P3NK-3402-03Z0

FUJITSU Network Si-R
Si-R brinシリーズ

Webリファレンス V2

FUJITSU

はじめに

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

2009年 2月初版
2014 年 3月第2版
2016 年12月第3版

目次

はじめに 2
本書の使いかた 6
本書の読者と前提知識 6
本装置のマニュアルの構成 7
1 「設定メニュー」を表示する 8
2 「設定メニュー」の画面体系 9
2.1 かんたん設定メニュー 9
2.2 詳細設定メニュー 9
2.2.1 基本設定 9
2.2.2 ルータ設定 10
3 プライベート LAN 構築かんたん設定 19
3.1 必須設定 19
3.2 オプション設定 20
4 セグメント接続／分割かんたん設定 21
4.1 LAN0 21
4.2 LAN1（スイッチ） 21
5 PPPoE かんたん設定 22
5.1 必須設定 22
5.2 オプション設定 22
6 パスワード情報 24
6.1 基本情報 24
6.2 ログインパスワード情報 25
6.3 ログインユーザ情報 26
7 装置情報 28
7.1 ルータ名称情報 28
7.2 タイムサーバ情報 29
7.3 システムログ情報 30
7.4 ファームウェア更新情報 31
7.5 異常時動作情報 32
7.6 IPv4 ループバック情報 33
7.7 IPv6 ループバック情報 34
7.8 サーバ機能情報 34
7.8.1 アプリケーションフィルタ情報 35
8 スケジュール情報 37
8.1 月間／週間予約情報 37
8.2 構成定義切り替え予約情報 38
9 スイッチ情報 39
9.1 基本情報 39
9.2 ポート情報 40
10 LAN 情報 41
10.1 インタフェース：物理 LAN 42
10.1.1 共通情報 42
10.1.2 IP 関連 54
10.1.3 IPv6 関連 86
10.1.4 ブリッジ関連 113
10.2 インタフェース：VLAN 120
10.2.1 共通情報 120
11 相手情報 123
11.1 ネットワーク情報 123

11.1.1 共通情報 124
11.1.2 接続先情報 126
11.1.3 PPP 関連 153
11.1.4 IP 関連 154
11.1.5 IPv6 関連 185
11.1.6 ブリッジ関連 213
12 テンプレート情報 220
12.1 接続種別：IPsec/IKE（RADIUS/AAA） 221
12.1.1 共通情報 221
12.1.2 IP 関連 224
12.1.3 IPv6 関連 243
12.1.4 IPsec/IKE 関連 258
12.2 接続種別：IPsec/IKE（動的 VPN 共有鍵認証方式） 264
12.2.1 共通情報 264
12.2.2 IPsec/IKE 関連 266
12.2.3 動的 VPN 関連 269
13 LLDP 情報 273
13.1 基本情報 273
14 認証情報 275
14.1 MAC アドレス認証情報 275
15 AAA 情報 276
15.1 グループ ID 情報 276
15.1.1 共通情報 276
15.1.2 AAA ユーザ情報 277
15.1.3 RADIUS 関連 288
16 ACL 情報 296
16.1 ACL 定義情報 297
16.1.1 基本定義情報 297
16.1.2 IP 定義情報 298
16.1.3 TCP 定義情報 299
16.1.4 UDP 定義情報 299
16.1.5 ICMP 定義情報 300
16.1.6 IPv6 定義情報 301
16.1.7 MAC 定義情報 302
17 IP 情報 303
17.1 基本情報 303
18 ルーティングプロトコル情報 304
18.1 インタフェース情報 304
18.2 ルーティングマネージャ情報 305
18.2.1 再配布情報 305
18.2.2 優先度情報 307
18.2.3 ECMP 情報 308
18.3 RIP 関連 309
18.3.1 RIP タイマ情報 309
18.3.2 RIP マルチパス情報 310
18.3.3 RIP 再配布フィルタリング情報 310
18.3.4 RIP ユニキャスト送信情報 312
18.3.5 RIP 相手フィルタリング情報 313
18.4 BGP 関連 314
18.4.1 BGP 情報 314
18.4.2 IPv4 BGP ネットワーク情報 315
18.4.3 IPv4 BGP 集約経路情報 316
18.4.4 BGP 相手情報 317

18.4.5 IPv4 BGP 再配布フィルタリング情報 323
18.5 OSPF 関連 324
18.5.1 ルータ ID 情報 324
18.5.2 OSPF エリア情報 325
18.5.3 AS 境界ルータ情報 331
18.5.4 AS 外部経路集約情報 331
18.5.5 OSPF 再配布フィルタリング情報 332
18.6 IPv6 ルーティングマネージャ情報 334
18.6.1 IPv6 再配布情報 334
18.6.2 IPv6 優先度情報 335
18.7 IPv6 RIP 関連 336
18.7.1 IPv6 RIP タイマ情報 336
18.7.2 IPv6 RIP マルチパス情報 337
18.7.3 IPv6 RIP 再配布フィルタリング情報 337
19 マルチキャスト情報 339
19.1 IP マルチキャスト情報 339
19.2 IP マルチキャストスタティック RP 情報 341
19.3 IP マルチキャストスタティック経路情報 342
20 UPnP 情報 343
20.1 基本情報 343
21 ブリッジ情報 344
21.1 ブリッジグループ情報 344
21.1.1 ブリッジグループ情報（グループ識別子 0 の場合）....345
21.1.2 ブリッジグループ情報（グループ識別子 1 ～ 7 の場合）....347
22 動的 VPN 情報 348
22.1 サーバ関連情報 348
22.1.1 基本情報 348
22.2 クライアント関連情報 349
22.2.1 基本情報 349
22.2.2 ドメイン情報 349
23 SNMP 情報 354
23.1 基本情報 354
23.2 SNMPv1/v2c 情報 356
23.3 SNMPv3 情報 358
23.3.1 ユーザ情報 358
23.3.2 MIB ビュー情報 361
23.4 トラップ情報 362
24 ProxyDNS 情報／ URL フィルタ情報 363
24.1 共通情報 364
24.2 順引き情報 365
24.3 逆引き情報 367
25 ホストデータベース情報 369
索引 371

本書の使いかた

本書では、本装置の設定メニューで表示される画面について説明しています。
また、CD-ROM の中の README ファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

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

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

ヒント	**本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。**
こんな事に気をつけて	**本装置をご使用になる際に、注意していただきたいことを説明しています。**
補足	**操作手順で説明しているもののほかに、補足情報を説明しています。**
参照	**操作方法など関連事項を説明している箇所を示します。**
警告	**製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。**
注意	**製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。**

設定例の記述について

設定は Si-R80brin を例に記述しています。
Si-R90brin の場合は、説明の中で物理ポートを指す “LAN1 ポート” といった記述は “SW1 ポート” へ読み替えてください。

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-R80brin　ご利用にあたって	Si-R80brin 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-R90brin　ご利用にあたって	Si-R90brin の設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
コマンドリファレンス - 構成定義編 -	構成定義コマンドの項目やパラメタの詳細な情報を説明しています。
コマンドリファレンス - 運用管理編 -	運用管理コマンド、その他のコマンドの項目やパラメタの詳細な情報を説明しています。
Web ユーザーズガイド	Web 画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Web 設定事例集	Web 画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Web リファレンス（本書）	Web 画面の項目の詳細な情報を説明しています。

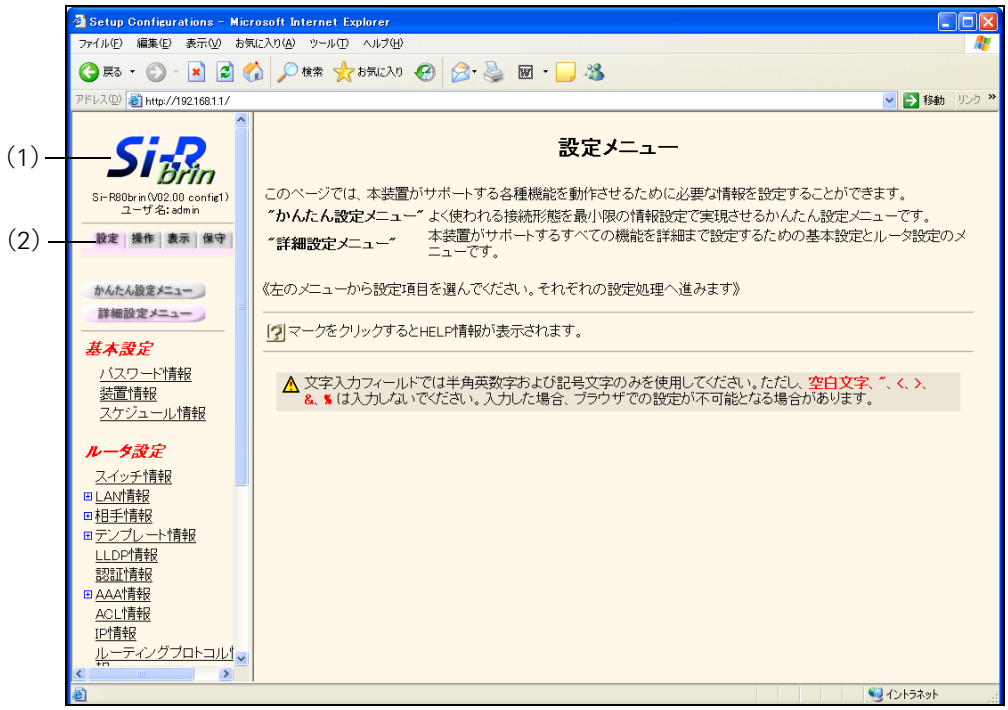
1　「設定メニュー」を表示する

「かんたん設定」をサポートしているかどうかで［設定］タブをクリックしたときに表示される画面が異なります。

こ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　マニュアル「Webユーザーズガイド」



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　　：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。

☛ 参照　マニュアル「Webユーザーズガイド」

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　マニュアル「Webユーザーズガイド」

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

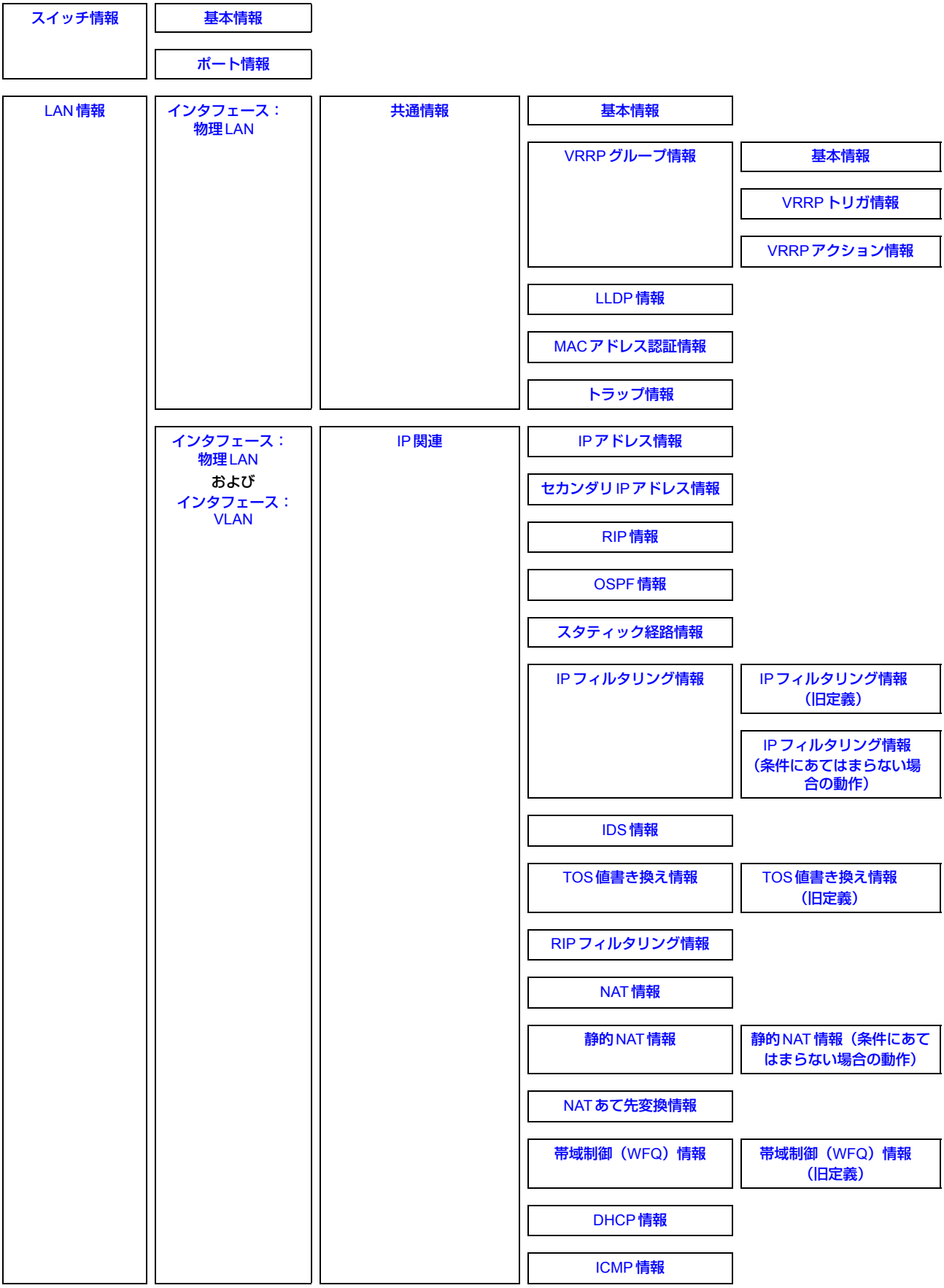
プライベート LAN 構築かんたん設定	必須設定
	オプション設定
セグメント接続／分割かんたん設定	LAN0
	LAN1（スイッチ）
PPPoE かんたん設定	必須設定
	オプション設定

2.2 詳細設定メニュー

2.2.1 基本設定

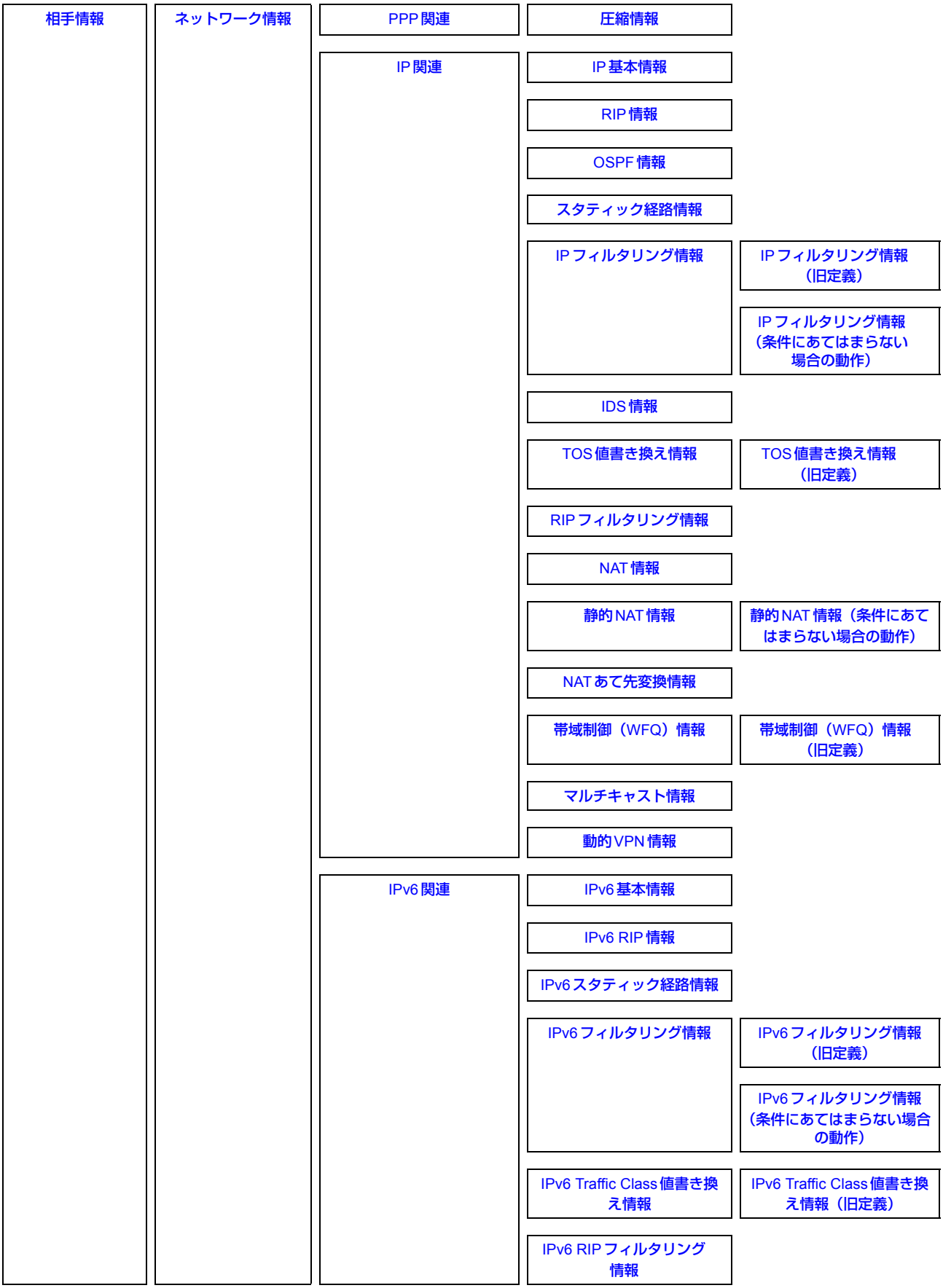
パスワード情報	基本情報	
	ログインパスワード情報	
	ログインユーザ情報	
装置情報	ルータ名称情報	
	タイムサーバ情報	
	システムログ情報	
	ファームウェア更新情報	
	異常時動作情報	
	IPv4 ループバック情報	
	IPv6 ループバック情報	
	サーバ機能情報	アプリケーションフィルタ情報
スケジュール情報	月間／週間予約情報	
	構成定義切り替え予約情報	

2.2.2 ルータ設定

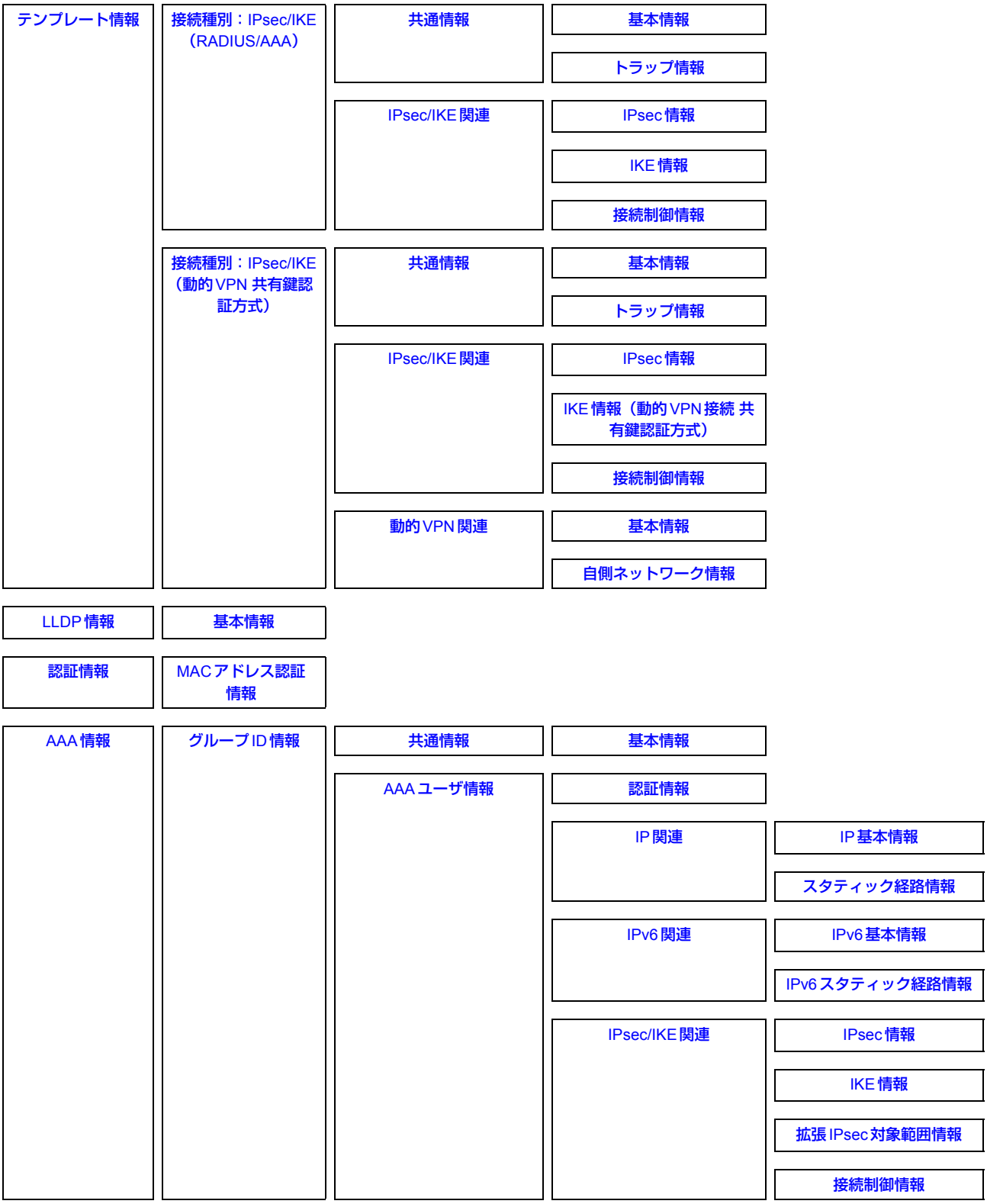

スイッチ情報
基本情報
ポート情報
LAN 情報
インタフェース：物理 LAN
共通情報
基本情報
VRRP グループ情報
基本情報
VRRP トリガ情報
VRRP アクション情報
LLDP 情報
MAC アドレス認証情報
トラップ情報
インタフェース：物理 LAN
および
インタフェース：VLAN
IP 関連
IP アドレス情報
セカンダリ IP アドレス情報
RIP 情報
OSPF 情報
スタティック経路情報
IP フィルタリング情報
IP フィルタリング情報（旧定義）
IP フィルタリング情報（条件にあてはまらない場合の動作）
IDS 情報
TOS 値書き換え情報
TOS 値書き換え情報（旧定義）
RIP フィルタリング情報
NAT 情報
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）
DHCP 情報
ICMP 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
マルチキャスト情報
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 DHCP 情報
ブリッジ関連
ブリッジ情報
MAC フィルタリング情報
MAC フィルタリング情報（旧定義）
静的 MAC 学習テーブル情報
帯域制御（WFQ）情報
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
トラップ情報

- 相手情報
- ネットワーク情報
- 共通情報
  - 基本情報
  - トラップ情報
- 接続先情報
  - 接続先種別：PPPoE 接続
    - 基本情報
    - 接続制御情報
    - PPP 情報
    - PPPoE 情報
    - マルチルーティング情報
    - トラップ情報
  - 接続先種別：IP トンネル接続
    - 基本情報
    - 接続制御情報
    - トラップ情報
  - 接続先種別：IPsec/IKE 接続
    - 基本情報
    - 接続制御情報
    - IPsec 情報（自動鍵）
    - IPsec 情報（手動鍵）
    - IPsec 情報（動的 VPN）
    - IKE 情報（共有鍵認証方式）
    - IKE 情報（動的 VPN 接続 共有鍵認証方式）
    - 拡張 IPsec 対象範囲情報
    - マルチルーティング情報
    - 動的 VPN 関連（基本情報）
    - 動的 VPN 関連（相手側ネットワーク情報）
    - トラップ情報
  - 接続種別：別インタフェースから送出
    - 基本情報
    - 接続制御情報
    - マルチルーティング情報
    - トラップ情報
  - 接続先種別：パケット破棄
    - 基本情報


相手情報
ネットワーク情報
PPP 関連
圧縮情報
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）
マルチキャスト情報
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

相手情報	ネットワーク情報	IPv6 関連	IPv6 帯域制御（WFQ）情報	IPv6 帯域制御（WFQ）情報（旧定義）
			IPv6 DHCP 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	
テンプレート情報	接続種別：IPsec/IKE（RADIUS/AAA） および 接続種別：IPsec/IKE（動的 VPN 共有鍵認証方式）	IP 関連	IP 基本情報	
			IP フィルタリング情報	IP フィルタリング情報（旧定義）
				IP フィルタリング情報（条件にあてはまらない場合の動作）
			IDS 情報	
			TOS 値書き換え情報	TOS 値書き換え情報（旧定義）
			NAT 情報	
			静的 NAT 情報	静的 NAT 情報（条件にあてはまらない場合の動作）
			NAT あて先変換情報	
			帯域制御（WFQ）情報	帯域制御（WFQ）情報（旧定義）
		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）


テンプレート情報
接続種別：IPsec/IKE（RADIUS/AAA）
共通情報
基本情報
トラップ情報
IPsec/IKE 関連
IPsec 情報
IKE 情報
接続制御情報
接続種別：IPsec/IKE（動的 VPN 共有鍵認証方式）
共通情報
基本情報
トラップ情報
IPsec/IKE 関連
IPsec 情報
IKE 情報（動的 VPN 接続 共有鍵認証方式）
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
LLDP 情報
基本情報
認証情報
MAC アドレス認証情報
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
接続制御情報

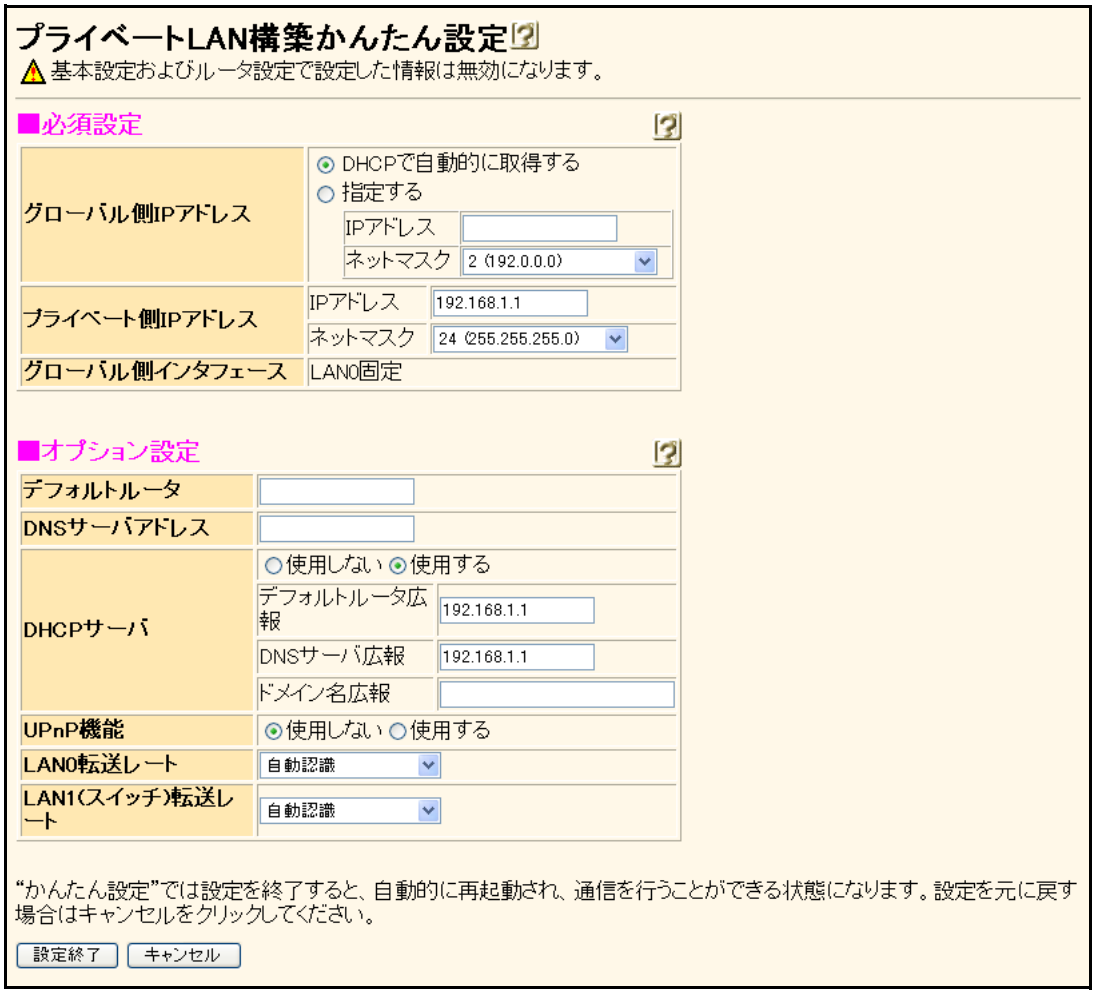

AAA 情報
グループ ID 情報
RADIUS 関連
基本情報
サーバ情報（クライアント機能）
送信情報（クライアント機能）
クライアント情報（サーバ機能）
ACL 情報
ACL 定義情報
基本定義情報
IP 定義情報
TCP 定義情報
UDP 定義情報
ICMP 定義情報
IPv6 定義情報
MAC 定義情報
IP 情報
基本情報
ルーティングプロトコル情報
インタフェース情報
ルーティングマネージャ情報
再配布情報
優先度情報
ECMP 情報
RIP 関連
RIP タイマ情報
RIP マルチパス情報
RIP 再配布フィルタリング情報
RIP ユニキャスト送信情報
RIP 相手フィルタリング情報


ルーティングプロトコル情報
BGP 関連
BGP 情報
IPv4 BGP ネットワーク情報
IPv4 BGP 集約経路情報
BGP 相手情報
BGP 相手基本情報
IPv4 BGP フィルタリング情報
BGP 拡張機能情報
IPv4 BGP 再配布フィルタリング情報
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 RP 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


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
SNMP情報
基本情報
SNMPv1/v2c情報
SNMPv3情報
ユーザ情報
MIBビュー情報
トラップ情報
ProxyDNS情報／URLフィルタ情報
共通情報
順引き情報
逆引き情報
ホストデータベース情報

3　プライベートLAN構築かんたん設定

［操作］　［かんたん設定メニュー］→「プライベートLAN構築」



3.1　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サーバが稼動している必要があります。**
- **グローバル側IPアドレスで“指定する”で設定すると、RIP情報が流れていないネットワークではデフォルトルータとDNSサーバアドレスを設定する必要があります。**

IPアドレス／ネットマスク

本装置のグローバル側のIPアドレスとネットマスクを指定します。

こんな事に気をつけて

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

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

グローバル側のインタフェースは、LAN0（基本ポート0）固定となります。

3.2　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せん。ProxyDNSを使用する場合は、本装置のIPアドレスを指定します。

ドメイン名広報

ドメイン名を80文字以内で指定します。省略するとDHCPサーバによる広報を行いません。なお、RFC1034では英数字、“.”（ピリオド）、“-”（ハイフン）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／LAN1（スイッチ）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。

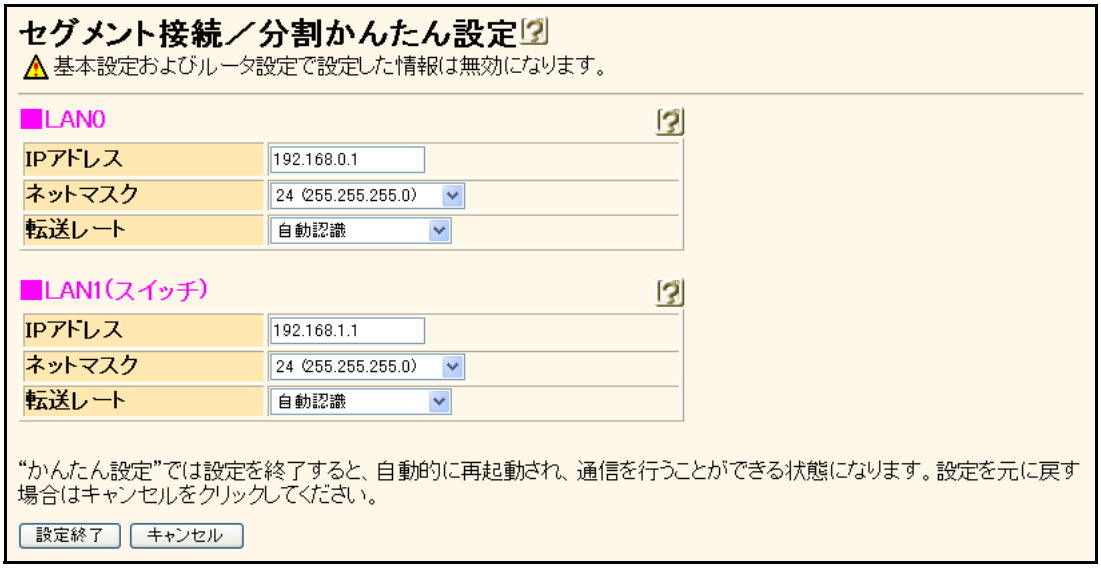
LAN1（スイッチ）転送レートで選択した値は、スイッチポート（SW1～4）で有効になります。

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。
- **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。**

4　セグメント接続／分割かんたん設定

［操作］　［かんたん設定メニュー］→「セグメント接続／分割」



4.1　LAN0

LAN0（基本ポート0）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。

4.2　LAN1（スイッチ）

LAN1（スイッチ）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（スイッチ）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。

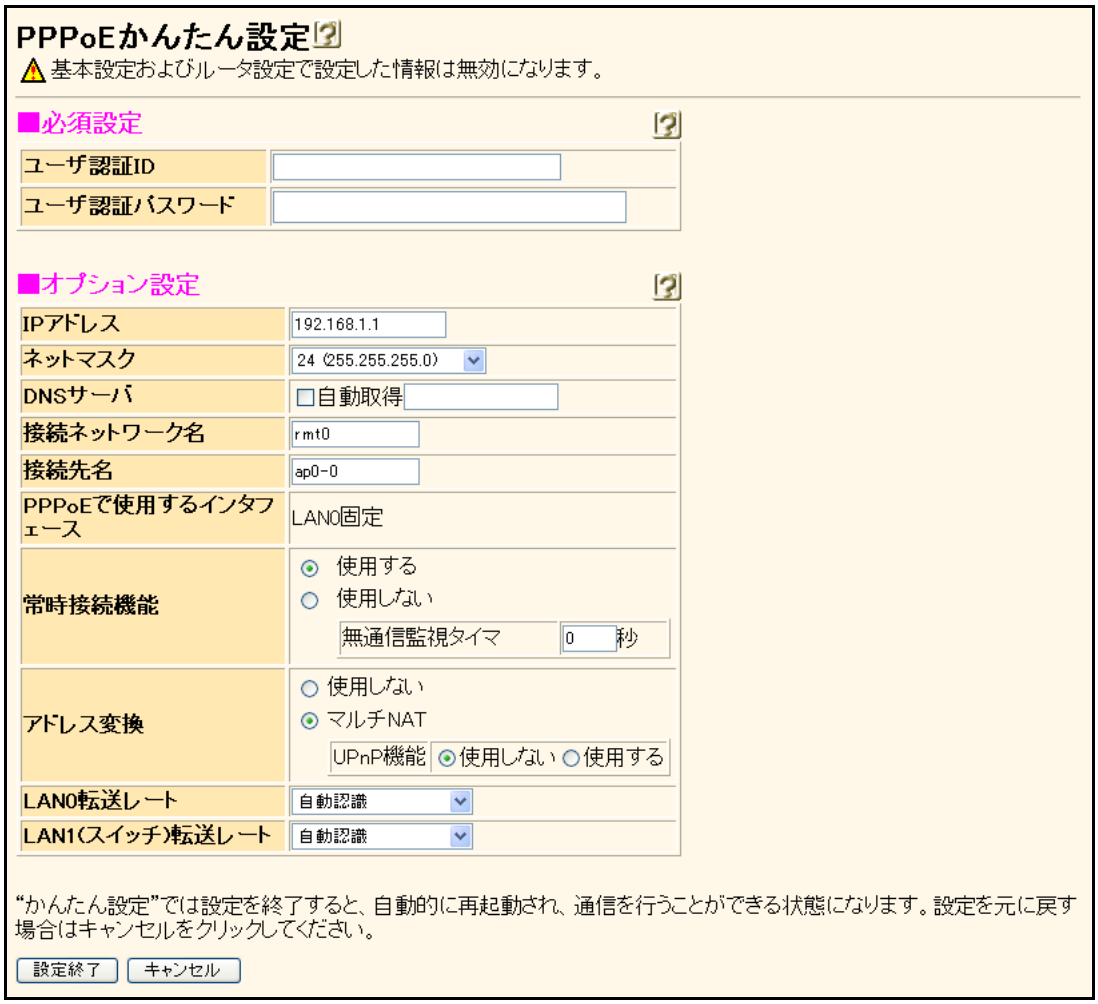
転送レートで選択した値は、スイッチポート（SW1～4）で有効になります。

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。**
- **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。**

5　PPPoE かんたん設定

［操作］　［かんたん設定メニュー］→「PPPoE 接続」



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、LAN1（スイッチ）がプライベート側となります。

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 ／ LAN1（スイッチ）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。

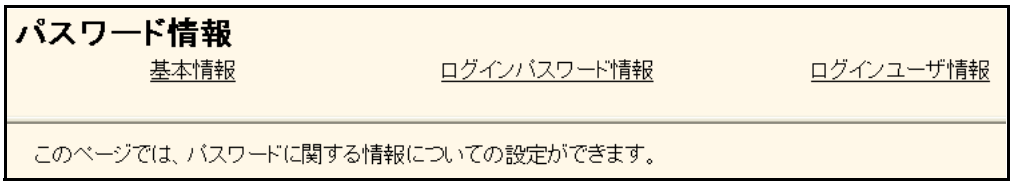
LAN1（スイッチ）転送レートで選択した値は、スイッチポート（SW1 ～4）で有効になります。

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。**
- **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。**

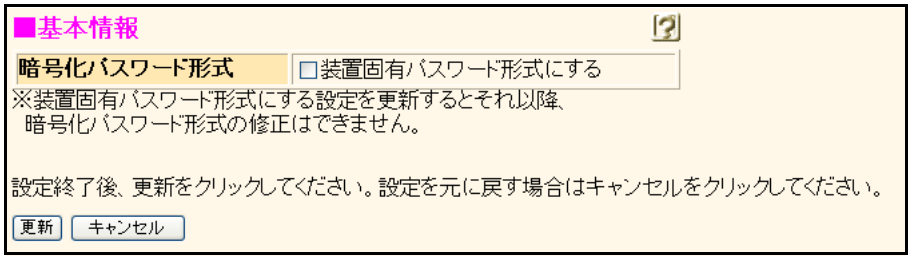
6　パスワード情報

［操作］　基本設定「パスワード情報」



6.1　基本情報

［操作］　基本設定「パスワード情報」→［基本情報］



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。

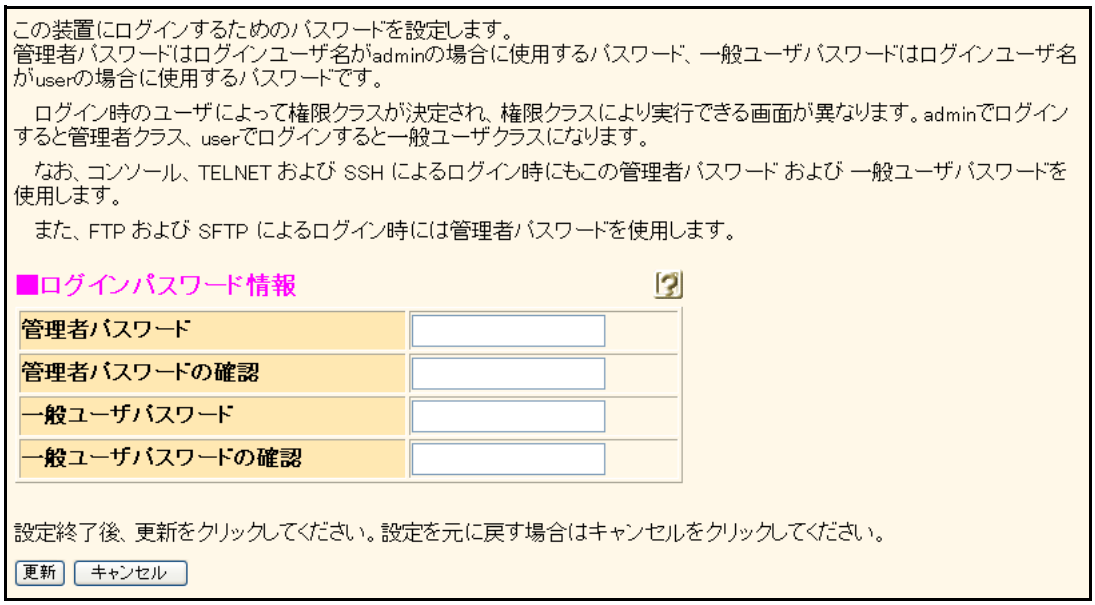
なお、暗号化パスワード形式の設定は更新直後から有効になります。

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。**

6.2 ログインパスワード情報

［操作］ 基本設定「パスワード情報」→［ログインパスワード情報］



本装置を操作するときのパスワードを設定します。

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

なお、パスワードの設定は更新直後から有効になります。

管理者パスワード

ログインユーザ名が admin の場合に、64 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

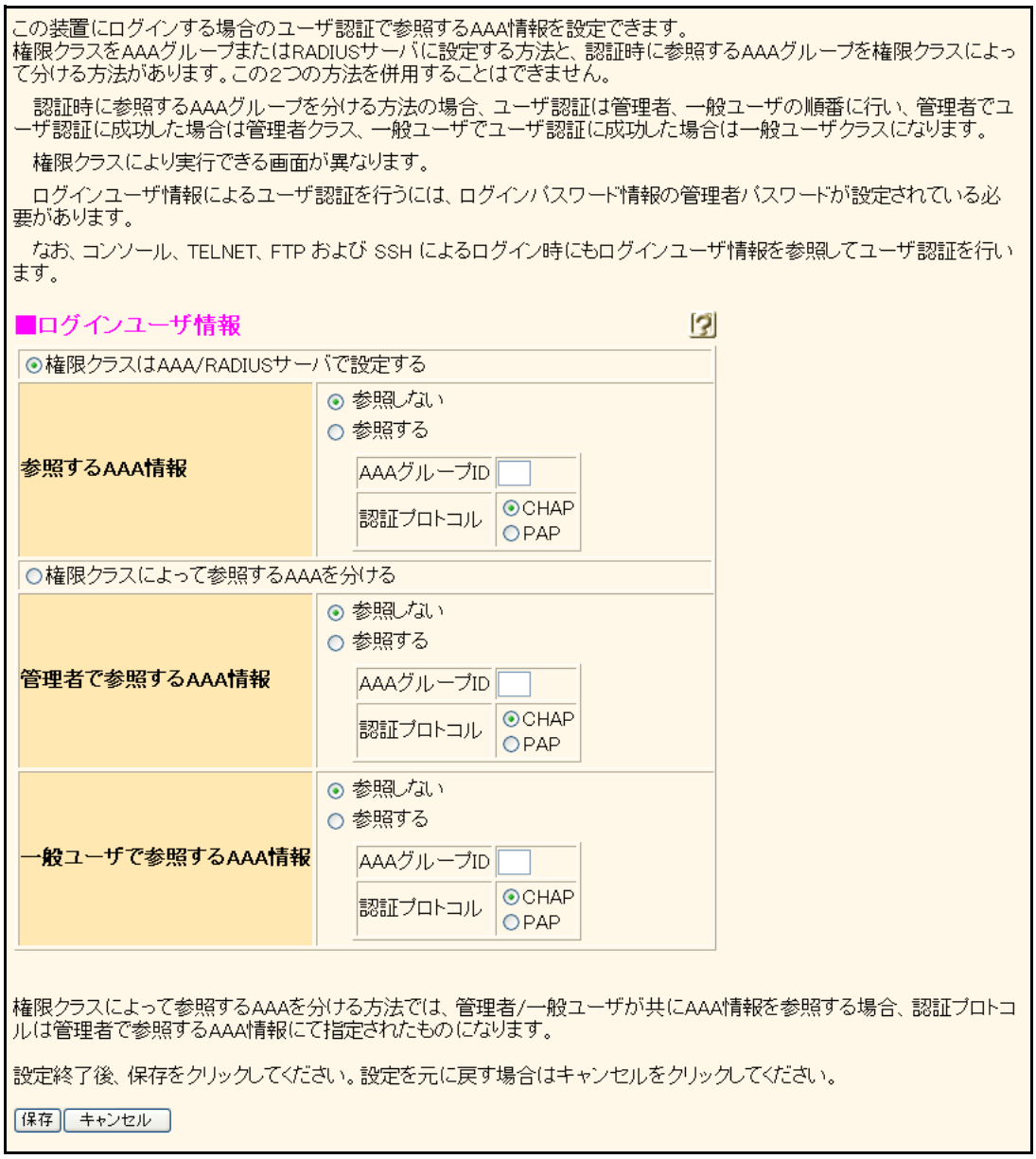
ログインユーザ名が user の場合に、64 文字以内でパスワードを指定します。user でログインすると権限クラスが一般ユーザクラスになります。

一般ユーザパスワードの確認

上記で指定した一般ユーザパスワードをもう一度指定します。

6.3 ログインユーザ情報

［操作］　基本設定「パスワード情報」→［ログインユーザ情報］



本装置にログインするときのユーザ認証で参照する AAA 情報を設定します。

以下の 2 つの方法があり、どちらかを選択します。

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

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

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

参照する AAA 情報

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

AAA グループ ID

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

認証プロトコル

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

管理者で参照する AAA 情報／一般ユーザで参照する AAA 情報

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

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

AAA グループ ID

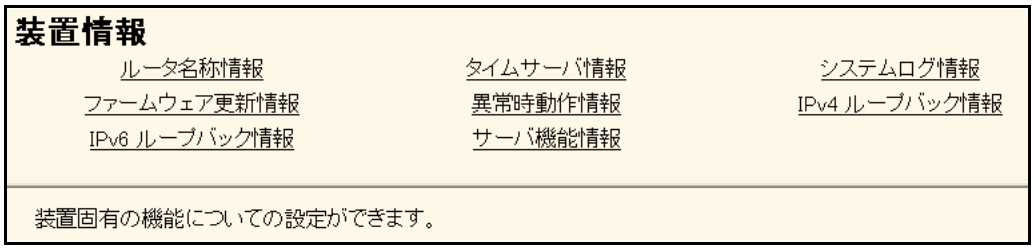
ユーザ認証を行う場合に参照する AAA のグループ ID を、10 未満の 10 進数で指定します。

認証プロトコル

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

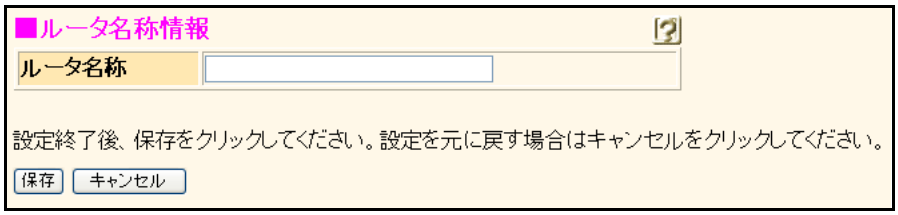
7　装置情報

［操作］　基本設定「装置情報」



7.1　ルータ名称情報

［操作］　基本設定「装置情報」→［ルータ名称情報］



ルータ名称

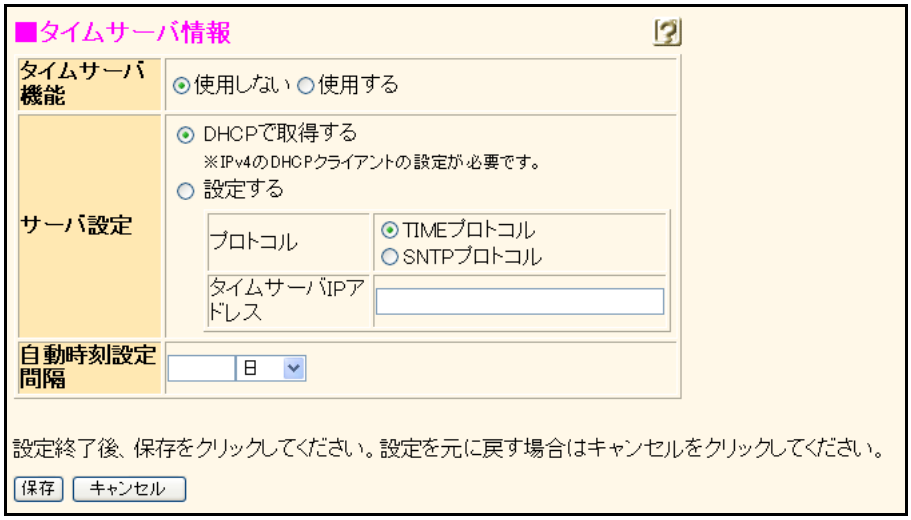
本装置の任意な名称を32文字以内で指定します。ルータ名称を設定すると、DHCPクライアント機能でDHCPサーバにルータ名称が広報されます。そのため、DHCPサーバからはこの名称で管理することができます。

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。

7.2 タイムサーバ情報

［操作］　基本設定「装置情報」→［タイムサーバ情報］



タイムサーバ機能

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

サーバ設定

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

プロトコル

タイムサーバから時刻情報を取得するときのプロトコルを選択します。

TIMEプロトコル
TIMEプロトコル（TCP）を使用する場合に指定します。

SNTPプロトコル
簡易NTPプロトコル（UDP）を使用する場合に指定します。

タイムサーバIPアドレス

タイムサーバのIPv4／IPv6アドレスを指定します。

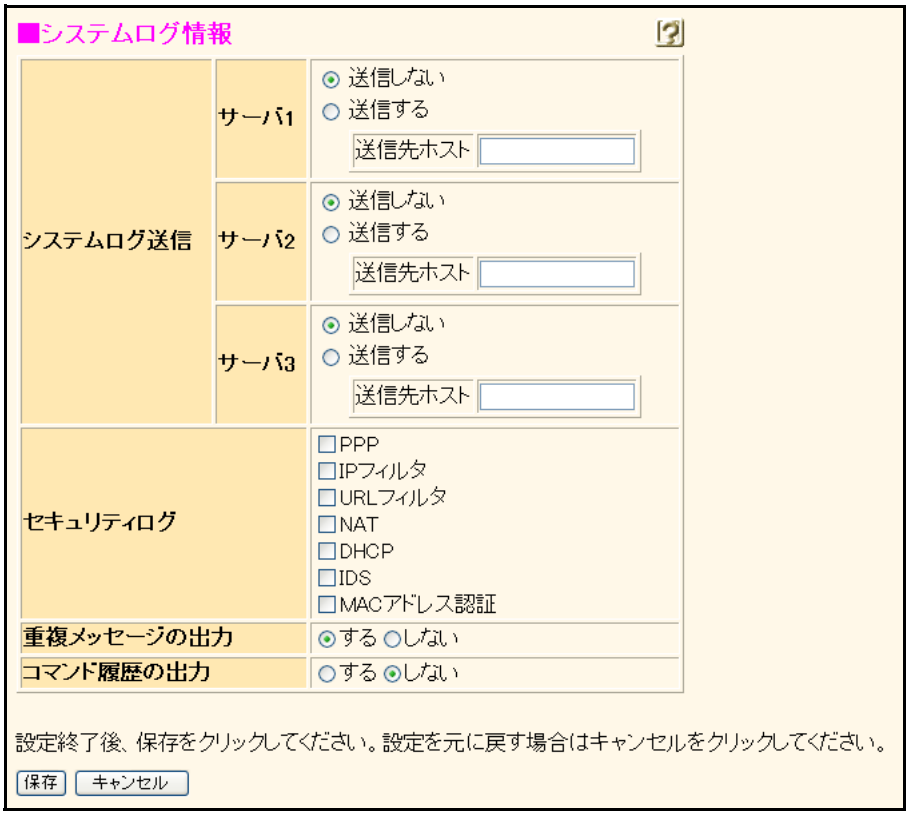
有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254
::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

自動時刻設定間隔

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

7.3　システムログ情報

［操作］　基本設定「装置情報」→［システムログ情報］



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、マニュアル「コマンドリファレンス-構成定義編-」の「syslog pri」および「syslog facility」を参照してください。

システムログ送信

syslog形式で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。送信先のサーバは3台まで定義できます。

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

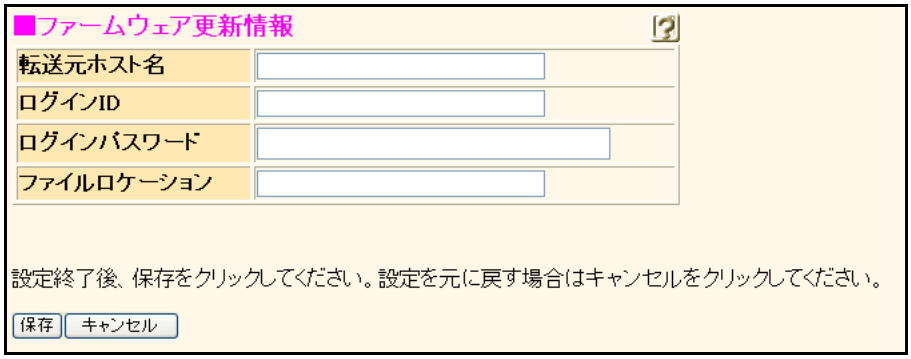
システムログにメッセージを出力するとき、直前に出力したメッセージと重複した場合に出力する場合は、“する”を選択します。

コマンド履歴の出力

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

7.4　ファームウェア更新情報

［操作］　基本設定「装置情報」→［ファームウェア更新情報］



ファームウェアを入れ替えたり、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:ffff
fec0:: ～ feff:ffff: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

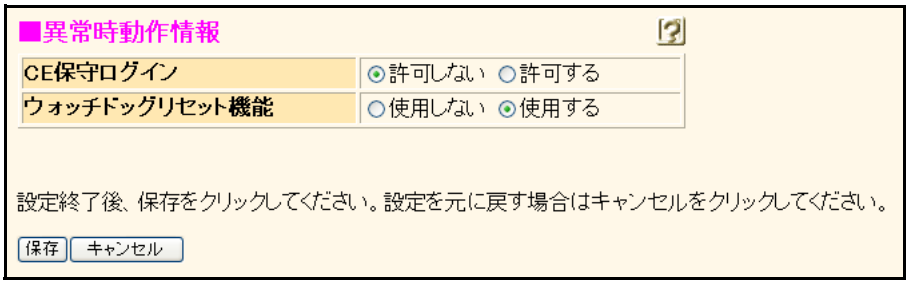
ファームウェア更新用のパスワードを 32 文字以内で指定します。

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。

7.5　異常時動作情報

［操作］　基本設定「装置情報」→［異常時動作情報］



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

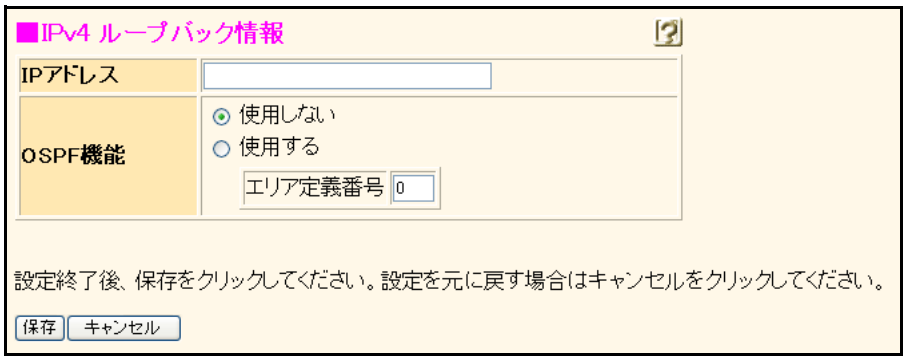
CE ログインを許可する場合は、“ 許可する ” を選択します。CE ログインを許可することで、CE の保守作業を円滑に進めることができます。

ウォッチドッグリセット機能

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

7.6　IPv4 ループバック情報

［操作］　基本設定「装置情報」→［IPv4 ループバック情報］



IP アドレス

ループバックインタ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、ループバックアドレスを使用しないものとします。

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

こんな事に気をつけて

- **ほかのインタフェースと違うネットワークの IP アドレスを設定してください。**
- **127.0.0.1 はループバックインタ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。

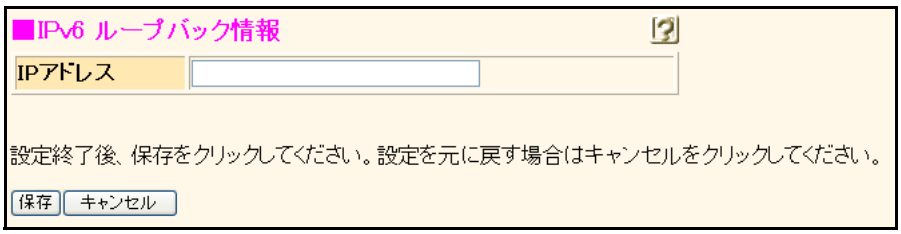
OSPF を使用できるインタフェースは、装置全体で 50 個までです。

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。省略時は 0 が設定されます。

7.7　IPv6 ループバック情報

［操作］　基本設定「装置情報」→［IPv6 ループバック情報］



IP アドレス

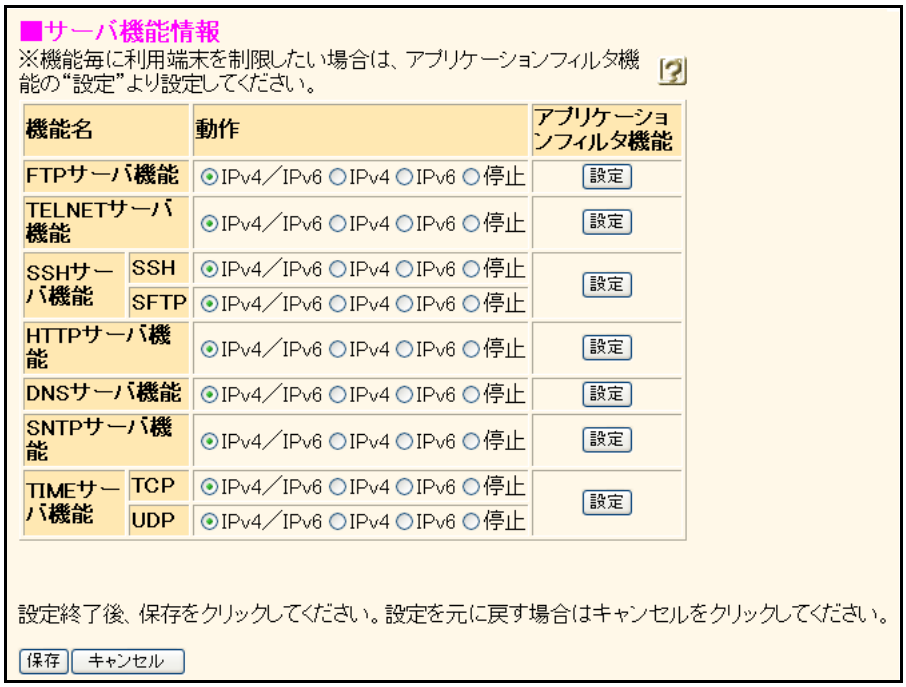
ループバックインタフェースに割り当てる追加 IPv6 アドレスを 128 ビットで指定します。本装置ではプレフィックス長は 128 に固定となります。省略時は、ループバックアドレスを使用しないものとします。

こんな事に気をつけて

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

7.8　サーバ機能情報

［操作］　基本設定「装置情報」→［サーバ機能情報］



サーバ機能情報

本装置の以下のサーバ機能を設定します。

- FTP サーバ機能
- TELNET サーバ機能
- SSH サーバ機能（SSH ／ SFTP）
- HTTP サーバ機能
- DNS サーバ機能
- SNTP サーバ機能
- TIME サーバ機能（TCP ／ UDP）

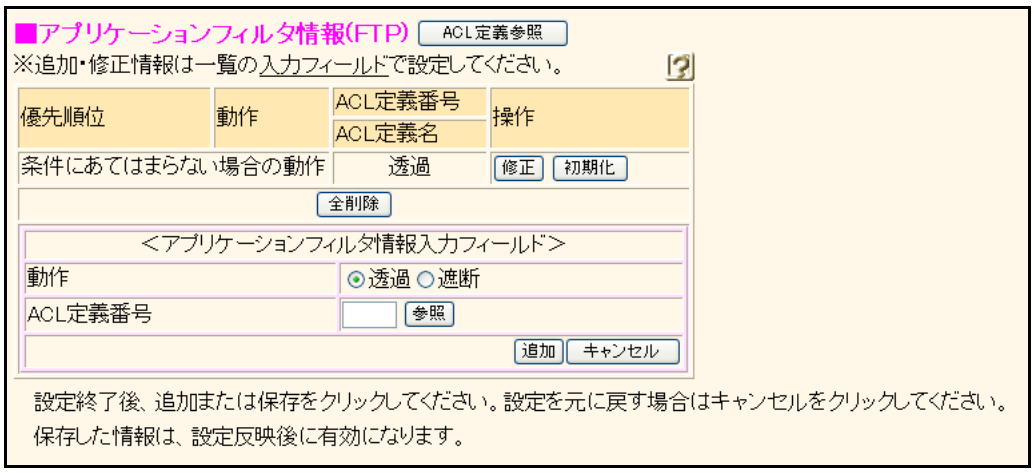
各サーバ機能に対して、有効にするプロトコルを以下から選択します。

- 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。

7.8.1 アプリケーションフィルタ情報

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



こんな事に気をつけて

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

動作

アプリケーションフィルタの動作を以下の 2 つから選択します。

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

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

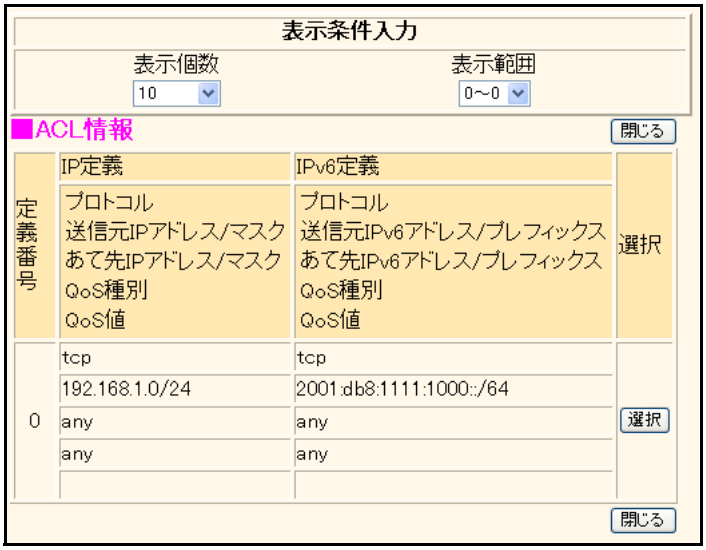
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- IPv6 定義

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

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

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



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

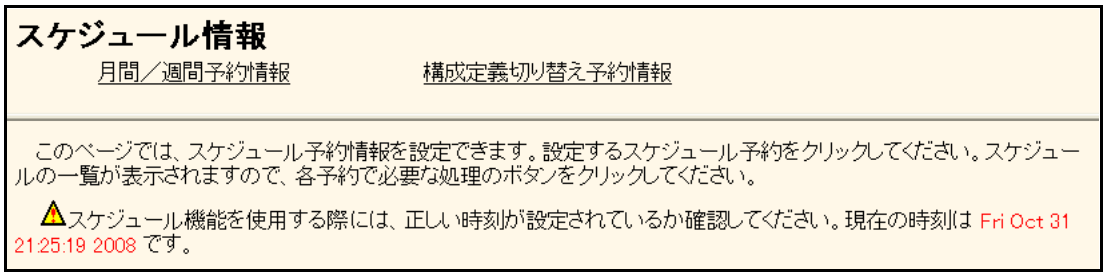
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

8　スケジュール情報

［操作］　基本設定「スケジュール情報」

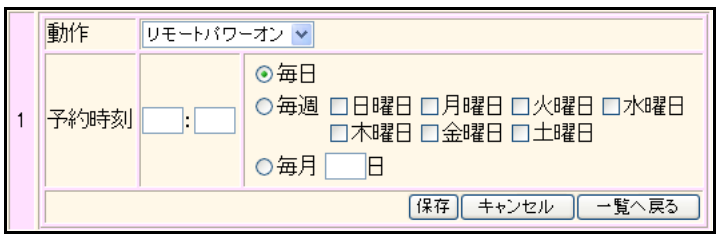


8.1　月間／週間予約情報

［操作］　基本設定「スケジュール情報」→［月間／週間予約情報］

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。

［操作］　基本設定「スケジュール情報」→［月間／週間予約情報］→［修正］



動作

リモートパワーオンだけをサポートしています。

リモートパワーオン

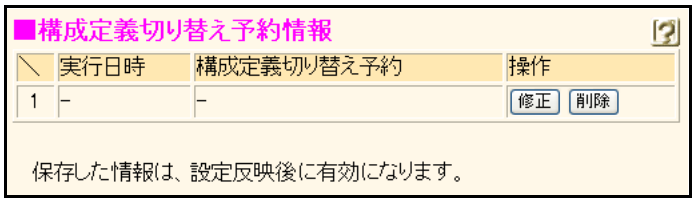
予約時刻にホストデータベース情報でMACアドレスが登録されているWake up on LANに対応したすべてのパソコンに対してリモートパワーオン処理を実施します。

予約時刻

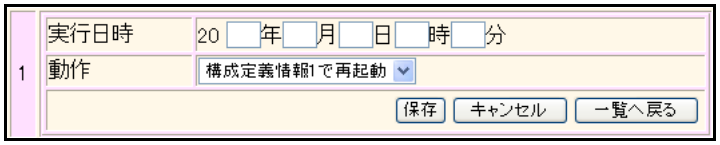
選択した動作を実行（開始）する時刻と実行周期を指定します。

8.2 構成定義切り替え予約情報

［操作］　基本設定「スケジュール情報」→［構成定義切り替え予約情報］



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



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

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

こんな事に気をつけて

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

実行日時

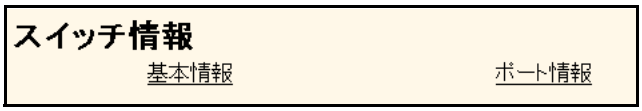
構成定義情報を切り替える日時を西暦で2000～2036年の範囲で指定します。

動作

切り替える構成定義情報を指定します。

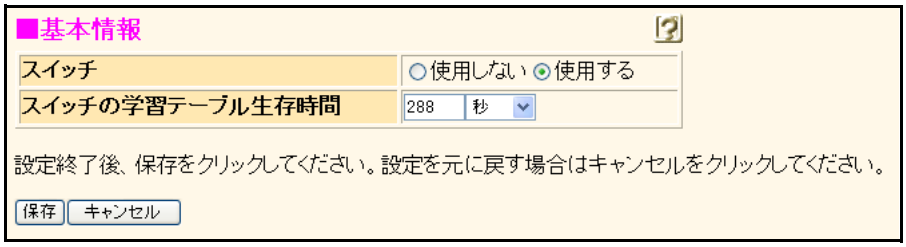
9　スイッチ情報

［操作］　ルータ設定「スイッチ情報」



9.1　基本情報

［操作］　ルータ設定「スイッチ情報」→［基本情報］



スイッチ

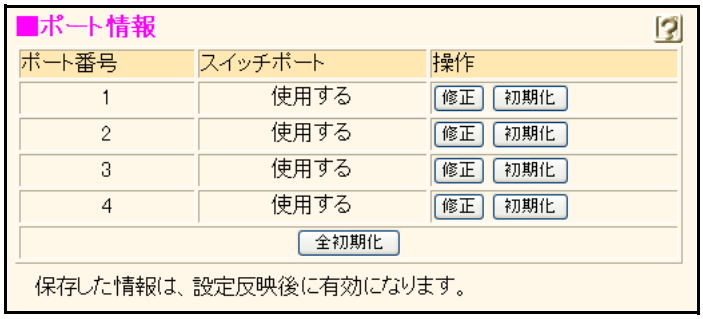
LAN1 ポートのモードを設定します（Si-R90brin では設定できません）。
“ 使用する ” を選択した場合、LAN1 ポートはスイッチポート（SW1 ～ 4）として利用できます。

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。

9.2 ポート情報

［操作］　ルータ設定「スイッチ情報」→［ポート情報］



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

［操作］　ルータ設定「スイッチ情報」→［ポート情報］→［修正］

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。

10　LAN 情報

［操作］　ルータ設定「LAN 情報」

現在、設定されている LAN インタフェースの定義が表示されています。LAN インタフェースには、物理インタフェースと VLAN インタフェースがあります。装置全体での LAN インタフェースの定義数は、2 つ合わせて 10 個まで設定できます。ただし、物理インタフェースの有効な定義数は 2 個までです。処理するボタンをクリックし、次のページへ進みます。

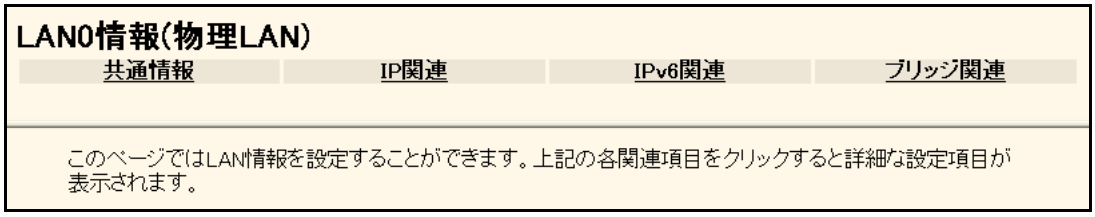
インタフェース

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。

10.1 インタフェース：物理 LAN

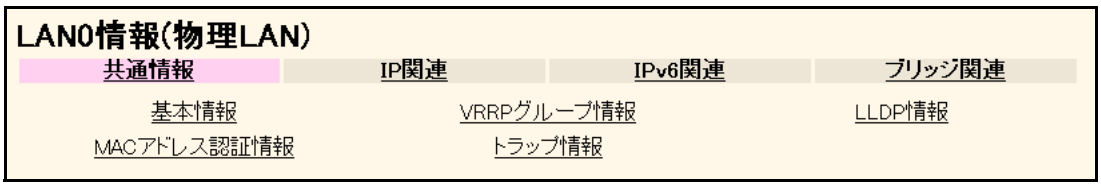
［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］



「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。

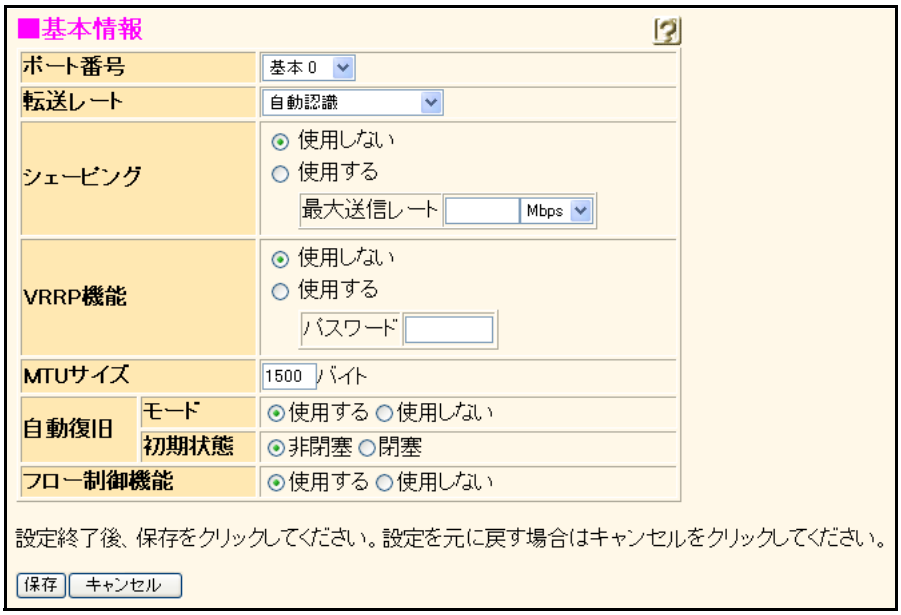
10.1.1 共通情報

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



10.1.1.1 基本情報

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



ポート番号

起動時に使用する物理ポート番号を選択します。

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）
- 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 1 ～ 100000 Kbps の範囲で指定します。Kbps は 1000bps を、Mbps は 1000Kbps を意味します。

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。

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

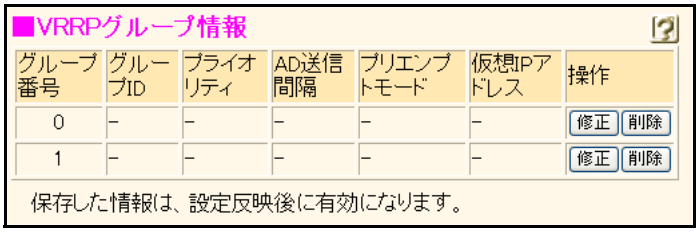
初期状態を " 閉塞 " にすると、閉塞状態で動作を開始し、オペレータからの閉塞状態解除指示を待ちます。

フロー制御機能

フロー制御の動作を行う場合は、" 使用する " を選択します。

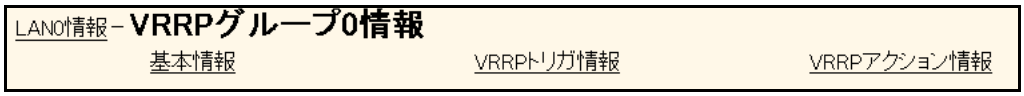
10.1.1.2 VRRP グループ情報

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



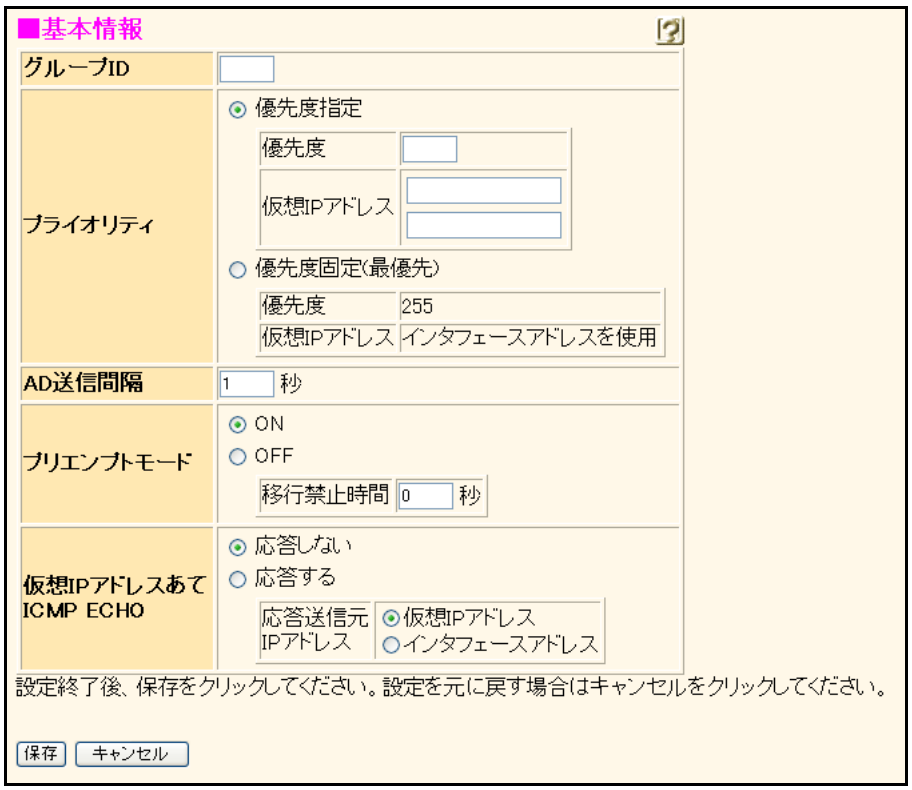
現在、設定されている VRRP グループ情報の定義が表示されています。VRRP グループは、それぞれのインタフェースで 2 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

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



10.1.1.2.1 基本情報

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



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。本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

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を構成するほかの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、本装置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、マスタの交替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。

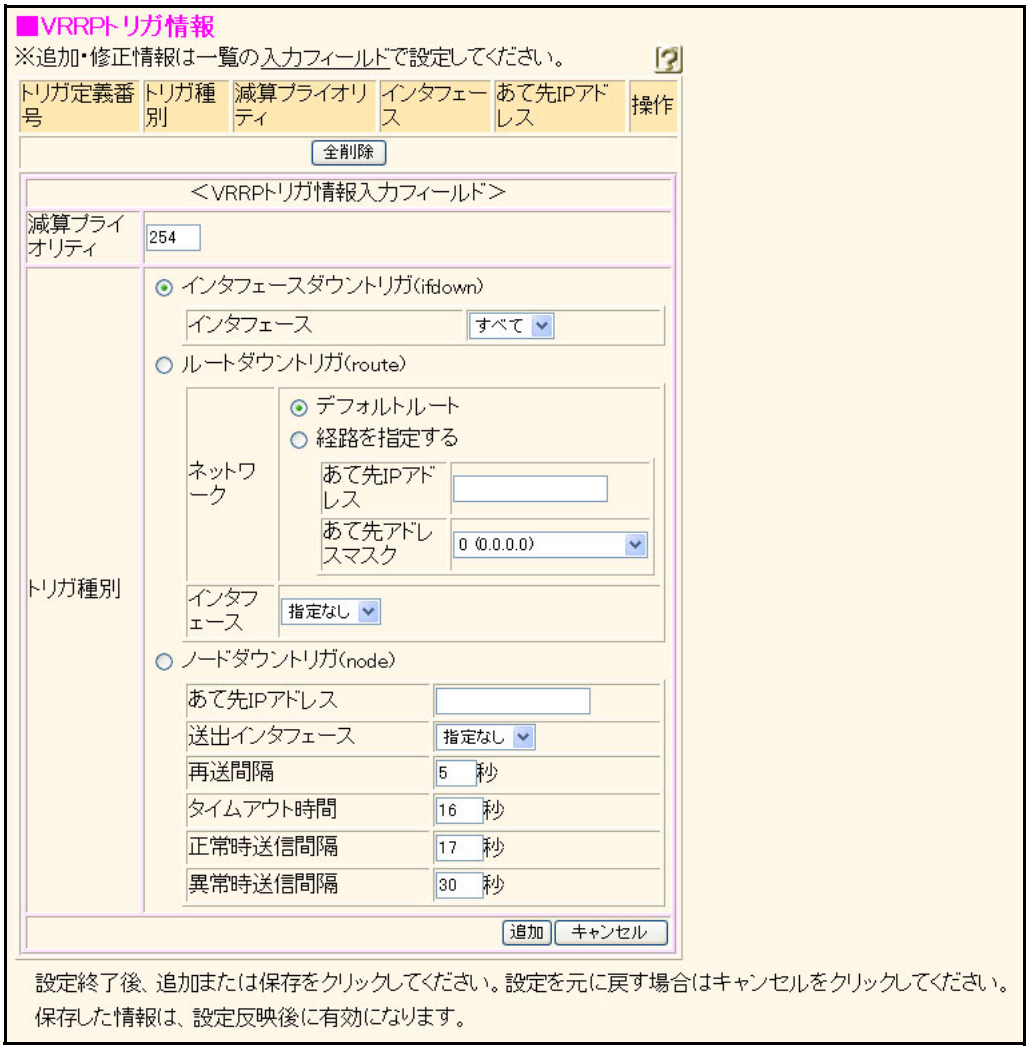
“応答する”を選択した場合は、応答パケットの送信元IPアドレスを設定します。

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”のどちらかを選択します。

10.1.1.2.2 VRRP トリガ情報

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



現在、設定されている VRRP トリガ情報の定義が表示されています。VRRP トリガの定義数は、装置全体で 50 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。

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

減算プライオリティ

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

トリガ種別

トリガとなる種別を以下の3つから選択します。

- インタフェースダウントリガ（ifdown）
  指定されたインタ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パケット送信元IPアドレスは、VRRPが設定されたLANインタフェースのIPv4アドレスとなります。応答を受信するための経路情報が正しくない場合は、不当に異常を検出することがあります。

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。

インタフェースダウントリガ（ifdown）を指定する場合

“すべて”を選択した場合は、すべてのLANインタフェースが対象です。

ルートダウントリガ（route）を指定する場合

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

ネットワーク

“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、あて先IPアドレス、あて先アドレスマスクを指定します。

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指定します。指定したホストまたはネットワーク範囲へのパケット送出経路が対象となります。

あて先IPアドレス

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

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

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。

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

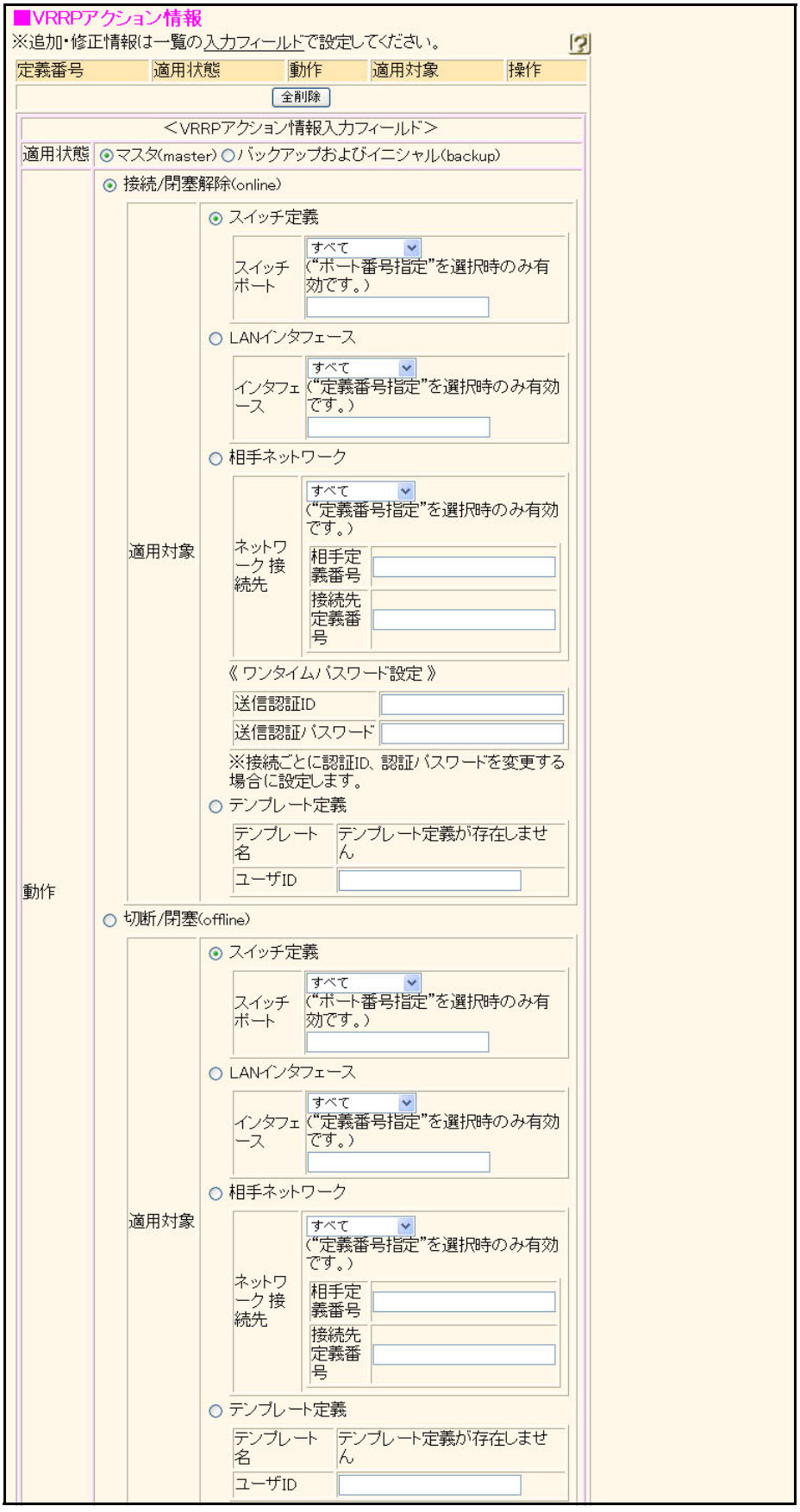
ICMP ECHOパケットの応答が正常に受信されている状態で、次にICMP ECHOパケットを送信する時間を、（[タイムアウト時間+1] ～255）秒の範囲で指定します。正常に受信されている状態での周期送信間隔です。省略時は、タイムアウト時間+1秒が設定されます。

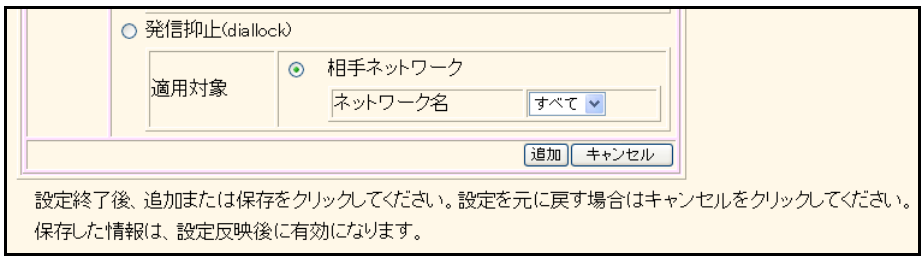
異常時送信間隔

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。

10.1.1.2.3 VRRP アクション情報

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





現在、設定されているVRRPアクション情報の定義が表示されています。VRRPアクションの定義数は、装置全体で10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。

設定した適用状態にVRRPが状態変化すると動作を適用します。条件にあてはまるすべて動作が適用されます。

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3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。

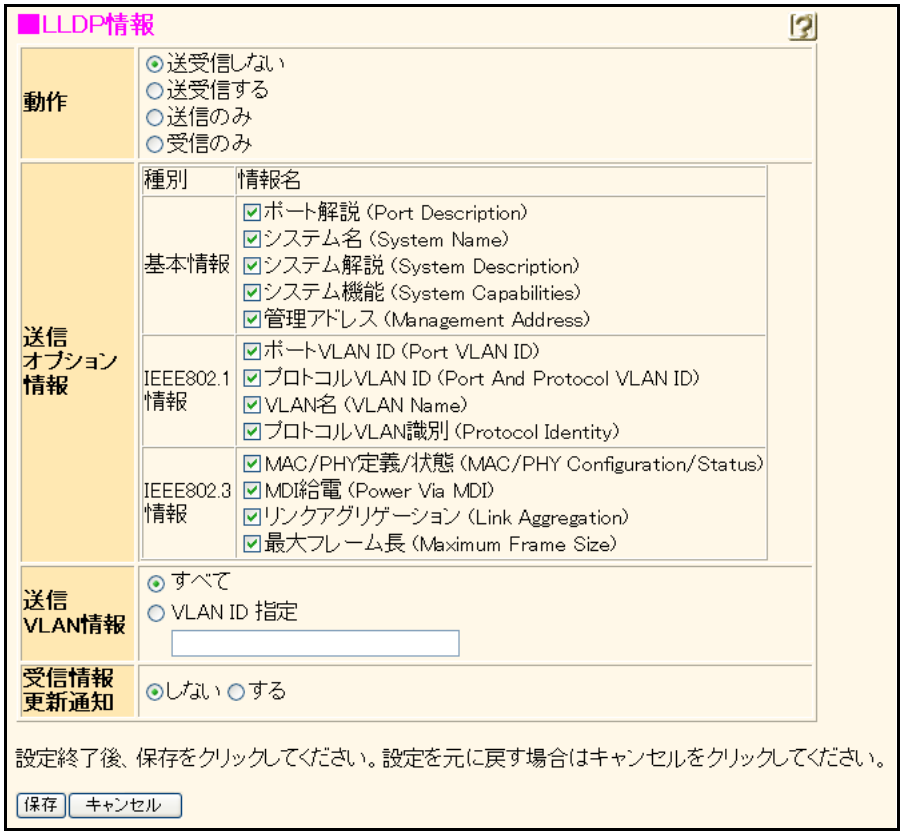
適用対象

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。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。最大5組まで設定できます。
- 相手ネットワーク（online、offline）
  ネットワーク接続先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したユーザ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）
  発信抑止の対象となるネットワークを選択します。

10.1.1.3 LLDP 情報

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



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

こんな事に気をつけて

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

動作

LLDP の動作を選択します。

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

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

送信オプション情報

送信するオプション情報を選択します。

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

オプション情報をすべて送信しないようにしても、必須情報が常に送信されます。

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

送信 VLAN 情報

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

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

受信情報更新通知

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

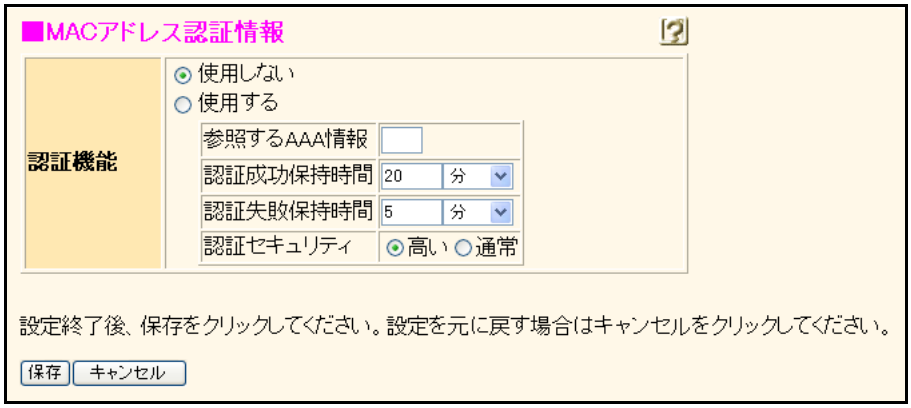
- 新たな LLDP 情報を受信した
- 受信していた LLDP 情報の有効時間が経過して受信情報を破棄した
- 有効時間が 0 の LLDP 情報を受信して受信情報を破棄した
- LLDP 最大受信数を超えて LLDP 情報を受信したため受信情報を破棄した
- 「表示メニュー」-「LLDP 関連」-「隣接情報」の［隣接情報クリア］ボタンをクリックして受信情報を破棄した
- clear lldp neighbors コマンドを実行して受信情報を破棄した

こんな事に気をつけて

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

10.1.1.4 MACアドレス認証情報

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



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。

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。

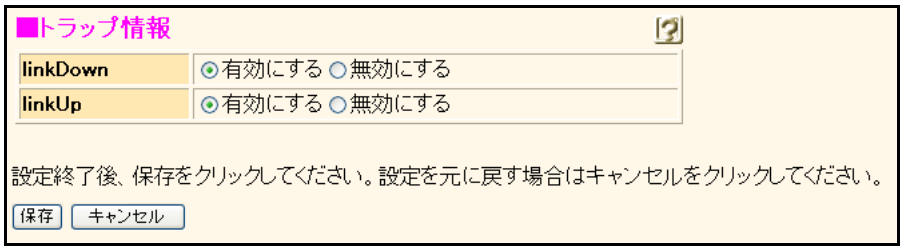
認証セキュリティ

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。

10.1.1.5 トラップ情報

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



トラップ情報

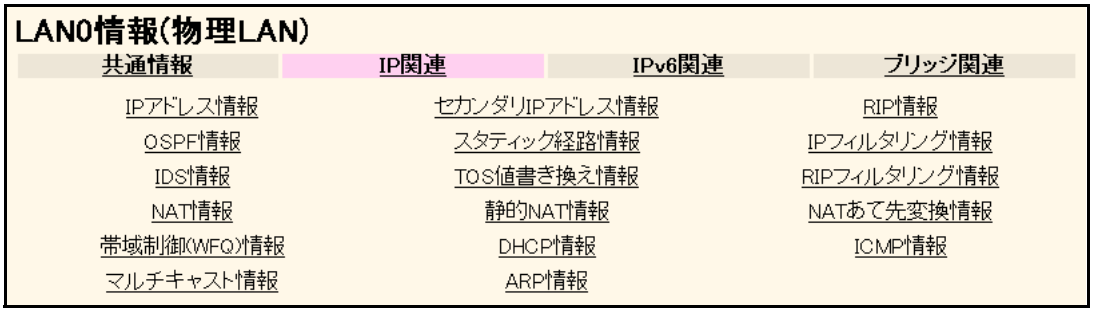
SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP エージェント機能を利用しない場合は、この設定は意味を持ちません。

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

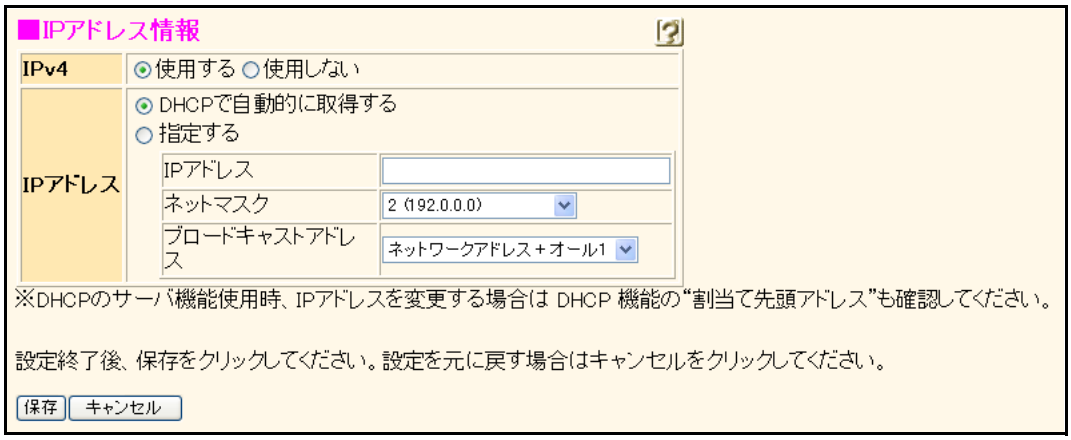
10.1.2　IP関連

［操作］　ルータ設定「LAN情報（物理LAN）」→［修正］→［IP関連］



10.1.2.1　IPアドレス情報

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



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。

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

こんな事に気をつけて

IPアドレスに0.0.0.0を指定すると通信ができなくなります。

ネットマスク

本装置のネットマスクを指定します。

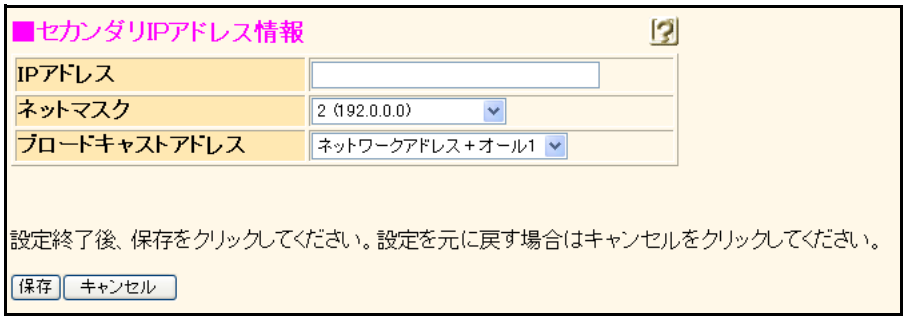
ブロードキャストアドレス

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

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

10.1.2.2 セカンダリ IP アドレス情報

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



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）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

ネットマスク

セカンダリアドレスのネットマスクを指定します。

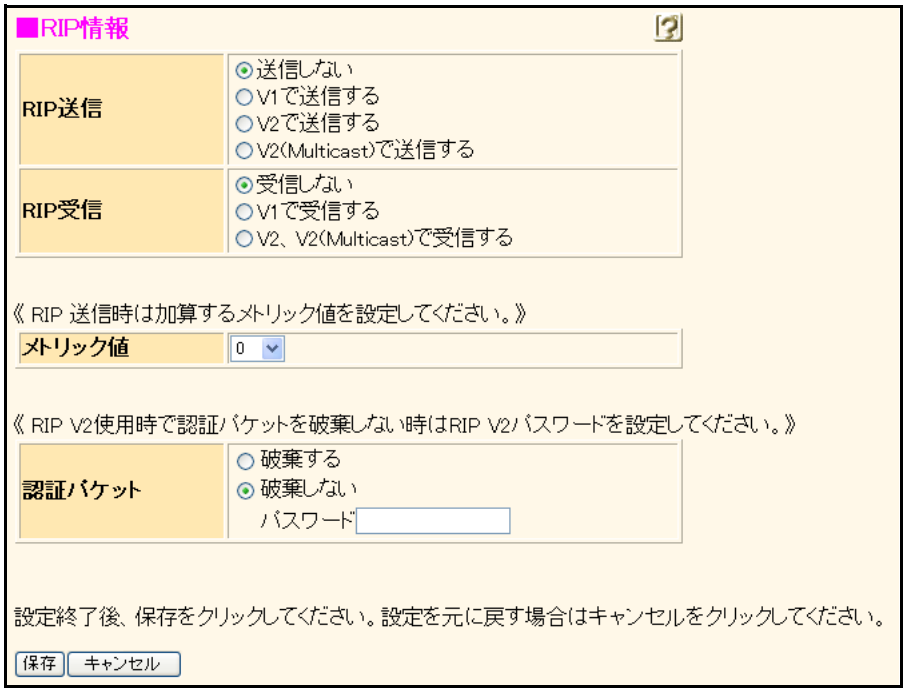
ブロードキャストアドレス

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

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

10.1.2.3 RIP 情報

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



RIP を使用できるインタフェースの定義数は、装置全体で 50 個まで設定できます。

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

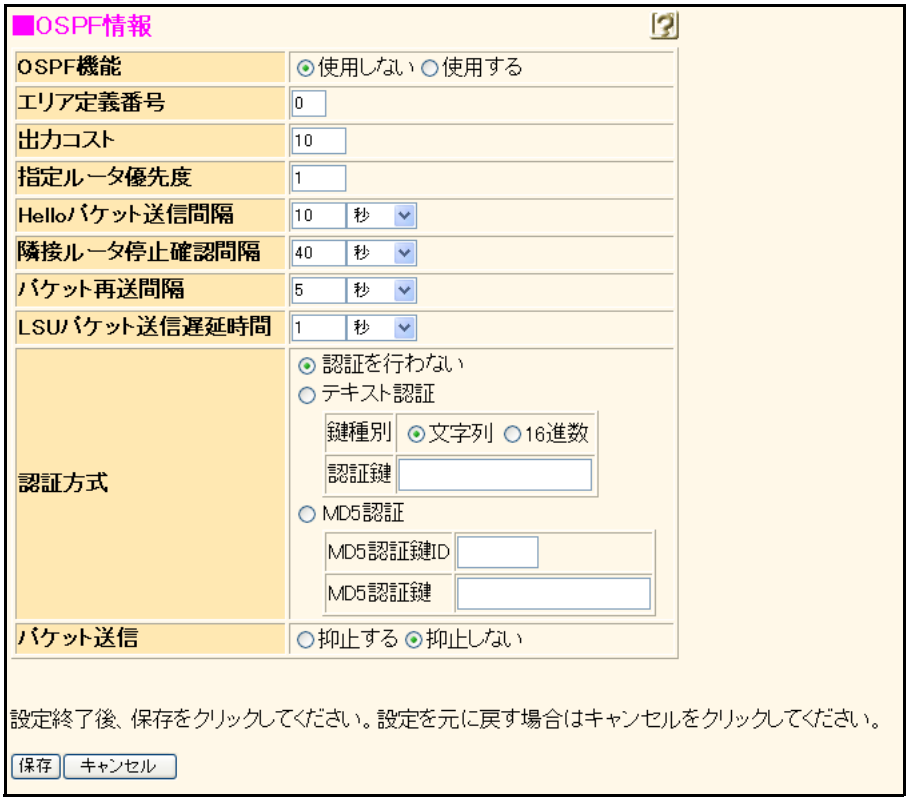
RIP 送信時に加算するメトリック値を選択します。

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。

10.1.2.4 OSPF 情報

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



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、装置全体で 50 個まで設定できます。

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薦めします。通常は “40 秒 ” を指定します。

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

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

パケット再送間隔

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

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
3 ～ 65535 秒

LSU パケット送信遅延時間

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

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

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

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が “ 文字列 ” の場合は、8 文字以内で指定します。鍵種別が “16 進数 ” の場合は、16 進数を使用して 16 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

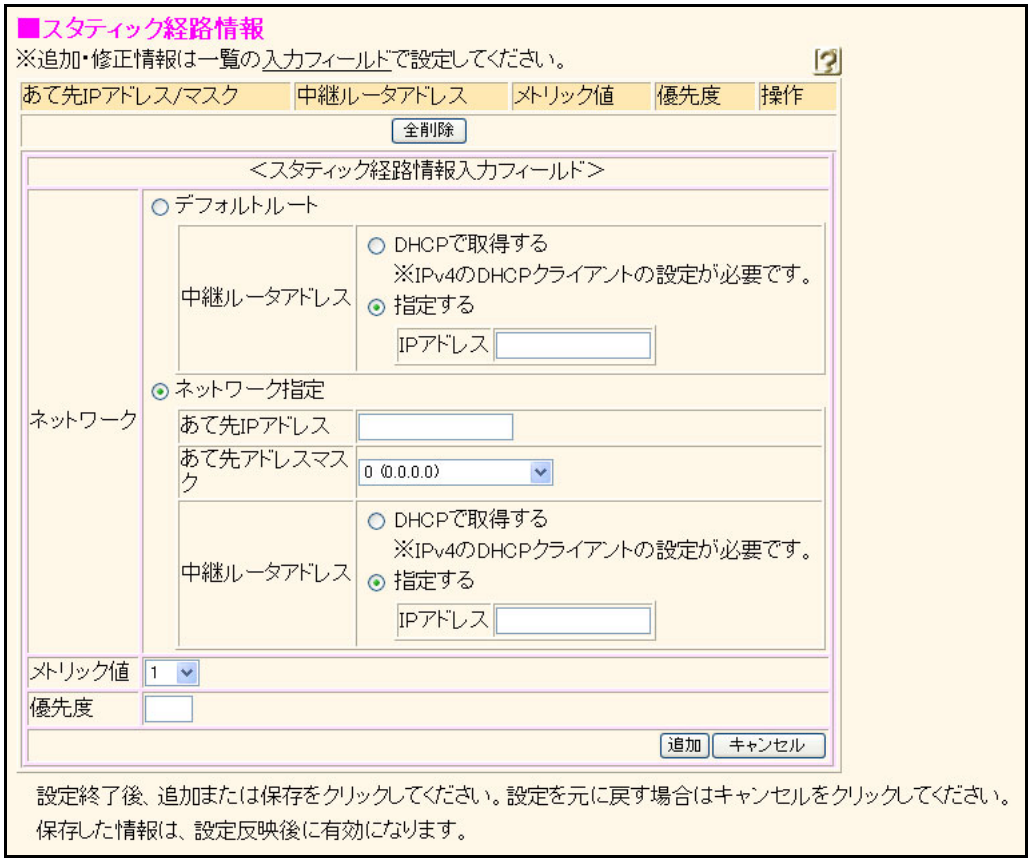
MD5 認証鍵を指定します。16 文字以内で指定します。

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。

10.1.2.5 スタティック経路情報

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



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、装置全体で128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。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
  中継ルータアドレスを指定します。
  - DHCPで取得する
    受け取ったゲートウェイアドレスを中継ルータアドレスとして使用します。
  - 指定する
    中継ルータアドレスをIPアドレスで指定します。
- ネットワーク指定
  あて先IPアドレス、あて先アドレスマスク、中継ルータアドレスを指定します。
  なお、あて先IPアドレスに0.0.0.0、あて先アドレスマスクに0（0.0.0.0）を設定した場合、“デフォルトルート”を指定したものとして動作します。

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進数で指定します。
優先度は数値の小さい方がより高い優先度を示します。

- 中継ルータアドレスとして“指定する”を選択した場合
  0～254の10進数で指定します。省略時は、0が指定されたものとみなされます。
- 中継ルータアドレスとして“DHCPで取得する”を選択した場合
  1～254の10進数で指定します。省略時は、1が指定されたものとみなされます。

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

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

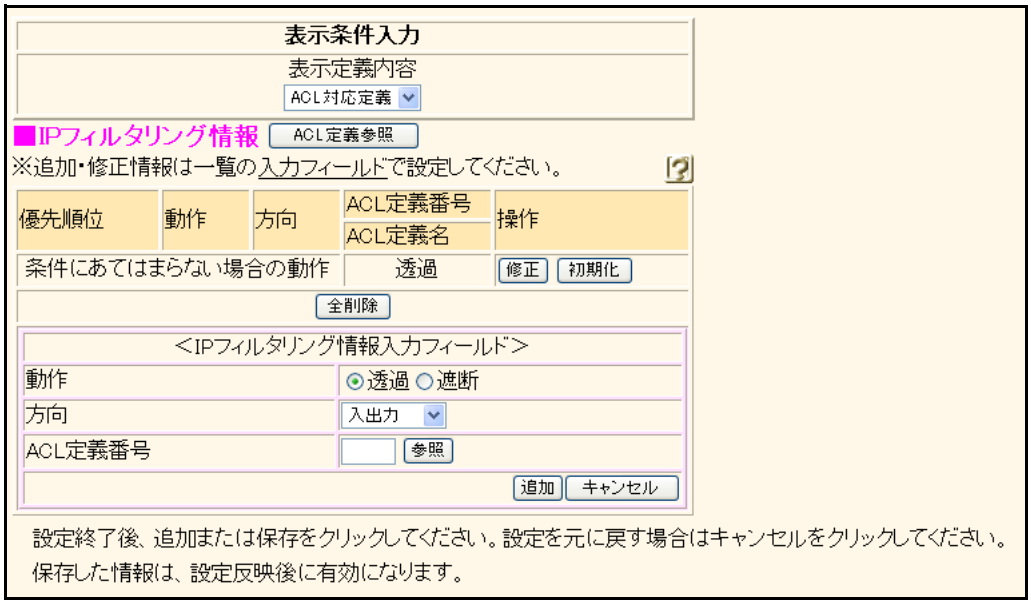
こんな事に気をつけて

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

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

10.1.2.6 IP フィルタリング情報

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



現在、設定されている IP 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。IP フィルタリングの定義数は、64 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。

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

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

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

動作

IP フィルタリングの動作を以下の 2 つから選択します。

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

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
  入力パケットだけをフィルタリングする対象とします。
- 出力のみ
  出力パケットだけをフィルタリングする対象とします。
- リバース
  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下の2つを逆転した条件でフィルタリングします。
  - 送信元IPアドレス／アドレスマスクとあて先IPアドレス／アドレスマスク
  - 送信元ポート番号とあて先ポート番号

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

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

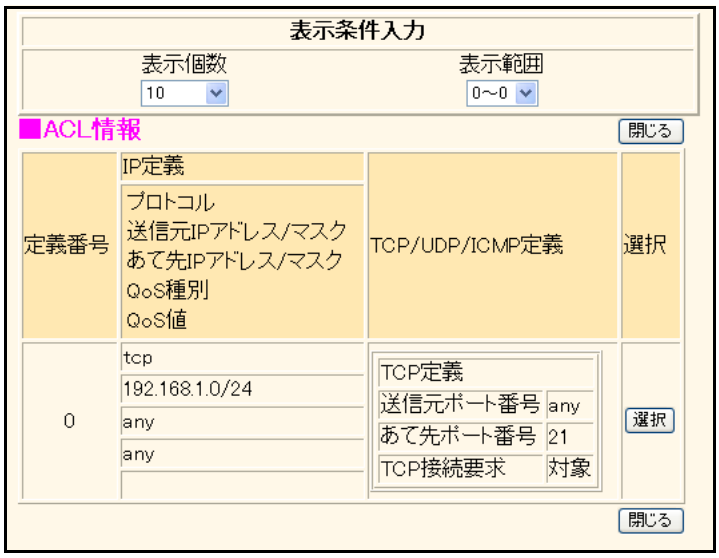
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

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

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

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



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

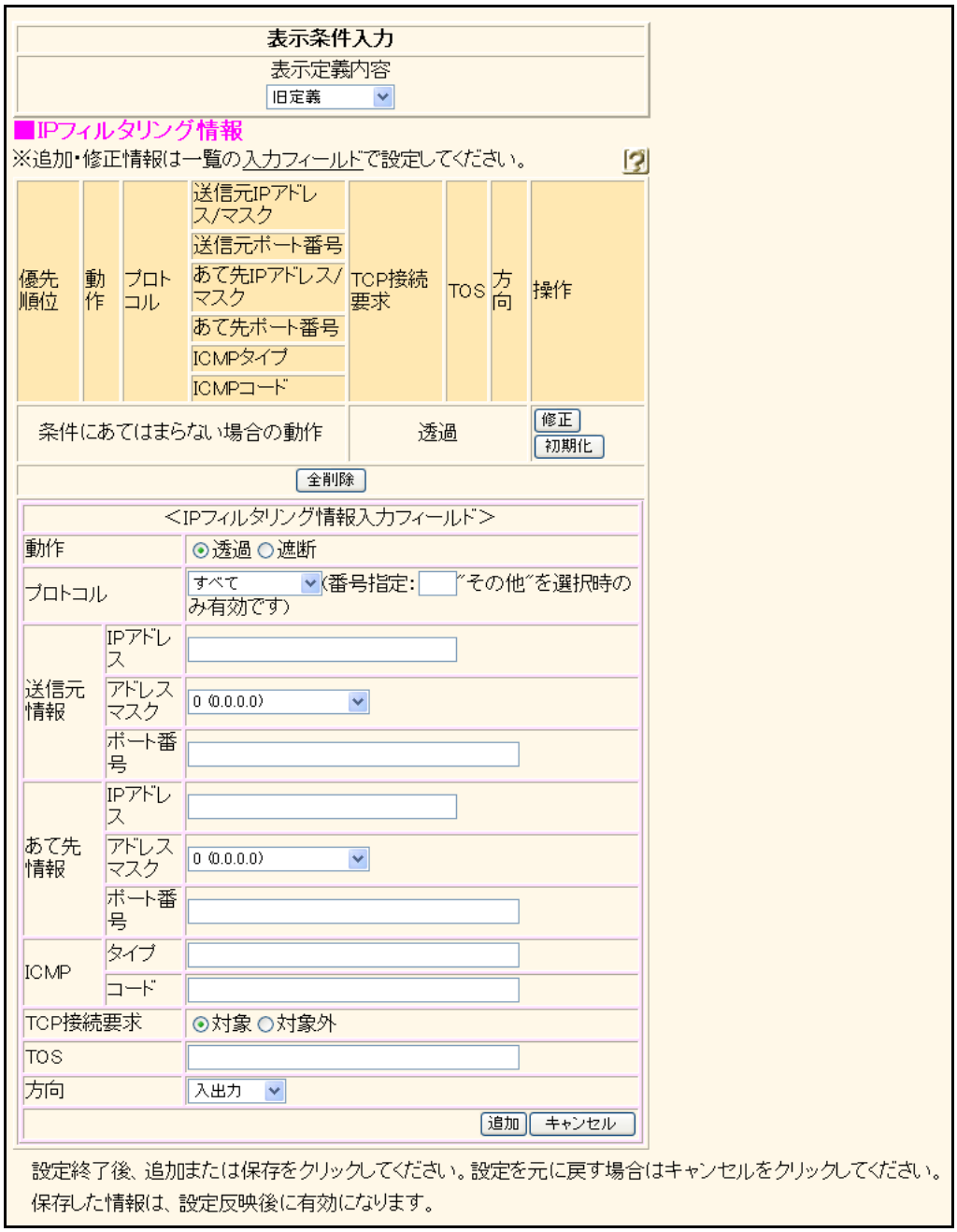
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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。

10.1.2.6.1 IP フィルタリング情報（旧定義）

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



表示条件入力に、“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

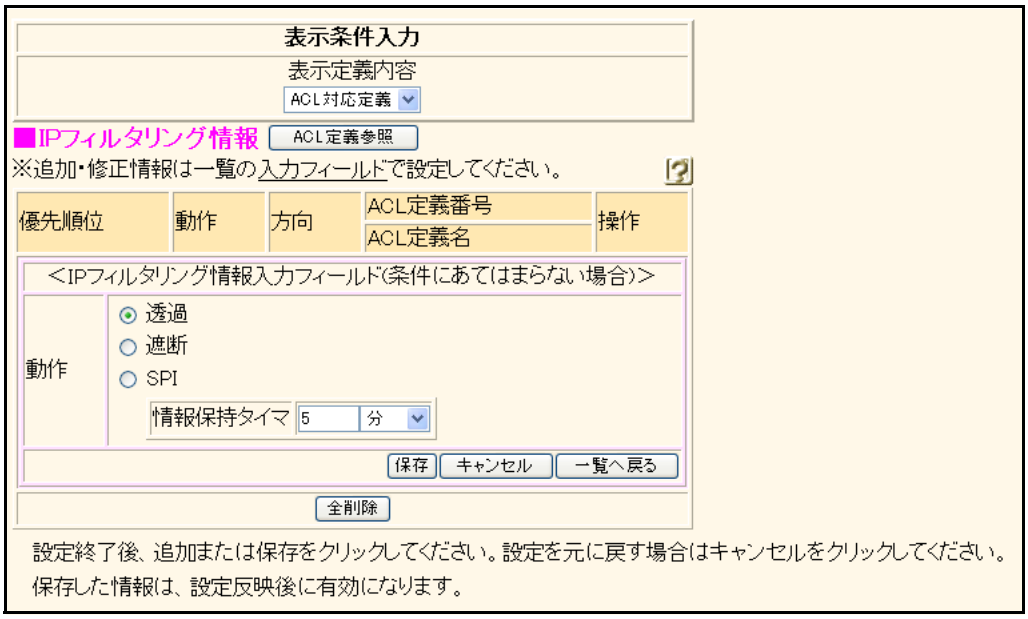
フィルタリングする方向を以下の4つから選択します。

- 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。

10.1.2.6.2 IP フィルタリング情報（条件にあてはまらない場合の動作）

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IP 関連］→［IP フィルタリング情報］→「条件にあてはまらない場合の動作」［修正］



「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。

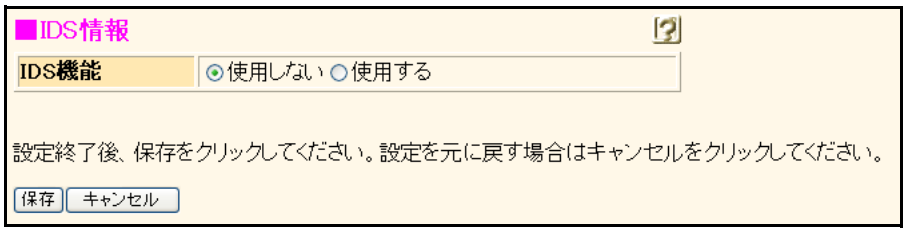
- 透過
  IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
  IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
  IP フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

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。

10.1.2.7 IDS 情報

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

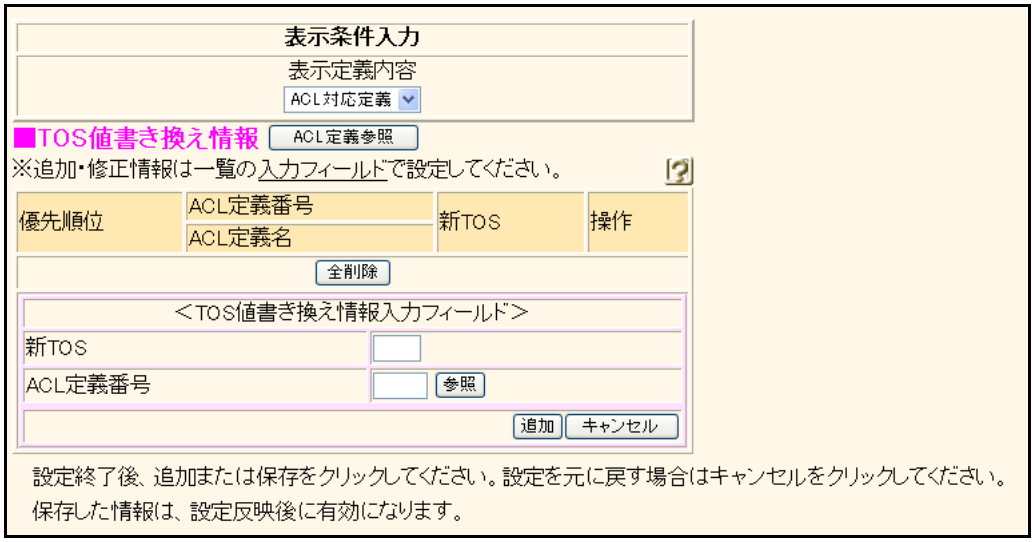


IDS 機能

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。

10.1.2.8 TOS 値書き換え情報

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



現在、設定されている TOS 値書き換え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。TOS 値書き換えの定義数は、32 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。

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

新 TOS

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

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

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

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

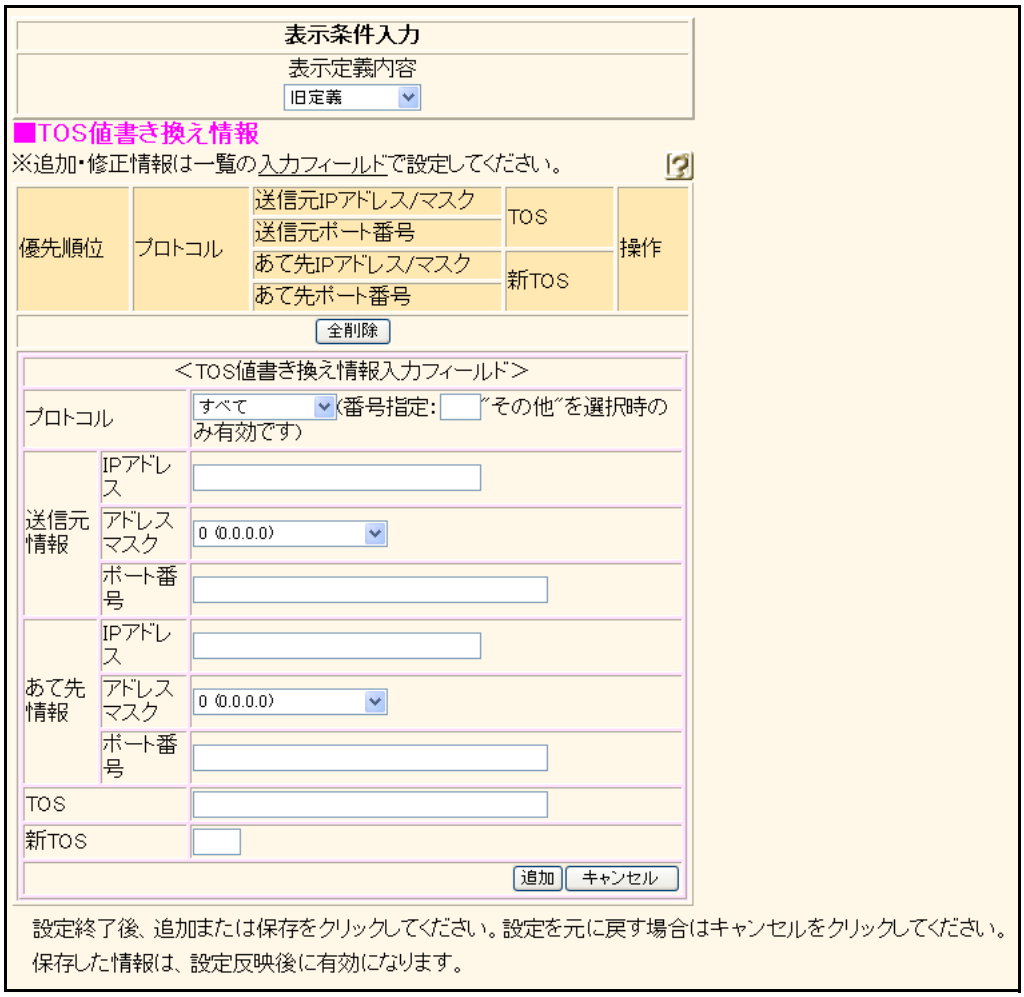
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

10.1.2.8.1 TOS値書き換え情報（旧定義）

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



表示条件入力に、“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

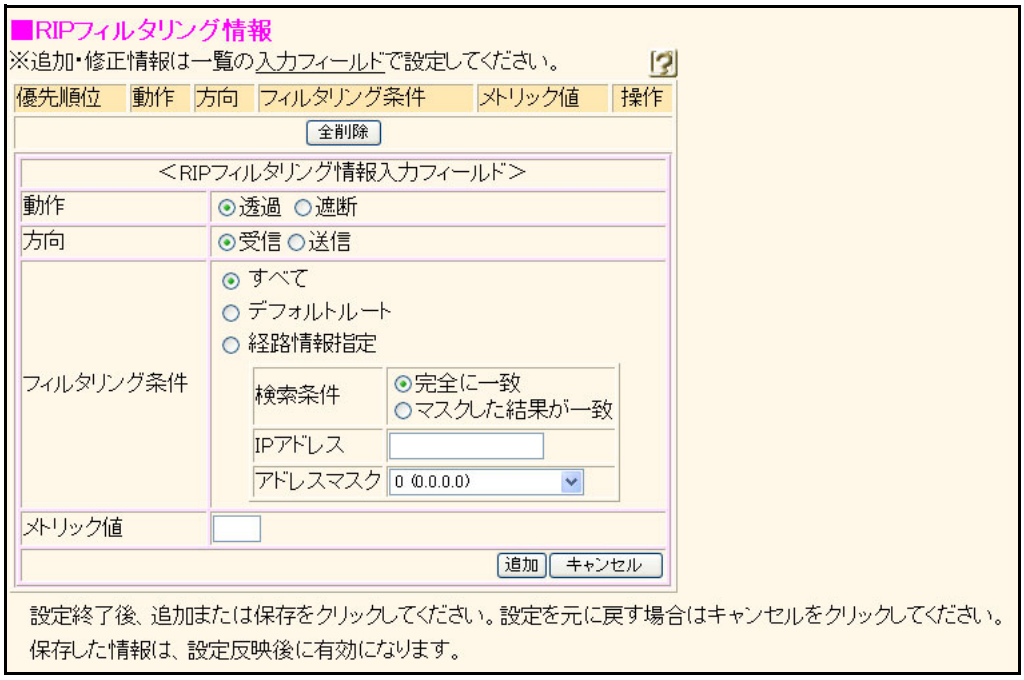
TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0 ～ ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、“,” で区切ります。範囲指定の場合は、“-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値が書き換えの対象となります。

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。

10.1.2.9 RIP フィルタリング情報

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



現在、設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、装置全体で 200 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。

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

検索条件

検索条件を選択します。

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

メトリック値

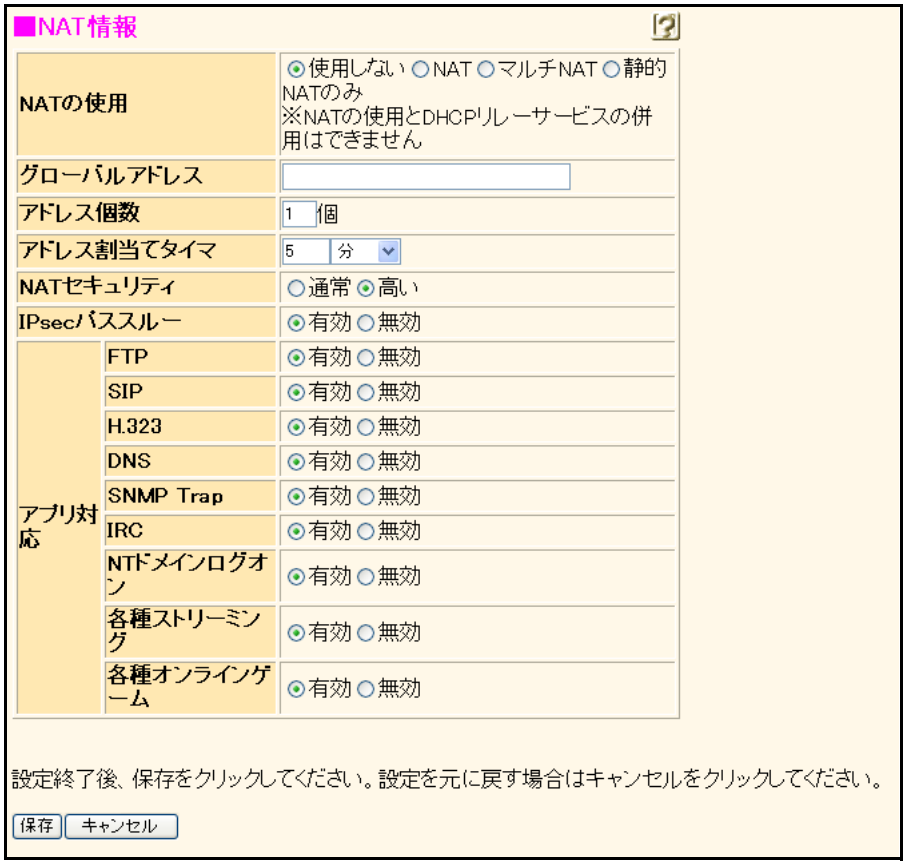
フィルタリング結果で透過になったRIP経路情報のメトリック値を変更ができます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

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

10.1.2.10 NAT情報

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



NAT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。

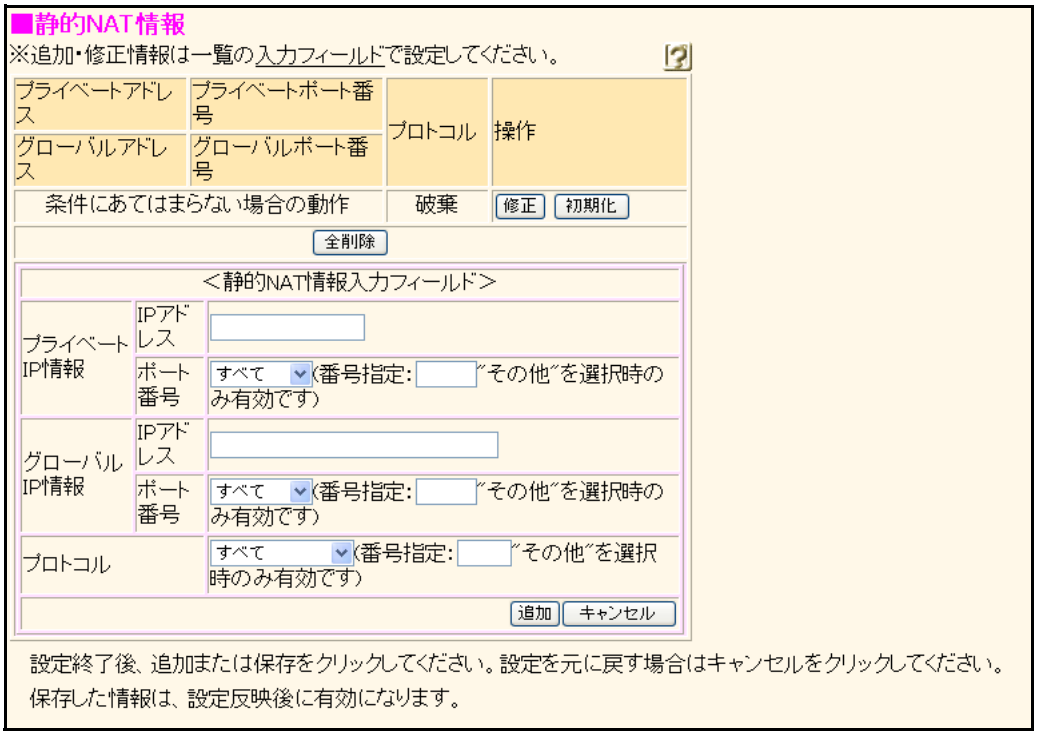
アプリ対応

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

10.1.2.11 静的 NAT 情報

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



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、装置全体で 64 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。

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

プライベート IP 情報

IP アドレス

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

ポート番号

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

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

例）プライベートポート番号：1000
　　グローバルポート番号：10000-11000
　　NAT 変換後
　　プライベートポート番号：1000-2000

グローバル IP 情報

IP アドレス

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

IP アドレスを指定する場合は、-" で区切った 1 組の範囲を指定します。

ポート番号

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

プロトコル

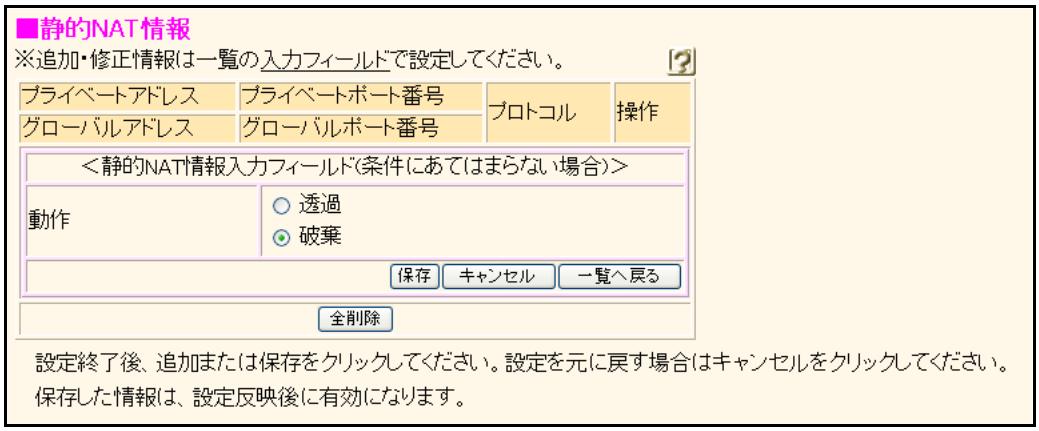
固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

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

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

10.1.2.11.1 静的NAT情報（条件にあてはまらない場合の動作）

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



「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。

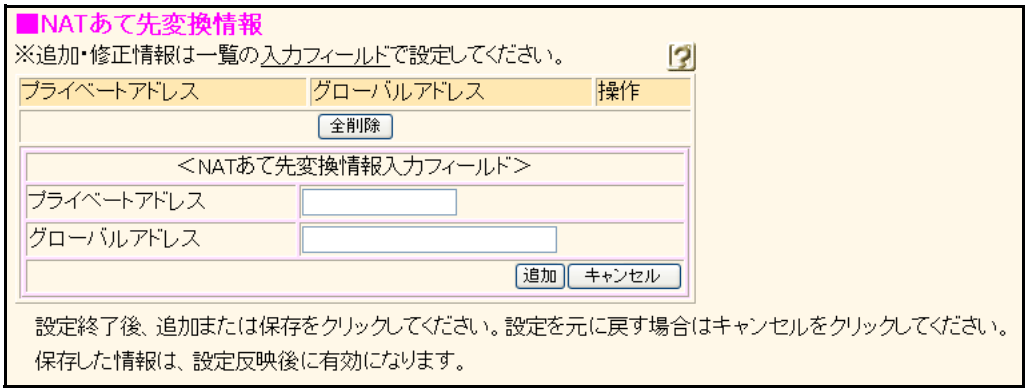
動作

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。

10.1.2.12 NAT あて先変換情報

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



現在、設定されている NAT あて先変換情報の定義が表示されています。NAT あて先変換の定義数は、装置全体で 64 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。

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。

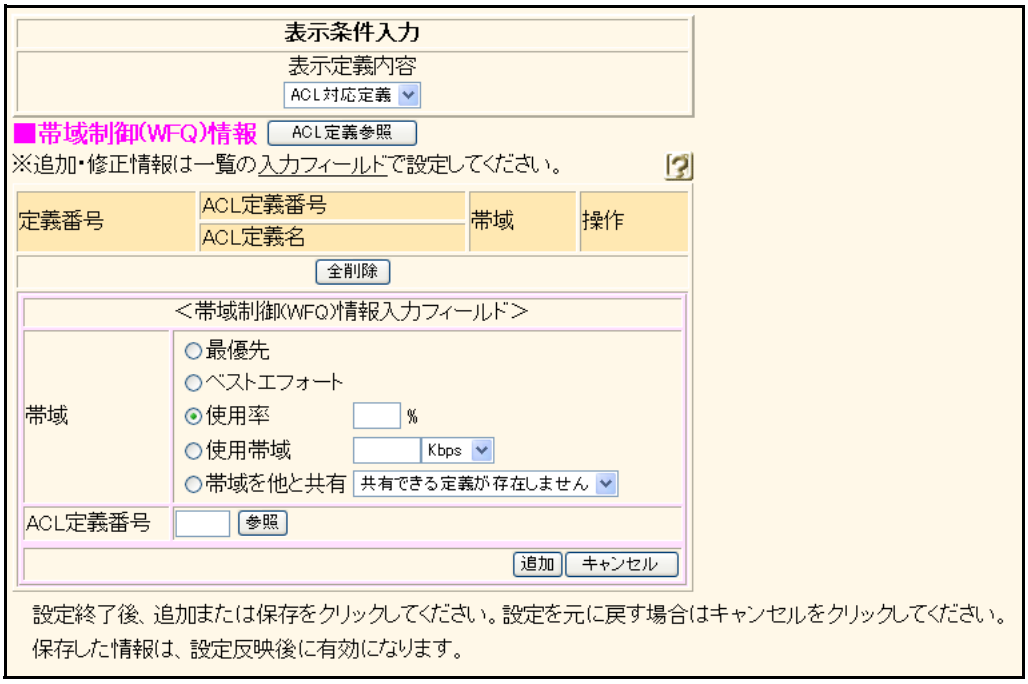
例）プライベートアドレス：192.168.1.100
　　グローバルアドレス：172.16.1.100-172.16.1.200
　　NAT あて先変換後
　　プライベートアドレス：192.168.1.100-192.168.1.200

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。

10.1.2.13 帯域制御（WFQ）情報

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



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、装置全体で 64 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。
設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

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

帯域

帯域の使用率または帯域値を指定します。

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

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

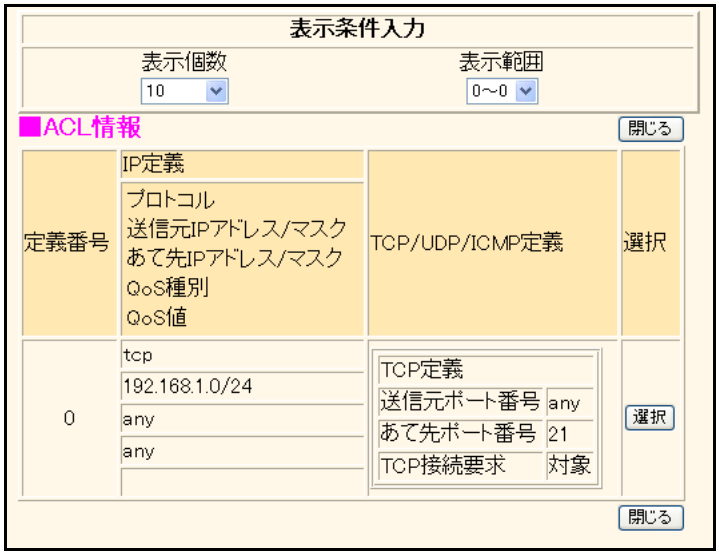
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

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



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

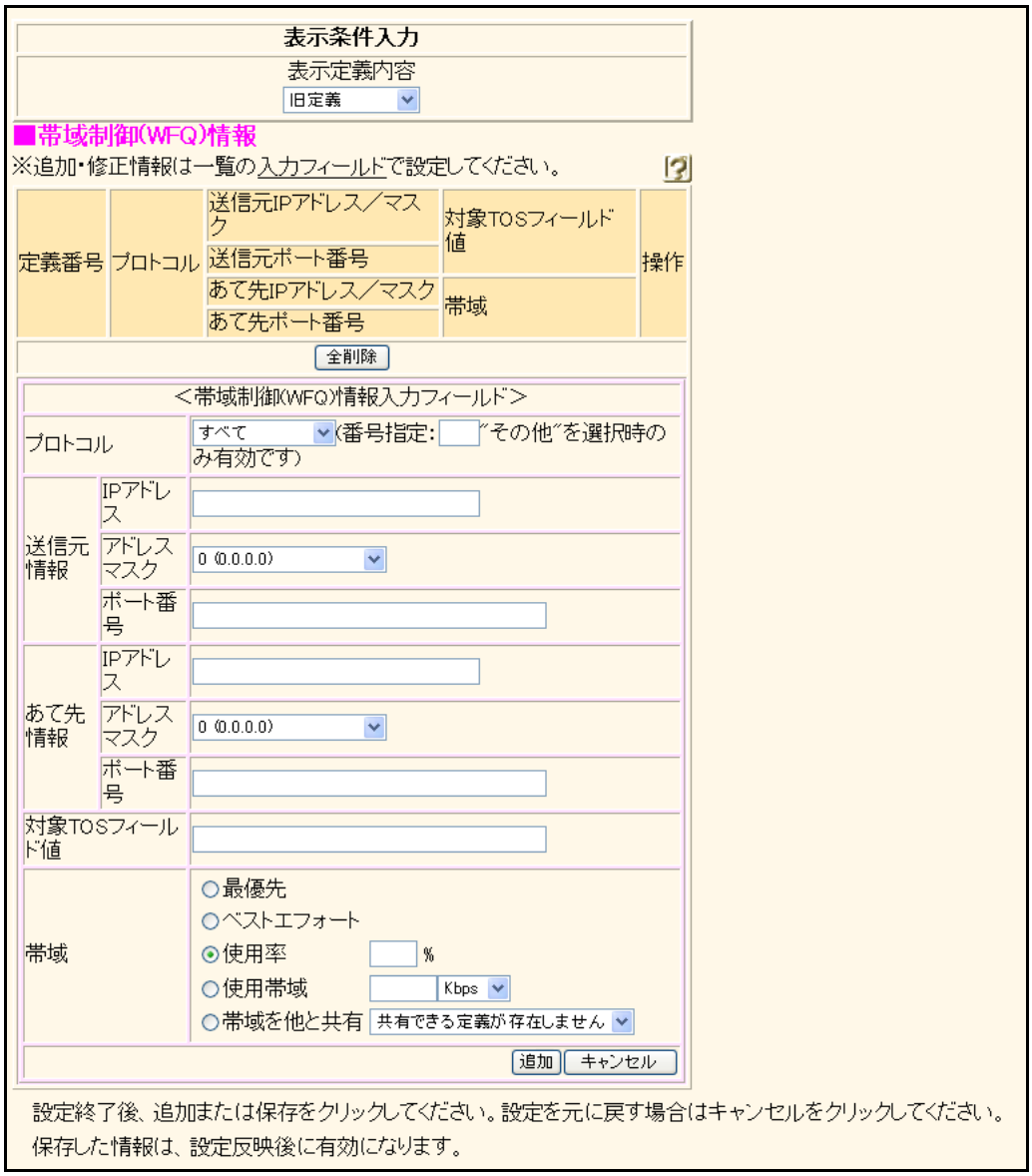
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

10.1.2.13.1 帯域制御（WFQ）情報（旧定義）

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



表示条件入力に、“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。

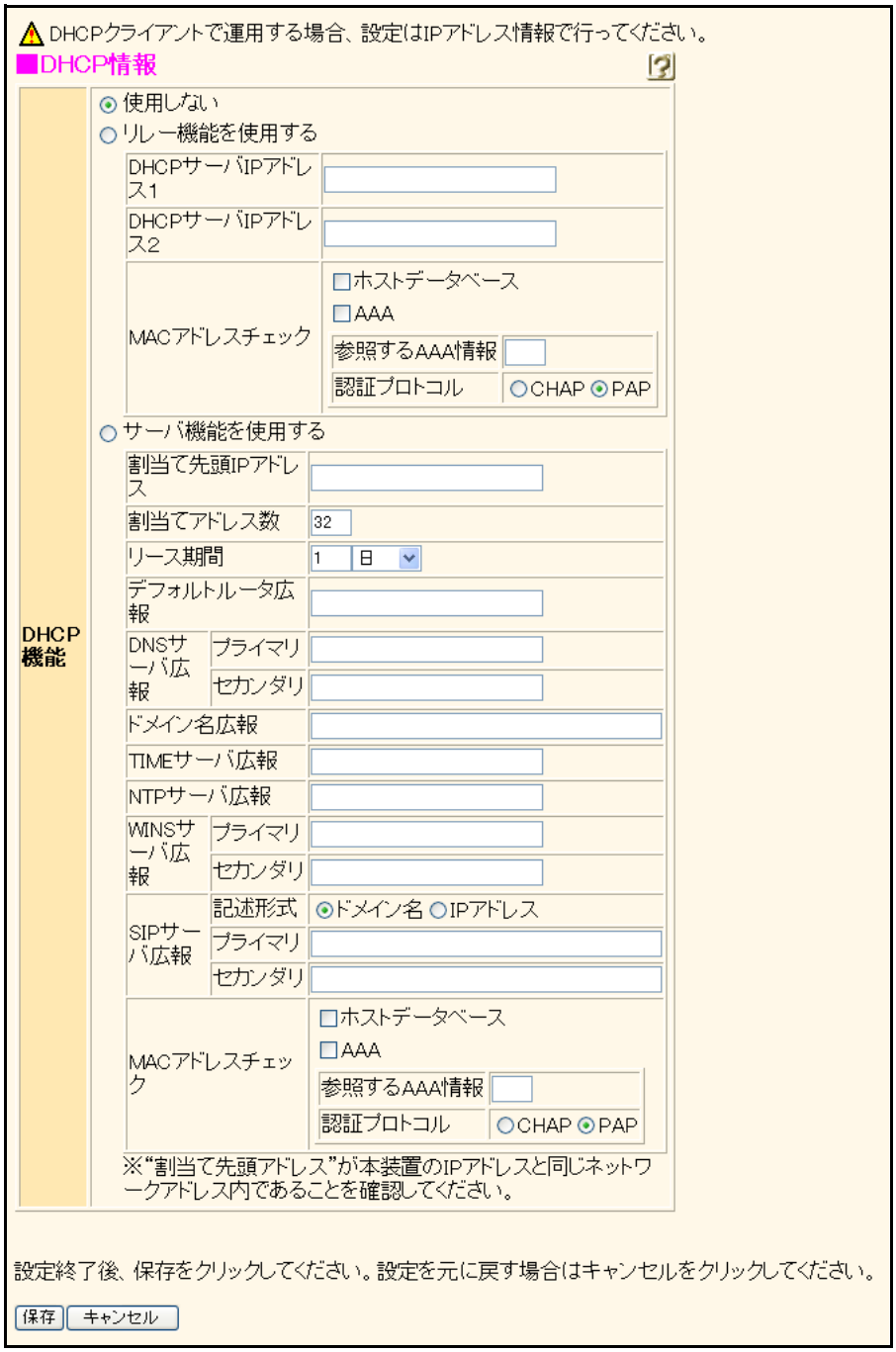
- 最優先
  最優先データとして扱われます。
- ベストエフォート
  非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
  割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
  1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
  ほ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

10.1.2.14 DHCP 情報

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



DHCP 機能

それぞれのインタフェースのDHCP機能を以下の3つから選択します。

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

割当て先頭 IP アドレス

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

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

割当てアドレス数

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

リース期間

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

デフォルトルータ広報

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

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

DNS サーバ広報

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

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

セカンダリ DNS サーバ広報

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

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

ドメイン名広報

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

TIME サーバ広報

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

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

NTP サーバ広報

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

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

WINS サーバ広報

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

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

SIP サーバ広報

ドメイン名を使用して SIP サーバを広報する場合は、記述形式の " ドメイン名 " を選択して 80 文字以内で指定します。なお、RFC1034 では英数字、"-"（ハイフン）、"."（ピリオド）でドメイン名をつけることを推奨しています。

また、IP アドレスを使用して SIP サーバを広報する場合は、記述形式の "IP アドレス " を選択して IP アドレスを指定します。ドメイン名と IP アドレスの混在指定はできません。プライマリ／セカンダリサーバ共に省略すると DHCP サーバによる広報を行いません。

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

MAC アドレスチェック

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

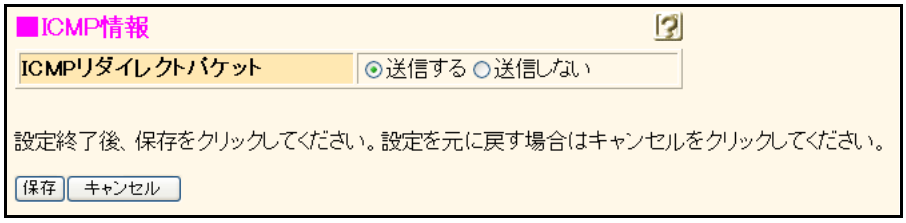
- ホストデータベース
  ホストデータベース情報を使用します。
- AAA
  AAA 情報を使用します。
  参照する AAA 情報のグループ ID を 10 未満の 10 進数で指定します。
  認証プロトコルを CHAP と PAP から選択します。

こんな事に気をつけて

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

10.1.2.15 ICMP 情報

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

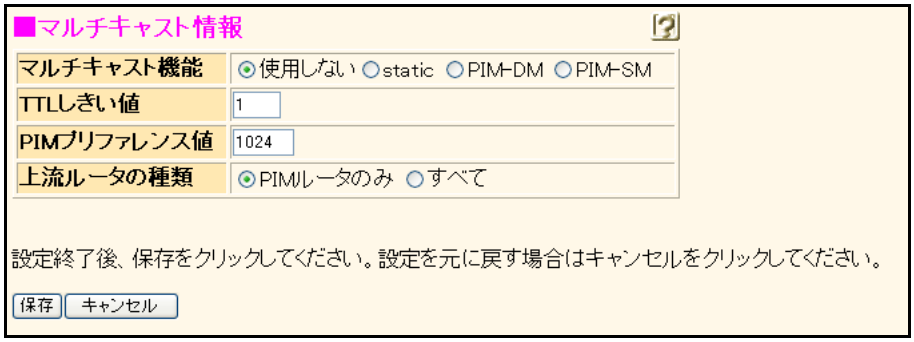


ICMP リダイレクトパケット

ICMP リダイレクトパケットを送信する場合は、" 送信する " を選択します。

10.1.2.16 マルチキャスト情報

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



マルチキャストを使用できるインタフェースの定義数は、装置全体で 20 個まで設定できます。

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。

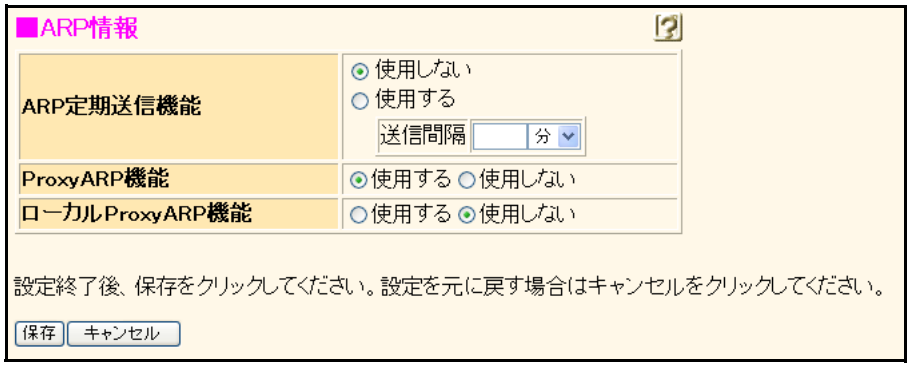
上流ルータが PIM ルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“ すべて ” を選択します。

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。

10.1.2.17 ARP 情報

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



ARP 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

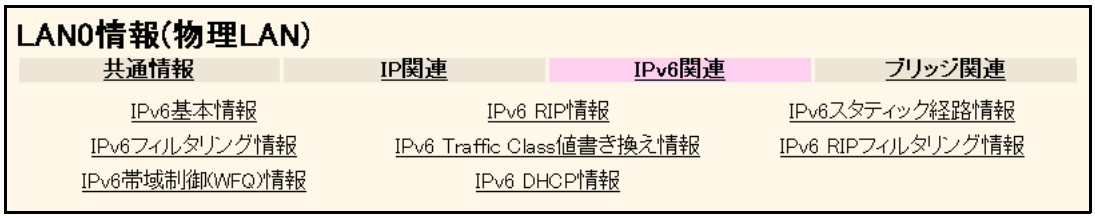
本装置を経由して到達できる IPv4 アドレスに対する ARP 要求に対し代理応答する機能です。代理応答させない場合は “ 使用しない ” を選択します。

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。

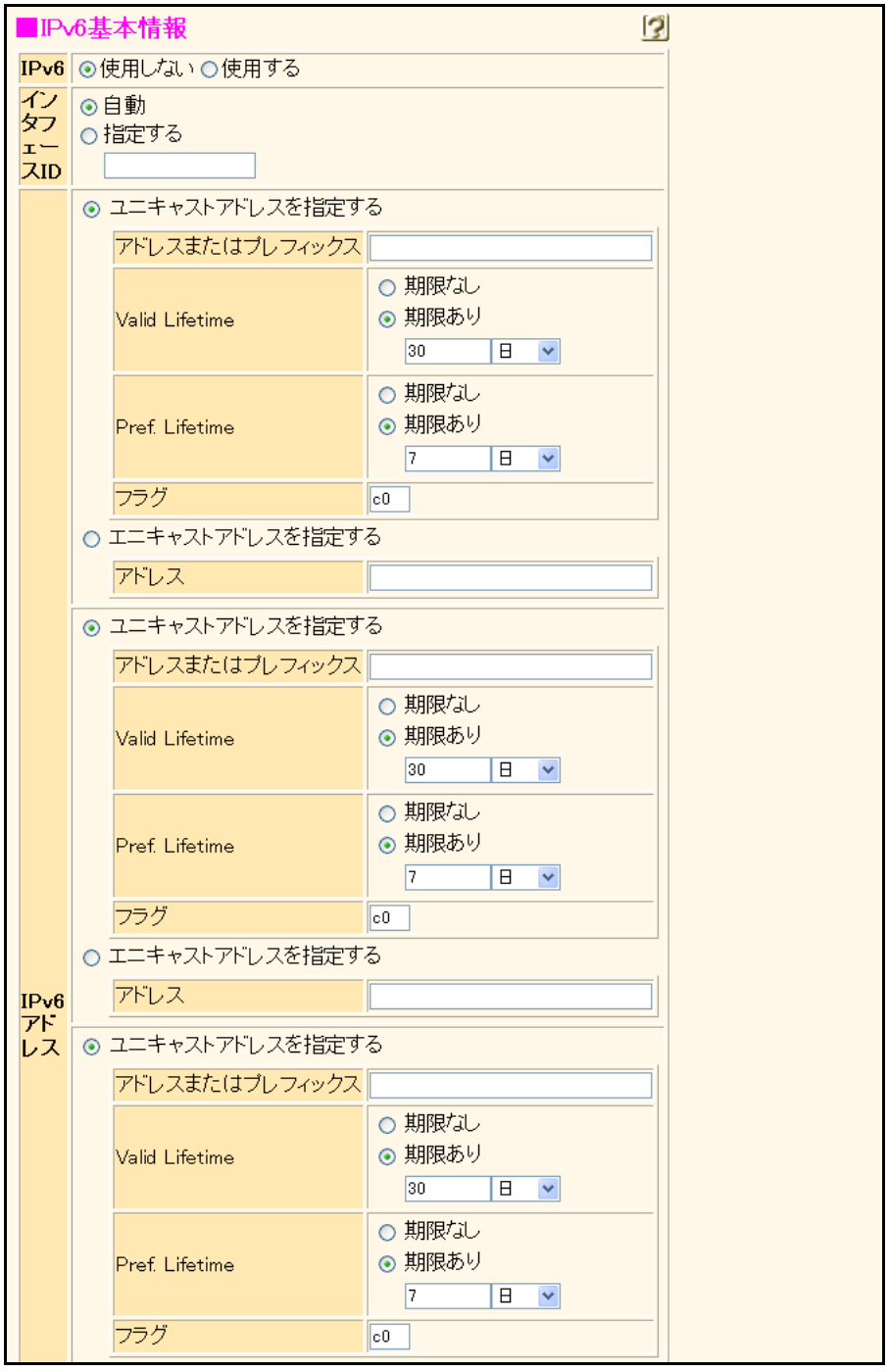
10.1.3 IPv6 関連

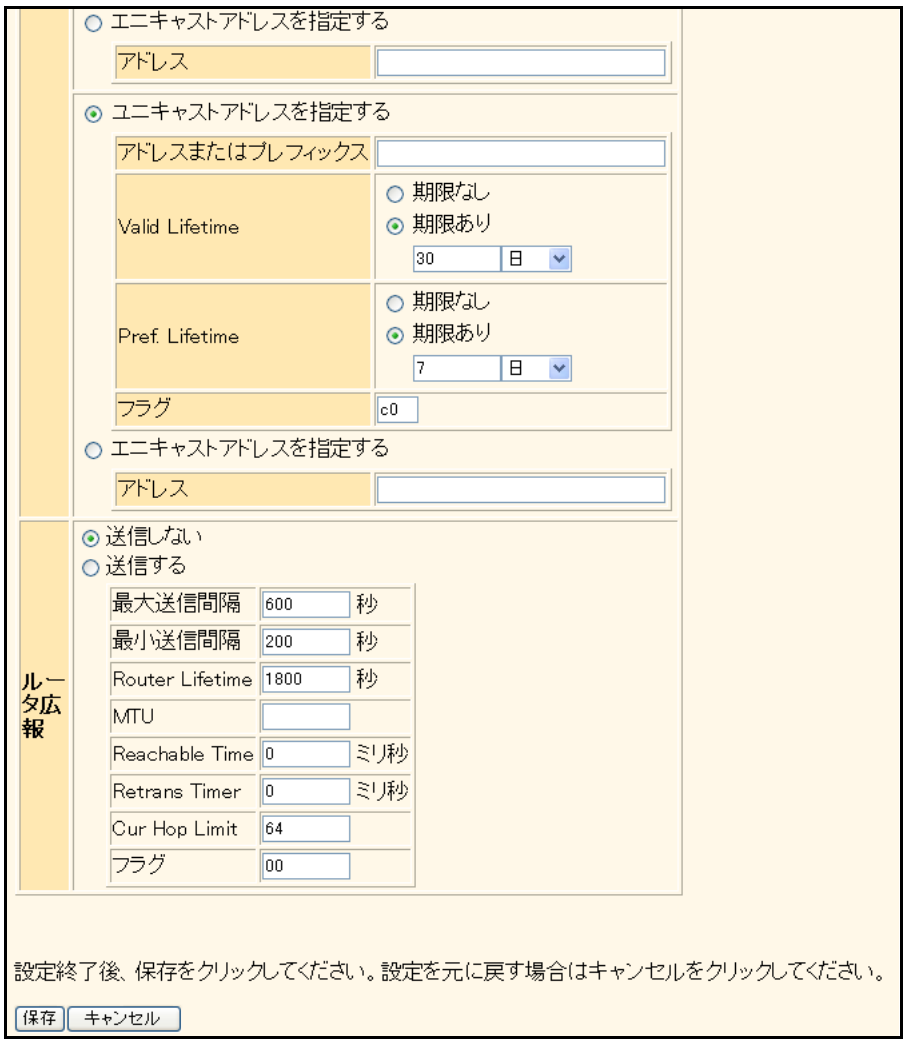
［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］



10.1.3.1 IPv6 基本情報

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





IPv6

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

インタフェース ID を設定します。

- 自動
  装置の MAC アドレスから自動生成されるインタフェース ID を使用します。通常は、“ 自動 ” を選択します。
- 指定する
  16 ビットごとに区切り文字（:）を入れて、16 進数を使用して 16 桁でインタフェース 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ユニキャストアドレスまたはエニキャストアドレスを 4 個まで設定できます。

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

アドレスまたはプレフィックス

本装置のLAN側のIPv6アドレスを標準的なIPv6アドレス表記方式で指定します。本装置ではプレフィックス長は64に固定されます。インタフェース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

IPv6アドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCPクライアントが取得したValid Lifetimeと比較して短い方が有効になります。

Pref. Lifetime

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

有効範囲）
0～365日
0～8760時間
0～525600分
0～31536000秒

IPv6アドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCPクライアントが取得したPreferred Lifetimeと比較して短い方が有効になります。

フラグ

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

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

通常は“c0”を指定します。

アドレス

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

ルータ広報

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

最大送信間隔

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

有効範囲）4～1800

最小送信間隔

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

有効範囲）3～最大送信間隔の3／4

Router Lifetime

ルータ広報で送信する Router Lifetime を指定します。初期値は 1800 秒です。省略はできません。

有効範囲）0 または最大送信間隔～9000

MTU

ルータ広報で送信する MTU option を指定します。省略時は、MTU option を含みません。

有効範囲）1280 ～ 1500

Reachable Time

ルータ広報で送信する Reachable Time を指定します。省略値は 0 ミリ秒です。

有効範囲）0 ～ 3600000

Retrans Timer

ルータ広報で送信する Retrans Timer を指定します。省略値は 0 ミリ秒です。

有効範囲）0 ～ 4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit を指定します。省略値は 64 です。

有効範囲）0 ～ 255

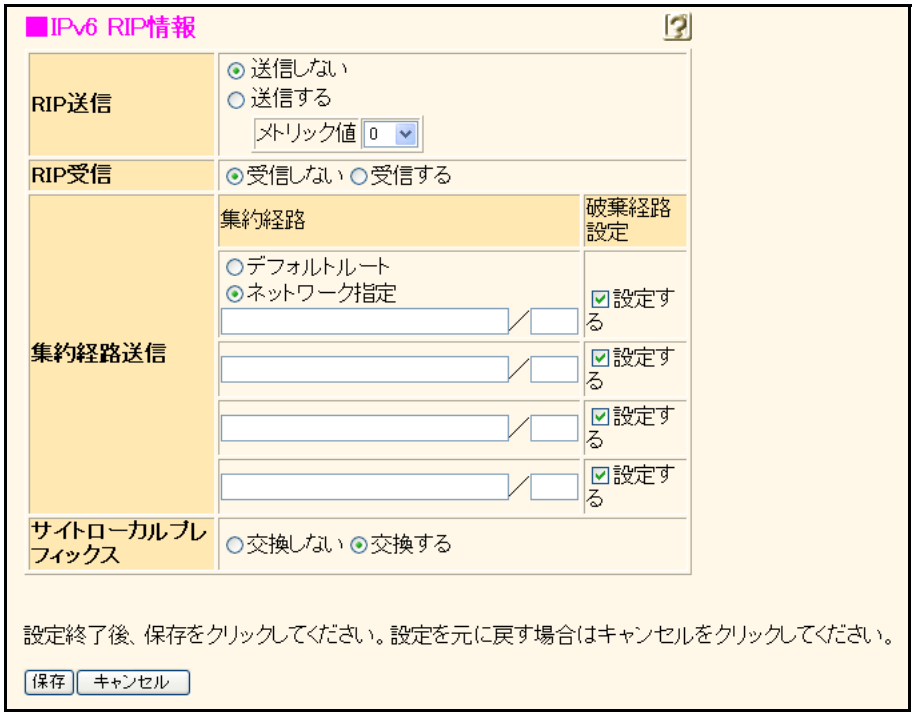
フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を 16 進数を使用して 2 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

10.1.3.2 IPv6 RIP 情報

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



RIP を使用できるインタフェースの定義数は、装置全体で 58 個まで設定できます。

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。

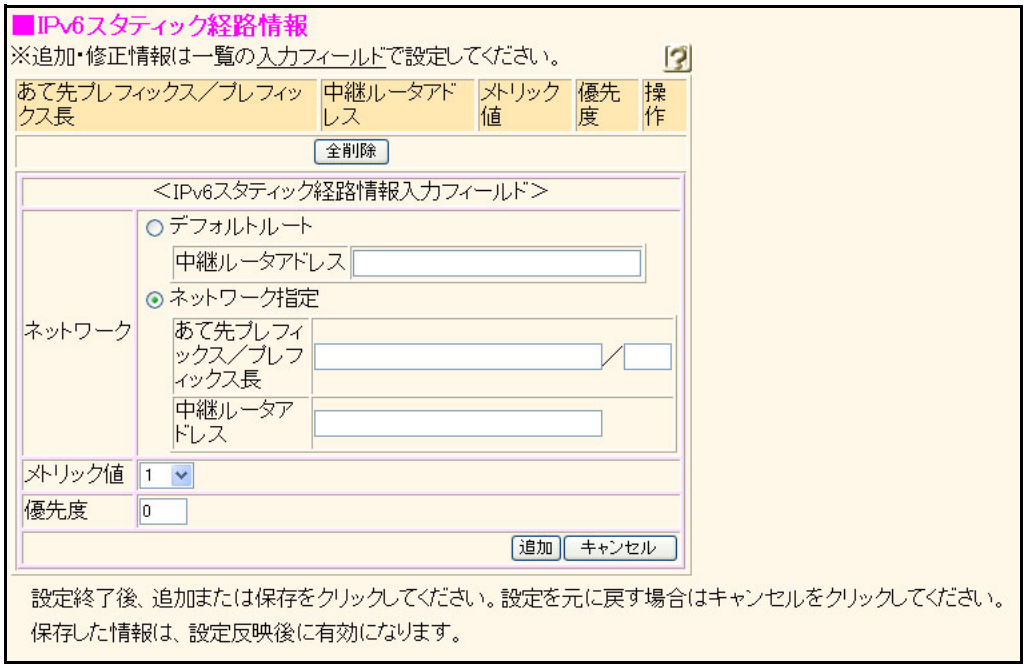
チェックしたときは、集約経路情報と同じあて先の経路情報が破棄経路としてルーティングテーブルが設定されます。

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。

10.1.3.3 IPv6スタティック経路情報

［操作］　ルータ設定「LAN情報（物理LAN）」→［修正］→［IPv6関連］→［IPv6スタティック経路情報］



現在、設定されているIPv6スタティック経路情報の定義が表示されています。IPv6スタティック経路の定義数は、装置全体で128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。

IPv6経路情報を固定で設定できます。ただし、デフォルトルートは装置に1つしか設定できません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。

- デフォルトルート
  中継ルータアドレスを指定します。
- ネットワーク指定
  あて先プレフィックス／プレフィックス長、中継ルータアドレスを指定します。
  あて先プレフィックスにリンクローカルアドレスは指定できません。ICMPv6 Redirectを正常に動作させるためには、中継ルータアドレスはリンクローカルアドレスで指定する必要があります。
  なお、あて先プレフィックス／プレフィックス長に::/0を設定した場合、“デフォルトルート”を指定したものとして動作します。

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

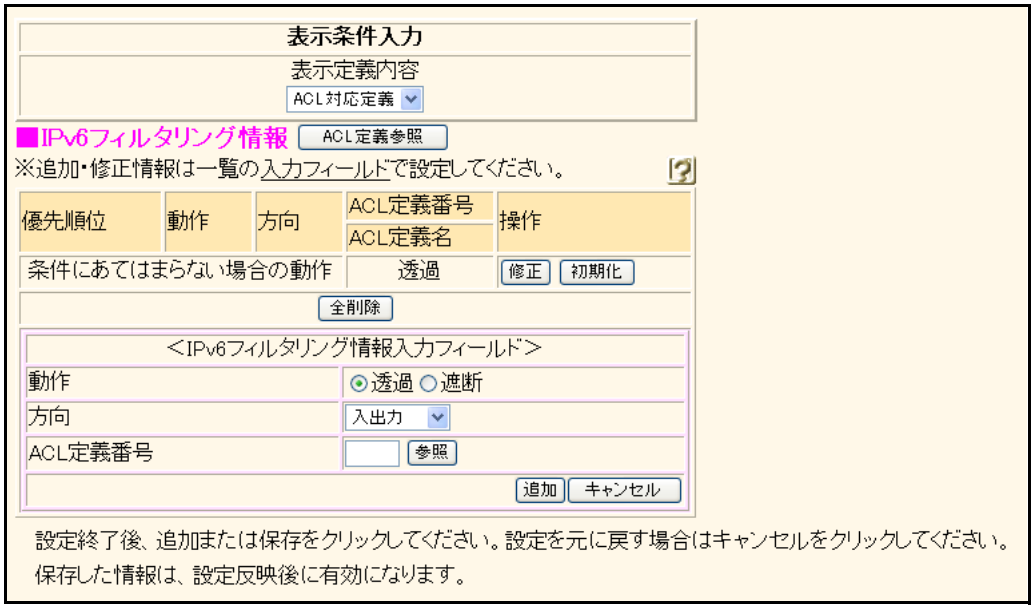
こんな事に気をつけて

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。**

10.1.3.4 IPv6 フィルタリング情報

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 フィルタリング情報］



現在、設定されている IPv6 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。IPv6 フィルタリングの定義数は、64 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。

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

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

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

動作

IPv6 フィルタリングの動作を以下の 2 つから選択します。

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

方向

フィルタリングする方向を選択します。

- 入力のみ
  入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
  出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
  - 送信元IPv6アドレス／プレフィックス長とあて先IPv6アドレス／プレフィックス長
  - 送信元ポート番号とあて先ポート番号

  リバースを指定した場合、入力パケットはIPv6アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

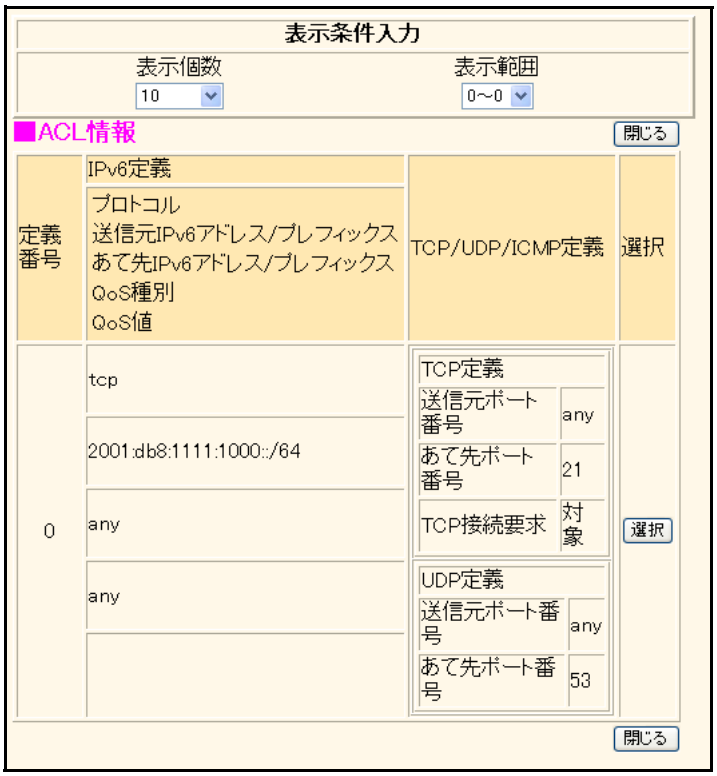
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 フィルタリング情報］→「ACL 定義番号の［参照］」



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

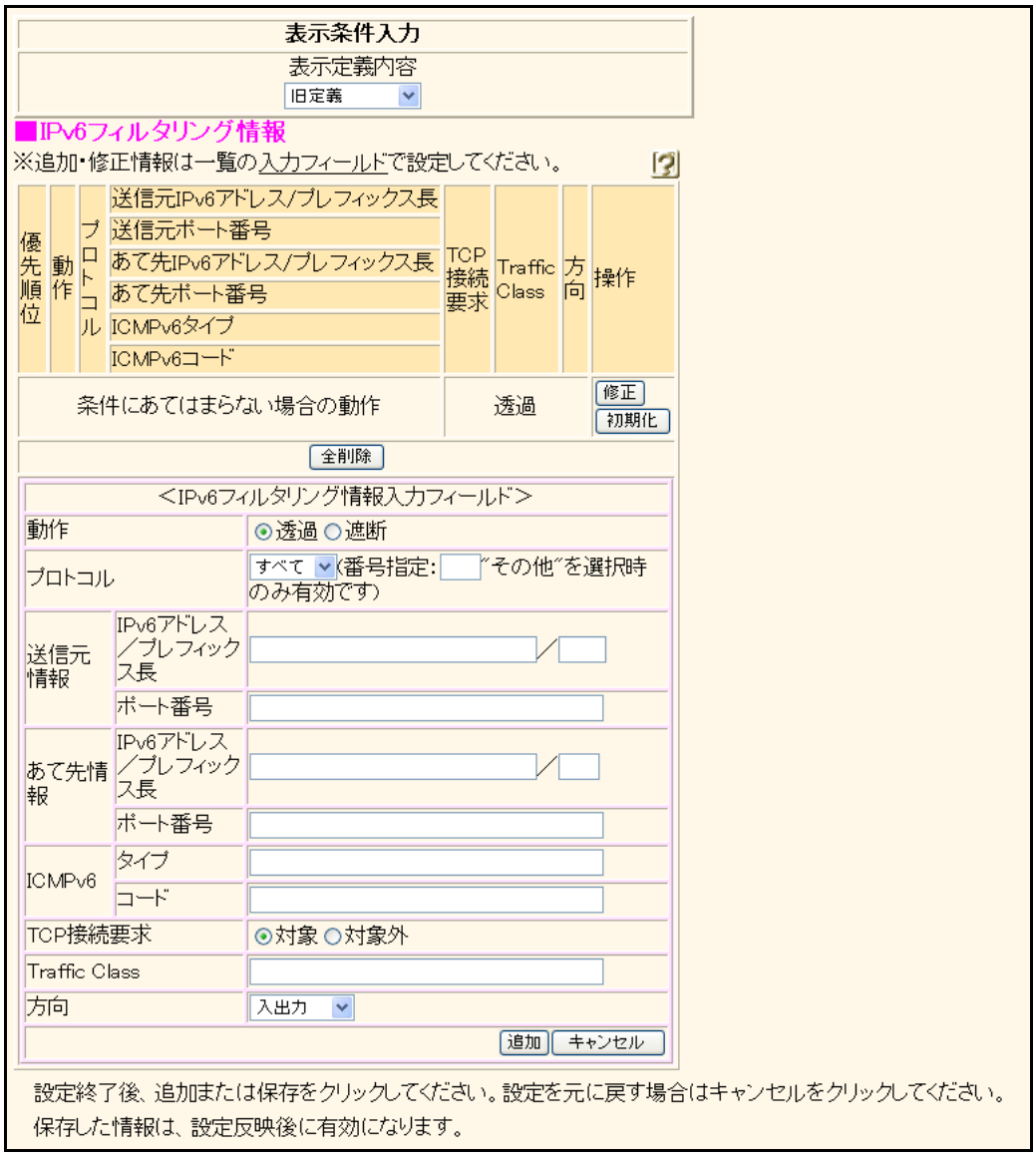
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 フィルタリング情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

10.1.3.4.1 IPv6 フィルタリング情報（旧定義）

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 フィルタリング情報］→「表示条件入力（旧定義）」



表示条件入力に、“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

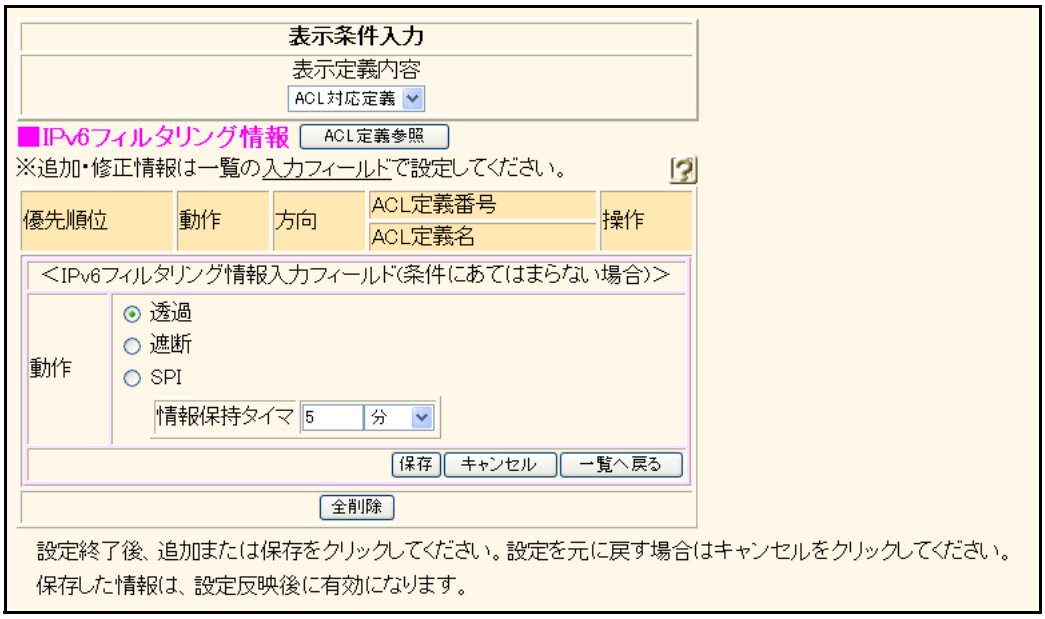
フィルタリングする方向を選択します。

- 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。

10.1.3.4.2 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］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 フィルタリング情報］→「条件にあてはまらない場合の動作」［修正］



「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。

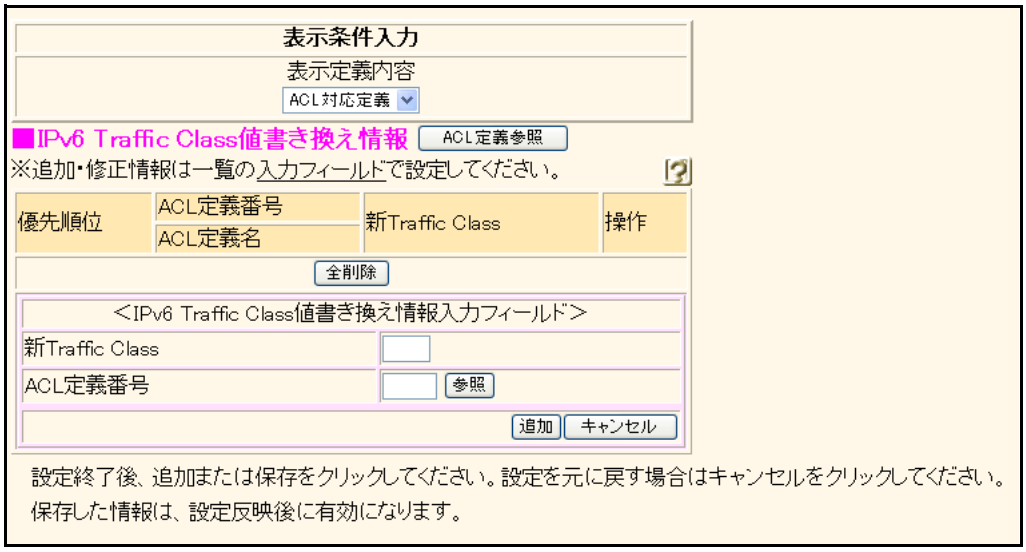
- 透過
  IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
  IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
  IPv6 フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

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。

10.1.3.5 IPv6 Traffic Class 値書き換え情報

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］
→［IPv6 Traffic Class 値書き換え情報］



現在、設定されている IPv6 Traffic Class 値書き換え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 Traffic Class 値書き換えの定義数は、32 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。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 Traffic Class

IPv6 パケットに新しく指定する IPv6 Traffic Class 値を 16 進数を使用して、0 ～ ff の範囲で指定します。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

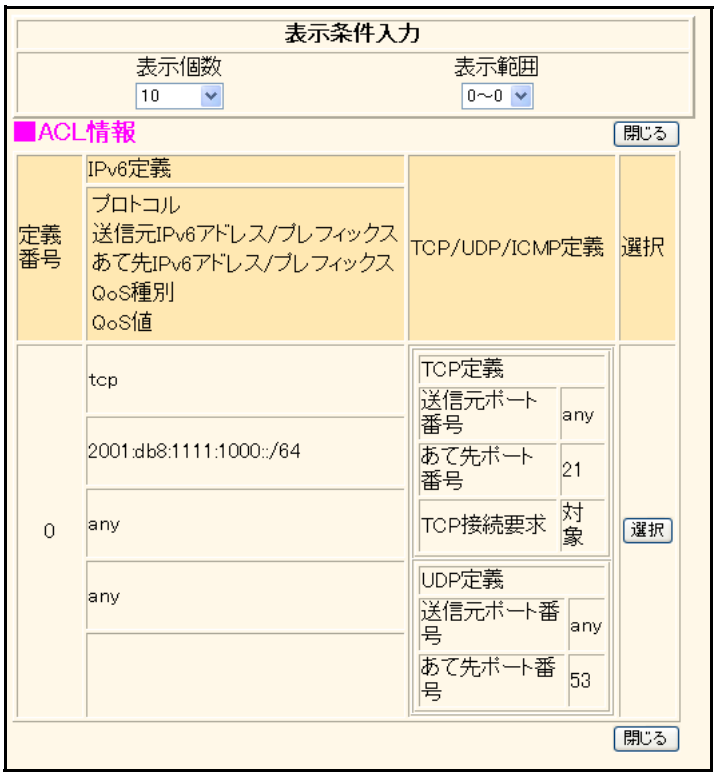
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］
→［IPv6 Traffic Class 値書き換え情報］→「ACL 定義番号の［参照］」



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

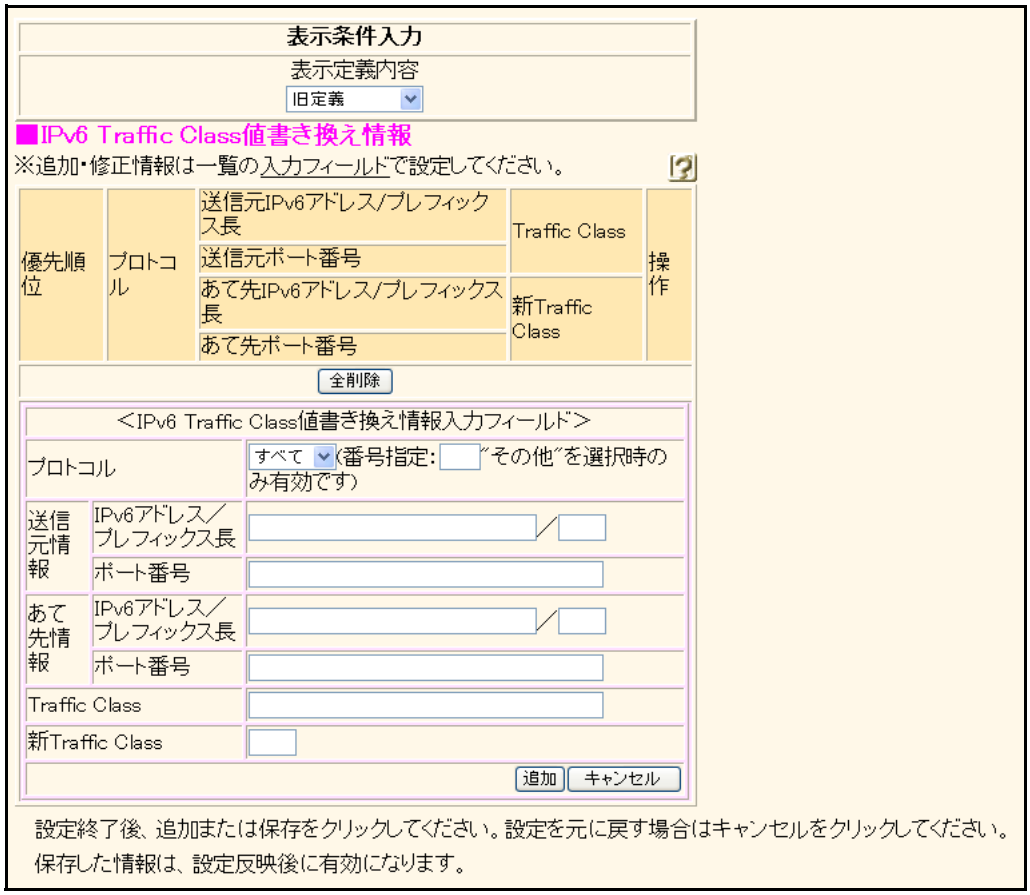
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 Traffic Class 値書き換え情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 Traffic Class 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

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

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］
→［IPv6 Traffic Class 値書き換え情報］→「表示条件入力（旧定義）」



表示条件入力に、“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

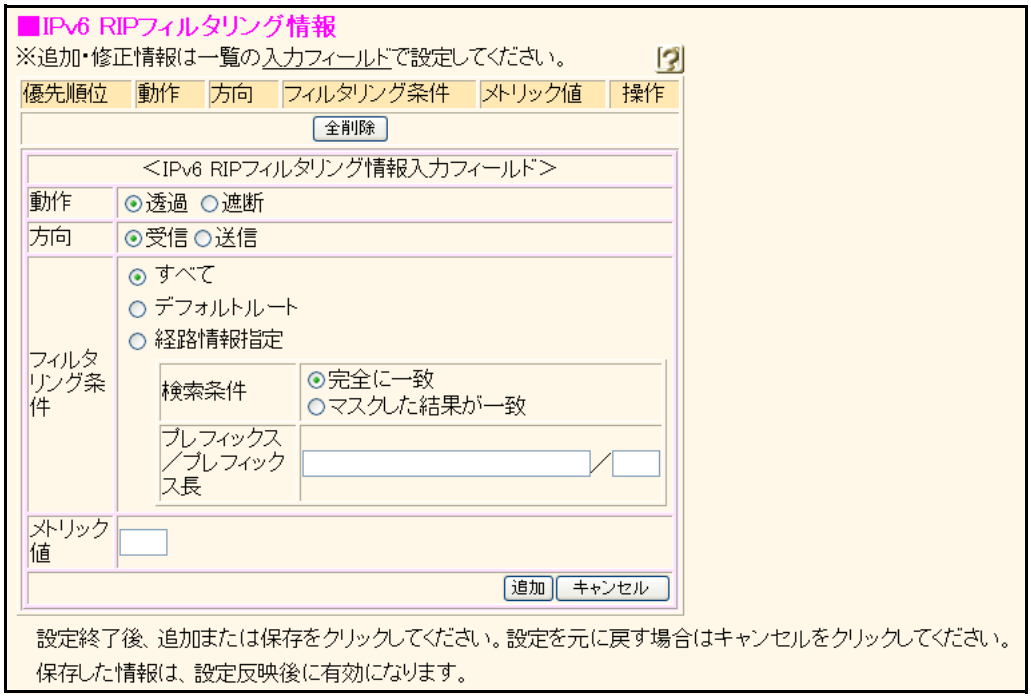
IPv6 Traffic Class 値書き換え条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0 ～ ff の範囲または “any” で指定します。Traffic Class フィールド値を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての IPv6 Traffic Class 値が書き換えの対象となります。

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。

10.1.3.6 IPv6 RIP フィルタリング情報

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 RIP フィルタリング情報］



現在、設定されている RIP フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、装置全体で 200 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。

RIP 受信（送信）時には、優先順位の高い定義から順に受信（送信）方向の条件を参照し、一致した条件があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、受信（送信）方向のすべての条件に一致しない RIP 経路情報は遮断されます。

動作

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

- 透過
  条件と一致した場合に RIP 経路情報を透過します。
- 遮断
  条件と一致した場合に RIP 経路情報を遮断します。

方向

フィルタリングを RIP 受信時に行うか、RIP 送信時に行うかを選択します。

- 受信
  RIP 受信時に、フィルタリングを行います。
- 送信
  RIP 送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を選択します。

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

検索条件

検索条件を選択します。

- 完全に一致
  指定したプレフィックスとプレフィックス長が完全に一致した RIP 経路情報をフィルタリング対象とします。
- マスクした結果が一致
  指定したプレフィックスと、RIP 経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その RIP 経路情報をフィルタリング対象とします。

メトリック値

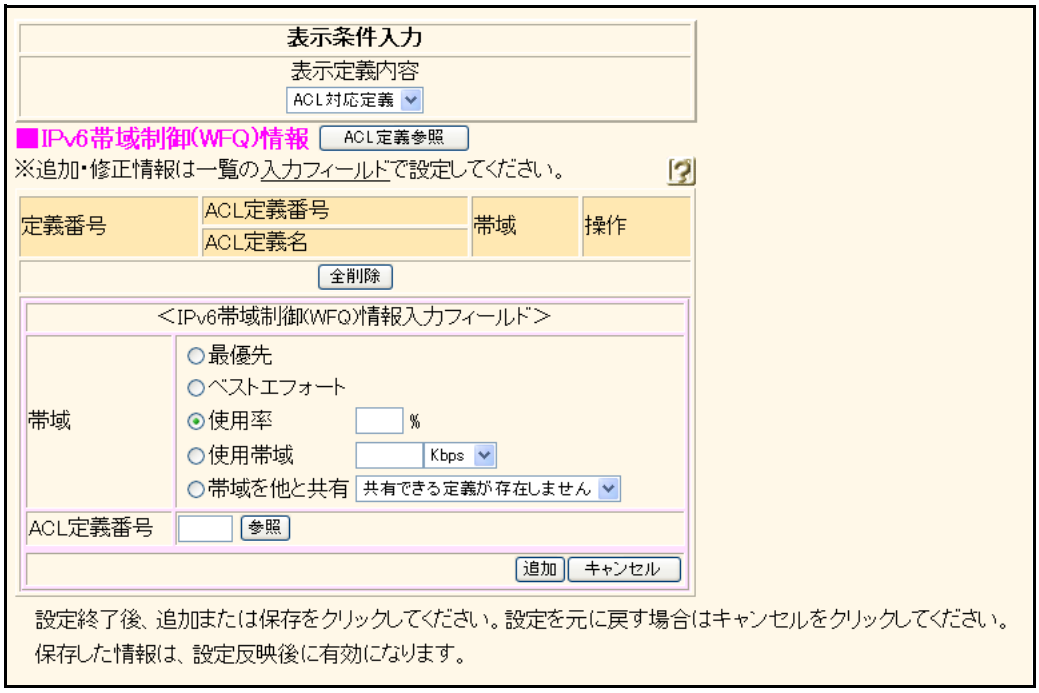
フィルタリング結果で透過になった RIP 経路情報のメトリック値を変更できます。送信時の RIP 経路にメトリック値を設定した場合、「RIP 情報」で設定した加算メトリック値は加算されません。省略または 0 を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

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

10.1.3.7 IPv6 帯域制御（WFQ）情報

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



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、64 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。

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

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

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

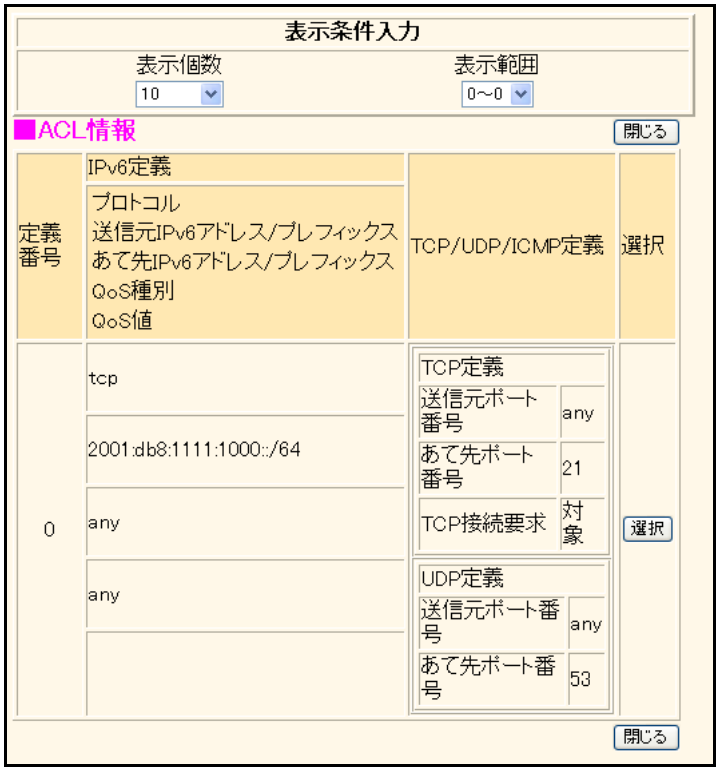
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 帯域制御（WFQ）情報］→「ACL 定義番号の［参照］」



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

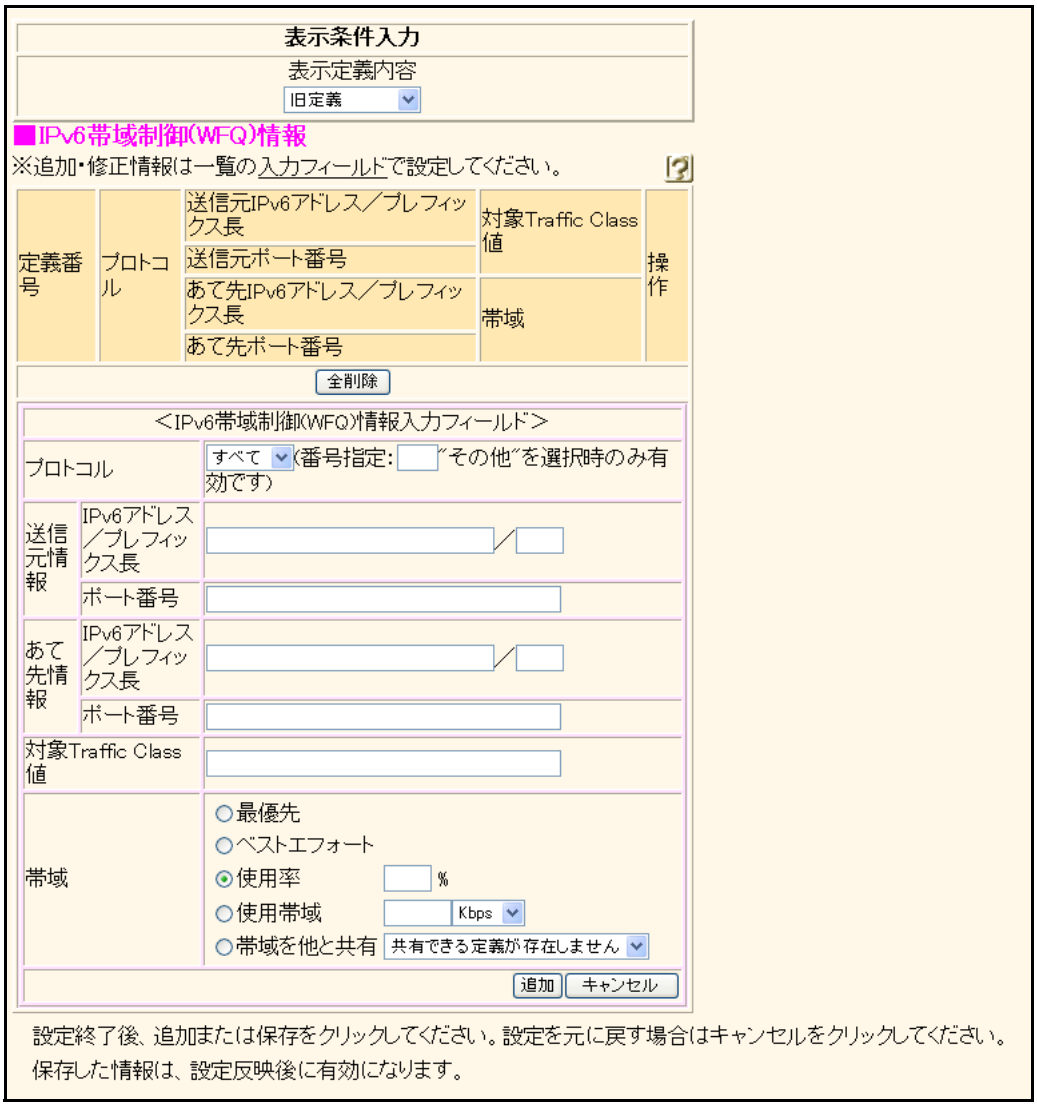
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 帯域制御（WFQ）情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 帯域制御（WFQ）情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

10.1.3.7.1 IPv6 帯域制御（WFQ）情報（旧定義）

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［IPv6 関連］→［IPv6 帯域制御（WFQ）情報］→「表示条件入力（旧定義）」



表示条件入力に、“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。

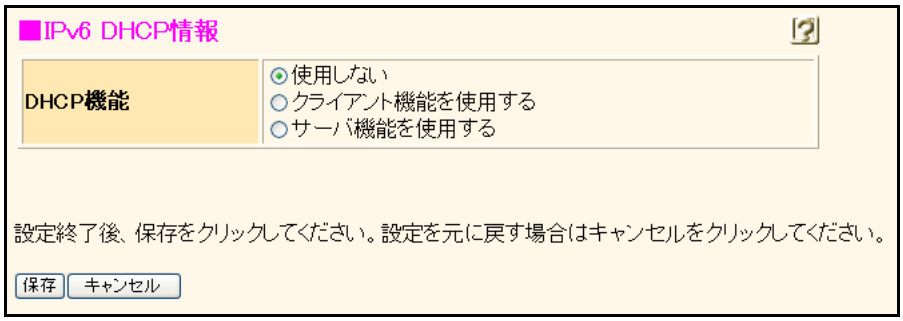
こんな事に気をつけて

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。

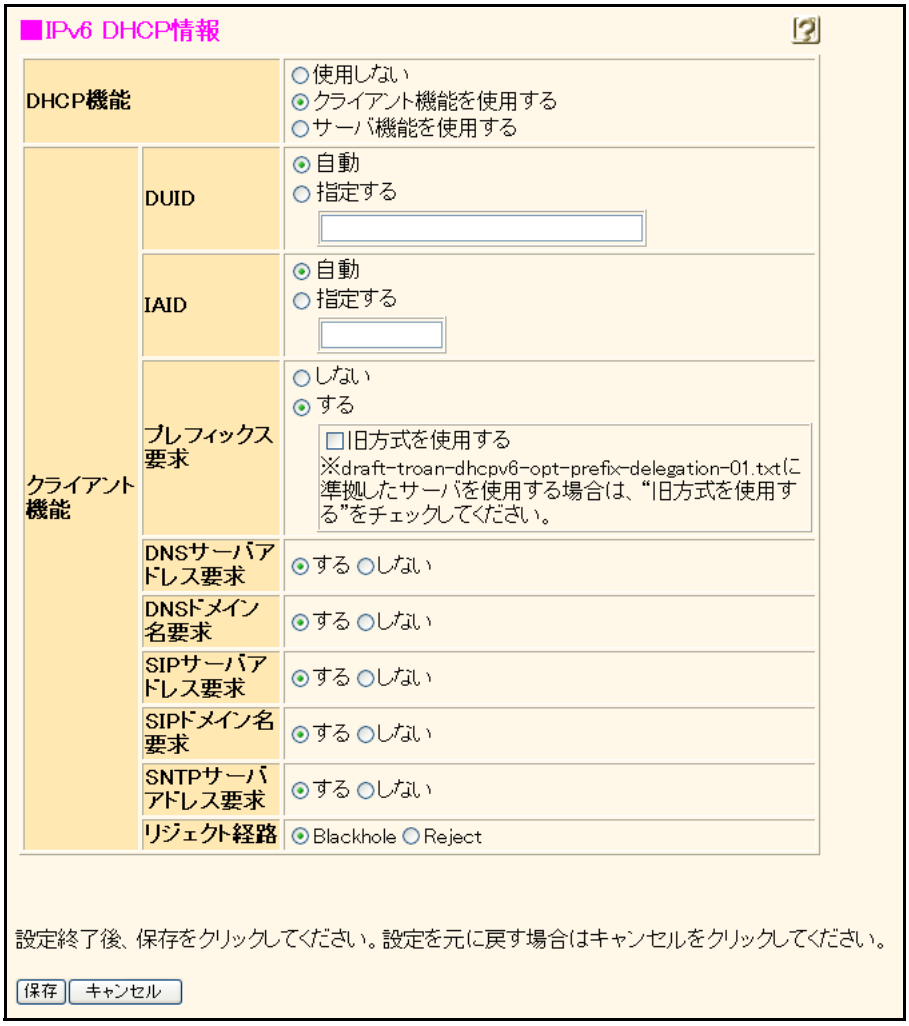
10.1.3.8 IPv6 DHCP 情報

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

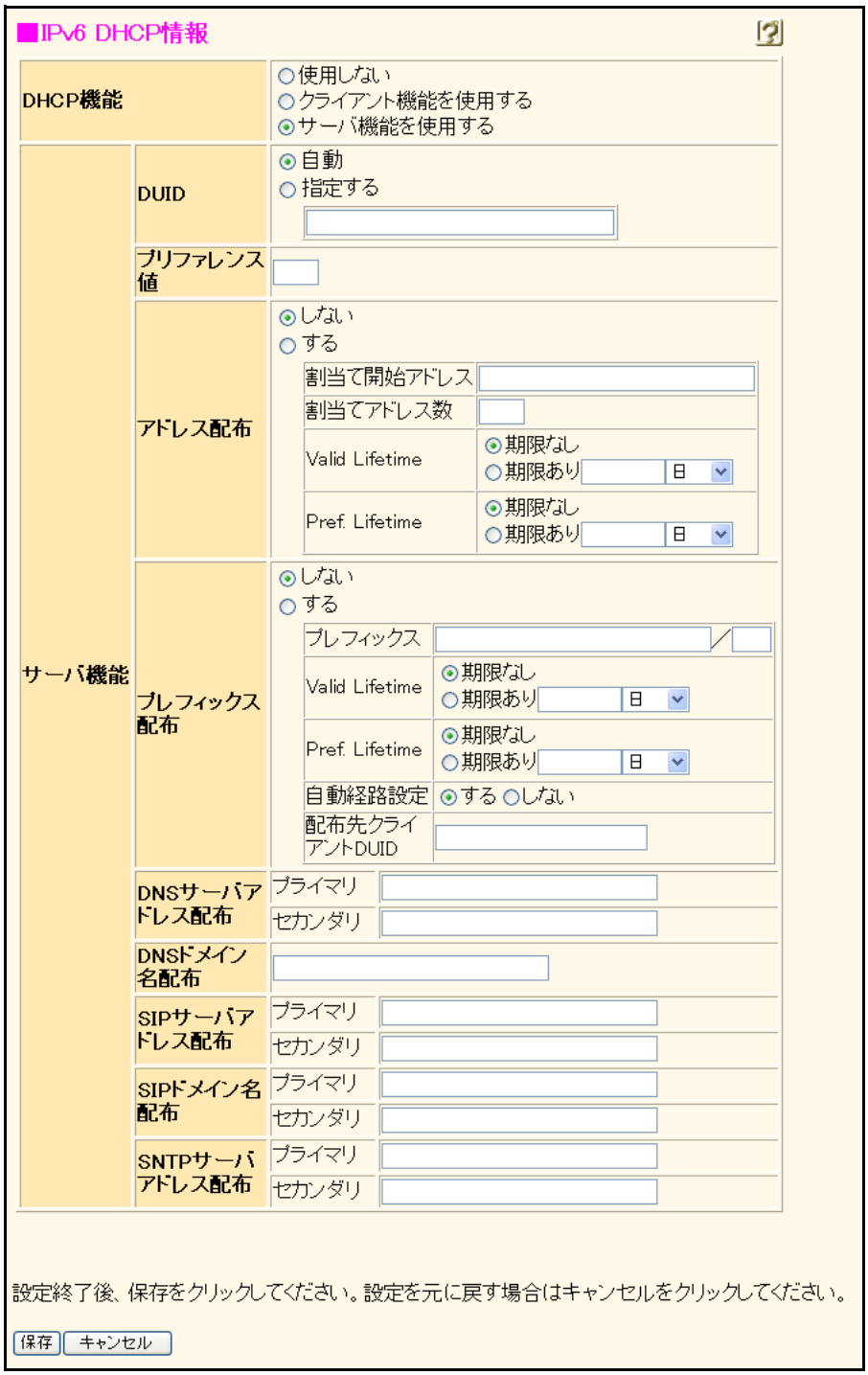
DHCP 機能で、“ 使用しない ” を選択した場合



DHCP 機能で、“ クライアント機能を使用する ” を選択した場合



DHCP 機能で、“ サーバ機能を使用する ” を選択した場合



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
  IPv6 DHCP 機能を使用しません。
- クライアント機能を使用する
  本装置を該当インタフェースの IPv6 DHCP クライアントとして使用します。
- サーバ機能を使用する
  本装置を該当インタフェースのネットワークの IPv6 DHCP サーバとして使用します。

クライアント機能

本装置を該当インタフェースの IPv6 DHCP クライアントとして使用する場合に設定します。

DUID

DUID を以下の 2 つから選択します。

- 自動
  DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
  260 桁以内の 16 進数で表記した DUID を指定します。

IAID

IAID を以下の 2 つから選択します。

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

プレフィックス要求

DHCP サーバにプレフィックスを要求するかどうかを設定します。DHCP サーバにプレフィックスを要求する場合は、“ する ” を選択します。“ する ” を選択した場合に、draft-troan-dhcpv6-opt-prefix-delegation-01.txt に準拠したサーバを利用するときは、“ 旧方式を使用する ” をチェックします。

DNS サーバアドレス要求

DHCP サーバに DNS サーバアドレスを要求するかどうかを設定します。DHCP サーバに DNS サーバアドレスを要求する場合は、“ する ” を選択します。

DNS ドメイン名要求

DHCP サーバに DNS ドメイン名を要求するかどうかを設定します。DHCP サーバに DNS ドメイン名を要求する場合は、“ する ” を選択します。

SIP サーバアドレス要求

DHCP サーバに SIP サーバアドレスを要求するかどうかを設定します。DHCP サーバに SIP サーバアドレスを要求する場合は、“ する ” を選択します。

SIP ドメイン名要求

DHCP サーバに SIP ドメイン名を要求するかどうかを設定します。DHCP サーバに SIP ドメイン名を要求する場合は、“ する ” を選択します。

SNTP サーバアドレス要求

DHCP サーバに SNTP サーバアドレスを要求するかどうかを設定します。DHCP サーバに SNTP サーバアドレスを要求する場合は、“ する ” を選択します。

リジェクト経路

DHCP サーバから取得したプレフィックスのリジェクト経路を以下の 2 つから選択します。

- Blackhole
  リジェクト経路あてのパケットを受信しても送信元にエラーを報告しません。
- Reject
  リジェクト経路あてのパケットを受信した場合、送信元にエラーを報告します。

サーバ機能

本装置を該当インタフェースのネットワークの IPv6 DHCP サーバとして使用する場合に設定します。

DUID

- 自動
  DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
  260 桁以内の 16 進数で表記した DUID を指定します。

プリファレンス値

DHCP サーバのプリファレンス値を 0 ～ 255 の範囲の 10 進数で指定します。DHCP クライアントはこの値が大きい DHCP サーバを選択します。省略時は 0 が設定されます。

アドレス配布

DHCP クライアントに割り当てる IPv6 アドレスを設定します。クライアントに IPv6 アドレスを割り当てる場合は、“ する ” を選択し、以降の項目を設定します。

“ しない ” を選択した場合、ホストデータベース設定による静的なアドレス割り当てだけが行われます。

割当て開始アドレス
クライアントに割り当てる連続した IPv6 アドレス群の先頭の IPv6 アドレスを指定します。

有効範囲）
::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

割当てアドレス数
クライアントに割り当てる IPv6 アドレス数を 0 ～ 300 の範囲で指定します。ホストデータベース機能を使用すると特定の IPv6 DHCP クライアントに対して固有の IPv6 アドレスを割り当てることができます。この場合の IPv6 アドレスは、割り当て開始 IPv6 アドレスと割り当てアドレス数によって規定される動的割り当て範囲である必要はありません。

こんな事に気をつけて

割り当てアドレスとして IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は、上位を “dhcp@ インタフェース名 ” 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インタフェースを指定してください。

Valid Lifetime
割り当てる IPv6 アドレスの Valid Lifetime を指定します。

有効範囲）
0 ～ 365 日
0 ～ 8760 時間
0 ～ 525600 分
0 ～ 31536000 秒

Pref. Lifetime
割り当てる IPv6 アドレスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲）
0 ～ 365 日
0 ～ 8760 時間
0 ～ 525600 分
0 ～ 31536000 秒

プレフィックス配布

DHCP クライアントに割り当てるプレフィックスを設定します。クライアントにプレフィックスを割り当てる場合は、“ する ” を選択し、以降の項目を設定します。

プレフィックス
クライアントに割り当てるプレフィックスとプレフィックス長を設定します。プレフィックス長は 48 ～ 64 の範囲で指定します。

こんな事に気をつけて

配布するプレフィックスとして IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は、上位を “dhcp@ インタフェース名 ” 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インタフェースを指定してください。

Valid Lifetime
割り当てるプレフィックスの Valid Lifetime を指定します。

有効範囲）
0 ～ 365 日
0 ～ 8760 時間
0 ～ 525600 分
0 ～ 31536000 秒

Pref. Lifetime
割り当てるプレフィックスの Preferred Lifetime を指定します。Pref. Lifetime は、Valid Lifetime より短い時間になるように設定してください。

有効範囲）
0 ～ 365 日
0 ～ 8760 時間
0 ～ 525600 分
0 ～ 31536000 秒

自動経路設定
クライアントに割り当てたプレフィックスへの経路を自動で設定する場合は、“ する ” を選択します。

配布先クライアント DUID
配布先クライアントの DUID を、260 桁以内の 16 進数で指定します。

DNS サーバアドレス配布

配布する DNS サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する DNS サーバアドレスとして IPv6 DHCP クライアントが取得した DNS サーバアドレスを使用する場合は、“dhcp@ インタフェース名 ” の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリ DNS サーバの指定はできません。

DNS ドメイン名配布

配布する DNS ドメイン名を設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する DNS ドメイン名として IPv6 DHCP クライアントが取得した DNS ドメイン名を使用する場合は、“dhcp@ インタフェース名 ” の形式で指定します。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インタフェースを指定してください。

SIP サーバアドレス配布

配布する SIP サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SIP サーバアドレスとして IPv6 DHCP クライアントが取得した SIP サーバアドレスを使用する場合は、“dhcp@ インタフェース名 ” の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリ SIP サーバの指定はできません。

SIP ドメイン名配布

配布する SIP ドメイン名を設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SIP ドメイン名として IPv6 DHCP クライアントが取得した SIP ドメイン名を使用する場合は、“dhcp@ インタフェース名 ” の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリ SIP サーバの指定はできません。

SNTP サーバアドレス配布

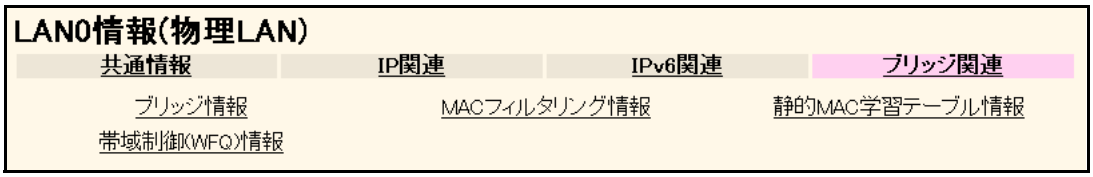
配布する SNTP サーバの IPv6 アドレスを設定します。省略すると DHCP サーバによる配布を行いません。

こんな事に気をつけて

配布する SNTP サーバアドレスとして IPv6 DHCP クライアントが取得した SNTP サーバアドレスを使用する場合は、“dhcp@ インタフェース名 ” の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリ SNTP サーバの指定はできません。

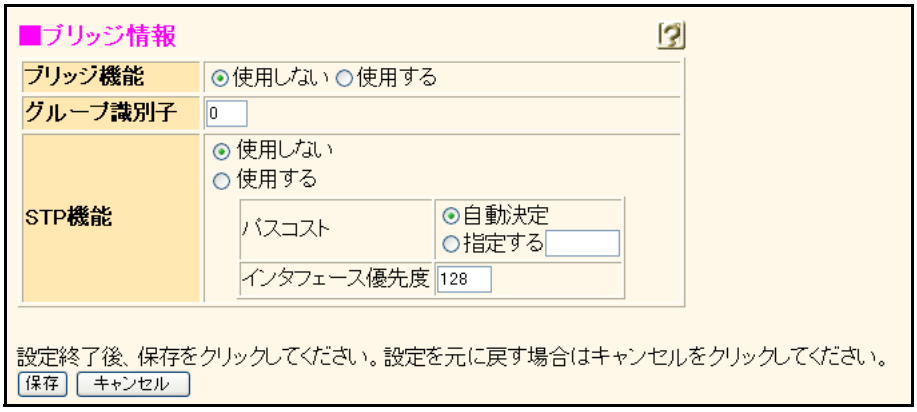
10.1.4　ブリッジ関連

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［ブリッジ関連］



10.1.4.1　ブリッジ情報

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［ブリッジ関連］→［ブリッジ情報］



ブリッジ機能

接続相手とブリッジで通信する場合は、“ 使用する ” を選択します。

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

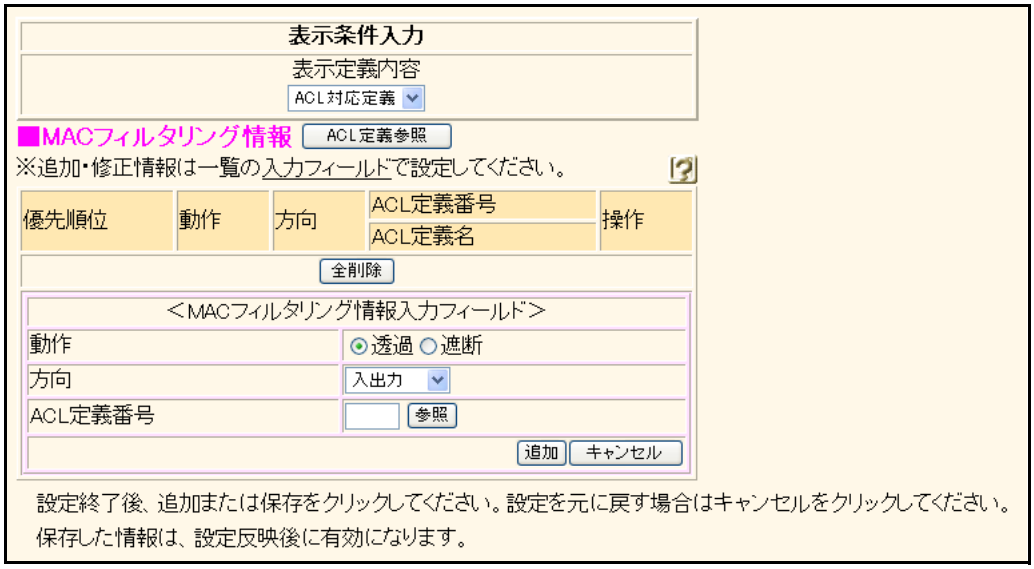
STP で利用するパスコストを選択します。“ 指定する ” を選択する場合は、1 ～ 65535 の範囲で指定します。パスコストの適性値が不明な場合は、“ 自動決定 ” を選択すると、自動的にパスコストが決定されます。

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。

10.1.4.2 MAC フィルタリング情報

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



現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、128 個まで定義できます。処理するボタンをクリックし、次のページへ進みます。

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。

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。

動作

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

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

方向

フィルタリングする方向を指定します。

- 入力
  入力パケットのみをフィルタリング対象とする場合に指定します。
- 出力
  出力パケットのみをフィルタリング対象とする場合に指定します。
- リバース
  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
  - 送信元 MAC アドレスとあて先 MAC アドレス
- 入出力
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に指定します。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- MAC 定義

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

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

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

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

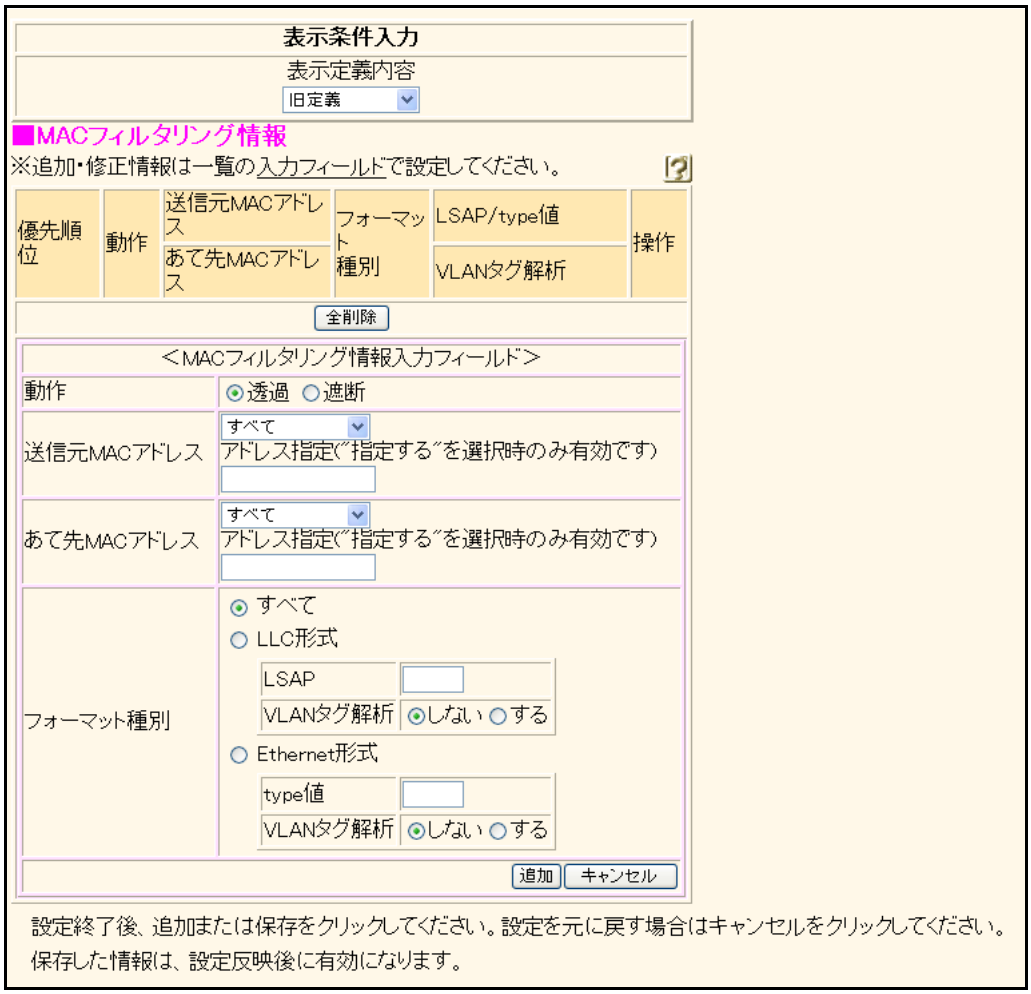
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

10.1.4.2.1 MAC フィルタリング情報（旧定義）

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［ブリッジ関連］→［MAC フィルタリング情報］→「表示定義内容（旧定義）」



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

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。

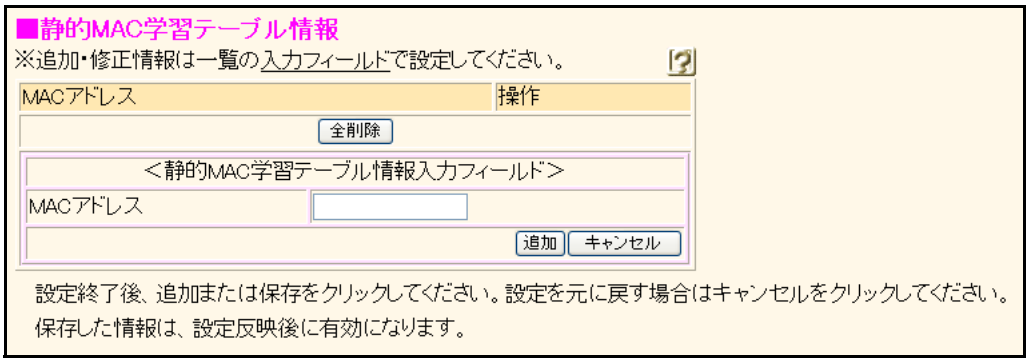
フォーマット種別

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。

10.1.4.3 静的 MAC 学習テーブル情報

［操作］　ルータ設定「LAN 情報（物理 LAN）」→［修正］→［ブリッジ関連］→［静的 MAC 学習テーブル情報］



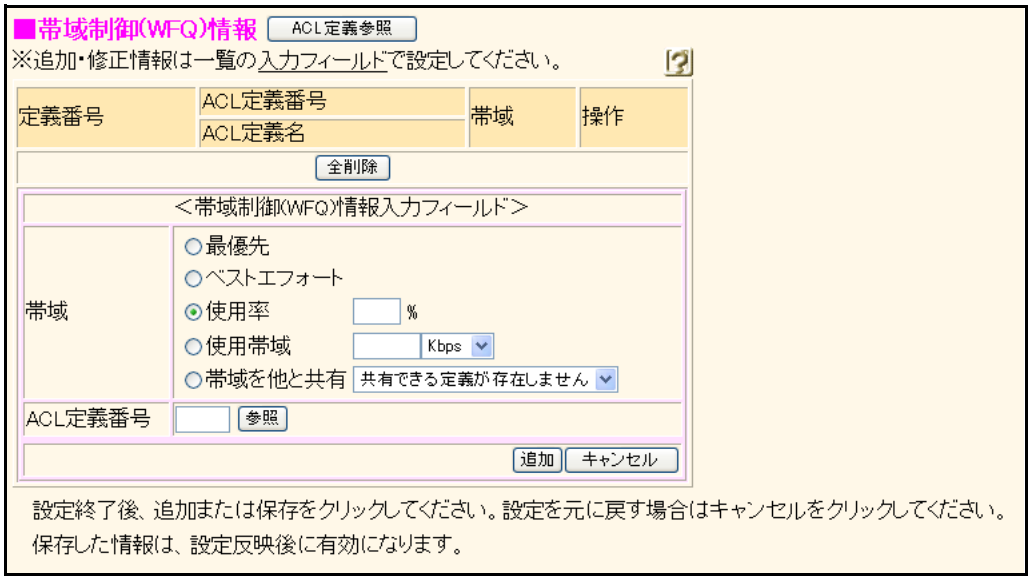
現在、設定されている静的 MAC 学習テーブルの定義が表示されています。静的 MAC 学習テーブル情報の定義数は、装置全体で 200 個まで定義できます。処理するボタンをクリックし、次のページへ進みます。

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。

10.1.4.4 帯域制御（WFQ）情報

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



現在、設定されている帯域制御の定義が表示されています。帯域制御の定義数は、64 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。

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。
- 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する場合に選択します。

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- MAC 定義

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

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

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

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

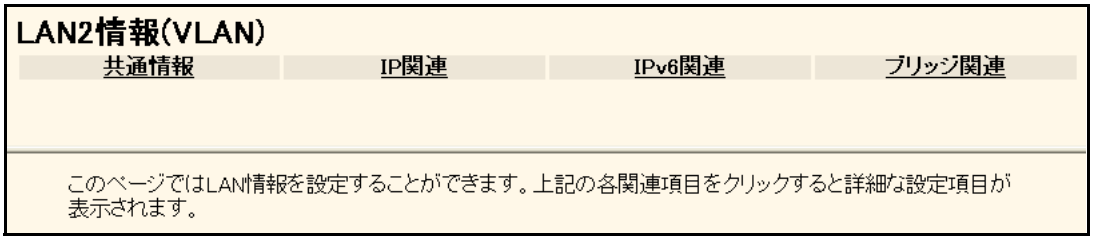
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「帯域制御（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。

10.2 インタフェース：VLAN

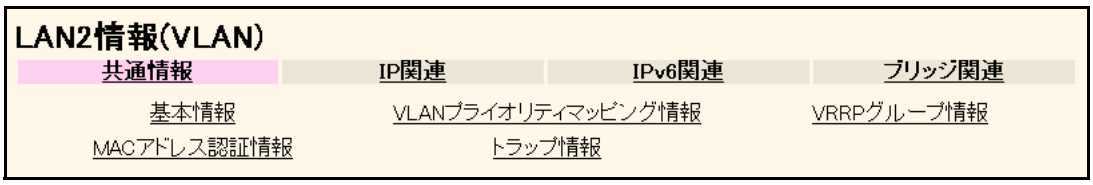
［操作］　ルータ設定「LAN 情報（VLAN）」→［追加］



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

10.2.1 共通情報

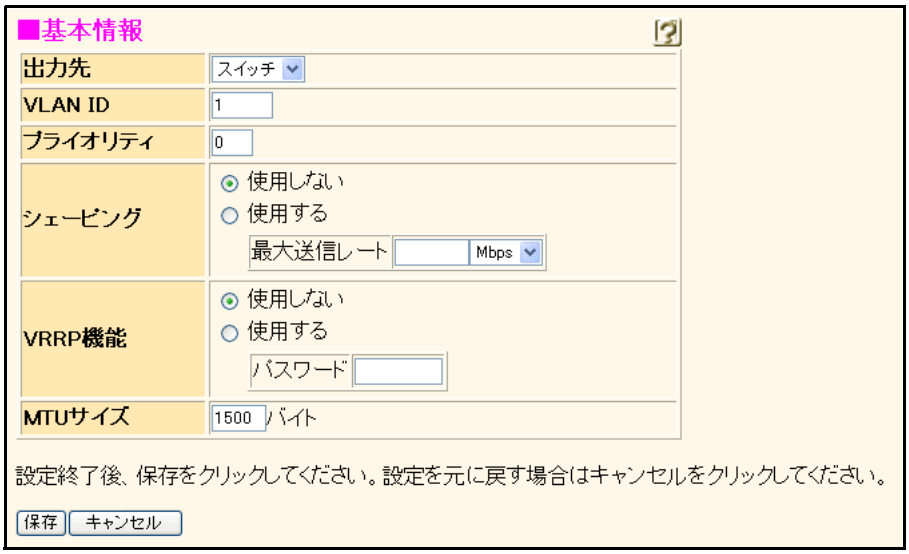
［操作］　ルータ設定「LAN 情報（VLAN）」→［追加］→［共通情報］



「VRRP グループ情報」、「MAC アドレス認証情報」および「トラップ情報」は、「インタフェース：物理 LAN」を参照してください。

10.2.1.1 基本情報

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



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。

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。

最大送信レート

最大送信レートを1～100000Kbpsの範囲で指定します。Kbpsは1000bpsを、Mbpsは1000Kbpsを意味します。

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。

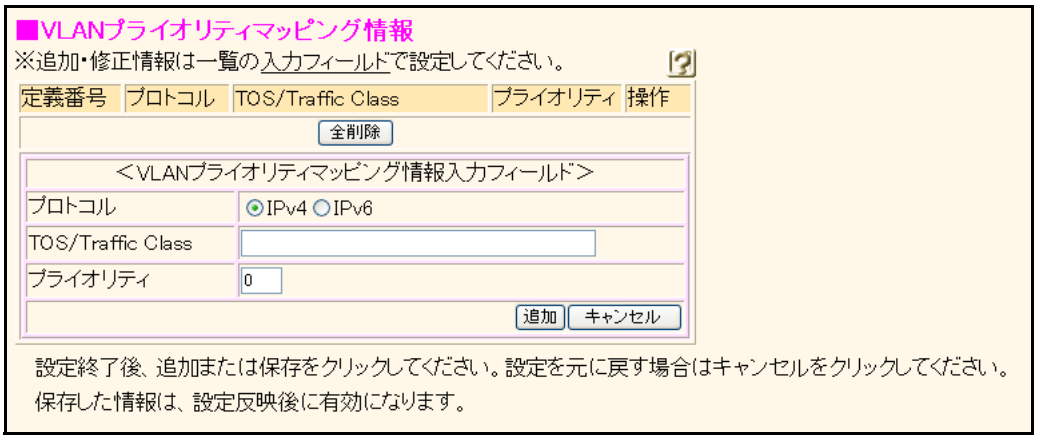
RIPを利用する場合は、576バイト以上を指定します。576バイト未満のMTUサイズを指定するとRIPパケットが送信されない場合があります。

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。

10.2.1.2 VLAN プライオリティマッピング情報

［操作］　ルータ設定「LAN 情報（VLAN）」→［追加］→［共通情報］
→［VLAN プライオリティマッピング情報］



現在、設定されているプライオリティマッピング情報の定義が表示されています。VLAN プライオリティマッピングの定義数は、装置全体で 100 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。

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

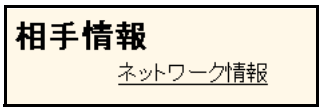
IP の TOS フィールド値または IPv6 の Traffic Class フィールド値を “any”、または 16 進数を使用して、0 ～ ff の範囲で指定します。複数の値を指定する場合は、“,” で区切ります。範囲指定の場合は、“-” で区切ります。10 組まで指定できます。省略時は “any” が設定されます。

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。

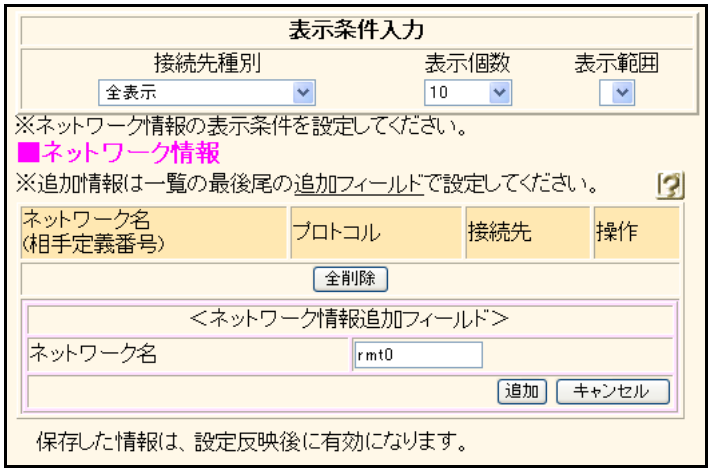
11　相手情報

［操作］　ルータ設定「相手情報」



11.1　ネットワーク情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］



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、50 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。

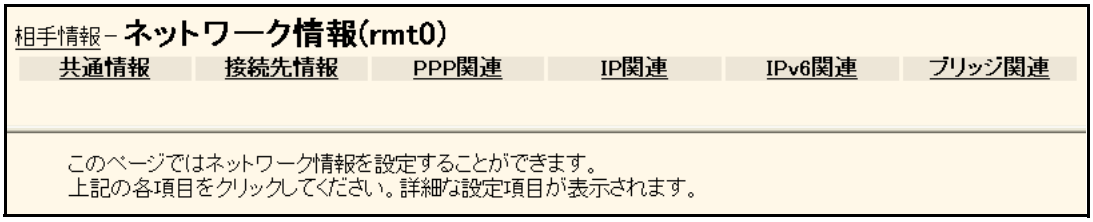
表示条件入力

ネットワーク情報の表示条件を接続先種別、表示個数、および表示範囲によって指定することができます。設定することによって、ネットワーク情報の一覧に見たい情報だけを表示させることができます。

ネットワーク名

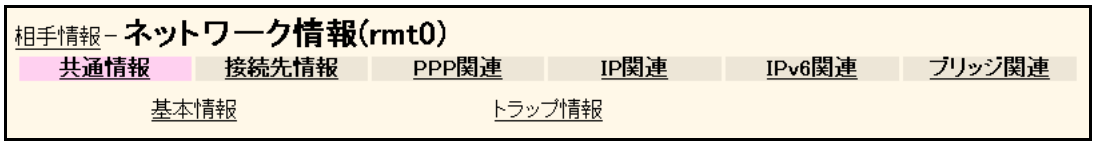
このネットワークを識別するための名称を８文字以内で指定します。

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］



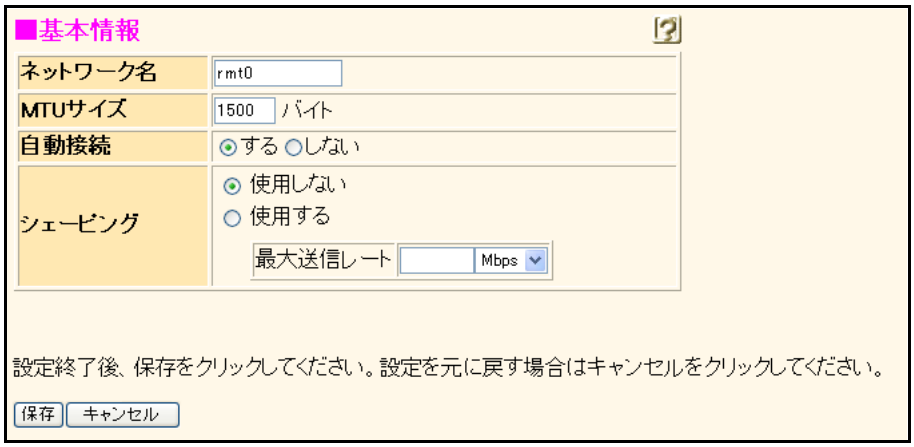
11.1.1　共通情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［共通情報］



11.1.1.1　基本情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［共通情報］→［基本情報］



ルーティングの対象となるネットワークの情報を設定します。

ネットワーク名

このネットワークを識別するための名称を８文字以内で指定します。

MTU サイズ

最大パケット送信サイズ（Maximum Transmission Unit）を 200 ～ 1500 バイトの範囲で指定します。IPv6 通信で利用する場合は、1280 バイト以上の値を指定します。

また、IPv6 トンネル（IPv6 over IPv4）を利用する場合は、1280 バイトを指定します。

PPPoE（PPP over Ethernet）を利用する場合は、1454 バイトを指定します。

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

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

自動接続

データ通信発生時に自動的に接続する場合は、“ 使用する ” を選択します。

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

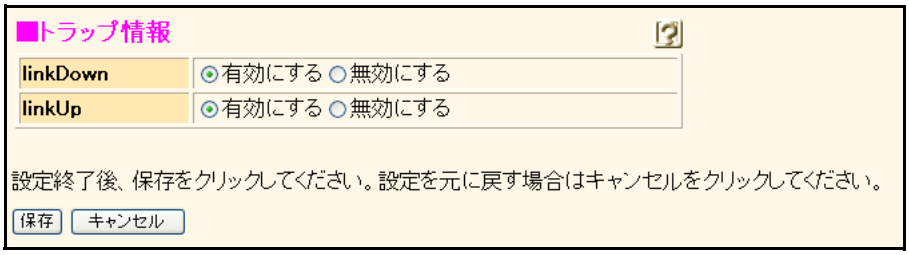
最大送信レートを 1 ～ 100000Kbps または 1 ～ 100Mbps の範囲で指定します。Kbps は 1000bps を、Mbps は 1000Kbps を意味します。

こんな事に気をつけて

- **シェーピング機能は、接続先種別が IP トンネルでは動作しません。**
- **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。**

11.1.1.2 トラップ情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［共通情報］→［トラップ情報］



トラップ情報

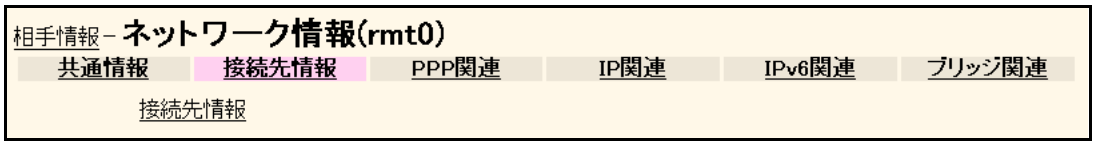
SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP エージェント機能を使用しない場合は、この設定は意味を持ちません。

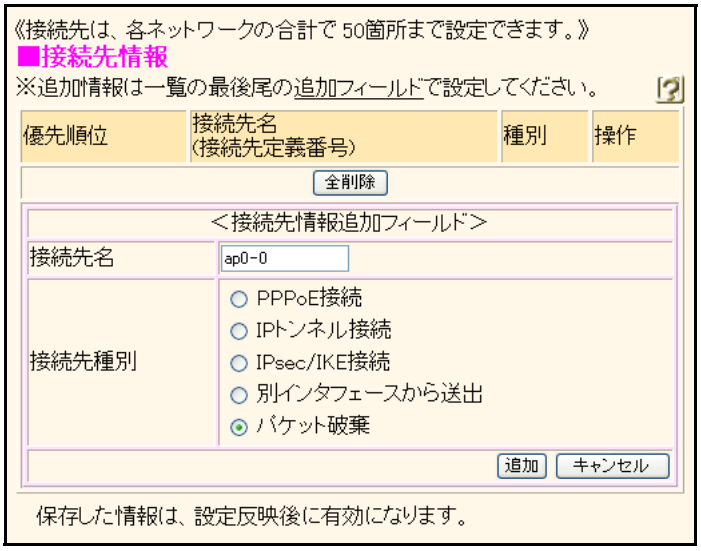
- linkDown
  linkDown トラップを通知します。
- linkUp
  linkUp トラップを通知します。

11.1.2 接続先情報

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



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



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、装置全体で 50 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。

選択する接続種別によって、表示が異なります。

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。

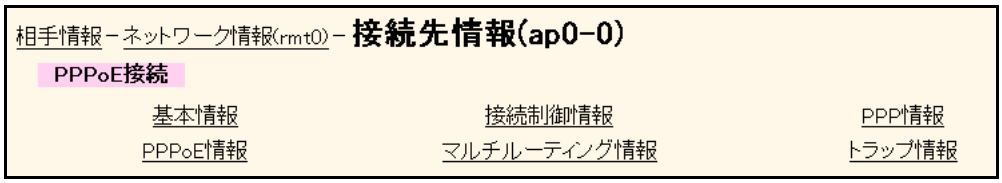
接続先種別

この接続先の種別を以下から選択します。

- PPPoE 接続
  PPPoE を使用して接続する場合に選択します。使用するには LAN 情報を設定してください。
- IP トンネル接続
  IP トンネルを使用して接続する場合に選択します。IP トンネルに使用する IPv6 または IPv4 の設定は別の LAN 情報または相手情報で設定します。
- IPsec/IKE 接続
  IPsec/IKE トンネルを使用して接続する場合に選択します。IPsec/IKE トンネルに使用する IPv4 と IPv6 の設定は別の相手情報で設定します。
- 別インタフェースから送出
  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。
- 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。

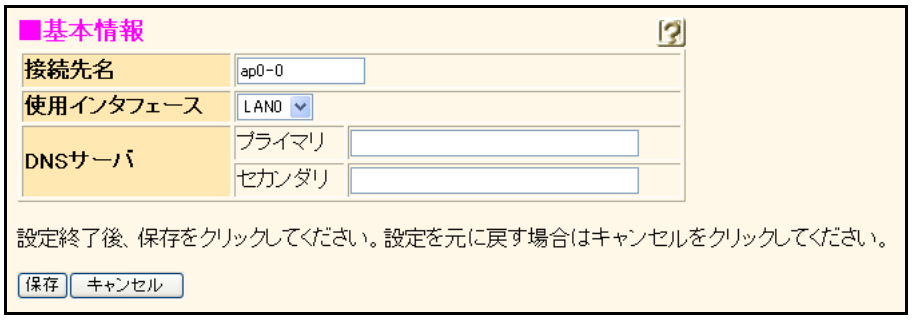
11.1.2.1 接続先種別：PPPoE 接続

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（PPPoE 接続）］→［追加］



11.1.2.1.1 基本情報

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



接続先名

この接続先を識別するための名称を８文字以内で指定します。この名前は手動接続の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。

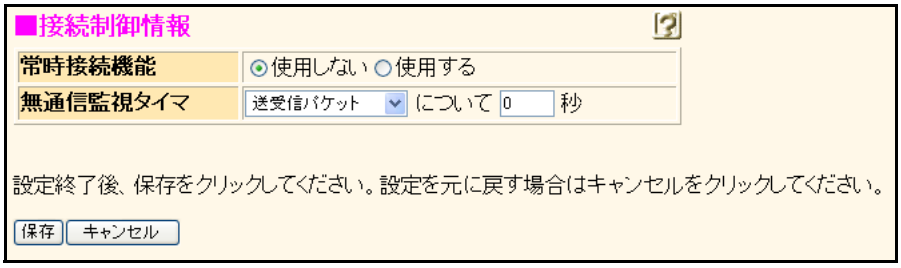
DNS サーバ

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。プライマリのみを省略することはできません。255.255.255.255 を指定した場合は、DNS サーバは使用しません。また、この IP アドレスは PPP のネゴシエーションの中で相手から要求があった場合、相手に受け渡す DNS サーバアドレスとしても使用します。

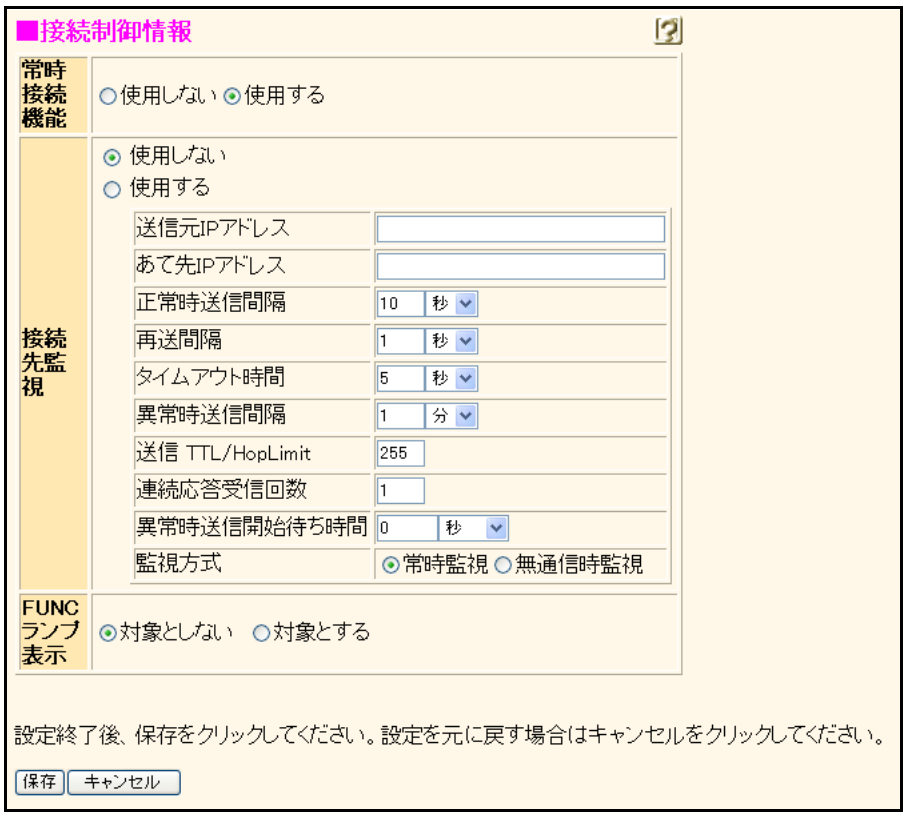
11.1.2.1.2 接続制御情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（PPPoE 接続）］→［追加］→［接続制御情報］

常時接続機能で、“ 使用する ” を選択した場合



常時接続機能で、“ 使用する ” を選択した場合



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。「接続先監視」を設定します。“ 使用しない ” を選択した場合は、「無通信監視タイマ」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。

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。

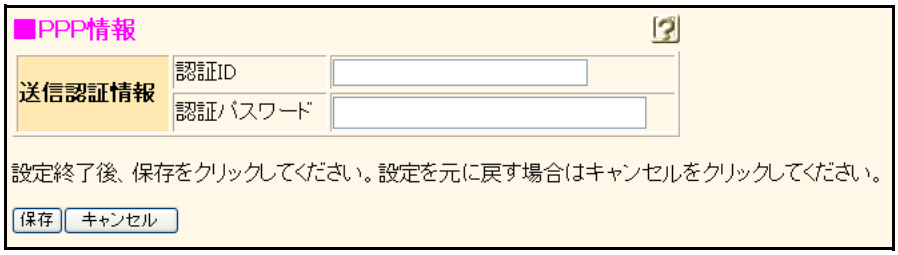
- 常時監視
  常時、監視を行います。
- 無通信時監視
  無通信時に、監視を行います。

FUNCランプ表示

接続先状態をFUNCランプ表示対象とするか、または表示対象としないかを選択します。

11.1.2.1.3 PPP 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（PPPoE 接続）］→［追加］→［PPP 情報］



送信認証情報

認証 ID

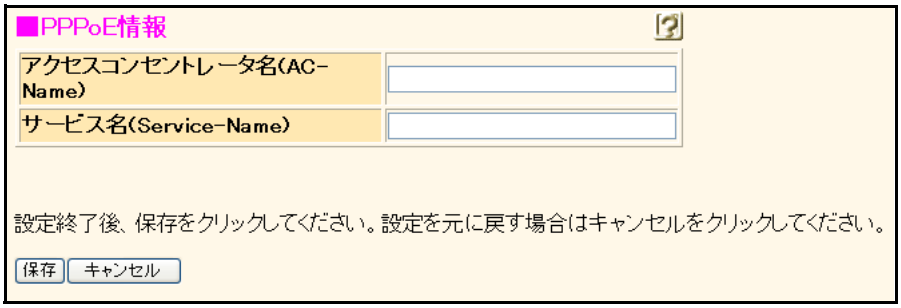
送信時に使用する認証 ID を 64 文字以内の文字列で指定します。

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。

11.1.2.1.4 PPPoE 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（PPPoE 接続）］→［追加］→［PPPoE 情報］



アクセスコンセントレータ名（AC-Name）

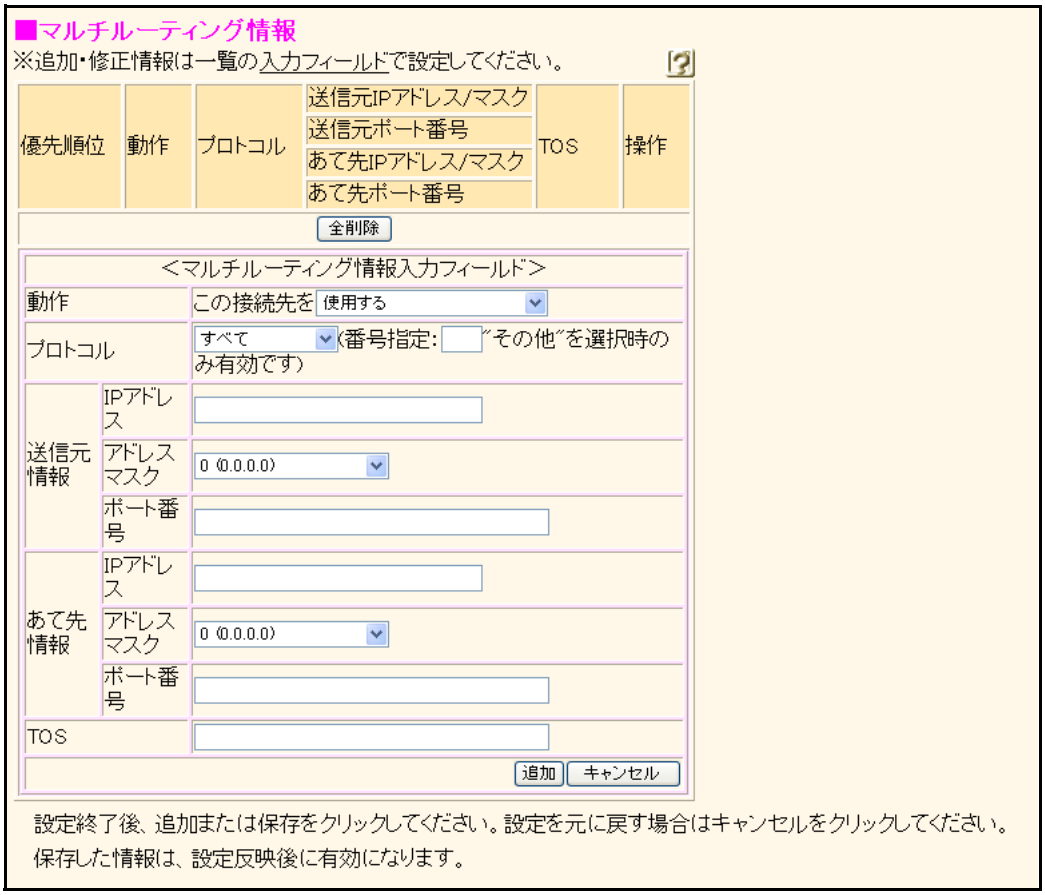
アクセスコンセントレータ名を 64 文字以内の文字列で指定します。

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。

11.1.2.1.5 マルチルーティング情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（PPPoE 接続）］→［追加］→［マルチルーティング情報］



現在、設定されているマルチルーティング情報の定義が表示されています。処理は優先順位1から順に行われます。マルチルーティングの定義数は、装置全体で50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。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された動作を行います。

動作

マルチルーティングの動作を以下の3つから選択します。

- 使用する
  条件と一致した場合に、この接続先を使用します。
- 使用しない
  条件と一致した場合に、この接続先を使用しません。
- バックアップとして使用する
  条件と一致し、以降の接続先を使用することができない場合に、この接続先を使用します。

プロトコル

マルチルーティング条件としてプロトコルを以下の6つから選択します。（）内はプロトコル番号です。

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

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

送信元／あて先情報

マルチルーティング条件としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

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

ポート番号

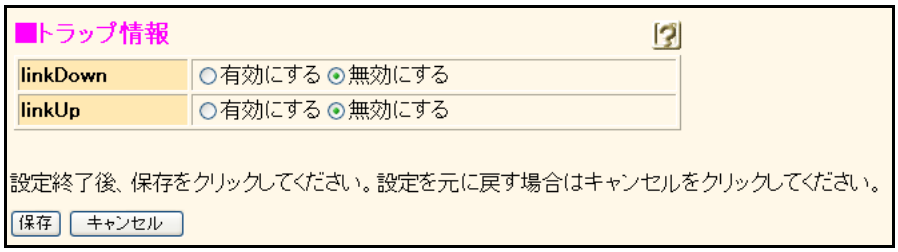
マルチルーティング条件としてポート番号を 10 進数を使用して、1 ～ 65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号がマルチルーティングの対象となります。また、ポート番号を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切ります。送信元情報とあて先情報で合わせて 10 組まで指定できます。

TOS

マルチルーティング条件として IP パケットの TOS（Type of Service）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。

11.1.2.1.6 トラップ情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（PPPoE 接続）］→［追加］→［トラップ情報］



トラップ情報

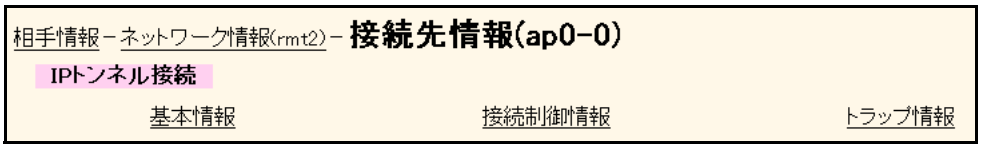
SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP エージェント機能を使用しない場合は、この設定は意味を持ちません。

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

11.1.2.2 接続先種別：IP トンネル接続

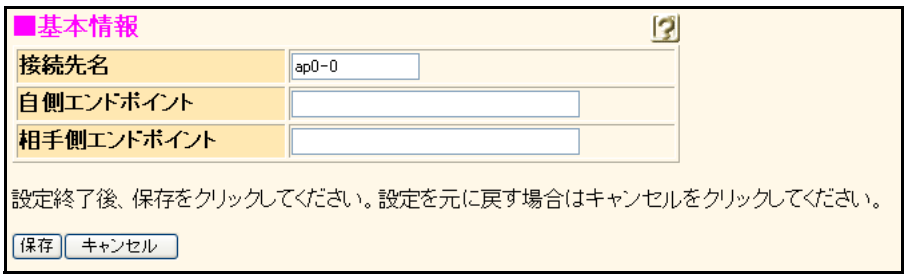
［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IP トンネル接続）］→［追加］



「トラップ情報」は、「接続先種別：PPPoE 接続」を参照してください。

11.1.2.2.1 基本情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IP トンネル接続）］→［追加］→［基本情報］



接続先名

この接続先を識別するための名称を８文字以内で指定します。

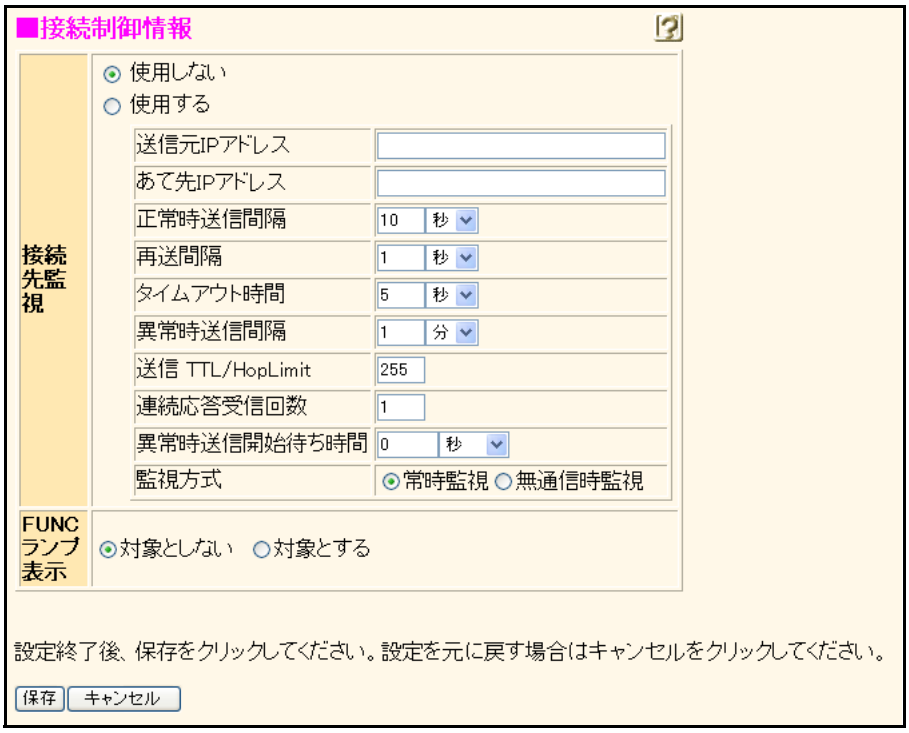
自側／相手側エンドポイント

自側（相手側）のトンネルエンドポイントとなる IPv4 アドレスまたは IPv6 アドレスを指定します。

有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.25.255.254
192.0.0.1 ～ 223.255.255.254
::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

11.1.2.2.2 接続制御情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IP トンネル接続）］→［追加］→［接続制御情報］



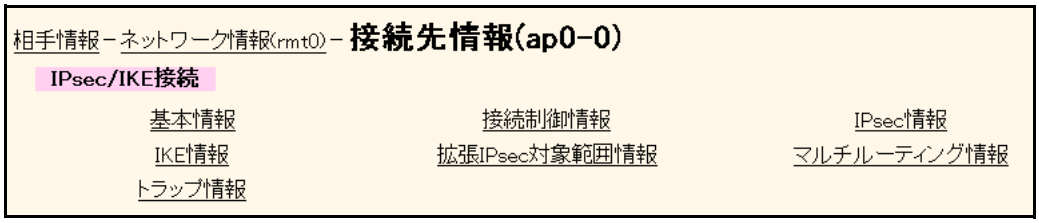
接続先監視および FUNC ランプ表示の項目は、「接続先種別：PPPoE 接続」を参照してください。

11.1.2.3 接続先種別：IPsec/IKE 接続

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

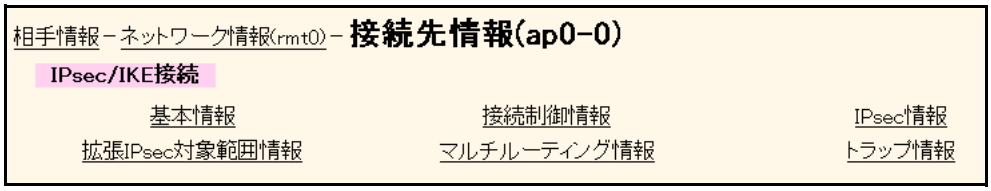
「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、以下の方式で設定を保存した場合

- Aggressive Mode（Initiator）共有鍵認証方式
- Aggressive Mode（Responder）共有鍵認証方式
- Main Mode 共有鍵認証方式



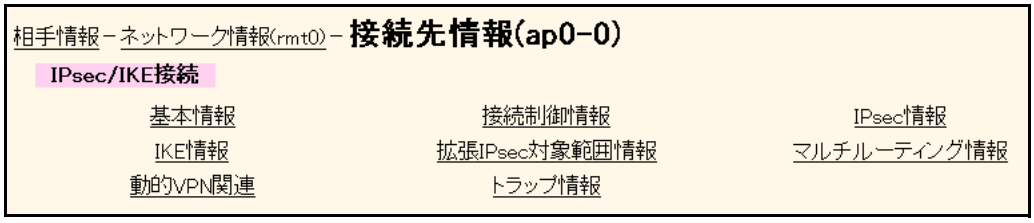
「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、以下の方式で設定を保存した場合

- 手動鍵使用
- IKE は他の接続先情報を使用



「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、以下の方式で設定を保存した場合

- 動的 VPN 接続 共有鍵認証方式

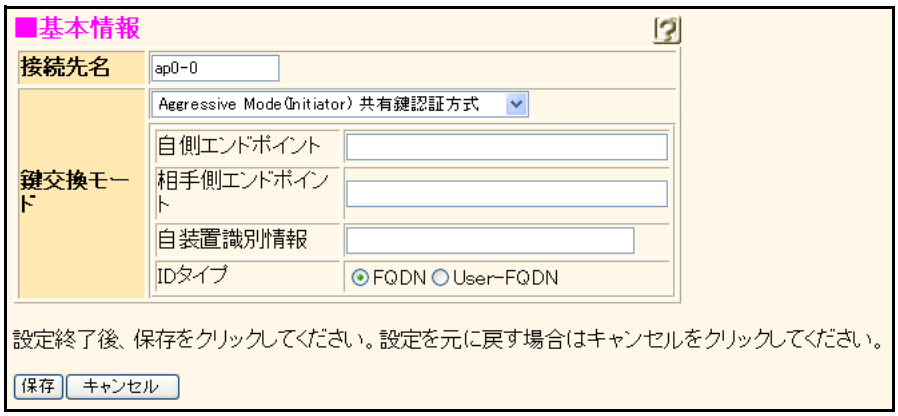


「マルチルーティング情報」および「トラップ情報」は、「接続先種別：PPPoE 接続」を参照してください。

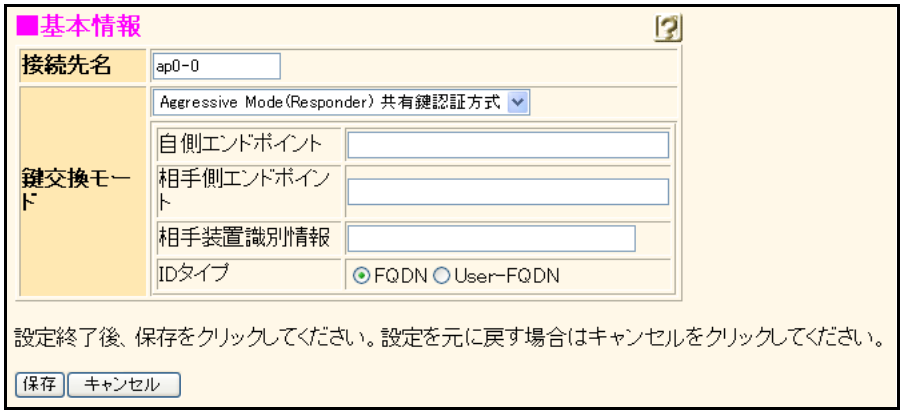
11.1.2.3.1 基本情報

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

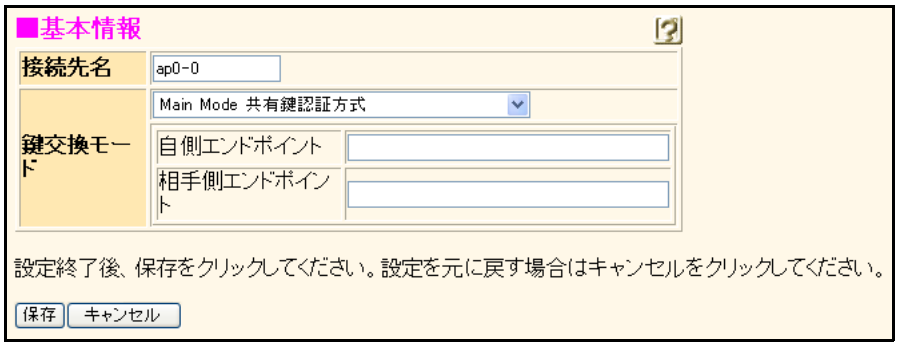
鍵交換モードで、“Aggressive Mode（Initiator）共有鍵認証方式 ” を選択した場合



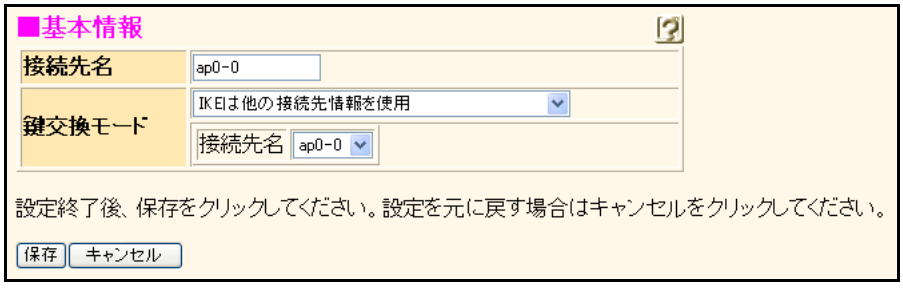
鍵交換モードで、“Aggressive Mode（Responder）共有鍵認証方式 ” を選択した場合



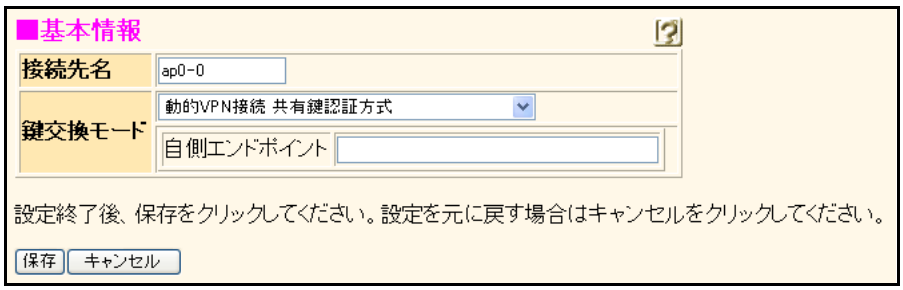
鍵交換モードで、“Main Mode 共有鍵認証方式 ” および “ 手動鍵使用 ” を選択した場合



鍵交換モードで、“IKE は他の接続先情報を使用 ” を選択した場合



鍵交換モードで、“動的VPN接続 共有鍵認証方式”を選択した場合



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）共有鍵認証方式
  自側エンドポイントが可変IPアドレスでIPsec/IKEを利用して通信をする場合に選択します。自側エンドポイントが固定IPアドレスでAggressive Modeを使用する場合は、自側エンドポイントを指定してください。
  Aggressive Mode（Initiator）共有鍵認証方式を利用する場合、相手エンドポイント装置にAggressive Mode（Responder）共有鍵認証方式の設定がされている必要があります。
- Aggressive Mode（Responder）共有鍵認証方式
  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）共有鍵認証方式を利用する場合、相手エンドポイント装置にAggressive Mode（Initiator）共有鍵認証方式の設定がされている必要があります。
- Main Mode 共有鍵認証方式
  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 共有鍵認証方式を利用する場合、相手エンドポイント装置にMain Mode 共有鍵認証方式の設定がされている必要があります。
- 手動鍵使用
  手動鍵設定でのIPsecを利用して通信する場合に選択します。
  手動鍵を利用する場合、相手エンドポイント装置に手動鍵の設定がされている必要があります。
- 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 共有鍵認証方式
  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）共有鍵認証方式”または“動的VPN接続 共有鍵認証方式”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

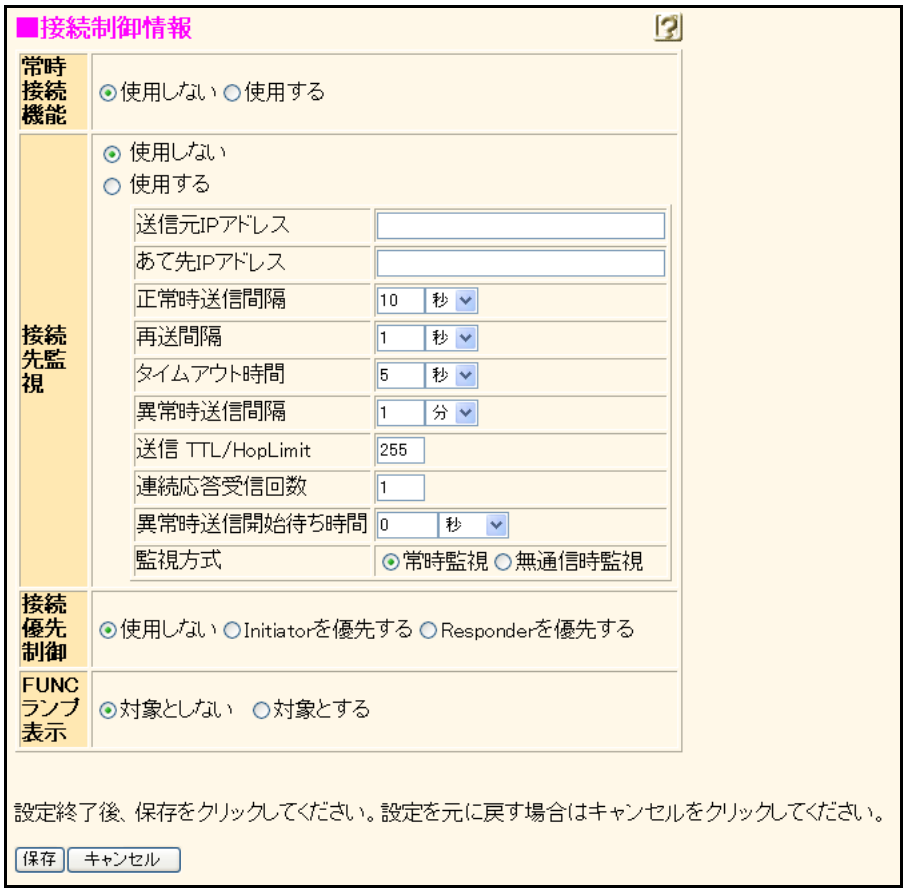
ネゴシエーションの交換タイプを選択します。

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。

11.1.2.3.2 接続制御情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IPsec/IKE 接続）］→［追加］→［接続制御情報］



接続先監視および FUNC ランプ表示の項目は、「接続先種別：PPPoE 接続」を参照してください。

常時接続機能

“ 使用する ” を選択すると、ほかの設定や通信の有無にかかわらず接続状態を保持します。また、IKE ネゴシエーション失敗などによる IPsec SA ができない場合や IPsec SA が解放された場合は、自動で IKE ネゴシエーションによる再接続を行います。ただし、本装置で手動切断を行うと、次に手動接続を行うまで自動接続動作は行いません。

接続優先制御

IKE SA を確立するための IKE ネゴシエーションが競合した場合の接続優先制御を以下の 3 つから選択します。

- 使用しない
  そのまま IKE ネゴシエーションを続けます。
- Initiator を優先する
  Initiator の要求を残し、Responder 要求を無視します。
- Responder を優先する
  Responder の要求を残し、Initiator の要求を終了します。

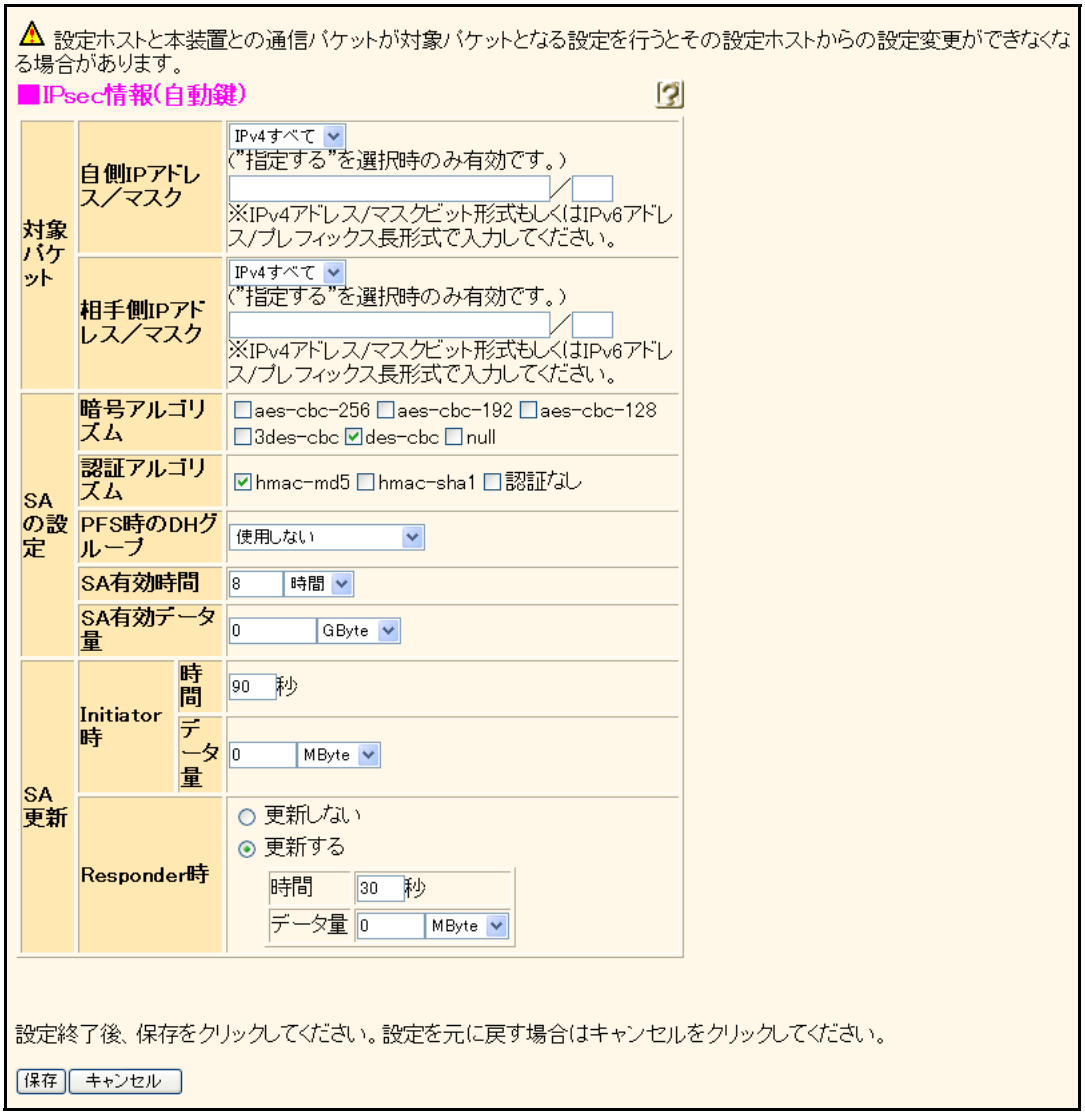
こんな事に気をつけて

自装置と接続相手装置の両方で接続優先制御を行う場合は、それぞれ異なる優先方法を選択してください。同じ優先制御を行うと、競合した場合に IKE ネゴシエーションが失敗します。この機能を利用する場合は、以下の設定を奨励します。

- **一方の装置で Initiator 接続を優先し、一方の装置で Responder 接続を優先する。**

11.1.2.3.3 IPsec 情報（自動鍵）

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



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 共有鍵認証方式”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。

11.1.2.3.4 IPsec 情報（手動鍵）

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

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）の項目は、「IPsec 情報（自動鍵）」を参照してください。

SA の設定（送信用）／（受信用）

SPI 値

SPI 値は、暗号情報や認証情報を定義したセキュリティパラメタインデックスです。相手装置の設定と同じ値を指定する必要があります。SPI 値を 100 ～ ffffffff の 16 進数の範囲で指定します。

暗号アルゴリズム

トンネリングするパケットの暗号アルゴリズムを選択します。“暗号化しない”を選択した場合は、パケットの暗号化を行いません。

暗号鍵

- 鍵識別
  鍵の識別を指定します。
- 鍵
  暗号アルゴリズムで使用する暗号鍵を16進数および文字列を使用して、以下の範囲で指定します。

暗号アルゴリズム	入力範囲（16進数鍵）	入力範囲（文字列鍵）
DES-CBC	1～16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。

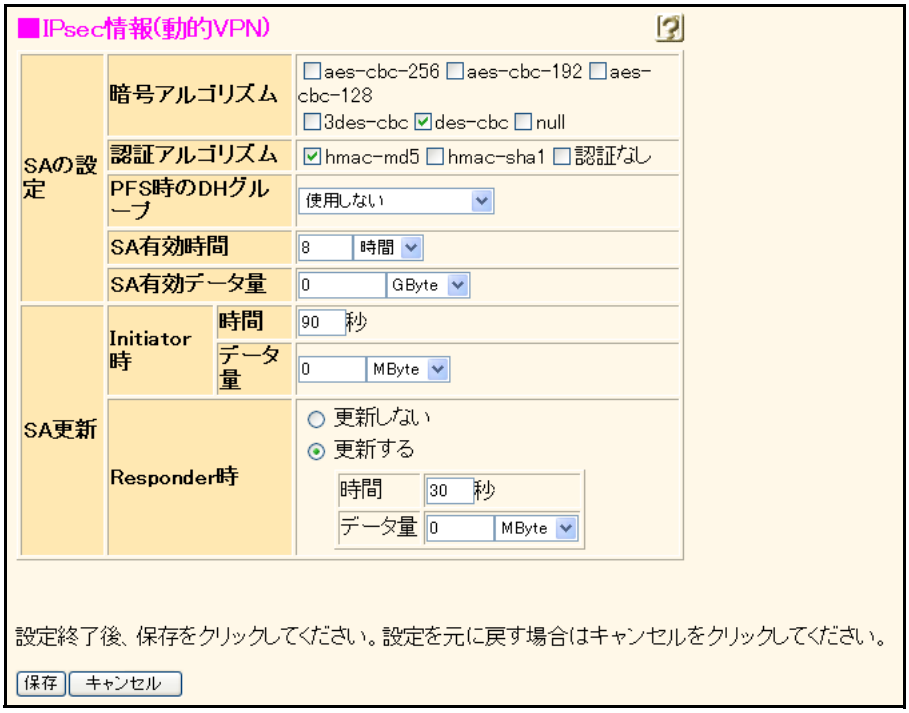
暗号アルゴリズム	入力範囲（16進数鍵）	入力範囲（文字列鍵）
HMAC-MD5	1～32桁	16文字
HMAC-SHA1	1～40桁	20文字

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。

11.1.2.3.5 IPsec 情報（動的 VPN）

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

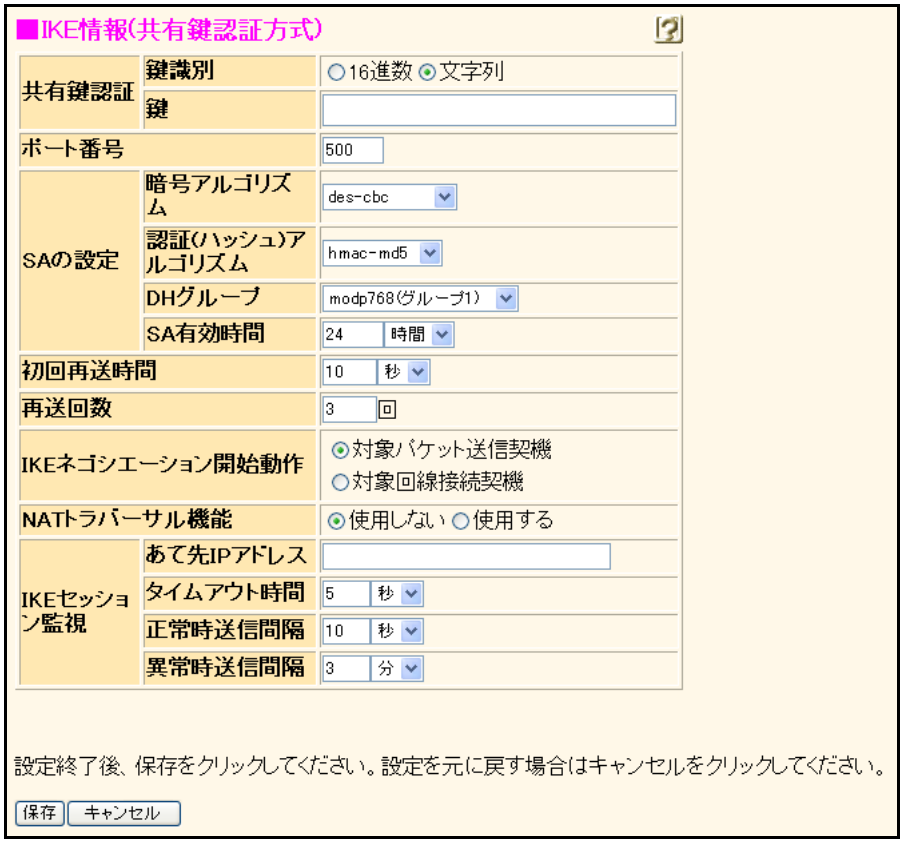


この画面は、「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“ 動的 VPN 接続 共有鍵認証方式 ” を選択した場合に表示されます。

各項目の説明は、「IPsec 情報（自動鍵）」を参照してください。

11.1.2.3.6 IKE 情報（共有鍵認証方式）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IPsec/IKE 接続）］→［追加］→［IKE 情報（共有鍵認証方式）］



この画面は、「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、以下を選択した場合に表示されます。

- Aggressive Mode（Initiator）共有鍵認証方式
- Aggressive Mode（Responder）共有鍵認証方式
- Main Mode 共有鍵認証方式
- IKE は他の接続先情報を使用

共有鍵認証

IKE の認証に用いる鍵を設定します。ここでは事前共有鍵（Pre-shared key）の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵識別

鍵の識別を選択します。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲（16 進数鍵）	入力範囲（文字列鍵）
1～256 桁	1～128 文字

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

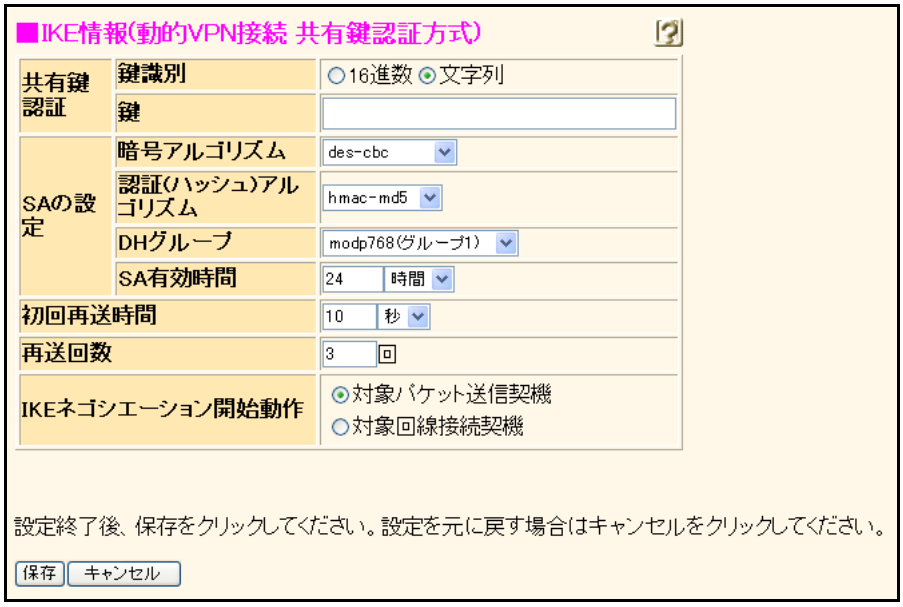
ICMP ECHO パケットのタイムアウトが発生してから応答が受信されるまでの周期送信する間隔を、10 進数を使用して 60 ～ 600 秒の範囲で指定します。応答が受信された場合は正常時送信間隔状態に戻ります。省略時は、3 分が設定されます。

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。

11.1.2.3.7 IKE 情報（動的 VPN 接続 共有鍵認証方式）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IPsec/IKE 接続）］→［追加］→［IKE 情報（動的 VPN 接続 共有鍵認証方式）］

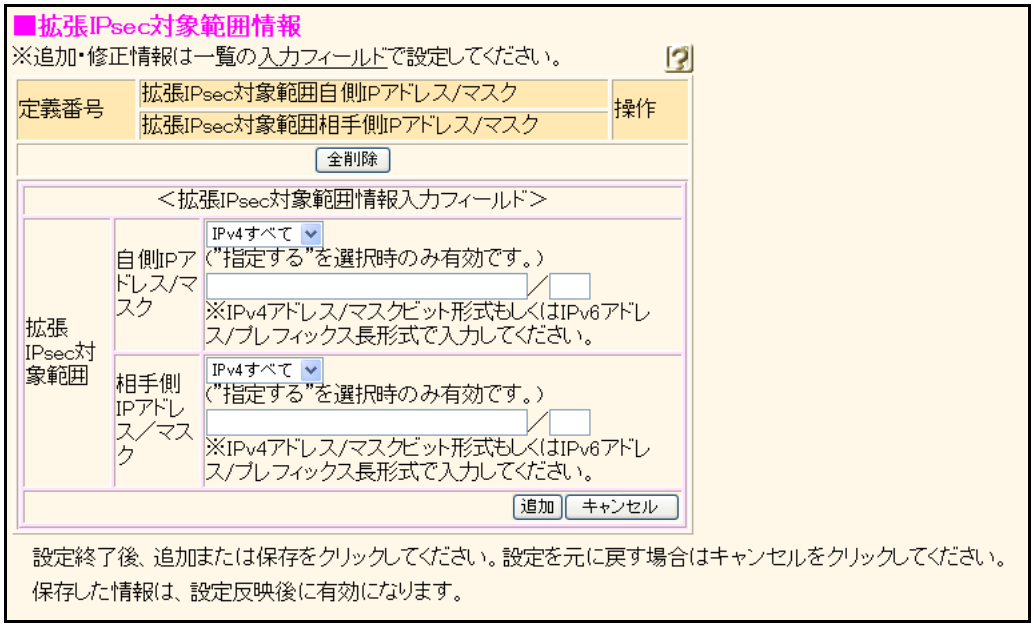


この画面は、「IPsec/IKE 接続」－「基本情報」の鍵交換モードで、“ 動的 VPN 接続 共有鍵認証方式 ” を選択した場合に表示されます。

各項目の説明は、「IKE 情報（共有鍵認証方式）」を参照してください。

11.1.2.3.8 拡張 IPsec 対象範囲情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［接続先情報（IPsec/IKE 接続）］→［追加］→［拡張 IPsec 対象範囲情報］



現在、設定されている拡張 IPsec 対象範囲情報の定義が表示されています。拡張 IPsec 対象範囲の定義数は、装置全体で 50 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。

拡張 IPsec 対象範囲設定は、自側（相手側）IP アドレス／アドレスマスクを複数定義することができます。

拡張 IPsec 対象範囲設定は、IPsec 情報の対象パケットで定義した対象パケット以外を通過させる機能であるため、Security Policy Database（SPD）や IKE ネゴシエーション（自動鍵設定のみ）には使用されません。

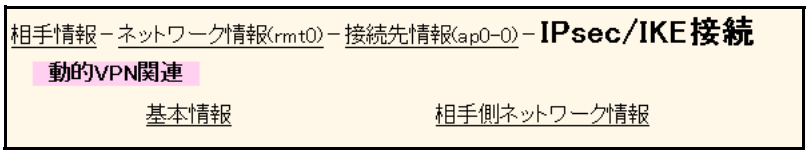
SPD や IKE ネゴシエーションに使用する ID ペイロードの設定（自動鍵設定のみ）は、IPsec 情報の対象パケットで設定してください。

自側（相手側）IP アドレス／アドレスマスク

拡張 IPsec 対象範囲の送信元 IP アドレスおよびアドレスマスクと、あて先 IP アドレスおよびアドレスマスクを指定します。IPv4 形式または IPv6 形式のアドレスを設定してください。

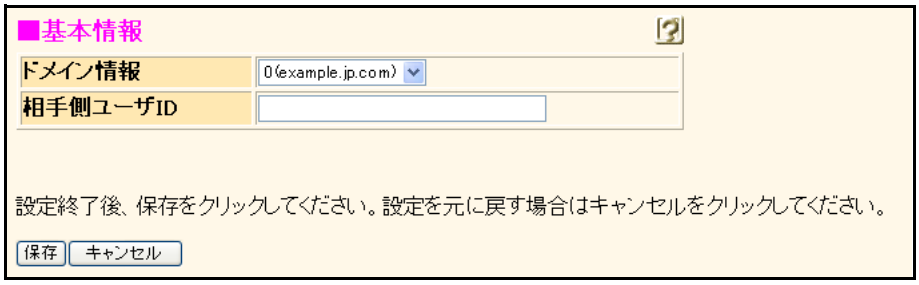
11.1.2.3.9 動的VPN関連

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



11.1.2.3.10 動的VPN関連（基本情報）

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



ドメイン情報

動的VPN接続で使用するドメイン情報を選択します。

選択できない場合は、「動的VPN情報」－「クライアント関連情報」－「ドメイン情報」を設定してください。

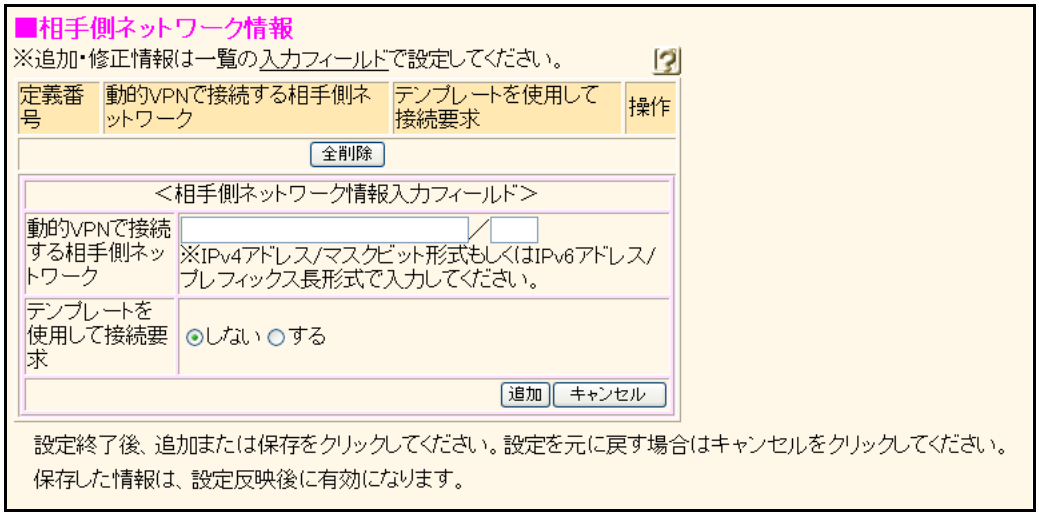
相手側ユーザID

動的VPN接続時に識別する相手側ユーザIDを50文字以内で指定します。
使用できる文字は、半角英数字、“-”、“_”、“.” です。

相手側ユーザIDは、ドメイン名と結合して動的VPN接続要求を受信したときに接続先情報を決定するために使用されます。

11.1.2.3.11 動的VPN関連（相手側ネットワーク情報）

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



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、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で接続する相手側ネットワーク

動的VPNで接続する相手側ネットワークをIPv4アドレスとマスクビット数（またはマスク値）またはIPv6アドレスとプレフィックス長で指定します。

- IPv4アドレスを指定する場合
  IPv4アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから1で連続した値にしてください。
  デフォルトルートを設定する場合は、
  0.0.0.0/0（0.0.0.0/0.0.0.0）を指定します。
- IPv6アドレスを指定する場合
  IPv6アドレスとプレフィックスの組み合わせで指定します。リンクローカルアドレスは指定できません。
  デフォルトルートを設定する場合は、::/0を指定します。

テンプレートを使用して接続要求

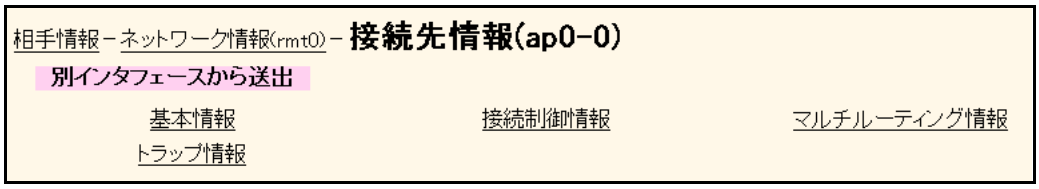
指定した相手側ネットワークが動的VPNの接続契機となるIPv4/IPv6パケットの検出条件の設定でinvite条件に一致した場合に、テンプレートを使用して接続要求を発行するかどうかを選択します。

相手側ネットワークは、相手装置から動的VPN接続要求を受信したときに接続先を特定する条件として使用されます。

また、“しない”を選択した場合は、自装置からの動的VPN接続要求を発行するときにテンプレートを使用しないで、本接続先から動的VPN接続要求を発行します。接続先から動的VPN接続をするときは、通常“しない”を選択してください。

11.1.2.4 接続種別：別インタフェースから送出

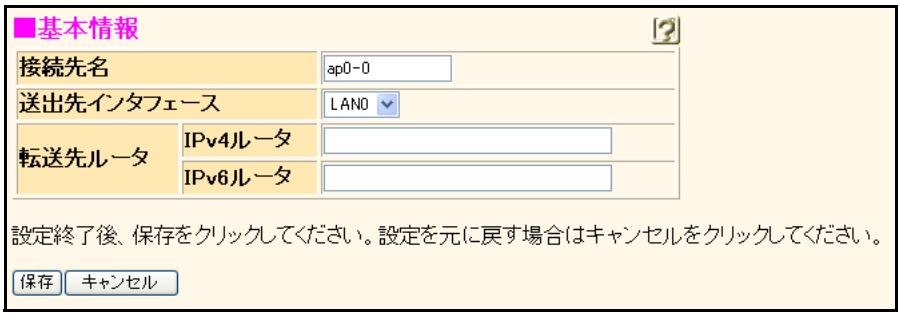
［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］
→［接続先情報（別インタフェースから送出)］→［追加］



「接続制御情報」、「マルチルーティング情報」および「トラップ情報」は、「接続先種別：PPPoE 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。

11.1.2.4.1 基本情報

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



接続先名

この接続先を識別するための名称を８文字以内で指定します。

送出先インタフェース

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。

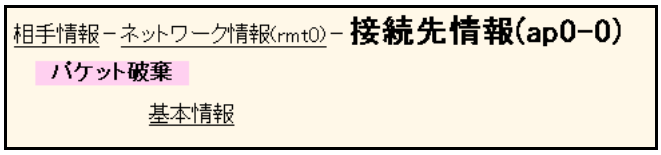
有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254
::2 ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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 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。

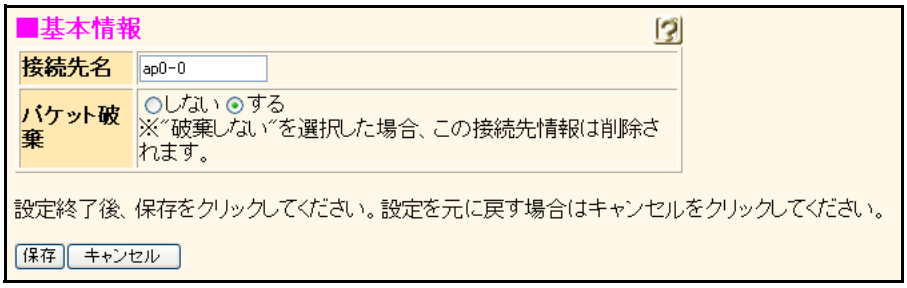
11.1.2.5　接続先種別：パケット破棄

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



11.1.2.5.1 基本情報

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



接続先名

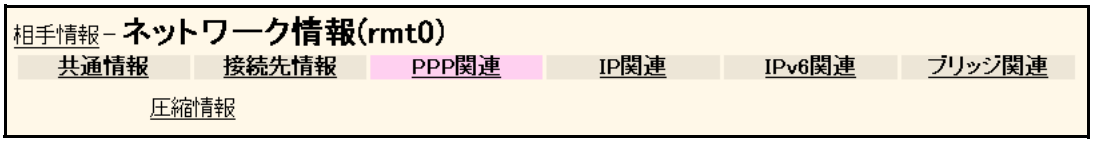
この接続先を識別するための名称を８文字以内で指定します。この接続先利用時には、すべてのパケットが破棄されます。

パケット破棄

送信するパケットをすべて破棄する場合は、“ する ” を選択します。

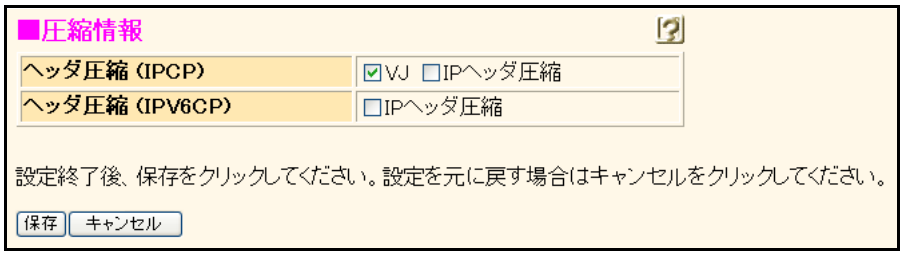
11.1.3　PPP 関連

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［PPP 関連］



11.1.3.1　圧縮情報

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



送信するパケットのヘッダ部分の圧縮を行う機能です。使用する設定の場合も、実際にヘッダ圧縮を行うかどうかは、相手ホストとのネゴシエーションで決まります。

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。

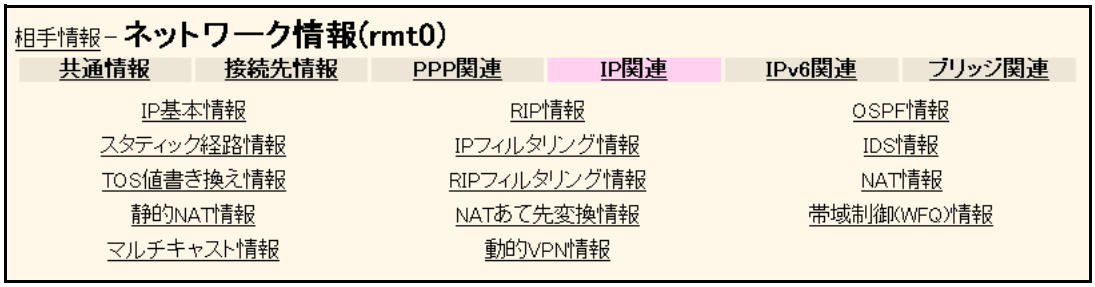
ヘッダ圧縮（IPV6CP）

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。

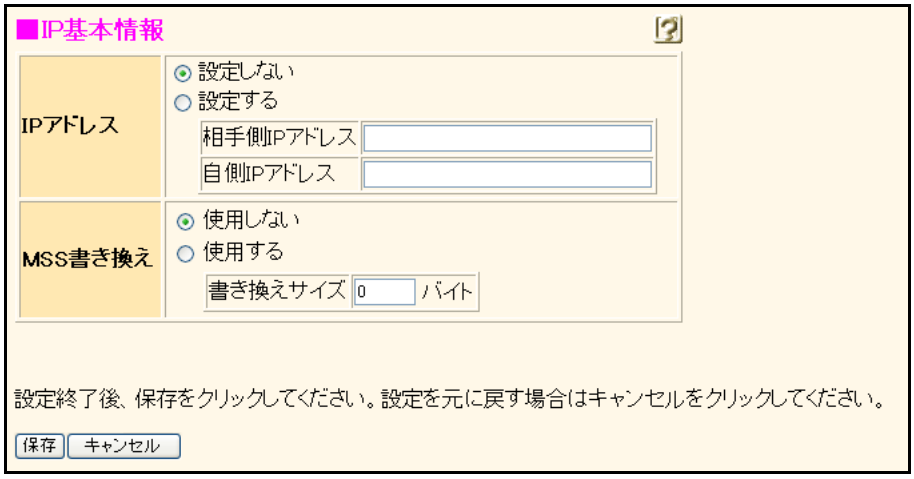
11.1.4　IP 関連

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］



11.1.4.1　IP 基本情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［IP 基本情報］



IP 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

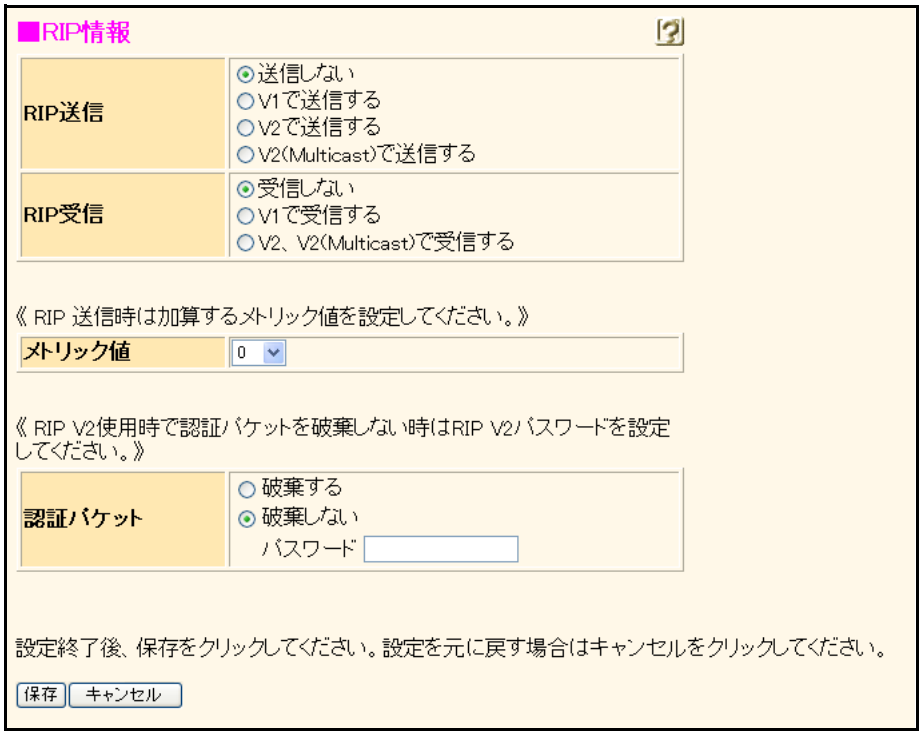
OSPF を使用するインタフェースはそれぞれ異なったネットワークに属する IP アドレスを設定する必要があります。同じネットワークに属する IP アドレスを設定した場合、OSPF を使用しないインタフェースとして扱われます。

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。

11.1.4.2 RIP 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［RIP 情報］



RIP を使用できるインタフェースの定義数は、装置全体で 50 個まで設定できます。

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

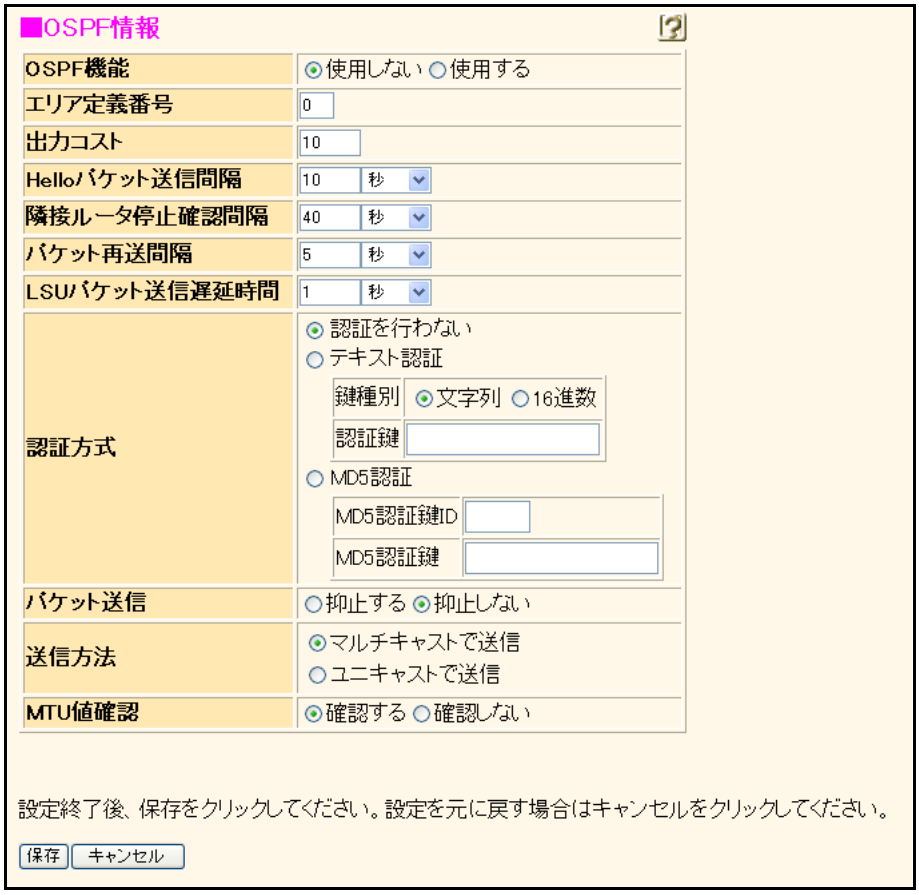
RIP 送信時に加算するメトリック値を選択します。

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。

11.1.4.3 OSPF 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［OSPF 情報］



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、装置全体で 50 個まで設定できます。

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薦めします。通常は “40 秒 ” を指定します。

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

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

パケット再送間隔

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

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
3 ～ 65535 秒

LSU パケット送信遅延時間

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

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

LSA は、生成されてから 1 時間が経過すると破棄されます。LSU 送信遅延時間に 1 時間以上を指定しないでください。正しくルーティングできない場合があります。

認証方式

パケット認証方式を選択します。

鍵種別

テキスト認証で使用する鍵の種別を選択します。

認証鍵

テキスト認証で使用する鍵を指定します。鍵種別が “ 文字列 ” 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

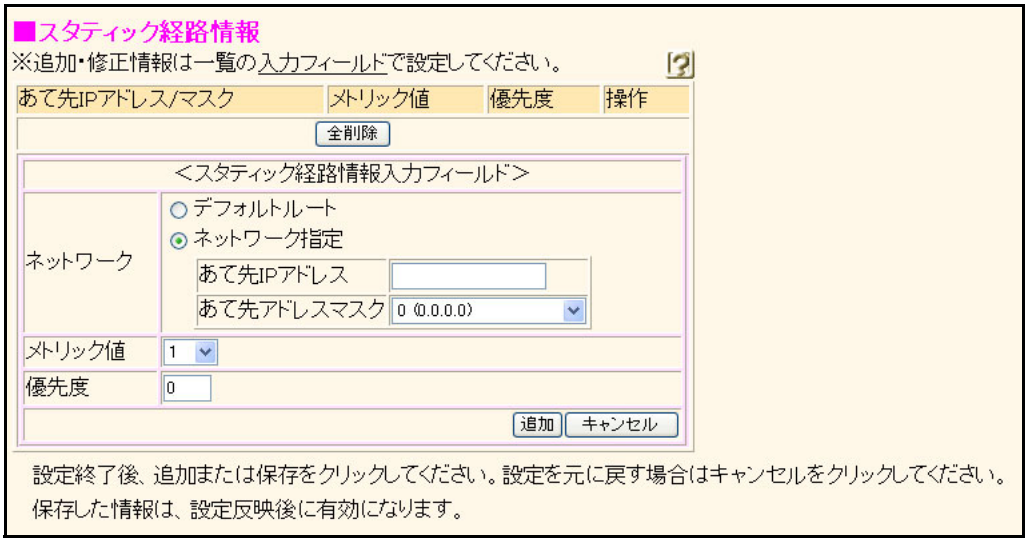
OSPFパケットの送信方法を選択します。OSPFパケットをマルチキャストで受信できない装置と接続する場合は、“ユニキャストで送信”を選択します。

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。

11.1.4.4 スタティック経路情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［スタティック経路情報］



現在、設定されているスタティック経路の情報の定義が表示されています。スタティック経路の定義数は、装置全体で 128 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。

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。

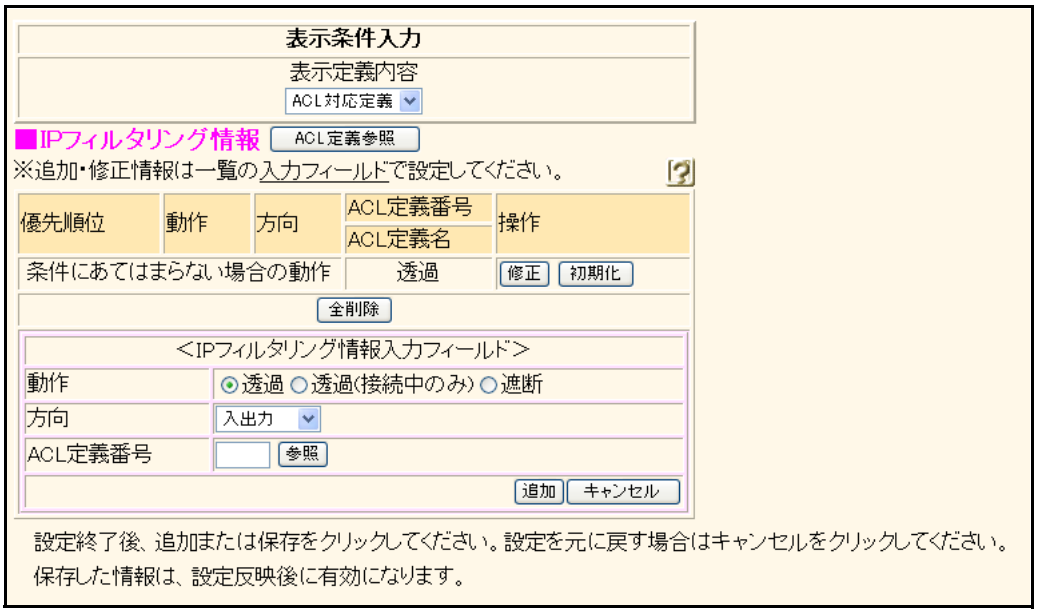
こんな事に気をつけて

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。**

11.1.4.5 IP フィルタリング情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［IP フィルタリング情報］



現在、設定されている IP 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 から順に行います。IP フィルタリングの定義数は、64 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。

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

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

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

動作

IP フィルタリングの動作を以下の 3 つから選択します。

- 透過
  条件と一致する場合にパケットを透過します。
- 透過（接続中のみ）
  条件と一致する場合に、回線が接続しているときはパケット透過し、切断しているときは遮断します。
- 遮断
  条件と一致する場合にパケットを遮断します。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
  入力パケットだけをフィルタリングする対象とします。
- 出力のみ
  出力パケットだけをフィルタリングする対象とします。
- リバース
  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
  - 送信元IPアドレス／アドレスマスクとあて先IPアドレス／アドレスマスク
  - 送信元ポート番号とあて先ポート番号

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

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

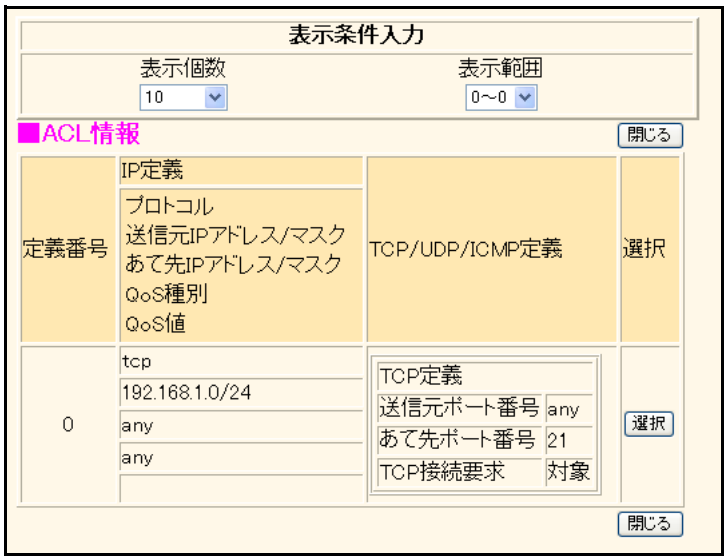
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［IP フィルタリング情報］→「ACL 定義番号の［参照］」



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

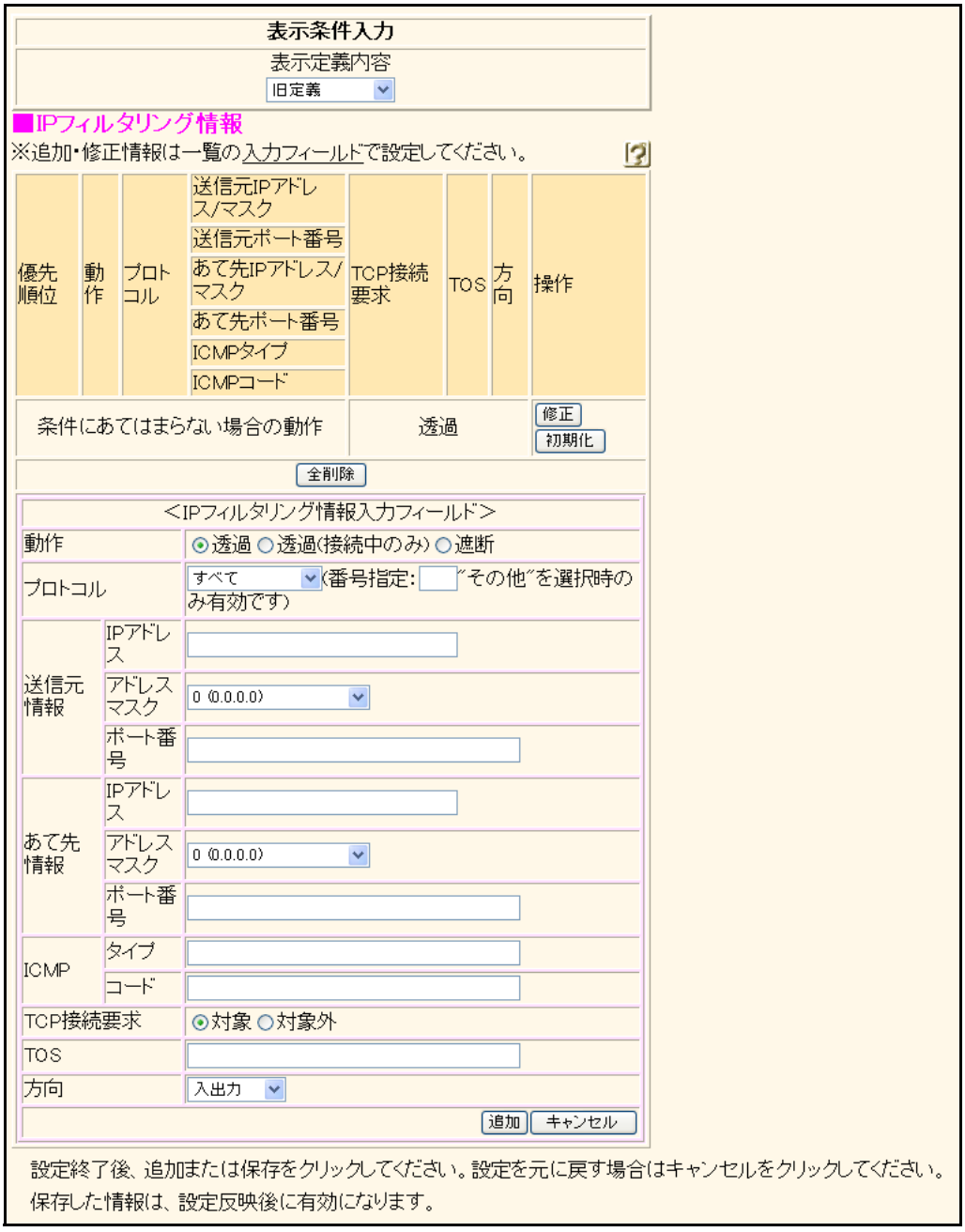
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

11.1.4.5.1 IP フィルタリング情報（旧定義）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［IP フィルタリング情報］→「表示条件入力（旧定義）」



表示条件入力に、“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

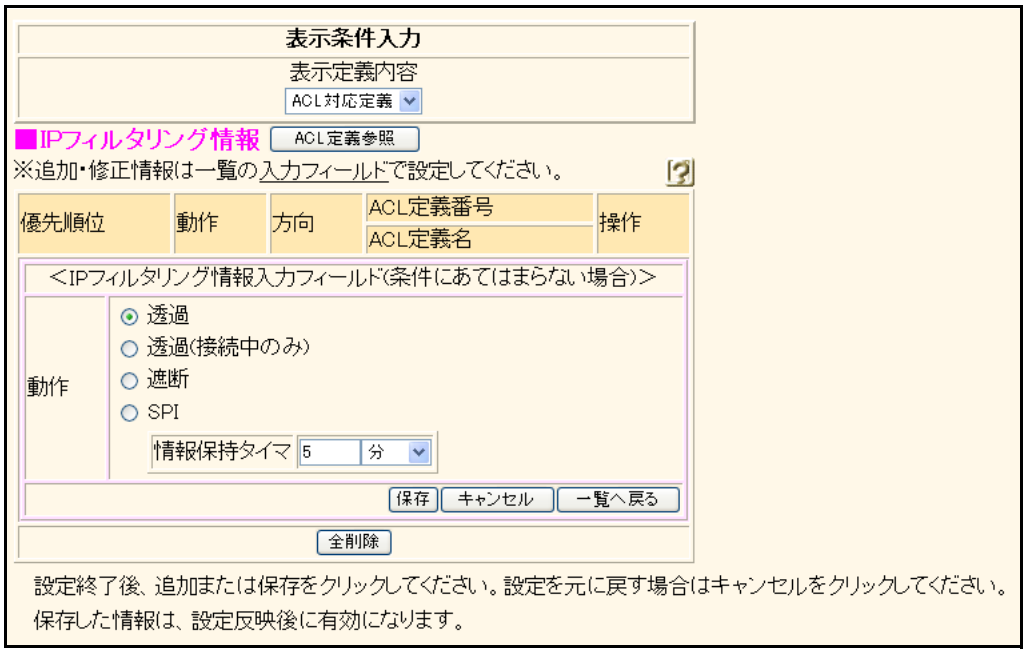
フィルタリングする方向を以下の4つから選択します。

- 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。

11.1.4.5.2 IP フィルタリング情報（条件にあてはまらない場合の動作）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［IP フィルタリング情報］→「条件にあてはまらない場合の動作」［修正］



「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。

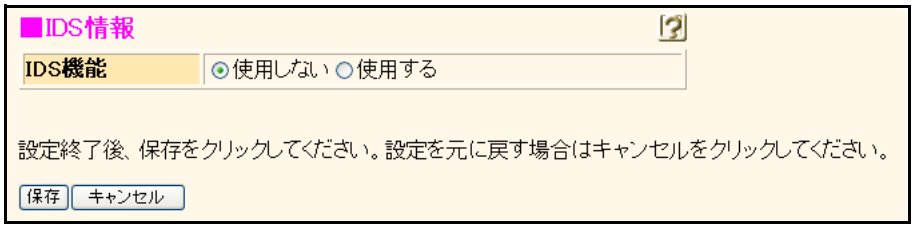
- 透過
  IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 透過（接続中のみ）
  IP フィルタリング定義のどれにも一致しない場合に、回線が接続しているときはパケットを透過し、切断しているときは遮断します。
- 遮断
  IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
  IP フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過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

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。

11.1.4.6 IDS 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［IDS 情報］

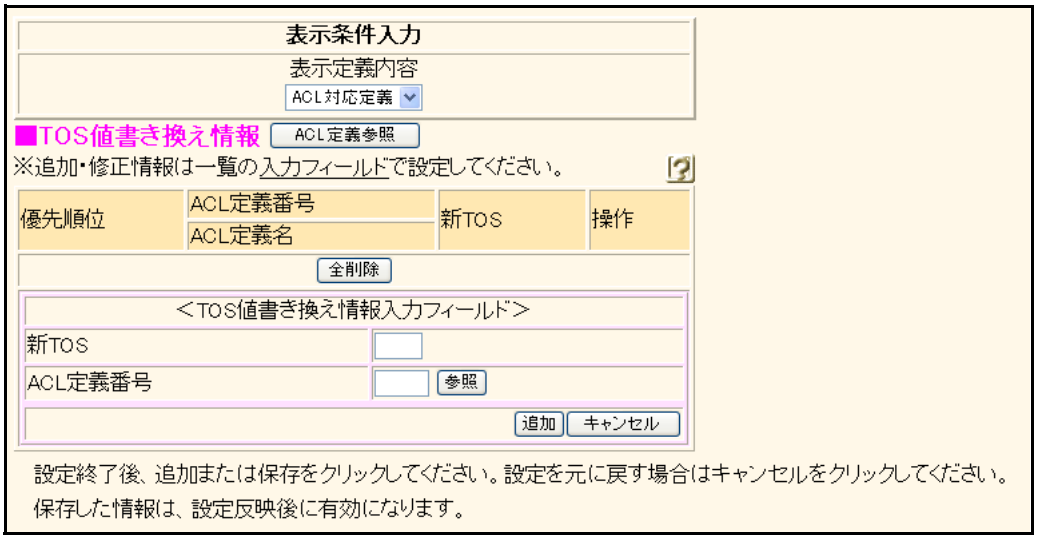


IDS 機能

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

11.1.4.7 TOS 値書き換え情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［TOS 値書き換え情報］



現在、設定されている TOS 値書き換え情報の定義が表示されています。処理は優先順位 1 から順に行います。TOS 値書き換えの定義数は、32 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。

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 TOS

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

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

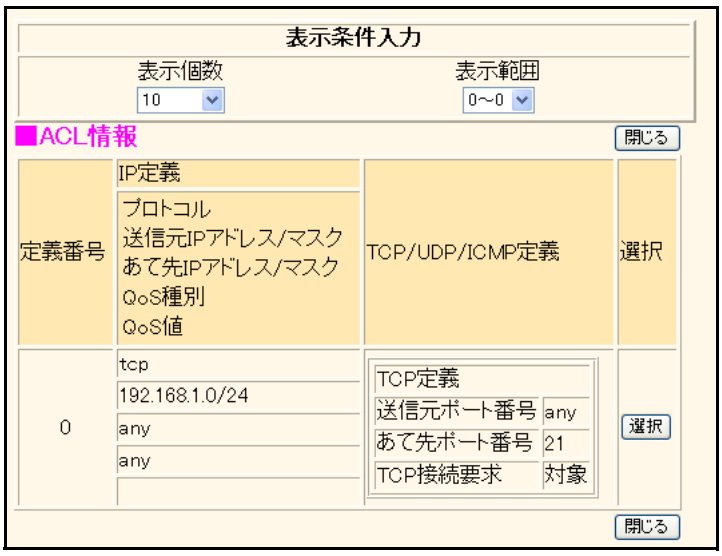
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［TOS 値書き換え情報］→「ACL 定義番号の［参照］」



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

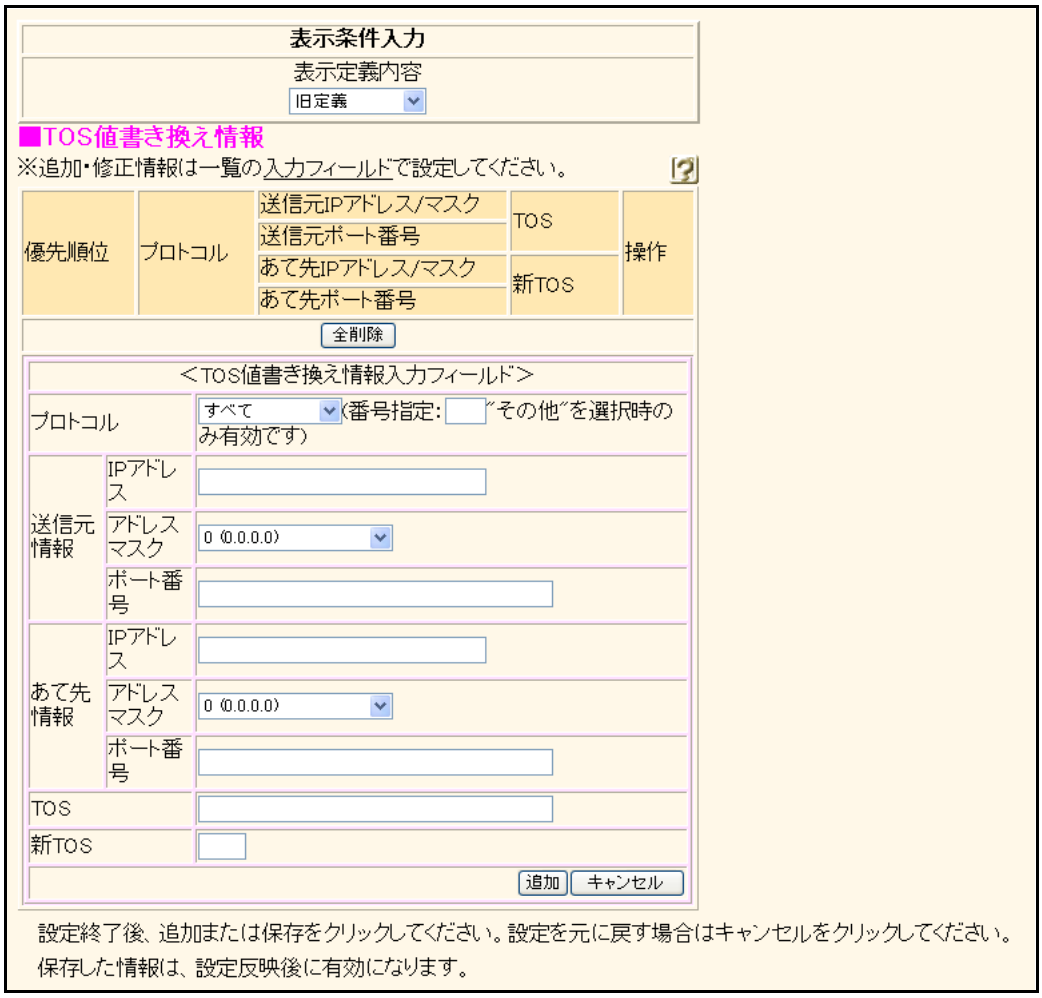
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

11.1.4.7.1 TOS 値書き換え情報（旧定義）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［TOS 値書き換え情報］→「表示条件入力（旧定義）」



表示条件入力に、“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

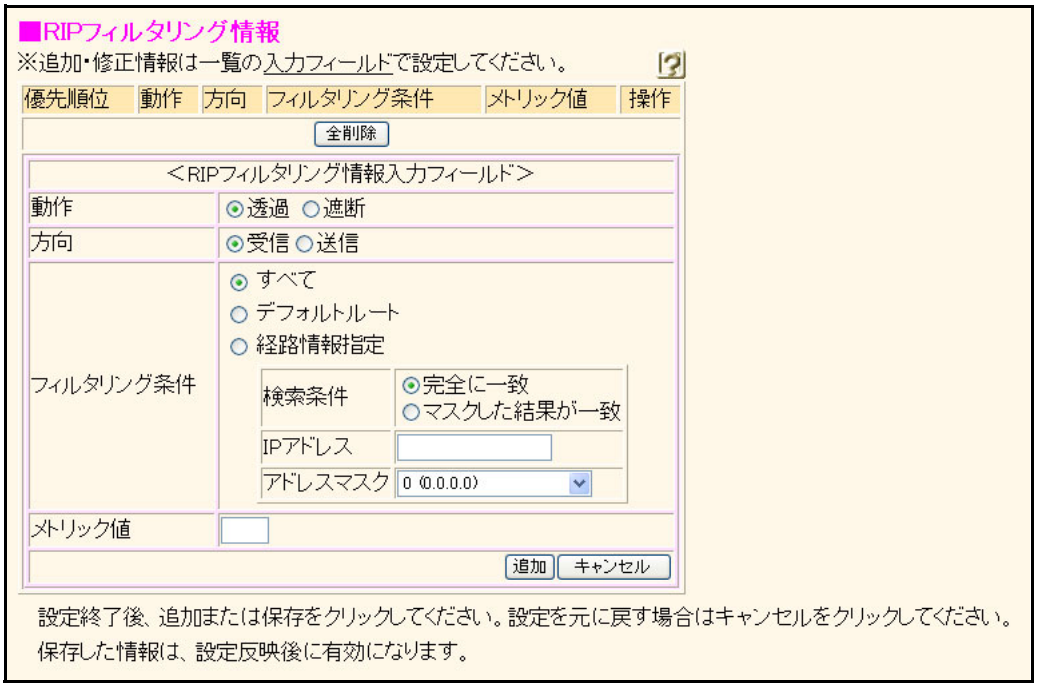
TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0 ～ ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、“,” で区切ります。範囲指定の場合は、“-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値が書き換えの対象となります。

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。

11.1.4.8 RIP フィルタリング情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］
→［RIP フィルタリング情報］



現在、設定されている RIP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、装置全体で 200 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。

優先順位の高い定義から順に条件を参照し、一致した経路情報があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、（送信方向／受信方向の）すべての条件に一致しない RIP 経路情報は遮断されます。

動作

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

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

方向

フィルタリング条件に該当するかどうかをチェックします。RIP パケット受信時にチェックするか、送信時にチェックするかを選択します。

フィルタリング条件

フィルタリング条件を選択します。

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

検索条件

検索条件を選択します。

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

メトリック値

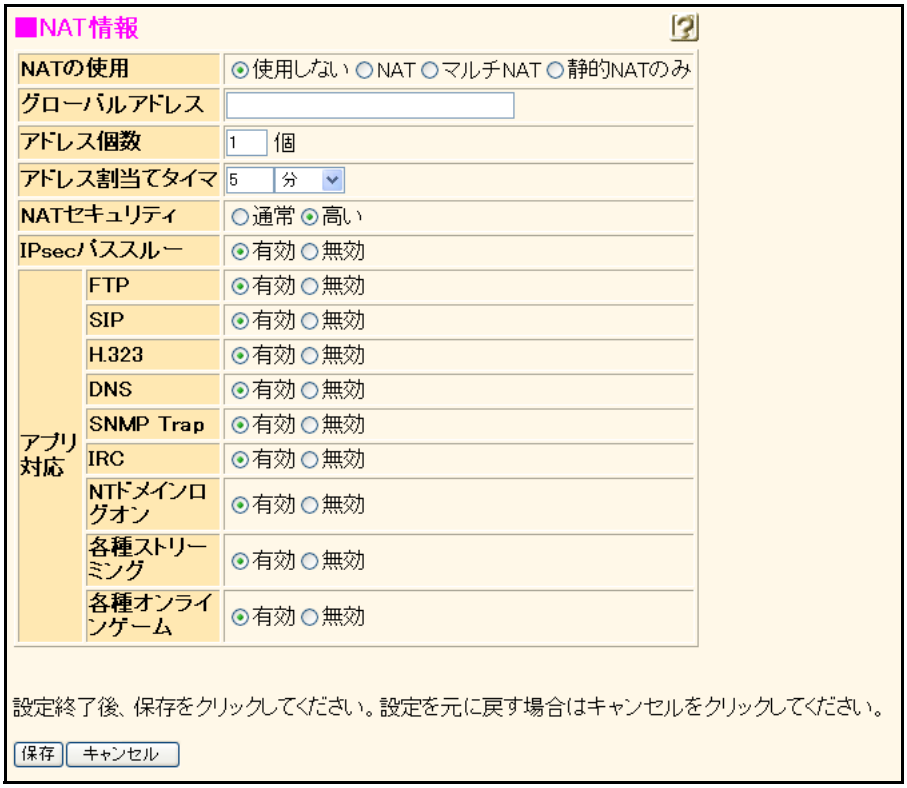
フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

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

11.1.4.9 NAT情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP関連］→［NAT情報］



NAT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。

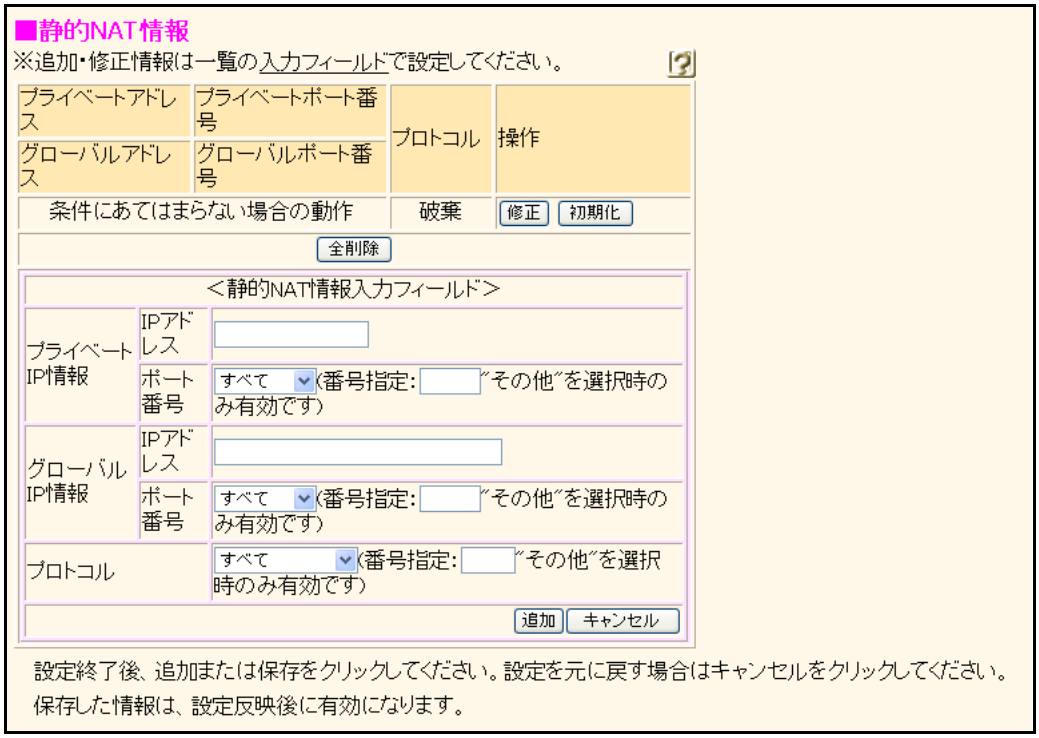
アプリ対応

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

11.1.4.10 静的 NAT 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［静的 NAT 情報］



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、装置全体で 64 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。

プライベート IP 情報

IP アドレス

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

ポート番号

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

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

例）プライベートポート番号：1000
　　グローバルポート番号：10000-11000
　　NAT 変換後
　　プライベートポート番号：1000-2000

グローバル IP 情報

IP アドレス

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

IP アドレスを指定する場合は、"-" で区切った 1 組の範囲を指定します。

ポート番号

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

プロトコル

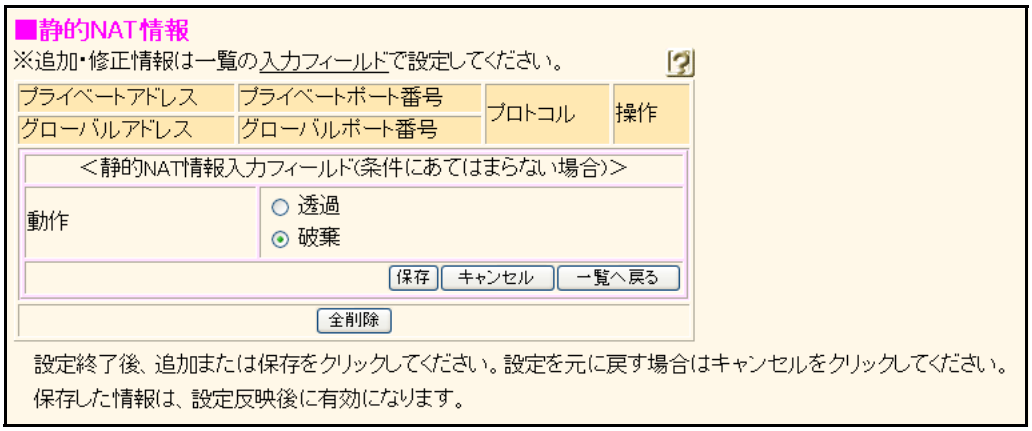
固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

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

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

11.1.4.10.1 静的NAT情報（条件にあてはまらない場合の動作）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP関連］→［静的NAT情報］→「条件にあてはまらない場合の動作」［修正］



「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。

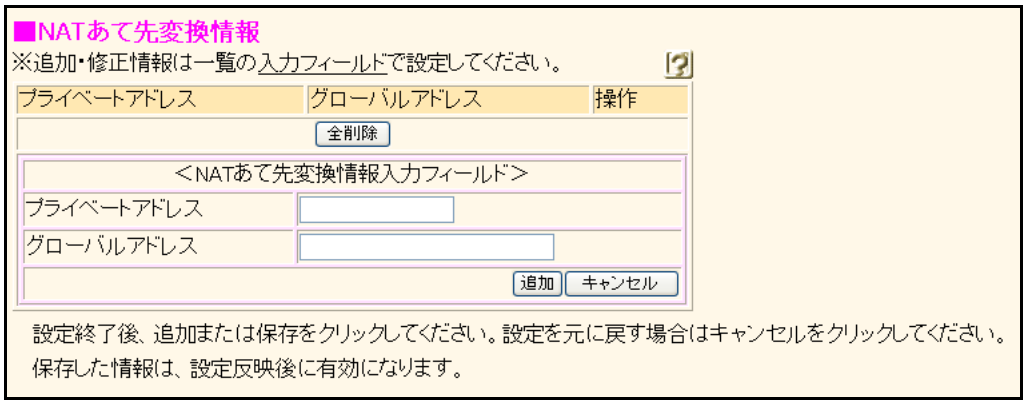
動作

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。

11.1.4.11 NATあて先変換情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP関連］→［NATあて先変換情報］



現在、設定されているNATあて先変換情報の定義が表示されています。NATあて先変換の定義数は、装置全体で64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。

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。

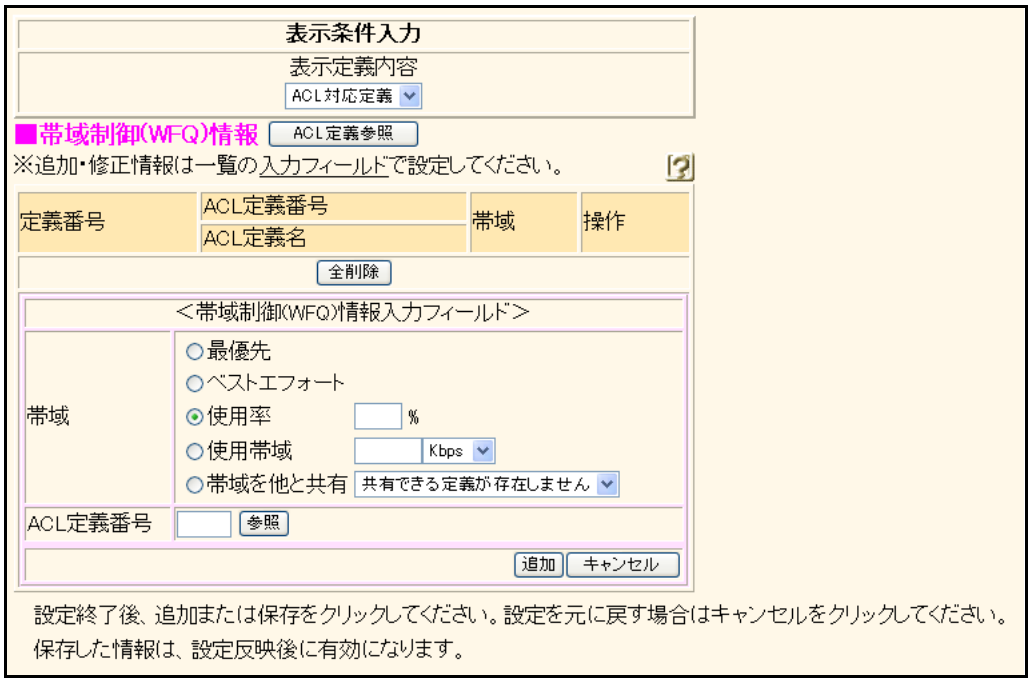
例）プライベートアドレス：192.168.1.100
　　グローバルアドレス：172.16.1.100-172.16.1.200
　　NATあて先変換後
　　プライベートアドレス：192.168.1.100-192.168.1.200

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。

11.1.4.12 帯域制御（WFQ）情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［帯域制御（WFQ）情報］



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、装置全体で 64 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。

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

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

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

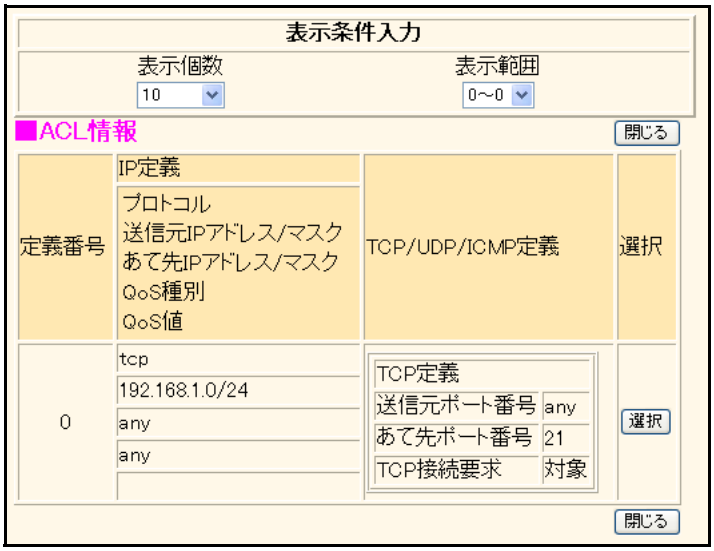
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［帯域制御（WFQ）情報］→「ACL 定義番号の［参照］」



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

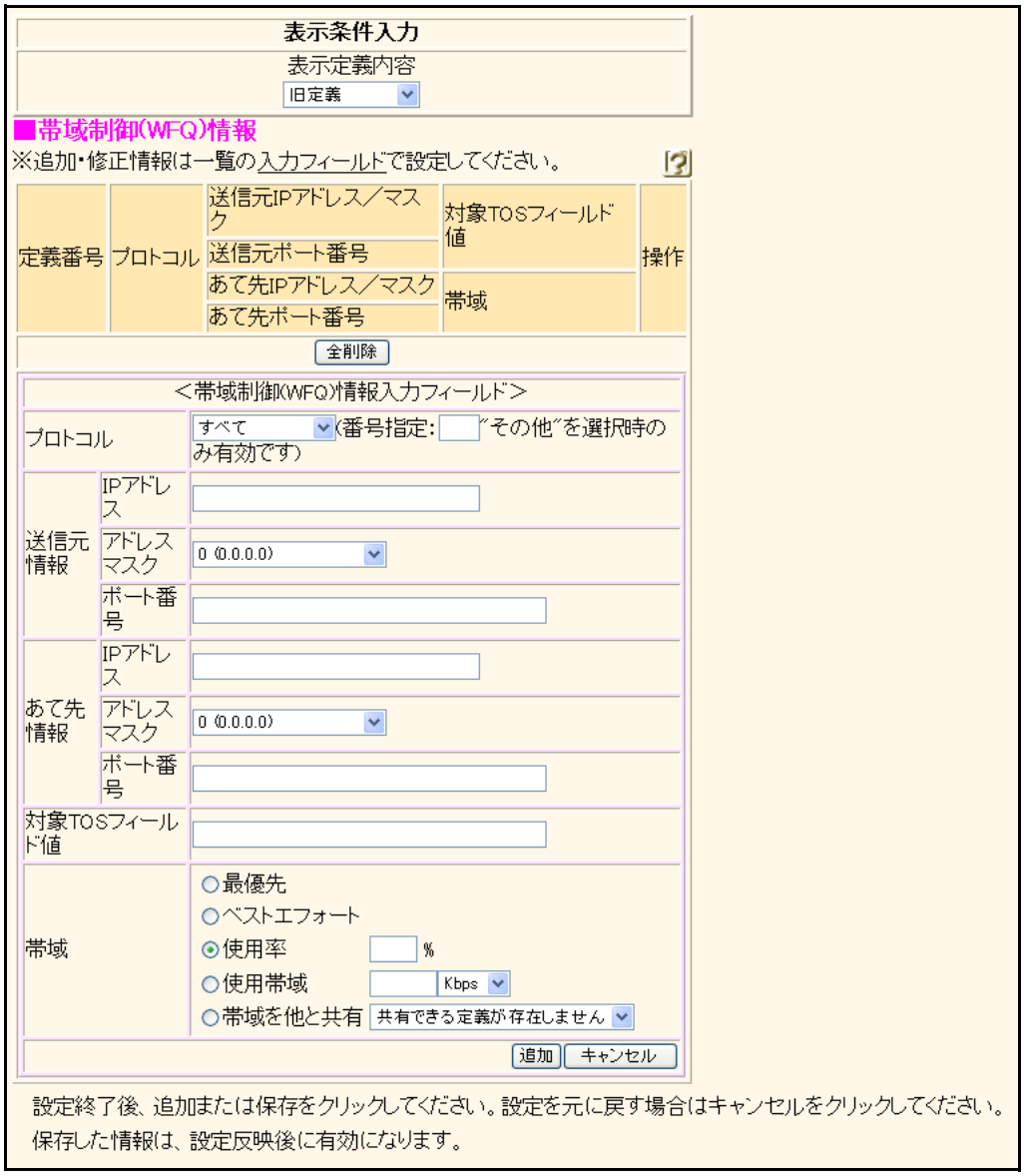
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

11.1.4.12.1 帯域制御（WFQ）情報（旧定義）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［帯域制御（WFQ）情報］→「表示条件入力（旧定義）」



表示条件入力に、" 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。

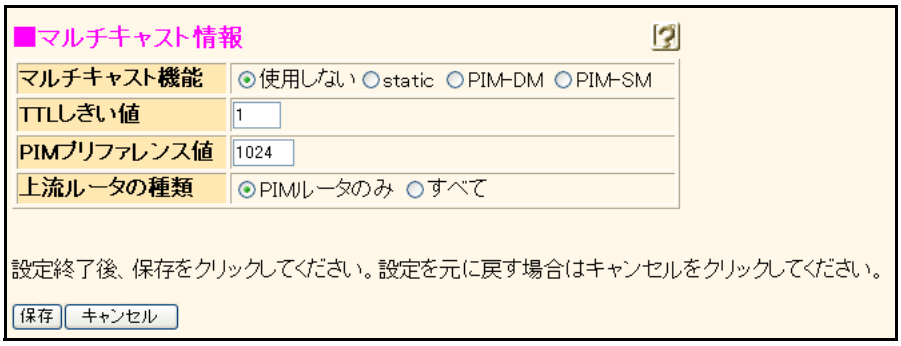
- 最優先
  最優先データとして扱われます。
- ベストエフォート
  非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
  割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
  1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
  ほ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

11.1.4.13 マルチキャスト情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［マルチキャスト情報］



マルチキャスト機能

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、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。

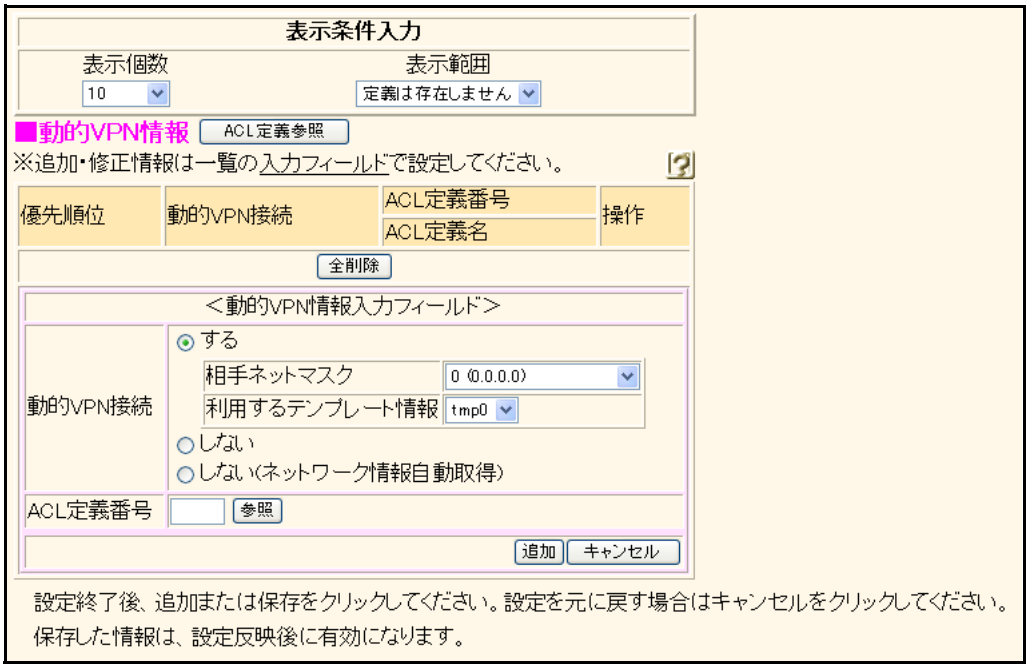
上流ルータが PIM ルータでない場合（マルチキャストパケットをスタティック経路によって転送するルータであった場合）に転送を許可する場合は、“ すべて ” を選択します。

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。

11.1.4.14 動的VPN情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP関連］→［動的VPN情報］



現在、設定されている動的VPN接続契機パケットの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、装置全体で432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。

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

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動的VPN接続契機パケットの検出を行います。ただし、分割されたパケットに対しては正しく行えません。

動的VPN接続

動的VPN接続を行う場合は、“する”を選択します。

“しない（ネットワーク情報自動取得）”は、相手情報に接続先情報の動的VPN接続定義が行われている必要があります。また、相手情報ごとに1つしか選択できません。

相手ネットマスク

動的VPN接続を開始する場合に、相手を識別するための情報として相手ネットマスクを0～32から選択します。

利用するテンプレート情報

動的VPN接続に利用するテンプレート情報を選択します。

ACL定義番号

［参照］ボタンをクリックして、ACL定義番号を指定します。

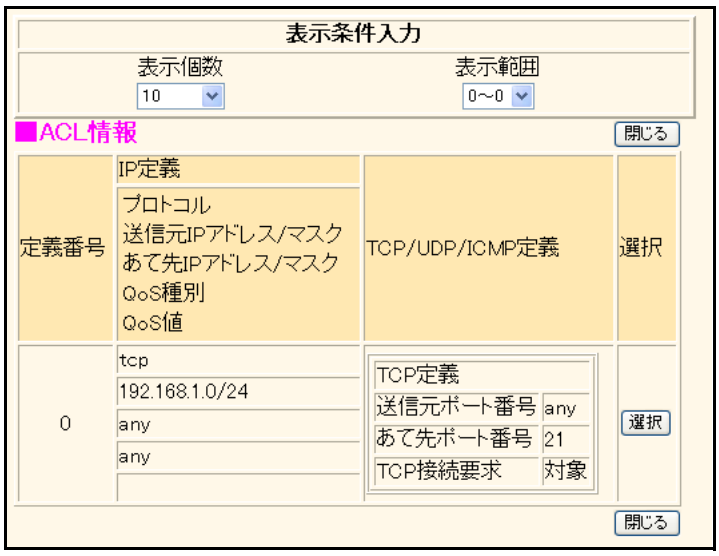
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IP 関連］→［動的 VPN 情報］→「ACL 定義番号の［参照］」



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

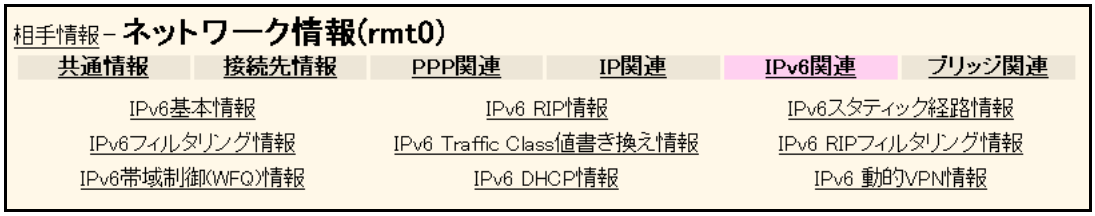
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

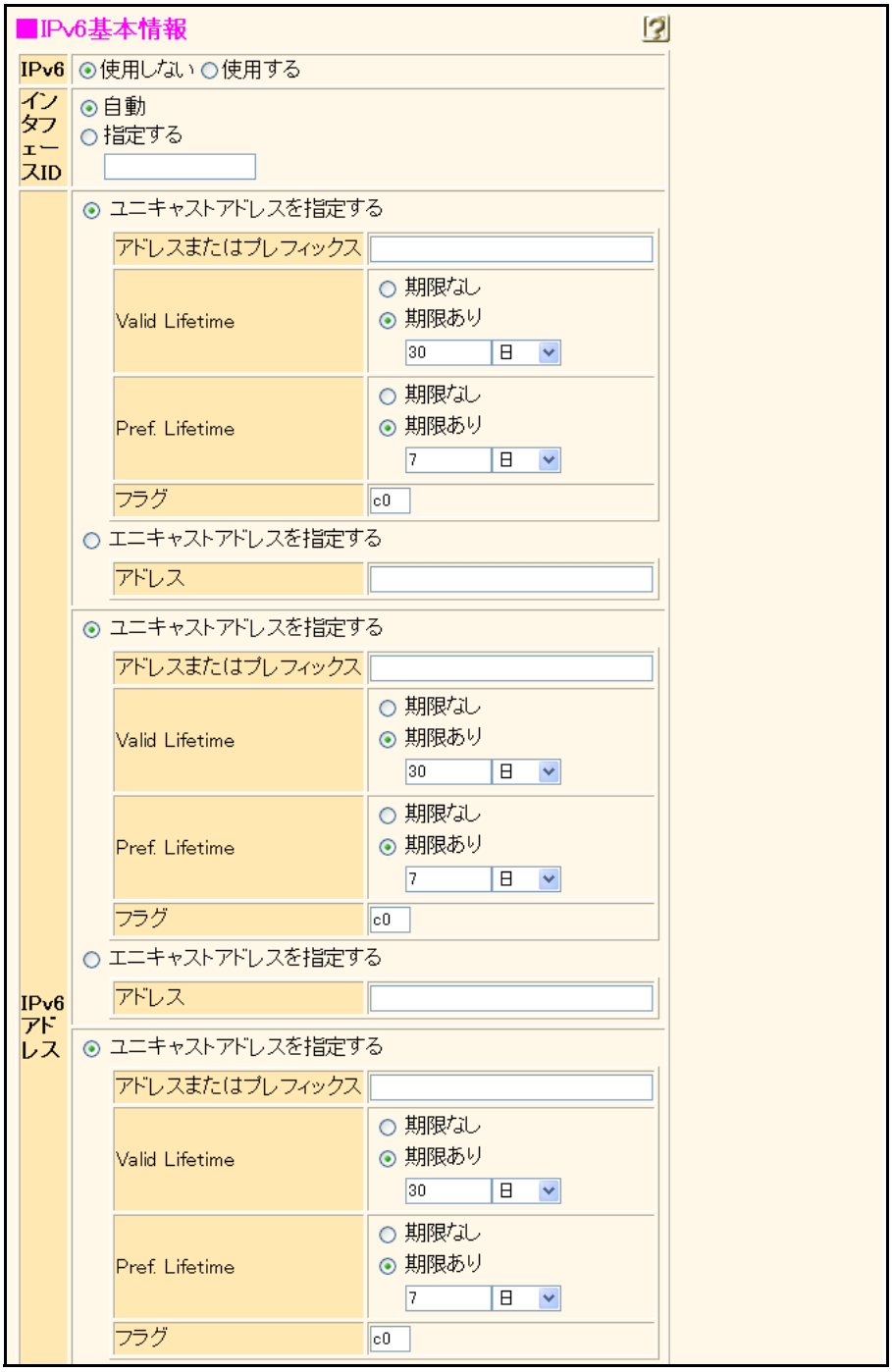
11.1.5　IPv6 関連

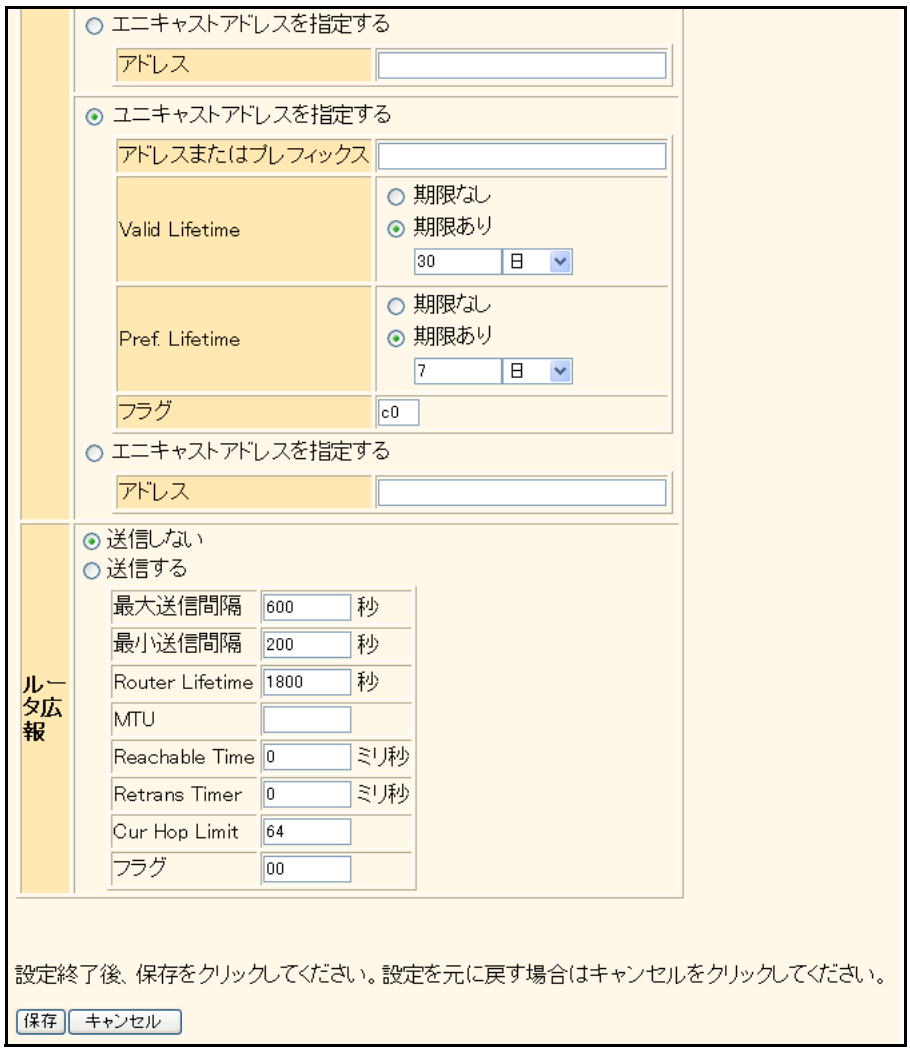
［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］



11.1.5.1　IPv6 基本情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］→［IPv6 基本情報］





IPv6

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

インタフェース ID を設定します。

- 自動
  装置の MAC アドレスから自動生成されるインタフェース ID を使用します。通常は、“ 自動 ” を選択します。
- 指定する
  16 ビットごとに区切り文字（:）を入れて、16 進数を使用して 16 桁でインタフェース 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ユニキャストアドレスまたはエニキャストアドレスを 4 個まで設定できます。

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

アドレスまたはプレフィックス

本装置のLAN側のIPv6アドレスを標準的なIPv6アドレス表記方式で指定します。本装置ではプレフィックス長は64に固定されます。インタフェース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

IPv6アドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCPクライアントが取得したValid Lifetimeと比較して短い方が有効になります。

Pref. Lifetime

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

有効範囲）
0～365日
0～8760時間
0～525600分
0～31536000秒

IPv6アドレスにIPv6 DHCPクライアントが取得したプレフィックスを使用する指定をした場合は、IPv6 DHCPクライアントが取得したPreferred Lifetimeと比較して短い方が有効になります。

フラグ

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

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

通常は“c0”を指定します。

アドレス

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

ルータ広報

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

最大送信間隔

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

有効範囲）4～1800

最小送信間隔

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

有効範囲）3～最大送信間隔の3／4

Router Lifetime

ルータ広報で送信する Router Lifetime を指定します。初期値は 1800 秒です。省略はできません。

有効範囲）0 または最大送信間隔～ 9000

MTU

ルータ広報で送信する MTU option を指定します。省略時は、MTU option を含みません。

有効範囲）1280 ～ 1500

Reachable Time

ルータ広報で送信する Reachable Time を指定します。省略値は 0 ミリ秒です。

有効範囲）0 ～ 3600000

Retrans Timer

ルータ広報で送信する Retrans Timer を指定します。省略値は 0 ミリ秒です。

有効範囲）0 ～ 4294967295

Cur Hop Limit

ルータ広報で送信する Cur Hop Limit を指定します。省略値は 64 です。

有効範囲）0 ～ 255

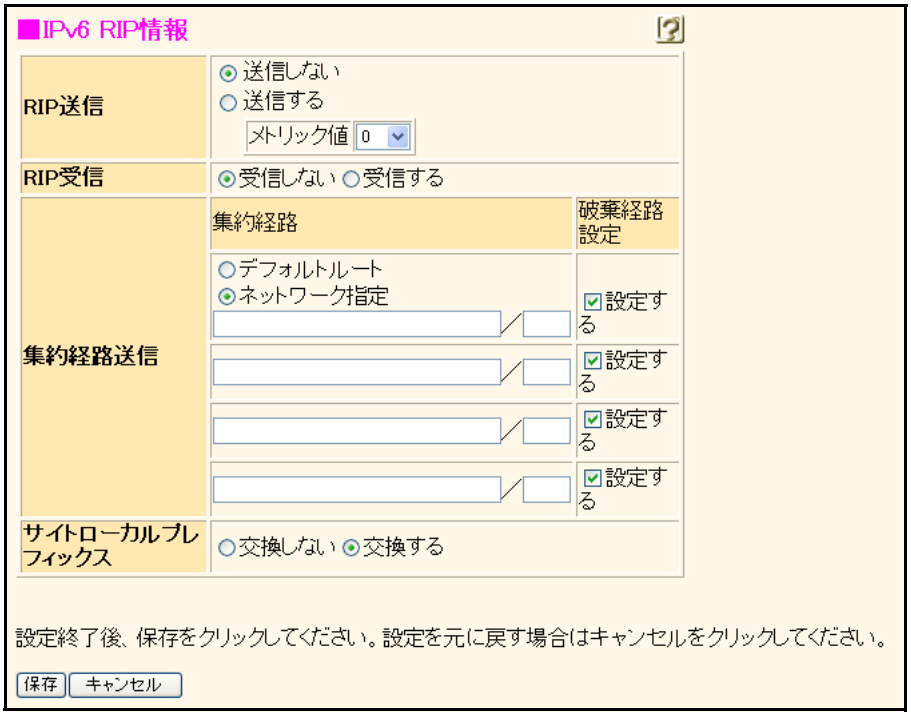
フラグ

ルータ広報の本体部分に設定するフラグフィールドの内容を 16 進数を使用して 2 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

11.1.5.2 IPv6 RIP 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］→［IPv6 RIP 情報］



RIP を使用できるインタフェースの定義数は、装置全体で 58 個まで設定できます。

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。

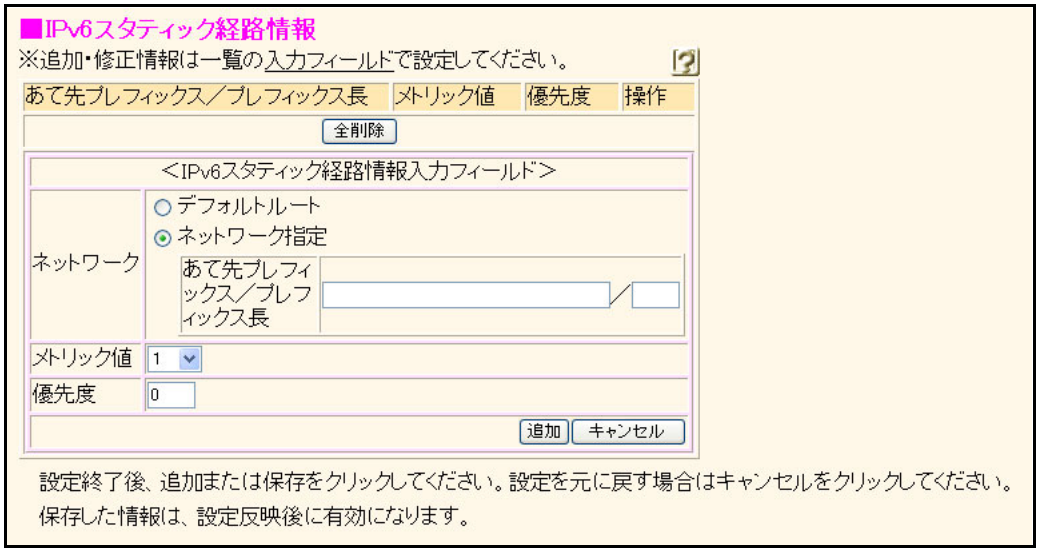
チェック時は、集約経路情報と同じあて先の経路情報が破棄経路としてルーティングテーブルに設定されます。

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。

11.1.5.3 IPv6 スタティック経路情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］→［IPv6 スタティック経路情報］



現在、設定されている IPv6 スタティック経路情報の定義が表示されています。IPv6 スタティック経路の定義数は、装置全体で 128 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。

IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に 1 つしか設定できません。

ネットワーク

“デフォルトルート”または“ネットワーク指定”を選択します。“ネットワーク指定”を選択した場合は、あて先プレフィックスとプレフィックス長を指定します。あて先プレフィックスにリンクローカルアドレスは指定できません。なお、あて先プレフィックス／プレフィックス長に ::/0 を設定した場合、“デフォルトルート”を指定したものとして動作します。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1 ～ 15 から選択します。RIP に再配布したときは、設定した RIP メトリック値 +1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10 進数を使用して 0 ～ 254 の範囲で指定します。省略時は、0 が設定されます。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

プロトコル	優先度
RIP	120
DNS	15
DHCP	10

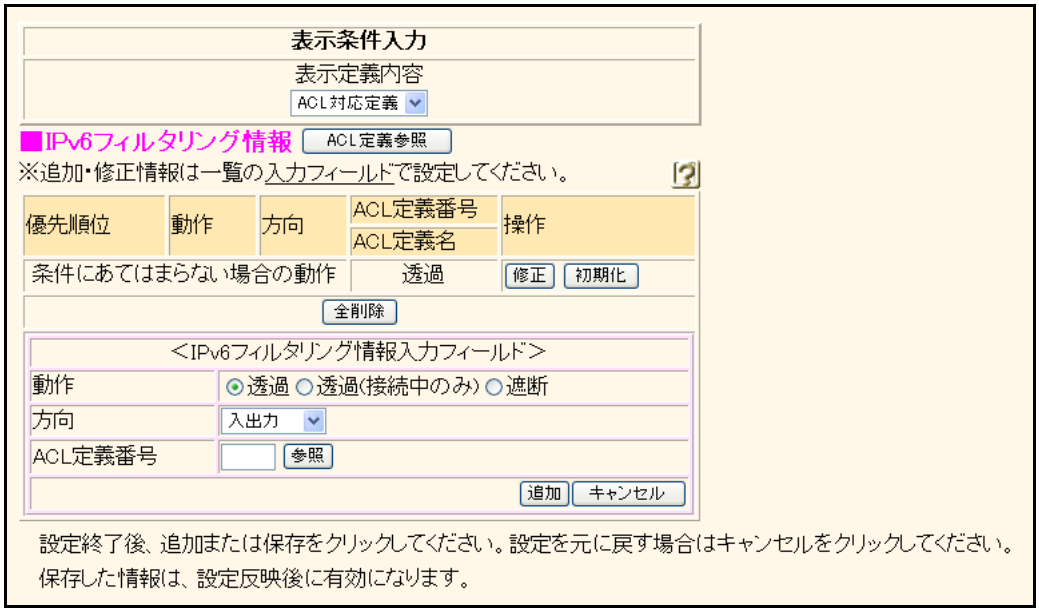
こんな事に気をつけて

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。**

11.1.5.4 IPv6 フィルタリング情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 フィルタリング情報］



現在、設定されている IPv6 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 から順に行います。IPv6 フィルタリングの定義数は、64 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。

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。

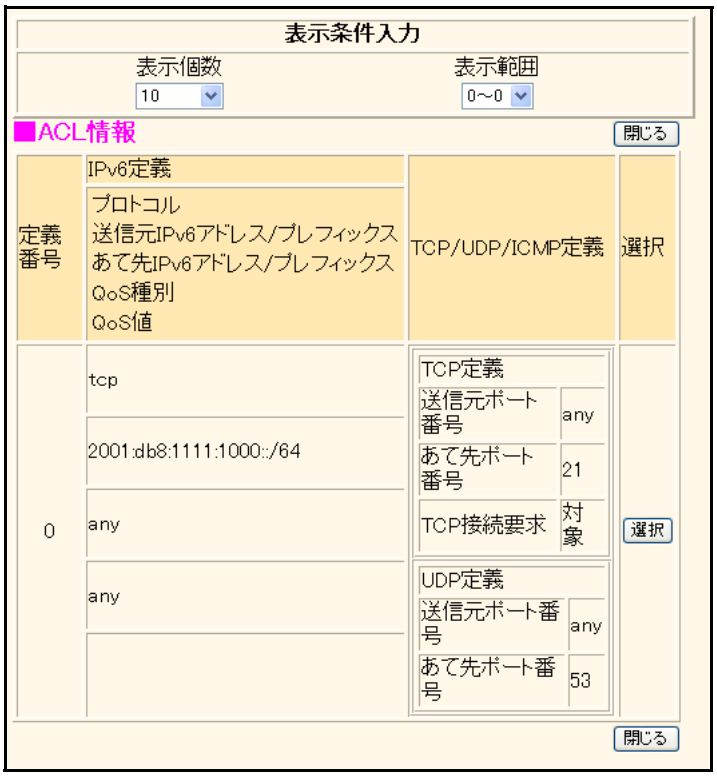
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 フィルタリング情報］→「ACL 定義番号の［参照］」



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

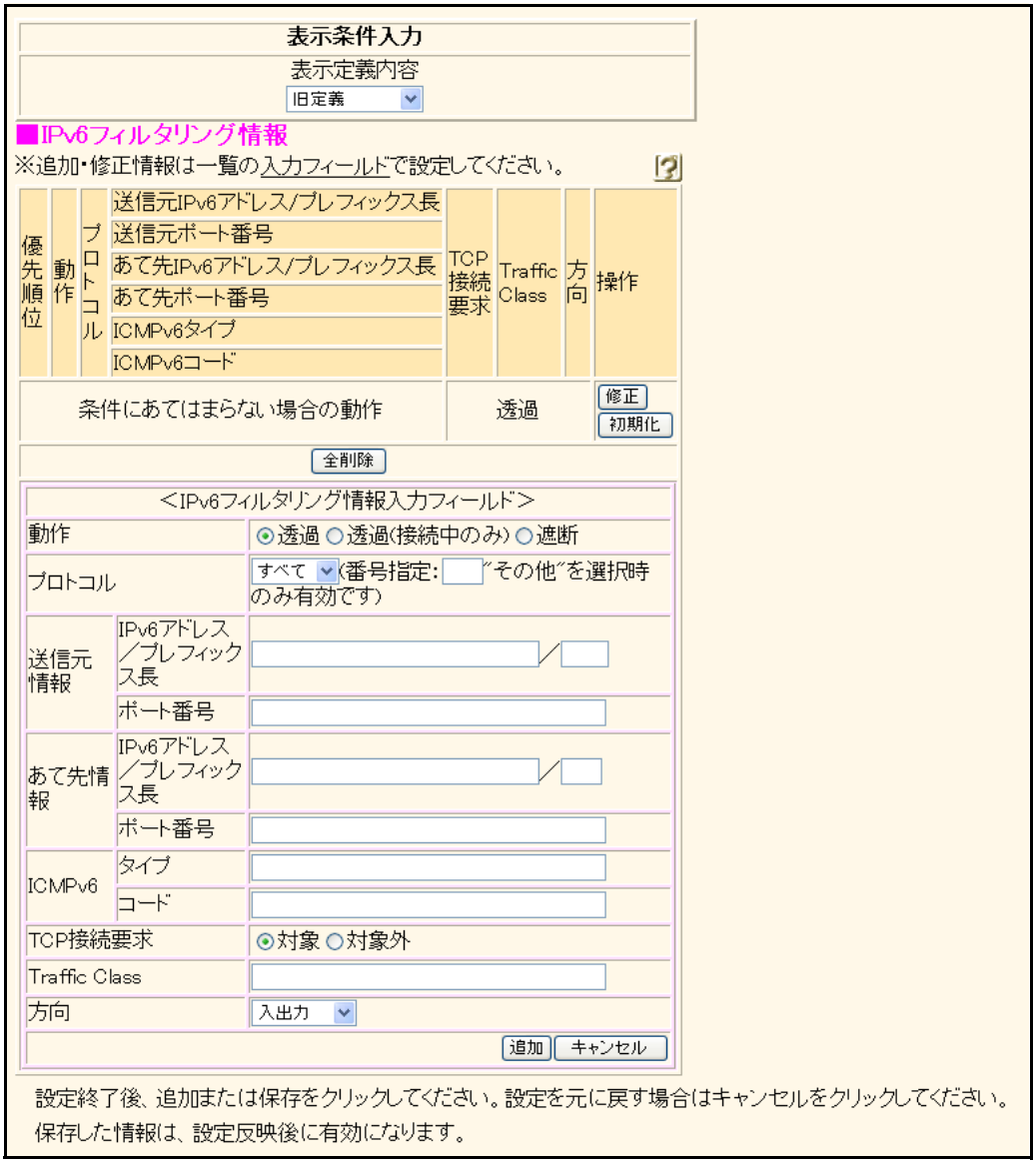
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 フィルタリング情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 フィルタリング情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

11.1.5.4.1 IPv6 フィルタリング情報（旧定義）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 フィルタリング情報］→「表示条件入力（旧定義）」



表示条件入力に、" 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

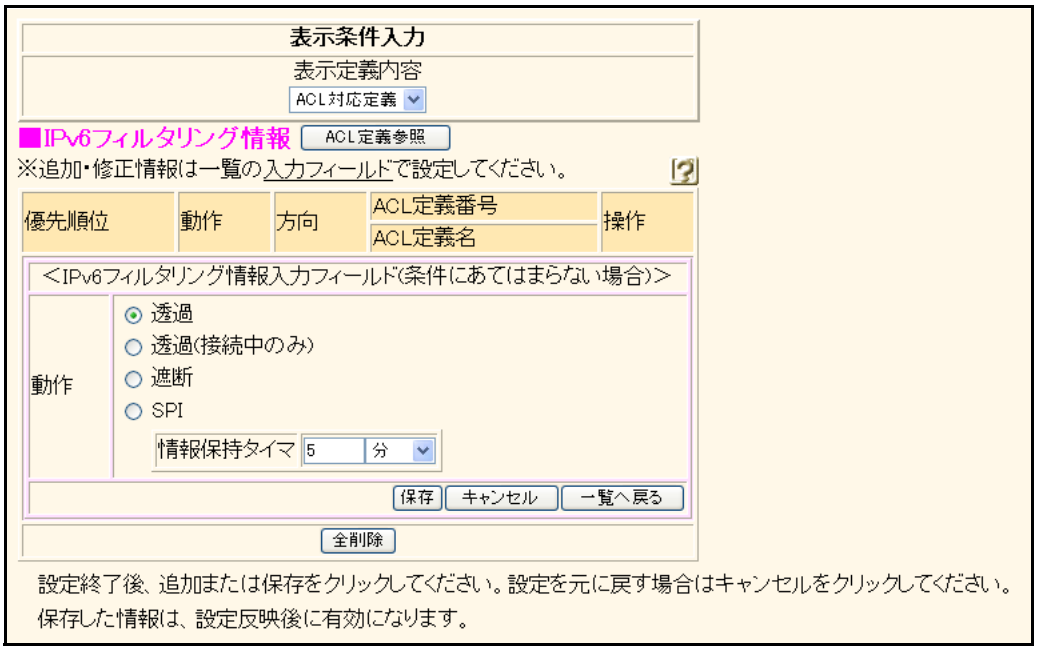
フィルタリングする方向を選択します。

- 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。

11.1.5.4.2 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］　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］



「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。

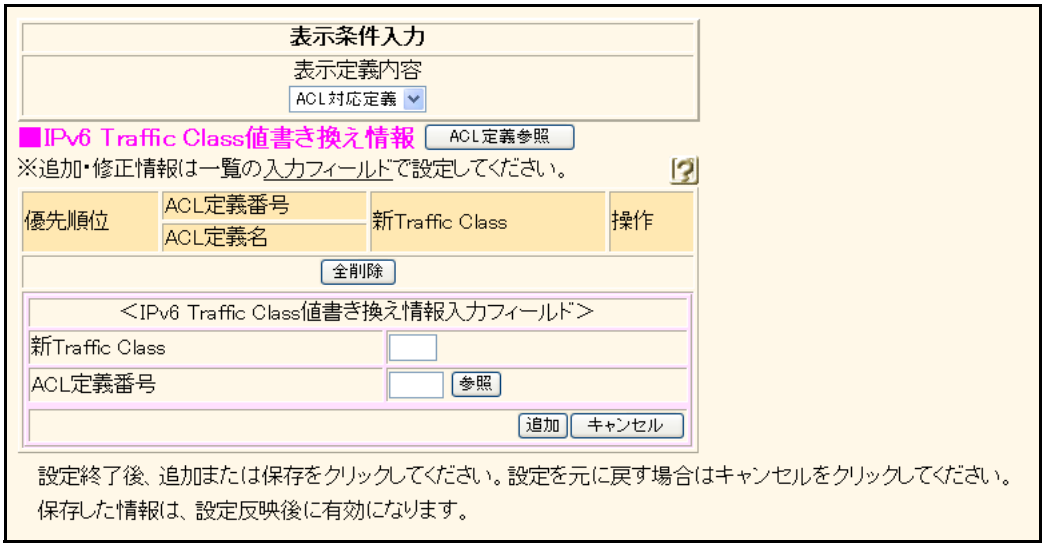
- 透過
  IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 透過（接続中のみ）
  条件と一致する場合に、回線が接続されていればパケットを透過し、切断されていれば遮断します。
- 遮断
  IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
  IPv6 フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

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。

11.1.5.5 IPv6 Traffic Class 値書き換え情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 Traffic Class 値書き換え情報］



現在、設定されている IPv6 Traffic Class 値書き換え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 Traffic Class 値書き換えの定義数は、32 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。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 Traffic Class

IPv6 パケットに新しく指定する IPv6 Traffic Class 値を 16 進数を使用して、0 ～ ff の範囲で指定します。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

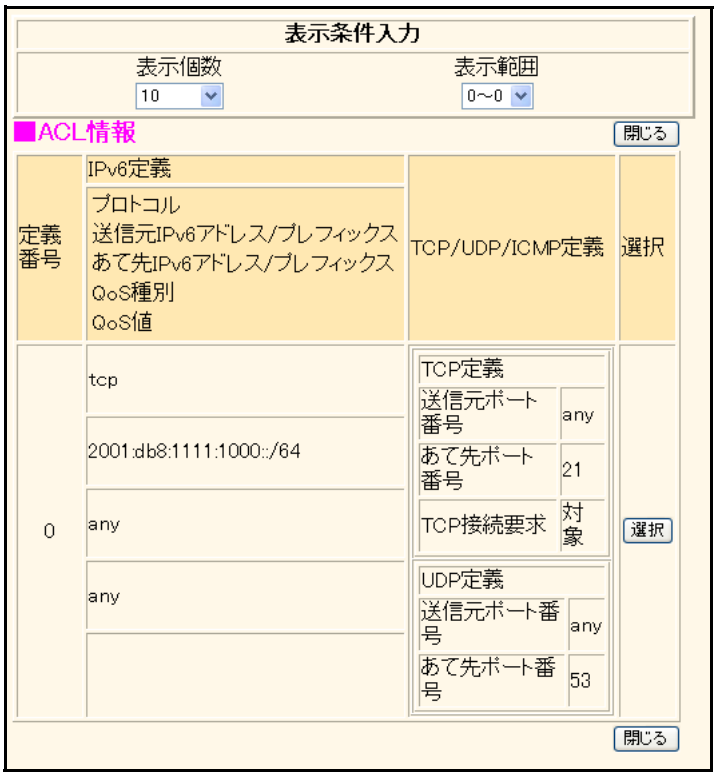
別の画面に「ACL 情報」で設定した ACL 定義が表示されます。ACL 情報の以下の定義を使用します。

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 Traffic Class 値書き換え情報］→「ACL 定義番号の［参照］」



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

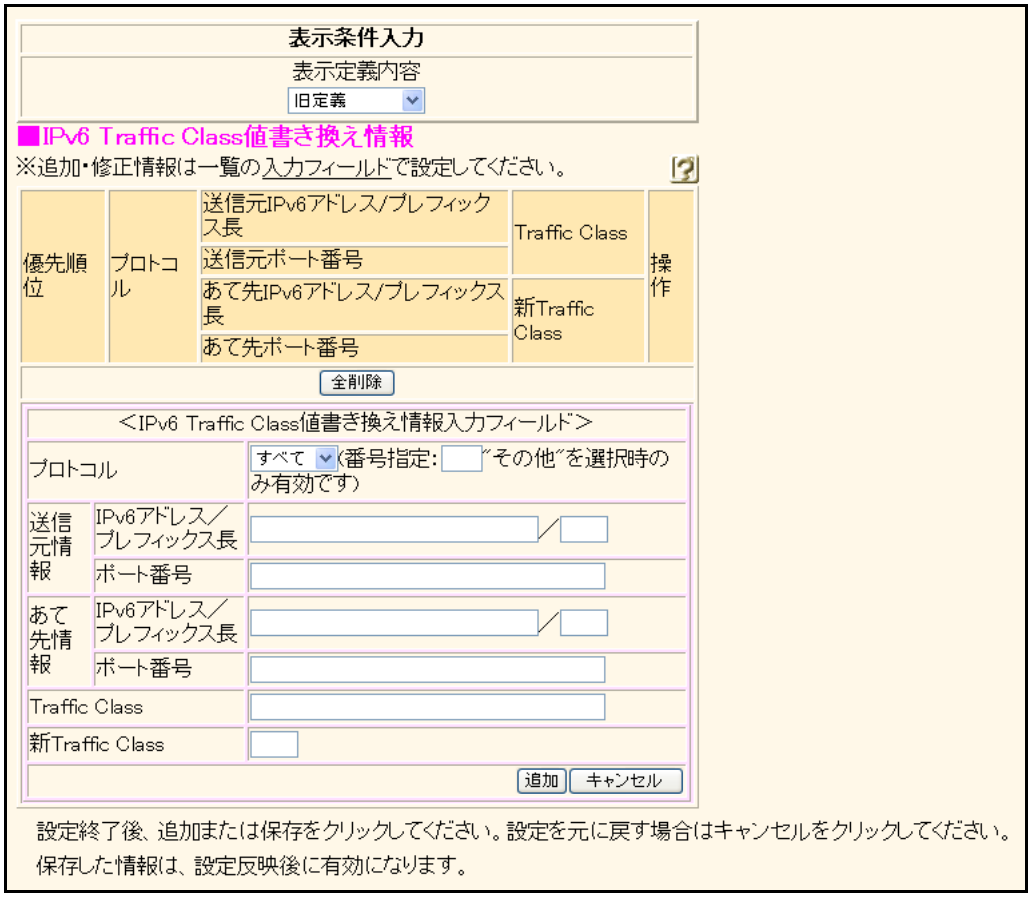
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 Traffic Class 値書き換え情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 Traffic Class 値書き換え情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 Traffic Class 値書き換え情報］→「表示条件入力（旧定義）」



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

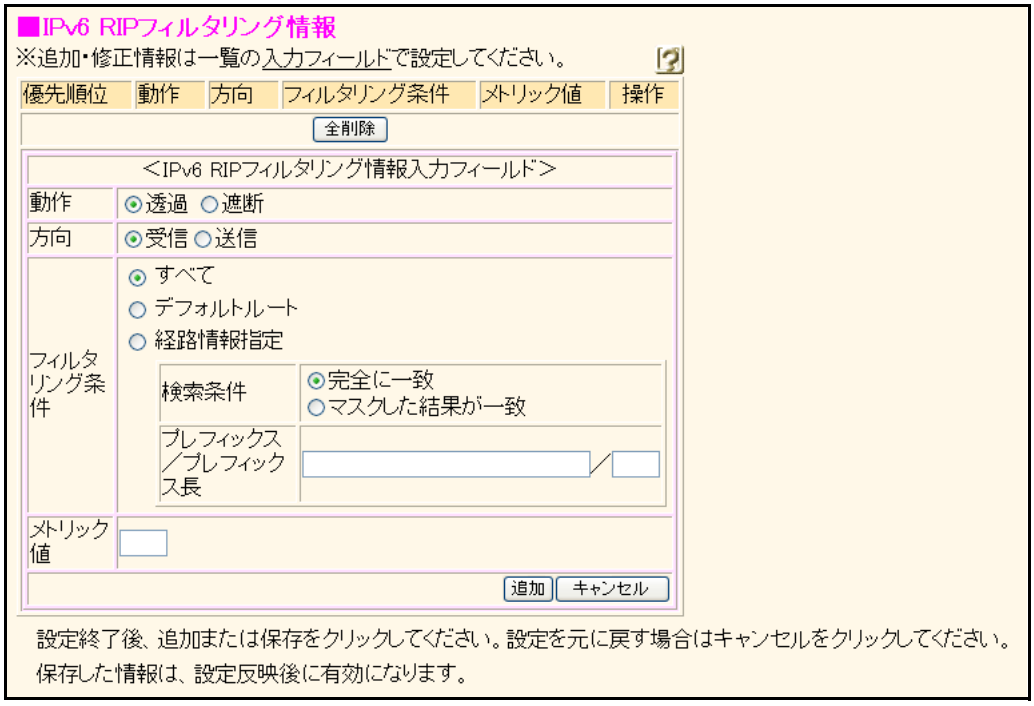
IPv6 Traffic Class 値書き換え条件として IPv6 パケットの IPv6 Traffic Class 値を 16 進数を使用して 0 ～ ff の範囲または “any” で指定します。Traffic Class フィールド値を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての IPv6 Traffic Class 値が書き換えの対象となります。

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。

11.1.5.6 IPv6 RIP フィルタリング情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 RIP フィルタリング情報］



現在、設定されている RIP フィルタリング定義が表示されています。処理は優先順位 1 から順に行われます。RIP フィルタリングの定義数は、装置全体で 200 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。

RIP 受信（送信）時には、優先順位の高い定義から順に受信（送信）方向の条件を参照し、一致した条件があった時点で定義された動作を行います。なお、一致した以降の条件は参照されません。また、受信（送信）方向のすべての条件に一致しない RIP 経路情報は遮断されます。

動作

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

- 透過
  条件と一致した場合に RIP 経路情報を透過します。
- 遮断
  条件と一致した場合に RIP 経路情報を遮断します。

方向

フィルタリングを RIP 受信時に行うか、RIP 送信時に行うかを選択します。

- 受信
  RIP 受信時に、フィルタリングを行います。
- 送信
  RIP 送信時に、フィルタリングを行います。

フィルタリング条件

フィルタリング条件を選択します。

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

検索条件

検索条件を選択します。

- 完全に一致
  指定したプレフィックスとプレフィックス長が完全に一致したRIP経路情報をフィルタリング対象とします。
- マスクした結果が一致
  指定したプレフィックスと、RIP経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、そのRIP経路情報をフィルタリング対象とします。

メトリック値

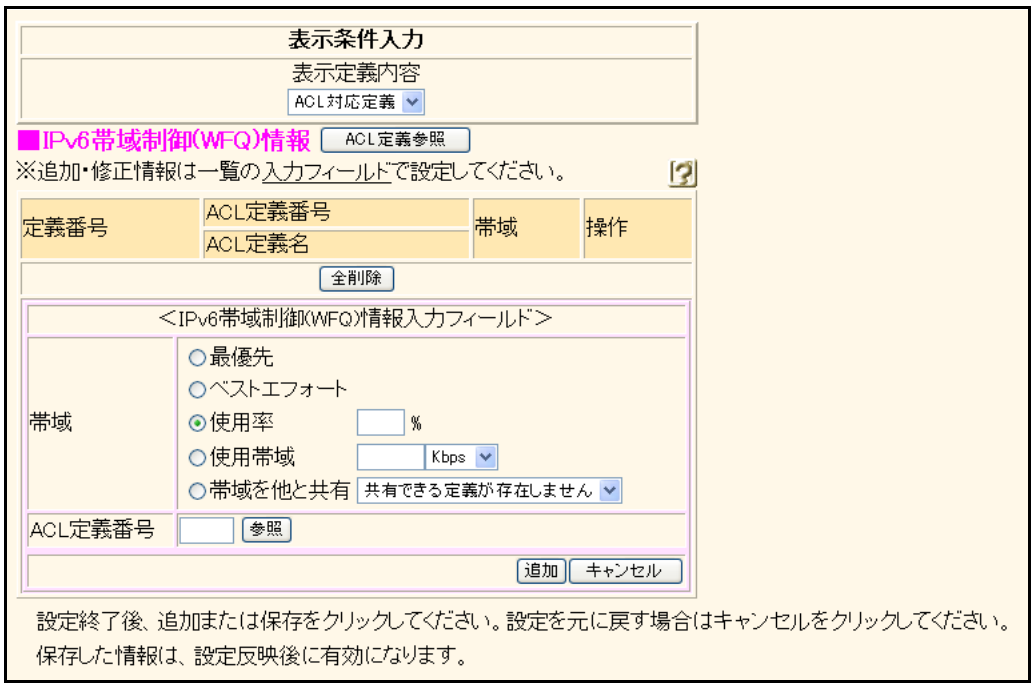
フィルタリング結果で透過になったRIP経路情報のメトリック値を変更できます。送信時のRIP経路にメトリック値を設定した場合、「RIP情報」で設定した加算メトリック値は加算されません。省略または0を指定した場合は、フィルタリングでメトリック値の変更は行いません。

こんな事に気をつけて

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

11.1.5.7 IPv6帯域制御（WFQ）情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6関連］→［IPv6帯域制御（WFQ）情報］



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、64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。
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

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

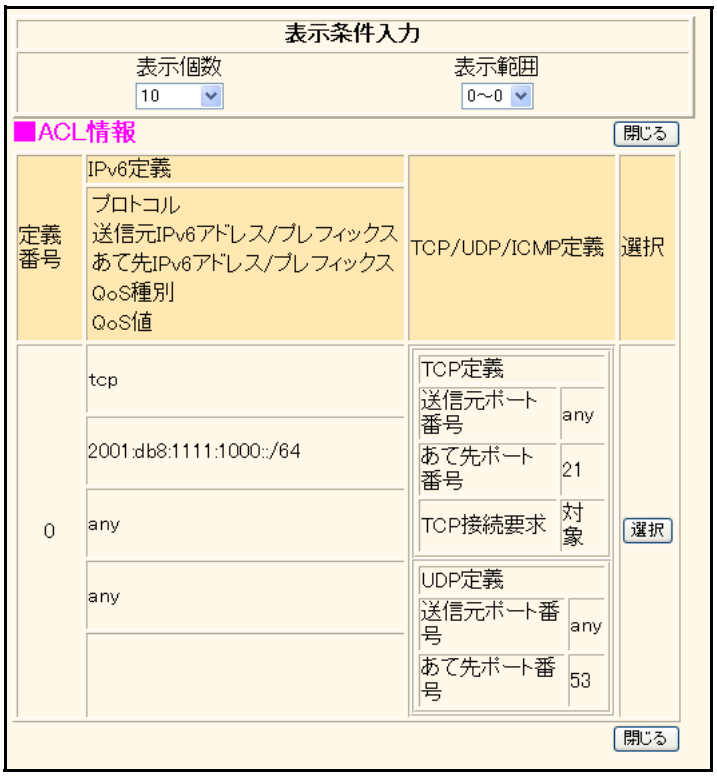
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 帯域制御（WFQ）情報］→「ACL 定義番号の［参照］」



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

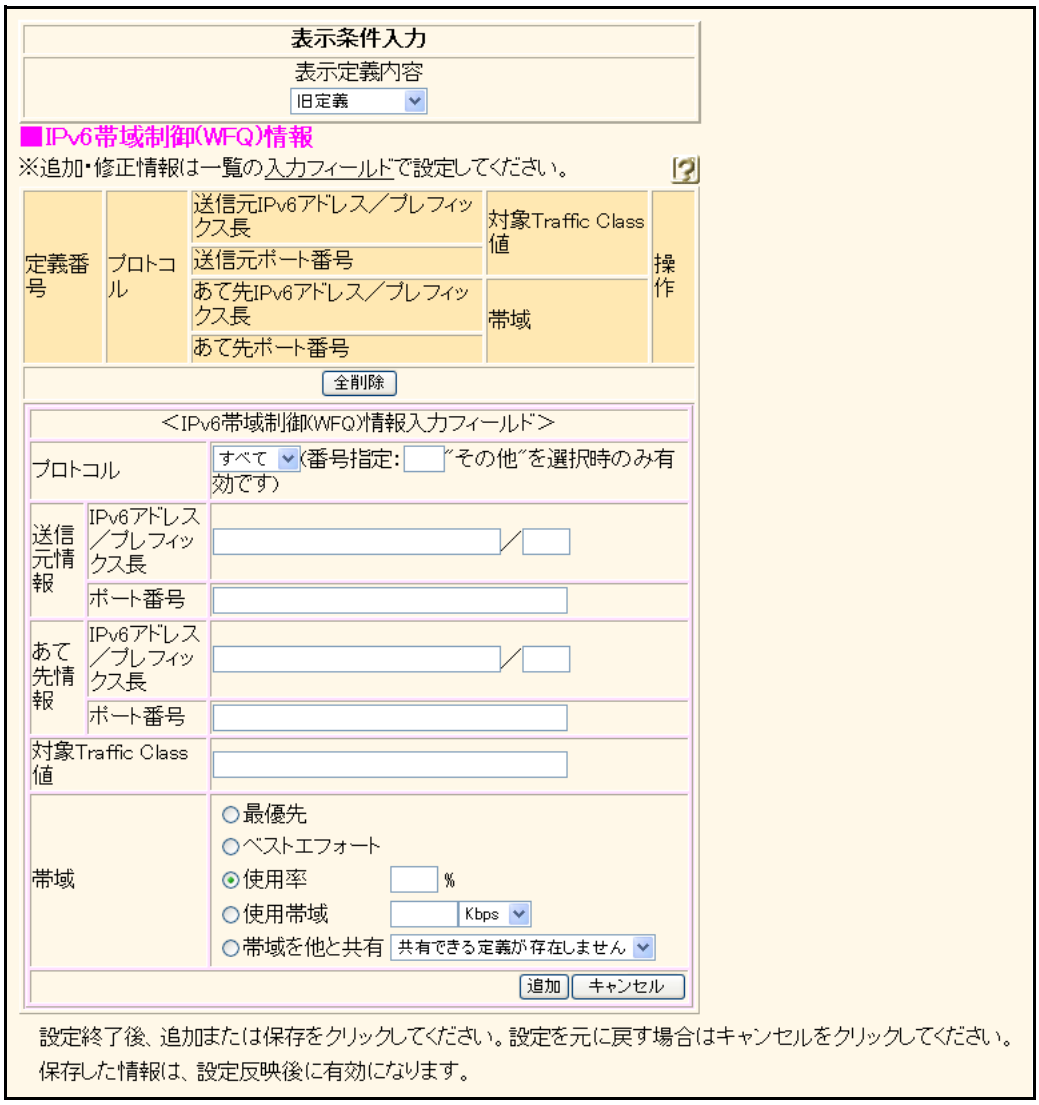
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 帯域制御（WFQ）情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 帯域制御（WFQ）情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

11.1.5.7.1 IPv6 帯域制御（WFQ）情報（旧定義）

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］
→［IPv6 帯域制御（WFQ）情報］→「表示条件入力（旧定義）」



表示条件入力に、“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。

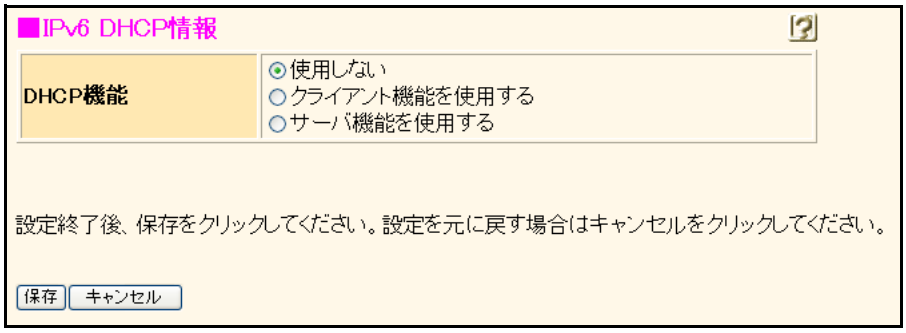
こんな事に気をつけて

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。

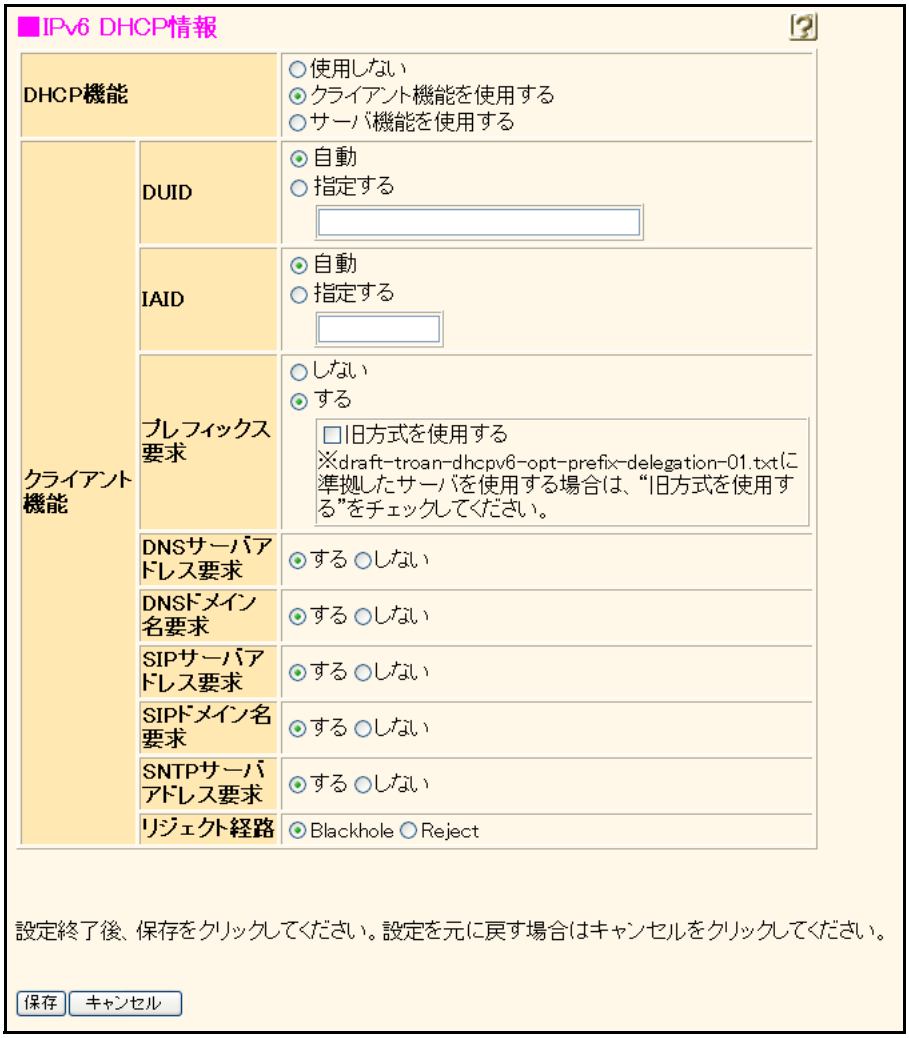
11.1.5.8 IPv6 DHCP 情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］→［IPv6 DHCP 情報］

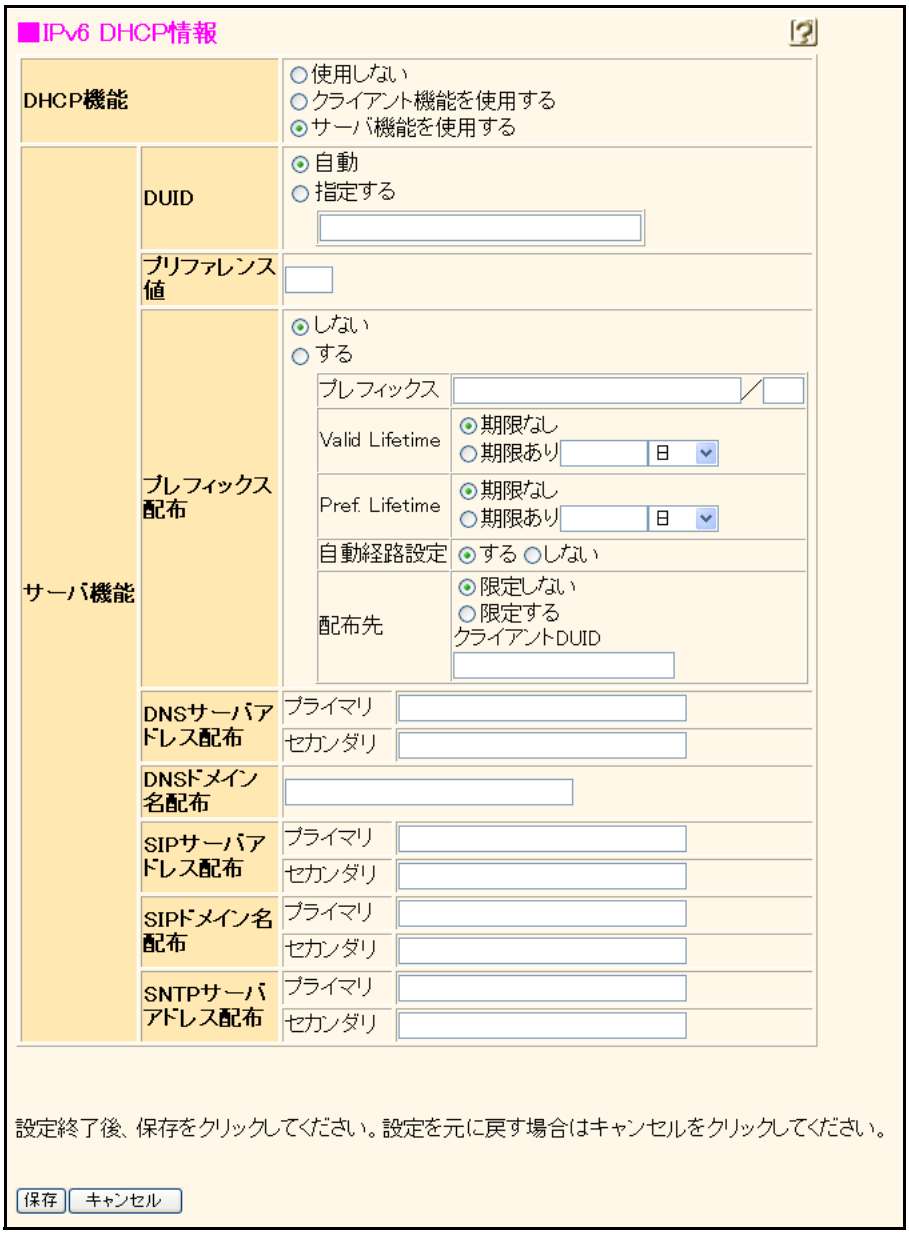
DHCP 機能で、“ 使用しない ” を選択した場合



DHCP 機能で、“ クライアント機能を使用する ” を選択した場合



DHCP 機能で、“ サーバ機能を使用する ” を選択した場合



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
  IPv6 DHCP 機能を使用しません。
- クライアント機能を使用する
  本装置を該当インタフェースの IPv6 DHCP クライアントとして使用します。
- サーバ機能を使用する
  本装置を該当インタフェースのネットワークの IPv6 DHCP サーバとして使用します。

クライアント機能

本装置を該当インタフェースの IPv6 DHCP クライアントとして使用する場合に設定します。

DUID

DUID を以下の 2 つから選択します。

- 自動
  DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
  260 桁以内の 16 進数で表記した DUID を指定します。

IAID

IAID を以下の 2 つから選択します。

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

プレフィックス要求

DHCP サーバにプレフィックスを要求するかどうかを設定します。DHCP サーバにプレフィックスを要求する場合は、“ する ” を選択します。“ する ” を選択した場合に、draft-troan-dhcpv6-opt-prefix-delegation-01.txt に準拠したサーバを利用するときは、“ 旧方式を使用する ” をチェックします。

DNS サーバアドレス要求

DHCP サーバに DNS サーバアドレスを要求するかどうかを設定します。DHCP サーバに DNS サーバアドレスを要求する場合は、“ する ” を選択します。

DNS ドメイン名要求

DHCP サーバに DNS ドメイン名を要求するかどうかを設定します。DHCP サーバに DNS ドメイン名を要求する場合は、“ する ” を選択します。

SIP サーバアドレス要求

DHCP サーバに SIP サーバアドレスを要求するかどうかを設定します。DHCP サーバに SIP サーバアドレスを要求する場合は、“ する ” を選択します。

SIP ドメイン名要求

DHCP サーバに SIP ドメイン名を要求するかどうかを設定します。DHCP サーバに SIP ドメイン名を要求する場合は、“ する ” を選択します。

SNTP サーバアドレス要求

DHCP サーバに SNTP サーバアドレスを要求するかどうかを設定します。DHCP サーバに SNTP サーバアドレスを要求する場合は、“ する ” を選択します。

リジェクト経路

DHCP サーバから取得したプレフィックスのリジェクト経路を以下の 2 つから選択します。

- Blackhole
  リジェクト経路あてのパケットを受信しても送信元にエラーを報告しません。
- Reject
  リジェクト経路あてのパケットを受信した場合、送信元にエラーを報告します。

サーバ機能

本装置を該当インタフェースのネットワークの IPv6 DHCP サーバとして使用する場合に設定します。

DUID

- 自動
  DUID-LL フォーマットで自動生成される DUID を使用します。通常は、この設定を使用します。
- 指定する
  260 桁以内の 16 進数で表記した DUID を指定します。

プリファレンス値

DHCP サーバのプリファレンス値を 0 ～ 255 の範囲の 10 進数で指定します。DHCP クライアントはこの値が大きい DHCP サーバを選択します。省略時は 0 が設定されます。

プレフィックス配布

DHCP クライアントに割り当てるプレフィックスを設定します。クライアントにプレフィックスを割り当てる場合は、“ する ” を選択し、以降の項目を設定します。

プレフィックス
クライアントに割り当てるプレフィックスとプレフィックス長を指定します。プレフィックス長は 48 ～ 64 の範囲で指定します。

こんな事に気をつけて

配布するプレフィックスとして IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は、上位を “dhcp@ インタフェース名 ” 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インタフェースを指定してください。

Valid Lifetime

割り当てるプレフィックスのValid Lifetimeを指定します。

有効範囲）

0～365日

0～8760時間

0～525600分

0～31536000秒

Pref. Lifetime

割り当てるプレフィックスのPreferred Lifetimeを指定します。Pref. Lifetimeは、Valid Lifetimeより短い時間になるように設定してください。

有効範囲）

0～365日

0～8760時間

0～525600分

0～31536000秒

自動経路設定

クライアントに割り当てたプレフィックスへの経路を自動で設定する場合は、“する”を選択します。

配布先

特定のクライアントにだけプレフィックスを配布する場合は、260桁以内の16進数で表記したDUIDを指定します。省略時は、DUIDに関係なく配布されます。

DNSサーバアドレス配布

配布するDNSサーバのIPv6アドレスを設定します。省略するとDHCPサーバによる配布を行いません。

こんな事に気をつけて

配布するDNSサーバアドレスとしてIPv6 DHCPクライアントが取得したDNSサーバアドレスを使用する場合は、“dhcp@インタフェース名”の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリDNSサーバの指定はできません。

DNSドメイン名配布

配布するDNSドメイン名を設定します。省略するとDHCPサーバによる配布を行いません。

こんな事に気をつけて

配布するDNSドメイン名としてIPv6 DHCPクライアントが取得したDNSドメイン名を使用する場合は、“dhcp@インタフェース名”の形式で指定します。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インタフェースを指定してください。

SIPサーバアドレス配布

配布するSIPサーバのIPv6アドレスを設定します。省略するとDHCPサーバによる配布を行いません。

こんな事に気をつけて

配布するSIPサーバアドレスとしてIPv6 DHCPクライアントが取得したSIPサーバアドレスを使用する場合は、“dhcp@インタフェース名”の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリSIPサーバの指定はできません。

SIPドメイン名配布

配布するSIPドメイン名を設定します。省略するとDHCPサーバによる配布を行いません。

こんな事に気をつけて

配布するSIPドメイン名としてIPv6 DHCPクライアントが取得したSIPドメイン名を使用する場合は、“dhcp@インタフェース名”の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリSIPサーバの指定はできません。

SNTPサーバアドレス配布

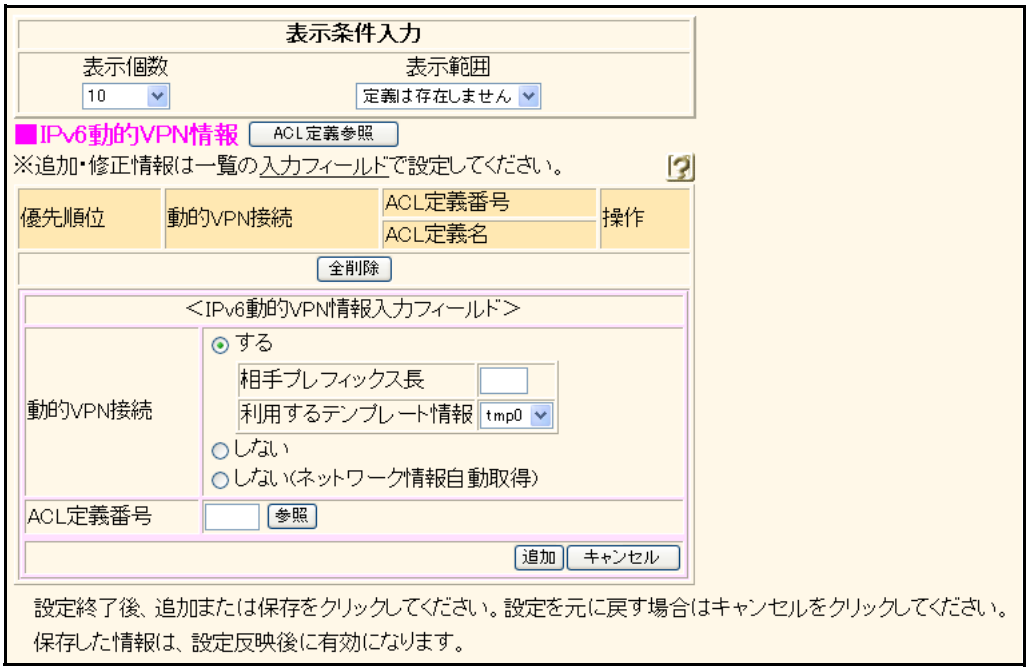
配布するSNTPサーバのIPv6アドレスを設定します。省略するとDHCPサーバによる配布を行いません。

こんな事に気をつけて

配布するSNTPサーバアドレスとしてIPv6 DHCPクライアントが取得したSNTPサーバアドレスを使用する場合は、“dhcp@インタフェース名”の形式で指定します。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インタフェースを指定してください。またその場合、セカンダリSNTPサーバの指定はできません。

11.1.5.9 IPv6 動的VPN情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6関連］→［IPv6 動的VPN情報］



現在、設定されている 動的VPN接続契機パケット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。動的VPN接続契機パケットの検出条件の定義数は、装置全体で432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。

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

優先順位の高い定義から順にパケットをチェックし、すべての条件が一致した場合に定義された動的VPN接続契機パケットの検出を行います。ただし、分割されたパケットに対しては正しく行えません。

動的VPN接続

動的VPN接続を行う場合は、“する”を選択します。

“しない（ネットワーク情報自動取得）”は、相手情報に接続先情報の動的VPN接続定義が行われている必要があります。また、相手情報ごとに1つしか選択できません。

相手プレフィックス長

動的VPN接続を開始する場合に、相手を識別するための情報として相手プレフィックス長を0～128の10進数で指定します。

利用するテンプレート情報

動的VPN接続に利用するテンプレート情報を選択します。

ACL定義番号

［参照］ボタンをクリックして、ACL定義番号を指定します。

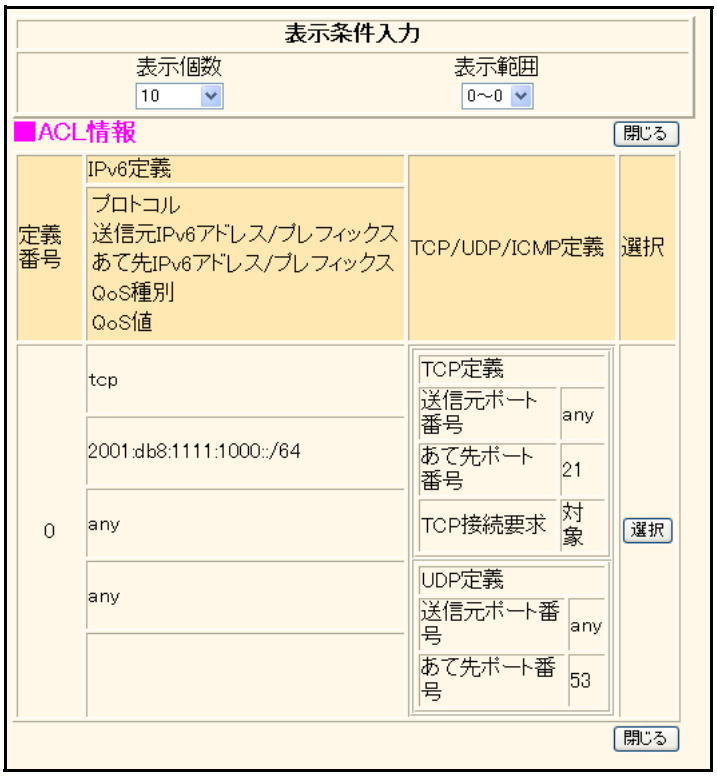
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［IPv6 関連］→［IPv6 動的 VPN 情報］→「ACL 定義番号の［参照］」



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

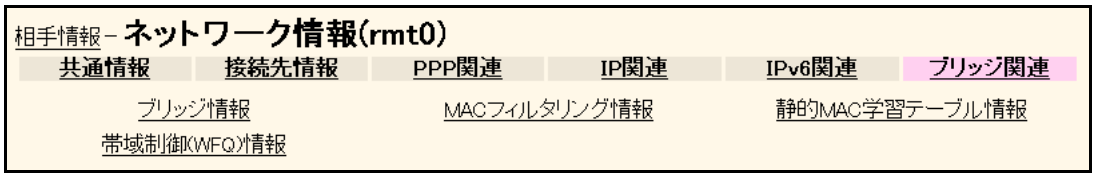
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「IPv6 動的 VPN 情報」の ACL 定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「IPv6 動的 VPN 情報」に ACL 定義番号が設定され、画面が閉じます。［ACL 定義参照］ボタンをクリックした場合は、［選択］ボタンは表示されません。［閉じる］ボタンをクリックして、画面を閉じてください。

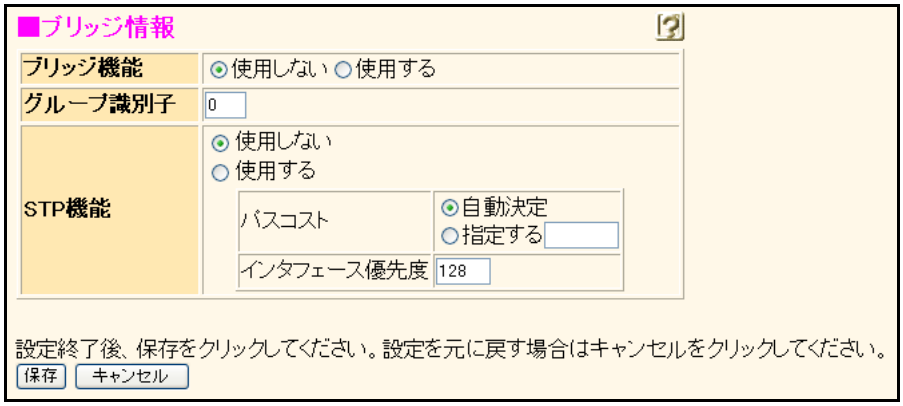
11.1.6　ブリッジ関連

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］



11.1.6.1　ブリッジ情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］→［ブリッジ情報］



ブリッジ機能

接続相手とブリッジで通信する場合は、“使用する”を選択します。

グループ識別子

ブリッジのグループ識別子を10進数で指定します。0～7の範囲で指定します。省略時は0が設定されます。

STP機能

STP機能を利用して経路制御を行う場合は、“使用する”を選択し、以下の項目を設定します。グループ識別子に0を設定した場合だけ、STPを利用することができます。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

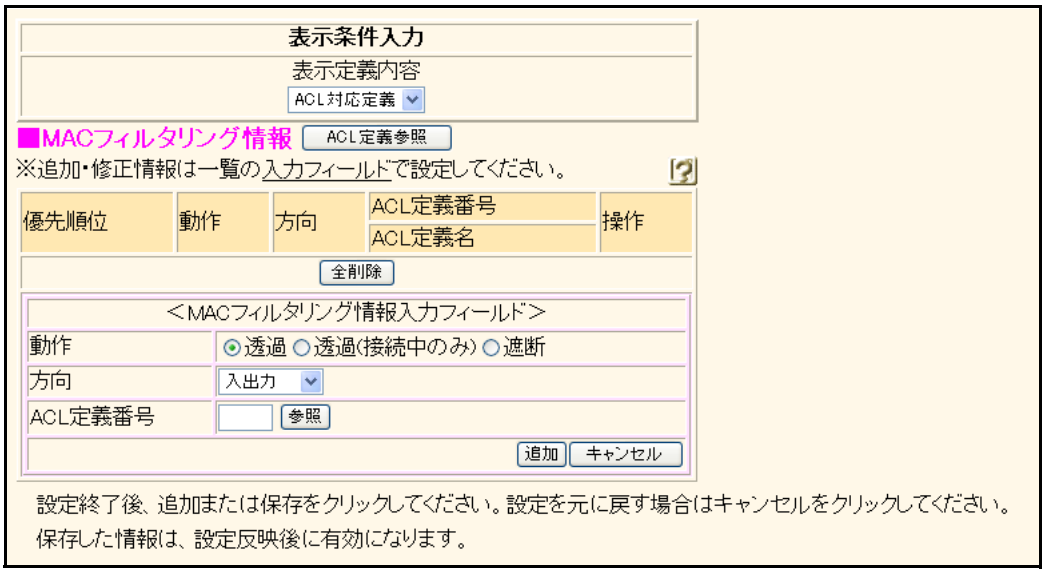
STPで利用するパスコストを選択します。“指定する”を選択する場合は、1～65535の範囲で指定します。パスコストの適性値が不明な場合は、“自動決定”を選択すると、自動的にパスコストが決定されます。

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。

11.1.6.2 MAC フィルタリング情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］
→［MAC フィルタリング情報］



現在、設定されている MAC フィルタリング情報の定義が表示されています。MAC フィルタリングの定義数は、128 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。

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。

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。

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

- MAC 定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］→［MAC フィルタリング情報］→「ACL 定義番号の［参照］」

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

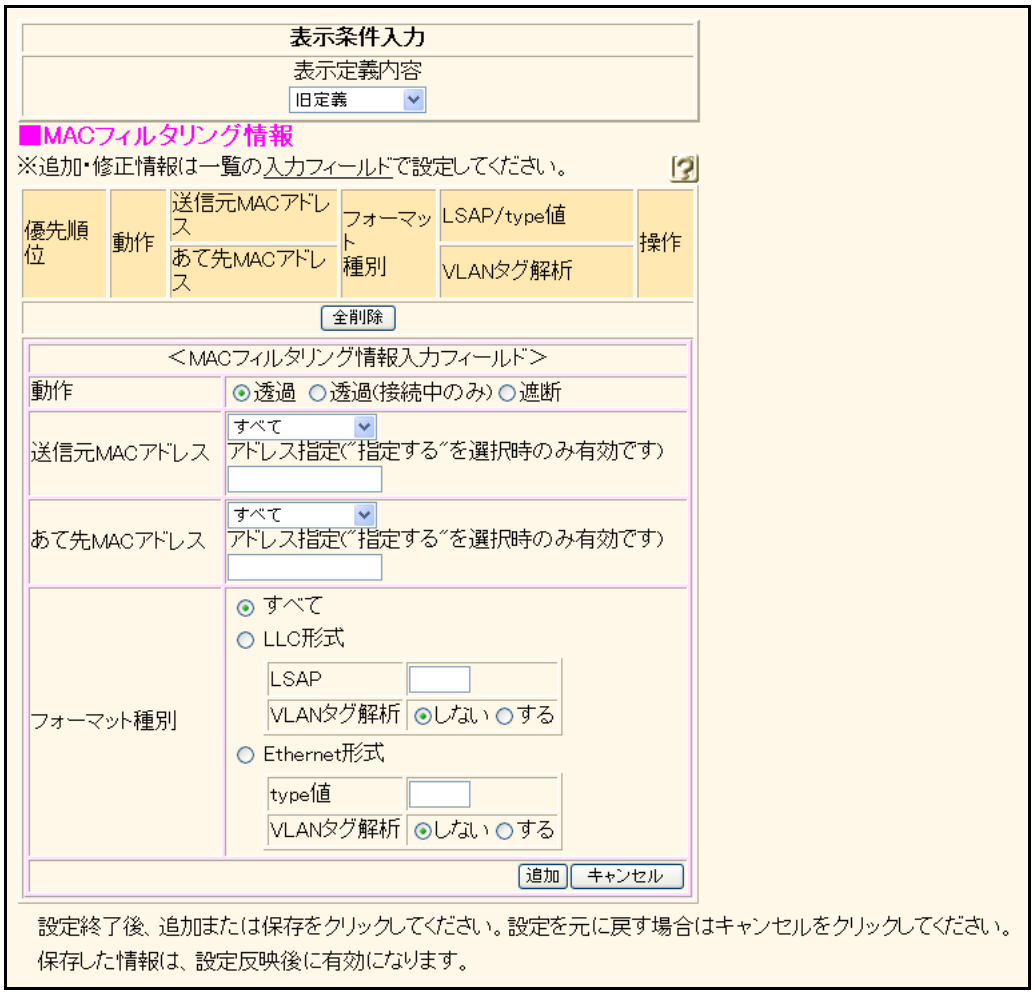
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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。

11.1.6.2.1 MAC フィルタリング情報（旧定義）

［操作］　ルータ設定「相手情報」→「ネットワーク情報」→［修正］→［ブリッジ関連］→［MAC フィルタリング情報］→「表示定義内容（旧定義）」



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

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。

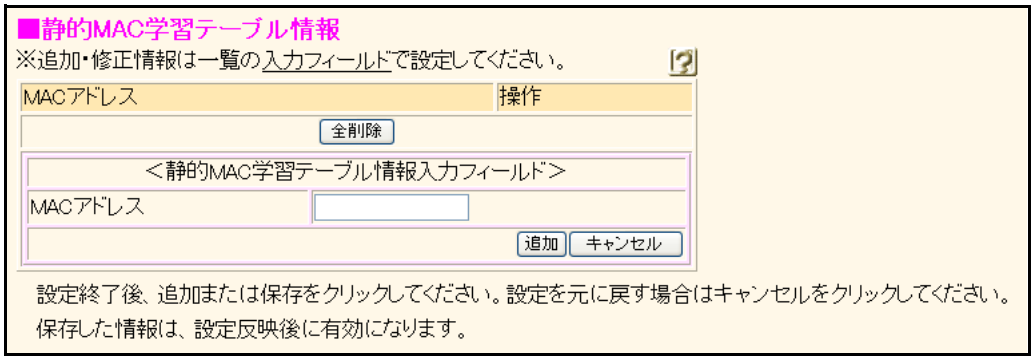
フォーマット種別

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。

11.1.6.3 静的MAC学習テーブル情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］→［静的MAC学習テーブル情報］



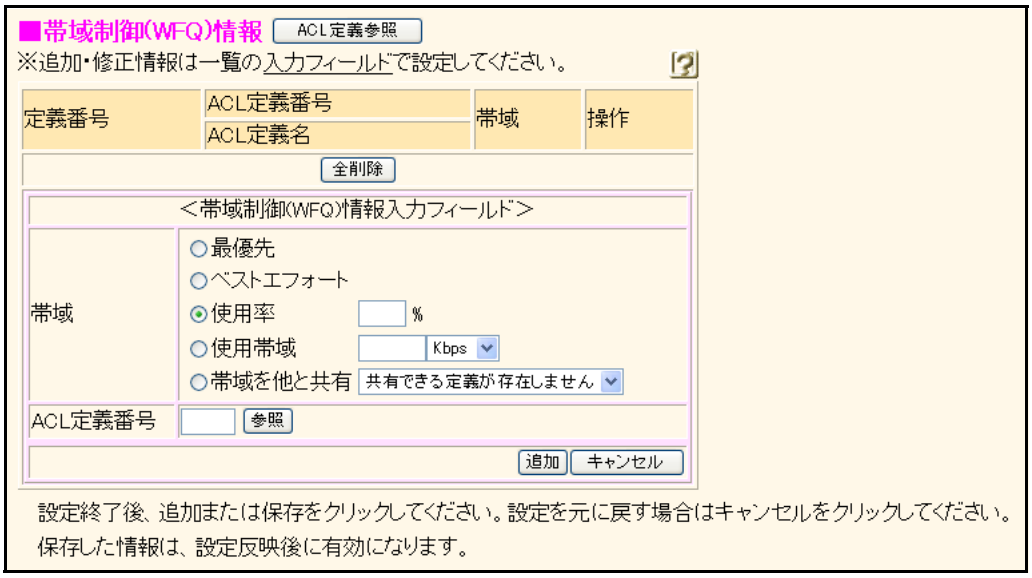
現在、設定されている静的MAC学習テーブルの定義が表示されています。静的MAC学習テーブルの定義数は、装置全体で200個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

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。

11.1.6.4 帯域制御（WFQ）情報

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］→［帯域制御（WFQ）情報］



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、64 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。

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

帯域

帯域の使用率または帯域値を指定します。

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

こんな事に気をつけて

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- MAC 定義

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

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

［操作］　ルータ設定「相手情報」→［ネットワーク情報］→［追加］→［ブリッジ関連］
→［帯域制御（WFQ）情報］→「ACL 定義番号の［参照］」

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

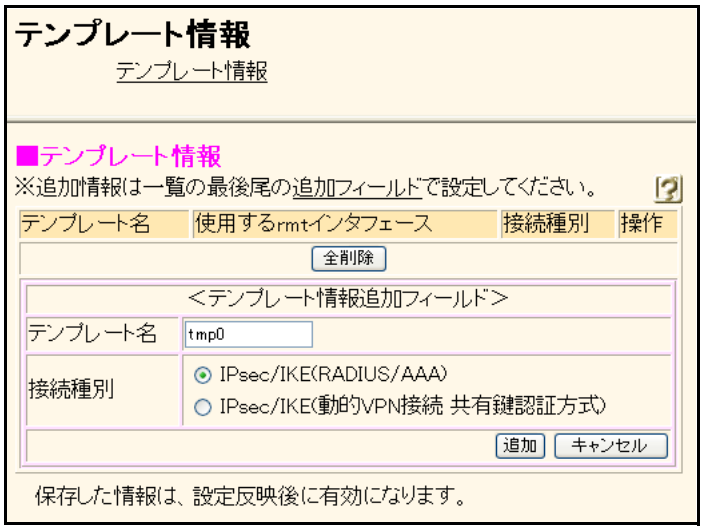
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「帯域制御（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。

12　テンプレート情報

［操作］　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の定義が表示されています。テンプレート情報の最大定義数は、装置全体で２個まで設定できます。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。

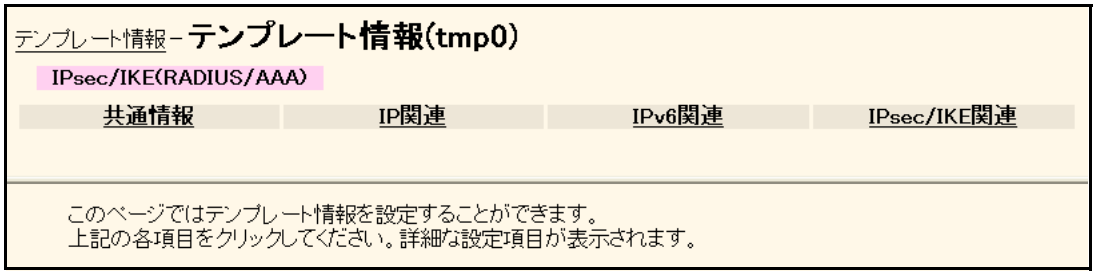
接続種別

接続種別を以下の２つから選択します。

- IPsec/IKE（RADIUS/AAA）
  不特定の相手からIKEネゴシエーション要求を受信したときにRADIUS/AAAの登録情報を検索して接続する場合に選択します。
- IPsec/IKE（動的VPN接続 共有鍵認証方式）
  動的VPN接続契機パケットを検出して動的VPN接続を行う場合、または不特定の相手からの動的VPN接続要求を許可する場合に選択します。動的VPN接続で使用されるIKEで共有鍵認証方式を使用する場合に選択します。動的VPN接続を行う場合は、「相手情報」－［ネットワーク情報］－［IP関連］－［動的VPN情報］で動的VPN接続契機パケットを監視する設定をしてください。

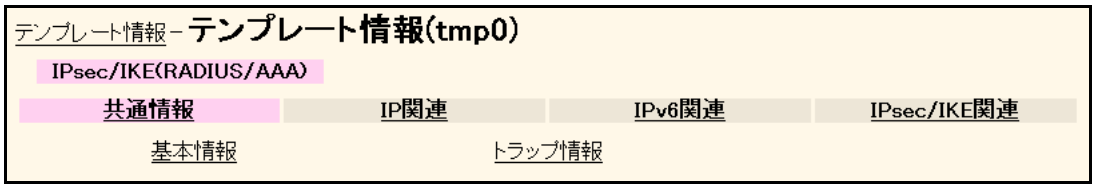
12.1 接続種別：IPsec/IKE（RADIUS/AAA）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］



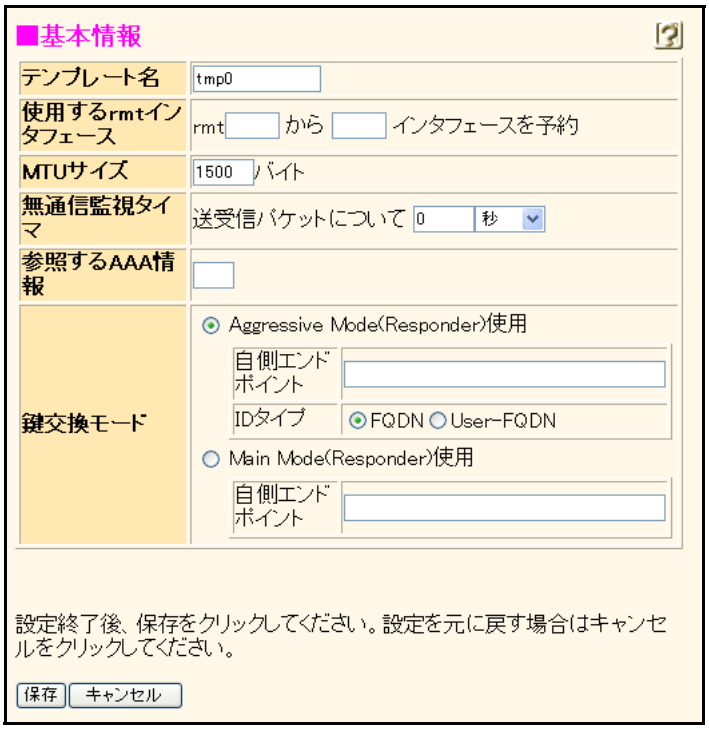
12.1.1 共通情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［共通情報］



12.1.1.1 基本情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［共通情報］→［基本情報］



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

テンプレート着信用に予約した rmt インタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTU サイズ

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を 10 進数を使用して 200 ～ 1500 で指定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションにより、相手 MRU 値と相手 MRRU 値を MTU 値まで小さくすることができるようになります。省略時は、1500 が指定されます。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を 0 ～ 14400 秒の範囲で指定します。0 秒を指定した場合は、監視を行いません。設定された間、監視対象となるパケットがない場合に無通信として IPsec 接続を切断します。省略時は、無通信監視を行わないものとみなされます。

送信パケットおよび受信パケットが通信監視対象となります。

参照する AAA 情報

テンプレート着信で認証および着信時に参照する AAA グループ ID を、10 進数を使用して 10 未満で指定します。

鍵交換モード

鍵交換モードを以下の 2 つから選択します。

- Aggressive Mode（Responder）使用
  相手側エンドポイントが可変 IP アドレスで IPsec/IKE を利用して通信する場合に選択します。Aggressive Mode（Responder）を利用する場合、相手エンドポイント装置に Aggressive Mode（Initiator）を設定してください。
- Main Mode（Responder）使用
  相手側および自側エンドポイントが固定 IP アドレスで IPsec/IKE を利用して通信する場合に選択します。
  Main Mode（Responder）を利用する場合、相手エンドポイント装置に Main Mode を設定してください。

自側エンドポイント

IPv4/IPv6 アドレスを指定します。

有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254
::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

こんな事に気をつけて

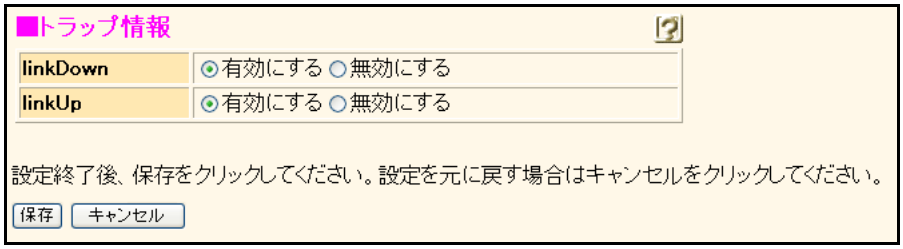
テンプレート着信機能（AAA 認証および、RADIUS 認証）を使用した IPsec 通信では、自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。

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。

12.1.1.2 トラップ情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［共通情報］→［トラップ情報］



トラップ情報

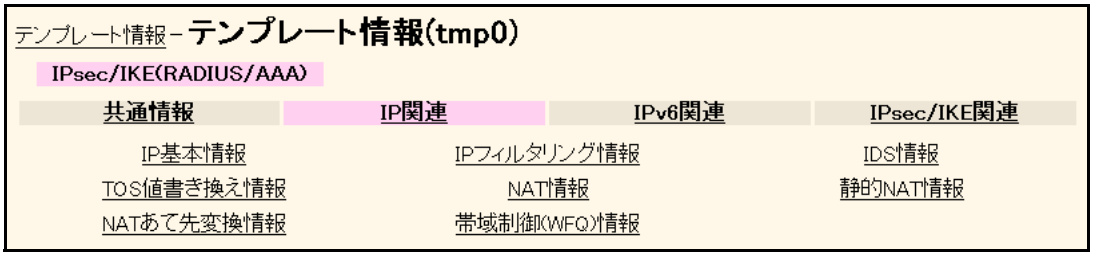
SNMP マネージャに対して、以下の各トラップを有効にするか無効にするかを選択します。

SNMP エージェント機能を利用しない場合は、この設定は意味を持ちません。

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

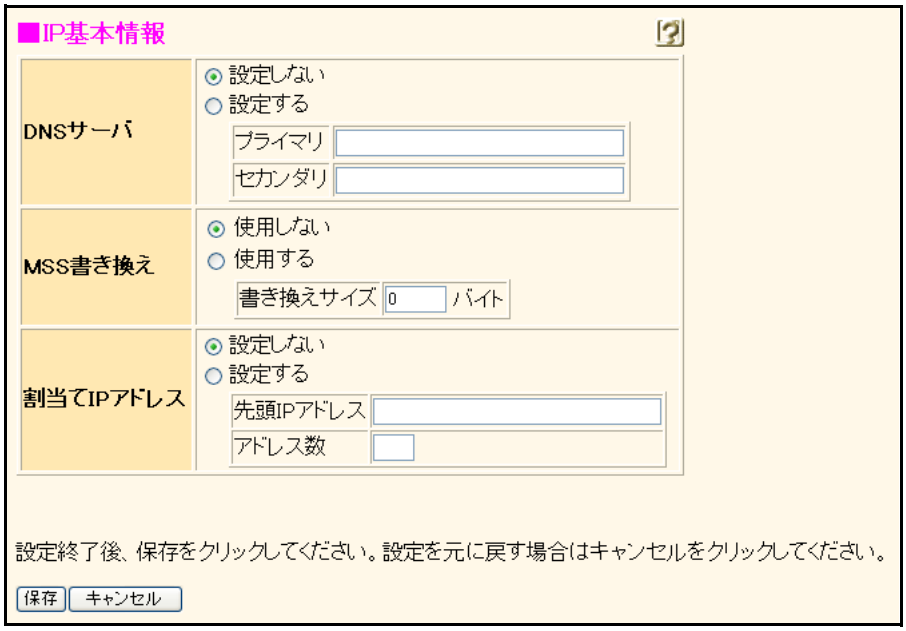
12.1.2　IP 関連

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］



12.1.2.1　IP 基本情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［IP 基本情報］



DNS サーバ

接続の際に使用する DNS サーバの IP アドレスを指定します。省略するか 0.0.0.0 を指定した場合は、DNS サーバアドレスがないもの（0.0.0.0）とみなします。プライマリのみを省略することはできません。

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

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。

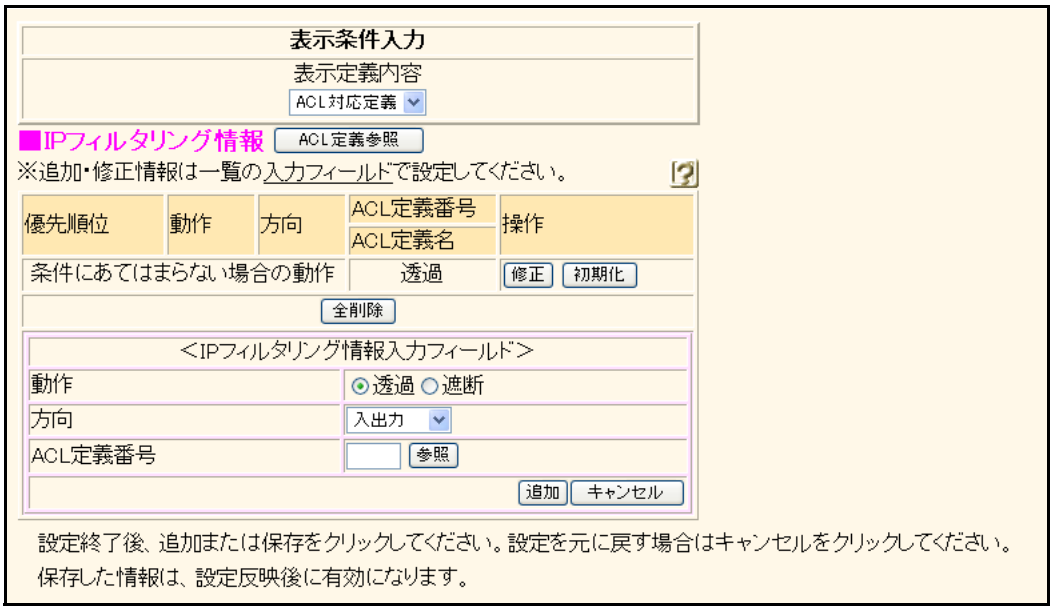
割当てIPアドレス

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、50個です。

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

12.1.2.2 IPフィルタリング情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP関連］→［IPフィルタリング情報］



現在、設定されているIPフィルタリング情報のACL定義が表示されています。処理は優先順位1から順に行います。IPフィルタリングの定義数は、64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。

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

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

表示条件入力は、“ACL対応定義”または“旧定義”から選択します。初期値は、ACL対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

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

動作

IP フィルタリングの動作を以下の2つから選択します。

- 透過
  条件と一致する場合にパケットを透過します。
- 遮断
  条件と一致する場合にパケットを遮断します。

方向

フィルタリングする方向を以下の4つから選択します。

- 入力のみ
  入力パケットだけをフィルタリングする対象とします。
- 出力のみ
  出力パケットだけをフィルタリングする対象とします。
- リバース
  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
  - 送信元IPアドレス／アドレスマスクとあて先IPアドレス／アドレスマスク
  - 送信元ポート番号とあて先ポート番号

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

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

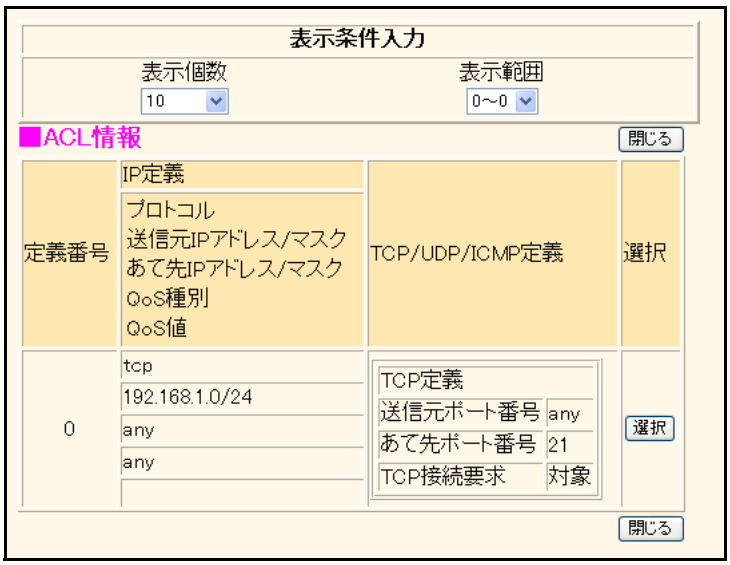
別の画面に「ACL情報」で設定したACL定義が表示されます。ACL情報の以下の定義を使用します。

- IP定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［IP フィルタリング情報］→「ACL 定義番号の［参照］」



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

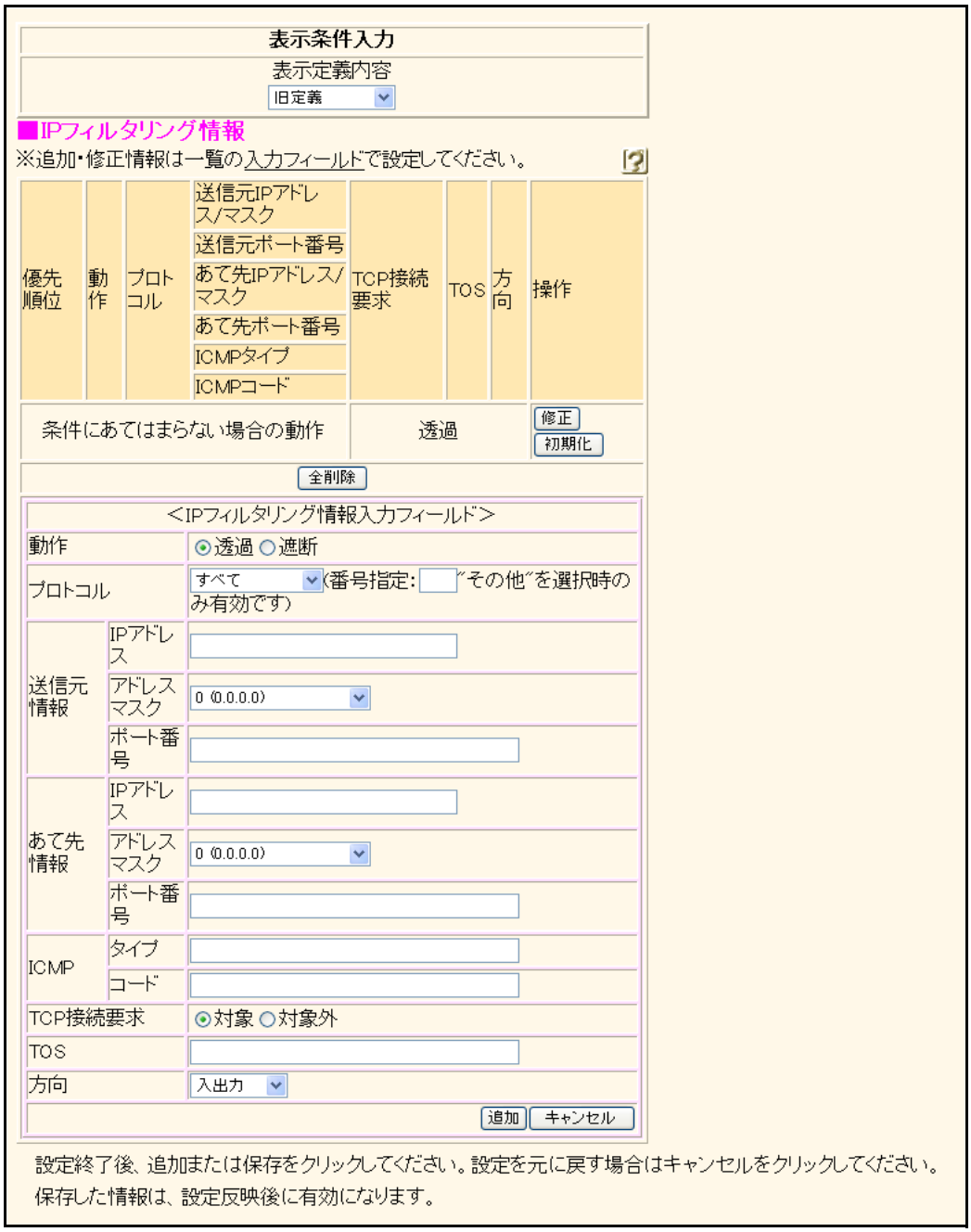
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

12.1.2.2.1 IP フィルタリング情報（旧定義）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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

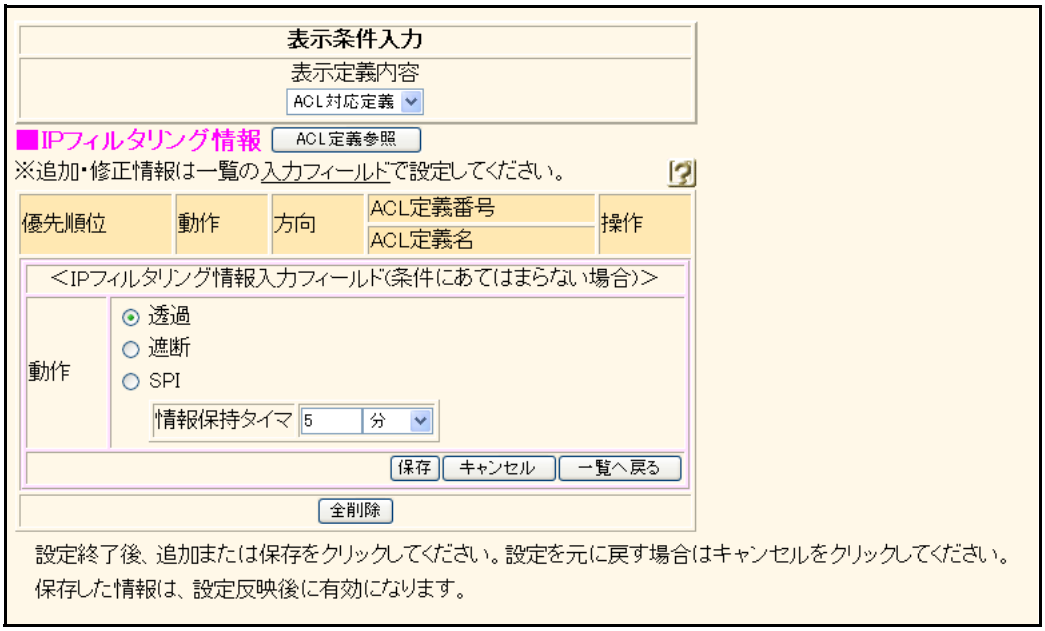
フィルタリングする方向を以下の4つから選択します。

- 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。

12.1.2.2.2 IP フィルタリング情報（条件にあてはまらない場合の動作）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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］



「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。

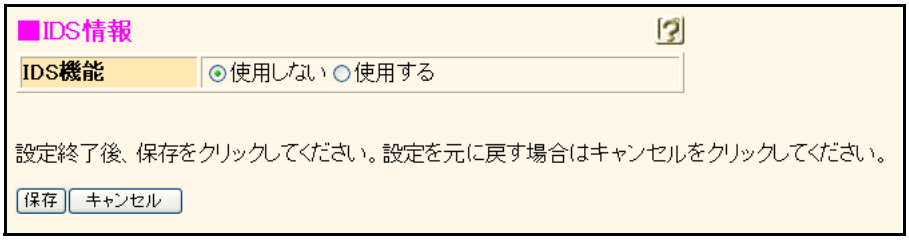
- 透過
  IP フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
  IP フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
  IP フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

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。

12.1.2.3 IDS 情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［IDS 情報］

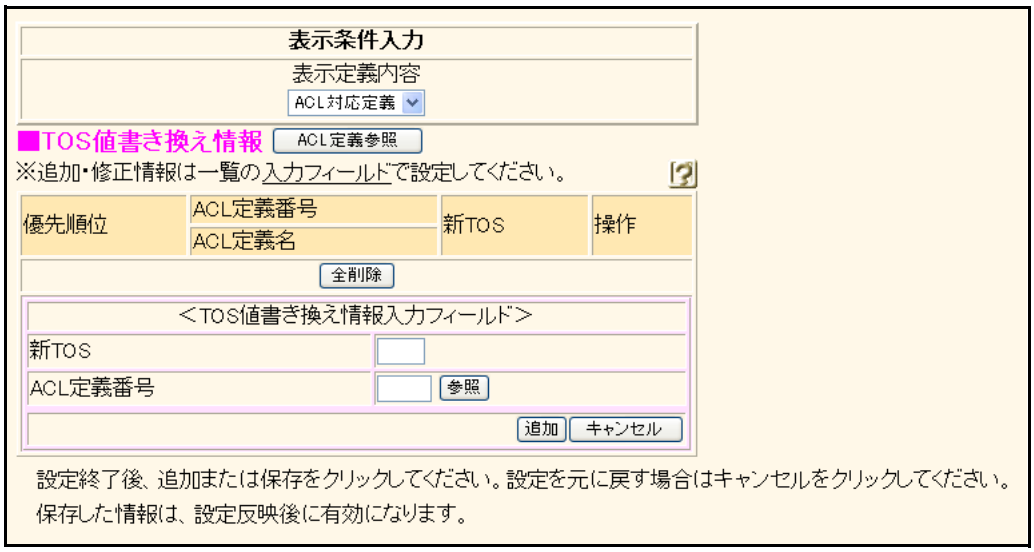


IDS 機能

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

12.1.2.4 TOS 値書き換え情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［TOS 値書き換え情報］



現在、設定されている TOS 値書き換え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。TOS 値書き換えの定義数は、32 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。

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

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［TOS 値書き換え情報］→「ACL 定義番号の［参照］」

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

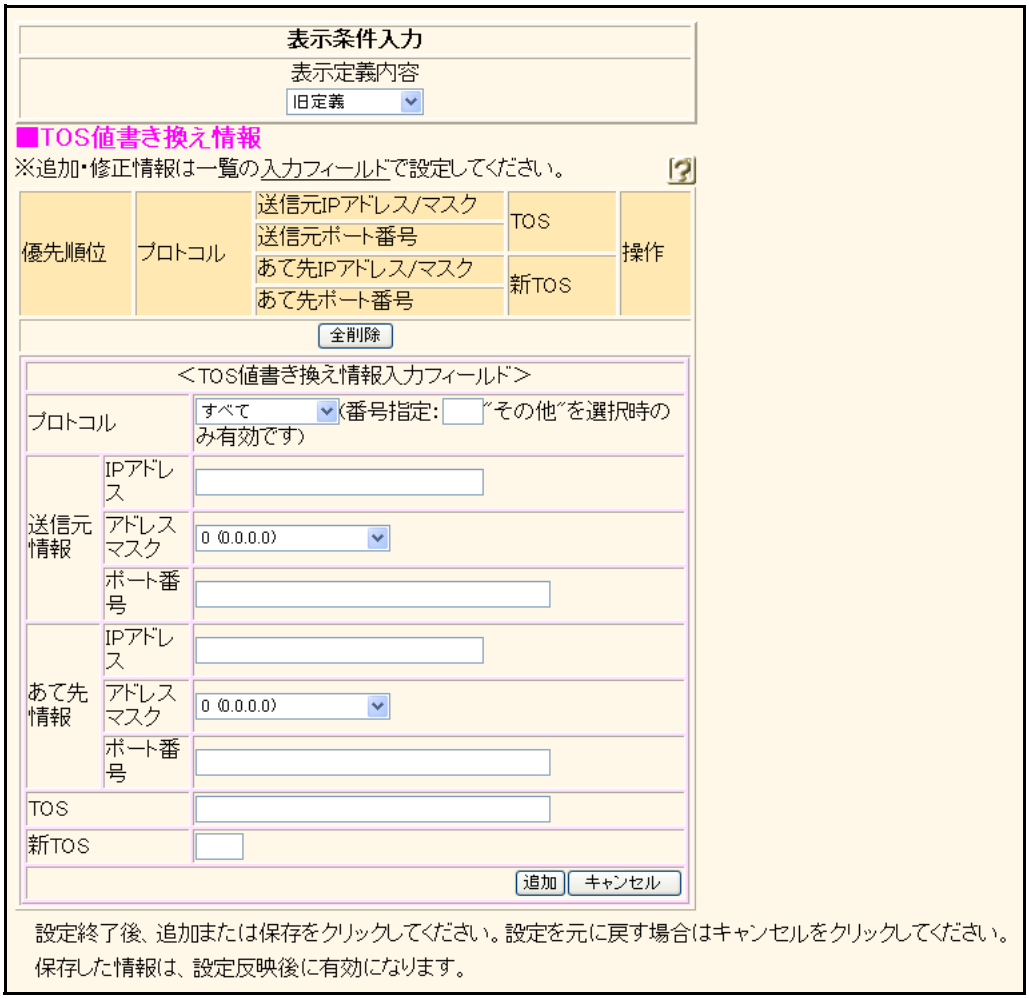
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

12.1.2.4.1 TOS値書き換え情報（旧定義）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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

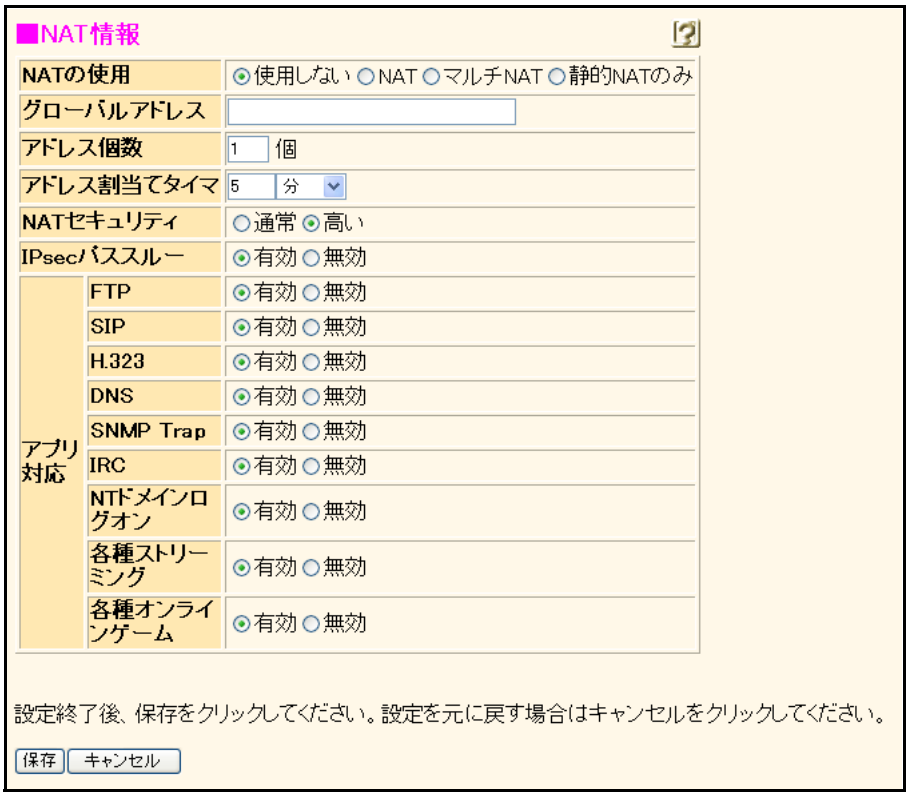
TOS 値書き換えの条件として IP パケットの TOS フィールド値を 16 進数を使用して、0 ～ ff の範囲または “any” で指定します。TOS フィールド値を複数指定する場合は、“,” で区切ります。範囲指定の場合は、“-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての TOS フィールド値が書き換えの対象となります。

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。

12.1.2.5 NAT 情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［NAT 情報］



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。

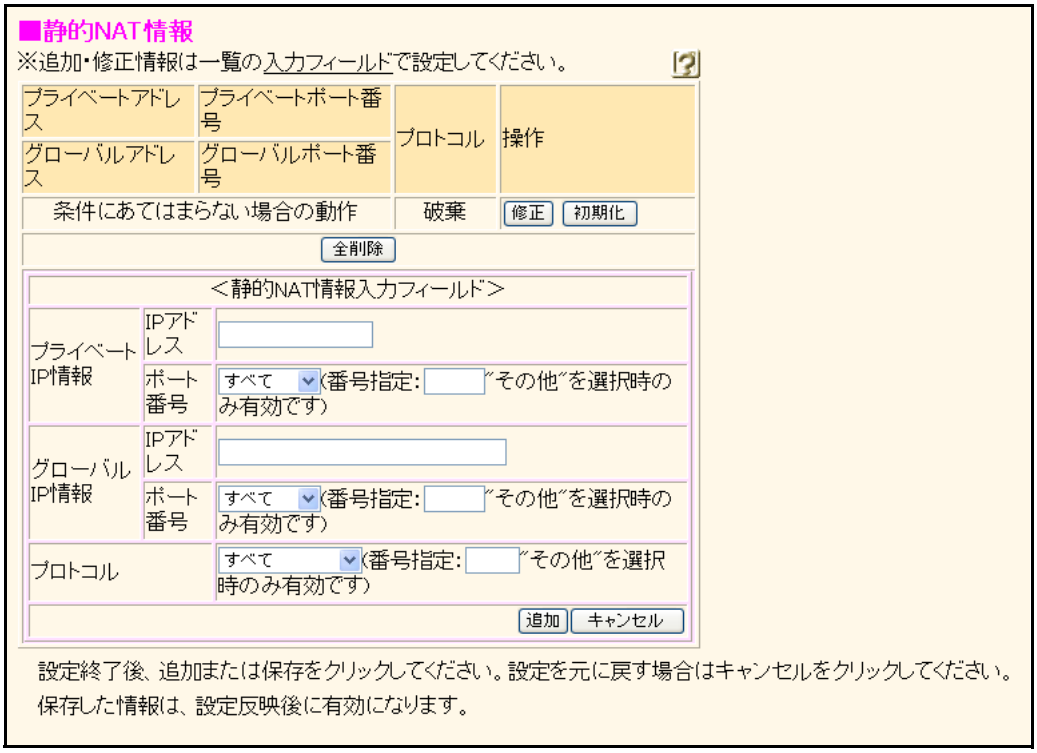
アプリ対応

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

12.1.2.6 静的NAT情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP関連］→［静的NAT情報］



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、装置全体で64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。

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

プライベートIP情報

IPアドレス

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

ポート番号

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

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

例）プライベートポート番号：1000
　　グローバルポート番号：10000-11000
　　NAT変換後
　　プライベートポート番号：1000-2000

グローバルIP情報

IPアドレス

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

IPアドレスを指定する場合は、-”で区切った1組の範囲を指定します。

ポート番号

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

プロトコル

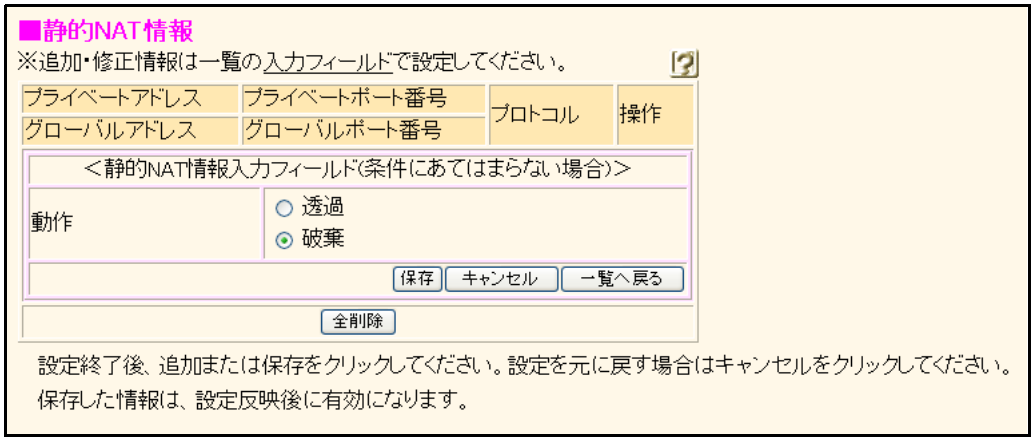
固定でアドレス変換を行う場合に対象となるプロトコルを以下の8つから選択します。()内はプロトコル番号です。

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

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

12.1.2.6.1 静的NAT情報（条件にあてはまらない場合の動作）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP関連］→［静的NAT情報］→「条件にあてはまらない場合の動作」［修正］



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

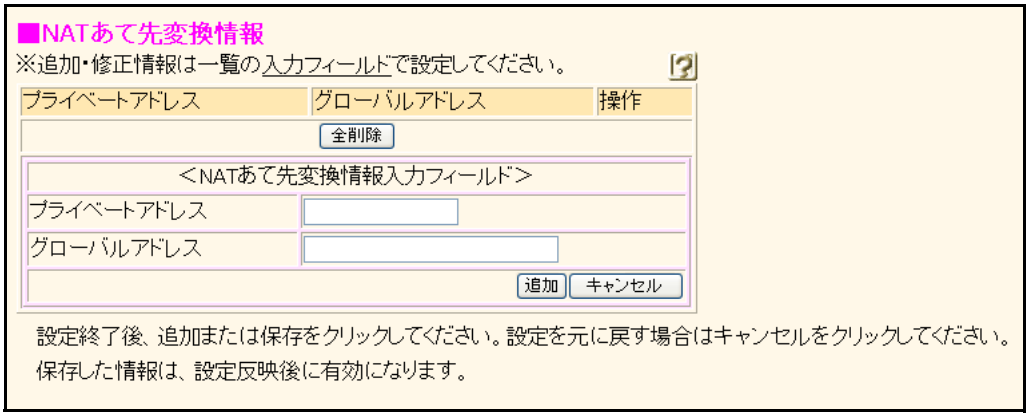
動作

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

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

12.1.2.7 NATあて先変換情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP関連］→［NATあて先変換情報］



現在、設定されているNATあて先変換情報の定義が表示されています。NATあて先変換の定義数は、装置全体で64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。

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。

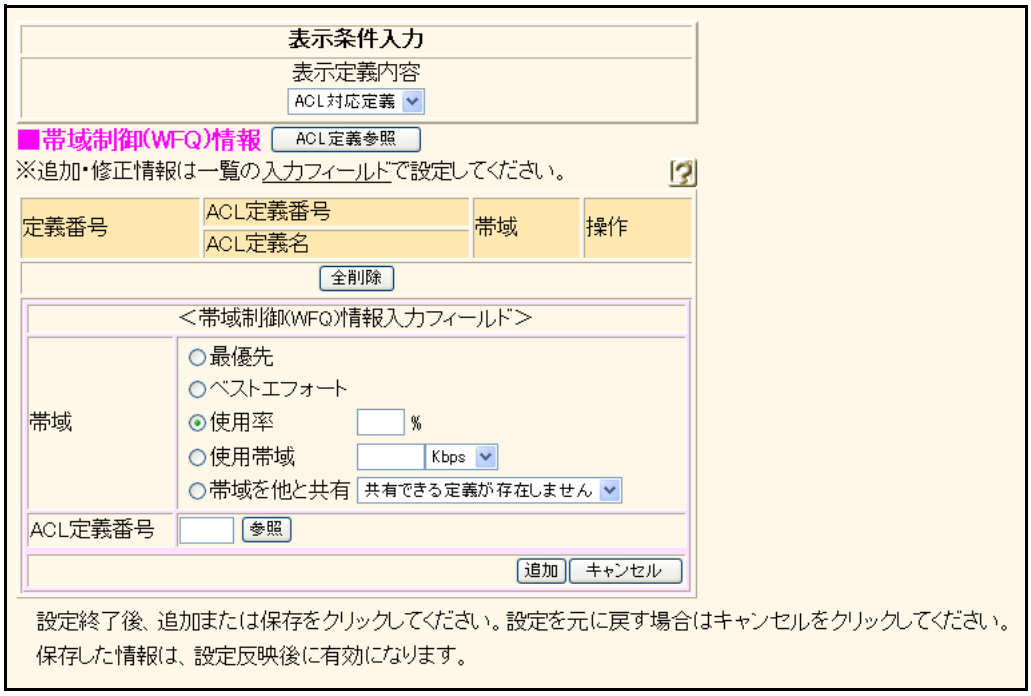
例）プライベートアドレス：192.168.1.100
　　グローバルアドレス：172.16.1.100-172.16.1.200
　　NATあて先変換後
　　プライベートアドレス：192.168.1.100-192.168.1.200

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。

12.1.2.8 帯域制御（WFQ）情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［帯域制御（WFQ）情報］



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、装置全体で 64 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。
設定された任意のプロトコル、IP アドレス、ポート番号、TOS フィールド値の条件を元に帯域を割り当てます。

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

帯域

帯域の使用率または帯域値を指定します。

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

こんな事に気をつけて

シェーピングを使用しない場合、帯域制御機能は有効に動作しません。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- IP 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IP 関連］→［帯域制御（WFQ）情報］→「ACL 定義番号の［参照］」

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

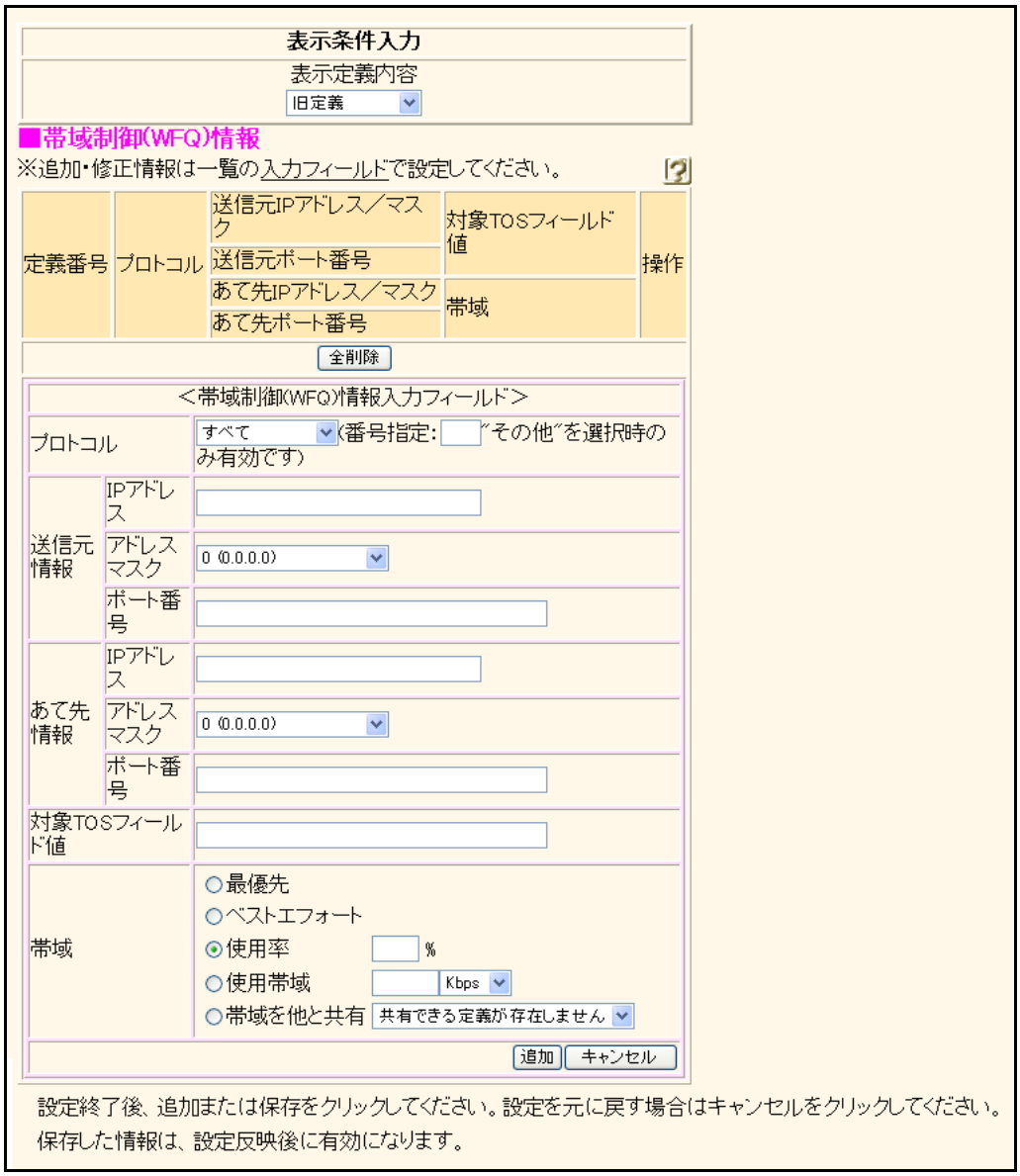
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

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

12.1.2.8.1 帯域制御（WFQ）情報（旧定義）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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。

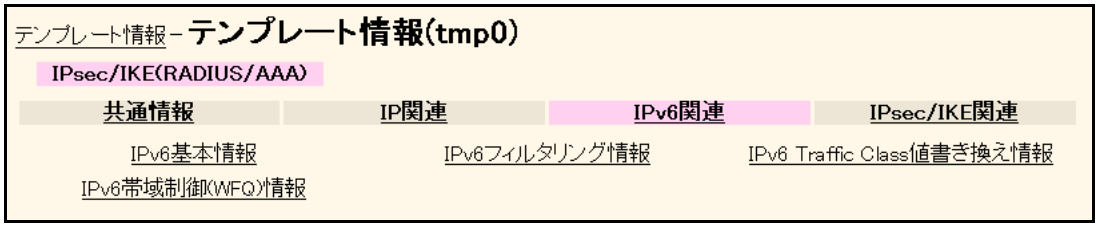
帯域

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。

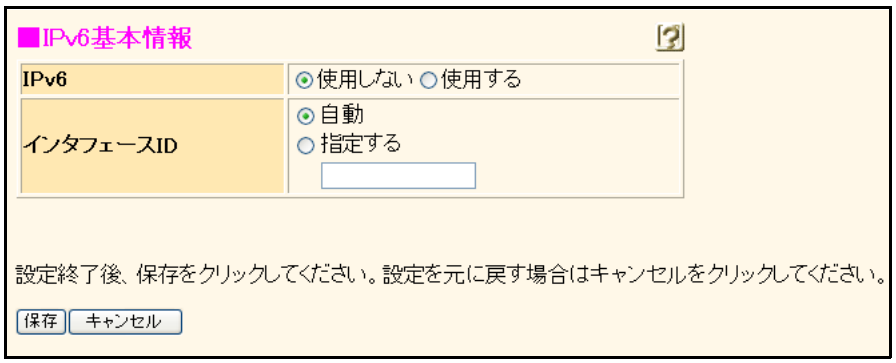
12.1.3 IPv6 関連

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］



12.1.3.1 IPv6 基本情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 基本情報］



IPv6

テンプレート着信で使用する rmt インタフェースで、IPv6 の通信を使用する場合は、“ 使用する ” を選択します。

インタフェース ID

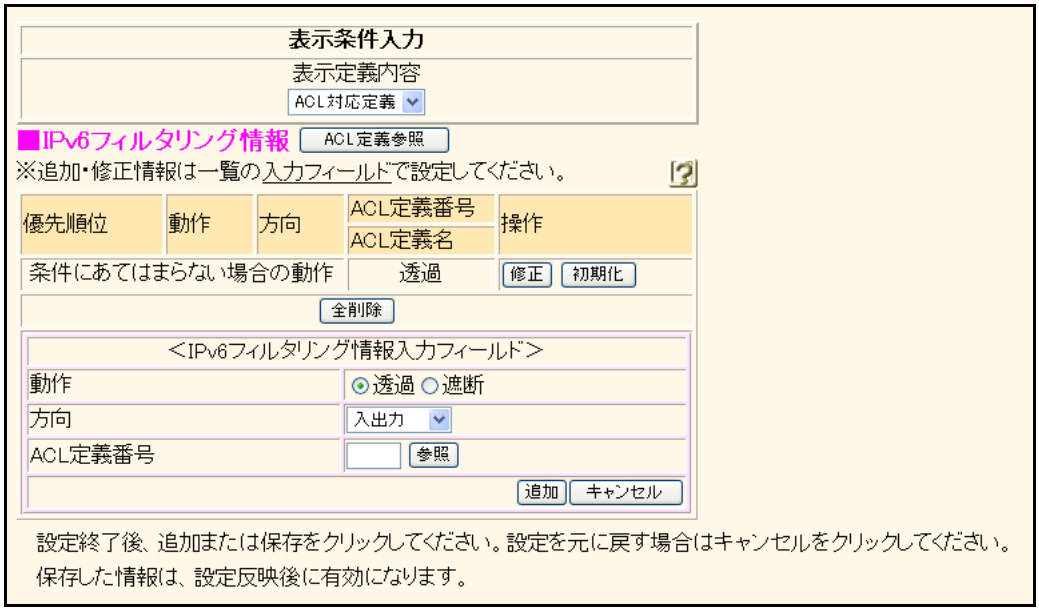
テンプレート着信で使用する rmt インタフェースで利用する ID を設定します。“ 自動 ” を選択する場合は、装置の MAC アドレスから自動生成される EUI-64 形式のインタフェース ID を使用します。通常は、“ 自動 ” を選択します。

“ 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

12.1.3.2 IPv6 フィルタリング情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 フィルタリング情報］



現在、設定されている IPv6 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 から順に行います。IPv6 フィルタリングの定義数は、64 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。

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

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

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

こんな事に気をつけて

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

動作

IPv6 フィルタリングの動作を以下の 2 つから選択します。

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

方向

フィルタリングする方向を選択します。

- 入力のみ
  入力パケットのみをフィルタリングする対象とする場合に指定します。
- 出力のみ
  出力パケットのみをフィルタリングする対象とする場合に指定します。
- リバース
  入力パケットと出力パケットの両方をフィルタリング対象とします。ただし、入力パケットについては以下のものを逆転した条件でフィルタリングします。
  - 送信元IPv6アドレス／プレフィックス長とあて先IPv6アドレス／プレフィックス長
  - 送信元ポート番号とあて先ポート番号

  リバースを指定した場合は、入力パケットはIPv6アドレスとポート番号だけを逆転した条件でフィルタリングされます。このため、「TCP接続要求」を有効にしている場合は、入力パケットに対してもTCPプロトコルのコネクション接続要求がフィルタリング対象に含まれます。
- 入出力
  入力パケットと出力パケットの両方をフィルタリング対象とする場合に選択します。

ACL定義番号

[参照]ボタンをクリックして、ACL定義番号を指定します。

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

- IPv6定義
- TCP定義
- UDP定義
- ICMP定義

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

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 フィルタリング情報］→「ACL 定義番号の［参照］」

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

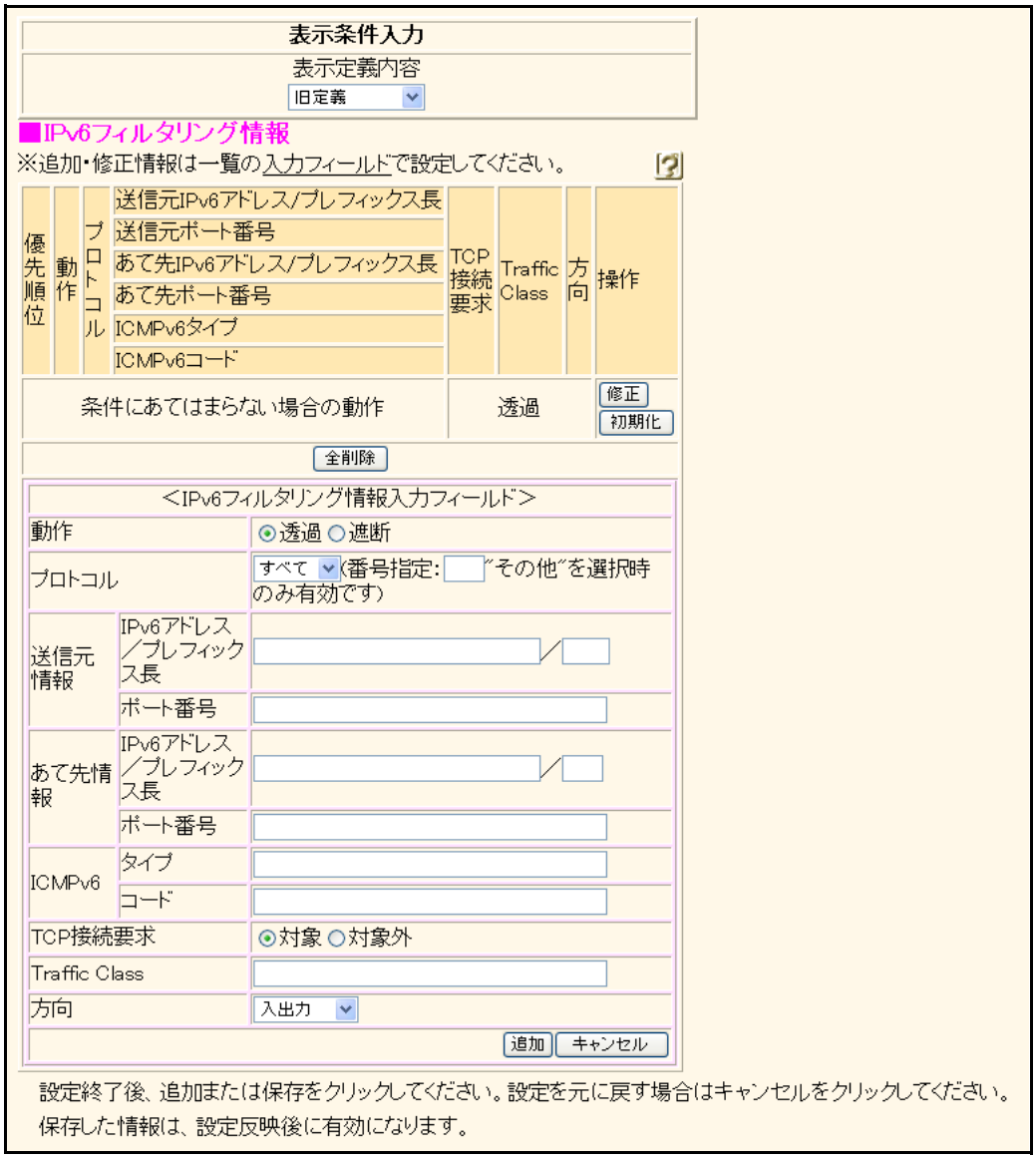
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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。

12.1.3.2.1 IPv6 フィルタリング情報（旧定義）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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

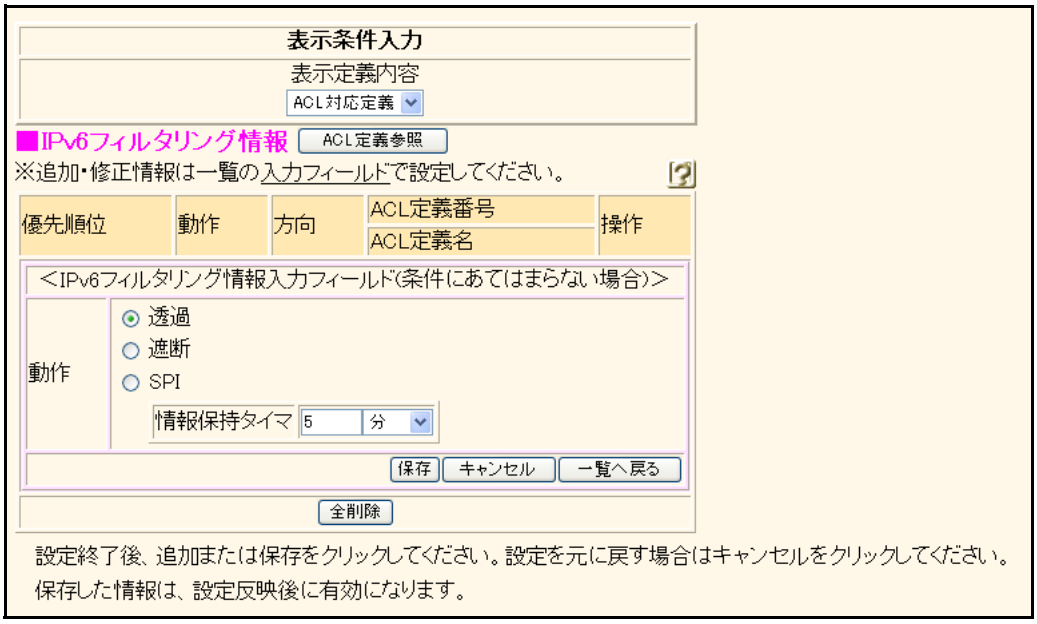
フィルタリングする方向を選択します。

- 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。

12.1.3.2.2 IPv6 フィルタリング情報（条件にあてはまらない場合の動作）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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］



「条件にあてはまらない場合の動作」は、このテンプレートに設定されている IPv6 フィルタリング定義のどれにも一致しないときの動作です。動作を設定して、［保存］ボタンをクリックすることによって、動作を決定することができます。

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

こんな事に気をつけて

動作に遮断や SPI を指定し、IPv6 フィルタリング情報で WWW や DHCP に対するアクセスを透過する設定を行わなかった場合、本装置に対し WWW ブラウザからアクセスできない、または、DHCP 機能が使用できなくなることがあります。

動作

IPv6 フィルタリング定義のどれにも一致しない場合の動作を以下の 3 つから選択します。

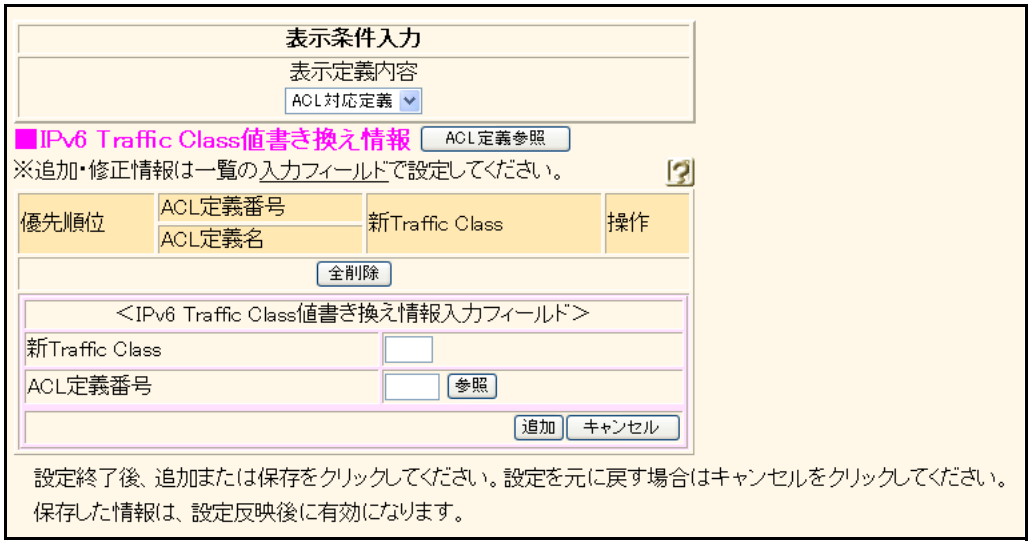
- 透過
  IPv6 フィルタリング定義のどれにも一致しない場合にパケットを透過します。
- 遮断
  IPv6 フィルタリング定義のどれにも一致しない場合にパケットを遮断します。
- SPI
  IPv6 フィルタリング定義のどれにも一致しないで、プロトコルが TCP の場合は、セッション開始パケットを送信したときだけ、セッションの後続パケットを透過します。プロトコルが UDP やそれ以外の場合は、以前送信したパケットに対応する受信パケットだけを透過します。

情報保持タイマ

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。

12.1.3.3 IPv6 Traffic Class 値書き換え情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 Traffic Class 値書き換え情報］



現在、設定されている IPv6 Traffic Class 値書き換え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 Traffic Class 値書き換えの定義数は、32 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。

優先順位の高い定義から順にパケットのチェックを行い、すべての条件が一致した場合に定義された IPv6 Traffic Class 値書き換えを行います。ただし、分割されたパケットに対しては正しく扱えません。

表示条件入力は、“ACL 対応定義 ” または “ 旧定義 ” から選択します。初期値は、ACL 対応定義情報が表示されています。

なお、設定画面は表示条件によって異なりますが、優先順位は通し番号となります。

新 Traffic Class

IPv6 パケットに新しく指定する Traffic Class 値を 16 進数を使用して、0 ～ ff の範囲で指定します。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 Traffic Class 値書き換え情報］→「ACL 定義番号の［参照］」

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

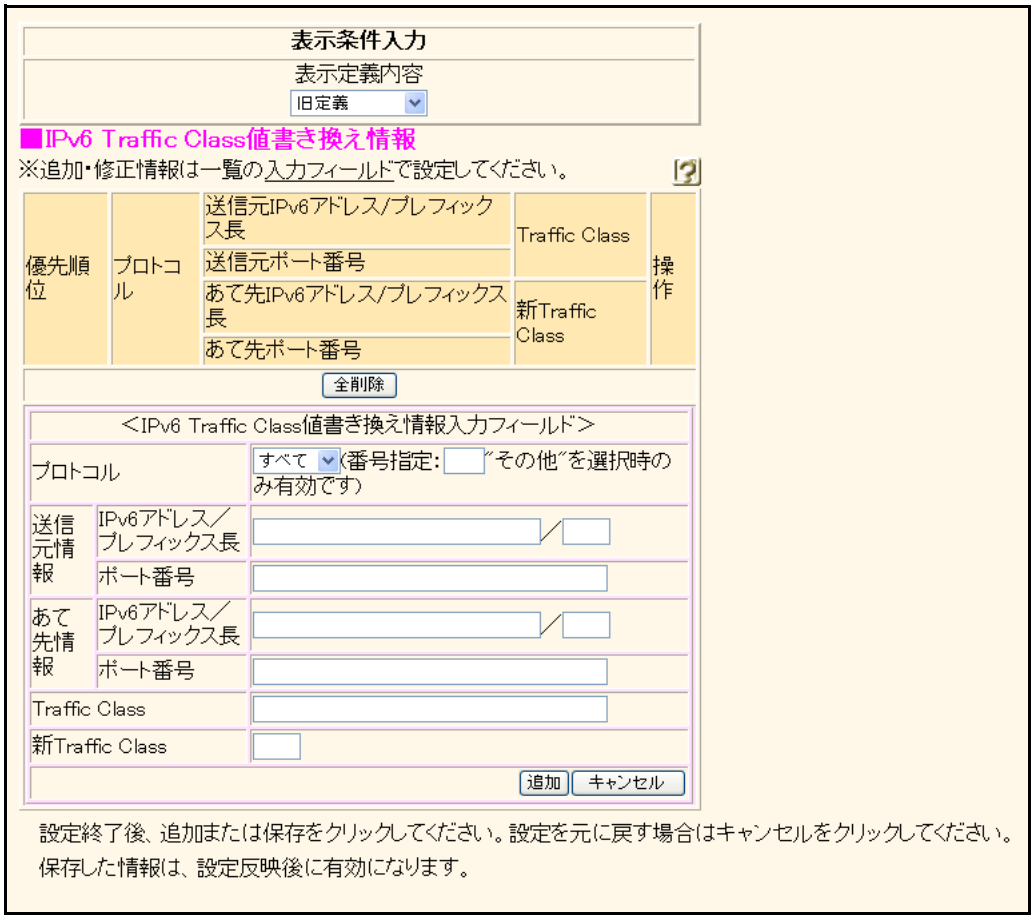
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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。

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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

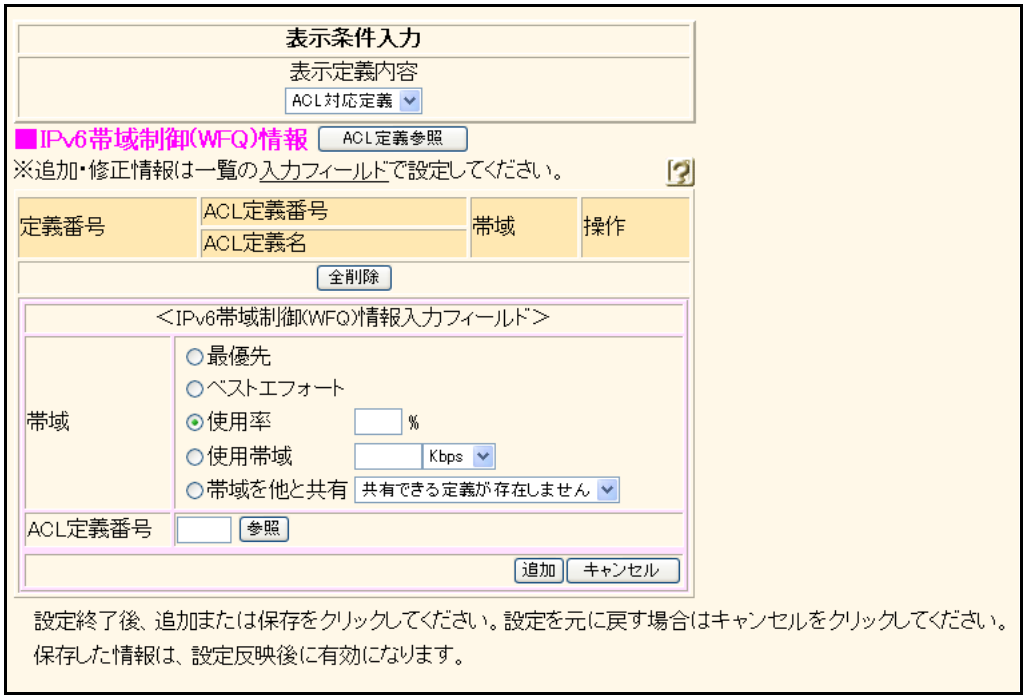
Traffic Class 値書き換え条件として IPv6 パケットの Traffic Class 値を 16 進数を使用して 0 ～ ff の範囲または “any” で指定します。Traffic Class フィールド値を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切ります。10 組まで指定できます。省略時は “any” が設定され、すべての Traffic Class 値が書き換えの対象となります。

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。

12.1.3.4 IPv6 帯域制御（WFQ）情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 帯域制御（WFQ）情報］



現在、設定されている帯域制御情報の定義が表示されています。帯域制御の定義数は、64 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。

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

帯域制御機能を有効に動作させる場合は、シェーピングを使用してください。

ACL 定義番号

［参照］ボタンをクリックして、ACL 定義番号を指定します。

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

- IPv6 定義
- TCP 定義
- UDP 定義
- ICMP 定義

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

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

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPv6 関連］→［IPv6 帯域制御（WFQ）情報］→「ACL 定義番号の［参照］」

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

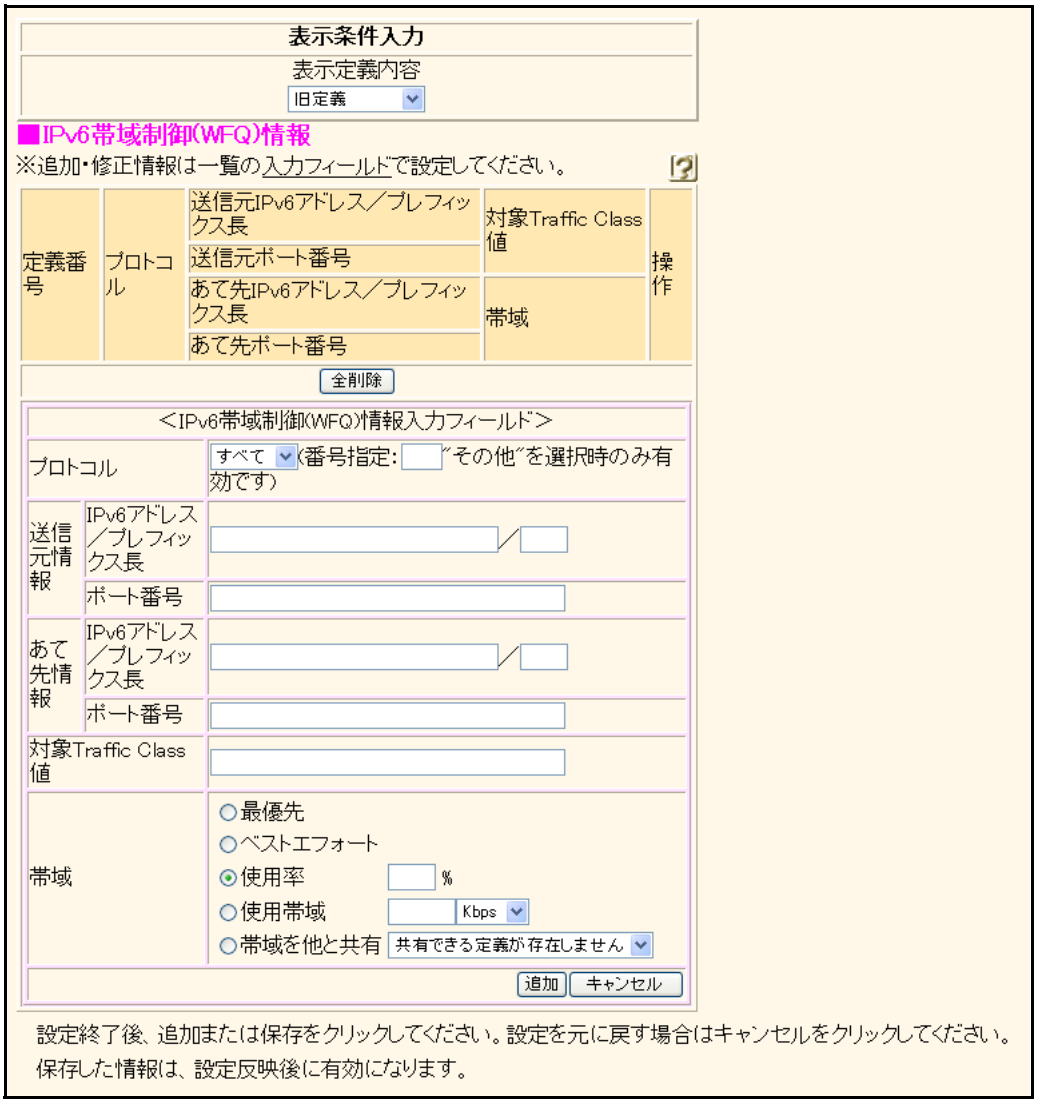
表示条件入力では、表示個数および表示範囲を指定することができます。設定することによって、ACL 定義情報の一覧に見たい情報だけを表示させることができます。

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

「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。

12.1.3.4.1 IPv6 帯域制御（WFQ）情報（旧定義）

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［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。

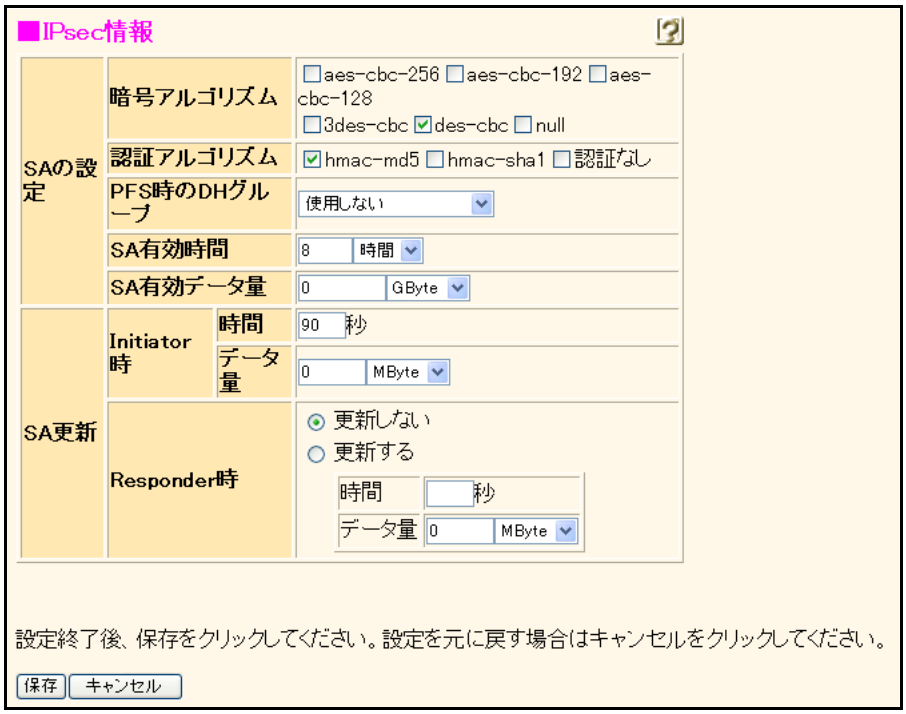
- 最優先
  最優先データとして扱われます。
- ベストエフォート
  非優先（ベストエフォート）として扱われます。
- 使用率で指定する場合
  割り当てる帯域（%）を10進数を使用して、1～99の範囲で指定します。同じ相手ネットワークの中で、帯域トータルが100を超える場合は、それらの比率に従って帯域が割り当てられます。
- 使用する帯域値を指定する場合
  1～100000Kbpsまたは1～100Mbpsの範囲で指定します。全定義の合計が回線速度を超えた場合、それぞれ指定した値の比で帯域を割り当てます。残った帯域は定義に一致しないデータ用の帯域となります。
- 帯域値を他と共有
  ほ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

12.1.4 IPsec/IKE 関連

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPsec/IKE 関連］

12.1.4.1 IPsec 情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPsec/IKE 関連］→［IPsec 情報］



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、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。

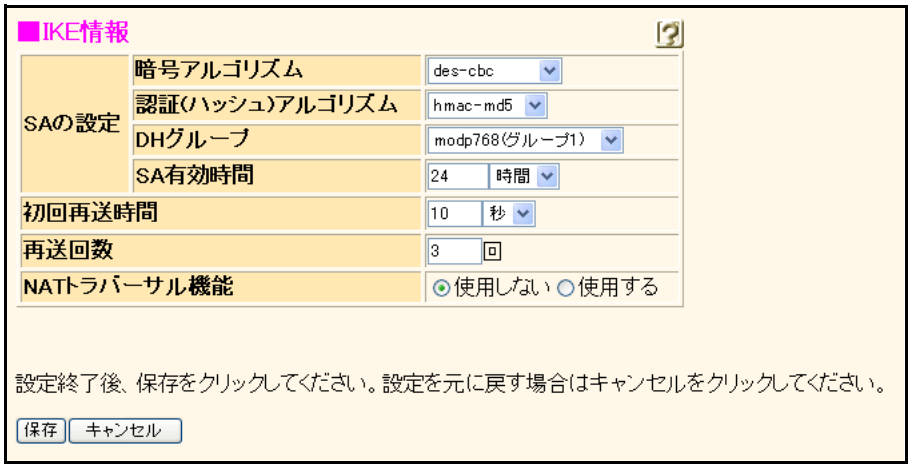
相手側の Initiator 時の SA 更新時間とデータ量と同じにならないように指定してください。

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。

12.1.4.2 IKE 情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPsec/IKE 関連］→［IKE 情報］



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

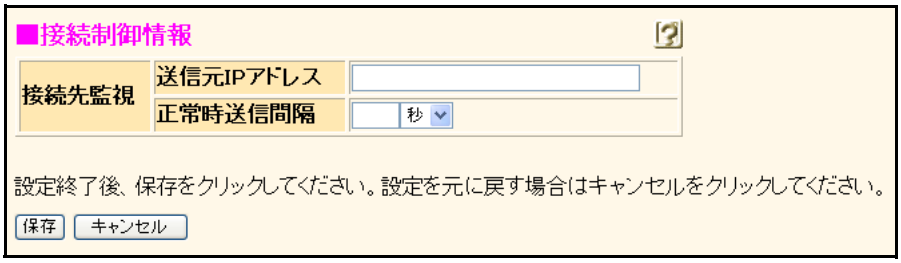
IKE ネゴシエーションパケットや ESP パケットの送信元 IP アドレス、あて先 IP アドレスまたはポート番号が NAT 変換される環境では、“ 使用する ” を選択します。

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。**

12.1.4.3 接続制御情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（RADIUS/AAA））」→［追加］→［IPsec/IKE 関連］→［接続制御情報］



接続先監視

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みなされます。あて先 IP アドレスは、接続する AAA ユーザ情報により RADIUS サーバに登録している情報を使用する場合があります。

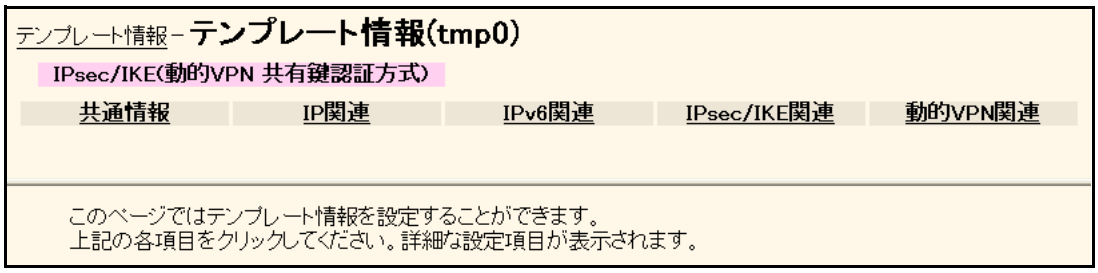
- 送信元 IP アドレス　：「テンプレート情報」の「接続制御情報」で指定した送信元 IP アドレス
- あて先 IP アドレス　：「AAA 情報」の「接続制御情報」で指定したあて先 IP アドレス
- 無通信監視タイマ　：「テンプレート情報」の「共通情報」で指定した無通信監視タイマ
  （省略または 1 ～ 9 秒が指定されている場合は 10 秒）
- 正常時送信間隔　：ICMP ECHO パケットの応答が正常に受信されている状態で、次に ICMP ECHO パケットを送信する間隔を、1 秒～ 60 秒の 10 進数で指定します。省略時は、無通信監視タイマの 1/2 を正常時送信間隔として動作します。
  （1 ～ 9 秒が指定されている場合は 5 秒）
- タイムアウト時間　：正常時送信間隔と同等
- リトライ間隔　：2 秒
- 監視モード　：無通信時に監視する

接続先監視と無通信監視タイマの動作は以下のとおりです。

	接続先監視あり		接続先監視なし
	正常時送信間隔あり	正常時送信間隔なし	
無通信監視タイマあり	正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で無通信監視タイマのみ動作する
無通信監視タイマなし	正常時送信間隔は設定値でその他は無通信監視タイマが 10 秒で設定されたものとみなし接続先監視のみ動作する	無通信監視タイマが 10 秒で設定されたものとみなし接続先監視のみ動作する	動作しない

12.2 接続種別：IPsec/IKE（動的VPN 共有鍵認証方式）

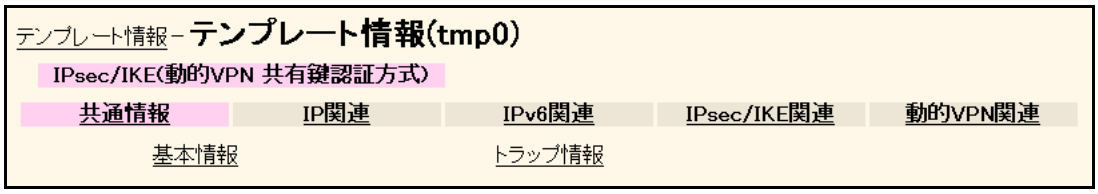
［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的VPN 共有鍵認証方式））」→［追加］



「IP 関連」および「IPv6 関連」は、「接続種別：IPsec/IKE（RADIUS/AAA）」を参照してください。

12.2.1 共通情報

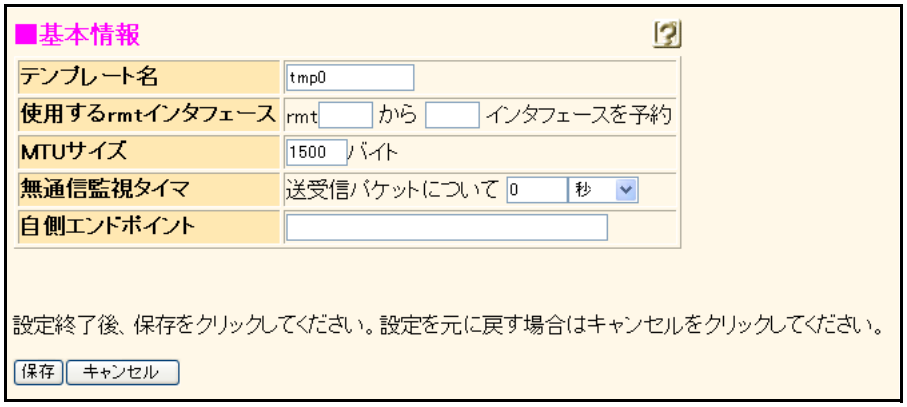
［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的VPN 共有鍵認証方式））」→［追加］→［共通情報］



「トラップ情報」は、「接続種別：IPsec/IKE（RADIUS/AAA）」を参照してください。

12.2.1.1 基本情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的VPN 共有鍵認証方式））」→［追加］→［共通情報］→［基本情報］



テンプレート名

テンプレートの名称を８文字以内で指定します。

使用する rmt インタフェース

テンプレート着信で使用する開始 rmt インタフェース番号とインタフェース数を 10 進数を使用して指定します。

こんな事に気をつけて

テンプレート着信用に予約した rmt インタフェース番号に該当する相手定義番号には一切設定しないでください。定義が存在する場合は、該当する相手定義を削除してから予約してください。予約した範囲に該当する相手定義が存在した場合は、テンプレート着信は無効になります。

MTU サイズ

テンプレート着信で使用する rmt インタフェースに対して送信するパケットの MTU 値を 10 進数を使用して 200 ～ 1500 で指定します。MTU 値を変更すると、rmt インタフェースに対して送信するパケットの最大長が変更されます。省略時は、1500 が指定されます。

無通信監視タイマ

テンプレート着信で接続したときの無通信監視時間を設定します。通信監視の対象パケットの無通信監視時間を 0 ～ 14400 秒の範囲で指定します。省略または 10 秒未満を指定した場合は、**10 秒**が指定されます。設定された間、監視対象となるパケットがない場合に無通信として IPsec 接続を切断します。

送信パケットおよび受信パケットが通信監視対象となります。

自側エンドポイント

テンプレート着信で IPsec/IKE 接続するときの自側エンドポイントの IPv4/IPv6 アドレスを指定します。

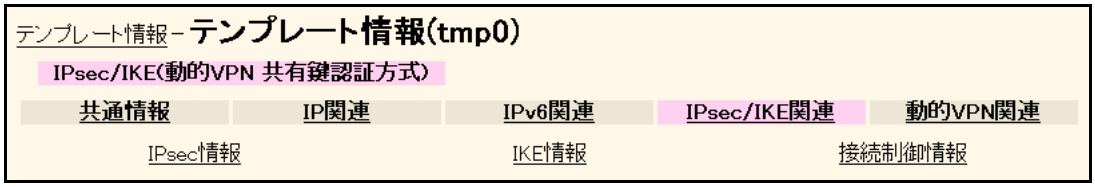
有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254
::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

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。**

12.2.2 IPsec/IKE 関連

［操作］ ルータ設定「テンプレート情報（IPsec/IKE（動的 VPN 共有鍵認証方式））」→［追加］→［IPsec/IKE 関連］



「IPsec 情報」は、「接続種別：IPsec/IKE（RADIUS/AAA）」を参照してください。

※SA 更新の Responder 時の初期画面は、"更新する" となります。

12.2.2.1 IKE 情報（動的 VPN 接続 共有鍵認証方式）

［操作］ ルータ設定「テンプレート情報（IPsec/IKE（動的 VPN 共有鍵認証方式））」→［追加］→［IPsec/IKE 関連］→［IKE 情報（動的 VPN 共有鍵認証方式）］

共有鍵認証

IKE の認証に用いる鍵を設定します。ここでは事前共有鍵（Pre-shared key）の設定を行います。事前共有鍵は、IKE を利用した IPsec 通信を行う相手ごとに、また相手装置側でも同じ鍵を設定する必要があります。

鍵識別

鍵の識別を選択します。

鍵

鍵を 16 進数および文字列で以下の範囲で指定します。

入力範囲（16 進数鍵）	入力範囲（文字列鍵）
1～256 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。

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

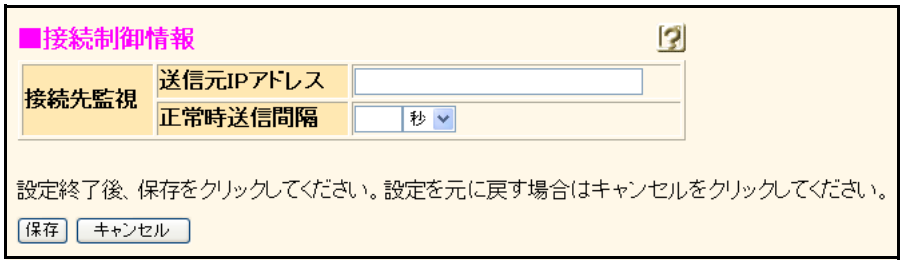
IKE の初回再送時間を 10 進数を使用して、1 ～ 60 秒の範囲で指定します。省略時は、10 秒が設定されます。

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。

12.2.2.2 接続制御情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的 VPN 共有鍵認証方式））」→［追加］→［IPsec/IKE 関連］→［接続制御情報］



接続先監視

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みなされます。接続先監視は相手装置から指定された接続先監視アドレスがあて先IPアドレスとなりますので双方の装置で指定する必要があります。片方の装置のみで接続先監視を指定した場合は、接続先監視は行われません。

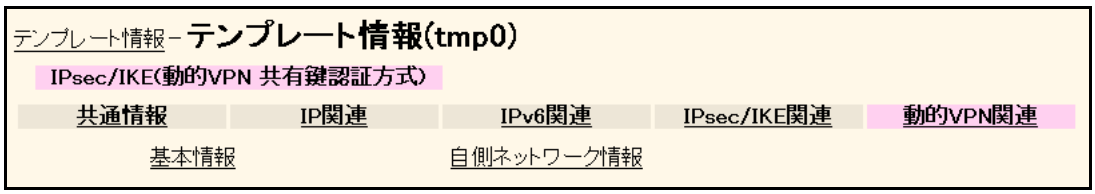
- 送信元IPアドレス　：「テンプレート情報」の「接続制御情報」で指定した送信元IPアドレス
- あて先IPアドレス　：動的VPN接続で交換された相手のIPアドレス
- 無通信監視タイマ　：「テンプレート情報」の「共通情報」で指定した無通信監視タイマ
（省略または1～9秒が指定されている場合は10秒）
- 正常時送信間隔　：ICMP ECHOパケットの応答が正常に受信されている状態で、次にICMP ECHOパケットを送信する間隔を、1秒～60秒の10進数で指定します。省略時は、無通信監視タイマの1/2を正常時送信間隔として動作します。
（1～9秒が指定されている場合は5秒）
- タイムアウト時間　：正常時送信間隔と同等
- リトライ間隔　：2秒
- 監視モード　：無通信時に監視する

接続先監視と無通信監視タイマの動作は以下のとおりです。

	接続先監視あり		接続先監視なし
	正常時送信間隔あり	正常時送信間隔なし	
無通信監視タイマあり	正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で無通信監視タイマのみ動作する
無通信監視タイマなし	正常時送信間隔は設定値でその他は無通信監視タイマが10秒で設定されたものとみなし接続先監視が動作する	無通信監視タイマが10秒で設定されたものとみなし接続先監視が動作する	無通信監視タイマが10秒で設定されたものとみなし無通信監視タイマのみ動作する

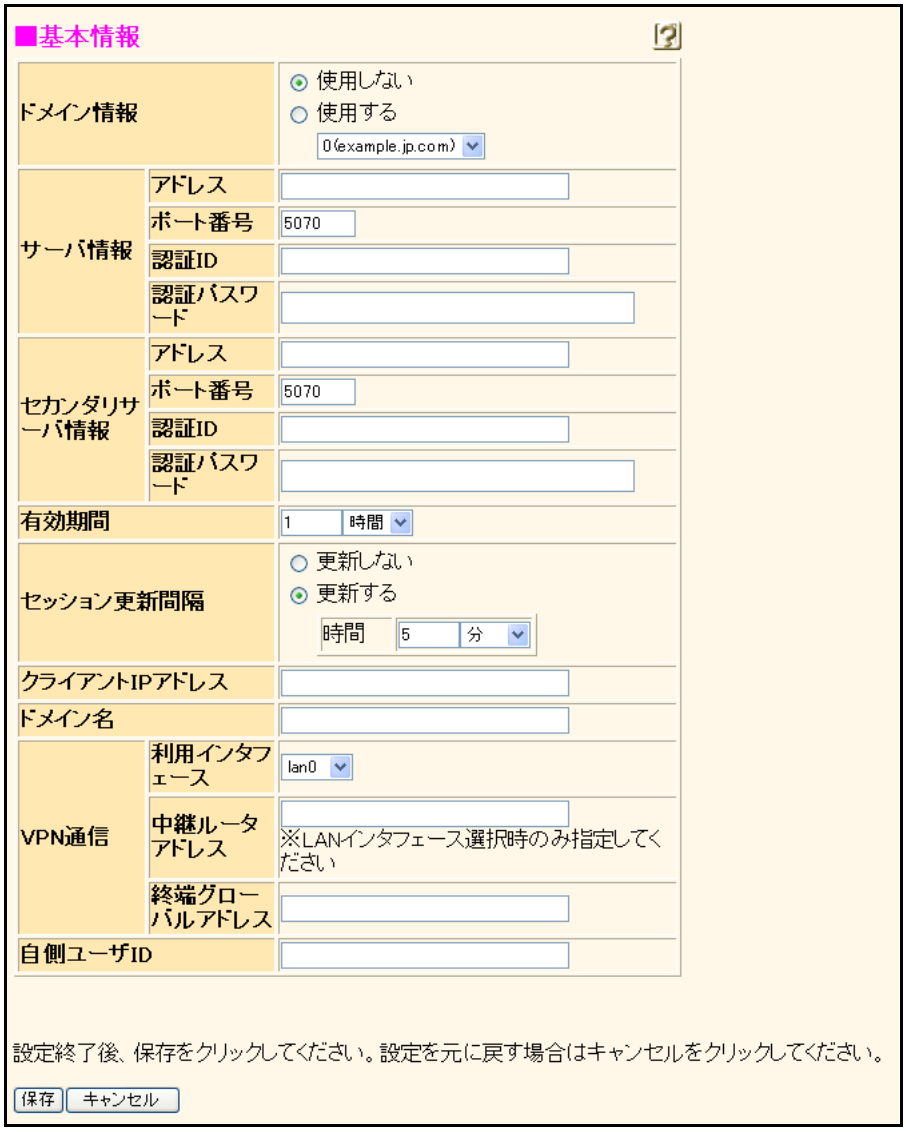
12.2.3 動的VPN関連

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的VPN 共有鍵認証方式））」→［追加］
→［動的VPN関連］



12.2.3.1 基本情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的VPN 共有鍵認証方式））」→［追加］
→［動的VPN関連］→［基本情報］



ドメイン情報

動的VPN接続で使用するドメイン情報を選択します。

“使用する”を選択すると、表示される画面が変わります。ドメイン情報だけを設定します。ドメイン情報は、「動的VPN情報」－クライアント関連情報「ドメイン情報」の設定を使用します。選択できない場合は、「動的VPN情報」－クライアント関連情報「ドメイン情報」を設定してください。

使用しない場合は、以下の項目を設定します。

サーバ／セカンダリサーバ情報

アドレス

動的VPNサーバのアドレスを指定します。

IPアドレス指定する場合

有効範囲）

1.0.0.1 ～ 126.255.255.254

128.0.0.1 ～ 191.255.255.254

192.0.0.1 ～ 223.255.255.254

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

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

FQDN指定する場合

FQDNを80文字以内で設定してください。

なお、RFC1034では英数字、"-"（ハイフン）、"."（ピリオド）でドメイン名をつけることを推奨しています。

こんな事に気をつけて

FQDN指定する場合は、クライアントIPアドレスのアドレスファミリに従ってIPアドレスを取得します。

ポート番号

動的VPNサーバが要求を受信するポート番号を10進数を使用して、1～65535の範囲で指定します。省略時は、5070が設定されます。

認証ID

動的VPNサーバへ自装置情報を登録するときに使用する認証IDを50文字以内の文字列で指定します。

認証パスワード

動的VPNサーバへ自装置情報を登録するときに使用する認証パスワードを50文字以内の文字列で指定します。

有効期間

動的VPNサーバに登録する自装置の有効期間を90～86400秒の範囲で指定します。省略時は、1時間が設定されます。

セッション更新間隔

確立した動的VPNセッションを更新する時間を90秒～3600秒の範囲で指定します。

省略時は、5分が指定されます。

“更新しない”を選択した場合、確立した動的VPNセッションを更新しません。

動的VPNセッションを更新しない場合、動的VPN接続で確立したIPsec/IKEセッションを継続 することが可能になりますが、回線障害などにより動的VPNセッションが残ってしまうことがあるので通常は、セッション更新間隔を利用してください。

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。

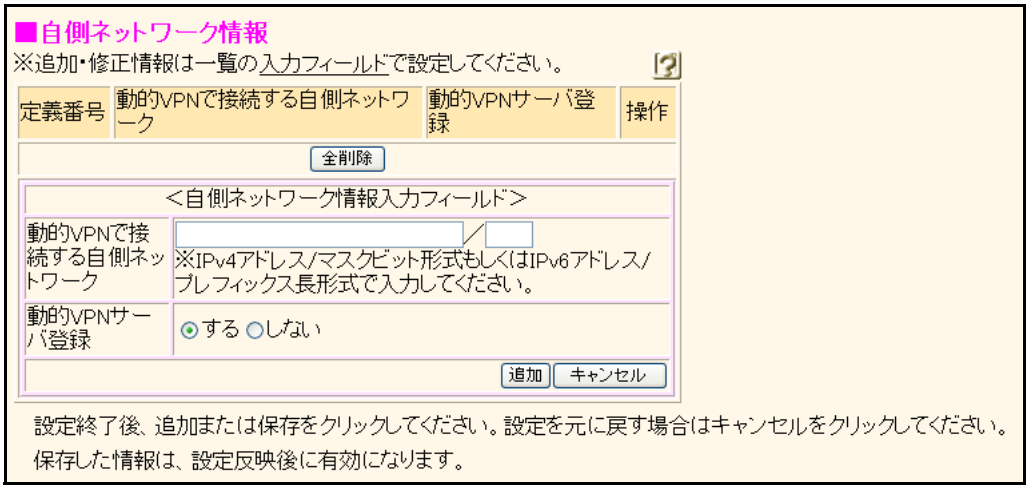
例）自側ユーザIDにshisya、ドメイン名にexample.comを指定した場合
shisya@example.com

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。

12.2.3.2 自側ネットワーク情報

［操作］　ルータ設定「テンプレート情報（IPsec/IKE（動的 VPN 共有鍵認証方式））」→［追加］
→［動的 VPN 関連］→［自側ネットワーク情報］



現在、設定されている自側ネットワーク情報の定義が表示されています。自側ネットワークの定義数は、20 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

動的 VPN で接続する自側ネットワーク

動的 VPN で接続する自側ネットワークを IPv4 アドレスとマスクビット数（またはマスク値）または IPv6 アドレスとプレフィックス長で指定します。

- IPv4 アドレスを指定する場合
  IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  デフォルトルートを設定する場合は、
  0.0.0.0/0（0.0.0.0/0.0.0.0）を指定します。
- IPv6 アドレスを指定する場合
  IPv6 アドレスとプレフィックスの組み合わせで指定します。リンクローカルアドレスは指定できません。
  デフォルトルートを設定する場合は、::/0 を指定します。
  IPv6 DHCP クライアントが取得したプレフィックスを使用する場合は、上位を“dhcp@インタフェース名”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。

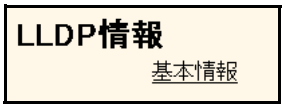
“する”を設定した場合、通信パケット契機で動的 VPN 接続をすることができます。

“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
IPsecIKE)c0a80100/24@example.com
IPsecIKE)2001:db8:1111:1::/64@example.com

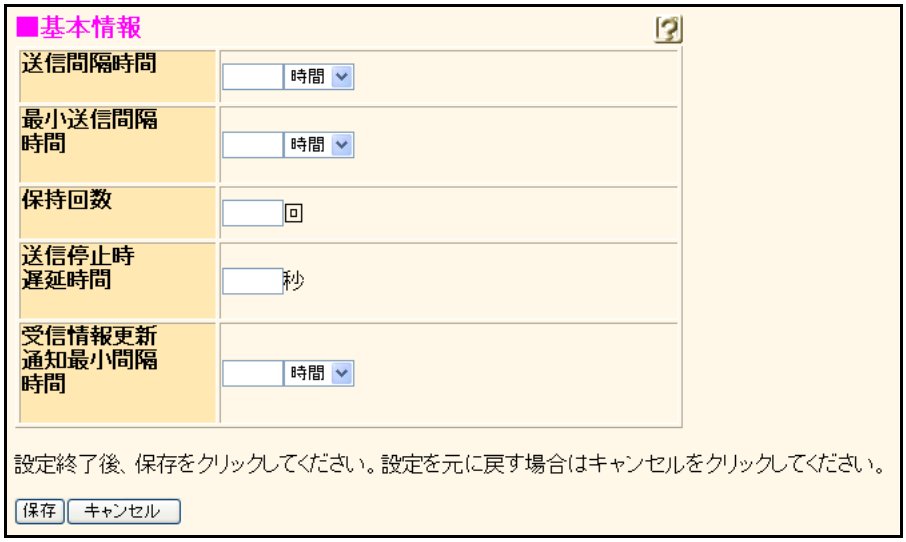
13　LLDP 情報

［操作］　ルータ設定「LLDP 情報」



13.1　基本情報

［操作］　ルータ設定「LLDP 情報」→［基本情報］



LLDP（Link Layer Discovery Protocol：隣接探索プロトコル）の装置全体に関する設定を行います。

こんな事に気をつけて

ポートごとの設定は、「LAN 情報」-「基本情報」-「LLDP 情報」で行ってください。

送信間隔時間

LLDP 情報を定期的に送信する間隔時間を 5 ～ 32768 秒の範囲で指定します。

最小送信間隔時間

最小送信間隔時間を 1 秒～（0.25× 送信間隔時間）の範囲で指定します。

設定変更などにより LLDP 情報が変化したときに即座に LLDP 情報を送信しますが、最後に LLDP 情報を送信してから最小送信間隔時間経過していない場合は、最小送信間隔時間が経過するまで待ってから LLDP 情報を送信します。

保持回数

本装置の LLDP 情報を受信した隣接装置が本装置の LLDP 情報を保持すべき有効時間を、送信間隔時間の回数で 2 ～ 10 回の範囲で指定します。

本装置の LLDP 情報の有効時間（TTL）は以下の式により計算されます。

有効時間＝送信間隔時間×保持回数

ただし、計算結果が 65535 秒を超えた場合は、有効時間を 65535 秒とします。

送信停止後遅延時間

「LAN 情報」-「基本情報」-「LLDP 情報」の「動作」で LLDP 情報を送信しないように設定変更したとき、送信処理を初期状態に戻すまでの遅延時間を 1 ～ 10 秒の範囲で指定します。

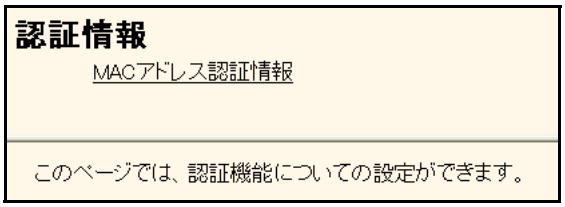
受信情報更新通知最小間隔時間

受信情報更新通知の最小間隔時間を 5 ～ 3600 秒の範囲で指定します。

受信情報（隣接情報）が更新されたときに SNMP トラップを送信して受信情報が更新されたことを通知します。そのあと、最小間隔時間が経過するまでの間に受信情報が何度更新されても SNMP トラップを送信しないで、最小間隔時間経過後に SNMP トラップを 1 回だけ送信して受信情報が更新されたことを再通知します。

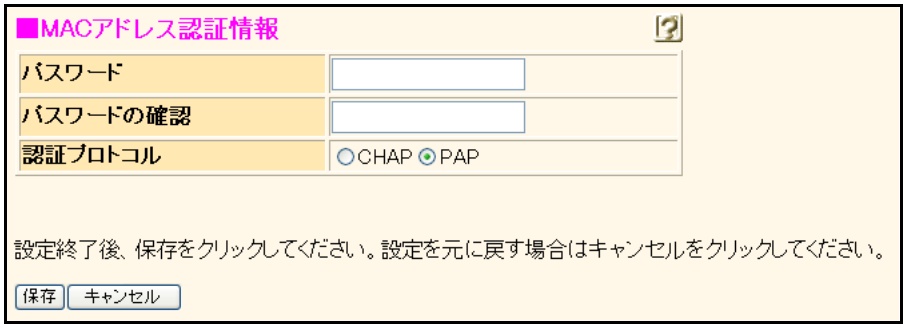
14　認証情報

［操作］　ルータ設定「認証情報」



14.1　MACアドレス認証情報

［操作］　ルータ設定「認証情報」→［MACアドレス認証情報］



パスワード

MACアドレス認証で使用するパスワードを、0x21、0x23～0x7eの文字で構成される128文字以内の文字列で指定します。省略時は、認証端末のMACアドレスをパスワードとして使用します。

パスワードの確認

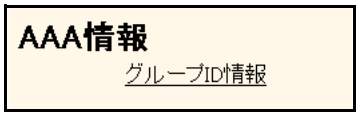
上記で指定したパスワードをもう一度指定します。

認証プロトコル

MACアドレス認証の認証プロトコルを選択します。

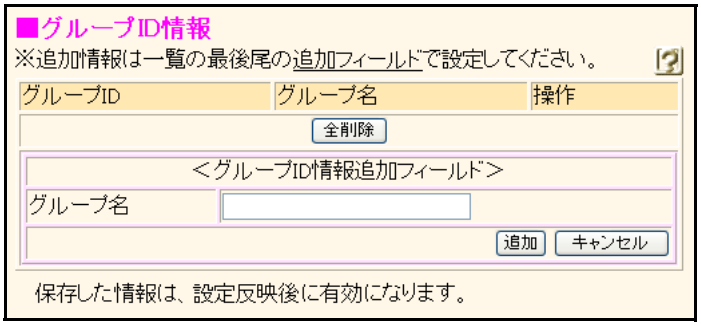
15　AAA 情報

［操作］　ルータ設定「AAA 情報」



15.1　グループ ID 情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］



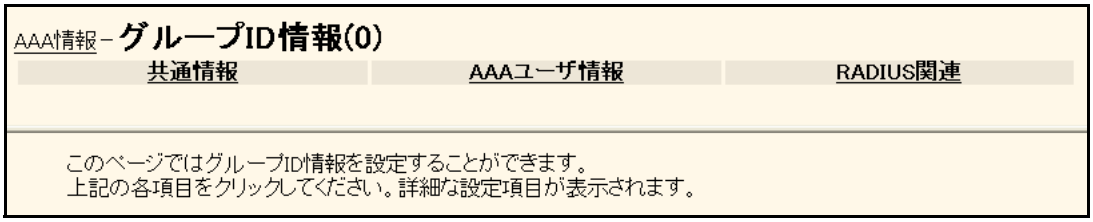
現在、設定されているグループ ID 情報の定義が表示されています。グループ ID 情報の定義数は、10 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

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

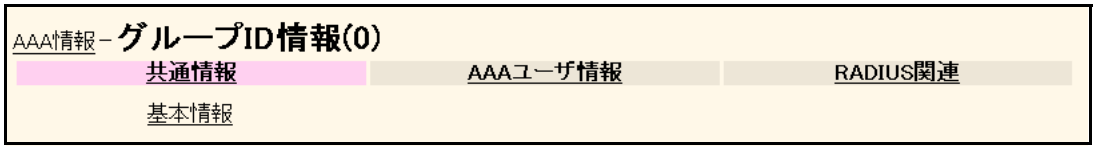
グループ名を 0x21、0x23 ～ 0x7e の 32 文字以内の ASCII 文字列で指定します。

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］



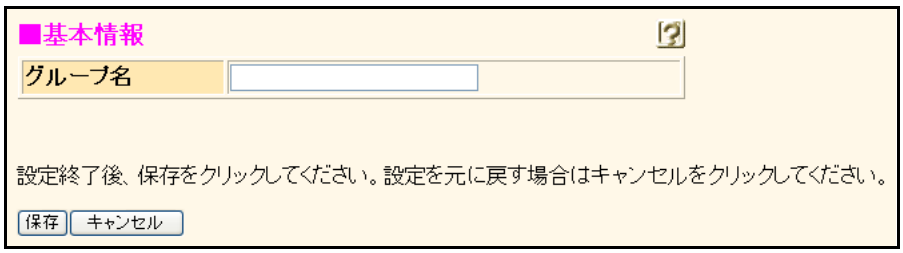
15.1.1　共通情報

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



15.1.1.1 基本情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［共通情報］→［基本情報］

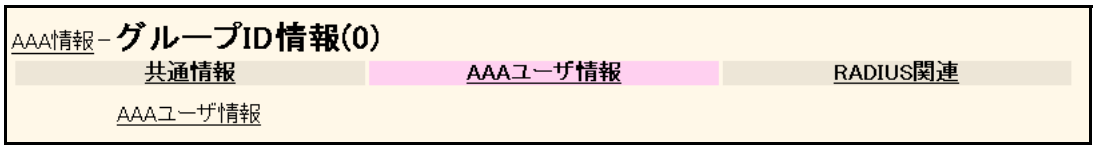


グループ名

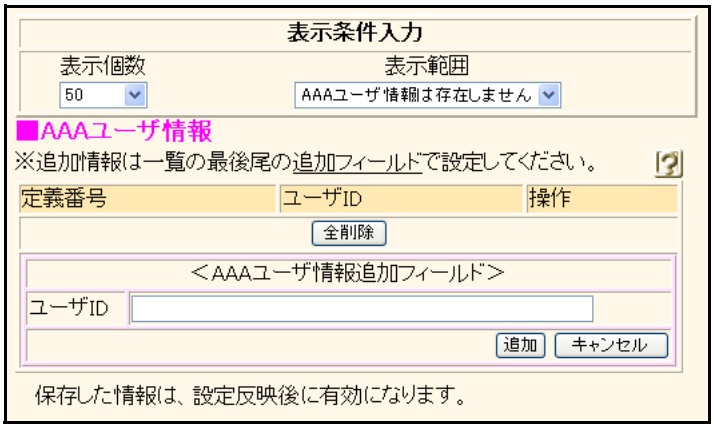
グループ名を 0x21、0x23～0x7e を使用して 32 文字以内で指定します。

15.1.2 AAA ユーザ情報

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



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

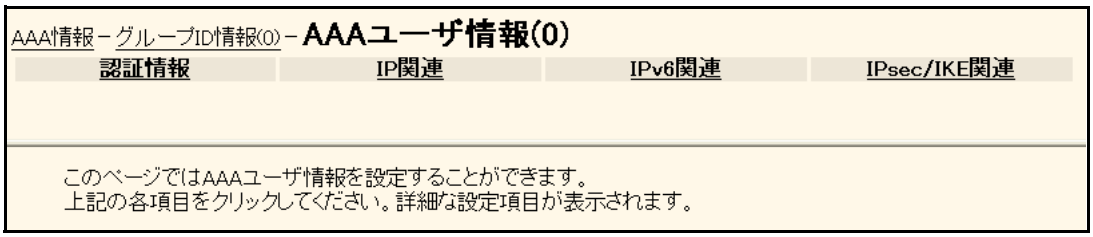


現在、設定されている AAA ユーザ情報の定義が表示されています。AAA ユーザ情報の定義数は、装置全体で 200 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

ユーザ ID

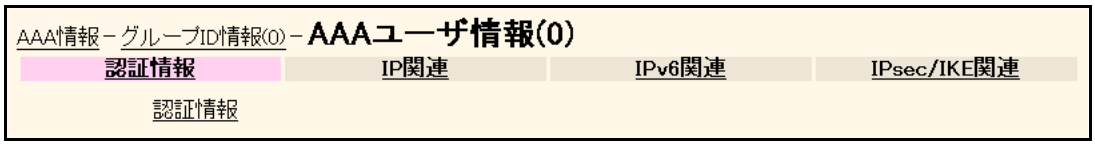
ユーザ ID を 0x21、0x23～0x7e を使用して 64 文字以内で指定します。
MAC アドレス認証で利用する場合は、アクセスを許可する端末の MAC アドレスを 16 進数 12 桁（コロンで区切らない）で指定してください。
省略時は認証情報を使用できません。

［操作］　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］

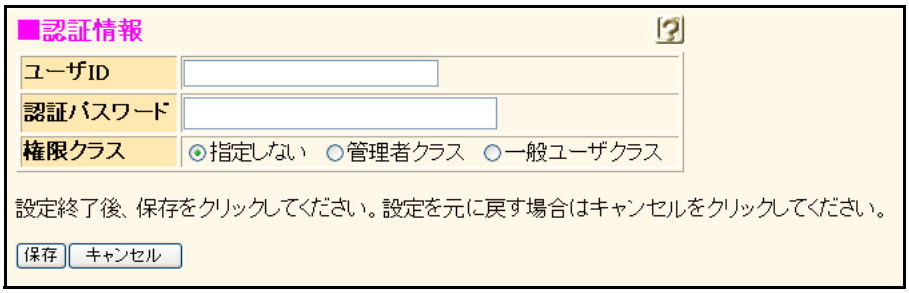


15.1.2.1　認証情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［認証情報］



［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［認証情報］→［認証情報］



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。

権限クラス

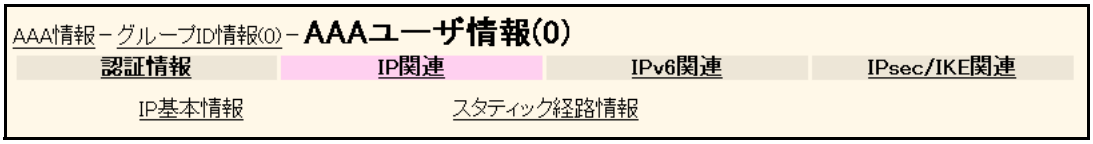
ログインユーザを設定する場合は、権限クラスを設定します。

「パスワード情報」-「ログインユーザ情報」の設定によって、以下を選択します。

- “ 権限クラスは AAA/RADIUS サーバで指定する ” を選択した場合
  “ 管理者クラス ” または “ 一般ユーザクラス ” を選択します。
- “ 権限クラスによって参照する AAA を分ける ” を選択した場合
  “ 指定しない ” を選択します。

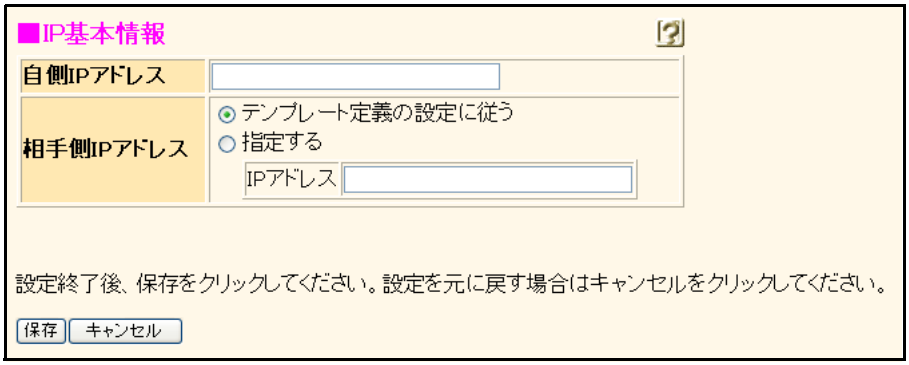
15.1.2.2 IP関連

［操作］　ルータ設定「AAA情報」→［グループID情報］→［追加］→［AAAユーザ情報］→［追加］→［IP関連］



15.1.2.2.1 IP基本情報

［操作］　ルータ設定「AAA情報」→［グループID情報］→［追加］→［AAAユーザ情報］→［追加］→［IP関連］→［IP基本情報］



自側IPアドレス

自側IPアドレスを指定します。省略または0.0.0.0を指定した場合は、IPアドレスなし（unnumbered）として動作します。

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

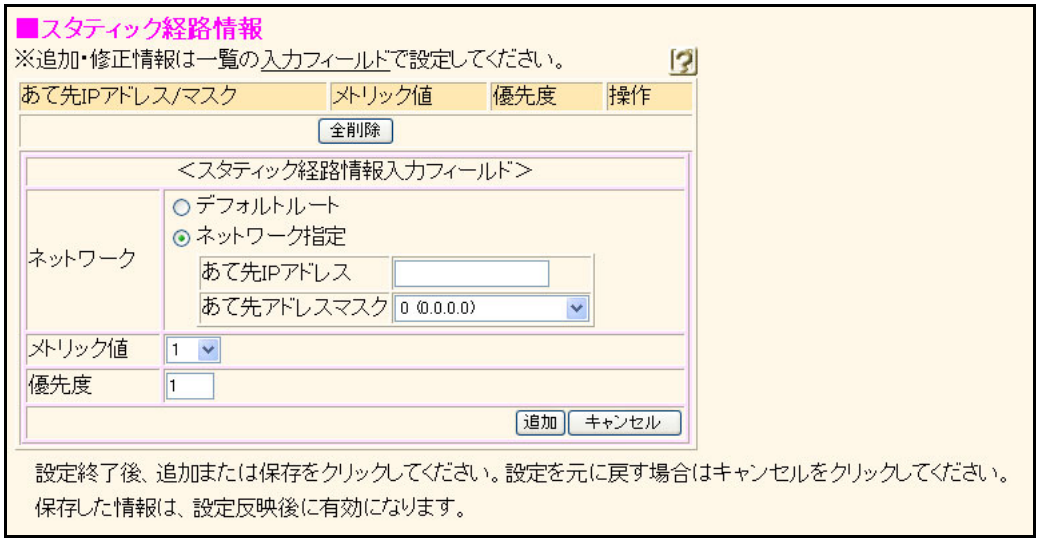
相手側IPアドレス

相手側IPアドレスとしてテンプレート定義で指定した割当てIPアドレスの設定内容に従うか、個別に指定するかを選択します。“指定する”を選択し、0.0.0.0を指定した場合は、設定をIPアドレスなし（unnumbered）として動作します。

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

15.1.2.2.2 スタティック経路情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IP 関連］→［スタティック経路情報］



現在、設定されているスタティック経路情報の定義が表示されます。スタティック経路の定義数は、装置全体で 128 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

ネットワーク

“ デフォルトルート ” または “ ネットワーク指定 ” を選択します。“ ネットワーク指定 ” を選択した場合は、あて先 IP アドレス／アドレスマスクを指定します。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1 ～ 15 から選択します。RIP に再配布したときは、設定した RIP メトリック値 +1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10 進数を使用して 1 ～ 254 の範囲で指定します。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

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

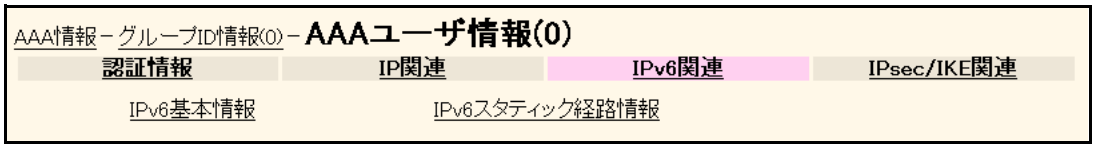
複数のスタティック経路情報で ECMP 機能を使用するときは、あて先、RIP メトリック値、優先度がそれぞれ同じになるようにスタティック経路情報を設定します。また、ECMP 機能を使用する場合は、「ルーティングプロトコル情報」－「ルーティングマネージャ情報」にある「ECMP 情報」で ECMP を使用するように設定します。ECMP となるスタティック経路情報は、同じあて先への経路情報ごとに装置全体で 4 個まで定義できます。

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合、優先度が同じで、メトリック値が違うスタティック経路情報は同時に設定できません。

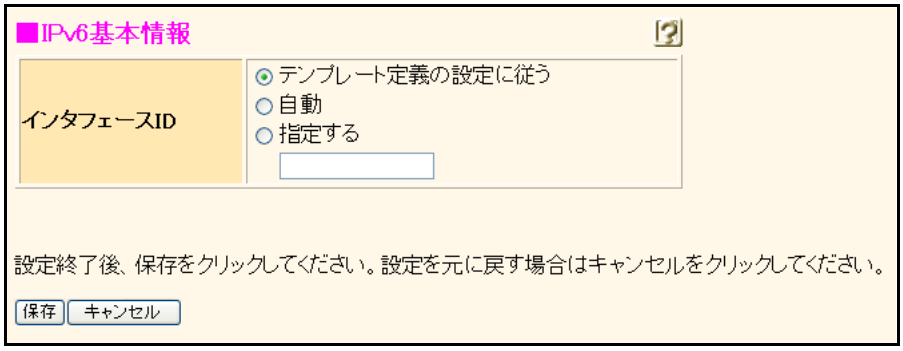
15.1.2.3 IPv6 関連

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPv6 関連］



15.1.2.3.1 IPv6 基本情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPv6 関連］→［IPv6 基本情報］



インタフェース ID

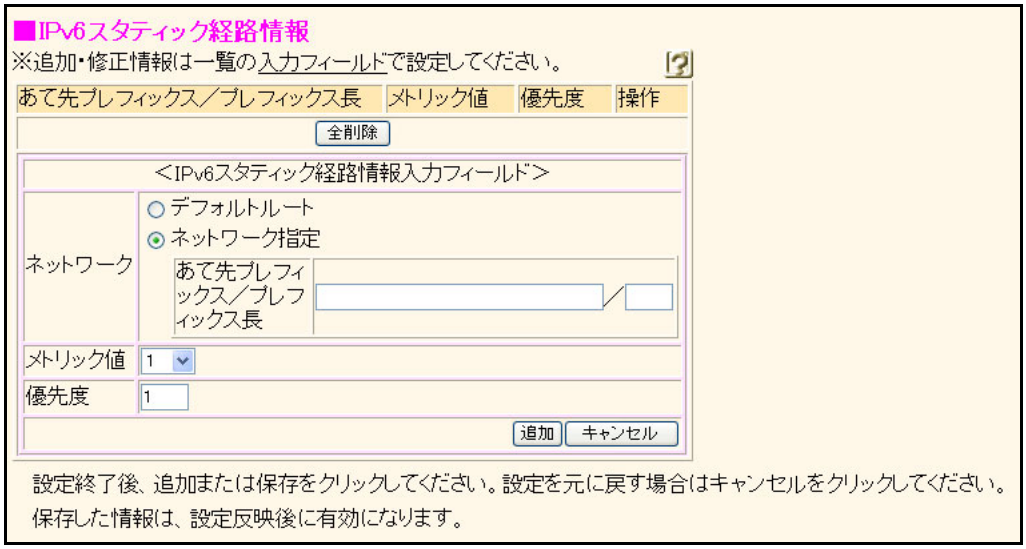
“ 自動 ” を選択する場合は、装置の MAC アドレスから自動生成されるインタフェース ID を使用します。通常は、“ 自動 ” を選択します。

“ 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

15.1.2.3.2 IPv6 スタティック経路情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPv6 関連］→［IPv6 スタティック経路情報］



現在、設定されているスタティック経路情報の定義が表示されます。IPv6 スタティック経路の定義数は、装置全体で 128 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

IPv6 経路情報を固定で設定できます。ただし、デフォルトルートは装置に 1 つしか設定できません。

ネットワーク

“ デフォルトルート ” または “ ネットワーク指定 ” を選択します。“ ネットワーク指定 ” を選択した場合は、あて先プレフィックス／プレフィックス長を指定します。あて先ネットワークにリンクローカルアドレスは指定できません。

メトリック値

このスタティック経路情報を RIP に再配布するときのメトリック値を、1 ～ 15 から選択します。RIP に再配布したときは、設定した RIP メトリック値 +1 のメトリック値で RIP テーブルに登録されます。

優先度

このスタティック経路情報の優先度を、10 進数を使用して 1 ～ 254 の範囲で指定します。優先度は、同じあて先への経路情報が複数あるときに優先経路を選択するために使用され、より小さい値が、より高い優先度を示します。スタティック経路情報以外の優先度には、以下の初期値が設定されています。

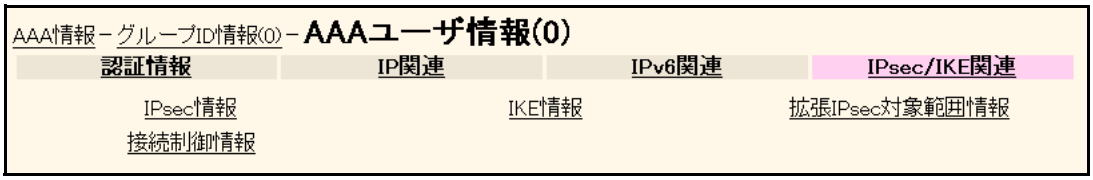
プロトコル	優先度
RIP	120
DNS	15
DHCP	10

こんな事に気をつけて

同じネットワーク（あて先）へのスタティック経路情報を複数設定する場合、優先度が同じスタティック経路情報は同時に設定できません。

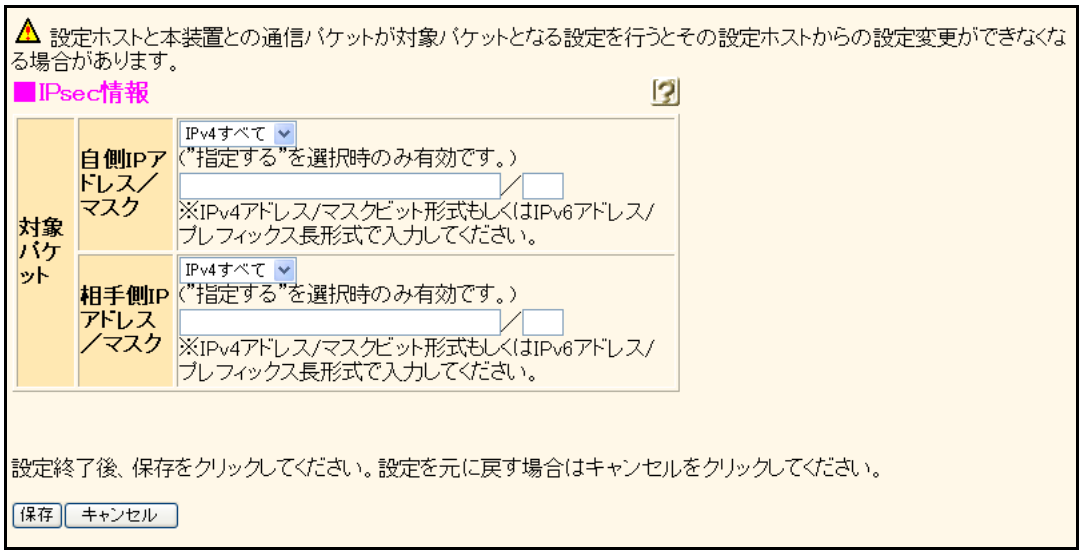
15.1.2.4 IPsec/IKE 関連

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPsec/IKE 関連］



15.1.2.4.1 IPsec 情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPsec/IKE 関連］→［IPsec 情報］



対象パケット

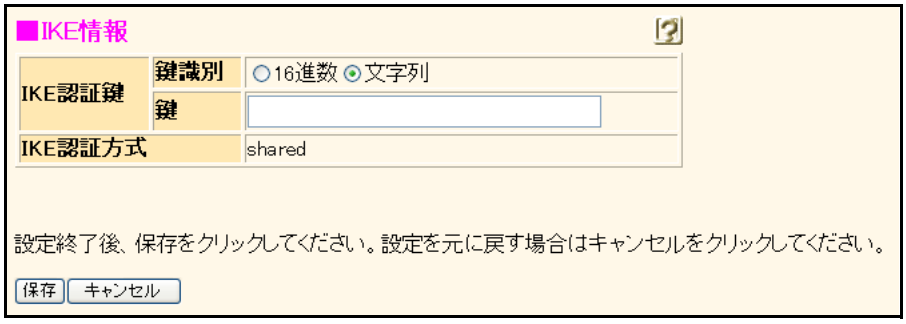
自側／相手側 IP アドレス／マスク

IPsec を適用するセッションの送信元 IP アドレスおよびアドレスマスクと、あて先 IP アドレスおよびアドレスマスクを以下の 3 つから選択します。アドレスを指定する場合は、“ 指定する ” を指定します。

- IPv4 すべて
  IPv4 アドレスをすべて選択します。
- IPv6 すべて
  IPv6 アドレスをすべて選択します。
- 指定する
  IP アドレス／マスクを IPv4/IPv6 形式で指定します。

15.1.2.4.2 IKE 情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPsec/IKE 関連］→［IKE 情報］



IKE 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。

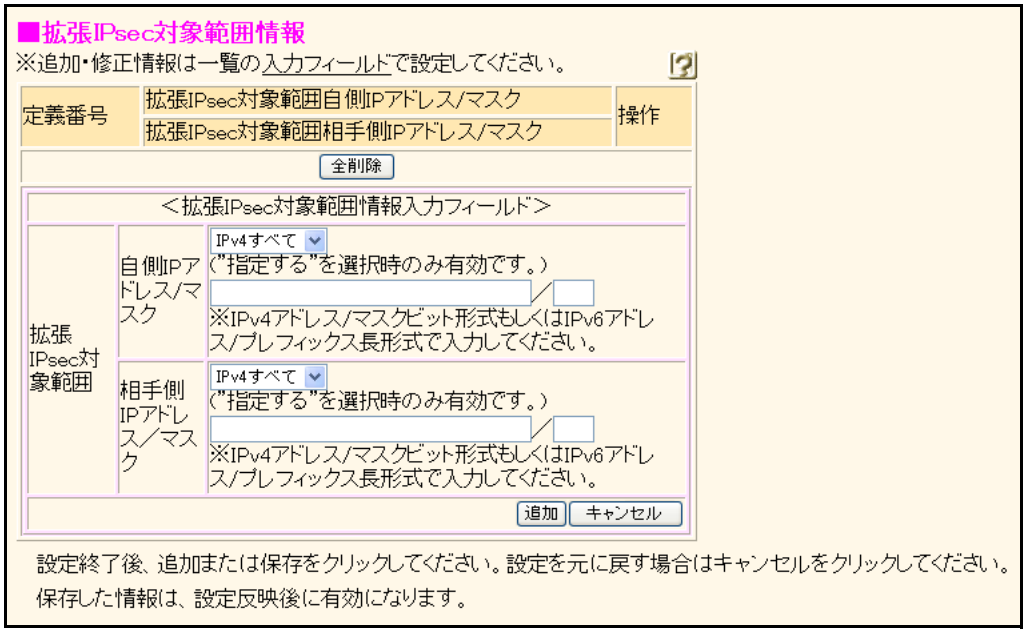
入力範囲（16 進数鍵）	入力範囲（文字列鍵）
1～256 桁	1～128 文字

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。

15.1.2.4.3 拡張 IPsec 対象範囲情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPsec/IKE 関連］→［拡張 IPsec 対象範囲情報］



現在、設定されている拡張 IPsec 対象範囲情報の定義が表示されています。拡張 IPsec 対象範囲の定義数は、装置全体で 50 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。

拡張 IPsec 対象範囲設定は、自側（相手側）IP アドレス／アドレスマスクを複数定義することができます。

拡張 IPsec 対象範囲設定は、IPsec 情報の対象パケットで定義した対象パケット以外を通過させる機能であるため、Security Policy Database（SPD）や IKE ネゴシエーション（自動鍵設定のみ）には使用されません。

SPD や IKE ネゴシエーションに使用する ID ペイロードの設定（自動鍵設定のみ）は、IPsec 情報の対象パケットで設定してください。

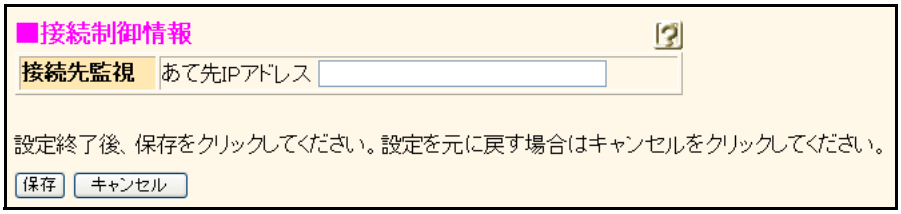
自側（相手側）IP アドレス／アドレスマスク

自側（相手側）アドレス／アドレスマスクを複数定義することができます。

拡張 IPsec 対象範囲の送信元 IP アドレスおよびアドレスマスクと、あて先 IP アドレスおよびアドレスマスクを指定します。IPv4 形式または IPv6 形式のアドレスを設定してください。

15.1.2.4.4 接続制御情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［AAA ユーザ情報］→［追加］→［IPsec/IKE 関連］→［接続制御情報］



接続先監視

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みなされます。

- 送信元IPアドレス　：「テンプレート情報」－「接続制御情報」で指定する送信元IPアドレス
- あて先IPアドレス　：「AAA情報」－「接続制御情報」で指定するあて先IPアドレス
- 無通信監視タイマ　：「テンプレート情報」－「共通情報」で指定する無通信監視タイマ（省略または1～9秒が指定されている場合は10秒）
- 正常時送信間隔　：「テンプレート情報」－「接続制御情報」で指定する正常時送信間隔 指定する無通信監視タイマの1/2（1～9秒が指定されている場合は5秒）
- タイムアウト時間　：指定する無通信監視タイマの1/2（1～9秒が指定されている場合は5秒）
- リトライ間隔　：2秒
- 監視モード　：無通信時に監視する

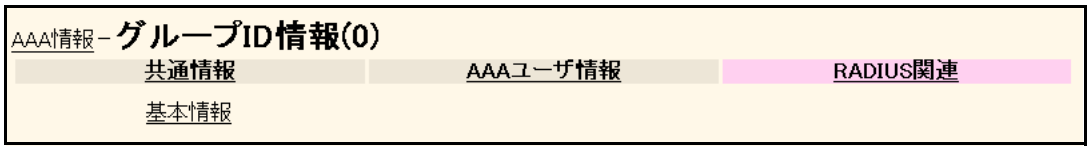
接続先監視と無通信監視タイマの動作は以下のとおりです。

	接続先監視あり		接続先監視なし
	正常時送信間隔あり	正常時送信間隔なし	
無通信監視タイマあり	正常時送信間隔は設定値でその他は無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で動作する	無通信監視タイマの設定値で無通信監視タイマのみ動作する
無通信監視タイマなし	正常時送信間隔は設定値でその他は無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する	無通信監視タイマが10秒で設定されたものとみなし接続先監視のみ動作する	動作しない

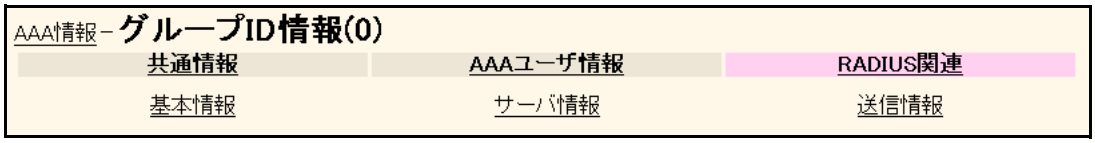
15.1.3 RADIUS 関連

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

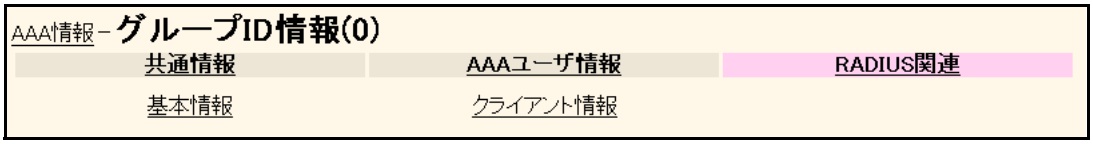
「基本情報」の RADIUS サービスで、“ 使用しない ” を選択して保存した場合



「基本情報」の RADIUS サービスで、“ クライアント機能 ” を選択して保存した場合

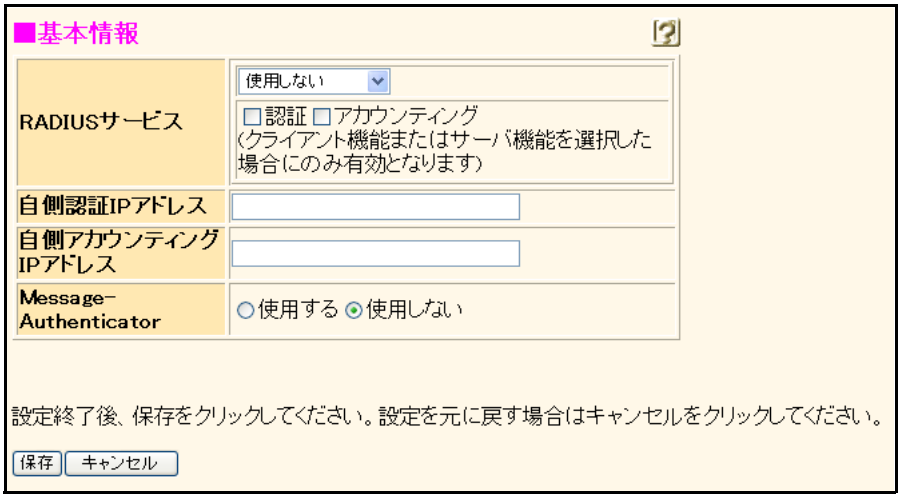


「基本情報」の RADIUS サービスで、“ サーバ機能 ” を選択して保存した場合



15.1.3.1 基本情報

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［RADIUS 関連］→［基本情報］



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。

自側アカウンティング IP アドレス

自側 RADIUS アカウンティング装置の IP アドレスを指定します。

有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254
::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

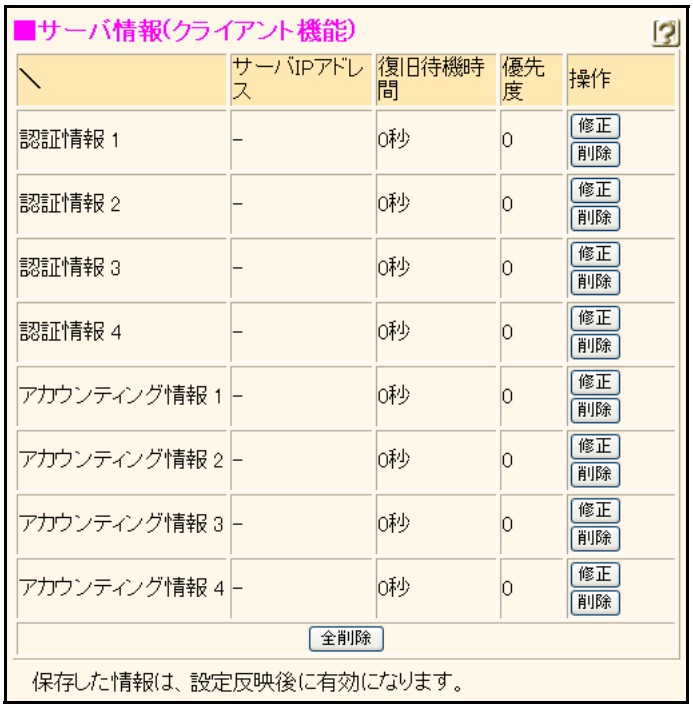
本装置を RADIUS アカウンティングサーバとして使用する場合は、RADIUS アカウンティングクライアントと通信するときに使用する IP アドレスを設定します。本装置を RADIUS アカウンティングクライアントとして使用する場合は、RADIUS アカウンティングサーバと通信するときに使用する IP アドレスを設定します。省略時は、相手側の RADIUS アカウンティング装置と通信する自側 IP アドレスを自動的に選択するものとみなされます。

Message-Authenticator

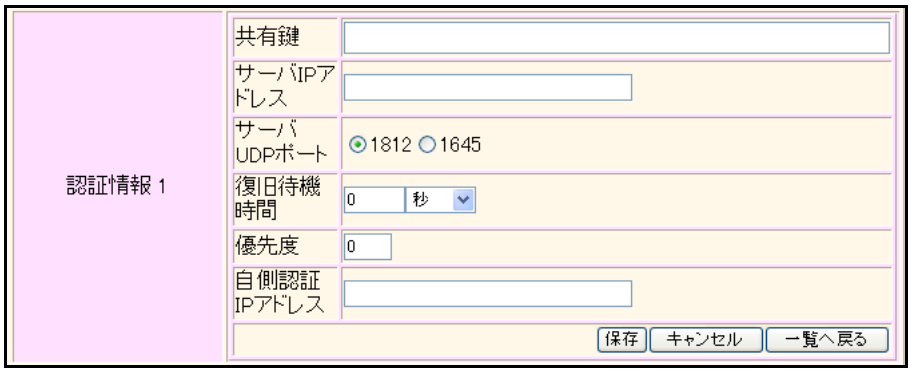
Message-Authenticator による認証を行う場合は、“ 使用する ” を選択します。本装置では、認証要求メッセージにのみ使用します。

15.1.3.2 サーバ情報（クライアント機能）

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［RADIUS 関連］→［サーバ情報（クライアント機能）］



認証情報



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。

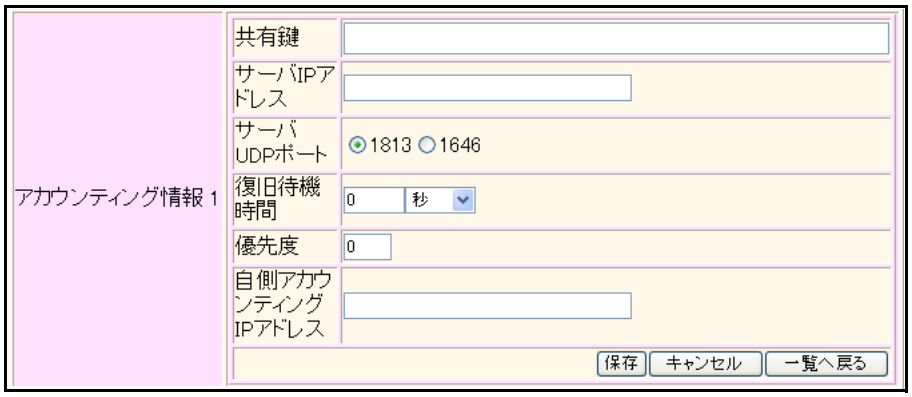
自側認証 IP アドレス

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

このクライアントで RADIUS 認証サーバとの通信に使用する IP アドレスを設定してください。省略時は、RADIUS 関連「基本情報」の自側認証 IP アドレスの設定に従います。

アカウンティング情報



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ティング要求するRADIUSアカウンティングサーバのUDPポート番号を設定します。

- 1813
  アカウンティング要求するRADIUSアカウンティングサーバが最新のRFC仕様のUDPポートで実装されている場合
- 1646
  アカウンティング要求するRADIUSアカウンティングサーバが旧RFC仕様のUDPポートで実装されている場合

復旧待機時間

RADIUSサーバがdead状態になってから、自動的に再びalive状態に復旧するまでの時間を指定します。単位は、日、時間、分、秒のどれかを指定します。

有効範囲）

0 ～ 86400 秒

0 ～ 1440 分

0 ～ 24 時間

0 ～ 1 日

0秒を指定した場合は、自動的にalive状態に復旧しません。省略時は、自動的に復旧しません。

RADIUSサーバから送信間隔と再送間隔で設定した応答待ち受け時間を経過しても応答が得られなかった場合、そのRADIUSサーバは dead 状態となり、優先度は最非優先となります。dead 状態となったRADIUSサーバは、alive状態のサーバが存在する限り使わなくなります。本設定は、dead 状態になってから、設定した優先度となる alive状態へ自動的に復旧するための待ち時間を設定します。

dead状態からalive状態に復旧するためには、以下の条件を満たす必要があります。

- 本設定の時間が経過した場合
- 利用可能なすべてのサーバが dead 状態となったあと、dead 状態のRADIUSサーバにパケットを送信し、応答が得られた場合
- 運用コマンドで、手動で復旧させた場合

優先度

同一グループ内での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。

自側アカウンティングIPアドレス

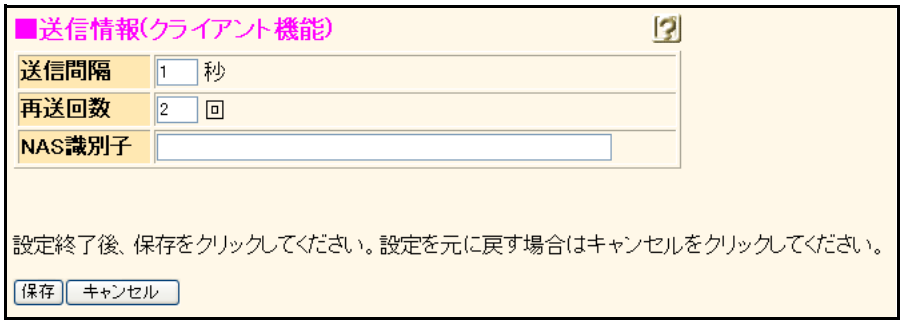
自側RADIUSアカウンティング装置でこのクライアントに対して使用するIPアドレスを設定します。本定義の内容は、RADIUS関連「基本情報」の自側アカウンティングIPアドレスの設定より優先されます。

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

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

15.1.3.3 送信情報（クライアント機能）

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［RADIUS 関連］→［送信情報（クライアント機能）］



送信間隔

RADIUS サーバ未応答時のパケットの送信間隔を 10 進数を使用して、1 ～ 10 秒の範囲の秒単位で指定します。

再送回数

RADIUS サーバ未応答時のパケットの再送回数を 10 進数を使用して、1 ～ 10 回の範囲で指定します。

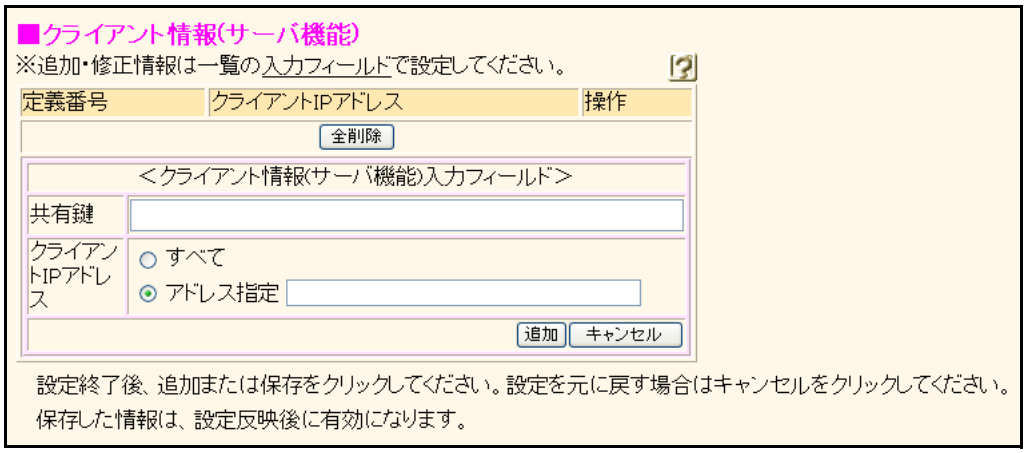
サーバからの応答待ち受け時間は、送信間隔 ×（再送回数 ＋ 1）秒となります。省略時は送信間隔を 1 秒、再送回数を 2 回として動作します。この場合は、サーバからの応答待ち受け時間パケットの初回送信後、3 秒となります。

NAS 識別子

RADIUS 認証クライアントおよびアカウンティングクライアントが RADIUS サーバに送出する NAS-Identifier アトリビュートの値を 64 文字以内で指定します。省略時は、NAS-Identifier アトリビュートを送信しません。

15.1.3.4 クライアント情報（サーバ機能）

［操作］　ルータ設定「AAA 情報」→［グループ ID 情報］→［追加］→［RADIUS 関連］→［クライアント情報（サーバ機能）］



現在、設定されている RADIUS 情報（サーバ機能）の定義が表示されています。クライアント情報（サーバ機能）の定義数は、1 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。

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。

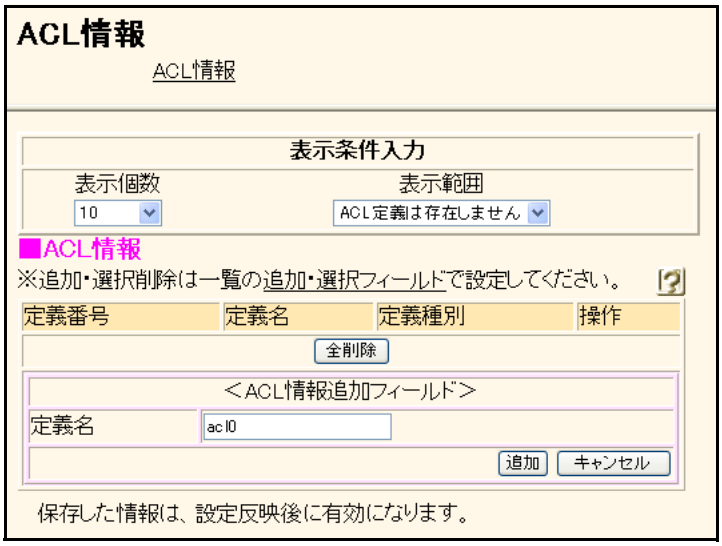
クライアント IP アドレス

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

16　ACL 情報

［操作］　ルータ設定「ACL 情報」

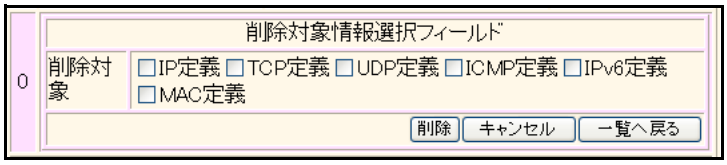


現在、設定されている ACL 定義が表示されています。ACL の定義数は、150 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

定義名

ACL 定義を識別する定義名を 50 文字以内で指定します。

［操作］　ルータ設定「ACL 情報」→［選択削除］

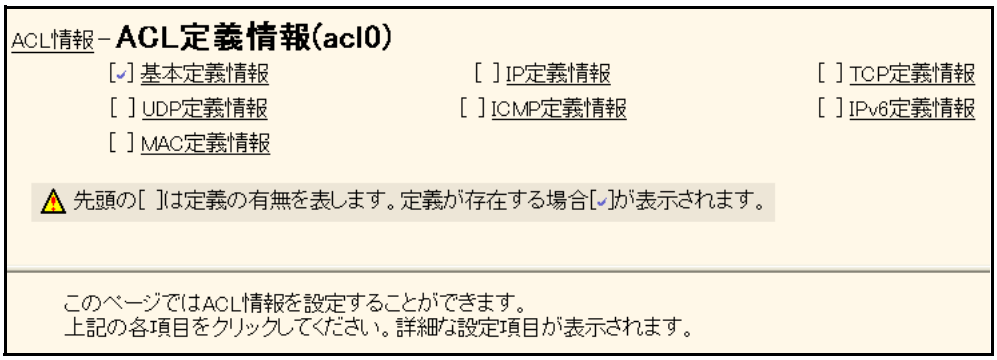


削除対象

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。

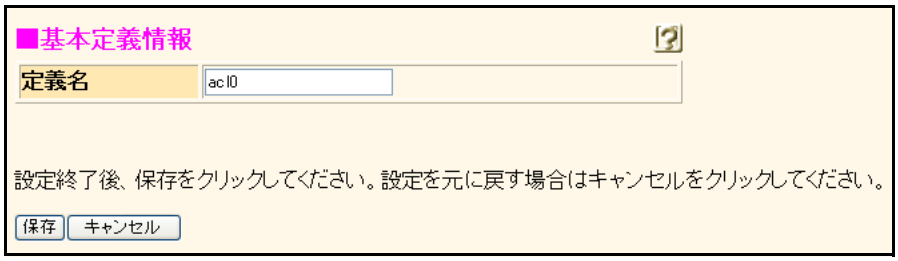
16.1 ACL 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］



16.1.1 基本定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［基本定義情報］

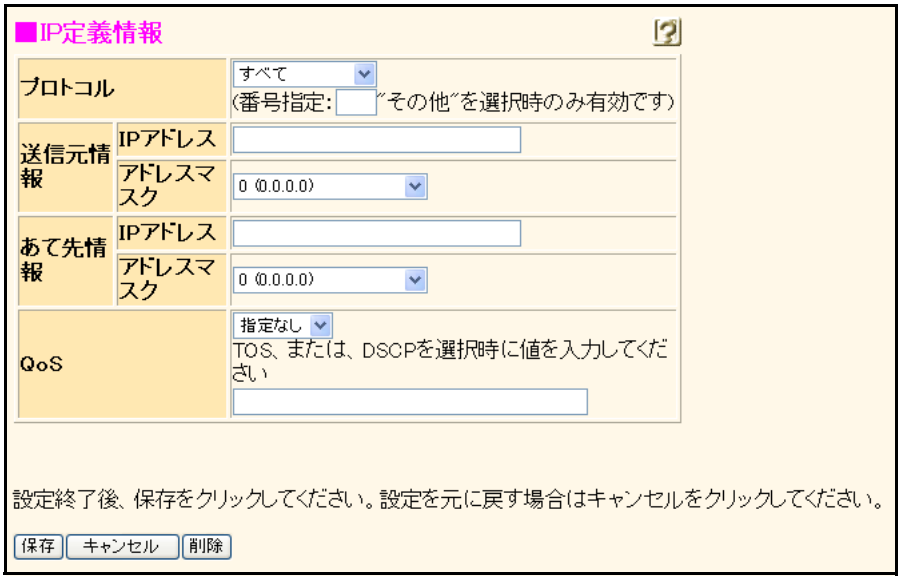


定義名

ACL 定義を識別する定義名を 50 文字以内で指定します。

16.1.2　IP 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［IP 定義情報］



プロトコル

IP 定義としてプロトコルを以下の 6 つから選択します。() 内はプロトコル番号です。

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

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

送信元／あて先情報

IP 定義としてのアドレス情報を設定します。

IP アドレス／アドレスマスク

IP 定義としての IP アドレスおよびアドレスマスクを指定します。以下が等しい場合に条件に一致します。

- チェック対象となるパケットの IP アドレスと定義するアドレスマスクの論理積
- 定義する IP アドレスとアドレスマスクの論理積

0.0.0.0/0 を指定した場合、または、省略した場合はすべての IP アドレス／アドレスマスクを対象とします。

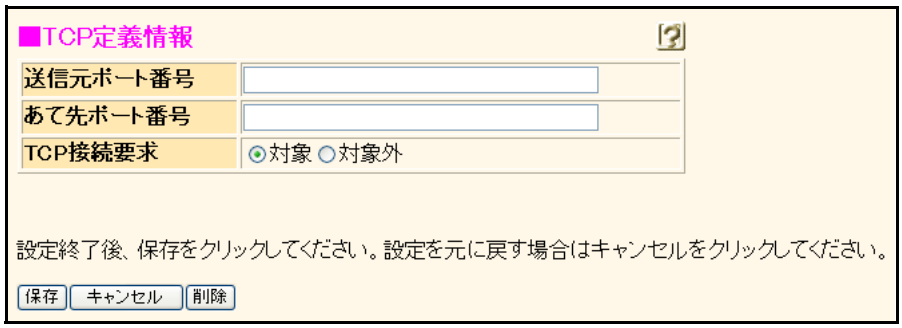
QoS

対象とする QoS を判断する方法を以下の 3 つから選択します。

- 指定なし
  すべての TOS 値、および、すべての DSCP 値を対象とする場合に選択します。
- TOS
  TOS 値で対象を判断する場合に選択します。複数指定する場合は、“,” で区切ります。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

16.1.3　TCP 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［TCP 定義情報］



送信元／あて先ポート番号

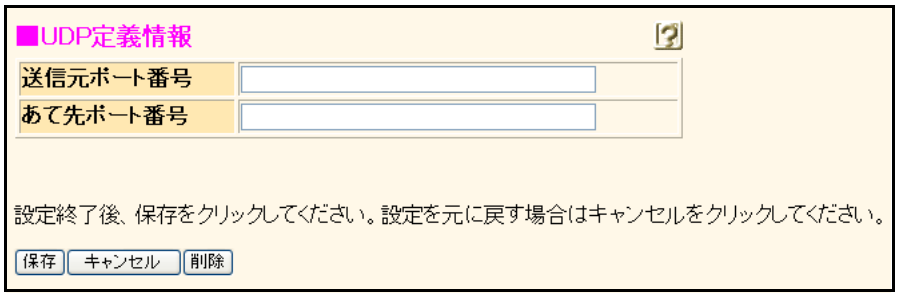
TCP 定義としてポート番号を 10 進数を使用して、1 ～ 65535 の範囲または “any” で指定します。“any” を指定した場合は、すべてのポート番号が TCP 定義の対象となります。また、ポート番号を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切ります。送信元情報とあて先情報で合わせて 10 組まで指定できます。省略時は、“any” が設定されます。

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。

16.1.4　UDP 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［UDP 定義情報］

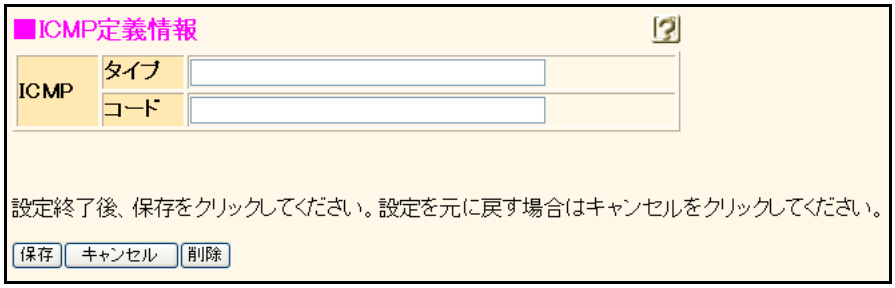


送信元／あて先ポート番号

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。

16.1.5　ICMP 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［ICMP 定義情報］



ICMP

タイプ

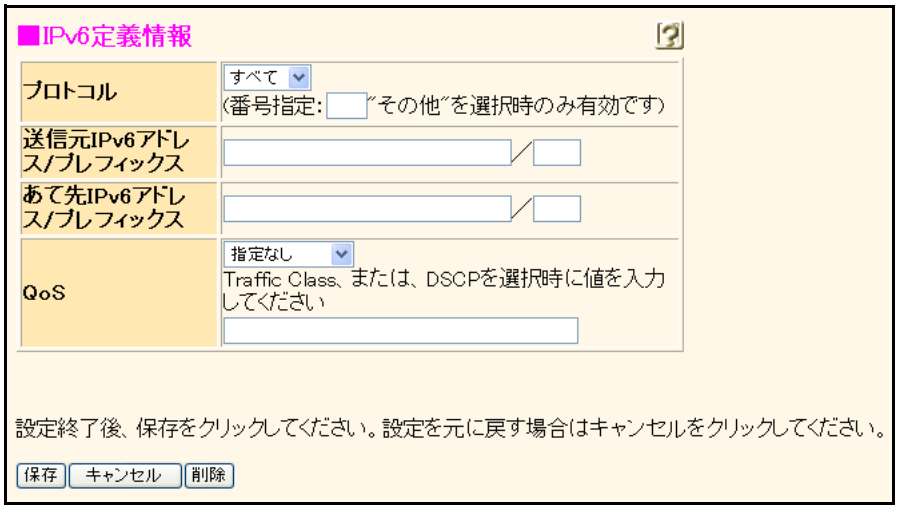
ICMP 定義として ICMP パケットのタイプ値を 10 進数を使用して 0 ～ 255 の範囲または “any” で指定します。ICMP タイプ値を複数指定する場合は “,” で区切ります。範囲指定の場合は “-” で区切ります。10 組まで指定できます。

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。

16.1.6　IPv6 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［IPv6 定義情報］



プロトコル

IPv6 定義としてプロトコルを以下の 5 つから選択します。() 内はプロトコル番号です。

- すべて
- tcp（6）
- udp（17）
- icmpv6（58）
- その他

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

送信元／あて先 IPv6 アドレス

IPv6 定義としての IPv6 アドレスおよびプレフィックス長を指定します。::/0 を指定した場合、または、省略した場合はすべての IPv6 アドレス／プレフィックス長を対象とします。

以下が等しい場合に条件に一致します。

- チェック対象となるパケットの IPv6 アドレスと定義するプレフィックス長の論理積
- 定義する IPv6 アドレスとプレフィックス長の論理積

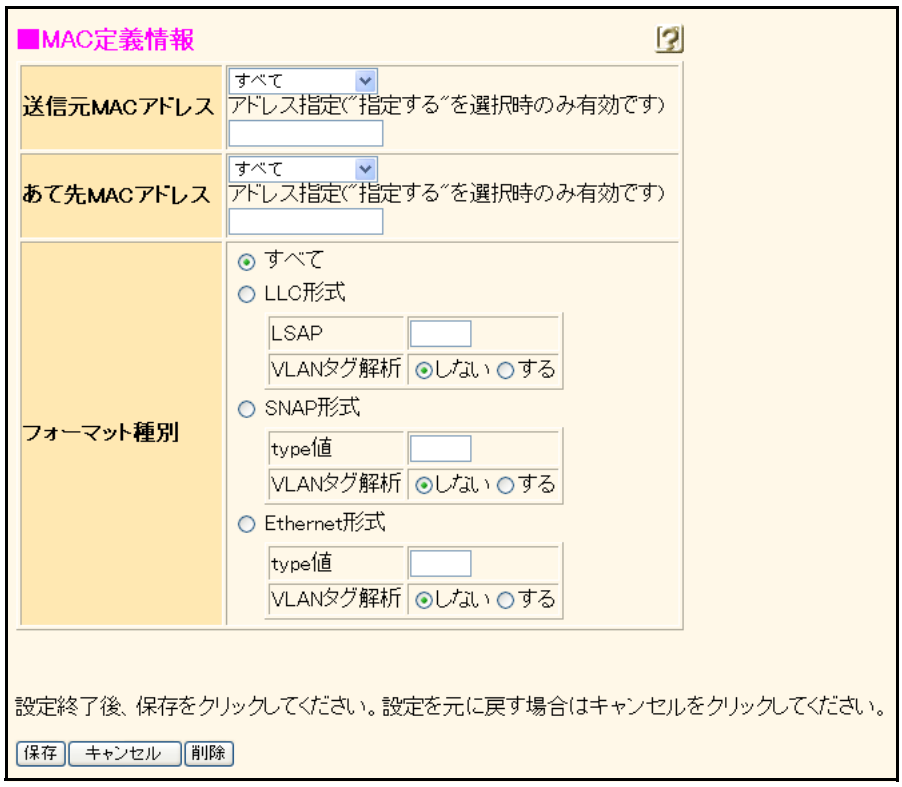
QoS

対象とする QoS を判断する方法を以下の 3 つから選択します。

- 指定なし
  すべての TOS 値、および、すべての DSCP 値を対象とする場合に選択します。
- Traffic Class
  Traffic Class 値で対象を判断する場合に選択します。複数指定する場合は、"," で区切ります。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

16.1.7　MAC 定義情報

［操作］　ルータ設定「ACL 情報」→［追加］→［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。

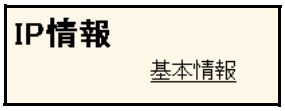
フォーマット種別

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。

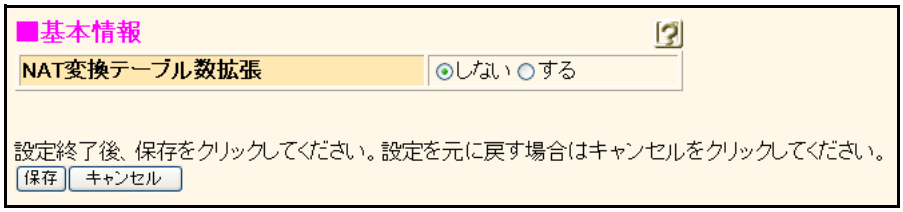
17　IP 情報

［操作］　ルータ設定「IP 情報」



17.1　基本情報

［操作］　ルータ設定「IP 情報」→［基本情報］



NAT 変換テーブル数拡張

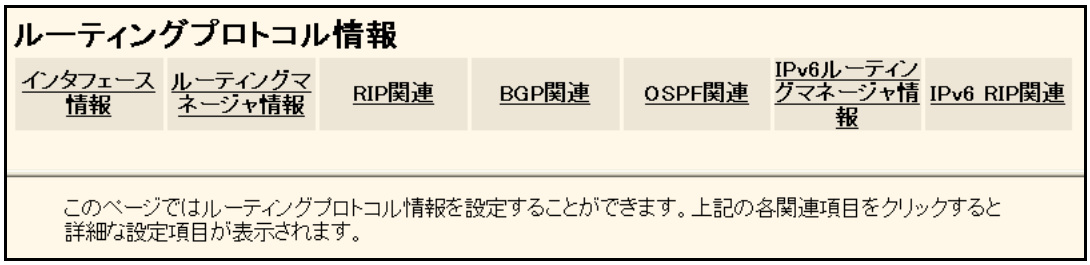
NAT 変換テーブル数を拡張する場合は、“ する ” を選択します。

こんな事に気をつけて

“NAT 変換テーブル数拡張 ” を “ する ” で、OSPF、BGP のどちらかを使用する設定から、どちらも使用しない設定に変更する場合、設定を有効にするために本装置の再起動が必要です。

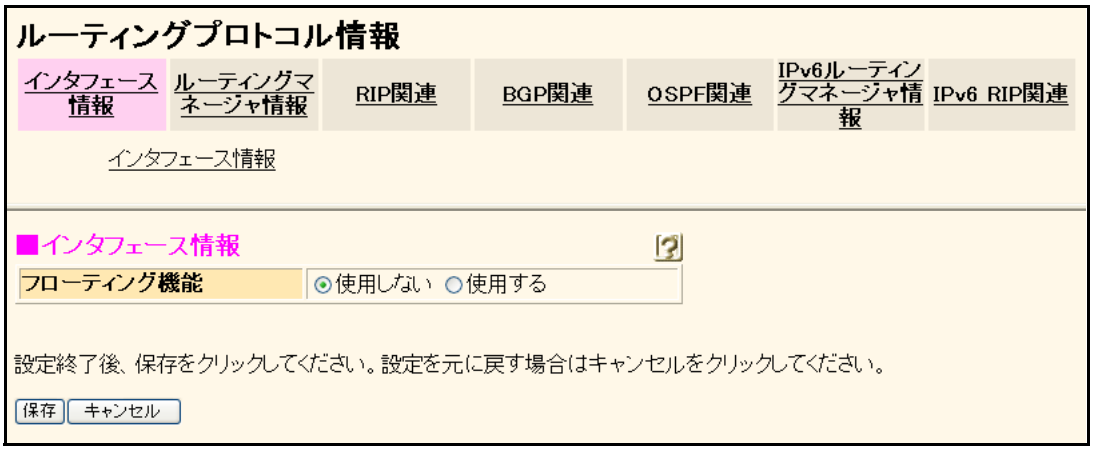
18　ルーティングプロトコル情報

［操作］　ルータ設定「ルーティングプロトコル情報」



18.1　インタフェース情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［インタフェース情報］



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。

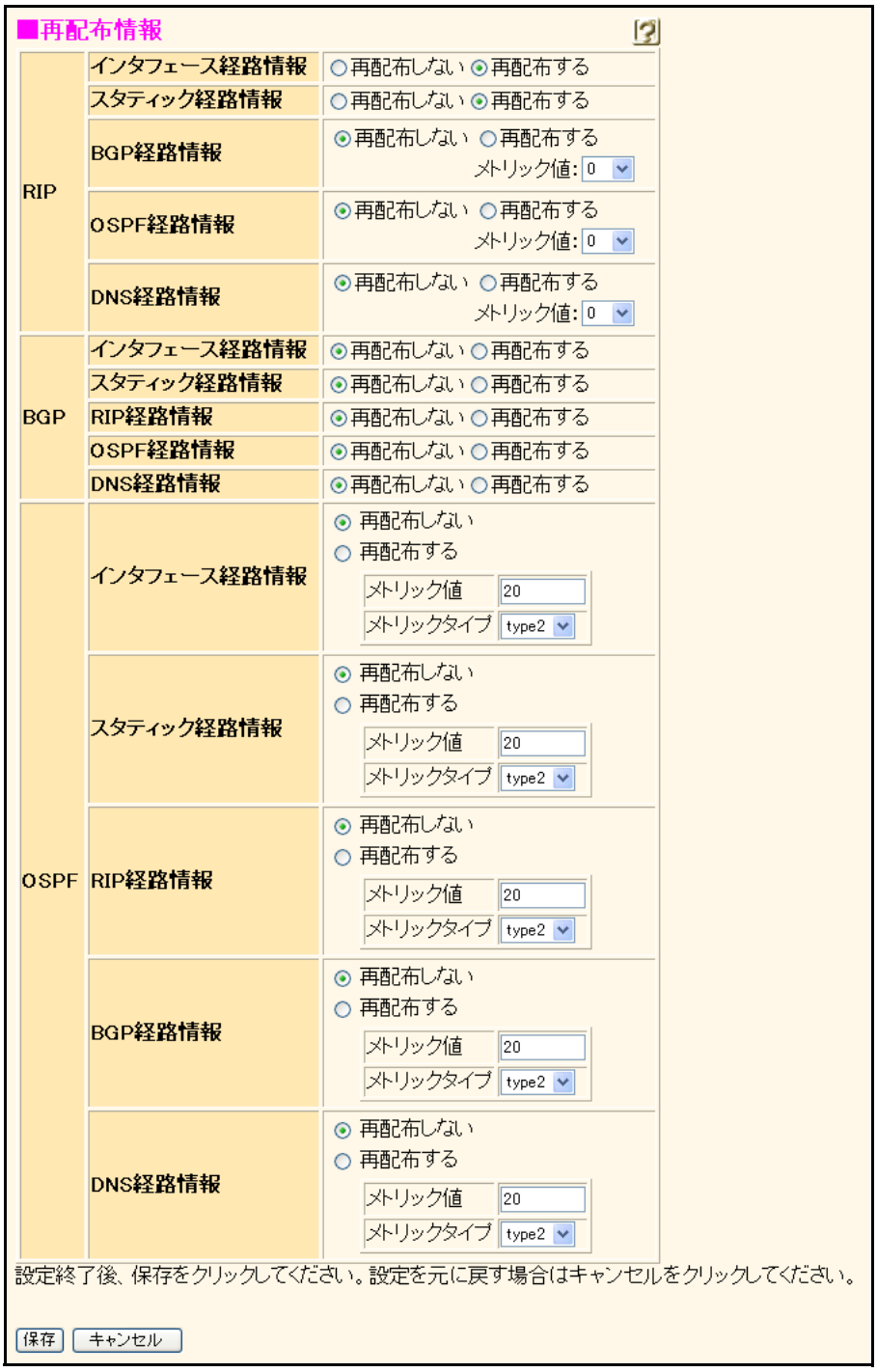
本設定は、IPv4機能、IPv6機能で共通です。

18.2 ルーティングマネージャ情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［ルーティングマネージャ情報］

18.2.1 再配布情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［ルーティングマネージャ情報］→［再配布情報］



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

デフォルトルートをBGPで広報する場合は、BGP相手情報でデフォルトルートを“広報する”に設定してください。

RIP経路情報

RIP経路情報をBGPに再配布する場合は、“再配布する”を選択します。

OSPF経路情報

OSPF経路情報をBGPに再配布する場合は、“再配布する”を選択します。

DNS経路情報

DNS経路情報をBGPに再配布する場合は、“再配布する”を選択します。

OSPF広報

OSPFに再配布する経路情報を設定します。

インタフェース経路情報

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。

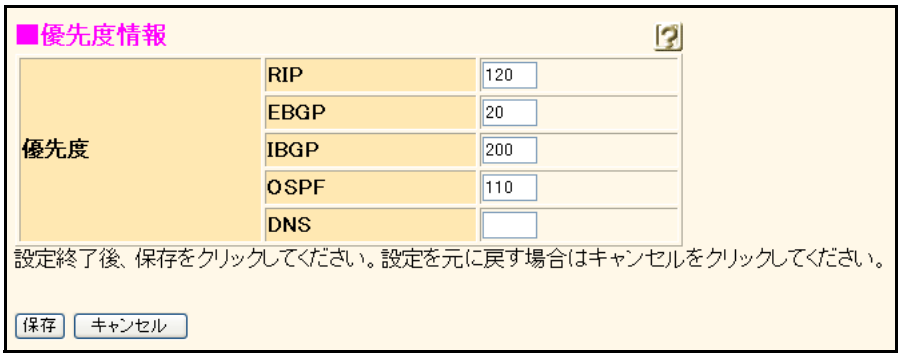
DNS 経路情報

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。

18.2.2 優先度情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［ルーティングマネージャ情報］→［優先度情報］



優先度

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

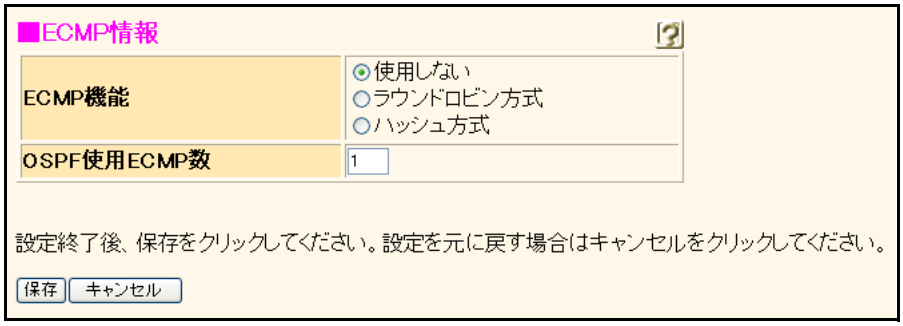
DNS 経路情報の優先度を指定します。省略時は、15 が設定されます。

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。**

18.2.3　ECMP 情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［ルーティングマネージャ情報］→［ECMP 情報］



ECMP 機能

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。

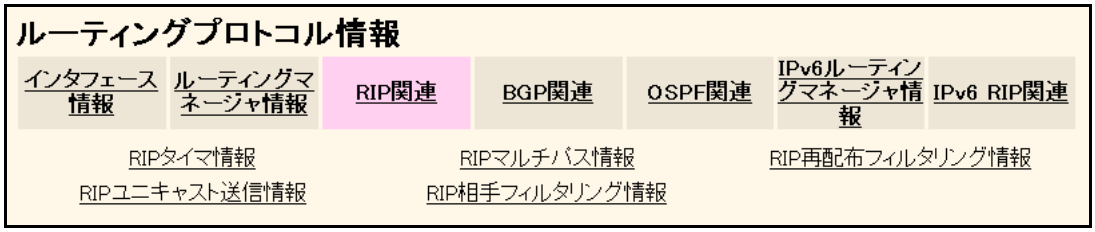
- ラウンドロビン方式
  ラウンドロビン方式とは、パケットごとに送出パスを順次切り替える方式です。すべてのトラフィックがほぼ均等に分散される利点がある一方、通信の連続性（それぞれの通信セッションが同じパスを利用する）とパケットの到達順は送信時から保証されないという欠点があります。
- ハッシュ方式
  ハッシュ方式とは、送信元 IP アドレス、あて先 IP アドレスを元にハッシュ値を計算し、その値に従って送出パスを決定する方式です。通信の連続性および到達順はほぼ保証されますが、トラフィックが一部の通信パスにかたよる可能性があります。

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。

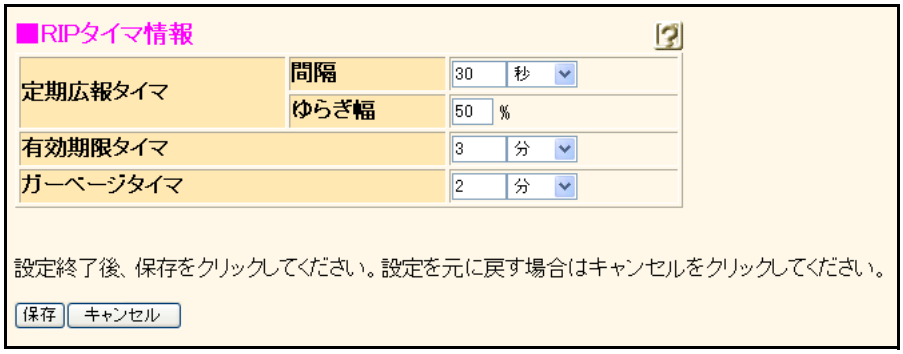
18.3 RIP 関連

［操作］　ルータ設定「ルーティングプロトコル情報」→［RIP 関連］



18.3.1 RIP タイマ情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［RIP 関連］→［RIP タイマ情報］



定期広報タイマ

間隔

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

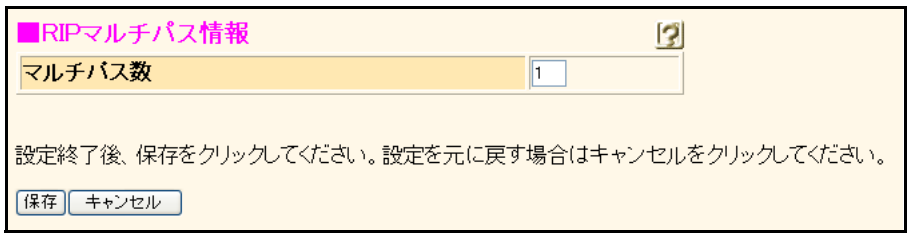
ガーベージタイマ

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

18.3.2　RIP マルチパス情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［RIP 関連］→［RIP マルチパス情報］

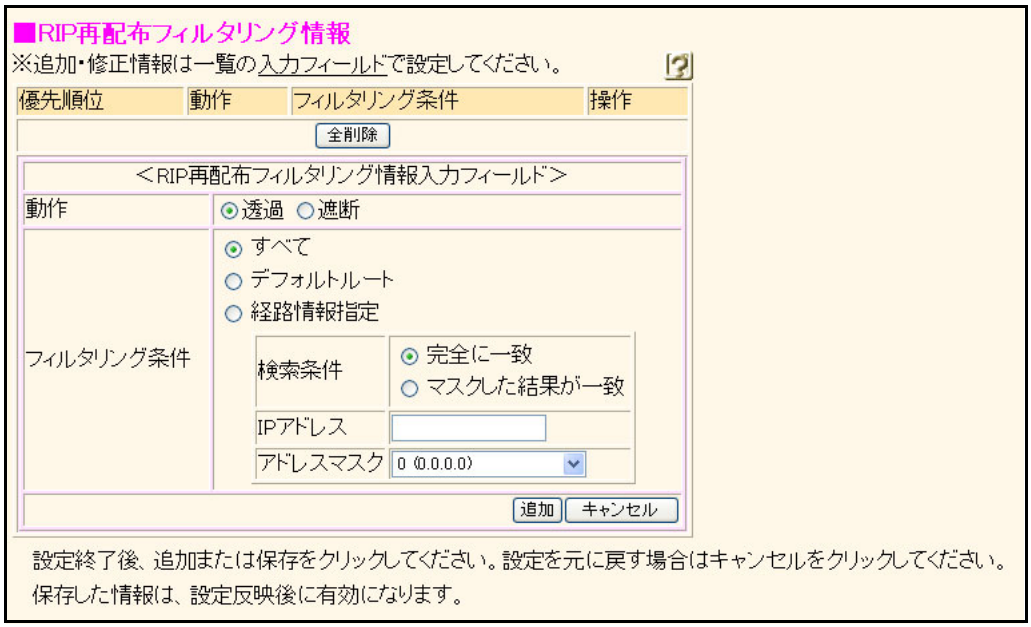


マルチパス数

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。

18.3.3　RIP 再配布フィルタリング情報

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



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、装置全体で 50 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。

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

動作

RIPに再配布する経路情報の動作を以下の2つから選択します。

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

フィルタリング条件

フィルタリング条件を選択します。

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

検索条件

検索条件を選択します。

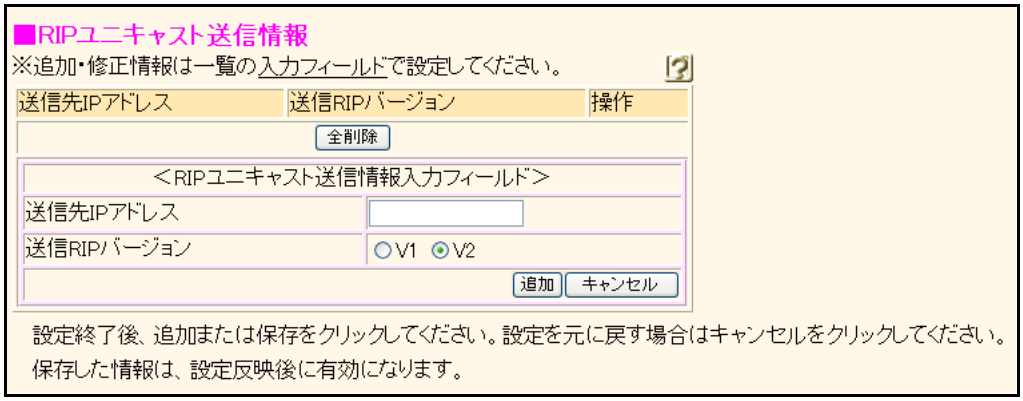
- 完全に一致
  指定したIPアドレスとアドレスマスクが完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
  指定したIPアドレスと、再配布経路情報のそれぞれを指定したアドレスマスクでマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

18.3.4　RIP ユニキャスト送信情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［RIP 関連］→［RIP ユニキャスト送信情報］



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、装置全体で 30 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。

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

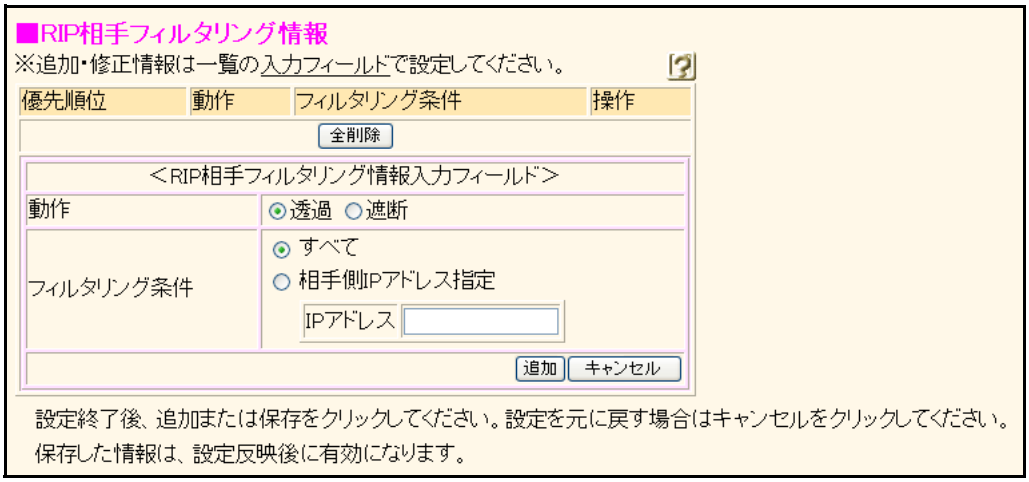
192.0.0.1 ～ 223.255.255.254

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。

18.3.5　RIP 相手フィルタリング情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［RIP 関連］→［RIP 相手フィルタリング情報］



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、装置全体で 30 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。

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

動作

受信した RIP 情報の動作を以下の 2 つから選択します。

- 透過
  フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを透過します。
- 遮断
  フィルタリング条件と一致した場合に、相手ルータからの RIP パケットを遮断します。

フィルタリング条件

対象とする相手情報を選択します。

- すべて
  すべての相手ルータからの RIP パケットをフィルタリング対象とします。
- 相手側 IP アドレス指定
  指定した RIP 送信元 IP アドレスをフィルタリング対象とします。

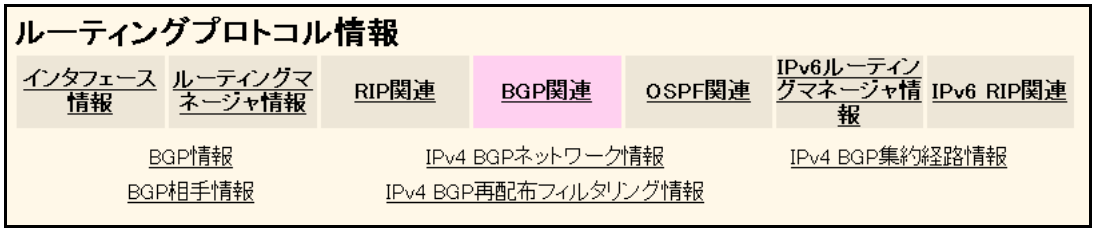
  有効範囲）
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254

こんな事に気をつけて

すべてのフィルタリング条件に一致しない相手ルータからの RIP パケットは遮断されます。

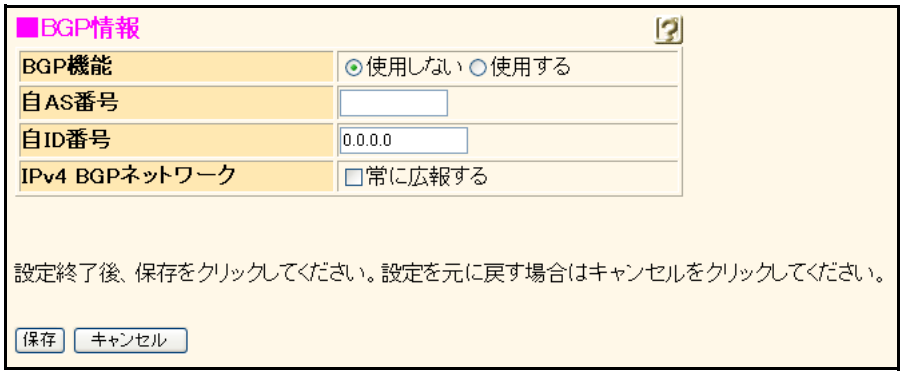
18.4 BGP 関連

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］



18.4.1 BGP 情報

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



BGP 機能

BGP を使用する場合は、“ 使用する ” を選択します。

こんな事に気をつけて

- **経路情報を、ルーティングテーブルの最大数または BGP エントリの最大数まで保持している場合、BGP で受信した経路情報は破棄されます。**
  破棄された経路情報は、そのあと、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。
  ルーティングテーブルには、「BGP セッションの操作」を行うことで反映できます。
- **NAT 機能とは併用できません。**

自 AS 番号

本装置の属する AS 番号を 10 進数を使用して、0.1 ～ 65535.65535 の範囲で指定します。省略はできません。

自 ID 番号

BGP 接続で、自装置を一意に示す ID を設定します。ID は、ほかルータと重複しない値を指定します。
省略時は、以下の基準に従い BGP ID が自動選択されます。

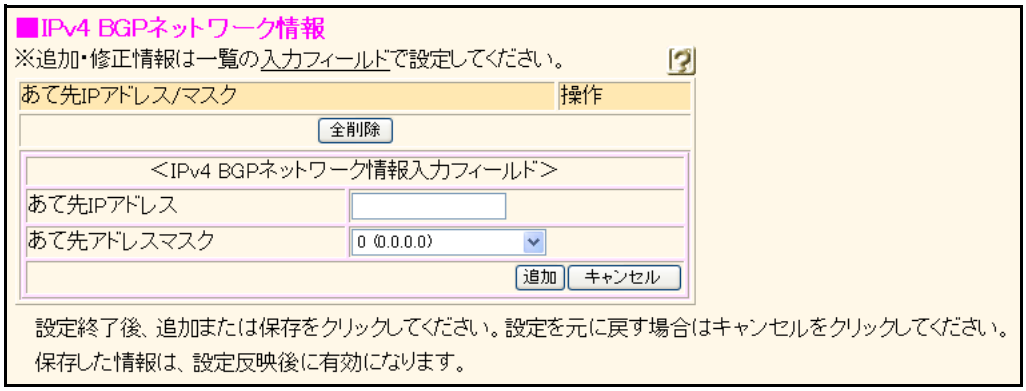
- IPv4 ループバック情報に IPv4 アドレスが設定されている場合は、その IPv4 アドレスを使用します。
- IPv4 ループバック情報に IPv4 アドレスが設定されていない場合は、LAN 情報／相手情報に設定されている IPv4 アドレスの中からインタフェースの Up/Down の状態に関係なく最大のものを選択します。なお、相手情報の相手側 IP アドレスおよび LAN 情報のセカンダリ IP アドレスは、選択対象となりません。

IPv4 BGP ネットワーク

IPv4 BGP ネットワークを、常に広報する場合に指定します。指定しない場合は、IPv4 BGP ネットワーク情報で設定したネットワークが経路情報として有効な場合だけ BGP で広報します。指定した場合は、経路情報に関係なく IPv4 BGP ネットワーク情報で設定した経路情報を BGP で広報します。

18.4.2　IPv4 BGP ネットワーク情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［IPv4 BGP ネットワーク情報］



現在、設定されている IPv4 BGP ネットワーク情報の定義が表示されています。BGP ネットワーク情報の定義数は、装置全体で 16 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。

BGP ネットワーク情報を設定することによって、必要な経路情報だけを選択して広報することができます。無効となった経路情報は広報されません。経路情報の状態変更を認識するには最大 15 秒かかります。なお、BGP ネットワーク情報は、広報する経路情報を BGP に再配布する必要はありません。

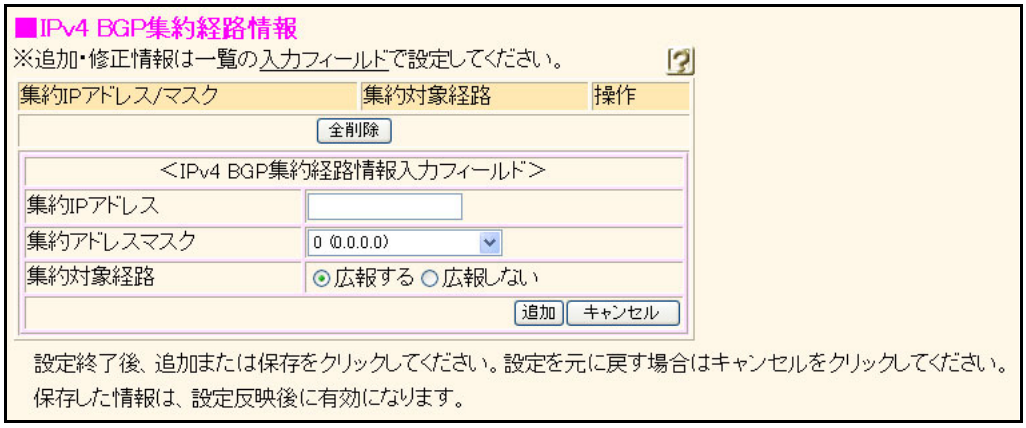
「BGP 情報」で IPv4 BGP ネットワークを常に広報すると指定することにより、設定した BGP ネットワーク情報を経路情報の状態に関係なく広報することができます。

あて先 IP アドレス／アドレスマスク

広報する経路情報のあて先 IP アドレスとアドレスマスクを指定します。

18.4.3　IPv4 BGP 集約経路情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［IPv4 BGP 集約経路情報］



現在、設定されている IPv4 BGP 集約経路情報の定義が表示されています。BGP 集約経路情報の定義数は、装置全体で 16 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。

BGP 集約情報を設定することによって、集約経路に含まれる経路情報（集約対象経路）があった場合に、集約経路情報を生成して広報することができます。集約対象経路がすべて無効となった場合、集約経路情報は広報されません。

集約 IP アドレス／集約アドレスマスク

集約経路情報の集約 IP アドレスと集約アドレスマスクを指定します。

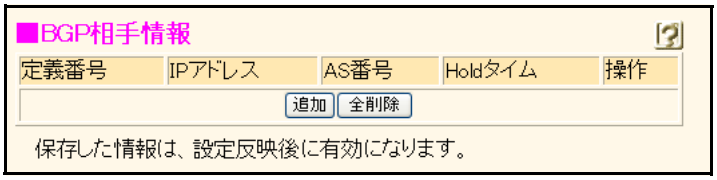
集約対象経路

集約対象となるのは、BGP に再配布された経路情報または BGP ネットワーク情報で有効となっている経路情報です。

- 広報する
  集約経路情報のほかに集約経路情報で集約される個々の経路の両方を広報します。
- 広報しない
  集約経路情報を広報し、集約される個々の経路情報は広報しません。

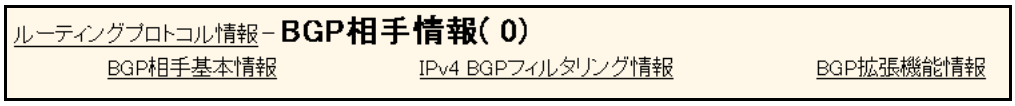
18.4.4　BGP 相手情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［BGP 相手情報］



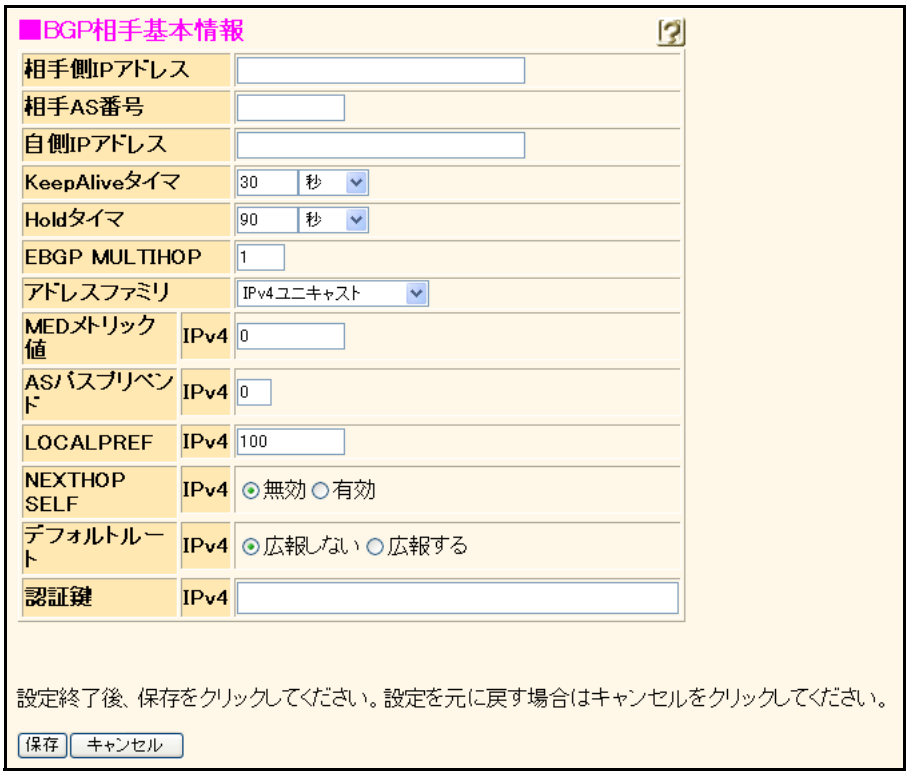
現在、設定されている BGP の相手情報の定義が表示されています。BGP の相手情報の定義数（BGP 最大接続数）は、装置全体で 4 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［BGP 相手情報］→［追加］



18.4.4.1　BGP 相手基本情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［BGP 相手情報］→［追加］
→［BGP 相手基本情報］



相手側 IP アドレス

BGP 接続を行う相手装置の IP アドレスを指定します。

IPv4 アドレスは以下の範囲で指定します。

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

相手 AS 番号

BGP 接続する相手装置の AS 番号を 10 進数を使用して、0.1 ～ 65535.65535 の範囲で指定します。

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。

IPv4 アドレスは以下の範囲で指定します。

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

KeepAlive タイマ

相手装置との通信状態を確認するために送信する KeepAlive メッセージの送信間隔を指定します。Hold タイマ設定値の 1/3 以上を設定した場合、Hold タイマ設定値の 1/3 が設定されます。また、ネゴシエーションにより相手装置の Hold タイマ値が採用され、その 1/3 よりも大きな値を KeepAlive タイマで設定していた場合は、相手装置の Hold タイマ値の 1/3 を KeepAlive タイマ値として使用します。省略時は、30 秒に設定されます。

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

Keep Alive タイマの値は、Hold タイマより小さい値を指定してください。

Hold タイマ

相手装置との間で、通信異常と判断する無通信状態の時間（タイマ）を指定します。このタイマ値は、相手装置とのネゴシエーションで決まり、装置間でより小さな値が使用されます。省略時は、90 秒に設定されます。

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
3 ～ 65535 秒

こんな事に気をつけて

相手装置とのネゴシエーションによって、相手装置の Hold タイマ値が使用された場合は、その値の 3 分の 1 の値が KeepAlive タイマとして使用されます。

EBGP MULTIHOP

相手装置と EBGP マルチホップ接続する場合の IP パケットのホップ数（IPv4 パケットの TTL 値）を 10 進数を使用して、1 ～ 255 の範囲で指定します。省略時は、1 に設定されます。

BGP 相手装置とルータを経由して接続する場合は、経由するルータの数を加算します。

アドレスファミリ

BGP で送受信する経路情報のアドレスファミリを指定します。

MED メトリック値

EBGP で広報する IPv4 経路情報に付加する MED メトリック値を 10 進数を使用して、0 ～ 4294967295 の範囲で指定します。省略時は、0 に設定されます。

こんな事に気をつけて

IPv4 BGP フィルタリング設定で、送信用のフィルタを設定した場合、本設定は無効となります。

AS パスプリペンド

EBGP で広報する IPv4 経路情報に付加する AS 番号の個数を 10 進数を使用して、0 ～ 4 の範囲で指定します。省略時は、0 に設定されます。

こんな事に気をつけて

IPv4 BGP フィルタリング設定で、送信用のフィルタを設定した場合、本設定は無効となります。

LOCALPREF

EBGP で受信する IPv4 経路情報のローカル優先度を 10 進数を使用して、0 ～ 4294967295 の範囲で指定します。省略時は、100 に設定されます。

こんな事に気をつけて

IPv4 BGP フィルタリング設定で、送信用のフィルタを設定した場合、本設定は無効となります。

NEXTHOP SELF

IBGP で広報する IPv4 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

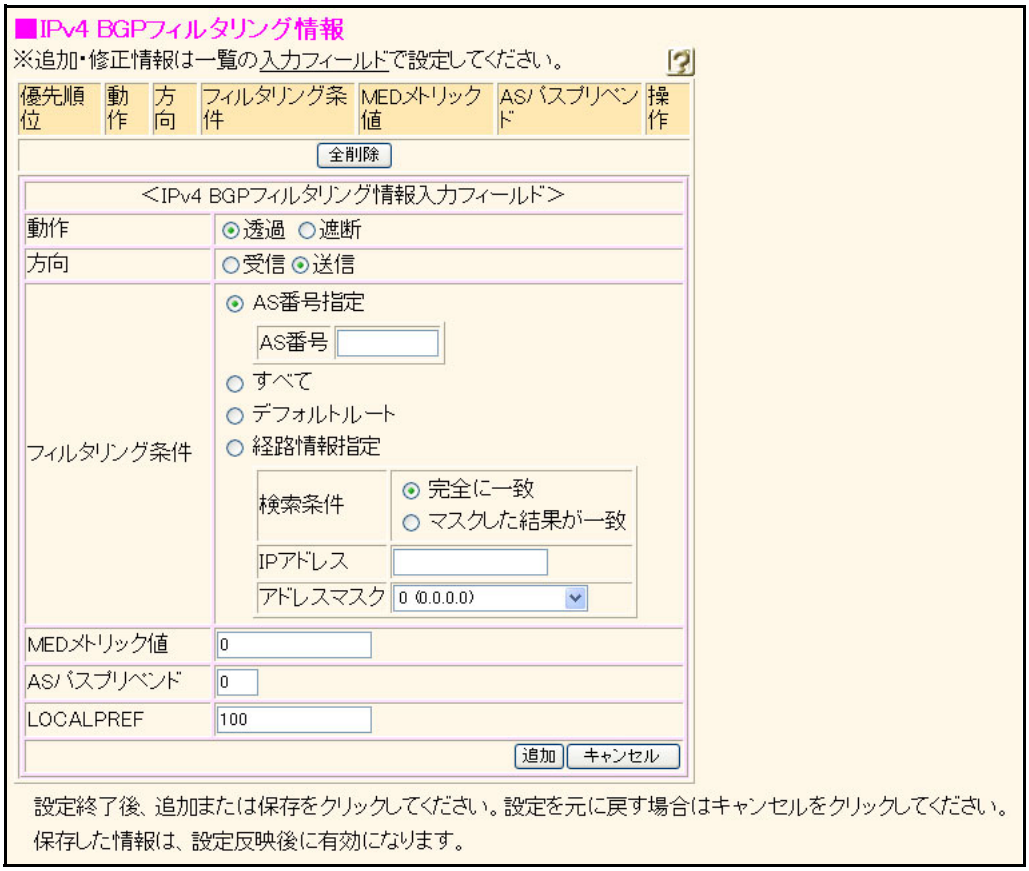
BGP で IPv4 デフォルトルートの広報を許可する場合は、“ 広報する ” を選択します。

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。

18.4.4.2 IPv4 BGP フィルタリング情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［BGP 相手情報］→［追加］→［IPv4 BGP フィルタリング情報］



現在、設定されている IPv4 BGP フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP フィルタリングの定義数は、装置全体で 200 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。

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。

動作

フィルタリング条件に該当する経路情報の動作を以下の 2 つから選択します。

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

方向

フィルタリング条件に該当するかどうかをチェックするタイミングを選択します。

- 受信
  BGP パケット受信時にチェックします。
- 送信
  BGP パケット送信時にチェックします。

フィルタリング条件

フィルタリング条件を選択します。

- AS 番号指定
  経由した AS 番号をフィルタリングの対象とします。AS 番号は 0.1 ～ 65535.65535 の範囲で指定します。
- すべて
  すべての経路情報をフィルタリング対象とします。
- デフォルトルート
  デフォルトルートをフィルタリング対象とします。
- 経路情報指定
  フィルタリングの対象とする経路情報を指定できます。経路情報を指定するときは、BGP 経路の検索条件として、“ 完全に一致 ” または、“ マスクした結果が一致 ” を選択します。

検索条件

検索条件を選択します。

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

MED メトリック値

フィルタリング結果で透過になった BGP 経路情報のメトリック値を変更できます。MED メトリック値は、10 進数を使用して、0 ～ 4294967295 の範囲で指定します。省略時は、0 が設定されます。

こんな事に気をつけて

- **送信時のフィルタを設定した場合、「BGP 相手基本情報」の MED メトリック値の設定は無効となります。**
- **MED メトリック値の設定は、EBGP 送信時のフィルタリングでだけ有効となります。受信時のフィルタリングでの MED メトリック値の設定は無効となります。**

AS パスプリペンド

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、10 進数を使用して、0 ～ 4 の範囲で指定します。省略時は、0 が設定されます。

こんな事に気をつけて

- **送信時のフィルタリングを設定した場合、「BGP 相手基本情報」の AS パスプリ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

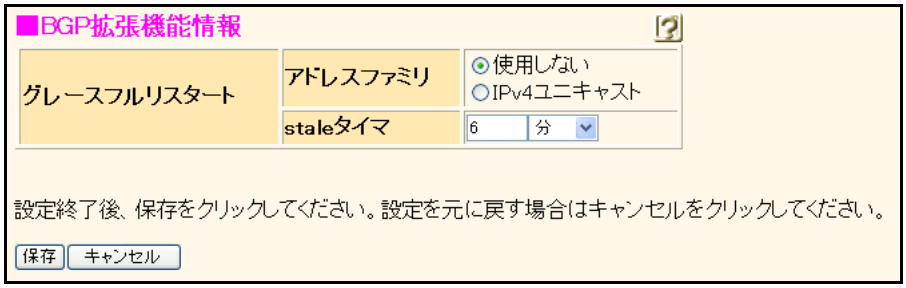
フィルタリング結果で透過になった EBGP 経路情報に対して、付加する LOCALPREF を 10 進数を使用して、0 ～ 4294967295 の範囲で指定します。省略時は、100 が設定されます。

こんな事に気をつけて

- **受信時のフィルタリングを設定した場合、「BGP 相手基本情報」の LOCALPREF は無効となります。**
- **LOCALPREF は、EBGP 受信時のフィルタリングでだけ有効となります。送信時のフィルタリングに本設定を行っても、LOCALPREF の設定は無効となります。**

18.4.4.3 BGP 拡張機能情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［BGP 相手情報］→［追加］→［BGP 拡張機能情報］



グレースフルリスタート

グレースフルリスタートの使用に関して設定します。

アドレスファミリ

相手装置との BGP セッションでグレースフルリスタート機能を使用するアドレスファミリを指定します。相手装置との間で、ここで指定したアドレスファミリに対してのみ、グレースフルリスタートの処理が実施されます。本装置ではレシーブルータの機能のみが有効になります。

stale タイマ

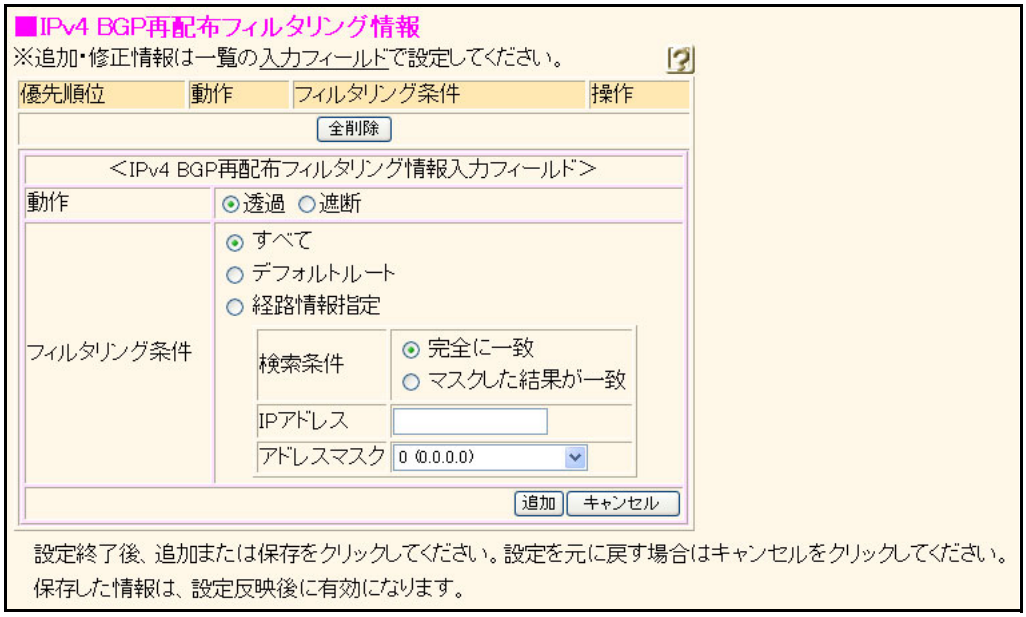
相手装置とのグレースフルリスタート処理による BGP セッションの切断が発生した場合に、その相手装置から受信した経路を削除するまでの最大待ち時間を指定します。指定した時間の間、経路をルーティングテーブルに保持することにより、パケットの転送能力を保持したまま、グレースフルリスタート処理の完了を待ち合わせます。初期値は 360 秒です。このタイマ値は、相手装置から OPEN メッセージで通知されるグレースフルリスタートの Restart タイマより大きくしておく必要があります。小さい値を設定すると、自動的に Restart タイマの値に変更されます。

こんな事に気をつけて

グレースフルリスタートのアドレスファミリで指定されていないアドレスファミリに対しては、このタイマは有効になりません。その場合、このタイマの設定にかかわらず、そのアドレスファミリの経路はグレースフルリスタート開始時に即時に削除されます。

18.4.5　IPv4 BGP 再配布フィルタリング情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［BGP 関連］→［IPv4 BGP 再配布フィルタリング情報］



現在、設定されている IPv4 BGP 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。BGP 再配布フィルタリング情報の定義数は、装置全体で 50 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。

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

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

動作

BGP に再配布するフィルタリング条件の動作を以下の 2 つから選択します。

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

フィルタリング条件

フィルタリング条件を選択します。

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

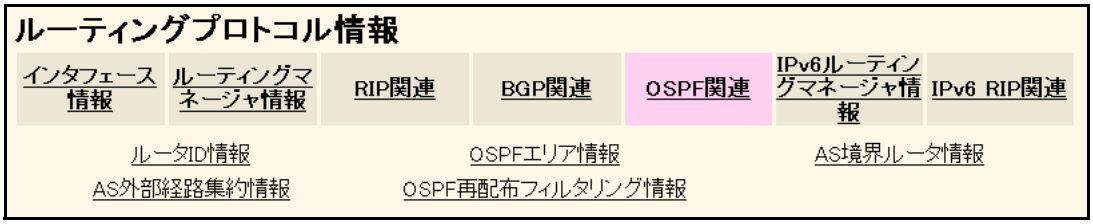
検索条件

検索条件を選択します。

- 完全に一致
  指定した IP アドレスと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。

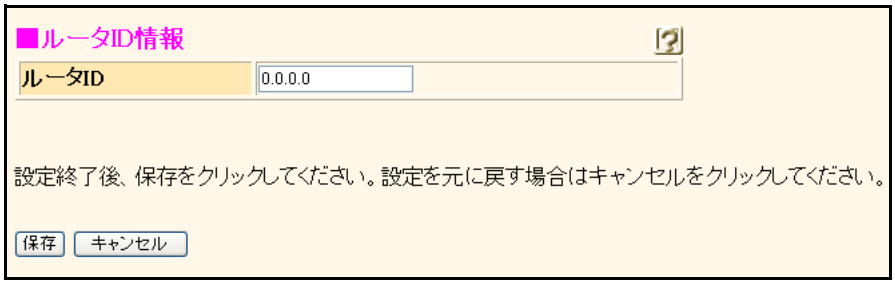
18.5 OSPF 関連

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］



18.5.1 ルータ ID 情報

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



ルータ ID

OSPF 接続で、自装置を唯一に示す ID を設定します。ID は、ほかルータと重複しない値を指定し、一般的には自装置の IPv4 アドレスを使用します。

設定を省略または 0.0.0.0 を指定した場合、以下のとおり ID を自動的に選択し、使用します。

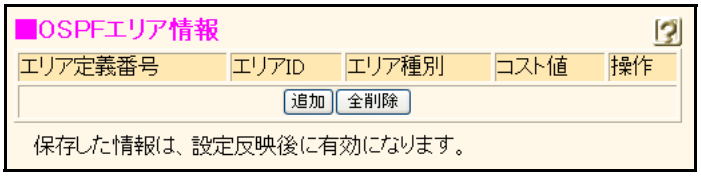
- ループバックインタフェースに追加 IP アドレスが設定されている場合は、その IP アドレスを選択し、使用します。
- ループバックインタフェースに追加 IP アドレスが設定されていない場合は、LAN インタフェース／リモートインタフェースに設定されている IPv4 アドレスの中からインタフェースの Up／Down の状態に関係なく最大の IPv4 アドレスを選択し、使用します。なお、リモートインタフェースの相手側 IP アドレスと LAN インタフェースのセカンダリ IP アドレスは選択対象となりません。

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。

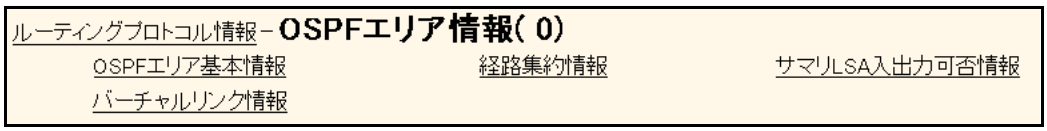
18.5.2　OSPF エリア情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［OSPF エリア情報］



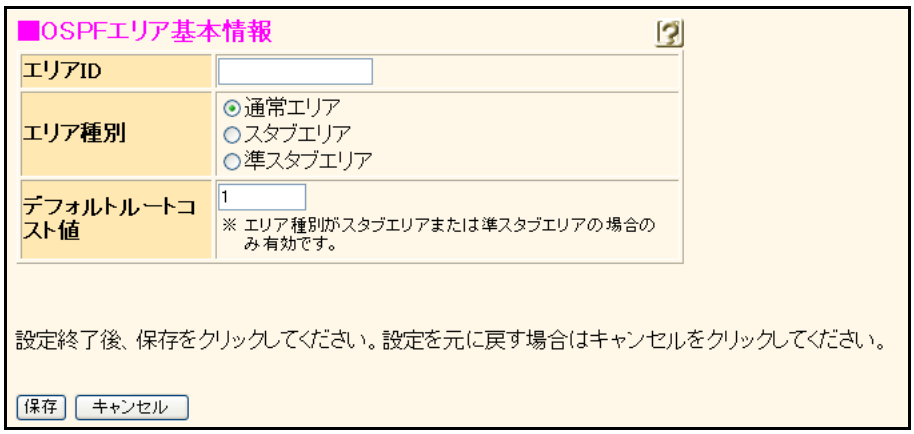
現在、設定されている OSPF エリア情報の定義が表示されています。エリア定義数は、装置全体で 2 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［OSPF エリア情報］→［追加］



18.5.2.1　OSPF エリア基本情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［OSPF エリア情報］→［追加］
→［OSPF エリア基本情報］



エリア ID

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

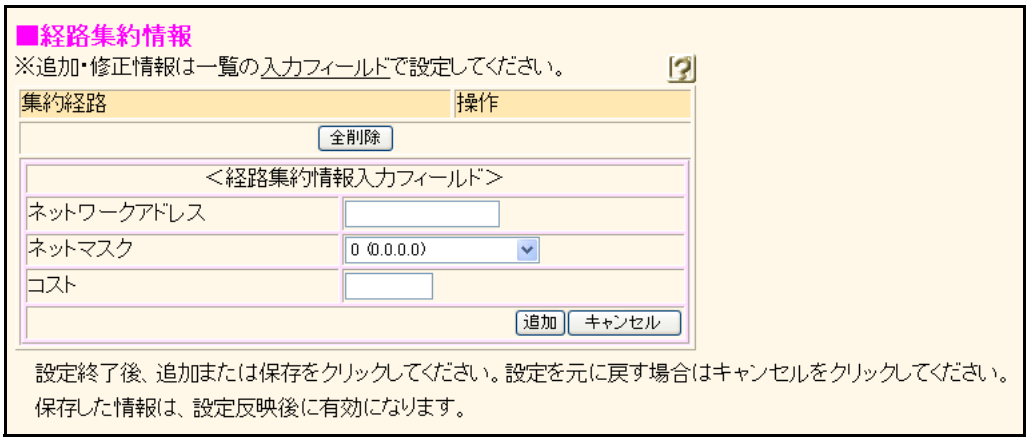
バックボーンエリアにスタブエリアまたは準スタブエリアを設定した場合も、通常エリアとして動作します。

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。

18.5.2.2 経路集約情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［OSPF エリア情報］→［追加］→［経路集約情報］



現在、設定されている経路集約情報の定義が表示されています。1 エリアでの経路集約情報の定義数は、4 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。

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

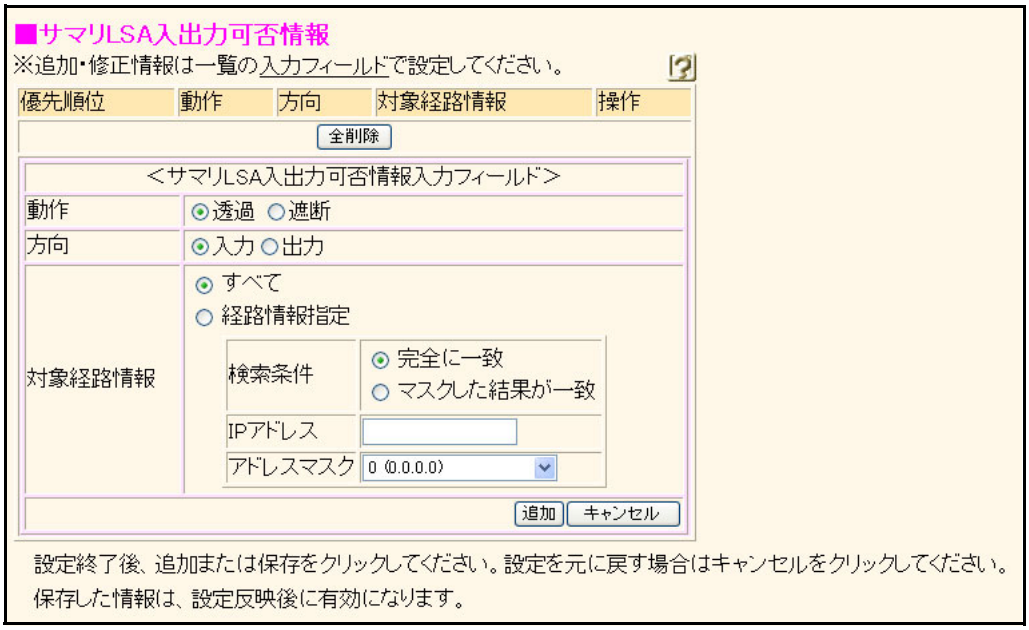
ネットマスクを選択します。

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。

18.5.2.3 サマリ LSA 入出力可否情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［OSPF エリア情報］→［追加］→［サマリ LSA 入出力可否情報］



現在、設定されているサマリ LSA 入出力可否定義が表示されています。処理は優先順位 1 から順に行われます。サマリ LSA 入出力可否の定義数は、装置全体で 30 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。

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。

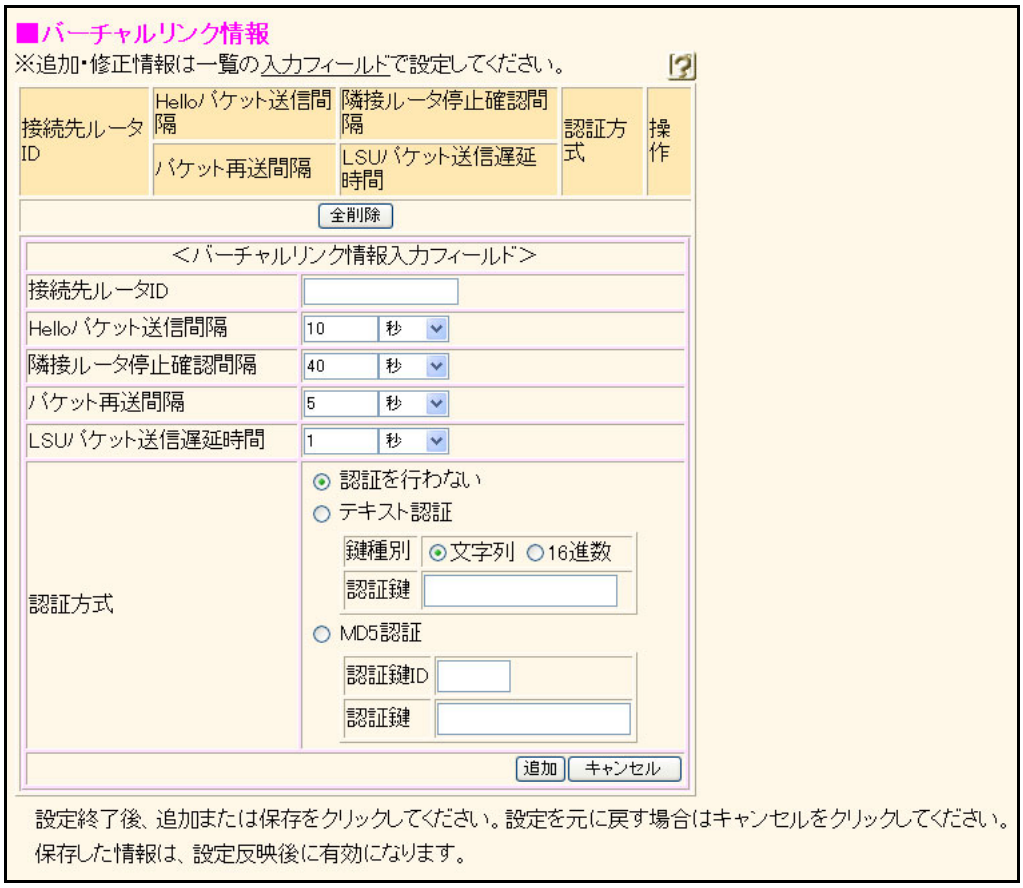
こんな事に気をつけて

「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**

18.5.2.4 バーチャルリンク情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［OSPF エリア情報］→［追加］→［バーチャルリンク情報］



現在、設定されているバーチャルリンク情報の定義が表示されています。バーチャルリンク情報の定義数は、OSPF エリア情報ごとに 2 個まで（装置全体では 4 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。

接続先ルータ ID

接続先ルータの OSPF ルータ ID を指定します。

Hello パケット送信間隔

バーチャルリンク接続先との OSPF 隣接関係の維持に使用する Hello パケットの送信間隔を指定します。奨励値は“10 秒”です。

有効範囲）
1 ～ 18 時間
1 ～ 1092 分
1 ～ 65535 秒

こんな事に気をつけて

バーチャルリンク接続先と同じ Hello パケット送信間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

隣接ルータ停止確認間隔

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

有効範囲）
1～18時間
1～1092分
1～65535秒

こんな事に気をつけて

バーチャルリンク接続先と同じ隣接ルータ停止確認間隔を指定してください。異なる値を指定するとルーティングを行うことができません。

パケット再送間隔

バーチャルリンクでOSPFパケットを再送する間隔を指定します。

有効範囲）
1～18時間
1～1092分
1～65535秒

LSUパケット送信遅延時間

LSU（Link State Update）パケットの送信遅延時間を指定します。LSUパケットでは、LSA（Link StateAdvertisement）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、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

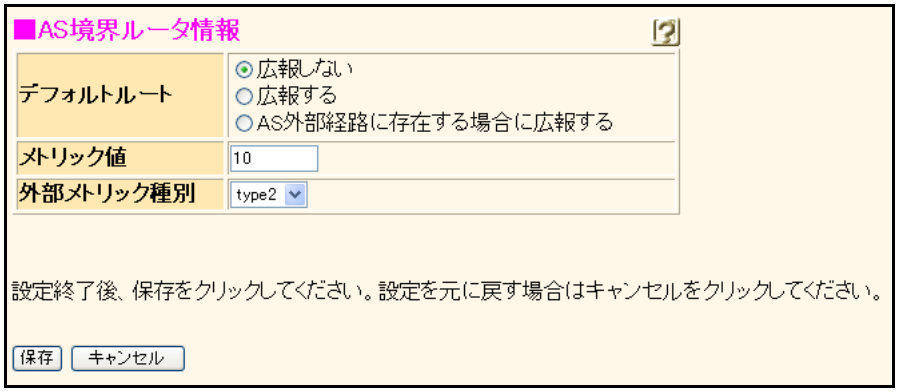
バーチャルリンクのMD5認証で使用する鍵IDを1～255の範囲で指定します。

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。

18.5.3　AS 境界ルータ情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［AS 境界ルータ情報］



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

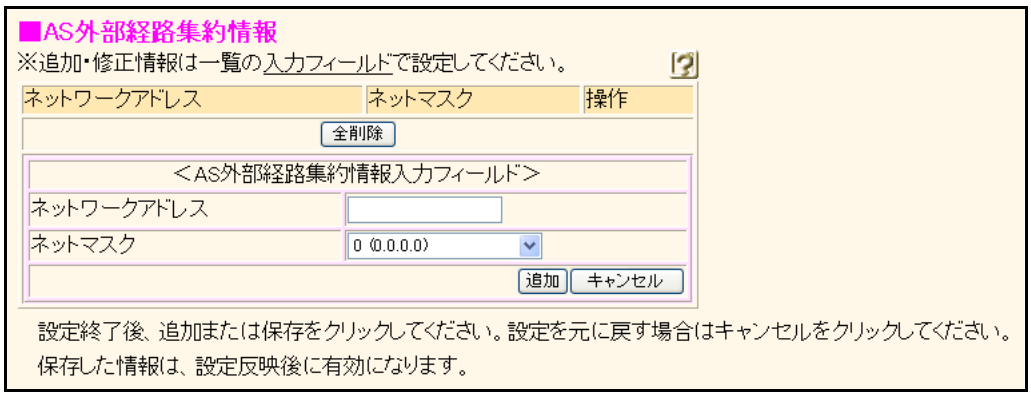
デフォルトルートのメトリック値を 0 ～ 16777214 の範囲で指定します。省略時は、10 が設定されます。

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。

18.5.4　AS 外部経路集約情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［OSPF 関連］→［AS 外部経路集約情報］



現在、設定されている AS 外部経路集約情報の定義が表示されています。AS 外部経路集約情報の定義数は、装置全体で 4 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。

ネットワークアドレス

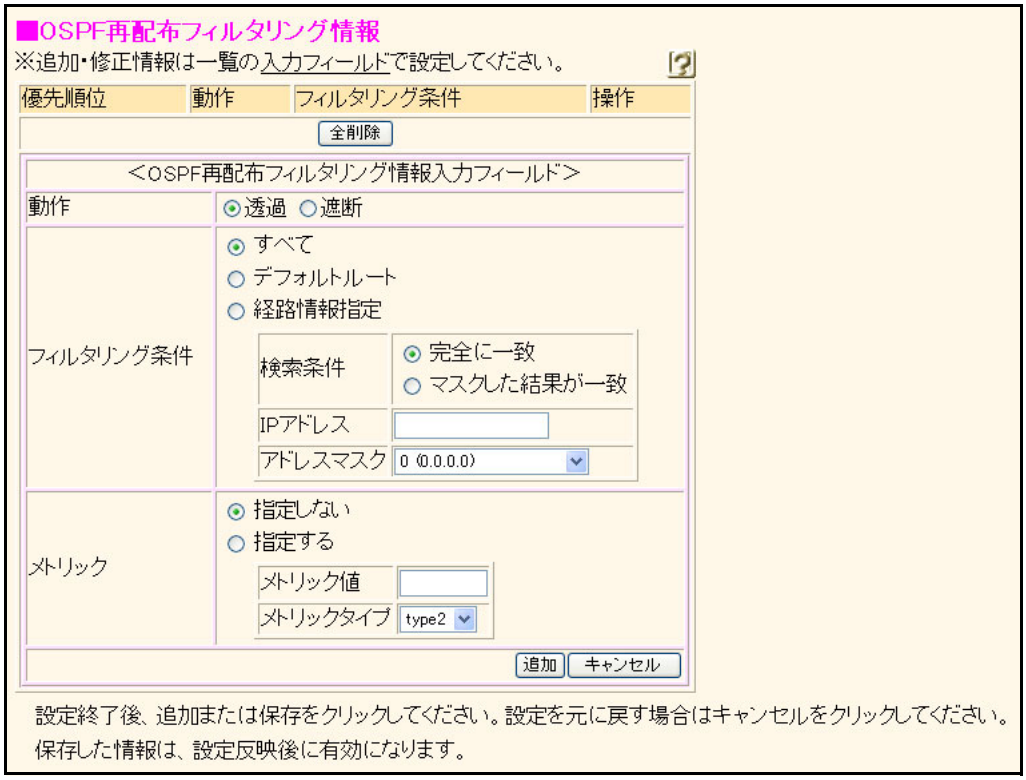
AS 外部経路で集約するネットワークアドレスを指定します。

ネットマスク

ネットマスクを選択します。

18.5.5　OSPF 再配布フィルタリング情報

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



現在、設定されている OSPF 再配布フィルタリング情報の定義が表示されています。処理は優先順位 1 から順に行われます。OSPF 再配布フィルタリング情報の定義数は、装置全体で 50 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。

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

こんな事に気をつけて

すべてのフィルタリング条件に一致しない再配布経路情報は遮断されます。

動作

OSPF に再配布する再配布経路情報の動作を以下の 2 つから選択します。

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

フィルタリング条件

フィルタリング条件を選択します。

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

検索条件

検索条件を選択します。

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

こんな事に気をつけて

デフォルトルートをOSPFに再配布する場合は、「AS境界ルータ情報」の設定も必要となります。

メトリック

経路情報をOSPFに再配布する際のメトリック値、メトリックタイプを指定する場合は、“指定する”を選択します。“指定しない”を選択した場合は、「ルーティングマネージャ情報」で設定したメトリック値、および、メトリックタイプとなります。なお、本設定は動作に“透過”を設定した場合に有効です。

メトリック値

OSPFに再配布する際のメトリック値を0～16777214の範囲で指定します。

こんな事に気をつけて

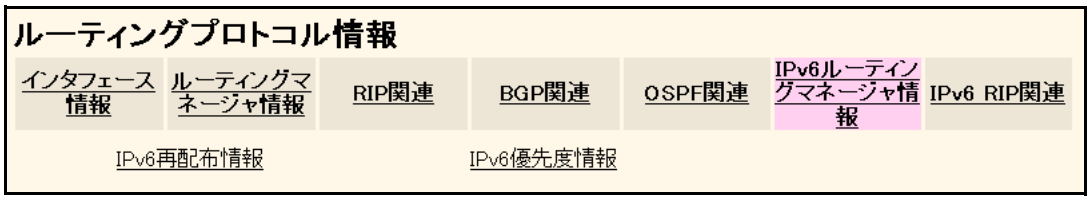
動作に遮断を指定した場合、メトリック値は指定できません。

メトリックタイプ

OSPFに再配布する際のメトリックタイプを選択します。

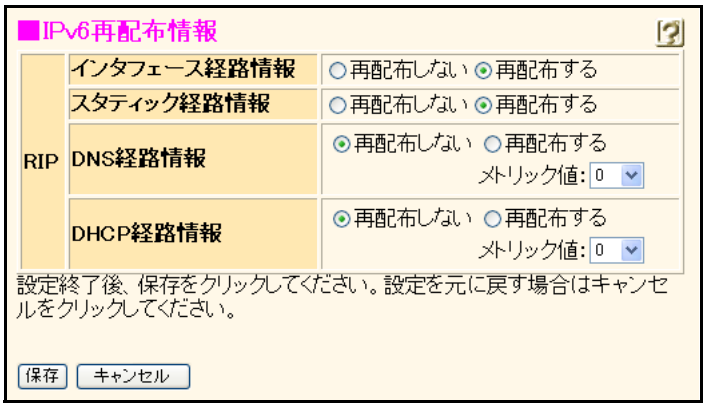
18.6 IPv6 ルーティングマネージャ情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 ルーティングマネージャ情報］



18.6.1 IPv6 再配布情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 ルーティングマネージャ情報］
→［IPv6 再配布情報］



RIP

以下の各経路情報を RIP に再配布するかどうかを設定します。経路情報を RIP に再配布する場合は、“ 再配布する ” を選択します。

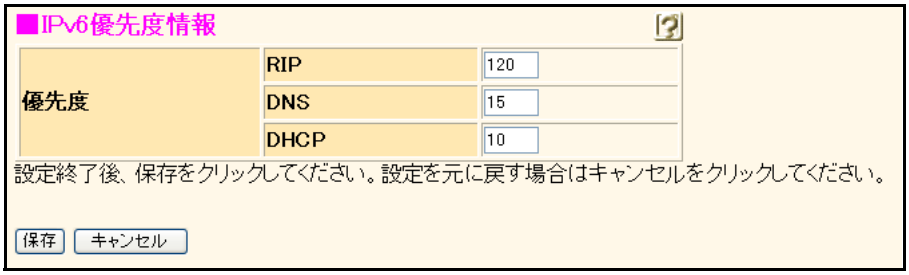
- インタフェース経路情報
- スタティック経路情報
- DNS 経路情報
- DHCP 経路情報

メトリック値

RIP に再配布する際のメトリック値を選択します。

18.6.2　IPv6 優先度情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 ルーティングマネージャ情報］→［IPv6 優先度情報］



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

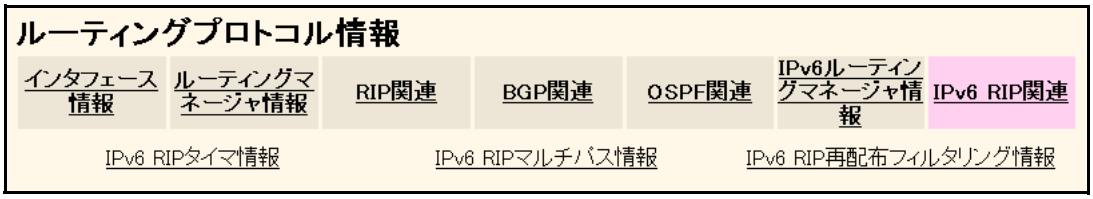
DHCP 経路情報の優先度を指定します。省略時は、10 が設定されます。

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。**

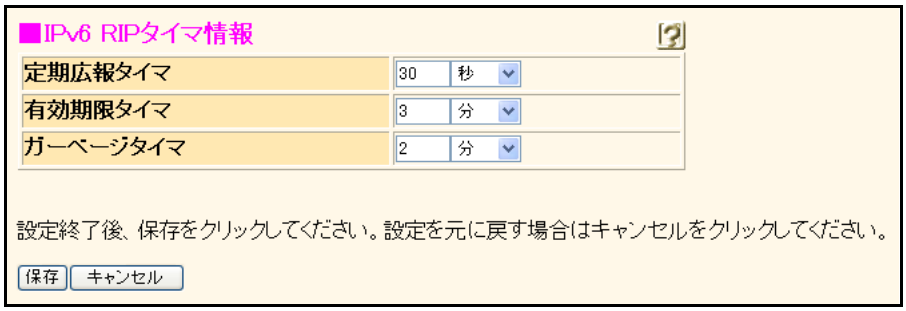
18.7 IPv6 RIP 関連

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 RIP 関連］



18.7.1 IPv6 RIP タイマ情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 RIP 関連］→［IPv6 RIP タイマ情報］



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

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

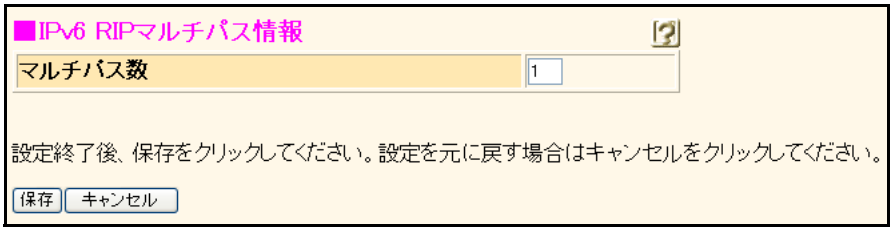
ガーベージタイマ

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

18.7.2　IPv6 RIP マルチパス情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 RIP 関連］→［IPv6 RIP マルチパス情報］

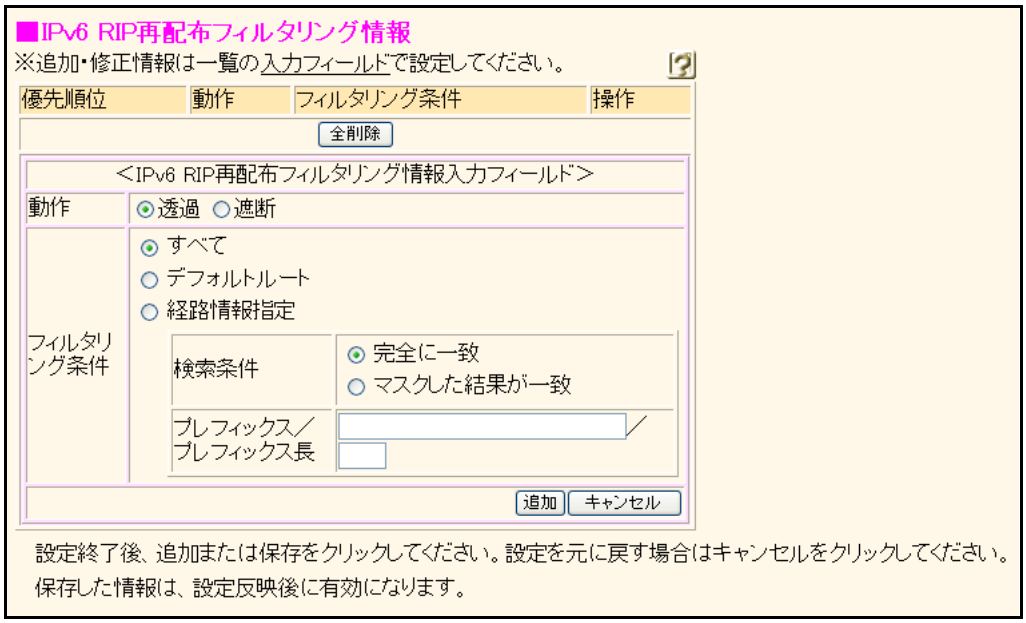


マルチパス数

RIP で受信可能な同じあて先への経路情報数を 1 ～ 2 の範囲で指定します。省略時は、1 が設定されます。

18.7.3　IPv6 RIP 再配布フィルタリング情報

［操作］　ルータ設定「ルーティングプロトコル情報」→［IPv6 RIP 関連］
→［IPv6 RIP 再配布フィルタリング情報］



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、装置全体で 50 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。

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

動作

RIPに再配布する経路情報の動作を以下の2つから選択します。

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

フィルタリング条件

フィルタリング条件を選択します。

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

検索条件

検索条件を選択します。

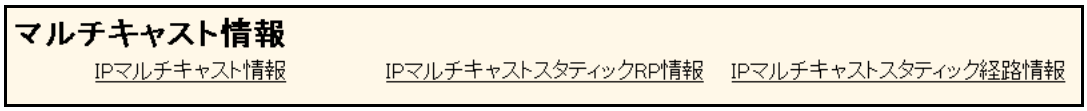
- 完全に一致
  指定したプレフィックスとプレフィックス長が完全に一致した再配布経路情報をフィルタリング対象とします。
- マスクした結果が一致
  指定したプレフィックスと、再配布経路情報のそれぞれを、指定したプレフィックス長でマスクした結果が一致した場合、その再配布経路情報をフィルタリング対象とします。

こんな事に気をつけて

すべてのフィルタリング条件に一致しない経路情報は遮断されます。

19　マルチキャスト情報

［操作］　ルータ設定「マルチキャスト情報」



19.1　IP マルチキャスト情報

［操作］　ルータ設定「マルチキャスト情報」→［IP マルチキャスト情報］

IGMP

IGMP Membership Report 送信抑止

IGMP Query 受信時の応答動作を指定します。

- する
  IGMPv2（RFC2236）仕様に従い、他ホストからの IGMP Membership Report を受信した場合は、重複によるトラフィック増加の防止のため、本装置からは IGMP Membership Report を送出しません。
- しない
  常に送信します。

PIM-SM

RP 候補

ランデブー・ポイント（RP）の設定です。マルチキャスト・ルーティングプロトコルに PIM-SM を利用する場合は、RP として動作するルータがネットワーク上に 1 台以上必要です。RP の設定は、1 台のルータだけで行っても、複数のルータで行っても構いません。トラフィックを分散する場合は、複数台のルータで RP の設定を行っておきます。

IPアドレス
RPとして動作するインタフェースの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1 ～ 100000Kbpsまたは1 ～ 100Mbpsの範囲で指定します。

register

PIM Registerパケットを設定します。マルチキャスト・パケットを送信するルータ上で行います。

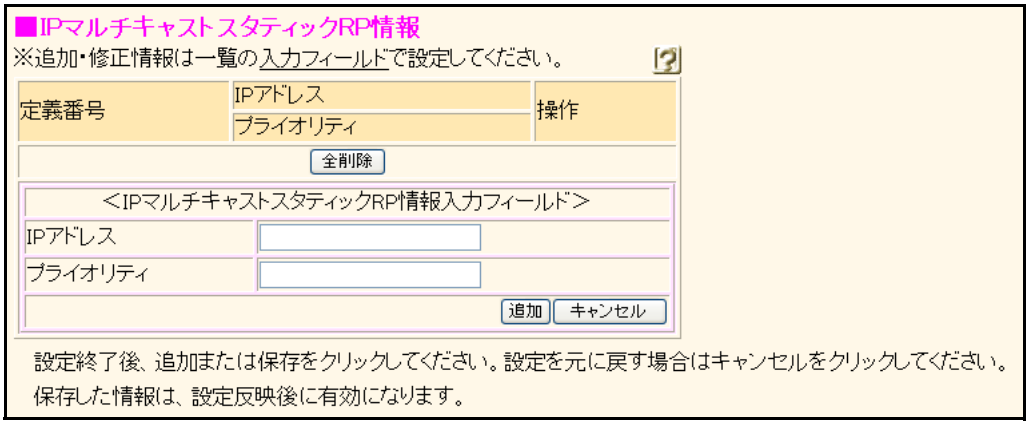
チェックサム
PIM Registerパケットの送信時のチェックサムの計算方法を設定することができます。

PIM Registerパケットのチェックサムの計算範囲は、RFC2362ではヘッダ部だけで計算するように定義されていますが、一部のルータはパケット全体で計算します。このようなルータがRPを行う場合は、PIM Registerパケットが受信されない可能性があるため、チェックサムの計算範囲を“パケット全体”に変更する必要があります。

本装置はPIM Registerパケットの受信時に、ヘッダ部（RC2362準拠）とパケット全体の2つの方法で計算するため、本装置がRPを行う場合は、どちらの計算方法のパケットを受信しても問題はありません。

19.2 IP マルチキャストスタティック RP 情報

［操作］　ルータ設定「マルチキャスト情報」→［IP マルチキャストスタティック RP 情報］



現在、設定されている IP マルチキャストスタティック RP 情報の定義が表示されています。IP マルチキャストスタティック RP の定義数は、装置全体で 10 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。

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。

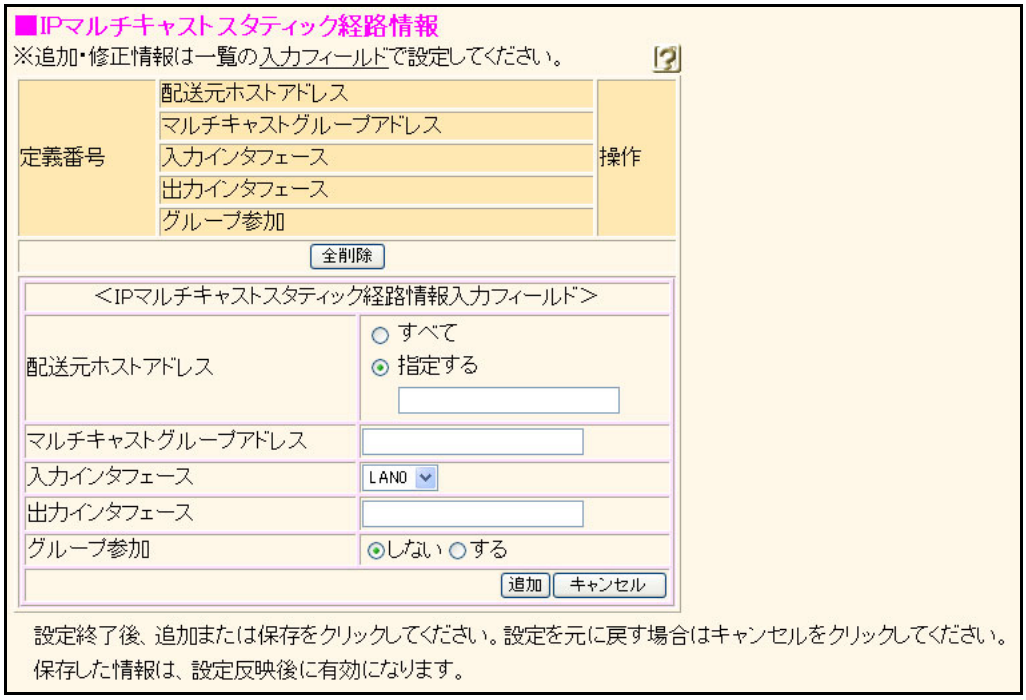
有効範囲）
1.0.0.1 ～ 126.255.255.254
128.0.0.1 ～ 191.255.255.254
192.0.0.1 ～ 223.255.255.254

プライオリティ

RP のプライオリティ情報を 10 進数を使用して、0 ～ 255 の範囲で指定します。数が大きいほど優先度は高くなります。初期値は 0 です。

19.3 IP マルチキャストスタティック経路情報

［操作］　ルータ設定「マルチキャスト情報」→［IP マルチキャストスタティック経路情報］



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、装置全体で 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。

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 アドレスで指定します。

入力インタフェース

入力インタフェースを選択します。

出力インタフェース

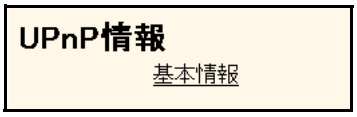
出力インタフェースを指定します。LAN0 ～ max または、rmt0 ～ max で指定してください。複数指定する場合は、"," で区切ります。範囲指定の場合は "-" で区切ります。出力インタフェースは 20 個まで設定できます。

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。

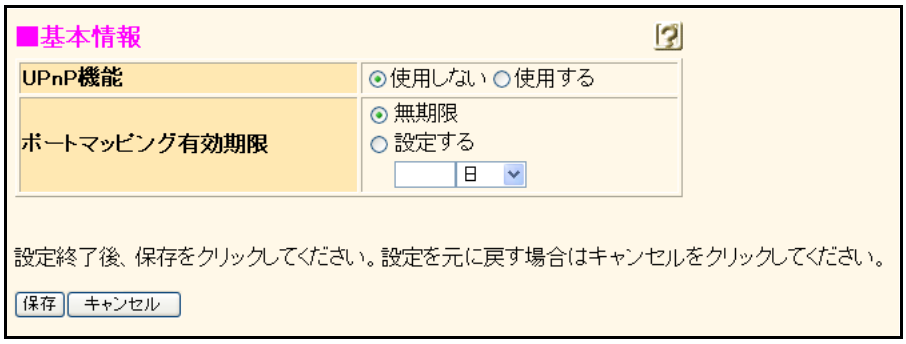
20　UPnP 情報

［操作］　ルータ設定「UPnP 情報」



20.1　基本情報

［操作］　ルータ設定「UPnP 情報」→［基本情報］



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薦めします。**
- **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 トラバーサル機能が動作します。**

ポートマッピング有効期限

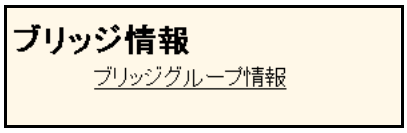
UPnP クライアントがポートマッピングを無期限で設定しようとしたときに、強制的に設定する有効期限を指定します。設定したポートマッピングが使用されなくなってから有効期限を過ぎたとき、そのポートマッピングを強制的に削除します。

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

21　ブリッジ情報

［操作］　ルータ設定「ブリッジ情報」



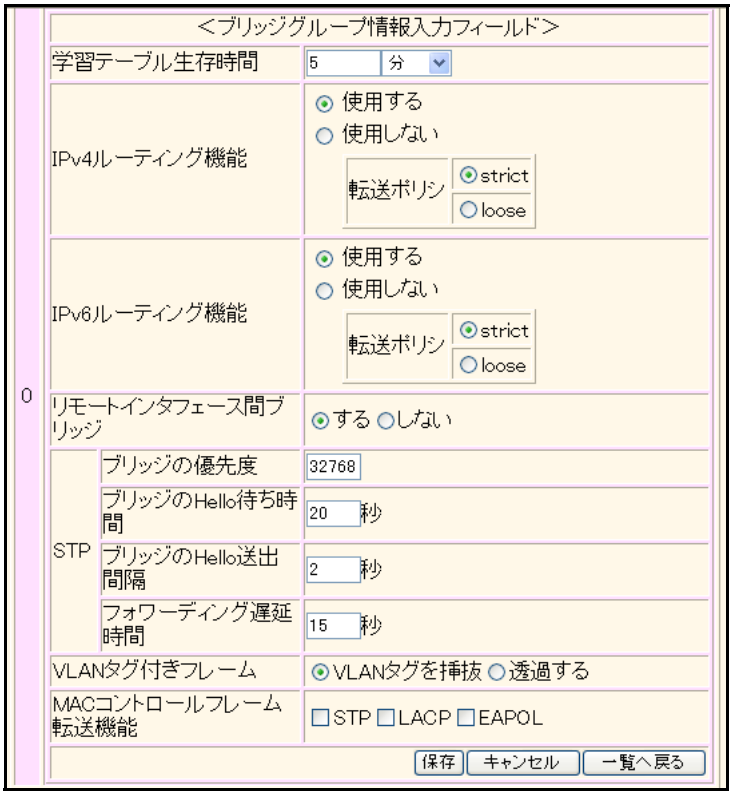
21.1　ブリッジグループ情報

［操作］　ルータ設定「ブリッジ情報」→［ブリッジグループ情報］

ブリッジグループ情報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、８個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

21.1.1　ブリッジグループ情報（グループ識別子 0 の場合）

［操作］　ルータ設定「ブリッジ情報」→［ブリッジグループ情報］→「グループ識別子 0」［修正］



学習テーブル生存時間

学習テーブル生存時間を指定します。グループ識別子 0 で設定した学習テーブル生存時間が全グループで使用されます。初期値は 5 分です。

有効範囲）
1 ～ 11 日
1 ～ 277 時間
1 ～ 16666 分
10 ～ 1000000 秒

IPv4 ルーティング機能

IPv4 をルーティングによって制御する場合は、“ 使用する ” を選択します。

転送ポリシ

IPv4 ブリッジを行う場合に、グループ外からグループ内へ、およびグループ内からグループ外へ、ルーティングによって転送するかどうかを選択します。

受信フレームのあて先 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

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

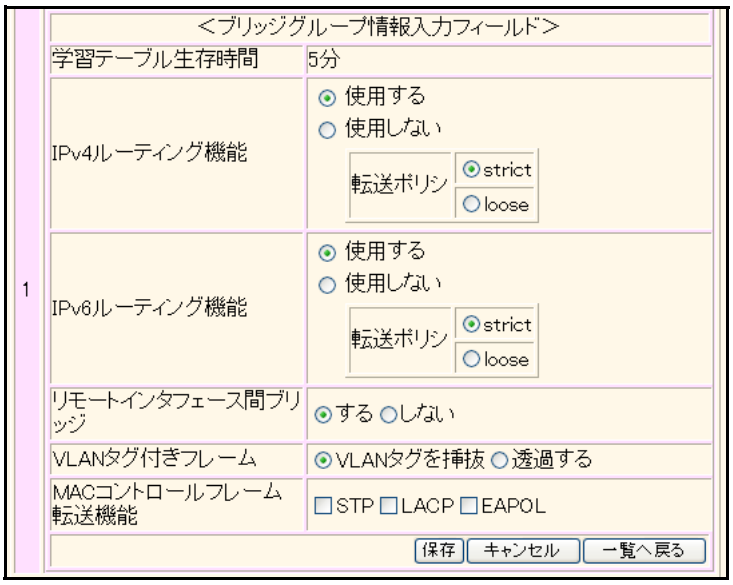
VLAN インタフェースで受信した VLAN タグ付きフレームのタグを透過転送するかどうかを設定します。VLAN タグを挿抜する設定の場合、VLAN インタフェースで受信してリモートインタフェースへ出力する際には VLAN タグを除去して転送し、リモートインタフェースで受信して VLAN インタフェースへ出力する際には VLAN タグを挿入して転送します。

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。

21.1.2　ブリッジグループ情報（グループ識別子１～７の場合）

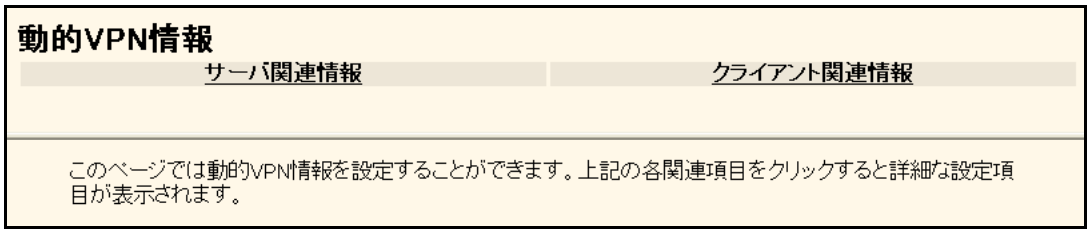
［操作］　ルータ設定「ブリッジ情報」→［ブリッジグループ情報］→［グループ識別子1］［修正］



各項目の説明は、「ブリッジグループ情報（グループ識別子０の場合）」を参照してください。

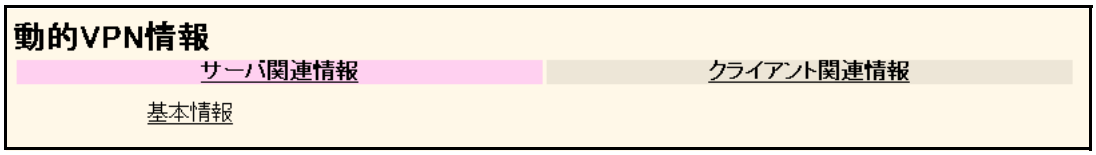
22　動的 VPN 情報

［操作］　ルータ設定「動的 VPN 情報」



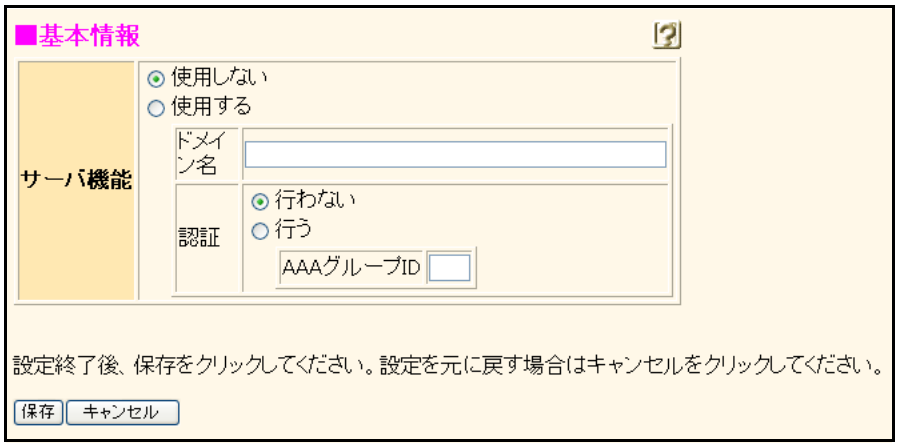
22.1　サーバ関連情報

［操作］　ルータ設定「動的 VPN 情報」→［サーバ関連情報］



22.1.1　基本情報

［操作］　ルータ設定「動的 VPN 情報」→［サーバ関連情報］→［基本情報］



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

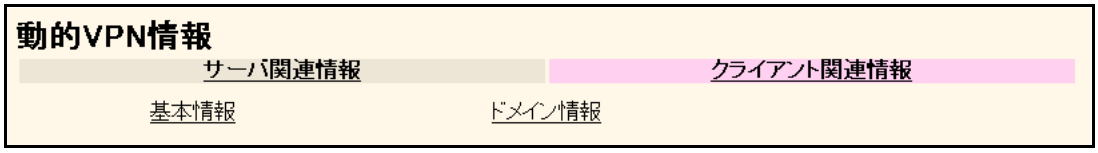
動的 VPN サーバでメッセージの認証を行う場合は “ 行う ” を選択し、参照する AAA のグループ ID を設定します。

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。

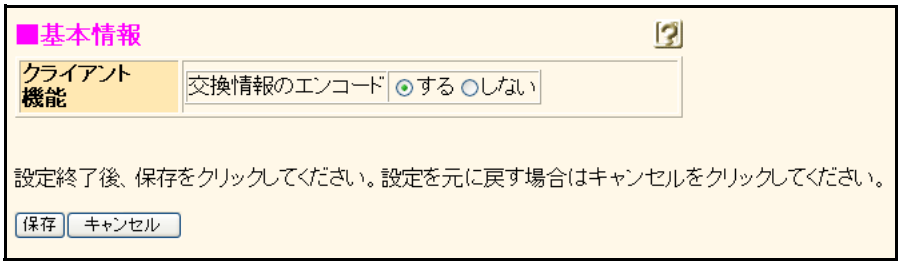
22.2 クライアント関連情報

［操作］　ルータ設定「動的VPN情報」→［クライアント関連情報］



22.2.1 基本情報

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



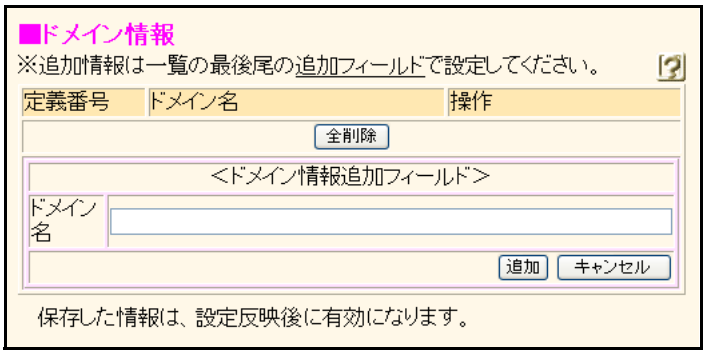
クライアント機能

交換情報のエンコード

動的VPN機能を使用する際に交換情報をエンコードするかどうかを選択します。“する”を選択した場合はbase64でエンコードします。

22.2.2 ドメイン情報

［操作］　ルータ設定「動的VPN情報」→［クライアント関連情報］→［ドメイン情報］



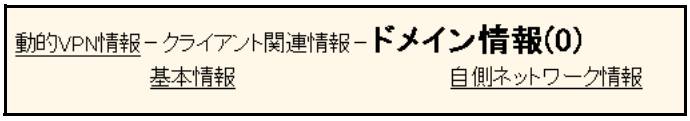
現在、設定されているドメイン情報の定義が表示されています。ドメイン情報の定義数は、2個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

ドメイン名

ドメイン名を80文字以内で指定します。

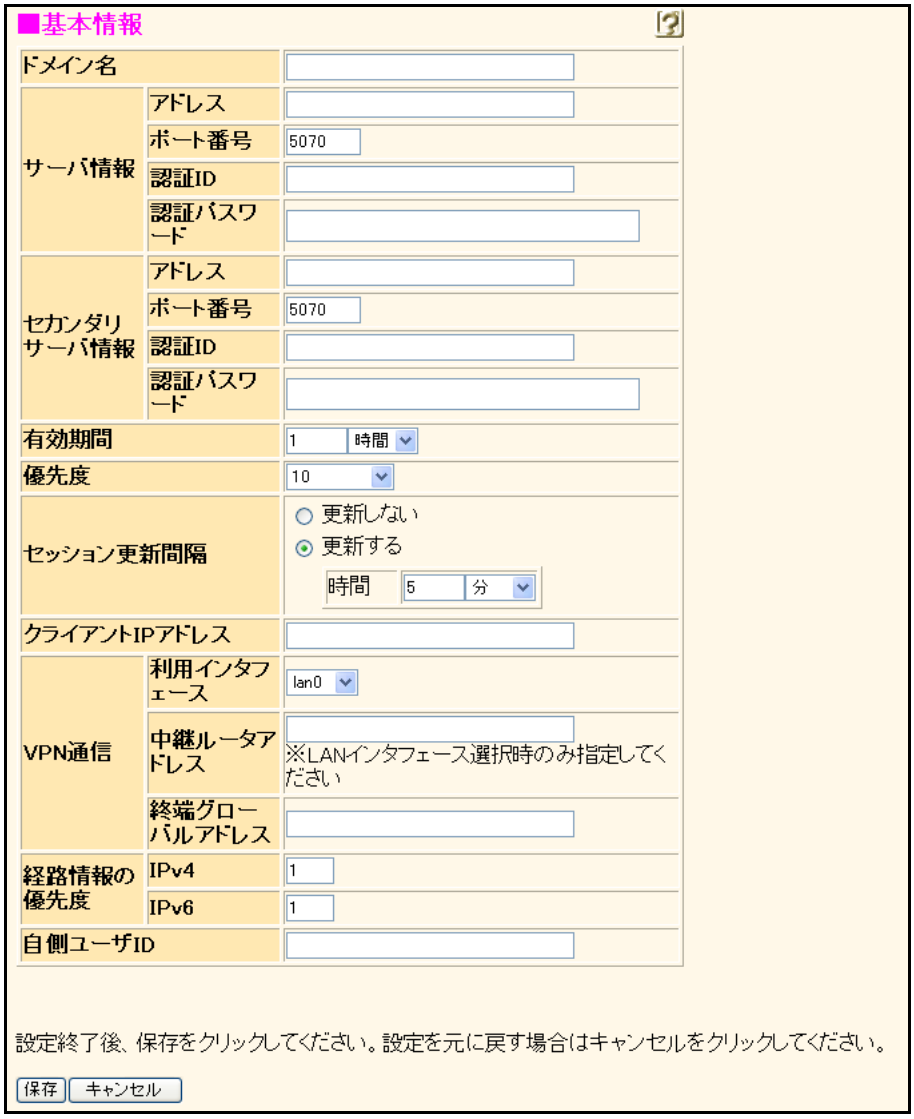
ドメイン名は、動的VPNサーバに登録する自側情報（ユーザID）に使用されます。

［操作］　ルータ設定「動的VPN情報」→［クライアント関連情報］→［ドメイン情報］→［追加］



22.2.2.1　基本情報

［操作］　ルータ設定「動的VPN情報」→［クライアント関連情報］→［ドメイン情報］→［追加］
→［基本情報］



ドメイン名

ドメイン名を80文字以内で指定します。

ドメイン名は、動的VPNサーバに登録する自側情報
（ユーザID）に使用されます。

サーバ情報／セカンダリサーバ情報

アドレス

動的VPNサーバのアドレスを指定します。

- IPアドレスを指定する場合
  有効範囲）
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254
  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
- FQDN指定する場合
  FQDNを80文字以内で設定します。
  なお、RFC1034では英数字、“-”（ハイフン）、“.”（ピリオド）でドメイン名をつけることを推奨しています。

こんな事に気をつけて

FQDN指定する場合は、クライアントIPアドレスのアドレスファミリに従ってIPアドレスを取得します。

ポート番号

動的VPNサーバが要求を受信するポート番号を10進数を使用して、1～65535の範囲で指定します。省略時は、5070が指定されます。

認証ID

動的VPNサーバへ自装置情報を登録するときに使用する認証IDを50文字以内の文字列で指定します。

認証パスワード

動的VPNサーバへ自装置情報を登録するときに使用する認証パスワードを50文字以内の文字列で指定します。

有効期間

動的VPNサーバに登録する自装置の有効期間を90～86400秒の範囲で指定します。省略時は、1時間が指定されます。

優先度

動的VPNクライアントを冗長構成にした場合の優先度を選択します。

セッション更新間隔

確立した動的VPNセッションを更新する時間を90～3600秒の範囲で指定します。省略時は、5分が指定されます。

“更新しない”を選択した場合、確立した動的VPNセッションを更新しません。動的VPNセッションを更新しない場合、動的VPN接続で確立したIPsec/IKEセッションを継続することが可能になりますが、回線障害などにより動的VPNセッションが残ってしまうことがあるので通常は、セッション更新間隔を利用してください。

クライアントIPアドレス

クライアントのIPアドレスを指定します。

クライアントのIPアドレスは、動的VPNサーバとの通信および相手動的VPNクライアントとの情報交換に使用されます。

動的VPNサーバおよび相手動的VPNクライアントとの通信がIPsec対象となる場合は、IPsec対象範囲に含まれるインタフェースの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。

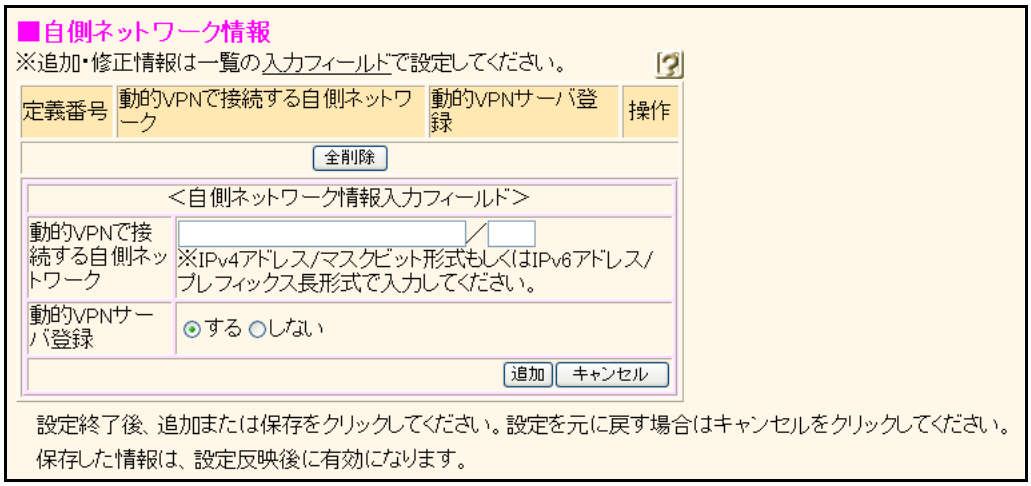
例）自側ユーザIDにshisya、ドメイン名にexample.comを指定した場合
shisya@example.com

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。

22.2.2.2 自側ネットワーク情報

［操作］　ルータ設定「動的VPN情報」→［クライアント関連情報］→［ドメイン情報］→［追加］→［自側ネットワーク情報］



現在、設定されているド自側ネットワーク情報の定義が表示されています。自側ネットワーク情報の定義数は、20個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

動的VPNで接続する自側ネットワーク

動的VPNで接続する自側ネットワークをIPv4アドレスとマスクビット数（またはマスク値）またはIPv6アドレスとプレフィックス長で指定します。

- IPv4アドレスを指定する場合
  IPv4アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから1で連続した値にしてください。
  デフォルトルートを設定する場合は、
  0.0.0.0/0（0.0.0.0/0.0.0.0）を指定します。
- IPv6アドレスを指定する場合
  IPv6アドレスとプレフィックスの組み合わせで指定します。リンクローカルアドレスは指定できません。
  デフォルトルートを設定する場合は、::/0を指定します。
  IPv6 DHCPクライアントが取得したプレフィックスを使用する場合は、上位を“dhcp@インタフェース名”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。

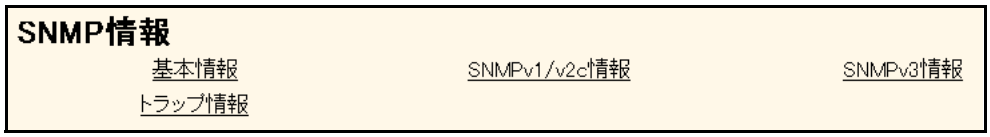
通常は、動的VPNサーバに登録してください。

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
IPsecIKE)c0a80100/24@example.com
IPsecIKE)20010db81111000100000000000000000/64@example.com

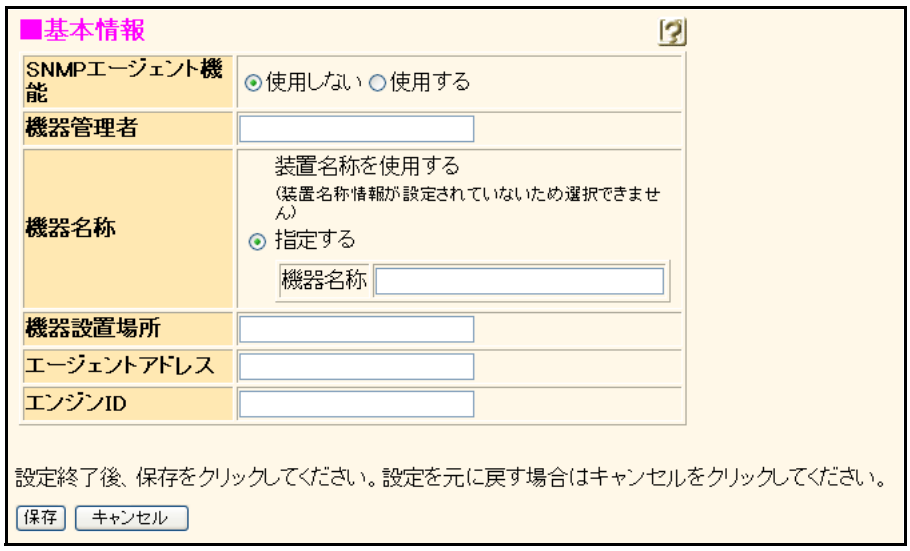
23 SNMP情報

［操作］　ルータ設定「SNMP情報」



23.1 基本情報

［操作］　ルータ設定「SNMP情報」→［基本情報］



SNMPエージェント機能

SNMPエージェント機能を使用すると、SNMPホストの動作しているほかのシステムから本装置の状態を監視できます。SNMPエージェント機能を使用する場合は“使用する”を選択し、以下の項目を設定します。

こんな事に気をつけて

“使用する”から“使用しない”に設定を変更した場合は、定義されているすべてのSNMP情報が削除されます。

機器管理者

本装置の管理者名を40文字以内で指定します。省略時は、機器管理者名を設定しないものとみなされます。

機器名称

機器名称として装置名称を使用する場合は、“装置名称を使用する”を選択します。“指定する”を選択した場合は、本装置の名称を32文字以内で指定します。省略時は、機器名称を設定しないものとみなされます。

機器設置場所

本装置の設置場所を72文字以内で指定します。省略時は、機器設置場所を設定しないものとみなされます。

エージェントアドレス

SNMP エージェントの IP アドレスを指定します。省略時は、エージェントアドレスを設定しないものとみなされます。

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

エンジン ID

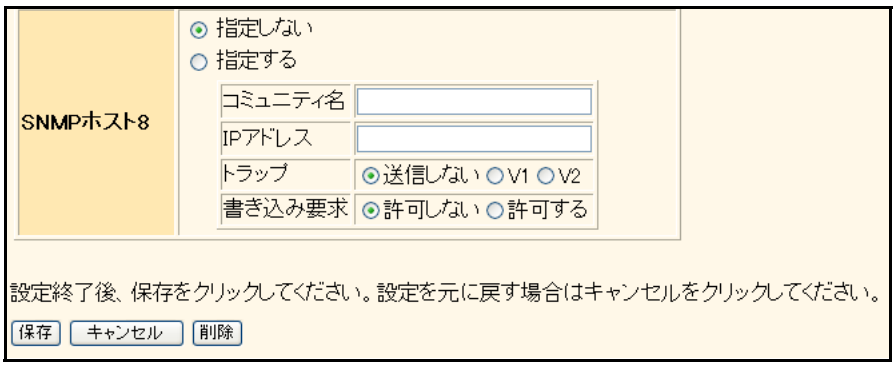
SNMPv3 の SNMP エンジン ID を 27 文字以内で指定します。省略時は、エンジン ID を自動生成します。

装置に設定される SNMP エンジン ID の値は、以下のとおりです。

- 設定した場合
  - 第 1 ～ 5 オクテット：0x800000d304 固定
  - 第 6 オクテット以降：本設定のエンジン ID
- 省略した場合
  - 第 1 ～ 5 オクテット：0x800000d380 固定
  - 第 6 オクテット以降：ランダム値

23.2 SNMPv1/v2c 情報

［操作］　ルータ設定「SNMP 情報」→［SNMPv1/v2c 情報］



SNMP ホスト

SNMP によるアクセスを許可するホストを設定します。ホストは 8 個まで定義できます。“public とする ” を選択すると、コミュニティ名 “public” で任意のホストからのアクセスを許可します。コミュニティ名を変える場合やホストを限定する場合は、“ 指定する ” を選択し、コミュニティ名・IP アドレス・トラップ・書き込み要求を指定します。

コミュニティ名

SNMP により情報交換するグループのコミュニティ名を 32 文字以内で指定します。

IP アドレス

SNMP によるアクセスを許可するホストの IP アドレスを指定します。“0.0.0.0” を指定すると、任意のホストからのアクセスを許可します。

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

トラップ

この SNMP ホストに対して SNMPv1 トラップを送信する場合は、“V1” を、SNMP v2 トラップを送信する場合は、“V2” を選択します。

ただし、任意のホスト（0.0.0.0）を指定している場合は、トラップの送信は行われません。

書き込み要求

この SNMP ホストから書き込み要求を許可する場合は、“ 許可する ” を選択します。

ただし、任意のホスト（0.0.0.0）を指定している場合は、書き込み要求は許可されません。

23.3 SNMPv3 情報

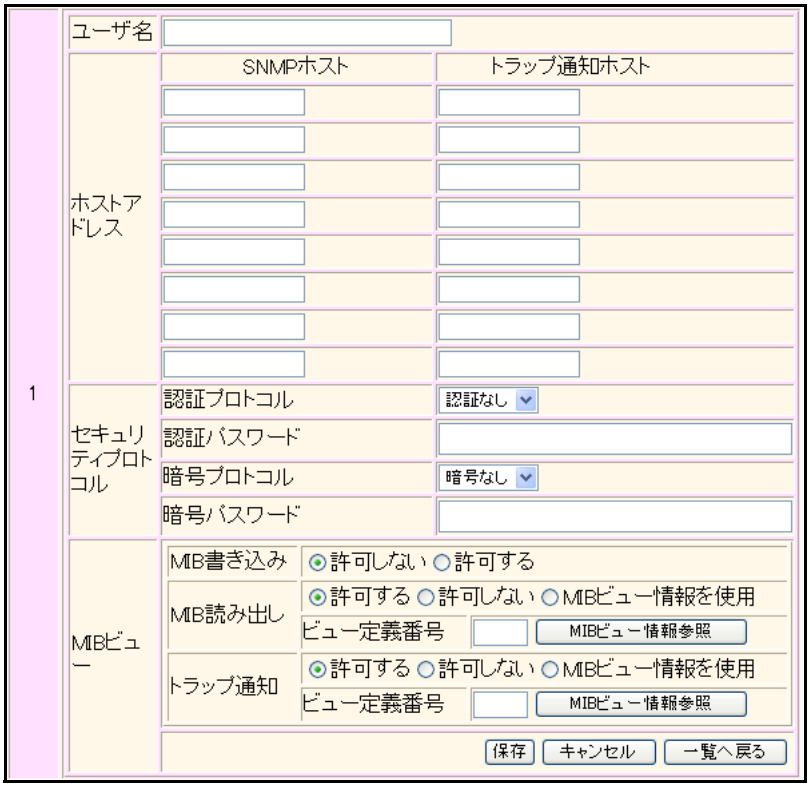
［操作］　ルータ設定「SNMP 情報」→［SNMPv3 情報］

23.3.1 ユーザ情報

［操作］　ルータ設定「SNMP 情報」→［SNMPv3 情報］→［ユーザ情報］

現在、設定されている SNMPv3 情報が表示されています。SNMPv3 情報は、装置全体で 8 個まで設定することができます。処理するボタンをクリックし、次のページへ進みます。

［操作］　ルータ設定「SNMP 情報」→［SNMPv3 情報］→［ユーザ情報］→［修正］



ユーザ名

SNMPv3 の SNMP ユーザ名を 32 文字以内で指定します。SNMPv3 機能を使用する場合は、必ず設定してください。

ホストアドレス

SNMPv3 によるアクセスを許可するホストの IP アドレスとトラップを通知するホストの IP アドレスを指定します。アクセスを許可するホストの IP アドレスとトラップを通知するホストの IP アドレスは、装置全体で合わせて 8 個まで定義できます。省略時は、ホストアドレスを設定しないものとみなされます。

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

セキュリティプロトコル

認証プロトコル

SNMPv3 による認証プロトコルを選択します。

“ 認証なし ” を選択した場合、認証プロトコルは使用されません。

認証パスワード

SNMPv3 による認証プロトコルで使用する、認証パスワードを以下の範囲の文字列で指定します。

認証プロトコル	パスワード長
MD5	8 ～ 16 文字
SHA	8 ～ 20 文字

認証プロトコルに “ 認証なし ” を選択した場合は、省略できます。

暗号プロトコル

SNMPv3 による暗号プロトコルを選択します。

“ 暗号なし ” を選択した場合、暗号プロトコルは使用されません。また、暗号プロトコルを指定した場合は、認証プロトコルを指定してください。

暗号パスワード

SNMPv3 による暗号プロトコルで使用する、暗号パスワードを以下の範囲の文字列で指定します。

暗号プロトコル	パスワード長
DES	8～16 文字

暗号プロトコルに " 暗号なし " を選択した場合は、省略できます。

MIB ビュー

MIB 書き込み

SNMPv3 による MIB 書き込みのアクセス権を許可する場合は、" 許可する " を選択します。

MIB 読み出し

SNMPv3 による MIB 読み出しのアクセス権を許可する場合は、" 許可する " を選択します。

"MIB ビュー情報を参照 " を選択した場合は、必ずビュー定義番号を指定してください。

トラップ通知

SNMPv3 によるトラップ通知のアクセス権を許可する場合は、" 許可する " を選択します。

"MIB ビュー情報を参照 " を選択した場合は、必ずビュー定義番号を指定してください。

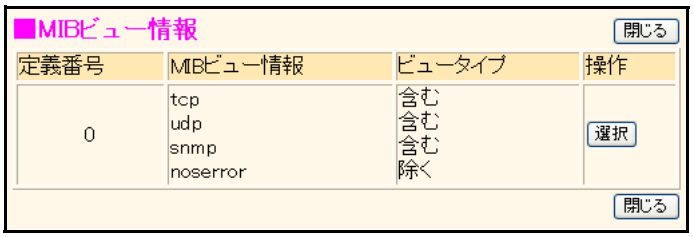
ビュー定義番号

［MIB ビュー情報参照］をクリックして、ビュー定義番号を指定します。

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

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

［操作］　ルータ設定「SNMP 情報」→［SNMPv3 情報］→［ユーザ情報］→［修正］→「ビュー定義番号の［MIB ビュー情報参照］」



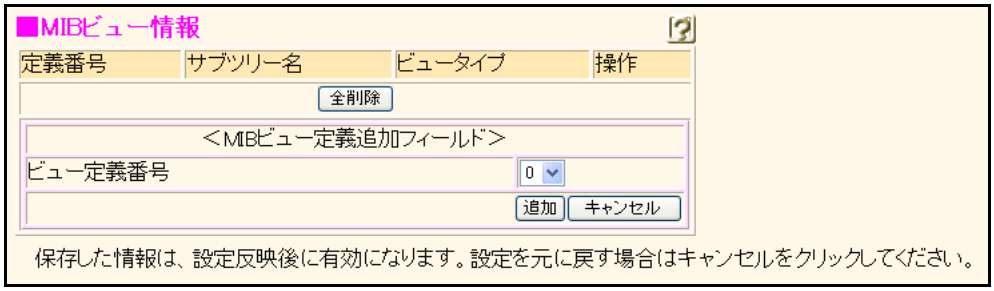
「MIB ビュー情報」-［追加］／［修正］で設定した MIB ビュー定義情報が表示されています。ここで表示されている画面は、表示例であり、初期値ではありません。

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

「ユーザ情報」の MIB ビュー定義番号に設定する定義番号欄の［選択］ボタンをクリックすると、「ユーザ情報」にビュー定義番号が設定され、画面が閉じます。

23.3.2　MIB ビュー情報

［操作］　ルータ設定「SNMP 情報」→［SNMPv3 情報］→［MIB ビュー情報］



現在、設定されている MIB ビュー情報の定義が表示されています。MIB ビュー情報は、装置全体で 8 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

［操作］　ルータ設定「SNMP 情報」→［SNMPv3 情報］→［MIB ビュー情報］→［追加］

サブツリー名

MIB ビュー対象とするサブツリー名を選択します。

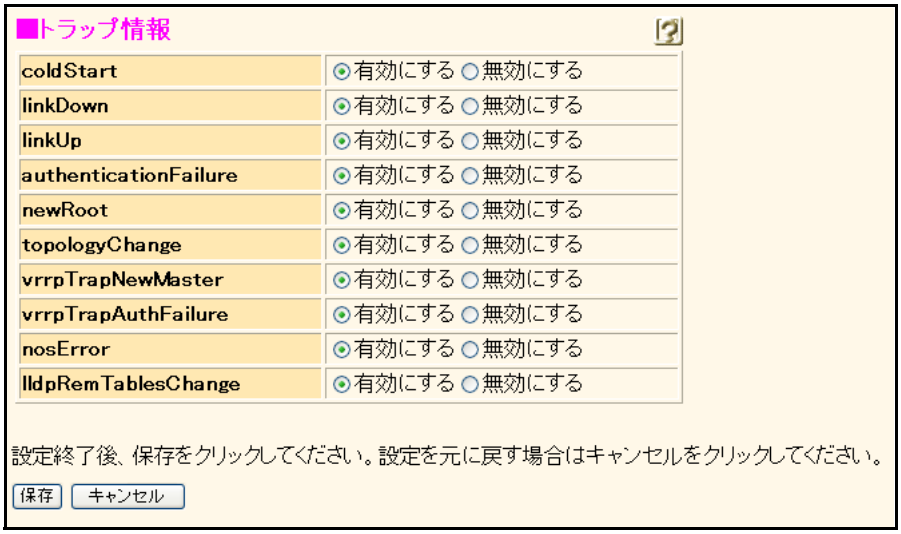
同じビュー定義番号を持つ MIB ビュー情報の設定で、同一サブツリー名を複数選択した場合、最初に選択したサブツリー情報が有効となります。

ビュータイプ

選択したサブツリー名を MIB ビューに含むか、それとも除くかを指定します。

23.4 トラップ情報

［操作］　ルータ設定「SNMP 情報」→［トラップ情報］



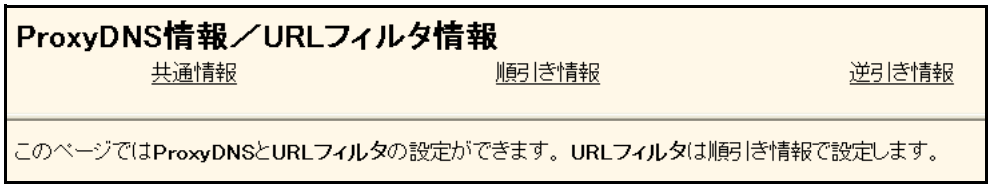
トラップ情報

以下の各トラップを有効にするか無効にするかを選択します。

- coldStart
  本装置の起動時および再起動時に 1 回だけ通知します。
- linkDown
  本装置の通信リンクに障害があったときに通知します。また、装置の再起動時や構成定義反映時にも送信される場合があります。
- linkUp
  本装置の通信リンクの中のどれかが UP 状態になったときに通知します。
- authenticationFailure
  SNMP の認証失敗時に通知します。
- newRoot
  本装置がルートブリッジになるときに通知します。
- topologyChange
  本装置がブリッジネットワークの構成変更を検出したとき、つまりラーニング状態からフォワーディング状態に、またはフォワーディング状態からブロッキング状態に変更するときに通知します。
- vrrpTrapNewMaster
  本装置が VRRP グループでマスタとなったときに通知します。
- vrrpTrapAuthFailure
  本装置で受信した VRRP-AD メッセージの認証方法が異常、または VRRP グループに設定された認証方法やパスワードが一致しないときに通知します。
- nosError
  本装置になんらかの異常（ハードウェア異常）が発生したときに通知します。このトラップは異常が発生したことだけを通知します。
- lldpRemTablesChange
  隣接装置情報管理テーブルに変化があったときに通知します。

24　ProxyDNS 情報／ URL フィルタ情報

［操作］　ルータ設定「ProxyDNS 情報 URL フィルタ情報」



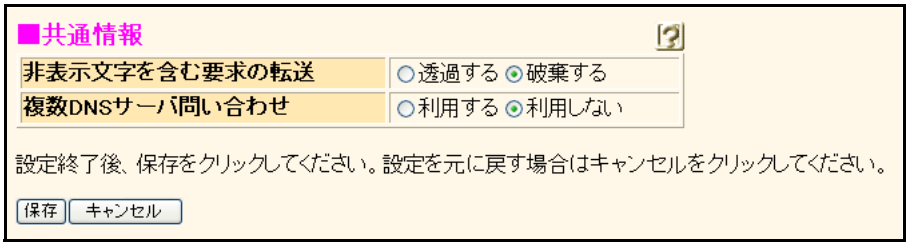
ヒント

◆ 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。

24.1 共通情報

［操作］　ルータ設定「ProxyDNS 情報 URL フィルタ情報」→［共通情報］



非表示文字を含む要求の転送

DNS 問い合わせ名（QNAME）に非表示文字が含まれる場合に、その問い合わせのパケットを透過するか破棄するかを選択します。

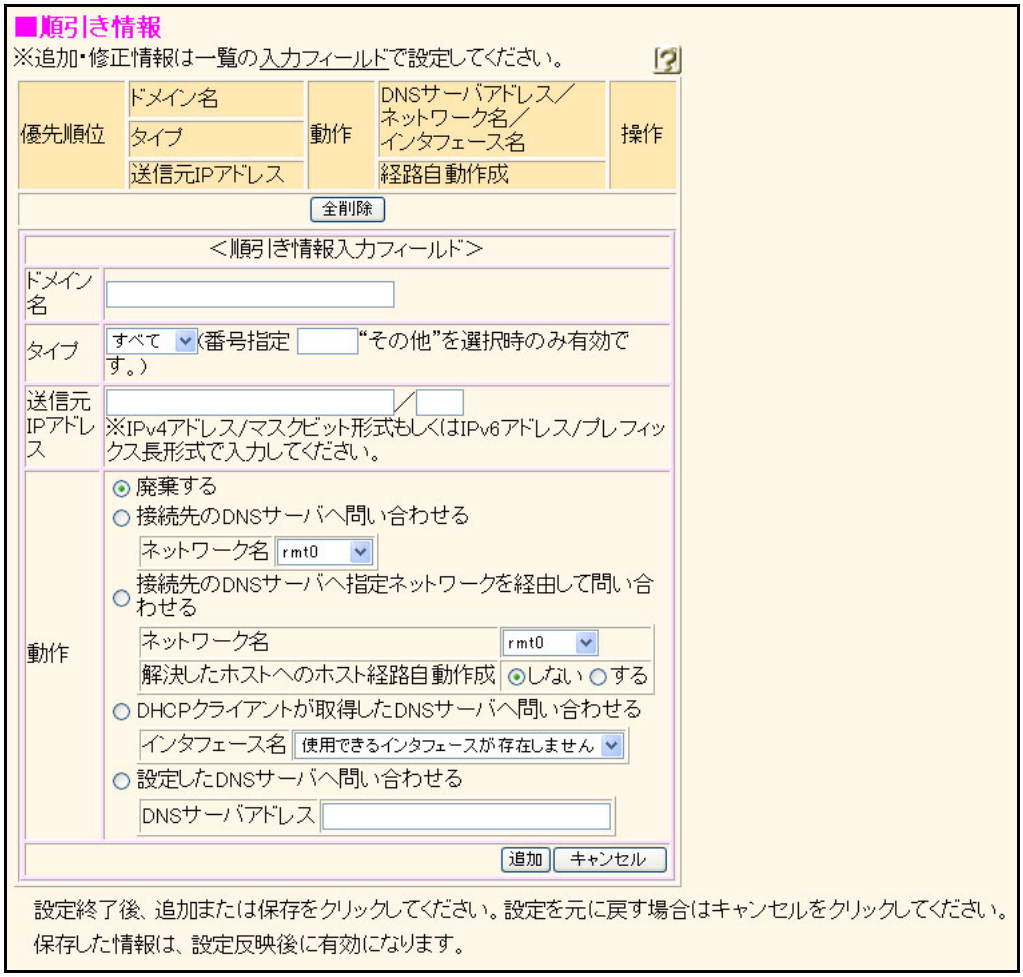
複数 DNS サーバ問い合わせ

DNS 問い合わせを転送する場合に、複数 DNS サーバに対して問い合わせを行うかどうかを選択します。

- 利用する
  利用できる複数の DNS サーバすべてに問い合わせを転送します。
- 利用しない
  プライマリ DNS サーバにのみ問い合わせを転送します。

24.2 順引き情報

［操作］　ルータ設定「ProxyDNS 情報 URL フィルタ情報」→［順引き情報］



順引き情報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、32 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。

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

ドメイン名

対象とするドメイン名の範囲を80文字以内で指定します。ただし、以下のように、“*”および“?”はワイルドカードとして使用されるため、ドメイン名には使用できません。なお、ドメイン名のチェックには大文字／小文字の区別はありません。

“*”：0文字以上の任意の文字に一致する

“?”：1文字の任意文字に一致する

記述例）

条件	一致
www.*.com	www.testa.com、www.test1.test.com
test	www.test.com、test.com、test.co.jp
www.test？.com	www.test1.com、www.test2.com、www.testA.com

タイプ

対象とする問い合わせタイプを以下から選択します。()内はタイプの番号です。

- すべて（PTR（12）を除く）
- A（1）
- NS（2）
- CNAME（5）
- SOA（6）
- HINFO（13）
- MX（15）
- AAAA（28）
- SRV（33）
- その他

任意のタイプを指定する場合は、“その他”を選択し、10進数を使用して、1～11、13～65535の範囲で指定します。

送信元IPアドレス

フィルタリング条件としての送信元IPアドレスをIPv4アドレス／ネットマスク、またはIPv6アドレス／プレフィックスの形式で設定します。

0.0.0.0/0、::/0を指定した場合、または、省略した場合は、すべてのアドレスを対象とするものとして動作します。

動作

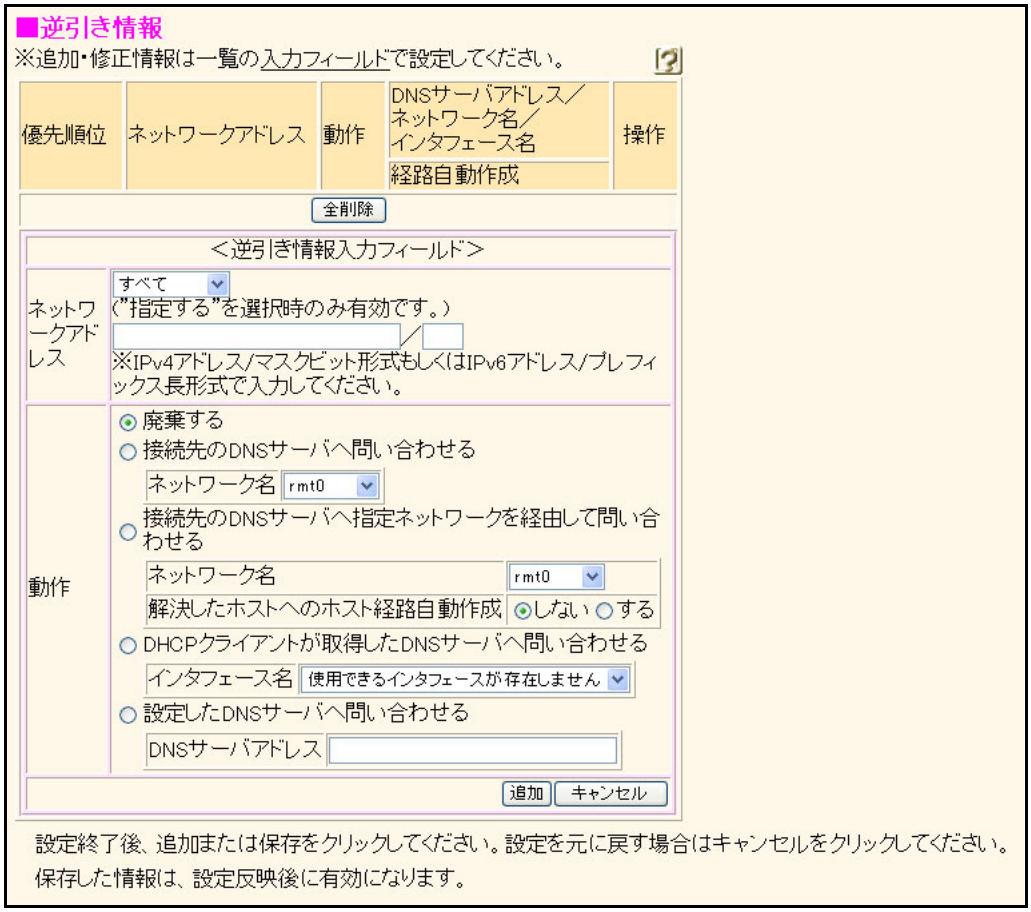
対象ドメイン、問い合わせタイプ、送信元IPアドレスに対する動作を以下の4つから選択します。

- 廃棄する
  該当ドメインの転送を無効にするフィルタ（URLフィルタ）または、該当問い合わせタイプのDNSパケットの転送を無効にするフィルタ（問い合わせタイプフィルタ）として利用します。
- 接続先のDNSサーバへ問い合わせる
  接続先情報で設定されたDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
- 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる
  接続先情報で設定したDNSサーバへ問い合わせます。どのネットワークで使用するかを選択します。選択したネットワークに複数の接続先が登録されている場合は、マルチルーティングと優先順位に従って接続先を決定します。
  “接続先のDNSサーバへ問い合わせる”との違いは、必ず指定したネットワークを経由してDNSサーバへ問い合わせることです。また、解決したホストへのホスト経路自動作成に“する”を選択することにより、DNS解決したホストへのホスト経路を自動で作成することができます。
- DHCPクライアントが取得したDNSサーバへ問い合わせる
  DHCPクライアントが取得したDNSサーバへ問い合わせます。DHCPクライアントが動作しているインタ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

24.3 逆引き情報

［操作］　ルータ設定「ProxyDNS 情報 URL フィルタ情報」→［逆引き情報］



逆引き情報は 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、32 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。

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

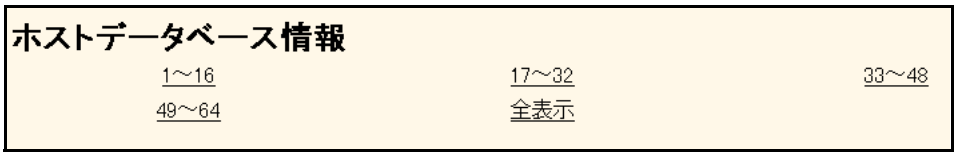
対象ドメインに対する動作を以下の3つから選択します。

- 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。

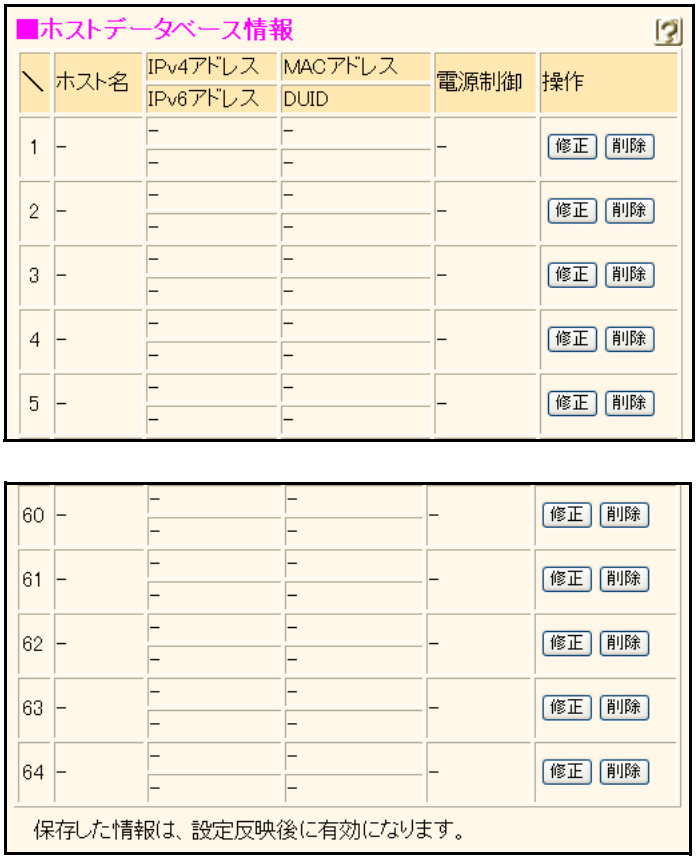
  有効範囲）
  1.0.0.1 ～ 126.255.255.254
  128.0.0.1 ～ 191.255.255.254
  192.0.0.1 ～ 223.255.255.254
  ::2 ～ fe7f:ffff:ffff:ffff:ffff:ffff:ffff:ffff
  fec0:: ～ feff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

25　ホストデータベース情報

［操作］　ルータ設定「ホストデータベース情報」



［操作］　ルータ設定「ホストデータベース情報」→［全表示］



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、装置全体で 64 個まで設定できます。処理するボタンをクリックし、次のページへ進みます。

［操作］　ルータ設定「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」「IPv4 アドレス」または「IPv6 アドレス」のペアを登録することにより、ProxyDNS の DNS サーバ機能を使用することができます。
- リモートパワーオン機能
  「MAC アドレス」を登録することにより、Wakeup on LAN 機能を使用することができます。
- IPv4 DHCP スタティック機能
  「IPv4 アドレス」「MAC アドレス」のペアを登録することにより、DHCP で割り当てられる IPv4 アドレスを端末固有のものとすることができます。
- IPv6 DHCP スタティック機能
  「IPv6 アドレス」「DUID」のペアを登録することにより、IPv6 DHCP で割り当てられる IPv6 アドレスを端末固有のものとすることができます。

ホスト名

DNS サーバ機能で使用されます。80 文字以内で指定します。使用できる文字は半角英数字、“.”、“-” です。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 IPv4 DHCP スタティック機能で使用されます。

IPv6 アドレス

DNS サーバ機能および IPv6 DHCP スタティック機能で使用されます。

MAC アドレス

IPv4 DHCP スタティック機能およびリモートパワーオン機能で使用されます。MAC アドレスは以下の形式で指定します。

xx:xx:xx:xx:xx:xx（xx は 2 桁の 16 進数）

DUID

IPv6 DHCP スタティック機能で使用されます。260 桁以内の 16 進数で表記した DUID を指定します。

電源制御（リモート電源制御）

本装置と同じセグメントに存在する Wakeup on LAN 対応機器を、リモートパワーオン指示の対象とする場合は、“ 対象 ” を選択します。

この設定はスケジュール機能や手動操作でリモートパワーオンを指示する場合に使用されます。

索引

A

AAA 情報 276
AAA ユーザ情報 277
ACL 情報 296
ACL 定義情報 297
AH 140, 258
ARP 情報 85
AS 外部経路集約情報 331
AS 境界ルータ情報 331

B

BGP 相手基本情報 317
BGP 相手情報 317
BGP 拡張機能情報 322
BGP 関連 314
BGP 情報 314

D

DHCP 情報 81
DNS サーバ機能 363, 370
DNS サーバの自動切り替え機能 363
DNS 問い合わせタイプフィルタ機能 363

E

ECMP 情報 308
ESP 140, 258

I

ICMP 情報 83
ICMP 定義情報 300
IDS 情報
  LAN 情報 67
  相手情報 167
  テンプレート情報 231
IKE 情報
  AAA 情報 284
  相手情報
    拡張 IPsec 対象範囲情報 148
  テンプレート情報
    RADIUS/AAA 260
    動的 VPN 共有鍵認証方式 266
IKE 情報（共有鍵認証方式）
  相手情報 145
IKE 情報（動的 VPN 接続 共有鍵認証方式）
  相手情報
    動的 VPN 147
IPsec/IKE 関連
  AAA 情報 283
  テンプレート情報
    RADIUS/AAA 258
    動的 VPN 共有鍵認証方式 266
IPsec 情報
  AAA 情報 283
  相手情報
    自動鍵 139
    手動鍵 142
    動的 VPN 144
  テンプレート情報 258
IPv4 BGP 再配布フィルタリング情報 323
IPv4 BGP 集約経路情報 316
IPv4 BGP ネットワーク情報 315
IPv4 BGP フィルタリング情報 320
IPv4 DHCP スタティック機能 370
IPv4 ループバック情報 33
IPv6 DHCP 情報
  LAN 情報 108
  相手情報 207
IPv6 DHCP スタティック機能 370
IPv6 RIP 関連 336
IPv6 RIP 再配布フィルタリング情報 337
IPv6 RIP 情報
  LAN 情報 89
  相手情報 189
IPv6 RIP タイマ情報 336
IPv6 RIP フィルタリング情報
  LAN 情報 102
  相手情報 201
IPv6 RIP マルチパス情報 337
IPv6 Traffic Class 値書き換え情報
  LAN 情報 98
  相手情報 197
  テンプレート情報 250
IPv6 動的 VPN 情報 211
IPv6 関連
  AAA 情報 281
  LAN 情報 86
  相手情報 185
  テンプレート情報 243
IPv6 基本情報
  AAA 情報 281
  LAN 情報 86
  相手情報 185
  テンプレート情報 243
IPv6 再配布情報 334
IPv6 スタティック経路情報
  AAA 情報 282
  LAN 情報 91
  相手情報 190
IPv6 帯域制御（WFQ）情報
  LAN 情報 104
  相手情報 202
  テンプレート情報 254
IPv6 定義情報 301
IPv6 フィルタリング情報
  LAN 情報 92
  相手情報 191

テンプレート情報 244
IPv6 優先度情報 335
IPv6 ルーティングマネージャ情報 334
IPv6 ループバック情報 34
IP アドレス情報 54
IP 関連
AAA 情報 279
LAN 情報 54
相手情報 154
テンプレート情報 224
IP 基本情報
AAA 情報 279
相手情報 154
テンプレート情報 224
IP 情報 303
IP 定義情報 298
IP フィルタリング情報
LAN 情報 61
相手情報 160
テンプレート情報 225
IP マルチキャスト情報 339
IP マルチキャストスタティック RP 情報 341
IP マルチキャストスタティック経路情報 342

L

LAN 情報 41
LLDP 情報 273
LAN 情報 50

M

MAC アドレス認証情報
LAN 情報 52
認証情報 275
MAC 定義情報 302
MAC フィルタリング情報
LAN 情報 114
相手情報 214
MIB ビュー情報 361

N

NAT あて先変換情報
LAN 情報 76
相手情報 177
テンプレート情報 238
NAT 情報
LAN 情報 72
相手情報 173
テンプレート情報 234

O

OSPF エリア基本情報 325
OSPF エリア情報 325
OSPF 関連 324
OSPF 再配布フィルタリング情報 332
OSPF 情報
LAN 情報 57
相手情報 156

P

PPPoE 情報 130
PPP 関連
相手情報 153
PPP 情報
PPPoE 接続 130
ProxyDNS 情報 363

R

RADIUS 関連 288
RIP 相手フィルタリング情報 313
RIP 関連 309
RIP 再配布フィルタリング情報 310
RIP 情報
LAN 情報 56
相手情報 155
RIP タイマ情報 309
RIP フィルタリング情報
LAN 情報 71
相手情報 172
RIP マルチパス情報 310
RIP ユニキャスト送信情報 312

S

SNMPv1/v2c 情報 356
SNMPv3 情報 358
SNMP 情報 354

T

TCP 定義情報 299
TOS 値書き換え情報
LAN 情報 67
相手情報 168
テンプレート情報 231

U

UDP 定義情報 299
UPnP 情報 343
URL フィルタ機能 363
URL フィルタ情報 363

V

VLAN プライオリティマッピング情報 122
VRRP アクション情報 48
VRRP グループ情報 44
VRRP トリガ情報 46

あ

相手情報 123
圧縮情報
　相手情報 153
アプリケーションフィルタ情報 35

い

異常時動作情報 32
インタフェース情報 304

お

オプション設定
　PPPoE 接続 22
　プライベート LAN 接続 20

か

拡張 IPsec 対象範囲情報 285
かんたん設定
　PPPoE 接続 22
　プライベート LAN 構築 19
かんたん設定メニュー 8

き

基本情報
　AAA 情報
　　RADIUS 関連 288
　　共通情報 277
　IP 情報 303
　LAN 情報
　　VRRP グループ情報 44
　　共通情報（VLAN） 120
　　共通情報（物理 LAN） 42
　LLDP 情報 273
　SNMP 情報 354
　UPnP 情報 343
　相手情報
　　IPsec/IKE 接続 136
　　IP トンネル接続 133
　　PPPoE 接続 127
　　共通情報 124
　　パケット破棄 152
　　別インタフェースから送出 151
　スイッチ情報 39
　テンプレート情報
　　RADIUS/AAA 221
　　動的 VPN 共有鍵認証方式 264, 269
　動的 VPN 情報
　　クライアント関連情報 349, 350
　　サーバ関連情報 348
　パスワード情報 24
基本定義情報 297
逆引き情報 367
共通情報
　AAA 情報 276
　LAN 情報（VLAN） 120
　LAN 情報（物理 LAN） 42
　ProxyDNS 情報／ URL フィルタ情報 364
　相手情報 124
　テンプレート情報
　　RADIUS/AAA 221
　　動的 VPN 共有鍵認証方式 264

く

クライアント機能
　サーバ情報 290
　送信情報 294
クライアント情報
　サーバ機能 295
グループ ID 情報 276

け

経路集約情報 326
月間／週間予約情報 37

こ

構成定義切り替え予約情報 38

さ

サーバ機能情報 34
再配布情報 305

し

自側ネットワーク情報
　動的 VPN 共有鍵認証方式 272
　動的 VPN 情報 353
システムログ情報 30
順引き情報 365
詳細設定メニュー 8

す

スイッチ情報 39
スケジュール情報 37
スタティック経路情報
　AAA 情報 280
　LAN 情報 59
　相手情報 159

せ

静的 MAC 学習テーブル情報 117
静的 NAT 情報
　LAN 情報 74
　相手情報 175
　テンプレート情報 236
セカンダリ IP アドレス情報 55
セグメント接続／分割 21

接続先監視 263, 268, 287
接続先情報 126
接続先種別
IPsec/IKE 接続 135
IP トンネル接続 133
PPPoE 接続 127
パケット破棄 152
別インタフェースから送出 151
接続制御情報
AAA 情報 286
相手情報
IPsec/IKE 接続 138
IP トンネル接続 134
PPPoE 接続 128
テンプレート情報
RADIUS/AAA 262
動的 VPN 共有鍵認証方式 267
設定メニュー 8

そ

装置情報 28

た

帯域制御（WFQ）情報 118
LAN 情報 77
相手情報
IP 関連 178
ブリッジ関連 218
テンプレート情報 239
タイムサーバ情報 29

て

テンプレート情報 220

と

動的 VPN 関連
テンプレート情報
動的 VPN 共有鍵認証方式 269
動的 VPN 情報 348
相手情報 183
ドメイン情報
動的 VPN 情報 349
トラップ情報
LAN 情報 53
SNMP 情報 362
相手情報
PPPoE 接続 132
共通情報 125
テンプレート情報
RADIUS/AAA 223

に

認証情報 275
AAA 情報 278

ね

ネットワーク情報 123

は

バーチャルリンク情報 329
パスワード情報 24

ひ

必須設定
PPPoE 接続 22
プライベート LAN 接続 19

ふ

ファームウェア更新情報 31
ブリッジ関連
LAN 情報 113
相手情報 213
ブリッジグループ情報 344
ブリッジ情報 344
LAN 情報 113
相手情報 213

ほ

ポート情報 40
ホストデータベース情報 369

ま

マニュアル構成 7
マルチキャスト情報 339
LAN 情報 84
相手情報 182
マルチルーティング情報 131

ゆ

ユーザ情報 358
優先度情報 307

り

リモートパワーオン機能 370

る

ルータ ID 情報 324
ルータ名称情報 28
ルーティングプロトコル情報 304
ルーティングマネージャ情報 305

ろ

ログインパスワード情報 25
ログインユーザ情報 26

Si-R brin シリーズ　Web リファレンス

P3NK-3402-03Z0

発行日　　2016 年 12 月

発行責任　　富士通株式会社