

GeoStream Si-R シリーズ

Webリファレンス
V32

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。

2006年 9月初版

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

All rights reserved, Copyright© 富士通株式会社 2006

目次

はじめに	2
本書の使いかた	5
本書の読者と前提知識	5
本書における商標の表記について	5
本装置のマニュアルの構成	6
1 「設定メニュー」を表示する	7
2 「設定メニュー」の画面体系	8
2.1 かんたん設定メニュー	8
2.2 基本設定	9
2.3 ルータ設定	10
3 インターネットへ ISDN 接続かんたん設定	20
3.1 必須設定	20
3.2 オプション設定	21
4 インターネットへ専用線接続かんたん設定	23
4.1 必須設定	23
4.2 オプション設定	23
5 PPPoE かんたん設定	25
5.1 必須設定	25
5.2 オプション設定	25
6 オフィスへ ISDN 接続かんたん設定	27
6.1 必須設定	27
6.2 オプション設定	28
7 オフィスへ専用線接続かんたん設定	29
7.1 必須設定	29
7.2 オプション設定	29
8 プライベート LAN 構築かんたん設定	31
8.1 必須設定	31
8.2 オプション設定	32
9 セグメント接続／分割かんたん設定	33
9.1 LAN0	33
9.2 LAN1	33
10 パスワード情報	34
10.1 基本情報	34
10.2 ログインパスワード情報	35
11 装置情報	36
11.1 ルータ名称情報	36
11.2 タイムサーバ情報	37
11.3 システムログ情報	38
11.4 SNMP 情報	39
11.5 ファームウェア更新情報	42
11.6 異常時動作情報	43
11.7 ループバック情報	44
11.8 サーバ機能情報	45
11.9 MAC アドレス認証情報	49
12 スケジュール情報	50
12.1 月間／週間予約情報	50
12.2 電話番号変更予約情報	52
12.3 構成定義切り替え予約情報	53
13 WAN 情報	54
13.1 WAN 情報	54

14 スイッチ情報	62
14.1 基本情報	62
14.2 ポート情報	63
15 LAN 情報	65
15.1 インタフェース：物理 LAN	66
15.2 インタフェース：VLAN	150
16 シリアル情報	154
16.1 共通情報	154
16.2 モデム情報	155
17 相手情報	156
17.1 ネットワーク情報	156
17.2 着信相手識別情報	288
18 テンプレート情報	289
18.1 接続種別：ISDN	290
18.2 接続種別：IPsec/IKE (RADIUS/AAA)	333
18.3 接続種別：IPsec/IKE (動的 VPN)	341
19 AAA 情報	351
19.1 グループ ID 情報	351
20 ACL 情報	372
20.1 ACL 定義情報	373
21 ポリシーグループ情報	379
21.1 ポリシーグループ定義情報	379
22 ルーティングプロトコル情報	384
22.1 インタフェース情報	384
22.2 ルーティングマネージャ情報	384
22.3 RIP 関連	390
22.4 BGP 関連	395
22.5 OSPF 関連	408
22.6 IPv6 ルーティングマネージャ情報	419
22.7 IPv6 RIP 関連	421
23 マルチキャスト情報	424
23.1 IP マルチキャスト情報	424
23.2 IP マルチキャストスタティック経路情報	426
24 UPnP 情報	427
24.1 基本情報	427
25 MPLS 情報	428
25.1 基本情報	428
26 ブリッジ情報	429
26.1 ブリッジグループ情報	429
27 動的 VPN 情報	433
27.1 サーバ関連情報	433
27.2 クライアント関連情報	434
28 ProxyDNS 情報／URL フィルタ情報	439
28.1 順引き情報	440
28.2 逆引き情報	442
29 ホストデータベース情報	444
索引.....	446

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 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。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。



ヒント 本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。

こんな事に気をつけて

本装置をご使用になる際に、注意していただきたいことを説明しています。



参照 操作方法など関連事項を説明している箇所を示します。



適用機種 本装置の機能を使用する際に、対象となる機種名を示します。

本書における商標の表記について

Microsoft、Windows および Windows NT 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。

Hi/fn および LZS は、Hi/fn,inc. 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。

Windows® 95 の正式名称は、Microsoft® Windows® 95 operating system です。

Windows® 2000 の正式名称は、Microsoft® Windows® 2000 Server Network operating system、または Microsoft® Windows® 2000 Professional operating system です。

その他の各製品名は、各社の商標、または登録商標です。

本装置のマニュアルの構成

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

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

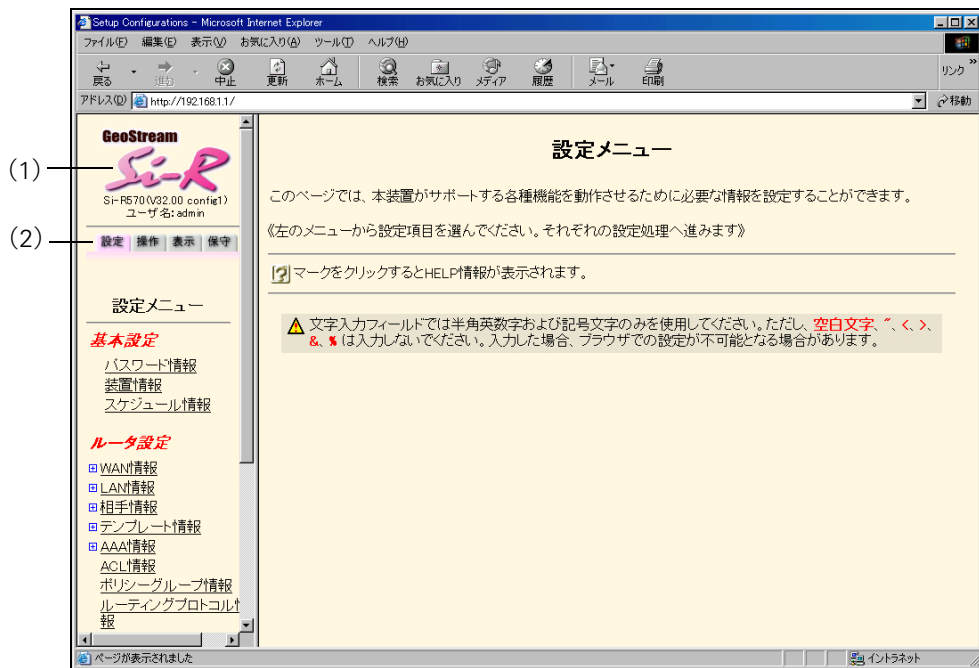
1 「設定メニュー」を表示する

「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 Si-R シリーズ Web ユーザーズガイド「1.3 本装置にログインする」(P10)



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-R180、220B 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-R240、260B、370、570 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

Si-R シリーズ Web ユーザーズガイド「2.1 操作メニューを使う」(P21)、「2.2 表示メニューを使う」(P35)、「2.3 保守メニューを使う」(P39)

こんな事に気をつけて

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

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

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
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
	SNMP 情報
	ファームウェア更新情報
	異常時動作情報
	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
	MAC アドレス認証情報
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	WAN 情報	回線インタフェース：ISDN	基本情報	
			接続制御情報	
		回線インタフェース：専用線	基本情報	
		回線インタフェース：フレームリレー	基本情報	
		回線インタフェース：ATM	基本情報	
		回線インタフェース：データ通信カード	基本情報	
スイッチ情報	基本情報			
	ポート情報			
LAN 情報	インタフェース：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
			MAC アドレス認証情報	
	インタフェース：物理 LAN および インタフェース：VLAN	IP 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	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)
			RIP フィルタリング情報	
			NAT 情報	

LAN情報	インタフェース： 物理LAN および インタフェース： VLAN	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	
			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	
			DHCP 情報	
			ICMP 情報	
			マルチキャスト情報	
			BGP/MPLS VPN 情報	
			BGP/MPLS VPN スタティック経路情報	
			ARP 情報	
			スタティック ARP 情報	
		IPv6 関連	IPv6 基本情報	
			IPv6 RIP 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 ポリシールーティング情報	
		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	

LAN情報	インタフェース： 物理LAN および インタフェース： VLAN	MPLS 関連	MPLS 基本情報	
			LDP 情報	
			EoMPLS 情報	
	インタフェース： 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	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	
シリアル情報	共通情報			
	モデム情報			
相手情報	ネットワーク情報	共通情報	基本情報	
		接続先情報	ATM 接続	基本情報
				接続制御情報
				マルチルーティング情報
			専用線接続	基本情報
				接続制御情報
				PPP 情報
				マルチルーティング情報
			ISDN 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
			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

相手情報	ネットワーク情報	接続先情報	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
			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
			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
			IP トンネル接続	基本情報
				接続制御情報
			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
				IKE 情報（動的VPN）
				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）

相手情報	ネットワーク情報	接続先情報	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
			MPLS トンネル接続	基本情報
				接続制御情報
				マルチルーティング情報
			パケット破棄	基本情報
		PPP 関連	圧縮情報	
			MP 情報	
		IP 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	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)
			RIP フィルタリング情報	
			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	
			CLP 値設定情報	CLP 値設定情報 (旧定義)
			マルチキャスト情報	

相手情報	ネットワーク情報	IP 関連	EXP 値書き換え情報	EXP 値書き換え情報 (旧定義)
			動的VPN 情報	
		IPv6 関連	IPv6 基本情報	
			IPv6 RIP 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	
		PPP 関連	認証情報	
			圧縮情報	
	接続種別：ISDN、 接続種別：IPsec/IKE (RADIUS/AAA) および 接続種別：IPsec/IKE (動的VPN)	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)
	接続種別：IPsec/IKE (RADIUS/AAA)	共通情報	基本情報	
		IPsec/IKE 関連	IPsec 情報	
			IKE 情報	
			接続制御情報	

テンプレート情報	接続種別：IPsec/IKE (動的VPN)	共通情報	基本情報	
		IPsec/IKE 関連	IPsec 情報	
			IKE 情報	
			接続制御情報	
		動的VPN 関連	基本情報	
			自側ネットワーク情報	
AAA 情報	グループID 情報	共通情報	基本情報	
		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
			サブリカント関連	接続制御情報
				サブリカント情報
		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
ルーティングプロ トコル情報	インタフェース情報	
	ルーティングマネー ジャ情報	再配布情報
		優先度情報
		ECMP 情報
	RIP 関連	RIP タイマ情報
		RIP マルチパス情報
		RIP 再配布フィルタリング 情報
		RIP ユニキャスト送信情報
		RIP 相手フィルタリング 情報
	BGP 関連	BGP 情報
		BGP ネットワーク情報
		BGP 集約経路情報
		BGP 相手情報
		BGP 相手基本情報
		BGP フィルタリング情報
		BGP 拡張機能情報
		BGP 再配布フィルタリング 情報
		VRF 情報
		MPLS 連携情報

ルーティングプロ トコル情報	OSPF 関連	ルータ ID 情報	
		OSPF エリア情報	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
		AS 境界ルータ情報	
		AS 外部経路集約情報	
		OSPF 再配布フィルタ リング情報	
	IPv6 ルーティング マネージャ情報	IPv6 再配布情報	
		IPv6 優先度情報	
	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	
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
ProxyDNS 情報／ URL フィルタ情報	順引き情報		
	逆引き情報		
ホストデータ ベース情報			

3 インターネットへISDN 接続かんたん設定

適用機種 Si-R220B

[操作] 「設定メニュー」→[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	
ユーザ認証ID	
ユーザ認証パスワード	

■オプション設定

IPアドレス	192.168.3.1
ネットマスク	24 (255.255.255.0)
DNSサーバ	☒ 自動取得
接続先の電話番号2	
接続先の電話番号3	
常時接続機能	☐ 使用する ☒ 使用しない 無通信監視タイマ 0 秒 課金単位時間 0
接続先ネットワーク名	rmt1
接続先名	ap0-0
アドレス変換	☐ 使用しない ☒ マルチNAT UPnP機能 ☒ 使用しない ☐ 使用する
MP	☐ 使用する ☒ 使用しない
かんたんフィルタ	☐ 使用する ☒ 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。

設定終了 キャンセル

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[®]、Windows[®] 95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によって定期的に出送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-R220B

[操作] 「設定メニュー」→[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	☒ 64Kbps ☒ 128Kbps
DNSサーバ	

オプション設定

接続ネットワーク名	fmt0						
接続先名	ap0-0						
ドメイン名							
アドレス変換	☒ 使用しない ☐ マルチNAT <table> <tr> <td>グローバルアドレス</td> <td></td> </tr> <tr> <td>アドレス個数</td> <td>1 個</td> </tr> <tr> <td>UPnP機能</td> <td>☒ 使用しない ☐ 使用する</td> </tr> </table>	グローバルアドレス		アドレス個数	1 個	UPnP機能	☒ 使用しない ☐ 使用する
グローバルアドレス							
アドレス個数	1 個						
UPnP機能	☒ 使用しない ☐ 使用する						

“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。

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-R180,220B

[操作] 「設定メニュー」→[かんたん設定メニュー]→インターネットへ「PPPoE 接続」
(Si-R180 の場合は「設定メニュー」→[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	
ユーザ認証パスワード	

■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)
DNSサーバ	☐ 自動取得
接続ネットワーク名	rmt0
接続先名	ap0-0
PPPoEで使用するインタフェース	☒ LAN0 ☐ LAN1
常時接続機能	☒ 使用する ☐ 使用しない 無通信監視タイマ 0 秒
アドレス変換	☐ 使用しない ☒ マルチNAT UPnP機能 ☒ 使用しない ☐ 使用する
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。

Si-R180 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 桁以内で指定します。

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フェースの反対側のインタフェースが自動的にプライベート側となります。Si-R180 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 で使用するインタフェース

PPPoE で使用するインタフェースを選択します。Si-R180 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-R180 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-R180 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-R220B

[操作] 「設定メニュー」→[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	
ユーザ認証ID(発信)	
ユーザ認証パスワード(発信)	
ユーザ認証ID(着信)	
ユーザ認証パスワード(着信)	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
相手ルータのIPアドレス	192.168.2.1
相手ルータのネットマスク	24 (255.255.255.0)

■オプション設定

DHCPサーバ	☒ 使用しない ☐ 使用する DNSサーバ広報
常時接続機能	☐ 使用する ☒ 使用しない 無通信監視タイマ 60 秒 課金単位時間 0
接続ネットワーク名	rmt1
接続先名	ap0-0
MP	☐ 使用する ☒ 使用しない
ヘッダ圧縮	☐ VJ ☐ IPヘッダ圧縮
データ圧縮	☐ 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。

ユーザ認証パスワード／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-R220B

[操作] 「設定メニュー」→[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	☐ 64Kbps ☒ 128Kbps

■オプション設定

接続ネットワーク名	fmt1
接続先名	ap0-0
DHCPサーバ	☒ 使用しない ☐ 使用する DNSサーバ広報
ヘッダ圧縮	☐ VJ ☐ IPヘッダ圧縮
データ圧縮	☐ 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。

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タ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-R180,220B

[操作] 「設定メニュー」→[かんたん設定メニュー]→LAN間接続「プライベートLAN接続」
(Si-R180の場合は「設定メニュー」→[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	☒ DHCPで自動的に取得する ☐ 指定する	
	IPアドレス	
	ネットマスク	24 (192.0.0.0)
プライベート側IPアドレス	IPアドレス	192.168.1.1
	ネットマスク	24 (255.255.255.0)
グローバル側インタフェース	☒ LAN0 ☐ LAN1	

■オプション設定 

デフォルトルータ		
DNSサーバアドレス		
DHCPサーバ	☐ 使用しない ☒ 使用する	
	デフォルトルータ広報	192.168.1.1
	DNSサーバ広報	192.168.1.1
	ドメイン名広報	
UPnP機能	☒ 使用しない ☐ 使用する	
LAN0転送レート	自動認識	
LAN1転送レート	自動認識	

“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-R180 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サーバが稼働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フェース

LAN0とLAN1のどちらをグローバル側のインタフェースにするか選択します。Si-R180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先に存在する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す。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-R180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-R180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-R180,220B

[操作] 「設定メニュー」→[かんたん設定メニュー]→LAN間接続「セグメント接続／分割」
(Si-R180の場合は「設定メニュー」→[かんたん設定メニュー]→「セグメント接続／分割」)

セグメント接続／分割かんたん設定 

 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。

■LAN0 

IPアドレス	192.168.0.1
ネットマスク	24 (255.255.255.0)
転送レート	自動認識

■LAN1 

IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
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-R180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-R180のみ「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-R180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-R180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] 「設定メニュー」→基本設定「パスワード情報」

パスワード情報	
<u>基本情報</u>	<u>ログインパスワード情報</u>
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] 「設定メニュー」→基本設定「パスワード情報」→[基本情報]

■基本情報 	
暗号化パスワード形式	☐ 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。	
更新	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] 「設定メニュー」→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 FTP によるログイン時にもこのパスワードが使用されます。

■ログインパスワード情報 

管理者パスワード	
管理者パスワードの確認	
一般ユーザパスワード	
一般ユーザパスワードの確認	

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、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の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

ユーザ名が admin の場合に、16 文字以内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。

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

ユーザ名が user の場合に、16 文字以内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。

一般ユーザパスワードの確認

上記で指定したユーザパスワードをもう一度指定します。

11 装置情報

適用機種 全機種

[操作] 「設定メニュー」→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
SNMP情報	ファームウェア更新情報	異常時動作情報
ループバック情報	サーバ機能情報	MACアドレス認証情報

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] 「設定メニュー」→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

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] 「設定メニュー」→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 ☒ 使用しない ☐ 使用する

サーバ設定 ☒ DHCPで取得する
※IPv4のDHCPクライアントの設定が必要です。
☐ 設定する

プロトコル ☒ TIMEプロトコル
☐ SNTPプロトコル

タイムサーバIPアドレス

自動時刻設定 間隔

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

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、内部時計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] 「設定メニュー」→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

☒ 送信しない
☐ 送信する

送信先ホスト

セキュリティログ

☐ PPP
☐ IPフィルタ
☐ URLフィルタ
☐ NAT
☐ DHCP
☐ IDS
☐ MACアドレス認証

重複メッセージの出力

☒ する ☐ 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。

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システムログ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、「[Si-R シリーズ コマンドリファレンス](#)」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 形式でシステムログ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

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、MAC アドレス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。

11.4 SNMP 情報

[操作] 「設定メニュー」→基本設定「装置情報」→[SNMP 情報]

■SNMP情報	
SNMPエージェント機能	☒ 使用しない ☐ 使用する
ルータ管理者	
機器名称	ルータ名称を使用する (ルータ名称情報が設定されていないため選択できません) ☒ 指定する 機器名称
機器設置場所	
エージェントアドレス	
SNMPホスト1	☒ publicとする(任意のホストを対象とする) ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ 送信する 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト2	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ 送信する 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト3	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ 送信する 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト4	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ 送信する 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト5	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ 送信する 書き込み要求 ☒ 許可しない ☐ 許可する
SNMPホスト6	☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ ☒ 送信しない ☐ 送信する 書き込み要求 ☒ 許可しない ☐ 許可する

SNMPホスト7		☒ 指定しない ☐ 指定する コミュニティ名 IPアドレス トラップ 書き込み要求 ☒ 送信しない ☐ 送信する ☒ 許可しない ☐ 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 IPアドレス トラップ 書き込み要求 ☒ 送信しない ☐ 送信する ☒ 許可しない ☐ 許可する
トラップ	coldStart	☒ 有効にする ☐ 無効にする
	linkDown	☒ 有効にする ☐ 無効にする
	linkUp	☒ 有効にする ☐ 無効にする
	authenticationFailure	☒ 有効にする ☐ 無効にする
	newRoot	☒ 有効にする ☐ 無効にする
	topologyChange	☒ 有効にする ☐ 無効にする
	vrrpTrapNewMaster	☒ 有効にする ☐ 無効にする
	vrrpTrapAuthFailure	☒ 有効にする ☐ 無効にする
	nosError	☒ 有効にする ☐ 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。

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 マネージャ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”を選択し、以下の項目を設定します。

ルータ管理者

本装置の管理者名を 40 文字以内で指定します。区切り文字は、“_” や “.” を使用します。

機器名称

機器名称としてルータ名称を使用する場合は、“ルータ名称を使用する”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。

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。

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。トラップ送信時の自装置のアドレスにも使用されます。SNMP エージェント機能を使用する場合は必ず設定してください。“0.0.0.0”を指定すると、エージェントアドレスを指定しないものとみなします。

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

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 つまで指定できます。“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・トラップ送信可否を指定します。

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ホストに対してトラップを送信する場合は、“送信する”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、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。

トラップ

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の中のどれかがUP状態になったとき、SNMPマネージャに対して通知します。

linkUp

本装置の通信リンクに障害があったときに、SNMPマネージャに対して通知します。

また、装置の再起動時および構成定義反映時にも送信される場合があります。

authenticationFailure

SNMPのコミュニティの認証に失敗したときに、SNMPマネージャに対して通知します。

newRoot

本装置がルートブリッジになるときに、SNMPマネージャに対して通知します。

topologyChange

本装置が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SNMPマネージャに対して通知します。

vrrpTrapNewMaster

本装置がVRRPグループでマスタルータとなったときに通知します。

vrrpTrapAuthFailure

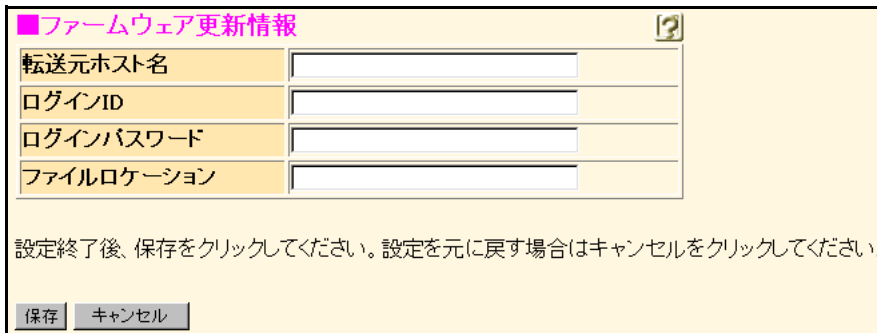
本装置で受信したVRRP-ADメッセージの認証方法が異常、またはVRRPグループに設定された認証方法やパスワードが一致しないときに通知します。

nosError

本装置になんらかの障害が発生したことを通知するトラップです。このトラップは障害が発生したことだけを通知します。それ以上の情報は、ほかのMIBにより報告します。

11.5 ファームウェア更新情報

[操作] 「設定メニュー」→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。

11.6 異常時動作情報

[操作] 「設定メニュー」→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	☒ 許可しない ☐ 許可する
ウォッチドッグリセット機能	☐ 使用しない ☒ 使用する
冷却ファン異常時の動作	☒ 運用継続 ☐ システムダウン
温度異常時の動作	☒ 運用継続 ☐ システムダウン
システムダウン時の電源制御	☒ 切断する ☐ 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。

CE 保守ログイン

CE 専用パスワードは、CE が保守作業を円滑に実施するために設定します。CE ログインを許可する場合は、“許可する”を選択します。

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起動する場合は、“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り再起動します。

冷却ファン異常時の動作

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、そのまま運用を継続するかを選択します。

Si-R180、220B、240、260B には、“冷却ファン異常時の動作”の項目はありません。

温度異常時の動作

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

Si-R180 には、“温度異常時の動作”の項目はありません。

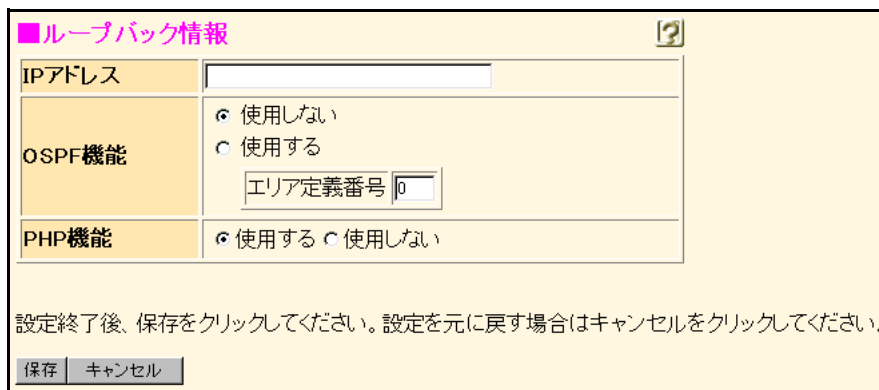
システムダウン時の電源制御

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。

Si-R570 以外の装置には、“システムダウン時の電源制御”の項目はありません。

11.7 ループバック情報

[操作] 「設定メニュー」→基本設定「装置情報」→[ループバック情報]



IP アドレス

ループバックインタ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、IP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

- ほかのインタフェースと違うネットワークのIPアドレスを設定する必要があります。
- 127.0.0.1はループバックインタ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た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フェースも含めて、OSPFを使用できるインタフェースは、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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。

11.8 サーバ機能情報

[操作] 「設定メニュー」→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	☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
TELNETサーバ機能	☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
SSHサーバ機能	SSH ☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
	SFTP ☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	
HTTPサーバ機能	☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
DNSサーバ機能	☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
SNTPサーバ機能	☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
TIMEサーバ機能	TCP ☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	設定
	UDP ☒ IPv4 / ☐ IPv6 ☐ IPv4 ☐ IPv6 ☐ 停止	

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。

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。

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

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。

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。

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] 「設定メニュー」→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
1	透過	6	修正 削除 移動 (移動先の優先順位)
2	透過	9	修正 削除 移動 (移動先の優先順位)
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 ☒ 透過 ☐ 遮断

ACL定義番号 参照

追加 キャンセル

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すると、有効なACL情報が表示されます。使用するACL定義を選択してください。アプリケーションフィルタ処理ではACL情報の以下の定義を使用します。

IP 定義

送信元IPアドレスが設定されているときだけ有効

IPv6 定義

送信元IPv6アドレスが設定されているときだけ有効

- 送信元IPアドレス
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。何も指定しない場合はすべてのIPアドレス/アドレスマスクをフィルタリングの対象とします。
- 送信元IPv6アドレス
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。チェック対象となったパケットのIPv6アドレスと定義したプレフィックス長の論理積と、定義した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たとみなします。何も指定しない場合はすべてのIPv6アドレス/プレフィックス長をフィルタリングの対象とします。

11.9 MACアドレス認証情報

[操作] 「設定メニュー」→基本設定「装置情報」→[MACアドレス認証情報]

■MACアドレス認証情報

パスワード

パスワードの確認

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

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。

12 スケジュール情報

[操作] 「設定メニュー」→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 Tue Nov 12 12:05:16 2002 です。		

Si-R180、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] 「設定メニュー」→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-R180、260B には、「終了時刻」の項目はありません。

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

Si-R180、260B には、“終了時刻” の項目はありません。

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／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-R180、260B では、リモートパワーオンだけをサポートしています。

終了時刻

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。

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。

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。

12.2 電話番号変更予約情報

適用機種 Si-R220B,240,370,570

[操作] 「設定メニュー」→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	-	-	修正 削除
2	-	-	修正 削除
3	-	-	修正 削除
4	-	-	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] 「設定メニュー」→基本設定「スケジュール情報」→[電話番号変更予約情報]→[修正]

■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	実行日時	20 年 月 日 時 分	
	電話番号変更情報	変更前1	変更後1
		変更前2	変更後2
		変更前3	変更後3
		変更前4	変更後4
		保存 キャンセル 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] 「設定メニュー」→基本設定「スケジュール情報」→[構成定義切り替え予約情報]

■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	-	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] 「設定メニュー」→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]

■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	実行日時 20 年 月 日 時 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」で知ることができます。

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-R220B,240,260B,370,570

[操作] 「設定メニュー」→ルータ設定「WAN 情報」

WAN情報
WAN情報

■WAN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。

インタフェース	ポート	回線インタフェース	操作
<WAN情報追加フィールド>			
回線インタフェース		ISDN	
			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 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-R220B、240 は 1 個、Si-R260B、370 は 16 個、Si-R570 は 132 個までを装置全体で設定できます。

13.1 WAN 情報

回線インタフェース

本装置に接続する回線の種類を選択します。

- ISDN (Si-R220B、370、570)
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-R220B、370、570)
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-R220B、370、570)
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-R240)
データ通信カードを使用する場合に選択します。

13.1.1 回線インタフェース：ISDN

適用機種 Si-R220B,370,570

13.1.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「WAN 情報」→[追加]→[基本情報]

■基本情報	
ポート	スロット0-0
自動接続	☐ すべて禁止 ☒ 相手毎に設定
着信動作	☐ すべて禁止 ☒ 相手毎に設定
自局番号チェック	☒ しない ☐ する
	チェックする番号1 電話番号を指定 サブアドレス
	チェックする番号2 電話番号を指定 サブアドレス
	グローバル着信 ☐ 利用しない ☒ 利用する
発信者番号通知	☒ 網契約に従う ☐ しない ☐ する
	通知する電話番号 電話番号を指定 サブアドレス
レイヤ1起動種別	☒ 常時起動 ☐ 呼毎起動
	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。

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。

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」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。

13.1.1.2 接続制御情報

[操作] 「設定メニュー」→ルータ設定「WAN 情報」→[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

☒ しない
☐ する

上限時間

日

制御動作

☒ 発信抑止のみ
☐ システムログ出力のみ

課金額による発信抑止

☒ しない
☐ する

上限金額

3000 円

制御動作

☒ 発信抑止のみ
☐ 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。省略することはできません。

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

制限を行う総通信時間を、1～999999 円の範囲で指定します。省略することはできません。

57

WAN 情報

13.1.2 回線インタフェース：専用線

適用機種 Si-R220B,370,570

13.1.2.1 基本情報

[操作] 「設定メニュー」→ルータ設定「WAN 情報」→[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

フラグ監視

☒ 無効にする ☐ 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

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-R220B 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。

13.1.3 回線インタフェース：フレームリレー

適用機種 Si-R220B,370,570

13.1.3.1 基本情報

[操作] 「設定メニュー」→ルータ設定「WAN 情報」→[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	☐ 使用しない ☒ 使用する
CLLMメッセージ	☐ 使用しない ☒ 使用する
輻輳通知ビット	☒ FECN ☒ 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
- ユーザー-ユーザー間の 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。

13.1.4 回線インタフェース：ATM

適用機種 Si-R260B,370,570

13.1.4.1 基本情報

[操作] 「設定メニュー」→ルータ設定「WAN 情報」→[追加]→[基本情報]

■基本情報

ポート

▼

スロット0-0

VPI

0

VP速度

指定しない

指定する

Mbps

OAM(F4)

受け付けがない

受け付ける

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

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	
	ATM155M 拡張モジュール H1	200Kbps～50Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R370	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。

13.1.5 回線インタフェース：データ通信カード

適用機種 Si-R240

13.1.5.1 基本情報

[操作] 「設定メニュー」→ルータ設定「WAN 情報」→[追加]→[基本情報]

■基本情報

ポート

スロット 0-0

PIN

☐ 使用しない

☒ 使用する

PINコード

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

ポート

本装置では、データ通信カード接続で使用するポートは固定です。

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コードを設定してください。

14 スイッチ情報

適用機種 Si-R180

[操作] 「設定メニュー」→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

14.1 基本情報

[操作] 「設定メニュー」→ルータ設定「スイッチ情報」→[基本情報]

■基本情報

スイッチ

☐ 使用しない
☒ 使用する

VLAN tag

☒ 透過しない
☐ 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。

14.2 ポート情報

[操作] 「設定メニュー」→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	操作
		Untagged VLAN ID	
1	使用する	1111 2222	修正 初期化
2	使用する	3333 1234	修正 初期化
3	使用しない	1245 2344	修正 初期化
4	使用する	2341 1423	修正 初期化
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] 「設定メニュー」→ルータ設定「スイッチ情報」→[ポート情報]→[修正]

■ポート情報			
ポート番号	スイッチポート	Tagged VLAN ID	操作
		Untagged VLAN ID	
1	使用する	1111 2222	修正 初期化
2	<ポート情報入力フィールド> スイッチポート ☒ 使用する ☐ 使用しない 転送レート 自動認識 MDI ☒ 自動 ☐ MDI ☐ MDI-X フロー制御機能 ☒ 使用する ☐ 使用しない VLAN ID Tagged 3333 Untagged 1234 保存 キャンセル 一覧へ戻る		
3	使用しない	1245 2344	修正 初期化
4	使用する	2341 1423	修正 初期化
全初期化			

保存した情報は、設定反映後に有効になります。

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、“,” で区切ります。範囲指定の場合は“-” で区切ります。

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。

15 LAN 情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「LAN 情報」

LAN情報

LAN情報

■LAN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。

インタフェース	ポート/VLAN ID	プロトコル	操作
LAN0	基本 0	IPv4 使用する [192.168.1.1]	修正 削除
		IPv6 使用しない	
		ブリッジ 使用しない	
		MPLS 使用しない	
		EoMPLS 使用しない	

<LAN情報追加フィールド>

インタフェース

物理LAN

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 LAN インタフェースが表示されています。LAN インタフェースは、装置全体で物理インタフェースと VLAN インタフェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) を参照してください。ただし、物理インタ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。

インタフェース

設定する LAN インタフェースの種別を以下の中から選択します。

- 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。

15.1 インタフェース：物理 LAN

[操作] 「設定メニュー」→ルータ設定「LAN0 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」で選択するインタフェースによって表示が異なります。

15.1.1 共通情報

[操作] 「設定メニュー」→ルータ設定「LAN0 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
基本情報	VRRPグループ情報	MACアドレス認証情報

15.1.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「LAN0 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 0 backup バックアップなし
優先使用ポート	☒ master ☐ 先にリンクアップしたポート
転送レート	自動認識
シェーピング	☒ 使用しない ☐ 使用する 最大送信レート Mbps
VRRP機能	☒ 使用しない ☐ 使用する パスワード
MTUサイズ	1500 バイト
自動復旧	モード ☒ 使用する ☐ 使用しない 初期状態 ☒ 非閉塞 ☐ 閉塞
MDI	☒ 自動 ☐ MDI ☐ MDI-X
フロー制御機能	☒ 使用する ☐ 使用しない
使用ポート	☒ 自動 ☐ 通常 ☐ 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 以外では、基本情報の表示が、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-R180 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。

優先使用ポート

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)
- 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。

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 以外	1 ～ 100000Kbps
Si-R570	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。

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は設定します。このインタ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。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。

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 障害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 障害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-R180、220B、240、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-R220B、260B では LAN1 ～ 3 ポート、Si-R240 では LAN1 ポートのみで設定することができます。

Si-R220B、240、260B 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-R180 では、LAN0 ポートの設定のみ有効です。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”である場合にのみ有効です。

フロー制御機能 (Si-R370、570)

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)

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。

15.1.1.2 VRRP グループ情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[共通情報]→[VRRP グループ情報]

■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	プリエンプトモード	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、このインタフェースに設定されている 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] 「設定メニュー」→ルータ設定「LAN 情報」→[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

15.1.1.2.1 基本情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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	
プライオリティ	☒ 優先度指定 優先度 仮想IPアドレス ☐ 優先度固定(最優先) 優先度 255 仮想IPアドレス インタフェースアドレスを使用
AD送信間隔	1 秒
プリエンプトモード	☒ ON ☐ OFF 移行禁止時間 0 秒
仮想IPアドレスあて ICMP ECHO	☒ 応答しない ☐ 応答する 応答送信元 IPアドレス ☒ 仮想IPアドレス ☐ 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がマスタとなります。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 グループメンバとして動作します。また、仮想IPアドレスはこのインタフェースの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 グループメンバが存在する場合は、そのメンバに設定されたインタフェースのIPアドレスを指定します。自装置のインタ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::～febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff

AD 送信間隔

マスタが送信する 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、マスタより先にバックアップのシステムが立ち上がり、本来マスタになるべき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“インタフェースアドレス”のどちらを選択します。

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。ICMP ECHO パケットの送信元 IP アドレスは、VRRP が設定された LAN インタフェースの IP アドレスとなります。応答を受診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。

インタフェース

トリガの対象となるインタフェースを選択します。“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。

ネットワーク

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”を選択した場合は以降のあて先 IP アドレス、あて先アドレスマスクを設定します。

あて先 IP アドレス／あて先アドレスマスク

あて先 IP アドレスとあて先アドレスマスクでホスト経路またはネットワーク経路を設定します。

インタフェース

“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。

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 ~ 191.25.255.254

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

以下の範囲を指定した場合は IPv6 リンクローカルアドレスとなるため、送出インタフェースに IPv6 リンクローカルアドレスのインタフェースを設定してください。

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

送出インタフェース

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

なお、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。

15.1.1.2.3 VRRP アクション情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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 >				
	☒ マスタ(master) ☐ バックアップおよびミニシャル(backup)			
	☒ 接続/開塞解除(online)			
	☒ スイッチ定義 スイッチポート すべて ("ポート番号指定"を選択時のみ有効です。)			
	☐ LAN インタフェース インタフェース すべて ("定義番号指定"を選択時のみ有効です。)			
	☐ 相手ネットワーク ネットワーク 接続先 すべて ("定義番号指定"を選択時のみ有効です。) 相手定義番号 接続先定義番号			
	《ワンタイムパスワード設定》 送信認証ID 送信認証パスワード ※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。			
	☐ テンプレート定義 テンプレート名 tmp0 ユーザID			
動作	☐ 切断/開塞(offline)			
	☒ スイッチ定義 スイッチポート すべて ("ポート番号指定"を選択時のみ有効です。)			
	☐ LAN インタフェース インタフェース すべて ("定義番号指定"を選択時のみ有効です。)			
	☐ 相手ネットワーク ネットワーク 接続先 すべて ("定義番号指定"を選択時のみ有効です。) 相手定義番号 接続先定義番号			
	☐ テンプレート定義 テンプレート名 tmp0 ユーザID			

現在、このVRRP グループメンバに設定されている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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

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 (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)
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)
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。

15.1.1.3 MACアドレス認証情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[共通情報]→[MAC アドレス認証情報]

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。

参照する AAA 情報

MAC アドレス認証を行う場合に参照する 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。

15.1.2 IP 関連

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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	MPLS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あて先変換情報
帯域制御(WFQ)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スタティック経路情報		ARP情報		スタティックARP情報

15.1.2.1 IP アドレス情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[IP アドレス情報]

■IPアドレス情報

IPv4

☒ 使用する
 ☐ 使用しない

IPアドレス

☐ DHCPで自動的に取得する
 ☒ 指定する

IPアドレス

192.168.1.1

ネットマスク

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。

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。

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

本装置のネットマスクを指定します。

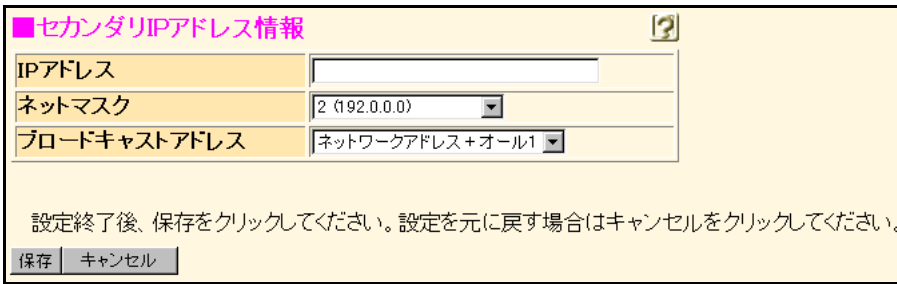
ブロードキャストアドレス

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)

15.1.2.2 セカンダリIPアドレス情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[セカンダリIPアドレス情報]



本装置は1つのインタフェースに複数の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)

10.0.0.1 ~ 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)

15.1.2.3 RIP 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[RIP 情報]

RIP 送信

☒ 送信しない
☐ V1 で送信する
☐ V2 で送信する
☐ V2 (Multicast) で送信する

RIP 受信

☒ 受信しない
☐ V1 で受信する
☐ V2、V2 (Multicast) で受信する

《 RIP 送信時は加算するメトリック値を設定してください。》

メトリック値

0

《 RIP V2 使用時で認証 / パケットを破棄しない時は RIP V2 パスワードを設定してください。》

認証パケット

☐ 破棄する
☒ 破棄しない

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

RIP を使用できるインタフェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

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。

15.1.2.4 OSPF 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[OSPF 情報]

■OSPF情報	
OSPF機能	☒ 使用しない ☐ 使用する
エリア定義番号	0
出力コスト	10
指定ルータ優先度	1
Hello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 ☒ 文字列 ☐ 16進数 認証鍵
	☐ MD5認証 MD5認証鍵ID MD5認証鍵
パケット送信	☐ 抑止する ☒ 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

ループバックインタフェースも含めて、OSPF を使用できるインタフェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

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勧めします。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 桁以内で指定します。16 桁未満の鍵を指定した場合、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場合は、“抑止する”を選択します。

15.1.2.5 スタティック経路情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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	中継ルータアドレス	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>				
☐ デフォルトルート				
中継ルータアドレス ☐ DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 ☒ 指定する IPアドレス				
☒ 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				
中継ルータアドレス ☐ DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。 ☒ 指定する IPアドレス				
メトリック値 1				
優先度				
追加 キャンセル				

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、Si-R シリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P37)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。

メトリック値

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

スタティック経路情報の優先度を 10 進数値で指定します。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 進数値で指定します。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 進数値で指定します。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。

15.1.2.6 IPフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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

<IPフィルタリング情報入力フィールド>

動作 ☒ 透過 ☐ 遮断

方向 入出力

ACL定義番号 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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[IP フィルタリング情報]
→[ACL 定義参照] または「ACL 定義番号の[参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
ACL 情報 開じる				
定義番号	IP 定義 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 Qos 種別 Qos 値	TCP/UDP/ICMP 定義	選択	
0	tcp 192.168.1.0/24 any any	TCP 定義 送信元ポート番号 any あて先ポート番号 21 TCP 接続要求 対象	選択 開じる	

「ACL 情報」 - [追加] / [修正] - 「IP 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。

15.1.2.6.1 IP フィルタリング情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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 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	TCP接続 要求	TOS	方向	操作
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		☒ 透過 ☐ 遮断					
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)					
	ポート番 号						
あて先情 報	IPアドレ ス						
	アドレス マスク	0 (0.0.0.0)					
	ポート番 号						
ICMP	タイプ						
	コード						
TCP接続要求		☒ 対象 ☐ 対象外					
TOS							
方向		入出力					
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、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。

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。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。

15.1.2.6.2 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] 「設定メニュー」→ルータ設定「LAN 情報」→[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	
<IPフィルタリング情報入力フィールド(条件にあてはまらない場合)>				
動作	☒ 透過 ☐ 遮断 ☐ 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。

情報保持タイマ

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。

15.1.2.7 IDS 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[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。

15.1.2.8 TOS 値書き換え情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[TOS 値書き換え情報]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[TOS 値書き換え情報]
→[ACL 定義参照] または「ACL 定義番号の[参照]」

表示条件入力				
表示個数 10		表示範囲 0~0		
■ACL 情報 開じる				
定義番号	IP 定義	TCP/UDP 定義	選択	
	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 Qos 種別 Qos 値			
0	tcp 192.168.1.0/24 any any	TCP 定義 送信元ポート番号 any あて先ポート番号 21 TCP 接続要求 対象	選択	
開じる				

「ACL 情報」 - [追加] / [修正] - 「IP 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。

15.1.2.8.1 TOS 値書き換え情報（旧定義）

〔操作〕 「設定メニュー」→ルータ設定「LAN 情報」→〔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 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 新TOS	操作
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: "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)		
	ポート番号			
あて先 情報	IPアドレス			
	アドレスマスク	0 (0.0.0.0)		
	ポート番号			
TOS				
新TOS				
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。

15.1.2.9 RIPフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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	☒ 透過 ☐ 遮断				
方向	☒ 受信 ☐ 送信				
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定				
	検索条件	☒ 完全に一致 ☐ マスクした結果が一致			
	IPアドレス				
	アドレスマスク	0.0.0.0			
メトリック値					
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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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。

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。

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
すべての経路情報がフィルタリングの対象となります。
- 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

- 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。

15.1.2.10 NAT 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[NAT 情報]

■NAT 情報		?
NAT の使用	☒ 使用しない ☐ NAT ☐ マルチ NAT ☐ 静的 NAT のみ ※NAT の使用と DHCP リレーサービスの併用はできません	
グローバルアドレス		
アドレス個数	1 個	
アドレス割当てタイマ	5 分	
NAT セキュリティ	☐ 通常 ☒ 高い	
IPsec パススルー	☒ 有効 ☐ 無効	
アプリ 対応	FTP	☒ 有効 ☐ 無効
	SIP	☒ 有効 ☐ 無効
	H.323	☒ 有効 ☐ 無効
	DNS	☒ 有効 ☐ 無効
	SNMP Trap	☒ 有効 ☐ 無効
	IRC	☒ 有効 ☐ 無効
	NTD メイン ログ オン	☒ 有効 ☐ 無効
	各種ストリーミング	☒ 有効 ☐ 無効
	各種オンラインゲーム	☒ 有効 ☐ 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。

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パスしか接続することができません。

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

15.1.2.11 静的 NAT 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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	グローバルアドレス	グローバルポート番号	プロトコル	操作
条件にあてはまらない場合の動作				破棄	修正 初期化
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				
	ポート番号	すべて (番号指定: “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				
	ポート番号	すべて (番号指定: “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: “その他”を選択時のみ有効です)			
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。

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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) を参照してください。処理するボタンをクリックします。

「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。

15.1.2.11.1 静的NAT情報（条件にあてはまらない場合の動作）

〔操作〕 「設定メニュー」→ルータ設定「LAN 情報」→〔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	☐ 透過 ☒ 破棄
----	---

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。

15.1.2.12 NAT あて先変換情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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		
グローバルアドレス		
		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。

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) を参照してください。処理するボタンをクリックします。

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、“-” で区切ります。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。

15.1.2.13 帯域制御（WFQ）情報

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

表示条件入力
表示定義内容
ACL 対応定義

■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

☐ 最優先
☐ ベストエフォート
☒ 使用率 %
☐ 使用帯域 Kbps
☐ 帯域を他と共有 共有できる定義が存在しません

ACL 定義番号 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、このインタフェースに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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[帯域制御 (WFQ) 情報]
→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
ACL 情報 開じる				
定義番号	IP 定義	TCP/UDP 定義	選択	
	プロトコル 送信元 IP アドレス/マスク 宛て先 IP アドレス/マスク Qos 種別 Qos 値			
0	tcp 192.168.1.0/24 any any	TCP 定義 送信元ポート番号 any 宛て先ポート番号 21 TCP 接続要求 対象	選択	
開じる				

「ACL 情報」 - [追加] / [修正] - 「IP 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。

15.1.2.13.1 帯域制御（WFQ）情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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 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	対象TOSフィールド値 帯域	操作
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: "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)		
	ポート番号			
あて先情報	IPアドレス			
	アドレスマスク	0 (0.0.0.0)		
	ポート番号			
対象TOSフィールド値				
帯域		☐ 最優先 ☐ ベストエフォート ☒ 使用率 % ☐ 使用帯域 Kbps ☐ 帯域を他と共有 共有できる定義が存在しません		
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。

15.1.2.14 Ingress ポリシールーティング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]
→[Ingress ポリシールーティング情報]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧 [\[2.3 システム最大値一覧\] \(P.37\)](#) 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] 「設定メニュー」→ルータ設定「LAN 情報」→[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参照] または「ポリシーグループ定義番号の[参照]」

表示条件入力		
表示個数	表示範囲	
10	0~0	
■ポリシーグループ情報 閉じる		
定義番号	定義内容	選択
0	パターン定義	
	バックアップとして使用	acl0
	使用しない	acl1
	使用する	acl0
	送出先定義	
lan0	192.168.100.10	選択
閉じる		

「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。

15.1.2.15 DHCP 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[DHCP 情報]

⚠ 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 

DHCP 機能

☒ 使用しない

☐ リレー機能を使用する

DHCPサーバIPアドレス 1	
DHCPサーバIPアドレス 2	
MACアドレスチェック	☐ ホストデータベース ☐ AAA 参照するAAA情報

☐ サーバ機能を使用する

割当て先頭IPアドレス	
割当てアドレス数	32
リース期間	1 日
デフォルトルータ広報	
DNSサーバ広報	
セカンダリDNSサーバ広報	
ドメイン名広報	
TIMEサーバ広報	
NTPサーバ広報	
MACアドレスチェック	☐ ホストデータベース ☐ AAA 参照するAAA情報

※“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

それぞれのインタフェースのDHCP機能を設定することができます。本装置を該当インタフェースのネットワークのDHCPサーバとして使用する場合は、“サーバ機能を使用する”を選択します。また、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サーバとして使用することもできます。その場合は、“リレー機能を使用する”を選択し、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。

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

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。

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。

15.1.2.16 ICMP 情報

[操作] 「設定メニュー」 → ルータ設定「LAN 情報」 → [修正] → [IP 関連] → [ICMP 情報]

■ ICMP 情報

ICMP リダイレクト パケット

☒ 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

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。

15.1.2.17 マルチキャスト情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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	☒ 使用しない ☐ static ☐ PIM-DM ☐ 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	☒ PIMルータのみ ☐ 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。

マルチキャストを使用できるインタフェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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。

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。

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。

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。

15.1.2.18 BGP/MPLS VPN 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[BGP/MPLS VPN 情報]

BGP/MPLS VPN情報

BGP/MPLS VPN機能

☒ 使用しない ☐ 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。

15.1.2.19 BGP/MPLS VPNスタティック経路情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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・修正情報は一覧の入力フィールド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
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

☐ デフォルトルート
 中継ルータアドレス
☒ 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

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 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37)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。

15.1.2.20 ARP 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IP 関連]→[ARP 情報]

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。

15.1.2.21 スタティック ARP 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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・修正情報は一覧の入力フィールド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
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			
MAC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。

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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

15.1.3 IPv6 関連

[操作] 「設定メニュー」→ルータ設定「LAN0 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スタティック経路情報
IPv6フィルタリング情報		IPv6 Traffic Class値書き換え情報		IPv6 RIPフィルタリング情報
IPv6帯域制御(WFQ)情報		IPv6 Ingressポリシールーティング情報		

「IPv6 帯域制御（WFQ）情報」は、LAN 情報（インタフェース：VLAN）では表示されません。

15.1.3.1 IPv6 基本情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 基本情報]

■ IPv6基本情報

IPv6

☒ 使用しない
☐ 使用する

インタフェースID

☒ 自動
☐ 指定する

IPv6 アドレス

アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラグ
	30 日 ☐	7 日 ☐	c0
	30 日 ☐	7 日 ☐	c0
	30 日 ☐	7 日 ☐	c0
	30 日 ☐	7 日 ☐	c0

ルータ広報

☒ 送信しない
☐ 送信する

最大送信間隔	600 秒
最小送信間隔	200 秒
Router Lifetime	1800 秒
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。

IPv6

IPv6 通信を行う場合は、“使用する”を選択します。

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 桁でインタフェース ID を指定します。このとき、他装置と同じインタフェース 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 IPv6 アドレスを 4 個まで設定できます。

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フェース ID を付与したものととなります。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、インタフェース ID 部分にはインタフェース 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

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

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

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

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。

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 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。省略値は 00 です。

- Managed address configuration flag 80
- Other stateful configuration flag 40

15.1.3.2 IPv6 RIP 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 RIP 情報]

■ IPv6 RIP 情報		
RIP送信	☒ 送信しない ☐ 送信する メトリック値 0	
RIP受信	☒ 受信しない ☐ 受信する	
集約経路送信	集約経路	破棄経路設定
	☐ デフォルトルート ☒ ネットワーク指定 	☒ 設定する
		☒ 設定する
		☒ 設定する
		☒ 設定する
サイトローカルプレフィックス	☐ 交換しない ☒ 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フェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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、同じあて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、そのあて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、そのあて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て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。

15.1.3.3 IPv6 スタティック経路情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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
全削除				
＜IPv6スタティック経路情報入力フィールド＞				
☐ デフォルトルート 中継ルータアドレス				
☒ 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 /				
中継ルータアドレス				
メトリック値 1				
優先度 0				
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 LAN 側に設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。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。

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）
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。
-

15.1.3.4 IPv6 フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[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	ACL 定義名	操作
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: ☒ 透過 ☐ 遮断

方向:

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、このインタフェースに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 フィルタリング情報]
→[ACL 定義参照] または「ACL 定義番号の[参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL 情報 閉じる				
定義番号	IPv6定義	TCP/UDP/ICMP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス 宛先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any 宛先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP定義 送信元ポート番号 any 宛先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「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。

15.1.3.4.1 IPv6 フィルタリング情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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IPv6アドレス/プレフィックス長	送信元ポート番号	宛先IPv6アドレス/プレフィックス長	宛先ポート番号	ICMPv6タイプ	ICMPv6コード	操作
			TCP接続要求	Traffic Class	方向				
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		☒ 透過 ☐ 遮断							
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		IPv6アドレス/プレフィックス長 /							
		ポート番号							
宛先情報		IPv6アドレス/プレフィックス長 /							
		ポート番号							
ICMPv6		タイプ							
		コード							
TCP接続要求		☒ 対象 ☐ 対象外							
Traffic Class									
方向		入出力							
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 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 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 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。

15.1.3.4.2 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] 「設定メニュー」→ルータ設定「LAN 情報」→[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]

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	
<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)>				
	☒ 透過 ☐ 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 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。

情報保持タイマ

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。

15.1.3.5 IPv6 Traffic Class 値書き換え情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]
→[IPv6 Traffic Class 値書き換え情報]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」- [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]
→[IPv6 Traffic Class 値書き換え情報]→[ACL 定義参照]または「ACL 定義番号の[参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL 情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス 宛先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any 宛先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any	UDP定義 送信元ポート番号 any 宛先ポート番号 53		
	any			
閉じる				

「ACL 情報」 - 「追加」 / 「修正」 - 「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。

15.1.3.5.1 IPv6 Traffic Class 値書き換え情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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		
全削除				
<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 (番号指定: ☐ “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			
	ポート番号			
あて先情報	IPv6アドレス/プレフィックス長			
	ポート番号			
Traffic Class				
新Traffic Class				
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 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 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。

15.1.3.6 IPv6 RIP フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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					
<IPv6 RIP フィルタリング情報入力フィールド>					
動作	☒ 透過 ☐ 遮断				
方向	☒ 受信 ☐ 送信				
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定				
	検索条件	☒ 完全に一致 ☐ マスクした結果が一致			
	プレフィックス / プレフィックス長	/			
メトリック値					
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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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指定します。

- すべて
すべての経路情報がフィルタリングの対象となります。
- 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。
 - 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”を選択すると、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。

15.1.3.7 IPv6帯域制御（WFQ）情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]→[IPv6 帯域制御（WFQ）情報]

現在、このネットワークに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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」（P37）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」 - [追加] / [修正] - 「IPv6 定義情報」で設定したACL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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]
→[IPv6 帯域制御 (WFQ) 情報]→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL 情報 閉じる				
定義番号	IPv6 定義	TCP/UDP 定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス 宛て先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP 定義 送信元ポート番号 any 宛て先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP 定義 送信元ポート番号 any 宛て先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「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。

15.1.3.7.1 IPv6 帯域制御 (WFQ) 情報 (旧定義)

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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				
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 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	対象Traffic Class 値 帯域	操作
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: ☐ “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			
	ポート番号			
あて先情報	IPv6アドレス／プレフィックス長			
	ポート番号			
対象Traffic Class 値				
帯域	☐ 最優先 ☐ ベストエフォート ☒ 使用率 % ☐ 使用帯域 Kbps ☐ 帯域を他と共有 共有できる定義が存在しません			
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 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 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。

15.1.3.8 IPv6 Ingress ポリシールーティング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[IPv6 関連]
→[IPv6 Ingress ポリシールーティング情報]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→ルータ設定「LAN 情報」→[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参照] または「ポリシーグループ定義番号の[参照]」

表示条件入力		
表示個数	表示範囲	
10	0~0	
■ポリシーグループ情報 閉じる		
定義番号	定義内容	選択
0	パターン定義	
	バックアップとして使用	acl0
	使用しない	acl1
	使用する	acl0
	選択	
送出先定義		
lan0	fe00::	
閉じる		

「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。

15.1.4 ブリッジ関連

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]

LAN0情報(物理LAN)			
共通情報	IP関連	IPv6関連	ブリッジ関連
ブリッジ情報		MACフィルタリング情報	静的MAC学習テーブル情報
帯域制御(WFQ)情報			

15.1.4.1 ブリッジ情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]→[ブリッジ情報]

■ブリッジ情報

ブリッジ機能

☒ 使用しない
 ☐ 使用する

グループ識別子

0

STP機能

☒ 使用しない
 ☐ 使用する

パスコスト

☒ 自動決定
 ☐ 指定する

インタフェース優先度

128

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

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。

インタフェース優先度

STPで使用するインタ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。

15.1.4.2 MACフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]→[MAC 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

MAC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	

全削除

<MACフィルタリング情報入力フィールド>

動作 ☒ 透過 ☐ 遮断

方向

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。

現在のインタフェースの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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」 - [追加] / [修正] - 「MAC 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正] → [ブリッジ関連] → [MAC フィルタリング情報] → 「ACL 定義参照」または「ACL 定義番号の [参照]」

表示条件入力		
表示個数	表示範囲	
10	1~1	
■ACL 情報 開じる		
定義番号	MAC 定義	選択
1	送信元MACアドレス	選択
	あて先MACアドレス	
	フォーマット種別	
	LSAP/type値	
	VLANタグ解析	
	any	
	00:00:0e:0a:12:34	
	llc	
	8080	
	しない	
閉じる		

「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。

15.1.4.2.1 MAC フィルタリング情報（旧定義）

〔操作〕 「設定メニュー」→ルータ設定「LAN 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）」

表示条件入力					
表示定義内容					
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ィールドで設定してください。					
優先順位	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	LSAP/type値 VLANタグ解析	操作
全削除					
<MACフィルタリング情報入力フィールド>					
動作	☒ 透過 ☐ 透過(接続中のみ) ☐ 遮断				
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 VLANタグ解析 ☒ しない ☐ する ☐ Ethernet形式 type値 VLANタグ解析 ☒ しない ☐ する				
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。					

現在のインタフェースの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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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”の場合は、LSAPを16進数を使用して、0～ffffの範囲で指定し、“Ethernet形式”の場合は、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。

15.1.4.3 静的 MAC 学習テーブル情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]
→[静的 MAC 学習テーブル情報]

■静的MAC学習テーブル情報

※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。

MACアドレス	操作
全削除	

<静的MAC学習テーブル情報入力フィールド>

MAC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。

現在、設定されている静的 MAC 学習テーブルの一覧です。静的 MAC 学習テーブル情報の定義数は、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) 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 桁の 16 進数) の形式で指定します。

15.1.4.4 帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[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

☐ 最優先
☐ ベストエフォート
☒ 使用率 %
☐ 使用帯域 Kbps
☐ 帯域を他と共有 共有できる定義が存在しません

ACL定義番号 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の一覧です。帯域制御の定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

使用する回線が 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。使用する回線が 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」- [追加] / [修正] - 「MAC 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[ブリッジ関連]
→[帯域制御 (WFQ) 情報]→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力		
表示個数	表示範囲	
10	1~1	
■ACL 情報 閉じる		
定義番号	MAC 定義	選択
	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値 VLANタグ解析	
1	any 00:00:0e:0a:12:34 llc 8080 しない	選択
閉じる		

「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 (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。

15.1.5 MPLS 関連

[操作] 「設定メニュー」→ルータ設定「LAN0 情報（物理 LAN）」→[修正]→[MPLS 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
MPLS基本情報	LDP情報	EoMPLS情報

15.1.5.1 MPLS 基本情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[MPLS 関連]→[MPLS 基本情報]

■MPLS基本情報

?

MPLS機能	☒ 使用しない ☐ 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。

15.1.5.2 LDP 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[MPLS 関連]→[LDP 情報]

■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		☒ DU ☐ DoD
LDP ラベル 保持方式		☐ liberal ☒ conservative
PHP 機能		☒ 使用する ☐ 使用しない
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 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 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。

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フェースに指定した場合は、そのインタフェースでは LDP を使用できません。

15.1.5.3 EoMPLS 情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報」→[修正]→[MPLS 関連]→[EoMPLS 情報]

■EoMPLS 情報	
EoMPLS 機能	☐ 使用しない ☒ 使用する
VC ID	
相手装置のIPv4アドレス	
VCタイプ	auto
EXP値書き換え	☒ 固定値 0 ☐ 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 と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 か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。

15.2 インタフェース：VLAN

[操作] 「設定メニュー」→ルータ設定「LAN0 情報 (VLAN)」→[修正] → [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

「IP 関連」、「IPv6 関連」、「ブリッジ関連」および「MPLS 関連」は、「インタフェース：物理 LAN」を参照してください。

15.2.1 共通情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報 (VLAN)」→[修正] → [共通情報]

LAN3情報(VLAN)		
共通情報	IP関連	IPv6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

「VRRP グループ情報」および「VRRP アクション情報」は、「インタフェース：物理 LAN」を参照してください。

15.2.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「LAN 情報 (VLAN)」→[修正] → [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

☒ 使用しない
☐ 使用する

最大送信レート

Mbps

VRRP機能

☒ 使用しない
☐ 使用する

パスワード

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フェースを選択します。すでに設定済みの物理インタ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-R180 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。

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。

15.2.1.2 VLAN プライオリティマッピング情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「LAN 情報 (VLAN)」→ [修正] → [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	TOS/Traffic Class	プライオリティ	操作
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	☒ IPv4 ☐ IPv6			
TOS/Traffic Class				
プライオリティ				
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、このLANに定義されているプライオリティマッピング情報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 Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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、“-” で区切ります。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。

15.2.1.3 MACアドレス認証情報

適用機種 全機種

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

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。

参照する AAA 情報

MAC アドレス認証を行う場合に参照する 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 シリアル情報

適用機種 Si-R220B

[操作] 「設定メニュー」 → [詳細設定メニュー] → ルータ設定「シリアル情報」

シリアル情報	
共通情報	モデム情報

16.1 共通情報

[操作] 「設定メニュー」 → [詳細設定メニュー] → ルータ設定「シリアル情報」 → [共通情報]

■ 共通情報 	
COMポート	☐ 使用しない ☒ 使用する
COMポート通信速度	115200 ▼
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	

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。

16.2 モデム情報

[操作] 「設定メニュー」→[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

☒ トーン式 ☐ パルス式

ダイヤルトーンの検出

☒ する ☐ しない

スピーカ

モード

キャリア検出までONにする

音量

☐ 小 ☒ 中 ☐ 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。

17 相手情報

[操作] 「設定メニュー」→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-R180、240、260B では、着信機能をサポートしていないため、「着信相手識別情報」は表示されません。

17.1 ネットワーク情報

適用機種 全機種

[操作] 「設定メニュー」→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	
全表示	10	1～9	
※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(1～9)			
※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
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	rmt0		
			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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P37)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] 「設定メニュー」→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。

17.1.1 共通情報

適用機種 全機種

[操作] 「設定メニュー」→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	

17.1.1.1 基本情報

[操作] 「設定メニュー」→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	☒ する ☐ しない
シェーピング	☒ 使用しない
	☐ 使用する
	最大送信レート 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。

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。

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。

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 以外	1 ～ 100000Kbps
Si-R570	1 ～ 1000000Kbps

17.1.2 接続先情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]

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

接続先情報

[操作] 「設定メニュー」→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>			
接続先名	ap0-0		
接続先種別	☐ ATM接続 VCI		
	☐ 専用線接続 ☐ ISDN接続 ダイヤル1 電話番号 サブアドレス		
	☐ フレームリレー接続 DLCI		
	☐ PPPoE接続 ☐ IPトンネル接続 ☐ IPsec/IKE接続 ☐ 別インターフェースから送出 ☐ MPLSトンネル接続 ☒ パケット破棄		
	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、Si-Rシリーズ 仕様一覧 [\[2.3 システム最大値一覧\]](#) (P37) 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-R180、220B、240、260B 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-R220B、370、570)
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。
- ISDN 接続 (Si-R220B、370、570)
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。

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。

- フレームリレー接続 (Si-R220B、370、570)
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は、Si-R シリーズ 仕様一覧 [「2.1 ソフトウェア仕様」](#) (P.30) 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-R220B)
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-R240)
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。本装置では、IP トンネル接続として、以下の 2 つがあります。
- IPv6 over IPv4
- Ethernet over IP
- 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。
- 別インタフェースから送出
パケット送出先として別インタ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。

17.1.2.1 ATM 接続

適用機種 Si-R260B,370,570

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：ATM 接続）]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
ATM接続		
基本情報	接続制御情報	マルチルーティング情報

17.1.2.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：ATM 接続）]→[基本情報]

■基本情報		
接続先名	ap0-0	
使用インタフェース	WAN0	
VCI	32	
VC速度	Kbps	
サービスタイプ	☒ CBR ☐ VBR 平均速度値 Kbps 最大バースト長 ☐ UBR+ 最低速度値 Kbps ☐ GFR+ 保証速度値 Kbps	
	OAM(F5) ☒ 受け付けない ☐ 受け付ける	
	到達性監視 ☒ 行わない ☐ 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	

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。

使用インタフェース

ATM 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 ATM 回線インタフェースの設定
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 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	
	ATM155M 拡張モジュール H1	64Kbps ~ 100Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R370	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	-	

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 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	
	ATM155M 拡張モジュール H1	64Kbps ~ 100Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R370	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	-	

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 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	
	ATM155M 拡張モジュール H1	64Kbps ~ 100Mbps (8Kbps 刻み、または 50Kbps 刻み)
Si-R370	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	-	

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。

17.1.2.1.2 接続制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：ATM 接続）]→[接続制御情報]

■接続制御情報

接続先監視

☒ 使用しない
☒ 使用する

送信元IPアドレス	
あて先IPアドレス	
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	100
異常時送信開始待ち時間	0 秒
監視方式	☒ 常時監視 ☐ 無通信時監視

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。

17.1.2.1.3 マルチルーティング情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：ATM 接続）]→[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 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
全削除					
<マルチルーティング情報入力フィールド>					
動作	この接続先を 使用する				
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)			
	ポート番号				
あて先 情報	IPアドレス				
	アドレス マスク	(0.0.0.0)			
	ポート番号				
TOS					
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、この接続先に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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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。
- 予約する
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

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。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。

17.1.2.2 専用線接続

適用機種 Si-R220B,370,570

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：専用線接続）]

相手情報 - ネットワーク情報(rmt0) - **接続先情報(ap0-0)**

専用線接続		
基本情報	接続制御情報	PPP情報
マルチルーティング情報		

「接続制御情報」および「マルチルーティング情報」は、[ATM接続] を参照してください。

17.1.2.2.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：専用線接続）]→[基本情報]

■基本情報 

接続先名	ap0-0
使用インタフェース	WAN1
DNSサーバ	

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

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 機能を使用する場合に必要です。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。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。

17.1.2.2.2 PPP 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：専用線接続）]→[PPP 情報]

■PPP情報 

MP接続	☒ 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

MP 接続

MP 接続を行う場合は、“する” を選択します。

17.1.2.3 ISDN 接続

適用機種 *Si-R220B,370,570*

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加 (接続先種別: ISDN 接続)]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
ISDN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	

「マルチルーティング情報」は、「ATM 接続」を参照してください。

17.1.2.3.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加 (接続先種別: ISDN 接続)]→[基本情報]

基本情報		
接続先名	ap0-0	
使用インタフェース	WAN2	
ダイヤル1	電話番号	03-7777-7777
	サブアドレス	
ダイヤル2	電話番号	
	サブアドレス	
ダイヤル3	電話番号	
	サブアドレス	
DNSサーバ		

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

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の電話番号にかからないときにはダイヤル2に、ダイヤル2の電話番号にかからないときはダイヤル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。

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。

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。

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

17.1.2.3.2 接続制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]→[追加 (接続先種別: ISDN 接続)]→[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
無通信監視タイマ	送受信パケット (について 0 秒)
課金単位時間	昼間(月～金) (08:00～19:00) 0 秒 夜間(土日の昼間) (19:00～23:00) 0 秒 深夜・早朝 (23:00～08:00) 0 秒
発信抑止	☐ 指定した時間を超えて接続しない 累計: 時間 ☐ 指定した課金を超えて接続しない 累計: 円
接続優先制御	☒ 使用しない ☐ 発信を優先する ☐ 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。

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、[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。

17.1.2.3.3 着信制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：ISDN 接続）]→[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
発信者番号による識別	☐ 番号チェックしない ☒ 接続先電話番号でチェックする ☐ 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
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。

17.1.2.3.4 PPP 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：ISDN 接続）]→[PPP 情報]

■PPP情報	
認証方式	☒ PAP ☒ 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	☒ しない ☐ する
	BAP/BACP利用 ☒ しない ☐ する ※発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効

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。

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。

17.1.2.4 フレームリレー接続

適用機種 Si-R220B,370,570

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：フレームリレー接続）]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
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

「接続制御情報」および「マルチルーティング情報」は、[ATM接続] を参照してください。

17.1.2.4.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：フレームリレー接続）]→[基本情報]

■基本情報

接続先名

ap0-0

使用インタフェース

WAN3

DLCI

16

CIR

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

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。

使用インタフェース

フレームリレー接続で使用するWANインタフェースを選択します。あらかじめWAN情報でフレームリレー回線インタ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、Si-Rシリーズ 仕様一覧「[2.1 ソフトウェア仕様](#)」(P30) 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。

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。

17.1.2.5 モデム接続

適用機種 Si-R220B

〔操作〕 「設定メニュー」→ルータ設定「相手情報」→〔ネットワーク情報〕→〔追加〕→〔接続先情報〕
→〔追加（接続先種別：モデム接続）〕

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
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	

「マルチルーティング情報」は、〔ATM 接続〕を参照してください。

17.1.2.5.1 基本情報

〔操作〕 「設定メニュー」→ルータ設定「相手情報」→〔ネットワーク情報〕→〔追加〕→〔接続先情報〕
→〔追加（接続先種別：モデム接続）〕→〔基本情報〕

■基本情報		
接続先名	ap0-0	
使用インタフェース	serial0	
ダイヤル1	電話番号	03-7777-7777
ダイヤル2	電話番号	
ダイヤル3	電話番号	
DNSサーバ		

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。

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。

使用インタフェース

本装置では、モデム接続で使用するインタ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の電話番号にかからないときにはダイヤル2に、ダイヤル2がかからないときはダイヤル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。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。

17.1.2.5.2 接続制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：モデム接続）]→[接続制御情報]

■接続制御情報	
無通信監視タイマ	送受信パケット (について 0 秒)
課金単位時間	昼間(月～金) (08:00～19:00) 0 秒
	夜間(土日の昼間) (19:00～23:00) 0 秒
	深夜・早朝 (23:00～08:00) 0 秒
発信抑止	☐ 指定した時間を超えて接続しない 累計: 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。

保存 キャンセル

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。

17.1.2.5.3 着信制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：モデム接続）]→[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。

17.1.2.5.4 PPP 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：モデム接続）]→[PPP 情報]

■PPP情報		
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	
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。

17.1.2.6 データ通信カード接続

適用機種 Si-R240

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：データ通信カード接続）]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
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	

「基本情報」、「着信制御情報」および「PPP 情報」は、[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」は、[ATM 接続] を参照してください。

17.1.2.6.1 接続制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：データ通信カード接続）]→[接続制御情報]

接続制御情報		
無通信監視タイマ	送受信パケット (について) 0 秒	
課金単位時間	昼間(月～金) (08:00～19:00)	0 秒
	夜間(土日の昼間) (19:00～23:00)	0 秒
	深夜・早朝 (23:00～08:00)	0 秒
強制切断	☐ 指定した時間を超えたら切断する	累計: 時間
	☐ 指定したパケット数を超えたら切断する	累計: / パケット(128/ バイト換算)
発信抑止	☐ 指定した時間を超えて接続しない	
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		

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止を接続時間によって行うことができます。発信抑止を行う場合は、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。

17.1.2.7 PPPoE 接続

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：PPPoE 接続）]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
■ 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	

「マルチルーティング情報」は、「ATM 接続」を参照してください。

17.1.2.7.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：PPPoE 接続）]→[基本情報]

■ 基本情報

接続先名

ap0-0

使用インタフェース

LAN1

DNSサーバ

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

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。

使用インタフェース

通信を行うインタ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。
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。

17.1.2.7.2 接続制御情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：PPPoE 接続）]→[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

無通信監視タイマ

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、[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。

17.1.2.7.3 PPP 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：PPPoE 接続）]→[PPP 情報]

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。

17.1.2.7.4 PPPoE 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：PPPoE 接続）]→[PPPoE 情報]

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。

17.1.2.8 IP トンネル接続

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IP トンネル接続）]

相手情報←ネットワーク情報(rmt0)← 接続先情報(ap0-0)	
IPTunnel接続	
基本情報	接続制御情報

「接続制御情報」は、「ATM 接続」を参照してください。

17.1.2.8.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IP トンネル接続）]→[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

- IPv6 over IPv4 の場合
IPv4 形式の IP アドレスを指定します。
- Ethernet over IP の場合
IPv4 トンネルの場合は IPv4 形式、IPv6 トンネルの場合は IPv6 形式のアドレスを指定します。

有効範囲)

10.0.1 ～ 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:ffff

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

17.1.2.9 IPsec/IKE 接続

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加 (接続先種別: IPsec/IKE 接続)]

「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“手動鍵使用” および “動的VPN 接続” 以外を選択した場合

相手情報－ネットワーク情報(rmt0)－接続先情報(ap0-0)		
IPsec/IKE接続		
基本情報	接続制御情報	IPsec情報
IKE情報	拡張IPsec対象範囲情報	マルチルーティング情報

「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“手動鍵使用” を選択した場合

相手情報－ネットワーク情報(rmt0)－接続先情報(ap0-0)		
IPsec/IKE接続		
基本情報	接続制御情報	IPsec情報
拡張IPsec対象範囲情報	マルチルーティング情報	

「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“動的VPN 接続” を選択した場合

相手情報－ネットワーク情報(rmt0)－接続先情報(ap0-0)		
IPsec/IKE接続		
基本情報	接続制御情報	IPsec情報
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		

「接続制御情報」および「マルチルーティング情報」は、[ATM 接続] を参照してください。

17.1.2.9.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[基本情報]

■基本情報

接続先名

ap0-0

鍵交換モード

☒ Aggressive Mode(Initiator)使用

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

IDタイプ ☒ FQDN ☐ User-FQDN

☐ Aggressive Mode(Responder)使用

自側エンドポイント

相手側エンドポイント

相手装置識別情報

IDタイプ ☒ FQDN ☐ User-FQDN

☐ Main Mode使用

相手側エンドポイント

自側エンドポイント

☐ 手動鍵使用

相手側エンドポイント

自側エンドポイント

☐ IKEは他の接続先情報を使用

接続先名

使用できる接続先情報が存在しません

☐ 動的VPN接続

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

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。

鍵交換モード

鍵交換モードを以下の6つから選択します。

- Aggressive Mode（Initiator）使用
自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（Initiator）を利用する場合、相手エンドポイント装置にAggressive Mode（Responder）を設定してください。

- 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 を利用して通信をする場合に選択します。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てください。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 使用
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 を設定してください。
- 手動鍵使用
手動鍵設定での IPsec を利用して通信を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。
- IKE は他の接続先情報を使用
同じ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。
- 動的 VPN 接続
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。

自側／相手側エンドポイント

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:ffff

fec0:: ~ feff:ffff: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、「鍵交換モード」で “Aggressive Mode (Initiator) 使用” または “動的 VPN 接続” を設定したときだけです。

自装置／相手装置識別情報

自装置／相手装置を識別する名前を 64 文字以内で指定します。

ID タイプ

ネゴシエーションの交換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。

17.1.2.9.2 IPsec 情報（自動鍵）

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[IPsec 情報（自動鍵）]

⚠ 設定ホストと本装置との通信パケットが対象パケットとなる設定を行うとその設定ホストからの設定変更ができなくなる場合があります。

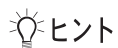
■ IPsec 情報(自動鍵) ?

対象 パケ ット	自側IPアドレ ス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
	相手側IPアド レス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。
SA の 設 定	暗号アルゴリ ズム	☐ aes-cbc-256 ☐ aes-cbc-192 ☐ aes-cbc-128 ☐ 3des-cbc ☒ des-cbc ☐ null
	認証アルゴリ ズム	☒ hmac-md5 ☐ hmac-sha1 ☐ 認証なし
	PFS時のDHグ ループ	使用しない
	SA有効時間	8 時間
	SA有効デー タ量	0 GByte
SA 更 新	Initiator 時 間 デ ー タ 量	90 秒 0 MByte
	Responder時	☐ 更新しない ☒ 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」の鍵交換モードで、“手動鍵使用” および “動的VPN 接続” 以外を選択した場合に表示されます。



ヒント

◆ 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	○	AH (認証)
○	認証なし	ESP (暗号)
○	○	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。

17.1.2.9.3 IPsec 情報（手動鍵）

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[IPsec 情報（手動鍵）]

⚠ 設定ホストと本装置との通信パケットが対象パケットとなる設定を行うとその設定ホストからの設定変更ができなくなる場合があります。

■ IPsec 情報(手動鍵) 

対象パケット (送信用)	自側IPアドレス		
	自側アドレスマスク	0 (0.0.0.0) 	
	相手側IPアドレス		
	相手側アドレスマスク	0 (0.0.0.0) 	
SAの設定 (送信用)	SPI値	(16進数)	
	暗号アルゴリズム	des-cbc 	
	暗号鍵	鍵識別	☒ 16進数 ☐ 文字列
		鍵	
	認証鍵	鍵識別	☒ 16進数 ☐ 文字列
		鍵	
対象パケット (受信用)	相手側IPアドレス		
	相手側アドレスマスク	0 (0.0.0.0) 	
	自側IPアドレス		
	自側アドレスマスク	0 (0.0.0.0) 	
SAの設定 (受信用)	SPI値	(16進数)	
	暗号アルゴリズム	des-cbc 	
	暗号鍵	鍵識別	☒ 16進数 ☐ 文字列
		鍵	
	認証鍵	鍵識別	☒ 16進数 ☐ 文字列
		鍵	

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。

この画面は、「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“手動鍵使用”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）」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 ～ fffffff 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 桁	8 文字
3DES-CBC	1～48 桁	24 文字
AES-CBC-128	1～32 桁	16 文字
AES-CBC-192	1～48 桁	24 文字
AES-CBC-256	1～64 桁	32 文字

16 進数で 16 桁（DES-CBC 指定時。3DES-CBC 指定時は 48 桁。AES-CBC-128 指定時は 32 桁。AES-CBC-192 指定時は 48 桁。AES-CBC-256 指定時は 64 桁。）未満の鍵を指定した場合は、16（64）桁になるまで、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。

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 桁	16 文字
HMAC-SHA1	1～40 桁	20 文字

16 進数で 32 桁（HMAC-MD5 指定時、HMAC-SHA1 指定時は 40 桁）未満の鍵を指定した場合は、32（40）桁になるまで、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。

17.1.2.9.4 IPsec 情報（動的VPN）

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[IPsec 情報（動的VPN）]

■ IPsec 情報(動的VPN)		?
SA の 設 定	暗号アルゴリズム	☐ aes-cbc-256 ☐ aes-cbc-192 ☐ aes-cbc-128 ☐ 3des-cbc ☒ des-cbc ☐ null
	認証アルゴリズム	☒ hmac-md5 ☐ hmac-sha1 ☐ 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte
SA更新	Initiator 時	時間 90 秒 データ量 0 MByte
	Responder 時	☐ 更新しない ☒ 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」の鍵交換モードで、“動的VPN 接続”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。

17.1.2.9.5 IKE 情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[IKE 情報]

■IKE情報		
IKE認証鍵	鍵識別	☐ 16進数 ☒ 文字列
	鍵	
IKE認証方式	shared	
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		☒ 対象パケット送信契機 ☐ 対象回線接続契機
NATトラバースル機能		☒ 使用しない ☐ 使用する
IKEセッション監視	あて先IPアドレス	
	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。

この画面は、「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“手動鍵使用” および “動的VPN 接続” 以外を選択した場合に表示されます。

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桁	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。

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／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。

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」画面の自側トンネルエンドポイント、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。

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。

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。

17.1.2.9.6 IKE 情報（動的VPN）

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]→[追加（接続先種別：IPsec/IKE 接続）]→[IKE 情報（動的VPN）]

■IKE情報(動的VPN)

?

IKE認証鍵	鍵識別	16進数 文字列
	鍵	
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		☒ 対象パケット送信契機 ☐ 対象回線接続契機

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」の鍵交換モードで、“動的VPN 接続”を選択した場合に表示されます。各項目の説明は、「IKE 情報」を参照してください。

17.1.2.9.7 拡張 IPsec 対象範囲情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[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。

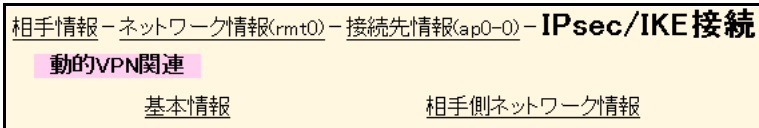
定義番号	拡張IPsec対象範囲自側IPアドレス/マスク	拡張IPsec対象範囲相手側IPアドレス/マスク	操作
	[全削除]		
＜拡張IPsec対象範囲情報入力フィールド＞			
拡張 IPsec対 象範囲	自側IPア ドレス/マ スク	IPv4すべて （"指定する"を選択時のみ有効です。） ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。	
	相手側 IPアドレ ス/マス ク	IPv4すべて （"指定する"を選択時のみ有効です。） ※IPv4アドレス/マスクビット形式もしくはIPv6アドレ ス/プレフィックス長形式で入力してください。	
		[追加] [キャンセル]	

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。

17.1.2.9.8 動的VPN関連

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加 (接続先種別: IPsec/IKE 接続)]→[基本情報 (鍵交換モード: 動的VPN 接続)]
→[保存]→[動的VPN 関連]



17.1.2.9.9 動的VPN関連 (基本情報)

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加 (接続先種別: IPsec/IKE 接続)]→[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。

17.1.2.9.10 動的VPN関連（相手側ネットワーク情報）

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：IPsec/IKE 接続）]→[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	※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。		
テンプレートを使用して接続要求	☒ しない ☐ する		
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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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/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。

17.1.2.10 別インタフェースから送出

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：別インタフェースから送出）]

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

「接続制御情報」および「マルチルーティング情報」は、[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。

17.1.2.10.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：別インタフェースから送出）]→[基本情報]

■基本情報		
接続先名	ap0-0	
送出先インタフェース	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。

送出先インタフェース

パケットを送出するインタ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、転送することができません。

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:ffff

17.1.2.11 MPLS トンネル接続

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：MPLS トンネル接続）]

相手情報 - ネットワーク情報(rmt0) - 接続先情報(ap0-0)		
MPLSトンネル接続		
基本情報	接続制御情報	マルチルーティング情報

「接続制御情報」および「マルチルーティング情報」は、[ATM 接続] を参照してください。

17.1.2.11.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：MPLS トンネル接続）]→[基本情報]

■基本情報		[?]
接続先名	ap0-0	
送出先インタフェース	LAN0 ▼	
IPv4転送先ルータ		
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。

送出先インタフェース

パケットを送出するインタ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

17.1.2.12 パケット破棄

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加（接続先種別：パケット破棄）]→[パケット破棄]

相手情報	ネットワーク情報(rmt0)	接続先情報(ap0-0)
パケット破棄 基本情報		

17.1.2.12.1 基本情報

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[接続先情報]
→[追加]→[パケット破棄]→[基本情報]

■基本情報 	
接続先名	ap0-0
パケット破棄	☐ しない ☒ する ※“破棄しない”を選択した場合、この接続先情報は削除されます。
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	

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。

17.1.3 PPP 関連

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[PPP 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
MPLS関連	
圧縮情報	MP情報

Si-R180、260B は、「MP 情報」は表示されません。

17.1.3.1 圧縮情報

[操作] 「設定メニュー」→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]

■圧縮情報

?

ヘッダ圧縮 (IPCP)	☒ VJ ☐ IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	☐ IPヘッダ圧縮
データ圧縮 (CCP)	☐ 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。

Si-R180、260B は、「データ圧縮」の項目はありません。

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-R220B、240、370、570)

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。

17.1.3.2 MP 情報

適用機種 Si-R220B,370,570

[操作] 「設定メニュー」→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

1

MP 回線最大リンク数

2

最小分割長

トラフィックによる増減

☒ 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。

保存

キャンセル

Si-R220B は、“MP 回線最大リンク数” の項目はありません。

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-R220B	1～2
Si-R370、570	1～23

MP 回線最大リンク数（Si-R370、570）

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

17.1.4 IP 関連

適用機種 全機種

[操作] 「設定メニュー」→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	MPLS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(WFQ)情報		
Ingressポリシ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-R180、220B、240 では、ATM をサポートしていないため、「CLP 値設定情報」は表示されません。

17.1.4.1 IP 基本情報

[操作] 「設定メニュー」→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

☐ 設定しない
☒ 設定する

相手IPアドレス

自側IPアドレス

MSS書き換え

☒ 使用しない
☐ 使用する

書き換えサイズ

0 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”の一方だけを指定し、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、誤って 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。

17.1.4.2 RIP 情報

[操作] 「設定メニュー」→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]

RIP情報

RIP送信

☒ 送信しない
☐ V1で送信する
☐ V2で送信する
☐ V2(Multicast)で送信する

RIP受信

☒ 受信しない
☐ V1で受信する
☐ V2、V2(Multicast)で受信する

《 RIP 送信時は加算するメトリック値を設定してください。》
 メトリック値

《 RIP V2使用時で認証/パケットを破棄しない時はRIP V2パスワードを設定してください。》

認証/パケット

☐ 破棄する
☒ 破棄しない
 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。

RIPを使用できるインタフェースの定義数は、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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

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。

17.1.4.3 OSPF 情報

[操作] 「設定メニュー」→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	☒ 使用しない ☐ 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	☒ 認証を行わない ☐ テキスト認証 鍵種別 ☒ 文字列 ☐ 16進数 認証鍵 ☐ MD5認証 MD5認証鍵ID MD5認証鍵
パケット送信	☐ 抑止する ☒ 抑止しない
送信方法	☒ マルチキャストで送信 ☐ ユニキャストで送信
MTU値確認	☒ 確認する ☐ 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。

ループバックインタフェースも含めて、OSPF を使用できるインタフェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

- 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フェースには上限があります。OSPF を使用するインタ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勧めします。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”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 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。

17.1.4.4 スタティック経路情報

[操作] 「設定メニュー」→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>

ネットワーク	☐ デフォルトルート ☒ ネットワーク指定
	あて先IPアドレス あて先アドレスマスク 0.0.0.0
メトリック値	1
優先度	0
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、相手側に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。Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) を参照してください。処理するボタンをクリックし、次の処理に進みます。

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。

17.1.4.5 IP フィルタリング情報

〔操作〕 「設定メニュー」→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
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	ACL 定義名	操作
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 ☒ 透過 ☐ 透過(接続中のみ) ☐ 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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
ACL 情報 開じる				
定義番号	IP定義 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 Qos種別 Qos値	TCP/UDP/ICMP定義	選択	
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象 選択 UDP定義 送信元ポート番号 any あて先ポート番号 53	開じる	

「ACL 情報」 - [追加] / [修正] - 「IP 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。

17.1.4.5.1 IP フィルタリング情報（旧定義）

[操作] 「設定メニュー」→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							
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 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	TCP接続 要求	TOS	方向	操作
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		☒ 透過 ☐ 透過(接続中のみ) ☐ 遮断					
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					
	ポート番 号						
あて先情 報	IPアドレ ス						
	アドレス マスク	0 0.0.0.0					
	ポート番 号						
ICMP	タイプ						
	コード						
TCP接続要求		☒ 対象 ☐ 対象外					
TOS							
方向		入出力					
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、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。

17.1.4.5.2 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] 「設定メニュー」→ルータ設定「相手情報」→[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 ACL定義名	操作
<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。

情報保持タイマ

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。

17.1.4.6 IDS 情報

[操作] 「設定メニュー」→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。

17.1.4.7 TOS 値書き換え情報

[操作] 「設定メニュー」→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]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」- [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照]または「ACL 定義番号の[参照]」

表示条件入力			
表示個数 10		表示範囲 0~0	
■ACL 情報 開じる			
定義番号	IP定義 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 Qos種別 Qos値	TCP/UDP定義	選択
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象 選択 UDP定義 送信元ポート番号 any あて先ポート番号 53	開じる

「ACL 情報」 - [追加] / [修正] - 「IP 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。

17.1.4.7.1 TOS 値書き換え情報 (旧定義)

[操作] 「設定メニュー」→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 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 新TOS	操作
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: ☐ “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)		
	ポート番号			
あて先 情報	IPアドレス			
	アドレスマスク	0 (0.0.0.0)		
	ポート番号			
TOS				
新TOS				
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。

17.1.4.8 RIPフィルタリング情報

[操作] 「設定メニュー」→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	☒ 透過 ☐ 遮断				
方向	☒ 受信 ☐ 送信				
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定				
	検索条件 ☒ 完全に一致 ☐ マスクした結果が一致				
	IPアドレス				
	アドレスマスク 0 0.0.0.0				
メトリック値					
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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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、(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。

17.1.4.9 NAT情報

[操作] 「設定メニュー」→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	☒ 使用しない ☐ NAT ☐ マルチNAT ☐ 静的NATのみ
グローバルアドレス	
アドレス個数	1 個
アドレス割当てタイマ	5 分
NATセキュリティ	☐ 通常 ☒ 高い
IPsecパススルー	☒ 有効 ☐ 無効
アプリ 対応	FTP ☒ 有効 ☐ 無効
	SIP ☒ 有効 ☐ 無効
	H.323 ☒ 有効 ☐ 無効
	DNS ☒ 有効 ☐ 無効
	SNMP Trap ☒ 有効 ☐ 無効
	IRC ☒ 有効 ☐ 無効
	NTドメインログオン ☒ 有効 ☐ 無効
	各種ストリーミング ☒ 有効 ☐ 無効
	各種オンラインゲーム ☒ 有効 ☐ 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。

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。

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パスしか接続することができません。

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

17.1.4.10 静的 NAT 情報

[操作] 「設定メニュー」→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	グローバルアドレス	グローバルポート番号	プロトコル	操作
条件にあてはまらない場合の動作				破棄	修正 初期化
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				
	ポート番号	すべて (番号指定: “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				
	ポート番号	すべて (番号指定: “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: “その他”を選択時のみ有効です)			
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。

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、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」](#) (P37) 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。

17.1.4.10.1 静的 NAT 情報（条件にあてはまらない場合の動作）

[操作] 「設定メニュー」→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	☐ 透過 ☒ 破棄
----	---

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。

17.1.4.11 NAT あて先変換情報

[操作] 「設定メニュー」→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		
グローバルアドレス		
		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。

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) を参照してください。処理するボタンをクリックします。

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、“-” で区切ります。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。

17.1.4.12 帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→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]

現在、このネットワークに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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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」- [追加] / [修正] - 「IP 定義情報」で設定したACL 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、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] 「設定メニュー」→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定義参照]または「ACL定義番号の[参照]」

表示条件入力			
表示個数 10		表示範囲 0~0	
■ACL情報 開じる			
定義番号	IP定義 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 Qos種別 Qos値	TCP/UDP定義	選択
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象 UDP定義 送信元ポート番号 any あて先ポート番号 53	選択 開じる

「ACL情報」- [追加] / [修正] - 「IP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。

17.1.4.12.1 帯域制御（WFQ）情報（旧定義）

[操作] 「設定メニュー」→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 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	対象TOSフィールド値 帯域	操作
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: ☐ “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)		
	ポート番号			
あて先情報	IPアドレス			
	アドレスマスク	0 (0.0.0.0)		
	ポート番号			
対象TOSフィールド値				
帯域		☐ 最優先 ☐ ベストエフォート ☒ 使用率 % ☐ 使用帯域 Kbps ☐ 帯域を他と共有 共有できる定義が存在しません		
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。

17.1.4.13 Ingress ポリシールーティング情報

[操作] 「設定メニュー」→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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P.37\)](#) 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] 「設定メニュー」→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参照] または「ポリシーグループ定義番号の[参照]」

表示条件入力		
表示個数	表示範囲	
10	0~0	
■ポリシーグループ情報 閉じる		
定義番号	定義内容	選択
0	パターン定義	
	バックアップとして使用	acl0
	使用しない	acl1
	使用する	acl0
	選択	
送出先定義		
lan0	192.168.100.10	
閉じる		

「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。

17.1.4.14 CLP 値設定情報

適用機種 Si-R260B,370,570

[操作] 「設定メニュー」→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]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」- [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力			
表示個数 10		表示範囲 0~0	
■ACL 情報 開じる			
定義番号	IP 定義 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 Qos種別 Qos値	TCP/UDP 定義	選択
0	tcp 192.168.1.0/24 any any	TCP 定義 送信元ポート番号 any あて先ポート番号 21 TCP 接続要求 対象 UDP 定義 送信元ポート番号 any あて先ポート番号 53	選択 開じる

「ACL 情報」 - [追加] / [修正] - 「IP 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。

17.1.4.14.1 CLP 値設定情報（旧定義）

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールド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 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
全削除					
<CLP値設定情報入力フィールド>					
CLP値	☒ 0を設定する ☐ 1を設定する				
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)			
	ポート番号				
あて先情報	IPアドレス				
	アドレスマスク	0 (0.0.0.0)			
	ポート番号				
TOS					
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、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、“,” で区切ります。範囲指定の場合は“-” で区切ります。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、すべての TOS フィールド値が CLP 値設定の対象となります。

17.1.4.15 マルチキャスト情報

[操作] 「設定メニュー」→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	☒ 使用しない ☐ static ☐ PIM-DM ☐ 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	☒ PIMルータのみ ☐ 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。

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。

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。

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。

17.1.4.16 EXP 値書き換え情報

[操作] 「設定メニュー」→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]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」 - [追加] / [修正] - 「IP 定義情報」、「TCP 定義情報」および「UDP 定義情報」で設定した ACL 定義が表示されます。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] 「設定メニュー」→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定義参照]または「ACL定義番号の[参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL情報 開じる				
定義番号	IP定義 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 Qos種別 Qos値	TCP/UDP定義		選択
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象 UDP定義 送信元ポート番号 any あて先ポート番号 53	選択	

「ACL情報」- [追加] / [修正] - 「IP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。

「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。

17.1.4.16.1 EXP 値書き換え情報（旧定義）

〔操作〕 「設定メニュー」→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 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 EXP	操作
全削除				
<EXP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: ☐ “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)		
	ポート番号			
あて先情報	IPアドレス			
	アドレスマスク	0 (0.0.0.0)		
	ポート番号			
TOS				
EXP				
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、“;” で区切ります。範囲指定の場合は“-” で区切ります。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。

17.1.4.17 動的VPN情報

[操作] 「設定メニュー」→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、このネットワークに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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P37)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。

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」- [追加] / [修正] - 「IP定義情報」で設定したACL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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力			
表示個数 10		表示範囲 0~0	
■ACL情報 閉じる			
定義番号	IP定義	TCP/UDP定義	
	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 QoS種別 QoS値		
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 80 あて先ポート番号 any TCP接続要求 対象	
閉じる			

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 定義が表示されています。

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。

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。

17.1.5 IPv6 関連

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[IPv6 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	MPLS関連
IPv6基本情報			IPv6 RIP情報		IPv6スタティック経路情報	
IPv6フィルタリング情報			IPv6 Traffic Class値書き換え情報		IPv6 RIPフィルタリング情報	
IPv6帯域制御(WFQ)情報			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	

Si-R180、220B、240 では、ATMをサポートしていないため、「IPv6 CLP 値設定情報」は表示されません。

17.1.5.1 IPv6 基本情報

[操作] 「設定メニュー」→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基本情報

IPv6

☒ 使用しない
☐ 使用する

インタフェースID

IPv6 アドレス

アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラグ
	30 日 ☐	7 日 ☐	☐ 0
	30 日 ☐	7 日 ☐	☐ 0
	30 日 ☐	7 日 ☐	☐ 0
	30 日 ☐	7 日 ☐	☐ 0

ルータ広報

☒ 送信しない
☐ 送信する

最大送信間隔	600 秒
最小送信間隔	200 秒
Router Lifetime	1800 秒
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。

IPv6

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 桁の 16 進数でインタフェース ID を指定します。このとき、他装置と違うインタフェース ID 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 IPv6 アドレスを 4 個まで設定できます。

アドレスまたはプレフィックス

本装置の相手側の IPv6 アドレスを標準的な IPv6 アドレスで指定します。本装置ではプレフィックス長は 64 に固定されます。インタフェース ID 部分がすべて 0 の場合は、指定するアドレスはプレフィックスとして解釈されます。実際に利用するアドレスは、そのアドレスにインタフェース 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、インタフェース ID 部分にはインタフェース 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

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

Pv6 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

期限を定めない場合（無期限の場合）は、チェックボックスをチェックします。

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 2 桁の 16 進数で指定します。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。

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 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。省略値は 00 です。

- Managed address configuration flag 80
- Other stateful configuration flag 40

17.1.5.2 IPv6 RIP 情報

[操作] 「設定メニュー」→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	☒ 送信しない ☐ 送信する メトリック値 0	
RIP受信	☒ 受信しない ☐ 受信する	
集約経路送信	集約経路	破棄経路設定
	☐ デフォルトルート ☒ ネットワーク指定 	☒ 設定する
		☒ 設定する
		☒ 設定する
サイトローカルプレフィックス	☐ 交換しない ☒ 交換する 	☒ 設定する

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フェースの定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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、同じあて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、そのあて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、そのあて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て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。

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。

17.1.5.3 IPv6スタティック経路情報

[操作] 「設定メニュー」→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]

現在、相手側に設定されている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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P.37)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/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
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。

17.1.5.4 IPv6 フィルタリング情報

[操作] 「設定メニュー」→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

表示定義内容

ACL 対応定義

■ IPv6 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	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

透過 透過(接続中のみ) 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、このインタフェースに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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。

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」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP/ICMP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス あて先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP定義 送信元ポート番号 any あて先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「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。

17.1.5.4.1 IPv6 フィルタリング情報 (旧定義)

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールド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	あて先ポート番号	ICMPv6タイプ	ICMPv6コード	TCP接続要求	Traffic Class	方向	操作
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

透過
透過(接続中のみ)
遮断

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

IPv6アドレス/プレフィックス長

ポート番号

あて先情報

IPv6アドレス/プレフィックス長

ポート番号

ICMPv6

タイプ

コード

TCP接続要求

対象
対象外

Traffic Class

方向

入力のみ

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 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 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 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。

17.1.5.4.2 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] 「設定メニュー」→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	
<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	☒ 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。

情報保持タイマ

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。

17.1.5.5 IPv6 Traffic Class 値書き換え情報

[操作] 「設定メニュー」→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]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」- [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス あて先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP定義 送信元ポート番号 any あて先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「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。

17.1.5.5.1 IPv6 Traffic Class 値書き換え情報（旧定義）

[操作] 「設定メニュー」→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）」

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		
全削除				
<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 (番号指定: ☐ “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			
	ポート番号			
あて先情報	IPv6アドレス/プレフィックス長			
	ポート番号			
Traffic Class				
新Traffic Class				
		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 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 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。

17.1.5.6 IPv6 RIP フィルタリング情報

[操作] 「設定メニュー」→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					
<IPv6 RIP フィルタリング情報入力フィールド>					
動作	☒ 透過 ☐ 遮断				
方向	☒ 受信 ☐ 送信				
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定				
	検索条件	☒ 完全に一致 ☐ マスクした結果が一致			
	プレフィックス / プレフィックス長	/			
メトリック値					
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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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
すべての経路情報がフィルタリングの対象となります。
- 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。

17.1.5.7 IPv6帯域制御（WFQ）情報

[操作] 「設定メニュー」→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

<IPv6帯域制御(WFQ)情報入力フィールド>

帯域

☐ 最優先
☐ ベストエフォート
☒ 使用率 %
☐ 使用帯域 Kbps
☐ 帯域を他と共有 共有できる定義が存在しません

ACL定義番号

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、このネットワークに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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P37)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」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス 宛先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any 宛先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP定義 送信元ポート番号 any 宛先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「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。

17.1.5.7.1 IPv6 帯域制御 (WFQ) 情報 (旧定義)

[操作] 「設定メニュー」→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	送信元ポート番号	対象Traffic Class値
		あて先IPv6アドレス／プレフィックス長	あて先ポート番号	帯域
				操作
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: ☐ “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			
	ポート番号			
あて先情報	IPv6アドレス／プレフィックス長			
	ポート番号			
対象Traffic Class値				
帯域	☐ 最優先 ☐ ベストエフォート ☒ 使用率 % ☐ 使用帯域 Kbps ☐ 帯域を他と共有 共有できる定義が存在しません			
	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 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 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。

17.1.5.8 IPv6 Ingress ポリシールーティング情報

[操作] 「設定メニュー」→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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→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参照] または「ポリシーグループ定義番号の[参照]」

表示条件入力		
表示個数	表示範囲	
10	0~0	
■ポリシーグループ情報 閉じる		
定義番号	定義内容	選択
0	パターン定義	
	バックアップとして使用	acl0
	使用しない	acl1
	使用する	acl0
	選択	
送出先定義		
lan0	fe00::	
閉じる		

「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。

17.1.5.9 IPv6 CLP 値設定情報

適用機種 Si-R260B,370,570

[操作] 「設定メニュー」→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]

IPv6 CLP 値設定情報 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	CLP 値	ACL 定義番号	操作
		ACL 定義名	

全削除

<CLP 値設定情報入力フィールド>

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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「2.3 システム最大値一覧」(P37) 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」- [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 定義が表示されます。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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の[参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス 宛先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any 宛先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP定義 送信元ポート番号 any 宛先ポート番号 53		
閉じる				

「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 定義情報の一覧にし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。

17.1.5.10 IPv6 DHCP 情報

[操作] 「設定メニュー」→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]

■IPv6 DHCP情報			
DHCP機能		☒ 使用しない ☐ クライアント機能を使用する ☐ サーバ機能を使用する	
クライアント／サーバ機能共通	DUID	☒ 自動 ☐ 文字列で指定する ☐ 16進数で指定する 	
	IAID	☒ 自動 ☐ 指定する 	
クライアント機能	プレフィックス要求	☐ しない ☒ する ☐ 旧方式を使用する ※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。	
	DNSサーバアドレス要求	☒ する ☐ しない	
	リジェクト経路	☒ Blackhole ☐ Reject	
サーバ機能	プリファレンス値	0	
	プレフィックス広報	☒ しない ☐ する プレフィックス / Valid Lifetime ☐ 期限有 日 ▼ ☒ 無期限 Pref. Lifetime ☐ 期限有 日 ▼ ☒ 無期限 自動経路設定 ☒ する ☐ しない	
		DNSサーバ広報	
		セカンダリDNSサーバ広報	
		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		

DHCP 機能

それぞれのインタフェースの IPv6 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。
- クライアント機能を使用する
該当インタフェースを IPv6 DHCP クライアントとして運用します。
- サーバ機能を使用する
本装置を該当インタ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／サーバ機能共通

DUID

DUID を以下の3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。
- 文字列で指定する
ASCII コードを使用して 130 文字以内で DUID を指定します。
- 16 進数で指定する
16 進数を使用して 260 桁以内で DUID を指定します。

クライアント機能

IAID

IAID を以下の2つから選択します。

- 自動
自動生成される IAID を使用します。通常は、この設定を使用します。
- 指定する
10 進数を使用して 1～4294967295 の範囲で指定します。

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報告をしません。
- Reject
リジェクト経路あてのパケットを受信した場合、送信元にエラー報告をします。

サーバ機能

プリファレンス値

DHCP サーバのプリファレンス値を 10 進数を使用して 0～255 の範囲で指定します。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。

プレフィックス広報

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。

有効範囲)

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

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

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ます。

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。

DNS サーバ広報

DNS サーバの IPv6 アドレスを指定します。省略時は、DHCP サーバによる広報を行いません。

有効範囲)

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

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

セカンダリ DNS サーバ広報

セカンダリ DNS サーバの IPv6 アドレスを指定します。省略時は、DHCP サーバによる広報を行いません。

有効範囲)

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

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

17.1.5.11 IPv6 EXP 値書き換え情報

[操作] 「設定メニュー」→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]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

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。

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」- [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 定義が表示されます。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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス あて先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any	UDP定義 送信元ポート番号 any あて先ポート番号 53		
	any			
閉じる				

「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。

17.1.5.12 IPv6 動的VPN 情報

[操作] 「設定メニュー」→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]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) 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。

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」- [追加] / [修正] - 「IPv6 定義情報」で設定したACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示回数		表示範囲		
10		0~0		
■ACL情報 開じる				
定義番号	IPv6定義	TCP/UDP/ICMP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス 宛先IPv6アドレス/プレフィックス Qos種別 Qos値			
0	tcp	TCP定義 送信元ポート番号 any 宛先ポート番号 21 TCP接続要求 対象		選択
	2001:db8:1111:1000::/64			
	any			
	any			
		UDP定義 送信元ポート番号 any 宛先ポート番号 53		
開じる				

「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 定義が表示されています。

表示条件入力では、表示回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。

17.1.6 ブリッジ関連

適用機種 全機種

[操作] 「設定メニュー」→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]

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
ブリッジ情報		
MACフィルタリング情報		
静的MAC学習テーブル情報		
帯域制御(WFQ)情報		

17.1.6.1 ブリッジ情報

[操作] 「設定メニュー」→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]

ブリッジ情報

?

ブリッジ機能	☒ 使用しない ☐ 使用する
グループ識別子	0
STP機能	☒ 使用しない ☐ 使用する
	バスコスト ☒ 自動決定 ☐ 指定する
	インタフェース優先度 128

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。

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。

インタフェース優先度

STPで使用するインタ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。

17.1.6.2 MACフィルタリング情報

[操作] 「設定メニュー」→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]

表示条件入力

表示定義内容

ACL対応定義

■MAC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	

全削除

<MACフィルタリング情報入力フィールド>

動作 ☒ 透過 ☐ 透過(接続中のみ) ☐ 遮断

方向

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。

現在のインタフェースの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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P37)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」 - [追加] / [修正] - 「MAC 定義情報」で設定した ACL 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、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] 「設定メニュー」→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 定義参照] または「ACL 定義番号の [参照]」

表示条件入力		
表示回数	表示範囲	
10	1~1	
ACL 情報 閉じる		
定義番号	MAC 定義	選択
	送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値 VLANタグ解析	
1	any 00:00:0e:0a:12:34 llc 8080 しない	選択
閉じる		

「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、表示回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。

17.1.6.2.1 MAC フィルタリング情報（旧定義）

〔操作〕 「設定メニュー」→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）」

表示条件入力					
表示定義内容					
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ィールドで設定してください。					
優先順位	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	LSAP/type値 VLANタグ解析	操作
全削除					
<MACフィルタリング情報入力フィールド>					
動作	☒ 透過 ☐ 透過(接続中のみ) ☐ 遮断				
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 VLANタグ解析 ☒ しない ☐ する ☐ Ethernet形式 type値 VLANタグ解析 ☒ しない ☐ する				
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。					

現在のインタフェースの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、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) 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”の場合は、LSAPを16進数を使用して、0～ffffの範囲で指定し、“Ethernet形式”の場合は、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。

17.1.6.3 静的MAC学習テーブル情報

[操作] 「設定メニュー」→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]

■静的MAC学習テーブル情報

※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。

MACアドレス	操作
	全削除

<静的MAC学習テーブル情報入力フィールド>

MAC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。

現在、設定されている静的MAC学習テーブルの一覧です。静的MAC学習テーブルの定義数は、Si-Rシリーズ 仕様一覧「2.3 システム最大値一覧」(P.37)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桁の16進数）の形式で指定します。

17.1.6.4 帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→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
0	1 acl1	ベストエフォート	修正 削除

全削除

<帯域制御(WFQ)情報入力フィールド>

帯域

☐ 最優先
☐ ベストエフォート
☒ 使用率 %
☐ 使用帯域 Kbps
☐ 帯域を他と共有 0

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、このインタフェースに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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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」- [追加] / [修正] - 「MAC 定義情報」で設定したACL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、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] 「設定メニュー」→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]→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力		
表示回数	表示範囲	
10	1~1	
■ACL情報 閉じる		
定義番号	MAC定義 送信元MACアドレス あて先MACアドレス フォーマット種別 LSAP/type値 VLANタグ解析	選択
1	any 00:00:0e:0a:12:34 llc 8080 しない	選択
閉じる		

「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、表示回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。

17.1.7 MPLS 関連

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「相手情報」→[ネットワーク情報]→[追加]→[MPLS 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
MPLS基本情報	LDP情報

17.1.7.1 MPLS 基本情報

[操作] 「設定メニュー」→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基本情報

?

MPLS機能	☒ 使用しない ☐ 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

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。

17.1.7.2 LDP 情報

[操作] 「設定メニュー」→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]

■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		☒ DU ☐ DoD
LDP ラベル 保持方式		☒ liberal ☐ conservative
PHP 機能		☒ 使用する ☐ 使用しない
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フェースに指定した場合は、そのインタフェースでは 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。

17.2 着信相手識別情報

適用機種 Si-R220B,240,370,570

[操作] 「設定メニュー」→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	☒ しない ☐ する
認証方式	☒ PAP ☒ CHAP
MP接続	☒ しない ☐ する BAP/BACP利用 ☒ 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

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-R240は“MP 接続”の項目はありません。

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-R220B、370、570)

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。

18 テンプレート情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「テンプレート情報」

現在、設定されているテンプレート情報が表示されます。テンプレート情報の最大定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

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3つから選択します。

- ISDN (Si-R220B、370、570)
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)
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。

18.1 接続種別：ISDN

適用機種 Si-R220B,370,570

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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

18.1.1 共通情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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			

18.1.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[共通情報]→[基本情報]

■基本情報

テンプレート名

tmp0

使用インタフェース

すべて

使用するrmtインタフェース

rmt から インタフェースを予約

MTUサイズ

1500 バイト

無通信監視タイマ

送受信パケット (について 0 秒)

参照するAAA情報

☒ 指定しない
☐ 指定する

AAAグループID

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。

使用インタフェース

テンプレート着信で使用する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ますようになります。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。

18.1.2 PPP 関連

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[PPP 関連]

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
認証情報		圧縮情報	

18.1.2.1 認証情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[PPP 関連]
→[認証情報]

■ 認証情報	
認証方式	☐ PAP ☐ CHAP ☒ PAP/CHAP
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以下の3つから選択します。

- PAP
- CHAP
- PAP/CHAP

18.1.2.2 圧縮情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[PPP 関連]
→[圧縮情報]

■圧縮情報	
ヘッダ圧縮 (IPCP)	☒ VJ ☐ IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	☐ IPヘッダ圧縮
データ圧縮 (CCP)	☐ 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。

18.1.3 IP 関連

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]

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
IP基本情報	IPフィルタリング情報	IDSL情報	
TOS値書き換え情報	NAT情報	静的NAT情報	
NATあて先変換情報	帯域制御(WFQ)情報	Ingressポリシールーティング情報	

18.1.3.1 IP 基本情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]
→ [IP 基本情報]

■IP基本情報

DNSサーバ	☒ 設定しない ☐ 設定する
MSS書き換え	☒ 使用しない ☐ 使用する 書き換えサイズ 0 バイト
割当てIPアドレス	☒ 設定しない ☐ 設定する 先頭IPアドレス アドレス数

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。

保存 キャンセル

DNS サーバ

相手先と接続するときに通知する DNS サーバのアドレスを設定します。“設定しない”を選択した場合は、DNS サーバが存在しない、または 0.0.0.0 となります。

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

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。

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、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) 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

18.1.3.2 IPフィルタリング情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[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	ACL定義名	操作
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 ☒ 透過 ☐ 透過(接続中のみ) ☐ 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、このテンプレートに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]
→[IP フィルタリング情報]→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力			
表示個数		表示範囲	
10		0~0	
■ACL 情報 閉じる			
定義番号	IP 定義 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 QoS種別 QoS値	TCP/UDP/ICMP定義	選択
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象	選択
	192.168.1.0/24		
	any	UDP定義 送信元ポート番号 any あて先ポート番号 53	
	any	ICMP定義 ICMPタイプ any ICMPコード any	
閉じる			

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 定義が表示されています。

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。

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。

18.1.3.2.1 IP フィルタリング情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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 送信元ポート番号 宛先IPアドレス/ マスク 宛先ポート番号 ICMPタイプ ICMPコード	TCP接続 要求	TOS	方向	操作
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		☒ 透過 ☐ 透過(接続中のみ) ☐ 遮断					
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)					
	ポート番 号						
宛先情 報	IPアドレ ス						
	アドレス マスク	0 (0.0.0.0)					
	ポート番 号						
ICMP	タイプ						
	コード						
TCP接続要求		☒ 対象 ☐ 対象外					
TOS							
方向		入出力					
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、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選択します。

18.1.3.2.2 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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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
			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 ☒ 透過 ☐ 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。

「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。

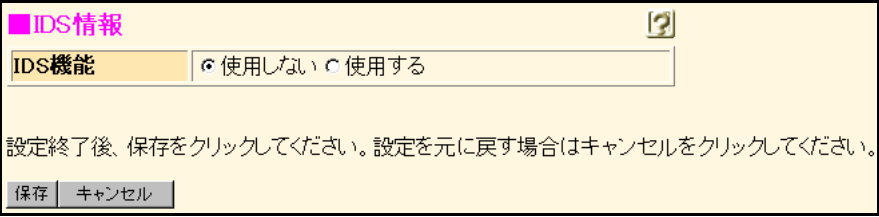
- 透過
IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
IP フィルタリング定義のどれにも一致しないで、プロトコルがTCPの場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルがUDPやそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイマ

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。

18.1.3.3 IDS 情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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。

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。

18.1.3.4 TOS 値書き換え情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]
→[TOS 値書き換え情報]

現在、このテンプレートに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

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」- [追加] / [修正] - 「IP 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]
→[TOS 値書き換え情報]→[ACL 定義参照]または「ACL 定義番号の[参照]」

表示条件入力				
表示個数		表示範囲		
10		0~0		
■ACL 情報 開じる				
定義番号	IP定義 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 Qos種別 Qos値	TCP/UDP定義		選択
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象 UDP定義 送信元ポート番号 any あて先ポート番号 53	選択	開じる

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 定義が表示されています。

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。

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。

18.1.3.4.1 TOS 値書き換え情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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 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 新TOS	操作
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: "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		
	ポート番号			
あて先 情報	IPアドレス			
	アドレスマスク	0 0.0.0.0		
	ポート番号			
TOS				
新TOS				
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。

18.1.3.5 NAT 情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[修正]→[IP 関連]→[NAT 情報]

■NAT情報		?
NATの使用	☒ 使用しない ☐ NAT ☐ マルチNAT ☐ 静的 NATのみ	
グローバルアドレス		
アドレス個数	1 個	
アドレス割当てタイマ	5 分	
NATセキュリティ	☐ 通常 ☒ 高い	
IPsecパススルー	☒ 有効 ☐ 無効	
アプリ対応	FTP	☒ 有効 ☐ 無効
	SIP	☒ 有効 ☐ 無効
	H.323	☒ 有効 ☐ 無効
	DNS	☒ 有効 ☐ 無効
	SNMP Trap	☒ 有効 ☐ 無効
	IRC	☒ 有効 ☐ 無効
	NTDメインログオン	☒ 有効 ☐ 無効
各種ストリーミング	☒ 有効 ☐ 無効	
各種オンラインゲーム	☒ 有効 ☐ 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。

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パスしか接続することができません。

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

18.1.3.6 静的 NAT 情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[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	グローバルアドレス	グローバルポート番号	プロトコル	操作
条件にあてはまらない場合の動作		破棄		修正	初期化
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				
	ポート番号	すべて (番号指定: “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				
	ポート番号	すべて (番号指定: “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: “その他” を選択時のみ有効です)				
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。

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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) を参照してください。処理するボタンをクリックします。

「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。

18.1.3.6.1 静的NAT情報（条件にあてはまらない場合の動作）

〔操作〕 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→〔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

☐ 透過
☒ 破棄

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。

18.1.3.7 NAT あて先変換情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[修正]→[IP 関連]
→[NAT あて先変換情報]

現在、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) を参照してください。処理するボタンをクリックします。

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、“-” で区切ります。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。

18.1.3.8 帯域制御 (WFQ) 情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報 (接続種別: ISDN)」→ [追加] → [IP 関連]
→ [帯域制御 (WFQ) 情報]

表示条件入力
表示定義内容
ACL対応定義

■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

☐ 最優先
☐ ベストエフォート
☒ 使用率 %
☐ 使用帯域 Kbps
☐ 帯域を他と共有 共有できる定義が存在しません

ACL定義番号 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、このインタフェースに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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P37)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」 - [追加] / [修正] - 「IP 定義情報」で設定したACL 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、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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]
→[帯域制御（WFQ）情報]→[ACL 定義参照]または「ACL 定義番号の[参照]」

表示条件入力			
表示個数 10		表示範囲 0~0	
■ACL 情報 閉じる			
定義番号	IP定義 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 Qos種別 Qos値	TCP/UDP定義	選択
0	tcp 192.168.1.0/24 any any	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象 UDP定義 送信元ポート番号 any あて先ポート番号 53	選択 閉じる

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」で設定した ACL 定義が表示されています。

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。

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。

18.1.3.8.1 帯域制御 (WFQ) 情報 (旧定義)

[操作] 「設定メニュー」→ルータ設定「テンプレート情報 (接続種別: 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 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	対象TOSフィールド値 帯域	操作
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: ☐ “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		
	ポート番号			
あて先情報	IPアドレス			
	アドレスマスク	0.0.0.0		
	ポート番号			
対象TOSフィールド値				
帯域		☐ 最優先 ☐ ベストエフォート ☒ 使用率 % ☐ 使用帯域 Kbps ☐ 帯域を他と共有 共有できる定義が存在しません		
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。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、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。

18.1.3.9 Ingress ポリシールーティング情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IP 関連]
→[Ingress ポリシールーティング情報]

現在、このテンプレートに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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参照] または「ポリシーグループ定義番号の[参照]」

表示条件入力		
表示個数	表示範囲	
10	0~0	
■ポリシーグループ情報 閉じる		
定義番号	定義内容	選択
0	パターン定義	
	バックアップとして使用	acl0
	使用しない	acl1
	使用する	acl0
	送出先定義	
lan0	192.168.100.10	選択
閉じる		

「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 IPv6 関連

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IPv6 関連]

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
IPv6基本情報	IPv6フィルタリング情報	IPv6 Traffic Class値書き換え情報	
IPv6帯域制御(WFQ)情報	IPv6 Ingressポリシールーティング情報		

18.1.4.1 IPv6 基本情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IPv6 関連]
→[IPv6 基本情報]

■IPv6基本情報

IPv6	☒ 使用しない ☐ 使用する
インタフェースID	☒ 自動 ☐ 指定する

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

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桁でインタフェース ID を指定します。このとき、他装置と同じインタフェース ID とならないような値を指定します。

記述例)

2001:db8:7654:3210

18.1.4.2 IPv6 フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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 ☒ 透過 ☐ 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、このテンプレートに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IPv6 関連]
→[IPv6 フィルタリング情報]→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力			
表示個数		表示範囲	
10		0~0	
■ACL情報			閉じる
定義番号	IPv6定義	TCP/UDP/ICMP定義	選択
	プロトコル 送信元IPv6アドレス/プレフィックス あて先IPv6アドレス/プレフィックス QoS種別 QoS値		
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象	選択
	any	UDP定義 送信元ポート番号 any あて先ポート番号 53 ICMP定義 ICMPタイプ any ICMPコード any	
	any		
	any		
			閉じる

「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 定義が表示されています。

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。

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。

18.1.4.2.1 IPv6 フィルタリング情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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

IPv6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	あて先ポート番号	ICMPv6タイプ	ICMPv6コード	TCP接続要求	Traffic Class	方向	操作
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

透過遮断

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

IPv6アドレス/プレフィックス長

ポート番号

あて先情報

IPv6アドレス/プレフィックス長

ポート番号

ICMPv6

タイプ

コード

TCP接続要求

対象対象外

Traffic Class

方向

入出力

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 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 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 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。

18.1.4.2.2 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〕 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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〕

IPv6 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	あて先ポート番号	ICMPv6タイプ	ICMPv6コード	TCP 接続 要求	Traffic Class	方向	操作
<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 ☒ 透過 ☐ 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、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。

情報保持タイマ

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。

18.1.4.3 IPv6 Traffic Class 値書き換え情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[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

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、このテンプレートに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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」- [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 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、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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IPv6 関連]
→[IPv6 Traffic Class 値書き換え情報]→[ACL 定義参照] または「ACL 定義番号の[参照]」

表示条件入力				
表示個数 10		表示範囲 0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス あて先IPv6アドレス/プレフィックス QoS種別 QoS値			
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象		選択
	any			
	any			
	any			
		UDP定義 送信元ポート番号 any あて先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 定義が表示されています。

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。

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。

18.1.4.3.1 IPv6 Traffic Class 値書き換え情報（旧定義）

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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）」

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		
全削除				
<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 (番号指定: ☐ “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			
	ポート番号			
あて先情報	IPv6アドレス/プレフィックス長			
	ポート番号			
Traffic Class				
新Traffic Class				
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 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 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。

18.1.4.4 IPv6帯域制御（WFQ）情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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

<IPv6帯域制御(WFQ)情報入力フィールド>

帯域

☐ 最優先
☐ ベストエフォート
☒ 使用率 %
☐ 使用帯域 Kbps
☐ 帯域を他と共有 共有できる定義が存在しません

ACL定義番号 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、このテンプレートに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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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」- [追加] / [修正] - 「IPv6 定義情報」で設定したACL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、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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IPv6 関連]
→[IPv6 帯域制御（WFQ）情報]→[ACL 定義参照] または「ACL 定義番号の [参照]」

表示条件入力				
表示個数 10		表示範囲 0~0		
■ACL情報 閉じる				
定義番号	IPv6定義	TCP/UDP定義		選択
	プロトコル 送信元IPv6アドレス/プレフィックス あて先IPv6アドレス/プレフィックス QoS種別 QoS値			
0	tcp	TCP定義 送信元ポート番号 any あて先ポート番号 21 TCP接続要求 対象		選択
	any			
	any			
	any			
		UDP定義 送信元ポート番号 any あて先ポート番号 53		
閉じる				

「ACL 情報」 - [追加] / [修正] - 「IPv6 定義情報」で設定した ACL 定義が表示されています。

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。

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。

18.1.4.4.1 IPv6 帯域制御 (WFQ) 情報 (旧定義)

[操作] 「設定メニュー」→ルータ設定「テンプレート情報 (接続種別: 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				
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 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	対象TOSフィールド値 帯域	操作
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: "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		
	ポート番号			
あて先情報	IPアドレス			
	アドレスマスク	0 0.0.0.0		
	ポート番号			
対象TOSフィールド値				
帯域		☐ 最優先 ☐ ベストエフォート ☒ 使用率 % ☐ 使用帯域 Kbps ☐ 帯域を他と共有 共有できる定義が存在しません		
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 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 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。

18.1.4.5 IPv6 Ingress ポリシールーティング情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：ISDN）」→[追加]→[IPv6 関連]
→[IPv6 Ingress ポリシールーティング情報]

現在、このテンプレートに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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参照] または「ポリシーグループ定義番号の[参照]」

表示条件入力		
表示個数	表示範囲	
10	0~0	
■ポリシーグループ情報 閉じる		
定義番号	定義内容	選択
0	パターン定義	
	バックアップとして使用	acl0
	使用しない	acl1
	使用する	acl0
	選択	
送出先定義		
lan0	fe00::	
閉じる		

「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。

18.2 接続種別：IPsec/IKE (RADIUS/AAA)

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：RADIUS/AAA）」→[追加]

テンプレート情報-テンプレート情報(tmp0)			
IPsec/IKE(RADIUS/AAA)			
共通情報	IP関連	IPv6関連	IPsec/IKE関連

「IP関連」および「IPv6関連」は、[接続種別：ISDN] を参照してください。

18.2.1 共通情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：RADIUS/AAA）」→[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(RADIUS/AAA)			
共通情報	IP関連	IPv6関連	IPsec/IKE関連
基本情報			

18.2.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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

無通信監視タイマ

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

☒ Aggressive Mode(Responder)使用

自側エンドポイント

IDタイプ

☒ FQDN ☐ User-FQDN

☐ Main Mode(Responder)使用

自側エンドポイント

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 以内で指定します。

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:ffff

fec0:: ～ feff:ffff: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、自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。

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。

18.2.2 IPsec/IKE 関連

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：RADIUS/AAA）」→ [追加]
→ [IPsec/IKE 関連]

テンプレート情報 - テンプレート情報(tmp0)

IPsec/IKE(RADIUS/AAA)			
共通情報	IP関連	IPv6関連	IPsec/IKE関連
IPsec情報		IKE情報	接続制御情報

18.2.2.1 IPsec 情報

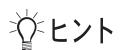
[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：RADIUS/AAA）」→ [追加]
→ [IPsec/IKE 関連] → [IPsec 情報]

■ IPsec 情報

SAの設定	暗号アルゴリズム	☐ aes-cbc-256 ☐ aes-cbc-192 ☐ aes-cbc-128 ☐ 3des-cbc ☒ des-cbc ☐ null	
	認証アルゴリズム	☒ hmac-md5 ☐ hmac-sha1 ☐ 認証なし	
	PFS時のDHグループ	使用しない	
	SA有効時間	8 時間	
	SA有効データ量	0 GByte	
SA更新	Initiator 時	時間	90 秒
		データ量	0 MByte
	Responder時	☒ 更新しない ☐ 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。

保存 キャンセル



ヒント

◆ 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	○	AH (認証)
○	認証なし	ESP (暗号)
○	○	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、0 KByte 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、0 KByte が設定されます。

18.2.2.2 IKE 情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：RADIUS/AAA）」→[追加]
→[IPsec/IKE 関連]→[IKE 情報]

■IKE情報		
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トラバース機能		☒ 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

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」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」画面の自側トンネルエンドポイントに 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。
-

18.2.2.3 接続制御情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：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	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

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

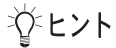
::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

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。



ヒント

◆ 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見なされます。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 進数値で指定します。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

18.3 接続種別：IPsec/IKE（動的VPN）

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[追加]

テンプレート情報 - テンプレート情報(tmp0)				
IPsec/IKE(動的VPN)				
共通情報	IP関連	IPv6関連	IPsec/IKE関連	動的VPN関連

「IP 関連」 および 「IPv6 関連」 は、[接続種別：ISDN] を参照してください。

18.3.1 共通情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[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)				
共通情報	IP関連	IPv6関連	IPsec/IKE関連	動的VPN関連
基本情報				

18.3.1.1 基本情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[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
無通信監視タイマ	送受信パケットについて 0 秒
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。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)

10.0.0.1 ～ 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。
-

18.3.2 IPsec/IKE 関連

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[追加]
→[IPsec/IKE 関連]

テンプレート情報 - テンプレート情報(tmp0)				
IPsec/IKE(動的VPN)				
共通情報	IP関連	IPv6関連	IPsec/IKE関連	動的VPN関連
IPsec情報		IKE情報		接続制御情報

「IPsec 情報」は、[接続種別：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。

18.3.2.1 IKE 情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[追加]
→[IPsec/IKE 関連] → [IKE 情報]

■IKE情報	
IKE 認証鍵	鍵識別 ☐ 16進数 ☒ 文字列
IKE 認証方式	shared
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

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指定します。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）を設定します。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。

16 進数鍵)

1 ～ 256 桁

文字列鍵)

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。

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。

18.3.2.2 接続制御情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[追加]
→ [IPsec/IKE 関連] → [接続制御情報]

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

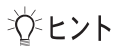
::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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。



ヒント

◆ 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見なされます。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 進数値で指定します。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

18.3.3 動的VPN関連

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[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)			
共通情報	IP関連	IPv6関連	IPsec/IKE関連
基本情報		自側ネットワーク情報	

18.3.3.1 基本情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[追加]
→[動的VPN関連]→[基本情報]

■基本情報

?

ドメイン情報		☒ 使用しない ☐ 使用する 0(example.jp.com)
サーバ情報	アドレス	
	ポート番号	5070
	認証ID	
	認証パスワード	
セカンダリサーバ情報	アドレス	
	ポート番号	5070
	認証ID	
	認証パスワード	
有効期間		1 時間
セッション更新間隔		☐ 更新しない ☒ 更新する 5 時間 5 分
クライアントIPアドレス		
ドメイン名		
VPN通信	利用インタフェース	lan0
	中継ルータアドレス	
	終端グローバルアドレス	
自側ユーザID		

※LANインタフェース選択時のみ指定してください

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。

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ーに従って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、送出インタフェースとなるインタフェースの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。

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フェースでlanインタフェースを指定した場合は、指定されたlanインタ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フェースでrmtインタフェースを指定した場合は、指定されたrmtインタ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。

18.3.3.2 自側ネットワーク情報

[操作] 「設定メニュー」→ルータ設定「テンプレート情報（接続種別：動的VPN）」→[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で接続する自側ネットワーク	動的VPNサーバ登録	操作
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	※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。		
動的VPNサーバ登録	☒ する ☐ しない		
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、このテンプレートに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/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。

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接続を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が設定されていれば、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
IPsec(IKE)c0a80100/24@example.com
IPsec(IKE)2001:db8:1111:1::/64@example.com

19 AAA 情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「AAA 情報」

AAA情報
グループID情報

19.1 グループID 情報

[操作] 「設定メニュー」→ルータ設定「AAA 情報」→ [グループ ID 情報]

■グループID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。

グループID	グループ名	操作
全削除		
<グループID情報追加フィールド>		
	グループ名	
		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、設定されているグループID 情報が表示されています。グループID 情報の定義数は Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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して、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] 「設定メニュー」→ルータ設定「AAA 情報」→ [グループ ID 情報] → [追加]

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連

19.1.1 共通情報

[操作] 「設定メニュー」→ルータ設定「AAA 情報」→ [グループ ID 情報] → [追加] → [共通情報]

AAA情報 - グループID情報(0)		
共通情報	AAAユーザ情報	RADIUS関連
基本情報		

19.1.1.1 基本情報

[操作] 「設定メニュー」→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]

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。

19.1.2 AAA ユーザ情報

[操作] 「設定メニュー」→ルータ設定「AAA 情報」→[グループ ID 情報]→[追加]→[AAA ユーザ情報]

[操作] 「設定メニュー」→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]

現在、設定されている AAA ユーザ情報が表示されています。AAA ユーザ情報の定義数は Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) 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 アドレス認証で利用する場合は、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。

[操作] 「設定メニュー」→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]

AAA情報-グループID情報(0)-AAAユーザ情報(0)				
認証情報	IP関連	IPv6関連	IPsec/IKE関連	サブリカント関連

19.1.2.1 認証情報

[操作] 「設定メニュー」→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]

AAA情報-グループID情報(0)-AAAユーザ情報(0)				
認証情報	IP関連	IPv6関連	IPsec/IKE関連	サブリカント関連
認証情報				

[操作] 「設定メニュー」→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]

■ 認証情報

ユーザID

認証パスワード

発信者番号による識別

☒ 番号チェックしない
☐ 番号チェックする

相手電話番号

相手サブアドレス

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-R180、240、260B には“発信者番号による識別”の項目はありません。

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 アドレス認証で利用する場合は、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 アドレス認証で利用する場合は、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。

発信者番号による識別

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 桁以内の 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 桁以内の 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

19.1.2.2 IP 関連

[操作] 「設定メニュー」→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]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)				
認証情報	IP関連	IPv6関連	IPsec/IKE関連	サブリカント関連
IP基本情報		スタティック経路情報		

19.1.2.2.1 IP 基本情報

[操作] 「設定メニュー」→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]

■ IP基本情報

自側IPアドレス

相手側IPアドレス

☒ テンプレート定義の設定に従う
☐ 指定する

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。

保存

キャンセル

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

19.1.2.2.2 スタティック経路情報

[操作] 「設定メニュー」→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＞			
ネットワーク	☐ デフォルトルート ☒ ネットワーク指定		
	あて先IPアドレス あて先アドレスマスク 0 0.0.0.0		
メトリック値	1		
優先度	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。

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。

19.1.2.3 IPv6 関連

[操作] 「設定メニュー」→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]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)				
認証情報	IP関連	IPv6関連	IPsec/IKE関連	サブリカント関連
IPv6基本情報		IPv6スタティック経路情報		

19.1.2.3.1 IPv6 基本情報

[操作] 「設定メニュー」→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]

■IPv6基本情報

インタフェースID

☒ テンプレート定義の設定に従う
☐ 自動
☐ 指定する

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

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桁でインタフェースIDを指定します。このとき、他装置と同じインタフェース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

19.1.2.3.2 IPv6 スタティック経路情報

[操作] 「設定メニュー」→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>

ネットワーク

☐ デフォルトルート

☒ ネットワーク指定

あて先プレフィックス/プレフィックス長

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。

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。

19.1.2.4 IPsec/IKE 関連

[操作] 「設定メニュー」→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]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)				
認証情報	IP関連	IPv6関連	IPsec/IKE関連	サブリカント関連
IPsec情報 接続制御情報		IKE情報	拡張IPsec対象範囲情報	

19.1.2.4.1 IPsec 情報

[操作] 「設定メニュー」→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]

⚠ 設定ホストと本装置との通信パケットが対象パケットとなる設定を行うとその設定ホストからの設定変更ができなくなる場合があります。

■ IPsec情報(自動鍵) 

対象 パケ ット	自側IPアド レス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アド レス/プレフィックス長形式で入力してください。
	相手側IPアド レス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アド レス/プレフィックス長形式で入力してください。

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

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。

19.1.2.4.3 拡張 IPsec 対象範囲情報

[操作] 「設定メニュー」→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	拡張 IPsec 対象範囲 相手側 IP アドレス/マスク	操作
[全削除]			
＜拡張 IPsec 対象範囲情報入力フィールド＞			
拡張 IPsec 対 象範囲	自側 IP アドレス/マスク	IPv4 すべて （“指定する”を選択時のみ有効です。） ☐ ☐ ※IPv4 アドレス/マスクビット形式もしくは IPv6 アドレス/プレフィックス長形式で入力してください。	
	相手側 IP アドレス/マスク	IPv4 すべて （“指定する”を選択時のみ有効です。） ☐ ☐ ※IPv4 アドレス/マスクビット形式もしくは IPv6 アドレス/プレフィックス長形式で入力してください。	
		[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。

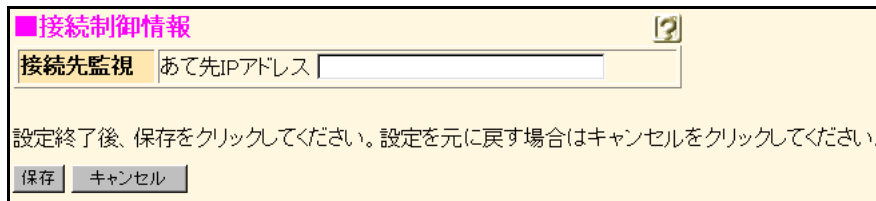
自側（相手側）IP アドレス／アドレスマスク

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。

19.1.2.4.4 接続制御情報

[操作] 「設定メニュー」→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:ffff



ヒント

◆ 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見なされます。

- ・ 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

19.1.2.5 サブリカント関連

[操作] 「設定メニュー」→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]→[サブリカント関連]

AAA情報 - グループID情報(0) - AAAユーザ情報(0)				
認証情報	IP関連	IPv6関連	IPsec/IKE関連	サブリカント関連
サブリカント情報				

19.1.2.5.1 サブリカント情報

[操作] 「設定メニュー」→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]→[サブリカント関連]→[サブリカント情報]

■サブリカント情報

割り当てるVLAN ID

サブリカントMACアドレスによる識別

☒ MACアドレスをチェックしない
☐ MACアドレスをチェックする

MAC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。

割り当てる VLAN ID

サブリカント（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

サブリカント MAC アドレスによる識別

サブリカント（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アドレスにサブリカントのMACアドレスをxx:xx:xx:xx:xx:xx（xxは2桁の16進数値）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、サブリカントの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。

19.1.3 RADIUS 関連

[操作] 「設定メニュー」→ルータ設定「AAA 情報」→[グループ ID 情報]→[追加]→[RADIUS 関連]

AAA情報 - グループID情報(3)	
共通情報	AAAユーザ情報
基本情報	RADIUS関連

19.1.3.1 基本情報

[操作] 「設定メニュー」→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

使用しない

☒ 認証 ☐ アカウンティング
(クライアント機能またはサーバ機能を選択した場合にのみ有効となります)

自側認証IPアドレス

自側アカウンティングIPアドレス

Message-Authenticator

☒ 使用する ☐ 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

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:ffff

fec0:: ~ feff:ffff: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。

自側アカウントिंगIPアドレス

自側 RADIUS アカウントिंग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 アカウントिंगサーバとして使用する場合は、RADIUS アカウントिंग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 アカウントिंगクライアントとして使用する場合は、RADIUS アカウントिंग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 アカウントिंग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。

19.1.3.2 サーバ情報 (クライアント機能)

[操作] 「設定メニュー」→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	修正 削除
認証情報 2	-	0秒	0	修正 削除
認証情報 3	-	0秒	0	修正 削除
認証情報 4	-	0秒	0	修正 削除
アカウント情報 1	-	0秒	0	修正 削除
アカウント情報 2	-	0秒	0	修正 削除
アカウント情報 3	-	0秒	0	修正 削除
アカウント情報 4	-	0秒	0	修正 削除
全削除				

認証情報

認証情報 1	共有鍵	
	サーバIPアドレス	
	サーバUDPポート	☒ 1812 ☐ 1645
	復旧待機時間	秒
	優先度	
	自側認証IPアドレス	
	保存 キャンセル 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:ffff

fec0:: ~ feff:ffff: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

同一グループ内での 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:ffff

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

このクライアントにて 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。

アカウントティング情報

アカウントティング情報 1	共有鍵	
	サーバIPアドレス	
	サーバUDPポート	☒ 1813 ☐ 1646
	復旧待機時間	秒
	優先度	
	自側アカウントティングIPアドレス	
		保存 キャンセル 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:ffff

fec0:: ~ feff:ffff: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トティング要求する 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
アカウントティング要求する 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
アカウントティング要求する 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れなくなります。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

同一グループ内での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、アカウントティングの際に使用する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、使用するRADIUSサーバはランダムに決定されます。

自側アカウントティングIPアドレス

自側RADIUSアカウントティ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」の自側アカウントティング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:ffff

fec0:: ～ fecf:ffff:ffff:ffff:ffff:ffff:ffff:ffff

このクライアントにてRADIUSアカウントティ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」の自側アカウントティングIPアドレスの設定に従います。

19.1.3.3 送信情報（クライアント機能）

〔操作〕 「設定メニュー」→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	1 秒	
再送回数	2 回	
NAS識別子		

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。

認証情報

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トینگ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。

19.1.3.4 クライアント情報（サーバ機能）

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールド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		
クライアントIPアドレス	☐ すべて ☒ アドレス指定 	
		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 RADIUS 情報（サーバ機能）が表示されています。RADIUS 情報（サーバ機能）の定義数は Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」（P37）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:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

20 ACL 情報

適用機種 全機種

[操作] 「設定メニュー」→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・選択削除は一覧の追加・選択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: acl10 追加 キャンセル

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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→ルータ設定「ACL 情報」→[選択削除]

表示条件入力

表示個数: 10 表示範囲: 0~0

■ACL 情報 (0~0)

※追加・選択削除は一覧の追加・選択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
0	削除対象	☐ IP 定義 ☐ TCP 定義 ☐ UDP 定義 ☐ IPv6 定義	削除 キャンセル 一覧へ戻る

全削除

保存した情報は、設定反映後に有効になります。

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。

20.1 ACL 定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→ [追加] / [修正]

ACL情報 - **ACL定義情報(ac10)**

☒ 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		

 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。

20.1.1 基本定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→ [追加] / [修正] → [基本定義情報]

基本定義情報

?

定義名

ac10

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。

20.1.2 IP 定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→[追加] / [修正] → [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。

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。

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。
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。
有効範囲)
0 ～ 63 の 10 進数

20.1.3 TCP 定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→[追加] / [修正] → [TCP 定義情報]

■TCP定義情報	
送信元ポート番号	
あて先ポート番号	
TCP接続要求	☒ 対象 ☐ 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。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。

20.1.4 UDP 定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→[追加] / [修正] → [UDP 定義情報]

■UDP定義情報	
送信元ポート番号	
あて先ポート番号	

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。省略時は、“any” が設定されます。

20.1.5 ICMP 定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→ [追加] / [修正] → [ICMP 定義情報]

■ICMP定義情報

ICMP

タイプ

コード

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

削除

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。

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” が設定されます。

20.1.7 MAC 定義情報

[操作] 「設定メニュー」→ルータ設定「ACL 情報」→[追加] / [修正] → [MAC 定義情報]

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。
- 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

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。

21 ポリシーグループ情報

適用機種 全機種

[操作] 「設定メニュー」→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		
表示回数 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追加ボタンで追加してください。		
定義番号	定義内容	操作
		追加 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定義が表示されています。ポリシーグループの定義数は、Si-Rシリーズ 仕様一覧「2.3 システム最大値一覧」(P37)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。

21.1 ポリシーグループ定義情報

[操作] 「設定メニュー」→ルータ設定「ポリシーグループ情報」→ [追加] / [修正]

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。		

21.1.1 パターン定義情報

[操作] 「設定メニュー」→ルータ設定「ポリシーグループ情報」→ [追加] / [修正]
→ [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
		ACL 定義名
		操作
		全削除
<パターン定義情報入力フィールド>		
動作	☒ 使用する ☐ 使用しない ☐ バックアップとして使用する	
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、このポリシーグループに設定されている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、Si-Rシリーズ 仕様一覧「2.3 システム最大値一覧」(P37)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。

[操作] 「設定メニュー」→ルータ設定「ポリシーグループ情報」→ [追加] / [修正]
→ [パターン定義情報] → [ACL 定義参照] または「ACL 定義番号の [参照]」

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」 - [追加] / [修正] - 「IP 定義情報」または「IPv6 定義情報」で設定した ACL 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、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。

表示条件入力			
表示個数		表示範囲	
10		0~0	
■ ACL 情報 閉じる			
定義番号	IP 定義	IPv6 定義	TCP/UDP/ICMP 定義 選択
	プロトコル	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	送信元 IPv6 アドレス/プレフィックス あて先 IPv6 アドレス/プレフィックス	
	QoS 種別	QoS 種別	
	QoS 値	QoS 値	
0	すべて	すべて	TCP 定義 送信元ポート番号 any あて先ポート番号 any TCP 接続要求 対象 UDP 定義 送信元ポート番号 any あて先ポート番号 any ICMP 定義 ICMP タイプ any ICMP コード any 選択
	any	any	
	any	any	
	any	any	
			閉じる

「ACL 情報」 - [追加] / [修正] - 「IP 定義情報」または「IPv6 定義情報」で設定した ACL 定義が表示されています。

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。

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。

21.1.2 送出先定義情報

[操作] 「設定メニュー」→ルータ設定「ポリシーグループ情報」→[追加] / [修正] →[送出先定義情報]

■送出先定義情報

?

送出先インタフェース	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

送出先インタフェース

パケットを送出するインタ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:ffff

こんな事に気をつけて

送出先インタフェースが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。

21.1.3 接続先監視定義情報

[操作] 「設定メニュー」→ルータ設定「ポリシーグループ情報」→[追加] / [修正]
→[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	
あて先IPアドレス	
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

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

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 日

22 ルーティングプロトコル情報

適用機種 全機種

[操作] 「設定メニュー」→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

22.1 インタフェース情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[インタフェース情報]

■ インタフェース情報

フローティング機能

☒ 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

フローティング機能

インタ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、インタフェースの状態変動に関係なく、インタ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。

22.2 ルーティングマネージャ情報

[操作] 「設定メニュー」→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
再配布情報		優先度情報		ECMP情報		

22.2.1 再配布情報

[操作] 「設定メニュー」→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	インタフェース経路情報	☐ 再配布しない ☒ 再配布する
	スタティック経路情報	☐ 再配布しない ☒ 再配布する
	BGP経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
	OSPF経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
	DNS経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
BGP	インタフェース経路情報	☒ 再配布しない ☐ 再配布する
	スタティック経路情報	☒ 再配布しない ☐ 再配布する
	RIP経路情報	☒ 再配布しない ☐ 再配布する
	OSPF経路情報	☒ 再配布しない ☐ 再配布する
	DNS経路情報	☒ 再配布しない ☐ 再配布する
OSPF	インタフェース経路情報	☒ 再配布しない ☐ 再配布する メトリック値 20 メトリックタイプ type2
	スタティック経路情報	☒ 再配布しない ☐ 再配布する メトリック値 20 メトリックタイプ type2
	RIP経路情報	☒ 再配布しない ☐ 再配布する メトリック値 20 メトリックタイプ type2
	BGP経路情報	☒ 再配布しない ☐ 再配布する メトリック値 20 メトリックタイプ type2
	DNS経路情報	☒ 再配布しない ☐ 再配布する メトリック値 メトリックタイプ type2
LDP	インタフェース経路情報	☐ 再配布しない ☒ 再配布する
	スタティック経路情報	☐ 再配布しない ☒ 再配布する
	RIP経路情報	☐ 再配布しない ☒ 再配布する
	BGP経路情報	☐ 再配布しない ☒ 再配布する
	OSPF経路情報	☐ 再配布しない ☒ 再配布する

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

RIPに再配布する経路情報を設定します。

インタフェース経路情報

インタ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。

インタフェース経路情報

インタ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

デフォルトルートは 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。

インタフェース経路情報

インタ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。

インタフェース経路情報

インタ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。

22.2.2 優先度情報

[操作] 「設定メニュー」→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	120
	EBGP	20
	IBGP	200
	OSPF	110
	DNS	

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

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。

22.2.3 ECMP 情報

[操作] 「設定メニュー」→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情報

ECMP機能

OSPF使用ECMP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。

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、通信の連続性（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。通信の連続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。

22.3 RIP 関連

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[RIP 関連]

ルーティングプロトコル情報					
インタフェース 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
RIPタイム情報		RIPマルチパス情報		RIP再配布フィルタリング情報	
RIPユニキャスト送信情報		RIP相手フィルタリング情報			

22.3.1 RIP タイマ情報

[操作] 「設定メニュー」→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]

■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。

保存 キャンセル

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

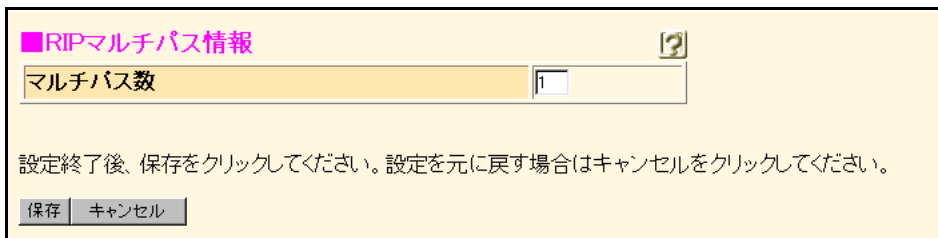
ガーベージタイマ

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

22.3.2 RIP マルチパス情報

[操作] 「設定メニュー」→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。

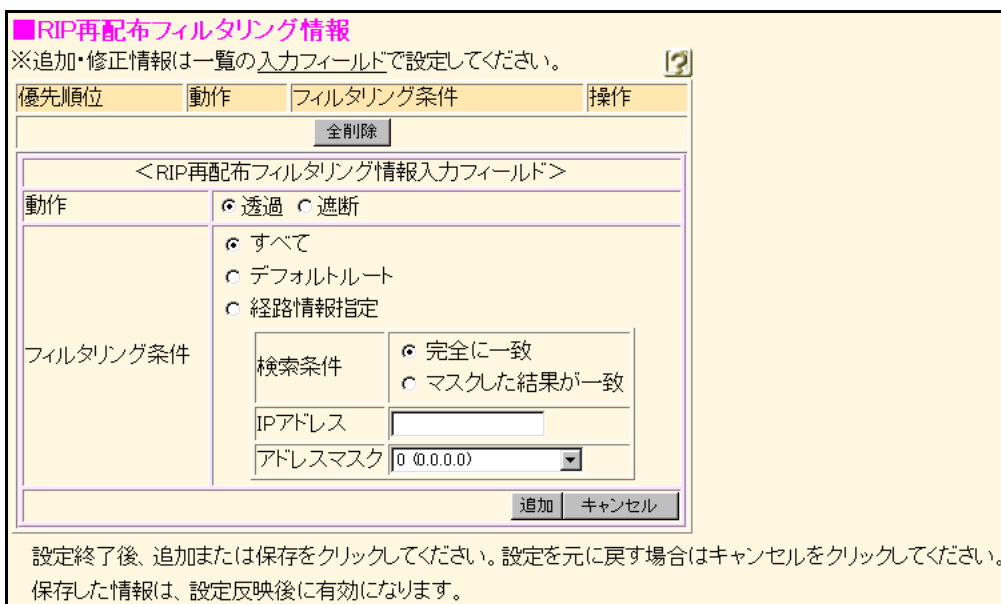
保存 キャンセル

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。

22.3.3 RIP 再配布フィルタリング情報

[操作] 「設定メニュー」→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
全削除			

<RIP再配布フィルタリング情報入力フィールド>

動作	☒ 透過 ☐ 遮断
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定
	検索条件 ☒ 完全に一致 ☐ マスクした結果が一致
	IPアドレス
	アドレスマスク 0.0.0.0

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 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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

対象とするフィルタリング条件を設定します。

- 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、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

- 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。

22.3.4 RIP ユニキャスト送信情報

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールド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
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

送信RIPバージョン ☐ V1 ☒ V2

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 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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。

22.3.5 RIP 相手フィルタリング情報

[操作] 「設定メニュー」→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
全削除			
<RIP 相手フィルタリング情報入力フィールド>			
動作	☒ 透過 ☐ 遮断		
フィルタリング条件	☒ すべて ☐ 相手側 IP アドレス指定		
	IP 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。

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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

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設定します。

- 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。

22.4 BGP 関連

[操作] 「設定メニュー」→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
BGP情報		BGPネットワーク情報		BGP集約経路情報		
BGP相手情報		BGP再配布フィルタリング情報		VRF情報		
MPLS連携情報						

22.4.1 BGP 情報

[操作] 「設定メニュー」→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

☒ 使用しない
☐ 使用する

自AS番号

自ID番号

0.0.0.0

BGPネットワーク

☐ 常に広報する

最大エントリ数

☒ 拡張しない
☐ 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 以外では、BGP 情報の表示が、上記の画面とは異なります。

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

- バージョン4だけをサポートしています。
- 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た場合でも、ルーティングテーブルに反映されません。
- NAT 機能とは併用できません。
- BGP 使用中に【設定反映】ボタンをクリックした場合、接続中のセッションが切断され、BGP が再起動されます。

自 AS 番号

本装置の属する AS 番号を 10 進数を使用して、1～65535 の範囲で指定します。自 AS 番号は省略できません。

自 ID 番号

BGP 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 / リモートインタフェースに設定されている IPv4 アドレスの中からインタフェースの 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。

BGP ネットワーク

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、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 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。

最大エントリ数 (Si-R570)

BGP テーブルエントリ数の最大値を 15 万経路に拡張する場合は、“拡張する”を選択します。

最大エントリ数の拡張は、拡張用 512M メモリモジュールを搭載しているときにだけ使用できます。拡張時に設定できる 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。

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
- BGP/MPLS VPN 機能
- BGP MPLS 解決機能

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 で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
 - アドレスファミリー情報を “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
-

22.4.2 BGP ネットワーク情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連]→[BGP ネットワーク情報]

現在、設定されている 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。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 ネットワーク情報の定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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 情報」で、「BGP ネットワーク」を常に広報すると設定することによって、「BGP ネットワーク情報」で設定した経路を経路情報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、BGP ネットワーク情報は広報されません。

22.4.3 BGP 集約経路情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連] → [BGP 集約経路情報]

BGP集約経路情報

※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。

集約IPアドレス/マスク	集約対象経路	操作
全削除		
<BGP集約経路情報入力フィールド>		
集約IPアドレス		
集約アドレスマスク	0 (0.0.0.0)	
集約対象経路	☒ 広報する ☐ 広報しない	
		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 BGP 集約経路情報の定義が表示されています。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があつた場合に、集約経路情報を生成して広報することができます。集約経路に含まれる経路情報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。

BGP 集約経路情報の定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

集約 IP アドレス／アドレスマスク

集約経路情報の集約 IP アドレスとアドレスマスクを指定します。

集約対象経路

- 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。

22.4.4 BGP 相手情報

[操作] 「設定メニュー」→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]

■BGP相手情報				
定義番号	IPアドレス	AS番号	Holdタイム	操作
追加 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→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	BGP フィルタリング情報	BGP 拡張機能情報

22.4.4.1 BGP 相手基本情報

[操作] 「設定メニュー」→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]

■BGP相手基本情報	
相手側IPアドレス	
相手AS番号	
自側IPアドレス	0.0.0.0
KeepAliveタイム	30 秒
Holdタイム	90 秒
MEDメトリック値	0
ASパスプリベンド	0
EBGP MULTIHOP	1
LOCALPREF	100
NEXTHOP SELF	☒ 無効 ☐ 有効
デフォルトルート	☒ 広報しない ☐ 広報する
認証鍵	

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。

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 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、1 ~ 65535 の範囲で指定します。指定する AS 番号は、自 AS 番号と異なる番号を指定します。IP-VPN 接続を行う場合は、自装置の属する AS 番号とは異なる値を設定する必要があります。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 を使用する場合は、相手情報は 1 つだけ設定することができます。
- IP-VPN 接続と BGP/MPLS VPN は併用することはできません。

自側 IP アドレス

BGP セッションに特定のインタ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。

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

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。KeepAlive タイマ値は以下の範囲で指定します。

有効範囲)

1 ~ 18 時間

1 ~ 1092 分

1 ~ 65535 秒

こんな事に気をつけて

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。Hold タイマ値は以下の範囲で指定します。

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。

MED メトリック値

EBGP で広報する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。

AS パスプリペンド

EBGP で広報する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。

EBGP MULTI HOP

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 TTL 値を 10 進数を使用して、1～255 の範囲で指定します。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 EBGP MULTI HOP に加算して指定します。また、リモート側の IP アドレスに LAN 側の IP アドレスを設定している場合は EBGP MULTI HOP を 1 加算して指定します。

LOCALPREF

EBGP で受信する経路情報のローカル優先度を指定します。ローカル優先度は、IBGP で広報され、同じ自律システム内での優先経路選択に使用され、大きい値がより高い優先度を示します。初期値は 100 です。

NEXTHOP SELF

IBGP で広報する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。

デフォルトルート

BGP で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。

22.4.4.2 BGP フィルタリング情報

[操作] 「設定メニュー」→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 フィルタリング情報]

BGP 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	MED メトリック値	AS バスプリベンド	操作
全削除						
<BGP フィルタリング情報入力フィールド>						
動作	☒ 透過 ☐ 遮断					
方向	☐ 受信 ☒ 送信					
フィルタリング条件	☒ AS 番号指定 AS 番号 ☐ すべて ☐ デフォルトルート ☐ 経路情報指定 検索条件 ☒ 完全に一致 ☐ マスクした結果が一致 IP アドレス アドレスマスク 0.0.0.0					
MED メトリック値	0					
AS バスプリベンド	0					
LOCAL PREF	100					
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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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 1 ～ 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

- 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

フィルタリング条件で透過になった 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、0 ～ 4294967295 の範囲で指定します。初期値は 0 です。

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 パスプリペンド

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 番号の個数を変更できます。AS パスプリペンドは、0 ～ 4 の範囲で指定します。初期値は 0 です。

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 パスプリペンドの設定は無効となります。
- AS パスプリペンドの設定は、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

フィルタリング条件で透過になった経路情報に対して、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。初期値は 100 です。

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。

22.4.4.3 BGP 拡張機能情報

[操作] 「設定メニュー」→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

?

アドレスファミリー情報	IPv4ユニキャスト
エンフォースマルチホップ	☒ 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

アドレスファミリー情報

BGPで使用するアドレスファミリーを選択します。

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する必要があります。

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は、本装置とルータを経由して接続される BGP neighbor と BGP マルチホップ設定を行わずに経路交換することができます。

エンフォースマルチホップを使用する場合は、“使用する”を選択します。“使用する”を選択した場合は、EBGPのマルチホップ環境で、TTL 値が1のUPDATEパケットを受信しても破棄されません。

22.4.5 BGP 再配布フィルタリング情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連]
→[BGP 再配布フィルタリング情報]

BGP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
全削除			
＜BGP再配布フィルタリング情報入力フィールド＞			
動作	☒ 透過 ☐ 遮断		
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定		
	検索条件	☒ 完全に一致 ☐ マスクした結果が一致	
	IPアドレス		
	アドレスマスク	0.0.0.0	
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 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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

対象とするフィルタリング条件を設定します。

- すべて
すべての経路情報をフィルタリング対象とする場合に指定します。
- 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する場合に指定します。
- 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

- 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。

22.4.6 VRF 情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連] → [VRF 情報]

VRF 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	ルート識別子		BGP/MPLS VPN 広報		操作
	AS 番号	識別番号	スタティック経路情報	インタフェース経路情報	
全削除					
<VRF 情報入力フィールド>					
ルート識別子	AS 番号	識別番号			
BGP/MPLS VPN 広報	スタティック経路情報	☒ 再配布しない ☐ 再配布する			
	インタフェース経路情報	☒ 再配布しない ☐ 再配布する			
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。

BGP/MPLS VPN は、VPN 単位に VRF 情報をもち、経路情報を別々に管理します。

VRF 情報の定義数は、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

ルート識別子

BGP/MPLS VPN で使用するルート識別子を AS 番号と ID で指定します。AS 番号は自装置の属する 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 の範囲で設定します。

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。BGP/MPLS VPN スタティック経路の経路情報を BGP に再配布する場合は、“再配布する”を選択します。

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 に再配布するかどうかを選択します。

インタフェース経路情報

VPN で使用するインタ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

「BGP/MPLS VPN 広報」－「スタティック経路」の設定で“再配布する”を選択し、また、スタティック経路情報と同じあて先の経路情報を 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。

22.4.7 MPLS 連携情報

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[BGP 関連] → [MPLS 連携情報]

■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。

保存

キャンセル

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” を選択した場合、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。MPLS トンネル接続上で BGP を用いる場合は、“使用しない” を選択してください。

22.5 OSPF 関連

[操作] 「設定メニュー」→ルータ設定「ルーティングプロトコル情報」→[OSPF 関連]

ルーティングプロトコル情報						
インタフェース 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
	ルータID情報		OSPFエリア情報		AS境界ルータ情報	
	AS外部経路集約情報		OSPF再配布フィルタリング情報			

22.5.1 ルータ ID 情報

[操作] 「設定メニュー」→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情報

?

ルータID

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

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／リモートインタフェースに設定されている IPv4 アドレスの中からインタフェースの 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。

22.5.2 OSPF エリア情報

[操作] 「設定メニュー」→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]

■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
追加 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、この装置に設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→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		

22.5.2.1 OSPF エリア基本情報

[操作] 「設定メニュー」→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]

■OSPFエリア基本情報	
エリアID	
エリア種別	☒ 通常エリア ☐ スタブエリア ☐ 準スタブエリア
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もしく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をクリックしてください。	
保存 キャンセル	

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値

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。

22.5.2.2 経路集約情報

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールドで設定してください。

集約経路

操作

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

ネットマスク

0 (0.0.0.0)

コスト

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、この装置に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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37) 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。

22.5.2.3 サマリLSA入出力可否情報

[操作] 「設定メニュー」→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				
＜サマリLSA入出力可否情報入力フィールド＞				
動作	☒ 透過 ☐ 遮断			
方向	☒ 入力 ☐ 出力			
対象経路情報	☒ すべて ☐ 経路情報指定			
	検索条件	☒ 完全に一致 ☐ マスクした結果が一致		
	IPアドレス			
	アドレスマスク	0.0.0.0		
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、設定されているサマリLSA入出力可否定義の一覧です。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Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P.37)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
-

22.5.2.4 バーチャルリンク情報

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールド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
	パケット再送間隔	LSU パケット送信遅延時間		

全削除

<バーチャルリンク情報入力フィールド>

接続先ルータID	
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 ☒ 文字列 ☐ 16進数 認証鍵 ☐ MD5認証 認証鍵ID 認証鍵

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、この装置に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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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 倍をお勧めします。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 桁以内で指定します。16 桁未満の鍵を指定した場合は、16 桁になるまで 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。

22.5.3 AS境界ルータ情報

[操作] 「設定メニュー」→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

☒ 広報しない
☐ 広報する
☐ AS外部経路に存在する場合に広報する

メトリック値

外部メトリック種別

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。

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。

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。

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。

22.5.4 AS 外部経路集約情報

[操作] 「設定メニュー」→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・修正情報は一覧の入力フィールド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
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		
ネットマスク	0.0.0.0	
		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、このネットワークに設定されている AS 外部経路集約情報の定義が表示されています。処理は、優先順位 1 から順に行われます。AS 外部経路集約情報の定義数は、Si-R シリーズ 仕様一覧 [「2.3 システム最大値一覧」\(P37\)](#) 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。

22.5.5 OSPF 再配布フィルタリング情報

[操作] 「設定メニュー」→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
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	☒ 透過 ☐ 遮断		
フィルタリング条件	☒ すべて ☐ デフォルトルート ☐ 経路情報指定		
	検索条件 ☒ 完全に一致 ☐ マスクした結果が一致 IPアドレス アドレスマスク 0.0.0.0		
メトリック	☒ 指定しない ☐ 指定する		
	メトリック値 メトリックタイプ type2		
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、このネットワークに設定されている 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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

対象とするフィルタリング条件を設定します。

- 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、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

- 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 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。

22.6 IPv6 ルーティングマネージャ情報

[操作] 「設定メニュー」→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再配布情報		IPv6優先度情報				

22.6.1 IPv6再配布情報

[操作] 「設定メニュー」→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	インタフェース経路情報	☐ 再配布しない ☒ 再配布する
	スタティック経路情報	☐ 再配布しない ☒ 再配布する
	DNS経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 0
	DHCP経路情報	☒ 再配布しない ☐ 再配布する メトリック値: 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

RIP

インタフェース経路情報

インタフェース経路情報を RIP に再配布するかどうかを選択します。

スタティック経路情報

スタティック経路情報を RIP に再配布するかどうかを選択します。

DNS 経路情報

DNS 経路情報を RIP に再配布するかどうかを選択します。

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。

DHCP 経路情報

DHCP 経路情報を RIP に再配布するかどうかを選択します。

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。

22.6.2 IPv6 優先度情報

[操作] 「設定メニュー」→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
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。

保存

キャンセル

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。

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。

22.7 IPv6 RIP 関連

[操作] 「設定メニュー」→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タイム情報		IPv6 RIPマルチパス情報		IPv6 RIP再配布フィルタリング情報	

22.7.1 IPv6 RIP タイマ情報

[操作] 「設定メニュー」→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タイマ情報

定期広報タイマ

30 秒

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。

保存

キャンセル

定期広報タイマ

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。

有効範囲)
10～3600 秒
1～60 分
1 時間

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。

有効範囲)
10～3600 秒
1～60 分
1 時間

22.7.2 IPv6 RIP マルチパス情報

[操作] 「設定メニュー」→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]

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。初期値は1です。

22.7.3 IPv6 RIP 再配布フィルタリング情報

[操作] 「設定メニュー」→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]

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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P.37)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

対象とするフィルタリング条件を設定します。

- 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、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

- 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。

23 マルチキャスト情報

適用機種 全機種

[操作] 「設定メニュー」→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 経路情報

23.1 IP マルチキャスト情報

[操作] 「設定メニュー」→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

RP候補

☒ しない
☐ する

IPアドレス
プライオリティ

PIM-SM BSR候補

☒ しない
☐ する

IPアドレス
プライオリティ

SPTへの経路変更

☐ しない
☒ 即時
☐ 転送速度 Kbps

☒ ヘッダ部 ☐ 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。

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 以外	1 ～ 100000Kbps
Si-R570	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（RFC2362 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。

23.2 IP マルチキャストスタティック経路情報

[操作] 「設定メニュー」→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	入力インタフェース	出力インタフェース	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	
マルチキャストグループアドレス	
入力インタフェース	LAN0 ▾
出力インタフェース	
グループ参加	☒ しない ☐ する

追加 キャンセル

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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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

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 アドレスで指定してください。

入力インタフェース

入力インタフェースを選択してください。

出力インタフェース

出力インタ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 "-" で区切ります。出力インタフェースは 20 個まで設定できます。

グループ参加

入力インタ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、入力インタフェースでは IGMP によるグループ参加を行います。

24 UPnP 情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「UPnP 情報」

UPnP 情報
基本情報

24.1 基本情報

[操作] 「設定メニュー」→ルータ設定「UPnP 情報」→[基本情報]

■基本情報

UPnP機能

☒ 使用しない
 ☐ 使用する

ポートマッピング有効期限

☒ 無期限
☐ 設定する
 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

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 機能を利用することで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すすめします。
- マルチ NAT 機能を使用しないインタフェースに 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フェースへの通信に対して VoIP NAT トラバースル機能が動作します。

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したときに、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てか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

25 MPLS 情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「MPLS 情報」

MPLS 情報
基本情報

25.1 基本情報

[操作] 「設定メニュー」→ルータ設定「MPLS 情報」→「基本情報」

■基本情報

MPLS TTL 伝達

☐ しない
☒ する

LDP

router ID

制御方式

☒ independent
☐ ordered

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。

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

26 ブリッジ情報

適用機種 全機種

[操作] 「設定メニュー」→ルータ設定「ブリッジ情報」

ブリッジ情報

ブリッジグループ情報

26.1 ブリッジグループ情報

[操作] 「設定メニュー」→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
5	5分	使用する	使用する	なし	修正 削除
6	5分	使用する	使用する	なし	修正 削除
7	5分	使用する	使用する	なし	修正 削除
8	5分	使用する	使用する	なし	修正 削除
9	5分	使用する	使用する	なし	修正 削除
10	5分	使用する	使用する	なし	修正 削除
11	5分	使用する	使用する	なし	修正 削除
12	5分	使用する	使用する	なし	修正 削除
13	5分	使用する	使用する	なし	修正 削除
14	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、Si-R シリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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。

26.1.1 ブリッジグループ情報（グループ識別子0の場合）

[操作] 「設定メニュー」→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	☒ 使用する ☐ 使用しない 転送ポリシー ☒ strict ☐ loose
IPv6ルーティング機能	☒ 使用する ☐ 使用しない 転送ポリシー ☒ strict ☐ loose
0 リモートインタフェース間ブリッジ	☒ する ☐ しない
ブリッジの優先度	32768
ブリッジのHello待ち時間	20 秒
STP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	☒ VLANタグを挿抜 ☐ 透過する
MACコントロールフレーム転送機能	☐ STP ☐ LACP ☐ EAPOL

保存 キャンセル 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。

転送ポリシー

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。

受信フレームのあて先 MAC アドレスが受信インタフェースあてであるが、あて先 IP アドレスが受信インタフェースあてではない場合、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。

転送ポリシー

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フェースあてであるが、あて先 IP アドレスが受信インタ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。

リモートインタフェース間ブリッジ

リモートインタフェースから受信したフレームを別のリモートインタ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 タグを挿抜する設定の場合、VLAN インタフェースで受信してリモートインタフェースへ出力する際には VLAN タグを除去して転送し、リモートインタフェースで受信して VLAN インタ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フェースでは STP は使用できません。

26.1.2 ブリッジグループ情報（グループ識別子 1～7 の場合）

[操作] 「設定メニュー」→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	☒ 使用する ☐ 使用しない
	転送ポリシー ☒ strict ☐ loose
IPv6ルーティング機能	☒ 使用する ☐ 使用しない
	転送ポリシー ☒ strict ☐ loose
リモートインタフェース間ブリッジ	☒ する ☐ しない
VLANタグ付きフレーム	☒ VLANタグを挿抜 ☐ 透過する
MACコントロールフレーム転送機能	☐ STP ☐ LACP ☐ EAPOL
保存 キャンセル 一覧へ戻る	

「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」、「リモートインタフェース間ブリッジ」、「VLAN タグ付きフレーム」および「MAC コントロールフレーム転送機能」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。

27 動的VPN情報

適用機種 全機種

[操作] 「設定メニュー」→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。	

27.1 サーバ関連情報

[操作] 「設定メニュー」→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	

27.1.1 基本情報

[操作] 「設定メニュー」→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

☒ 使用しない
☐ 使用する

ドメイン名

認証

☒ 行わない
☐ 行う

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

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。

27.2 クライアント関連情報

[操作] 「設定メニュー」→ルータ設定「動的VPN情報」→[クライアント関連情報]

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	ドメイン情報

27.2.1 基本情報

[操作] 「設定メニュー」→ルータ設定「動的VPN情報」→[クライアント関連情報]→[基本情報]

■基本情報

クライアント機能

交換情報のエンコード

☒ する
 ☐ 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

クライアント機能

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。

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。

27.2.2 ドメイン情報

[操作] 「設定メニュー」→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]

■ドメイン情報

※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	ドメイン名	操作
全削除		
<ドメイン情報追加フィールド> ドメイン名 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、Si-R シリーズ 仕様一覧 [\[2.3 システム最大値一覧\]](#) (P37) 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] 「設定メニュー」→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]

動的VPN情報－クライアント関連情報－**ドメイン情報(0)**
基本情報 自側ネットワーク情報

27.2.2.1 基本情報

[操作] 「設定メニュー」→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		
サーバ情報	アドレス	
	ポート番号	5070
	認証ID	
	認証パスワード	
セカンダリサーバ情報	アドレス	
	ポート番号	5070
	認証ID	
	認証パスワード	
有効期間	1 時間	
優先度	10	
セッション更新間隔	☐ 更新しない ☒ 更新する 5 時間 5 分	
クライアントIPアドレス		
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	
経路情報の優先度	IPv4	1
	IPv6	1
自側ユーザ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。

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ーに従って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、送出インタフェースとなるインタフェースの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フェースで lan インタフェースを指定した場合は、指定された lan インタ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フェースで rmt インタフェースを指定した場合は、指定された rmt インタ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。

27.2.2.2 自側ネットワーク情報

[操作] 「設定メニュー」→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で接続する自側ネットワーク	動的VPNサーバ登録	操作
	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	※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。		
動的VPNサーバ登録	☒ する ☐ しない		
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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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/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。

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接続を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
IPsec1KE)c0a80100/24@example.com
IPsec1KE)20010db8111100010000000000000000/64@example.com

28 ProxyDNS 情報／URL フィルタ情報

適用機種 全機種

[操作] 「設定メニュー」→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	
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。	



ヒント

◆ 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。

28.1 順引き情報

[操作] 「設定メニュー」→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 タイプ 送信元IPアドレス	動作	DNSサーバアドレス/ ネットワーク名/ インタフェース名 経路自動作成	操作
				

<順引き情報入力フィールド>

ドメイン名

タイプ (番号指定 “その他”を選択時のみ有効です。)

送信元IPアドレス /
 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。

動作

- ☒ 廃棄する
- ☐ 接続先のDNSサーバへ問い合わせる
 ネットワーク名
- ☐ 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

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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37)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。

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

28.2 逆引き情報

[操作] 「設定メニュー」→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＞				
ネットワークアドレス	すべて ("指定する" を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。			
動作	☒ 廃棄する ☐ 接続先のDNSサーバへ問い合わせる ネットワーク名 rmt0 ☐ 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる ネットワーク名 rmt0 解決したホストへのホスト経路自動作成 ☒ しない ☐ する ☐ DHCPクライアントが取得したDNSサーバへ問い合わせる インタフェース名 使用できるインタフェースが存在しません ☐ 設定したDNSサーバへ問い合わせる DNSサーバアドレス			
追加 キャンセル				

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、Si-Rシリーズ仕様一覧「[2.3 システム最大値一覧](#)」(P.37)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

29 ホストデータベース情報

適用機種 全機種

[操作] 「設定メニュー」→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

[1～16](#)

[17～32](#)

[33～48](#)

[49～64](#)

[全表示](#)

[操作] 「設定メニュー」→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

※全削除ボタンが一番最後にあります。

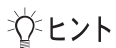
＼	ホスト名	IPv4アドレス IPv6アドレス	MACアドレス	電源制御	操作
1	-	-	-	-	修正 削除
2	-	-	-	-	修正 削除
3	-	-	-	-	修正 削除
4	-	-	-	-	修正 削除
5	-	-	-	-	修正 削除

58	-	-	-	-	修正 削除
59	-	-	-	-	修正 削除
60	-	-	-	-	修正 削除
61	-	-	-	-	修正 削除
62	-	-	-	-	修正 削除
63	-	-	-	-	修正 削除
64	-	-	-	-	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。

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、Si-Rシリーズ 仕様一覧「[2.3 システム最大値一覧](#)」(P37) 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] 「設定メニュー」→ルータ設定「ホストデータベース情報」→[修正]



ヒント

◆ 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」「IP 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。
- DHCP スタティック機能
「IP 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 IP 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。その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 DHCP スタティック機能で使用されます。

IPv6 アドレス

DNS サーバ機能で使用されます。

MAC アドレス

DHCP スタティック機能、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 桁の 16 進数)

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。

索引

A

AAA 情報	351
AAA ユーザ情報	352
ACL 情報	372
ACL 定義情報	373
AH	188, 335
ARP 情報	112
AS 外部経路集約情報	416
AS 境界ルータ情報	415

B

BGP/MPLS VPN 情報	110
BGP/MPLS VPN スタティック経路情報	111
BGP 相手基本情報	399
BGP 相手情報	399
BGP 拡張機能情報	404
BGP 関連	395
BGP 再配布フィルタリング情報	405
BGP 集約経路情報	398
BGP 情報	395
BGP ネットワーク情報	397
BGP フィルタリング情報	402

C

CLP 値設定情報	236
-----------------	-----

D

DHCP 情報	106
DHCP スタティック機能	445
DNS サーバ機能	439, 445
DNS サーバの自動切り替え機能	439
DNS 問い合わせタイプフィルタ機能	439

E

ECMP 情報	389
EoMPLS 情報	149
ESP	188, 335
EXP 値書き換え情報	241

I

ICMP 情報	108
ICMP 定義情報	376
IDS 情報	
LAN 情報	89
相手情報	218
テンプレート情報	301

IKE 情報	
AAA 情報	359
相手情報	193, 196
動的 VPN	195
テンプレート情報	
RADIUS/AAA	337
動的 VPN	343
Ingress ポリシールーティング情報	
LAN 情報	104
相手情報	234
テンプレート情報	314
IPsec/IKE 関連	
AAA 情報	358
テンプレート情報	
RADIUS/AAA	335
動的 VPN	343
IPsec 情報	
AAA 情報	358
相手情報	
自動鍵	187
手動鍵	190
動的 VPN	192
テンプレート情報	335
IPv6 CLP 値設定情報	270
IPv6 DHCP 情報	272
IPv6 EXP 値書き換え情報	274
IPv6 Ingress ポリシールーティング情報	
LAN 情報	136
相手情報	268
テンプレート情報	331
IPv6 RIP 関連	421
IPv6 RIP 再配布フィルタリング情報	422
IPv6 RIP 情報	
LAN 情報	117
相手情報	250
IPv6 RIP タイマ情報	421
IPv6 RIP フィルタリング情報	
LAN 情報	130
相手情報	262
IPv6 RIP マルチパス情報	422
IPv6 Traffic Class 値書き換え情報	
LAN 情報	126
相手情報	258
テンプレート情報	323
IPv6 動的 VPN 情報	276
IPv6 関連	
AAA 情報	356
LAN 情報	114
相手情報	247
テンプレート情報	316
IPv6 基本情報	
AAA 情報	356
LAN 情報	114
相手情報	247
テンプレート情報	316
IPv6 再配布情報	419

IPv6 スタティック経路情報	
AAA 情報	357
LAN 情報	118
相手情報	251
IPv6 帯域制御 (WFQ) 情報	
LAN 情報	132
相手情報	263
テンプレート情報	327
IPv6 定義情報	377
IPv6 フィルタリング情報	
LAN 情報	120
相手情報	252
テンプレート情報	317
IPv6 優先度情報	420
IPv6 ルーティングマネージャ情報	419
IP アドレス情報	76
IP 関連	
AAA 情報	354
LAN 情報	76
相手情報	204
テンプレート情報	294
IP 基本情報	
AAA 情報	354
相手情報	204
テンプレート情報	294
IP 定義情報	374
IP フィルタリング情報	
LAN 情報	83
相手情報	211
テンプレート情報	295
IP マルチキャスト情報	424
IP マルチキャストスタティック経路情報	426

L

LAN 情報	65
LDP 情報	
LAN 情報	147
相手情報	286

M

MAC アドレス認証情報	49, 75, 153
MAC 定義情報	378
MAC フィルタリング情報	
LAN 情報	139, 141, 281
相手情報	279
MPLS 関連	
相手情報	285
MPLS 基本情報	
LAN 情報	146
相手情報	285
MPLS 情報	428
MPLS 連携情報	407
MP 情報	203

N

NAT あて先変換情報	
LAN 情報	99, 309
相手情報	229
NAT 情報	
LAN 情報	95, 305
相手情報	225

O

OSPF エリア基本情報	409
OSPF エリア情報	409
OSPF 関連	408
OSPF 再配布フィルタリング情報	417
OSPF 情報	
LAN 情報	79
相手情報	206

P

PPPoE 情報	182
PPP 関連	
相手情報	202
テンプレート情報	292
PPP 情報	
ISDN 接続	173
PPPoE 接続	182
専用線接続	168
モデム接続	177
ProxyDNS 情報	439

R

RADIUS 関連	364
RADIUS 情報	
クライアント機能	366, 370
RIP 相手フィルタリング情報	394
RIP 関連	390
RIP 再配布フィルタリング情報	391
RIP 情報	
LAN 情報	78
相手情報	205
RIP タイマ情報	390
RIP フィルタリング情報	
LAN 情報	94
相手情報	223
RIP マルチパス情報	391
RIP ユニキャスト送信情報	393

S

SNMP 情報	39
---------------	----

T

TCP 定義情報	375
TOS 値書き換え情報	
LAN 情報	90
相手情報	219
テンプレート情報	302

U

UDP 定義情報	375
UPnP 情報	427
URL フィルタ機能	439
URL フィルタ情報	439

V

VLAN プライオリティマッピング情報	152
VRF 情報	406
VRRP アクション情報	73
VRRP グループ情報	69
VRRP トリガ情報	71

W

WAN 情報	54
--------------	----

あ

相手情報	156
圧縮情報	
相手情報	202
テンプレート情報	293
アプリケーションフィルタ情報	48

い

異常時動作情報	43
インタフェース情報	384

お

オプション設定	
PPPoE 接続	25
インターネットへ ISDN 接続	21
インターネットへ専用線接続	23
オフィスへ ISDN 接続	28
オフィスへ専用接続	29
プライベート LAN 接続	32

か

回線インタフェース	
ATM	60
ISDN	55
専用線	58

データ通信カード	61
フレームリレー	59
拡張 IPsec 対象範囲情報	360
かんたん設定	
PPPoE 接続	25
インターネットへ ISDN 接続	20
インターネットへ専用線接続	23
オフィスへ ISDN 接続	27
オフィスへ専用線接続	29
プライベート LAN 構築	31
かんたん設定メニュー	7

き

基本情報

AAA 情報	
RADIUS 関連	364
共通情報	352
LAN 情報	
VRRP グループ情報	69
共通情報 (VLAN)	150
共通情報 (物理 LAN)	66
MPLS 情報	428
UPnP 情報	427
相手情報	
ATM 接続	161
IPsec/IKE 接続	185
IP トンネル接続	183
ISDN 接続	169
MPLS トンネル接続	200
PPPoE 接続	180
共通情報	157
専用線接続	168
パケット破棄	201
フレームリレー接続	174
別インタフェースから送出	199
モデム接続	175
スイッチ情報	62
テンプレート情報	347
ISDN	290
RADIUS/AAA	333
動的 VPN	341
動的 VPN 情報	433, 434, 435
パスワード情報	34
基本定義情報	373
逆引き情報	442
共通情報	
AAA 情報	351
LAN 情報 (VLAN)	150
LAN 情報 (物理 LAN)	66
相手情報	157
シリアル情報	154
テンプレート情報	
ISDN	290
RADIUS/AAA	333
動的 VPN	341

く

クライアント情報

サーバ機能	371
グループ ID 情報	351

グループ識別子 0	430
グループ識別子 1 ～ 7	432

け

経路集約情報	410
月間／週間予約情報	50

こ

構成定義切り替え予約情報	53
--------------------	----

さ

サーバ機能情報	45
再配布情報	385
サブリカント関連	
AAA 情報	363
サブリカント情報	
AAA 情報	363

し

自側ネットワーク情報	350
動的 VPN 情報	438
システムログ情報	38
順引き情報	440
詳細設定メニュー	7
シリアル情報	154

す

スイッチ情報	62
スケジュール情報	50
スタティック ARP 情報	113
スタティック経路情報	
AAA 情報	355
LAN 情報	81
相手情報	209

せ

静的 MAC 学習テーブル情報	143
静的 NAT 情報	
LAN 情報	97, 307
相手情報	227
セカンダリ IP アドレス情報	77
セグメント接続／分割	33
接続先監視	340, 346, 362
接続先監視定義情報	382
接続先種別	
ATM 接続	161
ISDN 接続	169
専用線接続	168
フレームリレー接続	174
モデム接続	175
接続先情報	159

接続先種別	
IPsec/IKE 接続	184
IP トンネル接続	183
MPLS トンネル接続	200
PPPoE 接続	180
パケット破棄	201
別インタフェースから送出	199
接続制御情報	
AAA 情報	361
相手情報	
ATM 接続	164
ISDN 接続	170
PPPoE 接続	181
データ通信カード接続	178
モデム接続	176
テンプレート情報	
RADIUS/AAA	339
動的 VPN	345
設定メニュー	7

そ

送出先定義情報	381
装置情報	36

た

帯域制御 (WFQ) 情報	144
LAN 情報	100
相手情報	230, 283
テンプレート情報	310
タイムサーバ情報	37

ち

着信相手識別情報	288
着信制御情報	172, 177

て

テンプレート情報	289
電話番号変更予約情報	52

と

動的 VPN 関連	347
動的 VPN 情報	245, 433
ドメイン情報	
動的 VPN 情報	434

に

認証情報	
AAA 情報	353
テンプレート情報	292

ね

ネットワーク情報 156

は

バーチャルリンク情報 413

パスワード情報 34

パターン定義情報 379

ひ

必須設定

PPPoE 接続 25

インターネットへ ISDN 接続 20

インターネットへ専用線接続 23

オフィスへ ISDN 接続 27

オフィスへ専用線接続 29

プライベート LAN 接続 31

ふ

ファームウェア更新情報 42

ブリッジ関連

LAN 情報 138

相手情報 278

ブリッジグループ情報 429

ブリッジ情報 429

LAN 情報 138

相手情報 278

ほ

ポート情報 63

ホストデータベース情報 444

ポリシーグループ情報 379

ポリシーグループ定義情報 379

ま

マニュアル構成 6

マルチキャスト情報 424

LAN 情報 109

相手情報 240

マルチルーティング情報 166

も

モデム情報 155

ゆ

優先度情報 388

り

リモートパワーオン機能 445

る

ルータ ID 情報 408

ルータ名称情報 36

ルーティングプロトコル情報 384

ルーティングマネージャ情報 384

ループバック情報 44

ろ

ログインパスワード情報 35

Si-R シリーズ Web リファレンス

P3NK-2222-01Z0

発行日 2006年9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。