHCP リレーエージェントとして使用します。
- サーバ機能を使用する
本装置を該当インターフェースのネットワークのIPv6 DHCP サーバとして使用します。

クライアント機能

本装置を該当インターフェースのIPv6 DHCP クライアントとして使用する場合に設定します。

DUID

DUID を以下の2つから選択します。

- 自動
DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
260桁以内の16進数で表記した DUID を指定します。

IAID

IAID を以下の2つから選択します。

- 自動
自動生成される IAIID を使用します。通常は、この設定を使用します。
- 指定する
1~4294967295 の範囲の10進数で指定します。

プレフィックス要求

DHCP サーバにプレフィックスを要求するかどうかを設定します。DHCP サーバにプレフィックスを要求する場合は、“する”を選択します。“する”を選択した場合に、draft-troan-dhcpv6-opt-prefix-delegation-01.txt に準拠したサーバを利用するときは、“旧方式を使用する”をチェックします。

DNS サーバアドレス要求

DHCP サーバに DNS サーバアドレスを要求するかどうかを設定します。DHCP サーバに DNS サーバアドレスを要求する場合は、“する”を選択します。

DNS ドメイン名要求

DHCP サーバに DNS ドメイン名を要求するかどうかを設定します。DHCP サーバに DNS ドメイン名を要求する場合は、“する”を選択します。

SIP サーバアドレス要求

DHCP サーバに SIP サーバアドレスを要求するかどうかを設定します。DHCP サーバに SIP サーバアドレスを要求する場合は、“する”を選択します。

SIP ドメイン名要求

DHCP サーバに SIP ドメイン名を要求するかどうかを設定します。DHCP サーバに SIP ドメイン名を要求する場合は、“する”を選択します。

SNTP サーバアドレス要求

DHCP サーバに SNTP サーバアドレスを要求するかどうかを設定します。DHCP サーバに SNTP サーバアドレスを要求する場合は、“する”を選択します。

リジェクト経路

DHCP サーバから取得したプレフィックスのリジェクト経路を以下の2つから選択します。

- Blackhole
リジェクト経路あてのパケットを受信しても送信元にエラーを報告しません。
- Reject
リジェクト経路あてのパケットを受信した場合、送信元にエラーを報告します。

リレーエージェント機能

IPv6 DHCP リレーエージェントとして使用する場合に設定します。

リレー先インターフェース

IPv6 DHCP クライアントからの要求を中継し、送出するインターフェースを選択します。

リレー先サーバアドレス

リレー先サーバのIPv6 アドレスを設定します。

存在するリレー先インターフェースを指定してください。

送信元アドレス

サーバへのリレーパケットを送信する際の送信元アドレスとして、本装置に設定されている自側 IPv6 アドレスのどれかを指定します。

サーバ機能

本装置を該当インターフェースのネットワークの IPv6 DHCP サーバとして使用する場合に設定します。

DUID

- 自動
DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
260 衔以内の 16 進数で表記した DUID を指定します。

プリファレンス値

DHCP サーバのプリファレンス値を 0 ~ 255 の範囲の 10 進数で指定します。DHCP クライアントはこの値が大きい DHCP サーバを選択します。省略時は 0 が設定されます。

プレフィックス配布

DHCP クライアントに割り当てるプレフィックスを設定します。クライアントにプレフィックスを割り当てる場合は、“する”を選択し、以降の項目を設定します。

プレフィックス

クライアントに割り当てるプレフィックスとプレフィックス長を指定します。プレフィックス長は 48 ~ 64 の範囲で指定します。

こんな事に気をつけて

配布するプレフィックスとして 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場合は、上位を “dhcp@インターフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。

Valid Lifetime

割り当てるプレフィックスの Valid Lifetime を指定します。

有効範囲)

0 ~ 365 日

0 ~ 8760 時間

0 ~ 525600 分

0 ~ 31536000 秒

Pref. Lifetime

割り当てるプレフィックスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲)

0 ~ 365 日

0 ~ 8760 時間

0 ~ 525600 分

0 ~ 31536000 秒

自動経路設定

クライアントに割り当てたプレフィックスへの経路を自動で設定する場合は、“する”を選択します。

配布先

特定のクライアントにだけプレフィックスを配布する場合は、260 衔以内の 16 進数で表記した DUID を指定します。省略時は、DUID に関係なく配布されます。

DNS サーバアドレス配布

配布する DNS サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する DNS サーバアドレスとして IPv6 DHCP クライアントが取得した DNS サーバアドレスを使用する場合は、“dhcp@インターフェース名” の形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ DNS サーバの指定はできません。

DNS ドメイン名配布

配布する DNS ドメイン名を設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する DNS ドメイン名として IPv6 DHCP クライアントが取得した DNS ドメイン名を使用する場合は、“dhcp@インターフェース名”的形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。

SIP サーバアドレス配布

配布する SIP サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SIP サーバアドレスとして IPv6 DHCP クライアントが取得した SIP サーバアドレスを使用する場合は、“dhcp@インターフェース名”的形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ SIP サーバの指定はできません。

SIP ドメイン名配布

配布する SIP ドメイン名を設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SIP ドメイン名として IPv6 DHCP クライアントが取得した SIP ドメイン名を使用する場合は、“dhcp@インターフェース名”的形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ SIP サーバの指定はできません。

SNTP サーバアドレス配布

配布する SNTP サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SNTP サーバアドレスとして IPv6 DHCP クライアントが取得した SNTP サーバアドレスを使用する場合は、“dhcp@インターフェース名”的形式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているインターフェースを指定してください。またその場合、セカンダリ SNTP サーバの指定はできません。

18.1.5.12 IPv6 EXP 値書き換え情報

[操作] ルータ設定「相手情報」 → 「ネットワーク情報」 → 「追加」 → 「[IPv6 関連]」
→ 「[IPv6 EXP 値書き換え情報]」

■ IPv6 EXP 値書き換え情報 ACL 定義参照

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	ACL 定義番号	EXP	操作
<input type="button" value="全削除"/>			
<EXP 値書き換え情報入力フィールド>			
EXP	<input type="text"/>		
ACL 定義番号	<input type="text"/>	<input type="button" value="参照"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 EXP 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 EXP 値書き換えの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された IPv6 EXP 値を書き換えます。ただし、分割されたパケットに対しては正しく行えません。

EXP**ACL 定義番号**

書き換える IPv6 EXP 値を、0～7 の範囲で指定します。
省略時は、0 が設定されます。

[参照] ボタンをクリックして、ACL 定義番号を指定します。
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「IPv6 関連」
→「IPv6 EXP 値書き換え情報」→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」 / 「修正」 - 「IPv6 定義情報」、「TCP 定義情報」 および 「UDP 定義情報」 で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 EXP 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 EXP 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.5.13 IPv6 動的VPN情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 動的VPN情報]

表示条件入力

表示個数 10	表示範囲 定義は存在しません
------------	-------------------

■ IPv6動的VPN情報 [ACL定義参照](#)

※追加・修正情報は一覧ので設定してください。 [?](#)

優先順位	動的VPN接続	ACL定義番号	操作
		ACL定義名	
全削除			

<IPv6動的VPN情報入力フィールド>

動的VPN接続	<input checked="" type="radio"/> する	相手プレフィックス長	<input type="text"/>
	<input type="radio"/> しない	利用するテンプレート情報	tmp0
<input type="radio"/> しない (ネットワーク情報自動取得)			
ACL定義番号	<input type="text"/>	参照	追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている 動的VPN 接続契機パケットの ACL 定義が表示されています。処理は優先順位 1 から順に行われます。動的VPN接続契機パケットの検出条件の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動的VPN接続契機パケットの検出を行います。ただし、分割されたパケットに対しては正しく行えません。

動的VPN接続

動的VPN接続を行う場合は、“する”を選択します。

“しない (ネットワーク情報自動取得)”は、相手情報に接続先情報の動的VPN接続定義が行われている必要があります。また、相手情報ごとに1つしか選択できません。

相手プレフィックス長

動的VPN接続を開始する場合に、相手を識別するための情報として相手プレフィックス長を0～128の10進数で指定します

利用するテンプレート情報

動的VPN接続に利用するテンプレート情報を選択します。

ACL定義番号

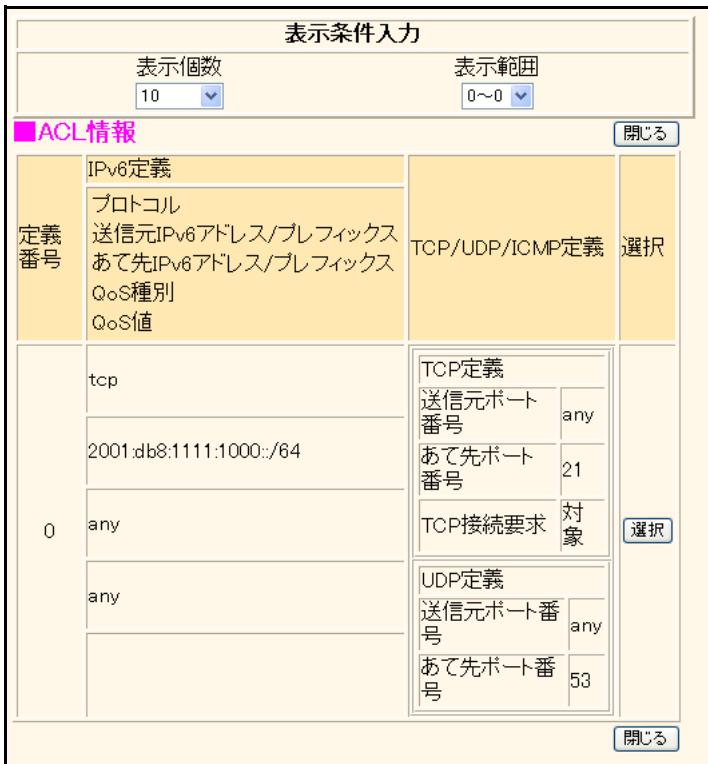
[参照]ボタンをクリックして、ACL定義番号を指定します。別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 関連]→[IPv6 動的VPN 情報]→「ACL 定義番号の [参照]」



「ACL情報」 - 「追加」／「修正」 - 「IPv6定義情報」、「TCP定義情報」および「UDP定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報だけを表示させることができます。

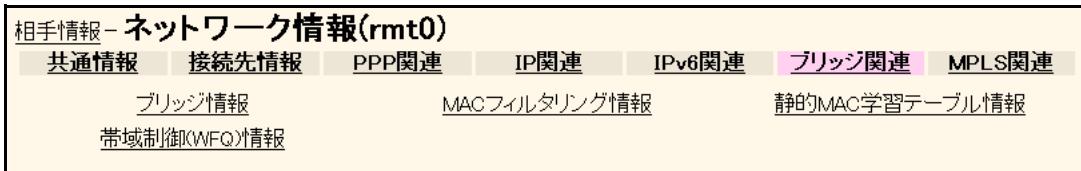
参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「IPv6動的VPN情報」のACL定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IPv6動的VPN情報」にACL定義番号が設定され、画面が閉じます。[ACL定義参照]ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

18.1.6 ブリッジ関連

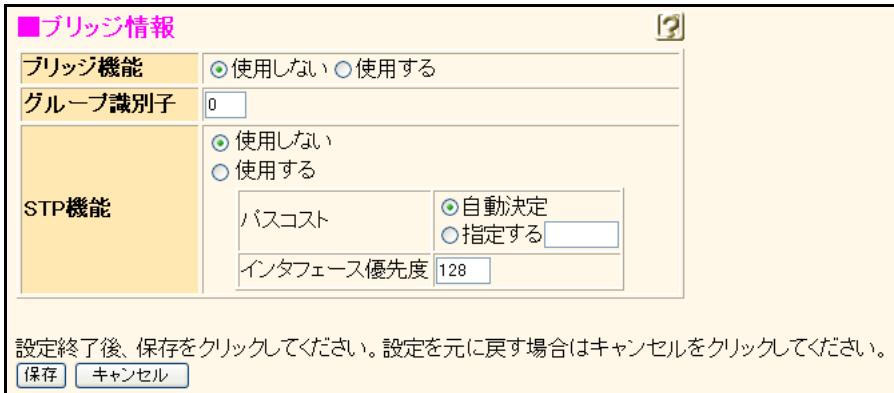
適用機種 全機種

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[ブリッジ関連]



18.1.6.1 ブリッジ情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[ブリッジ関連]→[ブリッジ情報]



ブリッジ機能

接続相手とブリッジで通信する場合は、“使用する”を選択します。

グループ識別子

ブリッジのグループ識別子を10進数で指定します。0～7の範囲で指定します。省略時は0が設定されます。

STP 機能

STP機能を利用して経路制御を行う場合は、“使用する”を選択し、以下の項目を設定します。グループ識別子に0を設定した場合だけ、STPを利用するすることができます。この設定項目はブリッジ機能を使用する場合だけ有効です。

パスコスト

STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

インターフェース優先度

STPで使用するインターフェースごとの優先度を0～255の範囲で指定します。値が小さい方が優先となります。

こんな事に気をつけて

ブリッジ機能をMPで使用する場合、「ネットワーク情報」→「PPP関連」→「MP情報」の受信パケット順序制御で“する”を選択してください。受信パケット順序制御しないと順序に依存するプロトコルの通信が停止する場合があります。

18.1.6.2 MAC フィルタリング情報

[操作] ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[ブリッジ関連]
→[MAC フィルタリング情報]

優先順位	動作	方向	ACL定義番号	操作
			ACL定義名	
全削除				
<MAC フィルタリング情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断	方向	入出力	
ACL定義番号	<input type="text"/>	参照	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

WAN モジュールで送受信する際にフィルタリング処理を行います。優先順位の高い定義から、順にフレームのチェックを行い、フィルタリング条件が一致した場合に定義された動作を行います。

動作

フィルタリング条件に一致したときの動作を以下の3つから選択します。

- 透過
フィルタリング条件と一致する場合に透過します。
- 透過（接続中のみ）
フィルタリング条件と一致した場合に、回線が接続しているときはフレームを透過し、切断しているときは遮断します。
- 遮断
フィルタリング条件と一致する場合に遮断します。

方向

フィルタリングする方向を指定します。

- 入力
入力パケットのみをフィルタリング対象とする場合に指定します。
- 出力
出力パケットのみをフィルタリング対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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 MAC アドレスとて先 MAC アドレス
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- MAC 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」→「ネットワーク情報」→「追加」→「ブリッジ関連」→「MAC フィルタリング情報」→「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」 / 「修正」 - 「MAC 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報をだけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「MAC フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「MAC フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

18.1.6.2.1 MAC フィルタリング情報（旧定義）

[操作] ルータ設定「相手情報」→「ネットワーク情報」→[修正]→[ブリッジ関連]→[MAC フィルタリング情報]→「表示定義内容（旧定義）」

優先順位	動作	送信元MACアドレス	フォーマット種別	LSAP/type値	VLANタグ解析	操作

■MAC フィルタリング情報
※追加・修正情報は一覧の入力フィールドで設定してください。

動作 透過 透過(接続中のみ) 遮断

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: すべて
アドレス指定（“指定する”を選択時のみ有効です）

フォーマット種別:

- すべて
- LLC形式

LSAP	<input type="text"/>
VLANタグ解析	<input checked="" type="radio"/> しない <input type="radio"/> する
- Ethernet形式

type値	<input type="text"/>
VLANタグ解析	<input checked="" type="radio"/> しない <input type="radio"/> する

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

LAN モジュールで送受信する際にフィルタリング処理を行います。優先順位の高い定義から順にフレームのチェックを行い、フィルタリング条件が一致した場合に定義された動作を行います。

動作

フィルタリング条件に一致したときの動作を指定します。
MAC フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 透過（接続中のみ）
フィルタリング条件と一致した場合に、回線が接続しているときはフレームを透過し、切断しているときは遮断します。
- 遮断
条件と一致した場合にパケットを遮断します。

送信元／あて先 MAC アドレス

MAC アドレスを以下の項目から選択します。“指定する”を選択する場合は、アドレス指定に MAC アドレスを 16 進数で指定します。

- すべて
すべての MAC アドレスを対象とします。
- ブロードキャスト
ブロードキャスト MAC アドレスを対象とします。
- マルチキャスト
ブロードキャスト MAC アドレスおよびマルチキャスト MAC アドレスを対象とします。
- 指定する
アドレス指定に指定する MAC アドレスを対象とします。MAC アドレスは、「xx:xx:xx:xx:xx:xx」(xx は 2 衔の 16 進数) の形式で指定します。

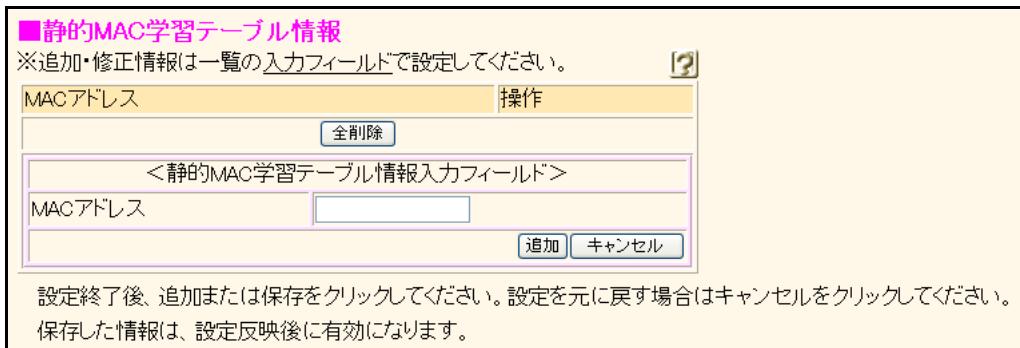
フォーマット種別

フィルタリング対象のフォーマットを以下の項目から選択します。“LLC 形式”的場合は、LSAP を 16 進数を使用して、0～ffff の範囲で指定し、“Ethernet 形式”的場合は、type 値を 16 進数を使用して、5dd～ffff の範囲で指定します。未入力時にはすべての値が対象となります。また、VLAN タグ付きパケットで VLAN タグの先を解析するか選択します。“する”を指定した場合は、VLAN タグ付きパケットでも正しく解析されます。

- LLC 形式
LLC 形式のパケットを対象とします。
- Ethernet 形式
Ethernet 形式のパケットを対象とします。
- すべて
すべてのパケットを対象とします。

18.1.6.3 静的 MAC 学習テーブル情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [ブリッジ関連]
→ [静的 MAC 学習テーブル情報]



現在、設定されている静的 MAC 学習テーブルの定義が表示されています。静的 MAC 学習テーブルの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

MAC アドレス

MAC アドレスは、「xx:xx:xx:xx:xx:xx」(xx は 2 衔の 16 進数) の形式で指定します。

18.1.6.4 帯域制御 (WFQ) 情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [ブリッジ関連]
→ [帯域制御 (WFQ) 情報]

■帯域制御(WFQ)情報 [ACL定義参照](#)

※追加・修正情報は一覧ので設定してください。 [?](#)

定義番号	ACL定義番号	帯域	操作
	ACL定義名		
全削除			
<帯域制御(WFQ)情報入力フィールド>			
帯域	<input type="radio"/> 最優先		
	<input type="radio"/> ベストエフォート		
	<input checked="" type="radio"/> 使用率	<input type="text"/> %	
	<input type="radio"/> 使用帯域	<input type="text"/> Kbps	▼
	<input type="radio"/> 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	<input type="text"/>	参照	
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報の ACL 定義が表示されています。帯域制御の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を 10 進数を使用して、1～99 の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが 100 を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbps または 1～100Mbps の範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- MAC 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「相手情報」 → [ネットワーク情報] → [追加] → [ブリッジ関連]
 → [帯域制御 (WFO) 情報] → 「ACL 定義番号の [参照]」



「ACL情報」 - [追加] / [修正] - 「MAC定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報だけを表示させることができます。

参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「帯域制御 (WFO) 情報」のACL定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「帯域制御 (WFO) 情報」にACL定義番号が設定され、画面が閉じます。「ACL定義参照」ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

18.1.7 MPLS 関連

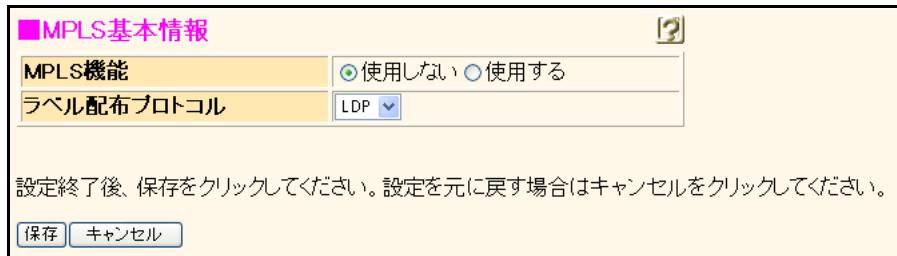
適用機種 全機種

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [MPLS 関連]



18.1.7.1 MPLS 基本情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [MPLS 関連] → [MPLS 基本情報]



MPLS 機能

リモート上で MPLS 機能を使用する場合は、“使用する”を選択します。

ラベル配布プロトコル

WAN 上で行うラベル配布プロトコルを選択します。

18.1.7.2 LDP情報

[操作] ルータ設定「相手情報」→ [ネットワーク情報] → [追加] → [MPLS 関連] → [LDP 情報]

Hello タイマ	
interval	5 秒
HoldTime	infinity 指定する 15 秒

KeepAlive タイマ	
interval	1 分
timeout	3 分

LDP ラベル広報方式	
LDP ラベル保持方式	DU DoD
PHP 機能	liberal conservative

IPv4 Transport アドレス	
Multicast Hello	送信する 送信しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

Hello タイマ

interval

Hello の送信間隔のタイマを 1 ~ 65535 秒の範囲で指定します。初期値は 5 秒です。省略はできません。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65535 秒

HoldTime

近隣関係の維持を判定するため HoldTime のタイマを 1 ~ 65534 秒の範囲で指定します。初期値は 15 秒です。省略はできません。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65534 秒

こんな事に気をつけて

HoldTime の値は、interval の値より小さくすることはできません。HoldTime の値は interval の値の 3 倍以上を設定することを推奨します。

KeepAlive タイマ

interval

KeepAlive の送信間隔のタイマを 1 ~ 65535 秒の範囲で指定します。初期値は 1 分です。省略はできません。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65535 秒

timeout

LDP セッションの維持を判定するための KeepAlive の timeout のタイマを 1 ~ 65535 秒の範囲で指定します。初期値は 3 分です。省略はできません。

有効範囲)

1 ~ 18 時間
1 ~ 1092 分
1 ~ 65535 秒

こんな事に気をつけて

timeout の値は、interval の値より小さくすることはできません。timeout の値は interval の値の 3 倍以上を設定することを推奨します。

LDP ラベル広報方式

Downstream Unsolicited を使用する場合は、“DU”を選択します。Downstream On Demand を使用する場合は、“DoD”を選択します。

LDP ラベル保持方式

liberal を使用する場合は “liberal” を選択します。
conservative を使用する場合は、“conservative” を選択します。

PHP 機能

インターフェースあての LSP の PHP 機能を設定します。
PHP 機能を無効にする場合は、“使用しない”を選択します。
PHP 機能を有効にする場合は、“使用する”を選択します。
MPLS トンネル接続を使用する場合に、自側エンドポイントと IP アドレスが同じとき、設定に関係なく “使用しない” が設定されます。

IPv4 Transport アドレス

インターフェース単位で LDP が相手装置との通信に用いる送信元 IPv4 アドレスを分ける必要がある場合、本装置に設定された IPv4 アドレスを指定します。

0.0.0.0 を指定した場合は、「MPLS 情報」の IPv4 Transport Address の設定に従います。省略時は、0.0.0.0 が設定されます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

こんな事に気をつけて

IPv4 Transport アドレスは、必ず本装置に存在するアドレスを指定してください。
本装置に存在しないアドレスをインターフェースに指定した場合は、そのインターフェースでは LDP を使用できません。

Multicast Hello

LDP Multicast Hello を送出するかどうかを設定します。

こんな事に気をつけて

MPLS トンネル接続を使用するインターフェースのトンネルエンドポイントに指定した装置が EoMPLS 通信の相手装置となる場合は、本設定を必ず“送信しない”に設定してください。“送信する”を指定した場合は、VC ラベルを交換できない通常の LDP セッションが確立してしまうため、EoMPLS 通信で用いる VC LSP ができず、EoMPLS 通信を行う事ができません。それ以外の場合では必ず“送信する”を設定してください。“送信しない”を設定した場合は LDP の隣接関係が構築できず、LDP のセッションが確立できなくなります。

18.2 着信相手識別情報

適用機種 Si-R220C, 220D, 240B, 370, 370B, 570, 570B

[操作] ルータ設定「相手情報」→ [着信相手識別情報]

■着信相手識別情報	
着信許可	<input checked="" type="radio"/> しない <input type="radio"/> する
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
MP接続	<input checked="" type="radio"/> しない <input type="radio"/> する BAP/BACP利用 <input checked="" type="radio"/> しない <input type="radio"/> する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

発信者番号で識別できなかった相手からの着信について利用する情報です。

Si-R240B では、“MP 接続”の設定項目は表示されません。

着信許可

発信者番号で識別できなかった相手からの着信を許可する場合は、“する”を選択します。

認証方式

着信時に利用する認証プロトコルを選択します。どちらのプロトコルも選択しなかった場合は、認証を行いません。

MP接続（Si-R220C、220D、370、 370B、570、570B）

着信時にMP接続を行う場合は、“する”を選択します。

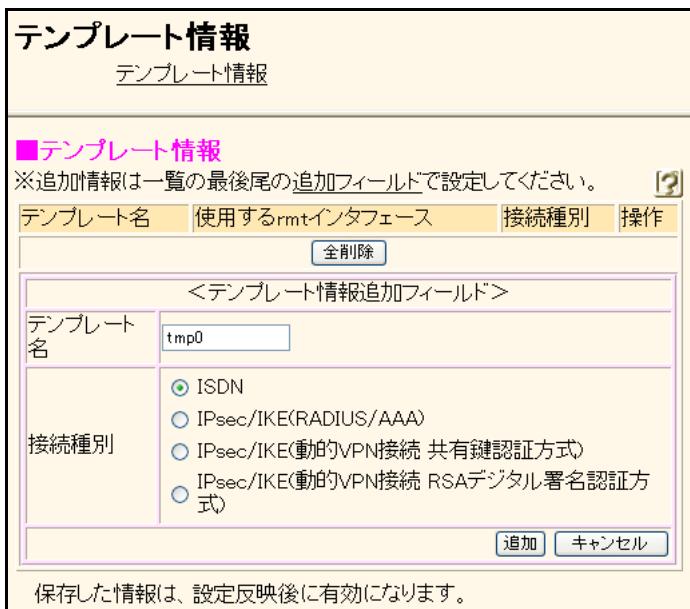
BAP/BACP利用

BAP/BACPを利用する場合は、“する”を選択します。

19 テンプレート情報

適用機種 全機種

[操作] ルータ設定「テンプレート情報」



テンプレート情報

テンプレート情報

■テンプレート情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

テンプレート名	使用するrmtインターフェース	接続種別	操作
全削除			

<テンプレート情報追加フィールド>

テンプレート名	tmp0
接続種別	<input checked="" type="radio"/> ISDN <input type="radio"/> IPsec/IKE(RADIUS/AAA) <input type="radio"/> IPsec/IKE(動的VPN接続 共有鍵認証方式) <input type="radio"/> IPsec/IKE(動的VPN接続 RSAデジタル署名認証方式)

追加 キャンセル

保存した情報は、設定反映後に有効になります。

現在、設定されているテンプレート情報の定義が表示されています。テンプレート情報の最大定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。必要な処理のボタンをクリックし、次のページへ進みます。

Si-R180B、240B、260B では、表示が上記の画面とは異なります。

テンプレート名

テンプレートの名称を8文字以内で指定します。

接続種別

接続種別を以下の4つから選択します。

- ISDN (Si-R220C、220D、370、370B、570、570B)
ISDN回線を使用して接続する場合に選択します。使用する場合は、「WAN情報」の回線インターフェースでISDNを設定してください。
- IPsec/IKE (RADIUS/AAA)
不特定の相手からIKEネゴシエーション要求を受信したときにRADIUS/AAAの登録情報を検索して接続する場合に選択します。

- IPsec/IKE (動的VPN接続 共有鍵認証方式)
動的VPN接続契機パケットを検出して動的VPN接続を行う場合、または不特定の相手からの動的VPN接続要求を許可する場合に選択します。動的VPN接続で使用されるIKEで共有鍵認証方式を使用する場合に選択します。動的VPN接続を行う場合は、「相手情報」 - [ネットワーク情報] - [IP関連] - [動的VPN情報] で動的VPN接続契機パケットを監視する設定をしてください。
- IPsec/IKE (動的VPN接続 RSAデジタル署名認証方式)
動的VPN接続契機パケットを検出して動的VPN接続を行う場合、または不特定の相手からの動的VPN接続要求を許可する場合に選択します。動的VPN接続で使用されるIKEでRSAデジタル署名認証方式を使用する場合に選択します。動的VPN接続を行う場合は、「相手情報」 - [ネットワーク情報] - [IP関連] - [動的VPN情報] で動的VPN接続契機パケットを監視する設定をしてください。

19.1 接続種別：ISDN

適用機種 Si-R220C, 220D, 370, 370B, 570, 570B

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加]

テンプレート情報 - テンプレート情報(tmp0)

ISDN

共通情報 PPP関連 IP関連 IPv6関連

このページではテンプレート情報を設定することができます。
上記の各項目をクリックしてください。詳細な設定項目が表示されます。

19.1.1 共通情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [共通情報]

テンプレート情報 - テンプレート情報(tmp0)

ISDN

共通情報 PPP関連 IP関連 IPv6関連

基本情報 トランプ情報

19.1.1.1 基本情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [共通情報] → [基本情報]

■ 基本情報

テンプレート名	tmp0
使用インターフェース	すべて
使用するrmtインターフェース	rmt から インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイム	送受信パケットについて 0 秒
参考するAAA情報	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する AAAグループID

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

テンプレート名

テンプレートの名称を8文字以内で指定します。

使用インターフェース

テンプレート着信で使用するWANインターフェースを選択します。あらかじめ、WAN情報でISDN回線インターフェースを設定しておく必要があります。

使用する rmt インタフェース

テンプレート着信で使用する開始 rmt インタフェース番号とインターフェース数を 10 進数を使用して指定します。

こんな事に気をつけて

テンプレート着信に予約した rmt インタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTU サイズ

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を 10 進数を使用して 200～1500 で指定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションにより、相手 MRU 値と相手 MRRU 値を MTU 値まで小さくすることができるようになります。省略時は、1500 が指定されます。

19.1.1.2 トラップ情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [共通情報] → [トラップ情報]

■トラップ情報	
linkDown	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
linkUp	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

トラップ情報

SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP 機能を利用しない場合、および旧バージョン互換 MIB モードで利用する場合は、この設定は意味を持ちません。

- linkDown
linkDown トラップを通知します。
- linkUp
linkUp トラップを通知します。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を 0～14400 秒の範囲で指定します。0 秒を指定した場合は、監視を行いません。設定された間、監視対象となるパケットがない場合に無通信として回線を切断します。省略時は、無通信監視を行わないものとみなされます。

参照する AAA 情報

テンプレート着信で認証および着信時に参照する AAA 情報を指定する場合は、“指定する”を選択します。

AAA グループ ID

AAA グループ ID を 10 進数を使用して、10 未満で指定します。省略時は、AAA 情報は参照されません。

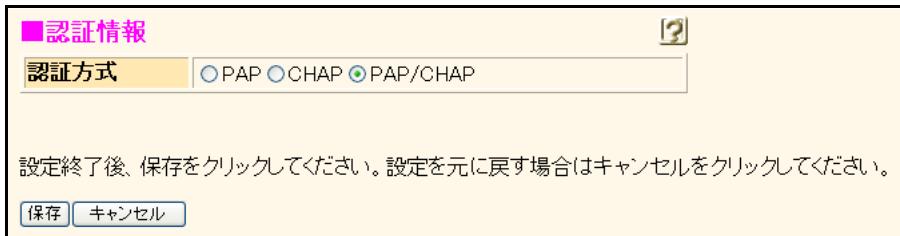
19.1.2 PPP 関連

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [PPP 関連]



19.1.2.1 認証情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [PPP 関連] → [認証情報]



認証方式

着信時に利用する認証プロトコルを以下の3つから選択します。

- PAP
- CHAP
- PAP/CHAP

19.1.2.2 圧縮情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [PPP 関連] → [圧縮情報]

■圧縮情報	
ヘッダ圧縮 (IPCP)	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	<input type="checkbox"/> IPヘッダ圧縮
データ圧縮 (CCP)	<input type="checkbox"/> LZS

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

送信するパケットのヘッダ部分の圧縮を行う機能です。使用する設定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

ヘッダ圧縮 (IPCP)

IPCPで使用する圧縮アルゴリズムを選択します。

- VJ
VJヘッダ圧縮 (RFC1144 準拠) を使用してヘッダ圧縮を行います。
- IPヘッダ圧縮
IPヘッダ圧縮 (RFC2507／RFC2508 準拠) を使用してヘッダ圧縮を行います。

ヘッダ圧縮 (IPV6CP)

IPV6CPで使用する圧縮アルゴリズムを選択します。

- IPヘッダ圧縮
IPヘッダ圧縮 (RFC2507／RFC2508 準拠) を使用してヘッダ圧縮を行います。

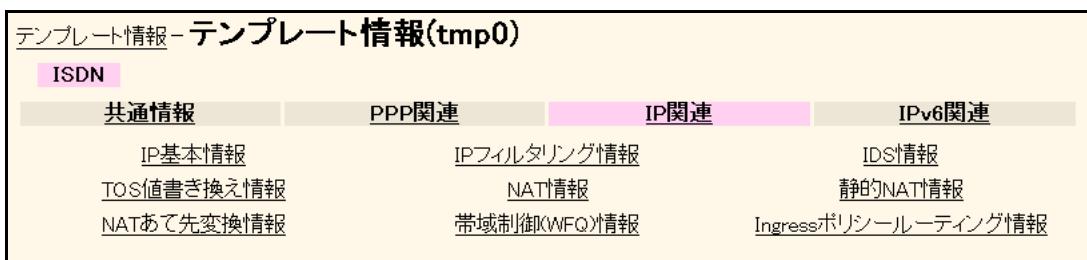
データ圧縮 (CCP)

CCPで使用するデータ圧縮アルゴリズムを選択します。

- LZS
LZS圧縮 (RFC1974 準拠) を使用してデータ圧縮を行います。

19.1.3 IP 関連

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連]



19.1.3.1 IP 基本情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [IP 基本情報]

■ IP 基本情報

DNS サーバ	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する プライマリ: <input type="text"/> セカンダリ: <input type="text"/>
MSS 書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 書き換えサイズ: <input type="text"/> バイト
割当て IP アドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する 先頭 IP アドレス: <input type="text"/> アドレス数: <input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

DNS サーバ

接続の際に使用する DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定した場合は、DNS サーバアドレスがないもの (0.0.0.0) とみなします。プライマリのみを省略することはできません。

有効範囲)

1.0.0.1 ~ 126.255.255.254
 128.0.0.1 ~ 191.255.255.254
 192.0.0.1 ~ 223.255.255.254

割当て IP アドレス

AAA ユーザ情報で相手側 ID アドレスが指定されていない (IP アドレスが固定の必要がない) の着信相手に対して、割り当てる IP アドレスの範囲を設定します。割り当てアドレス数の定義最大値は、仕様一覧 [\[2.3 システム最大値一覧\] \(P43\)](#) を参照してください。

有効範囲)

1.0.0.1 ~ 126.255.255.254
 128.0.0.1 ~ 191.255.255.254
 192.0.0.1 ~ 223.255.255.254

MSS 書き換え

MSS 書き換え機能の設定をします。MSS 書き換え機能を使用する場合、“使用する”を選択し、書き換えサイズを 0 または 160 ~ 1460 の範囲で指定します。0 を指定した場合は、MSS 書き換え機能が無効となります。

19.1.3.2 IP フィルタリング情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [IP フィルタリング情報]

優先順位	動作	方向	ACL定義番号	操作
			ACL定義名	
条件にあてはまらない場合の動作		透過		<input type="button" value="修正"/> <input type="button" value="初期化"/>
<input type="button" value="全削除"/>				
<IP フィルタリング情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断			
方向	入出力 <input type="button" value="参照"/>			
ACL定義番号	<input type="button" value="参照"/>			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IP フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行います。IP フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 遮断
条件と一致する場合にパケットを遮断します。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
- 出力のみ
出力パケットだけをフィルタリングする対象とします。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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なお、入力パケットはIPアドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。

ACL 定義番号

[参照] ボタンをクリックして、ACL定義番号を指定します。

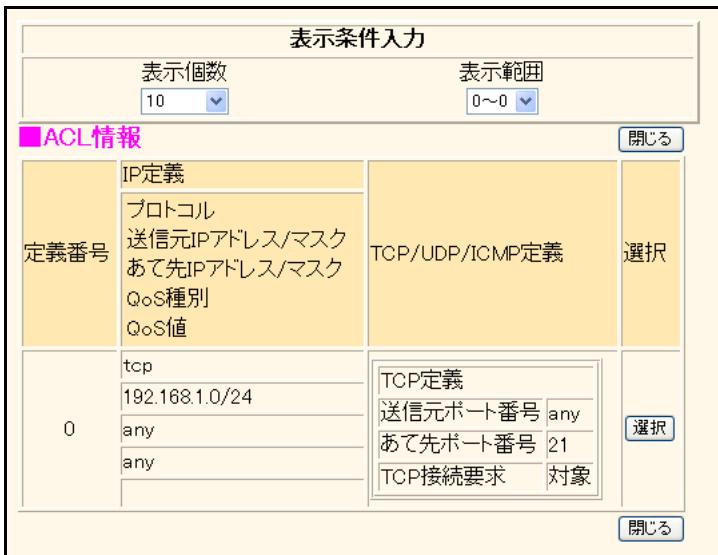
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の〔選択〕ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [IP フィルタリング情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IP フィルタリング情報」の ACL 定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IP フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。「ACL 定義参照」ボタンをクリックした場合は、「選択」ボタンは表示されません。「閉じる」ボタンをクリックして、画面を閉じてください。

19.1.3.2.1 IP フィルタリング情報（旧定義）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [IP フィルタリング情報]
→ 「表示条件入力（旧定義）」

表示条件入力							
表示定義内容 旧定義							
■ IP フィルタリング情報 ※追加・修正情報は一覧の <input type="text"/> で設定してください。							
優先順位	動作	プロトコル	送信元IPアドレス/マスク	TCP接続要求	TOS	方向	操作
			送信元ポート番号 あて先IPアドレス/マスク あて先ポート番号 ICMPタイプ ICMPコード				
条件にあてはまらない場合の動作			透過		<input type="button" value="修正"/> <input type="button" value="初期化"/>		
<input type="button" value="全削除"/>							
<IP フィルタリング情報入力フィールド>							
動作		<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
プロトコル		<input checked="" type="checkbox"/> すべて <input type="checkbox"/> (番号指定: <input type="text"/> "その他" を選択時のみ有効です)					
送信元情報	IP アドレス	<input type="text"/>					
	アドレスマスク	<input type="text"/> 0 (0.0.0.0)					
	ポート番号	<input type="text"/>					
あて先情報	IP アドレス	<input type="text"/>					
	アドレスマスク	<input type="text"/> 0 (0.0.0.0)					
	ポート番号	<input type="text"/>					
ICMP	タイプ	<input type="text"/>					
	コード	<input type="text"/>					
TCP接続要求		<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外					
TOS		<input type="text"/>					
方向		<input type="button" value="入出力"/> <input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

表示条件入力に、「旧定義」を選択した場合に、IP フィルタリング情報の旧定義が表示されます。

動作

IP フィルタリングの動作を以下の2つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 遮断
条件と一致する場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

フィルタリング条件としてのIP アドレスおよびアドレスマスクを指定します。

チェック対象となるパケットのIP アドレスと定義するアドレスマスクの論理積、定義するIP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

フィルタリング条件としてポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号をフィルタリングの対象とします。また、ポート番号を複数指定する場合は、“”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

ICMP

タイプ

フィルタリング条件としてICMPパケットのタイプ値を10進数を使用して0～255の範囲または“any”で指定します。ICMPタイプ値を複数指定する場合は、“”で区切れます。範囲指定の場合は“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのICMPタイプ値がフィルタリングの対象となります。

コード

フィルタリング条件としてICMPパケットのコード値を10進数を使用して0～255の範囲または“any”で指定します。ICMPコード値を複数指定する場合は、“”で区切れます。範囲指定の場合は“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのICMPコード値がフィルタリングの対象となります。

TCP 接続要求

TCPプロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルにTCPを設定した場合だけ有効です。

TOS

フィルタリング条件としてIPパケットのTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのTOSフィールド値がフィルタリングの対象となります。

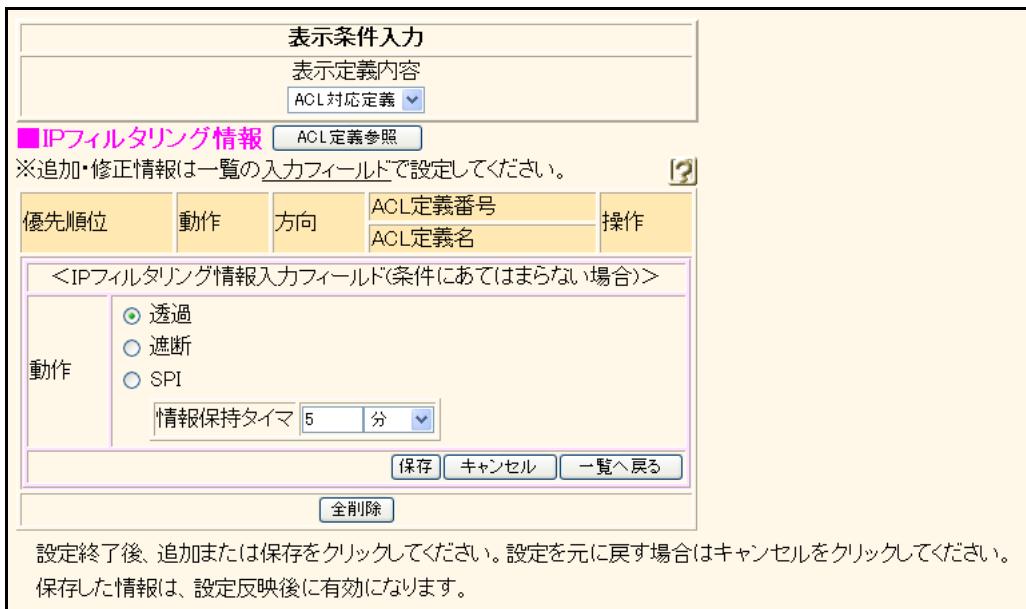
方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
入力パケットだけをフィルタリングする対象とします。
 - 出力のみ
出力パケットだけをフィルタリングする対象とします。
 - リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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
 - 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。
- なお、入力パケットはIPアドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。

19.1.3.2.2 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）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [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」[修正]



表示条件入力
表示定義内容
ACL 対応定義

■IP フィルタリング情報 [ACL 定義参照](#)

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	方向	ACL 定義番号	操作
	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 <input type="radio"/> SPI			
情報保持タイム 5 分				

保存 キャンセル 一覧へ戻る
全削除

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このテンプレートに設定されているIP フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断や SPI を指定し、IP フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IP フィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IP フィルタリング定義のどれにも一致しないで、プロトコルがTCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPI セッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

19.1.3.3 IDS情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [IDS情報]

IDS情報

IDS機能 使用しない 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

IDS機能

侵入などのセキュリティに影響を与えるパケットを検知する場合は、“使用する”を選択します。

19.1.3.4 TOS書き換え情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [TOS書き換え情報]

で設定してください。' (Addition and modification information is set in the input field of the list.) At the bottom are '全削除' (Delete All), '追加' (Add), and 'キャンセル' (Cancel) buttons. A note at the bottom right says: '設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。' (After setting is completed, click Add or Save. If you want to restore the original settings, click Cancel. The saved information becomes effective after the setting is reflected.)"/>

表示条件入力

表示定義内容
ACL対応定義

TOS書き換え情報 **ACL定義参照**

※追加・修正情報は一覧ので設定してください。

優先順位	ACL定義番号 ACL定義名	新TOS	操作
			全削除
<TOS書き換え情報入力フィールド>			
新TOS	<input type="text"/>		
ACL定義番号	<input type="text"/> 参照		
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている TOS 書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。TOS 書き換えの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された TOS 書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義”または“旧定義”から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新TOS

IPパケットに新しく指定するTOSフィールド値を16進数を使用して、0～ffの範囲で指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [TOS 値書き換え情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報を表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「TOS 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「TOS 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

19.1.3.4.1 TOS 値書き換え情報（旧定義）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [TOS 値書き換え情報]
 → 「表示条件入力（旧定義）」

表示条件入力																														
表示定義内容 旧定義																														
■TOS値書き換え情報																														
※追加・修正情報は一覧の入力フィールドで設定してください。																														
優先順位	プロトコル	送信元IPアドレス/マスク	TOS	操作																										
		送信元ポート番号	新TOS																											
あて先IPアドレス/マスク	あて先ポート番号																													
全削除																														
<TOS値書き換え情報入力フィールド> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">プロトコル</td> <td>すべて (番号指定: <input type="text"/> "その他"を選択時のみ有効です)</td> </tr> <tr> <td rowspan="3">送信元情報</td> <td>IPアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text"/> 0 (0.0.0.0)</td> </tr> <tr> <td>ポート番号</td> <td><input type="text"/></td> </tr> <tr> <td rowspan="3">あて先情報</td> <td>IPアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text"/> 0 (0.0.0.0)</td> </tr> <tr> <td>ポート番号</td> <td><input type="text"/></td> </tr> <tr> <td>TOS</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td>新TOS</td> <td><input type="text"/></td> <td></td> </tr> <tr> <td colspan="3" style="text-align: right;"> <input type="button" value="追加"/> <input type="button" value="キャンセル"/> </td> </tr> </table>					プロトコル		すべて (番号指定: <input type="text"/> "その他"を選択時のみ有効です)	送信元情報	IPアドレス	<input type="text"/>	アドレスマスク	<input type="text"/> 0 (0.0.0.0)	ポート番号	<input type="text"/>	あて先情報	IPアドレス	<input type="text"/>	アドレスマスク	<input type="text"/> 0 (0.0.0.0)	ポート番号	<input type="text"/>	TOS	<input type="text"/>		新TOS	<input type="text"/>		<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		
プロトコル		すべて (番号指定: <input type="text"/> "その他"を選択時のみ有効です)																												
送信元情報	IPアドレス	<input type="text"/>																												
	アドレスマスク	<input type="text"/> 0 (0.0.0.0)																												
	ポート番号	<input type="text"/>																												
あて先情報	IPアドレス	<input type="text"/>																												
	アドレスマスク	<input type="text"/> 0 (0.0.0.0)																												
	ポート番号	<input type="text"/>																												
TOS	<input type="text"/>																													
新TOS	<input type="text"/>																													
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>																														
設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存した情報は、設定反映後に有効になります。																														

表示条件入力に、"旧定義"を選択した場合に、TOS 値書き換え情報の旧定義が表示されます。

プロトコル

TOS 値書き換えの条件としてプロトコルを以下の 6つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、"その他"を選択し、10進数を使用して、1～255 の範囲で指定します。

送信元／あて先情報

TOS 値書き換え条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

TOS 値書き換え条件としての IP アドレスおよびアドレスマスクを指定します。

チェック対象となるパケットの IP アドレスと、定義する IP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。

ポート番号

TOS 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定する場合は、すべてのポート番号が TOS 書き換えの対象となります。また、ポート番号を複数指定する場合は、”,” で区切ります。範囲指定の場合は、”-” で区切ります。送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0～ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、”,” で区切ります。範囲指定の場合は、”-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値が書き換えの対象となります。

新 TOS

IP パケットに新しく指定する TOS フィールド値を 16 進数を使用して、0～ff の範囲で指定します。

19.1.3.5 NAT 情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [NAT 情報]

■NAT情報	
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ
グローバルアドレス	<input type="text"/>
アドレス個数	1 <input type="text"/> 個
アドレス割当てタイム	5 <input type="text"/> 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsec/パスルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
FTP	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SIP	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
H.323	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
DNS	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP Trap	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
IRC	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
NTTドメインログオン	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
各種ストリーミング	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
各種オンラインゲーム	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

NAT の使用

“マルチ NAT”を選択すると、複数の端末と併用できます。“静的 NAT のみ”を選択すると静的 NAT 情報の条件に一致しないパケットは変換されません。NAT を使用しない場合は、以降の設定は無効です。

こんな事に気をつけて

本装置では「相手情報」、「LAN 情報」および「テンプレート情報」の各インターフェースでアドレス変換機能を設定できます。ただし、使用する場合は、グローバルアドレスを使用するインターフェースだけで設定します。また、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。

グローバルアドレス

特定のグローバルアドレスを使用するときに指定します。指定しない場合は自動で割り当てられます。

アドレス個数

複数個のグローバルアドレスを使用する場合は、上述のグローバルアドレスを先頭とし連続した複数のアドレスを指定できます。その個数を1～16の範囲で指定します。なお、アドレス個数の設定はグローバルアドレスを指定した場合にだけ有効です。省略時は、1が設定されます。

アドレス割当てタイマ

アドレス変換情報は一定の時間、該当する通信が行われないと、自動的に解放されます。解放するための猶予時間を0～24時間の範囲で指定します。0を指定すると、タイマによる情報の解放は行われません。省略時は、5分が設定されます。

アプリ対応

使用するアプリケーションを選択し、それぞれに“有効”を設定します。

- FTP
- SIP
- H.323
- DNS
- SNMP Trap
- IRC
- NT ドメインログオン
- 各種ストリーミング
- 各種オンラインゲーム

NATセキュリティ

- 通常
相手サーバがNATを使用している際など、要求先とは別のアドレスから応答します。
- 高い
ftp や dns の要求する相手からの応答かどうかをチェックします。

IPsecパススルー

- 有効
相手ごとに1つのIPsecパスを接続することができます。
- 無効
IPsec クライアントがNAT トラバーサル機能を使用することができます。

こんな事に気をつけて

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 パスしか接続できません。

19.1.3.6 静的NAT情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP関連] → [静的NAT情報]

■静的NAT情報

※追加・修正情報は一覧ので設定してください。

プライベートアドレス	プライベートポート番号	プロトコル	操作
グローバルアドレス	グローバルポート番号		
条件にあてはまらない場合の動作		破棄	<input type="button" value="修正"/>
		<input type="button" value="初期化"/>	
<input type="button" value="全削除"/>			
<静的NAT情報入力フィールド>			
プライベート IP情報	IPアドレス	<input type="text"/>	
	ポート番号	すべて	(番号指定: <input type="text"/> "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	<input type="text"/>	
	ポート番号	すべて	(番号指定: <input type="text"/> "その他"を選択時のみ有効です)
プロトコル	すべて	(番号指定: <input type="text"/> "その他"を選択時のみ有効です)	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

NAT機能を使用すると、アドレス変換情報を固定で持つことができます。現在、設定されている固定のアドレス情報の定義が表示されています。静的NATの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

プライベートIP情報

IPアドレス

固定でアドレス変換を行う場合にローカルネットワーク側のIPアドレスを指定します。省略はできません。

ポート番号

固定でアドレス変換を行う場合にローカルネットワーク側のポート番号を選択します。“その他”を選択し、ポート番号を指定する場合は、10進数を使用して1～65535の範囲で指定します。

なお、グローバルポート番号を範囲指定した場合、その範囲のグローバルポート番号は指定したプライベートポート番号を先頭とした範囲に変換されます。

例) プライベートポート番号 : 1000

グローバルポート番号 : 10000-11000

NAT変換後

プライベートポート番号 : 1000-2000

グローバルIP情報

IPアドレス

固定でアドレス変換を行う場合にリモートネットワーク側のIPアドレスを指定します。省略時は、先頭のグローバルアドレスに対して有効な指定となります。

IPアドレスを指定する場合は、“-”で区切った1組の範囲を指定します。

ポート番号

固定でアドレス変換を行う場合にリモートネットワーク側のポート番号を選択します。“その他”を選択し、ポート番号を指定する場合は、10進数を使用して1～65535の範囲から1つ、または“-”で区切った1組の範囲を指定します。

プロトコル

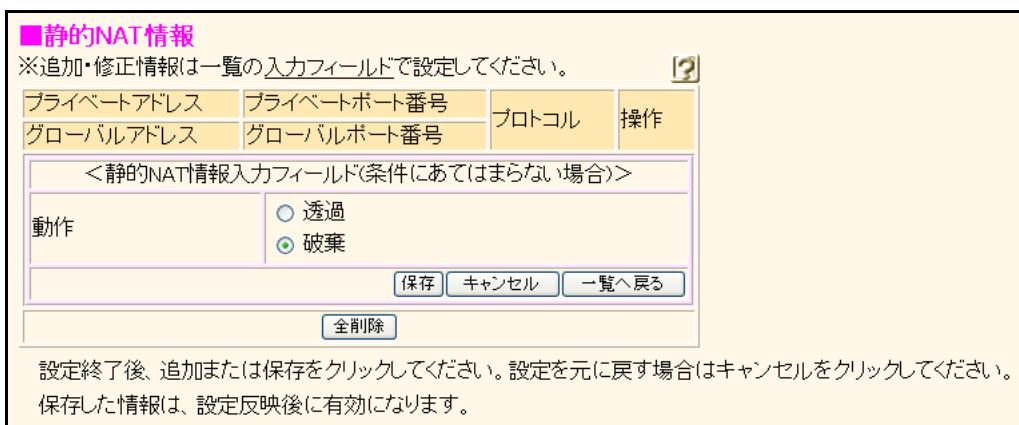
固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- esp (50)
- ah (51)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

19.1.3.6.1 静的 NAT 情報（条件にあてはまらない場合の動作）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [静的 NAT 情報]
→ 「条件にあてはまらない場合の動作」[修正]



「条件にあてはまらない場合の動作」は、このネットワークに設定されている静的 NAT 定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。

動作

静的 NAT 定義のどれにも一致しない場合の IP フィルタリングの動作を以下の2つから選択します。

- 透過
静的 NAT 定義のどれにも一致しない場合にパケットを透過します。
- 破棄
静的 NAT 定義のどれにも一致しない場合にパケットを破棄します。

19.1.3.7 NAT あて先変換情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [NAT あて先変換情報]

■NAT あて先変換情報

※追加・修正情報は一覧ので設定してください。

プライベートアドレス	グローバルアドレス	操作
<input type="button" value="全削除"/>		
<NAT あて先変換情報入力フィールド>		
プライベートアドレス	<input type="text"/>	<input type="button" value="追加"/>
グローバルアドレス	<input type="text"/>	<input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているNAT あて先変換情報の定義が表示されています。NAT あて先変換の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プライベートアドレス

ローカルネットワーク側のIP アドレスを指定します。

なお、グローバルアドレスを範囲指定した場合、その範囲のグローバルアドレスはここで指定したアドレスを先頭とした範囲に変換されます。

例) プライベートアドレス : 192.168.1.100

グローバルアドレス : 172.16.1.100-172.16.1.200

NAT あて先変換後

プライベートアドレス : 192.168.1.100-192.168.1.200

グローバルアドレス

リモートネットワーク側のIP アドレスを指定します。範囲指定する場合は、"-" で区切れます。範囲指定した場合、プライベートアドレスも自動的に範囲指定されます。

19.1.3.8 帯域制御 (WFQ) 情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [帯域制御 (WFQ) 情報]

定義番号	ACL定義番号	帯域	操作
	ACL定義名		
全削除			
<帯域制御(WFQ)情報入力フィールド>			
帯域	<input type="radio"/> 最優先		
	<input type="radio"/> ベストエフォート		
	<input checked="" type="radio"/> 使用率	<input type="text"/> %	
	<input type="radio"/> 使用帯域	<input type="text"/> Kbps	<input type="button" value="参照"/>
	<input type="radio"/> 帯域を他と共有	<input type="button" value="共有できる定義が存在しません"/>	
ACL定義番号	<input type="text"/>	<input type="button" value="参照"/>	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報の ACL 定義が表示されています。帯域制御の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を 10 進数を使用して、1～99 の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが 100 を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbps または 1～100Mbps の範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

こんな事に気をつけて

シェーピングを使用しない場合、帯域制御機能は有効に動作しません。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

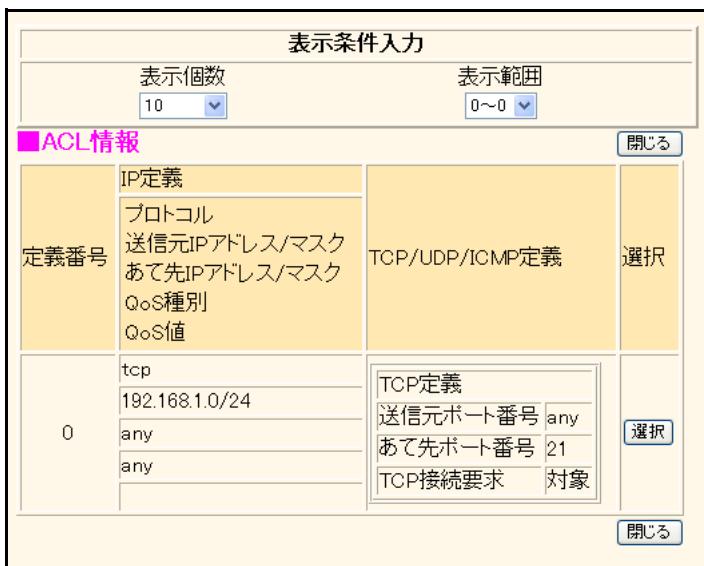
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → 「帯域制御 (WFO) 情報」→ 「ACL 定義番号の [参照]」



「ACL 情報」 - 「追加」／「修正」 - 「IP 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「帯域制御 (WFO) 情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「帯域制御 (WFO) 情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

19.1.3.8.1 帯域制御 (WFQ) 情報 (旧定義)

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連] → [帯域制御 (WFQ) 情報]
→ 「表示条件入力 (旧定義)」

表示条件入力																																
表示定義内容																																
旧定義																																
■帯域制御(WFQ)情報																																
※追加・修正情報は一覧の <input type="button" value="入力フィールド"/> で設定してください。																																
定義番号	送信元IPアドレス／マスク	対象TOSフィールド値	操作																													
プロトコル	送信元ポート番号	あて先IPアドレス／マスク	帯域																													
		あて先ポート番号																														
<input type="button" value="全削除"/>																																
<帯域制御(WFQ)情報入力フィールド>																																
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">プロトコル</td> <td style="width: 10%;">すべて</td> <td style="width: 10%;">(番号指定: <input type="text"/> "その他"を選択時の み有効です)</td> </tr> <tr> <td>送信元 情報</td> <td>IPアドレ ス</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>アドレス マスク</td> <td><input type="text"/> 0.0.0.0</td> </tr> <tr> <td></td> <td>ポート番 号</td> <td><input type="text"/></td> </tr> <tr> <td>あて先 情報</td> <td>IPアドレ ス</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>アドレス マスク</td> <td><input type="text"/> 0.0.0.0</td> </tr> <tr> <td></td> <td>ポート番 号</td> <td><input type="text"/></td> </tr> <tr> <td>対象TOSフィール ド値</td> <td colspan="3"><input type="text"/></td> </tr> <tr> <td>帯域</td> <td colspan="3"> <input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません </td> </tr> </table>				プロトコル	すべて	(番号指定: <input type="text"/> "その他"を選択時の み有効です)	送信元 情報	IPアドレ ス	<input type="text"/>		アドレス マスク	<input type="text"/> 0.0.0.0		ポート番 号	<input type="text"/>	あて先 情報	IPアドレ ス	<input type="text"/>		アドレス マスク	<input type="text"/> 0.0.0.0		ポート番 号	<input type="text"/>	対象TOSフィール ド値	<input type="text"/>			帯域	<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません		
プロトコル	すべて	(番号指定: <input type="text"/> "その他"を選択時の み有効です)																														
送信元 情報	IPアドレ ス	<input type="text"/>																														
	アドレス マスク	<input type="text"/> 0.0.0.0																														
	ポート番 号	<input type="text"/>																														
あて先 情報	IPアドレ ス	<input type="text"/>																														
	アドレス マスク	<input type="text"/> 0.0.0.0																														
	ポート番 号	<input type="text"/>																														
対象TOSフィール ド値	<input type="text"/>																															
帯域	<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません																															
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>																																

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

表示条件入力に、“旧定義”を選択した場合に、帯域制御 (WFQ) 情報の旧定義が表示されます。

プロトコル

帯域制御の対象となるプロトコルを以下の6つから選択します。() 内はプロトコル番号です。

- すべて
- TCP (6)
- UDP (17)
- ICMP (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IP アドレス／アドレスマスク

帯域制御の対象となるIP アドレスおよびアドレスマスクを指定します。対象となるパケットのIP アドレスと定義するアドレスマスクの論理積と、定義するIP アドレスとアドレスマスクの論理積が等しい場合に条件に一致します。省

略時は、すべてのIPアドレス／アドレスマスクが帯域制御の対象となります。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。省略時、または“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 TOS フィールド値

帯域制御の対象となるTOSフィールド値を16進数を使用して、0～ffの範囲または“any”で指定します。TOSフィールド値を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は、すべてのTOSフィールド値が帯域制御の対象となります。

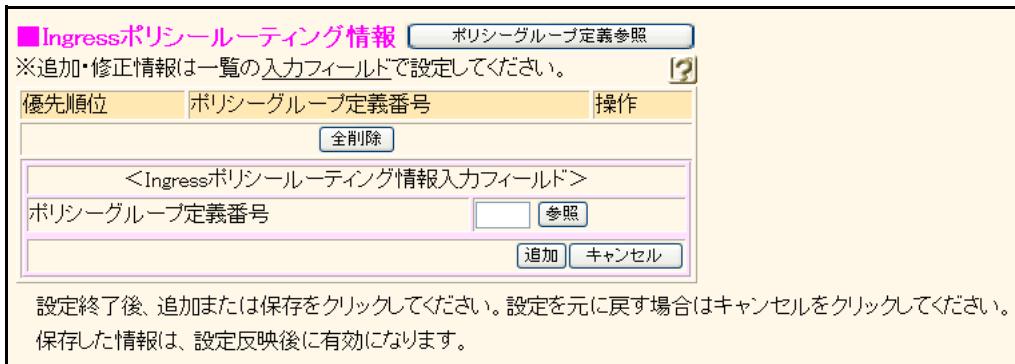
帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

19.1.3.9 Ingress ポリシールーティング情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連]
 → [Ingress ポリシールーティング情報]



現在、設定されている Ingress ポリシールーティング情報の定義が表示されています。処理は優先順位 1 から順に行われます。Ingress ポリシールーティング情報の定義数は、仕様一覧 「2.3 システム最大値一覧」 (P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に、指定されたポリシーグループに定義された送出先へパケットを送出します。

ポリシーグループ定義番号

[参照] ボタンをクリックして、ポリシーグループ定義番号を指定します。

別の画面に「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されます。指定する定義番号欄の [選択] ボタンをクリックし、ポリシーグループ定義番号を設定します。自動的に画面が閉じます。

なお、参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

- [操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IP 関連]
 → [Ingress ポリシールーティング情報] → 「ポリシーグループ定義番号の [参照]」



「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

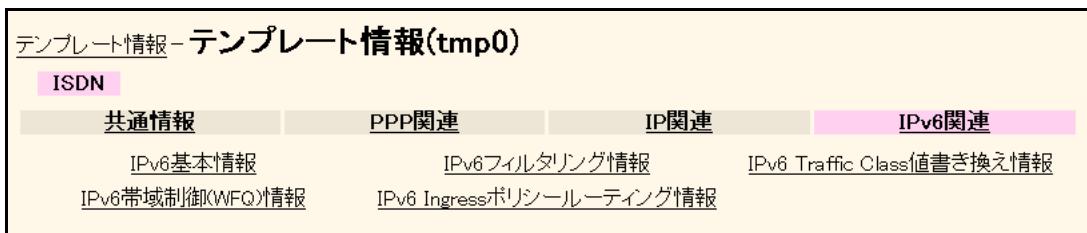
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ポリシーグループ定義情報の一覧に見たい情報だけを表示させることができます。

参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「Ingress ポリシールーティング情報」のポリシーグループ定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「Ingress ポリシールーティング情報」にポリシーグループ定義番号が設定され、画面が閉じます。[ポリシーグループ定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

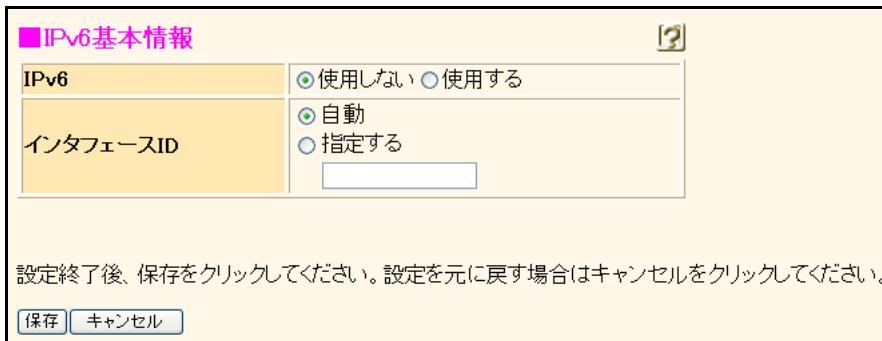
19.1.4 IPv6 関連

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連]



19.1.4.1 IPv6 基本情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 基本情報]



IPv6

テンプレート着信で使用する rmt インタフェースで、IPv6 の通信を使用する場合は、“使用する”を選択します。

インターフェース ID

テンプレート着信で使用する rmt インタフェースで利用する ID を設定します。“自動”を選択する場合は、装置の MAC アドレスから自動生成される EUI-64 形式のインターフェース ID を使用します。通常は、“自動”を選択します。

“指定する”を選択する場合は、16 ビットごとに区切り文字 (:) を入れて、16 進数を使用して 16 衔でインターフェース ID を指定します。このとき、他装置と同じインターフェース ID とならないような値を指定します。

記述例)

2001:db8:7654:3210

19.1.4.2 IPv6 フィルタリング情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 フィルタリング情報]

表示条件入力
表示定義内容
ACL対応定義

■ IPv6 フィルタリング情報 [ACL定義参照](#)

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	方向	ACL定義番号	操作
			ACL定義名	
条件にあてはまらない場合の動作	透過			修正 初期化
全削除				

<IPv6 フィルタリング情報入力フィールド>

動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
方向	入出力
ACL定義番号	参照

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 フィルタリング情報の ACL 定義が表示されています。処理は優先順位 1 から順に行います。IPv6 フィルタリングの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致する場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく行えません。

「条件にあてはまらない場合の動作」の [初期化] ボタンをクリックすると、初期状態（透過）が設定されます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

WWW や DHCP に対するアクセスを制限する設定を行った場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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IPv6アドレス／プレフィックス長とあて先IPv6アドレス／プレフィックス長
 - 送信元ポート番号とあて先ポート番号リバースを指定した場合は、入力パケットはIPv6アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

指定する定義番号欄の【選択】ボタンをクリックし、ACL定義番号を設定します。自動的に画面が閉じます。

なお、参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6関連] → [IPv6 フィルタリング情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報をだけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 フィルタリング情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

19.1.4.2.1 IPv6 フィルタリング情報（旧定義）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 フィルタリング情報]
→ 「表示条件入力（旧定義）」

表示条件入力

表示定義内容 旧定義																																																		
<p>■ IPv6 フィルタリング情報</p> <p>※追加・修正情報は一覧の<input type="text"/>で設定してください。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">優先順位</td> <td style="width: 10%;">動作</td> <td>送信元IPv6アドレス/プレフィックス長</td> <td>TCP接続要求</td> <td>Traffic Class</td> <td>方向</td> <td>操作</td> </tr> <tr> <td>動</td> <td>ブ</td> <td>送信元ポート番号</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>順</td> <td>ト</td> <td>あて先IPv6アドレス/プレフィックス長</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>位</td> <td>コ</td> <td>あて先ポート番号</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td>ル</td> <td>ICMPv6タイプ</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td>ICMPv6コード</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td colspan="2"></td> <td>条件にあてはまらない場合の動作</td> <td>透過</td> <td>修正</td> <td>初期化</td> <td></td> </tr> </table> <p style="text-align: right;">全削除</p>		優先順位	動作	送信元IPv6アドレス/プレフィックス長	TCP接続要求	Traffic Class	方向	操作	動	ブ	送信元ポート番号					順	ト	あて先IPv6アドレス/プレフィックス長					位	コ	あて先ポート番号						ル	ICMPv6タイプ							ICMPv6コード							条件にあてはまらない場合の動作	透過	修正	初期化	
優先順位	動作	送信元IPv6アドレス/プレフィックス長	TCP接続要求	Traffic Class	方向	操作																																												
動	ブ	送信元ポート番号																																																
順	ト	あて先IPv6アドレス/プレフィックス長																																																
位	コ	あて先ポート番号																																																
	ル	ICMPv6タイプ																																																
		ICMPv6コード																																																
		条件にあてはまらない場合の動作	透過	修正	初期化																																													
<p style="text-align: center;"><IPv6 フィルタリング情報入力フィールド></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">動作</td> <td><input checked="" type="radio"/> 透過 <input type="radio"/> 遮断</td> </tr> <tr> <td>プロトコル</td> <td>すべて <input checked="" type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)</td> </tr> <tr> <td>送信元情報</td> <td>IPv6アドレス/ プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/></td> </tr> <tr> <td>あて先情報</td> <td>IPv6アドレス/ プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/></td> </tr> <tr> <td>ICMPv6</td> <td>ポート番号 タイプ コード <input type="text"/></td> </tr> <tr> <td>TCP接続要求</td> <td><input checked="" type="radio"/> 対象 <input type="radio"/> 対象外</td> </tr> <tr> <td>Traffic Class</td> <td><input type="text"/></td> </tr> <tr> <td>方向</td> <td>入出力 <input type="button" value="▼"/></td> </tr> </table> <p style="text-align: right;">追加 キャンセル</p>		動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	プロトコル	すべて <input checked="" type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)	送信元情報	IPv6アドレス/ プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/>	あて先情報	IPv6アドレス/ プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/>	ICMPv6	ポート番号 タイプ コード <input type="text"/>	TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	Traffic Class	<input type="text"/>	方向	入出力 <input type="button" value="▼"/>																																	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断																																																	
プロトコル	すべて <input checked="" type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)																																																	
送信元情報	IPv6アドレス/ プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/>																																																	
あて先情報	IPv6アドレス/ プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/>																																																	
ICMPv6	ポート番号 タイプ コード <input type="text"/>																																																	
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外																																																	
Traffic Class	<input type="text"/>																																																	
方向	入出力 <input type="button" value="▼"/>																																																	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

表示条件入力に、“旧定義”を選択した場合に、IPv6 フィルタリング情報の旧定義が表示されます。

動作

IPv6 フィルタリングの動作を以下の 2 つから選択します。

- 透過
条件と一致する場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

プロトコル

フィルタリング条件としてプロトコルを以下の 5 つから選択します。（）内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、0～254 の範囲で指定します。

送信元／あて先情報

フィルタリング条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

フィルタリング条件としての IPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積、定義する IPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

ポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号がフィルタリングの対象となります。また、ポート番号を複数指定する場合は、”,” で区切れます。範囲指定の場合は、”-” で区切れます。送信元情報とあて先情報を合わせて 10 組まで指定できます。

ICMPv6

タイプ

フィルタリング条件として ICMPv6 パケットのタイプ値を 10 進数を使用して 0～255 の範囲または “any” で指定します。ICMPv6 タイプ値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての ICMPv6 タイプ値がフィルタリングの対象となります。

コード

フィルタリング条件として ICMPv6 パケットのコード値を 10 進数を使用して 0～255 の範囲または “any” で指定します。ICMPv6 コード値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての ICMPv6 コード値がフィルタリングの対象となります。

TCP 接続要求

TCP プロトコルでのコネクション接続要求をフィルタリングの対象に含める場合は、“対象”を選択します。プロトコルに TCP を設定した場合だけ有効です。

Traffic Class

フィルタリング条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0～ff の範囲または “any” で指定します。Traffic Class 値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての Traffic Class 値がフィルタリングの対象となります。

方向

フィルタリングする方向を選択します。

- 入力のみ
入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
入力パケットと出力パケットの両方をフィルタリング対象とします。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 IPv6 アドレス／プレフィックス長とあて先 IPv6 アドレス／プレフィックス長
 - 送信元ポート番号とあて先ポート番号
 リバースを指定した場合は、入力パケットは IPv6 アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP 接続要求」を有効にしている場合は、入力パケットに対しても TCP プロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。

19.1.4.2.2 IPv6 フィルタリング情報（条件にあてはまらない場合の動作）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 フィルタリング情報]
→ 「条件にあてはまらない場合の動作」[修正]

優先順位	動作	方向	ACL定義番号	操作
	<input checked="" type="radio"/> 透過		ACL定義名	
	<input type="radio"/> 遮断			
	<input type="radio"/> SPI			
	情報保持タイム 5 分			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

「条件にあてはまらない場合の動作」は、このテンプレートに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、[保存] ボタンをクリックすることによって、動作を決定することができます。優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えない場合があります。

こんな事に気をつけて

動作に遮断や SPI を指定し、IPv6 フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の3つから選択します。

- 透過
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IPv6 フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイム

SPI セッションに対応する情報は、一定の時間、該当する通信が行われない場合、自動的に解放されます。解放するための猶予時間を1秒～24時間の範囲で指定します。省略時は、5分が設定されます。セッションに対応する情報が解放された場合、それ以降のパケットは破棄されます。

19.1.4.3 IPv6 Traffic Class 値書き換え情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連]
→ [IPv6 Traffic Class 値書き換え情報]

優先順位	ACL定義番号	新Traffic Class	操作
ACL定義名			

新Traffic Class ACL定義番号

追加 **キャンセル**

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 Traffic Class 値書き換え情報の ACL 定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Traffic Class 値書き換えの定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 Traffic Class

IPv6 パケットに新しく指定する Traffic Class 値を 16 進数を使用して、0～ff の範囲で指定します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連]
 → [IPv6 Traffic Class 値書き換え情報] → 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

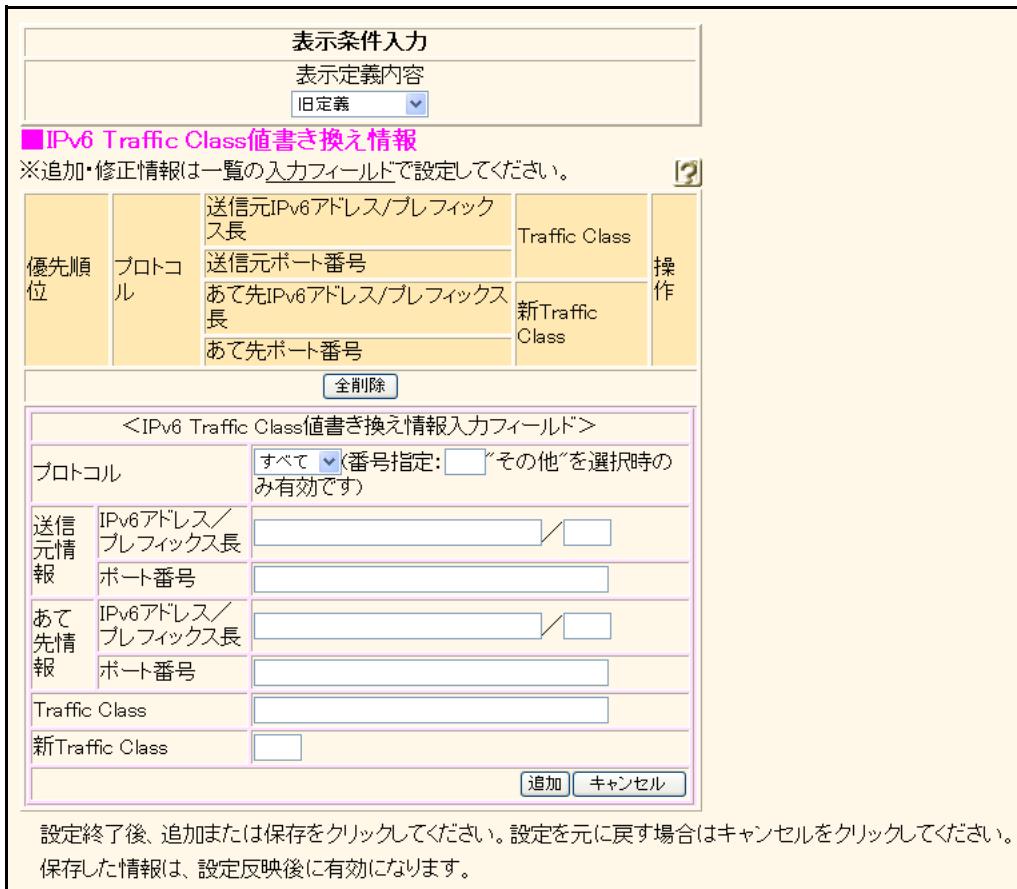
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報をだけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 Traffic Class 値書き換え情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「IPv6 Traffic Class 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

19.1.4.3.1 IPv6 Traffic Class 値書き換え情報（旧定義）

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連]
 → [IPv6 Traffic Class 値書き換え情報] → 「表示条件入力（旧定義）」



The screenshot shows the 'IPv6 Traffic Class 値書き換え情報' configuration screen. At the top, there is a dropdown menu set to 'Old Definition'. Below it, a table lists traffic class mapping rules:

優先順位	プロトコル	送信元IPv6アドレス/プレフィックス長	Traffic Class	操作
		送信元ポート番号	新Traffic Class	
		あて先IPv6アドレス/プレフィックス長		
		あて先ポート番号		

Below the table is a button labeled '全削除' (Delete All). A large pink box highlights the 'IPv6 Traffic Class 値書き換え情報' input field, which contains the following table:

<IPv6 Traffic Class 値書き換え情報入力フィールド>	
プロトコル	すべて <input checked="" type="checkbox"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)
送信元情報	IPv6アドレス/プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/>
ポート番号	<input type="text"/>
あて先情報	IPv6アドレス/プレフィックス長 <input type="text"/> <input checked="" type="checkbox"/>
ポート番号	<input type="text"/>
Traffic Class	<input type="text"/>
新Traffic Class	<input type="text"/>

At the bottom of the pink box are '追加' (Add) and 'キャンセル' (Cancel) buttons.

Below the form, a note states: '設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。保存した情報は、設定反映後に有効になります。'

表示条件入力に、"旧定義"を選択した場合に、IPv6 Traffic Class 値書き換え情報の旧定義が表示されます。

プロトコル

IPv6 Traffic Class 書き換え条件としてプロトコルを以下の5つから選択します。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

プロトコル番号を指定する場合は、"その他"を選択し、10進数を使用して、0～254の範囲で指定します。

送信元／あて先情報

IPv6 Traffic Class 値書き換え条件としてのアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

IPv6 Traffic Class 値書き換え条件としてのIPv6 アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6 アドレスと定義するプレフィックス長の論理積、定義するIPv6 アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

IPv6 Traffic Class 値書き換え条件としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が書き換えの対象となります。また、ポート番号を複数指定する場合は、”,” で区切れます。範囲指定の場合は “-” で区切れます。送信元情報とあて先情報を合わせて 10 組まで指定できます。

Traffic Class

Traffic Class 値書き換え条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0～ff の範囲または “any” で指定します。Traffic Class フィールド値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は “any” が設定され、すべての Traffic Class 値が書き換えの対象となります。

新 Traffic Class

IPv6 パケットに新しく指定する Traffic Class 値を 16 進数を使用して、0～ff の範囲で指定します。

19.1.4.4 IPv6 帯域制御 (WFQ) 情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報]

表示条件入力
表示定義内容
ACL対応定義

■ IPv6帯域制御(WFQ)情報 [ACL定義参照](#)

※追加・修正情報は一覧ので設定してください。

定義番号	ACL定義番号	帯域	操作
	ACL定義名		
全削除			

<IPv6帯域制御(WFQ)情報入力フィールド>

帯域	<input checked="" type="radio"/> 最優先
	<input type="radio"/> ベストエフォート
<input checked="" type="radio"/> 使用率	<input type="text"/> %
	<input type="radio"/> 使用帯域
<input type="radio"/> 帯域を他と共有	<input type="text"/> Kbps
	共有できる定義が存在しません
ACL定義番号	<input type="text"/> 参照

[追加](#) [キャンセル](#)

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている帯域制御情報の ACL 定義が表示されています。帯域制御の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

設定された任意のプロトコル、IPv6 アドレス、ポート番号、IPv6 Traffic Class 値の条件を元に帯域を割り当てます。

表示条件入力は、“ACL 対応定義” または “旧定義” から選択します。初期値は、ACL 対応定義情報が表示されています。なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を 10 進数を使用して、1～99 の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが 100 を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbps または 1～100Mbps の範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。

別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の「選択」ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 帯域制御 (WFO) 情報] → 「ACL 定義番号の [参照]」



「ACL情報」 - 「追加」／「修正」 - 「IPv6定義情報」および「TCP定義情報」で設定したACL定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL定義情報の一覧に見たい情報を表示させることができます。

参照するACL定義が存在しない場合は、「参照可能なACL情報が存在しません」が表示されます。[OK]ボタンをクリックして、設定をやり直してください。

「IPv6帯域制御 (WFO) 情報」のACL定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IPv6帯域制御 (WFO) 情報」にACL定義番号が設定され、画面が閉じます。[ACL定義参照]ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる]ボタンをクリックして、画面を閉じてください。

19.1.4.4.1 IPv6 帯域制御 (WFQ) 情報 (旧定義)

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連] → [IPv6 帯域制御 (WFQ) 情報]
→ 「表示条件入力 (旧定義)」

表示条件入力					
表示定義内容 <input type="button" value="旧定義"/>					
■ IPv6帯域制御(WFQ)情報					
※追加・修正情報は一覧の <input type="button" value="入力フィールド"/> で設定してください。					
定義番号	プロトコル	送信元IPv6アドレス／プレフィックス長	対象Traffic Class値	操作	帶域
		送信元ポート番号			
		あて先IPv6アドレス／プレフィックス長			
	あて先ポート番号				
<input type="button" value="全削除"/>					
<IPv6帯域制御(WFQ)情報入力フィールド>					
プロトコル		<input checked="" type="radio" value="すべて"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)			
送信元情報	IPv6アドレス／プレフィックス長	<input type="text"/> <input type="checkbox"/>			
	ポート番号	<input type="text"/>			
あて先情報	IPv6アドレス／プレフィックス長	<input type="text"/> <input type="checkbox"/>			
	ポート番号	<input type="text"/>			
対象Traffic Class値		<input type="text"/>			
帯域		<input type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input checked="" type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません			
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

表示条件入力に、"旧定義"を選択した場合に、IPv6 帯域制御 (WFQ) 情報の旧定義が表示されます。

プロトコル

帯域制御の対象となるプロトコルを以下の5つから選択します。()内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、"その他"を選択し、10進数を使用して、0~255の範囲で指定します。

送信元／あて先情報

帯域制御の対象となるアドレス情報を設定します。

IPv6 アドレス／プレフィックス長

帯域制御の対象となるIPv6アドレスおよびプレフィックス長を指定します。チェック対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積と、定義するIPv6アドレスとプレフィックス長の論理積が等しい場合に条件に一致します。

ポート番号

帯域制御の対象となるポート番号を10進数を使用して、1～65535の範囲または“any”で指定します。“any”を指定する場合は、すべてのポート番号が対象となります。また、ポート番号を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。送信元情報とあて先情報を合わせて10組まで指定できます。

対象 Traffic Class 値

帯域制御の対象となるIPv6パケットのTraffic Class値を16進数を使用して、0～ffの範囲または“any”で指定します。Traffic Class値を複数指定する場合は、“,”で区切れます。範囲指定の場合は、“-”で区切れます。10組まで指定できます。省略時は“any”が設定され、すべてのTraffic Class値が帯域制御の対象となります。

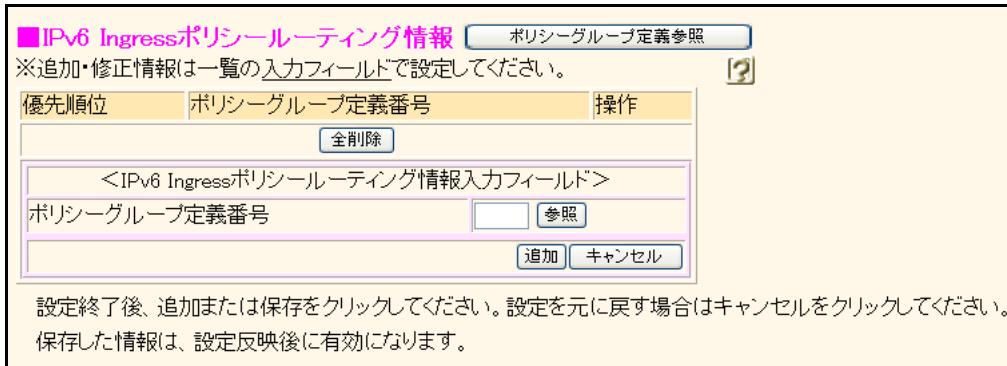
帯域

帯域の使用率または帯域値を指定します。

- 最優先
最優先データとして扱われます。
- ベストエフォート
非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
ほかの定義番号で定義されている帯域を共有します。

19.1.4.5 IPv6 Ingress ポリシールーティング情報

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連]
 → [IPv6 Ingress ポリシールーティング情報]



現在、設定されている IPv6 Ingress ポリシールーティング情報の定義が表示されています。処理は優先順位 1 から順に行われます。IPv6 Ingress ポリシールーティング情報の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に、指定されたポリシーグループに定義された送出先へパケットを送出します。

ポリシーグループ定義番号

[参照] ボタンをクリックして、ポリシーグループ定義番号を指定します。

別の画面に「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されます。指定する定義番号欄の「選択」ボタンをクリックし、ポリシーグループ定義番号を設定します。自動的に画面が閉じます。

なお、参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「テンプレート情報 (ISDN)」→ [追加] → [IPv6 関連]
 → [IPv6 Ingress ポリシールーティング情報] → 「ポリシーグループ定義番号の [参照]」



「ポリシーグループ情報」 - [追加] / [修正] で設定したポリシーグループ定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ポリシーグループ定義情報の一覧に見たい情報だけを表示させることができます。

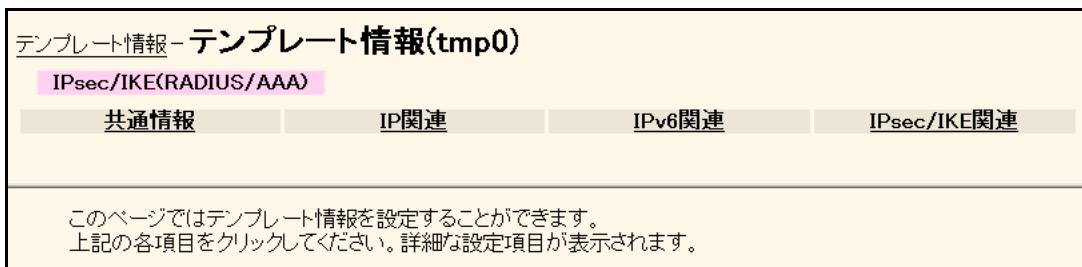
参照するポリシーグループ定義が存在しない場合は、「参照可能なポリシーグループ情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「IPv6 Ingress ポリシールーティング情報」のポリシーグループ定義番号に設定する定義番号欄の「選択」ボタンをクリックすると、「IPv6 Ingress ポリシールーティング情報」にポリシーグループ定義番号が設定され、画面が閉じます。[ポリシーグループ定義参照] ボタンをクリックした場合は、「選択」ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

19.2 接続種別：IPsec/IKE (RADIUS/AAA)

適用機種 全機種

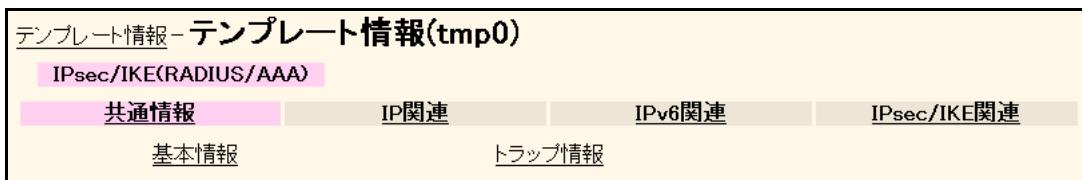
[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加]



「IP 関連」および「IPv6 関連」は、「接続種別：ISDN」を参照してください。

19.2.1 共通情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加] → [共通情報]



「Trap Information」は、「接続種別：ISDN」を参照してください。

19.2.1.1 基本情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加] → [共通情報]
→ [基本情報]

■ 基本情報	
テンプレート名	tmp0
使用するrmtインターフェース	rmt[]から[]インターフェースを予約
MTUサイズ	1500 バイト
無通信監視タイム	送受信パケットについて 0 秒
参照するAAA情報	[]
鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Responder)使用 自側エンドポイント: [] IDタイプ: <input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN <input type="radio"/> Main Mode(Responder)使用 自側エンドポイント: []
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 保存 キャンセル	

テンプレート名

テンプレートの名称を8文字以内で指定します。

使用する rmt インタフェース

テンプレート着信で使用する開始 rmt インタフェース番号とインターフェース数を10進数を使用して指定します。

こんな事に気をつけて

テンプレート着信用に予約した rmt インタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTU サイズ

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を10進数を使用して200～1500で指定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションにより、相手 MRU 値と相手 MRRU 値を MTU 値まで小さくすることができるようになります。省略時は、1500が指定されます。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を0～14400秒の範囲で指定します。0秒を指定した場合は、監視を行いません。設定された間、監視対象となるパケットがない場合に無通信として IPsec 接続を切断します。省略時は、無通信監視を行わないものとみなされます。

送信パケットおよび受信パケットが通信監視対象となります。

参照する AAA 情報

テンプレート着信で認証および着信時に参照する AAA グループ ID を、10進数を使用して10未満で指定します。

鍵交換モード

鍵交換モードを以下の2つから選択します。

- Aggressive Mode (Responder) 使用
相手側エンドポイントが可変IPアドレスでIPsec/IKEを利用して通信する場合に選択します。Aggressive Mode (Responder) を利用する場合、相手エンドポイント装置にAggressive Mode (Initiator) を設定してください。
- Main Mode (Responder) 使用
相手側および自側エンドポイントが固定IPアドレスでIPsec/IKEを利用して通信する場合に選択します。Main Mode (Responder) を利用する場合、相手エンドポイント装置にMain Mode を設定してください。

自側エンドポイント

IPv4/IPv6 アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254
::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:～feff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

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通信では、自側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。

ID タイプ

ネゴシエーションの交換 ID タイプを選択します。

19.2.2 IPsec/IKE 関連

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加] → [IPsec/IKE 関連]



19.2.2.1 IPsec 情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加] → [IPsec/IKE 関連] → [IPsec 情報]

SAの設定	暗号アルゴリズム	<input type="checkbox"/> aes-cbc-256 <input type="checkbox"/> aes-cbc-192 <input type="checkbox"/> aes-cbc-128 <input type="checkbox"/> 3des-cbc <input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 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更新	SA有効データ量	0 GByte
	Initiator時	時間 90 秒 データ量 0 MByte
	Responder時	<input checked="" type="radio"/> 更新しない <input type="radio"/> 更新する 時間 _____秒 データ量 0 MByte

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。



◆ IPsec で使用するプロトコル

IPsec で使用するプロトコルは、IPsec の設定により決定します。プロトコルは AH と ESP があり、1つの IPsec 情報定義に暗号情報と認証情報の両方を指定すると認証付き ESP となります。

アルゴリズムの組み合わせは、以下のとおりです。

暗号情報	認証情報	プロトコル
暗号化しない	<input type="radio"/>	AH (認証)
<input type="radio"/>	認証なし	ESP (暗号)
<input type="radio"/>	<input type="radio"/>	ESP (認証+暗号)

暗号情報○ : des-cbc、3des-cbc、null、aes-cbc-128、aes-cbc-192 または aes-cbc-256

認証情報○ : hmac-md5 または hmac-sha1

※ 「暗号化しない」とは、暗号アルゴリズムを1つも選択しないことを指します。

「認証なし」とは、認証アルゴリズムで“認証なし”を選択または認証アルゴリズムを1つも選択しないことを指します。

SAの設定

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを使用する場合に選択します。複数選択した場合、aes-cbc-256、aes-cbc-192、aes-sbs-128、3des-cbc、des-cbc、nullの順に比較されます。暗号アルゴリズムを選択しない場合は、パケットの暗号化を行いません。

認証アルゴリズム

トンネリングするパケットの認証アルゴリズムを選択します。複数選択した場合、hmac-md5、hmac-sha1、認証なしの順に比較されます。認証アルゴリズムを選択しない場合および“認証なし”だけを選択した場合は、パケットの認証を行いません。

PFS時のDHグループ

自動鍵交換の鍵を生成するための鍵素材です。値が大きい程セキュリティ強度は高くなります。ただし、装置の負荷が高くなる場合があります。使用しない場合は、“使用しない”を選択します。

SA有効時間

SAの有効期限を以下の範囲で指定します。指定した時間が経過した時点で、SAの有効期限が切れ、IKEによってSA情報や鍵情報が自動的に更新されます。省略時は、8時間が設定されます。

有効範囲)

600～86400秒

10～1440分

1～24時間

SA有効データ量

SAの有効期限をデータ量で指定します。指定したデータ量を経過した時点で、SAの有効期限が切れ、IKEによってSA情報や鍵情報が自動的に更新されます。省略時は、0が設定されデータ量によるSA更新が行われません。

有効範囲)

2400～110592000キロバイト

3～108000メガバイト

1～105ギガバイト

SA更新

SAの更新時間を設定します。

Initiator時

自側が Initiator の場合に、IPsec SA の有効時間または有効データ量が満了になる前に IPsec で SA の更新を行うための時間とデータ量を指定します。また、IPsec SA 更新のデータ量は、IPsec SA の有効データ量が定義されていない場合は無効となります。

相手側の Responder 時の SA 更新時間とデータ量と同じにならないように設定してください。

時間

30～180秒の範囲で指定します。省略時は、90秒が設定されます。

データ量

120～230400キロバイトの範囲で指定します。省略時は、0KByteが設定されます。

Responder時

自側が Responder の場合に、IPsec SA の有効時間または有効データ量が満了になる前に IPsec SA の更新を行う場合は、“更新する”を選択します。“更新する”を選択した場合、更新を行う時間とデータ量を設定します。“更新しない”を選択した場合、Responder 側からの SA の更新は行いません。また、IPsec SA 更新のデータ量は、IPsec SA の有効データ量が定義されていない場合は無効となります。

相手側の Initiator 時の SA 更新時間とデータ量と同じにならないように指定してください。

時間

30～180秒の範囲で指定します。省略時は、30秒が設定されます。

データ量

120～230400キロバイトの範囲で指定します。省略時は、0KByteが設定されます。

19.2.2.2 IKE情報 (IKEv1)

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加] → [IPsec/IKE 関連]
→ [IKE情報 (IKEv1)]

IKE情報(IKEv1)

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)
	SA有効時間	24 時間
	初回再送時間	10 秒
	再送回数	3 回
	NATトラバーサル機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
DPD機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する	
	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
	再送回数	3 回

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

SAの設定

暗号アルゴリズム

IKEセッションの送受信パケットを暗号化／複号化するためのアルゴリズムを選択します。

認証（ハッシュ）アルゴリズム

IKEセッションのネゴシエーションパケットを認証するためのアルゴリズムを選択します。

DHグループ (Diffie-Hellman グループ)

自動鍵交換で鍵を生成するための鍵素材を選択します。値が大きい程セキュリティ強度は高くなります。ただし、鍵生成のための計算に時間がかかるため、装置の負荷が高くなる場合があります。

SA有効時間

IKE SAの有効期限を以下の範囲で指定します。指定した時間が経過した時点で、SAの有効期限が切れ、IKE SA情報や鍵情報がIKEによって自動的に更新されます。省略時は、24時間が設定されます。

有効範囲)

600～86400秒

10～1440分

1～24時間

初回再送時間

IKEの初回再送時間を10進数を使用して、1～60秒の範囲で指定します。省略時は、10秒が設定されます。

再送回数

IKEの再送回数を10進数を使用して、1～10回の範囲で指定します。省略時は、3回が設定されます。

NAT トランザクション機能

IKE ネゴシエーションパケットや ESP パケットの送信元 IP アドレス、あと先 IP アドレスまたはポート番号が NAT 変換される環境では、“使用する”を選択します。

こんな事に気をつけて

- 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 トランザクションのバージョンが異なると、NAT トランザクションはできません。
NAT トランザクションは、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 トランザクション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 情報」画面の暗号アルゴリズムを設定してください。暗号アルゴリズム設定がない場合は動作しません。
- 「共通情報」画面の自側エンドポイントに 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。
- 「共通情報」画面の鍵交換モードに “Aggressive Mode (Responder) 使用” を選択してください。“Main Mode (Responder) 使用” を選択した場合は動作しません。

DPD 機能

DPD 機能を使用する場合は、“使用する”を選択します。

こんな事に気をつけて

無通信監視時間は再送時間 × (再送回数 + 1) 秒より大きくなるように指定してください。

IPsec 受信パケット無通信監視時間

DPD パケットの送信を開始する IPsec 受信パケット無通信監視時間を 10 進数を使用して、5 ~ 600 秒の範囲で指定します。省略時は、10 秒が設定されます。

再送時間

DPD パケットの再送時間を 10 進数を使用して、1 ~ 60 秒の範囲で指定します。省略時は、1 秒が設定されます。

再送回数

DPD パケットの再送回数を 10 進数を使用して、1 ~ 10 回の範囲で指定します。省略時は、3 回が設定されます。

19.2.2.3 接続制御情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (RADIUS/AAA))」→ [追加] → [IPsec/IKE 関連]
 → [接続制御情報]

■接続制御情報	
接続先監視	送信元IPアドレス 正常時送信間隔
	<input type="text"/> 秒
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

接続先監視

送信元 IP アドレス

接続先の生存確認を行うために ICMP ECHO パケットを送信する送信元 IP アドレスとして、本装置に設定している自側 IPv4/IPv6 アドレスを指定します。指定可能な範囲は以下のとおりです。タイムアウト時間までに応答がない場合に、IPsec 接続を切断します。省略時は、接続先監視を使用しないものとみなされます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

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 通信では、テンプレート定義の送信元 IP 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。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、ICMP ECHO パケットを次に送信する間隔を、10進数を使用して 1 ~ 60 秒の範囲で指定します。



◆ 接続先監視

接続先の生存確認を行うための動作情報を指定します。「AAA情報」の「接続制御情報」で指定したあて先IPアドレスに対してICMP ECHOパケットを送信し、タイムアウト時間までに応答がない場合この接続先を使用不可状態にします。省略時は、接続先監視を使用しないものとみなされます。あて先IPアドレスは、接続するAAAユーザ情報によりRADIUSサーバに登録している情報を使用する場合があります。

- 送信元IPアドレス : 「テンプレート情報」の「接続制御情報」で指定した送信元IPアドレス
- あて先IPアドレス : 「AAA情報」の「接続制御情報」で指定したあて先IPアドレス
- 無通信監視タイマ : 「テンプレート情報」の「共通情報」で指定した無通信監視タイマ
(省略または1~9秒が指定されている場合は10秒)
- 正常時送信間隔 : ICMP ECHOパケットの応答が正常に受信されている状態で、次にICMP ECHOパケットを送信する間隔を、1秒~60秒の10進数で指定します。省略時は、無通信監視タイマの1/2を正常時送信間隔として動作します。
(1~9秒が指定されている場合は5秒)
- タイムアウト時間 : 正常時送信間隔と同等
- リトライ間隔 : 2秒
- 監視モード : 無通信時に監視する

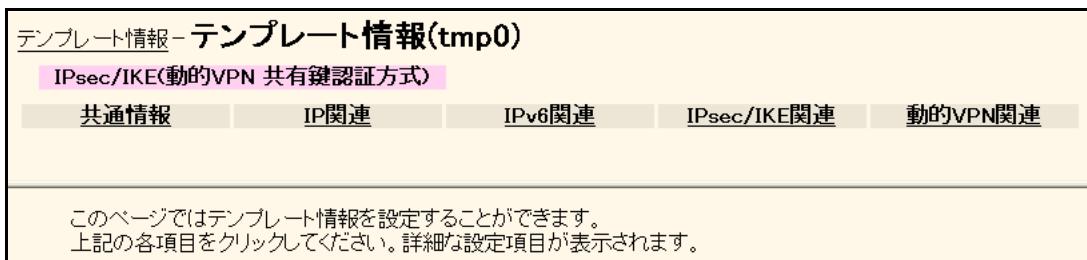
接続先監視と無通信監視タイマの動作は以下のとおりです。

	接続先監視あり		接続先監視なし
	正常時送信間隔あり	正常時送信間隔なし	
無通信監視タイマあり	正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で無通信監視タイマのみ動作する
無通信監視タイマなし	正常時送信間隔は設定値でその他は無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する	無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する	動作しない

19.3 接続種別：IPsec/IKE（動的VPN共有鍵認証方式）

適用機種 全機種

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]



「IP 関連」および「IPv6 関連」は、「接続種別：ISDN」を参照してください。

19.3.1 共通情報

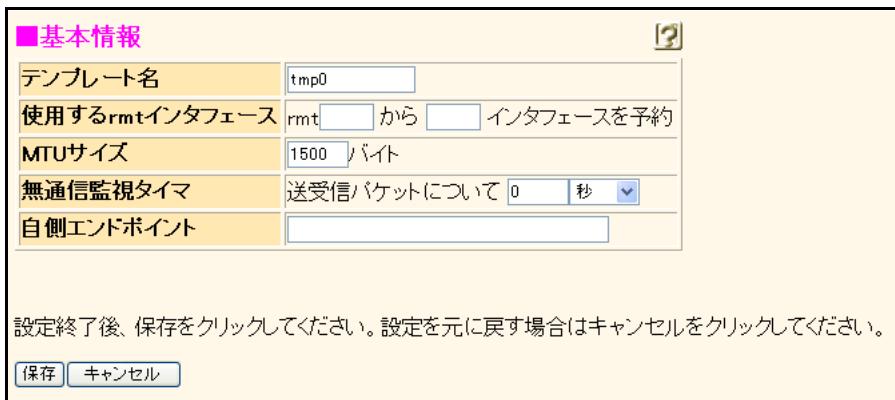
[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加] → [共通情報]



「Trap Information」は、「接続種別：ISDN」を参照してください。

19.3.1.1 基本情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加] → [共通情報] → [基本情報]



テンプレート名

テンプレートの名称を8文字以内で指定します。

使用する rmt インタフェース

テンプレート着信で使用する開始 rmt インタフェース番号とインターフェース数を 10 進数を使用して指定します。

こんな事に気をつけて

テンプレート着信用に予約した rmt インタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTU サイズ

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を 10 進数を使用して 200～1500 で指定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。省略時は、1500 が指定されます。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を 0～14400 秒の範囲で指定します。省略または 10 秒未満を指定した場合は、10 秒が指定されます。設定された間、監視対象となるパケットがない場合に無通信として IPsec 接続を切断します。

送信パケットおよび受信パケットが通信監視対象となります。

自側エンドポイント

テンプレート着信で IPsec/IKE 接続するときの自側エンドポイントの IPv4/IPv6 アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254
::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:～feff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

- 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場合は上位を “dhcp@インターフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には IPv6 DHCP クライアント機能が動作している rmt インタフェースを設定してください。
- 接続種別が動的 VPN の場合は、鍵交換モードは自動的に Main Mode となります。

19.3.2 IPsec/IKE 関連

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]
→ [IPsec/IKE 関連]



「IPsec 情報」は、「接続種別：IPsec/IKE (RADIUS/AAA)」を参照してください。

※SA 更新の Responder 時の初期画面は、"更新する"となります。

19.3.2.1 IKE 情報 (動的VPN接続 共有鍵認証方式)

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]
→ [IPsec/IKE 関連] → [IKE 情報 (動的VPN共有鍵認証方式)]

共有鍵認証	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	<input type="text"/>
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)
	SA有効時間	24 時間
初回再送時間	10 秒	
再送回数	3 回	
DPD機能	使用しない <input checked="" type="radio"/> 使用する <input type="radio"/>	
	IPsec受信パケット無通信監視時間	10 秒
	再送時間	1 秒
	再送回数	3 回

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

「共有鍵認証」以外の項目の説明は、「IKE 情報 (IKEv1)」を参照してください。

共有鍵認証

IKE の認証に用いる鍵を設定します。本装置の IKE の認証には事前共有鍵認証と RSA デジタル証明認証方式があります。ここでは事前共有鍵 (Pre-shared key) の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲 (16 進数鍵)	入力範囲 (文字列鍵)
1 ~ 256 行	1 ~ 128 文字

鍵識別

鍵の識別を選択します。

19.3.2.2 接続制御情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]
→ [IPsec/IKE 関連] → [接続制御情報]

■接続制御情報	
接続先監視	送信元IPアドレス 正常時送信間隔
	<input type="text"/> 秒
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

接続先監視

送信元IPアドレス

接続先の生存確認を行うために ICMP ECHO パケットを送信する送信元 IP アドレスとして、本装置に設定している自側 IPv4/IPv6 アドレスを指定します。指定可能な範囲は以下のとおりです。タイムアウト時間までに応答がない場合に、IPsec 接続を切断します。省略時は、接続先監視を使用しないものとみなされます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

- 接続先監視は相手装置から指定された接続先監視アドレスがあて先 IP アドレスとなるため、双方の装置で指定する必要があります。片方の装置のみで接続先監視を指定した場合は、接続先監視は行われません。
- 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場合は上位を “dhcp@ インタフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には IPv6 DHCP クライアント機能が動作している rmt インタフェースを設定してください。

正常時送信間隔

ICMP ECHO パケットの応答が正常に受信されている状態で、ICMP ECHO パケットを次に送信する間隔を、10進数を使用して 1 ~ 60 秒の範囲で指定します。



◆ 接続先監視

接続先の生存確認を行うための動作情報を指定します。指定した送信元 IP アドレスは動的 VPN 情報交換機能を使用して相手装置と交換します。相手装置から受信したあて先 IP アドレスに対して ICMP ECHO パケットを送信し、タイムアウト時間までに応答がない場合この接続先を使用不可状態にします。

送信元 IP アドレスを省略したときは、接続先監視を使用しないものとみなされます。接続先監視は相手装置から指定された接続先監視アドレスがあて先 IP アドレスとなりますので双方の装置で指定する必要があります。片方の装置のみで接続先監視を指定した場合は、接続先監視は行われません。

- 送信元 IP アドレス : 「テンプレート情報」の「接続制御情報」で指定した送信元 IP アドレス
- あて先 IP アドレス : 動的 VPN 接続で交換された相手の IP アドレス
- 無通信監視タイマ : 「テンプレート情報」の「共通情報」で指定した無通信監視タイマ
(省略または 1~9 秒が指定されている場合は 10 秒)
- 正常時送信間隔 : ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を、1 秒~60 秒の 10 進数で指定します。省略時は、無通信監視タイマの 1/2 を正常時送信間隔として動作します。
(1~9 秒が指定されている場合は 5 秒)
- タイムアウト時間 : 正常時送信間隔と同等
- リトライ間隔 : 2 秒
- 監視モード : 無通信時に監視する

接続先監視と無通信監視タイマの動作は以下のとおりです。

	接続先監視あり		接続先監視なし
	正常時送信間隔あり	正常時送信間隔なし	
無通信監視タイマあり	正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で無通信監視タイマのみ動作する
無通信監視タイマなし	正常時送信間隔は設定値でその他は無通信監視タイマが 10 秒で設定されたものとみなし接続先監視が動作する	無通信監視タイマが 10 秒で設定されたものとみなし接続先監視が動作する	無通信監視タイマが 10 秒で設定されたものとみなし無通信監視タイマのみ動作する

19.3.3 動的VPN関連

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]
→ [動的VPN関連]

テンプレート情報 - テンプレート情報(tmp0)

IPsec/IKE(動的VPN 共有鍵認証方式)

共通情報	IP関連	IPv6関連	IPsec/IKE関連	動的VPN関連
基本情報	自側ネットワーク情報			

19.3.3.1 基本情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]
→ [動的VPN関連] → [基本情報]

■ 基本情報

ドメイン情報		<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 0(example.jp.com)	
サーバ情報	アドレス	<input type="text"/>	
	ポート番号	5070	
	認証ID	<input type="text"/>	
セカンダリサーバ情報	アドレス	<input type="text"/>	
	ポート番号	5070	
	認証ID	<input type="text"/>	
有効期間		1 時間	
セッション更新間隔		<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間 5 分	
クライアントIPアドレス		<input type="text"/>	
ドメイン名		<input type="text"/>	
VPN通信	利用インターフェース	lan0	
	中継ルータアドレス	※LANインターフェース選択時のみ指定してください	
	終端グローバルアドレス	<input type="text"/>	
自側ユーザID		<input type="text"/>	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

ドメイン情報

動的VPN接続で使用するドメイン情報を選択します。

“使用する”を選択すると、表示される画面が変わります。ドメイン情報だけを設定します。ドメイン情報は、「動的VPN情報」→クライアント関連情報「ドメイン情報」の設定を使用します。選択できない場合は、「動的VPN情報」→クライアント関連情報「ドメイン情報」を設定してください。

使用しない場合は、以下の項目を設定します。

サーバ／セカンダリサーバ情報

アドレス

動的VPNサーバのアドレスを指定します。

IP アドレス指定する場合

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

FQDN 指定する場合

FQDN を 80 文字以内で設定してください。

なお、RFC1034 では英数字、"-" (ハイフン)、"." (ピリオド) でドメイン名をつけることを推奨しています。

こんな事に気をつけて

FQDN 指定する場合は、クライアントIPアドレスのアドレスファミリに従って IP アドレスを取得します。

ポート番号

動的VPNサーバが要求を受信するポート番号を10進数を使用して、1～65535の範囲で指定します。省略時は、5070が設定されます。

認証 ID

動的VPNサーバへ自装置情報を登録するときに使用する認証IDを50文字以内の文字列で指定します。

認証パスワード

動的VPNサーバへ自装置情報を登録するときに使用する認証パスワードを50文字以内の文字列で指定します。

有効期間

動的VPNサーバに登録する自装置の有効期間を90～86400秒の範囲で指定します。省略時は、1時間が設定されます。

セッション更新間隔

確立した動的VPNセッションを更新する時間を90秒～3600秒の範囲で指定します。

省略時は、5分が指定されます。

“更新しない”を選択した場合、確立した動的VPNセッションを更新しません。

動的VPNセッションを更新しない場合、動的VPN接続で確立したIPsec/IKEセッションを継続することが可能になりますが、回線障害などにより動的VPNセッションが残ってしまうことがあるので通常は、セッション更新間隔を利用して下さい。

クライアントIPアドレス

クライアントのIPアドレスを指定します。

クライアントのIPアドレスは、動的VPNサーバとの通信および相手動的VPNクライアントとの情報交換に使用されます。動的VPNサーバおよび相手動的VPNクライアントとの通信がIPsec対象となる場合は、IPsec対象範囲に含まれるインターフェースのIPアドレスを設定してください。IPsec対象とならない場合は、送出インターフェースとなるインターフェースのIPアドレスを設定してください。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

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場合は上位を “dhcp@インターフェース名” の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には IPv6 DHCP クライアント機能が動作している rmtインターフェースを設定してください。

ドメイン名

動的VPNサーバに登録する自側情報（ユーザID）に使用されるドメイン名を80文字以内で指定します。

VPN通信

利用インターフェース／中継ルータアドレス

動的VPNとして接続されるIPsecトンネルが通信に利用するインターフェースを指定します。

lanインターフェースを利用する場合は、中継ルータアドレスを必ず指定してください。

終端グローバルアドレス

相手装置に通知するVPN終端グローバルアドレスを指定します。

省略時に、VPN通信で利用するインターフェースでlanインターフェースを指定した場合は、指定されたlanインターフェースに設定されたアドレス、またはDHCPによりそのインターフェースに割り当てられたアドレスが利用されます。VPN通信で利用するインターフェースでrmtインターフェースを指定した場合は、指定されたrmtインターフェースに設定されたアドレス、またはPPPにより割り当てられたアドレスが利用されます。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

自側ユーザID

動的VPNサーバに登録する自側ユーザIDを50文字以内で指定します。

使用できる文字は、半角英数字、"-"、"_"、"_"です。

自側ユーザIDは、ドメイン名と結合して以下のように生成されて動的VPNサーバに登録されます。

例) 自側ユーザIDにshisya、ドメイン名にexample.comを指定した場合
shisya@example.com

こんな事に気をつけて

自側ユーザIDは、オペレータの指示で動的VPN接続を行う場合に設定してください。

19.3.3.2 自側ネットワーク情報

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN共有鍵認証方式))」→ [追加]
→ [動的VPN関連] → [自側ネットワーク情報]

■自側ネットワーク情報

※追加・修正情報は一覧ので設定してください。

定義番号	動的VPNで接続する自側ネットワーク	動的VPNサーバ登録	操作
<input type="button" value="全削除"/>			
<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	<input type="text"/> <small>※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。</small>	<input checked="" type="radio"/> する <input type="radio"/> しない	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている自側ネットワーク情報の定義が表示されています。自側ネットワークの定義数は、20個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

動的VPNで接続する自側ネットワーク

動的VPNで接続する自側ネットワークをIPv4アドレスとマスクビット数（またはマスク値）またはIPv6アドレスとプレフィックス長で指定します。

- IPv4アドレスを指定する場合
IPv4アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから1で連続した値にしてください。
デフォルトルートを設定する場合は、0.0.0.0/0 (0.0.0.0/0.0.0.0) を指定します。
- IPv6アドレスを指定する場合
IPv6アドレスとプレフィックスの組み合わせで指定します。リンクローカルアドレスは指定できません。
デフォルトルートを設定する場合は、::/0を指定します。
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場合は、上位を"dhcp@インターフェース名"の形式で指定し、下位80ビット分を標準的なIPv6アドレス表記方式で指定します。インターフェース名には、IPv6 DHCP クライアント機能が動作しているrmtインターフェースを指定してください。

こんな事に気をつけて

動的VPNで接続する自側ネットワークは、「動的VPN情報」 - 「クライアント関連情報」 - ドメイン情報「自側ネットワーク情報」の「動的VPNで接続する自側ネットワーク」と重複して指定することはできません。

動的VPNサーバ登録

自側ネットワークを自側ユーザIDとして動的VPNサーバに登録する場合は、“する”を選択します。

“する”を設定した場合、通信パケット契機で動的VPN接続することができます。

“しない”を設定した場合、「基本情報」の自側ユーザIDが設定されいれば、オペレータの指示で動的VPN接続をすることができます。通常は、動的VPNサーバに登録してください。動的VPNサーバに登録する場合は、自側ネットワークとドメイン名と結合して以下のように生成されて登録されます。

例) 自側ネットワークに192.168.1.0/24 (2001:db8:1111::1/64)、ドメイン名にexample.comを指定した場合
IPsecIKE)c0a80100/24@example.com
IPsecIKE)2001:db8:1111:1::64@example.com

19.4 接続種別：IPsec/IKE（動的VPN接続 RSAデジタル署名認証方式）

適用機種 全機種

[操作] ルータ設定「テンプレート情報（IPsec/IKE（動的VPN接続 RSAデジタル署名認証方式））」→ [追加]

テンプレート情報 - テンプレート情報(tmp0)

IPsec/IKE(動的VPN接続 RSAデジタル署名認証方式)

共通情報 IP関連 IPv6関連 IPsec/IKE関連 動的VPN関連

このページではテンプレート情報を設定することができます。
上記の各項目をクリックしてください。詳細な設定項目が表示されます。

「IP関連」および「IPv6関連」は、「接続種別：ISDN」を参照してください。

「動的VPN関連」は、「接続種別：IPsec/IKE（動的VPN共有鍵認証方式）」を参照してください。

19.4.1 共通情報

[操作] ルータ設定「テンプレート情報（IPsec/IKE（動的VPN接続 RSAデジタル署名認証方式））」→ [追加]
→ [共通情報]

テンプレート情報 - テンプレート情報(tmp0)

IPsec/IKE(動的VPN接続 RSAデジタル署名認証方式)

共通情報 IP関連 IPv6関連 IPsec/IKE関連 動的VPN関連

基本情報 トラップ情報

「トラップ情報」は、「接続種別：ISDN」を参照してください。

19.4.1.1 基本情報

[操作] ルータ設定「テンプレート情報（IPsec/IKE（動的VPN接続 RSAデジタル署名認証方式））」→ [追加]
→ [共通情報] → [基本情報]

■ 基本情報	
テンプレート名	tmp0
使用するrmtインターフェース	rmt[]から[]インターフェースを予約
MTUサイズ	1500 ノード
無通信監視タイム	送受信パケットについて[]秒

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

テンプレート名

テンプレートの名称を8文字以内で指定します。

使用する rmt インタフェース

テンプレート着信で使用する開始 rmt インタフェース番号とインターフェース数を 10 進数を使用して指定します。

こんな事に気をつけて

テンプレート着信用に予約した rmt インタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTU サイズ

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を 10 進数を使用して 200～1500 で指定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。省略時は、1500 が指定されます。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を 0～14400 秒の範囲で指定します。省略または 10 秒未満を指定した場合は、10 秒が指定されます。設定された間、監視対象となるパケットがない場合に無通信として IPsec 接続を切断します。

送信パケットおよび受信パケットが通信監視対象となります。

19.4.2 IPsec/IKE 関連

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN接続 RSAデジタル署名認証方式))」→ [追加] → [IPsec/IKE 関連]



「IPsec 情報」は、「接続種別：IPsec/IKE (RADIUS/AAA)」を参照してください。

「接続制御情報」は、「接続種別：IPsec/IKE (動的VPN共有鍵認証方式)」を参照してください。

※SA更新の Responder 時の初期画面は、"更新する"となります。

19.4.2.1 IKE 情報 (動的VPN接続 RSAデジタル署名認証方式)

[操作] ルータ設定「テンプレート情報 (IPsec/IKE (動的VPN接続 RSAデジタル署名認証方式))」→ [追加] → [IPsec/IKE 関連] → [IKE 情報 (動的VPN RSAデジタル署名認証方式)]

「RSAデジタル署名認証」以外の項目の説明は、「IKE情報(IKEv1)」を参照してください。

RSA デジタル署名認証

IKE の認証に用いる証明書を指定します。本装置の IKE の認証には事前共有鍵認証と RSA デジタル証明認証方式があります。ここでは RSA デジタル証明書の設定を行います。

こんな事に気をつけて

テンプレートが利用する機能に動的 VPN 機能が設定された場合に動作します。相手装置認証方式の設定に RSA デジタル署名認証方式が設定されていた場合に動作します。

自装置識別情報

自装置の識別情報の設定します。

自装置を識別する名前を 1 ~ 64 文字で指定します。

識別情報は、0x21、0x23 ~ 0x7e のコードで構成される ASCII 文字列で指定します。

ID タイプ

ネゴシエーションの交換 ID タイプを選択します。

こんな事に気をつけて

ID タイプに "X501_sbj" を設定する場合は、Aggressive モードで使用することはできません。

自装置証明書識別番号

自装置証明書の識別番号を選択します。

認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

秘密鍵識別番号

秘密鍵の識別番号を選択します。

認証方式として RSA デジタル署名方式を使用する場合は必ず設定してください。

自装置証明書情報の送信

自装置証明書の送信設定を選択します。

- 証明書要求ペイロード受信時
相手装置から証明書要求ペイロードを受信したときに、自装置証明書情報を送信します。
- 常時
相手装置から証明書要求ペイロードの受信にかかわらず、常に自装置証明書情報を送信します。

証明書要求

証明書要求の送信設定を選択します。

- 送信しない
証明書要求を送信しません。
- 送信する
証明書要求を送信します。

認証局識別番号

証明書要求の送信設定を「送信する」に選択した場合に、使用する認証局情報の識別番号を選択します。選択した認証局情報を証明書要求に入れて送信します。

「指定なし」を選択した場合は、何も入れないで証明書要求を送信します。

有効期限切れ証明書

有効期限が切れている証明書を使用するかどうかを選択します。

- 使用する
有効期限が切れている証明書をそのまま使用します。
- 使用しない
有効期限が切れている証明書を使用しません。この場合、IKE ネゴシエーションに失敗します。

20 LLDP 情報

適用機種 全機種

[操作] ルータ設定「LLDP情報」



20.1 基本情報

[操作] ルータ設定「LLDP情報」→ [基本情報]

■ 基本情報	
送信間隔時間	<input type="button" value="時間 ▾"/>
最小送信間隔時間	<input type="button" value="時間 ▾"/>
保持回数	<input type="button" value="回"/>
送信停止時遅延時間	<input type="button" value="秒"/>
受信情報更新通知最小間隔時間	<input type="button" value="時間 ▾"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

LLDP (Link Layer Discovery Protocol : 隣接探索プロトコル) の装置全体に関する設定を行います。

こんな事に気をつけて

ポートごとの設定は、「LAN情報」 - 「基本情報」 - 「LLDP情報」で行ってください。

送信間隔時間

LLDP情報を定期的に送信する間隔時間を5~32768秒の範囲で指定します。

最小送信間隔時間

最小送信間隔時間を1秒~(0.25×送信間隔時間)の範囲で指定します。

設定変更などによりLLDP情報が変化したときに即座にLLDP情報を送信しますが、最後にLLDP情報を送信してから最小送信間隔時間経過していない場合は、最小送信間隔時間が経過するまで待ってからLLDP情報を送信します。

保持回数

本装置のLLDP情報を受信した隣接装置が本装置のLLDP情報を保持すべき有効時間を、送信間隔時間の回数で2~10回の範囲で指定します。

本装置のLLDP情報の有効時間(TTL)は以下の式により計算されます。

$$\text{有効時間} = \text{送信間隔時間} \times \text{保持回数}$$

ただし、計算結果が65535秒を超えた場合は、有効時間を65535秒とします。

送信停止後遅延時間

「LAN 情報」 - 「基本情報」 - 「LLDP 情報」の「動作」で LLDP 情報を送信しないように設定変更したとき、送信処理を初期状態に戻すまでの遅延時間を 1 ~ 10 秒の範囲で指定します。

受信情報更新通知最小間隔時間

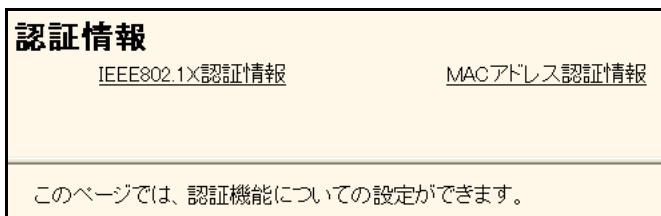
受信情報更新通知の最小間隔時間を 5 ~ 3600 秒の範囲で指定します。

受信情報（隣接情報）が更新されたときに SNMP トラップを送信して受信情報が更新されたことを通知します。その後、最小間隔時間が経過するまでの間に受信情報が何度も更新されても SNMP トラップを送信しないで、最小間隔時間経過後に SNMP トラップを 1 回だけ送信して受信情報が更新されたことを再通知します。

21 認証情報

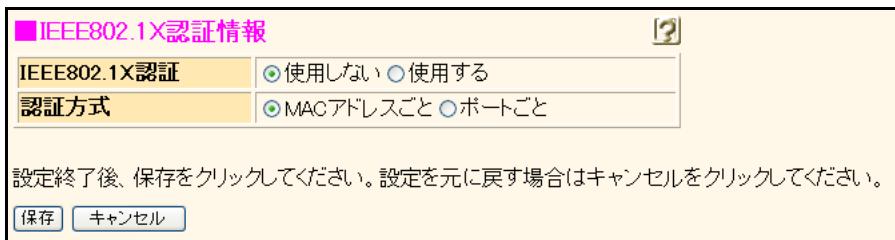
適用機種 全機種

[操作] ルータ設定「認証情報」



21.1 IEEE802.1X 認証情報

[操作] ルータ設定「認証情報」 → [IEEE802.1X 認証情報]



IEEE802.1X 認証

IEEE802.1X認証を装置として使用するかを選択します。

- 使用する
パケット送信元端末の IEEE802.1X 認証を行い、認められた端末である場合に中継を行い、認められていなければパケット破棄します。
- 使用しない
LAN インタフェースでは、IEEE802.1X 認証は行いません。

こんな事に気をつけて

“使用する”を選択した場合でも、「LAN 情報（物理 LAN / 無線 LAN）」の IEEE802.1X 認証情報で、認証機能を“使用しない”と設定されている場合は、認証は行われません。

認証方式

認証方式としてシステムデフォルト認証単位を指定します。

こんな事に気をつけて

- 認証方式としてポートごとの認証を選択し、そのポートに接続される端末 (Supplicant) の一台が認証許容された場合、同じポートに接続されるほかの端末からのアクセスがすべて透過として扱われます。
- 無線 LAN で利用する場合は、認証方式の設定は無効となり、常に MAC アドレスごとの認証を行います。

21.2 MACアドレス認証情報

[操作] ルータ設定「認証情報」→ [MACアドレス認証情報]

The screenshot shows a configuration page for MAC address authentication. It includes fields for password and confirmation, and a protocol selection section. A note at the bottom instructs users to click 'Save' after configuration.

■MACアドレス認証情報	
パスワード	<input type="text"/>
パスワードの確認	<input type="text"/>
認証プロトコル	<input checked="" type="radio"/> CHAP <input checked="" type="radio"/> PAP

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

パスワード

MACアドレス認証で使用するパスワードを、0x21、0x23～0x7eの文字で構成される128文字以内の文字列で指定します。省略時は、認証端末のMACアドレスをパスワードとして使用します。

パスワードの確認

上記で指定したパスワードをもう一度指定します。

認証プロトコル

MACアドレス認証の認証プロトコルを選択します。

22 AAA 情報

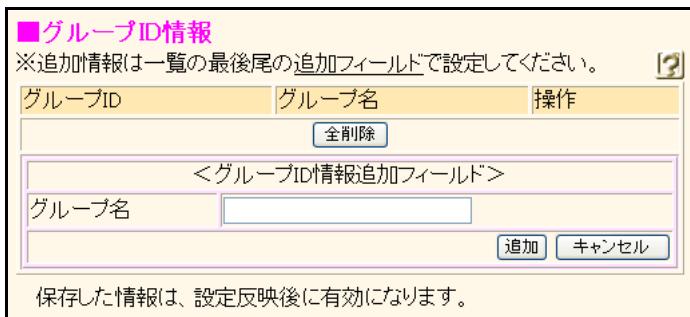
適用機種 全機種

[操作] ルータ設定「AAA情報」



22.1 グループID情報

[操作] ルータ設定「AAA情報」 → [グループID情報]



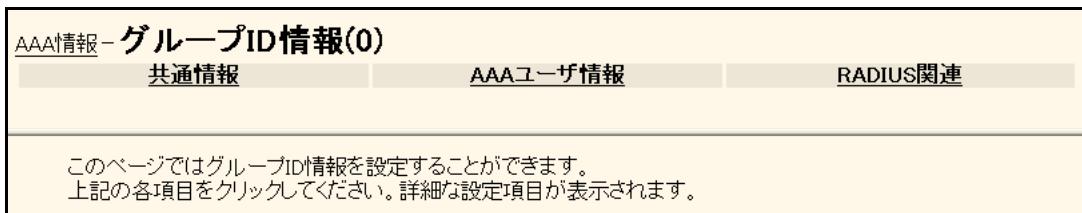
現在、設定されているグループID情報の定義が表示されています。グループID情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

本装置ではテンプレート定義により、通信アクセスを許可するユーザIDの認証情報と各種付加情報を通じて、依頼された接続情報の検索を行い、返答として要求された接続情報が通知されます。

グループ名

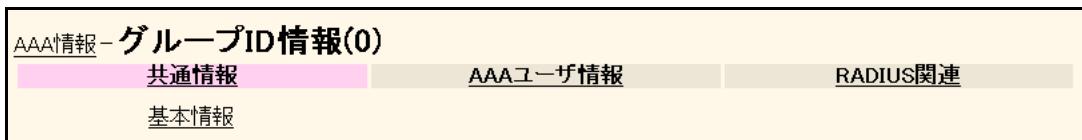
グループ名を0x21、0x23～0x7eの32文字以内のASCII文字列で指定します。

[操作] ルータ設定「AAA情報」 → [グループID情報] → [追加]



22.1.1 共通情報

[操作] ルータ設定「AAA情報」 → [グループID情報] → [追加] → [共通情報]



22.1.1.1 基本情報

[操作] ルータ設定「AAA 情報」 → [グループID 情報] → [追加] → [共通情報] → [基本情報]

■ 基本情報

グループ名

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

グループ名

グループ名を 0x21、0x23～0x7e を使用して 32 文字以内で指定します。

22.1.2 AAA ユーザ情報

[操作] ルータ設定「AAA 情報」 → [グループID 情報] → [追加] → [AAA ユーザ情報]

AAA情報 - グループID情報(0)

共通情報 AAAユーザ情報 RADIUS関連

AAAユーザ情報

[操作] ルータ設定「AAA 情報」 → [グループID 情報] → [追加] → [AAA ユーザ情報]
→ [AAA ユーザ情報]

表示条件入力

表示個数 50 表示範囲 AAAユーザ情報は存在しません

■ AAAユーザ情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	ユーザID	操作
		<input type="button" value="全削除"/>

<AAAユーザ情報追加フィールド>

ユーザID
<input type="text"/>

保存した情報は、設定反映後に有効になります。

現在、設定されている AAA ユーザ情報の定義が表示されています。AAA ユーザ情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ユーザ ID

ユーザ ID を 0x21、0x23～0x7e を使用して 64 文字以内で指定します。

MAC アドレス認証を利用する場合は、アクセスを許可する端末の MAC アドレスを 16 進数 12 衔（コロンで区切らない）で指定してください。

省略時は認証情報を使用できません。

[操作] ルータ設定「AAA 情報」→ [グループID情報] → [追加] → [AAA ユーザ情報] → [追加]

22.1.2.1 認証情報

[操作] ルータ設定「AAA 情報」→ [グループID情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [認証情報]

[操作] ルータ設定「AAA 情報」→ [グループID情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [認証情報] → [認証情報]

Si-R180B、260B では、"発信者番号による識別" の設定項目は表示されません。

ユーザID

ユーザIDを0x21、0x23～0x7eを使用して64文字以内の文字列で指定します。

MACアドレス認証を利用する場合は、アクセスを許可する端末のMACアドレスを16進数12桁（コロンで区切らない）で指定してください。

省略時は認証情報を使用できません。

認証パスワード

認証パスワードを0x21、0x23～0x7eを使用して64文字以内で指定します。

MACアドレス認証を利用する場合は、アクセスを許可する端末のMACアドレスを16進数12桁（コロンで区切らない）で指定してください。

省略時は、認証情報のパスワードは使用できません。表示画面では暗号化された認証パスワードが表示されます。

権限クラス

ログインユーザを設定する場合は、権限クラスを設定します。

「パスワード情報」 - 「ログインユーザ情報」の設定によって、以下を選択します。

- “権限クラスは AAA/RADIUS サーバで指定する”を選択した場合
“管理者クラス”または“一般ユーザクラス”を選択します。
- “権限クラスによって参照する AAA を分ける”を選択した場合
“指定しない”を選択します。

発信者番号による識別 (Si-R220C、220D、240B、370、 370B、570、570B)

CLID 相手判定で、発信者番号による識別を行う場合は、“番号チェックする”を設定します。

相手電話番号

相手の電話番号を 0～9 の数字と “*”、“#”、“-”、“(”、“)”、“\”を使用して、32 衔以内の ASCII 文字列で指定します。

相手サブアドレス

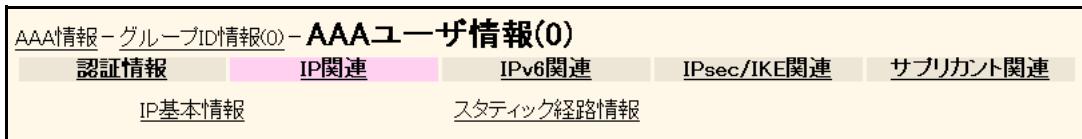
相手のサブアドレスを、0x21、0x23～0x7e を使用して、19 衔以内の ASCII 文字列で指定します。

こんな事に気をつけて

- PIAFS (64Kbps) 着信時には、相手サブアドレスは無視されますので、設定しないでください。
- 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

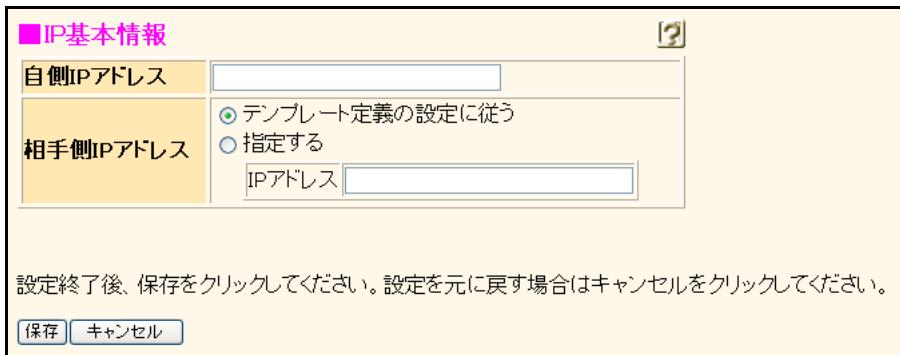
22.1.2.2 IP 関連

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IP 関連]



22.1.2.2.1 IP 基本情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IP 関連] → [IP 基本情報]



自側IPアドレス

自側IPアドレスを指定します。省略または0.0.0.0を指定した場合は、IPアドレスなし (unnumbered) として動作します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

相手側IPアドレス

相手側IPアドレスとしてテンプレート定義で指定した割当てIPアドレスの設定内容に従うか、個別に指定するかを選択します。“指定する”を選択し、0.0.0.0を指定した場合は、設定をIPアドレスなし (unnumbered) として動作します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

22.1.2.2.2 スタティック経路情報

[操作] ルータ設定「AAA情報」→[グループID情報]→[追加]→[AAAユーザ情報]→[追加]
→[IP関連]→[スタティック経路情報]

■スタティック経路情報

※追加・修正情報は一覧ので設定してください。

あて先IPアドレス/マスク	メトリック値	優先度	操作
全削除			
<スタティック経路情報入力フィールド>			
ネットワーク ネットワーク	<input type="radio"/> デフォルトルート		
	<input checked="" type="radio"/> ネットワーク指定	あて先IPアドレス	<input type="text"/>
		あて先アドレスマスク	<input type="text"/> 0.0.0.0
メトリック値	<input type="text"/> 1		
優先度	<input type="text"/> 1		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路情報の定義が表示されます。スタティック経路の定義数は、装置全体で256個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を選択した場合は、あて先IPアドレス／アドレスマスクを指定します。

メトリック値

このスタティック経路情報をRIPに再配布するときのメトリック値を、1～15から選択します。RIPに再配布したときは、設定したRIPメトリック値+1のメトリック値でRIPテーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10進数を使用して1～254の範囲で指定します。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
EBGP	20
OSPF	110
RIP	120
IBGP	200
DNS	15

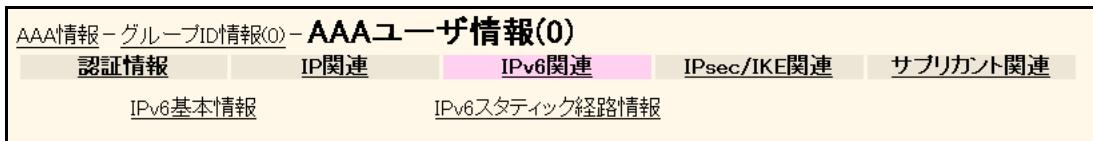
複数のスタティック経路情報でECMP機能を使用するときは、あて先、RIPメトリック値、優先度がそれぞれ同じになるようにスタティック経路情報を設定します。また、ECMP機能を使用する場合は、「ルーティングプロトコル情報」→「ルーティングマネージャ情報」にある「ECMP情報」でECMPを使用するように設定します。ECMPとなるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で4個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合、優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。

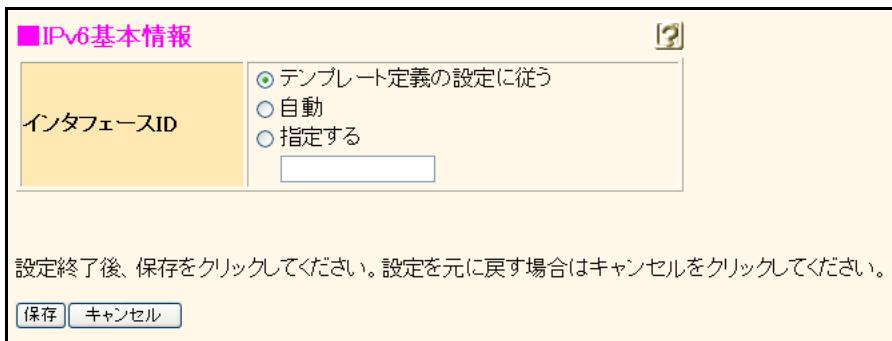
22.1.2.3 IPv6 関連

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IPv6 関連]



22.1.2.3.1 IPv6 基本情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IPv6 関連] → [IPv6 基本情報]



インタフェース ID

“自動”を選択する場合は、装置の MAC アドレスから自動生成されるインターフェース ID を使用します。

通常は、“自動”を選択します。

“指定する”を選択する場合は、16 ビットごとに区切り文字 (:) を入れて、16 進数を使用して 16 衔でインターフェース ID を指定します。このとき、他装置と同じインターフェース ID とならないような値を指定します。省略時は、テンプレート定義の設定に従います。

記述例)

2001:db8:7654:3210

22.1.2.3.2 IPv6 スタティック経路情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IPv6 関連] → [IPv6 スタティック経路情報]

■IPv6スタティック経路情報

※追加・修正情報は一覧の入力フィールドで設定してください。

あて先プレフィックス／プレフィックス長	メトリック値	優先度	操作
全削除			
<IPv6スタティック経路情報入力フィールド>			
<input checked="" type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定			
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 1 優先度 1			
追加 キャンセル			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているスタティック経路情報の定義が表示されます。IPv6 スタティック経路の定義数は、装置全体で 256 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に 1 つしか設定できません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を選択した場合は、あて先プレフィックス／プレフィックス長を指定します。あて先ネットワークにリンクローカルアドレスは指定できません。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1～15 から選択します。RIP に再配布したときは、設定した RIP メトリック値+1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10 進数を使用して 1～254 の範囲で指定します。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

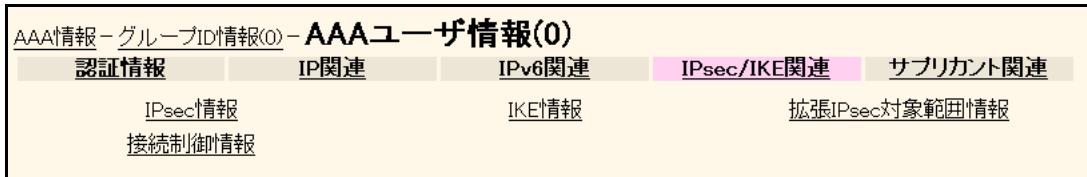
プロトコル	優先度
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合、優先度が同じスタティック経路情報は同時に設定できません。

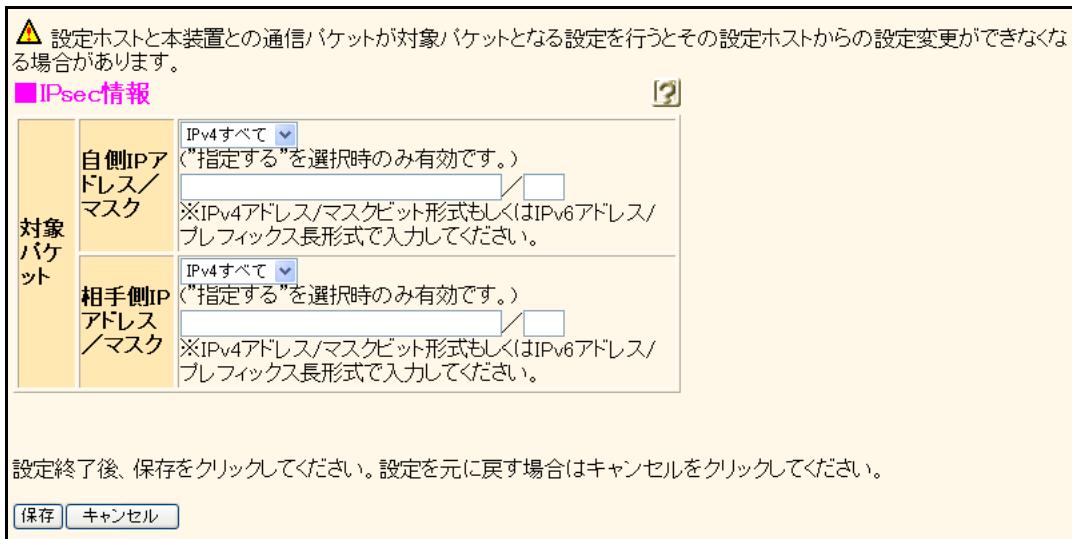
22.1.2.4 IPsec/IKE 関連

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IPsec/IKE 関連]



22.1.2.4.1 IPsec 情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IPsec/IKE 関連] → [IPsec 情報]



対象パケット

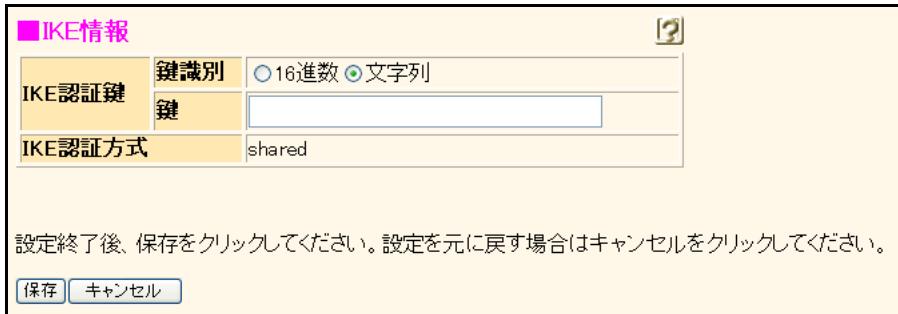
自側／相手側 IP アドレス／マスク

IPsec を適用するセッションの送信元 IP アドレスおよびアドレスマスクと、あて先 IP アドレスおよびアドレスマスクを以下の3つから選択します。アドレスを指定する場合は、“指定する”を指定します。

- IPv4 すべて
IPv4 アドレスをすべて選択します。
- IPv6 すべて
IPv6 アドレスをすべて選択します。
- 指定する
IP アドレス／マスクを IPv4/IPv6 形式で指定します。

22.1.2.4.2 IKE 情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加] → [IPsec/IKE 関連] → [IKE 情報]



■ IKE 情報	
IKE認証鍵	<input checked="" type="radio"/> 鍵識別 <input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列 鍵 <input type="text"/>
IKE認証方式	shared

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

IKE 認証鍵

IKE の認証に用いる鍵を設定します。本装置の IKE 認証には事前共有鍵方式を使用しているため、ここでは事前共有鍵（Pre-shared key）の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵識別

鍵の識別を選択します。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲（16 進数鍵）	入力範囲（文字列鍵）
1～256 行	1～128 文字

IKE 認証方式

IKE の鍵交換で、相手を認証するための認証方式を指定します。本装置では事前共有（秘密）鍵方式（shared）を使用します。

22.1.2.4.3 拡張 IPsec 対象範囲情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
 → [IPsec/IKE 関連] → [拡張 IPsec 対象範囲情報]

■拡張IPsec対象範囲情報

※追加・修正情報は一覧の入力フィールドで設定してください。

定義番号	拡張IPsec対象範囲自側IPアドレス/マスク	操作						
拡張IPsec対象範囲	相手側IPアドレス/マスク	<input type="button" value="全削除"/>						
<拡張IPsec対象範囲情報入力フィールド> <table border="1"> <tr> <td>自側IPアドレス/マスク</td> <td>IPv4すべて (*指定する"を選択時ののみ有効です。)</td> <td>※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。</td> </tr> <tr> <td>相手側IPアドレス/マスク</td> <td>IPv4すべて (*指定する"を選択時ののみ有効です。)</td> <td>※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。</td> </tr> </table>			自側IPアドレス/マスク	IPv4すべて (*指定する"を選択時ののみ有効です。)	※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	IPv4すべて (*指定する"を選択時ののみ有効です。)	※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。
自側IPアドレス/マスク	IPv4すべて (*指定する"を選択時ののみ有効です。)	※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	IPv4すべて (*指定する"を選択時ののみ有効です。)	※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。						
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>								

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている拡張 IPsec 対象範囲情報の定義が表示されています。拡張 IPsec 対象範囲の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

拡張 IPsec 対象範囲設定は、自側（相手側）IP アドレス／アドレスマスクを複数定義することができます。

拡張 IPsec 対象範囲設定は、IPsec 情報の対象パケットで定義した対象パケット以外を通過させる機能であるため、Security Policy Database (SPD) や IKE ネゴシエーション（自動鍵設定のみ）には使用されません。

SPD や IKE ネゴシエーションに使用する ID ペイロードの設定（自動鍵設定のみ）は、IPsec 情報の対象パケットで設定してください。

自側（相手側）IP アドレス／アドレスマスク

自側（相手側）アドレス／アドレスマスクを複数定義することができます。

拡張 IPsec 対象範囲の送信元 IP アドレスおよびアドレスマスクと、あて先 IP アドレスおよびアドレスマスクを指定します。IPv4 形式または IPv6 形式のアドレスを設定してください。

22.1.2.4.4 接続制御情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [IPsec/IKE 関連] → [接続制御情報]

■接続制御情報

接続先監視 あて先IPアドレス

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続先監視

あて先IPアドレス

接続先の生存確認を行うために ICMP ECHO パケットを送信する送信元 IP アドレスとして、本装置に設定している自側 IPv4/IPv6 アドレスを指定します。指定可能な範囲は以下のとおりです。タイムアウト時間までに応答がない場合に、IPsec 接続を切断します。省略時は、接続先監視を使用しないものとみなされます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff



◆ 接続先監視

接続先の生存確認を行うための動作情報を指定します。指定したあて先IPアドレスに対してICMP ECHOパケットを送信し、タイムアウト時間までに応答がない場合この接続先を使用不可状態にします。省略時は、接続先監視を使用しないものとみなされます。

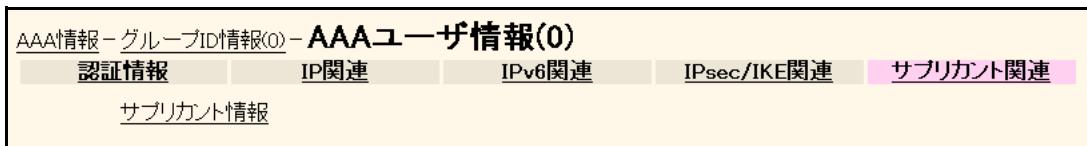
- 送信元IPアドレス : 「テンプレート情報」 - 「接続制御情報」で指定する送信元IPアドレス
- あて先IPアドレス : 「AAA情報」 - 「接続制御情報」で指定するあて先IPアドレス
- 無通信監視タイマ : 「テンプレート情報」 - 「共通情報」で指定する無通信監視タイマ
(省略または1~9秒が指定されている場合は10秒)
- 正常時送信間隔 : 「テンプレート情報」 - 「接続制御情報」で指定する正常時送信間隔
指定する無通信監視タイマの1/2(1~9秒が指定されている場合は5秒)
- タイムアウト時間 : 指定する無通信監視タイマの1/2(1~9秒が指定されている場合は5秒)
- リトライ間隔 : 2秒
- 監視モード : 無通信時に監視する

接続先監視と無通信監視タイマの動作は以下のとおりです。

	接続先監視あり		接続先監視なし
	正常時送信間隔あり	正常時送信間隔なし	
無通信監視タイマあり	正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で無通信監視タイマのみ動作する
無通信監視タイマなし	正常時送信間隔は設定値でその他は無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する	無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する	動作しない

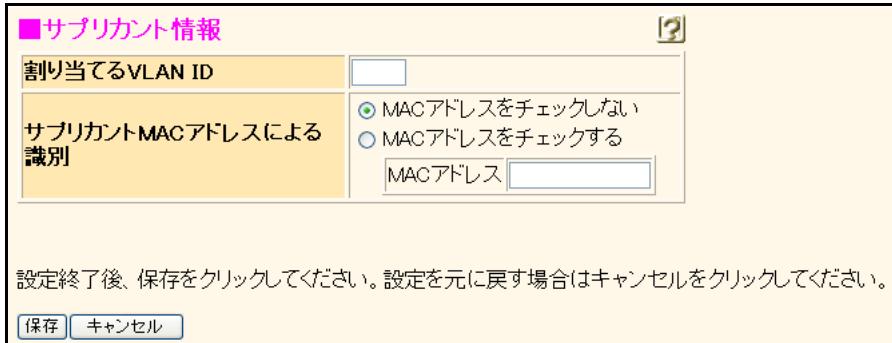
22.1.2.5 サプリカント関連

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [サプリカント関連]



22.1.2.5.1 サプリカント情報

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [AAA ユーザ情報] → [追加]
→ [サプリカント関連] → [サプリカント情報]



割り当てる VLAN ID

サプリカント（ユーザ端末）に割り当てるVLAN IDを指定します。省略時は、認証元の設定に従います。

この設定は、RADIUS サーバ機能で EAP 認証を行う場合にだけ有効です。

有効範囲)

1 ~ 4094

サプリカント MAC アドレスによる識別

サプリカント（ユーザ端末）の MAC アドレスをチェックするかどうかを選択します。

MAC アドレスをチェックする場合は、MAC アドレスにサプリカントの MAC アドレスを xx:xx:xx:xx:xx:xx (xx は 2 衝の 16 進数) の形式で指定します。MAC アドレスが一致しない場合は認証が成功しません。

複数のユーザ情報を用いて、同じユーザ名で異なる MAC アドレスを登録することで、複数の MAC アドレスを登録することができます。

MAC アドレスをチェックしない場合は、サプリカントの MAC アドレスを用いずパスワード情報だけを用いて認証を行います。この設定は、RADIUS サーバ機能で EAP 認証を行う場合にだけ有効です。

22.1.3 RADIUS 関連

[操作] ルータ設定「AAA 情報」→ [グループ ID 情報] → [追加] → [RADIUS 関連]

「基本情報」の RADIUS サービスで、" 使用しない " を選択した場合

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報		

「基本情報」の RADIUS サービスで、" クライアント機能 " を選択した場合

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報	サーバ情報	送信情報

「基本情報」の RADIUS サービスで、" サーバ機能 " を選択した場合

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報	クライアント情報	

22.1.3.1 基本情報

[操作] ルータ設定「AAA 情報」→ [グループ ID 情報] → [追加] → [RADIUS 関連] → [基本情報]

■ 基本情報	
RADIUSサービス	<input type="button" value="使用しない"/> <input type="checkbox"/> 認証 <input type="checkbox"/> 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	<input type="text"/>
自側アカウンティングIPアドレス	<input type="text"/>
Message-Authenticator	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

RADIUS サービス

本装置で使用する RADIUS 機能を以下から選択します。選択する RADIUS サービスによって、「RADIUS 情報」の表示が異なります。

- 使用しない
RADIUS 機能を使用しない
 - クライアント機能
本装置を RADIUS クライアントとして使用する
 - サーバ機能
本装置を RADIUS サーバとして使用する
- “クライアント機能”または“サーバ機能”を選択した場合は、以下から使用するサービスを指定します。
- 認証
RADIUS 認証機能を使用する
 - アカウンティング
RADIUS アカウンティング機能を使用する

こんな事に気をつけて

- 同一装置上で 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。
- RADIUS サーバ機能は、複数の AAA グループに対して定義することはできません。

自側認証 IP アドレス

自側 RADIUS 認証装置の IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

本装置を RADIUS 認証サーバとして使用する場合は、RADIUS 認証クライアントと通信するときに使用する IP アドレスを設定します。本装置を RADIUS 認証クライアントとして使用する場合は、RADIUS 認証サーバと通信するときに使用する IP アドレスを設定します。省略時は、相手側の RADIUS 認証装置と通信する自側 IP アドレスを自動的に選択するものとみなされます。

自側アカウンティング IP アドレス

自側 RADIUS アカウンティング装置の IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

本装置を RADIUS アカウンティングサーバとして使用する場合は、RADIUS アカウンティングクライアントと通信するときに使用する IP アドレスを設定します。本装置を RADIUS アカウンティングクライアントとして使用する場合は、RADIUS アカウンティングサーバと通信するときに使用する IP アドレスを設定します。省略時は、相手側の RADIUS アカウンティング装置と通信する自側 IP アドレスを自動的に選択するものとみなされます。

Message-Authenticator

Message-Authenticator による認証を行う場合は、“使用する”を選択します。本装置では、認証要求メッセージにのみ使用します。

22.1.3.2 サーバ情報（クライアント機能）

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [RADIUS 関連]
 → [サーバ情報（クライアント機能）]

■サーバ情報(クライアント機能)				
	サーバIPアドレス	復旧待機時間	優先度	操作
認証情報 1	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
認証情報 2	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
認証情報 3	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
認証情報 4	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
アカウンティング情報 1	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
アカウンティング情報 2	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
アカウンティング情報 3	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
アカウンティング情報 4	-	0秒	0	<input type="button" value="修正"/> <input type="button" value="削除"/>
<input type="button" value="全削除"/>				

保存した情報は、設定反映後に有効になります。

認証情報

認証情報 1	共有鍵	<input type="text"/>
	サーバIPアドレス	<input type="text"/>
	サーバ UDPポート	<input checked="" type="radio"/> 1812 <input type="radio"/> 1645
	復旧待機時間	0 <input type="button" value="秒"/>
	優先度	0
	自側認証IPアドレス	<input type="text"/>
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>		

共有鍵

本装置と RADIUS 認証サーバとの間で共有する共有鍵 (RADIUS シークレット) を 64 文字以内の文字列で指定します。

省略時は、共有鍵 (RADIUS シークレット) を設定しないものとみなされます。

サーバIPアドレス

本装置と通信する RADIUS 認証サーバの IP アドレスを設定します。

(有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

サーバ UDP ポート

RADIUS 認証クライアントが認証要求する RADIUS 認証サーバの UDP ポート番号を設定します。

- 1812
認証要求する RADIUS 認証サーバが最新の RFC 仕様の UDP ポートで実装されている場合
- 1645
認証要求する RADIUS 認証サーバが旧 RFC 仕様の UDP ポートで実装されている場合

復旧待機時間

RADIUS サーバが dead 状態になってから、自動的に再び alive 状態に復旧するまでの時間を指定します。単位は、日、時間、分、秒のどれかを指定します。

有効範囲)
0 ~ 86400 秒
0 ~ 1440 分
0 ~ 24 時間
0 ~ 1 日

0 秒を指定した場合は、自動的に alive 状態に復旧しません。省略時は、自動的に復旧しません。

RADIUS サーバから送信間隔と再送間隔で設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。

dead 状態から alive 状態に復旧するためには、以下の条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となったあと、dead 状態の RADIUS サーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

優先度

同一グループ内の RADIUS サーバを使用する優先度を指定します。0 を最優先、255 を最非優先とし、数字が小さい程、高い優先度となります。

有効範囲)
0 ~ 255

255 を指定した場合は、その RADIUS サーバは常に dead 状態となります。省略時は、0 が設定されます。

同一グループ内の複数の RADIUS サーバから、認証の際に使用する RADIUS サーバを決める際に使用する優先度を指定します。同一グループの中で、dead 状態になつていな、もっとも高い優先度の RADIUS サーバが使われます。もっとも高い優先度の RADIUS サーバが複数存在する場合は、使用する RADIUS サーバはランダムに決定されます。

自側認証 IP アドレス

自側 RADIUS 認証装置でこのクライアントに対して使用する IP アドレスを設定します。本定義の内容は、RADIUS 関連「基本情報」の自側認証 IP アドレスの設定より優先されます。

有効範囲)
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

このクライアントで RADIUS 認証サーバとの通信に使用する IP アドレスを設定してください。省略時は、RADIUS 関連「基本情報」の自側認証 IP アドレスの設定に従います。

アカウンティング情報

アカウンティング情報 1	共有鍵	<input type="text"/>
	サーバIPアドレス	<input type="text"/>
	サーバ UDPポート	<input checked="" type="radio"/> 1813 <input type="radio"/> 1646
	復旧待機時間	0 <input type="button" value="秒"/> <input type="button" value="分"/> <input type="button" value="時"/>
	優先度	<input type="text" value="0"/>
	自側アカウンティングIPアドレス	<input type="text"/>
	<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>	

共有鍵

本装置と RADIUS アカウンティングサーバとの間で共有する共有鍵 (RADIUS シークレット) を 64 文字以内の文字列で指定します。

省略時は、共有鍵 (RADIUS シークレット) を設定しないものとみなされます。

サーバIP アドレス

本装置と通信する RADIUS アカウンティングサーバの IP アドレスを設定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

サーバUDP ポート

RADIUS アカウンティングクライアントがアカウンティング要求する RADIUS アカウンティングサーバの UDP ポート番号を設定します。

- 1813
アカウンティング要求する RADIUS アカウンティングサーバが最新の RFC 仕様の UDP ポートで実装されている場合
- 1646
アカウンティング要求する RADIUS アカウンティングサーバが旧 RFC 仕様の UDP ポートで実装されている場合

復旧待機時間

RADIUS サーバが dead 状態になってから、自動的に再び alive 状態に復旧するまでの時間を指定します。単位は、日、時間、分、秒のどれかを指定します。

有効範囲)

0 ~ 86400 秒

0 ~ 1440 分

0 ~ 24 時間

0 ~ 1 日

0 秒を指定した場合は、自動的に alive 状態に復旧しません。省略時は、自動的に復旧しません。

RADIUS サーバから送信間隔と再送間隔で設定した応答待ち受け時間を経過しても応答が得られなかった場合、その RADIUS サーバは dead 状態となり、優先度は最非優先となります。dead 状態となった RADIUS サーバは、alive 状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive 状態へ自動的に復旧するための待ち時間を設定します。

dead 状態から alive 状態に復旧するためには、以下の条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となったあと、dead 状態の RADIUS サーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

優先度

同一グループ内の RADIUS サーバを使用する優先度を指定します。0 を最優先、255 を最非優先とし、数字が小さい程、高い優先度となります。

有効範囲)

0 ~ 255

255 を指定した場合はその RADIUS サーバは常に dead 状態となります。省略時は、0 が設定されます。

同一グループ内の複数の RADIUS サーバから、アカウントイングの際に使用する RADIUS サーバを決める際に使う優先度を指定します。同一グループの中で、dead 状態になっていない、もっとも高い優先度の RADIUS サーバが使われます。もっとも高い優先度の RADIUS サーバが複数存在する場合は、使用的 RADIUS サーバはランダムに決定されます。

自側アカウントイング IP アドレス

自側 RADIUS アカウントイング装置でこのクライアントに対して使用する IP アドレスを設定します。本定義の内容は、RADIUS 関連「基本情報」の自側アカウントイング IP アドレスの設定より優先されます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ ffff:ffff:ffff:ffff:ffff:ffff:ffff

このクライアントで RADIUS アカウントイングサーバとの通信に使用する IP アドレスを設定してください。省略時は、RADIUS 関連「基本情報」の自側アカウントイング IP アドレスの設定に従います。

22.1.3.3 送信情報（クライアント機能）

[操作] ルータ設定「AAA 情報」→ [グループID 情報] → [追加] → [RADIUS 関連]
 → [送信情報（クライアント機能）]

■送信情報(クライアント機能)	
送信間隔	<input type="text" value="1"/> 秒
再送回数	<input type="text" value="2"/> 回
NAS識別子	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

送信間隔

RADIUS サーバ未応答時のパケットの送信間隔を 10 進数を使用して、1～10 秒の範囲の秒単位で指定します。

再送回数

RADIUS サーバ未応答時のパケットの再送回数を 10 進数を使用して、1～10 回の範囲で指定します。

サーバからの応答待ち受け時間は、送信間隔 × (再送回数 + 1) 秒となります。省略時は送信間隔を 1 秒、再送回数を 2 回として動作します。この場合は、サーバからの応答待ち受け時間パケットの初回送信後、3 秒となります。

NAS 識別子

RADIUS 認証クライアントおよびアカウンティングクライアントが RADIUS サーバに送出する NAS-Identifier アトリビュートの値を 64 文字以内で指定します。省略時は、NAS-Identifier アトリビュートを送信しません。

22.1.3.4 クライアント情報（サーバ機能）

[操作] ルータ設定「AAA 情報」 → [グループID 情報] → [追加] → [RADIUS 関連]
 → [クライアント情報（サーバ機能）]

■クライアント情報(サーバ機能)

※追加・修正情報は一覧ので設定してください。

定義番号	クライアントIPアドレス	操作
[全削除]		
<クライアント情報(サーバ機能)入力フィールド>		
共有鍵	<input type="text"/>	
クライアントIPアドレス	<input checked="" type="radio"/> すべて <input checked="" type="radio"/> アドレス指定 <input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている RADIUS 情報（サーバ機能）の定義が表示されています。RADIUS 情報（サーバ機能）の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

共有鍵

本装置と RADIUS 認証クライアントとの間で共有する共有鍵（RADIUS シークレット）を 64 文字以内の文字列で指定します。省略時は、共有鍵（RADIUS シークレット）を設定しないものとみなされます。

クライアントIPアドレス

本装置と通信する RADIUS 認証クライアントの IP アドレスを以下から選択します。

- すべて
相手側となる RADIUS 認証クライアントを特定しません。
- アドレス指定
RADIUS 認証クライアントの IP アドレスを指定します。
有効範囲)
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

23 ACL 情報

適用機種 全機種

[操作] ルータ設定「ACL 情報」

表示条件入力			
表示個数 10	表示範囲 ACL定義は存在しません		
■ ACL情報			
※追加・選択削除は一覧の <u>追加</u> ・ <u>選択</u> フィールドで設定してください。 ?			
定義番号	定義名	定義種別	操作
全削除			
<ACL情報追加>フィールド 定義名 <input type="text" value="acl0"/> 追加 キャンセル			
保存した情報は、設定反映後に有効になります。			

現在、設定されている ACL 定義が表示されています。ACL の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

定義名

ACL 定義を識別する定義名を 50 文字以内で指定します。

[操作] ルータ設定「ACL 情報」 → [選択削除]

削除対象情報選択フィールド	
0 削除対象	<input type="checkbox"/> IP定義 <input type="checkbox"/> TCP定義 <input type="checkbox"/> UDP定義 <input type="checkbox"/> ICMP定義 <input type="checkbox"/> IPv6定義 <input type="checkbox"/> MAC定義
削除 キャンセル 一覧へ戻る	

削除対象

削除する定義を選択して、[削除] ボタンをクリックします。削除後、ACL 情報が再表示されます。

23.1 ACL 定義情報

[操作] ルータ設定「ACL 情報」→ [追加]

ACL情報 - ACL定義情報(acl0)

<input checked="" type="checkbox"/> 基本定義情報	<input type="checkbox"/> IP定義情報	<input type="checkbox"/> TCP定義情報
<input type="checkbox"/> UDP定義情報	<input type="checkbox"/> ICMP定義情報	<input type="checkbox"/> IPv6定義情報
<input type="checkbox"/> MAC定義情報		

▲ 先頭の[]は定義の有無を表します。定義が存在する場合[]が表示されます。

このページではACL情報を設定することができます。
上記の各項目をクリックしてください。詳細な設定項目が表示されます。

23.1.1 基本定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [基本定義情報]

■ 基本定義情報

定義名	<input type="text" value="acl0"/>	
------------	-----------------------------------	---

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

定義名

ACL 定義を識別する定義名を 50 文字以内で指定します。

23.1.2 IP 定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [IP 定義情報]

■IP定義情報	
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)
送信元情報	IPアドレス アドレスマスク 0 (0.0.0.0)
あて先情報	IPアドレス アドレスマスク 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

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル** **削除**

プロトコル

IP 定義としてプロトコルを以下の 6 つから選択します。() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmp (1)
- IPv6 over IPv4 (41)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255 の範囲で指定します。

送信元／あて先情報

IP 定義としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

IP 定義としての IP アドレスおよびアドレスマスクを指定します。以下が等しい場合に条件に一致します。

- チェック対象となるパケットの IP アドレスと定義するアドレスマスクの論理積
- 定義する IP アドレスとアドレスマスクの論理積

0.0.0.0/0 を指定した場合、または、省略した場合はすべての IP アドレス／アドレスマスクを対象とします。

QoS

対象とする QoS を判断する方法を以下の 3 つから選択します。

- 指定なし
すべての TOS 値、および、すべての DSCP 値を対象とする場合に選択します。
- TOS
TOS 値で対象を判断する場合に選択します。複数指定する場合は、" " で区切れます。範囲指定の場合は "-" で区切れます。10 組まで指定できます。
有効範囲)
0～ff の 16 進数
- DSCP
DSCP 値で対象を判断する場合に選択します。複数指定する場合は、" " で区切れます。範囲指定の場合は "-" で区切れます。10 組まで指定できます。
有効範囲)
0～63 の 10 進数

23.1.3 TCP 定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [TCP 定義情報]

■TCP定義情報	
送信元ポート番号	<input type="text"/>
あて先ポート番号	<input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル** **削除**

送信元／あて先ポート番号

TCP 定義としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が TCP 定義の対象となります。また、ポート番号を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切れます。送信元情報とあて先情報で合わせて 10 組まで指定できます。省略時は、“any” が設定されます。

TCP 接続要求

TCP プロトコルでのコネクション接続要求を ACL 定義の対象に含める場合は、“対象” を選択します。

23.1.4 UDP 定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [UDP 定義情報]

■UDP定義情報	
送信元ポート番号	<input type="text"/>
あて先ポート番号	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル** **削除**

送信元／あて先ポート番号

UDP 定義としてポート番号を 10 進数を使用して、1～65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が UDP 定義の対象となります。また、ポート番号を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切れます。送信元情報とあて先情報で合わせて 10 組まで指定できます。省略時は、“any” が設定されます。

23.1.5 ICMP 定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [ICMP 定義情報]

■ ICMP定義情報

ICMP	タイプ	<input type="text"/>
	コード	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

ICMP

タイプ

ICMP 定義として ICMP パケットのタイプ値を 10 進数を使用して 0～255 の範囲または “any” で指定します。ICMP タイプ値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。

コード

ICMP 定義として ICMP パケットのコード値を 10 進数を使用して 0～255 の範囲または “any” で指定します。ICMP コード値を複数指定する場合は “,” で区切れます。範囲指定の場合は “-” で区切れます。10 組まで指定できます。省略時は、“any” が設定されます。

23.1.6 IPv6 定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [IPv6 定義情報]

■ IPv6 定義情報	
プロトコル	すべて (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)
送信元IPv6アドレス/プレフィックス	<input type="text"/> ✓ <input type="checkbox"/>
あて先IPv6アドレス/プレフィックス	<input type="text"/> ✓ <input type="checkbox"/>
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 <input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル 削除

プロトコル

IPv6定義としてプロトコルを以下の5つから選択します。
() 内はプロトコル番号です。

- すべて
- tcp (6)
- udp (17)
- icmpv6 (58)
- その他

任意のプロトコル番号を指定する場合は、“その他”を選択し、10進数を使用して、1～255の範囲で指定します。

送信元／あて先IPv6 アドレス

IPv6定義としてのIPv6アドレスおよびプレフィックス長を指定します。::/0を指定した場合、または、省略した場合はすべてのIPv6アドレス／プレフィックス長を対象とします。

以下が等しい場合に条件に一致します。

- チェック対象となるパケットのIPv6アドレスと定義するプレフィックス長の論理積
- 定義するIPv6アドレスとプレフィックス長の論理積

QoS

対象とするQoSを判断する方法を以下の3つから選択します。

- 指定なし
すべてのTOS値、および、すべてのDSCP値を対象とする場合に選択します。
- Traffic Class
Traffic Class値で対象を判断する場合に選択します。
複数指定する場合は、","で区切れます。範囲指定の場合は"-"で区切れます。10組まで指定できます。
(有効範囲)
0～ffの16進数
- DSCP
DSCP値で対象を判断する場合に選択します。複数指定する場合は、","で区切れます。範囲指定の場合は"-"で区切れます。10組まで指定できます。
(有効範囲)
0～63の10進数

23.1.7 MAC 定義情報

[操作] ルータ設定「ACL 情報」→ [追加] → [MAC 定義情報]

■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

すべて
アドレス指定("指定する"を選択時のみ有効です)

フォーマット種別

すべて
 LLC形式
 SNAP形式
 Ethernet形式

LSAP
VLANタグ解析 しない する

type値
VLANタグ解析 しない する

type値
VLANタグ解析 しない する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル 削除

送信元／あて先 MAC アドレス

対象とする MAC アドレスを以下の項目から選択します。“指定する”を選択する場合は、アドレス指定に MAC アドレスを 16 進数で指定します。

- **すべて**
すべての MAC アドレスを対象とします。
- **プロードキャスト**
プロードキャスト MAC アドレスを対象とします。
- **マルチキャスト**
プロードキャスト MAC アドレスおよびマルチキャスト MAC アドレスを対象とします。
- **指定する**
アドレス指定に指定する MAC アドレスを対象とします。MAC アドレスは、「xx:xx:xx:xx:xx:xx」(xx は 2 行の 16 進数) の形式で指定します。

フォーマット種別

対象とするフォーマットを以下の項目から選択します。LSAP または type 値が未入力の場合は、すべての値が対象となります。

また、VLAN タグ付きパケットで VLAN タグの先を解析するかを選択します。“する”を指定した場合は、VLAN タグ付きパケットでも正しく解析されます。

- **すべて**
すべてのパケットを対象とします。
- **LLC 形式**
LLC 形式のパケットを対象とします。
LSAP を 16 進数を使用して、0～ffff の範囲で指定します。
- **SNAP 形式**
SNAP 形式のパケットを対象とします。
type 値を 16 進数を使用して、0～ffff の範囲で指定します。
- **Ethernet 形式**
Ethernet 形式のパケットを対象とします。
type 値を 16 進数を使用して、5dd～ffff の範囲で指定します。

24 ポリシーグループ情報

適用機種 全機種

[操作] ルータ設定「ポリシーグループ情報」

ポリシーグループ情報

ポリシーグループ情報

表示条件入力		
表示個数 10	表示範囲 ポリシーグループ定義は存在しません	
■ポリシーグループ情報 ※追加情報は一覧の最後尾の <u>追加</u> ボタンで追加してください。		
定義番号	定義内容	操作
<input type="button" value="追加"/> <input type="button" value="全削除"/>		
保存した情報は、設定反映後に有効になります。		

現在、設定されているポリシーグループの定義が表示されています。ポリシーグループの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

24.1 ポリシーグループ定義情報

[操作] ルータ設定「ポリシーグループ情報」 → [追加]

ポリシーグループ情報 - ポリシーグループ定義情報(0)

パターン定義情報	送出先定義情報	接続先監視定義情報
このページではポリシーグループ情報を設定することができます。 上記の各項目をクリックしてください。詳細な設定項目が表示されます。		

24.1.1 パターン定義情報

[操作] ルータ設定「ポリシーグループ情報」 → [追加] → [パターン定義情報]

■パターン定義情報 [ACL定義参照](#)

※追加・修正情報は一覧ので設定してください。

優先順位	動作	ACL定義番号	操作
<input type="button" value="全削除"/>			
<パターン定義情報入力フィールド>			
動作	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> バックアップとして使用する	ACL定義番号	<input type="button" value="参照"/>
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている ACL パターン定義が表示されています。処理は優先順位 1 から順に行われます。ACL パターンの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

動作

ポリシーグループの動作を以下の3つから選択します。

- 使用する
条件と一致した場合に、このポリシーグループを使用します。
- 使用しない
条件と一致した場合に、このポリシーグループを使用しません。
- バックアップとして使用する
条件と一致し以降のポリシーグループを使用することができない場合に、このポリシーグループを使用します。

ACL 定義番号

[参照] ボタンをクリックして、ACL 定義番号を指定します。別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

指定する定義番号欄の [選択] ボタンをクリックし、ACL 定義番号を設定します。自動的に画面が閉じます。

なお、参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「ポリシーグループ情報」→ [追加] → [パターン定義情報]
→ 「ACL 定義番号の [参照]」



「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」、「IPv6 定義情報」および「TCP 定義情報」で設定した ACL 定義が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

参照する ACL 定義が存在しない場合は、「参照可能な ACL 情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「パターン定義情報」の ACL 定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「パターン定義情報」に ACL 定義番号が設定され、画面が閉じます。[ACL 定義参照] ボタンをクリックした場合は、[選択] ボタンは表示されません。[閉じる] ボタンをクリックして、画面を閉じてください。

24.1.2 送出先定義情報

[操作] ルータ設定「ポリシーグループ情報」→ [追加] → [送出先定義情報]

■送出先定義情報	
送出先インターフェース	LAN0
転送先ルータ	IPv4ルータ IPv6ルータ

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

送出先インターフェース

パケットを送出するインターフェースを指定します。

転送先ルータ (IPv4 ルータ / IPv6 ルータ)

lanインターフェースにパケットを送出する際の転送先ルータのアドレスを設定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ feff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

送出先インターフェースがlanインターフェースの場合は必ず設定してください。転送ルータのアドレスには利用するlanインターフェースと同一のセグメントにする必要があります。異なるセグメントの場合、転送することはできません。

24.1.3 接続先監視定義情報

[操作] ルータ設定「ポリシーグループ情報」→ [追加] → [接続先監視定義情報]

■接続先監視定義情報		
接続先監視	送信元IPアドレス	<input type="text"/>
	あて先IPアドレス	<input type="text"/>
	正常時送信間隔	10 <input type="button" value="秒"/>
	再送間隔	1 <input type="button" value="秒"/>
	タイムアウト時間	5 <input type="button" value="秒"/>
	異常時送信間隔	1 <input type="button" value="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 <input type="button" value="秒"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

接続先監視

接続先の生存確認を行うための動作情報を選択します。指定したあて先IPアドレスにICMP ECHOパケットを送信します。タイムアウト時間までに応答がない場合に、この接続先を使用できない状態にします。その後、異常時送信間隔ごとにICMP ECHOパケットを送信し、接続先の復旧を待ち、復旧後にこの接続先を使用できる状態にします。

こんな事に気をつけて

パターン定義情報、送出先定義情報が設定されていない場合、接続先監視機能は動作しません。

送信元IPアドレス

ICMP ECHOパケットの送信元IPアドレスとして、本装置に設定している自側IPv4/IPv6アドレスのどれかを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

あて先IPアドレス

監視対象となる接続先のIPv4/IPv6アドレスを指定します。指定可能な範囲は以下のとおりです。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

::2～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

正常時送信間隔

ICMP ECHOパケットの応答が正常に受信されている状態で、ICMP ECHOパケットを次に送信する間隔を、10進数を使用して1～60秒の範囲で指定します。

再送間隔

ICMP ECHOパケットの正常時の送信に対して応答がない場合、ICMP ECHOパケットを再送する間隔を、10進数を使用して1～(タイムアウト時間-1)秒の範囲で指定します。省略時は、1秒が設定されます。

タイムアウト時間

ICMP ECHOパケットの送信から生存確認失敗とするまでの時間を、10進数を使用して5～180秒の範囲で指定します。タイムアウト時間までに応答がない場合、監視対象との接続に障害が発生したとみなし、この接続先を使用できない状態にします。

異常時送信間隔

ICMP ECHO パケットのタイムアウトが発生してから、接続先の障害が復旧し応答が受信されるまでの間、ICMP ECHO パケットを送信する間隔を、10進数を使用して 60 ~ 600 秒の範囲で指定します。

送信 TTL / HopLimit

ICMP ECHO パケットを送信するときの IP TTL 値を、1 ~ 255 の範囲で指定します。省略時は、255 が設定されます。

連続応答受信回数

異常状態から正常状態へ復旧するために必要な連続応答受信回数を、10進数を使用して 1 ~ 100 の範囲で指定します。省略時は、1 が設定されます。

異常時送信開始待ち時間

正常状態から異常状態に遷移した場合に、最初の ICMP ECHO パケットを送信するまでの待ち時間を指定します。0 秒を指定した場合は、待ち合わせをしません。省略時は、0 秒が設定されます。

有効範囲)

0 ~ 86400 秒

0 ~ 1440 分

0 ~ 24 時間

0 ~ 1 曜日

25 IP 情報

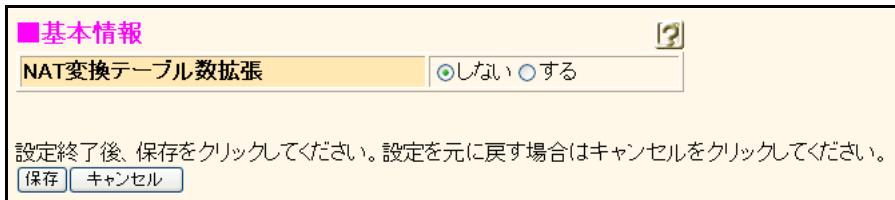
適用機種 全機種

[操作] ルータ設定「IP 情報」



25.1 基本情報

[操作] ルータ設定「IP 情報」 → [基本情報]



NAT 変換テーブル数拡張

NAT 変換テーブル数を拡張する場合は、“する”を選択します。

こんな事に気をつけて

“NAT 変換テーブル数拡張”を“する”で、OSPF、BGP のどちらかを使用する設定から、どちらも使用しない設定に変更する場合、設定を有効にするために本装置の再起動が必要です。

26 ルーティングプロトコル情報

適用機種 全機種

[操作] ルータ設定「ルーティングプロトコル情報」

ルーティングプロトコル情報

インターフェース情報	ルーティングマネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
------------	---------------	-------	-------	--------	-------------------	------------	-------------

このページではルーティングプロトコル情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

26.1 インタフェース情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [インターフェース情報]

■インターフェース情報

フローティング機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
-----------	---

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

フローティング機能

インターフェースのフローティング機能を使用する場合は、“使用する”を選択します。“使用しない”を選択した場合、インターフェースの状態変動に関係なく、インターフェース経路をルーティングテーブルに追加します。“使用する”を選択した場合、インターフェースが通信可能（リンクアップなど）状態であればインターフェース経路をルーティングテーブルに追加します。通信不可能（リンクダウンなど）状態であれば、ルーティングテーブルから削除します。また、ルーティングプロトコル優先度が0のスタティック経路情報についても、インターフェースの状態変動によってルーティングテーブルへの追加／削除を制御します。

本設定は、IPv4 機能、IPv6 機能で共通です。

26.2 ルーティングマネージャ情報

[操作] ルータ設定「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]

ルーティングプロトコル情報

インターフェース情報	ルーティングマネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
------------	---------------	-------	-------	--------	-------------------	------------	-------------

再配布情報 優先度情報 ECMP情報

26.2.1 再配布情報

[操作] ルータ設定「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]

■再配布情報		
RIP	インターフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
BGP	インターフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
OSPF	インターフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 20 メトリックタイプ: type2
LDP	インターフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

RIP

RIP に再配布する経路情報を設定します。

インターフェース経路情報

インターフェース経路情報を RIP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を RIP に再配布する場合は、“再配布する”を選択します。

BGP 経路情報

BGP 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

OSPF 経路情報

OSPF 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

DNS 経路情報

DNS 経路情報を RIP に再配布する場合は、“再配布する”を選択します。

メトリック値

RIP に再配布する際のメトリック値を選択します。

BGP

BGP に再配布する経路情報を設定します。

インターフェース経路情報

インターフェース経路情報を BGP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を BGP に再配布する場合は、“再配布する”を選択します。

こんな事に気をつけて

デフォルトルートを BGP で広報する場合は、BGP 相手情報でデフォルトルートを“広報する”に設定してください。

RIP 経路情報

RIP 経路情報を BGP に再配布する場合は、“再配布する”を選択します。

OSPF 経路情報

OSPF 経路情報を BGP に再配布する場合は、“再配布する”を選択します。

DNS 経路情報

DNS 経路情報を BGP に再配布する場合は、“再配布する”を選択します。

OSPF 広報

OSPF に再配布する経路情報を設定します。

インターフェース経路情報

インターフェース経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

スタティック経路情報

スタティック経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

RIP 経路情報

RIP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

BGP 経路情報

BGP 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

DNS 経路情報

DNS 経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

メトリック値

OSPF に再配布する際のメトリック値を選択します。

LDP

LDP に再配布する経路情報を設定します。

インターフェース経路情報

インターフェース経路情報を LDP に再配布する場合は、“再配布する”を選択します。

スタティック経路情報

スタティック経路情報を LDP に再配布する場合は、“再配布する”を選択します。

RIP 経路情報

RIP 経路情報を LDP に再配布する場合は、“再配布する”を選択します。

BGP 経路情報

BGP 経路情報を LDP に再配布する場合は、“再配布する”を選択します。

OSPF 経路情報

OSPF 経路情報を LDP に再配布する場合は、“再配布する”を選択します。

26.2.2 優先度情報

[操作] ルータ設定「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」→「優先度情報」

■ 優先度情報		
優先度	RIP	<input type="text" value="120"/>
	EBGP	<input type="text" value="20"/>
	IBGP	<input type="text" value="200"/>
	OSPF	<input type="text" value="110"/>
	DNS	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティック経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。優先度を10進数を使用して、1～254の範囲で指定し、より小さい値が、より高い優先度を示します。

RIP

RIP経路情報の優先度を指定します。省略時は、120が設定されます。

EBGP

EBGP経路情報の優先度を指定します。省略時は、20が設定されます。

IBGP

IBGP経路情報の優先度を指定します。省略時は、200が設定されます。

OSPF

OSPF経路情報の優先度を指定します。省略時は、110が設定されます。

DNS

DNS経路情報の優先度を指定します。省略時は、15が設定されます。

こんな事に気をつけて

- ・ 優先度は、ほかのプロトコルやスタティック経路情報に設定されている値と同じ値は指定しないでください。
- ・ スタティック経路情報の優先度の初期値は0です。

26.2.3 ECMP 情報

[操作] ルータ設定「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」→「ECMP情報」

ECMP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> ラウンドロビン方式 <input type="radio"/> ハッシュ方式
OSPF使用ECMP数	1

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

ECMP 機能

IPv4 ルーティング機能で、ECMP (Equal-Cost Multipath) を使用しない場合は、“使用しない”を選択します。また、ECMP を使用する場合は、ECMP の送出パス選択方式を、以下の2つから選択します。

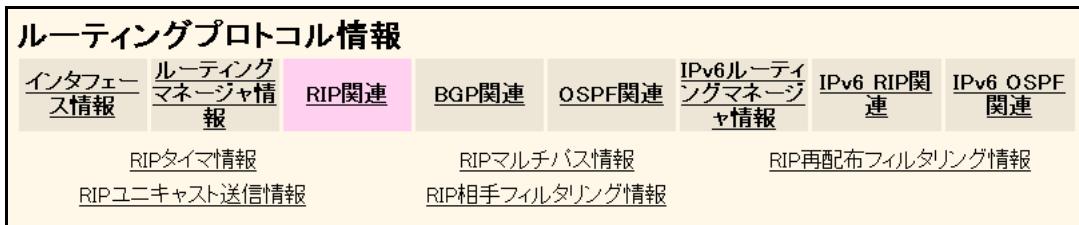
- ラウンドロビン方式
ラウンドロビン方式とは、パケットごとに送出パスを順次切り替える方式です。すべてのトラフィックがほぼ均等に分散される利点がある一方、通信の連續性（それぞれの通信セッションが同じパスを利用する）とパケットの到達順は送信時から保証されないという欠点があります。
- ハッシュ方式
ハッシュ方式とは、送信元IPアドレス、あて先IPアドレスを元にハッシュ値を計算し、その値に従って送出パスを決定する方式です。通信の連續性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

OSPF 使用 ECMP 数

OSPF が生成した経路情報で、ECMP で扱う経路の最大値を1～4の範囲で指定します。ECMP 機能を使用しない場合は、設定は無効となります。

26.3 RIP 関連

[操作] ルータ設定「ルーティングプロトコル情報」→ [RIP 関連]



26.3.1 RIP タイマ情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [RIP 関連] → [RIP タイマ情報]

定期広報タイマ	間隔	30 秒
	ゆらぎ幅	50 %
有効期限タイマ		3 分
ガーベージタイマ		2 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

定期広報タイマ

間隔

RESPONSE パケットで定期的に経路を広報する間隔を指定します。初期値は 30 秒です。指定できる範囲は以下のとおりです。

有効範囲)

10 ~ 3600 秒

1 ~ 60 分

1 時間

ゆらぎ幅

定期広報タイマのゆらぎ幅を指定します。初期値は 50 % です。指定できる範囲は以下のとおりです。

有効範囲)

0 ~ 50 %

有効期限タイマ

RESPONSE パケットで更新されない経路情報の有効期限を指定します。初期値は 180 秒です。指定できる範囲は以下のとおりです。

有効範囲)

10 ~ 3600 秒

1 ~ 60 分

1 時間

ガーベージタイマ

有効期限が切れた場合に、その経路情報をメトリック 16 で広報する時間を指定します。初期値は 120 秒です。指定できる範囲は以下のとおりです。

有効範囲)

10 ~ 3600 秒

1 ~ 60 分

1 時間

26.3.2 RIP マルチパス情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [RIP 関連] → [RIP マルチパス情報]

■RIPマルチパス情報

マルチパス数

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

マルチパス数

RIPで受信可能な同じあて先への経路情報数を指定します。指定できる範囲は1～2です。

26.3.3 RIP 再配布フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [RIP 関連] → [RIP 再配布フィルタリング情報]

■RIP再配布フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	フィルタリング条件	操作								
	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報対指定	<input type="button" value="全削除"/>								
<RIP再配布フィルタリング情報入力フィールド> <table border="1"> <tr> <td>動作</td> <td><input checked="" type="radio"/> 透過 <input type="radio"/> 遮断</td> </tr> <tr> <td>フィルタリング条件</td> <td> <input checked="" type="radio"/> 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 </td> </tr> <tr> <td>IPアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text"/> 0.0.0.0</td> </tr> </table>				動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	フィルタリング条件	<input checked="" type="radio"/> 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	<input type="text"/>	アドレスマスク	<input type="text"/> 0.0.0.0
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断										
フィルタリング条件	<input checked="" type="radio"/> 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致										
IPアドレス	<input type="text"/>										
アドレスマスク	<input type="text"/> 0.0.0.0										

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP 再配布フィルタリング情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

RIP に再配布する経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。
なお、IP アドレスに 0.0.0.0、アドレスマスクに 0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

検索条件を選択します。

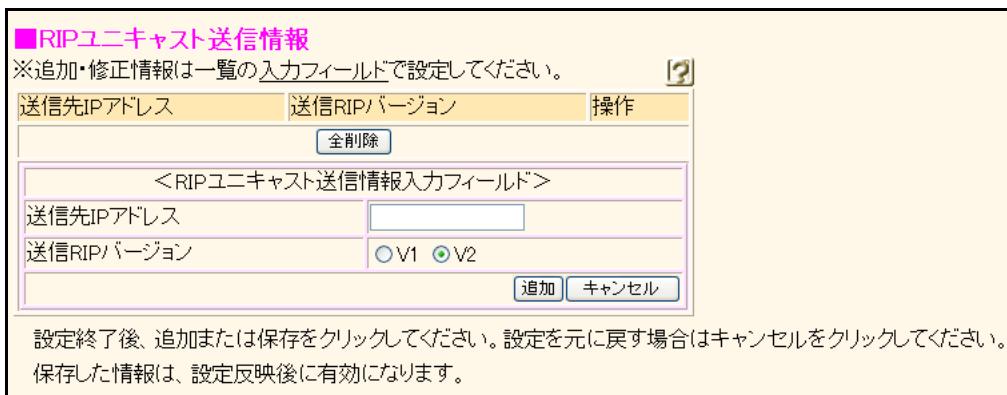
- 完全に一致
指定した IP アドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定した IP アドレスと、再配布経路情報のそれぞれを指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

26.3.4 RIP ユニキャスト送信情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [RIP 関連] → [RIP ユニキャスト送信情報]



■RIP ユニキャスト送信情報

※追加・修正情報は一覧ので設定してください。

送信先IPアドレス	送信RIPバージョン	操作
<input type="button" value="全削除"/>		
<RIP ユニキャスト送信情報入力フィールド>		
送信先IPアドレス	<input type="text"/>	
送信RIPバージョン	<input type="radio"/> V1	<input checked="" type="radio"/> V2
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP ユニキャスト送信情報の定義が表示されています。RIP ユニキャスト送信情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

送信先IP アドレス

RIP をユニキャストで送信する送信先の IP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

送信 RIP バージョン

ユニキャストで送信する RIP のバージョンを選択します。

26.3.5 RIP 相手フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [RIP 関連] → [RIP 相手フィルタリング情報]

■RIP相手フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	フィルタリング条件	操作
全削除			
<RIP相手フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 <input checked="" type="radio"/> すべて <input type="radio"/> 相手側IPアドレス指定 <input type="text"/> IPアドレス	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP 相手フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP 相手フィルタリング情報の定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した相手情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

受信した RIP 情報の動作を以下の 2 つから選択します。

- 透過
フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを透過します。
- 遮断
フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを遮断します。

フィルタリング条件

対象とする相手情報を選択します。

- すべて
すべての相手ルータからの RIP パケットをフィルタリング対象とします。
- 相手側 IP アドレス指定
指定した RIP 送信元 IP アドレスをフィルタリング対象とします。

(有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254

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相手ルータからの RIP パケットは遮断されます。

26.4 BGP 関連

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連]

ルーティングプロトコル情報							
インターフェース情報	ルーティングマネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
			BGP情報	IPv4 BGPネットワーク情報	IPv6 BGPネットワーク情報		
				IPv4 BGP集約経路情報	IPv6 BGP集約経路情報	BGP相手情報	
				IPv4 BGP再配布フィルタリング情報	IPv6 BGP再配布フィルタリング情報		IPv4 VRFI情報
				IPv4 MPLS連携情報			

26.4.1 BGP 情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 情報]

■BGP情報	
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
自AS番号	<input type="text"/>
自ID番号	0.0.0
IPv4 BGPネットワーク	<input type="checkbox"/> 常に広報する
IPv6 BGPネットワーク	<input type="checkbox"/> 常に広報する
IPv4 最大エントリ数	<input checked="" type="radio"/> 拡張しない <input type="radio"/> 拡張する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

Si-R570、570B以外では、“IPv4最大エントリ数”の設定項目は表示されません。

BGP 機能

BGPを使用する場合は、“使用する”を選択します。

こんな事に気をつけて

- 経路情報を、ルーティングテーブルの最大数またはBGPエントリの最大数まで保持している場合、BGPで受信した経路情報は破棄されます。
破棄された経路情報は、その後、ルーティングテーブルまたはBGPエントリに空きができる場合でも、ルーティングテーブルに反映されません。
ルーティングテーブルには、「BGPセッションの操作」を行うことで反映できます。
- NAT機能とは併用できません。

自 ID 番号

BGP接続で、自装置を一意に示すIDを設定します。IDは、ほかルータと重複しない値を指定します。
省略時は、以下の基準に従いBGP IDが自動選択されます。

- IPv4ループバック情報にIPv4アドレスが設定されている場合は、そのIPv4アドレスを使用します。
- IPv4ループバック情報にIPv4アドレスが設定されていない場合は、LAN情報／相手情報に設定されているIPv4アドレスの中からインターフェースのUp/Downの状態に関係なく最大のものを選択します。なお、相手情報の相手側IPアドレスおよびLAN情報のセカンダリIPアドレスは、選択対象となりません。

自 AS 番号

本装置の属するAS番号を10進数を使用して、0.1～65535.65535の範囲で指定します。省略はできません。

こんな事に気をつけて

IPv4アドレスが1つも設定されていないIPv6環境の場合は、自ID番号を必ず設定してください。

IPv4 BGP ネットワーク

IPv4 BGP ネットワークを、常に広報する場合に指定します。指定しない場合は、IPv4 BGP ネットワーク情報で設定したネットワークが経路情報として有効な場合だけ BGP で広報します。指定した場合は、経路情報に関係なく IPv4 BGP ネットワーク情報で設定した経路情報を BGP で広報します。

IPv6 BGP ネットワーク

IPv6 BGP ネットワークを、常に広報する場合に指定します。指定しない場合は、IPv6 BGP ネットワーク情報で設定したネットワークが経路情報として有効な場合だけ BGP で広報します。指定した場合は、経路情報に関係なく IPv6 BGP ネットワーク情報で設定した経路情報を BGP で広報します。

IPv4 最大エントリ数 (Si-R570、570B)

BGP IPv4 フルルート用に IPv4 最大エントリを拡張する場合は、“**拡張する**”を選択します。

拡張しないを選択した場合、エントリの最大は 6000 エントリです。拡張するを選択した場合、エントリの最大は 150000 エントリとなります。

IPv4 最大エントリの拡張は、拡張用 512M メモリモジュールが搭載されているときにだけ使用できます。IPv4 最大エントリの拡張で設定できる BGP セッションは、「BGP 相手情報」の定義番号 0 に設定された EBGP (マルチホップを除く) の 1 セッションだけです。

IPv4 最大エントリ数の拡張は、以下の機能と併用して使用することはできません。

- BGPへの再配布および BGP 経路情報の RIP/OSPF/LDPへの再配布機能
- IPv4 BGP/MPLS VPN 機能
- IPv4 BGP MPLS 解決機能
- IPv6 OSPF 機能
- BGP IPv6 機能

こんな事に気をつけて

最大エントリ数の拡張は、以下のどれかの場合に無効となります。

- 拡張用 512M メモリモジュールが搭載されていない。
- 「BGP 相手情報」に定義番号 0 以外が設定されている。
- 「BGP 相手情報」の定義番号 0 以下のどちらかが設定されている。
 - EBGP マルチホップ、BGP エンフォースマルチホップまたは IBGP として動作するように設定
 - アドレスファミリ情報を“VPN IPv4 ユニキャスト”として設定
- BGP で MPLS 解決が有効になっている。
- 再配布機能で以下のどれかが有効になっている。
 - BGPへのインターフェース経路情報の再配布
 - BGPへのスタティック経路情報の再配布
 - BGPへの RIP 経路情報の再配布
 - BGPへの OSPF 経路情報の再配布
 - BGPへの DNS 経路情報の再配布
 - RIPへの BGP 経路情報の再配布
 - OSPFへの BGP 経路情報の再配布
 - LDPへの BGP 経路情報の再配布

26.4.2 IPv4 BGP ネットワーク情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv4 BGP ネットワーク情報]

■ IPv4 BGPネットワーク情報

※追加・修正情報は一覧ので設定してください。

あて先IPアドレス/マスク	操作
<input type="button" value="全削除"/>	
<IPv4 BGPネットワーク情報入力フィールド>	
あて先IPアドレス	<input type="text"/>
あて先アドレスマスク	0 0.0.0.0 <input type="button" value="▼"/>
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv4 BGP ネットワーク情報の定義が表示されています。BGP ネットワーク情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP ネットワーク情報を設定することによって、必要な経路情報だけを選択して広報することができます。無効となった経路情報は広報されません。経路情報の状態変更を認識するには最大 15 秒かかります。なお、BGP ネットワーク情報は、広報する経路情報を BGP に再配布する必要はありません。

「[BGP 情報](#)」で IPv4 BGP ネットワークを常に広報すると指定することにより、設定した BGP ネットワーク情報を経路情報の状態に関係なく広報することができます。

あて先IPアドレス／アドレスマスク

広報する経路情報のあて先 IP アドレスとアドレスマスクを指定します。

こんな事に気をつけて

BGP/MPLS VPN では、IPv4 BGP ネットワーク情報は広報されません。

26.4.3 IPv6 BGP ネットワーク情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv6 BGP ネットワーク情報]

■IPv6 BGPネットワーク情報

※追加・修正情報は一覧ので設定してください。

あて先ネットワークアドレス/プレフィックス長	操作
<input type="button" value="全削除"/>	<input type="button" value=""/>
<IPv6 BGPネットワーク情報入力フィールド>	
あて先ネットワークアドレス /プレフィックス長	<input type="text"/> <input checked="" type="checkbox"/> <input type="checkbox"/>
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 BGP ネットワーク情報の定義が表示されています。BGP ネットワーク情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP ネットワーク情報を設定することによって、必要な経路情報だけを選択して広報することができます。無効となつた経路情報は広報されません。経路情報の状態変更を認識するには最大 15 秒かかります。なお、BGP ネットワーク情報は、広報する経路情報を BGP に再配布する必要はありません。

「[BGP 情報](#)」で IPv6 BGP ネットワークを常に広報すると指定することにより、設定した BGP ネットワーク情報を経路情報の状態に関係なく広報することができます。

あて先ネットワークアドレス／プレフィックス長

広報する経路情報のあて先ネットワークアドレスとプレフィックス長を指定します。

26.4.4 IPv4 BGP 集約経路情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv4 BGP 集約経路情報]

■ IPv4 BGP集約経路情報

※追加・修正情報は一覧ので設定してください。

集約IPアドレス/マスク	集約対象経路	操作
<input type="button" value="全削除"/>		
<IPv4 BGP集約経路情報入力フィールド>		
集約IPアドレス	<input type="text"/>	
集約アドレスマスク	0 (0.0.0.0) <input type="button" value="▼"/>	
集約対象経路	<input checked="" type="radio"/> 広報する <input type="radio"/> 広報しない	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているIPv4 BGP集約経路情報の定義が表示されています。BGP集約経路情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP集約情報を設定することによって、集約経路に含まれる経路情報（集約対象経路）があった場合に、集約経路情報を生成して広報することができます。集約対象経路がすべて無効となった場合、集約経路情報は広報されません。

集約IPアドレス／集約アドレスマスク

集約経路情報の集約IPアドレスと集約アドレスマスクを指定します。

集約対象経路

集約対象となるのは、BGPに再配布された経路情報またはBGPネットワーク情報で有効となっている経路情報です。

- 広報する
集約経路情報のほかに集約経路情報で集約される個々の経路の両方を広報します。
- 広報しない
集約経路情報を広報し、集約される個々の経路情報は広報しません。

こんな事に気をつけて

BGP/MPLS VPNでは、「BGP集約経路情報」の設定は無効となります。

26.4.5 IPv6 BGP 集約経路情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv6 BGP 集約経路情報]

■ IPv6 BGP集約経路情報

※追加・修正情報は一覧ので設定してください。

集約IPアドレス/プレフィックス長	集約対象経路	操作
<input type="text"/>	<input checked="" type="checkbox"/>	<input type="button" value="全削除"/>
<IPv6 BGP集約経路情報入力フィールド>		
集約IPアドレス/プレフィックス長	<input checked="" type="checkbox"/>	<input type="checkbox"/>
集約対象経路	<input checked="" type="radio"/> 広報する	<input type="radio"/> 広報しない
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているIPv6 BGP集約経路情報の定義が表示されています。BGP集約経路情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP集約情報を設定することによって、集約経路に含まれる経路情報（集約対象経路）があった場合に、集約経路情報を生成して広報することができます。集約対象経路がすべて無効となった場合、集約経路情報は広報されません。

集約IPアドレス／プレフィックス長

集約経路情報の集約IPアドレスとプレフィックス長を指定します。

集約対象経路

集約対象となるのは、BGPに再配布された経路情報またはBGPネットワーク情報で有効となっている経路情報です。

- 広報する
集約経路情報のほかに集約経路情報で集約される個々の経路の両方を広報します。
- 広報しない
集約経路情報を広報し、集約される個々の経路情報は広報しません。

26.4.6 BGP 相手情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 相手情報]

定義番号	IPアドレス	AS番号	Holdタイム	操作
				<input type="button" value="追加"/> <input type="button" value="全削除"/>

保存した情報は、設定反映後に有効になります。

現在、設定されている BGP の相手情報の定義が表示されています。BGP の相手情報の定義数（BGP 最大接続数）は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

こんな事に気をつけて

BGP/MPLS VPN を使用する場合、相手情報は 1 つだけ設定できます。

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 相手情報] → [追加]

ルーティングプロトコル情報 - BGP 相手情報 (0)

BGP相手基本情報 IPv4 BGPフィルタリング情報 IPv6 BGPフィルタリング情報

BGP拡張機能情報

26.4.6.1 BGP 相手基本情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 相手情報] → [追加]
→ [BGP 相手基本情報]

相手側IPアドレス	<input type="text"/>	
相手AS番号	<input type="text"/>	
自側IPアドレス	<input type="text"/>	
KeepAliveタイム	30	秒 <input type="button" value="▼"/>
Holdタイム	90	秒 <input type="button" value="▼"/>
EBGP MULTIHOP	<input type="text" value="1"/>	
アドレスファミリ	IPv4ユニキャスト <input type="button" value="▼"/>	
MEDメトリック 値	IPv4 <input type="text" value="0"/>	IPv6 <input type="text" value="0"/>
ASパスプリペン ド	IPv4 <input type="text" value="0"/>	IPv6 <input type="text" value="0"/>
LOCALPREF	IPv4 <input type="text" value="100"/>	IPv6 <input type="text" value="100"/>
NEXTHOP SELF	IPv4 <input checked="" type="radio"/> 無効 <input type="radio"/> 有効	IPv6 <input checked="" type="radio"/> 無効 <input type="radio"/> 有効
デフォルトルー ト	IPv4 <input checked="" type="radio"/> 広報しない <input type="radio"/> 広報する	IPv6 <input checked="" type="radio"/> 広報しない <input type="radio"/> 広報する
認証鍵	IPv4 <input type="text"/>	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

相手側 IP アドレス

BGP 接続を行う相手装置の IP アドレスを指定します。

IPv4 アドレスは以下の範囲で指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

IPv6 アドレスは、標準的な IPv6 アドレス表記方式で指定します。

リンクローカルアドレスは指定できません。

相手 AS 番号

BGP 接続する相手装置の AS 番号を 10 進数を使用して、0.1 ~ 65535.65535 の範囲で指定します。BGP/MPLS VPN を使用する場合は、本装置と同じ AS 番号を設定します。

こんな事に気をつけて

BGP/MPLS VPN を使用する場合、相手情報は 1 つだけ設定することができます。

自側 IP アドレス

BGP セッションに特定のインターフェースアドレスを設定する場合に指定します。設定しない場合、BGP セッションで使用するインターフェースの IP アドレスが自動的に使用されます。BGP/MPLS VPN を使用する場合は、「装置情報」 - 「ループバック情報」に設定した IP アドレスを設定します。

IPv4 アドレスは以下の範囲で指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

IPv6 アドレスは、標準的な IPv6 アドレス表記方式で指定します。

リンクローカルアドレスは指定できません。

KeepAlive タイマ

相手装置との通信状態を確認するために送信する KeepAlive メッセージの送信間隔を指定します。Hold タイマ設定値の 1/3 以上を設定した場合、Hold タイマ設定値の 1/3 が設定されます。また、ネゴシエーションにより相手装置の Hold タイマ値が採用され、その 1/3 よりも大きな値を KeepAlive タイマで設定していた場合は、相手装置の Hold タイマ値の 1/3 を KeepAlive タイマ値として使用します。省略時は、30 秒に設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

Keep Alive タイマの値は、Hold タイマより小さい値を指定してください。

Hold タイマ

相手装置との間で、通信異常と判断する無通信状態の時間（タイマ）を指定します。このタイマ値は、相手装置とのネゴシエーションで決まり、装置間でより小さな値が使用されます。省略時は、90 秒に設定されます。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

3 ~ 65535 秒

こんな事に気をつけて

相手装置とのネゴシエーションによって、相手装置の Hold タイマ値が使用された場合は、その値の 3 分の 1 の値が KeepAlive タイマとして使用されます。

EBGP MULTIHOP

相手装置と EBGP マルチホップ接続する場合の IP パケットのホップ数 (IPv4 パケットの TTL 値、IPv6 パケットの hoplimit 値) を 10 進数を使用して、1 ~ 255 の範囲で指定します。省略時は、1 に設定されます。

BGP 相手装置とルータを経由して接続する場合は、経由するルータの数を加算します。

アドレスファミリ

BGPで送受信する経路情報のアドレスファミリを指定します。

こんな事に気をつけて

BGP/MPLS VPNを使用する場合は、VPN IPv4 ユニキャストを設定します。

MED メトリック値

EBGPで広報するIPv4/IPv6経路情報に付加するMEDメトリック値を10進数を使用して、0～4294967295の範囲で指定します。省略時は、0に設定されます。

こんな事に気をつけて

IPv4/IPv6 BGP フィルタリング設定で、送信用のフィルタを設定した場合、本設定は無効となります。

デフォルトルート

BGPでIPv4/IPv6 デフォルトルートの広報を許可する場合は、“広報する”を選択します。

認証鍵

相手装置との間で、TCP-MD5認証を使用する場合の認証鍵を指定します。省略時は、TCP-MD5認証なしで接続します。0x22（ダブルクォーテーション）を除く0x21～0x7eの範囲のコードで構成される50文字以下のASCII文字列で指定します。

ASパスプリpend

EBGPで広報するIPv4/IPv6経路情報に付加するAS番号の個数を10進数を使用して、0～4の範囲で指定します。省略時は、0に設定されます。

こんな事に気をつけて

IPv4/IPv6 BGP フィルタリング設定で、送信用のフィルタを設定した場合、本設定は無効となります。

LOCALPREF

EBGPで受信するIPv4/IPv6経路情報のローカル優先度を10進数を使用して、0～4294967295の範囲で指定します。省略時は、100に設定されます。

こんな事に気をつけて

IPv4/IPv6 BGP フィルタリング設定で、送信用のフィルタを設定した場合、本設定は無効となります。

NEXTHOP SELF

IBGPで広報するIPv4/IPv6経路情報のネクストホップ情報を、自装置のIPアドレスに変更する場合は、“有効”を選択します。

26.4.6.2 IPv4 BGP フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 相手情報] → [追加]
→ [IPv4 BGP フィルタリング情報]

■ IPv4 BGP フィルタリング情報

※追加・修正情報は一覧ので設定してください。 [?]

優先順位	動作	方向	フィルタリング条件	MEDメトリック値	ASパスプレンド	操作
<input type="button" value="全削除"/>						
<IPv4 BGP フィルタリング情報入力フィールド>						
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信					
フィルタリング条件	<input checked="" type="radio"/> AS番号指定 AS番号 <input type="text"/> <input type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 IPアドレス <input type="text"/> アドレスマスク <input type="text"/> 0.0.0.0					
MEDメトリック値	<input type="text"/> 0					
ASパスプレンド	<input type="text"/> 0					
LOCALPREF	<input type="text"/> 100					
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>						

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているIPv4 BGP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP フィルタリングの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP 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。なお、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BGP 経路情報は遮断されます。

BGP 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。なお、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BGP 経路情報は遮断されます。

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- BGP/MPLS VPN で、BGP フィルタリング情報は無効となります。

動作

フィルタリング条件に該当する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかどうかをチェックするタイミングを選択します。

- 受信
BGPパケット受信時にチェックします。
- 送信
BGPパケット送信時にチェックします。

フィルタリング条件

フィルタリング条件を選択します。

- AS番号指定
経由したAS番号をフィルタリングの対象とします。
AS番号は0.1～65535.65535の範囲で指定します。
- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。
経路情報を指定するときは、BGP経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致したBGP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、BGP経路情報のそれぞれを指定したアドレスマスクでマスクした結果が一致した場合、そのBGP経路情報をフィルタリング対象とします。

MED メトリック値

フィルタリング結果で透過になったBGP経路情報のメトリック値を変更できます。MEDメトリック値は、10進数を使用して、0～4294967295の範囲で指定します。省略時は、0が設定されます。

こんな事に気をつけて

- 送信時のフィルタを設定した場合、「BGP相手基本情報」のMEDメトリック値の設定は無効となります。
- MEDメトリック値の設定は、EBGP送信時のフィルタリングでだけ有効となります。受信時のフィルタリングでのMEDメトリック値の設定は無効となります。

ASパスプリpend

フィルタリング結果で透過になったBGP経路情報に付加するAS番号の個数を、10進数を使用して、0～4の範囲で指定します。省略時は、0が設定されます。

こんな事に気をつけて

- 送信時のフィルタリングを設定した場合、「BGP相手基本情報」のASパスプリpendの設定は無効となります。
- ASパスプリpendの設定は、EBGP送信時のフィルタリングでだけ有効となります。受信時のフィルタリングに本設定を行っても、AS番号の追加は行われません。

LOCALPREF

フィルタリング結果で透過になったEBGP経路情報に対して、付加するLOCALPREFを10進数を使用して、0～4294967295の範囲で指定します。省略時は、100が設定されます。

こんな事に気をつけて

- 受信時のフィルタリングを設定した場合、「BGP相手基本情報」のLOCALPREFは無効となります。
- LOCALPREFは、EBGP受信時のフィルタリングでだけ有効となります。送信時のフィルタリングに本設定を行っても、LOCALPREFの設定は無効となります。

26.4.6.3 IPv6 BGP フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 相手情報] → [追加] → [IPv6 BGP フィルタリング情報]

■IPv6 BGPフィルタリング情報

※追加・修正情報は一覧ので設定してください。 [\[?\] \[?\]](#)

優先順位	動作	方向	フィルタリング条件	操作
全削除				
<IPv6 BGPフィルタリング情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断			
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信			
フィルタリング条件	<input checked="" type="radio"/> AS番号指定 AS番号 <input type="text"/> <input type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 IPアドレス /プレフィックス長 <input type="text"/> / <input type="text"/>			
	MEDメトリック値 <input type="text"/>			
	AS/パスリベンド <input type="text"/>			
	LOCALPREF <input type="text"/>			
追加 キャンセル				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているIPv6 BGP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP フィルタリングの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP 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。なお、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BGP 経路情報は遮断されます。

BGP 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。なお、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BGP 経路情報は遮断されます。

こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- BGP/MPLS VPN で、BGP フィルタリング情報は無効となります。

動作

フィルタリング条件に該当する経路情報の動作を以下の2つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

方向

フィルタリング条件に該当するかどうかをチェックするタイミングを選択します。

- 受信
BGPパケット受信時にチェックします。
- 送信
BGPパケット送信時にチェックします。

フィルタリング条件

フィルタリング条件を選択します。

- AS番号指定
経由したAS番号をフィルタリングの対象とします。
AS番号は0.1～65535.65535の範囲で指定します。
- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。
経路情報を指定するときは、BGP経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したIPアドレスとプレフィックス長が完全に一致したBGP経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、BGP経路情報のそれぞれを指定したプレフィックス長でマスクした結果が一致した場合、そのBGP経路情報をフィルタリング対象とします。

MED メトリック値

フィルタリング結果で透過になったBGP経路情報のメトリック値を変更できます。MEDメトリック値は、10進数を使用して、0～4294967295の範囲で指定します。省略時は、0が設定されます。

こんな事に気をつけて

- 送信時のフィルタを設定した場合、「BGP相手基本情報」のMEDメトリック値の設定は無効となります。
- MEDメトリック値の設定は、EBGP送信時のフィルタリングでだけ有効となります。受信時のフィルタリングでのMEDメトリック値の設定は無効となります。

ASパスプリpend

フィルタリング結果で透過になったBGP経路情報に付加するAS番号の個数を、10進数を使用して、0～4の範囲で指定します。省略時は、0が設定されます。

こんな事に気をつけて

- 送信時のフィルタリングを設定した場合、「BGP相手基本情報」のASパスプリpendの設定は無効となります。
- ASパスプリpendの設定は、EBGP送信時のフィルタリングでだけ有効となります。受信時のフィルタリングに本設定を行っても、AS番号の追加は行われません。

LOCALPREF

フィルタリング結果で透過になったEBGP経路情報に対して、付加するLOCALPREFを10進数を使用して、0～4294967295の範囲で指定します。省略時は、100が設定されます。

こんな事に気をつけて

- 受信時のフィルタリングを設定した場合、「BGP相手基本情報」のLOCALPREFは無効となります。
- LOCALPREFは、EBGP受信時のフィルタリングでだけ有効となります。送信時のフィルタリングに本設定を行っても、LOCALPREFの設定は無効となります。

26.4.6.4 BGP 拡張機能情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [BGP 相手情報] → [追加]
→ [BGP 拡張機能情報]

■BGP拡張機能情報	
エンフォースマルチホップ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
グレースフルリスタート	<input checked="" type="radio"/> 使用しない <input type="radio"/> IPv4ユニキャスト
staleタイム	6 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

エンフォースマルチホップ

エンフォースマルチホップとして動作させるかどうかを設定します。エンフォースマルチホップは、EBGPのマルチホップ接続で EBGPマルチホップの TTL 値に 1 が設定されても、受信した経路情報を破棄しないようとする機能です。

MPLS-IX 接続で EBGP を用いて経路交換を行う場合は、通常、LSP 未確立時には EBGP を確立しないようにするために、TTL 値 1 での EBGP が用いられます。LSP 確立時は、TTL 値の減算なしでフォワーディングされるため、TTL 値 1 での BGP マルチホップでの経路交換が可能となります。

通常のマルチホップ接続では、相手装置からの経路を TTL 値 1 で受信した場合は破棄しますが、本設定で受け取ることが可能となります。

グレースフルリスタート

グレースフルリスタートの使用に関して設定します。

アドレスファミリ

相手装置との BGP セッションでグレースフルリスタート機能を使用するアドレスファミリを指定します。相手装置との間で、ここで指定したアドレスファミリに対してのみ、グレースフルリスタートの処理が実施されます。本装置ではレシーブルータの機能のみが有効になります。

stale タイマ

相手装置とのグレースフルリスタート処理による BGP セッションの切断が発生した場合に、その相手装置から受信した経路を削除するまでの最大待ち時間を指定します。指定した時間の間、経路をルーティングテーブルに保持することにより、パケットの転送能力を保持したまま、グレースフルリスタート処理の完了を待ち合わせます。初期値は 360 秒です。このタイマ値は、相手装置から OPEN メッセージで通知されるグレースフルリスタートの Restart タイマより大きくしておく必要があります。小さい値を設定すると、自動的に Restart タイマの値に変更されます。

こんな事に気をつけて

グレースフルリスタートのアドレスファミリで指定されていないアドレスファミリに対しては、このタイマは有効になりません。その場合、このタイマの設定にかかわらず、そのアドレスファミリの経路はグレースフルリスタート開始時に即時に削除されます。

26.4.7 IPv4 BGP 再配布フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv4 BGP再配布フィルタリング情報]

■ IPv4 BGP再配布フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	フィルタリング条件	操作
	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定	<input type="button" value="全削除"/>
		<input checked="" type="radio"/> 検索条件 <input type="radio"/> IPアドレス <input type="radio"/> アドレスマスク	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
		<input type="text" value="IPアドレス"/>	<input type="text" value="0.0.0.0"/>
			<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv4 BGP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP 再配布フィルタリング情報の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

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遮断されます。
- BGP/MPLS VPN で、BGP 再配布フィルタリング情報は無効となります。

動作

BGP に再配布するフィルタリング条件の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。

経路情報指定

フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定した IP アドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定した IP アドレスと、再配布経路情報のそれぞれを指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

26.4.8 IPv6 BGP 再配布フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv6 BGP再配布フィルタリング情報]

■ IPv6 BGP再配布フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	フィルタリング条件	操作
	<input type="button" value="全削除"/>		
<IPv6 BGP再配布フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断		
	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	
フィルタリング条件	検索条件	IPアドレス /プレフィックス長	
		<input type="text"/> / <input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IPv6 BGP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP 再配布フィルタリング情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

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遮断されます。

動作

BGP に再配布するフィルタリング条件の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。

経路情報指定

フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致” または、“マスクした結果が一致” を選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定した IP アドレスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定した IP アドレスと、再配布経路情報のそれぞれを指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

26.4.9 IPv4 VRF 情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv4 VRF 情報]

■ IPv4 VRF情報

※追加・修正情報は一覧ので設定してください。

定義番号	ルート識別子	BGP/MPLS VPN広報	操作	
	ルート識別用AS番号	識別番号	スタティック経路情報	インターフェース経路情報
<input type="button" value="全削除"/>				
<IPv4 VRF情報入力フィールド>				
ルート識別子	ルート識別用AS番号	<input type="text"/>		
	識別番号	<input type="text"/>		
BGP/MPLS VPN広報	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する		
	インターフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているIPv4 VRF情報の定義が表示されています。VRF情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

BGP/MPLS VPNは、VPN単位にVRF情報を持ち、経路情報を別々に管理します。

ルート識別子

BGP/MPLS VPNで使用するルート識別子をルート識別用AS番号とIDで指定します。ルート識別用AS番号は自装置の属するルート識別用AS番号を10進数を使用して1～65535の範囲で設定します。識別番号は、VPNを一意に示すIDを10進数を使用して0～4294967295の範囲で指定します。

こんな事に気をつけて

ほかのVRF情報で設定されている識別番号と同じ値を設定することはできません。

BGP/MPLS VPN 広報

BGP/MPLS VPNでBGPに再配布する経路情報を選択します。

スタティック経路情報

本装置に設定されているBGP/MPLS VPNスタティック経路情報をBGPに再配布する場合は、“再配布する”を選択します。

インターフェース経路情報

VPNで使用するインターフェースの経路情報をBGPに再配布する場合は、“再配布する”を選択します。

こんな事に気をつけて

「[スタティック経路情報](#)」の設定で“再配布する”を選択し、
スタティック経路情報と同じあと先の経路情報をBGP/
MPLS VPNで受信した場合、BGP/MPLS VPNスタティック
経路情報を優先します。

26.4.10 IPv4 MPLS 連携情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [BGP 関連] → [IPv4 MPLS 連携情報]

■ IPv4 MPLS 連携情報 

MPLS 解決 使用しない 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

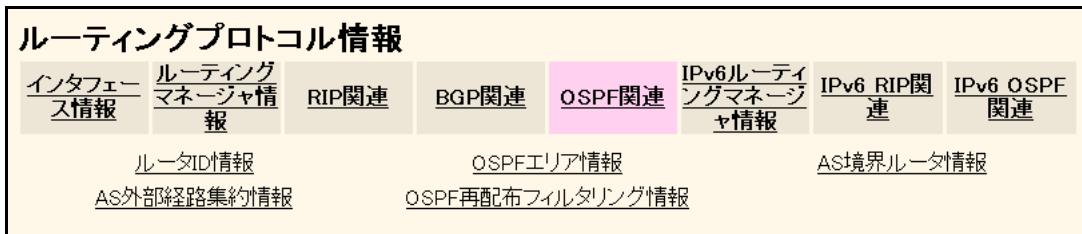
MPLS 解決

MPLS 解決を使用する場合は、“使用する”を選択します。

- 使用する
BGP で受信した経路の解決に MPLS を使用し、MPLS のラベルパスにマッピングします。
- 使用しない
MPLS トンネル接続上で BGP を使用します。

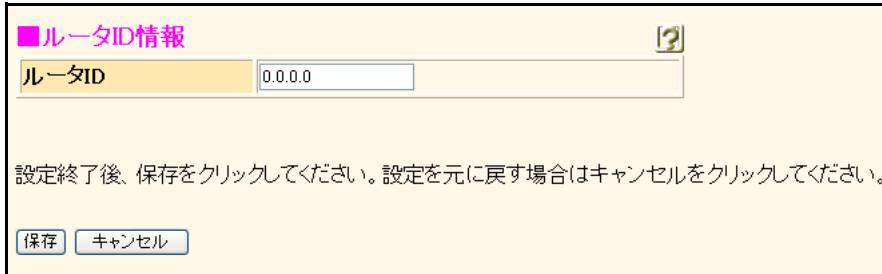
26.5 OSPF 関連

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連]



26.5.1 ルータ ID 情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [ルータ ID 情報]



ルータ ID

OSPF 接続で、自装置を唯一に示す ID を設定します。ID は、ほかルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。

設定を省略または 0.0.0.0 を指定した場合、以下のとおり ID を自動的に選択し、使用します。

- ループバックインターフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択し、使用します。
- ループバックインターフェースに追加 IP アドレスが設定されていない場合は、LAN インタフェース／リモートインターフェースに設定されている IPv4 アドレスの中からインターフェースの Up / Down の状態に関係なく最大の IPv4 アドレスを選択し、使用します。なお、リモートインターフェースの相手側 IP アドレスと LAN インタフェースのセカンダリ IP アドレスは選択対象となりません。

こんな事に気をつけて

OSPF ルータ ID は、他装置と重複しないように指定してください。正しくルーティングできない場合があります。

26.5.2 OSPF エリア情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF関連] → [OSPFエリア情報]

エリア定義番号	エリアID	エリア種別	コスト値	操作
				<input type="button" value="追加"/> <input type="button" value="全削除"/>

保存した情報は、設定反映後に有効になります。

現在、設定されている OSPF エリア情報の定義が表示されています。エリア定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF関連] → [OSPFエリア情報] → [追加]

ルーティングプロトコル情報 - **OSPFエリア情報(0)**

[OSPFエリア基本情報](#) [経路集約情報](#) [サマリLSA入出力可否情報](#)

[バーチャルリンク情報](#)

26.5.2.1 OSPF エリア基本情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF関連] → [OSPFエリア情報] → [追加]
→ [OSPFエリア基本情報]

エリアID	<input type="text"/>
エリア種別	<input checked="" type="radio"/> 通常エリア <input type="radio"/> スタブエリア <input type="radio"/> 準スタブエリア
デフォルトルートコスト	<input type="text" value="1"/>

* エリア種別がスタブエリアまたは準スタブエリアの場合のみ有効です。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルセルをクリックしてください。

エリアID

エリアIDをアドレス（ドット形式）または10進数を使用して指定します。

こんな事に気をつけて

OSPFを利用する場合は、エリアIDを必ず設定してください。

エリア種別

バックボーンエリア以外のエリアに対し、エリア種別を選択します。

こんな事に気をつけて

バックボーンエリアにスタブエリアまたは準スタブエリアを設定した場合も、通常エリアとして動作します。

デフォルトルートコスト

エリア境界ルータがスタブエリアまたは準スタブエリアに広報するデフォルトルートのコストを0～16777215の範囲で指定します。

26.5.2.2 経路集約情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報] → [追加] → [経路集約情報]

■経路集約情報

※追加・修正情報は一覧ので設定してください。

集約経路		操作
<input type="button" value="全削除"/>		
<経路集約情報入力フィールド>		
ネットワークアドレス	<input type="text"/>	
ネットマスク	<input type="text" value="0 0.0.0.0"/>	<input type="button" value="▼"/>
コスト	<input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている経路集約情報の定義が表示されています。1 エリアでの経路集約情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワークアドレス

エリア内部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

コスト

集約経路情報のコストを10進数を使用して0～16777215の範囲で指定します。省略時は、集約される経路情報の中でもっとも大きい値のコストが使用されます。

26.5.2.3 サマリ LSA 入出力可否情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報] → [追加] → [サマリ LSA 入出力可否情報]

■サマリLSA入出力可否情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	方向	対象経路情報	操作
全削除				
<サマリLSA入出力可否情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断			
方向	<input checked="" type="radio"/> 入力 <input type="radio"/> 出力			
	<input checked="" type="radio"/> すべて <input type="radio"/> 経路情報指定			
対象経路情報	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 IPアドレス <input type="text"/> アドレスマスク <input type="text"/>			
				<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているサマリ LSA 入出力可否定義が表示されています。処理は優先順位 1 から順に行われます。サマリ LSA 入出力可否の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

サマリ LSA の入力時は、優先順位の高い定義から順に入力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。

また、入力方向のすべての対象経路情報に一致しないサマリ LSA 経路情報は遮断されます。サマリ LSA の出力時は、優先順位の高い定義から順に出力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、出力方向のすべての対象経路情報に一致しないサマリ LSA 経路情報は遮断されます。

動作

対象経路情報に該当するサマリ LSA の動作を以下の 2 つから選択します。

- 透過
対象経路情報と一致した場合にサマリ LSA をエリア間で透過します。
- 遮断
対象経路情報と一致した場合にサマリ LSA をエリア間で遮断します。

方向

サマリ LSA 入出力可否の判断を行うタイミングを選択します。

- 入力
サマリ入出力可否の判断を、ほかのエリアからの入力時に行う場合にチェックします。
- 出力
サマリ入出力可否の判断を、ほかのエリアからの出力時に行う場合にチェックします。

対象経路情報

入力可否の対象となる経路情報を選択します。

- **すべて**
すべてのサマリ LSA を入出力可否情報の対象とします。
- **経路情報指定**
入出力可否の対象とする経路情報を指定します。
経路情報を指定するときは、サマリ LSA 経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。“完全に一致”を選択すると、指定した IP アドレスとアドレスマスクが完全に一致したサマリ LSA 経路情報を入出力可否の対象とします。
“マスクした結果が一致”を選択すると、指定した IP アドレスと、サマリ LSA 経路情報を、指定したアドレスマスクでマスクした結果が一致した場合、そのサマリ LSA 経路情報を入出力可否の対象とします。

こんな事に気をつけて

- 「OSPF 関連集約経路情報」で設定している集約経路情報は、そのエリアからの出力時には遮断できません。
以下の経路情報は、サマリ LSA 入出力可否の対象となりません。
- 各エリアの AS 境界ルータから注入された AS 外部経路
 - スタブエリアおよび準スタブエリアのエリア境界ルータが注入するデフォルト経路
 - type4 のサマリ LSA

26.5.2.4 バーチャルリンク情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF 関連] → [OSPF エリア情報] → [追加]
→ [バーチャルリンク情報]

■バーチャルリンク情報

※追加・修正情報は一覧ので設定してください。

接続先ルータ ID	Helloパケット送信間隔	隣接ルータ停止確認間隔	認証方式	操作
	Helloパケット送信間隔 パケット再送間隔	隣接ルータ停止確認間隔 LSUパケット送信遅延時間		

<バーチャルリンク情報入力フィールド>

接続先ルータID	<input type="text"/>
Helloパケット送信間隔	10 秒
隣接ルータ停止確認間隔	40 秒
パケット再送間隔	5 秒
LSUパ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	<input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数
認証鍵	<input type="text"/>
- MD5認証

認証鍵ID	<input type="text"/>
認証鍵	<input type="text"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているバーチャルリンク情報の定義が表示されています。バーチャルリンク情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

接続先ルータ ID

接続先ルータの OSPF ルータ ID を指定します。

Hello パケット送信間隔

バーチャルリンク接続先との OSPF 隣接関係の維持に使用する Hello パケットの送信間隔を指定します。奨励値は“10秒”です。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ Hello パケット送信間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

隣接ルータ停止確認間隔

バーチャルリンクでの OSPF 隣接関係の維持に使用する、隣接ルータ停止確認間隔を指定します。Hello パケット送信間隔より大きな値を設定する必要があります。Hello パケット送信間隔の 4 倍をお薦めします。通常は “40 秒” を指定します。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ隣接ルータ停止確認間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

パケット再送間隔

バーチャルリンクで OSPF パケットを再送する間隔を指定します。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

LSU パケット送信遅延時間

LSU (Link State Update) パケットの送信遅延時間を指定します。LSU パケットでは、LSA (Link State Advertisement) を作成してからの経過時間に対し、この設定時間を加算して広報します。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

一般的な装置では、LSU を作成してからの経過時間が 1 時間となった LSA を破棄します。このため、LSU 送信遅延時間に 1 時間以上を設定した場合は、正しくルーティングできない場合があります。

認証方式

パケットに対する認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が “文字列” の場合は、8 文字以内で指定します。鍵種別が “16 進数” の場合は、16 進数を使用して 16 衔以内で指定します。16 衔未満の鍵を指定した場合は、左詰めで設定され、残りは 16 衔になるまで 0x0 でパディングされます。

MD5 認証鍵 ID

バーチャルリンクの MD5 認証で使用する鍵 ID を 1 ~ 255 の範囲で指定します。

MD5 認証鍵

バーチャルリンクの MD5 認証で使用する鍵を指定します。16 文字以内で指定します。

26.5.3 AS境界ルータ情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF関連] → [AS境界ルータ情報]

■AS境界ルータ情報

デフォルトルート	<input checked="" type="radio"/> 広報しない <input type="radio"/> 広報する <input type="radio"/> AS外部経路に存在する場合に広報する
メトリック値	10
外部メトリック種別	type2

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

デフォルトルート

デフォルトルートを広報する際の条件を選択します。

外部メトリック種別

外部メトリックの種別を選択します。

メトリック値

デフォルトルートのメトリック値を0～16777214の範囲で指定します。省略時は、10が設定されます。

26.5.4 AS外部経路集約情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF関連] → [AS外部経路集約情報]

■AS外部経路集約情報

※追加・修正情報は一覧ので設定してください。

ネットワークアドレス	ネットマスク	操作
<input type="button" value="全削除"/>		
<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	<input type="text"/>	
ネットマスク	0.0.0.0	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているAS外部経路集約情報の定義が表示されています。AS外部経路集約情報の定義数は、仕様一覧「2.3 システム最大値一覧」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ネットワークアドレス

AS外部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

26.5.5 OSPF再配布フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [OSPF関連] → [OSPF再配布フィルタリング情報]

■OSPF再配布フィルタリング情報

※追加・修正情報は一覧ので設定してください。

優先順位	動作	フィルタリング条件	操作
	<input type="button" value="全削除"/>		
<OSPF再配布フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 <input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定		
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 IPアドレス <input type="text"/> アドレスマスク <input type="text"/> 0.0.0.0	
メトリック		<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する メトリック値 <input type="text"/> メトリックタイプ <input type="button" value="type2"/>	
	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている OSPF 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。OSPF 再配布フィルタリング情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#) (P43)」 を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

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再配布経路情報は遮断されます。

動作

OSPF に再配布する再配布経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- 全て
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。
なお、IP アドレスに 0.0.0.0、アドレスマスクに 0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

検索条件を選択します。

- 完全に一致
指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したIPアドレスと、再配布経路情報のそれぞれを、指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

デフォルトルートをOSPFに再配布する場合は、「AS境界ルータ情報」の設定も必要となります。

メトリック

経路情報をOSPFに再配布する際のメトリック値、メトリックタイプを指定する場合は、“指定する”を選択します。“指定しない”を選択した場合は、「ルーティングマネージャ情報」で設定したメトリック値、および、メトリックタイプとなります。なお、本設定は動作に“透過”を設定した場合に有効です。

メトリック値

OSPFに再配布する際のメトリック値を0～16777214の範囲で指定します。

こんな事に気をつけて

動作に遮断を指定した場合、メトリック値は指定できません。

メトリックタイプ

OSPFに再配布する際のメトリックタイプを選択します。

26.6 IPv6ルーティングマネージャ情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6ルーティングマネージャ情報]

ルーティングプロトコル情報							
インターフェース情報	ルーティングマネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
IPv6再配布情報	IPv6優先度情報						

26.6.1 IPv6 再配布情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6ルーティングマネージャ情報]
→ 「IPv6再配布情報」

■ IPv6再配布情報		?
RIP	インターフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0 <input type="button" value="▼"/>
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0 <input type="button" value="▼"/>
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0 <input type="button" value="▼"/>
	DHCP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0 <input type="button" value="▼"/>
BGP	インターフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	DHCP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
OSPF	インターフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="button" value="type2 ▼"/>
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="button" value="type2 ▼"/>
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="button" value="type2 ▼"/>
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="button" value="type2 ▼"/>

	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="button" value="type2"/>
	DHCP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="button" value="type2"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

RIP

以下の各経路情報を RIP に再配布するかどうかを設定します。経路情報を RIP に再配布する場合は、“再配布する”を選択します。

- ・ インタフェース経路情報
- ・ スタティック経路情報
- ・ BGP 経路情報
- ・ OSPF 経路情報
- ・ DNS 経路情報
- ・ DHCP 経路情報

メトリック値

RIP に再配布する際のメトリック値を選択します。

BGP

以下の各経路情報を BGP に再配布するかどうかを設定します。経路情報を BGP に再配布する場合は、“再配布する”を選択します。

- ・ インタフェース経路情報
- ・ スタティック経路情報
- ・ RIP 経路情報
- ・ OSPF 経路情報
- ・ DNS 経路情報
- ・ DHCP 経路情報

OSPF

以下の各経路情報を OSPF に再配布するかどうかを設定します。経路情報を OSPF に再配布する場合は、“再配布する”を選択します。

- ・ インタフェース経路情報
- ・ スタティック経路情報
- ・ RIP 経路情報
- ・ BGP 経路情報
- ・ DNS 経路情報
- ・ DHCP 経路情報

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。省略時は、20 が設定されます。

メトリックタイプ

AS 外部経路のメトリックタイプを指定します。

こんな事に気をつけて

DHCP 経路情報を “再配布する” と選択しても、DHCP 経路情報の Blackhole 経路、Reject 経路は、再配布できません。

26.6.2 IPv6 優先度情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6ルーティングマネージャ情報]
 → [IPv6 優先度情報]

■ IPv6 優先度情報		
優先度	RIP	120
	EBGP	20
	IBGP	200
	OSPF	110
	DNS	15
	DHCP	10

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

優先度

複数のルーティングプロトコルで同じ経路情報を受信した場合や受信した経路情報がスタティック経路情報と同じだった場合、どの経路情報を優先的に使用するかを優先度で判断します。

優先度は、10進数を使用して1～254で指定します。より小さい値が、より高い優先度を示します。

RIP

RIP 経路情報の優先度を指定します。省略時は、120が設定されます。

EBGP

EBGP 経路情報の優先度を指定します。省略時は、20が設定されます。

IBGP

IBGP 経路情報の優先度を指定します。省略時は、200が設定されます。

OSPF

OSPF 経路情報の優先度を指定します。省略時は、110が設定されます。

DNS

DNS 経路情報の優先度を指定します。省略時は、15が設定されます。

DHCP

DHCP 経路情報の優先度を指定します。省略時は、10が設定されます。

こんな事に気をつけて

- ・ 優先度は、ほかのプロトコルやスタティック経路情報に設定されている値と同じ値は指定しないでください。
- ・ スタティック経路情報の優先度の初期値は0です。

26.7 IPv6 RIP 関連

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]

ルーティングプロトコル情報							
インターフェース情報	ルーティングマネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
IPv6 RIPタイム情報	IPv6 RIPマルチバス情報	IPv6 RIP再配布フィルタリング情報					

26.7.1 IPv6 RIP タイマ情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連] → [IPv6 RIP タイマ情報]

■ IPv6 RIPタイム情報	
定期広報タイム	30 秒
有効期限タイム	3 分
ガーベージタイム	2 分

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

定期広報タイム

RESPONSE パケットで定期的に経路を広報する間隔を指定します。初期値は30秒です。

有効範囲)

10～3600秒

1～60分

1時間

ガーベージタイム

有効期限が切れた場合に、その経路情報をメトリック16で広報する時間を指定します。初期値は120秒です。

有効範囲)

10～3600秒

1～60分

1時間

有効期限タイム

RESPONSE パケットで更新されない経路情報の有効期限を指定します。初期値は180秒です。

有効範囲)

10～3600秒

1～60分

1時間

26.7.2 IPv6 RIP マルチパス情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連] → [IPv6 RIP マルチパス情報]

■ IPv6 RIPマルチパス情報

マルチパス数

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

マルチパス数

RIPで受信可能な同じあて先への経路情報数を1～2の範囲で指定します。省略時は、1が設定されます。

26.7.3 IPv6 RIP 再配布フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 RIP 関連]
→ [IPv6 RIP 再配布フィルタリング情報]

■ IPv6 RIP再配布フィルタリング情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	フィルタリング条件	操作								
	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定	<input type="button" value="全削除"/>								
<IPv6 RIP再配布フィルタリング情報入力フィールド> <table border="1"> <tr> <td>動作</td> <td><input checked="" type="radio"/> 透過 <input type="radio"/> 遮断</td> </tr> <tr> <td>フィルタリング条件</td> <td> <input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定 </td> </tr> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>プレフィックス／ プレフィックス長</td> <td><input type="text" value=""/></td> </tr> </table>				動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	プレフィックス／ プレフィックス長	<input type="text" value=""/>
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断										
フィルタリング条件	<input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定										
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致										
プレフィックス／ プレフィックス長	<input type="text" value=""/>										

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている RIP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP 再配布フィルタリング情報の定義数は、仕様一覧 「2.3 システム最大値一覧」 (P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

動作

RIP に再配布する経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または、“マスクした結果が一致”を選択します。
なお、`::/0`を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、再配布経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

26.8 IPv6 OSPF 関連

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連]

ルーティングプロトコル情報							
インターフェース情報	ルーティングマネージャ情報	RIP関連	BGP関連	OSPF関連	IPv6ルーティングマネージャ情報	IPv6 RIP関連	IPv6 OSPF関連
IPv6 ルータID情報		IPv6 OSPFエリア情報			IPv6 AS境界ルータ情報		
IPv6 OSPF再配布フィルタリング情報							

26.8.1 IPv6 ルータ ID 情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 ルータ ID 情報]

■ IPv6 ルータID情報	
ルータID	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。	
保存	キャンセル

ルータ ID

IPv6 OSPF 接続で自装置を一意に示す ID を指定します。

ID はほかのルータと重複しない値を指定してください。

ルータ ID の設定を削除する場合は、ルータ ID の値を省略して保存してください。

こんな事に気をつけて

IPv6 OSPF を利用する場合は、OSPF ルータ ID を必ず設定してください。未設定時の自動設定機能はありません。

26.8.2 IPv6 OSPF エリア情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 OSPF エリア情報]

■ IPv6 OSPF エリア情報				
エリア定義番号	エリアID	エリア種別	コスト値	操作
				<input type="button" value="追加"/> <input type="button" value="全削除"/>

保存した情報は、設定反映後に有効になります。

現在、設定されている OSPF エリア情報の定義が表示されています。装置全体でのエリア定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 OSPF エリア情報]
→ [追加]

ルーティングプロトコル情報 - IPv6 OSPF エリア情報 (0)

IPv6 OSPF エリア基本情報 IPv6 経路集約情報 IPv6 エリア間プレフィックスLSA入出力可否情報

26.8.2.1 IPv6 OSPF エリア基本情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 OSPF エリア情報]
→ [追加] → [IPv6 OSPF エリア基本情報]

■ IPv6 OSPF エリア基本情報	
エリアID	0.0.0.0
エリア種別	<input checked="" type="radio"/> 通常エリア <input type="radio"/> スタブエリア
デフォルトルートコスト値	1 ※ エリア種別がスタブエリアの場合のみ有効です。

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

エリア ID

エリア ID を 0.0.0.0 ~ 255.255.255.255 の IPv4 アドレス表記（ドット形式）または 0 ~ 4294967295 の 10 進数表記で指定します。バックボーンエリアの場合は、0.0.0.0 または 0 を指定します。

こんな事に気をつけて

OSPF を利用する場合は、エリア ID を必ず設定してください。

エリア種別

バックボーンエリア以外のエリアに対し、エリア種別を選択します。

こんな事に気をつけて

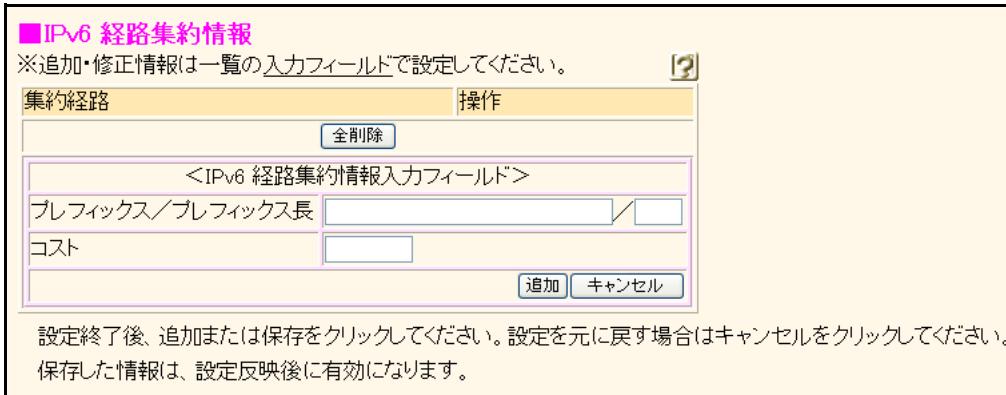
バックボーンエリアにスタブエリアと設定した場合も、通常エリアとして動作します。

デフォルトルートコスト値

エリア境界ルータがスタブエリアに広報するデフォルトルートのコストを 1 ~ 16777215 の範囲の 10 進数で指定します。

26.8.2.2 IPv6 経路集約情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 OSPF エリア情報]
 → [追加] → [IPv6 経路集約情報]



現在、設定されている経路集約情報の定義が表示されています。経路集約情報の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

プレフィックス／プレフィックス長

エリア内部経路を集約する経路情報を指定します。

コスト

集約経路情報のコストを、0 ~ 16777215 の範囲の10進数で指定します。省略時は、集約される経路情報の中で、もっとも大きい値のコストが使用されます。

26.8.2.3 IPv6 エリア間プレフィックス LSA入出力可否情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 OSPF エリア情報] → [追加] → [IPv6 エリア間プレフィックス LSA入出力可否情報]

■IPv6 エリア間プレフィックスLSA入出力可否情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	方向	対象経路情報	操作
[全削除]				
<IPv6 エリア間プレフィックスLSA入出力可否情報入力フィールド>				
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断			
方向	<input checked="" type="radio"/> 入力 <input type="radio"/> 出力			
	<input checked="" type="radio"/> すべて <input type="radio"/> 経路情報指定			
対象経路情報	<input checked="" type="radio"/> 検索条件 <input type="radio"/> マスクした結果が一致		<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	
	プレフィックス/ プレフィックス長	<input type="text"/> ✓		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>				

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているエリア間プレフィックス LSA 入出力可否定義が表示されています。処理は優先順位 1 から順に行われます。エリア間プレフィックス LSA 入出力可否の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

エリア間プレフィックス LSA の入力時は、優先順位の高い定義から順に入力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、入力方向のすべての対象経路情報に一致しないエリア間プレフィックス LSA 経路情報は遮断されます。

エリア間プレフィックス LSA の出力時は、優先順位の高い定義から順に出力方向の対象経路情報を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の対象経路情報は参照されません。また、出力方向のすべての対象経路情報に一致しないエリア間プレフィックス LSA 経路情報は遮断されます。

動作

対象経路情報に該当するエリア間プレフィックス LSA の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合に経路情報を透過します。
- 遮断
条件と一致した場合に経路情報を遮断します。

対象経路情報

入出力可否の対象となる経路情報を選択します。

- すべて
すべてのエリア間プレフィックス LSA が入出力可否の対象となります。
- 経路情報指定
入出力可否の対象とする経路情報を指定できます。
経路情報を指定するときは、エリア間プレフィックス LSA 経路の検索条件として、“完全に一致” または “マスクした結果が一致” を選択します。

方向

エリア間プレフィックス LSA 入出力可否の判断をほかのエリアからの入力時に行うか、ほかのエリアへの出力時に行うかを選択します。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致したエリア間プレフィックスLSA経路情報を入出力可否の対象とします。
- マスクした結果が一致
指定したプレフィックスと、エリア間プレフィックスLSA経路情報を、指定したプレフィックス長でマスクした結果が一致した場合、そのエリア間プレフィックスLSA経路情報を入出力可否の対象とします。

こんな事に気をつけて

- 「IPv6 OSPF 関連」の「IPv6 経路集約情報」で設定している経路集約情報は、そのエリアからの出力時には遮断できません。
- 以下の経路情報は、エリア間プレフィックスLSA入出力可否の対象となりません。
 - スタブエリアのエリア境界ルータが注入するデフォルト経路

26.8.3 IPv6 AS境界ルータ情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連] → [IPv6 AS境界ルータ情報]

■ IPv6 AS境界ルータ情報	
デフォルトルート	<input checked="" type="radio"/> 広報しない <input type="radio"/> 広報する <input type="radio"/> AS外部経路に存在する場合に広報する
メトリック値	10
外部メトリック種別	type2

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

デフォルトルート

デフォルトルートを広報する際の条件を選択します。

外部メトリック種別

外部メトリックの種別を選択します。

メトリック値

デフォルトルートのメトリック値を0～16777214の範囲の10進数で指定します。省略時は、10が設定されます。

26.8.4 IPv6 OSPF 再配布フィルタリング情報

[操作] ルータ設定「ルーティングプロトコル情報」→ [IPv6 OSPF 関連]
 → [IPv6 OSPF 再配布フィルタリング情報]

■IPv6 OSPF再配布フィルタリング情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	動作	フィルタリング条件	操作
	<input type="button" value="全削除"/>		
<IPv6 OSPF再配布フィルタリング情報入力フィールド>			
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断 <input checked="" type="radio"/> すべて <input type="radio"/> デフォルトルート <input type="radio"/> 経路情報指定 <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> 検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致 プレフィックス/ プレフィックス長 </div>		
	フィルタリング条件		
メトリック		<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する メトリック値 <input type="text"/> メトリックタイプ <input type="button" value="type2"/>	
	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
 保存した情報は、設定反映後に有効になります。

現在、設定されている OSPF 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。OSPF 再配布フィルタリング情報の定義数は、仕様一覧 「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。

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再配布経路情報は遮断されます。

動作

OSPF に再配布する再配布経路情報の動作を以下の 2 つから選択します。

- 透過
条件と一致した場合にパケットを透過します。
- 遮断
条件と一致した場合にパケットを遮断します。

フィルタリング条件

フィルタリング条件を選択します。

- すべて
すべての経路情報をフィルタリング対象とします。
- デフォルトルート
デフォルトルートをフィルタリング対象とします。
- 経路情報指定
フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、再配布経路の検索条件として、“完全に一致”または“マスクした結果が一致”を選択します。
なお、::/0 を指定した場合、デフォルトルートをフィルタリング対象とします。

検索条件

検索条件を選択します。

- 完全に一致
指定したプレフィックスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
指定したプレフィックスと、再配布経路情報のプレフィックスのそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

デフォルトルートを OSPF に再配布する場合は、「IPv6 AS 境界ルータ情報」の設定も必要となります。

メトリック

経路情報を OSPF に再配布する際のメトリック値、メトリックタイプを指定する場合は、“指定する”を選択します。“指定しない”を選択した場合は、「IPv6 ルーティングマネージャ情報」で設定したメトリック値、および、メトリックタイプとなります。なお、本設定は動作に“透過”を設定した場合に有効です。

メトリック値

OSPF に再配布する際のメトリック値を 0～16777214 の範囲で指定します。

こんな事に気をつけて

動作に遮断を指定した場合、メトリック値は指定できません。

メトリックタイプ

OSPF に再配布する際のメトリックタイプを選択します。

27 マルチキャスト情報

適用機種 全機種

[操作] ルータ設定「マルチキャスト情報」

マルチキャスト情報

[IPマルチキャスト情報](#)

[IPマルチキャストスタティックRP情報](#)

[IPマルチキャストスタティック経路情報](#)

27.1 IPマルチキャスト情報

[操作] ルータ設定「マルチキャスト情報」 → [IPマルチキャスト情報]

■ IPマルチキャスト情報

IGMP	IGMP Membership Report 送信抑止	<input checked="" type="radio"/> する <input type="radio"/> しない
	RP候補	<input checked="" type="radio"/> しない <input type="radio"/> する IPアドレス <input type="text" value="0.0.0.0"/> ブライオリティ <input type="text" value="0"/>
		<input checked="" type="radio"/> しない <input type="radio"/> する IPアドレス <input type="text" value="0.0.0.0"/> ブライオリティ <input type="text" value="0"/>
	SPTへの経路変更	<input type="radio"/> しない <input checked="" type="radio"/> 即時 <input type="radio"/> 転送速度 <input type="text" value=""/> Kbps
register	<input type="radio"/> ヘッダ部 <input checked="" type="radio"/> パケット全体	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

IGMP

IGMP Membership Report 送信抑止

IGMP Query 受信時の応答動作を指定します。

- する
IGMPv2 (RFC2236) 仕様に従い、他ホストからの IGMP Membership Report を受信した場合は、重複によるトラフィック増加の防止のため、本装置からは IGMP Membership Report を送出しません。
- しない
常に送信します。

PIM-SM

RP 候補

ランデブー・ポイント (RP) の設定です。マルチキャスト・ルーティングプロトコルに PIM-SM を利用する場合は、RP として動作するルータがネットワーク上に 1 台以上必要です。RP の設定は、1 台のルータだけで行っても、複数のルータで行っても構いません。トラフィックを分散する場合は、複数台のルータで RP の設定を行っておきます。

IP アドレス

RPとして動作するインターフェースのIPアドレスを指定します。0.0.0.0を指定または指定しない場合は、RPとして動作できるインターフェースを自動で検索します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

プライオリティ

RPのプライオリティ情報を10進数を使用して、0～255の範囲で指定します。数が小さいほど優先度は高くなります。初期値は0です。

BSR 候補

ブート・ストラップ・ルータ (BSR) の設定です。マルチキャスト・ルーティングプロトコルにPIM-SMを利用する場合は、BSRとして動作するルータがネットワーク上に必要です。BSRの設定は、1台のルータだけで行っても、複数のルータで行っても構いません。障害に強いネットワークを構成する場合は、複数台のルータでBSRの設定を行っておきます。

IP アドレス

BSRとして動作するインターフェースのIPアドレスを指定します。0.0.0.0を指定または指定しない場合は、BSRとして動作できるインターフェースを自動で検索します。

有効範囲)

1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254

プライオリティ

BSRのプライオリティ情報を10進数を使用して、0～255の範囲で指定します。数が大きいほど優先度は高くなります。初期値は0です。

SPTへの経路変更

SPT (Shortest Path Tree)への経路変更を選択します。SPTの設定は、マルチキャスト・パケットを受信者となるlast hop router上で行います。

即時

SPTへの経路変更を転送速度に関係なく即時行う場合に選択します。通常は、この設定を選択します。

転送速度

転送速度によってSPTへの経路変更を行う場合に選択します。マルチキャスト・トラフィックがしきい値となる転送速度を上回ったときにSPTが切り替わります。転送速度を以下の範囲で指定します。

機種	転送速度
Si-R570、570B以外	1～100000Kbps
Si-R570、570B	1～1000000Kbps

register

PIM Registerパケットを設定します。マルチキャスト・パケットを送信するルータ上で行います。

チェックサム

PIM Registerパケットの送信時のチェックサムの計算方法を設定することができます。

PIM Registerパケットのチェックサムの計算範囲は、RFC2362ではヘッダ部だけで計算するように定義されていますが、一部のルータはパケット全体で計算します。このようなルータがRPを行う場合は、PIM Registerパケットが受信されない可能性があるため、チェックサムの計算範囲を“パケット全体”に変更する必要があります。

本装置はPIM Registerパケットの受信時に、ヘッダ部 (RC2362準拠)とパケット全体の2つの方法で計算するため、本装置がRPを行う場合は、どちらの計算方法のパケットを受信しても問題はありません。

27.2 IP マルチキャストスタティック RP 情報

[操作] ルータ設定「マルチキャスト情報」→ [IP マルチキャストスタティック RP 情報]

■IP マルチキャストスタティック RP 情報

※追加・修正情報は一覧ので設定してください。

定義番号	IPアドレス	操作
	プライオリティ	
<input type="button" value="全削除"/>		
<IP マルチキャストスタティック RP 情報入力フィールド>		
IPアドレス	<input type="text"/>	
プライオリティ	<input type="text"/>	
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IP マルチキャストスタティック RP 情報の定義が表示されています。IP マルチキャストスタティック RP の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

IP アドレス

RPとして動作するインターフェースのIPアドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

プライオリティ

RPのプライオリティ情報を10進数を使用して、0～255の範囲で指定します。数が大きいほど優先度は高くなります。初期値は0です。

27.3 IP マルチキャストスタティック経路情報

[操作] ルータ設定「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]

■IP マルチキャストスタティック経路情報

※追加・修正情報は一覧の入力フィールドで設定してください。

定義番号	配送元ホストアドレス マルチキャストグループアドレス 入力インターフェース 出力インターフェース グループ参加	操作
全削除		
<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	<input type="radio"/> すべて <input checked="" type="radio"/> 指定する <input type="text"/>	
マルチキャストグループアドレス	<input type="text"/>	
入力インターフェース	LAN0	
出力インターフェース	<input type="text"/>	
グループ参加	<input checked="" type="radio"/> しない <input type="radio"/> する <input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている IP マルチキャストスタティック経路情報の定義が表示されています。IP マルチキャストスタティック経路の定義数は、仕様一覧 [\[2.3 システム最大値一覧\] \(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

配送元ホストアドレス

配送元ホストを IPv4 アドレスで指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

出力インターフェース

出力インターフェースを指定します。LAN0 ~ max または、rmt0 ~ max で指定してください。複数指定する場合は、" "で区切ります。範囲指定の場合は "-" で区切れます。出力インターフェースは 20 個まで設定できます。

マルチキャストグループアドレス

マルチキャストグループアドレスを 224.0.1.0 ~ 239.255.255.255 の範囲の IPv4 アドレスで指定します。

グループ参加

入力インターフェースでマルチキャストグループに参加するかどうかを指定します。"する"を選択した場合、入力インターフェースでは IGMP によるグループ参加を行います。

入力インターフェース

入力インターフェースを選択します。

28 UPnP 情報

適用機種 全機種

[操作] ルータ設定「UPnP 情報」



28.1 基本情報

[操作] ルータ設定「UPnP 情報」 → [基本情報]

■ 基本情報	
UPnP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する <input checked="" type="radio"/> 無期限 <input type="radio"/> 設定する <input type="text"/> 日 <input type="button" value="▼"/>
ポートマッピング有効期限	

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

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。

こんな事に気をつけて

- UPnP 対応装置のマニュアルを参照して、UPnP 機能を使用するように設定されていることを確認してください。
- UPnP 対応装置は DHCP 機能を利用して簡単に使用できるようになっていますので、本装置の DHCP サーバ機能を使用することをお薦めします。
- マルチ NAT 機能を使用しないインターフェースに UPnP 対応装置を接続してください。マルチ NAT 機能を使用するインターフェースへの通信に対して VoIP NAT トランザクション機能が動作します。

ポートマッピング有効期限

UPnP クライアントがポートマッピングを無期限で設定しようとすると、強制的に設定する有効期限を指定します。設定したポートマッピングが使用されなくなったら有効期限を過ぎたとき、そのポートマッピングを強制的に削除します。

無期限を選択した場合、UPnP クライアントがポートマッピングを削除するまでポートマッピングが設定されたままとなります。

有効範囲)	60～86400 秒
	1～1440 分
	1～24 時間
	1 日

29 MPLS 情報

適用機種 全機種

[操作] ルータ設定「MPLS 情報」

MPLS情報

基本情報

29.1 基本情報

[操作] ルータ設定「MPLS 情報」→「基本情報」

■ 基本情報	
MPLS TTL伝達	<input type="radio"/> しない <input checked="" type="radio"/> する
router ID	<input type="text"/>
LDP 制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
IPv4 Transport アドレス	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

MPLS TTL 伝達

MPLS から IP、または IP から MPLS にパケットを交換するときに、TTL の情報を伝達する場合は、“する”を選択します。

LDP

router ID

使用するルータを特定する ID を有効な IPv4 アドレスで指定します。0.0.0.0 の場合、LDP 機能は動作しません。

制御方式

LDP の制御方式を選択します。

IPv4 Transport アドレス

LDP がピアとの通信に使用する送信元 IPv4 アドレスを指定します。装置のループバックインターフェースに設定した IPv4 アドレスを指定します。0.0.0.0 を指定した場合は、LDP が動作するインターフェースの IPv4 アドレスが IPv4 Transport Address として使用されます。省略時は、0.0.0.0 が設定されます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

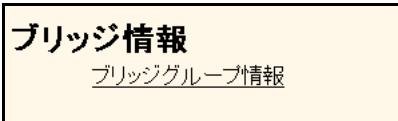
128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

30 ブリッジ情報

適用機種 全機種

[操作] ルータ設定「ブリッジ情報」



30.1 ブリッジグループ情報

[操作] ルータ設定「ブリッジ情報」 → [ブリッジグループ情報]

■ブリッジグループ情報					
グループ識別子	学習テーブル生存時間	IPv4ルーティング機能	IPv6ルーティング機能	MACコントロールフレーム転送機能	操作
0	5分	使用する	使用する	なし	修正 削除
1	5分	使用する	使用する	なし	修正 削除
2	5分	使用する	使用する	なし	修正 削除
3	5分	使用する	使用する	なし	修正 削除
4	5分	使用する	使用する	なし	修正 削除

15	5分	使用する	使用する	なし	修正 削除
16	5分	使用する	使用する	なし	修正 削除
17	5分	使用する	使用する	なし	修正 削除
18	5分	使用する	使用する	なし	修正 削除
19	5分	使用する	使用する	なし	修正 削除

全削除

保存した情報は、設定反映後に有効になります。

ブリッジグループ情報設定項目はブリッジ機能を使用する場合だけ有効です。ブリッジグループ情報の定義は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

30.1.1 ブリッジグループ情報（グループ識別子0の場合）

[操作] ルータ設定「ブリッジ情報」→「ブリッジグループ情報」→「グループ識別子0」[修正]

<ブリッジグループ情報入力フィールド>	
学習テーブル生存時間	5 分
IPv4ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシ <input checked="" type="radio"/> strict <input type="radio"/> loose
IPv6ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシ <input checked="" type="radio"/> strict <input type="radio"/> loose
リモートインターフェース間ブリッジ	<input checked="" type="radio"/> する <input type="radio"/> しない
STP	ブリッジの優先度: 32768 ブリッジのHello待ち時間: 20 秒 ブリッジのHello送出間隔: 2 秒 フォワーディング遅延時間: 15 秒
VLANタグ付きフレーム	<input checked="" type="radio"/> VLANタグを挿抜 <input type="radio"/> 透過する
MACコントロールフレーム転送機能	<input type="checkbox"/> STP <input type="checkbox"/> LACP <input type="checkbox"/> EAPOL
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>	

学習テーブル生存時間

学習テーブル生存時間を指定します。グループ識別子0で設定した学習テーブル生存時間が全グループで使用されます。初期値は5分です。

有効範囲)

- 1～11日
- 1～277時間
- 1～16666分
- 10～1000000秒

IPv4 ルーティング機能

IPv4をルーティングによって制御する場合は、“使用する”を選択します。

転送ポリシ

IPv4ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送するかどうかを選択します。

受信フレームの先 MAC アドレスが受信インターフェースであるが、先 IP アドレスが受信インターフェースではない場合、IPv4ブリッジ動作時に、グループ内からグループ外へルーティングによって転送します。

IPv4をルーティングするインターフェースで受信したパケットが、ルーティングによってIPv4をブリッジするインターフェースへ出力される場合、IPv4ブリッジ動作時に、グループ外からグループ内へルーティングによって転送します。

strict を選択した場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

- strict
IPv4 ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送しません。
- loose
IPv4 ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送します。

IPv6 ルーティング機能

IPv6をルーティングによって制御する場合は、“使用する”を選択します。

転送ポリシ

IPv6 ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送するかどうかを選択します。

受信フレームのあて先 MAC アドレスが受信インターフェースあてであるが、あて先 IP アドレスが受信インターフェースあてではない場合、IPv6 ブリッジ動作時に、グループ内からグループ外へルーティングによって転送します。

IPv6をルーティングするインターフェースで受信したパケットが、ルーティングによって IPv6をブリッジするインターフェースへ出力される場合、IPv6 ブリッジ動作時に、グループ外からグループ内へルーティングによって転送します。

strict を選択した場合、これらの転送をブロックすることで、ブリッジ転送対象外のパケットに対してもグループ内に閉じた通信を行うことができます。

- strict
IPv6 ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送しません。
- loose
IPv6 ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送します。

リモートインターフェース間ブリッジ

リモートインターフェースから受信したフレームを別のリモートインターフェースへブリッジする場合は、“する”を選択します。

STP

ブリッジの優先度

ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を 0～65535 の範囲で指定します。ブリッジの優先度は、値の小さい方がより優先となります。この設定項目は STP を使用する場合だけ有効です。

ブリッジの Hello 待ち時間

ルートブリッジまたは代表ブリッジから送出される構成情報 BPDU の待ち時間を 6～40 秒の範囲で指定します。この設定項目は STP を使用する場合だけ有効です。

ブリッジの Hello 送出間隔

ルートブリッジになったときに送出する構成情報 BPDU の送出間隔を 1～10 秒の範囲で指定します。この設定項目は STP を使用する場合および本装置がルートブリッジとして動作する場合だけ有効です。

フォワーディング遅延時間

構成情報 BPDU が、一番時間がかかる経路に届く時間を設定します。フォワーディング遅延時間を 4～30 秒の範囲で指定します。この設定項目は STP を使用する場合および本装置がルートブリッジとして動作する場合だけ有効です。

VLAN タグ付きフレーム

VLANインターフェースで受信した VLAN タグ付きフレームのタグを透過転送するかどうかを設定します。VLAN タグを挿入する設定の場合、VLANインターフェースで受信してリモートインターフェースへ出力する際には VLAN タグを除去して転送し、リモートインターフェースで受信して VLANインターフェースへ出力する際には VLAN タグを挿入して転送します。

MAC コントロールフレーム転送機能

MAC コントロールフレームをブリッジ転送するかどうかを設定します。ブリッジ転送をすると設定されたプロトコルの MAC コントロールフレームはそのグループ内のインターフェースに転送されます。ただし、本装置で有効となっている機能に関するフレームを転送する設定にした場合、転送される定義となっている機能は無効となります。具体的には、STP のフレームを転送すると定義した場合、そのグループのブリッジインターフェースでは STP は使用できません。

30.1.2 ブリッジグループ情報（グループ識別子1～7の場合）

[操作] ルータ設定「ブリッジ情報」→ [ブリッジグループ情報] → [グループ識別子1] [修正]

<ブリッジグループ情報入力フィールド>	
学習テーブル生存時間	5分
IPv4ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシ <input checked="" type="radio"/> strict <input type="radio"/> loose
IPv6ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシ <input checked="" type="radio"/> strict <input type="radio"/> loose
リモートインターフェース間ブリッジ	<input checked="" type="radio"/> する <input type="radio"/> しない
VLANタグ付きフレーム	<input checked="" type="radio"/> VLANタグを挿抜 <input type="radio"/> 透過する
MACコントロールフレーム 転送機能	<input type="checkbox"/> STP <input type="checkbox"/> LACP <input type="checkbox"/> EAPOL

各項目の説明は、「ブリッジグループ情報（グループ識別子0の場合）」を参照してください。

31 動的VPN情報

適用機種 全機種

[操作] ルータ設定「動的VPN情報」

動的VPN情報

サーバ関連情報	クライアント関連情報
---------	------------

このページでは動的VPN情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

31.1 サーバ関連情報

[操作] ルータ設定「動的VPN情報」 → [サーバ関連情報]

動的VPN情報

サーバ関連情報	クライアント関連情報
---------	------------

基本情報

31.1.1 基本情報

[操作] ルータ設定「動的VPN情報」 → [サーバ関連情報] → [基本情報]

■ 基本情報

サーバ機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する ドメイン名 <input type="text"/> 認証 <input checked="" type="radio"/> 行わない <input type="radio"/> 行う AAAグループID <input type="text"/>
-------	--

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

サーバ機能

本装置を動的VPNサーバとして使用する場合は、“使用する”を選択します。

ドメイン名

動的VPNで使用するドメイン名を80文字以内で指定します。

認証

動的VPNサーバでメッセージの認証を行う場合は“行う”を選択し、参照するAAAのグループIDを設定します。

AAAグループID

動的VPNサーバでメッセージ認証を行う場合は、参照するAAAのグループIDを10進数を使用して、10未満で指定します。

31.2 クライアント関連情報

[操作] ルータ設定「動的VPN情報」→ [クライアント関連情報]

31.2.1 基本情報

[操作] ルータ設定「動的VPN情報」→ [クライアント関連情報] → [基本情報]

クライアント機能

交換情報のエンコード

動的VPN機能を使用する際に交換情報をエンコードするかどうかを選択します。“する”を選択した場合はbase64でエンコードします。

こんな事に気をつけて
拠点装置のバージョンがV30の場合、“しない”を選択してください。

31.2.2 ドメイン情報

[操作] ルータ設定「動的VPN情報」→ [クライアント関連情報] → [ドメイン情報]

現在、設定されているドメイン情報の定義が表示されています。ドメイン情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

ドメイン名

ドメイン名を80文字以内で指定します。

ドメイン名は、動的VPNサーバに登録する自側情報（ユーザID）に使用されます。

[操作] ルータ設定「動的VPN情報」→[クライアント関連情報]→[ドメイン情報]→[追加]

<u>動的VPN情報 - クライアント関連情報 - ドメイン情報(0)</u>	
<u>基本情報</u>	<u>自側ネットワーク情報</u>

31.2.2.1 基本情報

[操作] ルータ設定「動的VPN情報」→[クライアント関連情報]→[ドメイン情報]→[追加]
→[基本情報]

■ 基本情報		
ドメイン名	<input type="text"/>	
サーバ情報	アドレス	<input type="text"/>
	ポート番号	5070
	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
セカンダリサーバ情報	アドレス	<input type="text"/>
	ポート番号	5070
	認証ID	<input type="text"/>
	認証パスワード	<input type="text"/>
有効期間	1 時間	
優先度	10	
セッション更新間隔	<input checked="" type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間 <input type="text"/> 分	
クライアントIPアドレス	<input type="text"/>	
VPN通信	利用インターフェース	lan0
	中継ルータアドレス	<input type="text"/> <small>※LANインターフェース選択時のみ指定してください。</small>
	終端グローバルアドレス	<input type="text"/>
経路情報の優先度	IPv4 1	
	IPv6 1	
自側ユーザID	<input type="text"/>	
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

ドメイン名

ドメイン名を80文字以内で指定します。

ドメイン名は、動的VPNサーバに登録する自側情報
(ユーザID)に使用されます。

サーバ情報／セカンダリサーバ情報

アドレス

動的VPNサーバのアドレスを指定します。

- IP アドレスを指定する場合
有効範囲)
1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

- FQDN 指定する場合
FQDN を 80 文字以内で設定します。

なお、RFC1034 では英数字、"-" (ハイフン)、"." (ピリオド) でドメイン名をつけることを推奨しています。

こんな事に気をつけて

FQDN 指定する場合は、クライアントIPアドレスのアドレスファミリに従って IP アドレスを取得します。

ポート番号

動的VPNサーバが要求を受信するポート番号を 10 進数を使用して、1 ~ 65535 の範囲で指定します。省略時は、5070 が指定されます。

認証 ID

動的VPNサーバへ自装置情報を登録するときに使用する認証 ID を 50 文字以内の文字列で指定します。

認証パスワード

動的VPNサーバへ自装置情報を登録するときに使用する認証パスワードを 50 文字以内の文字列で指定します。

有効期間

動的VPNサーバに登録する自装置の有効期間を 90 ~ 86400 秒の範囲で指定します。省略時は、1 時間が指定されます。

優先度

動的VPN クライアントを冗長構成にした場合の優先度を選択します。

セッション更新間隔

確立した動的VPN セッションを更新する時間を 90 ~ 3600 秒の範囲で指定します。省略時は、5 分が指定されます。

"更新しない" を選択した場合、確立した動的VPN セッションを更新しません。動的VPN セッションを更新しない場合、動的VPN 接続で確立した IPsec/IKE セッションを継続することが可能になりますが、回線障害などにより動的VPN セッションが残ってしまうことがあるので通常は、セッション更新間隔を利用してください。

クライアントIPアドレス

クライアントの IP アドレスを指定します。

クライアントの IP アドレスは、動的VPN サーバとの通信および相手動的VPN クライアントとの情報交換に使用されます。

動的VPN サーバおよび相手動的VPN クライアントとの通信が IPsec 対象となる場合は、IPsec 対象範囲に含まれるインターフェースの IP アドレスを指定してください。

IPsec 対象とならない場合は、送出インターフェースとなるインターフェースの IP アドレスを指定してください。

有効範囲)

1.0.0.1 ~ 126.255.255.254
128.0.0.1 ~ 191.255.255.254
192.0.0.1 ~ 223.255.255.254
::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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場合は、上位を "dhcp@インターフェース名" の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で指定します。インターフェース名には IPv6 DHCP クライアント機能が動作している rmt インタフェースを指定してください。

VPN 通信

利用インターフェース／中継ルータアドレス

動的VPN として接続される IPsec トンネルが通信に利用するインターフェースを指定します。

lan インタフェースを利用する場合は、中継ルータアドレスを必ず指定してください。

終端グローバルアドレス

相手装置に通知するVPN終端グローバルアドレスを指定します。

省略時に、VPN通信で利用するインターフェースでlanインターフェースを指定した場合は、指定されたlanインターフェースに設定されたアドレス、またはDHCPによりそのインターフェースに割り当てられたアドレスが利用されます。VPN通信で利用するインターフェースでrmtインターフェースを指定した場合は、指定されたrmtインターフェースに設定されたアドレス、またはPPPにより割り当てられたアドレスが利用されます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

経路情報の優先度

動的VPN情報交換で相手から配布されたIPv4またはIPv6経路情報の優先度を指定します。優先度を10進数を使用して、1~254の範囲で指定してください。優先度は数値の小さい方がより高い優先度を示します。

省略時は、1が指定されます。

自側ユーザID

動的VPNサーバに登録する自側ユーザIDを50文字以内で指定します。

使用できる文字は、半角英数字、“-”、“_”、“.”です。

自側ユーザIDは、ドメイン名と結合して以下のように生成されて動的VPNサーバに登録されます。

例) 自側ユーザIDにshisya、ドメイン名にexample.comを指定した場合
shisya@example.com

こんな事に気をつけて

自側ユーザIDは、オペレータの指示で動的VPN接続を行いたい場合に設定してください。

31.2.2.2 自側ネットワーク情報

[操作] ルータ設定「動的VPN情報」→[クライアント関連情報]→[ドメイン情報]→[追加]→[自側ネットワーク情報]

■自側ネットワーク情報

※追加・修正情報は一覧ので設定してください。

定義番号	動的VPNで接続する自側ネットワーク	動的VPNサーバ登録	操作				
	<input type="text"/>	<input type="text"/>	<input type="button" value="削除"/>				
<p><自側ネットワーク情報入力フィールド></p> <table border="1"> <tr> <td>動的VPNで接続する自側ネットワーク</td> <td><input type="text"/> <input type="checkbox"/></td> </tr> <tr> <td>動的VPNサーバ登録</td> <td><input checked="" type="radio"/>する <input type="radio"/>しない</td> </tr> </table> <p><input type="button" value="追加"/> <input type="button" value="キャンセル"/></p>				動的VPNで接続する自側ネットワーク	<input type="text"/> <input type="checkbox"/>	動的VPNサーバ登録	<input checked="" type="radio"/> する <input type="radio"/> しない
動的VPNで接続する自側ネットワーク	<input type="text"/> <input type="checkbox"/>						
動的VPNサーバ登録	<input checked="" type="radio"/> する <input type="radio"/> しない						

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されているド自側ネットワーク情報の定義が表示されています。自側ネットワーク情報の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

動的VPNで接続する自側ネットワーク

動的VPNで接続する自側ネットワークをIPv4アドレスとマスクビット数（またはマスク値）またはIPv6アドレスとプレフィックス長で指定します。

- IPv4 アドレスを指定する場合
IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
デフォルトルートを設定する場合は、
0.0.0.0/0 (0.0.0.0/0.0.0.0) を指定します。
 - IPv6 アドレスを指定する場合
IPv6 アドレスとプレフィックスの組み合わせで指定します。リンクローカルアドレスは指定できません。
デフォルトルートを設定する場合は、
:/0 を指定します。
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場合は、上位を "dhcp@インターフェース名" の形式で指定し、下位 80 ビット分を標準的な IPv6 アドレス表記方式で入力します。インターフェース名には、IPv6 DHCP クライアント機能が動作している rmt インターフェースを指定してください。

こんな事に気をつけて

動的VPNで接続する自側ネットワークは、「テンプレート情報」-動的VPN関連「自側ネットワーク情報」の“動的VPNで接続する自側ネットワーク”と重複して指定することはできません。

動的 VPN サーバ登録

自側ネットワークを自側ユーザIDとして動的VPNサーバ登録する場合は、“する”を選択します。

“する”を選択した場合、通信パケット契機で動的VPN接続することができます。

“しない”を選択した場合、「基本情報」の自側ユーザIDの指定がされていれば、オペレータの指示で動的VPN接続することができます。

通常は、動的VPNサーバに登録してください。

動的VPNサーバに登録する場合は、自側ネットワークと
ドメイン名と結合して以下のように生成されて登録され
ます。

例) 自側ネットワークに 192.168.1.0/24 (2001:db8:1111:1::/
64)、ドメイン名に example.com を指定した場合
IPsecIKE)c0a80100/24@example.com
IPsecIKE)20010db81111000100000000000000000000/
64@example.com

32 SIP-SIP ゲートウェイ情報

適用機種 全機種

[操作] ルータ設定「SIP-SIP ゲートウェイ情報」

SIP-SIP ゲートウェイ情報

[基本情報](#)

[内線情報](#)

[外線情報](#)

32.1 基本情報

[操作] ルータ設定「SIP-SIP ゲートウェイ情報」 → [基本情報]

■ 基本情報

SIP-SIP ゲートウェイ機能 使用しない 使用する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

[保存](#) [キャンセル](#)

SIP-SIP ゲートウェイ機能

本装置を SIP-SIP ゲートウェイとして使用する場合は、“使用する”を選択します。

32.2 内線情報

[操作] ルータ設定「SIP-SIP ゲートウェイ情報」→ [内線情報]

■内線情報		
サービス情報	サービス種別	IP PathfinderおよびCLシリーズ
	ユーザ名	<input type="text"/>
	認証ユーザ名	<input type="text"/>
	認証パスワード	<input type="password"/>
	着信転送先ユーザ名	<input type="text"/>
プライマリ Proxyサーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
セカンダリ Proxyサーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
バックアップ Proxyサーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
ユーザエージェント情報	自IPアドレス	<input type="text"/>
	サービスドメイン名	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

サービス情報

ユーザ名

ユーザ名を32文字以内の文字列で指定します。

認証ユーザ名

認証に使用するユーザ名を32文字以内の文字列で指定します。省略時は、認証を行いません。

認証パスワード

認証に使用するパスワードを32文字以内の文字列で指定します。省略時は、パスワードなしで認証を行います。

着信転送先ユーザ名

ユーザ名を32文字以内の文字列で指定します。

Proxy サーバ情報（プライマリ／セカンダリ／バックアップ）

使用する Proxy サーバの情報を設定します。

IP アドレス

Proxy サーバの IP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

ポート番号

Proxy サーバのポート番号を、1～65535 の範囲の10進数で指定します。省略時は、5060 が設定されます。

ユーザエージェント情報

ユーザエージェントの情報を設定します。

自 IP アドレス

ユーザエージェントの自 IP アドレスを指定します。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

サービスドメイン名

サービスドメイン名を、90文字以内の文字列で指定します。なお、RFC1034 では英数字、"-" (ハイフン)、"." (ピリオド) でドメイン名をつけることを推奨しています。

32.3 外線情報

[操作] ルータ設定「SIP-SIP ゲートウェイ情報」→ [外線情報]

■外線情報		
サービス情報	サービス種別	ひかり電話ビジネスタイプ
	ユーザ名	<input type="text"/>
	認証ユーザ名	<input type="text"/>
	認証パスワード	<input type="password"/>
Registrar サーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
プライマリ Proxyサーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
セカンダリ Proxyサーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
バックアップ Proxyサーバ情報	IPアドレス	<input type="text"/>
	ポート番号	5060
ユーザエージェント情報	自IPアドレス	<input type="text"/>
	サービスドメイン名	<input type="text"/>

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

サービス情報

ユーザ名

ユーザ名を32文字以内の文字列で指定します。ひかり電話ビジネスタイプの場合、IP電話番号（0AJ番号）を設定してください。

認証ユーザ名

認証に使用するユーザ名を32文字以内の文字列で指定します。省略時は、認証を行いません。

認証パスワード

認証に使用するパスワードを32文字以内の文字列で指定します。省略時は、パスワードなしで認証を行います。

Registrar サーバ情報

Registrar サーバの情報を設定します。

IP アドレス

Registrar サーバのIP アドレスを指定します。省略時は、Registrar サーバへの登録は行われません。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

ポート番号

Registrar サーバのポート番号を1~65535の範囲の10進数で指定します。省略時は、5060が設定されます。

Proxy サーバ情報（プライマリ ／セカンダリ／バックアップ）

使用する Proxy サーバの情報を設定します。

IP アドレス

Proxy サーバの IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

ポート番号

Proxy サーバのポート番号を、1 ~ 65535 の 10 進数で指定します。省略時は、5060 が設定されます。

ユーザエージェント情報

ユーザエージェントの情報を設定します。

自 IP アドレス

ユーザエージェントの自 IP アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

サービスドメイン名

サービスドメイン名を、90 文字以内の文字列で指定します。なお、RFC1034 では英数字、"-" (ハイフン)、"." (ピリオド) でドメイン名をつけることを推奨しています。

33 SNMP 情報

適用機種 全機種

[操作] ルータ設定「SNMP 情報」

SNMP情報		
基本情報	SNMPv1/v2c情報	SNMPv3情報
トラップ情報		

33.1 基本情報

[操作] ルータ設定「SNMP 情報」 → [基本情報]

■基本情報	
SNMPエージェント機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する <input type="radio"/> 使用する(旧バージョン互換MIBモード)
機器管理者	<input type="text"/>
機器名称	装置名称を使用する <small>(装置名称情報が設定されていないため選択できません)</small> <input checked="" type="radio"/> 指定する <input type="text"/> 機器名称
機器設置場所	<input type="text"/>
エージェントアドレス	<input type="text"/>
エンジンID	<input type="text"/>
設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。 <input type="button"/> 保存 <input type="button"/> キャンセル	

SNMP エージェント機能

SNMP エージェント機能を使用すると、SNMP ホストの動作しているほかのシステムから本装置の状態を監視できます。SNMP エージェント機能を使用する場合は“使用する”または“使用する（旧バージョン互換 MIB モード）”を選択し、以下の項目を設定します。

こんな事に気をつけて

“使用する”から“使用しない”に設定を変更した場合は、定義されているすべての SNMP 情報が削除されます。

機器名称

機器名称として装置名称を使用する場合は、“装置名称を使用する”を選択します。“指定する”を選択した場合は、本装置の名称を 32 文字以内で指定します。省略時は、機器名称を設定しないものとみなされます。

機器設置場所

本装置の設置場所を 72 文字以内で指定します。省略時は、機器設置場所を設定しないものとみなされます。

機器管理者

本装置の管理者名を 40 文字以内で指定します。省略時は、機器管理者名を設定しないものとみなされます。

エージェントアドレス

SNMP エージェントの IP アドレスを指定します。省略時は、エージェントアドレスを設定しないものとみなされます。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

エンジンID

SNMPv3 の SNMP エンジン ID を 27 文字以内で指定します。省略時は、エンジン ID を自動生成します。

装置に設定される SNMP エンジン ID の値は、以下のとおりです。

- 設定した場合
 - 第1～5オクテット : 0x800000d304 固定
 - 第6オクテット以降 : 本設定のエンジン ID
- 省略した場合
 - 第1～5オクテット : 0x800000d380 固定
 - 第6オクテット以降 : ランダム値

33.2 SNMPv1/v2c 情報

[操作] ルータ設定「SNMP 情報」→ [SNMPv1/v2c 情報]

■SNMPv1/v2c情報	
SNMPホスト1	<input checked="" type="radio"/> publicとする(任意のホストを対象とする) <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト2	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト3	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト4	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト5	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト6	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMPホスト7	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名: <input type="text"/> IPアドレス: <input type="text"/> トрап: <input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2 書き込み要求: <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する

SNMPホスト8

指定しない
 指定する

コミュニティ名	<input type="text"/>
IPアドレス	<input type="text"/>
トラップ	<input checked="" type="radio"/> 送信しない <input type="radio"/> V1 <input type="radio"/> V2
書き込み要求	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル** **削除**

SNMP ホスト

SNMPによるアクセスを許可するホストを設定します。ホストは8個まで定義できます。“publicとする”を選択すると、コミュニティ名“public”で任意のホストからのアクセスを許可します。コミュニティ名を変える場合やホストを限定する場合は、“指定する”を選択し、コミュニティ名・IPアドレス・トラップ・書き込み要求を指定します。

コミュニティ名

SNMPにより情報交換するグループのコミュニティ名を32文字以内で指定します。

IP アドレス

SNMPによるアクセスを許可するホストのIPアドレスを指定します。“0.0.0.0”を指定すると、任意のホストからのアクセスを許可します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

トラップ

このSNMPホストに対してSNMPv1トラップを送信する場合は、“V1”を、SNMP v2トラップを送信する場合は、“V2”を選択します。

ただし、任意のホスト(0.0.0.0)を指定している場合は、トラップの送信は行われません。

書き込み要求

このSNMPホストから書き込み要求を許可する場合は、“許可する”を選択します。

ただし、任意のホスト(0.0.0.0)を指定している場合は、書き込み要求は許可されません。

33.3 SNMPv3 情報

[操作] ルータ設定「SNMP 情報」→ [SNMPv3 情報]

SNMP情報	
SNMPv3情報	
ユーザ情報	MIBビュー情報

33.3.1 ユーザ情報

[操作] ルータ設定「SNMP 情報」→ [SNMPv3 情報] → [ユーザ情報]

定義番号	ユーザー名	SNMPホストアドレス	トラップ通知ホストアドレス	セキュリティプロトコル	MIBビュー MIB書き込み MIB読み出し トラップ通知	操作	
						修正	削除
1						修正	削除
2						修正	削除
3						修正	削除
4						修正	削除
5						修正	削除
6						修正	削除
7						修正	削除
8						修正	削除
全削除							

保存した情報は、設定反映後に有効になります。

現在、設定されている SNMPv3 情報が表示されています。SNMPv3 情報は、装置全体で 8 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「SNMP 情報」→[SNMPv3 情報]→[ユーザ情報]→[修正]

ユーザ名			
ホストアドレス	SNMPホスト	トラップ通知ホスト	
セキュリティ	認証プロトコル	認証なし	
	認証パスワード		
	暗号プロトコル	暗号なし	
	暗号パスワード		
MIBビュー	MIB書き込み	<input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する	
	MIB読み出し	<input checked="" type="radio"/> 許可する <input type="radio"/> 許可しない <input type="radio"/> MIBビュー情報を使用	
	トラップ通知	<input checked="" type="radio"/> 許可する <input type="radio"/> 許可しない <input type="radio"/> MIBビュー情報を使用	
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>			

ユーザ名

SNMPv3のSNMPユーザ名を32文字以内で指定します。
SNMPv3機能を使用する場合は、必ず設定してください。

ホストアドレス

SNMPv3によるアクセスを許可するホストのIPアドレスとトラップを通知するホストのIPアドレスを指定します。アクセスを許可するホストのIPアドレスとトラップを通知するホストのIPアドレスは、装置全体で合わせて8個まで定義できます。省略時は、ホストアドレスを設定しないものとみなされます。

有効範囲)

1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

セキュリティプロトコル

認証プロトコル

SNMPv3による認証プロトコルを選択します。

“認証なし”を選択した場合、認証プロトコルは使用されません。

認証パスワード

SNMPv3による認証プロトコルで使用する、認証パスワードを以下の範囲の文字列で指定します。

認証プロトコル	パスワード長
MD5	8～16 文字
SHA	8～20 文字

認証プロトコルに“認証なし”を選択した場合は、省略できます。

暗号プロトコル

SNMPv3による暗号プロトコルを選択します。

“暗号なし”を選択した場合、暗号プロトコルは使用されません。また、暗号プロトコルを指定した場合は、認証プロトコルを指定してください。

暗号パスワード

SNMPv3による暗号プロトコルで使用する、暗号パスワードを以下の範囲の文字列で指定します。

暗号プロトコル	パスワード長
DES	8～16文字

暗号プロトコルに“暗号なし”を選択した場合は、省略できます。

MIB ビュー

MIB 書き込み

SNMPv3によるMIB書き込みのアクセス権を許可する場合は、“許可する”を選択します。

MIB 読み出し

SNMPv3によるMIB読み出しのアクセス権を許可する場合は、“許可する”を選択します。

“MIB ビュー情報を参照”を選択した場合は、必ずビュー定義番号を指定してください。

トラップ通知

SNMPv3によるトラップ通知のアクセス権を許可する場合は、“許可する”を選択します。

“MIB ビュー情報を参照”を選択した場合は、必ずビュー定義番号を指定してください。

ビュー定義番号

[MIB ビュー情報参照] をクリックして、ビュー定義番号を指定します。

指定する定義番号欄の [選択] ボタンをクリックし、ビュー定義番号を設定します。自動的に画面が閉じます。

なお、参照するビュー定義が存在しない場合は、「参照可能なMIB ビュー情報が存在しません」が表示されます。

[OK] ボタンをクリックして、設定をやり直してください。

[操作] ルータ設定「SNMP 情報」→[SNMPv3 情報]→[ユーザ情報]→[修正]
→「ビュー定義番号の [MIB ビュー情報参照]」

■MIB ビュー情報			
定義番号	MIB ビュー情報	ビュータイプ	操作
0	tcp udp snmp noserror	含む 含む 含む 除く	[選択]

「MIB ビュー情報」 - [追加] / [修正] で設定したMIB ビュー定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

参照するビュー定義が存在しない場合は、「参照可能なMIB ビュー情報が存在しません」が表示されます。[OK] ボタンをクリックして、設定をやり直してください。

「ユーザ情報」のMIB ビュー定義番号に設定する定義番号欄の [選択] ボタンをクリックすると、「ユーザ情報」にビュー定義番号が設定され、画面が閉じます。

33.3.2 MIB ビュー情報

[操作] ルータ設定「SNMP 情報」→ [SNMPv3 情報] → [MIB ビュー情報]

■MIBビュー情報

定義番号	サブツリー名	ビュータイプ	操作
<input type="button" value="全削除"/>			
<MIBビュー定義追加フィールド>			
ビュー定義番号	<input type="text" value="0"/>	<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

保存した情報は、設定反映後に有効になります。設定を元に戻す場合はキャンセルをクリックしてください。

現在、設定されているMIBビュー情報の定義が表示されています。MIBビュー情報は、装置全体で8個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「SNMP 情報」 → [SNMPv3 情報] → [MIB ビュー情報] → [追加]

サブツリー名

MIB ビュー対象とするサブツリー名を選択します。

同じビュー定義番号を持つMIBビュー情報の設定で、同一サブツリー名を複数選択した場合、最初に選択したサブツリー情報が有効となります。

ビュータイプ

選択したサブツリー名をMIBビューに含むか、それとも
除外かを指定します。

33.4 トラップ情報

[操作] ルータ設定「SNMP 情報」→ [トラップ情報]

■トラップ情報	
coldStart	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
linkDown	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
linkUp	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
authenticationFailure	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
newRoot	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
topologyChange	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
vrrpTrapNewMaster	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
vrrpTrapAuthFailure	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
vrrpTrapProtoError	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
nosError	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする
lldpRemTablesChange	<input checked="" type="radio"/> 有効にする <input type="radio"/> 無効にする

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

トラップ情報

以下の各トラップを有効にするか無効にするかを選択します。

- coldStart
本装置の起動時および再起動時に1回だけ通知します。
- linkDown
本装置の通信リンクに障害があったときに通知します。また、装置の再起動時や構成定義反映時にも送信される場合があります。
- linkUp
本装置の通信リンクの中のどれかがUP状態になったときに通知します。
- authenticationFailure
SNMPの認証失敗時に通知します。
- newRoot
本装置がルートブリッジになるときに通知します。
- topologyChange
本装置がブリッジネットワークの構成変更を検出したとき、つまりラーニング状態からフォワーディング状態に、またはフォワーディング状態からブロッキング状態に変更するときに通知します。
- vrrpTrapNewMaster
本装置がVRRPグループでマスタとなったときに通知します。
- vrrpTrapAuthFailure
本装置で受信したVRRP-ADメッセージの認証方法が異常、またはVRRPグループに設定された認証方法やパスワードが一致しないときに通知します。

- vrrpTrapProtoError
本装置で受信したVRRP-ADメッセージがプロトコルエラーであったときに通知します。

- nosError
本装置になんらかの異常（ハードウェア異常）が発生したときに通知します。このトラップは異常が発生したことだけを通知します。

- lldpRemTablesChange
隣接装置情報管理テーブルに変化があったときに通知します。

34 ProxyDNS 情報／URL フィルタ情報

適用機種 全機種

[操作] ルータ設定「ProxyDNS 情報 URL フィルタ情報」

ProxyDNS情報／URLフィルタ情報

共通情報 順引き情報 逆引き情報

このページではProxyDNSとURLフィルタの設定ができます。URLフィルタは順引き情報で設定します。



◆ 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
パソコンに本装置の IP アドレスを DNS サーバとして登録しておくと、接続先によって問い合わせる DNS サーバを自動的に切り替えます。
- DNS サーバ機能
ホストデータベース情報にホスト名と IP アドレスのペアを登録しておくと、ProxyDNS は該当ホスト名へのアクセスを登録された IP アドレスへのアクセスとして切り替えます。
- URL フィルタ機能
特定のドメイン名（範囲指定も可）へのアクセスを禁止することができます。この機能は順引き情報設定で設定します。
- DNS 問い合わせタイプフィルタ機能
送信元 IP アドレス範囲から送信される特定の問い合わせタイプの DNS パケットを破棄することができます。この機能は順引き情報設定で設定します。

34.1 共通情報

[操作] ルータ設定「ProxyDNS 情報 URL フィルタ情報」→ [共通情報]

■共通情報	
非表示文字を含む要求の転送	<input type="radio"/> 透過する <input checked="" type="radio"/> 破棄する
複数DNSサーバ問い合わせ	<input type="radio"/> 利用する <input checked="" type="radio"/> 利用しない

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

非表示文字を含む要求の転送

DNS問い合わせ名 (QNAME) に非表示文字が含まれる場合に、その問い合わせのパケットを透過するか破棄するかを選択します。

複数 DNS サーバ問い合わせ

DNS問い合わせを転送する場合に、複数 DNS サーバに対して問い合わせを行うかどうかを選択します。

- 利用する
利用できる複数の DNS サーバすべてに問い合わせを転送します。
- 利用しない
プライマリ DNS サーバにのみ問い合わせを転送します。

34.2 順引き情報

[操作] ルータ設定「ProxyDNS 情報 URL フィルタ情報」→ [順引き情報]

■順引き情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	ドメイン名	動作	DNSサーバアドレス／ネットワーク名／インターフェース名	操作
	タイプ		送信元IPアドレス	経路自動作成

全削除

<順引き情報入力フィールド>

ドメイン名	<input type="text"/>
タイプ	すべて <input type="button" value="番号指定"/> “その他”を選択時ののみ有効です。 <input type="checkbox"/>
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	<ul style="list-style-type: none"> <input checked="" type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 <input type="button" value="rmt0"/> <input type="radio"/> 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 <input type="button" value="rmt0"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/>しない <input type="radio"/>する <input type="radio"/> DHCPクライアントが取得したDNSサーバへ問い合わせる インターフェース名 <input type="button" value="使用できるインターフェースが存在しません"/> <input type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス <input type="text"/>

追加 **キャンセル**

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

順引き情報はドメイン名により DNS サーバを切り替える範囲を指定する場合、特定のドメイン名へのアクセスを禁止する場合、送信元 IP アドレス範囲からの特定の問い合わせタイプの DNS パケットを破棄する場合など、ドメイン名・問い合わせタイプ・送信元 IP アドレスの組み合わせによりいろいろな使い方ができます。定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

ドメイン名

対象とするドメイン名の範囲を 80 文字以内で指定します。ただし、以下のように、 "*" および "?" はワイルドカードとして使用されるため、ドメイン名には使用できません。なお、ドメイン名のチェックには大文字／小文字の区別はありません。

"*" : 0 文字以上の任意の文字に一致する

"?" : 1 文字の任意文字に一致する

記述例)

条件	一致
www.*.com	www.testa.com、www.test1.test.com
test	www.test.com、test.com、test.co.jp
www.test? .com	www.test1.com、www.test2.com、www.testA.com

タイプ

対象とする問い合わせタイプを以下から選択します。() 内はタイプの番号です。

- すべて (PTR (12) を除く)
- A (1)
- NS (2)
- CNAME (5)
- SOA (6)
- HINFO (13)
- MX (15)
- AAAA (28)
- SRV (33)
- その他

任意のタイプを指定する場合は、“その他”を選択し、10進数を使用して、1～11、13～65535 の範囲で指定します。

送信元 IP アドレス

フィルタリング条件としての送信元 IP アドレスを IPv4 アドレス／ネットマスク、または IPv6 アドレス／プレフィックスの形式で設定します。

0.0.0.0/0、::/0 を指定した場合、または、省略した場合は、すべてのアドレスを対象とするものとして動作します。

動作

対象ドメイン、問い合わせタイプ、送信元 IP アドレスに対する動作を以下の4つから選択します。

- 廃棄する
該当ドメインの転送を無効にするフィルタ (URL フィルタ) または、該当問い合わせタイプの DNS パケットの転送を無効にするフィルタ (問い合わせタイプ フィルタ) として利用します。
- 接続先の DNS サーバへ問い合わせる
接続先情報で設定された DNS サーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
- 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
接続先情報で設定した DNS サーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
“接続先の DNS サーバへ問い合わせる”との違いは、必ず指定したネットワークを経由して DNS サーバへ問い合わせることです。また、解決したホストへのホスト経路自動作成に “する” を選択することにより、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。
- DHCP クライアントが取得した DNS サーバへ問い合わせる
DHCP クライアントが取得した DNS サーバへ問い合わせます。DHCP クライアントが動作しているインターフェース名を指定してください。
- 設定した DNS サーバへ問い合わせる
特定の DNS サーバへ問い合わせます。問い合わせる DNS サーバの IPv4/IPv6 アドレスを指定します。

有効範囲)

1.0.0.1 ~ 126.255.255.254

128.0.0.1 ~ 191.255.255.254

192.0.0.1 ~ 223.255.255.254

::2 ~ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff

fec0:: ~ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

34.3 逆引き情報

[操作] ルータ設定「ProxyDNS 情報 URL フィルタ情報」→ [逆引き情報]

■逆引き情報

※追加・修正情報は一覧の入力フィールドで設定してください。

優先順位	ネットワークアドレス	動作	DNSサーバアドレス／ネットワーク名／インターフェース名 経路自動作成	操作

全削除

<逆引き情報入力フィールド>

すべて
(指定する)を選択時ののみ有効です。)

ネットワークアドレス

※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
- 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

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

インターフェース名
- 設定したDNSサーバへ問い合わせる

DNSサーバアドレス

追加 **キャンセル**

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

逆引き情報はIP アドレスにより DNS サーバを切り替える範囲を指定する場合に使用します。定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。ただし、分割されたパケットに対しては正しく扱えません。

ネットワークアドレス

対象とするネットワークアドレスを以下の4つから選択します。

- すべて
IPv4 と IPv6 両方を選択します。
- IPv4 すべて
IPv4 アドレスをすべて選択します。
- IPv6 すべて
IPv6 アドレスをすべて選択します。
- 指定する
IPv4 アドレス/ネットマスクまたはIPv6 アドレス/プレフィックスの形式で指定します。

動作

対象ドメインに対する動作を以下の3つから選択します。

- 廃棄する
該当ネットワークの転送を無効にするフィルタを指定します。
- 接続先のDNSサーバへ問い合わせる
接続先情報で設定されたDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
接続先情報で設定したDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
“接続先のDNSサーバへ問い合わせる”との違いは、必ず指定したネットワークを経由してDNSサーバへ問い合わせることです。また、解決したホストへのホスト経路自動作成に“する”を選択することにより、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。
- DHCPクライアントが取得したDNSサーバへ問い合わせる
DHCPクライアントが取得したDNSサーバへ問い合わせます。DHCPクライアントが動作しているインターフェース名を指定してください
- 設定したDNSサーバへ問い合わせる
特定のDNSサーバへ問い合わせます。問い合わせるDNSサーバのIPv4/IPv6アドレスを指定します。
有効範囲)
1.0.0.1～126.255.255.254
128.0.0.1～191.255.255.254
192.0.0.1～223.255.255.254
.::2～fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0::～feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

35 ホストデータベース情報

適用機種 全機種

[操作] ルータ設定「ホストデータベース情報」

ホストデータベース情報					
<u>1~16</u>		<u>17~32</u>		<u>33~48</u>	
<u>49~64</u>		全表示			

[操作] ルータ設定「ホストデータベース情報」 → [全表示]

■ホストデータベース情報					
	ホスト名	IPv4アドレス	MACアドレス	電源制御	操作
		IPv6アドレス	DUID		
1	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
2	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
3	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
4	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
5	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
60	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
61	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
62	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
63	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
64	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>
	-	-	-	-	<input type="button" value="修正"/> <input type="button" value="削除"/>

保存した情報は、設定反映後に有効になります。

登録しているホストデータベース情報の定義が表示されています。ホストデータベースの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

[操作] ルータ設定「ホストデータベース情報」 → [修正]

ホスト名	<input type="text"/>
IPv4アドレス	<input type="text"/>
IPv6アドレス	<input type="text"/>
MACアドレス	<input type="text"/>
DUID	<input type="text"/>
リモート電源制御	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
<input type="button" value="保存"/> <input type="button" value="キャンセル"/> <input type="button" value="一覧へ戻る"/>	



◆ ホストデータベースには以下の機能があります。

- DNS サーバ機能
「ホスト名」「IPv4 アドレス」または「IPv6 アドレス」のペアを登録することにより、ProxyDNS の DNS サーバ機能を使用することができます。
- リモートパワーオン機能
「MAC アドレス」を登録することにより、Wakeup on LAN 機能を使用することができます。
- IPv4 DHCP スタティック機能
「IPv4 アドレス」「MAC アドレス」のペアを登録することにより、DHCP で割り当てられる IPv4 アドレスを端末固有のものとすることができます。
- IPv6 DHCP スタティック機能
「IPv6 アドレス」「DUID」のペアを登録することにより、IPv6 DHCP で割り当てられる IPv6 アドレスを端末固有のものとすることができます。

ホスト名

DNS サーバ機能で使用されます。80 文字以内で指定します。使用できる文字は半角英数字、"、"-”です。他の記号は使用できません。

IPv4 アドレス

DNS サーバ機能および IPv4 DHCP スタティック機能で使用されます。

IPv6 アドレス

DNS サーバ機能および IPv6 DHCP スタティック機能で使用されます。

MAC アドレス

IPv4 DHCP スタティック機能およびリモートパワーオン機能で使用されます。MAC アドレスは以下の形式で指定します。

xx:xx:xx:xx:xx:xx (xx は 2 衔の 16 進数)

DUID

IPv6 DHCP スタティック機能で使用されます。260 衔以内の 16 進数で表記した DUID を指定します。

電源制御（リモート電源制御）

本装置と同じセグメントに存在する Wakeup on LAN 対応機器を、リモートパワーオン指示の対象とする場合は、“対象”を選択します。

この設定はスケジュール機能や手動操作でリモートパワーオンを指示する場合に使用されます。

36 証明書関連情報

適用機種 全機種

[操作] ルータ設定「証明書関連情報」

証明書関連情報

自装置証明書情報	相手装置証明書情報	認証局証明書情報
----------	-----------	----------

このページでは証明書関連情報を設定することができます。上記の各関連項目をクリックすると詳細な設定項目が表示されます。

36.1 自装置証明書情報

[操作] ルータ設定「証明書関連情報」 → [自装置証明書情報]

証明書関連情報

自装置証明書情報	相手装置証明書情報	認証局証明書情報
----------	-----------	----------

自装置証明書要求の作成(鍵ペアの作成) 自装置証明書の設定

36.1.1 自装置証明書要求の作成（鍵ペアの作成）

[操作] ルータ設定「証明書関連情報」 → [自装置証明書情報]
→ [自装置証明書要求の作成（鍵ペアの作成）]

■自装置証明書要求の作成(鍵ペアの作成)

※追加・再作成は一覧ので設定してください。

鍵ペア識別番号	操作
<input type="button" value="全削除"/>	
<鍵ペア情報入力フィールド>	
鍵長	<input type="text" value="bit"/>
証明書要求で使用するハッシュアルゴリズム	<input checked="" type="radio"/> md5 <input type="radio"/> sha1
国名(C)	<input type="text" value="JP"/>
都道府県(ST)	<input type="text"/>
市区町村(L)	<input type="text"/>
組織または会社名(O)	<input type="text"/>
組織ユニットまたは部門(OU)	<input type="text"/>
ホスト名(CN)	<input type="text"/>
メールアドレス	<input type="text"/>
ドメイン名(DN)	<input type="text"/>
IPアドレス(IP)	<input type="text"/>
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>	

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている証明書要求情報が表示されています。証明書要求数は、仕様一覧 [\[2.3 システム最大値一覧\]\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

鍵長

RSA 鍵ペアの鍵長を 361～2048 の範囲の 10 進数で指定します。

証明書要求で使用するハッシュアルゴリズム

証明書要求に使用するハッシュアルゴリズムを選択します。

国名 (C)

自装置証明書を作成する情報の国名を、0x41～0x5a、0x61～0x7a の範囲のコードで構成される 2 文字の ASCII 文字列で指定します。

省略時は、自装置証明書に国名 (C) の設定は行いません。

都道府県 (ST)

自装置証明書を作成する情報の都道府県を、0x2f (スラッシュ) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

省略時は、自装置証明書に都道府県 (ST) の設定は行いません。

市区町村 (L)

自装置証明書を作成する情報の市区町村を、0x2f (スラッシュ) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

省略時は、自装置証明書に市区町村 (L) の設定は行いません。

組織または会社名 (O)

自装置証明書を作成する情報の組織または会社名を、0x2f (スラッシュ) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

省略時は、自装置証明書に組織または会社名 (O) の設定は行いません。

組織ユニットまたは部門 (OU)

自装置証明書を作成する情報の組織ユニットまたは部門を、0x2f (スラッシュ) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

省略時は、自装置証明書に組織ユニットまたは部門 (OU) の設定は行いません。

ホスト名 (CN)

自装置証明書を作成する情報のホスト名を、0x2f (スラッシュ) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

省略時は、自装置証明書にホスト名 (CN) の設定は行いません。

メールアドレス

自装置証明書を作成する情報のメールアドレスを、0x2f (スラッシュ) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。

省略時は、自装置証明書にメールアドレスの設定は行いません。

ドメイン名 (DN)

自装置証明書を作成する情報のサブジェクト代替名称 (DNS 名) を、0x2f (スラッシュ) と 0x40 (アットマーク) を除く 0x21、0x23～0x7e の範囲のコードで構成される 64 文字以内の ASCII 文字列で指定します。DNS 名には英字の大文字と小文字の区別がないため、すべて小文字で設定されます。

省略時は、自装置証明書にドメイン名 (DN) の設定は行いません。

IP アドレス (IP)

自装置証明書を作成する情報のサブジェクト代替名称 (IPv4 アドレス) を指定します。

36.1.2 自装置証明書の設定

[操作] ルータ設定「証明書関連情報」→[自装置証明書情報]→[自装置証明書の設定]

自装置証明書設定方式で、“取り込み”を選択した場合

■自装置証明書の設定

※追加・再設定は一覧ので設定してください。

自装置証明書識別番号	自装置証明書識別名	操作
<input type="button" value="全削除"/>		
<自装置証明書情報入力フィールド>		
自装置証明書識別名	my-cert0.pem	
自装置証明書設定方式	<input checked="" type="radio"/> 取り込み <input type="radio"/> 自己発行	
自装置証明書データ(Base64形式)		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

自装置証明書設定方式で、“自己発行”を選択した場合

■自装置証明書の設定

※追加・再設定は一覧ので設定してください。

自装置証明書識別番号	自装置証明書識別名	操作
<input type="button" value="全削除"/>		
<自装置証明書情報入力フィールド>		
自装置証明書識別名	my-cert0.pem	
自装置証明書設定方式	<input type="radio"/> 取り込み <input checked="" type="radio"/> 自己発行	
鍵ペア識別番号	0	
証明書要求で使用する ハッシュアルゴリズム	<input checked="" type="radio"/> md5 <input type="radio"/> sha1	
自装置証明書の有効期 限	<input type="text"/> 年 <input type="text"/> 月 <input type="text"/> 日	
失効日付		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている自装置証明書の定義が表示されています。自装置証明書の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

自装置証明書識別名

自装置証明書の設定を行うための識別名を、16 文字以内で指定します。

省略時は、自装置証明書識別名の設定は行いません。

自装置証明書設定方式

自装置証明書の設定方式を選択します。

- 取り込み
認証局で発行された自装置証明書を本装置に取り込む場合に選択します。
- 自己発行
自装置証明書を本装置で作成する場合に選択します。

自装置証明書データ（Base64 形式）

Base64 形式の自装置証明書データを指定します。開始行と終了行の間のデータを 100 行までの範囲で指定します。ただし、1 行は 64 文字以内で指定してください。

なお、以下の行は設定に含めません。

開始行：---BEGIN CERTIFICATE---

終了行：---END CERTIFICATE---

鍵ペア識別番号

RSA 鍵ペアの識別番号を、0～4 の範囲の 10 進数で指定します。

証明書要求で使用するハッシュアルゴリズム

自装置証明書に使用するハッシュアルゴリズムを選択します。

自装置証明書の有効期限失効日付

自装置証明書の有効期限失効日付を、1902～2037 年の範囲の西暦で指定します。

ただし、過去の日付や現在の日付は指定できません。

36.2 相手装置証明書情報

[操作] ルータ設定「証明書関連情報」→ [相手装置証明書情報]

証明書関連情報		
自装置証明書情報	相手装置証明書情報	認証局証明書情報
相手装置証明書の設定		

36.2.1 相手装置証明書の設定

[操作] ルータ設定「証明書関連情報」→ [相手装置証明書情報] → [相手装置証明書の設定]

■相手装置証明書の設定

※追加・再設定は一覧ので設定してください。

相手装置証明書識別番号	相手装置証明書識別名	操作
<input type="button" value="全削除"/>		
<相手装置証明書情報入力フィールド>		
相手装置証明書識別名 <input type="text" value="rmt-cert0.pem"/>		
相手装置証明書データ(Base64形式)		
<input type="text"/>		
<input type="button" value="追加"/> <input type="button" value="キャンセル"/>		

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている相手装置証明書の定義が表示されています。相手装置証明書の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

相手装置証明書識別名

相手装置証明書の設定を行うための識別名を、16 文字以内で指定します。

省略時は、相手装置証明書識別名の設定は行いません。

相手装置証明書データ (Base64 形式)

Base64 形式の相手装置証明書データを指定します。開始行と終了行の間のデータを 100 行までの範囲で指定します。ただし、1 行は 64 文字以内で指定してください。

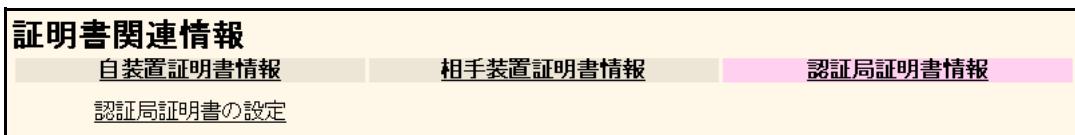
なお、以下の行は設定に含めません。

開始行：—BEGIN CERTIFICATE—

終了行：—END CERTIFICATE—

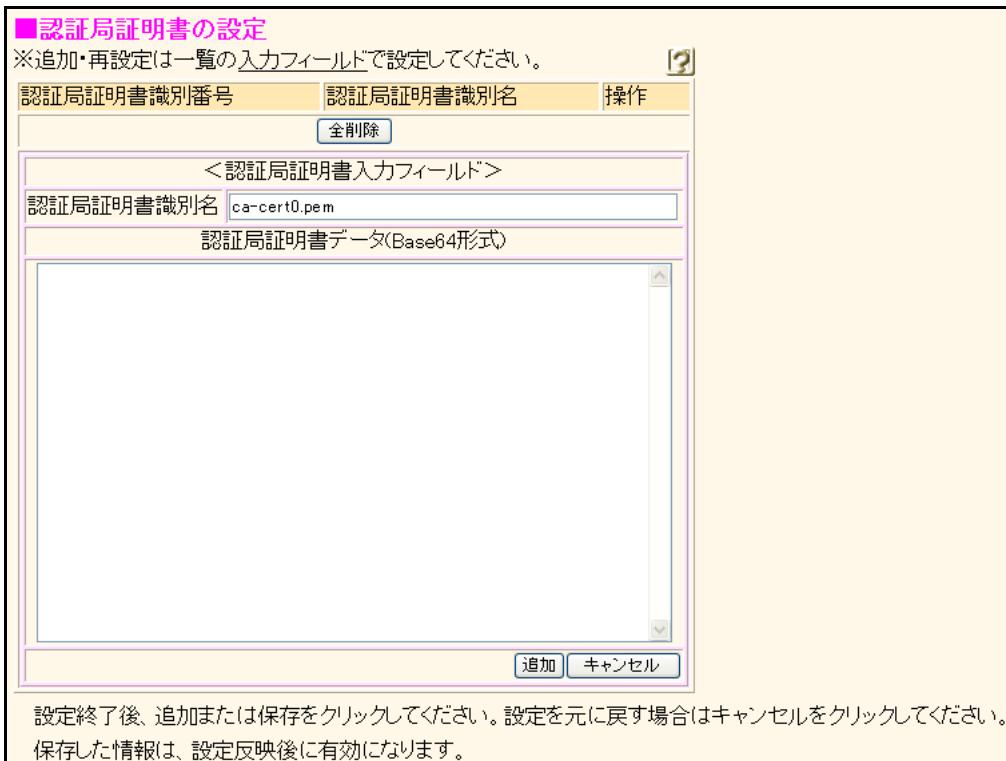
36.3 認証局証明書情報

[操作] ルータ設定「証明書関連情報」→ [認証局証明書情報]



36.3.1 認証局証明書の設定

[操作] ルータ設定「証明書関連情報」→ [認証局装置証明書情報] → [認証局証明書の設定]



現在、設定されている認証局証明書の定義が表示されています。認証局証明書の定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

認証局証明書識別名

認証局証明書の設定を行うための識別名を、16文字以内で指定します。

省略時は、認証局証明書識別名の設定は行いません。

認証局証明書データ (Base64 形式)

Base64 形式の認証局証明書データを指定します。開始行と終了行の間のデータを 100 行までの範囲で指定します。ただし、1 行は 64 文字以内で指定してください。

なお、以下の行は設定に含めません。

開始行：---BEGIN CERTIFICATE---

終了行：---END CERTIFICATE---

37 無線 LAN 管理情報

適用機種 全機種

[操作] 無線 LAN 管理設定「無線 LAN 管理情報」

無線 LAN 管理情報

管理グループ情報 管理機器情報 管理外機器情報

このページでは、無線 LAN 管理に関する情報についての設定ができます。

37.1 管理グループ情報

[操作] 無線 LAN 管理設定「無線 LAN 管理情報」 → [管理グループ情報]

■ 管理グループ情報

※ 追加情報は一覧の最後尾の「[追加](#)」で設定してください。

定義番号	グループ名	操作
		全削除
<管理グループ情報入力フィールド>		
グループ名	Group0	追加 キャンセル

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている管理グループ情報が表示されています。管理グループの定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

アクセスポイント群を管理・監視しやすいように任意のグループとしてまとめることができます。

グループ名

グループを識別するグループ名を8文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

37.2 管理機器情報

[操作] 無線 LAN 管理設定「無線 LAN 管理情報」→ [管理機器情報]

■管理機器情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。

定義番号	管理機器名	グループ	タイプ	IPアドレス	操作
全削除					
<管理機器情報入力フィールド>					
管理機器名	NewAP0				
[追加] [キャンセル]					

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている管理機器の定義が表示されています。管理機器の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

管理機器名

管理機器を識別する管理機器名を8文字以内で指定します。文字列には、0x21および0x23～0x7eのコードで構成されるASCII文字列を指定します。

[操作] 無線 LAN 管理設定「無線 LAN 管理情報」→ [管理機器情報] → [修正]

管理機器情報(0)

[基本情報](#)

37.2.1 基本情報

[操作] 無線 LAN 管理設定「無線 LAN 管理情報」→ [管理機器情報] → [修正] → [基本情報]

■ 基本情報

管理機器名	NewAP1
グループ	▼
IPアドレス	
無線LAN管理パスワード	
無線LAN管理パスワード(確認用)	
監視用	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
無線LAN端末の情報取得	<input checked="" type="radio"/> 情報取得する <input type="radio"/> 情報取得しない
近隣管理機器	▼ ▼ ▼ ▼ ▼

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 キャンセル

管理機器名

管理機器を識別する管理機器名を8文字以内で指定します。文字列には、0x21および0x23～0x7eのコードで構成されるASCII文字列を指定します。

グループ

管理機器が属するグループの定義番号を選択します。
管理機器がグループに属さない場合、空白を指定します。

設定値	意味
空白	管理機器は、グループに属しません。
数値	管理機器が属するグループの定義番号です。

IP アドレス

管理機器のIPv4アドレスを指定します。

指定可能な範囲は以下のとおりです。
有効範囲)
1.0.0.1～126.255.255.254

128.0.0.1～191.255.255.254

192.0.0.1～223.255.255.254

無線 LAN 管理パスワード

管理機器へ無線 LAN 管理でログインするためのパスワードを64文字以内で指定します。文字列には、0x21および0x23～0x7eのコードで構成されるASCII文字列を指定します。

また、入力したパスワードを検証するため、無線 LAN 管理パスワード（確認用）にも同じ値を指定します。

監視用

管理機器を無線 LAN の監視用として使用する場合は、“使用する”を選択します。

こんな事に気をつけて

監視用無線 LAN アクセスポイントは、以下の条件を満たす必要があります。

- 無線 LAN インタフェースの動作タイプが、無線 LAN アクセスポイント、または、スキャン専用モードであること。
- 周辺アクセスポイント検出の動作モードが有効であること。

無線 LAN 端末の情報取得

無線 LAN アクセスポイントに接続された無線 LAN 端末の情報取得を行う場合は、"情報取得する"を選択します。

近隣管理機器

無線 LAN の電波出力自動調整機能を使用する場合に、当該管理機器の無線電波が近隣にある管理機器（無線 LAN アクセスポイント）のうち、どの管理機器で検出させたいかを指定します。

近隣管理機器には、4つまでの管理機器を指定することができます。

近隣管理機器の指定がない場合、当該管理機器は無線 LAN の電波出力自動調整機能の対象から除外されます。

37.3 管理外機器情報

[操作] 無線 LAN 管理設定「無線 LAN 管理情報」→ [管理外機器情報]

■管理外機器情報

※追加情報は一覧の最後尾の「追加」で設定してください。

定義番号	管理外機器名	MACアドレス	操作
<input type="button" value="全削除"/>	<u><管理外機器情報入力フィールド></u>		
管理外機器名	Unmng0		
MACアドレス			<input type="button" value="追加"/> <input type="button" value="キャンセル"/>

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている管理外機器の定義が表示されています。管理外機器の定義数は、仕様一覧「[2.3 システム最大値一覧](#)」(P.43) を参照してください。処理するボタンをクリックし、次のページへ進みます。

使用している場所、目的などが明らかで管理・監視する必要がない機器を設定することができます。

管理外機器名

管理外機器を識別する管理外機器名を8文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

MACアドレス

管理外機器の MAC アドレスを指定します。MAC アドレスは、xx:xx:xx:xx:xx:xx (xx は2桁の16進数) の形式で指定します。

38 MACアドレスフィルタセット情報

適用機種 全機種

[操作] 無線 LAN 管理設定「MACアドレスフィルタセット情報」

MACアドレスフィルタセット情報

MACアドレスフィルタセット情報

■MACアドレスフィルタセット情報

※追加情報は一覧の最後尾の追加フィールドで設定してください。 [?](#)

定義番号	MACアドレスフィルタセット名	定義済フィルタ数	操作
全削除			
<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <MACアドレスフィルタセット情報入力フィールド> </div> <div style="display: flex; align-items: center;"> MACアドレスフィルタセット名 <input type="text" value="FilterSet0"/> 追加 キャンセル </div>			

設定終了後、追加または保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。
保存した情報は、設定反映後に有効になります。

現在、設定されている MAC アドレスフィルタセット情報が表示されています。MAC アドレスフィルタセットの定義数は、仕様一覧 [「2.3 システム最大値一覧」\(P.43\)](#) を参照してください。処理するボタンをクリックし、次のページへ進みます。

MACアドレスフィルタ名

MAC アドレスフィルタを識別する MAC アドレスフィルタセット名を 50 文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。

38.1 MACアドレスフィルタ情報

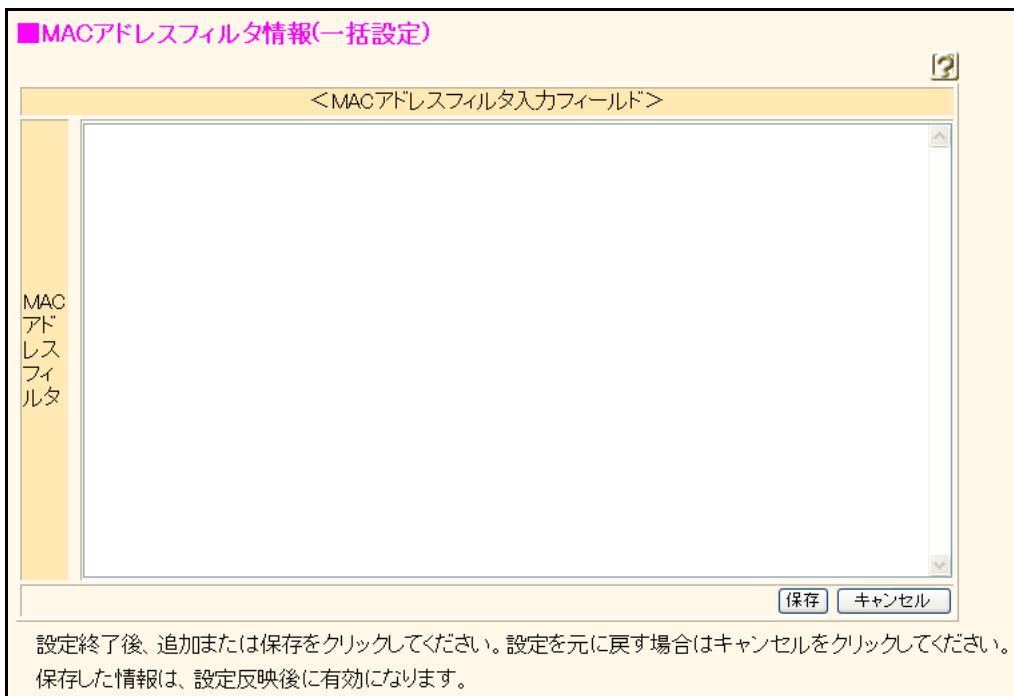
[操作] 無線 LAN 管理設定「MACアドレスフィルタセット情報」 → [追加] → [MACアドレスフィルタ]

MACアドレスフィルタ情報(1)

MACアドレスフィルタ情報

38.1.1 MACアドレスフィルタ情報（一括設定）

[操作] 無線 LAN 管理設定「MACアドレスフィルタセット情報」→ [追加] → [MACアドレスフィルタ]



MACアドレスフィルタ

MACアドレスフィルタセットに設定する MAC アドレス フィルタを一括で指定します。

MACアドレスフィルタは、以下の形式で指定します。

指定の MAC アドレスを許可する場合

MACアドレス,pass,[コメント]

指定の MAC アドレスを拒否する場合

MACアドレス,reject,[コメント]

MACアドレス

個別の MAC アドレスを対象とする場合は、
xx:xx:xx:xx:xx:xx (xx は 2 衔の 16 進数) の 形式で
指定します。

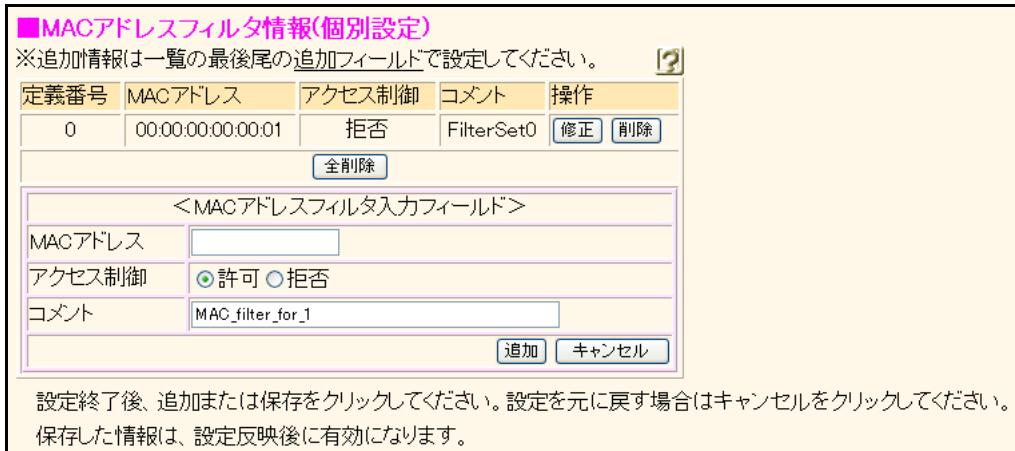
すべての MAC アドレスを対象とする場合は、any
を指定します。

コメント

50 文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字
列を指定します。
省略できます。

38.1.2 MAC アドレスフィルタ情報（個別設定）

[操作] 無線 LAN 管理設定「MAC アドレスフィルタセット情報」→ [追加] → [MAC アドレスフィルタ]
→ [保存]



MAC アドレスフィルタセットに1つ以上の MAC アドレスフィルタが設定されている場合、MAC アドレスフィルタの設定は個別設定で設定します。

MAC アドレス

個別の MAC アドレスを対象とする場合は、
xx:xx:xx:xx:xx:xx (xx は2桁の16進数) の形式で指定します。
すべての MAC アドレスを対象とする場合は、any を指定します。

アクセス制御

管理機器に MAC アドレスフィルタを適用する際の動作を指定します。

- 許可
指定の MAC アドレスが管理機器に繋がることを許可します。
- 拒否
指定の MAC アドレスが管理機器に繋がることを拒否します。

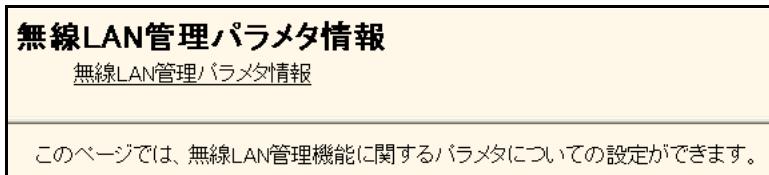
コメント

50 文字以内で指定します。文字列には、0x21 および 0x23～0x7e のコードで構成される ASCII 文字列を指定します。
省略できます。

39 無線 LAN 管理パラメタ情報

適用機種 全機種

[操作] 無線 LAN 管理設定「無線 LAN 管理パラメタ情報」



39.1 無線 LAN 管理パラメタ

[操作] 無線 LAN 管理設定「無線 LAN 管理パラメタ情報」 → [無線 LAN 管理パラメタ]

■ 無線 LAN 管理パラメタ			
管 理	管理情報取得	<input checked="" type="radio"/> しない <input type="radio"/> する 情報取得間隔 <input type="text" value="10"/> 秒 情報取得待機間隔 <input type="text" value="10"/> 秒 情報取得タイムアウト <input type="text" value="5"/> 秒	
	チャネル自動調整	共通	通信帯域幅 <input type="text" value="20"/> MHz
		5GHz帯	割当範囲 <input type="text" value="w52/53/56"/>
		2.4GHz帯	判定用RSSIしきい値 <input type="text" value="20"/> 開始チャネル <input type="text" value="1"/> チャネル割当間隔 <input type="text" value="5"/>
電波出力自動調整		RSSI最低しきい値 <input type="text" value="20"/>	
監 視	有線 LAN	<input checked="" type="radio"/> しない <input type="radio"/> する 稼動監視間隔 <input type="text" value="10"/> 秒 稼動監視待機間隔 <input type="text" value="10"/> 秒 稼動監視タイムアウト <input type="text" value="5"/> 秒 通信異常判定しきい値 <input type="text" value="6"/> 回	
	無線 LAN	<input checked="" type="radio"/> しない <input type="radio"/> する スキャンレポート取得間隔 <input type="text" value="10"/> 秒 スキャンレポート取得待機間隔 <input type="text" value="10"/> 秒 スキャンレポート取得タイムアウト <input type="text" value="5"/> 秒 通信異常判定しきい値 <input type="text" value="6"/> 回	
		無線 LAN 端末の RSSI 監視	RSSI評価回数 <input type="text" value="10"/> 回 RSSI最低しきい値 <input type="text" value="20"/>
		監視ログ	保持件数 <input type="text" value="1000"/> 件

設定終了後、保存をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

保存 **キャンセル**

管理情報取得

管理機器や無線 LAN 端末の情報取得を行う際の時間パラメタを設定します。

情報取得間隔

ある管理機器の情報を取得してから次の管理機器の情報を取得するまでの間隔の秒数を、1～600の範囲の10進数で指定します。

情報取得待機間隔

すべての情報取得対象の管理機器の情報を取得したあと、次の情報取得を開始するまでの待ち時間の秒数を、1～600の範囲の10進数で指定します。

情報取得タイムアウト

管理機器との通信時のタイムアウト時間の秒数を、1～60の範囲の10進数で指定します。

こんな事に気をつけて

情報取得間隔が短いほどリアルタイムに近い情報を得ることができます。本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

チャネル自動調整（共通）

通信帯域幅

無線 LAN チャネル自動調整時の通信帯域幅を指定します。

- 20
無線 LAN の通信帯域幅に 20MHz を使用します
- 40
無線 LAN の通信帯域幅に 40MHz を使用します。

チャネル自動調整（5GHz 帯）

割当範囲

5GHz 帯の無線 LAN チャネル自動調整時に、割り当てるチャネルの範囲を指定します。

- w52
5GHz 無線 LAN W52 で規程されたチャネルの中で割り当てを行います。
- w53
5GHz 無線 LAN W53 で規程されたチャネルの中で割り当てを行います。

- w56
5GHz 無線 LAN W56 で規程されたチャネルの中で割り当てを行います。
- w52/53
5GHz 無線 LAN W52 と W53 で規程されたチャネルの中で割り当てを行います。
- w52/53/56
5GHz 無線 LAN W52、W53 および W56 で規程されたチャネルの中で割り当てを行います。

チャネル自動調整（2.4GHz 帯）

判定用 RSSI しきい値

2.4GHz 帯の無線 LAN チャネル自動調整時に、使用済みのチャネルを割り当てる場合の RSSI のしきい値を 1～128 の範囲の10進数で指定します。

開始チャネル

2.4GHz 帯の無線 LAN チャネルを割り当てるときのチャネルのレイアウトの開始チャネルを 1～5 の範囲の10進数で指定します。

チャネル割当間隔

2.4GHz 帯の無線 LAN チャネルを割り当てるときのチャネルのレイアウトのチャネル割当間隔を、3～5 の範囲の10進数で指定します。

チャネルレイアウトは以下の式で求めることができます。

$<\text{ch_number}>, <\text{ch_number}> + (1 \times <\text{interval}>), \dots, <\text{ch_number}> + (n \times <\text{interval}>)$

開始チャネル : $<\text{ch_number}>$

チャネル割当間隔 : $<\text{interval}>$

電波出力自動調整

RSSI 最低しきい値

電波出力自動調整時に近隣の管理機器で計測される、調整対象の管理機器の RSSI のしきい値を 1～255 の範囲の10進数で指定します。

有線 LAN

管理機器の稼動監視の時間パラメタを設定します。

稼動監視間隔

ある管理機器に ping を送信し応答を得たあと、次の管理機器に ping を送信するまでの間隔の秒数を、1～600 の範囲の 10 進数で指定します。

稼動監視待機間隔

すべての監視対象の管理機器に ping を送信したあと、次の ping 送信を開始するまでの待ち時間の秒数を、1～600 の範囲の 10 進数で指定します。

稼動監視タイムアウト

管理機器からの ping 応答のタイムアウト時間の秒数を、1～60 の範囲の 10 進数で指定します。

こんな事に気をつけて

稼動監視間隔が短いほどリアルタイムに近い情報を得る事ができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

通信異常判定しきい値

有線 LAN の稼動監視で、指定した回数連続して ping に無応答の場合、対象の管理機器の有線 LAN を通信異常の疑いありと報告します。通信が確認できない連続回数が通信異常判定しきい値を超えると、対象の管理機器の有線 LAN を通信異常と報告します。

通信異常判定しきい値は 1～11 の範囲の 10 進数で指定します。

無線 LAN

監視用管理機器への無線 LAN のスキャンレポート取得の時間パラメタを設定します。

スキャンレポート取得間隔

ある監視用管理機器のスキャンレポートを取得してから次の監視用管理機器のスキャンレポートを取得するまでの間隔の秒数を、1～600 の範囲の 10 進数で指定します。

スキャンレポート取得待機間隔

すべての監視用管理機器からスキャンレポートを取得したあと、次のスキャンレポート取得を開始するまでの待ち時間の秒数を、1～600 の範囲の 10 進数で指定します。

スキャンレポート取得タイムアウト

監視用管理機器との通信時のタイムアウト時間の秒数を、1～60 の範囲の 10 進数で指定します。

こんな事に気をつけて

スキャンレポート取得間隔が短いほどリアルタイムに近い情報を得ることができますが、本装置とネットワークの負荷は増大します。システム、ネットワークのパフォーマンスに応じて適切な値を設定してください。

通信異常判定しきい値

無線 LAN の監視で、指定した回数連続して無線 LAN の監視結果に監視対象の管理機器が検出されない場合、その管理機器の無線 LAN を通信異常の疑いありと報告します。連続未検出回数が通信異常判定しきい値を超えると、対象の管理機器の無線 LAN を通信異常と報告します。

通信異常判定しきい値は 1～11 の範囲の 10 進数で指定します。

無線 LAN 端末の RSSI 監視

管理機器に接続している無線 LAN 端末からの RSSI を評価した結果が RSSI 最低しきい値を下回った場合、監視ログにその無線 LAN 端末と RSSI の評価値の情報を出力します。

RSSI 評価回数

1～50 の範囲の 10 進数で指定します。

RSSI 最低しきい値

1～255 の範囲の 10 進数で指定します。

こんな事に気をつけて

無線 LAN 端末の RSSI 監視は、無線 LAN 端末の情報を取得する管理機器に対してのみ実行することができます。

監視ログ

監視ログを設定します。

保持件数

監視ログの保持件数を、100～10000 の範囲の 10 進数で指定します。

索引

A

AAA 情報	411
AAA ユーザ情報	412
ACL 情報	433
ACL 定義情報	434
AH	231, 388
ARP 情報	135
ARP 認証関連	
LAN 情報	97
AS 外部経路集約情報	482
AS 境界ルータ情報	482

B

BGP/MPLS VPN 情報	133
BGP/MPLS VPN スタティック経路情報	134
BGP 相手基本情報	463
BGP 相手情報	463
BGP 拡張機能情報	470
BGP 関連	457
BGP 情報	457

C

CLP 値設定情報	285
-----------	-----

D

DHCP 情報	129
DNS サーバ機能	527, 534
DNS サーバの自動切り替え機能	527
DNS 問い合わせタイプフィルタ機能	527

E

ECMP 情報	451
EoMPLS 情報	180
ESP	231, 388
EXP 値書き換え情報	290

I

ICMP 情報	131
ICMP 定義情報	437
IDS 情報	
LAN 情報	113
相手情報	267
テンプレート情報	355

IEEE802.1X 認証情報

LAN 情報	
物理 LAN	94
無線 LAN	185
認証情報	409

IKE 情報

AAA 情報	420
相手情報	
拡張 IPsec 対象範囲情報	246
テンプレート情報	
動的 VPN RSA デジタル署名認証方式	405
動的 VPN 共有鍵認証方式	396
IKE 情報 (IKEv1 RSA デジタル署名認証方式)	
相手情報	241
IKE 情報 (IKEv1 共有鍵認証方式)	
相手情報	236

IKE 情報 (IKEv1)

テンプレート情報	
RADIUS/AAA	390
IKE 情報 (IKEv2 RSA デジタル署名認証方式)	
相手情報	243
IKE 情報 (IKEv2 共有鍵認証方式)	
相手情報	239
IKE 情報 (動的VPN接続 RSA デジタル署名認証方式)	
相手情報	
動的 VPN	245

IKE 情報 (動的 VPN 接続 共有鍵認証方式)

相手情報	
動的 VPN	244

Ingress ポリシールーティング情報

LAN 情報	127
相手情報	283
テンプレート情報	367

IPsec/IKE 関連

AAA 情報	419
テンプレート情報	
RADIUS/AAA	388
動的 VPN RSA デジタル署名認証方式	405
動的 VPN 共有鍵認証方式	396

IPsec 情報

AAA 情報	419
相手情報	
自動鍵	230
手動鍵	233
動的 VPN	235
テンプレート情報	388

IPv4 BGP 再配布フィルタリング情報

471

IPv4 BGP 集約経路情報

461

IPv4 BGP ネットワーク情報

459

IPv4 BGP フィルタリング情報

466

IPv4 DHCP スタティック機能

534

IPv4 MPLS 連携情報

474

IPv4 VRF 情報

473

IPv4 ループバック情報

52

IPv6 AS 境界ルータ情報

495

IPv6 BGP 再配布フィルタリング情報

472

IPv6 BGP 集約経路情報

462

IPv6 BGP ネットワーク情報	460
IPv6 BGP フィルタリング情報	468
IPv6 CLP 値設定情報	322
IPv6 DHCP 情報	
LAN 情報	163
相手情報	324
IPv6 DHCP スタティック機能	534
IPv6 EXP 値書き換え情報	328
IPv6 Ingress ポリシールーティング情報	
LAN 情報	161
相手情報	320
テンプレート情報	384
IPv6 OSPF エリア情報	492
IPv6 OSPF 関連	491
IPv6 OSPF 再配布フィルタリング情報	496
IPv6 OSPF 情報	
LAN 情報	142
相手情報	301
IPv6 RIP 関連	488
IPv6 RIP 再配布フィルタリング情報	489
IPv6 RIP 情報	
LAN 情報	141
相手情報	300
IPv6 RIP タイマ情報	488
IPv6 RIP フィルタリング情報	
LAN 情報	155
相手情報	314
IPv6 RIP マルチパス情報	489
IPv6 Traffic Class 値書き換え情報	
LAN 情報	151
相手情報	310
テンプレート情報	376
IPv6 エリア間プレフィックス LSA 入出力可否情報	494
IPv6 経路集約情報	493
IPv6 動的 VPN 情報	330
IPv6 関連	
AAA 情報	417
LAN 情報	137
相手情報	296
テンプレート情報	369
IPv6 基本情報	
AAA 情報	417
LAN 情報	137
相手情報	296
テンプレート情報	369
IPv6 再配布情報	485
IPv6 スタティック経路情報	
AAA 情報	418
LAN 情報	144
相手情報	303
IPv6 帯域制御 (WFQ) 情報	
LAN 情報	157
相手情報	315
テンプレート情報	380
IPv6 定義情報	438

IPv6 フィルタリング情報

LAN 情報	145
相手情報	304
テンプレート情報	370
IPv6 優先度情報	487
IPv6 ルータ ID 情報	491
IPv6 ルーティングマネージャ情報	485
IPv6 ループバック情報	53
IP アドレス情報	100
IP 関連	
AAA 情報	415
LAN 情報	100
相手情報	254
テンプレート情報	348
IP 基本情報	
AAA 情報	415
相手情報	254
テンプレート情報	348
IP 情報	445
IP 定義情報	435
IP フィルタリング情報	
LAN 情報	107
相手情報	260
テンプレート情報	349
IP マルチキャスト情報	498
IP マルチキャストスタティック RP 情報	500
IP マルチキャストスタティック経路情報	501

L

LAN 情報	81
LDP 情報	
LAN 情報	178
相手情報	340
LLDP 情報	407
LAN 情報	92

M

MAC アドレス認証情報

LAN 情報	96
認証情報	410
MAC アドレスフィルタ情報	545
MAC アドレスフィルタセット情報	545
MAC 定義情報	439
MAC フィルタリング情報	

LAN 情報	170
相手情報	333
無線 LAN 情報	76
MIB ビュー情報	525
MPLS 関連	
相手情報	339
MPLS 基本情報	
LAN 情報	177
相手情報	339
MPLS 情報	503
MP 情報	253

N

NAT あて先変換情報	
LAN 情報	122
相手情報	278
テンプレート情報	362
NAT 情報	
LAN 情報	118
相手情報	274
テンプレート情報	358

O

OSPF エリア基本情報	476
OSPF エリア情報	476
OSPF 関連	475
OSPF 再配布フィルタリング情報	483
OSPF 情報	
LAN 情報	103
相手情報	256

P

PPPoE 情報	223
PPP 関連	
相手情報	252
テンプレート情報	346
PPP 情報	
ISDN 接続	213
PPPoE 接続	222
専用線接続	207
モデム接続	218
ProxyDNS 情報	527

R

RADIUS 関連	425
RIP 相手フィルタリング情報	456
RIP 関連	452
RIP 再配布フィルタリング情報	453
RIP 情報	
LAN 情報	102
相手情報	255
RIP タイマ情報	452
RIP フィルタリング情報	
LAN 情報	117
相手情報	272
RIP マルチパス情報	453
RIP ユニキャスト送信情報	455

S

SIP-SIP ゲートウェイ情報	514
SNMPv1/v2c 情報	520
SNMPv3 情報	522
SNMP 情報	518

T

TCP 定義情報	436
TOS 値書き換え情報	
LAN 情報	113
相手情報	268
テンプレート情報	355

U

UDP 定義情報	436
UPnP 情報	502
URL フィルタ機能	527
URL フィルタ情報	527

V

VLAN プライオリティマッピング情報	183
VRSS アクション情報	90
VRSS グループ情報	85
VRSS トリガ情報	87

W

WAN 情報	62
--------	----

あ

相手情報	188
相手装置証明書情報	539
相手装置証明書の設定	539
圧縮情報	
相手情報	252
テンプレート情報	347
アプリケーションフィルタ情報	56

い

異常時動作情報	51
インターフェース情報	446

お

オプション設定	
PPPoE 接続	33
インターネットへ ISDN 接続	29
インターネットへ専用線接続	31
オフィスへ ISDN 接続	36
オフィスへ専用接続	37
プライベート LAN 接続	40

か

回線インターフェース	
ATM	68
ISDN	63
専用線	66
データ通信カード	69
フレームリレー	67
回線情報	71
外線情報	516
外部メディアスタート機能情報	57
拡張 IPsec 対象範囲情報	421
かんたん設定	
PPPoE 接続	33
インターネットへ ISDN 接続	28
インターネットへ専用線接続	31
オフィスへ ISDN 接続	35
オフィスへ専用線接続	37
プライベート LAN 構築	39
かんたん設定メニュー	11
管理外機器情報	544
管理機器情報	542
管理グループ情報	541

き

基本情報	
AAA 情報	
RADIUS 関連	425
共通情報	412
IP 情報	445
LAN 情報	
ARP 認証関連	97
VRP グループ情報	85
共通情報 (VLAN)	181
共通情報 (物理 LAN)	82
共通情報 (無線 LAN)	184
LLDP 情報	407
MPLS 情報	503
SIP-SIP ゲートウェイ情報	514
SNMP 情報	518
UPnP 情報	502
相手情報	
ATM 接続	194
IPsec/IKE 接続	226
IP トンネル接続	224
ISDN (バンドル) 接続	214
ISDN 接続	209
MPLS トンネル接続	250
PPPoE 接続	221
共通情報	189
専用線 (バンドル) 接続	208
専用線接続	201
データ通信カード接続	219
パケット破棄	251
フレームリレー接続	215
別インタフェースから送出	249
モデム接続	216
スイッチ情報	78

テンプレート情報

ISDN	344
RADIUS/AAA	386
動的 VPN RSA デジタル署名認証方式	403
動的 VPN 共有鍵認証方式	394, 399
動的 VPN 情報	
クライアント関連情報	509, 510
サーバ関連情報	508
パスワード情報	42
無線 LAN 管理情報	543
基本定義情報	434
逆引き情報	531
共通情報	
AAA 情報	411
LAN 情報 (VLAN)	181
LAN 情報 (無線 LAN)	184
LAN 情報 (物理 LAN)	82
ProxyDNS 情報／URL フィルタ情報	528
相手情報	189
シリアル情報	186
テンプレート情報	
ISDN	344
RADIUS/AAA	386
動的 VPN RSA デジタル署名認証方式	403
動的 VPN 共有鍵認証方式	394

く

クライアント機能

サーバ情報	427
送信情報	431
クライアント情報	
サーバ機能	432
グループ ID 情報	411
グループ識別子 0	505
グループ識別子 1～7	507

け

経路集約情報	477
月間／週間予約情報	58

こ

構成定義切り替え予約情報	61
--------------------	----

さ

サーバ機能情報	53
再配布情報	447
サプリカント関連	
AAA 情報	424
サプリカント情報	
AAA 情報	424

し**自側ネットワーク情報**

動的 VPN 共有鍵認証方式	402
動的 VPN 情報	513
システムログ情報	48
自装置証明書情報	535
自装置証明書の設定	537
自装置証明書要求の作成（鍵ペアの作成）	535
順引き情報	529
詳細設定メニュー	11
証明書関連情報	535
シリアル情報	186

す

スイッチ情報	78
スケジュール情報	58
スタティック ARP 情報	136
スタティック経路情報	
AAA 情報	416
LAN 情報	105
相手情報	259

せ

静的 MAC 学習テーブル情報	174
静的 NAT 情報	
LAN 情報	120
相手情報	276
テンプレート情報	360
セカンダリ IP アドレス情報	101
セグメント接続／分割	41
接続先監視	393, 398, 423
接続先監視定義情報	443
接続先種別	
ATM 接続	194
ISDN 接続	209
フレームリレー接続	215
モデム接続	216
接続先情報	191
接続先種別	
IPsec/IKE 接続	225
IP トンネル接続	224
MPLS トンネル接続	250
PPPoE 接続	221
パケット破棄	251
別インターフェースから送出	249

接続制御情報

AAA 情報	422
相手情報	
ATM 接続	197
IPsec/IKE 接続	229
ISDN 接続	210
PPPoE 接続	222
専用線接続	202
データ通信カード接続	220
モデム接続	217
テンプレート情報	
RADIUS/AAA	392
動的 VPN 共有鍵認証方式	397
設定メニュー	11

そ

送出先定義情報	442
装置情報	46

た

帯域制御 (WFQ) 情報	175
LAN 情報	123
相手情報	
IP 関連	279
ブリッジ関連	337
テンプレート情報	363
タイムサーバ情報	47

ち

着信相手識別情報	342
着信制御情報	
相手情報	
ISDN 接続	212
専用線接続	206
モデム接続	218

て

テンプレート情報	343
電話番号変更予約情報	60

と

動的 VPN 関連	
テンプレート情報	
動的 VPN 共有鍵認証方式	399
動的 VPN 情報	508
相手情報	294
ドメイン情報	
動的 VPN 情報	509
トラップ情報	
LAN 情報	99
SNMP 情報	526
相手情報	
共通情報	190
テンプレート情報	
ISDN	345

な

内線情報 515

に

認証／暗号化情報 73

認証局証明書情報 540

認証局証明書の設定 540

認証情報 409

AAA 情報 413

テンプレート情報 346

認証不要端末情報

LAN 情報

ARP 認証関連 98

ね

ネットワーク情報 188

は

バーチャルリンク情報 480

パスワード情報 42

パターン定義情報 440

ひ

必須設定

PPPoE 接続 33

インターネットへ ISDN 接続 28

インターネットへ専用線接続 31

オフィスへ ISDN 接続 35

オフィスへ専用線接続 37

プライベート LAN 接続 39

ふ

ファームウェア更新情報 50

ブリッジ関連

LAN 情報 169

相手情報 332

ブリッジグループ情報 504

ブリッジ情報 504

LAN 情報 169

相手情報 332

ほ

ポート情報 79

ホストデータベース情報 533

ポリシーグループ情報 440

ポリシーグループ定義情報 440

ま

マニュアル構成 10

マルチキャスト情報 498

LAN 情報 132

相手情報 289

マルチルーティング情報 199

む

無線 LAN 管理情報 541

無線 LAN 管理パラメタ 548

無線 LAN 管理パラメタ情報 548

無線 LAN 情報 70

も

モデル情報 187

ゆ

ユーザ情報 522

優先度情報 450

り

リモートパワーオン機能 534

る

ルータ ID 情報 475

ルータ名称情報 46

ルーティングプロトコル情報 446

ルーティングマネージャ情報 446

ろ

ログインパスワード情報 43

ログインユーザ情報 44

Si-R シリーズ Web リファレンス

P3NK-4032-05Z0

発行日 2014年6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。