P3NK-7132-02Z0

FUJITSU Network SR-S
Web設定事例集

V20

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。
認証機能などによりセキュリティを強化して、安全なネットワークを提供するために、本装置をご利用ください。

2020年 1月初　版
2022年 11月第 2版

目次

本書の使いかた

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

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

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

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

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

本書における商標の表記について

Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

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

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® 10 Home 64 ビット版	Windows 10 または Windows
Microsoft® Windows® 10 Pro 64 ビット版	

本装置のマニュアルの構成

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

マニュアル名称	内容
ご利用にあたって	本装置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	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（本書）	Web 画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Web リファレンス	Web 画面の項目の詳細な情報を説明しています。

1　VLAN 機能を使う

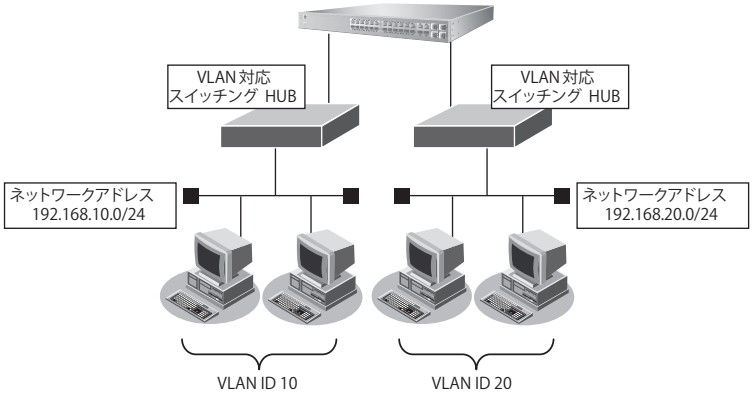
適用機種　全機種

1.1　ポート VLAN 機能を使う

適用機種　全機種

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

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER1、5 ポートを使用する
- VLAN 対応スイッチング HUB で VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER1 ポートの VLAN を設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

3.　以下の項目を指定します。

- VLAN
  Untagged　　→ 10

4.　［保存］ボタンをクリックします。

5.　手順 1.～4. を参考に、ETHER5 ポートを設定します。

- VLAN
  Untagged　→ 20

VLAN10 のネットワークを設定する

6.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

7.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

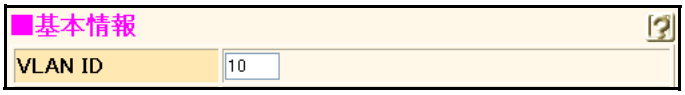
「LAN0 情報」ページが表示されます。

8.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- VLAN ID　→ 10



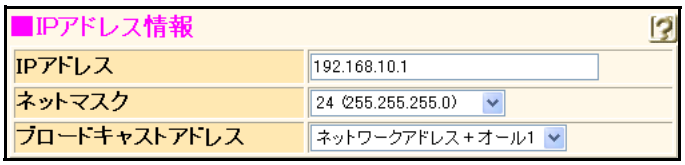
10.　［保存］ボタンをクリックします。

11.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

12.　以下の項目を指定します。

- IP アドレス　→ 192.168.10.1
- ネットマスク　→ 24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1



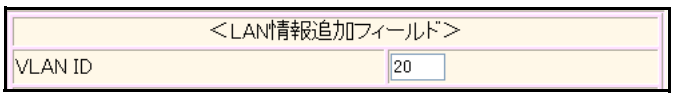
13.　［保存］ボタンをクリックします。

14.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

15.　以下の項目を指定します。

- VLAN ID　→ 20



16.　［追加］ボタンをクリックします。

「LAN1 情報」ページが表示されます。

17.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

18. 手順 12.～13. を参考に、以下の項目を設定します。

- IPアドレス →192.168.20.1
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール1

19. 画面左側の［設定反映］ボタンをクリックします。

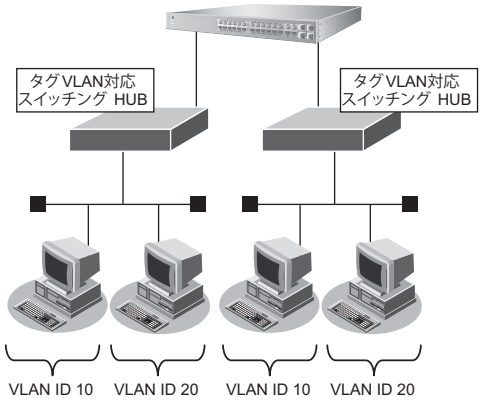
設定した内容が有効になります。

1.2　タグVLAN機能を使う

適用機種　全機種

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

SR-S332TR1の場合を例にします。



● 設定条件

- ETHER1、5ポートを使用する
- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER1、ETHER5ポートのVLANを設定する

1.　設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2.　以下の項目を指定します。

- ポートリスト　　→1,5

3.　［修正］ボタンをクリックします。

ether 1,5情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- VLAN
  Tagged　　→10,20

5.　［保存］ボタンをクリックします。

VLAN10、VLAN20 のネットワークを設定する

6. 「1.1 ポート VLAN 機能を使う」（P.9）の 手順 6. ～ 18. を参考に、VLAN のネットワークを設定します。

「LAN0 情報」-「共通情報」-「基本情報」

- VLAN ID →10

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス →192.168.10.1
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

「LAN 情報」

- VLAN ID →20

「LAN1 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス →192.168.20.1
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

7. **画面左側の［設定反映］ボタンをクリックします。**

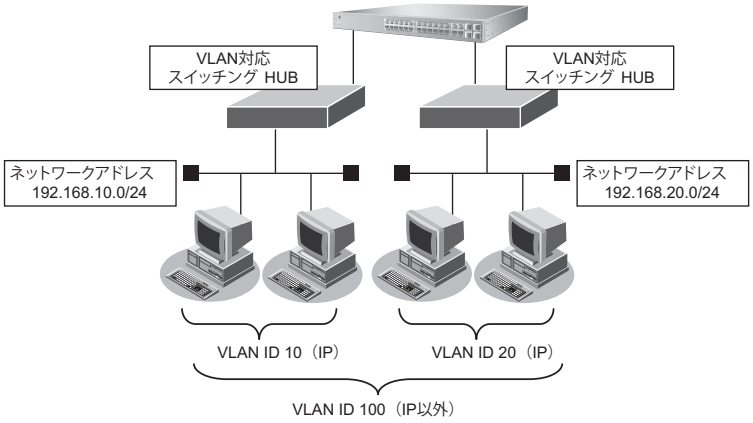
設定した内容が有効になります。

1.3 プロトコルVLAN機能を使う

適用機種 全機種

ここでは、IPプロトコルのパケットをそれぞれのポートでVLAN10およびVLAN20として送受信し、IPプロトコル以外のパケットについてはVLAN100として送受信する場合の設定方法を説明します。

SR-S332TR1の場合を例にします。



● 設定条件

- ETHER1、5ポートを使用する
- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24
  VLAN ID：100

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER1ポートのVLANを設定する

1. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2. 「ether情報」でポート番号が1の［修正］ボタンをクリックします。

ether 1情報の設定項目と「基本情報」が表示されます。

3. 以下の項目を指定します。

- VLAN
  Untagged　　→10,100

4. ［保存］ボタンをクリックします。

5. 手順1.～4.を参考に、ETHER5ポートを設定します。

- VLAN
  Untagged　　→20,100

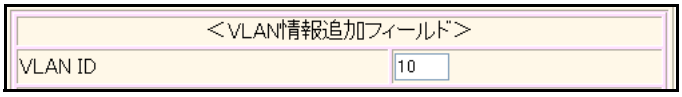
VLAN10 をプロトコル VLAN に設定する

6.　設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- VLAN ID　→ 10



8.　［追加］ボタンをクリックします。

「VLAN10 情報」ページが表示されます。

9.　「基本情報」をクリックします。

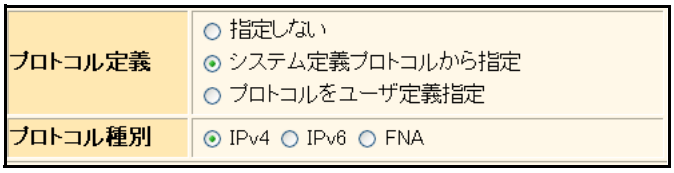
「基本情報」が表示されます。

10.　以下の項目を指定します。

- プロトコル定義　→システム定義プロトコルから指定

“ システム定義プロトコルから指定 ” を選択すると、「プロトコル種別」の設定項目が表示されます。

- プロトコル種別　→ IPv4



11.　［保存］ボタンをクリックします。

12.　手順 6. ～ 11. を参考に、以下の項目を設定します。

「VLAN 情報」

- VLAN ID　→ 20

「VLAN20 情報」-「基本情報」

- プロトコル定義　→システム定義プロトコルから指定
- プロトコル種別　→ IPv4

VLAN10、VLAN20 のネットワークを設定する

13.　「1.1 ポート VLAN 機能を使う」（P.9）の 手順 6. ～ 18. を参考に、VLAN のネットワークを設定します。

「LAN0 情報」-「共通情報」-「基本情報」

- VLAN ID　→ 10

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス　→ 192.168.10.1
- ネットマスク　→ 24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1

「LAN 情報」

- VLAN ID　→ 20

「LAN1情報」-「IP関連」-「IPアドレス情報」

- IPアドレス　→192.168.20.1
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1

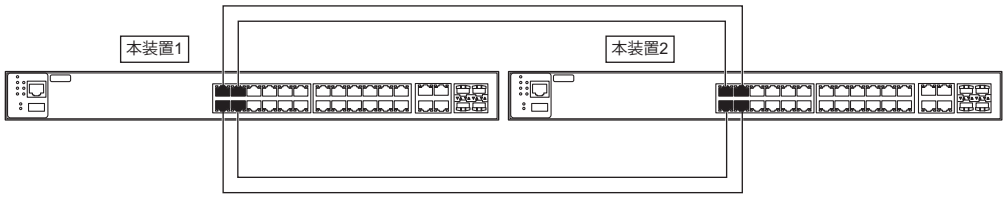
14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

2　リンクアグリゲーション機能を使う

適用機種　全機種

ここでは、4 ポートの 1000M 回線をリンクアグリゲーションとする場合の設定方法を説明します。
SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER1 ～ 4 ポートを使用する
- 通信速度を 1000Mbps 固定に変更する
- VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　以下の項目を指定します。

- ポートリスト　　→ 1-4

3.　［修正］ボタンをクリックします。

ether 1-4 情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- 通信速度　　→ 1000Mbps
- VLAN
  Tagged　　→ 10,20

5.　［保存］ボタンをクリックします。

6.　「ポート種別情報」をクリックします。

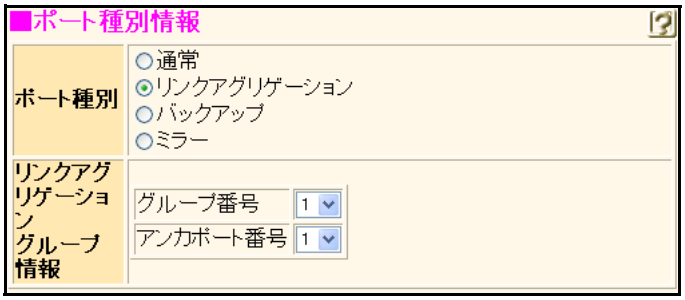
「ポート種別情報」が表示されます。

7.　以下の項目を指定します。

- ポート種別　→リンクアグリゲーション

“リンクアグリゲーション”を選択すると、「リンクアグリゲーショングループ情報」の設定項目が表示されます。

- リンクアグリゲーショングループ情報
  グループ番号　→1
  アンカポート番号　→1



8.　［保存］ボタンをクリックします。

9.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

10.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

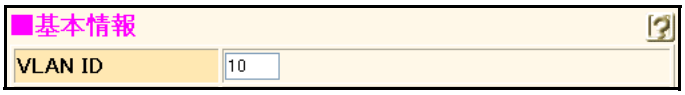
「LAN0 情報」ページが表示されます。

11.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

12.　以下の項目を指定します。

- VLAN ID　→10



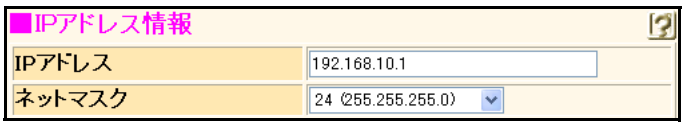
13.　［保存］ボタンをクリックします。

14.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

15.　以下の項目を指定します。

- IP アドレス　→192.168.10.1
- ネットマスク　→24（255.255.255.0）



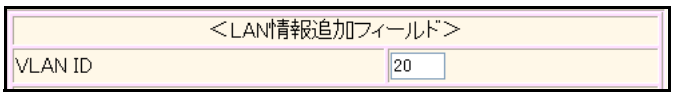
16.　［保存］ボタンをクリックします。

17.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

18. 以下の項目を指定します。

- VLAN ID →20



19. ［追加］ボタンをクリックします。

「LAN1 情報」ページが表示されます。

20. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

21. 手順 15.～16. を参考に、以下の項目を設定します。

- IP アドレス →192.168.20.1
- ネットマスク →24（255.255.255.0）

22. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「ether 情報」

- ポートリスト →1-4

「ether 1-4 情報」-「基本情報」

- 通信速度 →1000Mbps
- VLAN
  Tagged →10,20

「ether 1-4 情報」-「ポート種別情報」

- ポート種別 →リンクアグリゲーション

「LAN 情報」

「LAN0 情報」-「共通情報」-「基本情報」

- VLAN ID →10

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス →192.168.10.2
- ネットマスク →24（255.255.255.0）

「LAN 情報」

- VLAN ID →20

「LAN1 情報」-「IP 関連」-「IP アドレス情報」

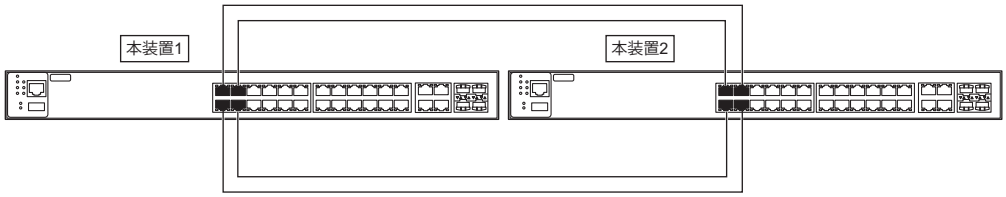
- IP アドレス →192.168.20.2
- ネットマスク →24（255.255.255.0）

☛参照 マニュアル「機能説明書」

2.1 LACP 機能を使う

適用機種　全機種

ここでは、4 ポートの 1000M 回線を LACP を利用したリンクアグリゲーションとする場合の設定方法を説明します。
SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER1 ～ 4 ポートを使用する
- 通信速度を 1000Mbps 固定に変更する
- VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
  VLAN ID：20　　ネットワークアドレス：192.168.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　以下の項目を指定します。

- ポートリスト　　→ 1-4

3.　［修正］ボタンをクリックします。

ether 1-4 情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- 通信速度　　→ 1000Mbps
- VLAN
  Tagged　　→ 10,20

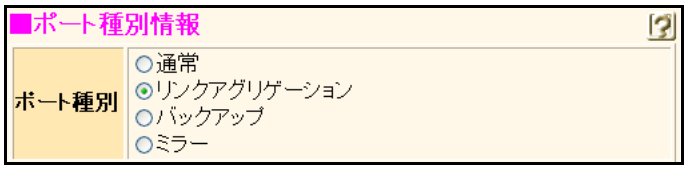
5.　［保存］ボタンをクリックします。

6.　「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

7.　以下の項目を指定します。

- ポート種別　→リンクアグリゲーション



8.　［保存］ボタンをクリックします。

9.　設定メニューの詳細設定で「リンクアグリゲーショングループ情報」をクリックします。

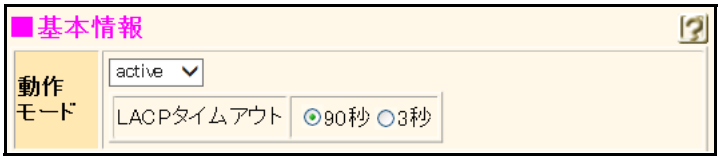
「リンクアグリゲーショングループ情報」ページが表示されます。

10.　「リンクアグリゲーショングループ情報」でリンクアグリゲーショングループ番号が1の［修正］ボタンをクリックします。

リンクアグリゲーショングループ1情報の設定項目と「基本情報」が表示されます。

11.　以下の項目を指定します。

- 動作モード　→active



12.　［保存］ボタンをクリックします。

13.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

14.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

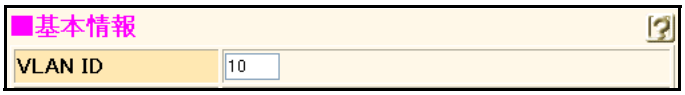
「LAN0情報」ページが表示されます。

15.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

16.　以下の項目を指定します。

- VLAN ID　→10



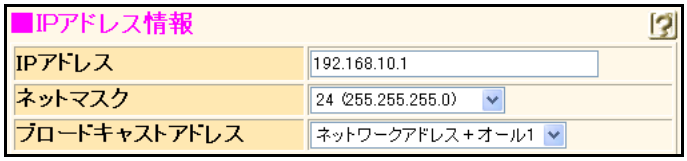
17.　［保存］ボタンをクリックします。

18.　「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

19. 以下の項目を指定します。

- IPアドレス　→192.168.10.1
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



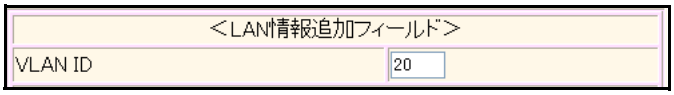
20. ［保存］ボタンをクリックします。

21. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

22. 以下の項目を指定します。

- VLAN ID　→20



23. ［追加］ボタンをクリックします。

「LAN1情報」ページが表示されます。

24. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

25. 手順19.～20.を参考に、以下の項目を設定します。

- IPアドレス　→192.168.20.1
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1

26. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ether情報」

- ポートリスト　→1-4

「ether 1-4情報」-「基本情報」

- 通信速度　→1000Mbps
- VLAN
  Tagged　→10,20

「ether 1-4情報」-「ポート種別情報」

- ポート種別　→リンクアグリゲーション

「リンクアグリゲーショングループ情報」

「リンクアグリゲーショングループ1情報」-「基本情報」

- 動作モード　→active

「LAN情報」

「LAN0情報」-「共通情報」-「基本情報」

- VLAN ID　→10

「LAN0情報」-「IP関連」-「IPアドレス情報」

- IPアドレス　→192.168.10.2
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1

「LAN情報」

- VLAN ID　→20

「LAN1情報」-「IP関連」-「IPアドレス情報」

- IPアドレス　→192.168.20.2
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1

☛ 参照 マニュアル「機能説明書」の「リンクアグリゲーション機能」、「LACP機能」に関する記述

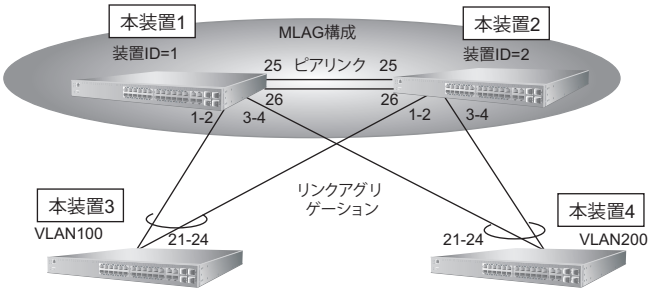
3　MLAG 機能を使う

適用機種　***SR-S332TR1, 352TR1***

ここでは、MLAG 機能を使用する場合の設定方法を説明します。

参照　マニュアル「機能説明書」

SR-S332TR1 の場合を例にします。



● 設定条件

2 台の SR-S332TR1 で MLAG を構成し、配下の SR-S332TR1 と接続する。

- ドメイン ID を 1 とする（初期値）
- 本装置 1 の装置 ID を 1、本装置 2 の装置 ID を 2 とする
- ETHER25、26 ポートをピアリンクポートとして使用する
- 本装置 3 は VLAN100、本装置 4 は VLAN200 を収容する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

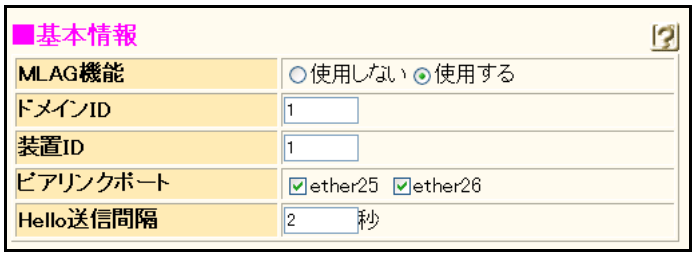
ETHER25、26 ポートをピアリンクポートとし MLAG 機能を設定する

1.　設定メニューの詳細設定で「MLAG 情報」をクリックします。

「MLAG 情報」ページの「基本情報」が表示されます。

2.　以下の項目を指定します。

- MLAG 機能　→使用する
- 装置 ID　→ 1
- ピアリンクポート　→ ether25,26



3. ［保存］ボタンをクリックします。

リンクアグリゲーション（グループ 1）を設定する

4. **設定メニューの詳細設定で「ether 情報」をクリックします。**

「ether 情報」ページが表示されます。

5. **以下の項目を指定します。**

- ポートリスト　→ 1-2

6. ［修正］ボタンをクリックします。

ether 1-2 情報の設定項目と「基本情報」が表示されます。

7. **以下の項目を指定します。**

- VLAN
  Tagged　→ 100

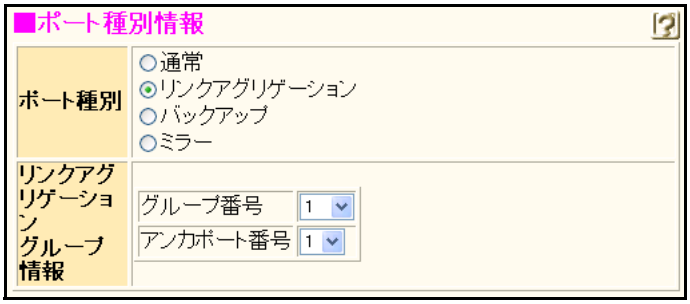
8. ［保存］ボタンをクリックします。

9. **「ポート種別情報」をクリックします。**

「ポート種別情報」が表示されます。

10. **以下の項目を指定します。**

- ポート種別　→リンクアグリゲーション
- リンクアグリゲーショングループ情報
  グループ番号　→ 1
  アンカポート番号　→ 1



11. ［保存］ボタンをクリックします。

リンクアグリゲーション（グループ 2）を設定する

12. **設定メニューの詳細設定で「ether 情報」をクリックします。**

「ether 情報」ページが表示されます。

13. 以下の項目を指定します。

- ポートリスト　→3-4

14. ［修正］ボタンをクリックします。

ether 3-4 情報の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

- VLAN
  Tagged　→200

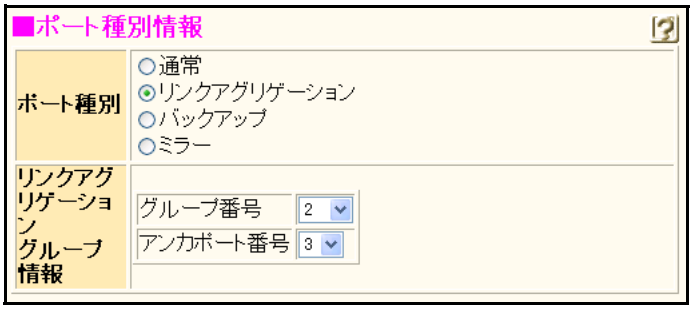
16. ［保存］ボタンをクリックします。

17. 「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

18. 以下の項目を指定します。

- ポート種別　→リンクアグリゲーション
- リンクアグリゲーショングループ情報
  グループ番号　→2
  アンカポート番号　→3



19. ［保存］ボタンをクリックします。

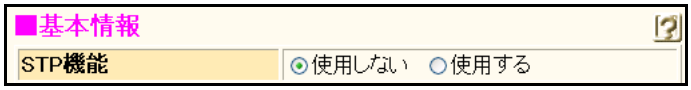
STP 機能を無効にし IP アドレスを設定する

20. 設定メニューの詳細設定で「STP 情報」をクリックします。

STP 情報の設定項目と「基本情報」が表示されます。

21. 以下の項目を指定します。

- STP 機能　→使用しない



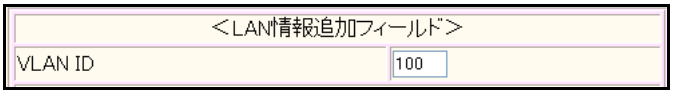
22. ［保存］ボタンをクリックします。

23. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

24. 以下の項目を指定します。

- VLAN ID →100



25. ［追加］ボタンをクリックします。

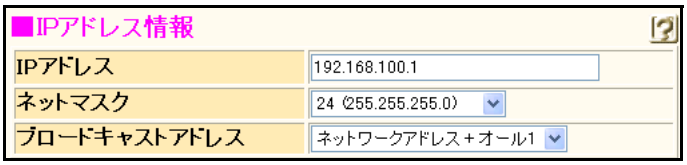
「VLAN0 情報」ページが表示されます。

26. 「IP 関連」をクリックします。

「IP アドレス情報」が表示されます。

27. 以下の項目を指定します。

- IP アドレス →192.168.100.1
- ネットマスク →24



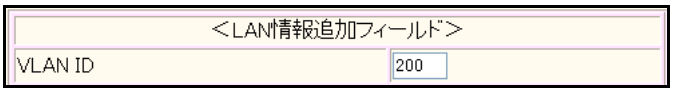
28. ［保存］ボタンをクリックします。

29. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

30. 以下の項目を指定します。

- VLAN ID →200



31. ［追加］ボタンをクリックします。

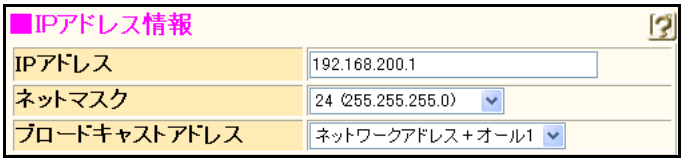
「VLAN1 情報」ページが表示されます。

32. 「IP 関連」をクリックします。

「IP アドレス情報」が表示されます。

33. 以下の項目を指定します。

- IP アドレス →192.168.200.1
- ネットマスク →24



34. ［保存］ボタンをクリックします。

35. 画面左側の［再起動］ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「MLAG情報」

「MLAG情報」-「基本情報」

- MLAG機能　→使用する
- 装置ID　→2
- ピアリンクポート　→ether25,26

「ether情報」

- ポートリスト　→1-2

「ether 1-2情報」-「基本情報」

- VLAN
  Tagged　→100

「ポート種別情報」

- ポート種別　→リンクアグリゲーション
- リンクアグリゲーショングループ情報
  グループ番号　→1
  アンカポート番号　→1

「ether情報」

- ポートリスト　→3-4

「ether 3-4情報」-「基本情報」

- VLAN
  Tagged　→200

「ポート種別情報」

- ポート種別　→リンクアグリゲーション
- リンクアグリゲーショングループ情報
  グループ番号　→2
  アンカポート番号　→3

「STP情報」

「STP情報」-「基本情報」

- STP機能　→使用しない

「LAN情報」-「LAN情報」

- VLAN ID　→100

「VLAN0情報」-「IP関連」-「IPアドレス情報」

- IPアドレス　→192.168.100.2
- ネットマスク　→24

「LAN情報」-「LAN情報」

- VLAN ID　→200

「VLAN1 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス　→ 192.168.200.2
- ネットマスク　→ 24

本装置 3 を設定する

リンクアグリゲーション（グループ 1）を設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　以下の項目を指定します。

- ポートリスト　→ 21-24

3.　［修正］ボタンをクリックします。

ether 21-24 情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- VLAN
  Tagged　→ 100

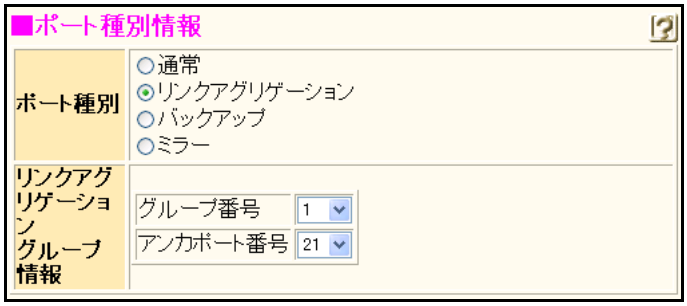
5.　［保存］ボタンをクリックします。

6.　「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

7.　以下の項目を指定します。

- ポート種別　→リンクアグリゲーション
- リンクアグリゲーショングループ情報
  グループ番号　→ 1
  アンカポート番号　→ 21



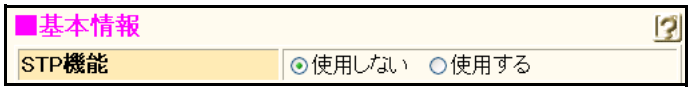
STP 機能を無効にし IP アドレスを設定する

8.　設定メニューの詳細設定で「STP 情報」をクリックします。

STP 情報の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- STP 機能　→使用しない



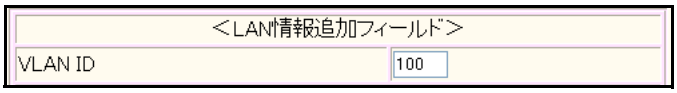
10.　［保存］ボタンをクリックします。

11.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

12.　以下の項目を指定します。

- VLAN ID　→ 100



13.　［追加］ボタンをクリックします。

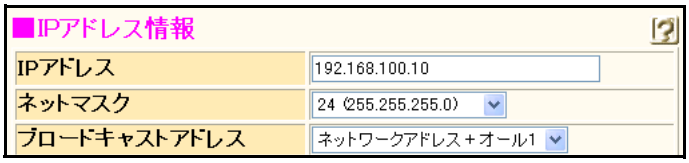
「VLAN0 情報」ページが表示されます。

14.　「IP 関連」をクリックします。

「IP アドレス情報」が表示されます。

15.　以下の項目を指定します。

- IP アドレス　→ 192.168.100.10
- ネットマスク　→ 24



16.　［保存］ボタンをクリックします。

17.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置4を設定する

「本装置3を設定する」を参考に、本装置4を設定します。

「ether情報」

- ポートリスト　→21-24

「ether 1-2情報」-「基本情報」

- VLAN
  Tagged　→200

「ポート種別情報」

- ポート種別　→リンクアグリゲーション
- リンクアグリゲーショングループ情報
  グループ番号　→2
  アンカポート番号　→21

「STP情報」

「STP情報」-「基本情報」

- STP機能　→使用しない

「LAN情報」

- VLAN ID　→200

「VLAN0情報」-「IP関連」-「IPアドレス情報」

- IPアドレス　→192.168.200.10
- ネットマスク　→24

4　バックアップポート機能を使う

適用機種　全機種

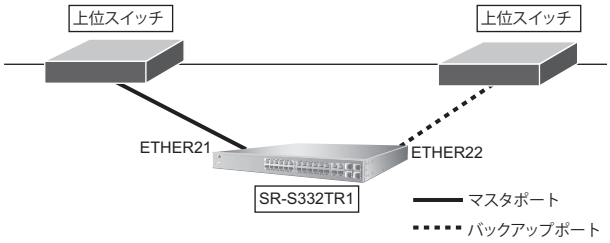
ここでは、アップリンクポートをバックアップポートとして利用する場合の設定方法について説明します。
アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。

こんな事に気をつけて

切替通知フレームを受信する上位スイッチが正しくMACアドレスを再学習するために最適な切替通知フレームの送信条件は、上位スイッチの仕様に依存します。本機能を利用する際は、必ず実機確認を行い最適な送信条件を事前に確認してください。

4.1　マスタポートを優先的に使用する

SR-S332TR1の場合を例にします。



● 設定条件

- ETHER21、22ポートをバックアップポートとして使用する
  （ETHER21をマスタポート、ETHER22をバックアップポートとする）
- マスタポートを優先的に使用する
- 稼動ポート切替発生時に、切替通知フレームをfdb-table（MACアドレス学習テーブルより通知）モードで送信する（100ミリ秒間隔で20フレームずつ、初回送信は500ミリ秒遅延させる）

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHER21ポートをバックアップポート（グループ1）のマスタポートに設定する

1.　設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2.　「ether情報」でポート番号が21の［修正］ボタンをクリックします。

ether21情報の設定項目と「基本情報」が表示されます。

3.　「ポート種別情報」をクリックします。

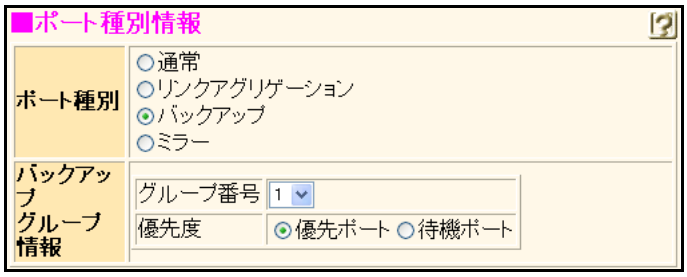
「ポート種別情報」が表示されます。

4.　以下の項目を指定します。

- ポート種別　→バックアップ

“バックアップ”を選択すると、「バックアップグループ情報」の設定項目が表示されます。

- バックアップグループ情報
  優先度　→優先ポート



5.　［保存］ボタンをクリックします。

ETHER22 ポートをバックアップポート（グループ 1）のバックアップポートに設定する

6.　手順 1.～5. を参考に、ETHER22 の以下の項目を設定します。

- ポート種別　→バックアップ

“バックアップ”を選択すると、「バックアップグループ情報」の設定項目が表示されます。

- バックアップグループ情報
  優先度　→待機ポート

7.　設定メニューの詳細設定で「バックアップグループ情報」をクリックします。

「バックアップグループ情報」ページが表示されます。

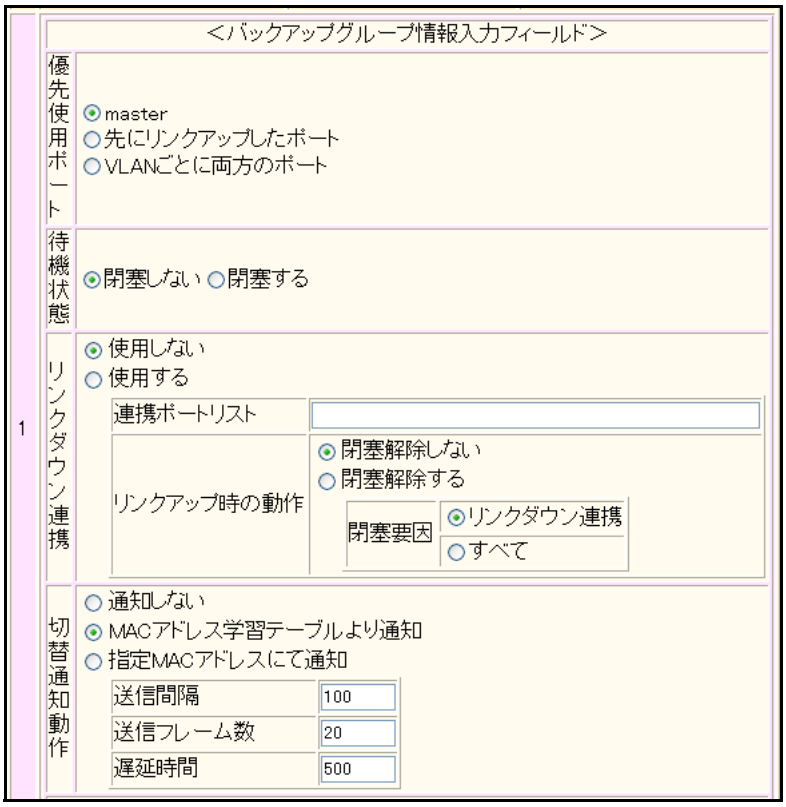
バックアップグループ 1 をマスタポート優先モードにし、切替通知動作を設定する

8.　「バックアップグループ情報」でグループ番号が 1 の［修正］ボタンをクリックします。

グループ番号 1 の「バックアップグループ情報入力フィールド」が表示されます。

9. 以下の項目を指定します。

- 優先使用ポート　→master
  切替通知動作　→MACアドレス学習テーブルより通知
  送信間隔　→100ミリ秒
  送信フレーム数　→20
  遅延時間　→500ミリ秒



10. ［保存］ボタンをクリックします。

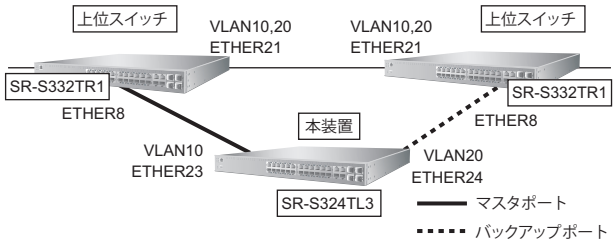
11. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

4.2 VLANごとに両方のポートを同時に使用する

ここでは、バックアップポートをVLANごとに両方のポートを同時に稼動させる場合の設定方法を説明します。本設定では、マスタポートとバックアップポートがVLANごとに同時に稼動するため通信帯域を有効に利用できます。どちらかのポートがリンクダウンした場合は、残された稼動ポートがもう一方のポートのVLANも動的にバックアップします。

上位スイッチをSR-S332TR1とし、SR-S324TL3をバックアップポートで接続する例とします。



こんな事に気をつけて

- **Vlan-based モード設定では STP 機能と同時に使用できません。**
- **上位スイッチの本装置接続ポートには、マスタポートとバックアップポート両方のタグVLANを設定する必要があります。**

● 設定条件

2台のSR-S332TR1を上位スイッチとしてSR-S324TL3を接続する。

[本装置]

- ETHER23、24ポートをバックアップポートとして使用する
  （ETHER23をマスタポート、ETHER24をバックアップポートとする）
- VLANごとに両方のポートを使用する
  （マスタポートでVLAN10、バックアップポートでVLAN20を優先使用する）
- 切替通知フレームをMAC-flushモード（指定MACアドレスにて通知）で送信する
  切替通知送信条件　：100ミリ秒間隔で10フレームずつ、初回送信は500ミリ秒遅延させる
  切替通知フレームの送信元MACアドレス
  　　：00:aa:aa:aa:aa:aa

[上位スイッチ]

- MACテーブルフラッシュ機能を使用する
  監視MACアドレス　：00:aa:aa:aa:aa:aa
  学習テーブルの初期化　：VLANごとに初期化する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

ETHER23 ポートをバックアップポート（グループ 3）のマスタポート（VLAN10 を優先動作）に設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 23 の［修正］ボタンをクリックします。

ether23 情報の設定項目と「基本情報」が表示されます。

3.　以下の項目を設定します。

- VLAN
  Tagged　→ 10

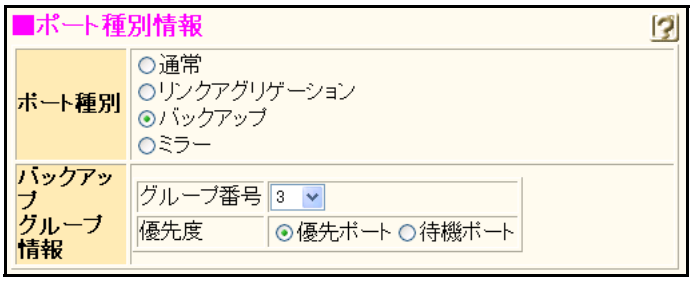
4.　［保存］ボタンをクリックします。

5.　「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

6.　以下の項目を設定します。

- ポート種別　→バックアップ
- バックアップグループ情報
  グループ番号　→ 3
  優先度　→優先ポート



7.　［保存］ボタンをクリックします。

ETHER24 ポートをバックアップポート（グループ 3）のマスタポート（VLAN20 を優先動作）に設定する

8.　手順 1.～7 を参考に、ETHER24 ポートの以下の項目を設定します。

「ether 情報」

「ether 24 情報」-「基本情報」

- VLAN
  Tagged　→ 20

「ether 24 情報」-「ポート種別」

- ポート種別　→バックアップ

- バックアップグループ情報
  グループ番号　→3
  優先度　→待機ポート

バックアップグループ3をVLANごとに両方のポートを使用するモードにし、バックアップポートの切替通知動作を設定する

9.　設定メニューの詳細設定で「バックアップグループ情報」をクリックします。

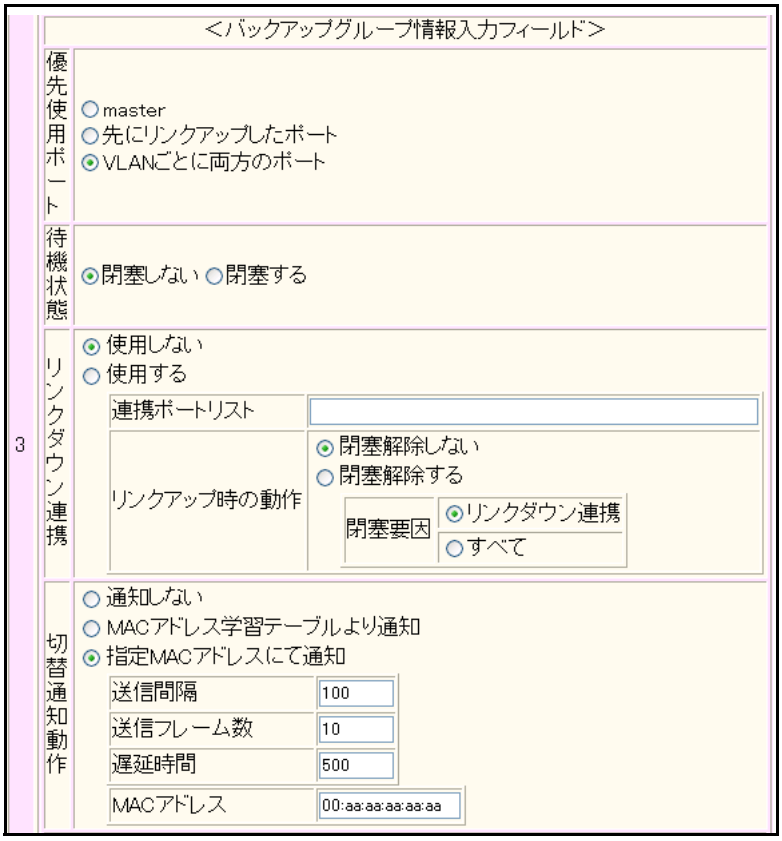
バックアップグループ情報の設定項目と、「バックアップグループ情報」が表示されます。

10.　グループ番号3の［修正］ボタンをクリックします。

グループ番号3の「バックアップグループ情報入力フィールド」が表示されます。

11.　以下の項目を設定します。

- 優先使用ポート　→VLANごとに両方のポート
- 切替通知動作　→指定MACアドレスにて通知
  送信間隔　→100ミリ秒
  送信フレーム数　→10
  遅延時間　→500ミリ秒
  MACアドレス　→00:aa:aa:aa:aa:aa



12.　［保存］ボタンをクリックします。

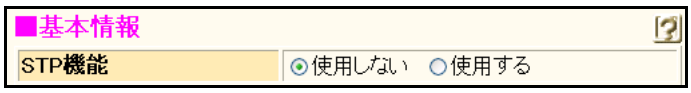
STP機能を無効にする

13.　設定メニューの詳細設定で「STP情報」をクリックします。

STP情報の設定項目と「基本情報」が表示されます。

14. 以下の項目を指定します。

- STP 機能　→使用しない



15. ［保存］ボタンをクリックします。

16. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

上位スイッチを設定する

ETHER ポートの VLAN を設定する

17. 手順 1. から手順 4. を参考に、ETHER8 と ETHER21 ポートの以下の項目を設定します。

- VLAN
  Tagged　→ 10,20

STP 機能を無効にする

18. 手順 13. から手順 15. を参考に、STP 機能を無効にします。

MAC テーブルフラッシュ機能を設定する

19. 設定メニューの詳細設定で「MAC 情報」をクリックします。

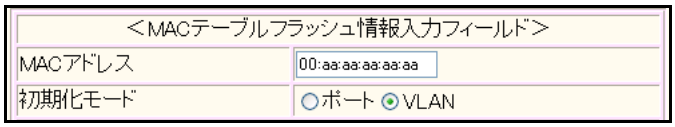
「MAC 情報」ページが表示されます。

20. 「MAC テーブルフラッシュ情報」をクリックします。

「MAC テーブルフラッシュ情報」が表示されます。

21. 以下の項目を設定します。

- MAC アドレス　：00:aa:aa:aa:aa:aa
- 初期化モード　：VLAN



22. ［追加］ボタンをクリックします。

23. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

5　MAC フィルタリング機能を使う

適用機種　全機種

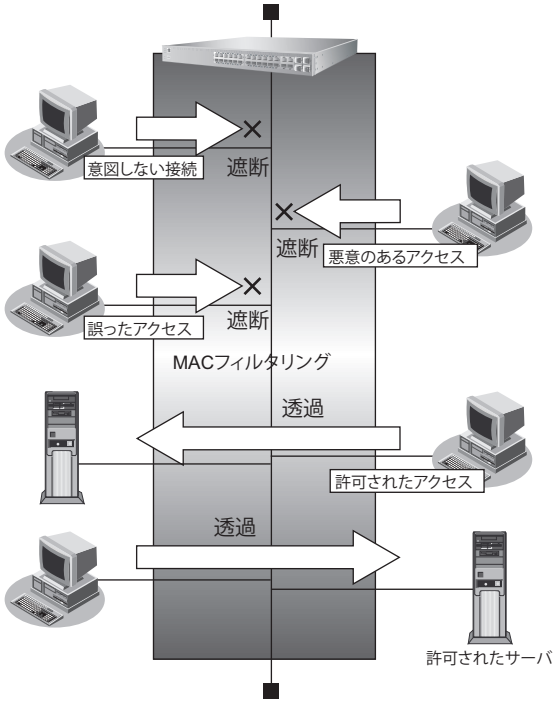
本装置を経由するパケットを、MAC アドレス、パケット形式、ETHERNET タイプ、VLAN ID、COS 値などの組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、ネットワークへの負荷を軽減することができます。

☛ 参照　マニュアル「機能説明書」

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。
MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ /QoS 資源の配分」の機能を " フィルタのみ "、プロトコルを "IPv4 のみ " に設定する必要があります。

- **MAC フィルタ機能 (IPv4)** ／ **IP フィルタリング機能 (IPv4)**
- **MAC フィルタ機能 (IPv6 フィルタ)** ／ **IP フィルタリング機能 (IPv6)**
- **優先制御情報書き換え機能 (IPv4)** ／ **DSCP 値書き換え機能 (IPv4)**
- **優先制御情報書き換え機能 (IPv6)** ／ **DSCP 値書き換え機能 (IPv6)**



フィルタリング条件

以下の条件を指定することによって、パケットデータの流れを制御できます。

- ACL の MAC 定義および VLAN 定義で指定した以下の情報
  - 送信元 MAC 情報（MAC アドレス／パケット形式／ ETHERNET タイプ／ LSAP）
  - あて先 MAC 情報（MAC アドレス／パケット形式／ ETHERNET タイプ／ LSAP）
  - VLAN ID
  - COS 値

  - 送信元IP情報（IPアドレス／アドレスマスク）
  - あて先IP情報（IPアドレス／アドレスマスク）
  - プロトコル
  - TCP・UDPのポート番号
  - ICMP TYPE、ICMP CODE
  - IPパケットのTOS値、DSCP値
- フィルタ処理の対象となるパケット入力ETHERポート
- フィルタ処理の対象となるパケットが入力ETHERポートに入力された場合の動作（遮断または透過）

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 特定の条件のパケットだけを透過させ、その他はすべて遮断する

B. 特定の条件のパケットだけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定MACアドレスからのパケットだけを許可する
- 特定MACアドレスへのパケットだけを許可する

また、設計方針Bの例として、以下の設定例について説明します。

- 特定パケット形式のパケットだけを禁止する

5.1 特定MACアドレスからのパケットだけを許可する

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストからの入力パケットだけを許可し、その他のホストからの入力パケットを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。
MACフィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS資源の配分」の機能を"フィルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- **MACフィルタ機能**(IPv4)／IP **フィルタリング機能**(IPv4)
- **MACフィルタ機能**(IPv6 **フィルタ**)／IP **フィルタリング機能**(IPv6)
- **優先制御情報書き換え機能**(IPv4)／DSCP **値書き換え機能**(IPv4)
- **優先制御情報書き換え機能**(IPv6)／DSCP **値書き換え機能**(IPv6)

● フィルタリング設計

- VLAN 10はETHER1～8ポートで構成されるポートVLANで、それぞれのポートでタグなしである
- VLAN 20はETHER1～4ポートおよびETHER9～12ポートで構成されるポートVLANで、ETHER1～4ポートでタグ付き、ETHER9～12ポートでタグなしである
- ETHER2ポートのVLAN 10ではMACアドレス00:0b:01:02:03:04のホストからの入力パケットだけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

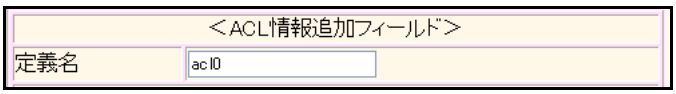
（1）VLAN IDが10で送信元MACアドレスが00:0b:01:02:03:04であるパケットの形式をACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →acl0



3. ［追加］ボタンをクリックします。

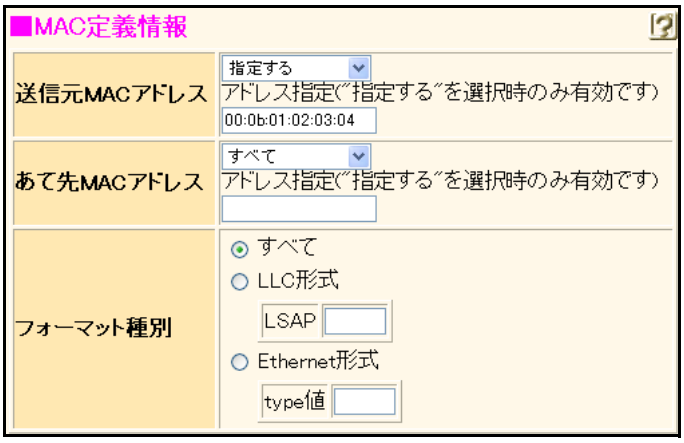
「ACL定義情報（acl0）」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元MACアドレス　→指定する
  アドレス指定　→00:0b:01:02:03:04
- あて先MACアドレス　→すべて
- フォーマット種別　→すべて



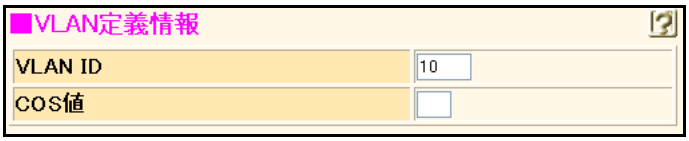
6.　［保存］ボタンをクリックします。

7.　「VLAN定義情報」をクリックします。

「VLAN定義情報」が表示されます。

8.　以下の項目を指定します。

- VLAN ID　→10
- COS値　→指定しない



9.　［保存］ボタンをクリックします。

（2）VLAN IDが10のすべてのパケットの形式をACLで設定する

10.　手順1. ～ 3.および手順7. ～ 9.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名　→acl1

「ACL定義情報（acl1）」-「VLAN定義情報」

- VLAN ID　→10
- COS値　→指定しない

（3）ETHER2 ポートで（1）で設定した形式のパケットを透過させる

11. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

12. 「ether 情報」でポート番号が 2 の［修正］ボタンをクリックします。

ether 2 情報の設定項目と「基本情報」が表示されます。

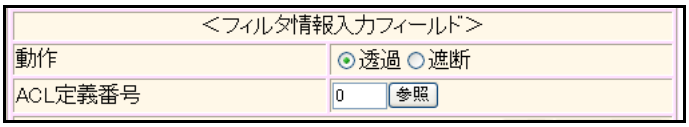
13. 「フィルタ情報」をクリックします。

「フィルタ情報」が表示されます。

14. 以下の項目を指定します。

- 動作　→透過
- ACL 定義番号　→ 0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15. ［追加］ボタンをクリックします。

（4）ETHER2 ポートで（2）で設定した形式のパケットを遮断する

16. 手順 14. ～ 15 を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL 定義番号　→ 1

17. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

5.2 特定MACアドレスへのパケットだけを許可する

適用機種 全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストへの送信パケットだけを許可し、その他のホストへの送信パケットを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。
MACフィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS資源の配分」の機能を"フィルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- **MACフィルタ機能**(IPv4)／IP **フィルタリング機能**(IPv4)
- **MACフィルタ機能**(IPv6 **フィルタ**)／IP **フィルタリング機能**(IPv6)
- **優先制御情報書き換え機能**(IPv4)／DSCP **値書き換え機能**(IPv4)
- **優先制御情報書き換え機能**(IPv6)／DSCP **値書き換え機能**(IPv6)

● フィルタリング設計

- VLAN 10はETHER1～8ポートで構成されるポートVLANで、それぞれのポートでタグなしである
- VLAN 20はETHER1～4ポートおよびETHER9～12ポートで構成されるポートVLANで、ETHER1～4ポートでタグ付き、ETHER9～12ポートでタグなしである
- ETHER4～8ポートのVLAN 10ではMACアドレス00:0b:01:02:03:04のホストへの送信パケットだけを許可し、その他はすべて禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

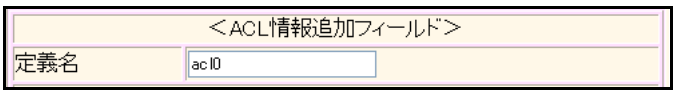
（1）VLAN IDが10であて先MACアドレスが00:0b:01:02:03:04であるパケットの形式をACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →acl0



3. ［追加］ボタンをクリックします。

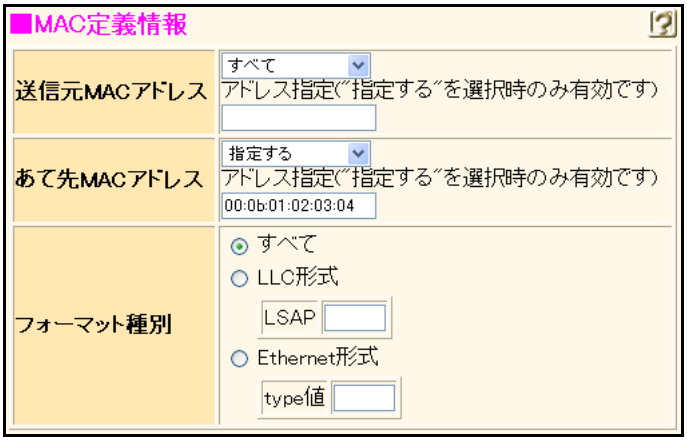
「ACL定義情報（acl0）」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元MACアドレス　→すべて
- あて先MACアドレス　→指定する
  アドレス指定　→00:0b:01:02:03:04
- フォーマット種別　→すべて



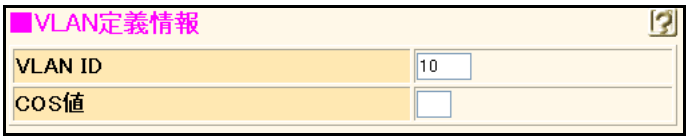
6.　［保存］ボタンをクリックします。

7.　「VLAN 定義情報」をクリックします。

「VLAN 定義情報」が表示されます。

8.　以下の項目を指定します。

- VLAN ID　→10
- COS 値　→指定しない



9.　［保存］ボタンをクリックします。

（2）VLAN ID が 10 のすべてのパケットの形式を ACL で設定する

10.　手順 1. ～ 3. および手順 7. ～ 9. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→acl1

「ACL 定義情報（acl1）」-「VLAN 定義情報」

- VLAN ID　→10
- COS 値　→指定しない

（3）ETHER4 ～ 8 ポートで（1）で設定した形式のパケットを透過させる

11. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

12. 以下の項目を指定します。

- ポートリスト　→4-8

13. ［修正］ボタンをクリックします。

ether 4-8 情報の設定項目と「基本情報」が表示されます。

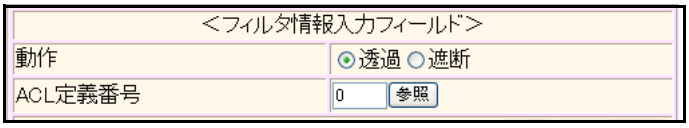
14. 「フィルタ情報」をクリックします。

「フィルタ情報」が表示されます。

15. 以下の項目を指定します。

- 動作　→透過
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



16. ［追加］ボタンをクリックします。

（4）ETHER4 ～ 8 ポートで（2）で設定した形式のパケットを遮断する

17. 手順 15. ～ 16. を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL 定義番号　→1

18. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

5.3 特定パケット形式のパケットだけを禁止する

適用機種 全機種

ここでは、VLAN 内の特定ポートで特定のパケット形式を持つ入力パケットだけを禁止し、その他の入力パケットを許可する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。
MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ /QoS 資源の配分」の機能を "フィルタのみ"、プロトコルを "IPv4 のみ" に設定する必要があります。

- **MAC フィルタ機能** (IPv4) ／ IP **フィルタリング機能** (IPv4)
- MAC **フィルタ機能** (IPv6 **フィルタ**) ／ IP **フィルタリング機能** (IPv6)
- **優先制御情報書き換え機能** (IPv4) ／ DSCP **値書き換え機能** (IPv4)
- **優先制御情報書き換え機能** (IPv6) ／ DSCP **値書き換え機能** (IPv6)

● フィルタリング設計

- VLAN 10 は ETHER1 ～ 8 ポートで構成されるポート VLAN で、それぞれのポートでタグなしである
- VLAN 20 は ETHER1 ～ 4 ポートおよび ETHER9 ～ 12 ポートで構成されるポート VLAN で、ETHER1 ～ 4 ポートでタグ付き、ETHER9 ～ 12 ポートでタグなしである
- ETHER1 ～ 4 ポートでは IP プロトコルの入力パケットだけを禁止し、その他はすべて許可する

上記のフィルタリング設計に従って設定を行う場合の設定例を SR-S332TR1 を例にして示します。

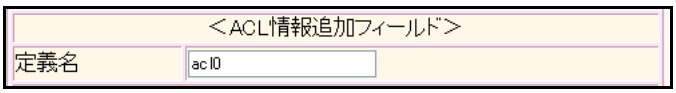
（1）IP プロトコルのパケット（IP, ARP, Reverse ARP）の形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →acl0



3. [追加] ボタンをクリックします。

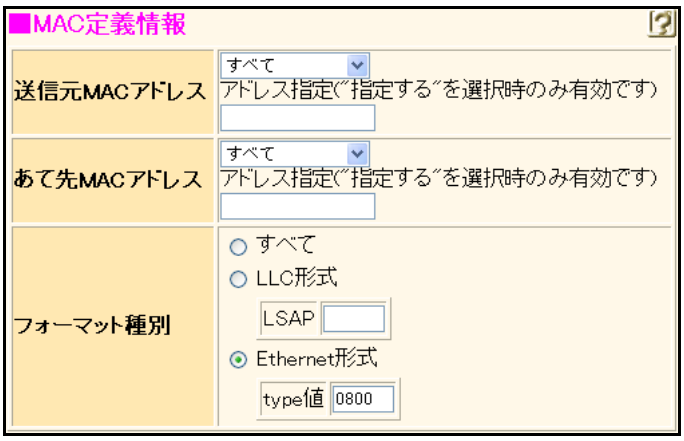
「ACL 定義情報（acl0）」ページが表示されます。

4. 「MAC 定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5. 以下の項目を指定します。

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →Ethernet 形式
  type 値 →0800



6. **［保存］ボタンをクリックします。**

7. **手順 1.～6. を参考に、以下の項目を設定します。**

「ACL 情報」

- 定義名 →acl1

「ACL 定義情報（acl1）」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →Ethernet 形式
  type 値 →0806

「ACL 情報」

- 定義名 →acl2

「ACL 定義情報（acl2）」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →Ethernet 形式
  type 値 →8035

（2）ETHER1～4 ポートで（1）で作成したパケットのパターンを遮断する

8. **設定メニューの詳細設定で「ether 情報」をクリックします。**

「ether 情報」ページが表示されます。

9. **以下の項目を指定します。**

- ポートリスト →1-4

10. **［修正］ボタンをクリックします。**

ether 1-4 情報の設定項目と「基本情報」が表示されます。

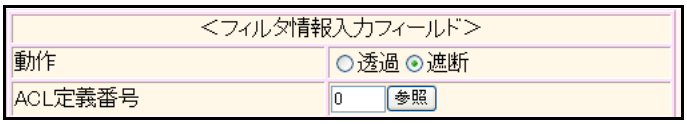
11. **「フィルタ情報」をクリックします。**

「フィルタ情報」が表示されます。

12. **以下の項目を指定します。**

- 動作　→遮断
- ACL 定義番号　→0

補足「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



13.　［追加］ボタンをクリックします。

14.　手順 12.～13. を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL 定義番号　→1

15.　手順 12.～13. を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL 定義番号　→2

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

5.4 VLAN単位で特定MACアドレス間の通信だけを遮断する

適用機種 全機種

ここでは、VLAN内のポートで特定のMACアドレスを持つホスト間の通信だけを遮断する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。
MACフィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS資源の配分」の機能を"フィルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- **MACフィルタ機能**(IPv4)／ IP **フィルタリング機能**(IPv4)
- **MACフィルタ機能**(IPv6 **フィルタ**)／ IP **フィルタリング機能**(IPv6)
- **優先制御情報書き換え機能**(IPv4)／DSCP **値書き換え機能**(IPv4)
- **優先制御情報書き換え機能**(IPv6)／DSCP **値書き換え機能**(IPv6)

● フィルタリング設計

- VLAN10はETHER1～4ポートでタグなし、ETHER5～8ポートでタグ付きで構成されるポートVLANである
- VLAN20はETHER1～4ポートでタグ付き、ETHER5～8ポートでタグなしで構成されるポートVLANである
- VLAN10ではMACアドレス00:0b:01:02:03:04のホストからMACアドレス00:0b:11:12:13:14間のTCP通信だけを禁止し、VLAN 20ではMACアドレス00:0b:21:22:23:24のホストからMACアドレス00:0b:31:32:33:34間のUDP通信だけを禁止する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

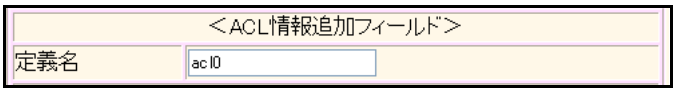
(1) 送信元MACアドレスが00:0b:01:02:03:04、あて先MACアドレスが00:0b:11:12:13:14であるTCPパケットの形式をACLで設定する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →acl0



3. [追加] ボタンをクリックします。

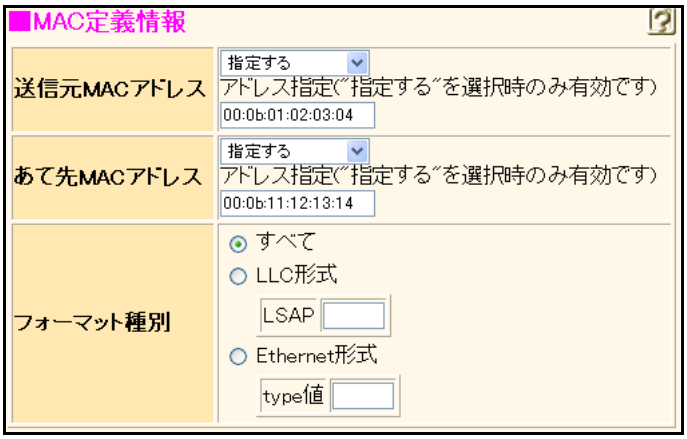
「ACL定義情報（acl0）」ページが表示されます。

4. 「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元MACアドレス　→指定する
  アドレス指定　→00:0b:01:02:03:04
- あて先MACアドレス　→指定する
  アドレス指定　→00:0b:11:12:13:14
- フォーマット種別　→すべて



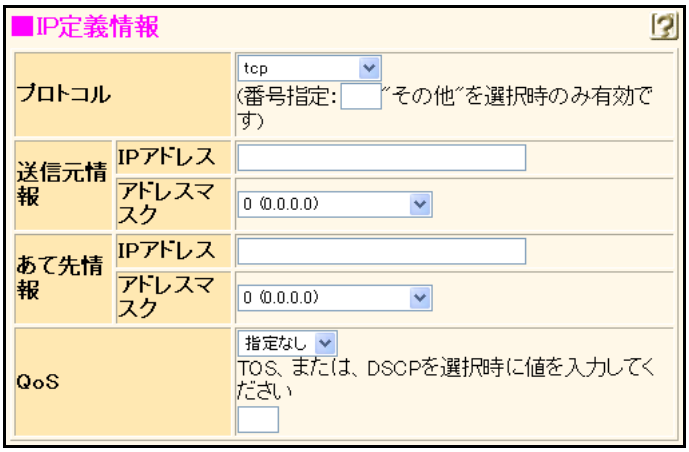
6.　［保存］ボタンをクリックします。

7.　「IP定義情報」をクリックします。

「IP定義情報」が表示されます。

8.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし



9.　［保存］ボタンをクリックします。

（2）送信元MACアドレスが00:0b:11:12:13:14、あて先MACアドレスが00:0b:01:02:03:04であるTCPパケットの形式をACLで設定する

10. **手順1.～9.を参考に、以下の項目を設定します。**

「ACL情報」

- 定義名 →acl1

「ACL定義情報（acl1）」-「MAC定義情報」

- 送信元MACアドレス →指定する
  アドレス指定 →00:0b:11:12:13:14
- あて先MACアドレス →指定する
  アドレス指定 →00:0b:01:02:03:04
- フォーマット種別 →すべて

「ACL定義情報（acl1）」-「IP定義情報」

- プロトコル →tcp
- 送信元情報
  IPアドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- あて先情報
  IPアドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- QoS →指定なし

（3）送信元MACアドレスが00:0b:21:22:23:24、あて先MACアドレスが00:0b:31:32:33:34であるUDPパケットの形式をACLで設定する

11. **手順1.～9.を参考に、以下の項目を設定します。**

「ACL情報」

- 定義名 →acl2

「ACL定義情報（acl2）」-「MAC定義情報」

- 送信元MACアドレス →指定する
  アドレス指定 →00:0b:21:22:23:24
- あて先MACアドレス →指定する
  アドレス指定 →00:0b:31:32:33:34
- フォーマット種別 →すべて

「ACL定義情報（acl2）」-「IP定義情報」

- プロトコル →udp
- 送信元情報
  IPアドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- あて先情報
  IPアドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- QoS →指定なし

（4）送信元MACアドレスが00:0b:31:32:33:34、あて先MACアドレスが00:0b:21:22:23:24であるUDPパケットの形式をACLで設定する

12.　手順1.～9.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名　→acl3

「ACL定義情報（acl3）」-「MAC定義情報」

- 送信元MACアドレス　→指定する
  アドレス指定　→00:0b:31:32:33:34
- あて先MACアドレス　→指定する
  アドレス指定　→00:0b:21:22:23:24
- フォーマット種別　→すべて

「ACL定義情報（acl3）」-「IP定義情報」

- プロトコル　→udp
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

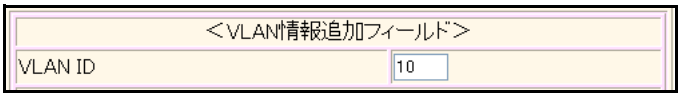
（5）VLAN10で（1）、（2）で設定した形式のパケットを遮断する

13.　設定メニューの詳細設定で「VLAN情報」をクリックします。

「VLAN情報」ページが表示されます。

14.　以下の項目を指定します。

- VLAN ID　→10



15.　［追加］ボタンをクリックします。

「VLAN10情報」ページが表示されます。

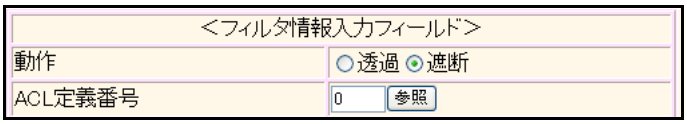
16.　「フィルタ情報」をクリックします。

「フィルタ情報」が表示されます。

17. 以下の項目を指定します。

- 動作 →遮断
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



18. ［追加］ボタンをクリックします。

19. 手順 17.～18. を参考に、以下の項目を設定します。

- 動作 →遮断
- ACL 定義番号 →1

（6）VLAN20 で（3）、（4）で設定した形式のパケットを遮断する

20. 手順 13.～18. を参考に、以下の項目を設定します。

「VLAN 情報」

- VLAN ID →20

「VLAN20 情報」-「フィルタ情報」

- 動作 →遮断
- ACL 定義番号 →2

21. 手順 17.～18. を参考に、以下の項目を設定します。

- 動作 →遮断
- ACL 定義番号 →3

22. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

5.5 VLAN 単位で特定パケット形式のパケットだけを許可する

適用機種 全機種

ここでは、VLAN 内のポートで特定のパケット形式を持つ入力パケットだけを許可し、その他の入力パケットを遮断する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、以下の機能を同時に使用することができません。
MAC フィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ /QoS 資源の配分」の機能を "フィルタのみ"、プロトコルを "IPv4 のみ" に設定する必要があります。

- **MAC フィルタ機能 (IPv4) ／ IP フィルタリング機能 (IPv4)**
- **MAC フィルタ機能 (IPv6 フィルタ) ／ IP フィルタリング機能 (IPv6)**
- **優先制御情報書き換え機能 (IPv4) ／ DSCP 値書き換え機能 (IPv4)**
- **優先制御情報書き換え機能 (IPv6) ／ DSCP 値書き換え機能 (IPv6)**

● フィルタリング設計

- VLAN10 は ETHER1 ～ 4 ポートでタグなし、ETHER5 ～ 8 ポートでタグ付きで構成されるポート VLAN である
- VLAN20 は ETHER1 ～ 4 ポートでタグ付き、ETHER5 ～ 8 ポートでタグなしで構成されるポート VLAN である
- VLAN10 では IP プロトコルの入力パケットだけを許可する
- VLAN 20 では FNA プロトコルの入力パケットだけを許可する

上記のフィルタリング設計に従って設定を行う場合の設定例を示します。

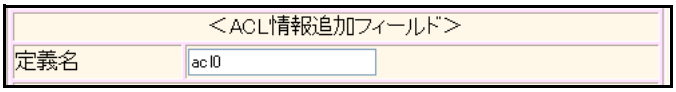
（1）IP プロトコルのパケット（IP, ARP, Reverse ARP）の形式を ACL で設定する

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →acl0



3. [追加] ボタンをクリックします。

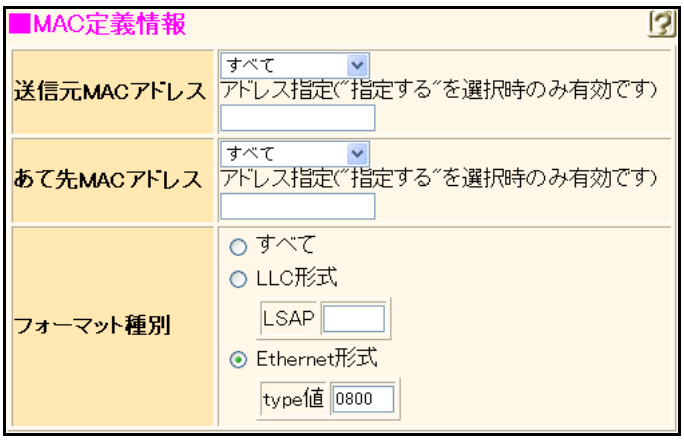
「ACL 定義情報（acl0）」ページが表示されます。

4. 「MAC 定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5. 以下の項目を指定します。

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →Ethernet 形式
  type 値 →0800



6. **［保存］ボタンをクリックします。**

7. **手順 1.～6. を参考に、以下の項目を設定します。**

「ACL 情報」

- 定義名 →acl1

「ACL 定義情報（acl1）」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →Ethernet 形式
  type 値 →0806

「ACL 情報」

- 定義名 →acl2

「ACL 定義情報（acl2）」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →Ethernet 形式
  type 値 →8035

（2）FNA プロトコルのパケットの形式を ACL で設定する

8. **手順 1.～6. を参考に、以下の項目を設定します。**

「ACL 情報」

- 定義名 →acl3

「ACL 定義情報（acl3）」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて
- あて先 MAC アドレス →すべて
- フォーマット種別 →LLC 形式
  LSAP →8080

「ACL 情報」

- 定義名 →acl4

「ACL 定義情報（acl4）」-「MAC 定義情報」

- 送信元 MAC アドレス →すべて

- あて先MACアドレス　→すべて
- フォーマット種別　→LLC形式
  LSAP　→0000

「ACL情報」

- 定義名　→acl5

「ACL定義情報（acl5）」-「MAC定義情報」

- 送信元MACアドレス　→すべて
- あて先MACアドレス　→すべて
- フォーマット種別　→LLC形式
  LSAP　→0001

（3）全プロトコルのパケットの形式をACLで設定する

9.　手順1. ～ 6 を参考に、以下の項目を設定します。

「ACL情報」

- 定義名　→acl6

「ACL定義情報（acl6）」-「MAC定義情報」

- 送信元MACアドレス　→すべて
- あて先MACアドレス　→すべて
- フォーマット種別　→すべて

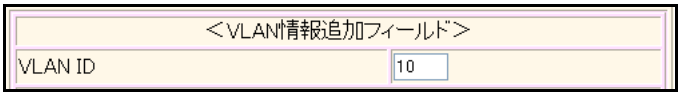
（4）VLAN10で（1）で作成したパケットのパターン以外を遮断する

10.　設定メニューの詳細設定で「VLAN情報」をクリックします。

「VLAN情報」ページが表示されます。

11.　以下の項目を指定します。

- VLAN ID　→10



12.　［追加］ボタンをクリックします。

「VLAN10情報」ページが表示されます。

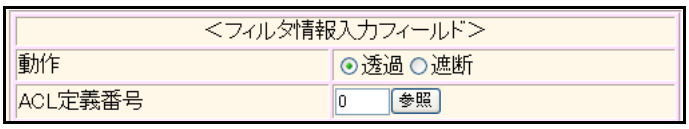
13.　「フィルタ情報」をクリックします。

「フィルタ情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→透過
- ACL定義番号　→0

補足　「ACL定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15. **［追加］ボタンをクリックします。**

16. **手順 14.～15. を参考に、以下の項目を設定します。**

- 動作 →透過
- ACL 定義番号 →1

17. **手順 14.～15. を参考に、以下の項目を設定します。**

- 動作 →透過
- ACL 定義番号 →2

18. **手順 14.～15. を参考に、以下の項目を設定します。**

- 動作 →遮断
- ACL 定義番号 →6

（5）VLAN20 で（2）で作成したパケットのパターン以外を遮断する

19. **手順 10.～15. を参考に、以下の項目を設定します。**

「VLAN 情報」

- VLAN ID →20

「VLAN20 情報」-「フィルタ情報」

- 動作 →透過
- ACL 定義番号 →3

20. **手順 14.～15. を参考に、以下の項目を設定します。**

- 動作 →透過
- ACL 定義番号 →4

21. **手順 14.～15. を参考に、以下の項目を設定します。**

- 動作 →透過
- ACL 定義番号 →5

22. **手順 14.～15. を参考に、以下の項目を設定します。**

- 動作 →遮断
- ACL 定義番号 →6

23. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

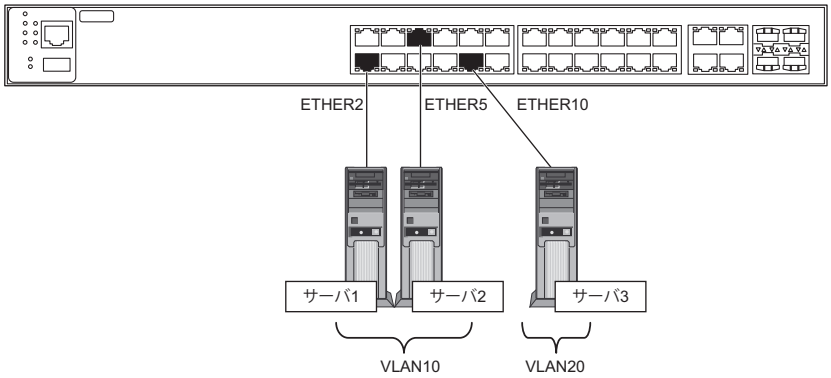
6　スタティックMACフォワーディング機能を使う

適用機種　全機種

スタティックMACフォワーディング機能を利用すると、構成定義によって、MACアドレスをスタティックにFDBに登録することができ、フラッディングによる余分なフレームがネットワーク上を流れることを防止できます。

ここでは、各ETHERポートに接続されるサーバのMACアドレスをスタティックエントリとして設定する方法を説明します。

SR-S332TR1の場合を例にします。



● 設定条件

- ETHER2、5ポートにサーバ1、2を接続し、VLANを10とする
- ETHER10ポートにサーバ3を接続し、VLANを20とする
- サーバ1のMACアドレス　：00:00:00:00:00:11
- サーバ2のMACアドレス　：00:00:00:00:00:22
- サーバ3のMACアドレス　：00:00:00:00:00:33

上記の設定条件に従って設定を行う場合の設定例を示します。

ETHERポートにVLANを設定する

1.　設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2.　「ether情報」でポート番号が2の［修正］ボタンをクリックします。

ether 2情報の設定項目と「基本情報」が表示されます。

3.　以下の項目を指定します。

- VLAN
  Untagged　→10

VLAN	Tagged	
	Untagged	10

4.　［保存］ボタンをクリックします。

5.　手順 1.～4. を参考に、以下の項目を設定します。

［ether 5］

- VLAN
  Untagged　→ 10

［ether 10］

- VLAN
  Untagged　→ 20

VLAN にスタティック MAC フォワーディングを設定する

6.　設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN 情報」ページが表示されます。

7.　以下の項目を指定します。

- VLAN ID　→ 10

＜VLAN情報追加フィールド＞	
VLAN ID	10

8.　［追加］ボタンをクリックします。

「VLAN10 情報」ページが表示されます。

9.　「静的 MAC 学習テーブル情報」をクリックします。

「静的 MAC 学習テーブル情報」が表示されます。

10.　以下の項目を指定します。

- MAC アドレス　→ 00:00:00:00:00:11
- ポート番号　→ 2

＜静的MAC学習テーブル情報入力フィールド＞	
MACアドレス	00:00:00:00:00:11
ポート番号	2

11.　［追加］ボタンをクリックします。

12.　静的 MAC 学習テーブルが追加されたことを確認し、画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

13. 手順6.～12.を参考に、以下の項目を設定します。

［サーバ2］

「VLAN情報」

- VLAN ID →10

「VLAN10情報」-「静的MAC学習テーブル情報」

- MACアドレス →00:00:00:00:00:22
- ポート番号 →5

［サーバ3］

「VLAN情報」

- VLAN ID →20

「VLAN20情報」-「静的MAC学習テーブル情報」

- MACアドレス →00:00:00:00:00:33
- ポート番号 →10

14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

7 QoS 機能を使う

適用機種 全機種

参照 マニュアル「機能説明書」

7.1 優先制御機能を使う

適用機種 全機種

本装置では、VLAN 機能のユーザプライオリティ値に出力ポート（自装置あてポート含む）の複数の優先度の異なるキューを対応付けることで、パケットの優先制御を行うことができます。

こんな事に気をつけて

- **本装置の初期設定は、マニュアル「機能説明書」を参照してください。**
- **SR-S312LE1/320LE1/324LE1 の場合のキューは 4 個、SR-S332TR1/352TR1/732TR1/752TR1 の場合のキューは 8 個となります。**

SR-S312LE1/320LE1/324LE1 の場合

● 優先制御設計

パケットのタイプ	CoS 値	装置内部のキュークラス
管理パケット	7	3
	6	
音声	5	
FAX／呼制御	4	2
映像	3	
	2	1
その他	1	
	0	0

上記の優先制御設計に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「QoS 情報」をクリックします。

「QoS 情報」ページが表示されます。

2. 「COS キュー情報」をクリックします。

「COS キュー情報」が表示されます。

3.　以下の項目を指定します。

- パケットのCOS値

  0→0

  1→1

  2→1

  3→2

  4→2

  5→3

  6→3

  7→3

4.　［保存］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

SR-S332TR1/352TR1/732TR1/752TR1 の場合

パケットのタイプ	CoS値	装置内部のキュークラス
管理パケット	7	4
	6	
音声	5	3
FAX／呼制御	4	2
映像	3	1
	2	
その他	1	0
	0	

上記の優先制御設定に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「QoS情報」をクリックします。

「QoS情報」ページが表示されます。

2.　「COSキュー情報」をクリックします。

「COSキュー情報」が表示されます。

3.　以下の項目を指定します。

- パケットのCOS値

  0→0

  1→0

  2→1

  3→1

  4→2

  5→3

  6→4

  7→4

4.　［保存］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

7.2 優先制御情報書き換え機能を使う

適用機種 全機種

本装置を経由して送出されるパケットをMACアドレス、パケット形式、ETHERNETタイプ、VLAN ID、COS値などの組み合わせで指定し、ETHERポートへの入力時に優先制御情報を書き換えることができます。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、以下の機能を同時に使用することができません。
MACフィルタ情報を有効にするためには、「装置情報」-「資源情報」で「フィルタ/QoS資源の配分」の機能を"フィルタのみ"、プロトコルを"IPv4のみ"に設定する必要があります。

- **MACフィルタ機能**(IPv4)／ **IPフィルタリング機能**(IPv4)
- **MACフィルタ機能**(IPv6 **フィルタ**)／ **IPフィルタリング機能**(IPv6)
- **優先制御情報書き換え機能**(IPv4)／**DSCP値書き換え機能**(IPv4)
- **優先制御情報書き換え機能**(IPv6)／**DSCP値書き換え機能**(IPv6)

書き換え条件

以下の条件を指定することによって、優先制御情報を書き換えることができます。

- ACLのMAC定義およびVLAN定義で指定した以下の情報
  - 送信元MAC情報（MACアドレス／パケット形式／ETHERNETタイプ／LSAP）
  - あて先MAC情報（MACアドレス／パケット形式／ETHERNETタイプ／LSAP）
  - VLAN ID
  - COS値
  - 送信元IP情報（IPアドレス／アドレスマスク）
  - あて先IP情報（IPアドレス／アドレスマスク）
  - TCP・UDPのポート番号
  - ICMP TYPE、ICMP CODE
  - IPパケットのTOS値、DSCP値
- 優先制御情報書き換えの対象となるパケット入力ETHERポート
- 優先制御情報書き換えの対象となるパケットが入力ETHERポートに入力された場合の以下の動作
  - パケットのCOS値を指定した値で書き換える
  - パケットのCOS値をパケットのip precedence値で書き換える
  - パケットのDSCP値を指定した値で書き換える
  - パケットのip precedence値を指定した値で書き換える
  - パケットのip precedence値をパケットのCOS値で書き換える
  - 入力パケットが出力される際に使用される出力ポートのキューを指定したキューに変更する

以下に設定例を示します。

パケットのCOS値を指定した値で書き換える

適用機種　全機種

ここでは、VLAN内の特定ポートで特定のMACアドレスを持つホストからの入力パケットのCOS値を指定した値に書き換える方法を説明します。

● 書き換え要求

- VLAN 20はETHER1～5ポートで構成されるポートVLANで、ETHER1～4ポートでタグ付き、ETHER5ポートでタグなしである
- ETHER5ポートのVLAN 20ではMACアドレス00:0b:01:02:03:04のホストからの入力パケットのCOS値を5に変更する

上記の書き換え要求に従って設定を行う場合の設定例を示します。

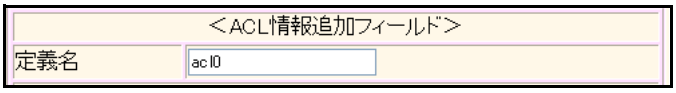
（1）VLAN IDが20で送信元MACアドレスが00:0b:01:02:03:04であるパケットの形式をACLで設定する

1.　設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→acl0



3.　［追加］ボタンをクリックします。

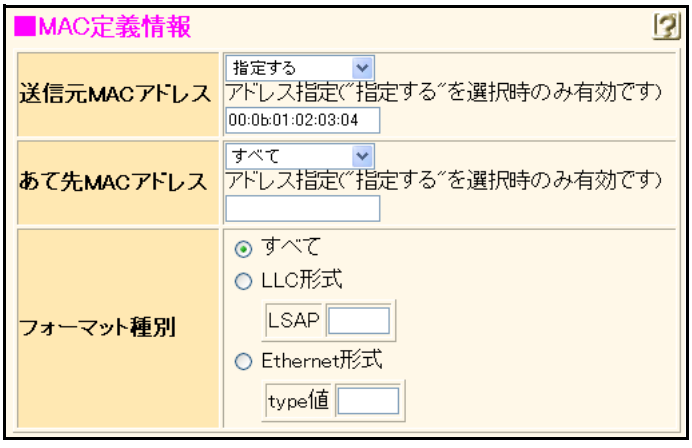
「ACL 定義情報（acl0）」ページが表示されます。

4.　「MAC定義情報」をクリックします。

「MAC定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元MACアドレス　→指定する
  アドレス指定　→00:0b:01:02:03:04
- あて先MACアドレス　→すべて
- フォーマット種別　→すべて



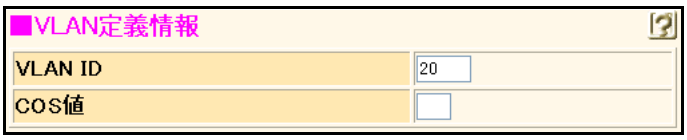
6.　［保存］ボタンをクリックします。

7.　「VLAN 定義情報」をクリックします。

「VLAN 定義情報」が表示されます。

8.　以下の項目を指定します。

- VLAN ID　→ 20
- COS 値　→指定しない



9.　［保存］ボタンをクリックします。

（2）ETHER5 ポートで（1）で設定した形式のパケットの COS 値を 5 に書き換える

10.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

11.　「ether 情報」でポート番号が 5 の［修正］ボタンをクリックします。

ether 5 情報の設定項目と「基本情報」が表示されます。

12.　「QoS 関連」をクリックします。

QoS 関連の設定項目と「基本情報」が表示されます。

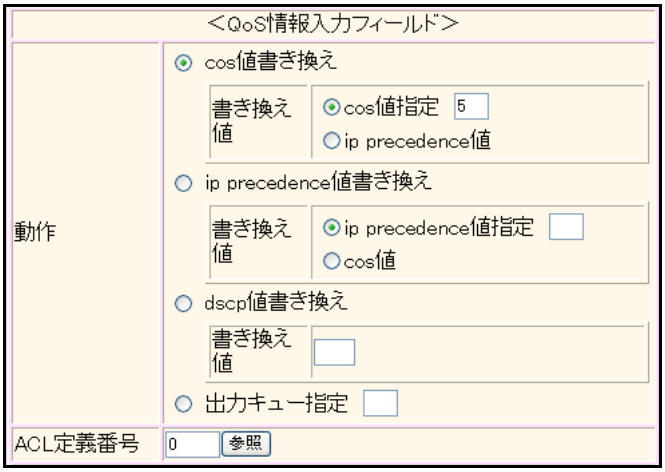
13.　QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS 情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→ cos 値書き換え
  書き換え値　→ cos 値指定　5
- ACL 定義番号　→ 0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

16. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パケットの COS 値をパケットの ip precedence 値で書き換える

適用機種　全機種

ここでは、VLAN 内の特定ポートで特定の MAC アドレスを持つホストへの送信パケットの COS 値をパケットの ip precedence 値で書き換える方法を説明します。

● 書き換え要求

- VLAN 10 は ETHER1 ～ 8 ポートで構成されるポート VLAN で、すべてタグ付きである
- ETHER1 ポートの VLAN 10 では MAC アドレス 00:0b:01:02:03:04 のホストへの送信パケットの COS 値をパケットの ip precedence 値で書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

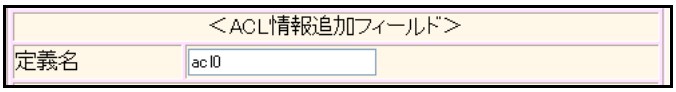
（1）VLAN ID が 10 であて先 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1.　設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ acl0



3.　［追加］ボタンをクリックします。

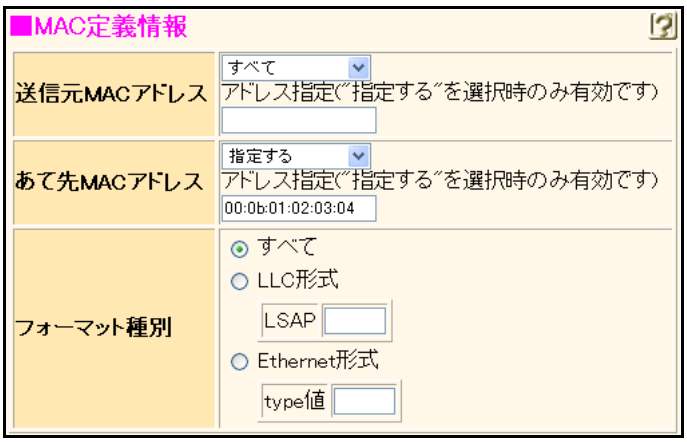
「ACL 定義情報（acl0）」ページが表示されます。

4.　「MAC 定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→指定する
  アドレス指定　→ 00:0b:01:02:03:04
- フォーマット種別　→すべて



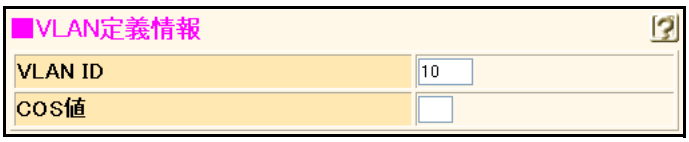
6.　［保存］ボタンをクリックします。

7.　「VLAN 定義情報」をクリックします。

「VLAN 定義情報」が表示されます。

8.　以下の項目を指定します。

- VLAN ID　→ 10
- COS 値　→指定しない



9.　［保存］ボタンをクリックします。

（2）ETHER1 ポートで（1）で設定した形式のパケットの COS 値をパケットの ip precedence 値で書き換える

10.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

11.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

12.　「QoS 関連」をクリックします。

QoS 関連の設定項目と「基本情報」が表示されます。

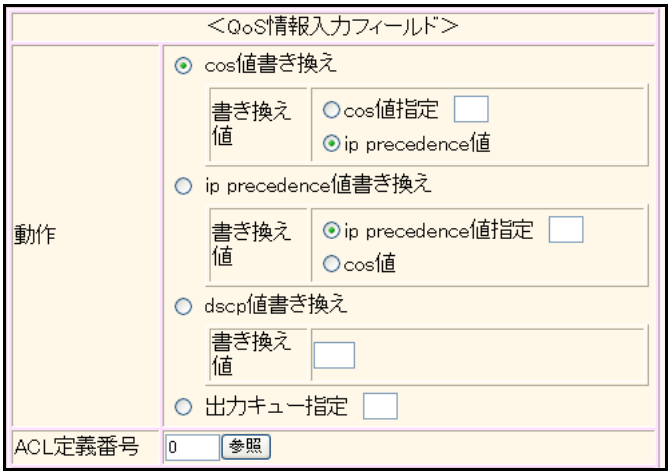
13.　QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS 情報」が表示されます。

14.　以下の項目を指定します。

- 動作　→ cos 値書き換え
  書き換え値　→ ip precedence 値
- ACL 定義番号　→ 0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パケットの DSCP 値を指定した値で書き換える

適用機種　全機種

ここでは、VLAN 内の特定ポートですべての入力パケットの DSCP 値を指定した値で書き換える方法を説明します。

● 書き換え要求

- VLAN 10 は ETHER1 ～ 8 ポートで構成されるポート VLAN で、すべてタグ付きである
- ETHER1 ポートでは全入力パケットの DSCP 値を 40 に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

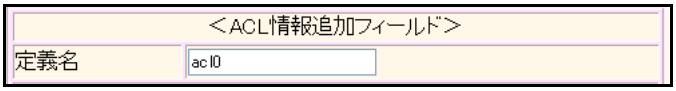
（1）すべてのパケットの形式を ACL で設定する

1.　設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ acl0



3.　［追加］ボタンをクリックします。

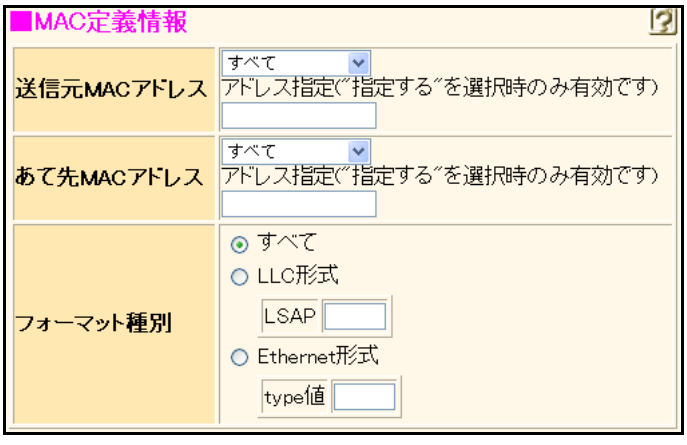
「ACL 定義情報（acl0）」ページが表示されます。

4.　「MAC 定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元 MAC アドレス　→すべて
- あて先 MAC アドレス　→すべて
- フォーマット種別　→すべて



6.　［保存］ボタンをクリックします。

（2）ETHER1 ポートで（1）で設定した形式のパケットの DSCP 値を 40 に書き換える

7.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

8.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

9.　「QoS 関連」をクリックします。

QoS 関連の設定項目と「基本情報」が表示されます。

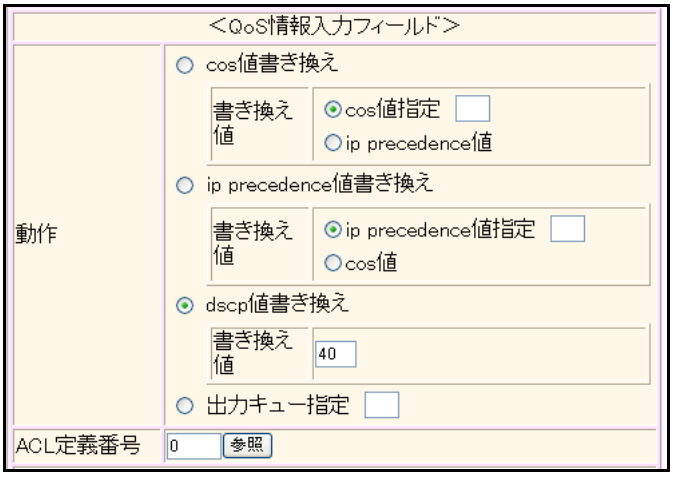
10.　QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS 情報」が表示されます。

11.　以下の項目を指定します。

- 動作　→ dscp 値書き換え
  書き換え値　→ 40
- ACL 定義番号　→ 0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



12.　［追加］ボタンをクリックします。

13.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パケットの ip precedence 値を指定した値で書き換える

適用機種　全機種

ここでは、VLAN 内の特定ポートで特定の COS 値の入力パケットの ip precedence 値を指定した値に書き換える方法を説明します。

● 書き換え要求

- VLAN 10 は ETHER1 ～ 8 ポートで構成されるポート VLAN で、すべてタグ付きである
- VLAN 10 では COS 値 5 のパケットが入力された場合に、入力パケットの ip precedence 値を 6 に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

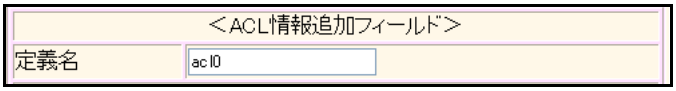
（1）VLAN ID が 10 で COS 値が 5 のパケットの形式を ACL で設定する

1.　設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ acl0



3.　［追加］ボタンをクリックします。

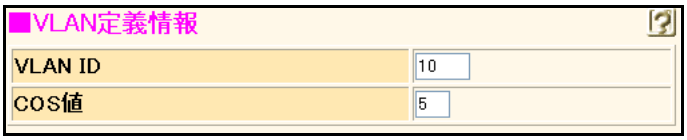
「ACL 定義情報（acl0）」ページが表示されます。

4.　「VLAN 定義情報」をクリックします。

「VLAN 定義情報」が表示されます。

5.　以下の項目を指定します。

- VLAN ID　→ 10
- COS 値　→ 5



6.　［保存］ボタンをクリックします。

（2）VLAN10 に属する ETHER1 ～ 8 ポートで（1）で設定した形式のパケットの ip precedence 値を 6 に書き換える

7.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

8.　以下の項目を指定します。

- ポートリスト　→ 1-8

9. ［修正］ボタンをクリックします。

ether 1-8 情報の設定項目と「基本情報」が表示されます。

10. 「QoS 関連」をクリックします。

QoS 関連の設定項目と「基本情報」が表示されます。

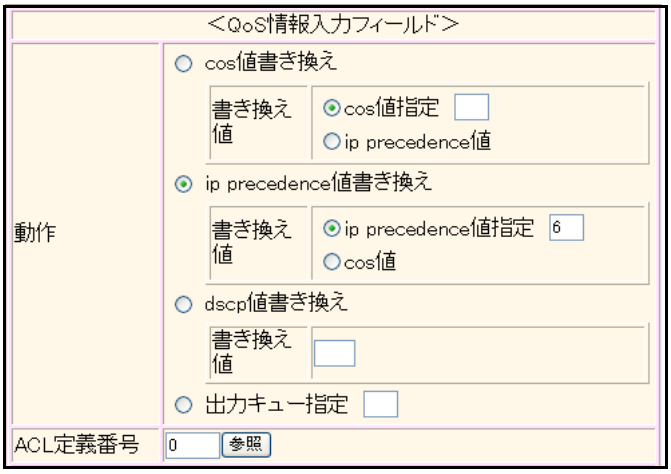
11. QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS 情報」が表示されます。

12. 以下の項目を指定します。

- 動作　→ip precedence 値書き換え
  書き換え値　→ip precedence 値指定　6
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



13. ［追加］ボタンをクリックします。

14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パケットの ip precedence 値をパケットの COS 値で書き換える

適用機種　全機種

ここでは、VLAN 内の特定ポートで特定の VLAN からの入力パケットの ip precedence 値をパケットの COS 値で書き換える方法を説明します。

● 書き換え要求

ETHER10 ポートは VLAN10、VLAN20、VLAN30 にタグ付き、VLAN100 にタグなしで属する

ETHER10 ポートからの VLAN 20、VLAN30、VLAN100 からの入力パケットの ip precedence 値をパケットの COS 値に書き換える

上記の書き換え要求に従って設定を行う場合の設定例を示します。

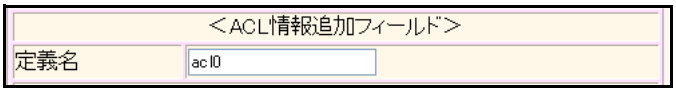
（1）VLAN ID が 20、30、100 のパケットの形式をそれぞれ ACL で設定する

1.　設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→acl0



3.　［追加］ボタンをクリックします。

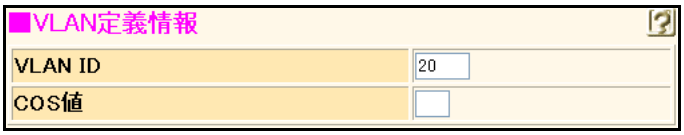
「ACL 定義情報（acl0）」ページが表示されます。

4.　「VLAN 定義情報」をクリックします。

「VLAN 定義情報」が表示されます。

5.　以下の項目を指定します。

- VLAN ID　→20
- COS 値　→指定しない



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→acl1

「ACL 定義情報（acl1）」-「VLAN 定義情報」

- VLAN ID　→30
- COS 値　→指定しない

「ACL 情報」

- 定義名　→acl2

「ACL 定義情報（acl2）」-「VLAN 定義情報」

- VLAN ID　→100
- COS 値　→指定しない

（2）ETHER10 ポートで（1）で作成した形式のパケットの ip precedence 値をパケットの COS 値に書き換える

8.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

9.　「ether 情報」でポート番号が 10 の［修正］ボタンをクリックします。

ether 10 情報の設定項目と「基本情報」が表示されます。

10. 「QoS 関連」をクリックします。

QoS 関連の設定項目と「基本情報」が表示されます。

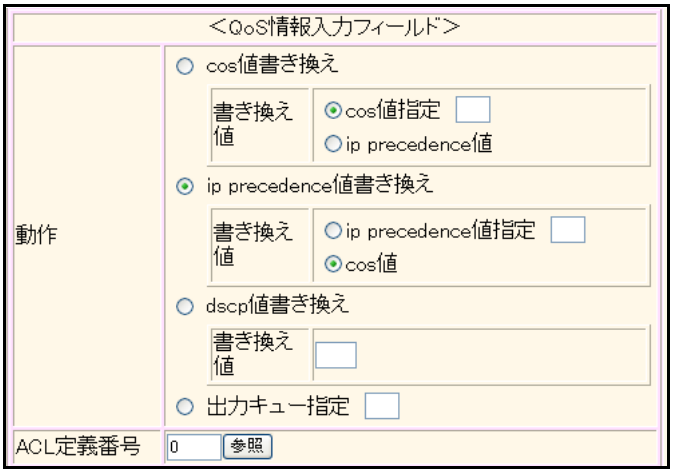
11. QoS 関連の設定項目の「QoS 情報」をクリックします。

「QoS 情報」が表示されます。

12. 以下の項目を指定します。

- 動作 →ip precedence 値書き換え
  書き換え値 →cos 値
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



13. ［追加］ボタンをクリックします。

14. 手順 12. ～ 13. を参考に、以下の項目を設定します。

- 動作 →ip precedence 値書き換え
  書き換え値 →cos 値
- ACL 定義番号 →1

15. 手順 12. ～ 13. を参考に、以下の項目を設定します。

- 動作 →ip precedence 値書き換え
  書き換え値 →cos 値
- ACL 定義番号 →2

16. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

VLAN 単位でパケットの出力キューを変更する

適用機種　全機種

ここでは、VLAN 内のポートで特定の MAC アドレスを持つホストからの入力パケットが出力ポートから出力される際に使用されるキューを変更する方法を説明します。

● 書き換え要求

- VLAN20 は ETHER1 ～ 5 ポートで構成されるポート VLAN で、ETHER1 ～ 4 ポートでタグ付き、ETHER5 ポートでタグなしである
- VLAN20 では MAC アドレス 00:0b:01:02:03:04 のホストからの入力パケットが出力される際に使用される出力ポートのキューを 3 に変更する

上記の書き換え要求に従って設定を行う場合の設定例を示します。

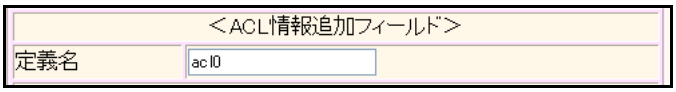
（1）送信元 MAC アドレスが 00:0b:01:02:03:04 であるパケットの形式を ACL で設定する

1.　設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ acl0



3.　［追加］ボタンをクリックします。

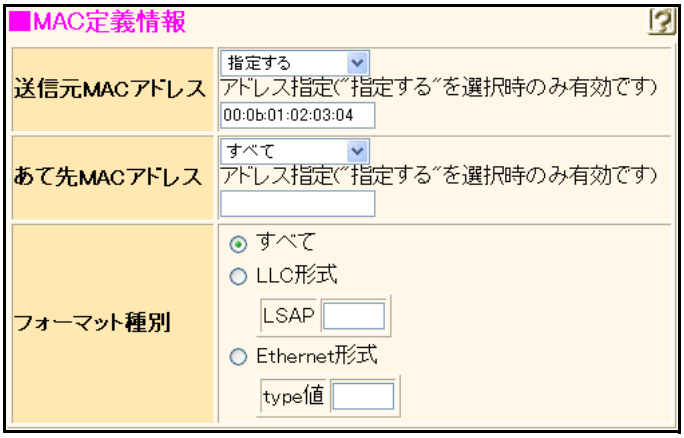
「ACL 定義情報（acl0）」ページが表示されます。

4.　「MAC 定義情報」をクリックします。

「MAC 定義情報」が表示されます。

5.　以下の項目を指定します。

- 送信元 MAC アドレス　→指定する
  アドレス指定　→ 00:0b:01:02:03:04
- あて先 MAC アドレス　→すべて
- フォーマット種別　→すべて



6.　［保存］ボタンをクリックします。

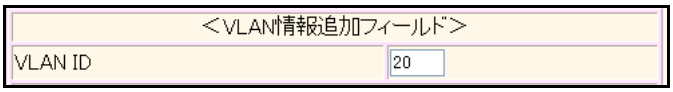
（2）VLAN20 で（1）で設定した形式のパケットが出力ポートから出力される際に使用されるキューを 3 に変更する

7.　設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN 情報」ページが表示されます。

8.　以下の項目を指定します。

- VLAN ID　→20



9.　［追加］ボタンをクリックします。

「VLAN20 情報」ページが表示されます。

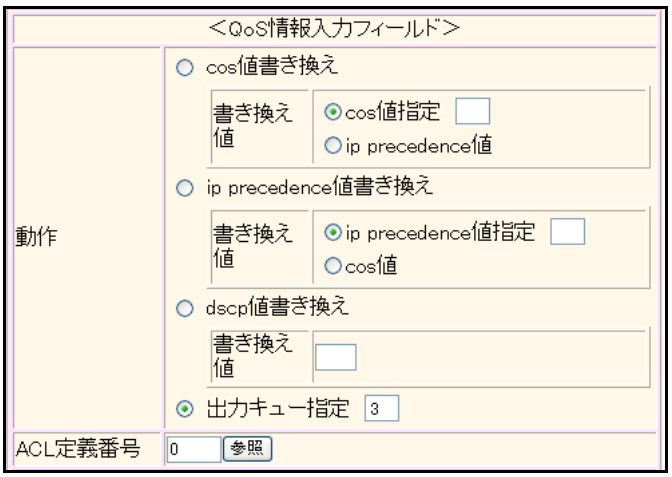
10.　「QoS 情報」をクリックします。

「QoS 情報」が表示されます。

11.　以下の項目を指定します。

- 動作　→出力キュー指定　3
- ACL 定義番号　→0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



12.　［追加］ボタンをクリックします。

13.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

8 STP 機能を使う

適用機種 全機種

ここでは、STP 機能を使用する場合の設定方法を説明します。

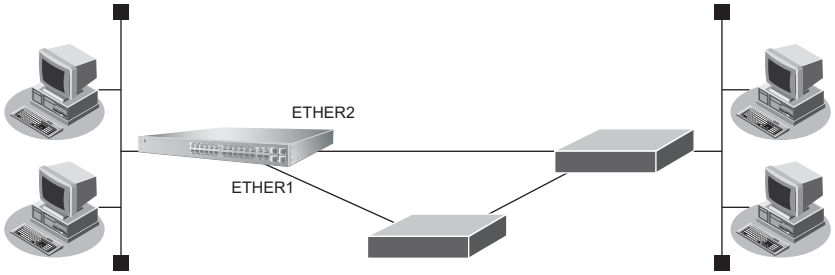
8.1 STP を使う

適用機種 全機種

STP を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

参照 マニュアル「機能説明書」

SR-S332TR1 の場合を例にします。



● 設定条件

- STP を使用する
- ETHER1、2 ポートを VID 10 のポート VLAN とする

上記の設定条件に従って設定を行う場合の設定例を示します。

VLAN を設定する

1. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2. 以下の項目を指定します。

- ポートリスト → 1-2

3. ［修正］ボタンをクリックします。

ether 1-2 情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- VLAN
  Untagged　→10

5.　［保存］ボタンをクリックします。

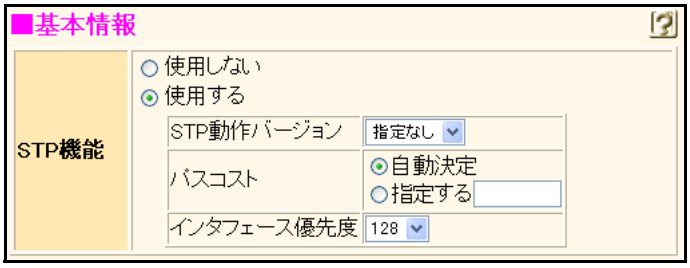
STP を設定する

6.　「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

7.　以下の項目を指定します。

- STP 機能　→使用する



8.　［保存］ボタンをクリックします。

9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

8.2 MSTP を使う

適用機種 全機種

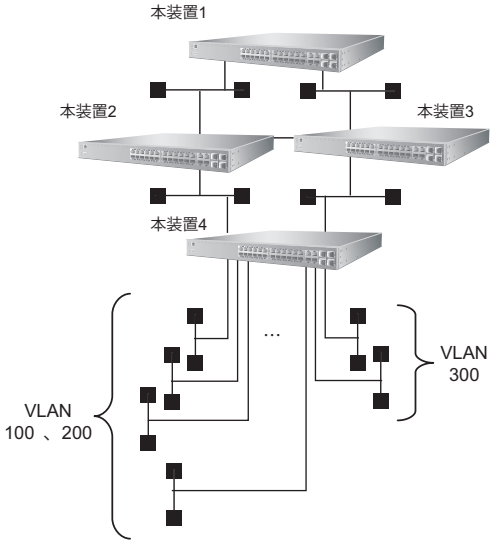
物理的にループしているネットワークでも、VLANの構成によっては、論理的にループしない場合があります。STPではループと判断して、一方のLANを通信に使わないで動作しますが、MSTPではVLAN単位に扱うことができるため、STPよりも効率的にネットワーク内のデータを流すことができます。

参照 マニュアル「機能説明書」

SR-S332TR1の場合を例にします。

● 設定条件

- 以下のようなVLAN環境下でMSTPを併用したVLAN単位でフレームの制御を行う
- 本装置1－本装置2間は1Gとする
- 本装置1－本装置3間は100Mとし、トラフィック量が多いものは本装置1－2間に流す
- 装置間の回線はクロスケーブルを使用する



[インスタンス0]

- ブリッジの優先順位　：本装置1→本装置2→本装置3→本装置4

[インスタンス1]

- ブリッジの優先順位　：本装置1→本装置2→本装置3→本装置4
- VLAN割り当て　：100、200

[インスタンス2]

- ブリッジの優先順位　：本装置1→本装置3→本装置2→本装置4
- VLAN割り当て　：300

[本装置1]

- ETHER1ポートで本装置2と接続し、回線速度は1Gとする
- ETHER2ポートで本装置3と接続し、回線速度は100Mとする
- ETHER1、2ポートのSTPパスコストは、全インスタンス20000とする

[本装置2]

- ETHER1 ポートで本装置 1 と接続し、回線速度は 1G とする
- ETHER2 ポートで本装置 3 と接続し、回線速度は 100M とする
- ETHER3 ポートで本装置 4 と接続し、回線速度は 1G とする
- ETHER1 ～ 3 ポートの STP パスコストは、全インスタンス 20000 とする

[本装置3]

- ETHER1 ポートで本装置 1 と接続し、回線速度は 100M とする
- ETHER2 ポートで本装置 2 と接続し、回線速度は 100M とする
- ETHER3 ポートで本装置 4 と接続し、回線速度は 100M とする
- ETHER1 ～ 3 ポートの STP パスコストは、全インスタンス 20000 とする

[本装置4]

- ETHER1 ポートで本装置 2 と接続し、回線速度は 1G とする
- ETHER2 ポートで本装置 3 と接続し、回線速度は 100M とする
- ETHER1、2 ポートの STP パスコストは、全インスタンス 20000 とする
- ETHER3 ～ 9 ポートで VID100 の端末と接続し、回線速度は 100M とする
- ETHER10 ～ 14 ポートで VID200 の端末と接続し、回線速度は 100M とする
- ETHER15、16 ポートで VID300 の端末と接続し、回線速度は 100M とする

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

MDI および VLAN を設定する

1. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2. 以下の項目を指定します。

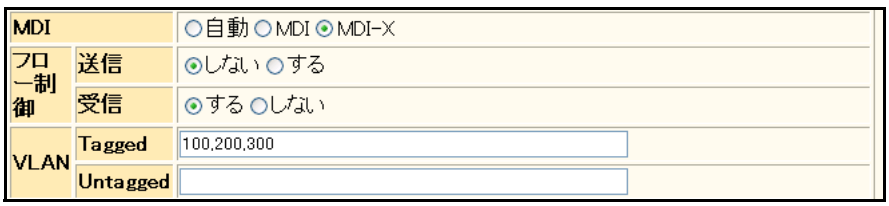
- ポートリスト → 1-2

3. ［修正］ボタンをクリックします。

ether 1-2 情報の設定項目と「基本情報」が表示されます。

4. 以下の項目を指定します。

- MDI → MDI-X
- VLAN
  Tagged → 100,200,300



5.　［保存］ボタンをクリックします。

ETHER1、2 ポートを設定する

6.　設定メニューの詳細設定で「ether 情報」をクリックします。

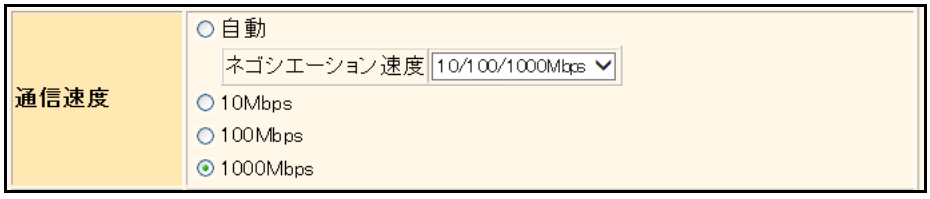
「ether 情報」ページが表示されます。

7.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

8.　以下の項目を指定します。

- 通信速度　→ 1000Mbps



9.　［保存］ボタンをクリックします。

10.　手順 6. ～ 9. を参考に、ETHER2 ポートを設定します。

- 通信速度　→ 100Mbps

ETHER1、2 ポートの STP パスコストを設定する

11.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

12.　以下の項目を指定します。

- ポートリスト　→ 1-2

13.　［修正］ボタンをクリックします。

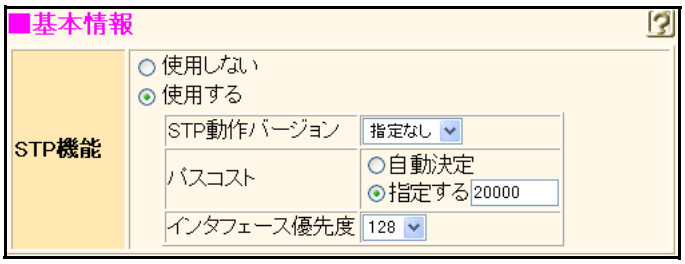
ether 1-2 情報の設定項目と「基本情報」が表示されます。

14.　「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

15.　以下の項目を指定します。

- STP 機能　→使用する
  パスコスト　→指定する
  →20000



16. ［保存］ボタンをクリックします。

17. 「MSTP インスタンス情報」をクリックします。

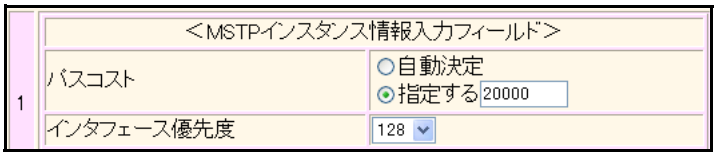
「MSTP インスタンス情報」が表示されます。

18. 「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

19. 以下の項目を指定します。

- パスコスト　→指定する
  →20000



20. ［保存］ボタンをクリックします。

21. 手順 18.～20. を参考に、インスタンス ID 2 を設定します。

- パスコスト　→指定する
  →20000

STP を設定する

22. 設定メニューの詳細設定で「STP 情報」をクリックします。

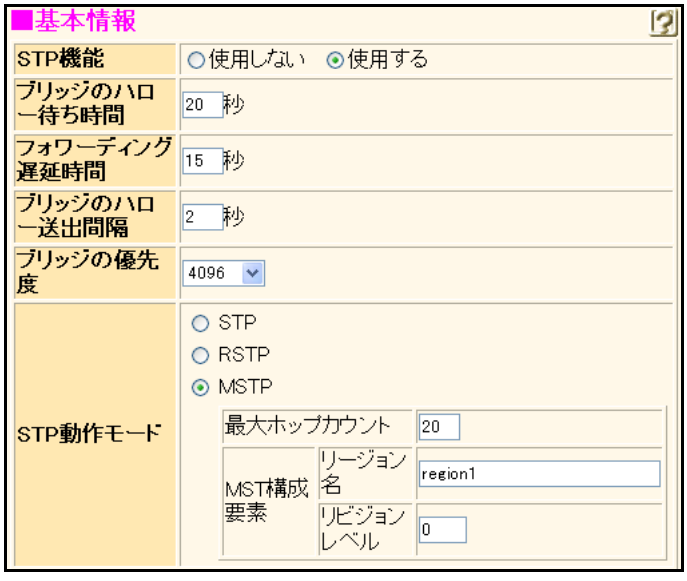
STP 情報の設定項目と「基本情報」が表示されます。

23. 以下の項目を指定します。

- STP 機能　→使用する

“ 使用する ” を選択すると、「ブリッジの優先度」および「STP 動作モード」の設定項目が表示されます。

- ブリッジの優先度　→4096
- STP 動作モード　→MSTP



24. ［保存］ボタンをクリックします。

25. 「MSTP インスタンス情報」をクリックします。

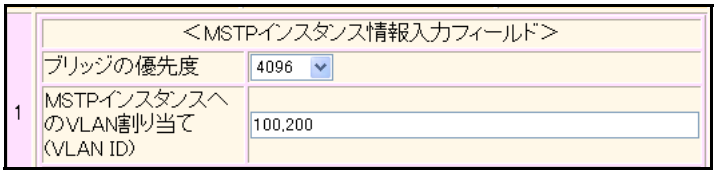
「MSTP インスタンス情報」が表示されます。

26. 「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

27. 以下の項目を指定します。

- ブリッジの優先度 →4096
- MSTP インスタンスへの VLAN 割り当て（VLAN ID）
  →100,200



28. ［保存］ボタンをクリックします。

29. 手順 26.～28. を参考に、インスタンス ID 2 を設定します。

- ブリッジの優先度 →4096
- MSTP インスタンスへの VLAN 割り当て（VLAN ID）
  →300

30. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

MDI および VLAN を設定する

1. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2. 以下の項目を指定します。

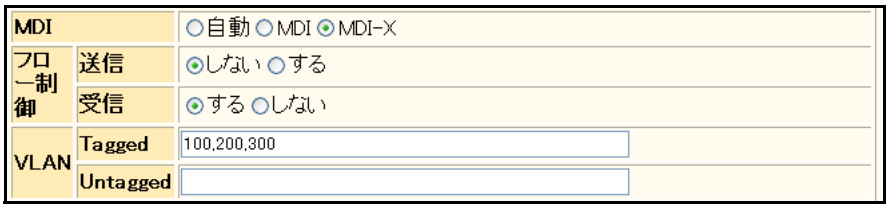
- ポートリスト →1-3

3. ［修正］ボタンをクリックします。

ether 1-3 情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- MDI　→MDI-X
- VLAN
  Tagged　→100,200,300



5.　［保存］ボタンをクリックします。

ETHER1～3ポートを設定する

6.　設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

7.　以下の項目を指定します。

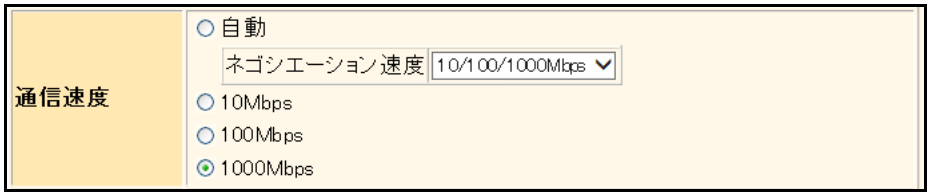
- ポートリスト　→1,3

8.　［修正］ボタンをクリックします。

ether 1,3情報の設定項目と「基本情報」が表示されます。

9.　以下の項目を指定します。

- 通信速度　→1000Mbps



10.　［保存］ボタンをクリックします。

11.　画面上部の「ether情報」をクリックします。

「ether情報」ページが表示されます。

12.　「ether情報」でポート番号が2の［修正］ボタンをクリックします。

ether 2情報の設定項目と「基本情報」が表示されます。

13.　手順9.～10.を参考に、以下の項目を設定します。

- 通信速度　→100Mbps

ETHER1~3ポートのSTPパスコストを設定する

14.　設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

15. 以下の項目を指定します。

- ポートリスト　→1-3

16. ［修正］ボタンをクリックします。

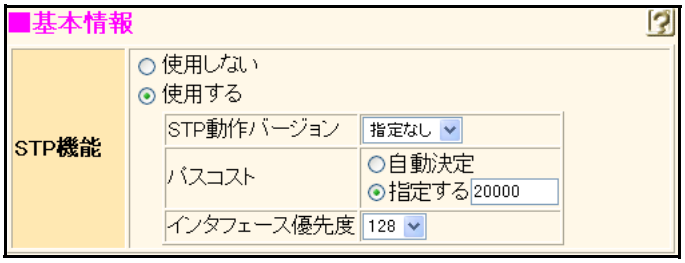
ether 1-3 情報の設定項目と「基本情報」が表示されます。

17. 「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

18. 以下の項目を指定します。

- STP 機能　→使用する
  パスコスト　→指定する
  →20000



19. ［保存］ボタンをクリックします。

20. 「MSTP インスタンス情報」をクリックします。

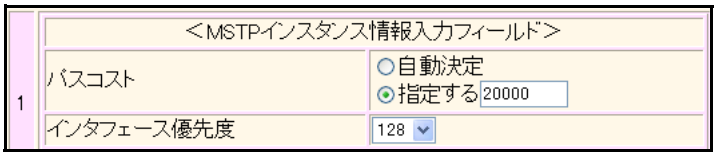
「MSTP インスタンス情報」が表示されます。

21. 「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

22. 以下の項目を指定します。

- パスコスト　→指定する
  →20000



23. ［保存］ボタンをクリックします。

24. 手順 21.～23. を参考に、インスタンス ID 2 を設定します。

- パスコスト　→指定する
  →20000

STP を設定する

25. 設定メニューの詳細設定で「STP 情報」をクリックします。

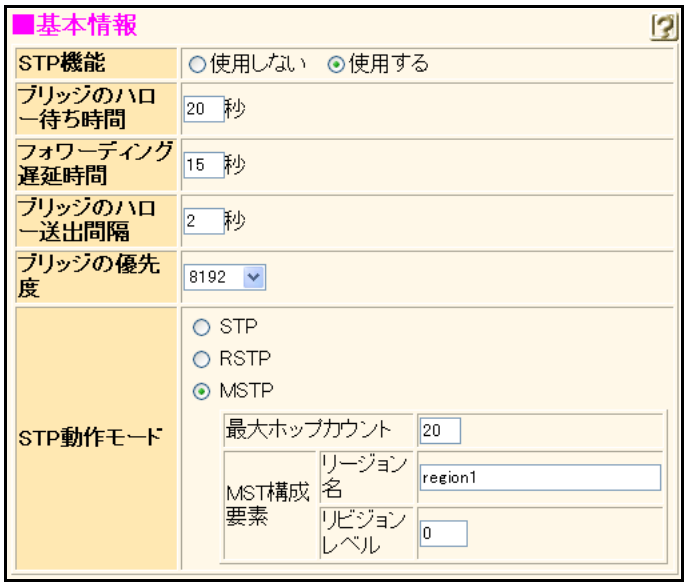
STP 情報の設定項目と「基本情報」が表示されます。

26. 以下の項目を指定します。

- STP 機能　→使用する

“ 使用する ” を選択すると、「ブリッジの優先度」および「STP 動作モード」の設定項目が表示されます。

- ブリッジの優先度　→8192
- STP 動作モード　→ MSTP



27. ［保存］ボタンをクリックします。

28. 「MSTP インスタンス情報」をクリックします。

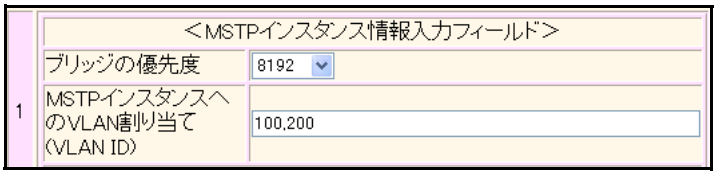
「MSTP インスタンス情報」が表示されます。

29. 「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

30. 以下の項目を指定します。

- ブリッジの優先度　→8192
- MSTP インスタンスへの VLAN 割り当て（VLAN ID）
  →100,200



31. ［保存］ボタンをクリックします。

32. 手順 29. ～ 31. を参考に、インスタンス ID 2 を設定します。

- ブリッジの優先度　→12288
- MSTP インスタンスへの VLAN 割り当て（VLAN ID）
  →300

33. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 3 を設定する

MDI および VLAN を設定する

1. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2. 以下の項目を指定します。

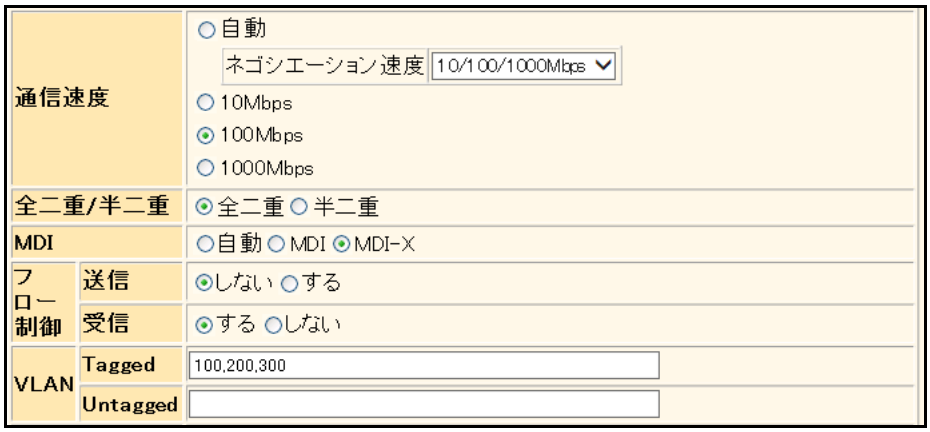
- ポートリスト → 1-3

3. ［修正］ボタンをクリックします。

ether 1-3 情報の設定項目と「基本情報」が表示されます。

4. 以下の項目を指定します。

- 通信速度 → 100Mbps
- MDI → MDI-X
- VLAN
  Tagged → 100,200,300



5. ［保存］ボタンをクリックします。

ETHER1 ～ 3 ポートの STP パスコストを設定する

6. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

7. 以下の項目を指定します。

- ポートリスト → 1-3

8. ［修正］ボタンをクリックします。

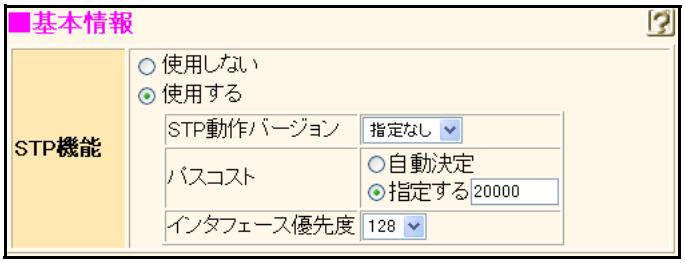
ether 1-3 情報の設定項目と「基本情報」が表示されます。

9. 「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

10. 以下の項目を指定します。

- STP 機能　→使用する
  パスコスト　→指定する
  →20000



11. ［保存］ボタンをクリックします。

12. 「MSTP インスタンス情報」をクリックします。

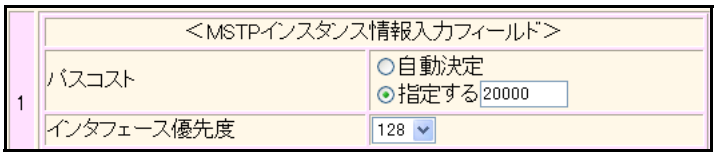
「MSTP インスタンス情報」が表示されます。

13. 「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

14. 以下の項目を指定します。

- パスコスト　→指定する
  →20000



15. ［保存］ボタンをクリックします。

16. 手順 13. ～ 15. を参考に、インスタンス ID 2 を設定します。

- パスコスト　→指定する
  →20000

STP を設定する

17. 設定メニューの詳細設定で「STP 情報」をクリックします。

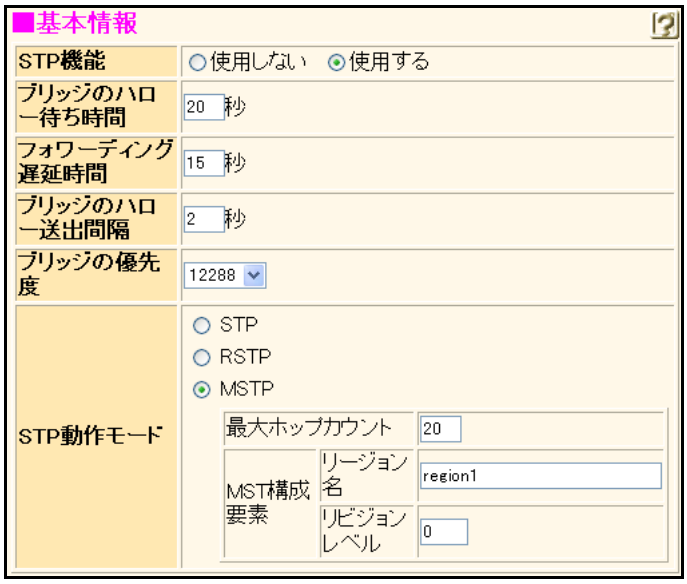
STP 情報の設定項目と「基本情報」が表示されます。

18. 以下の項目を指定します。

- STP 機能　→使用する

“ 使用する ” を選択すると、「ブリッジの優先度」および「STP 動作モード」の設定項目が表示されます。

- ブリッジの優先度　→ 12288
- STP 動作モード　→ MSTP



19. ［保存］ボタンをクリックします。

20. 「MSTP インスタンス情報」をクリックします。

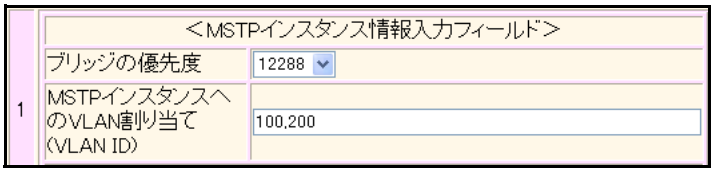
「MSTP インスタンス情報」が表示されます。

21. 「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

22. 以下の項目を指定します。

- ブリッジの優先度　→ 12288
- MSTP インスタンスへの VLAN 割り当て（VLAN ID）
  → 100,200



23. ［保存］ボタンをクリックします。

24.　手順21.～23.を参考に、インスタンスID 2を設定します。

- ブリッジの優先度　→8192
- MSTPインスタンスへのVLAN割り当て（VLAN ID）
  →300

25.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置4を設定する

MDIおよびVLANを設定する

1.　設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2.　以下の項目を指定します。

- ポートリスト　→1-16

3.　［修正］ボタンをクリックします。

ether 1-16情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- MDI　→MDI-X

5.　［保存］ボタンをクリックします。

ETHER1～16ポートを設定する

6.　設定メニューの詳細設定で「ether情報」をクリックします。

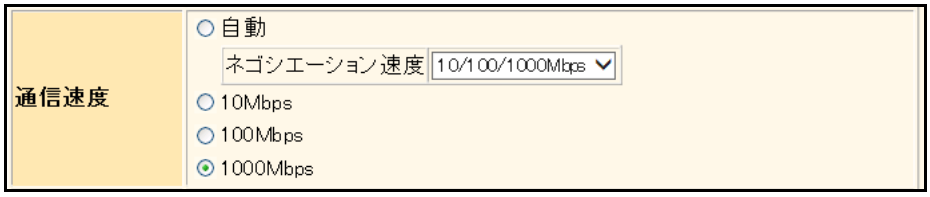
「ether情報」ページが表示されます。

7.　「ether情報」でポート番号が1の［修正］ボタンをクリックします。

ether 1情報の設定項目と「基本情報」が表示されます。

8.　以下の項目を指定します。

- 通信速度　→1000Mbps



9.　［保存］ボタンをクリックします。

10.　画面上部の「ether情報」をクリックします。

「ether情報」ページが表示されます。

11. 以下の項目を指定します。

- ポートリスト　→2-16

12. ［修正］ボタンをクリックします。

ether 2-16 情報の設定項目と「基本情報」が表示されます。

13. 手順 8. ～ 9. を参考に、以下の項目を設定します。

- 通信速度　→100Mbps

VLAN を設定する

14. 設定メニューの詳細設定で「ether 情報」をクリックします。

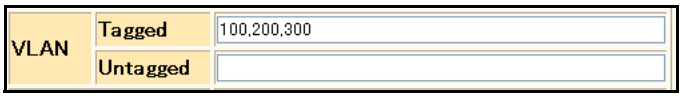
「ether 情報」ページが表示されます。

15. 「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

16. 以下の項目を指定します。

- VLAN
  Tagged　→100,200,300



17. ［保存］ボタンをクリックします。

18. 手順 14. ～ 17. を参考に、ETHER2 ポートを設定します。

「ether 2 情報」-「基本情報」

- VLAN
  tagged　→100,200,300

19. 画面上部の「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

20. 以下の項目を指定します。

- ポートリスト　→3-9

21. ［修正］ボタンをクリックします。

ether 3-9 情報の設定項目と「基本情報」が表示されます。

22. 以下の項目を指定します。

- VLAN
  Untagged　→100

23.　［保存］ボタンをクリックします。

24.　手順 19.～23. を参考に、ETHER10～14 ポートを設定します。

「ether 10-14 情報」-「基本情報」

- VLAN
  Untagged　　→200

25.　手順 19.～23. を参考に、ETHER15、16 ポートを設定します。

「ether 15-16 情報」-「基本情報」

- VLAN
  Untagged　　→300

ETHER1、2 ポートの STP パスコストを設定する

26.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

27.　以下の項目を指定します。

- ポートリスト　　→1-2

28.　［修正］ボタンをクリックします。

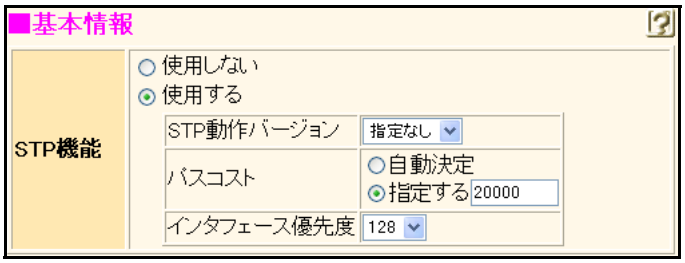
ether 1-2 情報の設定項目と「基本情報」が表示されます。

29.　「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

30.　以下の項目を指定します。

- STP 機能　　→使用する
  パスコスト　　→指定する
  　　→20000



31.　［保存］ボタンをクリックします。

32.　「MSTP インスタンス情報」をクリックします。

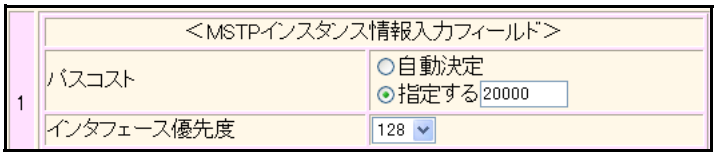
「MSTP インスタンス情報」が表示されます。

33.　「MSTP インスタンス情報」でインスタンス ID が 1 の［修正］ボタンをクリックします。

インスタンス ID 1 の「MSTP インスタンス情報入力フィールド」が表示されます。

34. 以下の項目を指定します。

- パスコスト　→指定する
  →20000



35. ［保存］ボタンをクリックします。

36. 手順33.～35.を参考に、インスタンスID 2を設定します。

- パスコスト　→指定する
  →20000

STPを設定する

37. 設定メニューの詳細設定で「STP情報」をクリックします。

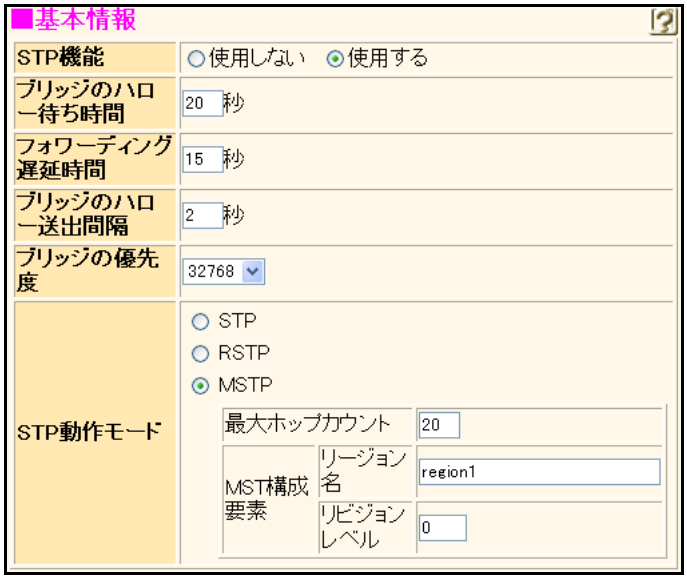
STP情報の設定項目と「基本情報」が表示されます。

38. 以下の項目を指定します。

- STP機能　→使用する

“使用する”を選択すると、「ブリッジの優先度」および「STP動作モード」の設定項目が表示されます。

- ブリッジの優先度　→32768
- STP動作モード　→MSTP



39. ［保存］ボタンをクリックします。

40. 「MSTPインスタンス情報」をクリックします。

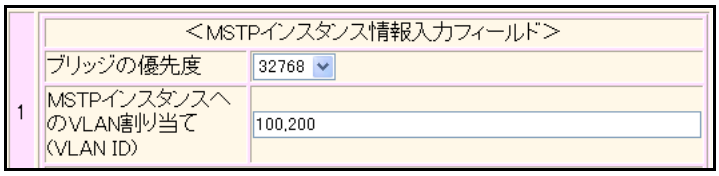
「MSTPインスタンス情報」が表示されます。

41. 「MSTPインスタンス情報」でインスタンスIDが1の［修正］ボタンをクリックします。

インスタンスID 1の「MSTPインスタンス情報入力フィールド」が表示されます。

42. 以下の項目を指定します。

- ブリッジの優先度　→32768
- MSTPインスタンスへのVLAN割り当て（VLAN ID）
  →100,200



43. ［保存］ボタンをクリックします。

44. 手順41.～43.を参考に、インスタンスID 2を設定します。

- ブリッジの優先度　→32768
- MSTPインスタンスへのVLAN割り当て（VLAN ID）
  →300

45. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

9 DHCPスヌープ機能を使う

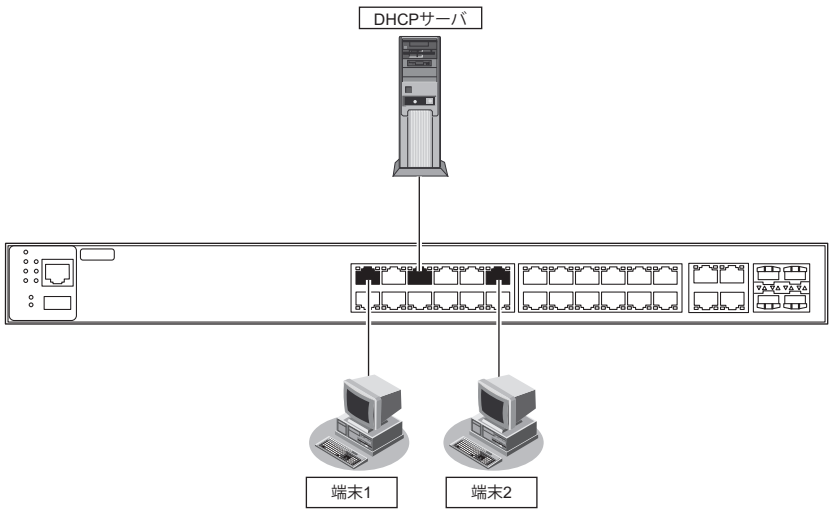
適用機種 全機種

DHCPスヌープ機能を使用すると、DHCPでIPアドレスが割り当てられた端末だけ通信を許可することができ、管理外の不正端末によるネットワークへの不正アクセスを防止することができます。

参照 マニュアル「機能説明書」

こんな事に気をつけて

- 本機能はIPv4の場合に使用できます。
- DHCPサーバは通信許可を“すべての端末”に設定されたポートに接続してください。
- 同一VLAN内でIPv4 DHCP機能を有効に設定した場合、このVLANでは本機能が無効になり、すべての端末が通信可能となります。
- 通信許可が“DHCPでIPアドレスを割り当てられた端末のみ”に設定されたポートで以下の条件に一致する場合、このポートでは本機能が無効になり、すべての端末が通信可能となります。
  - IEEE802.1X認証、Web認証およびMACアドレス認証のどれかが有効に設定されている場合
  - リンクアグリゲーションとして設定されている場合
  - タグVLANが設定されている場合
  - プロトコルVLANが設定されている場合
- 本装置では、一度登録された許可端末が存在しなくなってもエントリ自体はリース期間の満了まで消去しません。DHCPサーバでリース期間を適切に設定してください。
  また、不要なエントリが登録されている場合は、「表示メニュー」-「DHCPスヌープ関連」-「エントリ情報」で消去することができます。
- 監視可能なDHCPクライアント数を超えた場合、受信したDHCPパケットは破棄されエントリ登録されません。
  また、最大エントリ数に満たない場合でも登録できないことがあります。エントリ登録に失敗した場合は、登録に失敗したことを示すシステムログが記録されます。
- 本機能はDHCPパケットの往復を監視して動作します。DHCPクライアントとサーバ間の通信は必ず本装置を経由するようなネットワーク構成にしてください。
- 設定反映、または装置リセットを実行した場合、エントリが破棄される場合があります。この場合、端末がDHCPでIPアドレスを再取得するまで通信できなくなります。



● 設定条件

- VLAN10 で DHCP スヌープ機能を使用する
- ETHER ポートの通信許可
  ETHER1 ポート　：DHCP で IP アドレスを割り当てられた端末のみ
  ETHER5 ポート　：すべての端末
  ETHER11 ポート　：DHCP で IP アドレスを割り当てられた端末のみ

上記の設定条件に従って設定を行う場合の設定例を示します。

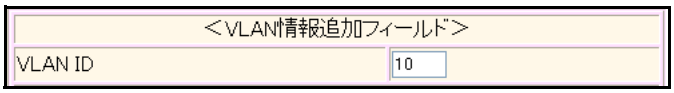
DHCP スヌープ機能を使用する

1.　設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN 情報」ページが表示されます。

2.　以下の項目を指定します。

- VLAN ID　→ 10



3.　［追加］ボタンをクリックします。

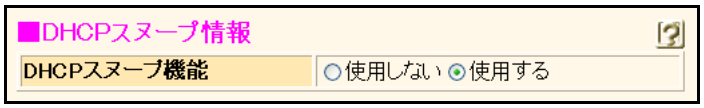
「VLAN10 情報」ページが表示されます。

4.　「DHCP スヌープ情報」をクリックします。

「DHCP スヌープ情報」が表示されます。

5.　以下の項目を指定します。

- DHCP スヌープ機能　→使用する



6.　［保存］ボタンをクリックします。

DHCP スヌープの ETHER ポートの通信許可を設定する

7.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

8.　「ether 情報」でポート番号が 1 の「修正」ボタンをクリックします。

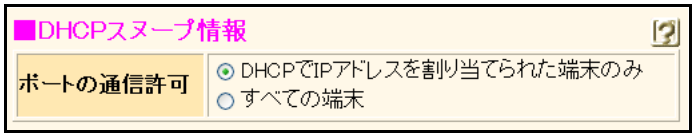
ether1 情報の設定項目と「基本情報」が表示されます。

9.　「DHCP スヌープ情報」をクリックします。

「DHCP スヌープ情報」が表示されます。

10.　以下の項目を設定します。

- ポートの通信許可　→ DHCP で IP アドレスを割り当てられた端末のみ



11. ［保存］ボタンをクリックします。

12. 「基本情報」をクリックします。

「基本情報」が表示されます。

- VLAN
  untagged →10

13. ［保存］ボタンをクリックします。

14. 手順6.～12.を参考にETHERポート5を設定します。

「ether5情報」-「DHCPスヌープ情報」

- ポートの通信許可 →すべての端末

「ether5情報」-「基本情報」

- VLAN
  untagged →10

15. 手順6.～12.を参考にETHERポート11を設定します。

「ether11情報」-「DHCPスヌープ情報」

- ポートの通信許可 →DHCPでIPアドレスを割り当てられた端末のみ

「ether11情報」-「基本情報」

- VLAN
  untagged →10

16. ［保存］ボタンをクリックします。

17. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

10　IGMP スヌープ機能を使う

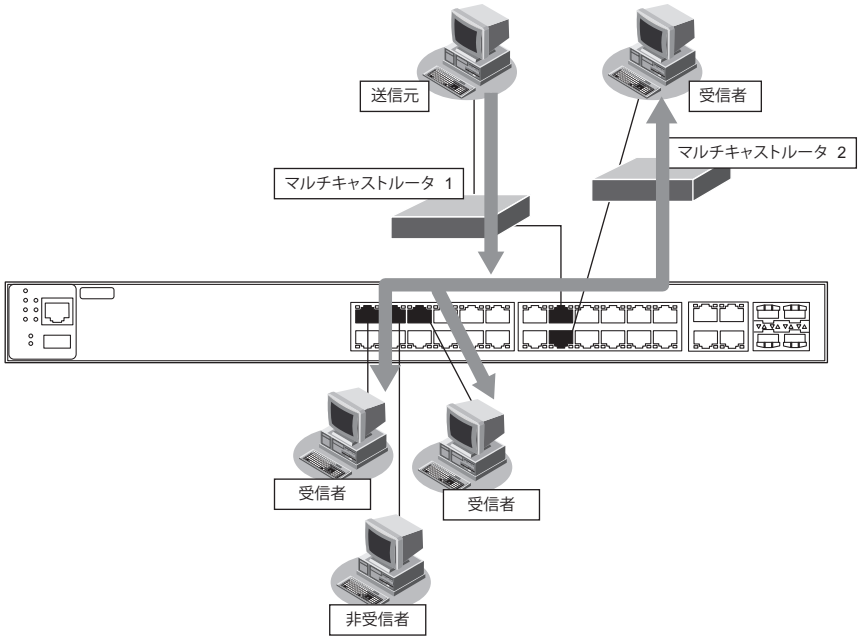
適用機種　全機種

IGMP スヌープ機能を使用すると、マルチキャストパケットを必要としているポートをIGMP パケットから検出し、そのポート以外へはマルチキャストパケットを転送しません。これにより、無用なトラフィックを端末やサーバに送出することが防止でき、マルチキャストを利用しているネットワークで端末やサーバの負荷を軽減することができます。

☛ 参照　マニュアル「機能説明書」

こんな事に気をつけて

- **マルチキャストルーティング機能が有効である lan 定義が存在する場合、IGMP スヌープ機能は無効となり、動作しません。**
- **IGMP を利用しないでマルチキャスト通信を行っている場合は、通信ができなくなる可能性があります。**
- **IGMP スヌープが有効である装置と接続するポートは、構成定義でマルチキャストルータポートとして設定してください。**
- **マルチキャストルータが 2 台以上接続される場合は、マルチキャストルータポートを構成定義で設定してください。マルチキャストルータポートが正しく認識されなくなり、マルチキャストルータの先に接続される端末がマルチキャストパケットを受信できなくなる場合があります。**
- **本装置では、一度登録されたグループアドレスはリスナ端末が存在しなくなった場合でもエントリ自体を消去しないで、出力ポートの情報のみを消去します。不要なグループアドレスが登録されている場合は、「表示メニュー」-「IGMP スヌープ関連」-「リスナ情報」で消去することができます。**
- **最大登録可能なマルチキャストグループアドレス数を超えた場合、超えたアドレスはすべて破棄されます。扱われるグループアドレスが最大登録可能数を超える場合は、IGMP スヌープ機能は利用しないでください。**
- **IGMP スヌープ機能を有効にした場合、「VLAN 情報」-「IGMP スヌープ情報」の「IGMP 送信元アドレス」に定義がないと送信元アドレスとして 0.0.0.0 を使用します。送信元アドレスが 0.0.0.0 である IGMP Query パケットを扱えない装置が接続されている場合、「VLAN 情報」-「IGMP スヌープ情報」の「IGMP 送信元アドレス」を設定してください。なお、マルチキャストルータが接続されているネットワークでは、マルチキャストルータのアドレスより大きな値となるアドレスを送信元アドレスとして指定してください。**
- **IGMP V1/V2 が混在する環境では、「VLAN 情報」-「IGMP スヌープ情報」で IGMP 代理応答モードを“代理応答しない”と選択してください。**
- **IPv4 マルチキャスト以外の通信（例：IPv6 通信）を利用するネットワークでは利用できません。IGMP スヌープ機能は有効にしないでください。**
- **マルチキャストルータが接続されないネットワークでは、「VLAN 情報」-「IGMP スヌープ情報」で Querier モードを動作可能としてください。**



● 設定条件

- IGMPスヌープ機能を利用する
- リスナ端末はそれぞれ以下に属する

リスナ端末1	ポート	：ETHER1、2ポート
	VLAN	：10
リスナ端末2	ポート	：ETHER3、4ポート
	VLAN	：11
リスナ端末3	ポート	：ETHER5、6ポート
	VLAN	：12

- マルチキャストルータ1はタグVLANを使用し、VLAN10～12を設定する
  ポートはETHER15に接続する
- マルチキャストルータ2はVLAN10に属し、ポートはETHER16に接続する

上記の設定条件に従って設定を行う場合の設定例を示します。

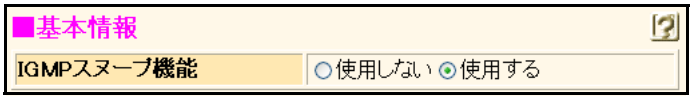
IGMPスヌープ機能を使用する

1.　設定メニューの詳細設定で「IGMPスヌープ情報」をクリックします。

「IGMPスヌープ情報」ページが表示されます。

2.　以下の項目を指定します。

- IGMPスヌープ機能　　→使用する



3.　［保存］ボタンをクリックします。

VLAN を設定する

4. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

5. 以下の項目を指定します。

- ポートリスト　→ 1-2

6. ［修正］ボタンをクリックします。

ether 1-2 情報の設定項目と「基本情報」が表示されます。

7. 以下の項目を指定します。

- VLAN
  Untagged　→ 10

8. ［保存］ボタンをクリックします。

9. 手順 4. ～ 8. を参考に、ETHER3 ～ 6、15、16 を設定します。

「ether 3 情報」-「基本情報」

- VLAN
  Untagged　→ 11

「ether 4 情報」-「基本情報」

- VLAN
  Untagged　→ 11

「ether 5 情報」-「基本情報」

- VLAN
  Untagged　→ 12

「ether 6 情報」-「基本情報」

- VLAN
  Untagged　→ 12

「ether 15 情報」-「基本情報」

- VLAN
  Tagged　→ 10-12

「ether 16 情報」-「基本情報」

- VLAN
  Untagged　→ 10

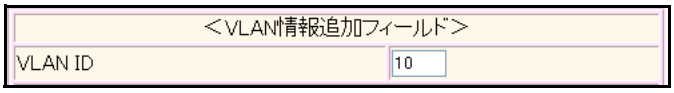
複数のマルチキャストルータが接続されるVLAN10にマルチキャストルータポートを設定する

10. 設定メニューの詳細設定で「VLAN情報」をクリックします。

「VLAN情報」ページが表示されます。

11. 以下の項目を指定します。

- VLAN ID →10



12. ［追加］ボタンをクリックします。

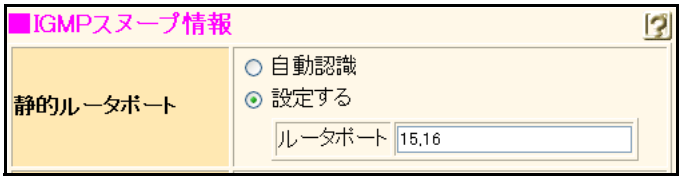
「VLAN10情報」ページが表示されます。

13. 「IGMPスヌープ情報」をクリックします。

「IGMPスヌープ情報」が表示されます。

14. 以下の項目を指定します。

- 静的ルータポート →設定する
  ルータポート →15,16



15. ［保存］ボタンをクリックします。

16. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

11　IEEE802.1X認証機能を使う

適用機種　全機種

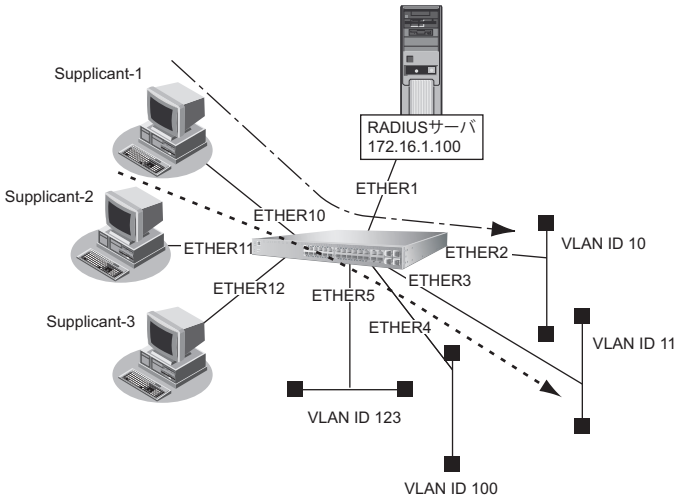
IEEE802.1X認証を使用すると、本装置に接続する端末ユーザがネットワークへのアクセス権限を持っているかを認証することができます。また、認証データベースで、ユーザごとに所属するVLAN IDを設定すると、認証されたユーザが所属するネットワークも同時に管理できます。これらの機能によりネットワークへのアクセスをユーザ単位で制御でき、ネットワークのセキュリティを向上することができます。

参照　マニュアル「機能説明書」

こんな事に気をつけて

- **IEEE802.1X 認証を利用するポートでは、事前にVLANを設定できません。ただし、以下の場合はその限りではありません。**
  - **Web 認証機能が併用されている場合の、Web 認証用のタグなしのポートVLAN 設定**
  - **VLAN タグ付きフレームを認証しないで透過する場合の、タグVLAN 設定**
- **IEEE802.1X 認証で利用するAAA のグループIDを正しく設定してください。**
- **ローカル認証で利用できる認証方式はEAP-MD5 のみです。**
- **マルチサプリカント環境で確認済みのサプリカントソフトは富士通製「Systemwalker Desktop Inspection 802.1X サプリカント」です。**
- **マルチサプリカント環境では課金情報のうち以下の項目が正しく採取できません。**
  - **送信パケット数**
  - **受信パケット数**
  - **送信バイト数**
  - **受信バイト数**

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER10～12 ポートでIEEE802.1X認証を使用する
- ETHER10～12 ポートで利用する認証データベース
  ETHER10、11 ポート　：RADIUS サーバ
  ETHER12 ポート　：ローカルで設定した認証情報

- AAA グループ ID
  ETHER10、11 ポート　：0
  ETHER12 ポート　：1
- Supplicant の MAC アドレスごとに認証を行う
- ETHER12 ポートで利用可能なユーザは以下のとおり

ユーザ ID	パスワード	割り当てる VLAN ID
Supp1	Supp1-pass	VLAN123
Supp2	Supp2-pass	VLAN100

- RADIUS サーバの IP アドレス　：172.16.1.100
- RADIUS サーバは VLAN13 に接続されている
- RADIUS サーバのシークレット　：radius-secret
- ETHER10、11 ポートで利用する RADIUS サーバで、認証処理と課金情報（※）の収集を行う

※）本装置がサポートする課金情報と対応する属性を以下に示します。

- 接続時間　：Acct-Session-Time
- 送信パケット数　：Acct-Output-Packets
- 受信パケット数　：Acct-Input-Packets
- 送信バイト数　：Acct-Output-Octets
- 受信バイト数　：Acct-Input-Packets

こんな事に気をつけて

- **RADIUS サーバにはユーザに VLAN ID を割り当てるために以下の属性を設定してください。設定方法については RADIUS サーバのマニュアルを参照してください。**

名前	番号	属性値（※）
Tunnel-Type	64	VLAN（13）
Tunnel-Media-Type	65	802（6）
Tunnel-Private-Group-ID	81	VLAN ID（10 進数表記を ASCII コードでコーディング）

※）（）内の数字は属性として設定される 10 進数の値

- **タグにより複数のトンネル属性が設定されている場合は、利用可能な値が指定されているもっとも小さなタグの情報がユーザに割り当てる VLAN 情報として選択されます。**

上記の設定条件に従って設定を行う場合の設定例を示します。

IEEE802.1X 認証を使用する

1.　設定メニューの詳細設定で「認証情報」をクリックします。

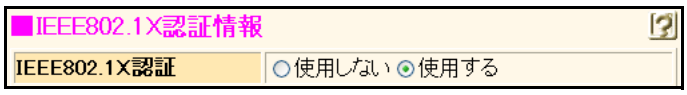
「認証情報」ページが表示されます。

2.　「IEEE802.1X 認証情報」をクリックします。

「IEEE802.1X 認証情報」が表示されます。

3.　以下の項目を指定します。

- IEEE802.1X 認証　→使用する



4. **［保存］ボタンをクリックします。**

RADIUS サーバの VLAN を設定する

5. **設定メニューの詳細設定で「LAN 情報」をクリックします。**

   「LAN 情報」ページが表示されます。

6. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**

   「LAN0 情報」ページが表示されます。

7. **「共通情報」をクリックします。**

   共通情報の設定項目と「基本情報」が表示されます。

8. **以下の項目を指定します。**

   - VLAN ID　→ 13

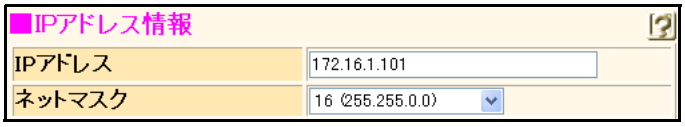
9. **［保存］ボタンをクリックします。**

10. **「IP 関連」をクリックします。**

    IP 関連の設定項目と「IP アドレス情報」が表示されます。

11. **以下の項目を指定します。**

    - IP アドレス　→ 172.16.1.101
    - ネットマスク　→ 16（255.255.0.0）



12. **［保存］ボタンをクリックします。**

RADIUS サーバを接続するポートを設定する

13. **設定メニューの詳細設定で「ether 情報」をクリックします。**

    「ether 情報」ページが表示されます。

14. **「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。**

    ether 1 情報の設定項目と「基本情報」が表示されます。

VLAN を設定する

15. **以下の項目を指定します。**

    - VLAN
      Untagged　→ 13

16. **［保存］ボタンをクリックします。**

IEEE802.1X により認証された Supplicant が接続される VLAN 情報を設定する

17.　手順 13.～16. を参考に、ETHER2～5 ポートを設定します。

「ether 2 情報」-「基本情報」

- VLAN
  Untagged　→ 10

「ether 3 情報」-「基本情報」

- VLAN
  Untagged　→ 11

「ether 4 情報」-「基本情報」

- VLAN
  Untagged　→ 100

「ether 5 情報」-「基本情報」

- VLAN
  Untagged　→ 123

IEEE802.1X 認証ポートを設定する

18.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

19.　以下の項目を指定します。

- ポートリスト　→ 10-11

20.　［修正］ボタンをクリックします。

ether 10-11 情報の設定項目と「基本情報」が表示されます。

21.　「IEEE802.1X 認証情報」をクリックします。

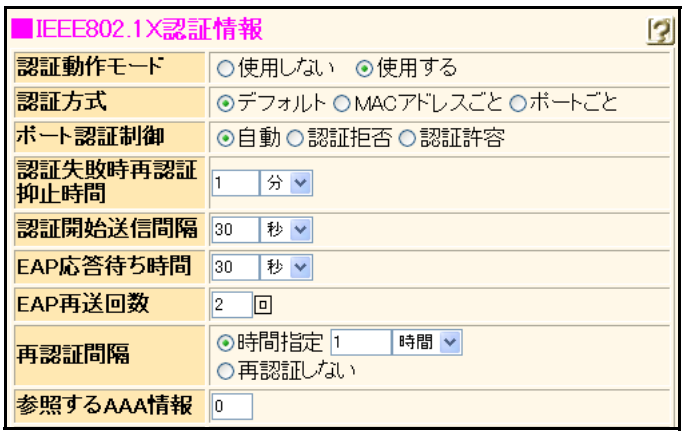
「IEEE802.1X 認証情報」が表示されます。

22.　以下の項目を指定します。

- 認証動作モード　→使用する

" 使用する " を選択すると、「参照する AAA 情報」の設定項目が表示されます。

- 参照する AAA 情報　→ 0



23.　［保存］ボタンをクリックします。

24.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

25.　「ether 情報」でポート番号が 12 の［修正］ボタンをクリックします。

ether 12 情報の設定項目と「基本情報」が表示されます。

26.　手順 21. ～ 23. を参考に、以下の項目を設定します。

- 認証動作モード　→使用する
- 参照する AAA 情報　→ 1

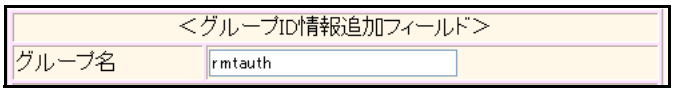
RADIUS サーバを利用する AAA グループ情報を設定する

27.　設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

28.　以下の項目を指定します。

- グループ名　→ rmtauth



29.　［追加］ボタンをクリックします。

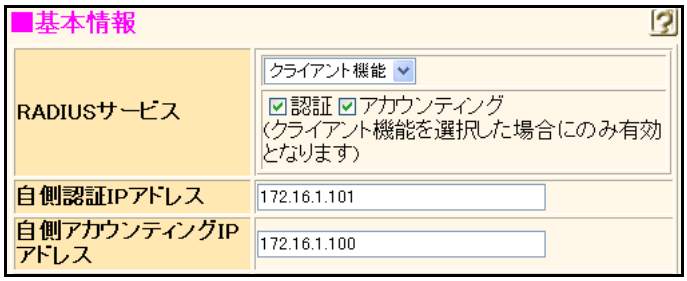
「グループ ID 情報（0）」ページが表示されます。

30.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

31.　以下の情報を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックする
- 自側認証 IP アドレス　→ 172.16.1.101
- 自側アカウンティング IP アドレス　→ 172.16.1.100



32.　［保存］ボタンをクリックします。

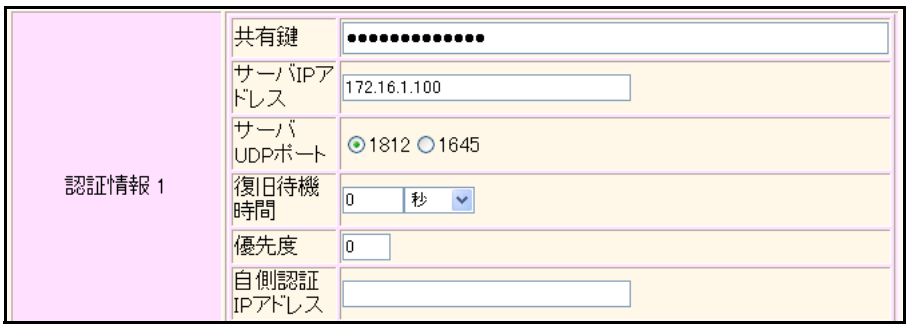
33.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

34.　「認証情報 1」の［修正］ボタンをクリックします。

35. 以下の項目を指定します。

- 認証情報 1
  共有鍵 →radius-secret
  サーバ IP アドレス →172.16.1.100



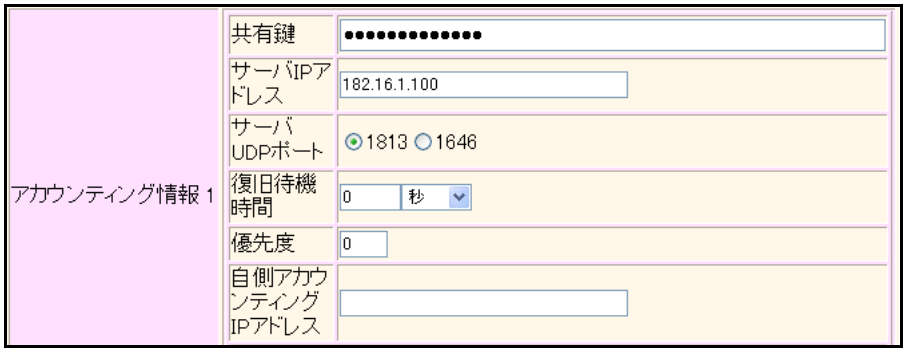
36. 認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

37. 「アカウンティング情報 1」の［修正］ボタンをクリックします。

38. 以下の項目を指定します。

- アカウンティング情報 1
  共有鍵 →radius-secret
  サーバ IP アドレス →172.16.1.100



39. アカウンティング情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

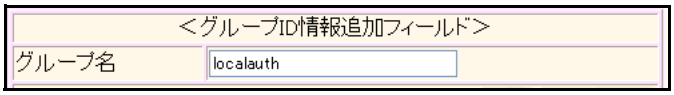
ローカル認証情報を利用する AAA グループ情報を設定する

40. 設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

41. 以下の項目を指定します。

- グループ名 →localauth



42. ［追加］ボタンをクリックします。

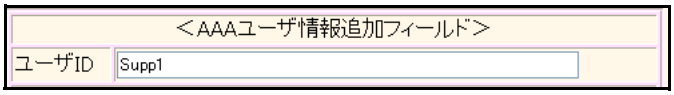
「グループ ID 情報（1）」ページが表示されます。

43. **「AAA ユーザ情報」をクリックします。**

AAA ユーザ情報の設定項目と「AAA ユーザ情報」が表示されます。

44. **以下の項目を指定します。**

- ユーザ ID　→ Supp1



45. **［追加］ボタンをクリックします。**

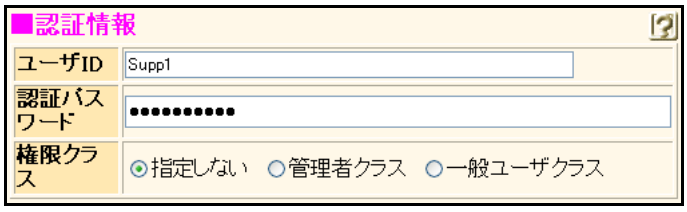
「AAA ユーザ情報（0）」ページが表示されます。

46. **「認証情報」をクリックします。**

認証情報の設定項目と「認証情報」が表示されます。

47. **以下の項目を指定します。**

- ユーザ ID　→ Supp1
- 認証パスワード　→ Supp1-pass



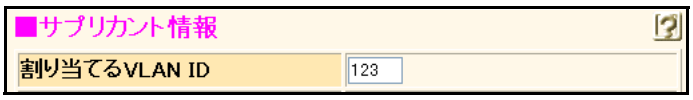
48. **［保存］ボタンをクリックします。**

49. **「サプリカント関連」をクリックします。**

サプリカント関連の設定項目と「サプリカント情報」が表示されます。

50. **以下の項目を指定します。**

- 割り当てる VLAN ID　→ 123



51. **［保存］ボタンをクリックします。**

52. **手順 44. ～ 51. を参考に、以下の項目を設定します。**

「グループ ID 情報（1）」-「AAA ユーザ情報（1）」-「認証情報」-「認証情報」

- ユーザ ID　→ Supp2
- 認証パスワード　→ Supp2-pass

「グループ ID 情報（1）」-「AAA ユーザ情報（1）」-「サプリカント関連」-「サプリカント情報」

- 割り当てる VLAN ID　→ 100

53. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

12 Web 認証機能を使う

適用機種 全機種

Web 認証機能を使用すると、認証が成功した場合のみ外部のネットワークに接続するため、セキュリティを向上させることができます。

参照 マニュアル「機能説明書」

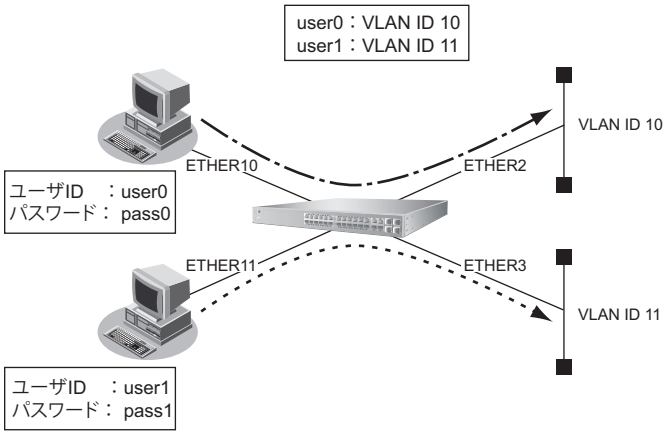
こんな事に気をつけて

- **Web 認証を利用するポートでは、Web 認証機能で用いるための VLAN として、タグなしのポート VLAN だけ指定できます。タグ VLAN およびプロトコル VLAN は設定しないでください。ただし、VLAN タグ付きフレームを認証しないで透過する場合の、タグ VLAN 設定はその限りではありません。**
- **認証用 VLAN への経路を広報しないように経路フィルタを設定してください。**
- **認証用 VLAN から外部へ IP パケットが透過しないように IP フィルタを設定してください。**

12.1 AAA でローカル認証を行う

適用機種 全機種

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER10、11 ポートで Web 認証機能を用いて、AAA グループ ID は 1 を使用する
- ETHER10、11 ポートの認証方法
  ETHER10 ポート ：MAC アドレス
  ETHER11 ポート ：ポート
- 認証プロトコルとして MD5-CHAP を使用する
- 認証用 VLAN の VLAN ID ：500
- 認証用 VLAN の LAN0 の IP アドレス ：192.168.1.0/24
- 認証用 VLAN では DHCP で IP アドレスを割り当てる
  割り当てる IP アドレス ：192.168.1.2/24 から 100 個
  リース期間 ：10 秒
  DNS サーバ IP アドレス ：192.168.1.1（本装置の IP アドレス）

- ログイン画面のリダイレクト動作　：有効
- ログイン画面のリダイレクト動作プロトコル　：HTTPS
- 認証用VLANのLAN0で許可する通信
  送信元IPアドレス　：192.168.1.0/24
  あて先IPアドレス　：192.168.1.1/32
- VLAN ID 10が割り当てられた場合は、ETHER2ポートと通信する
- VLAN ID 11が割り当てられた場合は、ETHER3ポートと通信する
- ユーザuser0とuser1をAAAグループ1に登録する
  user0で割り当てるVLAN ID 10
  user1で割り当てるVLAN ID 11

上記の設定条件に従って設定を行う場合の設定例を示します。

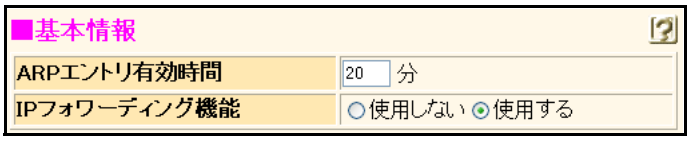
IPフォワーディング機能を有効に設定する

1.　設定メニューの詳細設定で「IP情報」をクリックします。

「IP情報」ページが表示されます。

2.　以下の項目を指定します。

- IPフォワーディング機能　→使用する



3.　［保存］ボタンをクリックします。

Web認証機能を使用するに設定する

4.　設定メニューの詳細設定で「認証情報」をクリックします。

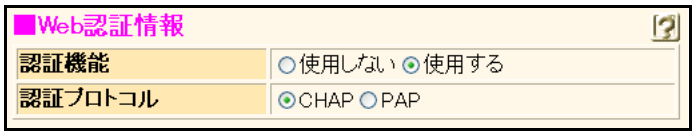
「認証情報」ページが表示されます。

5.　「Web認証情報」をクリックします。

「Web認証情報」が表示されます。

6.　以下の項目を指定します。

- 認証機能　→使用する
- 認証プロトコル　→CHAP



7.　［保存］ボタンをクリックします。

認証用VLANのVIDに500（LAN0）を設定する

8.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

9. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**

「LAN0 情報」ページが表示されます。

10. **「共通情報」をクリックします。**

共通情報の設定項目と「基本情報」が表示されます。

11. **以下の項目を指定します。**

- VLAN ID →500

12. **［保存］ボタンをクリックします。**

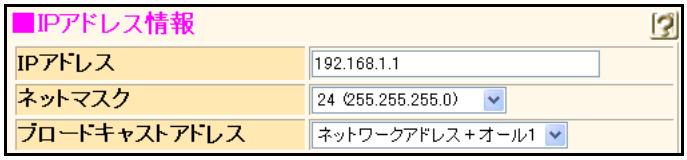
DHCP サーバ機能を設定する

13. **「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

14. **以下の項目を指定します。**

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



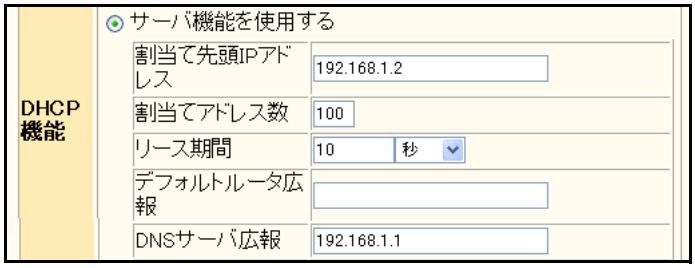
15. **［保存］ボタンをクリックします。**

16. **IP 関連の設定項目の「DHCP 情報」をクリックします。**

「DHCP 情報」が表示されます。

17. **以下の項目を指定します。**

- DHCP 機能 →サーバ機能を使用する
  割当て先頭 IP アドレス →192.168.1.2
  割当てアドレス数 →100
  リース期間 →10 秒
  DNS サーバ広報 →192.168.1.1



18. **［保存］ボタンをクリックします。**

認証ログイン画面のリダイレクト動作を設定する

19.　設定メニューの詳細設定で「認証情報」をクリックします。

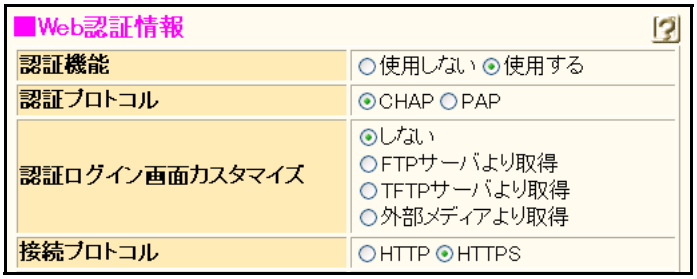
「認証情報」ページが表示されます。

20.　「Web 認証情報」をクリックします。

「Web 認証情報」が表示されます。

21.　以下の項目を設定します。

- 認証機能　→使用する
- 接続プロトコル　→ HTTPS



22.　［保存］ボタンをクリックします。

ETHER10、11 ポートでは STP を使用しない

23.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

24.　以下の項目を設定します。

- ポートリスト　→ 10,11

25.　［修正］ボタンをクリックします。

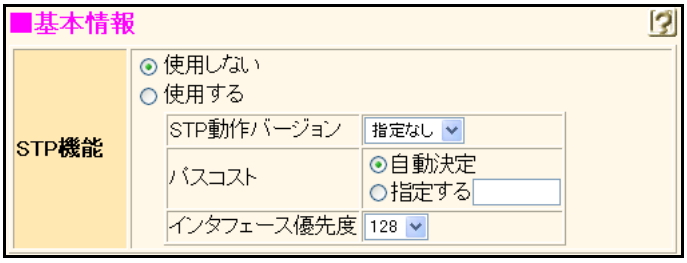
ether 10,11 情報の設定項目と「基本情報」が表示されます。

26.　「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

27.　以下の項目を指定します。

- STP 機能　→使用しない



28.　［保存］ボタンをクリックします。

ETHER10、11 ポートで Web 認証機能を使用する

29. 画面上部の「ether 10,11 情報」をクリックします。

ether 10,11 情報の設定項目と「基本情報」が表示されます。

30. 以下の項目を指定します。

- VLAN
  Untagged →500

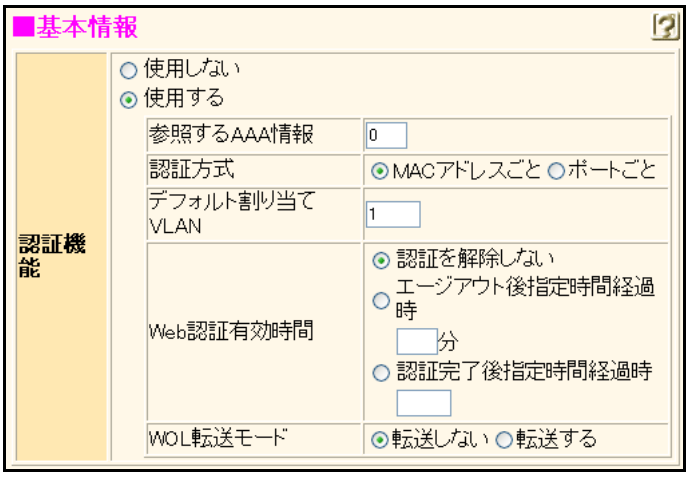
31. ［保存］ボタンをクリックします。

32. 「Web 認証関連」をクリックします。

Web 認証関連の設定項目と「基本情報」が表示されます。

33. 以下の項目を指定します。

- 認証機能 →使用する
  参照する AAA 情報 →0



34. ［保存］ボタンをクリックします。

35. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

36. 「ether 情報」でポート番号が 11 の［修正］ボタンをクリックします。

ether 11 情報の設定項目と「基本情報」が表示されます。

37. 「Web 認証関連」をクリックします。

Web 認証関連の設定項目と「基本情報」が表示されます。

38. 手順 33. ～ 34. を参考に、以下の項目を設定します。

- 認証機能 →使用する
  認証方式 →ポートごと

Web 認証後、VLAN ID が割り当てられたときに通信する ETHER ポートを設定する

39. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

40. 「ether 情報」でポート番号が 2 の［修正］ボタンをクリックします。

ether 2 情報の設定項目と「基本情報」が表示されます。

41. 以下の項目を指定します。

- VLAN
  Untagged →10

42. ［保存］ボタンをクリックします。

43. 手順 39. ～ 42. を参考に、ETHER3 ポートを設定します。

「ether 3 情報」-「基本情報」

- VLAN
  Untagged →11

外部と通信する ETHER ポートを設定する

44. 手順 39. ～ 42. を参考に、ETHER16 ポートを設定します。

「ether 16 情報」-「基本情報」

- VLAN
  Untagged →100

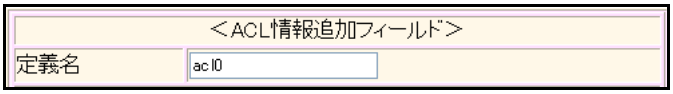
IP フィルタリング機能で使用する ACL 情報を設定する

45. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

46. 以下の項目を指定します。

- 定義名 →acl0



47. ［追加］ボタンをクリックします。

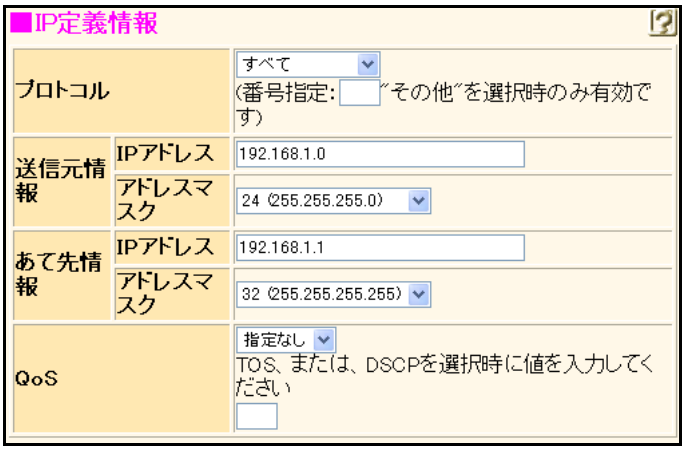
「ACL 定義情報（acl0）」ページが表示されます。

48. 「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

49.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IPアドレス　→192.168.1.1
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



50.　［保存］ボタンをクリックします。

51.　手順45.～50.を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→acl1

「ACL 定義情報（acl1）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→255.255.255.255
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし

「ACL 情報」

- 定義名　→acl2

「ACL 定義情報（acl2）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

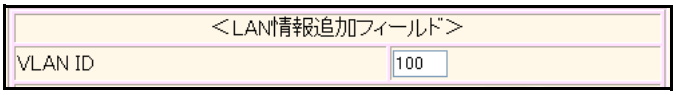
外部と通信するLAN1を設定する

52. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

53. 以下の項目を指定します。

- VLAN ID →100



54. ［追加］ボタンをクリックします。

「LAN1情報」ページが表示されます。

55. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

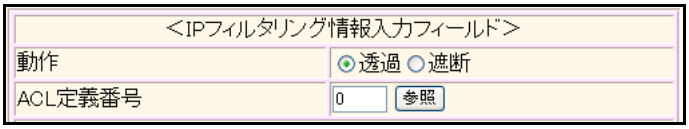
56. IP関連の設定項目の「IPフィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

57. 以下の項目を指定します。

- 動作 →透過
- ACL定義番号 →0

補足 「ACL定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



58. ［追加］ボタンをクリックします。

59. 手順57.～58.を参考に、以下の項目を設定します。

- 動作 →透過
- ACL定義番号 →1

60. 手順57.～58.を参考に、以下の項目を設定します。

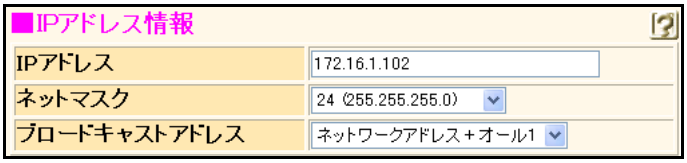
- 動作 →遮断
- ACL定義番号 →2

61. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

62.　以下の項目を指定します。

- IPアドレス　→172.16.1.102
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



63.　［保存］ボタンをクリックします。

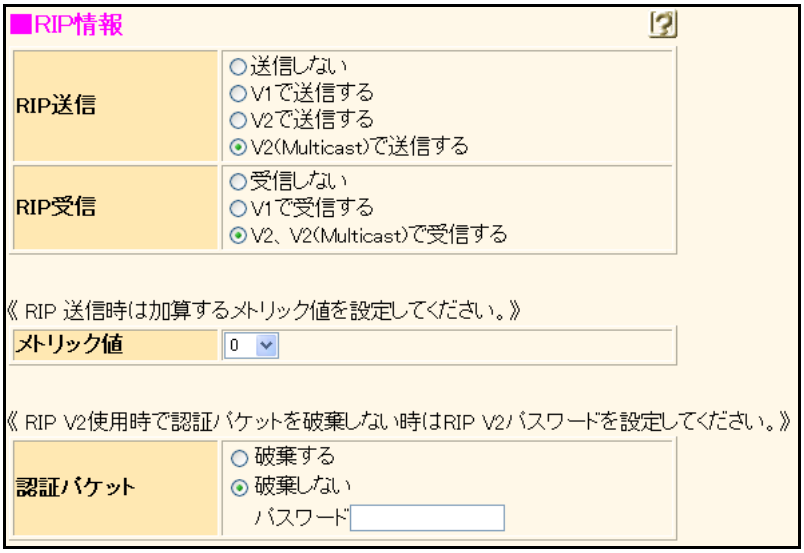
外部と通信するLAN1ではRIPを使用してダイナミックルーティングを行う

64.　IP関連の設定項目の「RIP情報」をクリックします。

「RIP情報」が表示されます。

65.　以下の項目を指定します。

- RIP送信　→V2（Multicast）で送信する
- RIP受信　→V2、V2（Multicast）で受信する
- メトリック値　→0
- 認証パケット　→破棄しない
  パスワード　→指定しない



66.　［保存］ボタンをクリックします

RIPを使用するインタフェースでは認証用VLANの192.168.1.0/24に対する経路を配布しない

67.　設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

68.　「RIP関連」をクリックします。

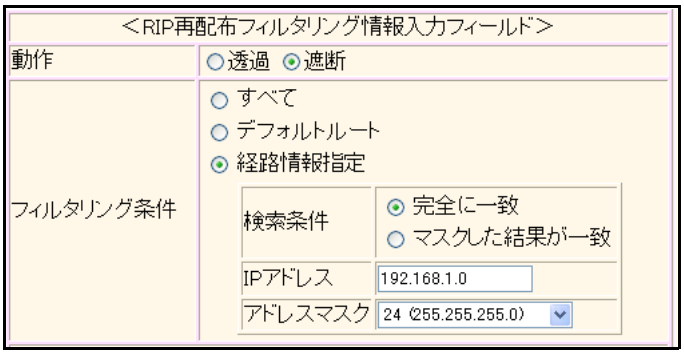
RIP関連の設定項目と「RIPタイマ情報」が表示されます。

69.　「RIP再配布フィルタリング情報」をクリックします。

「RIP再配布フィルタリング情報」が表示されます。

70. 以下の項目を指定します。

- 動作 →遮断
- フィルタリング条件 →経路情報指定
  検索条件 →完全に一致
  IPアドレス →192.168.1.0
  アドレスマスク →24（255.255.255.0）



71. ［追加］ボタンをクリックします

72. 手順70.～71.を参考に、以下の項目を設定します。

- 動作 →透過
- フィルタリング条件 →すべて

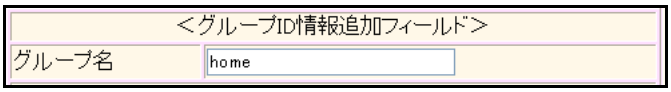
AAA情報を設定する

73. 設定メニューの詳細設定で「AAA情報」をクリックします。

「AAA情報」ページが表示されます。

74. 以下の項目を指定します。

- グループ名 →home



75. ［追加］ボタンをクリックします。

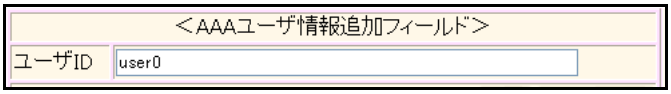
「グループID 情報（0)」ページが表示されます。

76. 「AAAユーザ情報」をクリックします。

AAAユーザ情報の設定項目と「AAAユーザ情報」が表示されます。

77. 以下の項目を指定します。

- ユーザID →user0



78. ［追加］ボタンをクリックします。

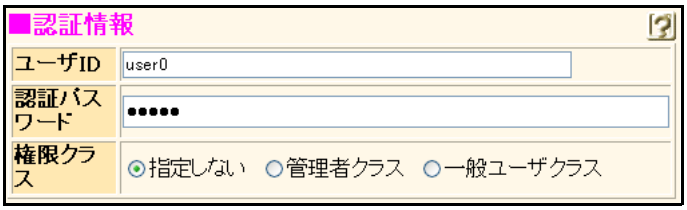
「AAAユーザ情報（0)」ページが表示されます。

79. 「認証情報」をクリックします。

認証情報の設定項目と「認証情報」が表示されます。

80. 以下の項目を指定します。

- ユーザ ID →user0
- 認証パスワード →pass0



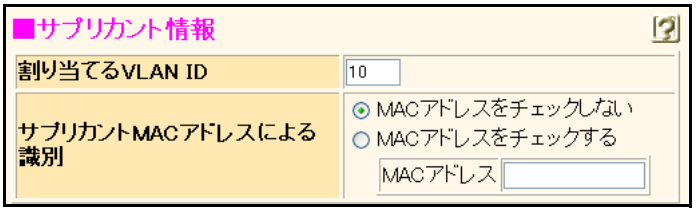
81. ［保存］ボタンをクリックします。

82. 「サプリカント関連」をクリックします。

サプリカント関連の設定項目と「サプリカント情報」が表示されます。

83. 以下の項目を指定します。

- 割り当てる VLAN ID →10
- サプリカント MAC アドレスによる識別 →MAC アドレスをチェックしない



84. ［保存］ボタンをクリックします。

85. 手順 73.～84. を参考に、以下の項目を設定します。

「グループ ID 情報（1）」-「AAA ユーザ情報」-「AAA ユーザ情報」

- ユーザ ID →user1

「AAA ユーザ情報（1）」-「認証情報」-「認証情報」

- ユーザ ID →user1
- 認証パスワード →pass1

「AAA ユーザ情報（1）」「サプリカント関連」-「サプリカント情報」

- 割り当てる VLAN ID →11
- サプリカント MAC アドレスによる識別 →MAC アドレスをチェックしない

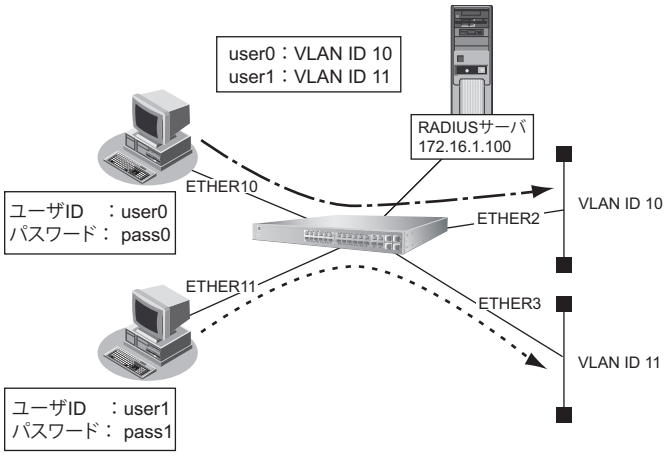
86. 画面左側の［再起動］ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

12.2 AAAでリモート認証を行う

適用機種　全機種

SR-S732TR1の場合を例にします。



● 設定条件

- ETHER10、11ポートでWeb認証機能を用いて、AAAグループIDは1を使用する
- ETHER10、11ポートの認証方法
  ETHER10ポート　：MACアドレス
  ETHER11ポート　：ポート
- RADIUSサーバのIPアドレス　：172.16.1.100
- 認証プロトコルとしてMD5-CHAPを使用する
- 認証用VLANのLAN0のIPアドレス　：192.168.1.0/24
- 認証用VLANではDHCPでIPアドレスを割り当てる
  割り当てるIPアドレス　：192.168.1.2/24から100個
  リース期間　：10秒
  DNSサーバIPアドレス　：192.168.1.1（本装置のIPアドレス）
- ログイン画面のリダイレクト動作　：有効
- ログイン画面のリダイレクト動作プロトコル　：HTTPS
- 認証用VLANのLAN0で許可する通信
  送信元IPアドレス　：192.168.1.0/24
  あて先IPアドレス　：192.168.1.1/32
- 認証成功後にリダイレクトするURL　：http://jp.fujitsu.com/
- 認証成功後にリダイレクトする時間　：15s

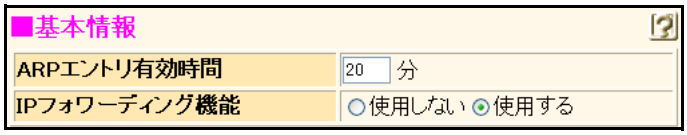
上記の設定条件に従って設定を行う場合の設定例を示します。

IPフォワーディング機能を有効に設定する

1.　設定メニューの詳細設定で「IP情報」をクリックします。

「IP情報」ページが表示されます。

2. **以下の項目を指定します。**
   - IP フォワーディング機能　→使用する



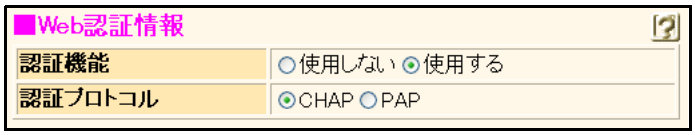
3. **［保存］ボタンをクリックします。**

Web 認証機能を使用する

4. **設定メニューの詳細設定で「認証情報」をクリックします。**
   「認証情報」ページが表示されます。

5. **「Web 認証情報」をクリックします。**
   「Web 認証情報」が表示されます。

6. **以下の項目を指定します。**
   - 認証機能　→使用する
   - 認証プロトコル　→ CHAP



7. **［保存］ボタンをクリックします。**

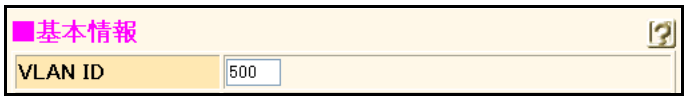
認証用 VLAN の VID に 500 を設定する

8. **設定メニューの詳細設定で「LAN 情報」をクリックします。**
   「LAN 情報」ページが表示されます。

9. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**
   「LAN0 情報」ページが表示されます。

10. **「共通情報」をクリックします。**
    共通情報の設定項目と「基本情報」が表示されます。

11. **以下の項目を指定します。**
    - VLAN ID　→ 500



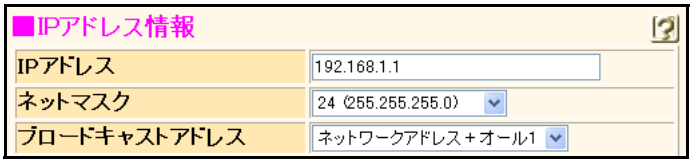
12. **［保存］ボタンをクリックします。**

DHCP サーバ機能を設定する

13. **「IP 関連」をクリックします。**
    IP 関連の設定項目と「IP アドレス情報」が表示されます。

14. 以下の項目を指定します。

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



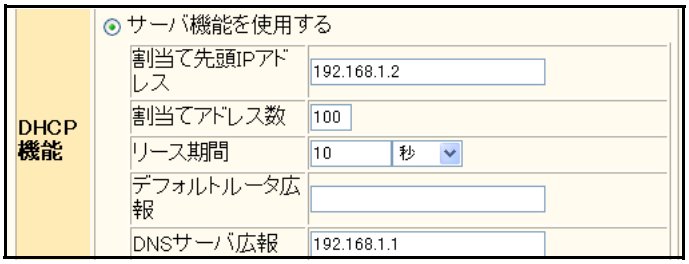
15. ［保存］ボタンをクリックします。

16. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

17. 以下の項目を指定します。

- DHCP 機能 →サーバ機能を使用する
  割当て先頭 IP アドレス →192.168.1.2
  割当てアドレス数 →100
  リース期間 →10 秒
  DNS サーバ広報 →192.168.1.1



18. ［保存］ボタンをクリックします。

認証ログイン画面のリダイレクト動作を設定する

19. 設定メニューの詳細設定で「認証情報」をクリックします。

「認証情報」ページが表示されます。

20. 「Web 認証情報」をクリックします。

「Web 認証情報」が表示されます。

21. 以下の項目を設定します。

- 認証機能 →使用する
- 接続プロトコル →HTTPS
- 認証成功後のリダイレクトURL →http://jp.fujitsu.com/
- 認証成功後のリダイレクト時間 →15秒

22. ［保存］ボタンをクリックします。

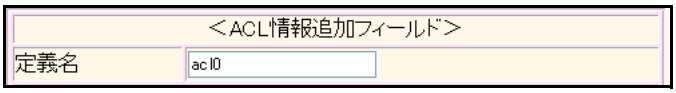
IP フィルタリング機能を設定する

23. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

24. 以下の項目を指定します。

- 定義名 →acl0



25. ［追加］ボタンをクリックします。

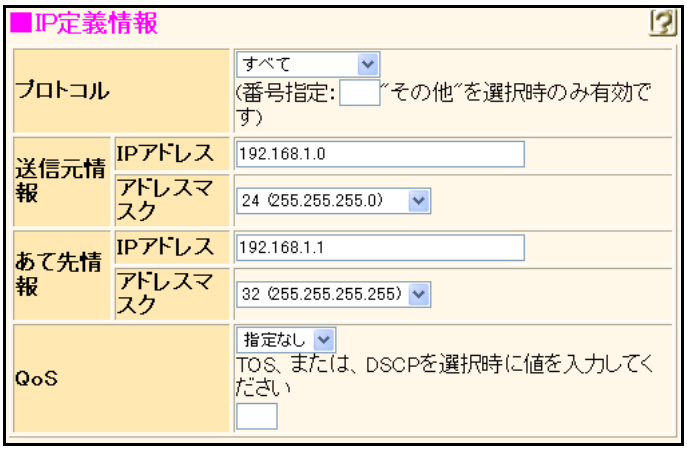
「ACL 定義情報（acl0）」ページが表示されます。

26. 「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

27.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IPアドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IPアドレス　→192.168.1.1
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



28.　［保存］ボタンをクリックします。

29.　手順23.～28.を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→acl1

「ACL 定義情報（acl1）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→255.255.255.255
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし

「ACL 情報」

- 定義名　→acl2

「ACL 定義情報（acl2）」-「IP 定義情報」

- プロトコル　→すべて
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

ETHER10、11 ポートでは STP を使用しない

30. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

31. 以下の項目を設定します。

- ポートリスト　→ 10,11

32. ［修正］ボタンをクリックします。

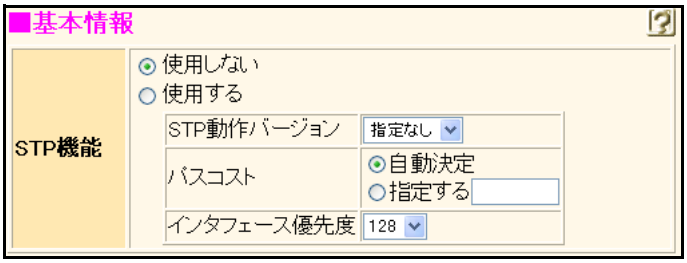
ether 10,11 情報の設定項目と「基本情報」が表示されます。

33. 「STP 関連」をクリックします。

STP 関連の設定項目と「基本情報」が表示されます。

34. 以下の項目を指定します。

- STP 機能　→使用しない



35. ［保存］ボタンをクリックします。

ETHER10、11 ポートで Web 認証機能を使用する

36. 画面上部の「ether 10,11 情報」をクリックします。

ether 10,11 情報の設定項目と「基本情報」が表示されます。

37. 以下の項目を指定します。

- VLAN
  Untagged　→ 500

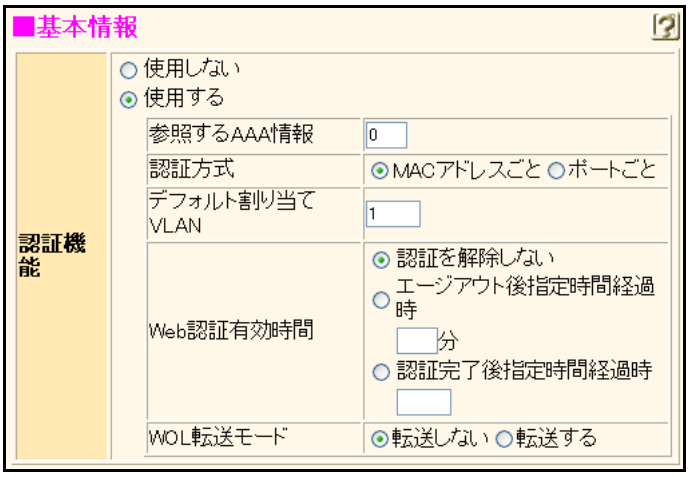
38. ［保存］ボタンをクリックします。

39. 「Web 認証関連」をクリックします。

Web 認証関連の設定項目と「基本情報」が表示されます。

40. 以下の項目を指定します。

- 認証機能　→使用する
  参照する AAA 情報　→ 0



41. ［保存］ボタンをクリックします。

42. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

43. 「ether 情報」でポート番号が 11 の［修正］ボタンをクリックします。

ether 11 情報の設定項目と「基本情報」が表示されます。

44. 「Web 認証関連」をクリックします。

Web 認証関連の設定項目と「基本情報」が表示されます。

45. 手順 39. ～ 41. を参考に、以下の項目を設定します。

- 認証機能　→使用する
  認証方式　→ポートごと

Web 認証後、VLAN ID が割り当てられたときに通信する ETHER ポートを設定する

46. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

47. 「ether 情報」でポート番号が 2 の［修正］ボタンをクリックします。

ether 2 情報の設定項目と「基本情報」が表示されます。

48. 以下の項目を指定します。

- VLAN
  Untagged　→ 10

49. ［保存］ボタンをクリックします。

50. 手順 46. ～ 49. を参考に、ETHER3 ポートを設定します。

- VLAN
  Untagged　→ 11

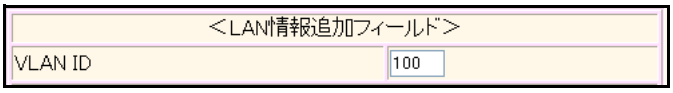
LAN1 を VLAN ID 100 に割り当てる

51. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

52. 以下の項目を指定します。

- VLAN ID →100



53. ［追加］ボタンをクリックします。

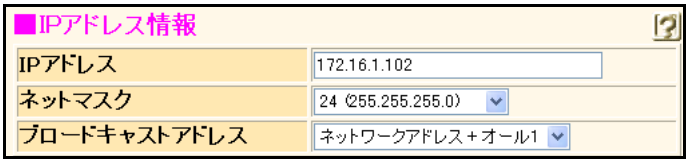
「LAN1 情報」ページが表示されます。

54. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

55. 以下の項目を指定します。

- IP アドレス →172.16.1.102
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1



56. ［保存］ボタンをクリックします。

フィルタリング動作を定義する

57. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

59. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

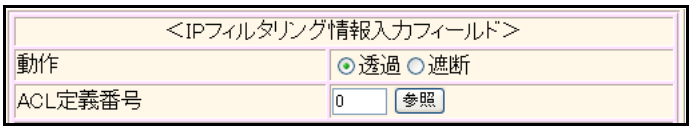
60. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

61. 以下の項目を指定します。

- 動作　→透過
- ACL 定義番号　→ 0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



62. ［追加］ボタンをクリックします。

63. 手順 61.～62. を参考に、以下の項目を設定します。

- 動作　→透過
- ACL 定義番号　→ 1

64. 手順 61.～62. を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL 定義番号　→ 2

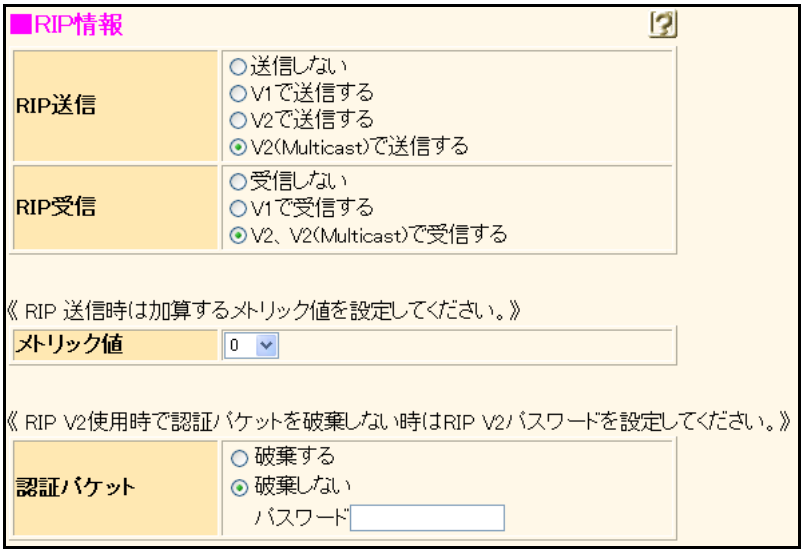
外部と通信する LAN1 では RIP を使用してダイナミックルーティングを行う

65. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

66. 以下の項目を指定します。

- RIP 送信　→ V2（Multicast）で送信する
- RIP 受信　→ V2、V2（Multicast）で受信する
- メトリック値　→ 0
- 認証パケット　→破棄しない
  パスワード　→指定しない



67. ［保存］ボタンをクリックします。

RIP を使用するインタフェースでは認証用 VLAN の 192.168.1.0/24 に対する経路を配布しない

68.　設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

69.　「RIP 関連」をクリックします。

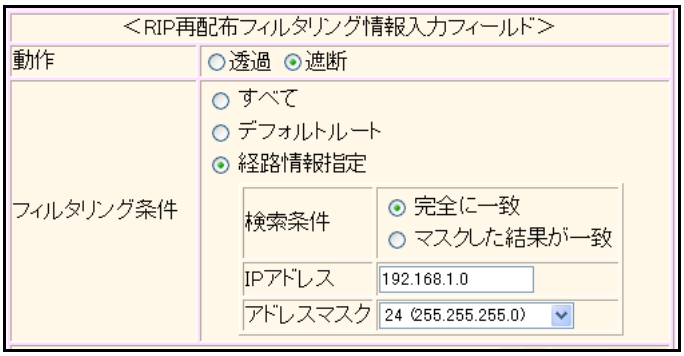
RIP 関連の設定項目と「RIP タイマ情報」が表示されます。

70.　「RIP 再配布フィルタリング情報」をクリックします。

「RIP 再配布フィルタリング情報」が表示されます。

71.　以下の項目を指定します。

- 動作　→遮断
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）



72.　［追加］ボタンをクリックします

73.　手順 71.～72. を参考に、以下の項目を設定します。

- 動作　→透過
- フィルタリング条件　→すべて

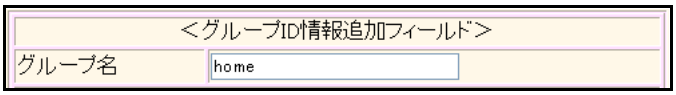
AAA 情報を設定する

74.　設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

75.　以下の項目を指定します。

- グループ名　→ home



76.　［追加］ボタンをクリックします。

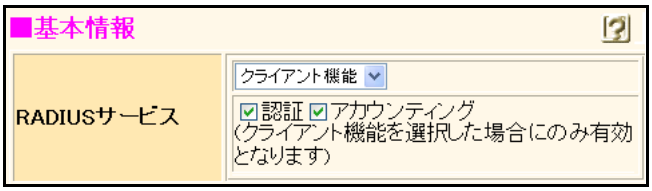
「グループ ID 情報（0）」ページが表示されます。

77.　「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

78. 以下の項目を指定します。

- RADIUS サービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックする



79. ［保存］ボタンをクリックします。

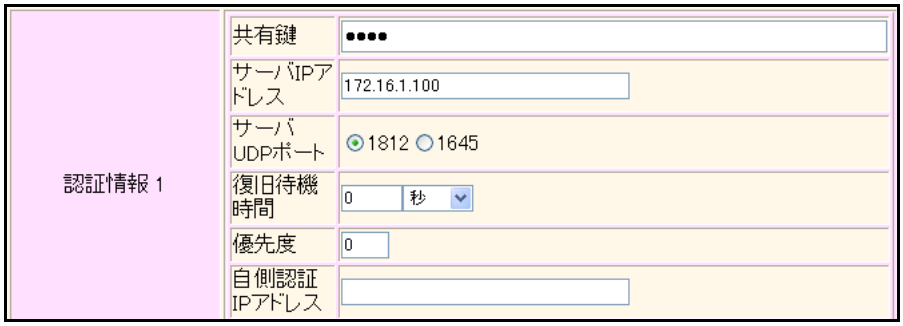
80. RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

81. 「認証情報 1」の［修正］ボタンをクリックします。

82. 以下の項目を指定します。

- 認証情報 1
  共有鍵　→ test
  サーバ IP アドレス　→ 172.16.1.100



83. 認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

84. 画面左側の［再起動］ボタンをクリックします。

本装置の再起動後、設定した内容が有効になります。

12.3 認証ログイン画面のカスタマイズを行う

適用機種　全機種

こんな事に気をつけて

- **カスタマイズされた画面は装置起動時にダウンロードされます。また webauthctl コマンドにて運用中に更新することも可能です。**
- **カスタマイズする画面ファイルは以下の弊社ホームページよりサンプルファイルを取得し利用ください。**

参照 URL: http://fenics.fujitsu.com/products/download/sr-s/firm/

● 設定条件

- カスタマイズ認証ログイン画面の取得先　：FTP サーバ
- FTP サーバの IP アドレス　：172.16.1.100
- FTP サーバのユーザ ID　：user-id
- FTP サーバのユーザパスワード　：user-pass
- カスタマイズするログイン画面ファイル　：/webauth/login.html
- カスタマイズするロゴ画像ファイル　：/webauth/logo.gif

上記の設定条件に従って設定を行う場合のコマンド例を示します。

補足 ここでは認証動作の設定は省略します。
認証動作の設定については、「12.1 AAA でローカル認証を行う」（P.111）「12.2 AAA でリモート認証を行う」（P.122）、を参照してください。

1. 設定メニューの詳細設定で「認証情報」をクリックします。

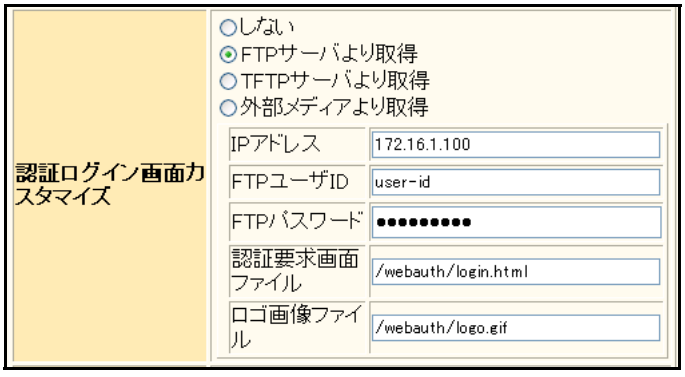
「認証情報」ページが表示されます。

2. 「Web 認証情報」をクリックします。

「Web 認証情報」が表示されます。

3. 以下の項目を設定します。

- 認証ログイン画面カスタマイズ →FTP サーバより取得
  IP アドレス →172.16.1.100
  FTP ユーザ ID →user-id
  FTP パスワード →user-pass
  認証要求画面ファイル →/webauth/login.html
  ロゴ画像ファイル →/webauth/logo.gif



4. **［保存］ボタンをクリックします。**

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

13　MACアドレス認証機能を使う

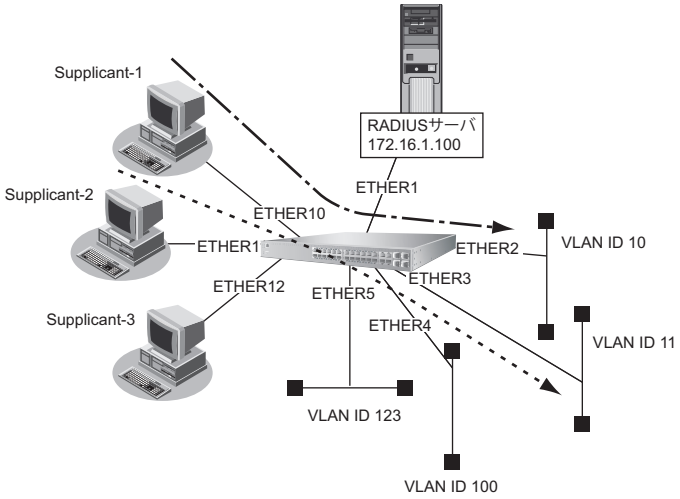
適用機種　全機種

MACアドレス認証機能を使用すると、本装置に接続する端末がネットワークへのアクセス権限を持っているかを認証することができます。

こんな事に気をつけて

- **MACアドレス認証を利用するポートでは、事前にVLANを設定できません。ただし、以下の場合はその限りではありません。**
  - **Web認証機能が併用されている場合の、Web認証用のタグなしのポートVLAN設定**
  - **VLANタグ付きフレームを認証しないで透過する場合の、タグVLAN設定**
- **MACアドレス認証で利用するAAAのグループIDを正しく設定してください。**

SR-S332TR1の場合を例にします。



● 設定条件

- ETHER10～12ポートでMACアドレス認証を使用する
- ETHER10～12ポートで利用する認証データベース
  ETHER10、11ポート　：RADIUSサーバ
  ETHER12ポート　：ローカルで設定した認証情報
- AAAグループID
  ETHER10、11ポート　：0
  ETHER12ポート　：1
- SupplicantのMACアドレスごとに認証を行う
- ETHER12ポートで利用可能なユーザは以下のとおり

MACアドレス	割り当てるVLAN ID
00:11:11:00:00:01	VLAN123
00:22:22:00:00:02	VLAN100

- RADIUSサーバのIPアドレス　：172.16.1.100
- RADIUSサーバはVLAN13に接続されている
- RADIUSサーバのシークレット　：radius-secret
- 認証プロトコルとしてMD5-CHAPを使用する

こんな事に気をつけて

- RADIUS サーバにはユーザに VLAN ID を割り当てるために以下の属性を設定してください。設定方法については RADIUS サーバのマニュアルを参照してください。

名前	番号	属性値（※）
Tunnel-Type	64	VLAN（13）
Tunnel-Media-Type	65	802（6）
Tunnel-Private-Group-ID	81	VLAN ID（10 進数表記を ASCII コードでコーディング）

※）（）内の数字は属性として設定される 10 進数の値

- タグにより複数のトンネル属性が設定されている場合は、利用可能な値が指定されているもっとも小さなタグの情報がユーザに割り当てる VLAN 情報として選択されます。

上記の設定条件に従って設定を行う場合の設定例を示します。

MAC アドレス認証を設定する

1. 設定メニューの詳細設定で「認証情報」をクリックします。

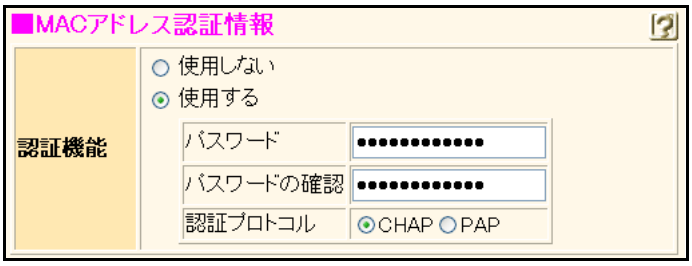
「認証情報」ページが表示されます。

2. 「MAC アドレス認証情報」をクリックします。

「MAC アドレス認証情報」が表示されます。

3. 以下の項目を指定します。

- 認証機能 →使用する
  パスワード →macauth-pass
  パスワードの確認 →macauth-pass
  認証プロトコル →CHAP



4. ［保存］ボタンをクリックします。

RADIUS サーバの VLAN を設定する

5. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

6. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

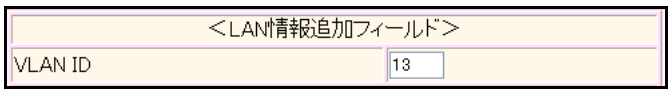
「LAN0 情報」ページが表示されます。

7. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

8.　以下の項目を指定します。

- VLAN ID　→13



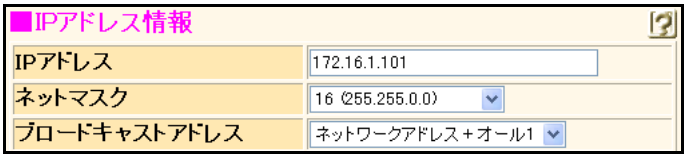
9.　［保存］ボタンをクリックします。

10.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

11.　以下の項目を設定します。

- IP アドレス　→172.16.1.101
- ネットマスク　→16（255.255.0.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1



12.　［保存］ボタンをクリックします。

RADIUS サーバを接続するポートを設定する

13.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

14.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

15.　以下の項目を設定します。

- VLAN
  Untagged　→13

16.　［保存］ボタンをクリックします。

MAC アドレス認証で認証された Supplicant が接続される VLAN 情報を設定する

17.　手順 13.～16. を参考に、ETHER2～5 ポートを設定します。

「ether 2 情報」-「基本設定」

- VLAN
  Untagged　→10

「ether 3 情報」-「基本設定」

- VLAN
  Untagged　→11

「ether 4 情報」-「基本設定」

- VLAN
  Untagged　→ 100

「ether 5 情報」-「基本設定」

- VLAN
  Untagged　→ 123

MAC アドレス認証ポートを設定する

18. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

19. 「ether 情報」でポート番号が 10 の［修正］ボタンをクリックします。

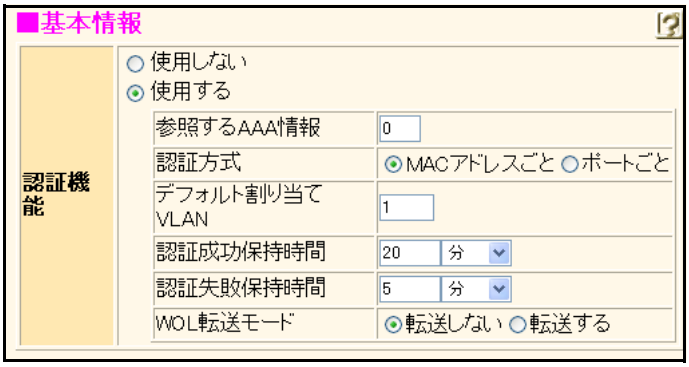
ether 10 情報の設定項目と「基本情報」が表示されます。

20. 「MAC アドレス認証関連」をクリックします。

MAC アドレス認証関連の設定項目と、「基本情報」が表示されます。

21. 以下の項目を設定します。

- 認証機能　→使用する
  参照する AAA 情報　→ 0



22. ［保存］ボタンをクリックします。

23. 手順 18. ～ 22. を参考に、ETHER11、12 ポートを設定します。

「ether 11 情報」-「MAC アドレス認証関連」-「基本情報」

- 認証機能　→使用する
  参照する AAA 情報　→ 0

「ether 12 情報」-「MAC アドレス認証関連」-「基本情報」

- 認証機能　→使用する
  参照する AAA 情報　→ 1

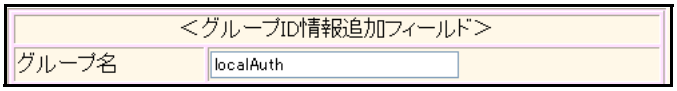
RADIUS サーバを利用する AAA グループ情報を設定する

24. 設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

25. 以下の項目を指定します。

- グループ名　→localAuth



26. ［追加］ボタンをクリックします。

27. 手順24.～25.を参考に、グループ名を設定します。

- グループ名　→radiusAuth

28. ［追加］ボタンをクリックします。

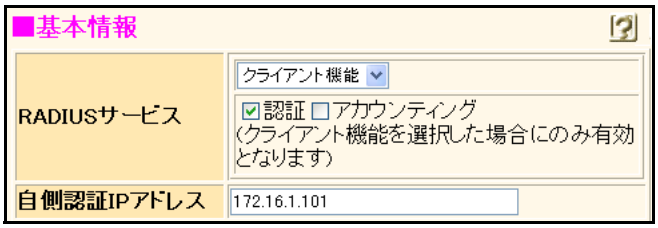
「グループID情報（1）」ページが表示されます。

29. 「RADIUS関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

30. 以下の情報を指定します。

- RADIUSサービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックしない
- 自側認証IPアドレス　→172.16.1.101



31. ［保存］ボタンをクリックします。

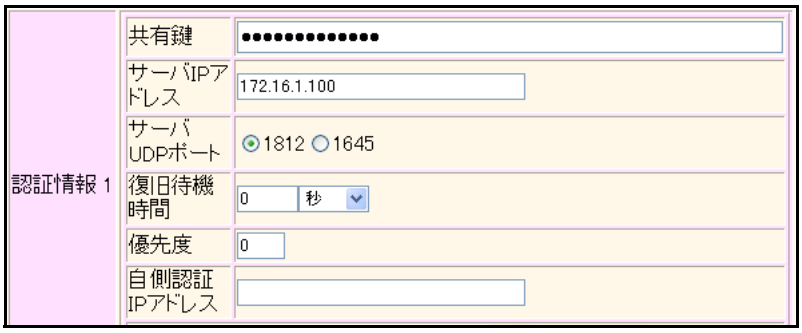
32. RADIUS関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

33. 「認証情報1」の［修正］ボタンをクリックします。

34. 以下の項目を指定します。

- 認証情報1
  共有鍵　→radius-secret
  サーバIPアドレス　→172.16.1.100



35. 認証情報 1 の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

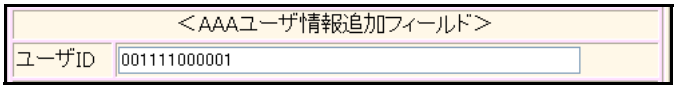
ローカル認証情報を利用する AAA グループ情報を設定する

36. 「AAA ユーザ情報」をクリックします。

AAA ユーザ情報の設定項目と「AAA ユーザ情報」が表示されます。

37. 以下の項目を指定します。

- ユーザ ID　→ 001111000001



38. ［追加］ボタンをクリックします。

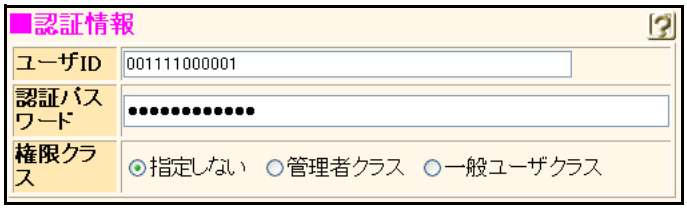
「AAA ユーザ情報（0）」ページが表示されます。

39. 「認証情報」をクリックします。

認証情報の設定項目と「認証情報」が表示されます。

40. 以下の項目を設定します。

- ユーザ ID　→ 001111000001
- 認証パスワード　→ macauth-pass



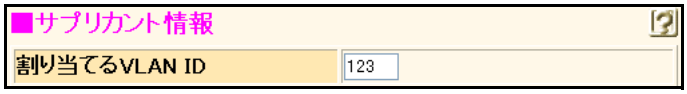
41. ［保存］ボタンをクリックします。

42. 「サプリカント関連」をクリックします。

サプリカント関連の設定項目と「サプリカント情報」が表示されます。

43. 以下の項目を設定します。

- 割り当てる VLAN ID　→ 123



44. ［保存］ボタンをクリックします。

45. 手順 36. ～ 44. を参考に、以下の項目を設定します。

「AAA ユーザ情報（1）」-「認証情報」-「認証情報」

- ユーザ ID　→ 002222000002
- 認証パスワード　→ macauth-pass

「AAA ユーザ情報（1）」-「サプリカント関連」-「サプリカント情報」

- 割り当てる VLAN ID　→ 100

46. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

14　接続端末数制限機能を使う

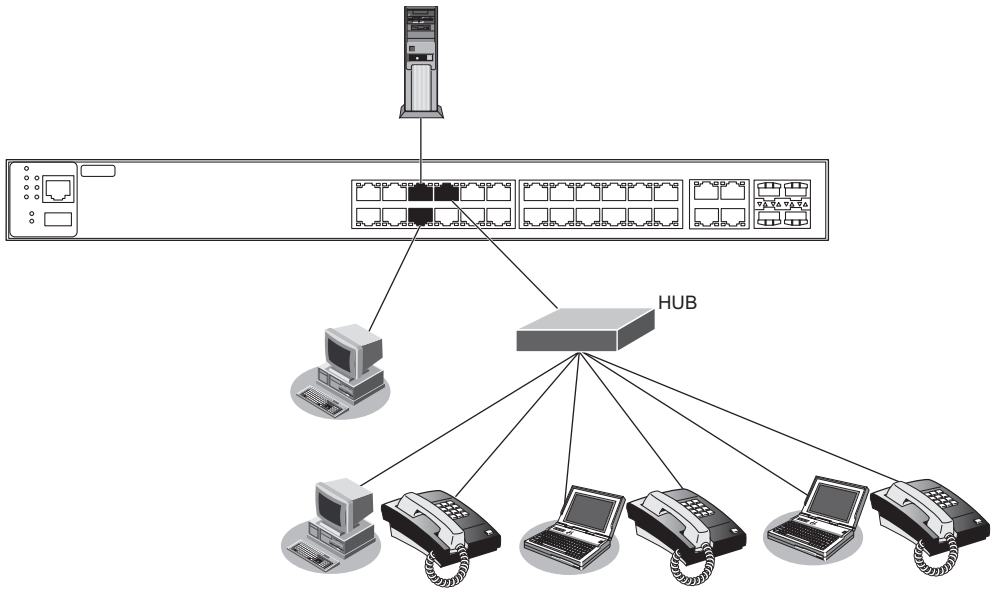
適用機種　全機種

接続端末数制限機能を使用すると、簡易的に本装置への不正接続を検出することができます。

こんな事に気をつけて

- **本機能は、不正接続を検出する機能であり、不正接続とみなした端末に対する通信の遮断は行いません。不正な接続を検出した際に通信を遮断したい場合はポート閉塞モードを有効にしてください。**
- **IEEE802.1X 認証、Web 認証および MAC アドレス認証のどれかを有効にしたポートでは、本機能は無効となります。**
- **リンクアグリゲーションとして設定されたポートでは、本機能は無効となります。**

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER5～7 ポートで接続端末数制限機能を使用する
- 接続許容端末数
  ETHER5、6 ポート　：1
  ETHER7 ポート　：6
- ポート閉塞モード
  ETHER5、6 ポート　：閉塞する
  ETHER7 ポート　：閉塞しない

上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 5 の［修正］ボタンをクリックします。

ether 5 情報の設定項目と「基本情報」が表示されます。

3.　「MAC 関連」をクリックします。

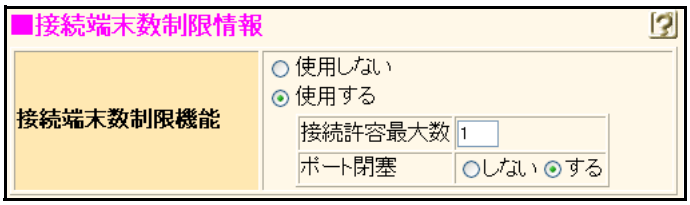
MAC 関連の設定項目と「ストーム制御情報」が表示されます。

4. MAC 関連の設定項目の「接続端末数制限情報」をクリックします。

「接続端末数制限情報」が表示されます。

5. 以下の項目を指定します。

- 接続端末数制限機能　→使用する
  接続許容最大数　→1
  ポート閉塞　→する



6. ［保存］ボタンをクリックします。

7. 手順 1.～6. を参考に、ETHER6、7 ポートを設定します。

「ether 6 情報」-「MAC 関連」-「接続端末数制限」

- 接続端末数制限機能　→使用する
  接続許容最大数　→1
  ポート閉塞　→する

「ether 7 情報」-「MAC 関連」-「接続端末数制限」

- 接続端末数制限機能　→使用する
  接続許容最大数　→6
  ポート閉塞　→しない

8. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

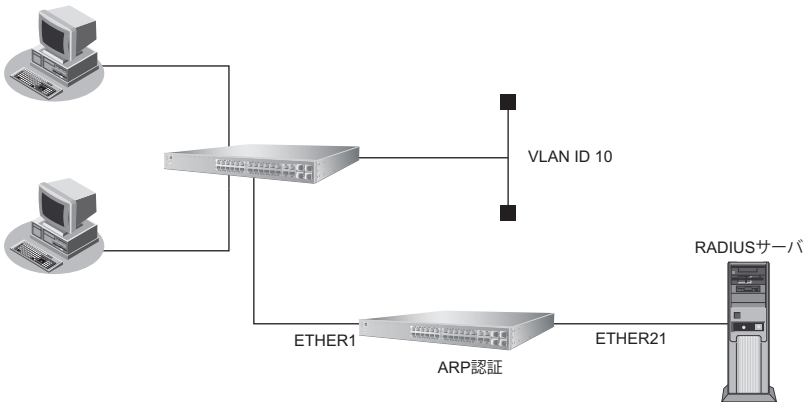
15　ARP 認証機能を使う

適用機種　全機種

ここでは、既存のネットワークに本装置を追加して、ARP 認証を行う場合の設定方法を説明します。

こんな事に気をつけて

ARP 認証で利用する AAA のグループ ID を正しく設定してください。



SR-S332TR1 の場合を例にします。

● 設定条件

- VLAN10 で ARP 認証を使用する
- ARP 認証で利用する認証データベース　：RADIUS サーバ
- AAA グループの ID　：0
- RADIUS サーバの IP アドレス　：172.16.1.100
- RADIUS サーバは VLAN20 に接続されている
- RADIUS サーバのシークレット　：radius-secret
- 認証失敗時の通信妨害を行う
- 通信妨害のための ARP パケット送信間隔　：10 秒

上記の設定条件に従って設定を行う場合の設定例を示します。

RADIUS サーバの VLAN を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- VLAN ID　→20

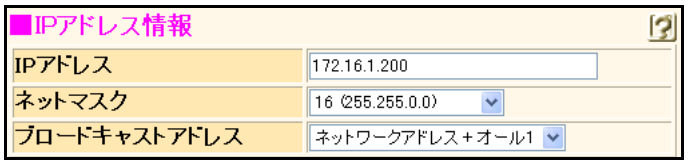
5.　［保存］ボタンをクリックします。

6.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

7.　以下の項目を指定します。

- IP アドレス　→172.16.1.200
- ネットマスク　→16（255.255.0.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1



8.　［保存］ボタンをクリックします。

RADIUS サーバを接続するポートを設定する

9.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

10.　「ether 情報」でポート番号が 21 の［修正］ボタンをクリックします。

ether 21 情報の設定項目と「基本情報」が表示されます。

11.　以下の項目を指定します。

- VLAN
  Untagged　→20

12.　［保存］ボタンをクリックします。

ARP 認証が動作する VLAN を設定する

13.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

14.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

- VLAN
  Untagged →10

16. ［保存］ボタンをクリックします。

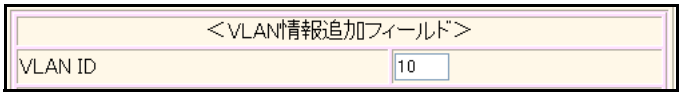
ARP 認証を設定する

17. 設定メニューの詳細設定で「VLAN 情報」をクリックします。

「VLAN 情報」ページが表示されます。

18. 以下の項目を指定します。

- VLAN ID →10



19. ［追加］ボタンをクリックします。

「VLAN10 情報」ページが表示されます。

20. 「ARP 認証関連」をクリックします。

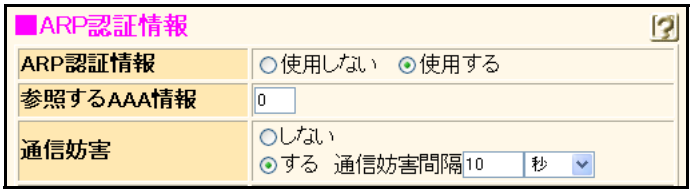
ARP 認証関連の設定項目と、「ARP 認証情報」が表示されます。

21. 以下の項目を指定します。

- ARP 認証情報 →使用する

“ 使用する ” を選択すると、「参照する AAA 情報」および「通信妨害」の設定項目が表示されます。

- 参照する AAA 情報 →0
- 通信妨害 →する
  通信妨害間隔 →10 秒



22. ［保存］ボタンをクリックします。

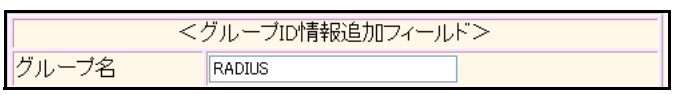
RADIUS サーバを利用する AAA グループ情報を設定する

23. 設定メニューの詳細設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

24. 以下の項目を指定します。

- グループ名 →RADIUS



25.　［追加］ボタンをクリックします。

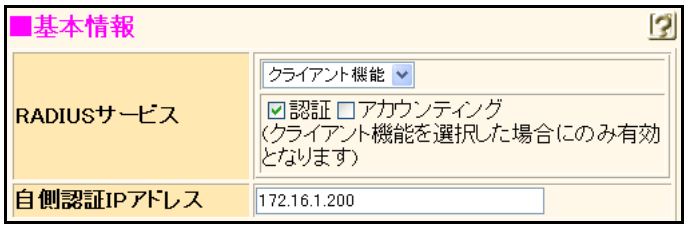
「グループID情報（0）」ページが表示されます。

26.　「RADIUS関連」をクリックします。

RADIUS関連の設定項目と「基本情報」が表示されます。

27.　以下の情報を指定します。

- RADIUSサービス　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックしない
- 自側認証IPアドレス　→172.16.1.200



28.　［保存］ボタンをクリックします。

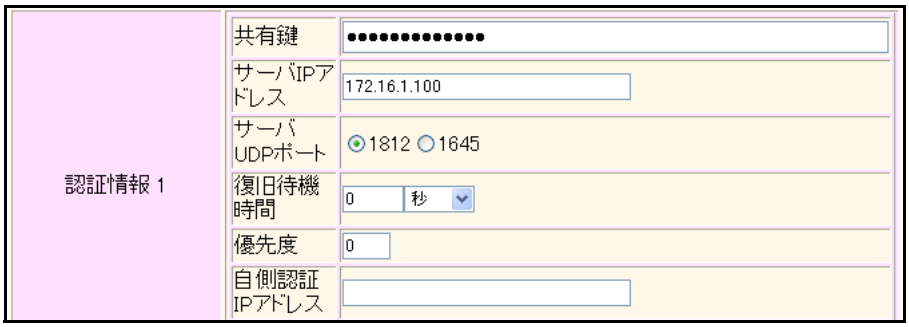
29.　RADIUS関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報（クライアント機能）」が表示されます。

30.　「認証情報1」の［修正］ボタンをクリックします。

31.　以下の項目を指定します。

- 認証情報1
  共有鍵　→radius-secret
  サーバIPアドレス　→172.16.1.100



32.　認証情報1の［保存］ボタンをクリックします。

「サーバ情報（クライアント機能）」に戻ります。

33.　画面左側の［設定反映］ボタンをクリックします。

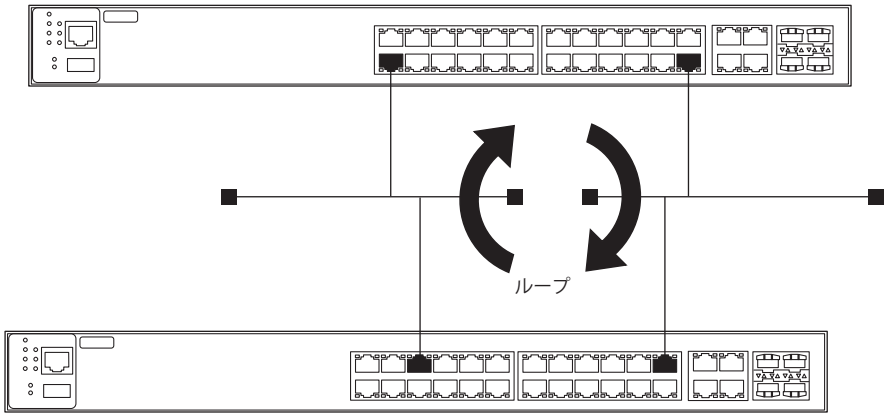
設定した内容が有効になります。

16　ループ検出機能を使う

適用機種　全機種

ループ検出機能を利用すると、ネットワーク上でのパケットのループを防止するためにループ検出およびループしているポートを閉鎖または論理的に遮断することができます。

ここではループ検出機能の設定方法を説明します。



● 設定条件

- ループ検出機能を有効にする
- ポート閉塞を行う
- ループ検出用フレームの送信間隔　：1 分

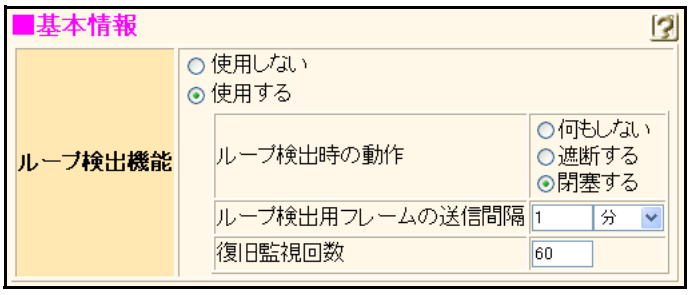
上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「ループ検出情報」をクリックします。

「ループ検出情報」ページが表示されます。

2.　以下の項目を指定します。

- ループ検出機能　→使用する
  ループ検出時の動作　→閉塞する
  ループ検出用フレームの送信間隔　→1 分



3.　［保存］ボタンをクリックします。

4.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

こんな事に気をつけて

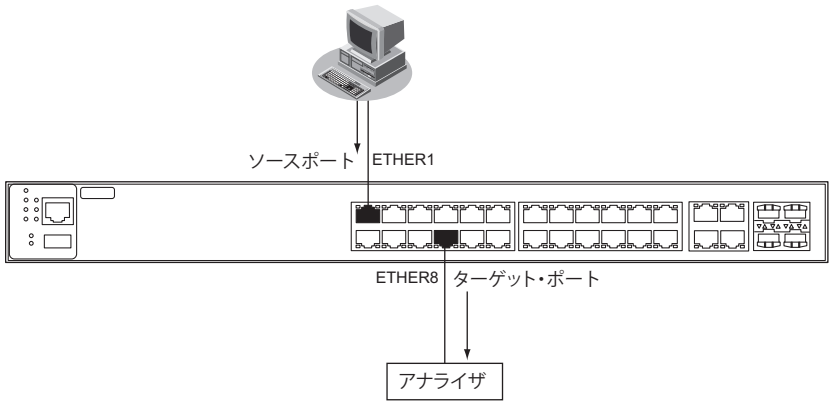
- 閉塞されたポートは自動では復旧しません。ポートが閉塞された状態から閉塞を解除させたい場合は、「操作メニュー」の「閉塞／閉塞解除」を使用してポート閉塞を解除してください。
- トラフィックが高負荷状態になった場合、ループを検出することができません。ブロードキャスト／マルチキャストストーム制御を併用してください。
- STP 機能が有効なポートでは、ループ検出時にポートを論理的に遮断する指定はできません。

17　ポート・ミラーリング機能を使う

適用機種　全機種

ポート・ミラーリング機能を利用すると、指定したターゲット・ポートから、指定したソースポートの受信／送信／送受信トラフィックを監視することができます。

ここでは、ETHER1 ポートをソースポート、ETHER8 ポートをターゲット・ポートとして設定し、ソースポートの受信トラフィックをターゲット・ポートへミラーリングする場合の設定方法を説明します。



● 設定条件

- ETHER1 ポートをソースポートとする（受信フレーム指定）
- ETHER8 ポートをターゲット・ポートとする

上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 8 の［修正］ボタンをクリックします。

ether 8 情報の設定項目と「基本情報」が表示されます。

3.　「ポート種別情報」をクリックします。

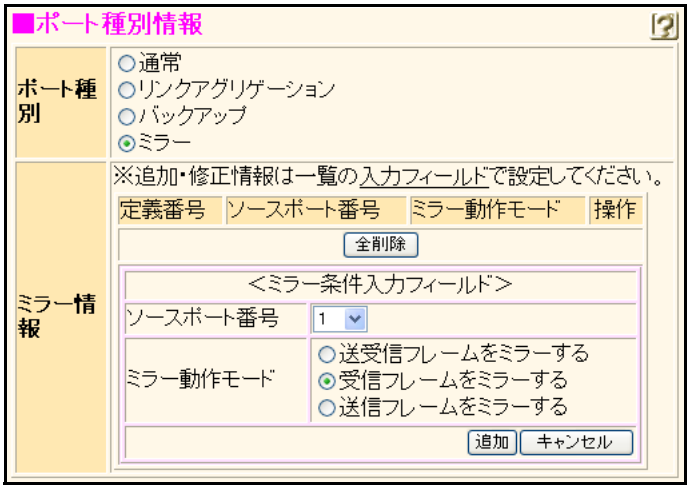
「ポート種別情報」が表示されます。

4.　以下の項目を指定します。

- ポート種別　→ミラー

“ミラー”を選択すると、「ミラー情報」の設定項目が表示されます。

- ミラー情報
  ソースポート番号　→1
  ミラー動作モード　→受信フレームをミラーする



5.　［追加］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

18　ether L3 監視機能を使う

適用機種　全機種

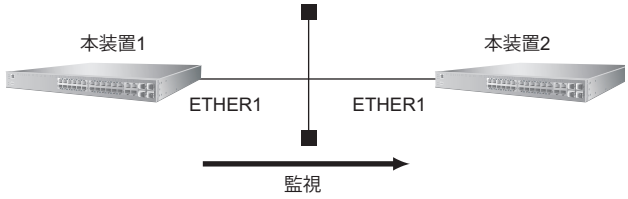
ether L3 監視機能を使用すると、指定した ETHER ポートから監視相手装置を監視することによって、経路上の障害を検出および監視をしているポートを閉塞します。

ここでは、ether L3 監視機能を使用する場合の設定方法を説明します。

こんな事に気をつけて

閉塞されたポートは自動では復旧しません。ポートが閉塞された状態から閉塞を解除させたい場合は、「操作メニュー」の「閉塞／閉塞解除」を使用してポート閉塞を解除してください。

SR-S332TR1 の場合を例にします。



● 設定条件

- ETHER1 ポートを使用する
- VLAN ID とネットワークアドレスを以下のように対応付ける
  VLAN ID：1　　ネットワークアドレス：192.168.10.0/24
- ether L3 監視機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

3.　以下の項目を指定します。

- VLAN
  Untagged　　→ 1

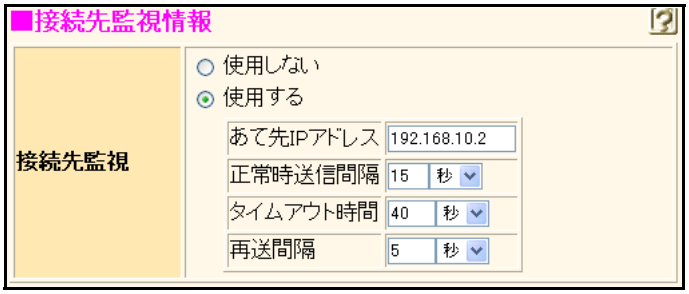
4.　［保存］ボタンをクリックします。

5.　「接続先監視情報」をクリックします。

「接続先監視情報」ページが表示されます。

6.　以下の項目を指定します。

- 接続先監視　→使用する
  あて先 IP アドレス　→ 192.168.10.2
  正常時送信間隔　→ 15 秒
  タイムアウト時間　→ 40 秒
  再送間隔　→ 5 秒



7.　［保存］ボタンをクリックします。

8.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

9.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

10.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

11.　以下の項目を指定します。

- VLAN ID　→ 1

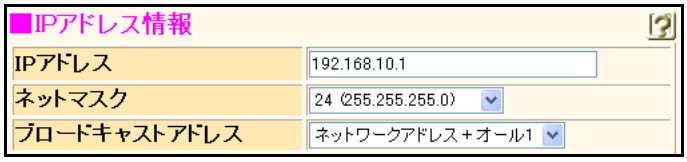
12.　［保存］ボタンをクリックします。

13.　［IP 関連］をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

14.　以下の項目を指定します。

- IP アドレス　→ 192.168.10.1
- ネットマスク　→ 24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1



15.　［保存］ボタンをクリックします。

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ether情報」

「ether 1情報」-「基本情報」

- VLAN
  Untagged →1

「LAN情報」

「LAN0情報」-「共通情報」-「基本情報」

- VLAN ID →1

「LAN0情報」-「IP関連」-「IPアドレス情報」

- IPアドレス →192.168.10.2
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール1

18.1 リンクアグリゲーション機能を使用したether L3監視機能を使う

適用機種 全機種

ここでは、リンクアグリゲーション機能を利用したポートでether L3監視機能を使用する場合の設定方法を説明します。

SR-S332TR1の場合を例にします。

● 設定条件

- ETHER1～4ポートを使用する
- 通信速度を1000Mbps固定に変更する
- VLAN IDとネットワークアドレスを以下のように対応付ける
  VLAN ID：10　　ネットワークアドレス：192.168.10.0/24
- ether L3監視機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

1. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2. 以下の項目を指定します。

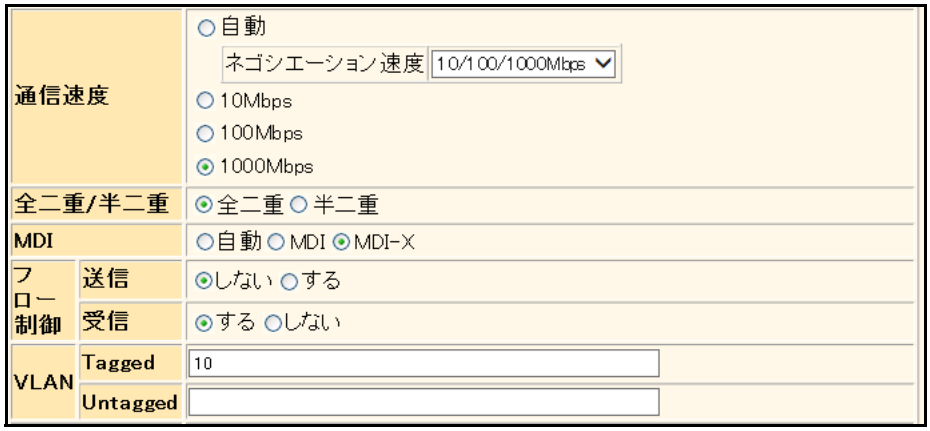
- ポートリスト　　→1-4

3. ［修正］ボタンをクリックします。

ether 1-4情報の設定項目と「基本情報」が表示されます。

4. 以下の項目を指定します。

- 通信速度　　→1000Mbps
- VLAN
  Tagged　　→10



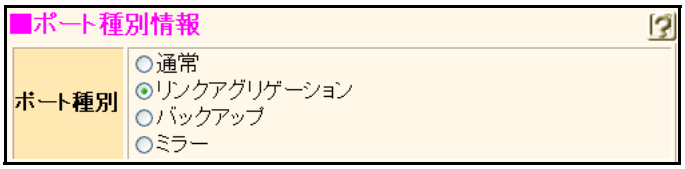
5. ［保存］ボタンをクリックします。

6.　「ポート種別情報」をクリックします。

「ポート種別情報」が表示されます。

7.　以下の項目を指定します。

- ポート種別　→リンクアグリゲーション



8.　［保存］ボタンをクリックします。

9.　設定メニューの詳細設定で「リンクアグリゲーショングループ情報」をクリックします。

「リンクアグリゲーショングループ情報」ページが表示されます。

10.　「リンクアグリゲーショングループ情報」でグループ番号が1の［修正］ボタンをクリックします。

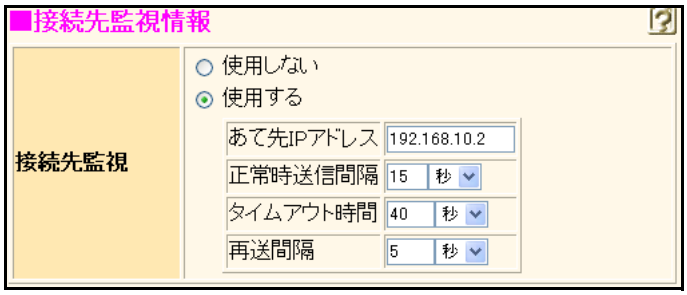
リンクアグリゲーショングループ1情報の設定項目と「基本情報」が表示されます。

11.　リンクアグリゲーショングループ1情報の設定項目の「接続先監視情報」をクリックします。

「接続先監視情報」が表示されます。

12.　以下の項目を指定します。

- 接続先監視　→使用する
  あて先IPアドレス　→192.168.10.2
  正常時送信間隔　→15秒
  タイムアウト時間　→40秒
  再送間隔　→5秒



13.　［保存］ボタンをクリックします。

14.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

15.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

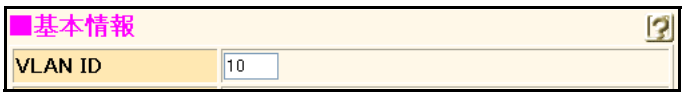
「LAN0情報」ページが表示されます。

16.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

17. 以下の項目を指定します。

- VLAN ID　→10



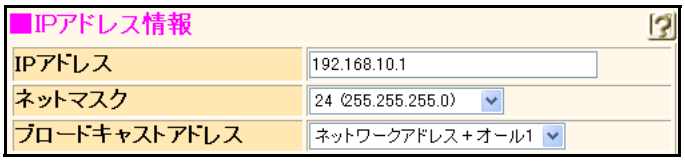
18. ［保存］ボタンをクリックします。

19. ［IP 関連］をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

20. 以下の項目を指定します。

- IP アドレス　→192.168.10.1
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1



21. ［保存］ボタンをクリックします。

22. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「ether 情報」

- ポートリスト　→1-4

「ether 1-4 情報」-「基本情報」

- 通信速度　→1000Mbps
- VLAN
  Tagged　→10

「ether 1-4 情報」-「ポート種別情報」

- ポート種別　→リンクアグリゲーション

「LAN 情報」

「LAN0 情報」-「共通情報」-「基本情報」

- VLAN ID　→10

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス　→192.168.10.2
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール 1

19　ポート閉塞機能を使う

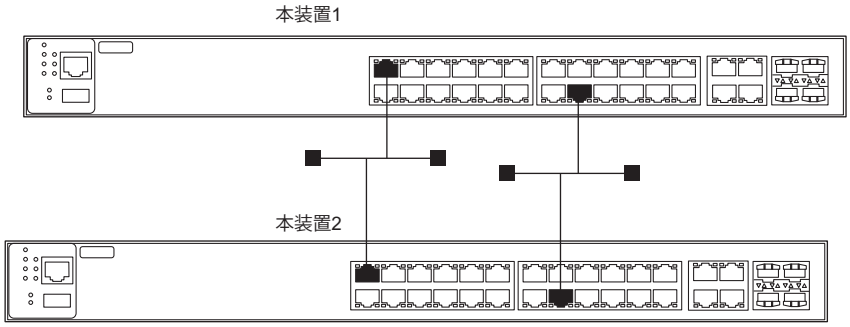
適用機種　全機種

ポート閉塞機能を利用すると、間欠障害発生時にも接続ポートが閉塞状態を保持するため、安定した通信を保つことができます。

ここでは、バックアップポート機能と併用し、マスタポートの間欠障害発生時にはマスタポートを閉塞し、バックアップポートだけを使用する場合を例に説明します。

こんな事に気をつけて

閉塞されたポートは自動では復旧しません。ポートが閉塞された状態から閉塞を解除させたい場合は、「操作メニュー」の「閉塞／閉塞解除」を使用してポート閉塞を解除してください。



● 設定条件

[本装置 1]

- 各装置で ETHER1、16 ポートをバックアップポートとして使用する
  （ETHER1 をマスタポート、ETHER16 をバックアップポートとし、マスタポートを優先的に使用する）
- リンクダウン回数による閉塞を行う
- リンクダウン回数の上限値の設定

[本装置 2]

- 各装置で ETHER1、16 ポートをバックアップポートとして使用する
  （ETHER1 をマスタポート、ETHER16 をバックアップポートとし、マスタポートを優先的に使用する）
- リンクダウン回数による閉塞を行う
- リンクダウン回数の上限値の設定

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置1を設定する

1. 設定メニューの詳細設定で「ether情報」をクリックします。

「ether情報」ページが表示されます。

2. 「ether情報」でポート番号が1の［修正］ボタンをクリックします。

ether 1情報の設定項目と「基本情報」が表示されます。

3. 以下の項目を指定します。

- リンクダウン回数の上限値　→5

4. ［保存］ボタンをクリックします。

5. 「ポート種別情報」をクリックします。

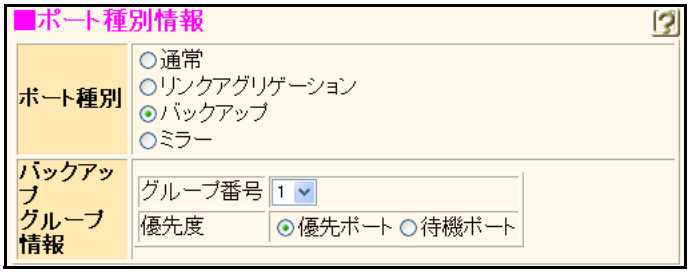
「ポート種別情報」ページが表示されます。

6. 以下の項目を指定します。

- ポート種別　→バックアップ

“バックアップ”を選択すると、「バックアップグループ情報」の設定項目が表示されます。

- バックアップグループ情報
  グループ番号　→1
  優先度　→優先ポート



7. ［保存］ボタンをクリックします。

8. 画面上部の「ether情報」をクリックします。

「ether情報」ページが表示されます。

9. 「ether情報」でポート番号が16の［修正］ボタンをクリックします。

ether 16情報の設定項目と「基本情報」が表示されます。

10. 手順5.～7.を参考に、以下の項目を設定します。

- ポート種別　→バックアップ
- バックアップグループ情報
  グループ番号　→1
  優先度　→待機ポート

11. 設定メニューの詳細設定で「バックアップグループ情報」をクリックします。

「バックアップグループ情報」ページが表示されます。

12. 「バックアップグループ情報」でバックアップグループ番号が1の［修正］ボタンをクリックします。

「バックアップグループ1情報」が表示されます。

13. 以下の項目を指定します。

- 優先使用ポート　→master

	<バックアップグループ情報入力フィールド>	
1	優先使用ポート	◉master ○先にリンクアップしたポート
	待機状態	◉閉塞しない ○閉塞する

14. ［保存］ボタンをクリックします。

15. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

「ether情報」

「ether 1情報」-「基本情報」

- リンクダウン回数の上限値　→5

「ether 1情報」-「ポート種別情報」

- ポート種別　→バックアップ
- バックアップグループ情報
  グループ番号　→1
  優先度　→優先ポート

「ether 16情報」-「ポート種別情報」

- ポート種別　→バックアップ
- バックアップグループ情報
  グループ番号　→1
  優先度　→待機ポート

「バックアップグループ情報」

「バックアップグループ1情報」

- 優先使用ポート　→master

20　LANをネットワーク間接続する

適用機種　***SR-S732TR1, 752TR1***

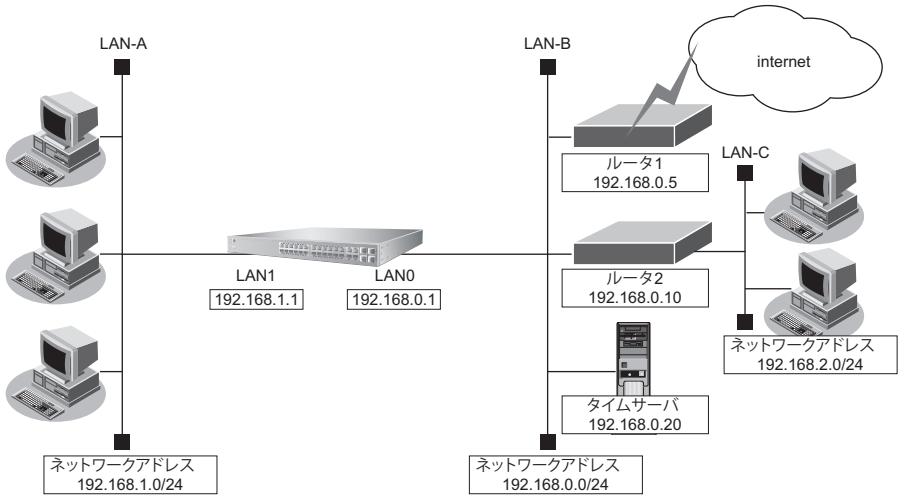
ここでは、既存のLAN-Bに新規のLAN-Aをネットワーク間接続し、静的に経路情報を設定する場合を例に説明します。

こんな事に気をつけて

マニュアル「Webユーザーズガイド」に従って設定した状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

参照　マニュアル「トラブルシューティング」
マニュアル「Webユーザーズガイド」

SR-S732TR1の場合を例にします。



● 設定条件

[LAN-A側]

- 通信速度は自動認識
- VLANはタグなし
- 本装置のLAN1側のIPアドレス　：192.168.1.1
- ネットワークアドレス／ネットマスク　：192.168.1.0/24
- DHCP機能を使用する

[LAN-B側]

- 通信速度は自動認識
- VLANはタグなし
- 本装置のLAN0側のIPアドレス　：192.168.0.1
- ネットワークアドレス／ネットマスク　：192.168.0.0/24
- DHCP機能を使用しない
- ルーティングプロトコルとしてRIP-V1を使用する

- インターネットにつながるルータ１と、事業所内のその他のネットワークにつながるルータ２が存在し、静的に経路情報を登録する
  ルータ１のIPアドレス　：192.168.0.5
  ルータ２のIPアドレス　：192.168.0.10
- LAN-Cのネットワークアドレス／ネットマスク　：192.168.2.0/24

[その他の条件]

- 自動時刻設定にする
  タイムサーバ　：使用する
  サーバ設定　：設定する
  プロトコル　：TIME プロトコル
  タイムサーバのアドレス　：192.168.0.20

ヒント

◆ TIME プロトコル、SNTP とは？

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

こんな事に気をつけて

- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- 「IP情報」-「基本情報」の「IPフォワーディング機能」の設定を変更した場合は、装置を再起動してください。

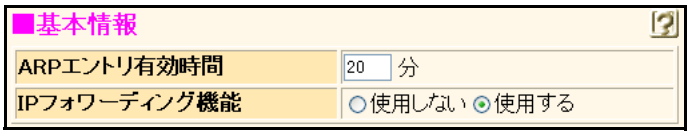
上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「IP情報」をクリックします。

「IP情報」ページが表示されます。

2.　以下の項目を指定します。

- IPフォワーディング機能　→使用する



3.　［保存］ボタンをクリックします。

LAN0 情報を設定する

1. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2. 「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

3. 以下の項目を指定します。

- VLAN
  Untagged →1

4. ［保存］ボタンをクリックします。

5. 「ether 情報」でポート番号が 2 の［修正］ボタンをクリックします。

ether 2 情報の設定項目と「基本情報」が表示されます。

6. 手順 3. ～ 4. を参考に、以下の項目を設定します。

- VLAN
  Untagged →2

7. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

8. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

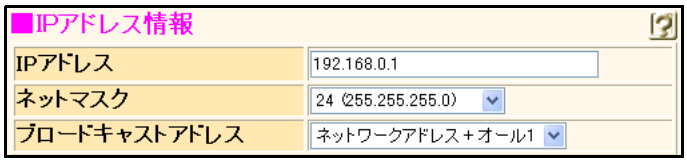
「LAN0 情報」ページが表示されます。

9. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

10. 以下の項目を指定します。

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



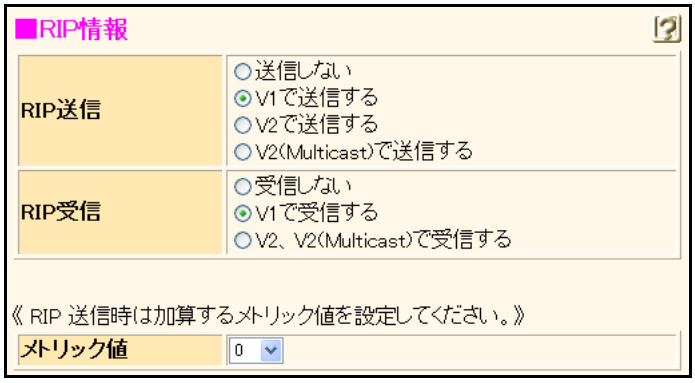
11. ［保存］ボタンをクリックします。

12. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

13. 以下の項目を指定します。

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



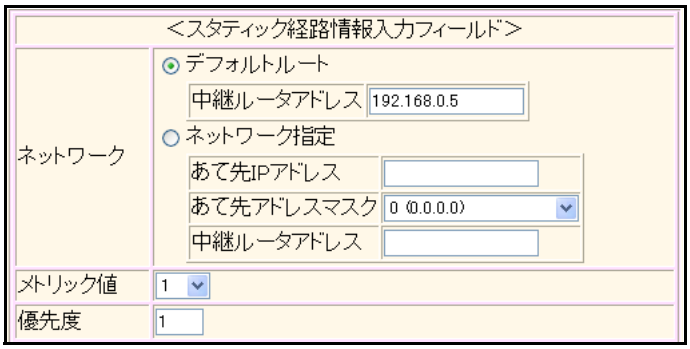
14. ［保存］ボタンをクリックします。

15. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

16. 以下の項目を指定します。

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



17. ［追加］ボタンをクリックします。

18. 手順16.～17.を参考に、以下の項目を設定します。

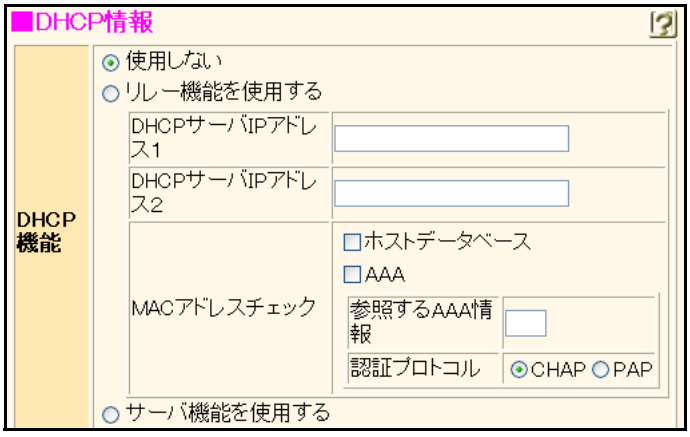
- ネットワーク　→ネットワーク指定
  あて先IPアドレス　→192.168.2.0
  あて先アドレスマスク　→24（255.255.255.0）
  中継ルータアドレス　→192.168.0.10
- メトリック値　→1
- 優先度　→1

19. IP関連の設定項目の「DHCP情報」をクリックします。

「DHCP情報」が表示されます。

20. 以下の項目を指定します。

- DHCP 機能　→使用しない



21. ［保存］ボタンをクリックします。

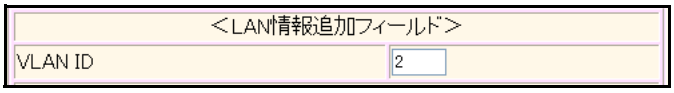
LAN1 情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- VLAN ID　→2



3. ［追加］ボタンをクリックします。

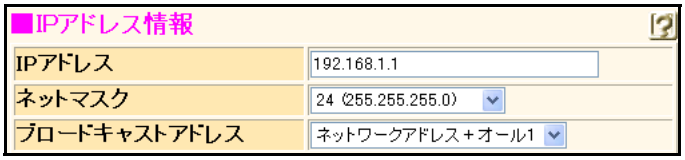
「LAN1 情報」ページが表示されます。

4. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

5. 以下の項目を指定します。

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



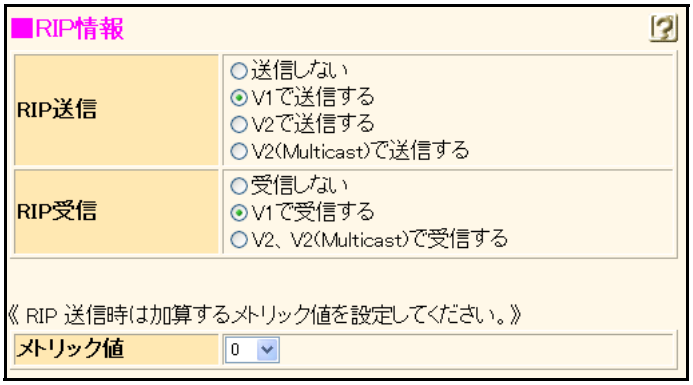
6. ［保存］ボタンをクリックします。

7. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

8.　以下の項目を指定します。

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



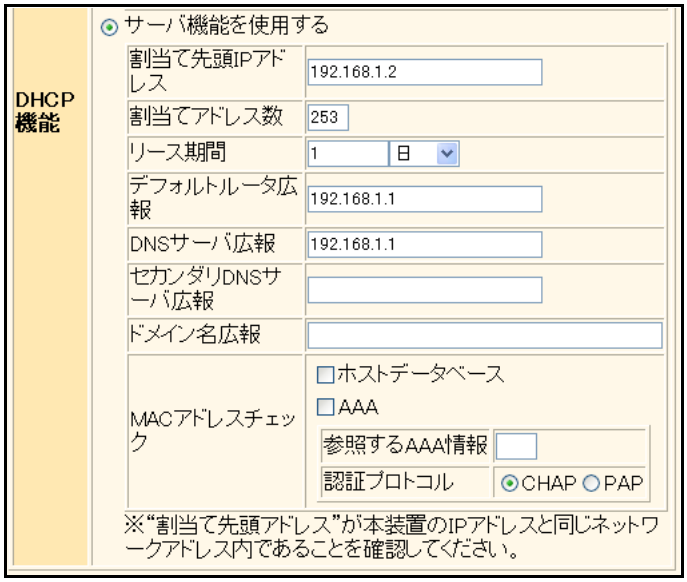
9.　［保存］ボタンをクリックします。

10.　IP関連の設定項目の「DHCP情報」をクリックします。

「DHCP情報」が表示されます。

11.　以下の項目を指定します。

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



12.　［保存］ボタンをクリックします。

自動時刻を設定する

1.　設定メニューの基本設定で「装置情報」をクリックします。

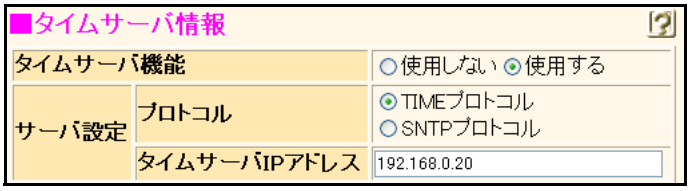
「装置情報」ページが表示されます。

2.　「タイムサーバ情報」をクリックします。

「タイムサーバ情報」が表示されます。

3.　以下の項目を指定します。

- タイムサーバ機能　→使用する
- サーバ設定
  プロトコル　→TIME プロトコル
  タイムサーバ IP アドレス　→ 192.168.0.20



4.　［保存］ボタンをクリックします。

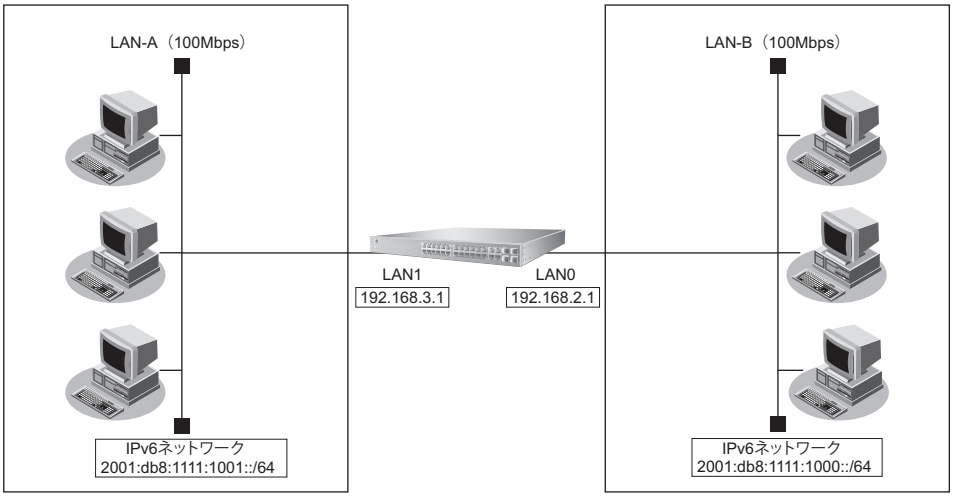
5.　画面左側の［再起動］ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

21 IPv4のネットワークにIPv6ネットワークを追加する

適用機種 ***SR-S732TR1, 752TR1***

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



● 設定条件

【LAN-A側】

- プレフィックス／プレフィックス長　：2001:db8:1111:1001::/64
- RA送信を行う
- VLANはタグなし

【LAN-B側】

- プレフィックス／プレフィックス長　：2001:db8:1111:1000::/64
- RA送信を行う
- VLANはタグなし

こんな事に気をつけて

- **IPv4のネットワークをすでに使用している場合の設定例です。新規にIPv6だけのネットワーク構成を設定する場合は、etherポートへのVLAN設定などが必要になります。**
- **「IPv6情報」-「基本情報」の「IPv6フォワーディング機能」の設定を変更した場合は、装置を再起動してください。**

上記の設定条件に従って設定を行う場合の設定例を示します。

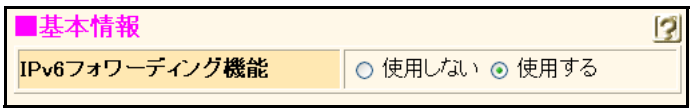
IPv6 フォワーディング機能を設定する

1. **設定メニューの詳細設定で「IPv6 情報」をクリックします。**

   「IPv6 情報」ページが表示されます。

2. **以下の項目を指定します。**

   - IPv6 フォワーディング機能　　→使用する



3. **［保存］ボタンをクリックします。**

LAN0 情報を設定する

1. **設定メニューの詳細設定で「LAN 情報」をクリックします。**

   「LAN 情報」ページが表示されます。

2. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**

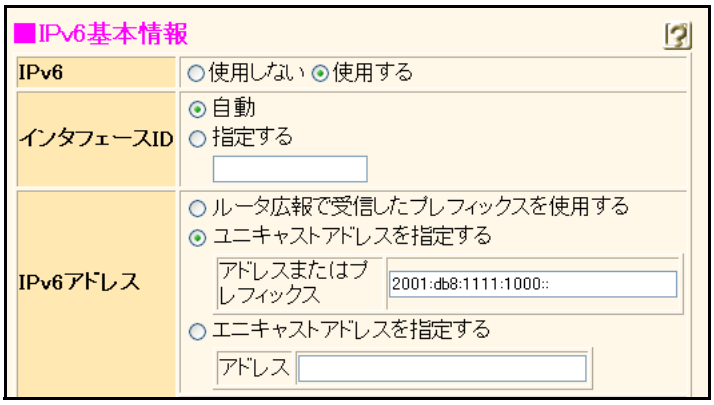
   「LAN0 情報」ページが表示されます。

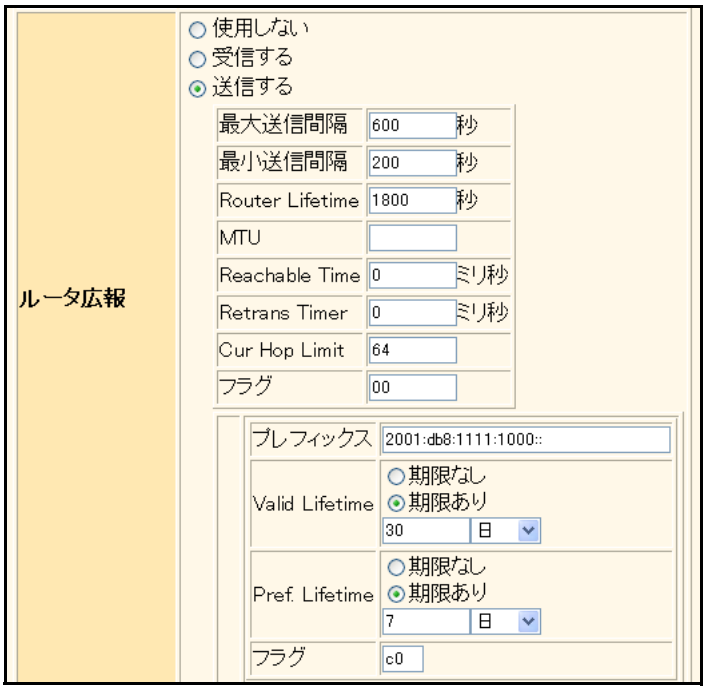
3. **「IPv6 関連」をクリックします。**

   IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス　→ユニキャストアドレスを指定する
  アドレスまたはプレフィックス　→ 2001:db8:1111:1000::
- ルータ広報　→送信する
  プレフィックス　→ 2001:db8:1111:1000::
  Valid Lifetime　→期限あり 30 日
  Pref. Lifetime　→期限あり 7 日
  フラグ　→ c0





5.　［保存］ボタンをクリックします。

LAN1 情報を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

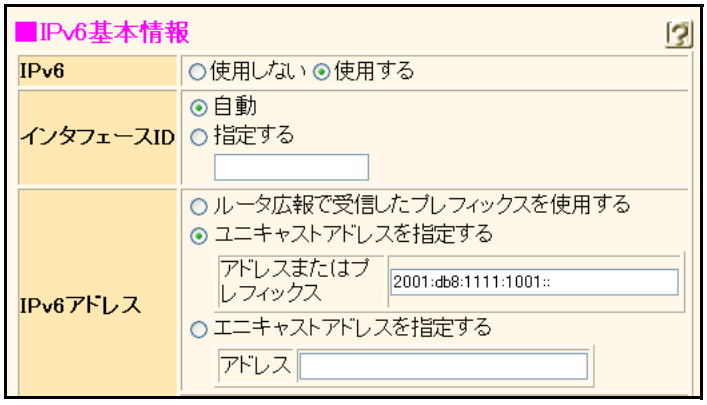
「LAN1 情報」ページが表示されます。

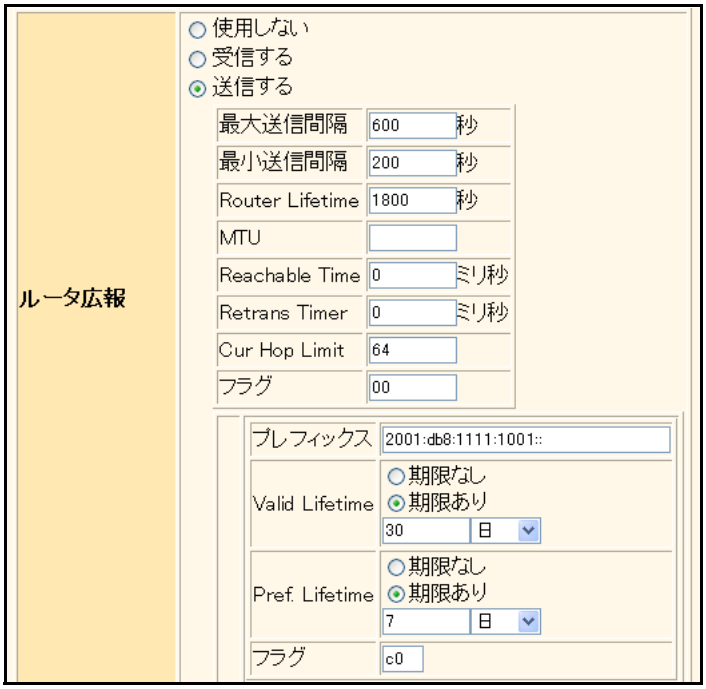
3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- インタフェース ID　→自動
- IPv6 アドレス　→ユニキャストアドレスを指定する
  アドレスまたはプレフィックス　→ 2001:db8:1111:1001::
- ルータ広報　→送信する
  プレフィックス　→ 2001:db8:1111:1001::
  Valid Lifetime　→期限あり 30 日
  Pref. Lifetime　→期限あり 7 日
  フラグ　→ c0





5.　［保存］ボタンをクリックします。

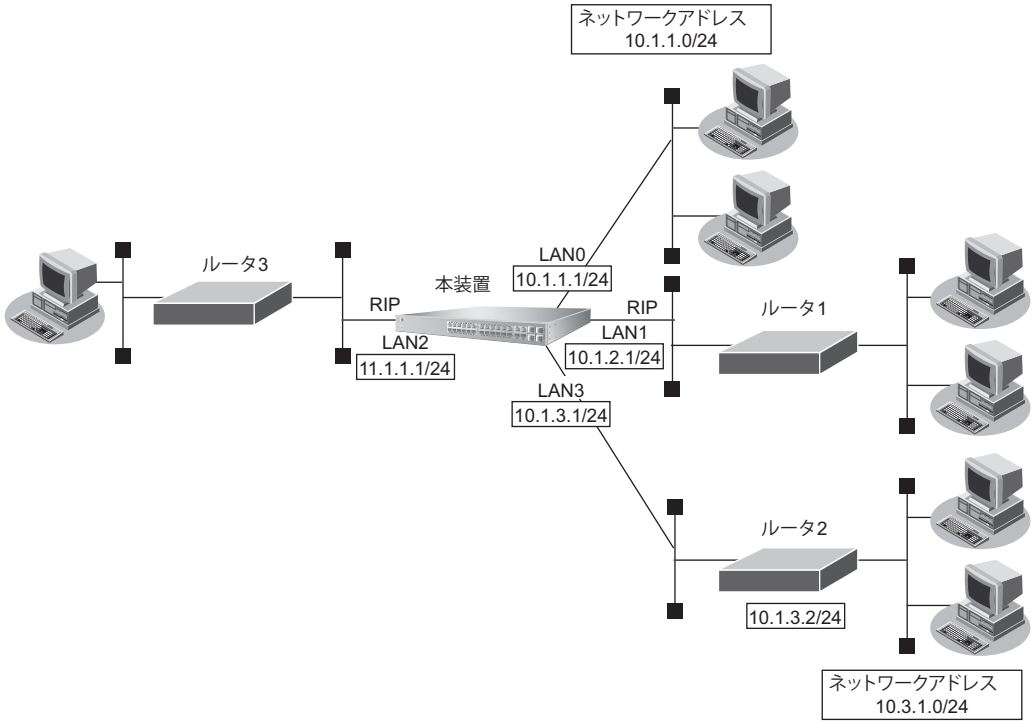
6.　画面左側の［再起動］ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

22　RIP を使用したネットワークを構築する（IPv4）

適用機種　***SR-S732TR1, 752TR1***

ここでは、RIPv2 を使用したダイナミックルーティングのネットワーク設定について説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 設定条件

- LAN0 のネットワークは、RIP ネットワークに広報する
- LAN1 で RIPv2 を使用する
- LAN2 で RIPv2 を使用する
- LAN3 でルータ 2 を経由するネットワークはスタティック経路で設定し、このスタティック経路を RIP ネットワークに広報する

上記の設定条件に従って設定を行う場合の設定例を示します。

RIP 基本情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

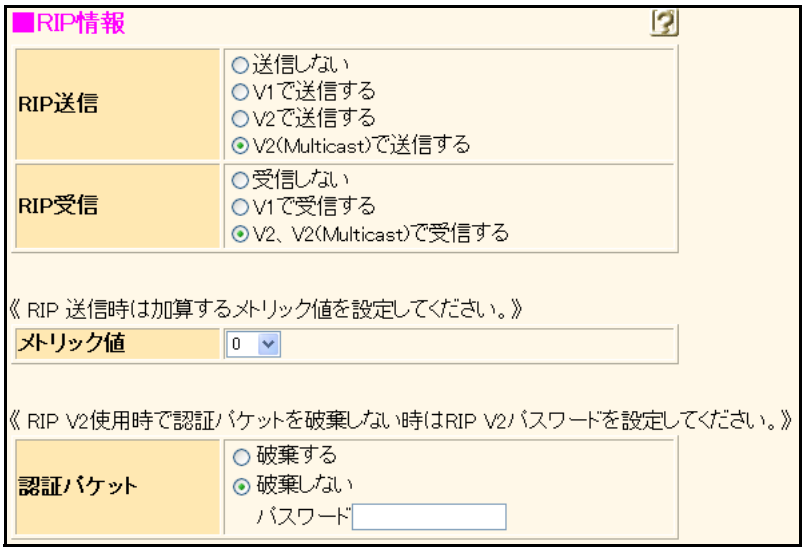
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

5. 以下の項目を指定します。

- RIP 送信　→ V2（Multicast）で送信する
- RIP 受信　→ V2、V2（Multicast）で受信する
- メトリック値　→ 0
- 認証パケット　→破棄しない
  パスワード　→指定しない



6. ［保存］ボタンをクリックします。

7. 手順 2.～6. を参考に、LAN2 情報を設定します。

「LAN2 情報」-「IP 関連」-「RIP 情報」

- RIP 送信　→ V2（Multicast）で送信する
- RIP 受信　→ V2、V2（Multicast）で受信する
- メトリック値　→ 0
- 認証パケット　→破棄しない
  パスワード　→指定しない

ルータ 2 を経由する経路をスタティック経路で設定する

8.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

9.　「LAN 情報」でインタフェースが LAN3 の［修正］ボタンをクリックします。

「LAN3 情報」ページが表示されます。

10.　「IP 関連」をクリックします。

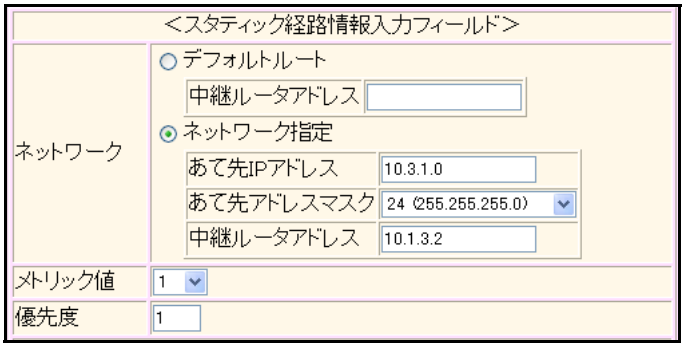
IP 関連の設定項目と「IP アドレス情報」が表示されます。

11.　IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

12.　以下の項目を指定します。

- ネットワーク　→ネットワーク指定
  あて先 IP アドレス　→ 10.3.1.0
  あて先アドレスマスク　→ 24（255.255.255.0）
  中継ルータアドレス　→ 10.1.3.2
- メトリック値　→ 1
- 優先度　→ 1



13.　［追加］ボタンをクリックします。

RIP への再配布経路を設定する

14.　設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

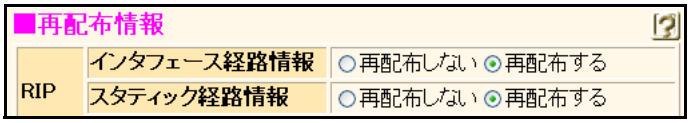
「ルーティングプロトコル情報」ページが表示されます。

15.　「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

16.　以下の項目を指定します。

- RIP
  インタフェース経路情報　→再配布する
  スタティック経路情報　→再配布する



17.　［保存］ボタンをクリックします。

18. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

ヒント

◆ RIP ユニキャスト送信

RIP の経路広報は通常マルチキャスト／ブロードキャストパケットを使用して行われますが、ユニキャストフレームを使用して広報することができます。

ユニキャスト送信は、以下の画面で設定します。

- 「設定メニュー」→詳細設定「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］
- 「設定メニュー」→詳細設定「LAN 情報」→［修正］→［IP 関連］→［RIP 情報］

ユニキャスト送信先に対して、加算メトリック、認証機能および RIP 機能を使用する場合は、送信先ネットワークが属するインタフェースの設定を行います。

◆ RIP マルチパス機能

RIP を利用した冗長ネットワークで通信経路に障害が発生した場合は、ルーティングテーブルから障害経路が削除されても、新しい経路情報を RIP 定期広報などで受信するまでは経路が切り替わりません。そこで、マルチパス機能を利用し、バックアップ経路として冗長な経路を 1 つ保持することで、障害経路が削除された直後に経路を切り替えることができます。

マルチパス機能は、以下の画面で設定します。

- 「設定メニュー」→詳細設定「ルーティングプロトコル情報」→［RIP 関連］→［RIP マルチパス情報］

こんな事に気をつけて

- 本装置の初期設定では、インタフェース経路とスタティック経路を RIP に再配布する設定となっています。再配布が不要な場合は、再配布しない設定を行ってください。
- メトリック値が同じ冗長経路を受信した場合、先に受信した RIP 経路を優先経路として扱います。ECMP としては動作しません。
- 複数のインタフェースで RIP を利用する場合、以下の条件式の範囲で広報 RIP パケット数を設計してください。
  条件式　　：広報 RIP パケット数×RIP 利用インタフェース数≪ 243
  広報 RIP パケット数は、広報 RIP 経路数を 25 で割り、小数点以下を切り上げた値です。広報 RIP 経路数は、経路フィルタにより減らすことができます。「広報 RIP パケット数×RIP 利用インタフェース数」の値は、本装置が集中して受信する RIP パケット数であり、この値が 243 に近ければ RIP 受信パケットの破棄など通信に影響が出る場合があります。このため、243 よりも十分小さくなるように設計してください。
  なお、破棄されたパケット数は、統計情報表示（show ip traffic udp）の統計値「dropped due to full socket buffers」で確認できます。

23　RIPの経路を制御する（IPv4）

適用機種　***SR-S732TR1, 752TR1***

本装置を経由して、ほかのルータに送受信する経路情報に対して、IPアドレスや方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIPによる経路情報

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件（IPアドレス／アドレスマスク）
- メトリック値

補足　メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にすべて以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。

ヒント

◆ IPアドレスとアドレスマスクの決め方

フィルタリング条件の要素には、「IPアドレス」と「アドレスマスク」があります。制御対象となる経路情報は、経路情報のIPアドレスとアドレスマスクが指定したIPアドレスとアドレスマスクと一致したものだけです。

例）　指定値　：172.21.0.0/16の場合

経路情報　：172.21.0.0/16は制御対象となる

172.21.0.0/24は制御対象とならない

また、フィルタリング条件のIPアドレスと指定したIPアドレスが、指定したアドレスマスクまで一致した場合に制御対象とすることもできます。

指定値　：172.21.0.0/16の場合

経路情報　：172.21.0.0/24は制御対象となる

172.21.10.0/24は制御対象となる

こんな事に気をつけて

RIPv1を使用している場合もアドレスマスクの設定が必要です。この場合、インタフェースのアドレスマスクを指定してください。また、アドレスクラスが異なる経路情報を制御する場合は、ナチュラルマスク値を指定してください。
例）192.168.1.1/24が設定されているインタフェースで10.0.0.0の経路情報を制御する場合は、10.0.0.0/8を指定します。

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する

B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針Bの例として、以下の設定例について説明します。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

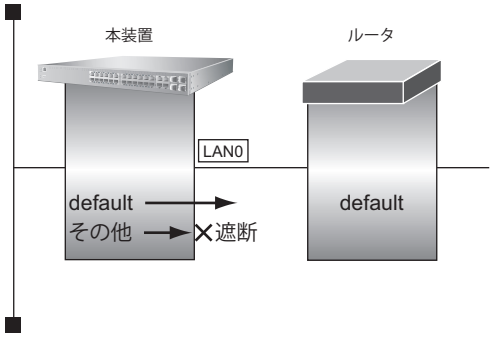
こんな事に気をつけて

- **フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。**
- **RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は遮断されます。**
- **RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は遮断されます。**

23.1 特定の経路情報の送信を許可する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IP関連」をクリックします。

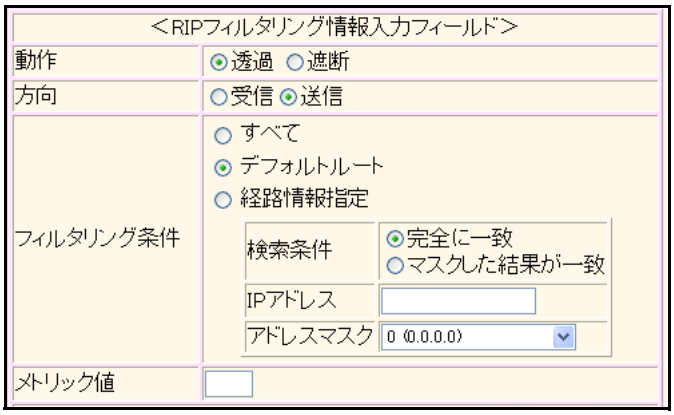
IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP関連の設定項目の「RIPフィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

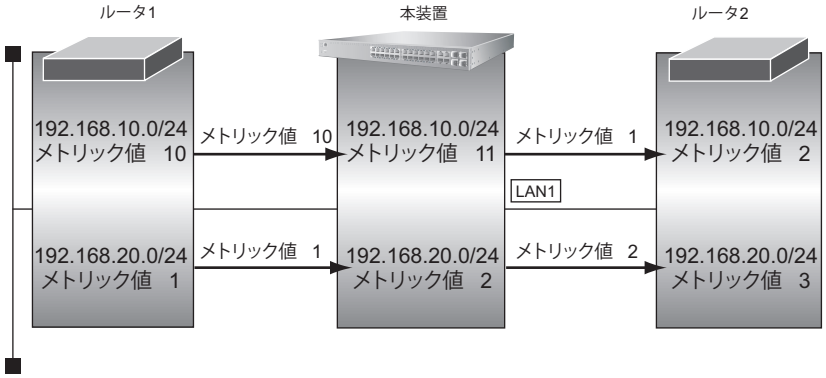
設定した内容が有効になります。

23.2 特定の経路情報のメトリック値を変更して送信する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置がルータ2へ192.168.10.0/24、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から192.168.10.0/24のメトリック値10と192.168.20.0/24のメトリック値1の経路情報を受信するものとします。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置から192.168.10.0/24の送信を許可する場合、メトリック値1に変更
- 192.168.10.0/24以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

「LAN1情報」ページが表示されます。

3. 「IP関連」をクリックします。

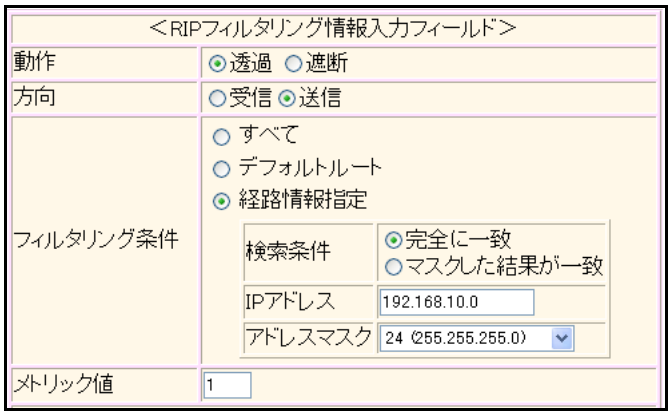
IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP関連の設定項目の「RIPフィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IPアドレス　→192.168.10.0
  アドレスマスク　→24（255.255.255.0）
- メトリック値　→1



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

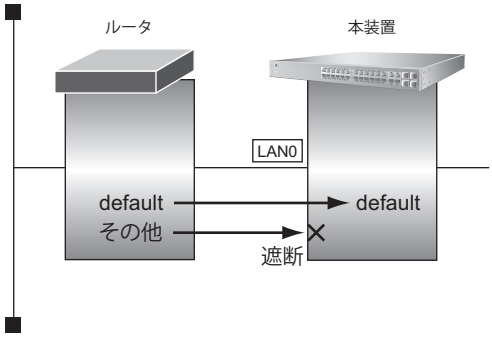
こんな事に気をつけて

- **送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。**
- **送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。**

23.3 特定の経路情報の受信を許可する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IP関連」をクリックします。

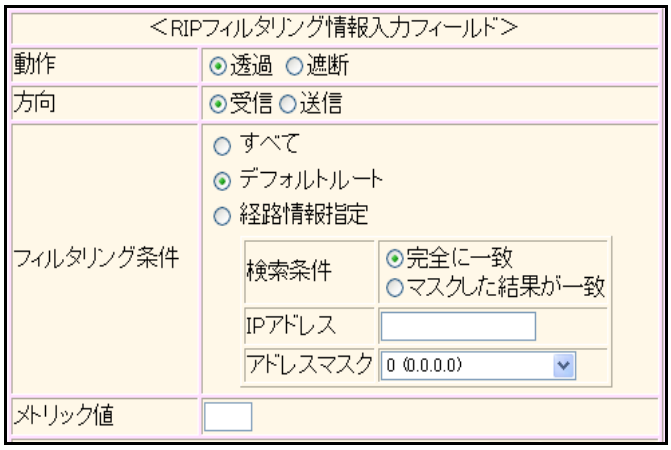
IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP関連の設定項目の「RIPフィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

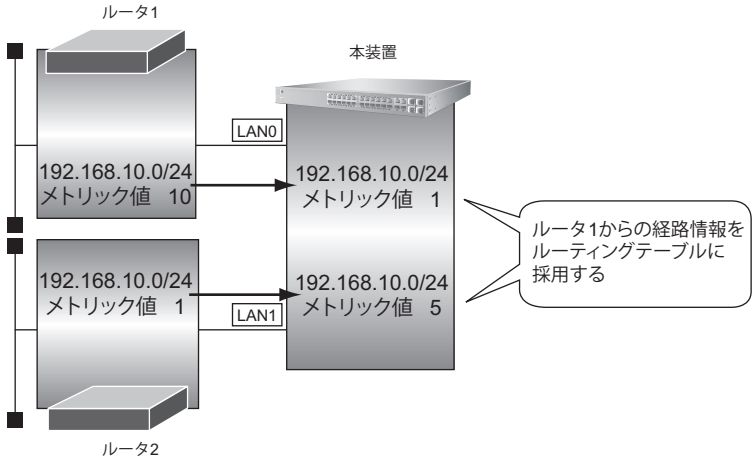
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

23.4 特定の経路情報のメトリック値を変更して受信する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置が、ルータ1とルータ2から同じあて先への経路情報192.168.10.0/24を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスとRIPv2を使用する設定がされている
- IPフォワーディング機能を使用する設定がされている

● フィルタリング設計

- ルータ1から、192.168.10.0/24の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、192.168.10.0/24の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IP関連」をクリックします。

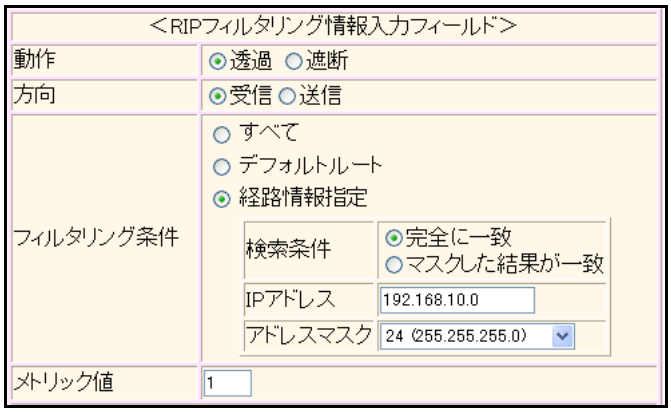
IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP関連の設定項目の「RIPフィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IPアドレス　→192.168.10.0
  アドレスマスク　→24（255.255.255.0）
- メトリック値　→1



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

「LAN1情報」ページが表示されます。

10.　「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

11.　IP関連の設定項目の「RIPフィルタリング情報」をクリックします。

「RIPフィルタリング情報」が表示されます。

12.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IPアドレス　→192.168.10.0
  アドレスマスク　→24（255.255.255.0）
- メトリック値　→5

13. 手順5.～6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

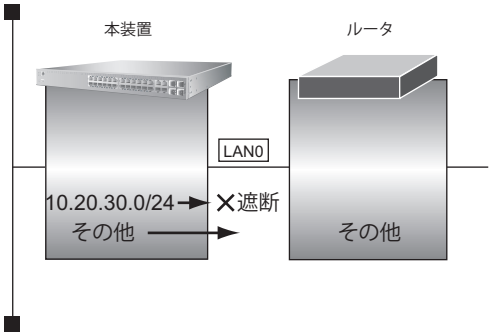
こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

23.5 特定の経路情報の送信を禁止する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置からルータへの 10.20.30.0/24 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスと RIPv2 を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへの 10.20.30.0/24 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

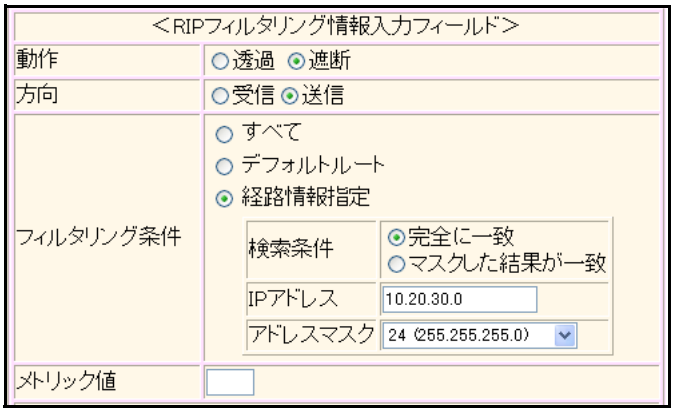
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IPアドレス　→10.20.30.0
  アドレスマスク　→24（255.255.255.0）
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

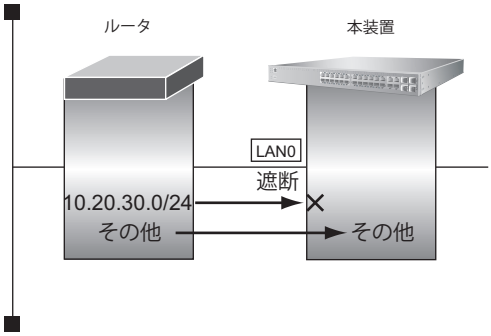
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

23.6 特定の経路情報の受信を禁止する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置は、ルータから 10.20.30.0/24 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスと RIPv2 を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置は 10.20.30.0/24 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

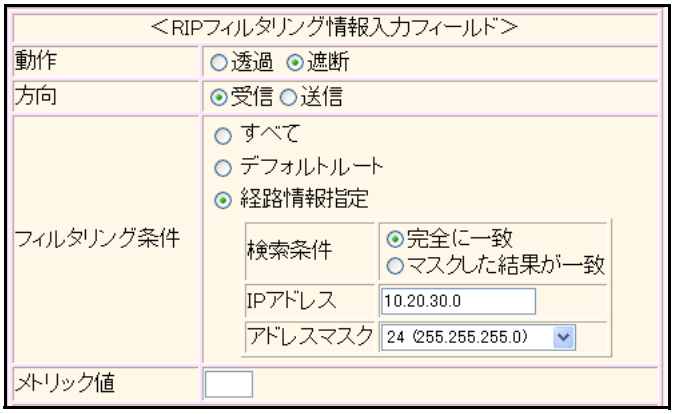
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  IPアドレス　→10.20.30.0
  アドレスマスク　→24（255.255.255.0）
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

24　RIPの経路を制御する（IPv6）

適用機種　***SR-S732TR1, 752TR1***

本装置を経由して、ほかのルータに送信する経路情報や、ほかのルータから受信する経路情報に対して、経路情報や方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または、不要な経路情報を遮断することができます。

経路情報のフィルタリング条件

対象となる経路情報

- RIPによる経路情報（IPv6）

指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング情報（プレフィックス／プレフィックス長）
- メトリック値

補足　メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にすべて以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。

ヒント

◆ プレフィックスとプレフィックス長の決め方

フィルタリング条件の要素には、「プレフィックス」と「プレフィックス長」があります。制御対象となる経路情報は、経路情報のプレフィックスとプレフィックス長が指定したプレフィックスとプレフィックス長と一致したものだけです。

例）　指定値　：2001:db8:1111::/32 の場合

経路情報　：2001:db8:1111::/32 は制御対象となる

2001:db8:1111::/64 は制御対象とはならない

また、経路情報のプレフィックスと指定したプレフィックスが、指定したプレフィックス長まで一致した場合に制御対象とすることもできます。

指定値　：2001:db8::/16 の場合

経路情報　：2001:db8::/32 は制御対象となる

2001:db8:1111::/32 は制御対象となる

フィルタリングの設計方針

フィルタリングの設計方針には大きく分類して以下の2つがあります。

A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する

B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針Bの例として、以下の設定例について説明します。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

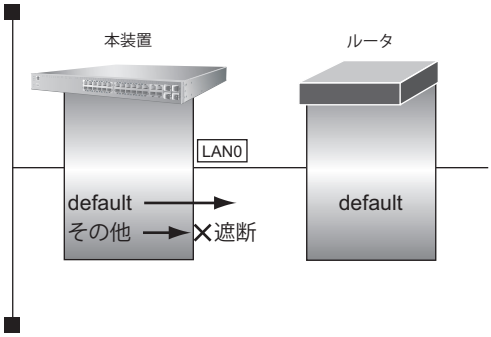
こんな事に気をつけて

- **フィルタリング条件には、優先度を示す定義番号があり、小さい値ほど、より高い優先度を示します。**
- **RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は遮断されます。**
- **RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は遮断されます。**

24.1 特定の経路情報の送信を許可する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明しています。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP（IPv6）を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IPv6関連」をクリックします。

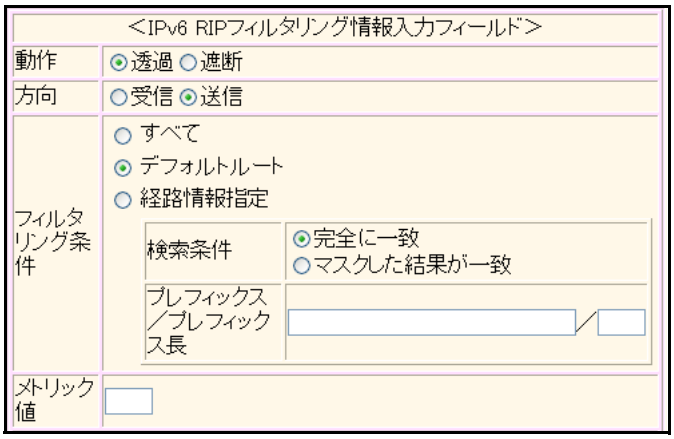
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→遮断
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

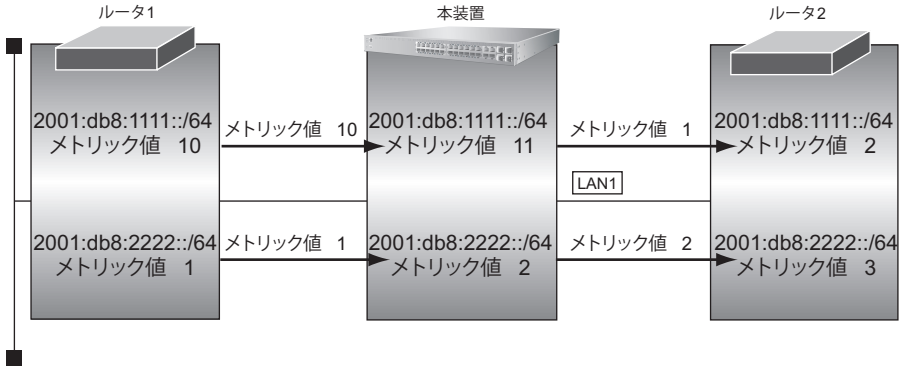
設定した内容が有効になります。

24.2 特定の経路情報のメトリック値を変更して送信する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置がルータ2へ2001:db8:1111::/64、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から2001:db8:1111::/64のメトリック値10と2001:db8:2222::/64のメトリック値1の経路情報を受信するものとします。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP（IPv6）を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置から2001:db8:1111::/64の送信を許可する場合、メトリック値1に変更
- 2001:db8:1111::/64以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

「LAN1情報」ページが表示されます。

3. 「IPv6関連」をクリックします。

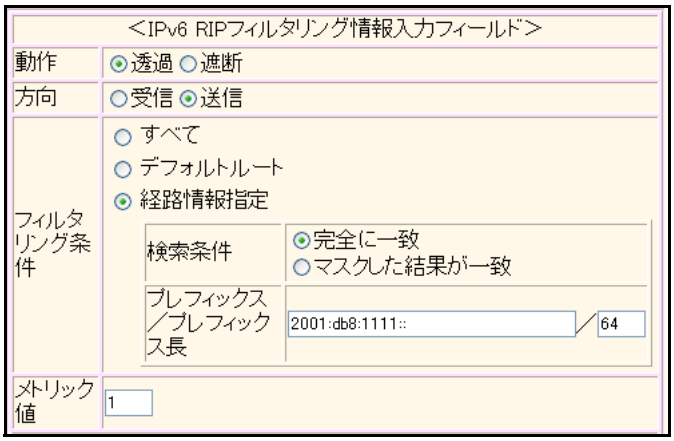
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→2001:db8:1111::/64
- メトリック値　→1



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→送信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

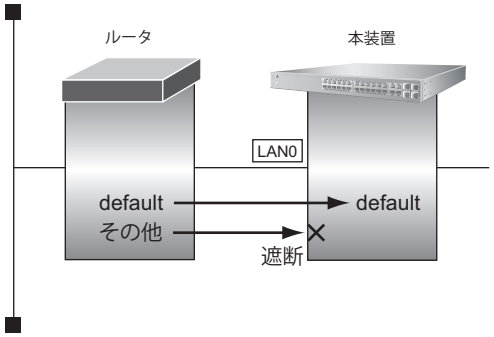
こんな事に気をつけて

- **送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。**
- **送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。**

24.3 特定の経路情報の受信を許可する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP（IPv6）を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IPv6関連」をクリックします。

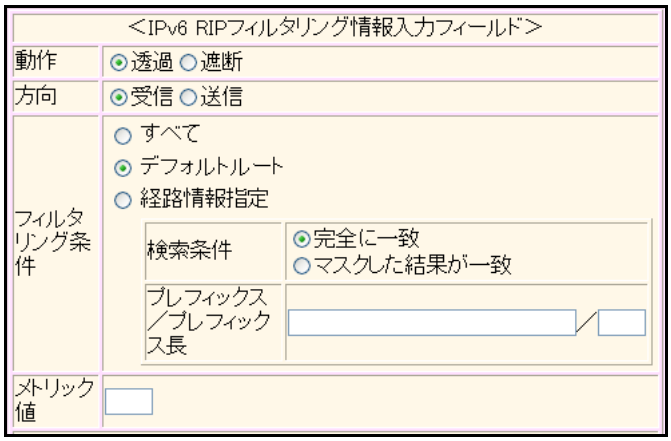
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→デフォルトルート
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

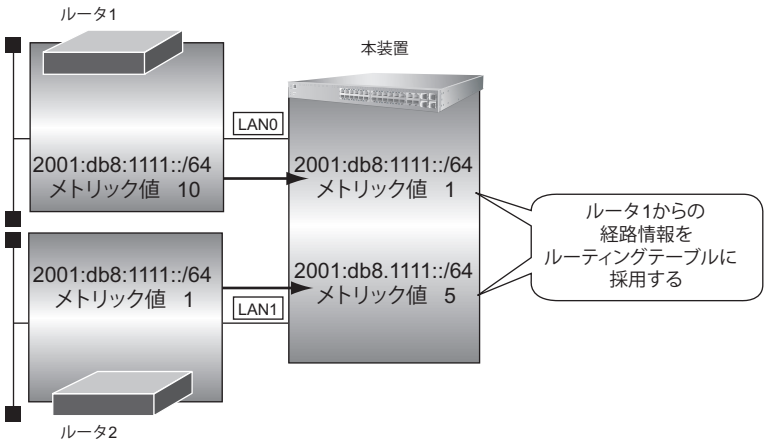
8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

24.4 特定の経路情報のメトリック値を変更して受信する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置が、ルータ1とルータ2から同じあて先への経路情報2001:db8:1111::/64を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP（IPv6）を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- ルータ1から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、2001:db8:1111::/64の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IPv6関連」をクリックします。

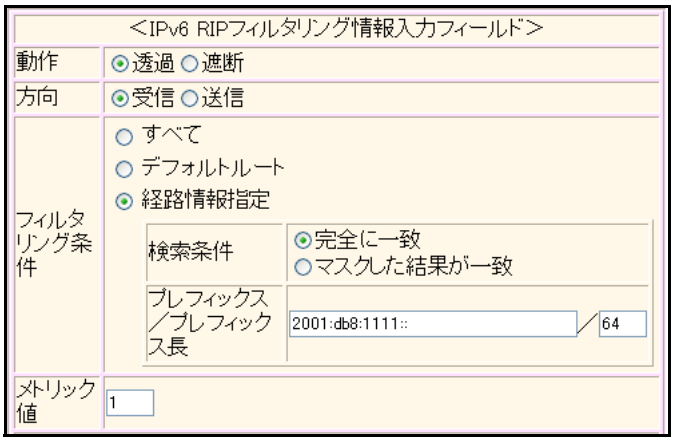
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

5. 以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →経路情報指定
  検索条件 →完全に一致
  プレフィックス／プレフィックス長 →2001:db8:1111::/64
- メトリック値 →1



6. ［追加］ボタンをクリックします。

7. 手順5.～6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

8. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

「LAN1情報」ページが表示されます。

10. 「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

11. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

12. 手順5.～6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →経路情報指定
  検索条件 →完全に一致
  プレフィックス／プレフィックス長 →2001:db8:1111::/64
- メトリック値 →5

13. 手順5.～6.を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

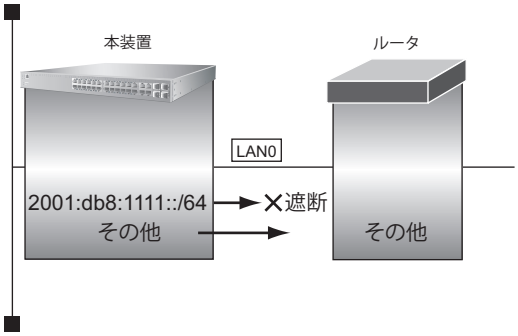
こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

24.5 特定の経路情報の送信を禁止する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置からルータへの2001:db8:1111::/64の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP（IPv6）を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置からルータへの2001:db8:1111::/64の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IPv6関連」をクリックします。

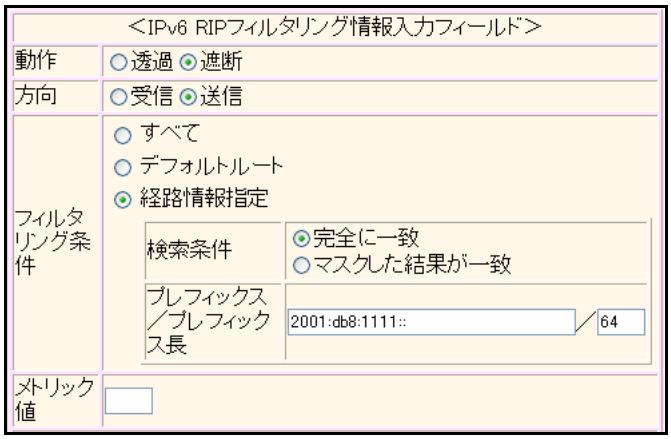
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

5. 以下の項目を指定します。

- 動作 →遮断
- 方向 →送信
- フィルタリング条件 →経路情報指定
  検索条件 →完全に一致
  プレフィックス／プレフィックス長 →2001:db8:1111::/64
- メトリック値 →指定しない



6. ［追加］ボタンをクリックします。

7. 手順5.～6.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

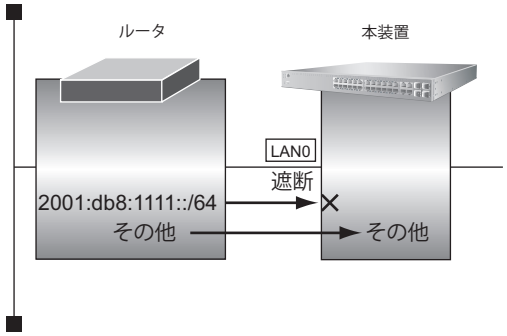
8. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

24.6 特定の経路情報の受信を禁止する

適用機種 ***SR-S732TR1, 752TR1***

ここでは、本装置は、ルータから2001:db8:1111::/64の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPv6機能とRIP（IPv6）を使用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている

● フィルタリング設計

- 本装置は2001:db8:1111::/64の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合の設定例を示します。

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IPv6関連」をクリックします。

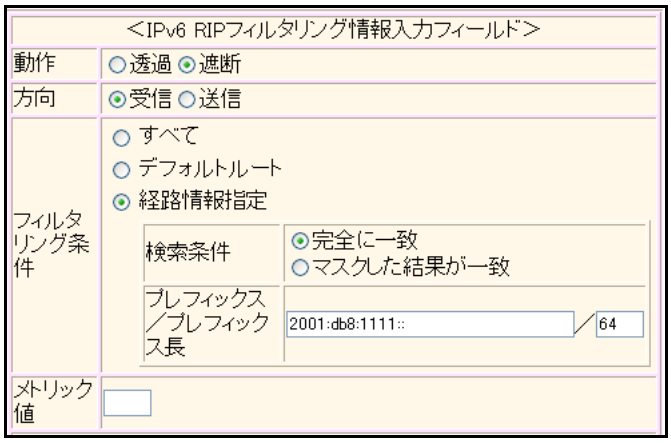
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

4. IPv6関連の設定項目の「IPv6 RIPフィルタリング情報」をクリックします。

「IPv6 RIPフィルタリング情報」が表示されます。

5.　以下の項目を指定します。

- 動作　→遮断
- 方向　→受信
- フィルタリング条件　→経路情報指定
  検索条件　→完全に一致
  プレフィックス／プレフィックス長　→2001:db8:1111::/64
- メトリック値　→指定しない



6.　［追加］ボタンをクリックします。

7.　手順5.～6.を参考に、以下の項目を設定します。

- 動作　→透過
- 方向　→受信
- フィルタリング条件　→すべて
- メトリック値　→指定しない

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

25　OSPF を使用したネットワークを構築する（IPv4）

適用機種　***SR-S732TR1, 752TR1***

ここでは、OSPFv2 を使用したダイナミックルーティングのネットワークの設定方法について説明します。

OSPF を使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。

エリアには、エリアごとにエリア ID を設定します。バックボーンエリアには必ず 0.0.0.0 のエリア ID を設定し、ほかのエリアには重複しないように 0.0.0.0 以外のエリア ID を設定します。

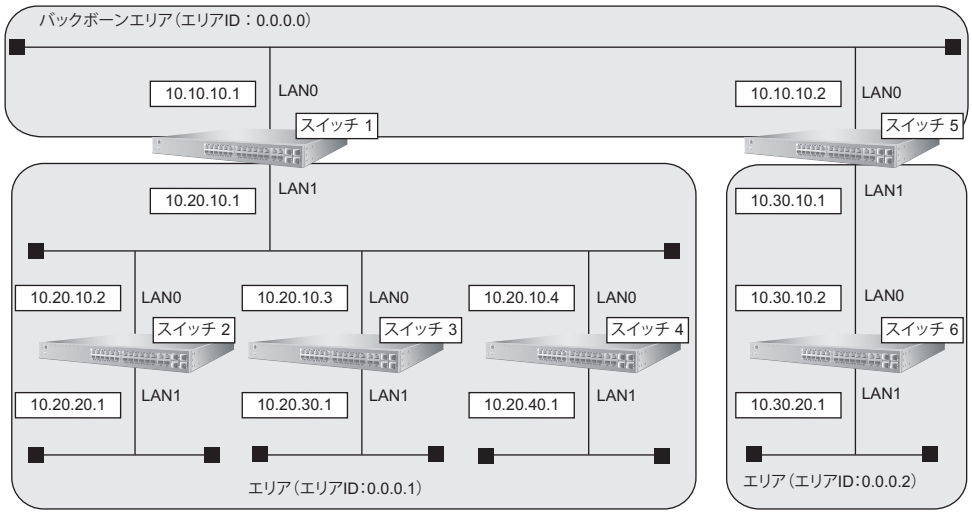
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

参照　マニュアル「機能説明書」

こんな事に気をつけて

- **OSPF を使用するインタフェースは、それぞれ異なったネットワークに属する IP アドレスを設定する必要があります。同じネットワークに属する IP アドレスを設定した場合、OSPF を使用しないと判断されます。**
- **ルータは、各エリアに 50 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2 つ以上のエリアの指定ルータ（Designated Router）とならないように設定してください。**
- **隣接する OSPF ルータどうしは、同じ MTU 値を設定してください。**
- **経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができても、OSPF の経路は、経路情報に反映されません。**
- **本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません（LSDB オーバフロー）。**
  また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源を再投入したり、または［設定反映］ボタンや［再起動］ボタンをクリックしても、正常に通信ができるまでに最大 60 分かかることがあります。
- **OSPF 使用中に［設定反映］ボタンをクリックした場合、自装置が広報したすべての LSA に対して MaxAge で再広報を行ったあとに、OSPF ネットワークへの経路情報が再作成されることがあります。**
- **OSPF で使用するインタフェースは、以下の条件で使用してください。**

本装置が DR を兼務する場合	本装置が DR を兼務しない場合
（25000÷本装置保有 LSA 数）未満	（50000÷本装置保有 LSA 数）未満



● 前提条件

- すべてのスイッチのすべてのインタフェースに IP アドレスの設定がされている
- すべてのスイッチに IP フォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN1 でのルータ優先度　：0
- エリア 0.0.0.1 への集約経路設定　：10.20.0.0/16

[スイッチ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：1
- LAN1 での passive-interface 設定　：設定する

[スイッチ 3 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：255
- LAN1 での passive-interface 設定　：設定する

[スイッチ 4 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- LAN0 でのルータ優先度　：1
- LAN1 での passive-interface 設定　：設定する

[スイッチ 5 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.2
- エリア 0.0.0.2 への集約経路設定　：10.30.0.0/16

［スイッチ 6 でのルーティングプロトコル情報］

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.2
- LAN1 での OSPF エリア ID　：0.0.0.2
- LAN1 での passive-interface 設定　：設定する

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチ 1 を設定する

LAN 情報を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3.　「IP 関連」をクリックします。

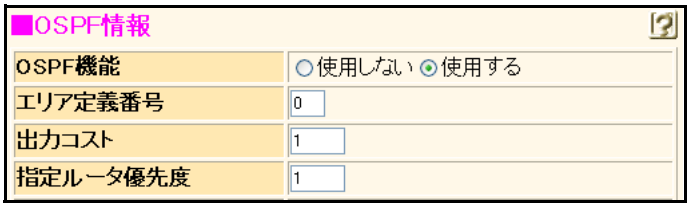
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→ 0



6.　［保存］ボタンをクリックします。

7.　手順 2. ～ 6. を参考に、LAN1 情報を指定します。

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 1
- 指定ルータ優先度　→ 0

OSPF 関連を設定する

8.　設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9.　「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10.　OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

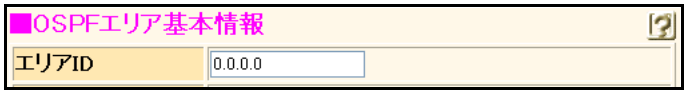
「OSPF エリア情報」が表示されます。

11.　［追加］ボタンをクリックします。

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

12.　以下の項目を指定します。

- エリア ID　→0.0.0.0



13.　［保存］ボタンをクリックします。

14.　画面上部の「ルーティングプロトコル情報」をクリックします。

OSPF 関連項目と「OSPF エリア情報」が表示されます。

15.　手順 11.～13. を参考に、以下の項目を設定します。

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

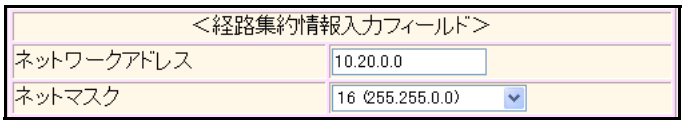
- エリア ID　→0.0.0.1

16.　OSPF エリア情報（1）の設定項目の「経路集約情報」をクリックします。

「経路集約情報」が表示されます。

17.　以下の項目を指定します。

- ネットワークアドレス　→10.20.0.0
- ネットマスク　→16（255.255.0.0）



18.　［追加］ボタンをクリックします。

19.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

スイッチ2を設定する

「スイッチ1を設定する」を参考に、スイッチ2を設定します。

「LAN情報」
「LAN0情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0
- 指定ルータ優先度　→1

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」
「OSPF関連」-「OSPFエリア情報（0）」-「OSPFエリア基本情報」

- エリアID　→0.0.0.1

スイッチ3を設定する

「スイッチ1を設定する」を参考に、スイッチ3を設定します。

「LAN情報」
「LAN0情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0
- 指定ルータ優先度　→255

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」
「OSPF関連」-「OSPFエリア情報（0）」-「OSPFエリア基本情報」

- エリアID　→0.0.0.1

スイッチ4を設定する

「スイッチ1を設定する」を参考に、スイッチ4を設定します。

「LAN情報」
「LAN0情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0
- 指定ルータ優先度　→1

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」
「OSPF 関連」-「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.1

スイッチ 5 を設定する

「スイッチ 1 を設定する」を参考に、スイッチ 5 を設定します。

「LAN 情報」
「LAN0 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

「ルーティングプロトコル情報」
「OSPF 関連」-「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.0

「OSPF 関連」-「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.2
- 経路集約情報
  ネットワークアドレス　→10.30.0.0
  ネットマスク　→16（255.0.0.0）

スイッチ 6 を設定する

「スイッチ 1 を設定する」を参考に、スイッチ 6 を設定します。

「LAN 情報」
「LAN0 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→0
- パケット送信　→抑止する

「ルーティングプロトコル情報」
「OSPF 関連」-「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.2

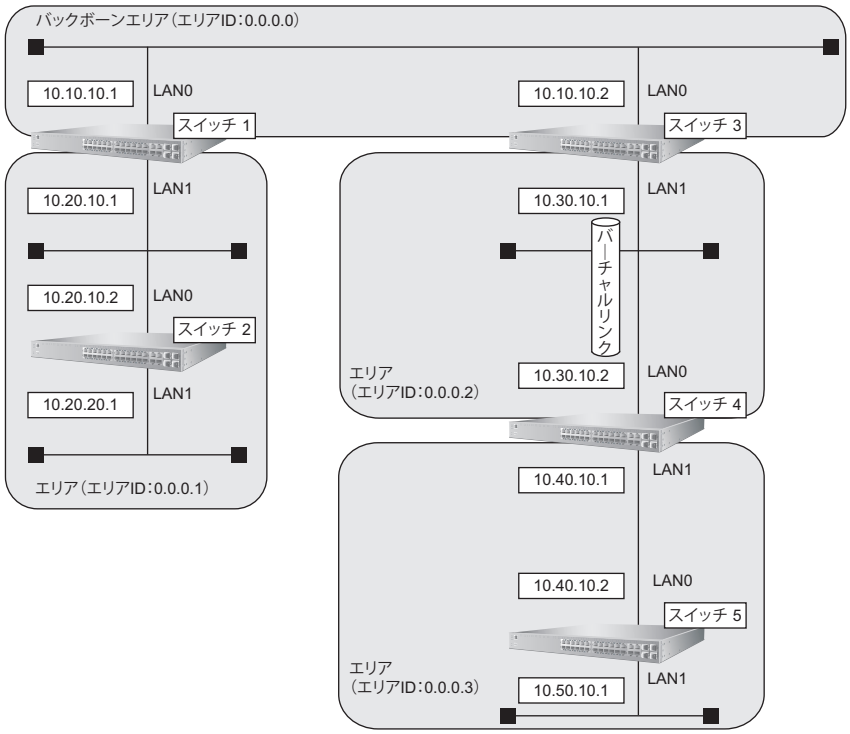
25.1 バーチャルリンクを使う

適用機種 ***SR-S732TR1, 752TR1***

バックボーンエリアと直接接続できないエリアを、バーチャルリンクを使用して接続する設定方法について説明します。

こんな事に気をつけて

- **バーチャルリンクは、スタブエリア、準スタブエリアを経由して使用することはできません。**
- **バーチャルリンクを使用する場合は、OSPF ルータ ID を設定する必要があります。設定する際は、OSPF ルータ ID が重複しないように設定してください。**



● 前提条件

- すべてのスイッチのすべてのインタフェースに IP アドレスの設定がされている
- すべてのスイッチに IP フォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1

[スイッチ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1

[スイッチ3でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのOSPFエリアID　：0.0.0.0
- LAN1でのOSPFエリアID　：0.0.0.2
- OSPFルータID　：10.30.10.1
- バーチャルリンク接続先OSPFルータID　：10.40.10.1

[スイッチ4でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのOSPFエリアID　：0.0.0.2
- LAN1でのOSPFエリアID　：0.0.0.3
- OSPFルータID　：10.40.10.1
- バーチャルリンク接続先OSPFルータID　：10.30.10.1

[スイッチ5でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのOSPFエリアID　：0.0.0.3
- LAN1でのOSPFエリアID　：0.0.0.3

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチ1を設定する

LAN0情報を設定する

1.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3.　「IP関連」をクリックします。

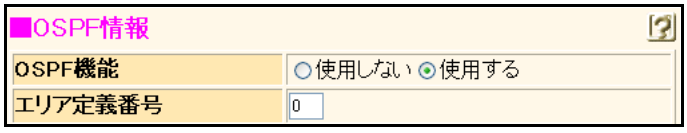
IP関連の設定項目と「IPアドレス情報」が表示されます。

4.　IP関連の設定項目の「OSPF情報」をクリックします。

「OSPF情報」が表示されます。

5.　以下の項目を指定します。

- OSPF機能　→使用する
- エリア定義番号　→0



6. **［保存］ボタンをクリックします。**

7. **手順 2. ～ 6. を参考に、LAN1 情報を設定します。**

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →1

OSPF 関連を設定する

8. **設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

9. **「OSPF 関連」をクリックします。**

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10. **OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**

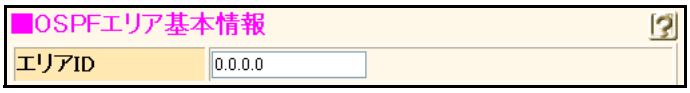
「OSPF エリア情報」が表示されます。

11. **［追加］ボタンをクリックします。**

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

12. **以下の項目を指定します。**

- エリア ID →0.0.0.0



13. **［保存］ボタンをクリックします。**

14. **画面上部の「ルーティングプロトコル情報」をクリックします。**

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

15. **手順 11. ～ 13. を参考に、以下の項目を設定します。**

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID →0.0.0.1

16. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

スイッチ 2 を設定する

「スイッチ 1 を設定する」を参考に、スイッチ 2 を設定します。

「LAN 情報」
「LAN0 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 0

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 0

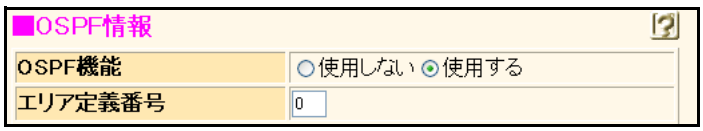
「ルーティングプロトコル情報」
「OSPF 関連」-「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID　→ 0.0.0.1

スイッチ 3 を設定する

LAN0 情報を設定する

1. **設定メニューの詳細設定で「LAN 情報」をクリックします。**
   「LAN 情報」ページが表示されます。
2. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**
   「LAN0 情報」ページが表示されます。
3. **「IP 関連」をクリックします。**
   IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. **IP 関連の設定項目の「OSPF 情報」をクリックします。**
   「OSPF 情報」が表示されます。
5. **以下の項目を指定します。**
   - OSPF 機能　→使用する
   - エリア定義番号　→ 0



6. **［保存］ボタンをクリックします。**
7. **手順 2.～6. を参考に、以下の項目を設定します。**
   「LAN1 情報」-「IP 関連」-「OSPF 情報」
   - OSPF 機能　→使用する
   - エリア定義番号　→ 1

OSPF 関連を設定する

8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

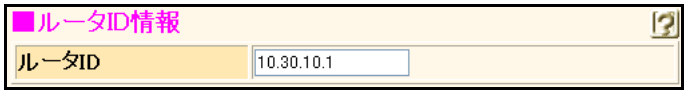
「ルーティングプロトコル情報」ページが表示されます。

9. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10. 以下の項目を指定します。

- ルータ ID → 10.30.10.1



11. ［保存］ボタンをクリックします。

12. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

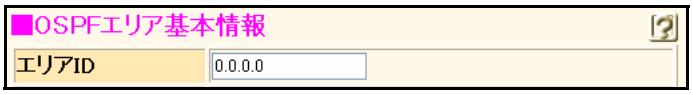
「OSPF エリア情報」が表示されます。

13. ［追加］ボタンをクリックします。

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

14. 以下の項目を指定します。

- エリア ID → 0.0.0.0



15. ［保存］ボタンをクリックします。

16. 画面上部の「ルーティングプロトコル情報」をクリックします。

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

17. 手順 13. ～ 15. を参考に、以下の項目を設定します。

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

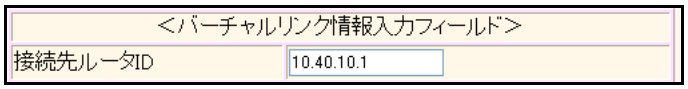
- エリア ID → 0.0.0.2

18. OSPF エリア情報（1）の設定項目の「バーチャルリンク情報」をクリックします。

「バーチャルリンク情報」が表示されます。

19. 以下の項目を指定します。

- 接続先ルータ ID → 10.40.10.1



20. ［追加］ボタンをクリックします。

21. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

スイッチ 4 を設定する

LAN0 情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

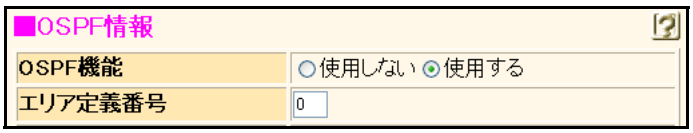
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5. 以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→ 0



6. ［保存］ボタンをクリックします。

7. 手順 2. ～ 6. を参考に、以下の項目を設定します。

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 1

OSPF 関連を設定する

8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

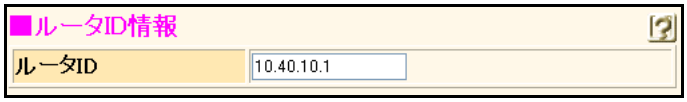
「ルーティングプロトコル情報」ページが表示されます。

9. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10. 以下の項目を指定します。

- ルータ ID　→ 10.40.10.1



11. ［保存］ボタンをクリックします。

12. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

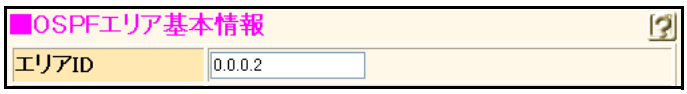
「OSPF エリア情報」が表示されます。

13. ［追加］ボタンをクリックします。

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

14. 以下の項目を指定します。

- エリア ID →0.0.0.2



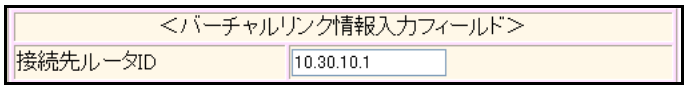
15. ［保存］ボタンをクリックします。

16. OSPF エリア情報（0）の「バーチャルリンク情報」をクリックします。

「バーチャルリンク情報」が表示されます。

17. 以下の項目を指定します。

- 接続先ルータ ID →10.30.10.1



18. ［追加］ボタンをクリックします。

19. 画面上部の「ルーティングプロトコル情報」をクリックします。

OSPF 関連の設定項目と「OSPF エリア基本情報」が表示されます。

20. 手順 13. ～ 15. を参考に、以下の項目を設定します。

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID →0.0.0.3

21. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

スイッチ 5 を設定する

「スイッチ 1 を設定する」を参考に、スイッチ 5 を設定します。

「LAN 情報」

「LAN0 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0

「ルーティングプロトコル情報」

「OSPF 関連」-「OSPF エリア情報（0）」-「OSPF エリア基本情報」

- エリア ID →0.0.0.3

25.2 スタブエリアを使う

適用機種 ***SR-S732TR1, 752TR1***

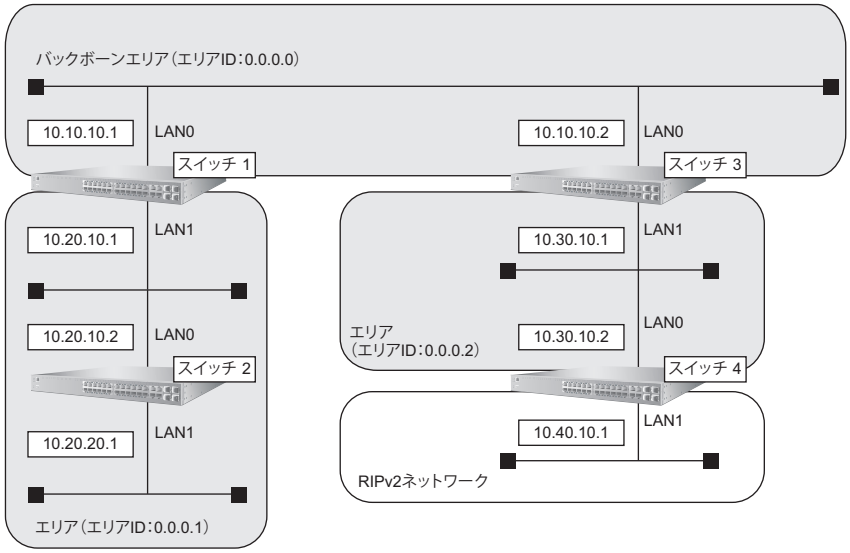
OSPF 以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

OSPF は、RIP で受信した経路情報、スタティック経路情報およびインタフェース経路情報を OSPF ネットワークに取り入れることができます。また、OSPF の経路情報を RIP で広報することができます。

OSPF 以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPF ネットワーク外の経路としてデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアから OSPF 以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア（NSSA）として運用します。

こんな事に気をつけて

OSPF 以外のネットワークと接続する場合、OSPF 以外のネットワークで使用するインタフェース経路情報を OSPF ネットワークに取り入れるように設定する必要があります。



● 前提条件

- すべてのスイッチのすべてのインタフェースに IP アドレスの設定がされている
- すべてのスイッチに IP フォワーディング機能を使用する設定がされている

● 設定条件

[スイッチ 1 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.0
- LAN1 での OSPF エリア ID　：0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ　：stub

[スイッチ 2 でのルーティングプロトコル情報]

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 での OSPF エリア ID　：0.0.0.1
- LAN1 での OSPF エリア ID　：0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ　：stub

[スイッチ3でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのOSPFエリアID　：0.0.0.0
- LAN1でのOSPFエリアID　：0.0.0.2
- エリアID 0.0.0.2のエリアタイプ　：nssa

[スイッチ4でのルーティングプロトコル情報]

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：RIP V2,OSPF
- LAN0でのOSPFエリアID　：0.0.0.2
- LAN1でのpassive-interface設定　：設定する
- エリアID0.0.0.2のエリアタイプ　：nssa
- OSPF経路のRIPでの広報　：再配布する
- RIP経路のOSPFでの広報　：再配布する

上記の設定条件に従って設定を行う場合の設定例を示します。

スイッチ1を設定する

LAN0情報を設定する

1. 設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2. 「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3. 「IP関連」をクリックします。

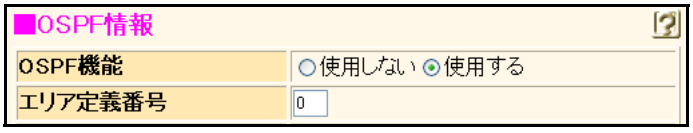
IP関連の設定項目と「IPアドレス情報」が表示されます。

4. IP関連の設定項目の「OSPF情報」をクリックします。

「OSPF情報」が表示されます。

5. 以下の項目を指定します。

- OSPF機能　→使用する
- エリア定義番号　→0



6. ［保存］ボタンをクリックします。

7. **手順2.～6.を参考に、以下の項目を設定します。**

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →1

OSPF関連を設定する

8. **設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

9. **「OSPF関連」をクリックします。**

OSPF関連の設定項目と「ルータID情報」が表示されます。

10. **OSPF関連の設定項目の「OSPFエリア情報」をクリックします。**

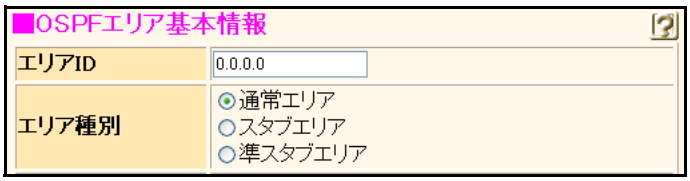
「OSPFエリア情報」が表示されます。

11. **［追加］ボタンをクリックします。**

OSPFエリア情報（0）の設定項目と「OSPFエリア基本情報」が表示されます。

12. **以下の項目を指定します。**

- エリアID →0.0.0.0



13. **［保存］ボタンをクリックします。**

14. **画面上部の「ルーティングプロトコル情報」をクリックします。**

OSPF関連の設定項目と「OSPFエリア情報」が表示されます。

15. **手順11.～13.を参考に、以下の項目を設定します。**

「OSPFエリア情報（1）」-「OSPFエリア基本情報」

- エリアID →0.0.0.1
- エリア種別 →スタブエリア

16. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

スイッチ2を設定する

「スイッチ1を設定する」を参考に、スイッチ2を設定します。

「LAN情報」

「LAN0情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0

「ルーティングプロトコル情報」

「OSPF関連」-「OSPFエリア情報（0）」-「OSPFエリア基本情報」

- エリアID　→0.0.0.1
- エリア種別　→スタブエリア

スイッチ3を設定する

「スイッチ1を設定する」を参考に、スイッチ3を設定します。

「LAN情報」

「LAN0情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→0

「LAN1情報」-「IP関連」-「OSPF情報」

- OSPF機能　→使用する
- エリア定義番号　→1

「ルーティングプロトコル情報」

「OSPF関連」-「OSPFエリア情報（0）」-「OSPFエリア基本情報」

- エリアID　→0.0.0.0

「OSPF関連」-「OSPFエリア情報（1）」-「OSPFエリア基本情報」

- エリアID　→0.0.0.2
- エリア種別　→準スタブエリア

スイッチ 4 を設定する

LAN0 情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

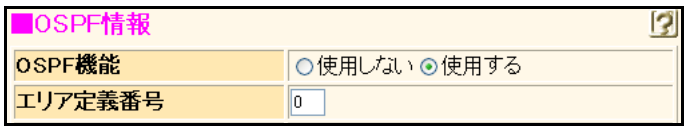
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5. 以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6. ［保存］ボタンをクリックします。

LAN1 情報を設定する

7. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

9. 「IP 関連」をクリックします。

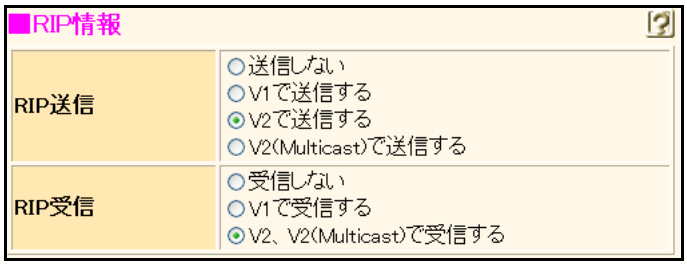
IP 関連の設定項目と「IP アドレス情報」が表示されます。

10. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

11. 以下の項目を指定します。

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



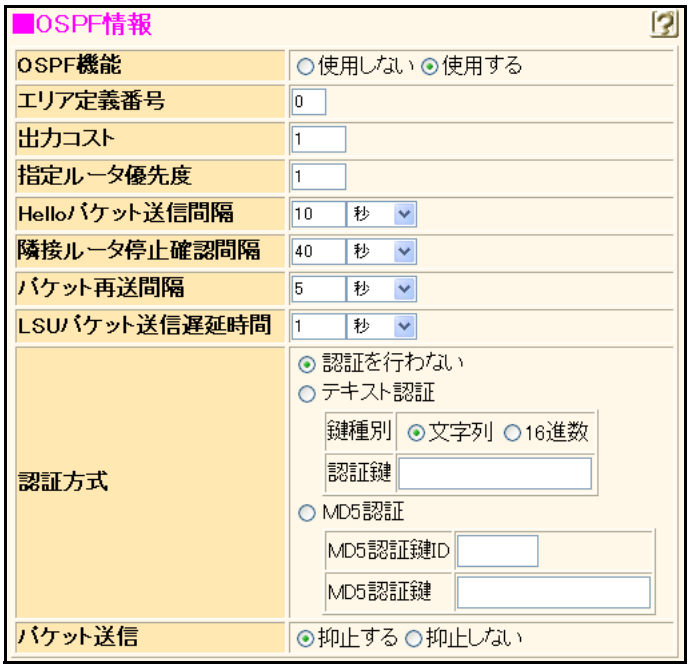
12. ［保存］ボタンをクリックします。

13. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

14. 以下の項目を指定します。

- OSPF 機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する



15. ［保存］ボタンをクリックします。

OSPF 関連を設定する

16. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

17. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

18. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

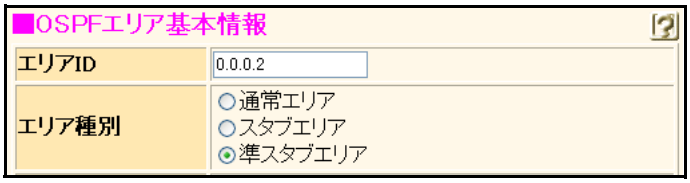
「OSPF エリア情報」が表示されます。

19. ［追加］ボタンをクリックします。

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

20. 以下の項目を指定します。

- エリア ID　→0.0.0.2
- エリア種別　→準スタブエリア



21. ［保存］ボタンをクリックします。

ルーティングマネージャ情報を設定する

22. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

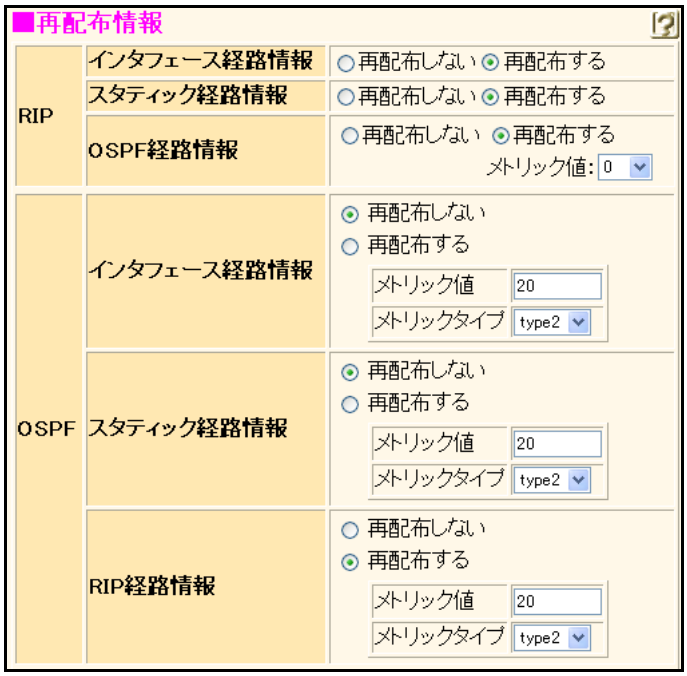
「ルーティングプロトコル情報」ページが表示されます。

23. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

24. 以下の項目を指定します。

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



25. ［保存］ボタンをクリックします。

26. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

26 OSPFの経路を制御する（IPv4）

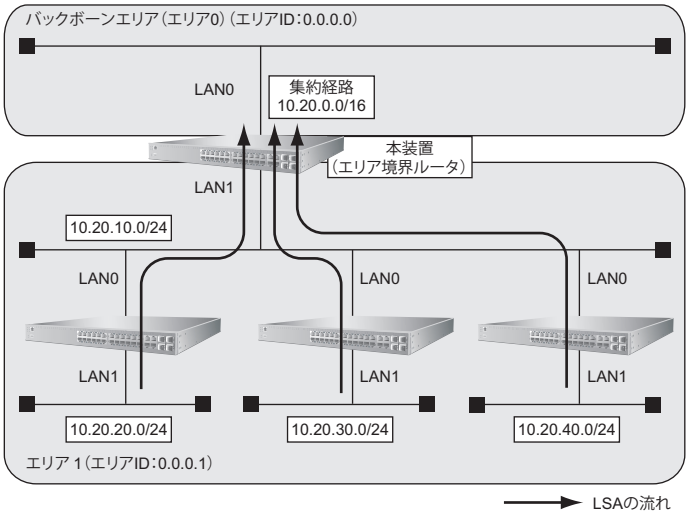
適用機種 ***SR-S732TR1, 752TR1***

本装置で、ほかのルータから受信する経路情報（LSA）に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

26.1 OSPFネットワークでエリアの経路情報（LSA）を集約する

適用機種 ***SR-S732TR1, 752TR1***

エリア内のLSAを、本装置（エリア境界ルータ）で集約して、バックボーンエリアへ取り込む場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースにIPアドレスの設定がされている
- IPフォワーディング機能を使用する設定がされている

● 経路情報の設計

- エリア内のLSAを、本装置（エリア境界ルータ）で集約してバックボーンエリアに取り込む

● 設定条件

- LAN0でのルーティングプロトコル　：OSPF
- LAN1でのルーティングプロトコル　：OSPF
- LAN0でのエリアID　：0.0.0.0
- LAN1でのエリアID　：0.0.0.1
- バックボーンエリアへの集約経路設定　：10.20.0.0/16

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

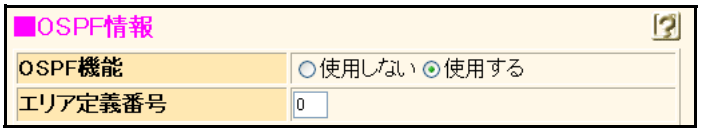
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5. 以下の項目を指定します。

- OSPF 機能　→使用する
- エリア定義番号　→0



6. ［保存］ボタンをクリックします。

7. 手順 1.～6. を参考に、LAN1 情報で以下の項目を設定します。

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

OSPF 関連を設定する

8. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

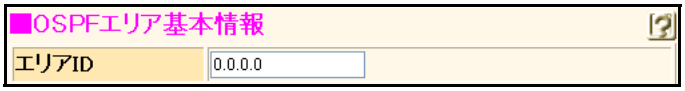
「OSPF エリア情報」が表示されます。

11. ［追加］ボタンをクリックします。

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

12. 以下の項目を指定します。

- エリア ID　→0.0.0.0



13. ［保存］ボタンをクリックします。

14. 画面上部の「ルーティングプロトコル情報」をクリックします。

OSPF 関連項目と「OSPF エリア情報」が表示されます。

15. 手順 11.～13. を参考に、以下の項目を設定します。

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID →0.0.0.1

16. OSPF エリア情報（1）の「経路集約情報」をクリックします。

「経路集約情報」が表示されます。

17. 以下の項目を指定します。

- ネットワークアドレス →10.20.0.0
- ネットマスク →16（255.255.0.0）

18. ［追加］ボタンをクリックします。

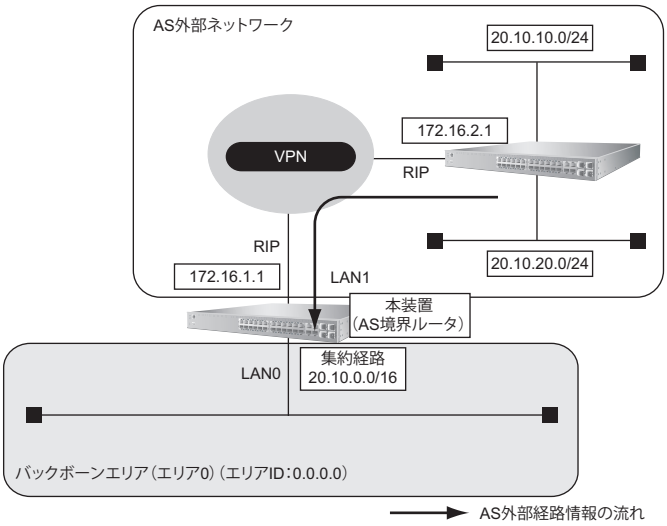
19. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

26.2 AS 外部経路を集約して OSPF ネットワークに広報する

適用機種 ***SR-S732TR1, 752TR1***

AS 外部（OSPF 以外）のネットワークの経路情報を本装置（AS 境界ルータ）で集約して、バックボーンエリアに広報する場合の設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- LAN1 インタフェースに RIPv2 を使用する設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

- AS 外部経路情報を本装置（AS 境界ルータ）で集約して OSPF ネットワーク（バックボーンエリア）に広報する
- その他の AS 外部経路情報はすべて遮断する

● 設定条件

- LAN0 でのルーティングプロトコル　：OSPF
- LAN0 でのエリア ID　：0.0.0.0
- バックボーンエリアへの集約経路設定　：20.10.0.0/16
- OSPF に再配布する RIP 経路　：20.10.0.0/16 でマスクした結果が一致する経路だけを再配布

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

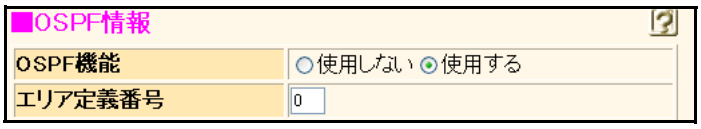
「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

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

5. **以下の項目を指定します。**
   - OSPF 機能　→使用する
   - エリア定義番号　→0



6. **［保存］ボタンをクリックします。**

OSPF 関連を設定する

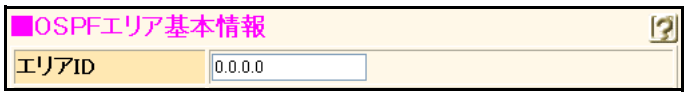
7. **設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。**
   「ルーティングプロトコル情報」ページが表示されます。

8. **「OSPF 関連」をクリックします。**
   OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

9. **OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**
   「OSPF エリア情報」が表示されます。

10. **［追加］ボタンをクリックします。**
    OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

11. **以下の項目を指定します。**
    - エリア ID　→0.0.0.0



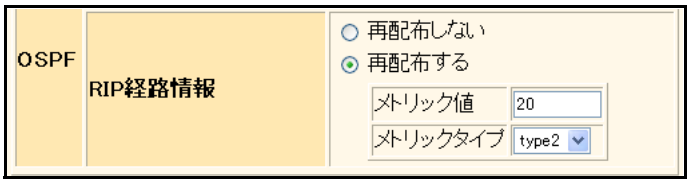
12. **［保存］ボタンをクリックします。**

ルーティングマネージャ情報を設定する

13. **設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。**
    「ルーティングプロトコル情報」ページが表示されます。

14. **「ルーティングマネージャ情報」をクリックします。**
    ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

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



16. **［保存］ボタンをクリックします。**

OSPF 関連を設定する

17. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

18. 「OSPF 関連」をクリックします。

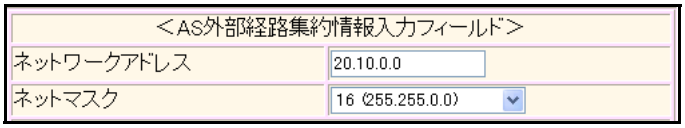
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

19. OSPF 関連の設定項目の「AS 外部経路集約情報」をクリックします。

「AS 外部経路集約情報」が表示されます。

20. 以下の項目を指定します。

- ネットワークアドレス →20.10.0.0
- ネットマスク →16（255.255.0.0）



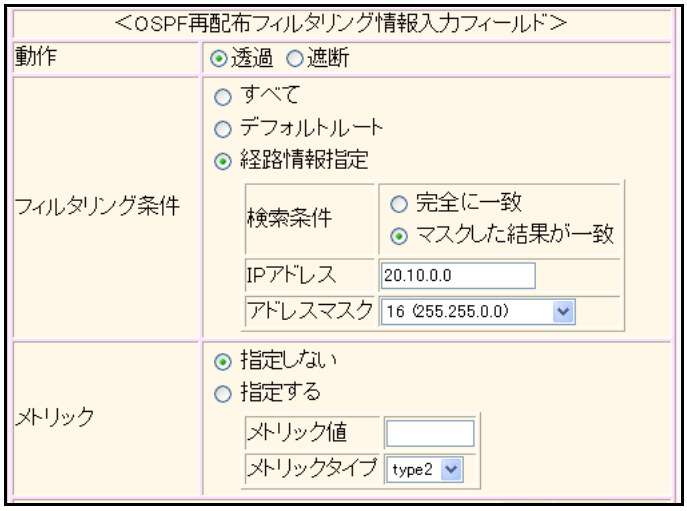
21. ［追加］ボタンをクリックします。

22. OSPF 関連項目の「OSPF 再配布フィルタリング情報」をクリックします。

「OSPF 再配布フィルタリング情報」が表示されます。

23. 以下の項目を指定します。

- 動作 →透過
- フィルタリング条件 →経路情報指定
  検索条件 →マスクした結果が一致
  IP アドレス →20.10.0.0
  アドレスマスク →16（255.255.0.0）
- メトリック →指定しない



24. ［追加］ボタンをクリックします。

25.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→遮断
- フィルタリング条件　→すべて
- メトリック　→指定しない

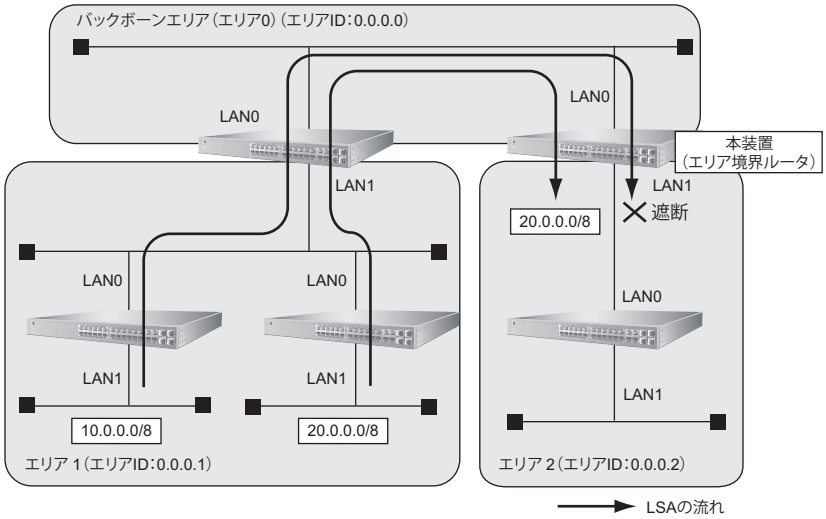
26.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

26.3 エリア境界ルータで不要な経路情報（LSA）を遮断する

適用機種 ***SR-S732TR1, 752TR1***

エリア境界ルータで、通信に使用しないTYPE3 サマリ LSA の経路情報を遮断する設定方法を説明します。



● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- IP フォワーディング機能を使用する設定がされている

● 経路情報の設計

- エリア 1 の 10.0.0.0/8 のネットワークとエリア 2 のネットワークでは通信を行わないため、10.0.0.0/8 の経路情報を遮断する
- その他はすべて透過させる

● 設定条件

- LAN0 でのルーティングプロトコル　：OSPF
- LAN1 でのルーティングプロトコル　：OSPF
- LAN0 でのエリア ID　：0.0.0.0
- LAN1 でのエリア ID　：0.0.0.2
- 10.0.0.0/8 の LSA を遮断

上記の経路情報に従って設定する場合の設定例を示します。

LAN 情報を設定する

1. 設定メニューの詳細設定で、「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

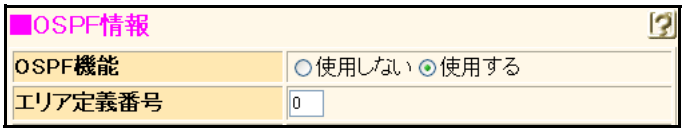
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. **IP 関連の設定項目の「OSPF 情報」をクリックします。**

「OSPF 情報」が表示されます。

5. **以下の項目を指定します。**

- OSPF 機能　→使用する
- エリア定義番号　→0



6. **［保存］ボタンをクリックします。**

7. **手順 2.～6. を参考に、以下の項目を設定します。**

「LAN1 情報」-「IP 関連」-「OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→1

OSPF 関連を設定する

8. **設定メニューの詳細設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

9. **「OSPF 関連」をクリックします。**

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10. **OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**

「OSPF エリア情報」が表示されます。

11. **［追加］ボタンをクリックします。**

OSPF エリア情報（0）の設定項目と「OSPF エリア基本情報」が表示されます。

12. **以下の項目を指定します。**

- エリア ID　→0.0.0.0

13. **［保存］ボタンをクリックします。**

14. **画面上部の「ルーティングプロトコル情報」をクリックします。**

OSPF 関連項目と「OSPF エリア情報」が表示されます。

15. **手順 11.～13. を参考に、以下の項目を設定します。**

「OSPF エリア情報（1）」-「OSPF エリア基本情報」

- エリア ID　→0.0.0.2

16. **画面上部の「ルーティングプロトコル情報」をクリックします。**

OSPF 関連項目と「OSPF エリア情報」が表示されます。

17. **エリア定義番号（1）の［修正］ボタンをクリックします。**

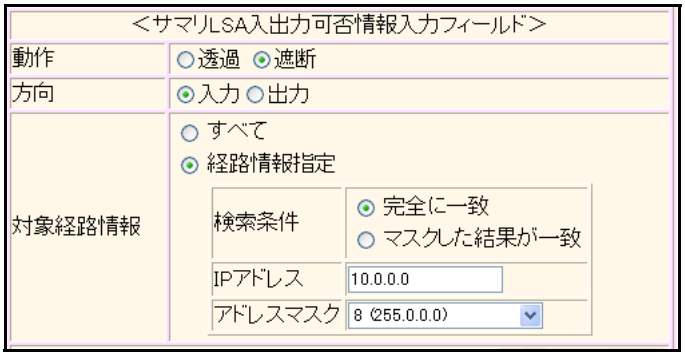
OSPF エリア情報（1）の設定項目と「OSPF エリア基本情報」が表示されます。

18. **OSPF エリア情報（1）の設定項目の「サマリ LSA 入出力可否情報」をクリックします。**

「サマリ LSA 入出力可否情報」が表示されます。

19. **以下の項目を指定します。**

- 動作 →遮断
- 方向 →入力
- 対象経路情報 →経路情報指定
  検索条件 →完全に一致
  IP アドレス →10.0.0.0
  アドレスマスク →8（255.0.0.0）



20. **［追加］ボタンをクリックします。**

21. **手順 19.～20. を参考に、以下の項目を設定します。**

- 動作 →透過
- 方向 →入力
- 対象経路情報 →すべて

22. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

27　OSPF 機能を使う（IPv6）

適用機種　*SR-S732TR1, 752TR1*

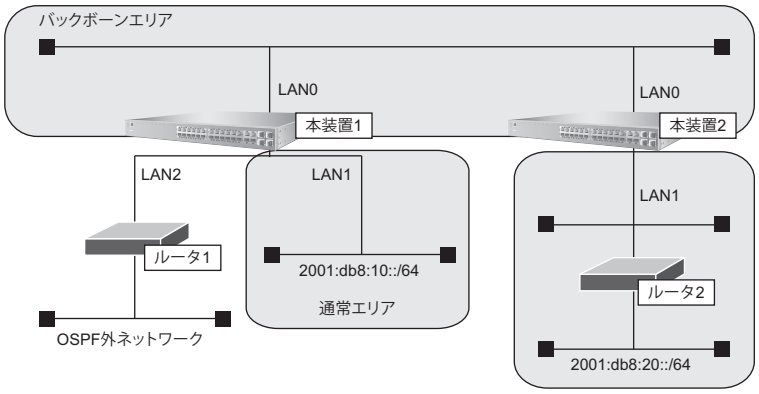
27.1　OSPF ネットワークを構築する

OSPF（IPv6）を使用したネットワークの構築について説明します。

こんな事に気をつけて

- **ルータは、各エリアに 30 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2 つ以上のエリアの指定ルータ（DR：Designated Router）とならないように設定してください。**
- **LAN を使用した隣接 OSPF ルータと MTU 値が一致しない場合は、隣接関係を構築できません。**
- **経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができても、OSPF の経路は、経路情報に反映されません。**
- **本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません（LSDB オーバフロー）。**
  また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源を再投入したり、［設定反映］ボタンや［再起動］ボタンをクリックしたりしても、正常に通信できるまでに最大 60 分かかることがあります。
- **OSPF で使用するインタフェースは、以下の条件で使用してください。**

本装置が DR を兼務する場合	本装置が DR を兼務しない場合
（10000÷本装置保有 LSA 数）未満	（20000÷本装置保有 LSA 数）未満



● 前提条件

- 本装置 1、2 のすべてのインタフェースで IPv6 機能を利用する設定がされている
- 本装置 1、2 に IPv6 フォワーディング機能を使用する設定がされている
- 本装置 1 の LAN1 には、グローバルアドレスが設定されている
- 本装置 1 の LAN2 には、OSPF 外ネットワークへの経路がスタティック設定されている

● 設定条件

- 本装置 1 はバックボーンエリアと通常エリアのエリア境界ルータであり、かつ、OSPF 外ネットワークへ到達するための AS 境界ルータとして運用する
- 本装置 2 はバックボーンエリアとスタブエリアのエリア境界ルータとして運用する。また、バックボーンエリアでは指定ルータとして運用する

- 各エリア ID は、以下のとおり
  バックボーンエリア　　: 0.0.0.0
  通常エリア　　: 0.0.0.1
  スタブエリア　　: 0.0.0.2

[本装置 1]

- LAN0 はバックボーンエリアに属する
- LAN1 は通常エリアに属し、ほかにルータが接続されていないため、Passive-interface として OSPF パケットを送信しないようにする
- OSPF ルータ ID は 100.0.0.1 とする
- スタティック経路を OSPF に再配布する

[本装置 2]

- LAN0 はバックボーンエリアに属し、バックボーンエリアの指定ルータとするため、指定ルータ優先度に 255 を設定する
- LAN1 はスタブエリアとする
- OSPF ルータ ID は 100.0.0.2 とする

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

LAN 情報を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3.　「IPv6 関連」をクリックします。

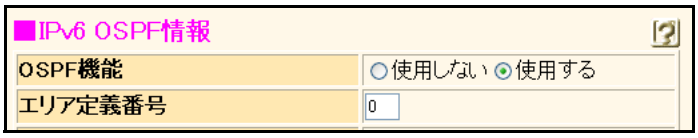
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　IPv6 関連の設定項目の「IPv6 OSPF 情報」をクリックします。

「IPv6 OSPF 情報」が表示されます。

5.　以下の項目を指定します。

- OSPF 機能　　→使用する
- エリア定義番号　　→0



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、「LAN1 情報」で以下の項目を指定します。

「LAN1 情報」-「IPv6 関連」-「IPv6 OSPF 情報」

- OSPF 機能　→使用する
- エリア定義番号　→ 1
- パケット送信　→抑止する

IPv6 OSPF 関連を設定する

8.　設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

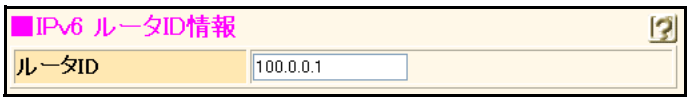
「ルーティングプロトコル情報」ページが表示されます。

9.　「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

10.　以下の項目を指定します。

- ルータ ID　→ 100.0.0.1



11.　［保存］ボタンをクリックします。

12.　IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。

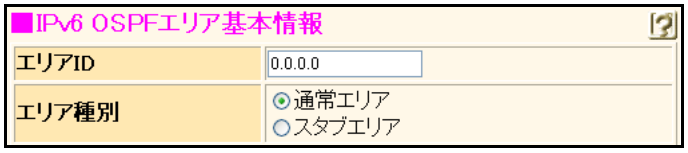
「IPv6 OSPF エリア情報」が表示されます。

13.　［追加］ボタンをクリックします。

IPv6 OSPF エリア情報（0）の「IPv6 OSPF エリア基本情報」が表示されます。

14.　以下の項目を指定します。

- エリア ID　→ 0.0.0.0
- エリア種別　→通常エリア



15.　［保存］ボタンをクリックします。

16.　画面上部のルーティングプロトコル情報をクリックします。

IPv6 OSPF 関連項目と「IPv6 OSPF エリア情報」が表示されます。

17.　手順 13.～15. を参考に、以下の項目を指定します。

- エリア ID　→ 0.0.0.1
- エリア種別　→通常エリア

ルーティングマネージャ情報を設定する

18.　設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

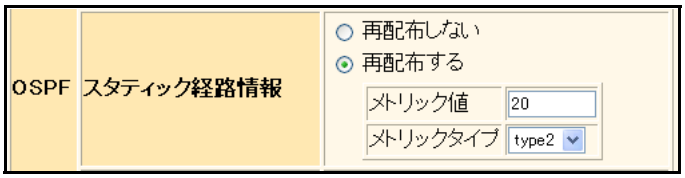
「ルーティングプロトコル情報」ページが表示されます。

19. 「IPv6 ルーティングマネージャ情報」をクリックします。

IPv6 ルーティングマネージャ情報の設定項目と「IPv6 再配布情報」が表示されます。

20. 以下の項目を指定します。

- OSPF
  スタティック経路情報　　→再配布する



21. ［保存］ボタンをクリックします。

22. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「LAN0 情報」-「IPv6 関連」
「IPv6 OSPF 情報」

- OSPF 機能　　→ 使用する
- エリア定義番号　　→ 0
- 指定ルータ優先度　　→ 255

「LAN1 情報」-「IPv6 関連」
「IPv6 OSPF 情報」

- OSPF 機能　　→ 使用する
- エリア定義番号　　→ 1

「ルーティングプロトコル情報」-「IPv6 OSPF 関連」
「IPv6 ルータ ID 情報」

- ルータ ID　　→ 100.0.0.2

「IPv6 OSPF エリア情報（0）」-「IPv6 OSPF 基本情報」

- エリア ID　　→ 0.0.0.0
- エリア種別　　→通常エリア

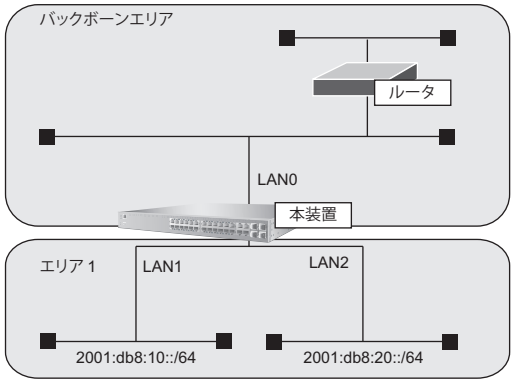
「IPv6 OSPF エリア情報（1）」-「IPv6 OSPF 基本情報」

- エリア ID　　→ 0.0.0.2
- エリア種別　　→スタブエリア

27.2 エリア境界ルータでエリア内部経路を集約する

適用機種 ***SR-S732TR1, 752TR1***

エリア境界ルータで、エリア内経路を集約してほかのエリアに広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定がされている
- IPv6 フォワーディング機能を使用する設定がされている
- 本装置はバックボーンエリアとエリア 1 のエリア境界ルータとして運用し、LAN0、LAN1、LAN2 で OSPF を使用する
- OSPF ルータ ID は、100.0.0.1
- 各エリア ID は、以下のとおり
  バックボーンエリア　　: 0.0.0.0（エリア定義番号 0）
  エリア 1　　: 0.0.0.1（エリア定義番号 1）
- 各インタフェースの IP アドレスは、以下のとおり
  LAN1　　: 2001:db8:10::1/64
  LAN2　　: 2001:db8:20::1/64

● 設定条件

- エリア 1 のエリア内部経路（2001:db8:10::/64、2001:db8:20::/64）は、集約経路（2001:db8::/32、コスト 100）としてバックボーンエリアに広報する

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

IPv6 OSPF 関連を設定する

1. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

2. 「IPv6 OSPF 関連」をクリックします。

IPv6 OSPF 関連の設定項目と「IPv6 ルータ ID 情報」が表示されます。

3. IPv6 OSPF 関連の設定項目の「IPv6 OSPF エリア情報」をクリックします。

「IPv6 OSPF エリア情報」が表示されます。

4. エリア定義番号1の［修正］ボタンをクリックします。

IPv6 OSPF エリア情報（1）の「IPv6 OSPF エリア基本情報」が表示されます。

5. 「IPv6経路集約情報」をクリックします。

「IPv6経路集約情報」が表示されます。

6. 以下の項目を指定します。

- プレフィックス／プレフィックス長　→2001:db8::/32
- コスト　→100

7. ［追加］ボタンをクリックします。

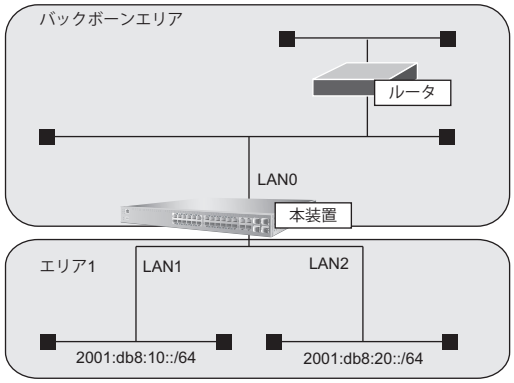
8. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

27.3 エリア境界ルータで不要な経路情報を遮断する

適用機種 ***SR-S732TR1, 752TR1***

エリア境界ルータで、ほかのエリアに対し特定のエリア内経路（エリア間プレフィックスLSA）を遮断して広報する設定について説明します。



● 前提条件

- 本装置のすべてのインタフェースでIPv6機能を利用する設定がされている
- IPv6フォワーディング機能を使用する設定がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、LAN0、LAN1、LAN2でOSPFを使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり
  バックボーンエリア　　: 0.0.0.0（エリア定義番号0）
  エリア1　　: 0.0.0.1（エリア定義番号1）
- 各インタフェースのIPアドレスは、以下のとおり
  LAN1　　: 2001:db8:10::1/64
  LAN2　　: 2001:db8:20::1/64

● 設定条件

- エリア1からバックボーンエリアへの広報で、2001:db8:20::/64は破棄し、その他のエリア内部経路は透過させる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置を設定する

1. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

2. 「IPv6 OSPF関連」をクリックします。

IPv6 OSPF関連の設定項目と「IPv6ルータID情報」が表示されます。

3. IPv6 OSPF関連の設定項目の「IPv6 OSPFエリア情報」をクリックします。

「IPv6 OSPFエリア情報」が表示されます。

4. エリア定義番号1の［修正］ボタンをクリックします。

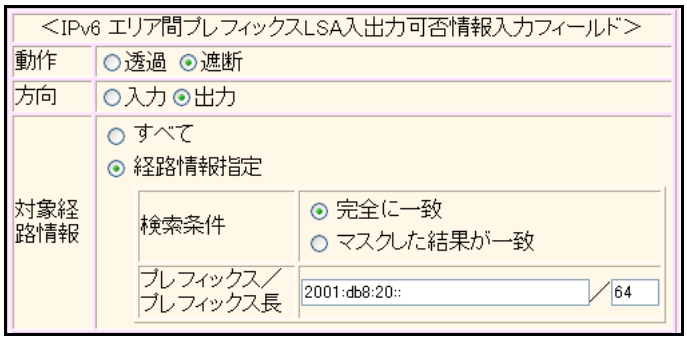
IPv6 OSPF エリア情報（1）の「IPv6 OSPF エリア基本情報」が表示されます。

5. 「IPv6エリア間プレフィックスLSA入出力可否情報」をクリックします。

「IPv6エリア間プレフィックスLSA入出力可否情報」が表示されます。

6. 以下の項目を指定します。

- 動作 →遮断
- 方向 →出力
- 対象経路情報 →経路情報指定
  検索条件 →完全に一致
  プレフィックス／プレフィックス長 →2001:db8:20::/64



7. ［追加］ボタンをクリックします。

8. 手順6.～7.を参考に、以下の項目を設定します。

- 動作 →透過
- 方向 →出力
- 対象経路情報 →すべて

9. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

28　マルチキャスト機能を使う

適用機種　***SR-S732TR1, 752TR1***

本装置には、マルチキャスト機能を動作させるために以下の2種類のプロトコルがあります。

- PIM-DM プロトコル
- PIM-SM プロトコル

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

参照　マニュアル「機能説明書」

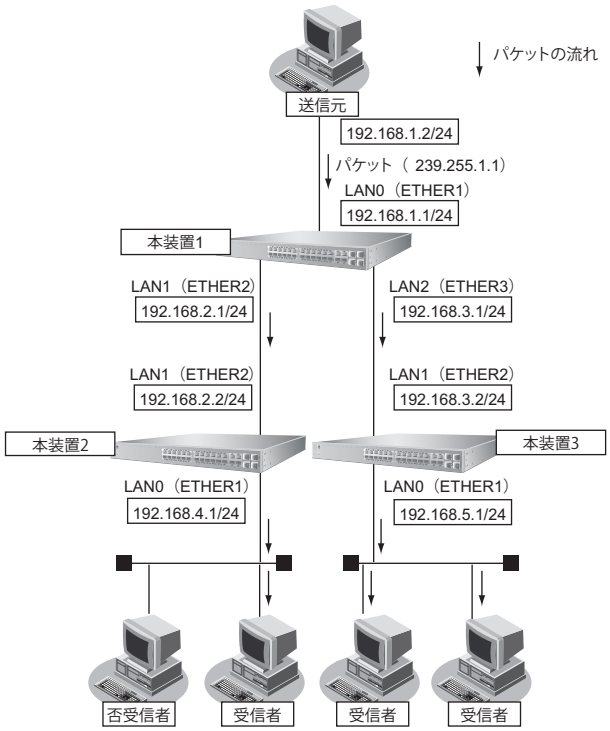
28.1　マルチキャスト機能（PIM-DM）を使う

適用機種　***SR-S732TR1, 752TR1***

マルチキャスト機能（PIM-DM）を使用すると、会社などのLAN内で、動画や音声などを配送することができます。

こんな事に気をつけて

マルチキャストでパケットを配送するルータは、すべてPIM-DMに対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。



ここでは、PIM-DMを利用してマルチキャストパケットを転送する場合の設定方法を説明します。

本装置1、本装置2、本装置3が以下のとおり設定されていることを前提とします。

● 前提条件

[本装置 1]

- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN0 の IP アドレス　：192.168.1.1/24
- LAN1 の IP アドレス　：192.168.2.1/24
- LAN2 の IP アドレス　：192.168.3.1/24

[本装置 2]

- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN0 の IP アドレス　：192.168.4.1/24
- LAN1 の IP アドレス　：192.168.2.2/24

[本装置 3]

- ユニキャストのルーティングテーブルの作成に RIP を使用する
- LAN0 の IP アドレス　：192.168.5.1/24
- LAN1 の IP アドレス　：192.168.3.2/24

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-DM を利用する

[本装置 1]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2 を使用し、それぞれ、ETHER1、ETHER2、ETHER3 に割り当てる

[本装置 2]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる

[本装置 3]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3.　「IP 関連」をクリックします。

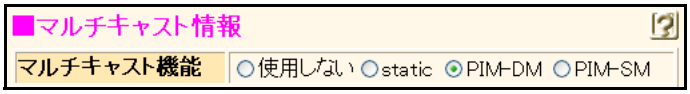
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4.　IP 関連の設定項目の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」が表示されます。

5.　以下の項目を指定します。

- マルチキャスト機能　→PIM-DM



6.　［保存］ボタンをクリックします。

7.　手順 1.～6. を参考に、以下の項目を設定します。

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

「LAN2 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

8.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

本装置 3 を設定する

「本装置 1 を設定する」を参考に、本装置 3 を設定します。

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→PIM-DM

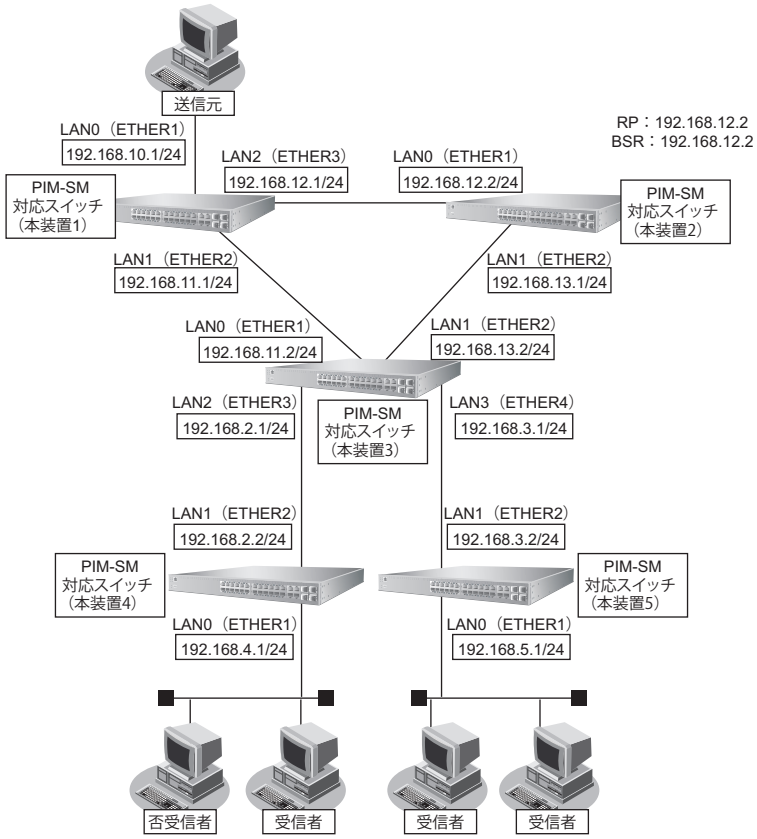
28.2 マルチキャスト機能（PIM-SM）を使う

適用機種 ***SR-S732TR1, 752TR1***

マルチキャスト機能（PIM-SM）を使用すると、インターネットなど、十分な帯域を保証されないネットワーク上で、マルチキャストパケットを配送することができます。

こんな事に気をつけて

- **マルチキャストパケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。**
- **ネットワーク内に BSR（Bootstrap Router：ブートストラップルータ）として動作するルータを 1 台以上置く必要があります。BSR は RP（Rendezvous Point：ランデブーポイント）の情報を広報します。**
- **ネットワーク内に RP として動作するルータを 1 台以上置く必要があります。パケットの配送は、RP を配送樹の頂点として開始され、その後、最短経路（SPT：Shortest Path Tree）に切り替わります。**
- **PIM-SM ではマルチキャストパケットの配送を RP を配送樹の頂点として開始するため、RP はネットワークの中心付近に置くことをお勧めします。**



ここでは、PIM-SM を利用してマルチキャストパケットを転送する場合の設定方法を説明します。

マルチキャストパケットは、はじめは RP である本装置 2 を経由して、本装置 1 →本装置 2 →本装置 3 →本装置 4 の順に配送されます（一度、本装置 1 から本装置 2 に送られ、本装置 2 を配送樹の頂点として配送されます）。本装置 4 へのパケット転送開始直後に、本装置 4 は SPT への切り替えを開始します。切り替えが行われると、本装置 1 →本装置 3 →本装置 4 のように、最短経路を利用して配送されます（本装置 1 を配送樹の頂点として配送されます）。同様の切り替えが本装置 5 でも行われます。

ここでは、本装置 1、本装置 2、本装置 3、本装置 4、本装置 5 が以下のとおりに設定されていることを前提とします。

● 前提条件

- ユニキャストのルーティングテーブルの作成に RIP を使用する

[本装置 1]

- LAN0 の IP アドレス　：192.168.10.1/24
- LAN1 の IP アドレス　：192.168.11.1/24
- LAN2 の IP アドレス　：192.168.12.1/24

[本装置 2]

- LAN0 の IP アドレス　：192.168.12.2/24
- LAN1 の IP アドレス　：192.168.13.1/24

[本装置 3]

- LAN0 の IP アドレス　：192.168.11.2/24
- LAN1 の IP アドレス　：192.168.13.2/24
- LAN2 の IP アドレス　：192.168.2.1/24
- LAN3 の IP アドレス　：192.168.3.1/24

[本装置 4]

- LAN0 の IP アドレス　：192.168.4.1/24
- LAN1 の IP アドレス　：192.168.2.2/24

[本装置 5]

- LAN0 の IP アドレス　：192.168.5.1/24
- LAN1 の IP アドレス　：192.168.3.2/24

● 設定条件

- マルチキャスト・ルーティングプロトコルには PIM-SM を利用する
  RP　：本装置 2（192.168.12.2）
  BSR　：本装置 2（192.168.12.2）
- SPT への切り替えを行う（初期値）

[本装置 1]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2 を使用し、それぞれ、ETHER1、ETHER2、ETHER3 に割り当てる

[本装置 2]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる
- RP　：192.168.12.2
- BSR　：192.168.12.2

[本装置 3]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2、LAN3 を使用し、それぞれ、ETHER1、ETHER2、ETHER3、ETHER4 に割り当てる

[本装置 4]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる

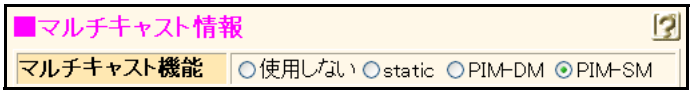
[本装置 5]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1. **設定メニューの詳細設定で「LAN 情報」をクリックします。**
   「LAN 情報」ページが表示されます。
2. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**
   「LAN0 情報」ページが表示されます。
3. **「IP 関連」をクリックします。**
   IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. **IP 関連の設定項目の「マルチキャスト情報」をクリックします。**
   「マルチキャスト情報」が表示されます。
5. **以下の項目を指定します。**
   - マルチキャスト機能　　→ PIM-SM



6. **［保存］ボタンをクリックします。**
7. **手順 1.～6. を参考に、以下の項目を設定します。**
   「LAN1 情報」-「IP 関連」-「マルチキャスト情報」
   - マルチキャスト機能　　→ PIM-SM

   「LAN2 情報」-「IP 関連」-「マルチキャスト情報」
   - マルチキャスト機能　　→ PIM-SM
8. **画面左側の［設定反映］ボタンをクリックします。**
   設定した内容が有効になります。

本装置 2 を設定する

1. **「本装置 1 を設定する」を参考に、以下の項目を設定します。**
   「LAN0 情報」-「IP 関連」-「マルチキャスト情報」
   - マルチキャスト機能　　→ PIM-SM

   「LAN1 情報」-「IP 関連」-「マルチキャスト情報」
   - マルチキャスト機能　　→ PIM-SM
2. **設定メニューの詳細設定で「マルチキャスト情報」をクリックします。**
   「マルチキャスト情報」ページが表示されます。
3. **「IP マルチキャスト情報」をクリックします。**
   「IP マルチキャスト情報」が表示されます。

4.　以下の項目を指定します。

- PIM-SM
  RP 候補　→する
  IP アドレス　→ 192.168.12.2
  BSR 候補　→する
  IP アドレス　→ 192.168.12.2

5.　［保存］ボタンをクリックします。

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

本装置 3 を設定する

「本装置 1 を設定する」を参考に、本装置 3 を設定します。

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

「LAN2 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

「LAN3 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

本装置 4 を設定する

「本装置 1 を設定する」を参考に、本装置 4 を設定します。

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

本装置 5 を設定する

「本装置 1 を設定する」を参考に、本装置 5 を設定します。

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

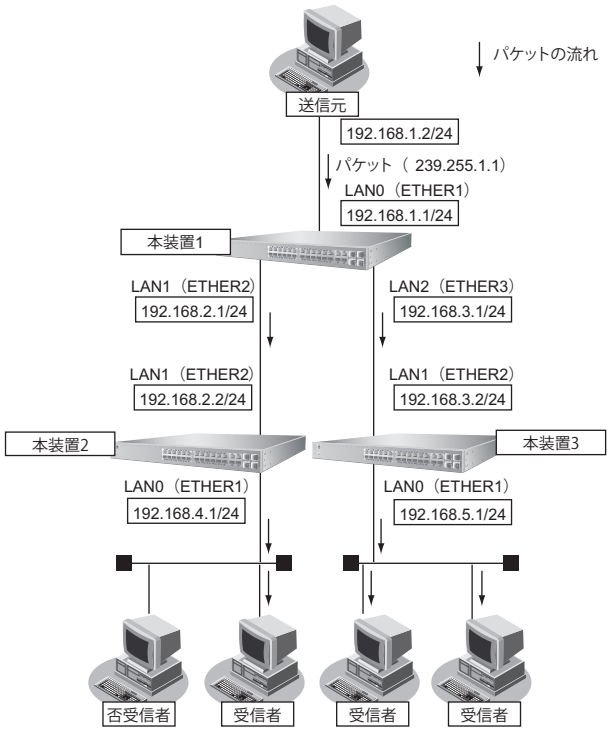
「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ PIM-SM

28.3 マルチキャスト機能（スタティックルーティング）を使う

適用機種 ***SR-S732TR1, 752TR1***

マルチキャスト機能（スタティックルーティング）を利用すると、マルチキャストパケットが配送される経路を静的に設定することができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。本装置1、本装置2、本装置3が以下のとおり設定されていることを前提とします。

● 前提条件

[本装置1]

- LAN0のIPアドレス　：192.168.1.1/24
- LAN1のIPアドレス　：192.168.2.1/24
- LAN2のIPアドレス　：192.168.3.1/24

[本装置2]

- LAN0のIPアドレス　：192.168.4.1/24
- LAN1のIPアドレス　：192.168.2.2/24

[本装置3]

- LAN0のIPアドレス　：192.168.5.1/24
- LAN1のIPアドレス　：192.168.3.2/24

● 設定条件

- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする

[本装置 1]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1、LAN2 を 使用し、それぞれ、ETHER1、ETHER2、ETHER3 に割り当てる

[本装置 2]

- マルチキャストパケットを転送するインタフェースとして LAN0、LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる

[本装置 3]

- マルチキャストパケットを転送するインタフェースとして LAN0, LAN1 を使用し、それぞれ、ETHER1、ETHER2 に割り当てる

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置 1 を設定する

1. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

3. 「IP 関連」をクリックします。

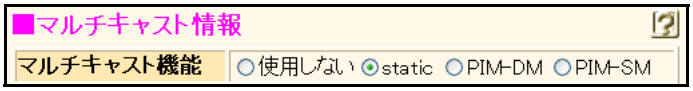
IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」が表示されます。

5. 以下の項目を指定します。

- マルチキャスト機能　→ static



6. ［保存］ボタンをクリックします。

7. 手順 1.～6. を参考に、以下の項目を設定します。

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ static

「LAN2 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ static

8. 設定メニューの詳細設定で「マルチキャスト情報」をクリックします。

「マルチキャスト情報」ページが表示されます。

9. 「IP マルチキャストスタティック経路情報」をクリックします。

「IP マルチキャストスタティック経路情報」が表示されます。

10. 以下の項目を指定します。

- 配送元ホストアドレス → 指定する
  → 192.168.1.2
- マルチキャストグループアドレス → 239.255.1.1
- 入力インタフェース → LAN0
- 出力インタフェース → lan1-lan2
- グループ参加 → しない

11. ［追加］ボタンをクリックします。

12. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

本装置 2 を設定する

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

「LAN 情報」

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能 → static

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能 → static

「マルチキャスト情報」

「IP マルチキャストスタティック経路情報」

- 配送元ホストアドレス → 指定する
  → 192.168.1.2
- マルチキャストグループアドレス → 239.255.1.1
- 入力インタフェース → LAN1
- 出力インタフェース → lan0
- グループ参加 → しない

本装置 3 を設定する

「本装置 1 を設定する」を参考に、本装置 3 を設定します。

「LAN 情報」

「LAN0 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ static

「LAN1 情報」-「IP 関連」-「マルチキャスト情報」

- マルチキャスト機能　→ static

「マルチキャスト情報」

「IP マルチキャストスタティック経路情報」

- 配送元ホストアドレス　→ 指定する
  → 192.168.1.2
- マルチキャストグループアドレス　→ 239.255.1.1
- 入力インタフェース　→ LAN1
- 出力インタフェース　→ lan0
- グループ参加　→ しない

29　IP フィルタリング機能を使う

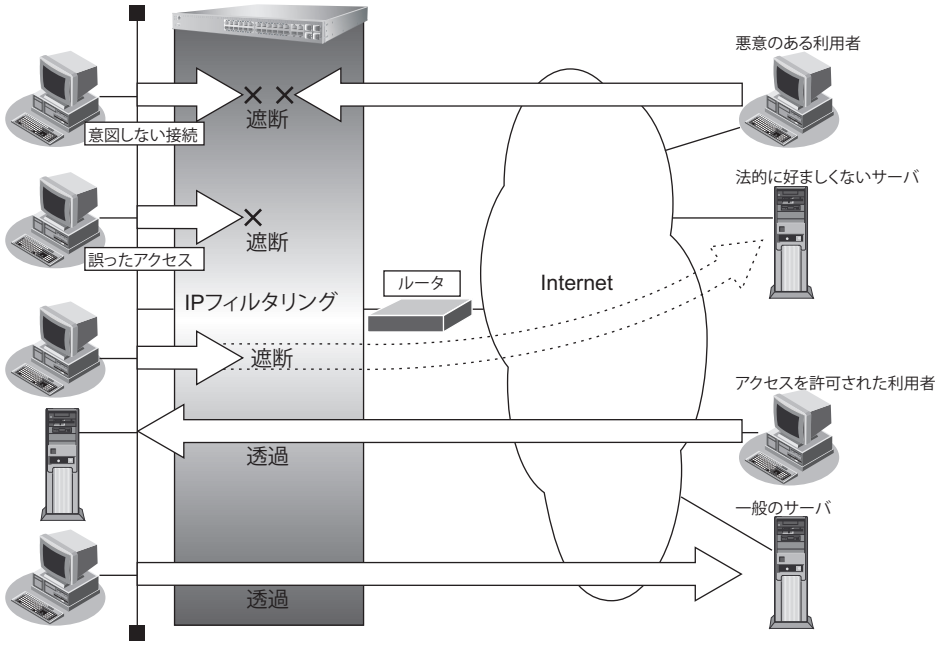
適用機種　全機種

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットを IP アドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させることができます。

☛ 参照　マニュアル「機能説明書」

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、フィルタリング機能 (IPv4/IPv6) および QoS 書き換え機能 (IPv4/IPv6) を同時に使用することができません。IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



IP フィルタリングの条件

本装置では、ACL 番号で指定した ACL 定義の中で、以下の条件を指定することによってデータの流れを制御できます。

- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- あて先情報（IP アドレス／アドレスマスク／ポート番号）
- IP パケットの TOS 値／ DSCP 値

ヒント

◆ IP アドレスとアドレスマスクの決め方

IP フィルタリング条件の要素には「IP アドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットの IP アドレスとアドレスマスクの論理積の結果が、指定した IP アドレスと一致したものに限ります。

IP フィルタリングの設計方針

IP フィルタリングの設計方針には大きく分類して以下の 2 つがあります。

A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる

B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する

ここでは、設計方針 A の例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する

また、設計方針 B の例として、以下の設定例について説明します。

- 外部の特定サーバへのアクセスだけを禁止する
- 外部から特定サーバへの ping だけを禁止する

こんな事に気をつけて

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

29.1 外部の特定サービスへのアクセスだけを許可する

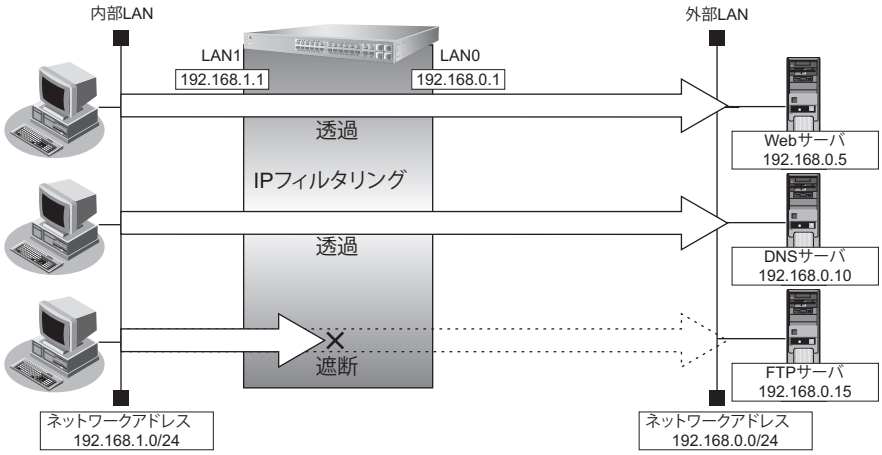
適用機種　全機種

ここでは、一時的にLANを作成し、外部LANのすべてのWebサーバに対してアクセスすることだけを許可し、ほかのサーバ（FTPサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、Webサーバ名を解決するために、DNSサーバへのアクセスは許可します。

補足　DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。
DNSサーバへのアクセスを許可することによって、Web サービス以外でドメイン名を指定した場合もDNSサーバへの発信が発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用することによって、DNSサーバへの発信を抑止することができます

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能(IPv4/IPv6)を同時に使用することができません。IPフィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS機能およびIPv4プロトコルを選択してください。



● フィルタリング設計

- 内部LANのホスト（192.168.1.0/24）から外部LANのWeb サーバへのアクセスを許可
- 内部LANのホスト（192.168.1.0/24）から外部LANのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- Webサーバへのアクセスを許可するには
  （1）192.168.1.0/24の任意のポートから、任意のWebサーバのポート80（http）へのTCPパケットを透過させる
- DNSサーバへのアクセスを許可するには
  （1）192.168.1.0/24の任意のポートから、DNSサーバのポート53（domain）へのUDPパケットを透過させる
- ICMPの通信を許可するためには
  （1）ICMPパケットを透過させる

- その他をすべて遮断するには
  (1)すべてのパケットを遮断する

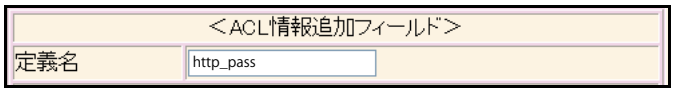
上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名　→ http_pass



3. [追加] ボタンをクリックします。

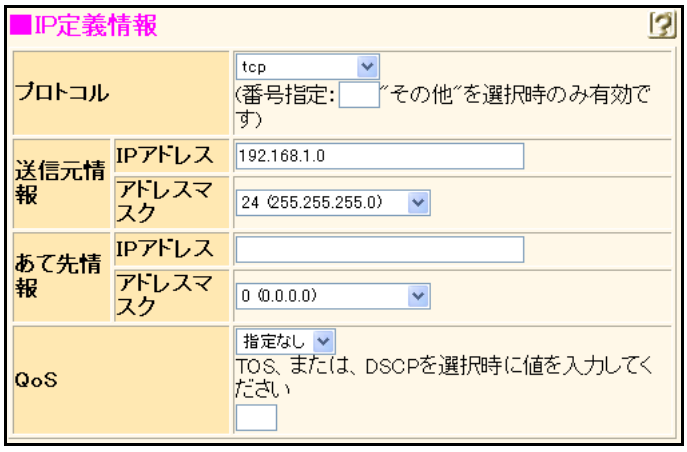
「ACL 定義情報（http_pass)」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→ 192.168.1.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→ 0（0.0.0.0）
- QoS　→指定なし



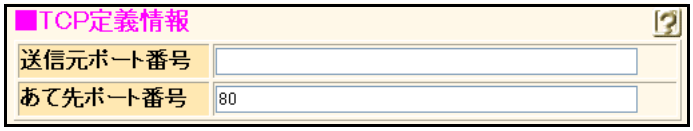
6. [保存] ボタンをクリックします。

7. 「TCP 定義情報」をクリックします。

「TCP 定義情報」が表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→80



9.　［保存］ボタンをクリックします。

10.　手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→dns_pass

「ACL 定義情報（dns_pass）」-「IP 定義情報」

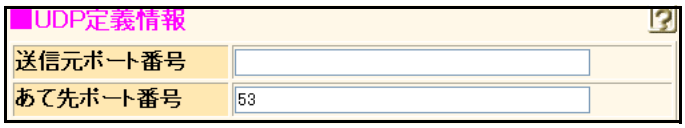
- プロトコル　→udp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→192.168.0.10
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし

11.　「UDP 定義情報」をクリックします。

「UDP 定義情報」が表示されます。

12.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→ 53



13.　［保存］ボタンをクリックします。

14.　手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→icmp_pass

「ACL 定義情報（icmp_pass）」-「IP 定義情報」

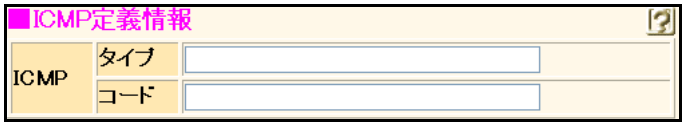
- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

15. 「ICMP 定義情報」をクリックします。

「ICMP 定義情報」が表示されます。

16. 以下の項目を指定します。

- ICMP
  タイプ →指定しない
  コード →指定しない



17. ［保存］ボタンをクリックします。

18. 手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名 →any_deny

「ACL 定義情報（any_deny）」-「IP 定義情報」

- プロトコル →すべて
- 送信元情報
  IP アドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- あて先情報
  IP アドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- QoS →指定なし

19. 設定メニューの詳細設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

21. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

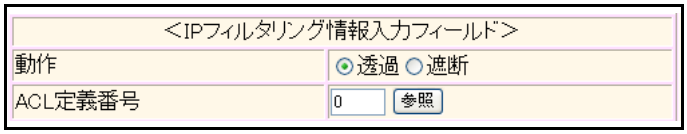
22. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

23. 以下の項目を指定します。

- 動作 →透過
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



24.　［追加］ボタンをクリックします。

25.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→透過
- ACL定義番号　→1

26.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→透過
- ACL定義番号　→2

27.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL定義番号　→3

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

29.2 外部の特定サービスへのアクセスだけを許可する（IPv6 フィルタリング）

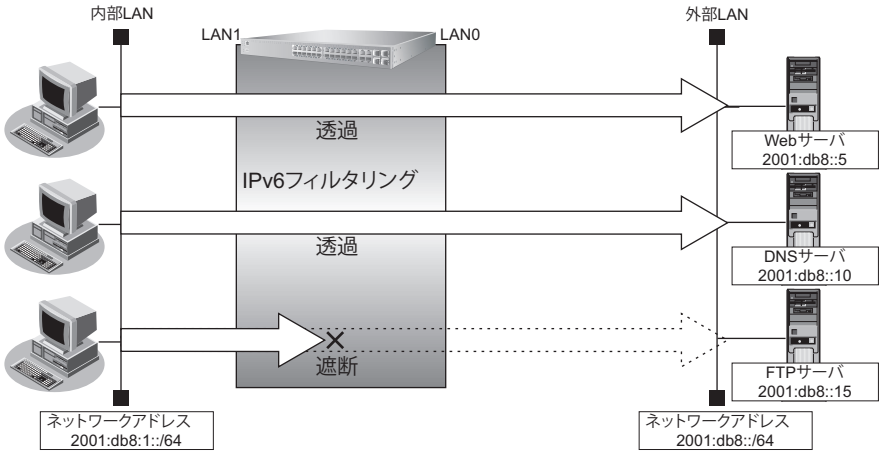
適用機種　全機種

ここでは、一時的に LAN を作成し、外部 LAN のすべての Web サーバに対してアクセスすることだけを許可し、ほかのサーバ（ftp サーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、Web サーバ名を解決するために、DNS サーバへのアクセスは許可します。

補足　DNS サーバに問い合わせが発生する場合、DNS サーバへのアクセスを許可する必要があります。
DNS サーバへのアクセスを許可することによって、Web サービス以外でドメイン名を指定した場合も DNS サーバへの発信が発生します。あらかじめ接続する Web サーバが決まっている場合は、本装置の DNS サーバ機能を利用することによって、DNS サーバへの発信を抑止することができます。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、フィルタリング機能 (IPv4/IPv6) および QoS 書き換え機能 (IPv4/IPv6) を同時に使用することができません。IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



● フィルタリング設計

- 内部 LAN 上のホスト（2001:db8:1::/64）から任意の Web サーバへのアクセスを許可
- 内部 LAN 上のホスト（2001:db8:1::/64）から外部 LAN の DNS サーバへのアクセスを許可
- ICMPv6 の通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6 の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6 の通信を透過させる設定を行ってください。

● フィルタリングルール

- Web サーバへのアクセスを許可するには
  （1）2001:db8:1::/64 の任意のポートから、任意のアドレスのポート 80（http）への TCP パケットを透過させる
- DNS サーバへのアクセスを許可するには
  （1）2001:db8:1::/64 の任意のポートから DNS サーバのポート 53（domain）への UDP パケットを透過させる
- ICMPv6 の通信を許可するためには
  （1）ICMPv6 パケットを透過させる
- その他をすべて遮断するには
  （1）すべてのパケットを遮断する

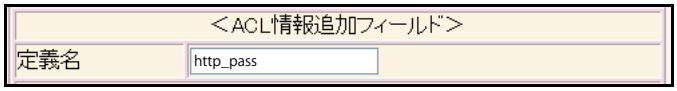
上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名　→ http_pass



3. ［追加］ボタンをクリックします。

「ACL 定義情報（http_pass）」ページが表示されます。

4. 「IPv6 定義情報」をクリックします。

「IPv6 定義情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル　→ tcp
- 送信元 IPv6 アドレス／プレフィックス　→ 2001:db8:1::/64
- あて先 IPv6 アドレス／プレフィックス　→指定しない
- QoS　→指定なし

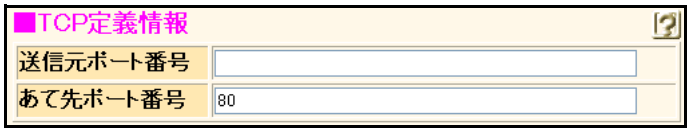
6. ［保存］ボタンをクリックします。

7. 「TCP 定義情報」をクリックします。

「TCP 定義情報」が表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→80



9.　［保存］ボタンをクリックします。

10.　手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→dns_pass

「ACL 定義情報（dns_pass）」-「IPv6 定義情報」

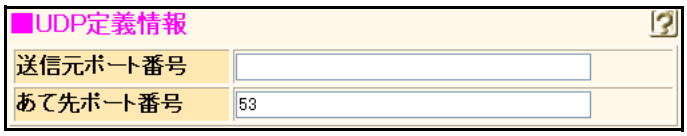
- プロトコル　→udp
- 送信元 IPv6 アドレス／プレフィックス　→2001:db8:1::/64
- あて先 IPv6 アドレス／プレフィックス　→指定しない
- QoS　→指定なし

11.　「UDP 定義情報」をクリックします。

「UDP 定義情報」が表示されます。

12.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53



13.　［保存］ボタンをクリックします。

14.　手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名　→icmp_pass

「ACL 定義情報（icmp_pass）」-「IPv6 定義情報」

- プロトコル　→icmpv6
- 送信元 IPv6 アドレス／プレフィックス　→指定しない
- あて先 IPv6 アドレス／プレフィックス　→指定しない
- QoS　→指定なし

15.　「ICMP 定義情報」をクリックします。

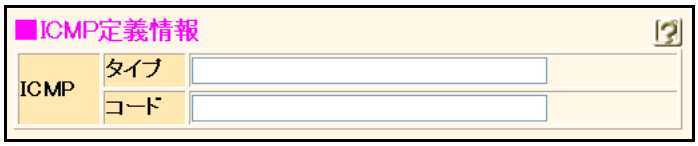
「ICMP 定義情報」が表示されます。

16. 以下の項目を指定します。

- ICMP

  タイプ →指定しない

  コード →指定しない



17. ［保存］ボタンをクリックします。

18. 手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名 →any_deny

「ACL 定義情報（any_deny）」-「IPv6 定義情報」

- プロトコル →すべて
- 送信元 IPv6 アドレス／プレフィックス →指定しない
- あて先 IPv6 アドレス／プレフィックス →指定しない
- QoS →指定なし

19. 設定メニューの詳細設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

21. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

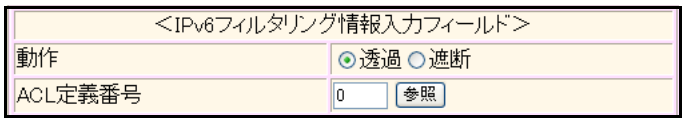
22. IPv6 関連の設定項目の「IPv6 フィルタリング情報」をクリックします。

「IPv6 フィルタリング情報」が表示されます。

23. 以下の項目を指定します。

- 動作 →透過
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



24. ［追加］ボタンをクリックします。

25. 手順 23.～24. を参考に、以下の項目を設定します。

- 動作 →透過
- ACL 定義番号 →1

26.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→透過
- ACL定義番号　→2

27.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL定義番号　→3

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

29.3 外部から特定サーバへのアクセスだけを許可する

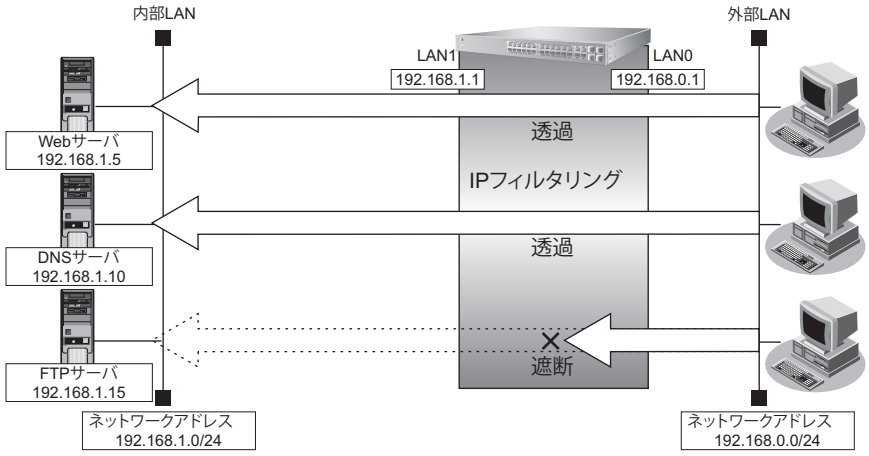
適用機種　全機種

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の設定方法を説明します。ただし、Webサーバ名を解決するためにDNSサーバへのアクセスは許可します。

補足　DNSサーバに問い合わせが発生する場合、DNSサーバへのアクセスを許可する必要があります。
DNSサーバへのアクセスを許可することによって、Webサービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するWebサーバが決まっている場合は、本装置のDNSサーバ機能を利用することで、DNSサーバへの問い合わせを抑止することができます。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能(IPv4/IPv6)を同時に使用することができません。IPフィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS機能およびIPv4プロトコルを選択してください。



● フィルタリング設計

- 内部LANのホスト（192.168.1.5/32）をWebサーバとして利用を許可
- 内部LANのネットワークへのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

● フィルタリングルール

- 内部LANのホストのWebサーバとしての利用を許可するには
  （1）192.168.1.5/32のポート80（http）へのTCPパケットを透過させる
- DNSサーバへのアクセスを許可するには
  （1）192.168.0.0/24の任意のポートからDNSサーバのポート53（domain）へのUDPパケットを透過させる
- ICMPの通信を許可するためには
  （1）ICMPパケットを透過させる
- その他をすべて遮断するには

（1）すべてのパケットを遮断する

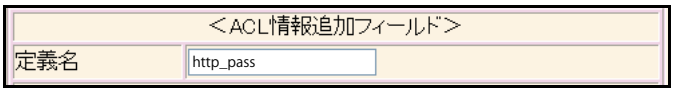
上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名　→ http_pass



3. ［追加］ボタンをクリックします。

「ACL 定義情報（http_pass）」ページが表示されます。

4. 「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5. 以下の項目を指定します。

- プロトコル　→ tcp
- 送信元情報
  IP アドレス　→ 192.168.0.0
  アドレスマスク　→ 24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→ 0（0.0.0.0）
- QoS　→指定なし

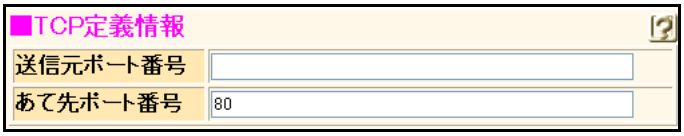
6. ［保存］ボタンをクリックします。

7. 「TCP 定義情報」をクリックします。

「TCP 定義情報」が表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→80



9.　［保存］ボタンをクリックします。

10.　手順1.～6.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名　→dns_pass

「ACL定義情報（dns_pass）」-「IP定義情報」

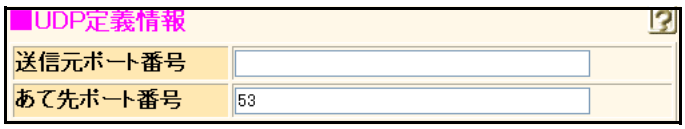
- プロトコル　→udp
- 送信元情報
  IPアドレス　→192.168.0.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IPアドレス　→192.168.1.10
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし

11.　「UDP定義情報」をクリックします。

「UDP定義情報」が表示されます。

12.　以下の項目を指定します。

- 送信元ポート番号　→指定しない
- あて先ポート番号　→53



13.　［保存］ボタンをクリックします。

14.　手順1.～6.を参考に、以下の項目を設定します。

「ACL情報」

- 定義名　→icmp_pass

「ACL定義情報（icmp_pass）」-「IP定義情報」

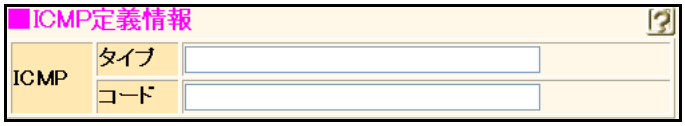
- プロトコル　→icmp
- 送信元情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IPアドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→指定なし

15. 「ICMP 定義情報」をクリックします。

「ICMP 定義情報」が表示されます。

16. 以下の項目を指定します。

- ICMP
  タイプ →指定しない
  コード →指定しない



17. ［保存］ボタンをクリックします。

18. 手順 1.～6. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名 →any_deny

「ACL 定義情報（any_deny）」-「IP 定義情報」

- プロトコル →すべて
- 送信元情報
  IP アドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- あて先情報
  IP アドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- QoS →指定なし

19. 設定メニューの詳細設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

20. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

21. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

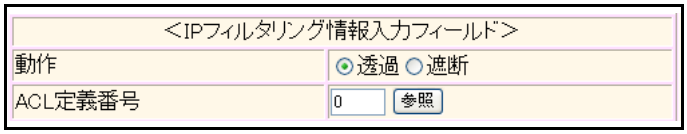
22. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

23. 以下の項目を指定します。

- 動作 →透過
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



24.　［追加］ボタンをクリックします。

25.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→透過
- ACL定義番号　→1

26.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→透過
- ACL定義番号　→2

27.　手順23.～24.を参考に、以下の項目を設定します。

- 動作　→遮断
- ACL定義番号　→3

28.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

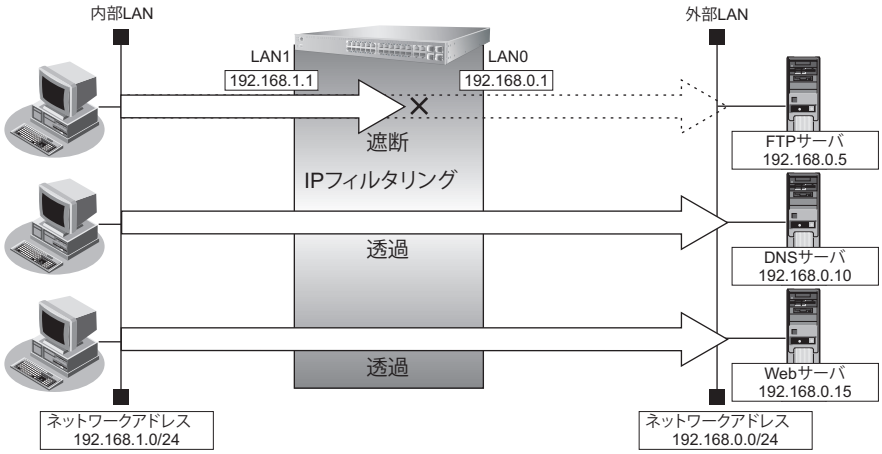
29.4 外部の特定サーバへのアクセスだけを禁止する

適用機種　全機種

ここでは、外部LANのFTPサーバに対するアクセスを禁止する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1では、フィルタリング機能(IPv4/IPv6)およびQoS書き換え機能(IPv4/IPv6)を同時に使用することができません。IPフィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS機能およびIPv4プロトコルを選択してください。



● フィルタリング設計

- 内部LANのホスト（192.168.1.0/24）から外部LANのFTPサーバ（192.168.0.5）へのアクセスを禁止

● フィルタリングルール

- FTPサーバへのアクセスを禁止するには

  (1)192.168.1.0/24から192.168.0.5のポート21（ftp）へのTCPパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→ftp_deny

＜ACL情報追加フィールド＞	
定義名	ftp_deny

3.　［追加］ボタンをクリックします。

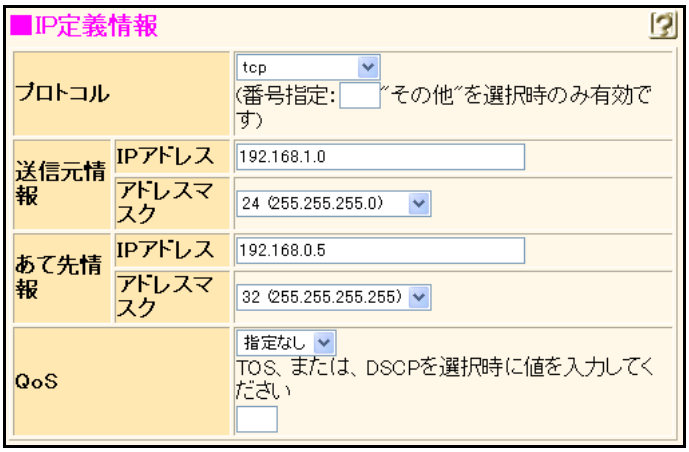
「ACL定義情報（ftp_deny)」ページが表示されます。

4.　「IP定義情報」をクリックします。

「IP定義情報」が表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IPアドレス　→192.168.0.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



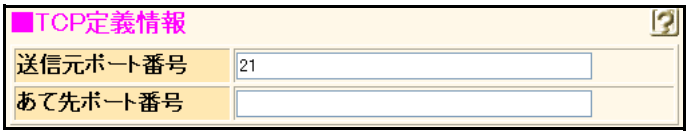
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」が表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　→21
- あて先ポート番号　→指定しない



9.　［保存］ボタンをクリックします。

10.　設定メニューの詳細設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

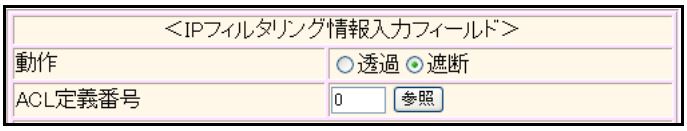
13.　IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14. 以下の項目を指定します。

- 動作 →遮断
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15. ［追加］ボタンをクリックします。

16. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

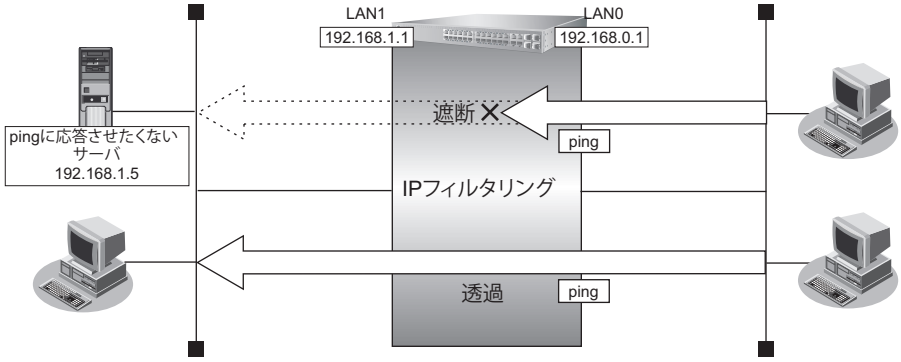
29.5 外部から特定サーバへの ping だけを禁止する

適用機種 全機種

ここでは、内部 LAN の特定のサーバに対する ping（ICMP ECHO）を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、フィルタリング機能 (IPv4/IPv6) および QoS 書き換え機能 (IPv4/IPv6) を同時に使用することができません。IP フィルタリングを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv4 プロトコルを選択してください。



● フィルタリング設計

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止
- その他はすべて通過

● フィルタリングルール

- 内部 LAN のサーバ（192.168.1.5/32）に対して外部からの ping（ICMP ECHO）を禁止するには
  (1) 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  (1) すべてのパケットを透過させる

上記のフィルタリングルールに従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →ping_deny

＜ACL情報追加フィールド＞	
定義名	ping_deny

3. [追加] ボタンをクリックします。

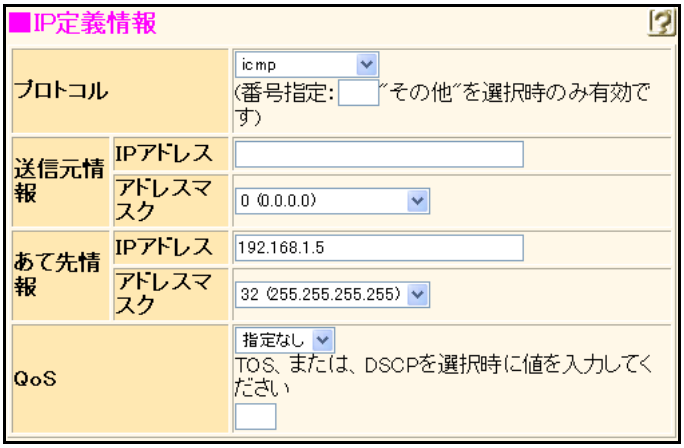
「ACL 定義情報（ping_deny）」ページが表示されます。

4. **「IP 定義情報」をクリックします。**

「IP 定義情報」が表示されます。

5. **以下の項目を指定します。**

- プロトコル　→icmp
- 送信元情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- あて先情報
  IP アドレス　→192.168.1.5
  アドレスマスク　→32（255.255.255.255）
- QoS　→指定なし



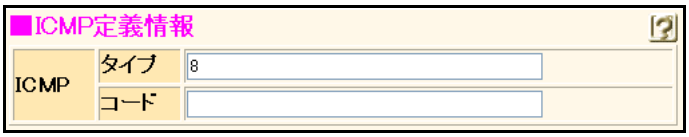
6. **［保存］ボタンをクリックします。**

7. **「ICMP 定義情報」をクリックします。**

「ICMP 定義情報」が表示されます。

8. **以下の項目を指定します。**

- ICMP
  タイプ　→8
  コード　→指定しない



9. **［保存］ボタンをクリックします。**

10. **設定メニューの詳細設定の「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

11. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**

「LAN0 情報」ページが表示されます。

12. **「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

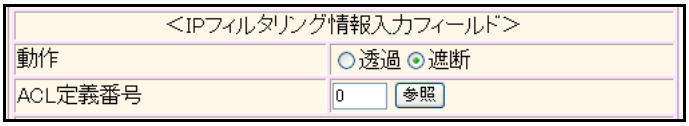
13. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

14. 以下の項目を指定します。

- 動作　→遮断
- ACL 定義番号　→0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15. ［追加］ボタンをクリックします。

16. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

30　DSCP 値書き換え機能を使う

適用機種　全機種

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットを IP アドレスとポート番号の組み合わせで DSCP 値を変更することにより、ポリシーベースネットワークのポリシーに合わせることができます。

参照　マニュアル「機能説明書」

こんな事に気をつけて

SR-S312LE1/320LE1/324LE1 では、フィルタリング機能および QoS 書き換え機能を同時に使用することができません。また、それぞれの機能で IPv4 および IPv6 条件を同時に使用することができません。
DSCP 値書き換えを有効にするためには「装置情報」-「資源情報」で、QoS 機能および IPv6 プロトコルを選択してください。

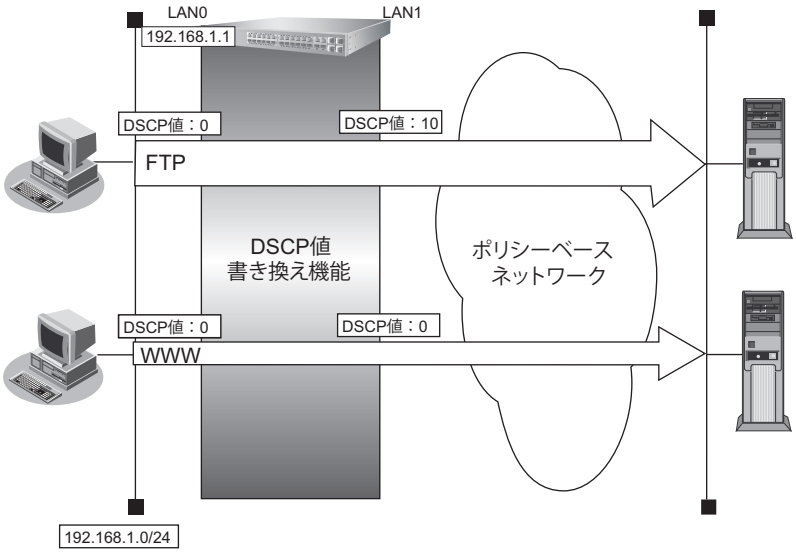
DSCP 値書き換え機能の条件

本装置では、ACL 番号で指定した ACL 定義の中で、以下の条件を指定することによってポリシーベースネットワークのポリシーに合った DSCP 値に書き換えることができます。

- プロトコル
- 送信元情報（IP アドレス／アドレスマスク／ポート番号）
- あて先情報（IP アドレス／アドレスマスク／ポート番号）
- IP パケットの TOS 値または DSCP 値（全機種）
  または、IPv6 パケットの Traffic Class 値または DSCP 値

ここではネットワークが以下のポリシーを持つ場合の設定方法を説明します。

- FTP（DSCP 値 10）を最優先とする
- その他はなし



● 設定条件

- 送信元 IP アドレス/アドレスマスク　：192.168.1.0/24
- 送信元ポート番号　：指定しない
- あて先 IP アドレス/アドレスマスク　：指定しない
- あて先ポート番号　：20（ftp-data のポート番号）、21（ftp のポート番号）
- プロトコル　：TCP
- DSCP 値　：0
- 新 DSCP 値　：10

上記の設定条件に従って設定を行う場合の設定例を示します。

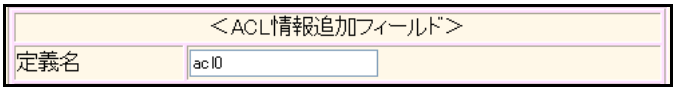
FTP サーバのアクセスで DSCP 値を 0 から 10 に書き換える

1.　設定メニューの詳細設定で「ACL 情報」をクリックします。

「ACL 情報」ページが表示されます。

2.　以下の項目を指定します。

- 定義名　→acl0



3.　［追加］ボタンをクリックします。

「ACL 定義情報（acl0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5.　以下の項目を指定します。

- プロトコル　→tcp
- 送信元情報
  IP アドレス　→192.168.1.0
  アドレスマスク　→24（255.255.255.0）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→0（0.0.0.0）
- QoS　→DSCP
  →0

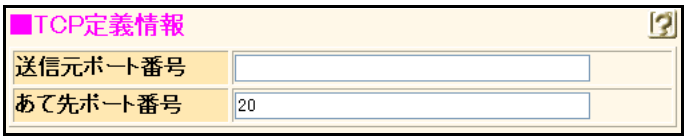
6.　［保存］ボタンをクリックします。

7.　「TCP 定義情報」をクリックします。

「TCP 定義情報」が表示されます。

8.　以下の項目を指定します。

- 送信元ポート番号　　→指定しない
- あて先ポート番号　　→ 20（ftp-data のポート番号）、21（ftp のポート番号）



9.　［保存］ボタンをクリックします。

10.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

11.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

「LAN0 情報」ページが表示されます。

12.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

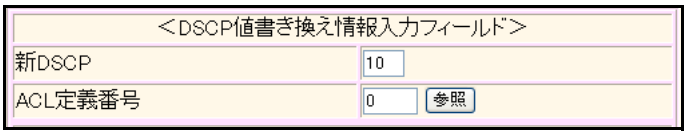
13.　「DSCP 値書き換え情報」をクリックします。

「DSCP 値書き換え情報」が表示されます。

14.　以下の項目を指定します。

- 新 DSCP　　→ 10
- ACL 定義番号　　→ 0

補足　「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



15.　［追加］ボタンをクリックします。

16.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

31 VRRP機能を使う

適用機種 ***SR-S732TR1, 752TR1***

VRRP機能は2つ以上のルータがグループを形成し、1台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタルータ（実際に経路情報を処理する装置）とバックアップルータ（マスタルータで異常を検出したときに経路情報の処理を引き継ぐ装置）を決定します。

本装置には、以下のVRRP機能があります。

- 簡易ホットスタンバイ機能
  動的に経路制御（RIPなど）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能
  VRRPのグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、2台のルータを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

☛ 参照 マニュアル「機能説明書」

こんな事に気をつけて

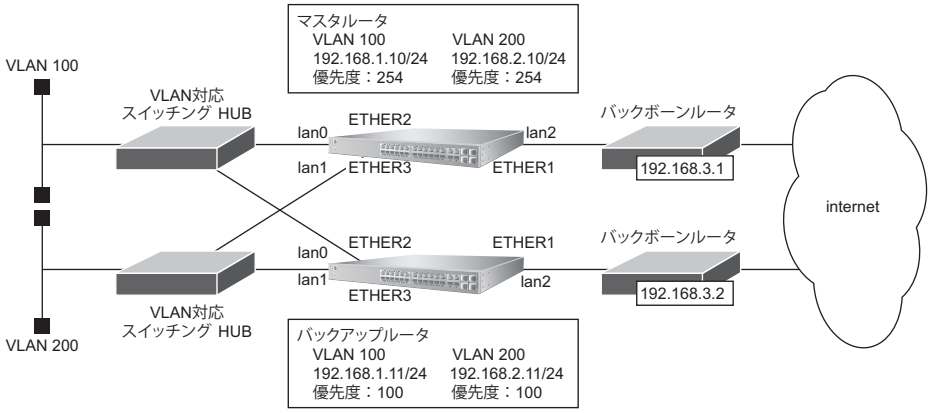
- **本装置の電源の投入、マスタルータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタルータとなることがあります。プリエンプトモードがonの場合は自動で切り戻りますが、プリエンプトモードがoffの場合は、操作メニューの「VRRP手動切り戻し」で切り戻しを行う必要があります。**
- **優先度の値が大きい方が優先的にマスタルータとなります。**
- **LANに接続される装置はデフォルトルートとして仮想IPアドレスを設定してください。**
- **VRRP機能では、VRRP-ADメッセージに以下のパケットを使用します。IPフィルタ設定時には、このパケットを遮断しないように設定する必要があります。**
  IPv4-VRRP
  あて先IPアドレス：224.0.0.18
  プロトコル番号：112
  IPv6-VRRP
  あて先IPアドレス：ff02::12
  IPv6 Next Header：112
- **IPv6 VRRPは、SR-S732TR1/752TR1の場合に使用できます。**

31.1 簡易ホットスタンバイ機能を使う

適用機種 ***SR-S732TR1, 752TR1***

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現することができます。

ここでは、インターネット側へはバックボーンルータを経由、ローカルLAN側をVLAN構成とする場合の設定方法を説明します。



● 設定条件

- 障害発生後の切り戻しは手動で行う
- マスタルータはインターネット側経路をノードダウントリガによって監視する

[VLAN 100]

- グループID　：10
- 仮想IPアドレス　：192.168.1.1

[VLAN 200]

- グループID　：20
- 仮想IPアドレス　：192.168.2.1

[マスタルータ]

- バックボーンルータへの接続ポート　：ETHER1 ポート
- VLAN 100への接続ポート　：ETHER2 ポート
- VLAN 200への接続ポート　：ETHER3 ポート
- 本装置のIPアドレス／ネットマスク　：192.168.1.10/24
- ノードダウントリガの監視IPアドレス　：202.168.2.1（プロバイダ側のDNSサーバアドレスなど）

[バックアップルータ]

- バックボーンルータへの接続ポート　：ETHER1 ポート
- VLAN 100への接続ポート　：ETHER2 ポート
- VLAN 200への接続ポート　：ETHER3 ポート
- 本装置のIPアドレス／ネットマスク　：192.168.1.11/24

上記の設定条件に従って設定を行う場合の設定例を示します。

マスタルータを設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

3.　以下の項目を指定します。

- VLAN
  Untagged　　→ 10

4.　［保存］ボタンをクリックします。

5.　手順 2. ～ 4. を参考に、ETHER2、3 ポートを設定します。

「ether 2 情報」-「基本情報」

- VLAN
  Tagged　　→ 100

「ether 3 情報」-「基本情報」

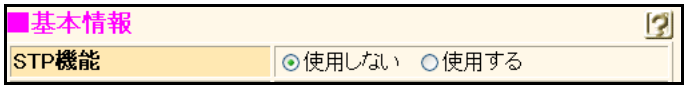
- VLAN
  Tagged　　→ 200

6.　設定メニューの詳細設定で「STP 情報」をクリックします。

「STP 情報」ページが表示されます。

7.　以下の項目を指定します。

- STP 機能　　→使用しない



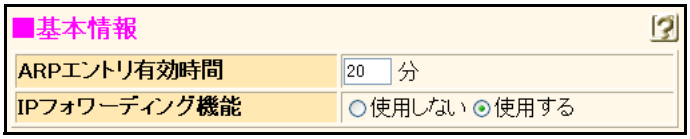
8.　［保存］ボタンをクリックします。

9.　設定メニューの詳細設定で「IP 情報」をクリックします。

「IP 情報」ページが表示されます。

10.　以下の項目を指定します。

- IP フォワーディング機能　　→使用する



11.　［保存］ボタンをクリックします。

12.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

13. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

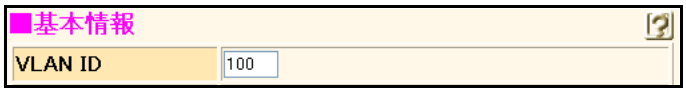
「LAN0 情報」ページが表示されます。

14. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

- VLAN ID →100



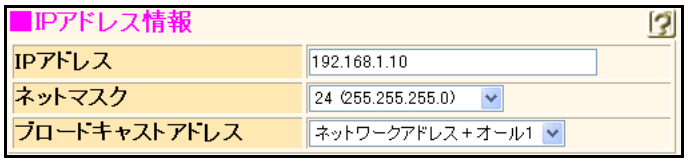
16. ［保存］ボタンをクリックします。

17. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

18. 以下の項目を指定します。

- IP アドレス →192.168.1.10
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1



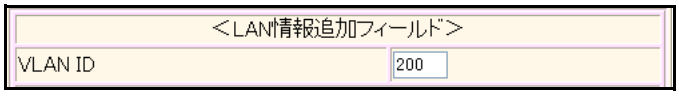
19. ［保存］ボタンをクリックします。

20. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

21. 以下の項目を指定します。

- VLAN ID →200



22. ［追加］ボタンをクリックします。

「LAN1 情報」ページが表示されます。

23. 手順 17. ～ 19. を参考に、LAN1 情報を設定します。

- IP アドレス →192.168.2.10
- ネットマスク →24（255.255.255.0）
- ロードキャストアドレス →ネットワークアドレス＋オール 1

24. **手順 20.～22. および手順 17.～19. を参考に、以下の項目を設定します。**

「LAN 情報」

- VLAN ID →10

「LAN2 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス →192.168.3.10
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

25. **手順 24. で設定した LAN2 情報の「IP 関連」をクリックします。**

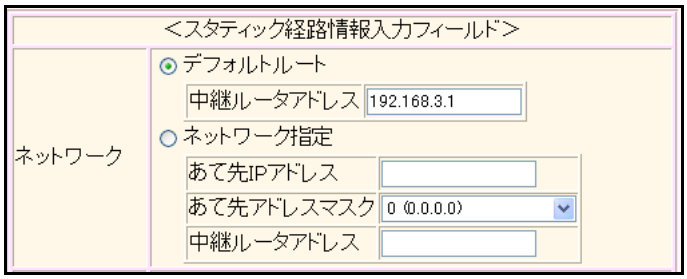
IP 関連の設定項目と「IP アドレス情報」が表示されます。

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

「スタティック経路情報」が表示されます。

27. **以下の項目を指定します。**

- ネットワーク →デフォルトルート
  中継ルータアドレス →192.168.3.1



28. **［追加］ボタンをクリックします。**

29. **設定メニューの詳細設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

30. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**

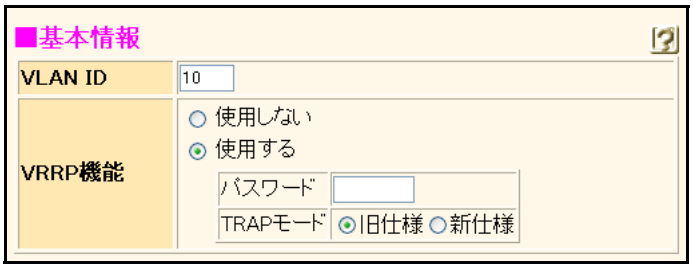
「LAN0 情報」ページが表示されます。

31. **「共通情報」をクリックします。**

共通情報の設定項目と「基本情報」が表示されます。

32. **以下の項目を指定します。**

- VRRP 機能 →使用する



33. **［保存］ボタンをクリックします。**

34. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

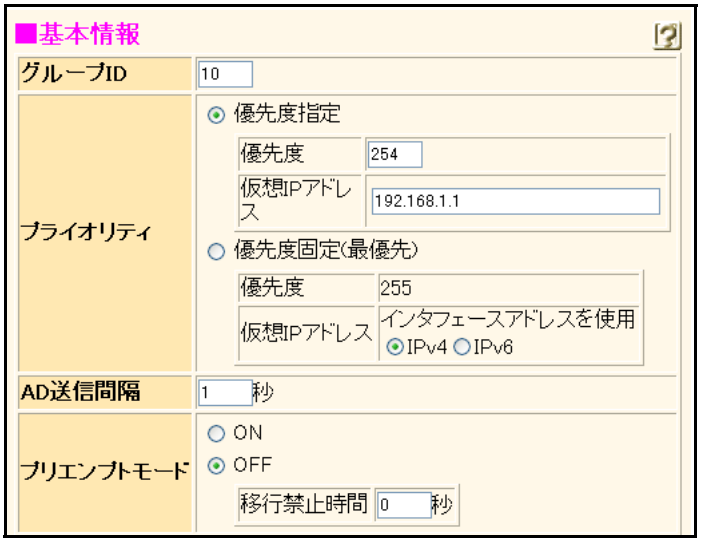
「VRRP グループ情報」が表示されます。

35. 「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ 0 情報の設定項目と「基本情報」が表示されます。

36. 以下の項目を指定します。

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ OFF



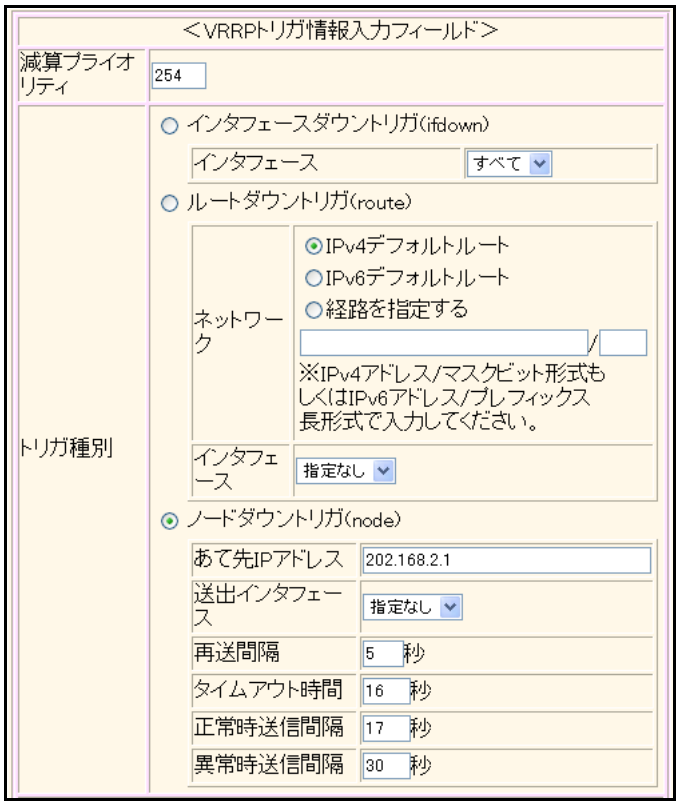
37. ［保存］ボタンをクリックします。

38. VRRP グループ 0 情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

39. 以下の項目を指定します。

- 減算プライオリティ →254
- トリガ種別 →ノードダウントリガ（node）
  あて先 IP アドレス →202.168.2.1
  送出インタフェース →指定なし
  再送間隔 →5
  タイムアウト時間 →16
  正常時送信間隔 →17
  異常時送信間隔 →30



40. ［追加］ボタンをクリックします。

41. 手順 29.～40. を参考に、以下の項目を設定します。

「LAN1 情報」-「共通情報」-「基本情報」

- VRRP 機能 →使用する

「LAN1 情報」-「共通情報」-「VRRP グループ 0 情報」-「基本情報」

- グループ ID →20
- プライオリティ →優先度指定
  優先度 →254
  仮想 IP アドレス →192.168.2.1
- プリエンプトモード →OFF

「LAN1 情報」-「共通情報」-「VRRP グループ 0 情報」-「VRRP トリガ情報」

- 減算プライオリティ　→ 254
- トリガ種別　→ノードダウントリガ（node）
  あて先 IP アドレス　→ 202.168.2.1
  送出インタフェース　→指定なし
  再送間隔　→ 5
  タイムアウト時間　→ 16
  正常時送信間隔　→ 17
  異常時送信間隔　→ 30

42. 画面左側の［再起動］ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

「ether 情報」

「ether 1 情報」-「基本情報」

- VLAN
  Untagged　→ 10

「ether 2 情報」-「基本情報」

- VLAN
  Tagged　→ 100

「ether 3 情報」-「基本情報」

- VLAN
  Tagged　→ 200

「STP 情報」

「基本情報」

- STP 機能　→使用しない

「IP 情報」

「基本情報」

- IP フォワーディング機能　→使用する

「LAN 情報」（LAN0）

- VLAN ID　→ 100

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス　→ 192.168.1.11
- ネットマスク　→ 24（255.255.255.0）

「LAN0 情報」-「共通情報」-「基本情報」

- VRRP 機能　→使用する

「LAN0 情報」-「共通情報」-「VRRP グループ 0 情報」-「基本情報」

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 100
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ ON

※ノードダウントリガは設定しません。

「LAN 情報」（LAN1）

- VLAN ID　→ 200

「LAN1 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス　→ 192.168.2.11
- ネットマスク　→ 24（255.255.255.0）

「LAN1 情報」-「共通情報」-「基本情報」

- VRRP 機能　→使用する

「LAN1 情報」-「共通情報」-「VRRP グループ 0 情報」-「基本情報」

- グループ ID　→ 20
- プライオリティ　→優先度指定
  優先度　→ 100
  仮想 IP アドレス　→ 192.168.2.1
- プリエンプトモード　→ ON

※ノードダウントリガは設定しません。

「LAN 情報」（LAN2）

- VLAN ID　→ 10

「LAN2 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス　→ 192.168.3.11
- ネットマスク　→ 24（255.255.255.0）

「LAN2 情報」-「IP 関連」-「スタティック経路情報」

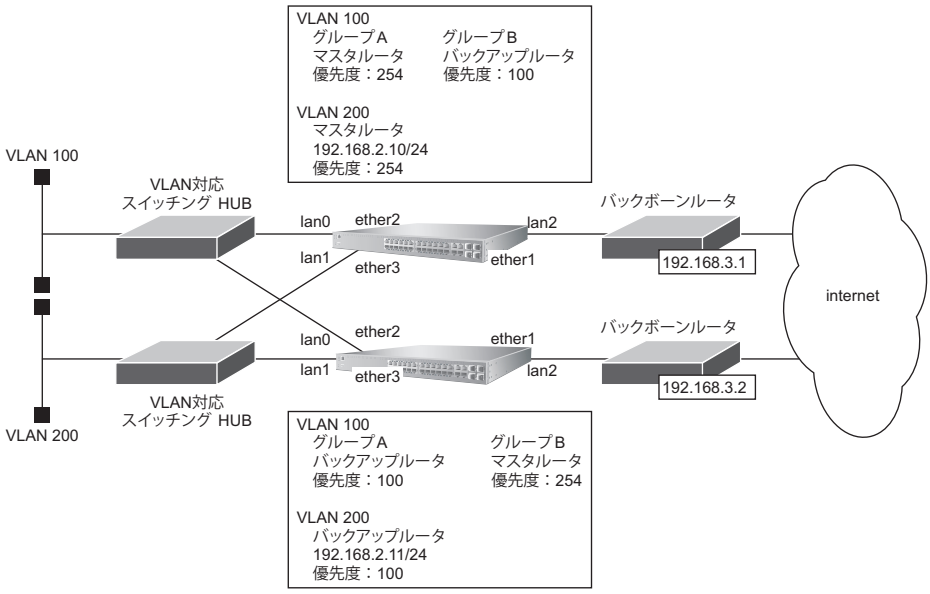
- ネットワーク　→デフォルトルート
- 中継ルータアドレス　→ 192.168.3.2

31.2 クラスタリング機能を使う

適用機種 ***SR-S732TR1, 752TR1***

本装置では、2台のルータに複数のグループIDを設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。

ここでは、インターネット側へはバックボーンルータを経由、ローカルLAN側をVLAN構成とする場合の設定方法を説明します（VLAN 100のみクラスタリング機能を使用する）。



● 設定条件

- 故障発生後の切り戻しは手動で行う
- マスタルータはバックボーンルータ側のインタフェースをインタフェースダウントリガにより監視する

[VLAN 100]

- ［グループA］
  - グループID　：10
  - 仮想IPアドレス　：192.168.1.1
- ［グループB］
  - グループID　：11
  - 仮想IPアドレス　：192.168.1.2

[VLAN 200]

- グループID　：20
- 仮想IPアドレス　：192.168.2.1

[マスタルータ]

- バックボーンルータへの接続ポート　：ETHER1 ポート
- VLAN 100への接続ポート　：ETHER2 ポート
- VLAN 200への接続ポート　：ETHER3 ポート
- 本装置のIPアドレス／ネットマスク　：192.168.1.10/24

[バックアップルータ]

- バックボーンルータへの接続ポート　：ETHER1 ポート
- VLAN 100 への接続ポート　：ETHER2 ポート
- VLAN 200 への接続ポート　：ETHER3 ポート
- 本装置の IP アドレス／ネットマスク　：192.168.1.11/24

こんな事に気をつけて

クラスタリング機能を有効に利用するには、端末からのトラフィック量に応じて、端末側で設定するデフォルトルートの定義を適切に分散してください。

上記の設定条件に従って設定を行う場合の設定例を示します。

マスタルータを設定する

1.　設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2.　「ether 情報」でポート番号が 1 の［修正］ボタンをクリックします。

ether 1 情報の設定項目と「基本情報」が表示されます。

3.　以下の項目を指定します。

- VLAN
  Untagged　→ 10

4.　［保存］ボタンをクリックします。

5.　手順 2. ～ 4. を参考に、ETHER2、3 ポートを設定します。

「ether 2 情報」-「基本情報」

- VLAN
  Tagged　→ 100

「ether 3 情報」-「基本情報」

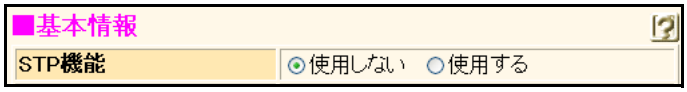
- VLAN
  Tagged　→ 200

6.　設定メニューの詳細設定で「STP 情報」をクリックします。

「STP 情報」ページが表示されます。

7.　以下の項目を指定します。

- STP 機能　→使用しない



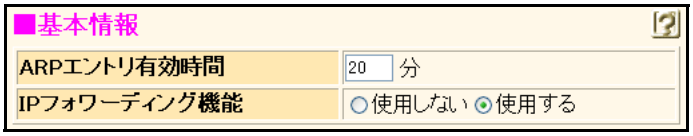
8.　［保存］ボタンをクリックします。

9.　設定メニューの詳細設定で「IP 情報」をクリックします。

「IP 情報」ページが表示されます。

10. 以下の項目を指定します。

- IP フォワーディング機能　　→使用する



11. ［保存］ボタンをクリックします。

12. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

13. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

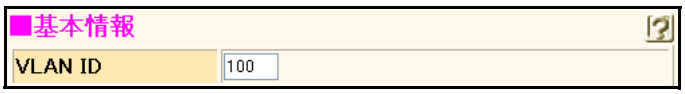
「LAN0 情報」ページが表示されます。

14. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

- VLAN ID　　→ 100



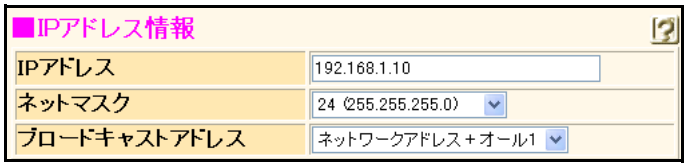
16. ［保存］ボタンをクリックします。

17. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

18. 以下の項目を指定します。

- IP アドレス　　→ 192.168.1.10
- ネットマスク　　→ 24（255.255.255.0）
- ブロードキャストアドレス　　→ネットワークアドレス＋オール 1



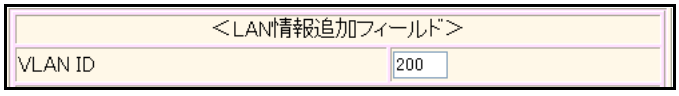
19. ［保存］ボタンをクリックします。

20. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

21. 以下の項目を指定します。

- VLAN ID　　→ 200



22. ［追加］ボタンをクリックします。

「LAN1 情報」ページが表示されます。

23. 手順 17. ～ 19. を参考に、LAN1 情報を設定します。

- IP アドレス →192.168.2.10
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

24. 手順 20. ～ 22. および手順 17. ～ 19. を参考に、以下の項目を設定します。

「LAN 情報」

- VLAN ID →10

「LAN2 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス →192.168.3.10
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

25. 手順 24. で設定した LAN2 情報の「IP 関連」をクリックします。

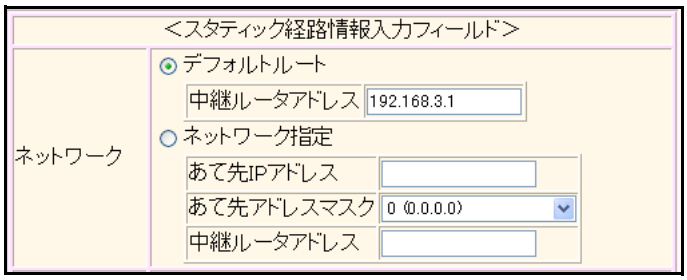
IP 関連の設定項目と「IP アドレス情報」が表示されます。

26. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

27. 以下の項目を指定します。

- ネットワーク →デフォルトルート
- 中継ルータアドレス →192.168.3.1



28. ［追加］ボタンをクリックします。

29. 設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

30. 「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

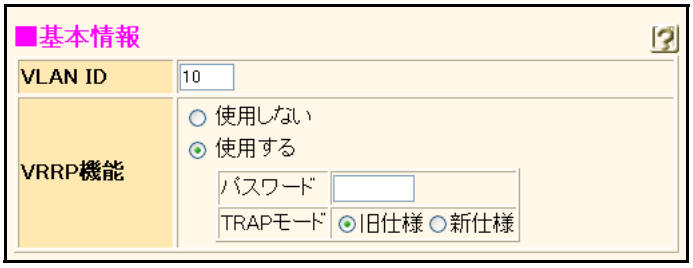
「LAN0 情報」ページが表示されます。

31. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

32. 以下の項目を指定します。

- VRRP 機能　→使用する



33. ［保存］ボタンをクリックします。

34. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

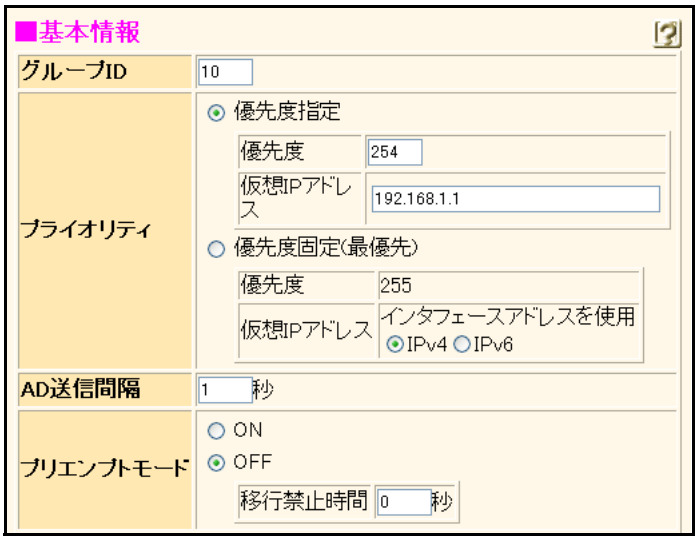
「VRRP グループ情報」が表示されます。

35. 「VRRP グループ情報」でグループ番号が 0 の［修正］ボタンをクリックします。

VRRP グループ 0 情報の設定項目と「基本情報」が表示されます。

36. 以下の項目を指定します。

- グループ ID　→ 10
- プライオリティ　→優先度指定
  優先度　→ 254
  仮想 IP アドレス　→ 192.168.1.1
- プリエンプトモード　→ OFF



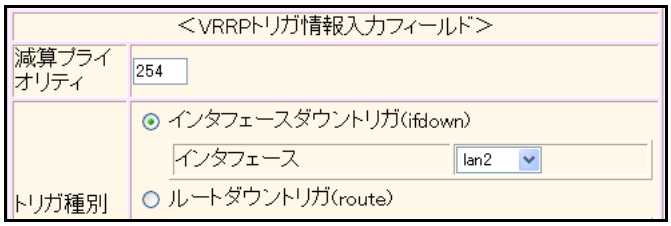
37. ［保存］ボタンをクリックします。

38. VRRP グループ 0 情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

39. 以下の項目を指定します。

- 減算プライオリティ →254
- トリガ種別 →インタフェースダウントリガ（ifdown）
  インタフェース →lan2



40. ［追加］ボタンをクリックします。

41. 手順34.～37.を参考に、グループ番号1を設定します。

- グループID →11
- プライオリティ →優先度指定
  優先度 →100
  仮想IPアドレス →192.168.1.2
- プリエンプトモード →ON

※インタフェースダウントリガは設定しません。

42. 手順29.～40.を参考に、以下の項目を設定します。

「LAN1情報」-「共通情報」-「基本情報」

- VRRP機能 →使用する

「LAN1情報」-「共通情報」-「VRRPグループ0情報」-「基本情報」

- グループID →20
- プライオリティ →優先度指定
  優先度 →254
  仮想IPアドレス →192.168.2.1
- プリエンプトモード →OFF

「LAN1情報」-「共通情報」-「VRRPグループ0情報」-「VRRPトリガ情報」

- 減算プライオリティ →254
- トリガ種別 →インタフェースダウントリガ（ifdown）
  インタフェース →lan2

43. 画面左側の［再起動］ボタンをクリックします。

装置の再起動後、設定した内容が有効になります。

バックアップルータを設定する

「マスタルータを設定する」を参考に、バックアップルータを設定します。

「ether 情報」

「ether 1 情報」-「基本情報」

- VLAN
  Untagged → 10

「ether 2 情報」-「基本情報」

- VLAN
  Tagged → 100

「ether 3 情報」-「基本情報」

- VLAN
  Tagged → 200

「STP 情報」

「基本情報」

- STP 機能 →使用しない

「IP 情報」

「基本情報」

- IP フォワーディング機能 →使用する

「LAN 情報」（LAN0）

- VLAN ID → 100

「LAN0 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス → 192.168.1.11
- ネットマスク → 24（255.255.255.0）

「LAN0 情報」-「共通情報」-「基本情報」

- VRRP 機能 →使用する

「LAN0 情報」-「共通情報」-「VRRP グループ 0 情報」-「基本情報」

- グループ ID → 10
- プライオリティ →優先度指定
  優先度 → 100
  仮想 IP アドレス → 192.168.1.1
- プリエンプトモード → ON

※インタフェースダウントリガは設定しません。

「LAN0 情報」-「共通情報」-「VRRP グループ 1 情報」-「基本情報」

- グループ ID → 11
- プライオリティ →優先度指定
  優先度 → 254
  仮想 IP アドレス → 192.168.1.2
- プリエンプトモード → OFF

「LAN0 情報」-「共通情報」-「VRRP グループ 1 情報」-「VRRP トリガ情報」

- 減算プライオリティ → 254

- トリガ種別　→インタフェースダウントリガ（ifdown）
  インタフェース　→lan2

「LAN 情報」（LAN1）

- VLAN ID　→200

「LAN1 情報」-「IP 関連」-「IP アドレス情報」

- IPアドレス　→192.168.2.11
- ネットマスク　→24（255.255.255.0）

「LAN1 情報」-「共通情報」-「基本情報」

- VRRP 機能　→使用する

「LAN1 情報」-「共通情報」-「VRRP グループ 0 情報」-「基本情報」

- グループID　→20
- プライオリティ　→優先度指定
  優先度　→100
  仮想IPアドレス　→192.168.2.1
- プリエンプトモード　→ON

※インタフェースダウントリガは設定しません。

「LAN 情報」（LAN2）

- VLAN ID　→10

「LAN2 情報」-「IP 関連」-「IP アドレス情報」

- IPアドレス　→192.168.3.11
- ネットマスク　→24（255.255.255.0）

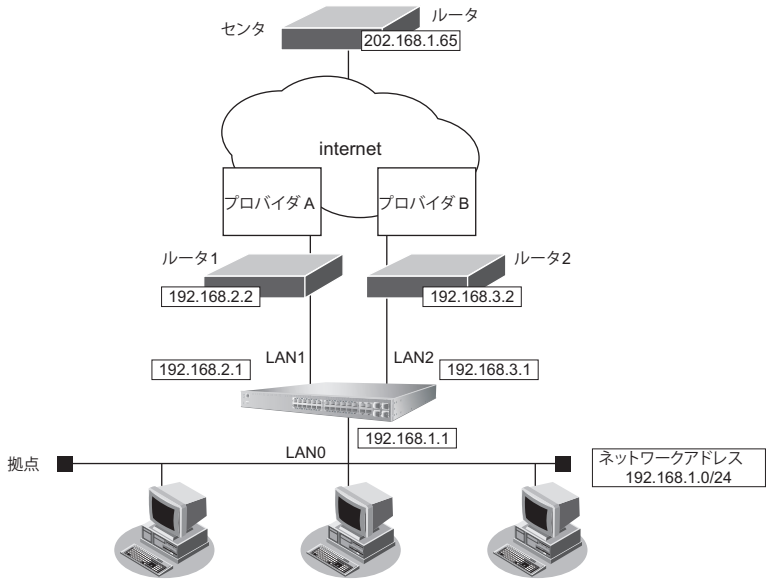
「LAN2 情報」-「IP 関連」-「スタティック経路情報」

- ネットワーク　→デフォルトルート
- 中継ルータアドレス　→192.168.3.2

32 ECMP 機能を使う

適用機種 ***SR-S732TR1, 752TR1***

ここでは、ECMP 機能を利用した負荷分散通信を行う場合の設定方法を説明します。



参照 マニュアル「機能説明書」

● 設定条件

- 拠点では、センタへの通信は、ルータ 1 とルータ 2 を利用して負荷分散して送信します。

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ether 情報」をクリックします。

「ether 情報」ページが表示されます。

2. 以下の項目を指定します。

- ポートリスト → 1-14

3. ［修正］ボタンをクリックします。

ether 1-14 情報の設定項目と「基本情報」が表示されます。

4. 以下の項目を指定します。

- VLAN
  Untagged → 10

5. **［保存］ボタンをクリックします。**

6. **設定メニューの詳細設定で「ether 情報」をクリックします。**

「ether 情報」ページが表示されます。

7. **「ether 情報」でポート番号が 15 の［修正］ボタンをクリックします。**

ether 15 情報の設定項目と「基本情報」が表示されます。

8. **手順 4. ～ 5. を参考に、以下の項目を設定します。**

- VLAN
  Untagged　→ 11

9. **手順 6. ～ 8. を参考に、ETHER16 ポートを設定します。**

- VLAN
  Untagged　→ 12

10. **設定メニューの詳細設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

11. **「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。**

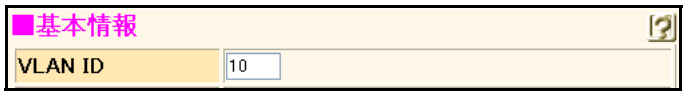
「LAN0 情報」ページが表示されます。

12. **「共通情報」をクリックします。**

共通情報の設定項目と「基本情報」が表示されます。

13. **以下の項目を指定します。**

- VLAN ID　→ 10



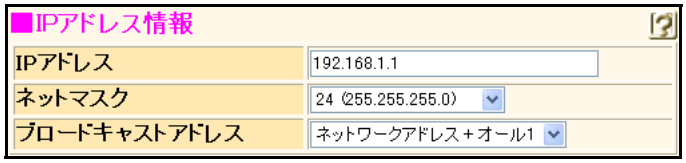
14. **［保存］ボタンをクリックします。**

15. **「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

16. **以下の項目を指定します。**

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



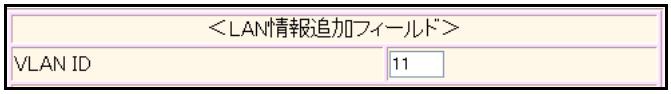
17. **［保存］ボタンをクリックします。**

18. **設定メニューの詳細設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

19. 以下の項目を指定します。

- VLAN ID →11



20. ［追加］ボタンをクリックします。

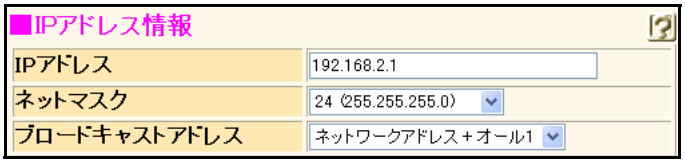
「LAN1 情報」ページが表示されます。

21. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

22. 以下の項目を指定します。

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



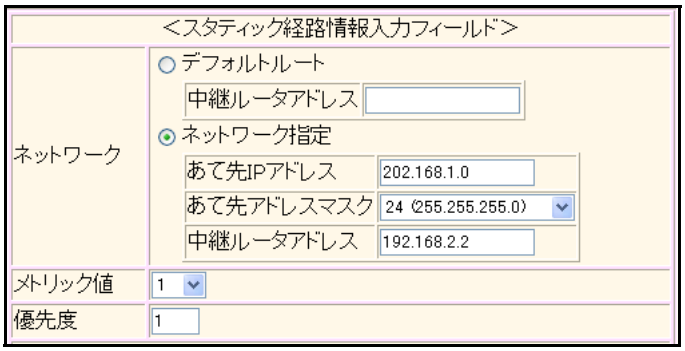
23. ［保存］ボタンをクリックします。

24. 「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

25. 以下の項目を指定します。

- ネットワーク →ネットワーク指定
  あて先 IP アドレス →202.168.1.0
  あて先アドレスマスク →24（255.255.255.0）
  中継ルータアドレス →192.168.2.2
- メトリック →1
- 優先度 →1



26. ［追加］ボタンをクリックします。

27. 手順 18.～26. を参考に、以下の項目を設定します。

「LAN 情報」

- VLAN ID →12

「LAN2 情報」-「IP 関連」-「IP アドレス情報」

- IP アドレス →192.168.3.1
- ネットマスク →24（255.255.255.0）
- ブロードキャストアドレス →ネットワークアドレス＋オール 1

「LAN2 情報」-「IP 関連」-「スタティック経路情報」

- ネットワーク →ネットワーク指定
  あて先 IP アドレス →202.168.1.0
  あて先アドレスマスク →24（255.255.255.0）
  中継ルータアドレス →192.168.3.2
- メトリック →1
- 優先度 →1

28. 設定メニューの詳細設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

29. 「ルーティングマネージャ情報」をクリックします。

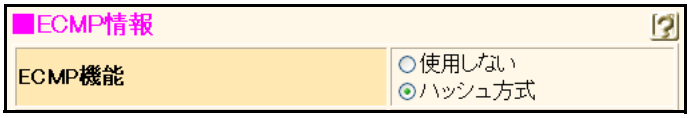
ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

30. 「ECMP 情報」をクリックします。

「ECMP 情報」が表示されます。

31. 以下の項目を指定します。

- ECMP 機能 →ハッシュ方式



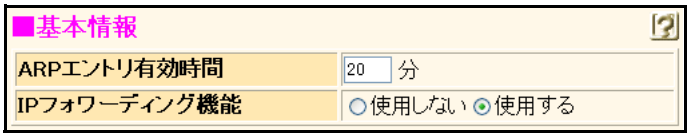
32. [保存] ボタンをクリックします。

33. 設定メニューの詳細設定の「IP 情報」をクリックします。

「IP 情報」ページが表示されます。

34. 以下の項目を指定します。

- IP フォワーディング機能 →使用する



35. [保存] ボタンをクリックします。

36. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

33 DHCP機能を使う

適用機種 全機種

本装置のDHCPには、以下の機能があります。

- DHCPサーバ機能
- DHCPスタティック機能
- DHCPリレーエージェント機能（SR-S732TR1/752TR1のみ）

参照 マニュアル「機能説明書」

本装置では、それぞれのインタフェースでDHCP機能が使用できます。

こんな事に気をつけて

- **1つのインタフェースでは、1つの機能だけ動作します。同時に複数の機能を動作することはできません。**
- **本装置のDHCPサーバは、リレーエージェントを経由して運用することはできません。**

33.1 DHCPサーバ機能を使う

適用機種 全機種

DHCPサーバ機能は、ネットワークに接続されているパソコンに対して、IPアドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびにIPアドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCPクライアント機能を持つパソコンはIPアドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- ドメイン名

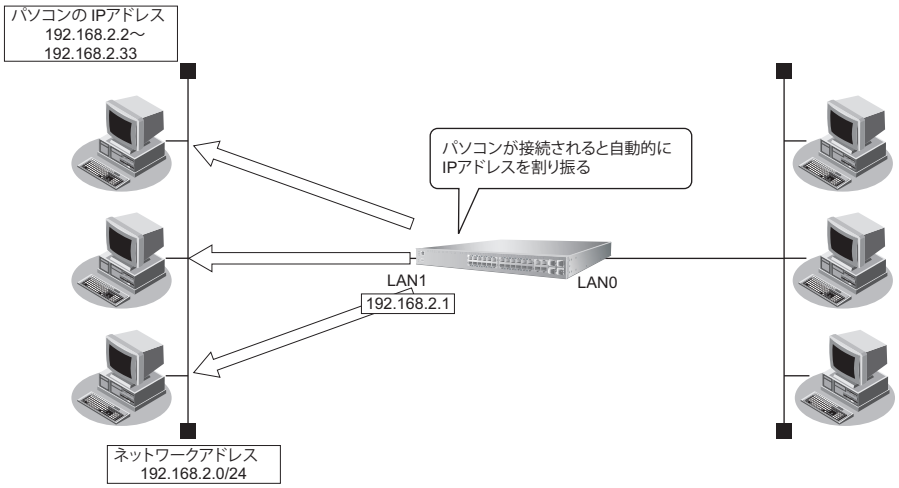
こんな事に気をつけて

- **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」

- **本装置のDHCPサーバ機能は、DHCPリレーエージェントのサーバにはなれません。**

ここでは、SR-S732TR1 の場合を例にして、DHCP サーバ機能を使用する場合の設定方法を説明します。



● 前提条件

- LAN0 が設定されている
- LAN1 は VLAN が設定されている

● 設定条件

- 本装置の IP アドレス　：192.168.2.1
- ブロードキャストアドレス　：3（ネットワークアドレス＋オール 1）
- パソコンに割り当てる IP アドレス　：192.168.2.2 ～ 192.168.2.33
- パソコンに割り当て可能 IP アドレス数　：32
- ネットワークアドレス／ネットマスク　：192.168.2.0/24
- DHCP サーバ機能を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

1.　「1.1 ポート VLAN 機能を使う」（P.9）の 手順 1. ～ 4. を参考に、ETHER1 ポートを設定します。

- VLAN
  Untagged　→ 10

2.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

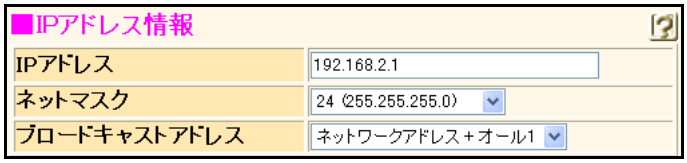
「LAN1 情報」ページが表示されます。

4.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

5.　以下の項目を指定します。

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



6.　［保存］ボタンをクリックします。

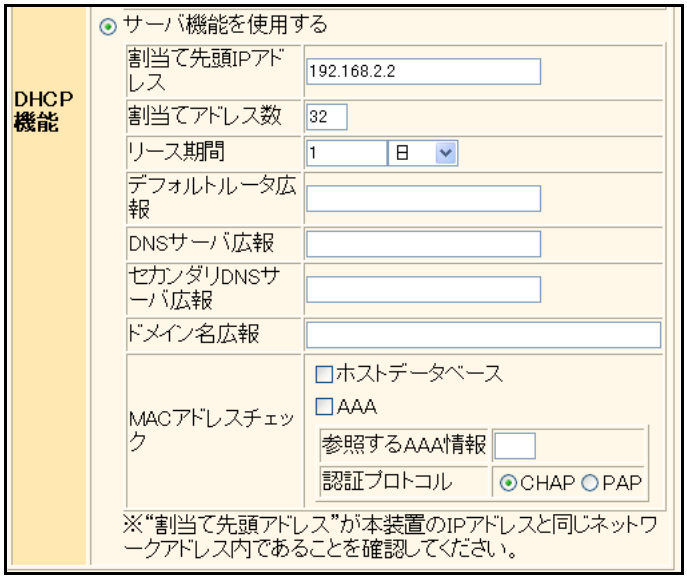
7.　IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

8.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する
  割当て先頭 IP アドレス　→192.168.2.2
  割当てアドレス数　→32

補足　DHCP サーバ機能で割り当てることのできる最大数は 253 です。



必要に応じて上記以外の項目を指定します。

9.　［保存］ボタンをクリックします。

10.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

33.2 DHCPスタティック機能を使う

適用機種　全機種

DHCPサーバは、使用していないIPアドレスを一定期間（またはパソコンがIPアドレスを返却するまで）割り当てます。不要になったIPアドレスは自動的に再利用されるため、パソコンのIPアドレスが変わることがあります。本装置では、IPアドレスとMACアドレスを対応付けることによって、登録されたパソコンからDHCP要求が発行されると、常に同じIPアドレスを割り当てることができます。これをDHCPスタティック機能と言います。

DHCPスタティック機能を利用する場合は、ホストデータベース情報にIPアドレスとMACアドレスを設定してください。

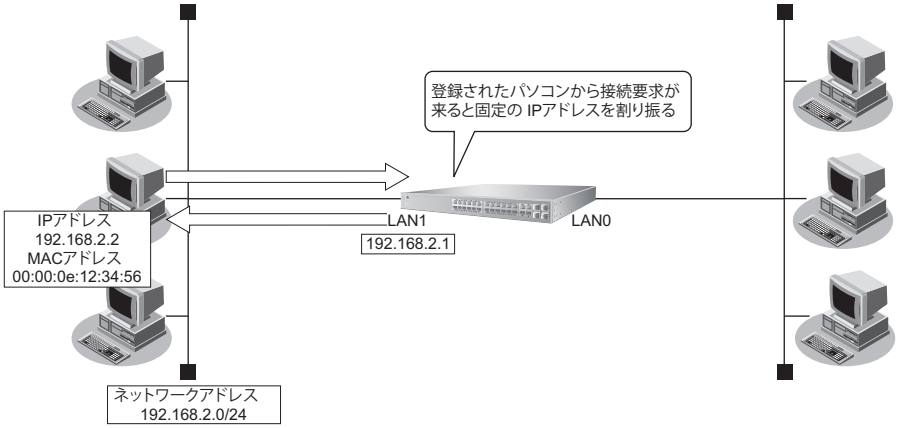
補足
- MACアドレスとは、LAN機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
- 本装置がサポートしているIPフィルタリング機能などはパソコンのIPアドレスが固定されていないと使いにくい場合があります。これらの機能とDHCPサーバ機能の併用を実現するために、本装置では「DHCPスタティック機能」をサポートしています。

こんな事に気をつけて

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

参照 マニュアル「Webユーザーズガイド」

ここでは、SR-S732TR1の場合を例にして、DHCPスタティック機能を使用する場合の設定方法を説明します。



● 設定条件

- ネットワークアドレス／ネットマスク　：192.168.2.0/24
- IPアドレスを固定するパソコンのMACアドレス：00:00:0e:12:34:56
- 割り当てIPアドレス　：192.168.2.2
- DHCPサーバ機能を使用する

こんな事に気をつけて

設定の「LAN0情報」、「LAN1情報」でDHCPサーバ機能を使用する設定をしていない場合は、DHCPスタティック機能の設定は有効になりません。

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

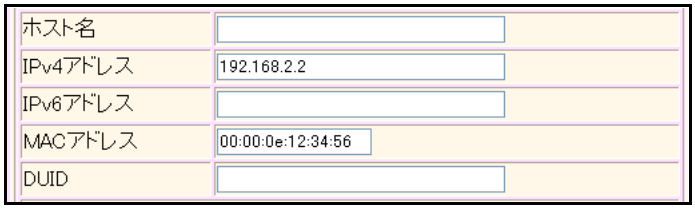
2. 未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報」が表示されます。

3. 以下の項目を指定します。

- IPv4アドレス　→192.168.2.2
- MACアドレス　→00:00:0e:12:34:56

補足 ホストデータベース情報は「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを設定します。



必要に応じて上記以外の項目を指定します。

4. ［保存］ボタンをクリックします。

5. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

補足 DHCPスタティック機能で設定できるホストの最大数は100です。

33.3 DHCP リレーエージェント機能を使う

適用機種 ***SR-S732TR1, 752TR1***

DHCP クライアントは、同じネットワーク上にあるサーバから、IP アドレスなどの情報を獲得することができます。

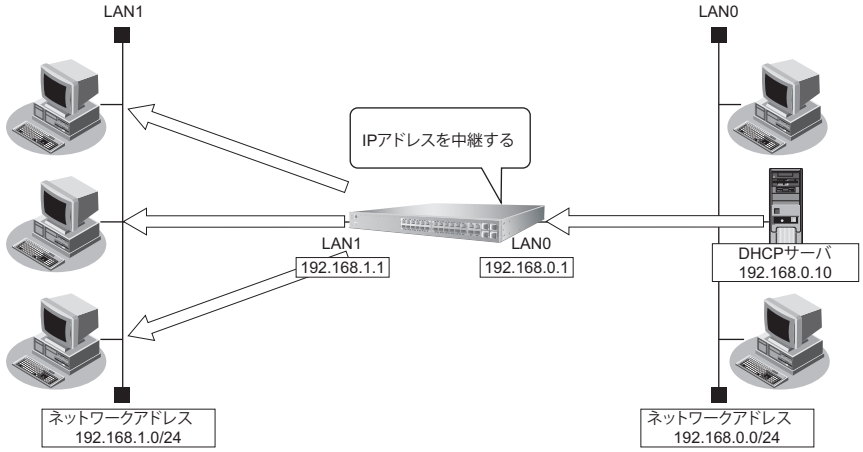
DHCP リレーエージェントは、遠隔地にある DHCP クライアントの要求を DHCP サーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークに DHCP サーバが存在する場合も同様に情報を獲得することができます。

こんな事に気をつけて

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

☛ **参照** マニュアル「Web ユーザーズガイド」

ここでは、DHCP リレーエージェント機能を使用する場合の設定方法を説明します。



● 前提条件

- LAN0 が設定されている
- LAN1 は VLAN が設定されている

● 設定条件

【LAN1】

- 本装置の IP アドレス　：192.168.1.1
- DHCP リレーエージェント機能を使用する

【LAN0】

- 本装置の IP アドレス　：192.168.0.1
- DHCP サーバ　：192.168.0.10

上記の設定条件に従って設定を行う場合の設定例を示します。

ここでは、LAN1 を使用した場合を例に説明します。LAN0 の場合も同様の手順で設定できます。

1. **「1.1 ポート VLAN 機能を使う」（P.9）の手順 1.～ 4. を参考に、ETHER1、2 ポートを設定します。**

ETHER1 ポート

- VLAN
  Untagged　→ 10

ETHER2 ポート

- VLAN
  Untagged　→ 20

2. **設定メニューの詳細設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

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

「LAN1 情報」ページが表示されます。

4. **「IP 関連」をクリックします。**

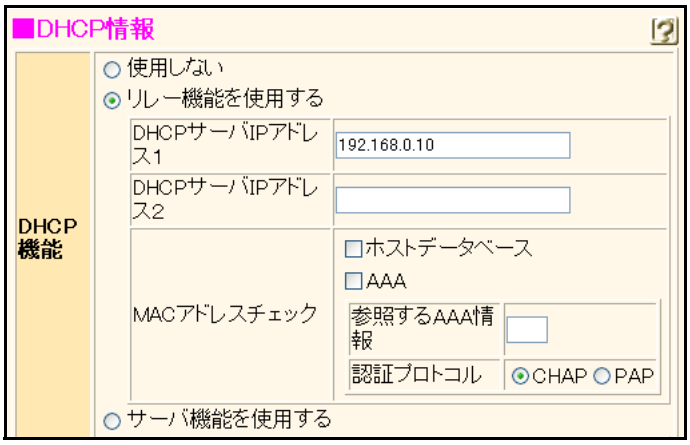
IP 関連の設定項目と「IP アドレス情報」が表示されます。

5. **IP 関連の設定項目の「DHCP 情報」をクリックします。**

「DHCP 情報」が表示されます。

6. **以下の項目を指定します。**

- DHCP 機能　→リレー機能を使用する
  DHCP サーバ IP アドレス 1　→ 192.168.0.10



7. **［保存］ボタンをクリックします。**

8. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になります。

33.4 IPv6 DHCP サーバ機能を使う

適用機種　全機種

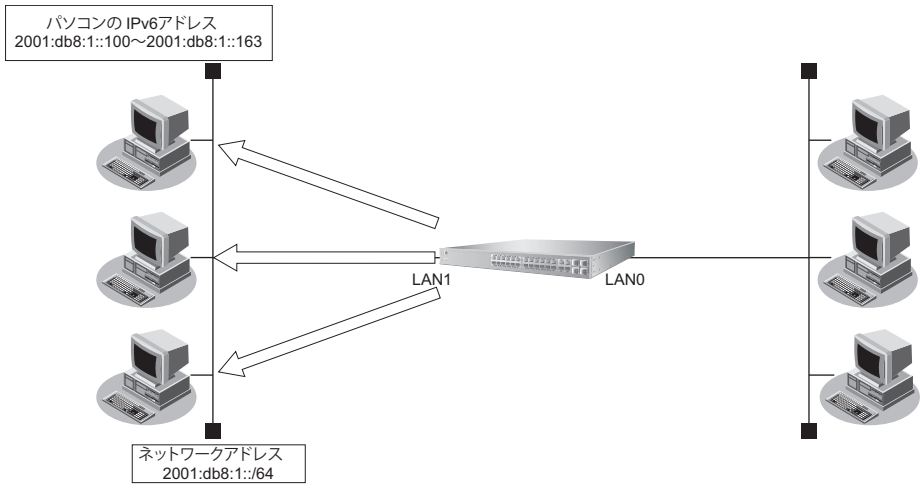
本装置のIPv6 DHCP サーバ機能は、以下の情報を広報することができます。

- IPv6アドレス
- IPv6プレフィックス
- DNSサーバのIPv6アドレス
- DNSドメイン名

こんな事に気をつけて

本装置のIPv6 DHCPサーバ機能は、IPv6 DHCPリレーエージェントのサーバにはなれません。

IPv6 DHCPサーバ機能を使用する場合の設定方法を説明します。



● 設定条件

- 本装置のIP アドレス　：2001:db8:1::1
- パソコンに割り当てるIPv6アドレス　：2001:db8:1::100～2001:db8:1::163
- パソコンに割り当て可能IPv6アドレス数　：100
- ネットワークアドレス／プレフィックス長　：2001:db8:1::/64
- Valid Lifetime　：30日
- Preferred Lifetime　：7日
- DNSサーバのIPv6アドレス　：2001:db8:1::53

上記の設定条件に従って設定を行う場合の設定例を示します。

IPv6 DHCP サーバ機能を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

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

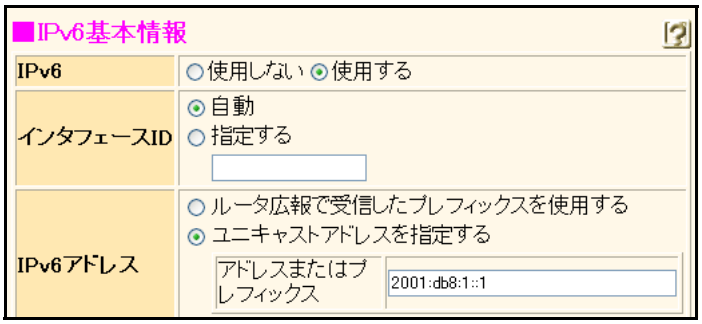
「LAN1 情報」ページが表示されます。

3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- IPv6 アドレス　→ユニキャストアドレスを指定する
  アドレスまたはプレフィックス　→ 2001:db8:1::1



5.　［保存］ボタンをクリックします。

6.　IPv6 関連の設定項目の「IPv6 DHCP 情報」をクリックします。

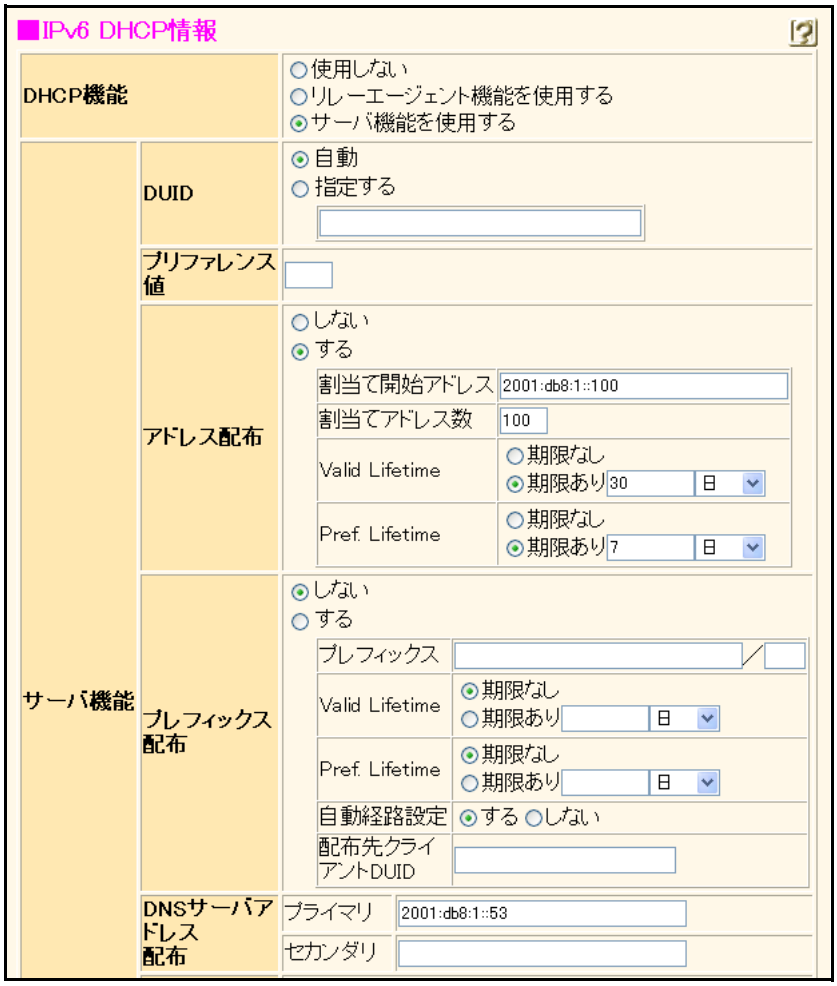
「IPv6 DHCP 情報」が表示されます。

7.　以下の項目を指定します。

- DHCP 機能　→サーバ機能を使用する

“ サーバ機能を使用する ” を選択すると、「サーバ機能」の設定項目が表示されます。

- サーバ機能
  アドレス配布　→する
  割当て開始アドレス　→ 2001:db8:1::100
  割当てアドレス数　→ 100
  Valid Lifetime　→期限あり 30 日
  Pref. Lifetime　→期限あり 7 日
  DNS サーバアドレス配布　→ 2001:db8:1::53



8.　［保存］ボタンをクリックします。

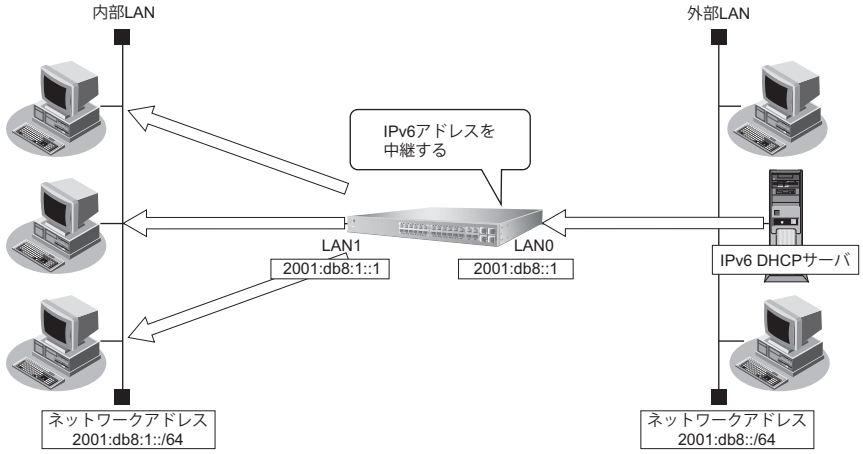
9.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

33.5 IPv6 DHCP リレーエージェント機能を使う

適用機種 ***SR-S732TR1, 752TR1***

ここでは、IPv6 DHCP リレーエージェント機能を使用する場合の設定方法を説明します。



● 設定条件

[内部 LAN 側]

- 本装置の IPv6 アドレス　：2001:db8:1::1
- IPv6 DHCP リレーエージェント機能を使用する

[外部 LAN 側]

- 本装置の IPv6 アドレス　：2001:db8::1

上記の設定条件に従って設定を行う場合の設定例を示します。

IPv6 DHCP リレーエージェント機能を設定する

1.　設定メニューの詳細設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2.　「LAN 情報」でインタフェースが LAN0 の［修正］ボタンをクリックします。

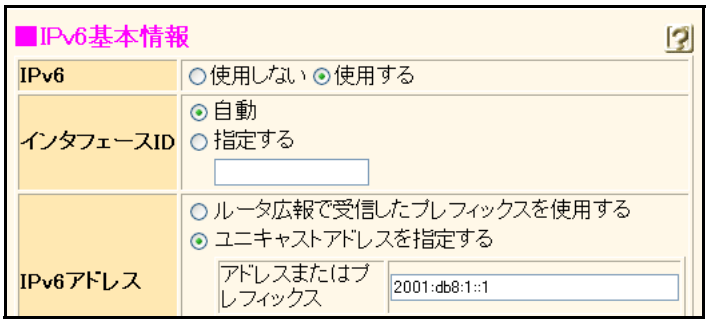
「LAN0 情報」ページが表示されます。

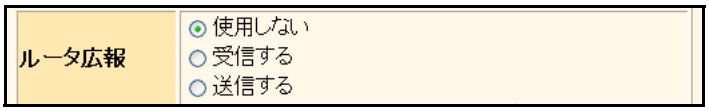
3.　「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

4.　以下の項目を指定します。

- IPv6　→使用する
- IPv6アドレス　→ユニキャストアドレスを指定する
  アドレスまたはプレフィックス　→2001:db8:1::1
- ルータ広報　→使用しない





5.　［保存］ボタンをクリックします。

6.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

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

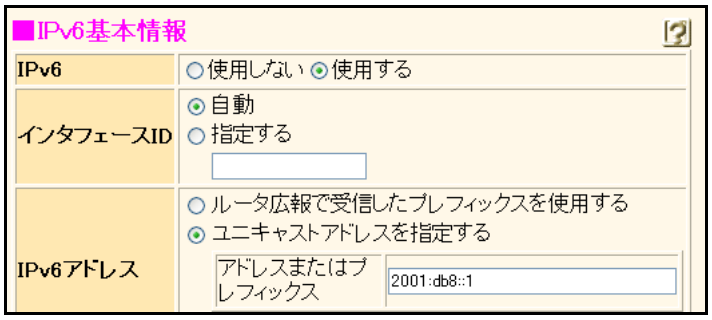
「LAN1情報」ページが表示されます。

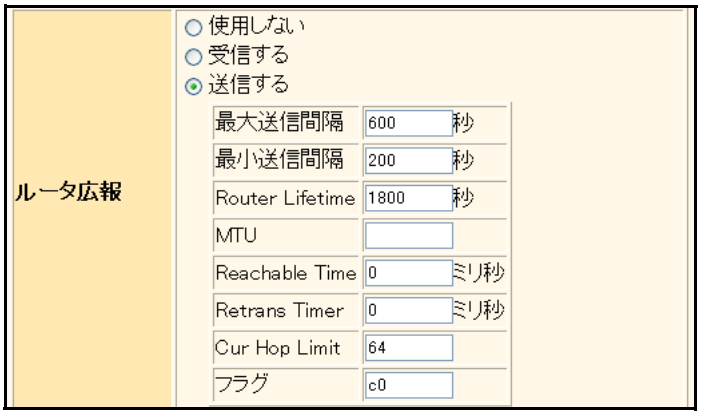
8.　「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

9.　以下の項目を指定します。

- IPv6　→使用する
- IPv6アドレス　→ユニキャストアドレスを指定する
  アドレスまたはプレフィックス　→2001:db8::1
- ルータ広報　→送信する
  フラグ　→c0





10.　［保存］ボタンをクリックします。

11.　IPv6関連の設定項目の「IPv6 DHCP情報」をクリックします。

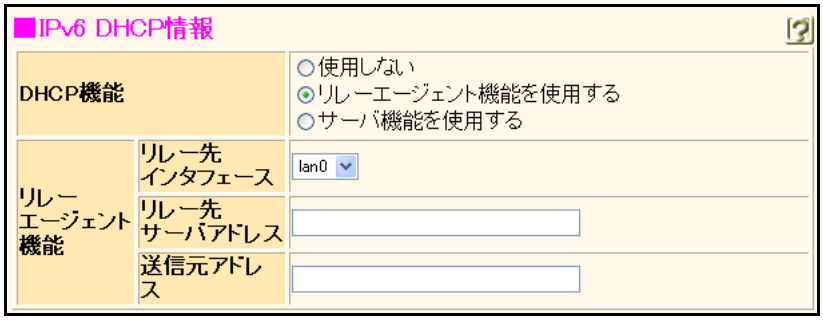
「IPv6 DHCP情報」が表示されます。

12. 以下の項目を指定します。

- DHCP 機能　→DHCP リレーエージェント機能を使用する

“DHCP リレーエージェント機能を使用する ” を選択すると、「リレーエージェント機能」の設定項目が表示されます。

- リレーエージェント機能
  リレー先インタフェース　→lan0



13. ［保存］ボタンをクリックします。

14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

34　DNS サーバ機能を使う（ProxyDNS）

適用機種　全機種

本装置の ProxyDNS には、以下の機能があります。

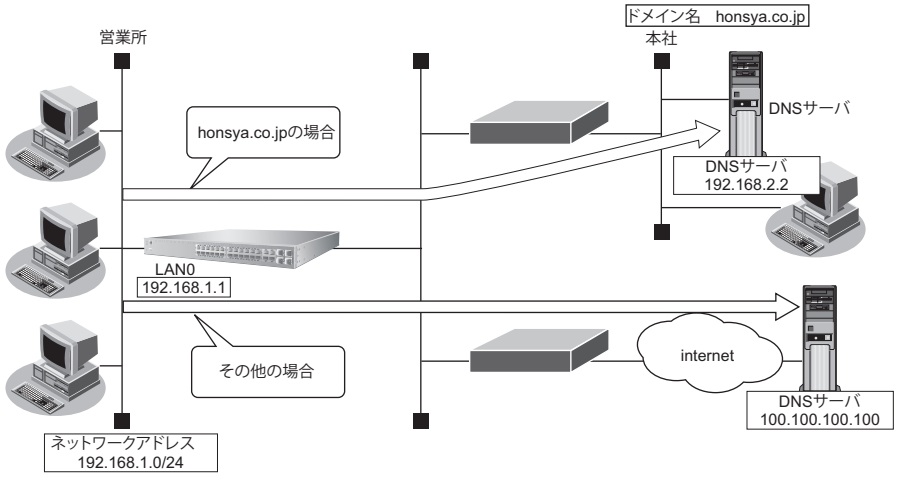
- DNS サーバの自動切り替え機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

参照 マニュアル「機能説明書」

34.1　DNS サーバの自動切り替え機能（順引き）を使う

適用機種　全機種

ProxyDNS は、パソコン側で本装置の IP アドレスを DNS サーバの IP アドレスとして登録するだけで、ドメインごとに使用する DNS サーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



● 設定条件

- 会社の DNS サーバを使用する場合
  使用するドメイン　：honsya.co.jp
  DNS サーバの IP アドレス　：192.168.2.2
- インターネット上の DNS サーバを使用する場合
  使用するドメイン　：honsya.co.jp 以外
  DNS サーバの IP アドレス　：100.100.100.100

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」

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS 情報を設定する

1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

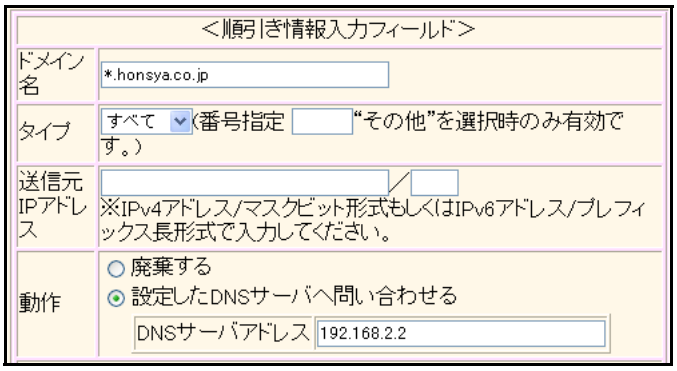
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

3. 以下の項目を指定します。

- ドメイン名　→＊.honsya.co.jp
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 192.168.2.2



4. ［追加］ボタンをクリックします。

5. 手順 3.～4. を参考に、以下の項目を設定します。

- ドメイン名　→＊
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 100.100.100.100

6. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を確認する

1. パソコン側が DHCP クライアントかどうか確認します。

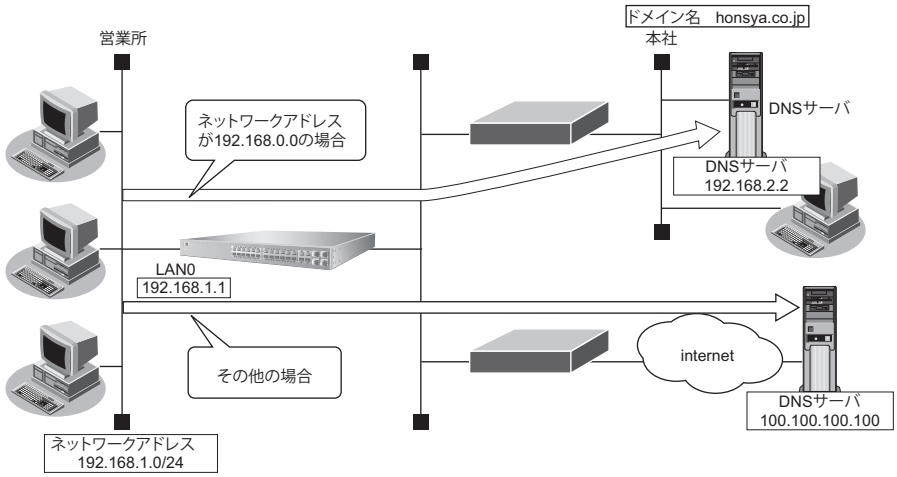
DHCP クライアントでない場合は設定します。

設定方法は、「34.2 DNS サーバの自動切り替え機能（逆引き）を使う」（P.318）の「パソコン側の設定を行う」（P.320）を参照してください。

34.2 DNS サーバの自動切り替え機能（逆引き）を使う

適用機種　全機種

ProxyDNSは、先に説明した順引きとは逆に、IPアドレスごとに使用するDNSサーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



● 設定条件

- 会社のDNSサーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0
  DNSサーバのIPアドレス　：192.168.2.2
- インターネット上のDNSサーバを使用する場合
  逆引き対象のネットワークアドレス　：192.168.0.0以外
  DNSサーバのIPアドレス　：100.100.100.100

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」

上記の設定条件に従って設定を行う場合の設定例を示します。

ProxyDNS 情報を設定する

1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

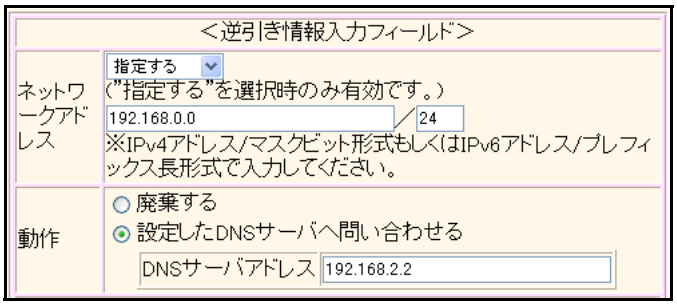
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2. 「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

3. 以下の項目を指定します。

- ネットワークアドレス　→指定する
  → 192.168.0.0/24
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 192.168.2.2



4. ［追加］ボタンをクリックします。

5. 手順 3.～4. を参考に、以下の項目を設定します。

- ネットワークアドレス　→すべて
- 動作　→設定した DNS サーバへ問い合わせる
  DNS サーバアドレス　→ 100.100.100.100

6. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

ここでは、Windows 10の場合を例に説明します。

1. **［Windowsロゴ］ボタン、［Windowsシステムツール］、［コントロールパネル］の順にクリックします。**
2. **［ネットワークとインターネット］をクリックします。**
3. **［ネットワークと共有センター］をクリックします。**
4. **［アダプターの設定の変更］をクリックします。**
5. **［イーサネット］アイコンを右クリックし、［プロパティ］ボタンをクリックします。**
   ［イーサネットのプロパティ］ダイアログボックスが表示されます。
6. **一覧から「インターネットプロトコルバージョン4（TCP/IPv4）」を選択します。**
7. **［プロパティ］ボタンをクリックします。**
   ［インターネットプロトコルバージョン4（TCP/IPv4）のプロパティ］ダイアログボックスが表示されます。
8. **「次のDNSサーバーのアドレスを使う」を選択します。**
9. **「優先DNSサーバー」に、本装置のIPアドレスを入力します。**
10. **［OK］ボタンをクリックします。**
    ［イーサネットのプロパティ］ダイアログボックスに戻ります。
11. **［閉じる］ボタンをクリックします。**
    設定した内容が有効になります。

34.3 DNS問い合わせタイプフィルタ機能を使う

適用機種　全機種

端末が送信するDNSパケットのうち、特定の問い合わせタイプ（QTYPE）のパケットを破棄することができます。

こんな事に気をつけて

ProxyDNS機能を使用する場合、問い合わせタイプがA（1）のDNS問い合わせパケットを破棄するように指定にすると、正常な通信が行えなくなります。

● 設定条件

- ドメイン名　：＊
- 問い合わせタイプ　：SOA（6）
- 動作　：破棄する

こんな事に気をつけて

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」

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1.　設定メニューの詳細設定で「ProxyDNS情報 URLフィルタ情報」をクリックします。

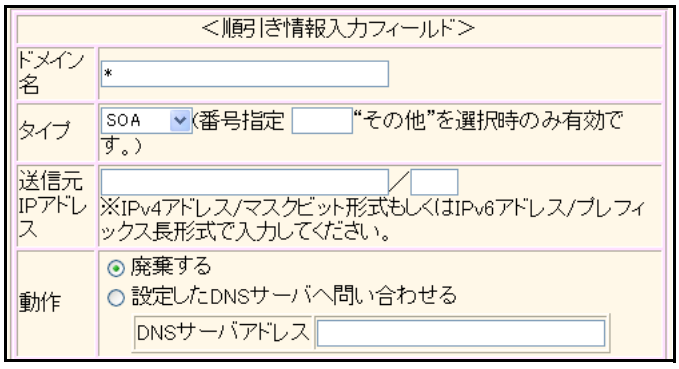
「ProxyDNS情報／URLフィルタ情報」ページが表示されます。

2.　「順引き情報」をクリックします。

「順引き情報」が表示されます。

3.　以下の項目を指定します。

- ドメイン名　→＊
- タイプ　→SOA
- 動作　→廃棄する



4.　［追加］ボタンをクリックします。

5.　画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、「34.2 DNS サーバの自動切り替え機能（逆引き）を使う」（P.318）の「 パソコン側の設定を行う」（P.320）を参照してください。

再起動後に、設定した内容が有効になります。

34.4 DNS サーバ機能を使う

適用機種 全機種

本装置のホストデータベースにホスト名と IP アドレスを登録します。登録したホストに対して DNS 要求があった場合は、ProxyDNS が DNS サーバの代わりに応答します。

● 設定条件

- ホスト名 ：host.com
- IPv4 アドレス ：192.168.1.2

こんな事に気をつけて

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

☛ 参照 マニュアル「Web ユーザーズガイド」

上記の設定条件に従って設定を行う場合の設定例を示します。

本装置側を設定する

1. 設定メニューの詳細設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

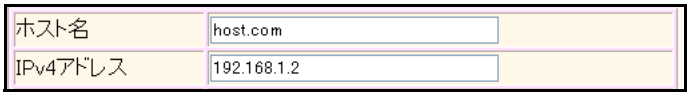
2. 未設定の欄の［修正］ボタンをクリックします。

「ホストデータベース情報」が表示されます。

3. 以下の項目を指定します。

- ホスト名 →host.com（パソコンの名前）
- IPv4 アドレス →192.168.1.2（パソコンの IP アドレス）

補足 ホストデータベース情報は「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。



4. ［保存］ボタンをクリックします。

5. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

パソコン側の設定を行う

パソコン側の設定を行います。

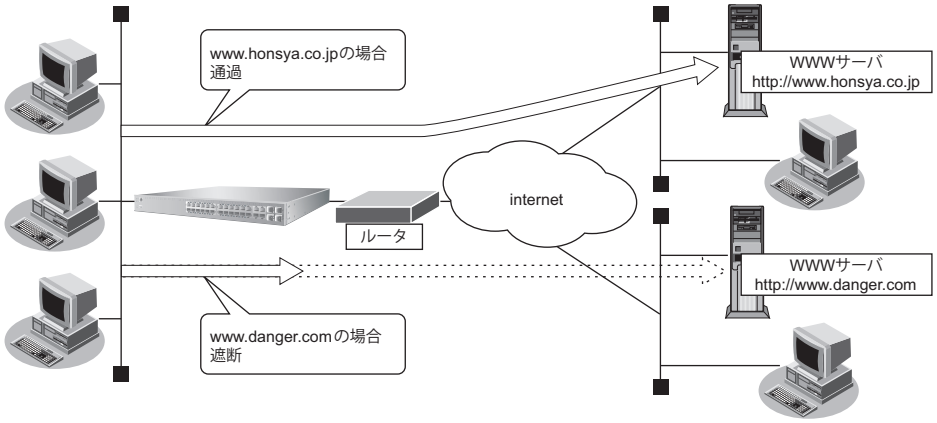
設定方法は、「34.2 DNS サーバの自動切り替え機能（逆引き）を使う」（P.318）の「 パソコン側の設定を行う」（P.320）を参照してください。

35 特定のURLへのアクセスを禁止する（URLフィルタ機能）

適用機種 全機種

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、ProxyDNS情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



参照 マニュアル「機能説明書」の「DNSサーバ機能」に関する記述

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

● 設定条件

- アクセスを禁止するドメイン名　：www.danger.com
- DNSサーバのIPアドレス　：100.100.100.100

こんな事に気をつけて

- **URLフィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。**
- **文字入力フィールドでは、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「"」、「<」、「>」、「&」、「%」は入力しないでください。**

参照 マニュアル「Webユーザーズガイド」

ヒント

◆「＊」は使えるの？

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「＊.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合の設定例を示します。

1. 設定メニューの詳細設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

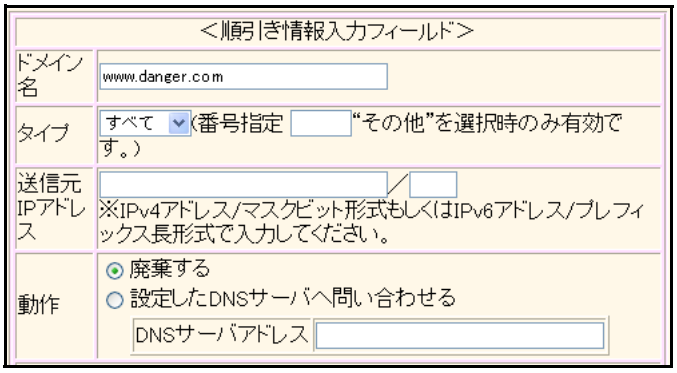
「ProxyDNS 情報／URL フィルタ情報」ページが表示されます。

2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

3. 以下の項目を指定します

- ドメイン名　→ www.danger.com
- 動作　→廃棄する



4. ［追加］ボタンをクリックします。

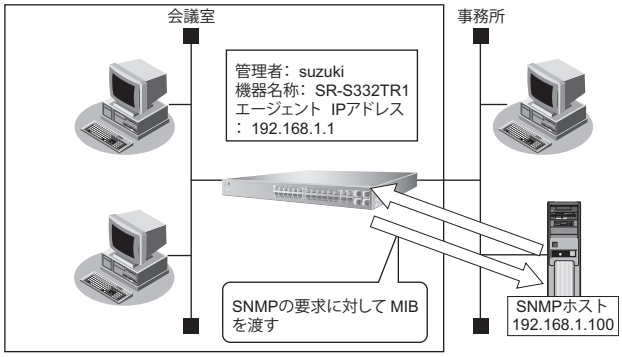
5. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

36　SNMP エージェント機能を使う

適用機種　全機種

本装置は、SNMP（Simple Network Management Protocol）エージェント機能をサポートしています。
ここでは、SNMP ホストに対して MIB 情報を通知する場合の設定方法を説明します。



☛参照 マニュアル「機能説明書」

ヒント

◆ SNMP とは？

SNMP（Simple Network Management Protocol）は、ネットワーク管理用のプロトコルです。SNMP ホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、SNMP ホストの要求に対して MIB（Management Information Base）という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMP エージェントから SNMP ホストに対して非同期通知を行うことができます。

☛参照 マニュアル「仕様一覧」

こんな事に気をつけて

- **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」

- **エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SNMP ホストとの通信ができなくなります。**
- **認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMP ホストの設定と同じ設定にします。誤ったプロトコルとパスワードを設定した場合は、SNMP ホストとの通信ができなくなります。**
- **SNMPv3 で認証／暗号プロトコルを使用する場合、snmp 設定反映時の認証／暗号鍵生成に時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。**

SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

SNMPv1 または SNMPv2c でのアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：SR-S332TR1
- 機器設置場所　：1F（1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- コミュニティ名　：public00

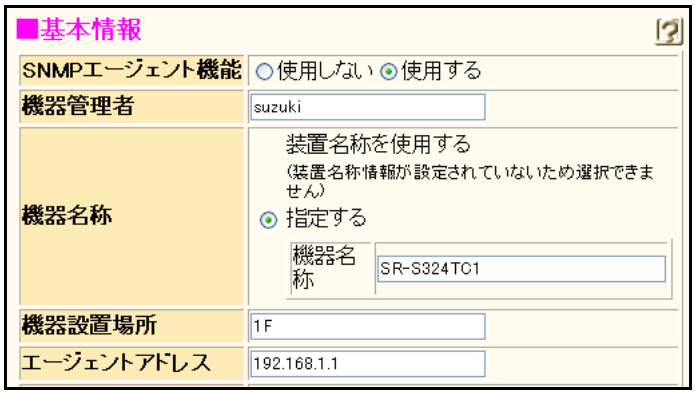
上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「SNMP 情報」をクリックします。

「SNMP 情報」ページが表示されます。

2.　以下の項目を指定します。

- SNMP エージェント機能　→使用する
- 機器管理者　→ suzuki
- 機器名称　→指定する（SR-S332TR1）
- 機器設置場所　→ 1F
- エージェントアドレス　→ 192.168.1.1



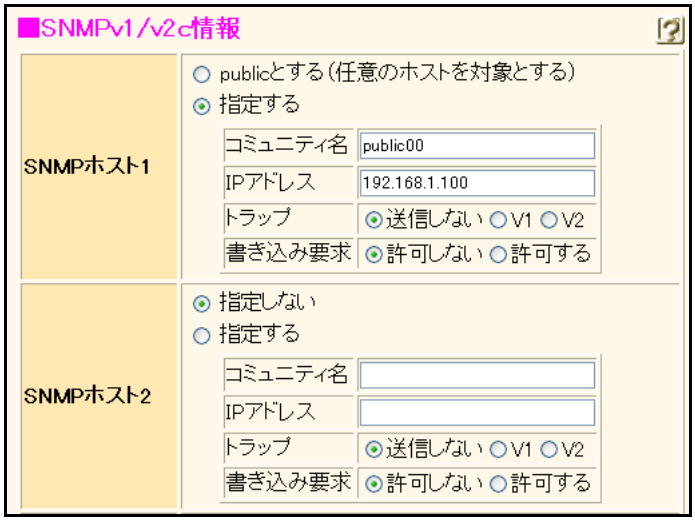
3.　［保存］ボタンをクリックします。

4.　「SNMPv1/v2c 情報」をクリックします。

「SNMPv1/v2c 情報」が表示されます。

5.　以下の項目を指定します。

- SNMP ホスト 1　→指定する
  コミュニティ名　→ public00
  IP アドレス　→ 192.168.1.100
- SNMP ホスト 2 以降　→指定しない



6.　［保存］ボタンをクリックします。

SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、以下の情報を設定します。

● 設定条件

- SNMP エージェント機能を使用する
- 管理者　：suzuki
- 機器名称　：SR-S332TR1
- 機器設置場所　：1F （1 階）
- エージェントアドレス　：192.168.1.1（自装置 IP アドレス）
- SNMP ホストアドレス　：192.168.1.100
- トラップ通知ホストアドレス　：192.168.1.100
- ユーザ名　：user00
  認証プロトコル　：MD5
  認証パスワード　：auth_password
  暗号プロトコル　：DES
  暗号パスワード　：priv_password
- MIB ビュー　：MIB 読み出しは system、interfaces グループのみ許可。
  トラップ通知は linkDown、linkUp トラップのみ許可。

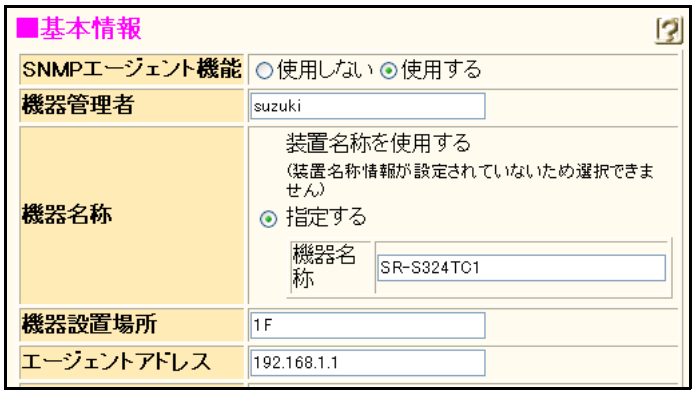
上記の設定条件に従って設定を行う場合の設定例を示します。

1.　設定メニューの詳細設定で「SNMP 情報」をクリックします。

「SNMP 情報」ページが表示されます。

2.　以下の項目を指定します。

- SNMP エージェント機能　→使用する
- 機器管理者　→ suzuki
- 機器名称　→指定する（SR-S332TR1）
- 機器設置場所　→ 1F
- エージェントアドレス　→ 192.168.1.1



3.　［保存］ボタンをクリックします。

4.　「SNMPv3 情報」をクリックします。

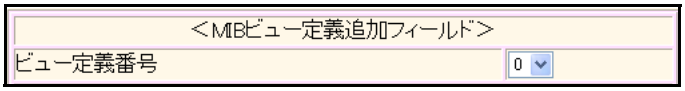
「SNMPv3 情報」ページが表示されます。

5.　SNMPv3 情報の設定項目の「MIB ビュー情報」をクリックします。

「MIB ビュー情報」が表示されます。

6.　以下の項目を指定します。

- ビュー定義番号　→ 0



7.　［追加］ボタンをクリックします。

8.　以下の項目を指定します。

- サブツリー名／ビュータイプ　→system ／含む
- サブツリー名／ビュータイプ　→interfaces ／含む
- サブツリー名／ビュータイプ　→linkdown ／含む
- サブツリー名／ビュータイプ　→linkup ／含む

9.　［保存］ボタンをクリックします。

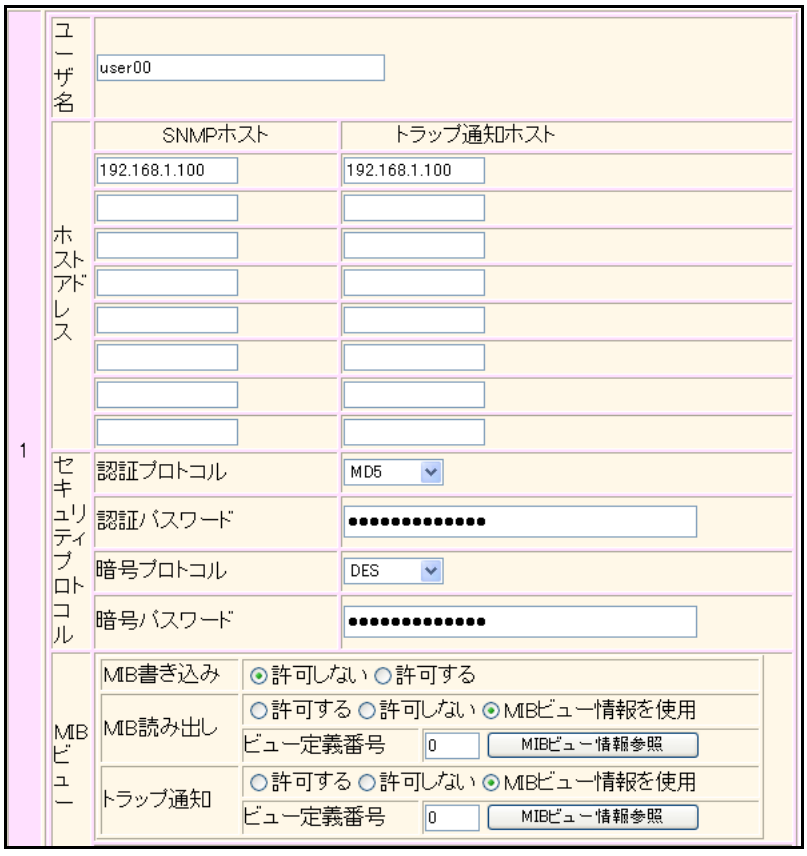
10.　SNMPv3 情報の設定項目の「ユーザ情報」をクリックします。

「ユーザ情報」が表示されます。

11.　ユーザ情報リストの［修正］ボタンをクリックします。

12. 以下の項目を指定します。

- ユーザ名　→user00
- ホストアドレス
  SNMP ホスト　→192.168.1.100
  トラップ通知ホスト　→192.168.1.100
- セキュリティプロトコル
  認証プロトコル　→MD5
  認証パスワード　→auth_password
  暗号プロトコル　→DES
  暗号パスワード　→priv_password
- MIB ビュー
  MIB 読み出し／ビュー定義番号　→MIB ビュー情報を使用／0
- トラップ通知／ビュー定義番号　→MIB ビュー情報を使用／0



13. ［保存］ボタンをクリックします。

14. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

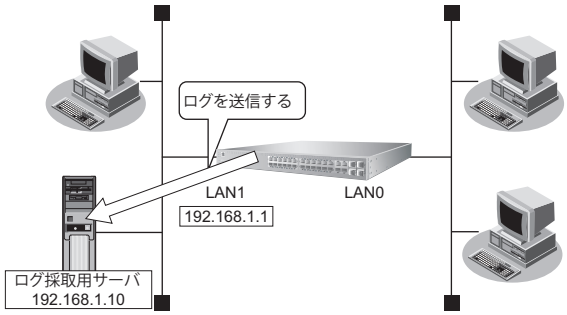
37　システムログを採取する

適用機種　全機種

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上のsyslogサーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- URLフィルタ（遮断したパケット）
- DHCP（配布したIPv4アドレス）

ここでは、システムログを採取する場合の設定方法を説明します。



● 設定条件

- 以下のセキュリティログを採取する
  - URLフィルタ
  - DHCP
- ログ受信用サーバのIPアドレス　：192.168.1.10

上記の設定条件に従ってシステムログを採取する場合の設定例を示します。

システムログ情報を設定する

1. 設定メニューの基本設定で「装置情報」をクリックします。

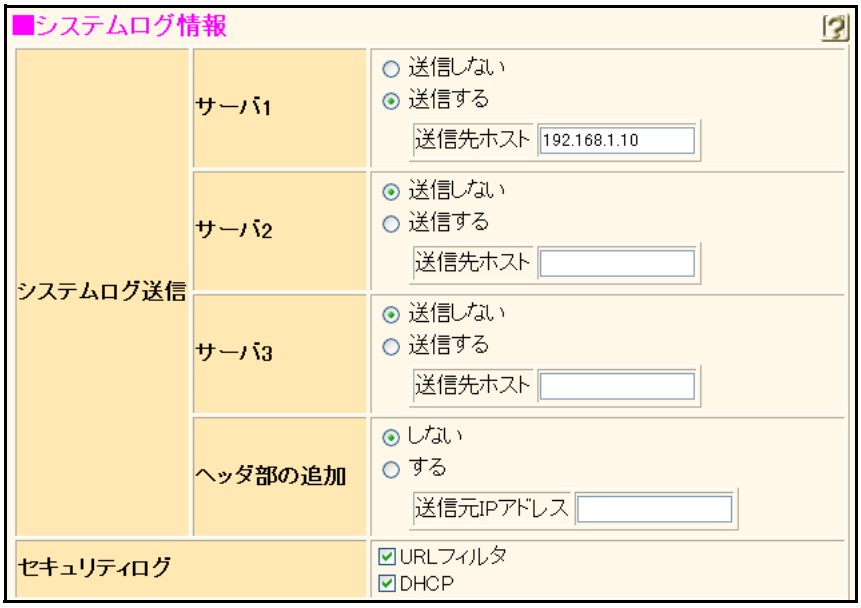
「装置情報」ページが表示されます。

2. 「システムログ情報」をクリックします。

「システムログ情報」が表示されます。

3. 以下の項目を指定します。

- システムログ送信　→送信する
  送信先ホスト　→192.168.1.10
- セキュリティログ　→URL フィルタ、DHCP



4. ［保存］ボタンをクリックします。

5. 画面左側の［設定反映］ボタンをクリックします。

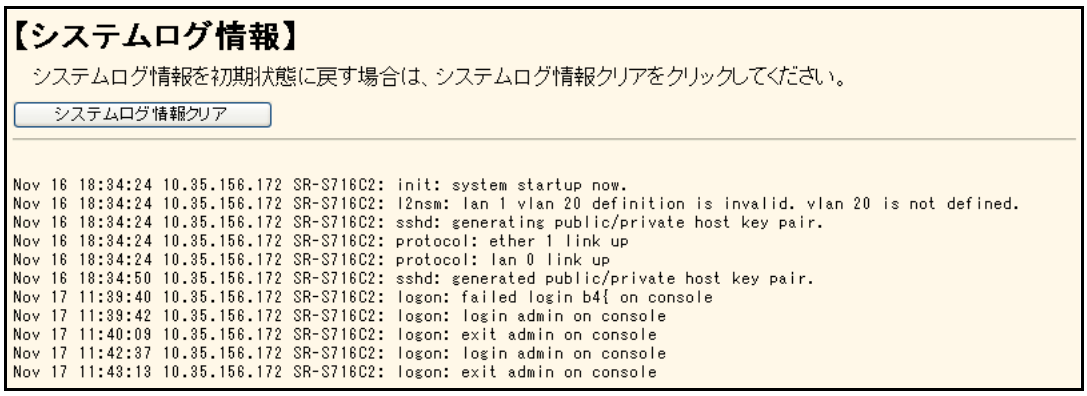
設定した内容が有効になります。

採取したシステムログを確認する

採取したシステムログの確認方法は、お使いのサーバによって異なります。
ここでは、本装置で確認する方法を説明します。

1. 表示メニューの「システム関連」の「システムログ情報」をクリックします。

「システムログ情報」ページが表示されます。



38　スケジュール機能を使う

適用機種　全機種

本装置のスケジュール機能は、以下のとおりです。

- 構成定義情報切り替え予約
  本装置は、内部に2つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

☛ 参照　マニュアル「Webユーザーズガイド」

38.1　構成定義情報の切り替えを予約する

適用機種　全機種

本装置は、内部に構成定義情報を2つ持つことができます。

ここでは、2006年12月1日6時30分に構成定義情報を構成定義情報1から構成定義情報2に切り替える場合の設定方法を説明します。

● 設定条件

- 実行日時　：2006年12月1日　6時30分
- 構成定義情報切り替え　：構成定義情報1の構成定義情報→構成定義情報2の構成定義情報

上記の設定条件に従って構成定義情報を切り替える場合の設定例を示します。

1.　設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

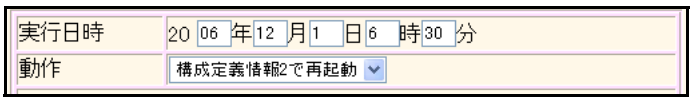
2.　「構成定義切り替え予約情報」をクリックします。

「構成定義切り替え予約情報」が表示されます。

3.　「構成定義切り替え予約情報」で未設定の欄の［修正］ボタンをクリックします。

4.　以下の項目を指定します。

- 実行日時　→2006年12月1日6時30分
- 動作　→構成定義情報2で再起動



5.　［保存］ボタンをクリックします。

6.　画面左側の［設定反映］ボタンをクリックします。

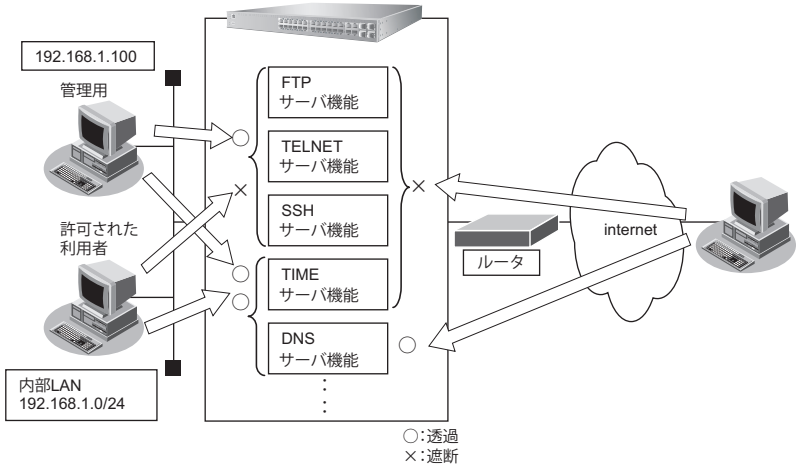
設定した内容が有効になります。

39 アプリケーションフィルタ機能を使う

適用機種 全機種

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

● 設定条件

- 管理用のホスト（192.168.1.100）からのみTELNET/FTP/SSHサーバ機能へのアクセスを許可する
- 内部LANのホスト（192.168.1.0/24）からのみTIMEサーバ機能へのアクセスを許可する
- その他のサーバ機能は制限しない

こんな事に気をつけて

IPフィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行っていてもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合の設定例を示します。

メンテナンス用のサーバ機能（TELNET/FTP/SSH）にアクセスできるパソコンを制限する

1. 設定メニューの詳細設定で「ACL情報」をクリックします。

「ACL 情報」ページが表示されます。

2. 以下の項目を指定します。

- 定義名 →acl0

＜ACL情報追加フィールド＞	
定義名	acl0

3. ［追加］ボタンをクリックします。

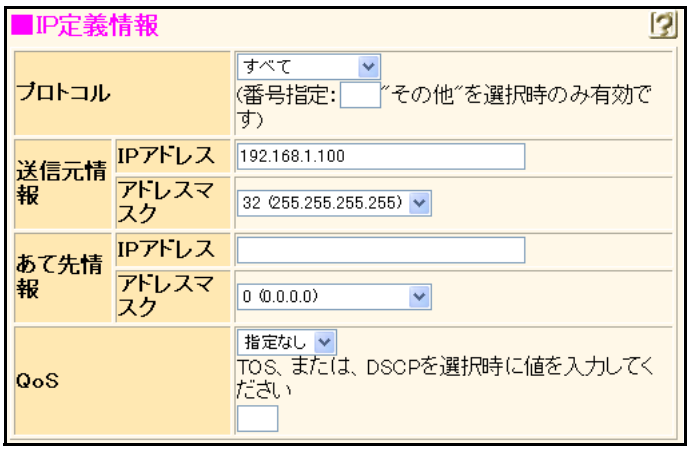
「ACL 定義情報（acl0）」ページが表示されます。

4.　「IP 定義情報」をクリックします。

「IP 定義情報」が表示されます。

5.　以下の項目を指定します。

- プロトコル　→すべて
- 送信元情報
  IP アドレス　→ 192.168.1.100
  アドレスマスク　→ 32（255.255.255.255）
- あて先情報
  IP アドレス　→指定しない
  アドレスマスク　→ 0（0.0.0.0）
- QoS　→指定なし



6.　［保存］ボタンをクリックします。

7.　設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

8.　「サーバ機能情報」をクリックします。

「サーバ機能情報」が表示されます。

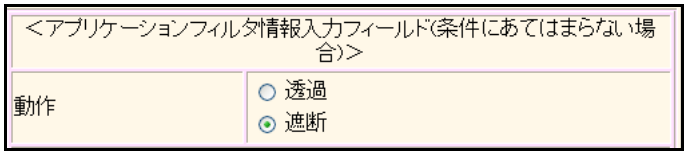
9.　「FTP サーバ機能」のアプリケーションフィルタ機能に対する［設定］ボタンをクリックします。

「アプリケーションフィルタ情報（FTP）」が表示されます。

10.　「条件にあてはまらない場合の動作」の［修正］ボタンをクリックします。

11.　以下の項目を指定します。

- 動作　→遮断



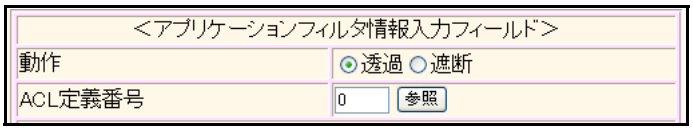
12.　［保存］ボタンをクリックします。

「アプリケーションフィルタ情報（FTP）」に戻ります。

13. 以下の項目を指定します。

- 動作 →透過
- ACL 定義番号 →0

補足 「ACL 定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



14. ［追加］ボタンをクリックします。

15. 手順 7. ～ 14. を参考に、TELNET サーバ機能、SSH サーバ機能に対しても同様の設定を行います。

TIME サーバ機能を使用できるパソコンを 192.168.1.0/24 のネットワークに制限する

16. 手順 1. ～ 14. を参考に、以下の項目を設定します。

「ACL 情報」

- 定義名 →acl1

「ACL 定義情報（acl1）」-「IP 定義情報」

- プロトコル →すべて
- 送信元情報
  IP アドレス →192.168.1.0
  アドレスマスク →24（255.255.255.0）
- あて先情報
  IP アドレス →指定しない
  アドレスマスク →0（0.0.0.0）
- QoS →指定なし

「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（TIME）」条件にあてはまらない場合の動作

- 動作 →遮断

「サーバ機能情報」-「アプリケーションフィルタ情報（TIME）」

- 動作 →透過
- ACL 定義番号 →1

17. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

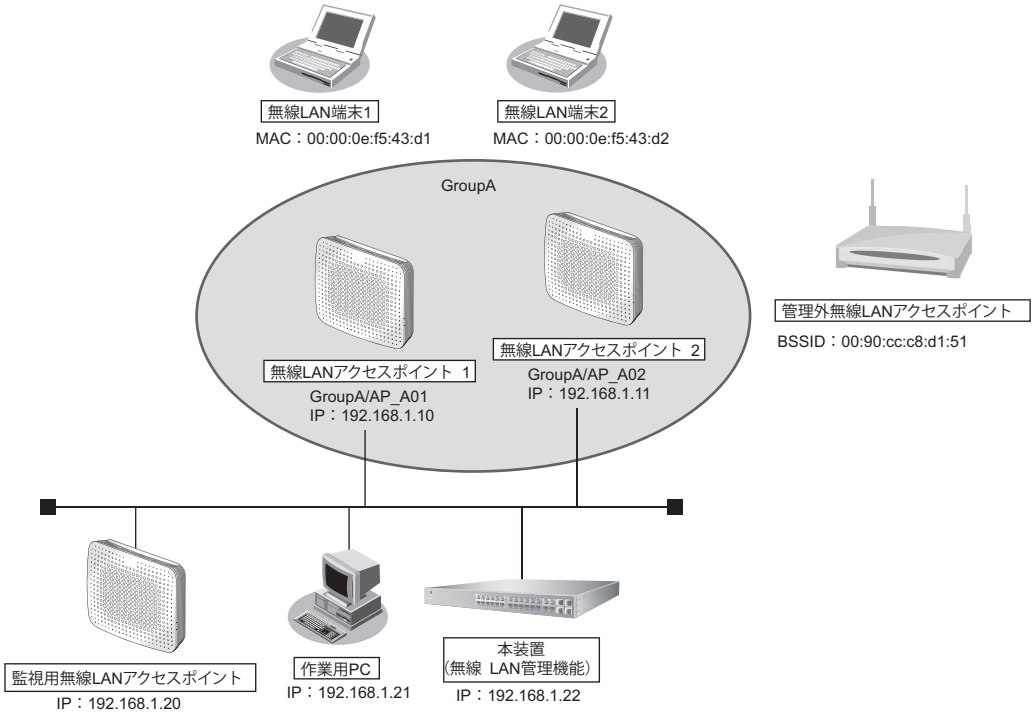
40　無線 LAN 管理機能を使う

適用機種　全機種

40.1　無線 LAN 管理機能の環境を設定する

適用機種　全機種

ここでは、複数の無線 LAN アクセスポイントによって構成されたネットワークを無線 LAN 管理機能で管理する場合の設定方法を説明します。



補足　無線 LAN の監視を実施する場合は、1 台以上の無線 LAN アクセスポイントを監視用に設定してください。

無線 LAN 管理機能で監視できる無線 LAN チャネルは、監視用に設定した無線 LAN アクセスポイントの周辺アクセスポイント検出機能の設定に依存します。周辺アクセスポイント検出機能の設定方法は、弊社製の無線 LAN アクセスポイント（SR-M50AP1/20AP1/20AP2）のマニュアルを参照してください。

こんな事に気をつけて

- **管理機器のログイン時の入力プロンプトは、システムデフォルトのままとしてください。管理機器のログイン時の入力プロンプトを変更された場合、無線 LAN 管理機器の動作は不定となります。**
- **管理機器で nodemgr アカウントの情報を変更した場合、無線 LAN 管理機能の対応するアカウント情報も同時に変更するようにしてください。**

● 設定条件

- 無線 LAN 管理対象
  管理グループ
  　グループ名　：GroupA
  無線 LAN アクセスポイント 1
  　管理機器名　：AP_A01
  　IP アドレス　：192.168.1.10
  　アカウント　：ユーザ ID：nodemgr、パスワード：nodemgr1
  無線 LAN アクセスポイント 2
  　管理機器名　：AP_A02
  　IP アドレス　：192.168.1.11
  　アカウント　：ユーザ ID：nodemgr、パスワード：nodemgr2
- 監視用無線 LAN アクセスポイント
  周辺アクセスポイント検出機能をスキャン専用モードで運用
  使用する無線 LAN モジュール　：ieee80211 1、ieee80211 2
  　管理機器名　：Watcher
  　IP アドレス　：192.168.1.20
  　監視用アカウント　：ユーザ ID：nodemgr、パスワード：nodemgr3
- 管理外無線 LAN アクセスポイント
  　MAC アドレス　：00:90:cc:c8:d1:51
- 管理情報取得の時間パラメタ（アクセスポイントモニタリング用）
  情報取得間隔　：10 秒
  情報取得待機間隔　：10 秒
  情報取得タイムアウト時間　：5 秒
- 監視のパラメタ（アクセスポイントモニタリング用）
  有線 LAN
  　稼動監視間隔　：10 秒
  　稼動監視待機間隔　：10 秒
  　稼動監視タイムアウト時間　：5 秒
  　稼動監視 通信異常判定しきい値　：6 回
  無線 LAN
  　スキャンレポート取得間隔　：10 秒
  　スキャンレポート取得待機間隔　：10 秒
  　スキャンレポート取得タイムアウト時間　：1 分
  　無線 LAN 監視 通信異常判定しきい値　：6 回
- 監視ログのパラメタ（アクセスポイントモニタリング／クライアントモニタリング用）
  監視ログ保持件数　：100 件
- 無線 LAN 端末の RSSI 監視のパラメタ（クライアントモニタリング用）
  RSSI 評価母数　：10 個
  RSSI 最低しきい値　：20

上記の設定条件に従って設定を行う場合の設定例を示します。

管理グループを設定する

1. 設定メニューの無線LAN管理設定で「無線LAN管理情報」をクリックします。

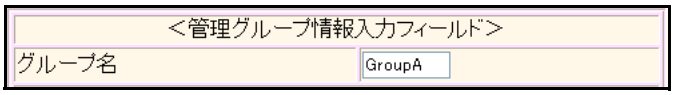
「無線LAN管理情報」ページが表示されます。

2. 「管理グループ情報」をクリックします。

「管理グループ情報」が表示されます。

3. 以下の項目を指定します。

- グループ名 →GroupA



4. [追加] ボタンをクリックします。

無線LANアクセスポイントを設定する

5. 設定メニューの無線LAN管理設定で「無線LAN管理情報」をクリックします。

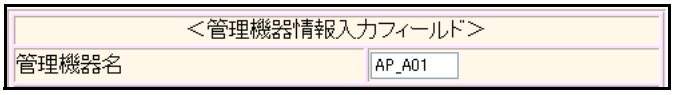
「無線LAN管理情報」ページが表示されます。

6. 「管理機器情報」をクリックします。

「管理機器情報」が表示されます。

7. 以下の項目を指定します。

- 管理機器名 →AP_A01



8. [追加] ボタンをクリックします。

管理機器情報の設定項目と「基本情報」が表示されます。

9.　無線LANアクセスポイント1について、以下の項目を指定します。

- グループ　→GroupA
- IPアドレス　→192.168.1.10
- 無線LAN管理パスワード　→nodemgr1
- 無線LAN管理パスワード（確認用）　→nodemgr1
- 監視用　→使用しない
- 無線LAN端末の情報取得　→情報取得する

補足　監視用を「使用する」に設定した無線LAN管理機器の無線LANの監視を実施する場合は、監視用を「使用する」に設定した無線LAN管理機器を相互に監視できる範囲内に2台以上設置してください。

10.　［保存］ボタンをクリックします。

11.　無線LANアクセスポイント1と同様に、無線LANアクセスポイント2について、以下の項目を指定します。

「無線LAN管理情報」-「管理機器情報」

- 管理機器名　→AP_A02

「管理機器情報（1）」-「基本情報」

- グループ　→GroupA
- IPアドレス　→192.168.1.11
- 無線LAN管理パスワード　→nodemgr2
- 無線LAN管理パスワード（確認用）　→nodemgr2
- 監視用　→使用しない
- 無線LAN端末の情報取得　→情報取得する

12.　［保存］ボタンをクリックします。

監視用無線LANアクセスポイントを設定する

13. 無線LANアクセスポイント1、2と同様に、監視用無線LANアクセスポイントについて、以下の項目を設定します。

「無線LAN管理情報」-「管理機器情報」

- 管理機器名 →Watcher

「管理機器情報（4）」-「基本情報」

- IPアドレス →192.168.1.20
- 無線LAN管理パスワード →nodemgr3
- 無線LAN管理パスワード（確認用） →nodemgr3
- 監視用 →使用する
- 無線LAN端末の情報取得 →情報取得しない

管理外無線LANアクセスポイントを設定する

管理外無線LANアクセスポイントとして登録します。

補足 使用目的が明確で管理不要な無線LANアクセスポイントを管理外無線LANアクセスポイントとして設定すると、不明無線LANアクセスポイントのモニタリングが容易となります。

14. 設定メニューの無線LAN管理設定で「無線LAN管理情報」をクリックします。

「無線LAN管理情報」ページが表示されます。

15. 「管理外機器情報」をクリックします。

「管理外機器情報」が表示されます。

16. 以下の項目を指定します。

- 管理外機器名 →UMAP01
- MACアドレス →00:90:cc:c8:d1:51

＜管理外機器情報入力フィールド＞	
管理外機器名	UMAP01
MACアドレス	00:90:cc:c8:d1:51

17. ［追加］ボタンをクリックします。

管理情報取得の時間パラメタを設定する

18. 設定メニューの無線LAN管理設定で「無線LAN管理パラメタ情報」をクリックします。

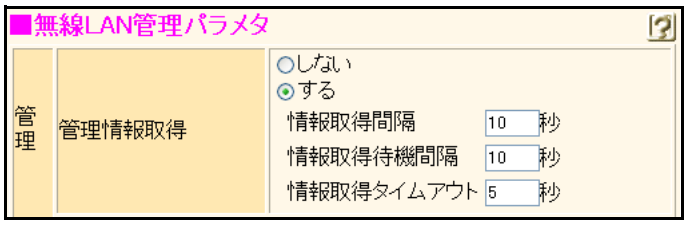
「無線LAN管理パラメタ情報」ページが表示されます。

19. 「無線LAN管理パラメタ情報」をクリックします。

「無線LAN管理パラメタ」が表示されます。

20. 以下の項目を指定します。

- 管理－管理情報取得　→する
  情報取得間隔　→10秒
  情報取得待機間隔　→10秒
  情報取得タイムアウト　→5秒



補足　管理－管理情報取得のパラメタ「情報取得間隔」と「情報取得待機間隔」の設定は、監視ポリシーに従って最適な値を設定するようにしてください。

21. ［保存］ボタンをクリックします。

有線LAN、無線LANの監視パラメタを設定する

有線LAN、無線LANの監視パラメタ、監視ログのパラメタや無線LAN端末のRSSI監視のパラメタなどを設定します。

22. 設定メニューの無線LAN管理設定で「無線LAN管理パラメタ情報」をクリックします。

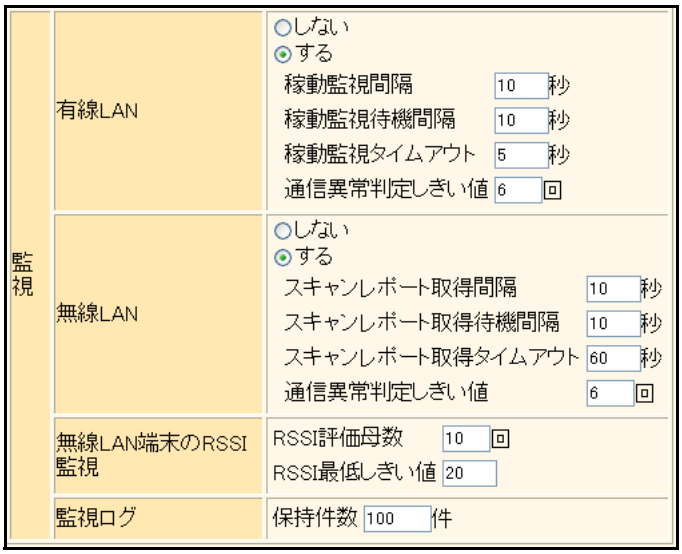
「無線LAN管理パラメタ情報」ページが表示されます。

23. 「無線LAN管理パラメタ情報」をクリックします。

「無線LAN管理パラメタ」が表示されます。

24. 以下の項目を指定します。

- 監視－有線 LAN →する
  稼動監視間隔 →10秒
  稼動監視待機間隔 →10秒
  稼動監視タイムアウト →5秒
  通信異常判定しきい値 →6回
- 監視－無線 LAN →する
  スキャンレポート取得間隔 →10秒
  スキャンレポート取得待機間隔 →10秒
  スキャンレポート取得タイムアウト →60秒
  通信異常判定しきい値 →6回
- 監視－無線 LAN 端末の RSSI 監視
  RSSI 評価母数 →10回
  RSSI 最低しきい値 →20
- 監視－監視ログ
  保持件数 →100件



補足 以下のパラメタは、監視ポリシーに従って最適な値を設定するようにしてください。
- 監視－有線 LAN のパラメタ「稼動監視間隔」と「稼動監視待機間隔」
- 監視－無線 LAN のパラメタ「スキャンレポート取得間隔」と「スキャンレポート取得待機間隔」

25. ［保存］ボタンをクリックします。

26. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

40.2 アクセスポイントモニタリングを行う

適用機種 全機種

無線 LAN 管理機能は、アクセスポイントモニタリングをすることができます。

補足
- モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワークの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を置いたあと、再度モニタリング結果を表示してみてください。
- 使用目的が明確で管理不要な無線 LAN アクセスポイントを管理外無線 LAN アクセスポイントとして設定すると、不明無線 LAN アクセスポイントのモニタリングが容易となります。

ここでは、「40.1 無線 LAN 管理機能の環境を設定する」（P.339）で構築した環境に対するアクセスポイントモニタリングの設定例を示します。

管理無線 LAN アクセスポイントのモニタリング結果の一覧を表示する

1. 表示メニューで「無線 LAN 管理関連」の「管理無線 LAN アクセスポイントの監視状況の一覧表示」をクリックします。

「管理無線 LAN アクセスポイントの監視状況の一覧表示」ページが表示され、管理無線 LAN アクセスポイントの監視状況の一覧が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan scan managed brief」を参照してください。

管理無線 LAN アクセスポイントの有線 LAN、無線 LAN のモニタリング結果を表示する

1. 表示メニューで「無線 LAN 管理関連」の「管理機器の詳細情報表示」をクリックします。

「管理機器の詳細情報表示」ページが表示され、稼動状況が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager node」を参照してください。

管理無線 LAN アクセスポイントの無線 LAN のモニタリング結果を表示する

1. 表示メニューで「無線 LAN 管理関連」の「管理無線 LAN アクセスポイントの監視状況の表示」をクリックします。

「管理無線 LAN アクセスポイントの監視状況の表示」ページが表示され、管理無線 LAN アクセスポイントの監視状況が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan scan managed」を参照してください。

管理外無線 LAN アクセスポイントのモニタリング結果を表示する

1. 表示メニューで「無線 LAN 管理関連」の「管理外無線 LAN アクセスポイントの監視状況の表示」をクリックします。

「管理外無線 LAN アクセスポイントの監視状況の表示」ページが表示され、管理外無線 LAN アクセスポイントの監視状況が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan scan unmanaged」を参照してください。

不明無線LANアクセスポイントのモニタリング結果を表示する

1. 表示メニューで「無線LAN管理関連」の「不明無線LANアクセスポイントの監視状況の表示」をクリックします。

「不明無線LANアクセスポイントの監視状況の表示」ページが表示され、不明無線LANアクセスポイントの監視状況が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan scan unknown」を参照してください。

40.3 クライアントモニタリングを行う

適用機種 全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントと接続している無線 LAN 端末のクライアントモニタリングをすることができます。

補足 モニタリングは各管理機器にアクセスして収集した結果を出力していますので、構成定義の設定直後や、ネットワークの状況によっては収集が完了しておらず、途中の状態が表示される場合があります。この場合は、しばらく時間を置いたあと、再度モニタリング結果を表示してみてください。

ここでは、「40.1 無線 LAN 管理機能の環境を設定する」（P.339）で構築した環境に対するクライアントモニタリングの設定例を示します。

無線 LAN 端末の受信信号強度のモニタリング結果を表示する

1. 表示メニューで「無線 LAN 管理関連」の「無線 LAN 端末の RSSI 最大値／最小値の一覧表示」をクリックします。

「無線 LAN 端末の RSSI 最大値／最小値の一覧表示」ページが表示され、無線 LAN 端末の受信信号強度状況が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan sta rssi」を参照してください。

無線 LAN 端末の接続状況をモニタリングする

1. 表示メニューで「無線 LAN 管理関連」の「無線 LAN インタフェースの無線 LAN 端末情報の表示」をクリックします。

「無線 LAN インタフェースの無線 LAN 端末情報の表示」ページが表示されます。

2. 無線 LAN 端末情報を表示させる管理機器を選択します。

選択した管理機器の無線 LAN 端末情報が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan sta」を参照してください。

無線 LAN 端末の接続拒否情報をモニタリングする

1. 表示メニューで「無線 LAN 管理関連」の「接続拒否の無線 LAN 端末情報の表示」をクリックします。

「接続拒否の無線 LAN 端末情報の表示」ページが表示されます。

2. 接続拒否の無線 LAN 端末情報を表示させる管理機器を選択します。

選択した管理機器の無線 LAN 端末情報が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan reject」を参照してください。

無線LANインタフェースのトレース情報をモニタリングする

1. 表示メニューで「無線LAN管理関連」の「無線LAN通信のトレース情報の表示」をクリックします。

「無線LAN通信のトレース情報の表示」ページが表示されます。

2. 無線LAN通信のトレース情報を表示させる管理機器を選択します。

選択した管理機器の無線LAN通信のトレース情報が確認できます。

参照 画面の表示結果については、マニュアル「コマンドリファレンス」の「show nodemanager logging wlan trace」を参照してください。

40.4 無線LANアクセスポイントにMACアドレスフィルタを配布する（MACアドレスフィルタ配布）

適用機種　全機種

無線LAN管理機能は、無線LANアクセスポイントへの無線LAN端末の（MACアドレスによる）接続許可情報を一括管理して配布することができます。

補足　管理機器のMACアドレスフィルタをクリアしたい場合は、MACアドレスフィルタを設定していないMACアドレスフィルタセットを配布してください。

● 設定条件

- 無線LANの接続を許可する端末
  無線LAN端末1（MACアドレス：00:00:0e:f5:43:d1）
  無線LAN端末2（MACアドレス：00:00:0e:f5:43:d2）
  無線LANの接続を拒否する端末
  上記以外
- MACアドレスフィルタの配布先
  無線LANアクセスポイント1
  無線LANアクセスポイント2

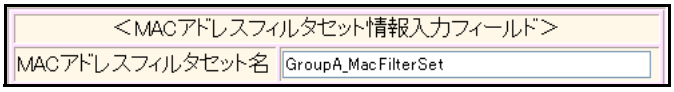
ここでは、「40.1 無線LAN管理機能の環境を設定する」（P.339）で構築した環境に対するMACアドレスフィルタ配布の設定例を示します。

1.　設定メニューの無線LAN管理設定で「MACアドレスフィルタセット情報」をクリックします。

「MACアドレスフィルタセット情報」ページが表示されます。

2.　以下の項目を指定します。

- MACアドレスフィルタセット名　→GroupA_MacFilterSet



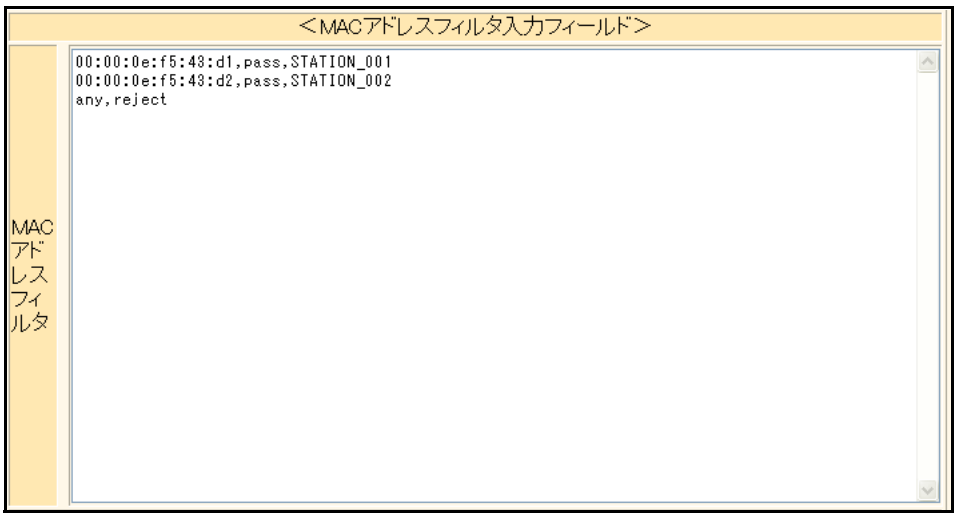
3.　［追加］ボタンをクリックします。

4.　「MACアドレスフィルタセット情報」でMACアドレスフィルタセット名がGroupA_MacFilterSetの［MACアドレスフィルタ］ボタンをクリックします。

MACアドレスフィルタ情報の設定項目と「MACアドレスフィルタ情報」が表示されます。

5.　以下の項目を指定します。

- MACアドレスフィルタ　→00:00:0e:f5:43:d1,pass,STATION_001
  00:00:0e:f5:43:d2,pass,STATION_002
  any,reject



6.　［保存］ボタンをクリックします。

7.　画面左側の［設定反映］ボタンをクリックします。

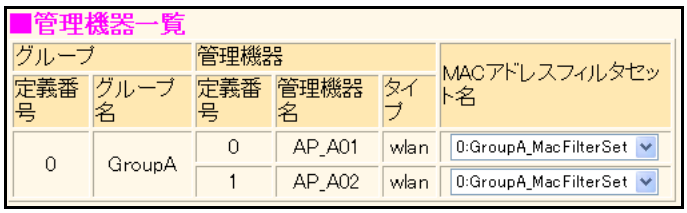
設定した内容が有効になります。

8.　操作メニューで「無線LAN管理操作」の「MACアドレスフィルタ配布」をクリックします。

「MACアドレスフィルタ配布」ページが表示されます。

9.　以下の項目を指定します。

- AP_A01のMACアドレスフィルタセット名　→0:GroupA_MacFilterSet
- AP_A02のMACアドレスフィルタセット名　→0:GroupA_MacFilterSet



補足　MACアドレスフィルタを配布しない管理機器のMACアドレスフィルタセット名は、空欄のままとしてください。

10.　［MACアドレスフィルタ配布］ボタンをクリックします。

MACアドレスフィルタ配布の実行結果が表示され、管理対象となった無線LANアクセスポイントにMACアドレスフィルタの配布が行われます。

参照　画面の実行結果については、マニュアル「コマンドリファレンス」の「nodemanagerctl update wlan filterset」を参照してください。

40.5 無線 LAN アクセスポイントの電波出力を調整する（電波出力自動調整）

適用機種　全機種

無線 LAN 管理機能は、無線 LAN アクセスポイントの電波出力を調整することができます。

補足 近隣管理機器には、電波出力自動調整機能で設定対象の無線 LAN アクセスポイントの無線を到達させたい無線 LAN アクセスポイントを設定します。ただし、電波出力自動調整による送信出力の調整には時間がかかりますので、必要以上に近隣管理機器を設定しないようにしてください。電波出力自動調整は、構成定義で設定した " 電波自動調整の RSSI 最低しきい値 " に近い値になるまで、以下の処理を繰り返します。

1. 近隣管理機器での周辺アクセスポイント情報の取得
   必要時間：約 60 秒 × 近隣管理機器の台数
2. 電波出力の確認
   RSSI 最低しきい値に近い値であれば終了
3. 無線 LAN アクセスポイントの無線送信出力の設定
   必要時間：約 10 秒
4. 無線送信出力の安定待ち
   必要時間：約 90 秒
5. 手順 1. の処理から繰り返し

こんな事に気をつけて

- **電波出力自動調整は、無線 LAN インタフェースの動作タイプが AP のみ（未設定を含む）で構成される無線 LAN アクセスポイントを対象とするようにしてください。**
- **電波出力自動調整の近隣機器には、以下の条件を満たす無線 LAN アクセスポイントを指定してください。**
  - **調整対象と同じ無線 LAN モジュールが動作している。**
  - **その無線 LAN モジュールの動作タイプは、AP、SCANONLY または未設定のみから構成される。**
- **電波出力自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で電波出力自動調整を行うようにしてください。**

● 設定条件

- 電波出力を調整する無線 LAN アクセスポイント
  無線 LAN アクセスポイント 1
  無線 LAN アクセスポイント 2
- 無線 LAN アクセスポイント 1 の近隣管理機器
  無線 LAN アクセスポイント 2、監視用無線 LAN アクセスポイント
- 無線 LAN アクセスポイント 2 の近隣管理機器
  無線 LAN アクセスポイント 1、監視用無線 LAN アクセスポイント
- 電波出力自動調整の RSSI 最低しきい値　：20

ここでは、「40.1 無線 LAN 管理機能の環境を設定する」（P.339）で構築した環境に対する電波出力自動調整の設定例を示します。

1. 設定メニューの無線 LAN 管理設定で「無線 LAN 管理情報」をクリックします。

「無線 LAN 管理情報」ページが表示されます。

2. 「管理機器情報」をクリックします。

「管理機器情報」が表示されます。

3. 「管理機器情報」で管理機器名が AP_A01 の［修正］ボタンをクリックします。

管理機器情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- 近隣管理機器　→1、4

5.　［保存］ボタンをクリックします。

6.　AP_A01と同様に、AP_A02について、以下の項目を指定します。

- 近隣管理機器　→0、4

7.　［保存］ボタンをクリックします。

8.　設定メニューの無線LAN管理設定で「無線LAN管理パラメタ情報」をクリックします。

「無線LAN管理パラメタ情報」ページが表示されます。

9.　「無線LAN管理パラメタ情報」をクリックします。

「無線LAN管理パラメタ」が表示されます。

10.　以下の項目を指定します。

- 管理－電波出力自動調整
  RSSI最低しきい値　→20

11.　［保存］ボタンをクリックします。

12.　画面左側の［設定反映］ボタンをクリックします。

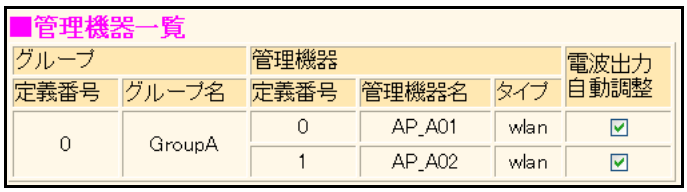
設定した内容が有効になります。

13.　操作メニューで「無線LAN管理操作」の「無線LAN電波出力の自動調整」をクリックします。

「無線LAN電波出力の自動調整」ページが表示されます。

14.　以下の項目を指定します。

- AP_A01の電波出力自動調整をチェック
- AP_A02の電波出力自動調整をチェック



15.　［電波出力自動調整］ボタンをクリックします。

電波出力自動調整の実行結果が表示され、管理対象となった無線LANアクセスポイントの電波出力が自動的に調整されます。

補足　電波出力の自動調整を開始したあとにキャンセルした場合、現在処理中の無線LANアクセスポイントの電波出力の調整が完了するまでバックグラウンドで処理を行います。この間、無線LAN管理機能のほかの操作はできません。

参照　画面の実行結果については、マニュアル「コマンドリファレンス」の「nodemanagerctl wlan autotxpower」を参照してください。

40.6 無線LANアクセスポイントの無線LANチャネルを調整する

適用機種 全機種

無線LAN管理機能は、無線LANアクセスポイントの無線LANチャネルを自動的に調整することができます。

こんな事に気をつけて

無線LANチャネル自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で無線LANチャネル自動調整を行うようにしてください。

● 設定条件

- IEEE802.11n通信時に使用する帯域幅
  通信帯域幅 ：40MHz
- 5GHz帯のチャネル自動調整
  割当範囲 ：w52/53/56
- 2.4GHz帯のチャネル自動調整
  判定用RSSIしきい値 ：20
  開始チャネル ：1
  チャネル割当間隔 ：5

ここでは、「40.1 無線LAN管理機能の環境を設定する」（P.339）で構築した環境に対する無線LANチャネル自動調整の設定例を示します。

1. 設定メニューの無線LAN管理設定で「無線LAN管理パラメタ情報」をクリックします。

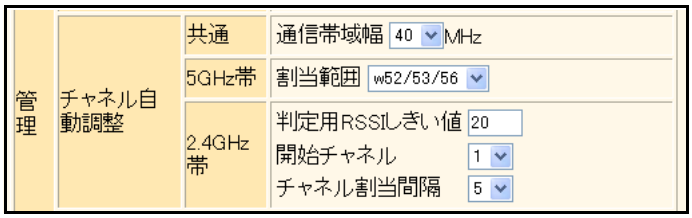
「無線LAN管理パラメタ情報」ページが表示されます。

2. 「無線LAN管理パラメタ情報」をクリックします。

「無線LAN管理パラメタ」が表示されます。

3. 以下の項目を指定します。

- 管理－チャネル自動調整－共通
  通信帯域幅 →40MHz
- 管理－チャネル自動調整－5GHz帯
  割当範囲 →w52/53/56
- 管理－チャネル自動調整－2.4GHz帯
  判定用RSSIしきい値 →20
  開始チャネル →1
  チャネル割当間隔 →5



4. ［保存］ボタンをクリックします。

5. 画面左側の［設定反映］ボタンをクリックします。

設定した内容が有効になります。

6.　操作メニューで「無線 LAN 管理操作」の「無線 LAN チャネルの自動調整」をクリックします。

「無線 LAN チャネルの自動調整」ページが表示されます。

7.　以下の項目を指定します。

- AP_A01 のチャネル自動調整をチェック
- AP_A02 のチャネル自動調整をチェック

■管理機器一覧

グループ		管理機器			チャネル自動調整
定義番号	グループ名	定義番号	管理機器名	タイプ	
0	GroupA	0	AP_A01	wlan	☑
		1	AP_A02	wlan	☑

8.　［チャネル自動調整］ボタンをクリックします。

無線 LAN チャネル自動調整の実行結果が表示され、管理対象となった無線 LAN アクセスポイントの無線 LAN チャネルが自動的に調整されます。

補足　無線 LAN チャネルの自動調整を開始したあとにキャンセルした場合、現在処理中の無線 LAN アクセスポイントの無線 LAN チャネルの調整が完了するまでバックグラウンドで処理を行います。この間、無線 LAN 管理機能のほかの操作はできません。

参照　画面の実行結果については、マニュアル「コマンドリファレンス」の「nodemanagerctl wlan autochannel」を参照してください。

40.7 災害用Wi-Fi機能を使う

適用機種 全機種

災害用Wi-Fi機能は、WEB画面からの一括操作で、管理下の無線LANアクセスポイントの無線LANインタフェース（SSID）を開放、閉塞できる機能です。

災害時の00000JAPAN機能として使用することができます。

こんな事に気をつけて

災害用Wi-Fi機能は管理者クラスでのみ使用できます。管理者クラスでログインしてください。

● 設定条件

- 無線LANインタフェースを開放する無線LANアクセスポイント
  無線LANアクセスポイント1
  無線LANアクセスポイント2
- 開放する無線LANインタフェース
  無線LANインタフェース8
  無線LANインタフェース16

こんな事に気をつけて

- **無線LANアクセスポイントの無線LANモジュールが有効になっていない場合、無線LANインタフェースを開放することができません。無線LANアクセスポイントで、以下のコマンドが設定されていることを確認してください。**

```
password nodemgr set <password>
ieee80211 1 use on
ieee80211 1 mode <mode>
ieee80211 2 use on
ieee80211 2 mode <mode>
wlan 8 ssid <ssid>
wlan 16 ssid <ssid>
nodemanager login service enable
```

ここでは、「40.1 無線LAN管理機能の環境を設定する」（P.339）で構築した環境に対する災害用Wi-Fi機能の設定例を示します。

災害用Wi-Fiを設定する

1. 設定メニューの無線LAN管理設定で「災害用Wi-Fi情報」をクリックします。

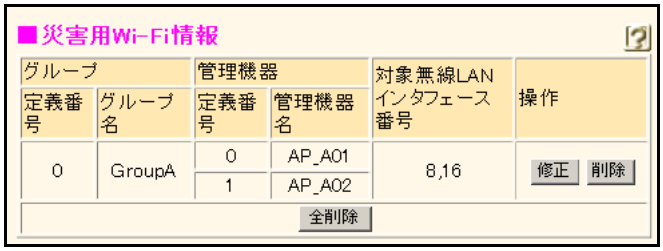
「災害用Wi-Fi情報」ページが表示されます。

2. ［修正］ボタンをクリックします。

「無線LANインタフェース設定」ページが表示されます。

3. wlan8とwlan16をチェックし、[保存] ボタンをクリックします。

「災害用Wi-Fi情報」ページに戻ります。



4. **画面左側の［設定反映］ボタンをクリックします。**

設定した内容が有効になると、トップページ左上に「災害用Wi-Fi」に関するボタンが表示されます。

災害用 Wi-Fi を開放する

5.　トップページ左上の「災害用 Wi-Fi」の［開放］ボタンをクリックします。

「本当に開放してもよろしいですか？」のプロンプトメッセージが出力されます。

6.　プロンプトメッセージの［OK］ボタンをクリックします。

設定された無線 LAN インタフェースが開放され、［開放］ボタンは［開放中］に変わります。

補足　開放または停止操作に失敗した場合、システムログ情報に管理機器情報と失敗した理由を出力します。
表示メニューのシステムログ情報で確認してください。また、すべての無線 LAN インタフェースに失敗した場合は、ボタン表示は［開放中］または［停止中］に変わりません。

41 装置を保護する

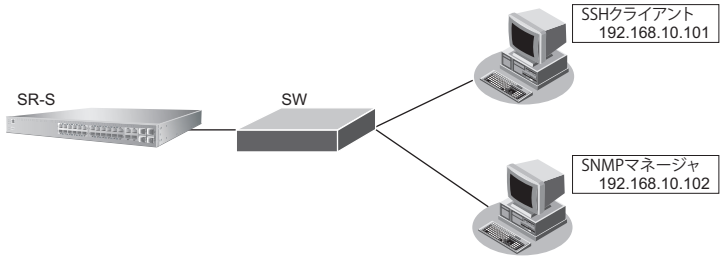
適用機種 全機種

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者(admin)用パスワードの設定
- オートログアウトの設定
- Telnet/SSHおよびSNMP接続に対するアクセス制限
- 不要なサービスの停止

41.1 設定例

以下にそれぞれの設定を行う場合の例を示します。



● 設定条件

- 管理者(admin) パスワード ：srs_admin-2022
- IPアドレス ：192.168.10.100/24
- オートログアウトの設定（ログインしたままの状態で指定時間無操作だった際に自動切断を行う）
  コンソールのオートログアウト時間 ：5分
  SSHのオートログアウト時間 ：5分
  ※SSH のオートログアウト時間は "telnetinfo autologout" と共通
- SNMP設定
  アクセス許可するSNMPマネージャ ：192.168.10.102
  コミュニティ名 ：private
  マネージャからの書き込み ：許可しない
- SSH接続を許可するホストのIPアドレス ：192.168.10.101
- Telnet接続 ：禁止

adminパスワードをsrs_admin-2022に設定する

1. 設定メニューの基本設定で「パスワード情報」をクリックします。

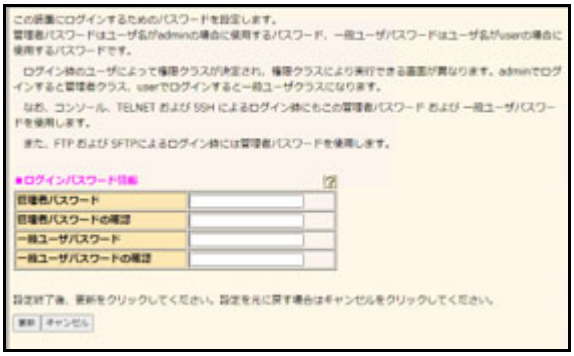
「パスワード情報」のページが表示されます。

2. 「パスワード情報」で「ログインパスワード情報」をクリックします。

「ログインパスワード情報」が表示されます。

3.　以下の項目を指定します。

- 管理者パスワード　→srs_admin-2022
- 管理者パスワードの確認　→srs_admin-2022



本装置を操作するときのパスワードを設定します。パスワードの設定は更新直後から有効になります。

4.　[更新]ボタンをクリックします。

コンソール接続のオートログアウト時間（コンソールおよびTelnet/SSHログインしたままで指定時間内に無操作時にオートログアウトを行う設定）およびtelnet/sshのオートログアウトまでの無操作時間を5分に設定する

1.　コンソールから以下の設定を行います。

consoleinfo autologout 5m

telnetinfo autologout 5m

VLAN1 のネットワークを設定する

1.　設定メニューの詳細設定で「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

2.　「LAN情報」でインタフェースがLAN0の［修正］ボタンをクリックします。

「LAN0情報」ページが表示されます。

3.　「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

4.　以下の項目を指定します。

- VLAN ID　→1

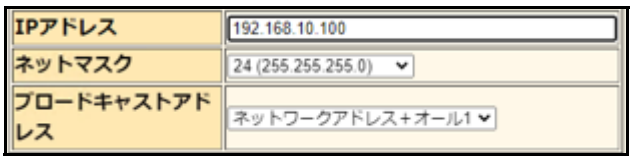
5.　［保存］ボタンをクリックします。

6.　「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

7.　以下の項目を指定します。

- IPアドレス　→192.168.10.100
- ネットマスク　→24（255.255.255.0）
- ブロードキャストアドレス　→ネットワークアドレス＋オール1



8. ［保存］ボタンをクリックします。

SNMP を有効にし、TRAP 送信を v1、書き込み許可を disable に設定

1. 設定メニューの詳細設定で「SNMP 情報」をクリックします。

   「SNMP 情報」ページが表示されます。

2. 以下の項目を指定します。

   - SNMP エージェント機能　→使用する
   - エージェントアドレス　→ 192.168.10.100

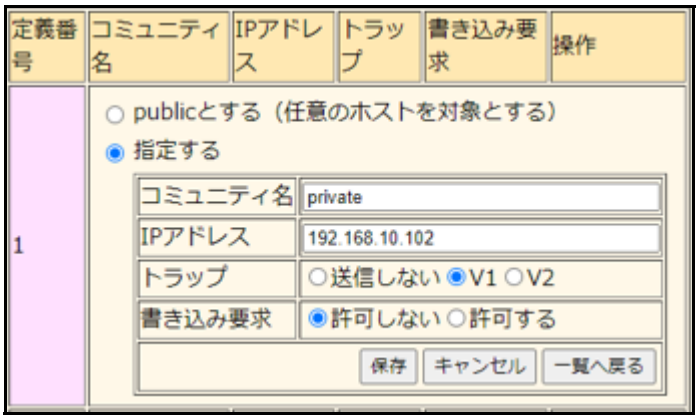
3. ［保存］ボタンをクリックします。
4. 「SNMPv1/v2c 情報」をクリックします。

   「SNMPv1/v2c 情報」が表示されます。

5. 定義番号 1 の「修正する」をクリックします。

6.　以下の項目を指定します。

- SNMP ホスト 1　→指定する
- コミュニティ名　→ private
- IP アドレス　→ 192.168.10.102
- トラップ　→ v1
- 書き込み要求　→許可しない



7.　［保存］ボタンをクリックします。

不要なサービスはすべて停止

1.　設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

2.　「サーバ機能情報」をクリックします。不要なサーバ機能を停止します。

- FTP サーバ機能　→停止
- TELNET サーバ機能　→停止
- SFTP サーバ機能　→停止
- DNS サーバ機能　→停止
- SNTP サーバ機能　→停止
- TIME サーバ機能 TCP　→停止
- TIME サーバ機能 UDP　→停止

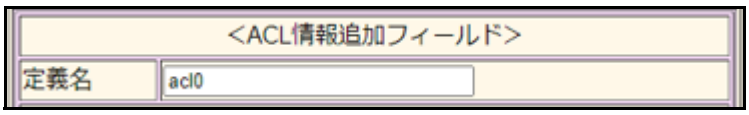
3. **［保存］ボタンをクリックします。**

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

特定の SSH/HTTP/HTTPS クライアントからの通信のみを許可し、他の SSH/HTTP/HTTPS 通信を破棄

1. **設定メニューの詳細設定で「ACL 情報」をクリックします。**
   「ACL 情報」ページが表示されます。

2. **以下の項目を指定します。**
   - 定義名　→acl0



3. **［追加］ボタンをクリックします。**
   「ACL 定義情報（acl0）」ページが表示されます。

4. **「IP 定義情報」をクリックします。**
   「IP 定義情報」が表示されます。

5. **以下の項目を指定します。**
   - プロトコル　→すべて
   - 送信元情報}
     IP アドレス　→192.168.10.101
     アドレスマスク　→32（255.255.255.255）
   - あて先情報
     IP アドレス　→指定しない
     アドレスマスク　→0（0.0.0.0）
   - QoS　→指定なし

6. **［保存］ボタンをクリックします。**

7. **設定メニューの基本設定で「装置情報」をクリックします。**
   「装置情報」ページが表示されます。

8. **「サーバ機能情報」をクリックします。**

「サーバ機能情報」が表示されます。

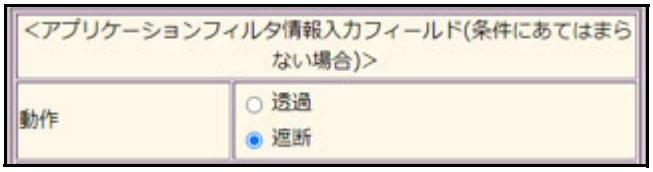
9. **「SSH サーバ機能」-「SSH」のアプリケーションフィルタ機能に対する［設定］ボタンをクリックします。**

「アプリケーションフィルタ情報（SSH）」が表示されます。

10. **「条件にあてはまらない場合の動作」の［修正］ボタンをクリックします。**

11. **以下の項目を指定します。**

- 動作 →遮断



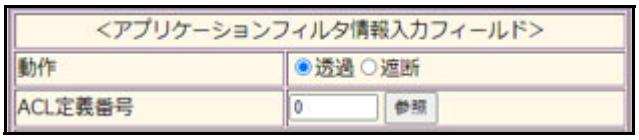
12. **［保存］ボタンをクリックします。**

「アプリケーションフィルタ情報（SSH）」に戻ります。

13. **以下の項目を指定します。**

- 動作 →透過
- ACL 定義番号 →0

補足 「ACL定義番号」を指定する際は、［参照］ボタンをクリックして、表示された画面から設定する定義番号欄の［選択］ボタンをクリックして設定します。



14. **［追加］ボタンをクリックします。**

15. **手順 9.～14. を参考に、「HTTP サーバ機能」、「HTTPS サーバ機能」をクリックし、特定の HTTP/HTTPS クライアントからの通信のみを許可し、他の HTTP/HTTPS 通信を破棄する設定を行います。**

索引

V

W

あ

え

か

き

く

こ

さ

し

す

せ

そ

た

て

と

は

ふ

ほ

ま

む

め

ゆ

り

る

ろ

SR-S　Web 設定事例集

P3NK-7132-02Z0

発行日　　2022 年 11 月

発行責任　　富士通株式会社