APRESIA®

TD61-6865A

# ApresiaLightGS シリーズ

# ユーザーズガイド

APRESIA Systems 株式会社

# 制 定 ・ 改 訂 来 歴 表

| No. | 年　　月　　日 | 内　　容 |
|---|---|---|
| - | 2019年1月29日 | 新規作成 |
| A | 2019年4月10日 | Appendix A～Dを追加 |
| | | |

# Contents

# 1. 本書について

本書は、IT ネットワークを構築・監理する実務者向けに作成したガイドブックです。
Web ブラウザーで表示する管理画面から ApresiaLightGS シリーズスイッチの設定管理を行う際に参考となる情報を提供します。

# 2. 免責事項

本書に記載されている画面や設定項目などは、一般的な使用を想定して説明しています。
そのため、ご使用の IT ネットワーク環境によっては、記載内容と異なる場合があります。
実際の使用状況や環境に応じて、設定してください。

# 3. 概要

ApresiaLightGS シリーズスイッチ（以後、スイッチ）は、Web ブラウザーを使用して容易に設定管理することができる、スマートタイプの L2 スイッチです。スモールビジネス向けに必要な機能を実装し、コストパフォーマンスの高いネットワークソリューションを提供します。

## 3.1. 管理機能

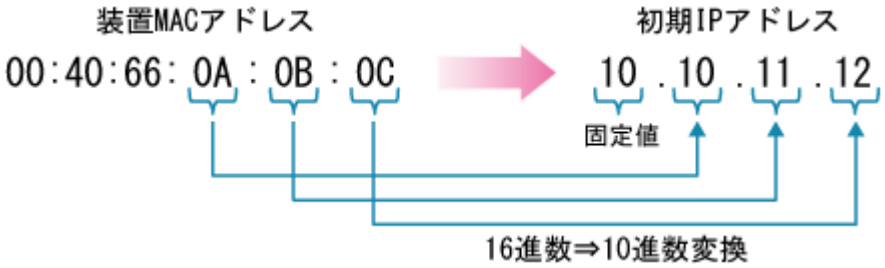
本スイッチは、Web ブラウザーによるスイッチ管理画面、および Simple Network Management Protocol（以後、SNMP）による管理機能を搭載しています。また、Secure Sockets Layer（以後、SSL）による拡張セキュリティーも使用できます。

### 3.1.1. 初期 IP アドレス設定

初回起動時の初期 IP アドレス（IPv4）は、以下の設定ルールに従って自動設定されています。ご使用の環境に合わせて IP アドレスを変更してください。

#### 3.1.1.1. 初期 IP アドレスの設定ルール

初期 IP アドレスの先頭 1 バイトは、固定値「10」です。2 バイトから 4 バイトまでは、装置 MAC アドレスの下位 3 バイトを 16 進数から 10 進数に変換した値で、自動的に設定されます。
装置 MAC アドレスが「00:40:66:0A:0B:0C」の場合、初期 IP アドレスは「10.10.11.12」となります。




#### 3.1.1.2. サブネットマスク

サブネットマスクは、固定長 8 ビット（255.0.0.0）に設定されます。

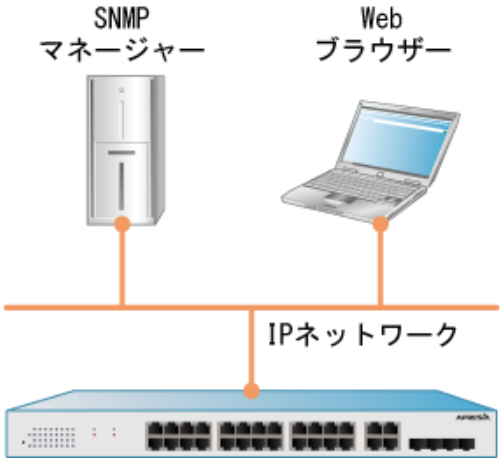
#### 3.1.1.3. 初期 IP アドレスの確認方法

初期 IP アドレスは、装置の銘板ラベル上に表記されています。また、管理画面で表示される MAC アドレス表示を元に、初期 IP アドレスの設定ルールに従って算出することもできます。

# 3.2. 操作方法

## 3.2.1. スイッチの操作

スイッチは、Web ブラウザーで接続する管理画面や、SNMP マネージャーから設定できます。
本書では、Web ブラウザーによる設定について説明します。




### 3.2.1.1. Web ブラウザーでの管理

Web ブラウザーを使用して、スイッチを管理することができます。使用する PC の IP アドレスとサブネットマスクは、スイッチの IP アドレスとサブネットマスクに応じて設定します。

例）スイッチの IP アドレスが 10.0.0.1、サブネットマスクが 255.0.0.0 の場合

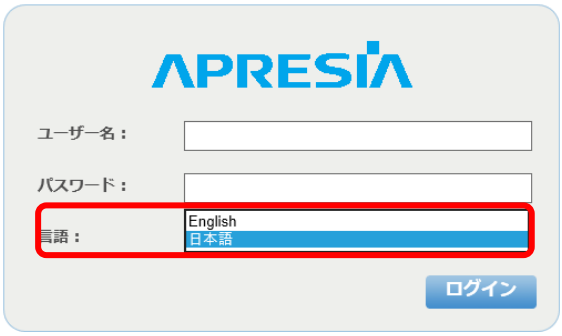
| 項目 | スイッチ | PC | 入力値 |
|---|---|---|---|
| IP アドレス | 10.0.0.1 | 10.X.X.Y | X は 0～255 の範囲で任意の値。<br>Y は 1～254 の範囲で任意の値（ただしスイッチと同一の IP アドレスにならないようにする）。 |
| サブネットマスク | 255.0.0.0 | 255.0.0.0 など | スイッチと同じ値を推奨。 |

上記の例の場合、Web ブラウザーのアドレスバーに「http://10.0.0.1（スイッチの IP アドレス）」を入力してアクセスします。アクセスに成功するとログイン画面が表示されますので、ユーザー名とパスワードを入力してログインします。
管理者アカウントのデフォルトユーザー名は「adpro」です。パスワードは設定されていません。

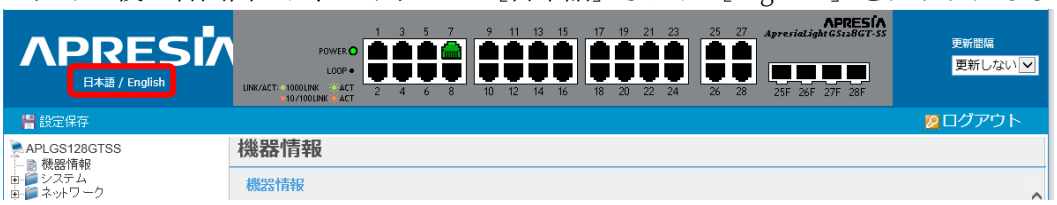
### n 管理画面の表示言語の設定

管理画面の表示言語として、日本語または英語を選択できます。
表示言語は、ログインページやログイン後の画面で変更できます。

・ ログインページでは、［言語］で［日本語］または［English］を選択します。




・ ログイン後の各画面では、ヘッダーの［日本語］または［English］をクリックします。




### n 管理者アカウントのパスワード設定

Web ブラウザーで初回にログインした後は、以降の手順に従って管理者アカウントのパスワードを設定してください。

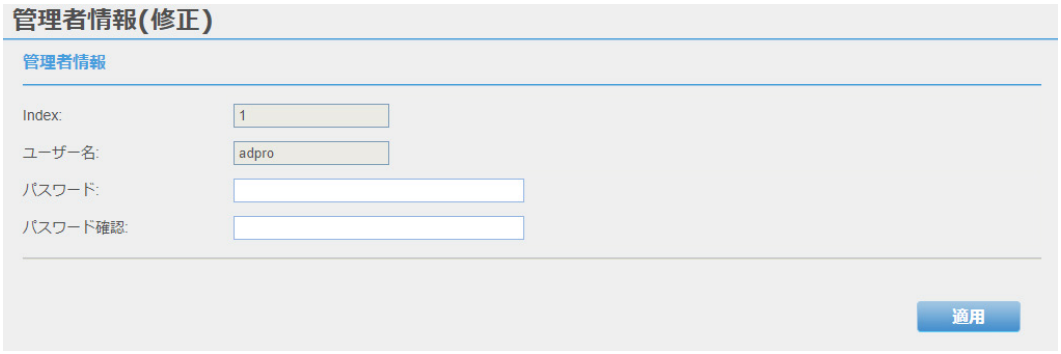
**1. メニューから［システム］＞［管理者設定］を選択します。**


**2. 管理者テーブルにある、管理者アカウント「adpro」の［変更］ボタンをクリックします。**

**3. パスワードを変更します。**

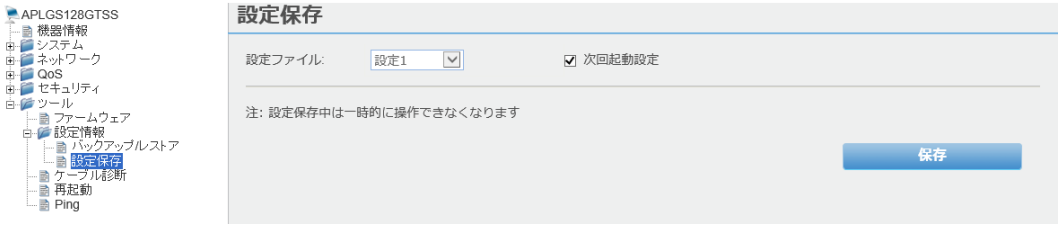
パスワードとパスワード確認の入力ボックスに新規パスワードを入力します。パスワードは最大 20 文字で設定可能です。21 文字目以降は入力されませんのでご注意ください。
パスワードを空欄にすると、パスワードなしとして指定されます。
新規パスワードを入力した後、［適用］ボタンをクリックするとパスワードが反映されます。入力した

パスワードが一致しない場合、エラーダイアログによる警告が表示されて入力がクリアされますので、もう一度パスワードを入力してください。




新規パスワードが設定されると、ログインセッションが切断されますので、新規パスワードで再度ログインしてください。
変更したパスワードをスイッチの再起動後にも反映するためには、以降の操作により設定を保存する必要があります。

**4. メニューから［ツール］＞［設定情報］＞［設定保存］を選択します。**




**5. 設定を保存します。**

［次回起動設定］のチェックボックスをオンにして、［保存］ボタンをクリックしてください。

# 4. 機器情報

## 4.1. 機器情報

［機器情報］ページで、システムの状態、ハードウェア情報、およびシステム情報など、各種情報を確認することができます。


| 基本情報 | |
|---|---|
| 起動時間 | スイッチの再起動や電源の再投入などが発生せず、スイッチが継続して起動している期間が表示されます。 |
| バージョン | 現在のファームウェアバージョンが表示されます。 |
| ブートローダー | 現在のブートローダーバージョンが表示されます。 |
| シリアル番号 | スイッチのシリアル番号が表示されます。 |

| ハードウェア | |
|---|---|
| DRAM | RAM のメモリーサイズが表示されます。 |
| Flash | フラッシュのメモリーサイズが表示されます。 |

| システム情報 | |
|---|---|
| システム名 | スイッチに設定したシステム名が表示されます。 |
| ロケーション | スイッチに設定したシステムロケーションが表示されます。 |
| 連絡先 | スイッチに設定したシステム管理者の情報が表示されます。 |

| MACアドレス、IPアドレス | |
|---|---|
| MACアドレス | スイッチのMACアドレスが表示されます。 |
| IPアドレス | スイッチに設定したIPv4アドレスが表示されます。 |
| サブネットマスク | スイッチに設定したIPv4サブネットマスクが表示されます。 |
| デフォルトゲートウェイ | スイッチに設定したIPv4デフォルトゲートウェイが表示されます。 |

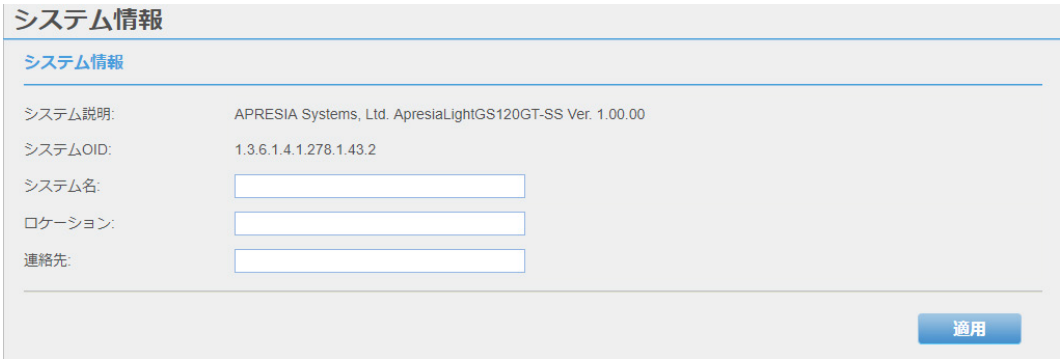
| IPv6情報 | |
|---|---|
| IPv6アドレス/プレフィックス長 | スイッチに設定したIPv6ユニキャストアドレスとプレフィックス長が表示されます。 |
| IPv6デフォルトゲートウェイ | スイッチに設定したIPv6デフォルトゲートウェイが表示されます。 |
| リンクローカルアドレス/プレフィックス長 | スイッチのIPv6リンクローカルアドレスとプレフィックス長が表示されます。 |

| 自動設定機能 | |
|---|---|
| DHCPクライアント | Dynamic Host Configuration Protocol（以後、DHCP）クライアントの状態（有効／無効）が表示されます。 |
| DHCPv6クライアント | DHCPv6クライアントの状態（有効／無効）が表示されます。 |

# 5. システム

## 5.1. システム情報

［システム情報］ページで、スイッチのシステム名、ロケーション、連絡先の情報を設定できます。
各種システム情報は、ネットワーク内のスイッチをネットワーク管理者が識別するために使用します。




| システム情報 | |
|---|---|
| システム説明 | スイッチの製品名が表示されます。 |
| システム OID | スイッチのオブジェクト識別子（以後、OID）が表示されます。<br>OID はシステムを一意に識別します。 |
| システム名 | スイッチを識別するシステム名を任意で 15 文字以内で入力します。 |
| ロケーション | スイッチの設置情報を示すシステムロケーションを任意で 30 文字以内で入力します。 |
| 連絡先 | スイッチのシステム管理者の情報を任意で 30 文字以内で入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

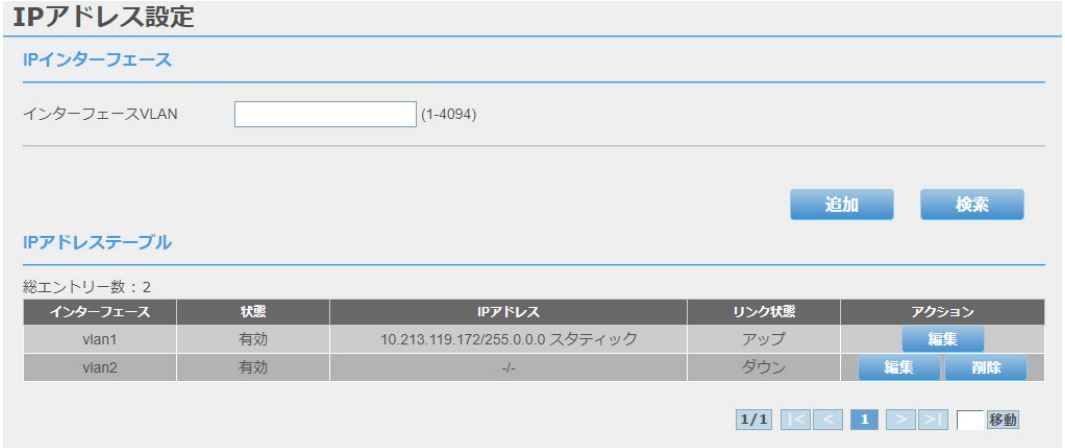
# 5.2. IP アドレス

## 5.2.1. IP アドレス設定

スイッチの管理用 IP アドレスは、VLAN インターフェース上に作成する IP インターフェースに設定されます。初期設定では、デフォルト VLAN（VLAN ID が 1 の VLAN）に IP インターフェースが作成されており、機器の MAC アドレスに対応した初期 IP アドレスが設定されています。

［IP アドレス設定］ページでは、作成済みの VLAN に対する IP インターフェースの登録や IP インターフェースの設定変更を行うことができます。たとえば、初期状態から IP アドレス設定だけを変えたい場合は、IP アドレステーブルのデフォルト VLAN のエントリー（vlan1）から［編集］ボタンをクリックし、編集画面から設定を変更します。

Note: 本画面では VLAN を新規登録することはできません。デフォルト VLAN 以外に対して IP インターフェースを割り当てる場合は、事前に［ネットワーク］＞［VLAN］＞［VLAN 設定］ページで設定してください。

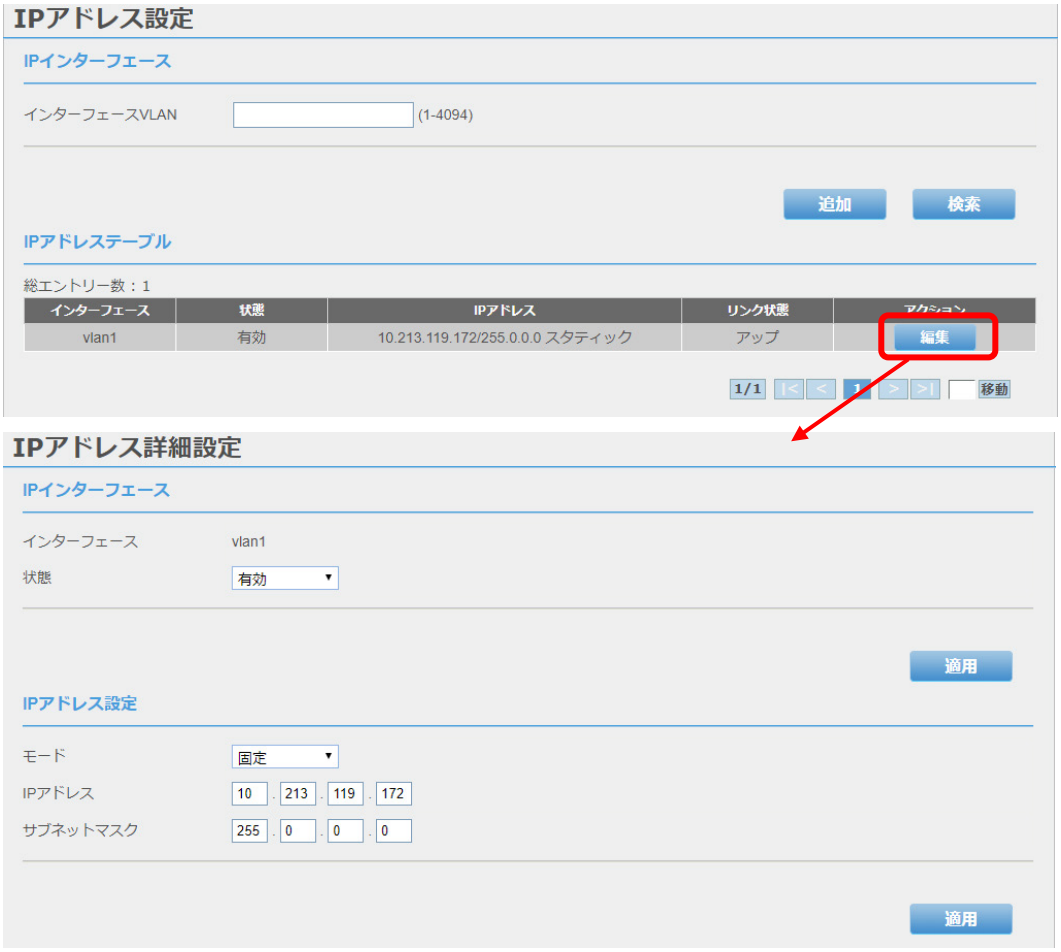



| IP インターフェース | |
|---|---|
| インターフェース VLAN | VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、指定した VLAN ID の VLAN インターフェースに IP インターフェースが追加されます。 |
| ［検索］ボタン | ［検索］ボタンをクリックすると、指定した VLAN ID の VLAN インターフェースのみを IP アドレステーブル上に表示します。 |

| IP アドレステーブル | |
|---|---|
| インターフェース | VLAN インターフェース名が表示されます。 |
| 状態 | IP インターフェースの状態（有効／無効）が表示されます。 |
| IP アドレス | IP インターフェースの IPv4 アドレスとモードが表示されます。 |

| | |
|---|---|
| リンク状態 | VLAN インターフェースのリンク状態が表示されます。<br>・ アップ:VLAN インターフェースでアクティブなポートが存在する<br>・ ダウン:VLAN インターフェースでアクティブなポートが存在しない |
| アクション | ［編集］ボタンをクリックすると、IP インターフェースの設定を変更できます。<br>［削除］ボタンをクリックすると、IP インターフェースが削除されます。VLAN インターフェースは削除されません。 |

IP アドレステーブルの［編集］ボタンをクリックすると、IP インターフェースの設定を変更できます。

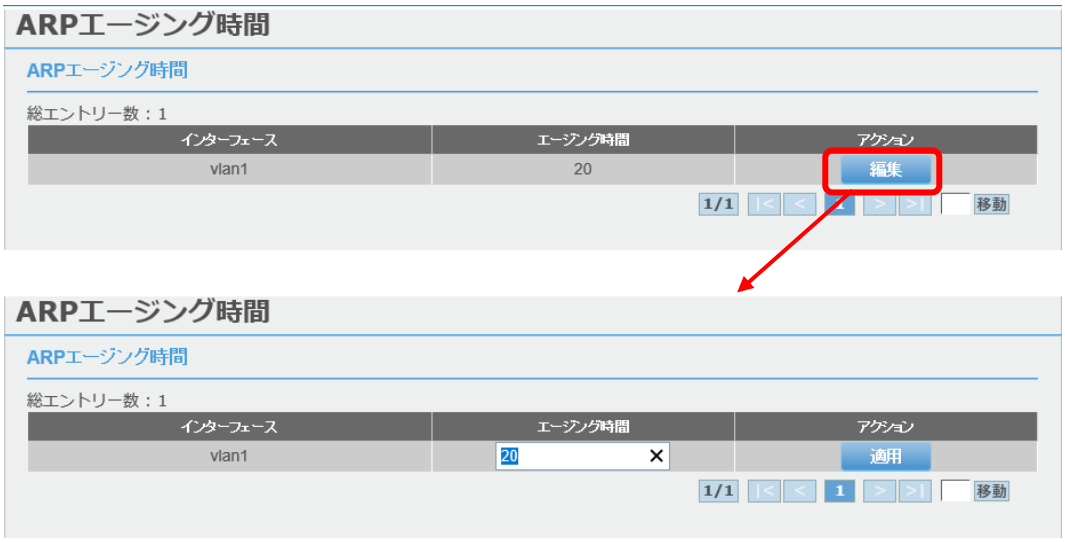



| IP インターフェース | |
|---|---|
| インターフェース | VLAN インターフェース名が表示されます。 |
| 状態 | IP インターフェースの状態（有効／無効）を選択します。IP アドレス設定を変更する場合、IP インターフェースの状態を有効にする必要があります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、IP インターフェースの状態の変更が適用されます。 |

| IP アドレス設定 | |
|---|---|
| モード | IP インターフェースの IPv4 アドレスのモードを選択します。<br>・ 固定：IP アドレスを手動で設定する<br>・ DHCP：DHCP サーバーから IP アドレスを取得する |
| IP アドレス | IP インターフェースの IP アドレスを入力します。 |
| サブネットマスク | IP インターフェースのサブネットマスクを入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

### 5.2.2. ARP エージング時間

［ARP エージング時間］ページで、IP インターフェースの ARP エージング時間を個別に変更できます。ARP エージング時間は、自動学習した ARP エントリーがその後更新されない場合に自然に失効するまでの期限を指します。たとえば、同一ネットワーク上の PC からスイッチ宛に Ping を実行すると、スイッチ上に ARP エントリーが自動的に作成されますが、ARP エージング時間が経過すると、その ARP エントリーは削除されます。




| ARP エージング時間 | |
|---|---|
| インターフェース | IP インターフェースがバインドされている VLAN インターフェース名が表示されます。 |
| エージング時間 | ARP エージング時間を表示します。（単位：分）<br>アクション列の［編集］ボタンをクリックすると、エージング時間を 0～65535 の範囲で指定することができます。（デフォルト：20）<br>0 に設定すると、ARP エントリーがタイムアウトされなくなります。 |
| アクション | ［編集］ボタンをクリックすると、ARP エージング時間の設定を変更できます。このとき、ボタンが［適用］ボタンに切り替わります。<br>［適用］ボタンをクリックすると、変更が適用されます。 |

## 5.2.3. ARP テーブル

［ARP テーブル］ページで、スイッチの ARP テーブルの情報を確認できます。また、スタティック ARP エントリーを手動で追加できます。

ARP テーブルは、ネットワーク内での ARP パケットの交換により自動的に作成される、同一ネットワーク内での IP アドレスと MAC アドレスのマッチングを登録したリストです。スイッチが管理通信などの IP パケットを送信する場合には ARP テーブルを参照します。

IP パケット送信時に対象ホストの IP アドレス（もしくはネクストホップ）に対する ARP エントリーを確認できない場合、スイッチは ARP パケットを使用してエントリーを登録しようとします。それでもエントリーを作成できなければ、スイッチは IP パケットを送信することができません。

スタティック ARP エントリーは手動で設定する ARP テーブルの永続的なエントリーで、IP アドレスと MAC アドレスのマッチングが確実である場合に管理者が登録することがあります。スタティック ARP エントリーには、スイッチに設定している IP インターフェースと同一ネットワーク内の IP アドレスを指定します。


| スタティック ARP | |
|---|---|
| IP アドレス | ARP エントリーの IP アドレスを入力します。 |
| MAC アドレス | ARP エントリーの MAC アドレスを入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、ARP エントリーが作成されます。 |

| ARP テーブル | |
|---|---|
| インターフェース名 | VLAN インターフェース名が表示されます。 |
| IP アドレス | ARP エントリーの IP アドレスが表示されます。 |
| MAC アドレス | ARP エントリーの MAC アドレスが表示されます。 |
| エージング時間 | ARP エントリーの ARP エージング時間（単位：分）が表示されます。 |
| ARP タイプ | ARP エントリーの種類が表示されます。<br>・ ダイナミック：自動学習により登録されたエントリー<br>・ スタティック：設定により登録されたエントリー |
| アクション | ［削除］ボタンをクリックすると、ARP エントリーが削除されます。 |

## 5.2.4. ルート設定

［ルート設定］ページでは、IPv4 のスタティックルートを設定することができます。
スタティックルートは、異なるネットワークのホストにパケットを送信する際、最初に送信ターゲットにする宛先デバイス（ルーターや L3 スイッチなど）を設定したものです。宛先デバイスの IP アドレスをネクストホップと呼びます。
スタティックルートは、宛先ネットワークを指定して個別に設定して登録することができますが、全ネットワークに対するネクストホップ（デフォルトルート）を指定することも可能です。スタティックルートを登録していない場合、異なるネットワークのホスト宛の通信を行うことができないため、スイッチが管理通信可能なホストは IP インターフェースと同一のネットワーク内に限定されます。

該当する有効なエントリーが複数存在する場合、ネットワークの範囲（ネットマスクの範囲）がより限定されているエントリーが選択されます。たとえば、デフォルトルート以外の有効なエントリーが該当する場合、そのエントリーはデフォルトルートより優先されます。


| ルート設定 | |
|---|---|
| IP アドレス | ［ネットマスク］と組み合わせて、ルート設定の対象となる宛先ネットワークを指定します。<br>［デフォルトルート］がチェックされている場合、すべてのネットワーク（0.0.0.0/0）を対象として指定します。<br>対象となるネットワークを直接指定する場合は、［デフォルトルート］のチェックを外し、ネットワークアドレスを入力してください。 |
| ネットマスク | ［IP アドレス］と組み合わせて、ルート設定の対象となる宛先ネットワークを指定します。<br>［デフォルトルート］がチェックされている場合、すべてのネットワーク（0.0.0.0/0）を対象として指定します。<br>対象となるネットワークを直接指定する場合は、［デフォルトルート］のチェックを外し、サブネットマスクを入力してください。 |

| | |
|---|---|
| ネクストホップ | ［IP アドレス］および［ネットマスク］で指定したネットワークを宛先とするパケットを転送する IP アドレスを指定します。<br>ネクストホップは、IP インターフェースと同一のネットワーク上にあるアドレスを指定する必要があります。 |
| 経路順位 | 経路順位（プライマリー／バックアップ）を選択します。<br>ルートの宛先 IPv4 アドレスには、プライマリーとバックアップのゲートウェイアドレスを１つずつ指定できます。<br>途中経路で障害が発生したなど、スイッチがプライマリールートへの疎通が取れないことを検知した場合、バックアップルートにパケットを転送します。 |
| ［適用］ボタン | ［適用］ボタンをクリックするとルートエントリーが登録されます。 |

| ルートテーブル | |
|---|---|
| IP アドレス | ルートエントリーのネットワークアドレスが表示されます。 |
| ネットマスク | ルートエントリーのサブネットマスクが表示されます。 |
| ネクストホップ | ルートエントリーのネクストホップアドレスが表示されます。 |
| 経路順位 | ルートエントリーの経路順位が表示されます。 |
| インターフェース | 関連する IP インターフェースがバインドされている VLAN インターフェース名が表示されます。 |
| アクション | ［削除］ボタンをクリックするとルートエントリーが削除されます。 |

## 5.2.5. IPv6 アドレス設定

スイッチの管理に IPv6 アドレスを使用する場合、VLAN インターフェース上に作成する IPv6 インターフェースに IPv6 アドレスを設定します。IPv6 インターフェースは、IP インターフェース（IPv4）と連動しており、どちらか一方を作成すると自動的にもう一方も VLAN インターフェースに割り当てられます。

［IPv6 アドレス設定］ページで、作成済みの VLAN に対する IPv6 インターフェースの登録や IPv6 インターフェースの設定変更を行うことができます。


| IPv6 インターフェース | |
|---|---|
| インターフェース VLAN | VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、指定した VLAN ID の VLAN インターフェースに IPv6 インターフェースが追加されます。 |
| ［検索］ボタン | ［検索］ボタンをクリックすると、指定した VLAN ID の VLAN インターフェースのみを IPv6 アドレステーブル上に表示します。 |

| IPv6 アドレステーブル | |
|---|---|
| インターフェース | VLAN インターフェース名が表示されます。 |
| 状態 | IPv6 インターフェースの状態（有効／無効）が表示されます。 |
| リンク状態 | IPv6 インターフェースのリンク状態が表示されます。<br>IPv6 インターフェースは、いずれかの VLAN メンバーポートのリンクがアップである必要があります。<br>・ アップ:VLAN インターフェースでアクティブなポートが存在する<br>・ ダウン:VLAN インターフェースでアクティブなポートが存在しない |
| アクション | ［詳細設定］ボタンをクリックすると、IPv6 インターフェースの設定を変更できます。<br>IPv6 インターフェース（および IP インターフェース）を削除する場合は、［システム］＞［IP アドレス］＞［IP アドレス設定］から、対応する IP インターフェースを削除してください。 |

IPv6 アドレステーブルの［詳細設定］ボタンをクリックすると、IPv6 インターフェースの設定を変更できます。


| IPv6 インターフェース | |
|---|---|
| インターフェース | VLAN インターフェース名が表示されます。 |
| 状態 | IPv6 インターフェースの状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、IPv6 インターフェースの状態の変更が適用されます。 |

| IP アドレス設定 | |
|---|---|
| DHCPv6 クライアント機能 | DHCPv6 クライアントの状態（有効／無効）を選択します。 |
| IPv6 アドレス/プレフィックス長 | IPv6 インターフェースのリンクローカルアドレスやグローバルユニキャスト IPv6 アドレスを手動で設定することができます。 |

| | |
|---|---|
| | デフォルトでは、IPv6 インターフェースの状態を有効にするとスイッチの MAC アドレスから IPv6 Modified EUI-64 識別子を生成して、リンクローカルアドレスを自動的に設定します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| ネイバー要請 | |
|---|---|
| ネイバー要請(NS)送信間隔 | NS メッセージを再送信する間隔を 1～3600（秒）の範囲で入力します。（デフォルト：1 秒） |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| IPv6 アドレステーブル | |
|---|---|
| アドレスタイプ | IPv6 アドレスの種類（グローバルユニキャスト IPv6 アドレス／リンクローカルアドレス）が表示されます。 |
| IPv6 アドレス | IPv6 アドレス／プレフィックス長の情報が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、IPv6 アドレスエントリーが削除されます。 |

## 5.2.6. IPv6 ネイバー

IPv6 ネットワークにおいて、同一ネットワークに存在するノードをネイバーと呼びます。IPv6 ネットワークでは、近隣捜索プロトコルを使用してネイバーの情報を収集し、IPv6 ネイバーテーブル（IPv4 での ARP テーブルに相当）のエントリーを自動的に作成します。

スタティック IPv6 ネイバーは手動で設定する IPv6 ネイバーテーブルの永続的なエントリーで、スタティック ARP エントリーと同様に IPv6 アドレスと MAC アドレスのマッチングが確実である場合に管理者が登録することがあります。

［IPv6 ネイバー］ページで、スイッチの IPv6 ネイバーテーブルの情報を確認できます。また、スタティック IPv6 ネイバーエントリーを手動で追加できます。

| スタティック IPv6 ネイバー | |
|---|---|
| ネイバーIPv6 アドレス | ネイバーの IPv6 アドレスを入力します。 |
| MAC アドレス | ネイバーの MAC アドレスを入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、指定したネイバーのスタティックエントリーが追加されます。 |

| IPv6 ネイバーテーブル | |
|---|---|
| ネイバーIPv6 アドレス | 自動学習やスタティックエントリーにより登録されたネイバーの IPv6 アドレスが表示されます。 |
| MAC アドレス | ネイバーの MAC アドレスが表示されます。 |
| タイプ | ネイバーのタイプが表示されます。<br>・ スタティック：設定により登録されたネイバー情報<br>・ ダイナミック：自動学習により登録されたネイバー情報 |
| アクション | ・ ［検索］ボタン：<br>ネイバーIPv6 アドレスと MAC アドレスを入力し、タイプを選択して、［検索］ボタンをクリックすると、指定した IPv6 ネイバーが表示されます。<br>・ ［削除］ボタン：<br>ネイバーIPv6 アドレスと MAC アドレスに「*」を入力して、［削除］ボタンをクリックすると、すべてのエントリーが削除されます。<br>また、各エントリーの［削除］ボタンをクリックすると、ネイバーエントリーが削除されます。 |

## 5.2.7. IPv6 ルート設定

［IPv6 ルート設定］ページでは、IPv6 のスタティックルートを設定することができます。

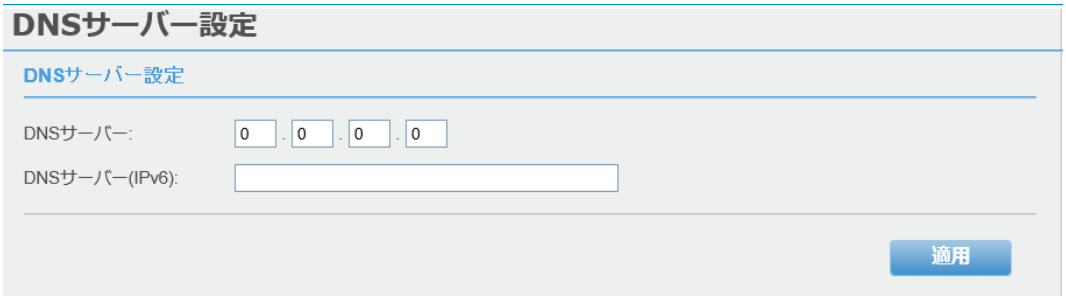
| IPv6 ルート設定 | |
|---|---|
| IPv6 アドレス/プレフィックス長 | ルート設定の対象となる宛先ネットワークを指定します。<br>［デフォルトルート］がチェックされている場合、すべてのネットワーク（::/0）を対象として指定します。<br>対象となるネットワークを直接指定する場合、［デフォルトルート］のチェックを外し、ネットワークアドレスを入力してください。 |
| インターフェース VLAN | VLAN インターフェースの VLAN ID を 1～4094 の範囲で入力します。 |
| IPv6 ネクストホップ | ［IPv6 アドレス/プレフィックス長］で指定したネットワークを宛先とするパケットを転送する IPv6 アドレスを指定します。 |
| 経路順位 | 経路順位（プライマリー／バックアップ）を選択します。<br>ルートの宛先 IPv6 アドレスには、プライマリーとバックアップの IPv6 ネクストホップアドレスを 1 つずつ指定できます。<br>途中経路で障害が発生したなど、スイッチがプライマリールートへの疎通が取れないことを検知した場合、バックアップルートにパケットを転送します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、ルートエントリーが作成されます。 |

| ルートテーブル | |
|---|---|
| IPv6 アドレス | ルートエントリーの IPv6 アドレス／プレフィックス長が表示されます。 |
| ネクストホップ | ルートエントリーの IPv6 ネクストホップアドレスが表示されます。 |
| インターフェース | VLAN インターフェース名が表示されます。 |
| プロトコル | プロトコルの種類が表示されます。<br>・ C：コネクティッドルート<br>・ S：スタティックルート<br>・ -：選択されたルート<br>・ *：有効なルート |
| アクション | ［削除］ボタンをクリックすると、ルートエントリーが削除されます。 |

# 5.3. DNS

本スイッチでは、利用する DNS サーバーを設定できます。SNTP サーバーをドメイン名で指定するなど、使用する機能によって名前解決が必要となる場合は、DNS サーバーを指定してください。

Note: DNS サーバーのアドレスは DHCP クライアント機能の自動取得の対象になりません。




| DNS サーバー設定 | |
|---|---|
| DNS サーバー | IPv4 の DNS サーバーアドレスを入力します。 |
| DNS サーバー(IPv6) | IPv6 の DNS サーバーアドレスを入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 5.4. IP アクセス制限

［IP アクセス制限］ページで、スイッチ管理画面へのアクセスを IP アドレス単位で制限することができます。IP アクセス制限機能が有効になると、登録された許可 IP アドレス以外のデバイスからの管理画面へのアクセスが許可されなくなります。

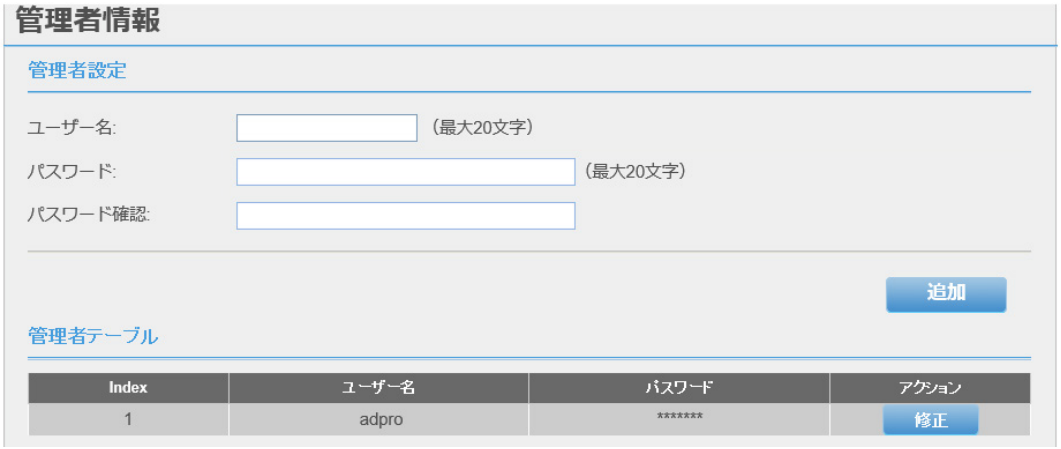

| IP アクセス制限 | |
|---|---|
| IP アクセス制限機能 | IP アクセス制限の状態（有効／無効）を選択します。（デフォルト：無効）<br>IP アクセス制限を使用すると、登録されたアクセス許可 IP アドレス以外からのスイッチ管理画面へのアクセスができなくなります。有効にする場合は、事前に少なくとも 1 つのアクセス許可 IP アドレスが登録されている必要があります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| アクセス許可 IP アドレス | |
|---|---|
| IP アドレス | スイッチ管理画面へのアクセスを設定できる IP アドレスを追加できます。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、IP アドレスが追加されます。 |

| IP アクセス制限リスト | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全 IP アドレスが削除されます。IP アクセス制限が有効の場合、使用できません。 |
| Index | 追加した IP アドレスのインデックス番号が表示されます。 |
| アクセス許可 IP アドレス | 追加した IP アドレスが表示されます。 |
| アクション | ［削除］ボタンをクリックすると、エントリーが削除されます。 |

# 5.5. 管理者設定

［管理者設定］ページで、パスワードの変更や、スイッチ管理画面へアクセスするアカウントの追加を行うことができます。
管理者アカウントのデフォルトユーザー名は「adpro」です。

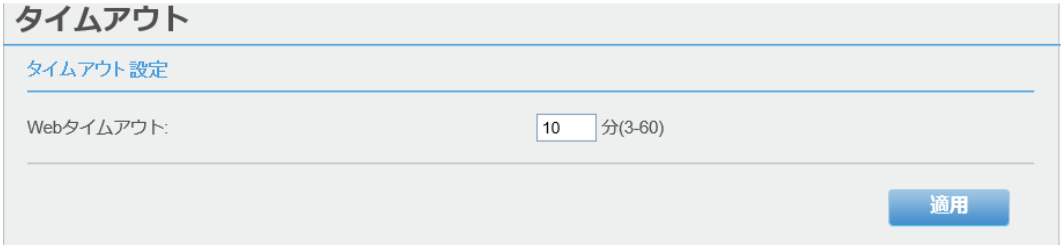



| 管理者情報 | |
|---|---|
| ユーザー名 | 新規アカウントのユーザー名を 20 文字以内の英数字で入力します。 |
| パスワード | 新規アカウントのパスワードを 20 文字以内の英数字で入力します。 |
| パスワード確認 | 確認のため、パスワードを再入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、新規アカウントが作成されます。 |

| 管理者テーブル | |
|---|---|
| Index | アカウントのインデックス番号が表示されます。<br>ユーザーアカウントは最大 8 個まで追加できます。 |
| ユーザー名 | 追加したアカウントの名前が表示されます。 |
| アクション | ［修正］ボタンをクリックすると、アカウントのパスワードを変更できます。<br>［削除］ボタンをクリックすると、アカウントが削除されます。<br>Note: インデックス番号 1 の「adpro」は、デフォルトユーザーのため削除できません。パスワードは変更できます。 |

# 5.6. タイムアウト設定

［タイムアウト設定］ページで、スイッチ管理画面からのタイムアウト設定を変更できます。




| タイムアウト設定 | |
|---|---|
| Web タイムアウト | スイッチ管理画面からタイムアウトするまでの時間を 3～60（分）の範囲で入力します。（デフォルト：10 分）<br>何らかの操作をせずに Web タイムアウト時間を経過すると、スイッチ管理画面とのセッションが自動的に切断され、再ログインが必要になります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 5.7. 時刻設定

［時刻設定］ページで、スイッチのシステム時刻を設定します。
システム時刻は手動で設定するか、Simple Network Time Protocol（以後、SNTP）を用いてサーバーから時刻情報を参照します。SNTP を使用した場合、定期的にサーバーから時刻情報を取得し、必要に応じて時間を補正します。
また、サマータイムを設定することもできます。


| 時刻 | |
|---|---|
| 時刻モード | システムの時刻モード（ローカル／SNTP）が表示されます。 |
| 時刻 | システムの現在時刻が表示されます。 |
| タイムゾーン | システムのタイムゾーンが表示されます。 |

| 時刻設定 | |
|---|---|
| 時刻モード | スイッチの時刻モードを選択します。<br>• ローカル：手動で時刻を設定します。<br>• SNTP：SNTP サーバーから自動的に時刻を取得します。 |

時刻モードで［ローカル］を選択した場合は、［ローカル時刻設定］を設定します。

| ローカル時刻設定 | |
|---|---|
| 日付 | スイッチの日付（年月日）を設定します。 |
| 時刻 | スイッチの時刻（時分秒）を設定します。 |

時刻モードで［SNTP］を選択した場合は、［SNTP 設定］を設定します。

| SNTP 設定 | |
|---|---|
| SNTP プライマリーサーバー | SNTP プライマリーサーバーを IPv4 アドレス、IPv6 アドレス、またはドメイン名で設定します。<br>Note: 時刻設定で［SNTP］を選択した場合は、必ず入力してください。 |
| SNTP セカンダリーサーバー | SNTP セカンダリーサーバーを IPv4 アドレス、IPv6 アドレス、またはドメイン名で設定します。 |
| SNTP 更新間隔 | SNTP サーバーと同期して時刻を更新する間隔を 1～60（分）の範囲で入力します。（デフォルト：1 分） |
| タイムゾーン | 適用するタイムゾーンを選択します。 |

タイムゾーンで選択した地域がサマータイムを採用している場合、［サマータイム設定］を設定します。

| サマータイム設定 | |
|---|---|
| サマータイム設定 | サマータイム設定の状態（有効／無効）を選択します。 |
| 開始日時 | サマータイムの開始日時を設定します。 |
| 終了日時 | サマータイムの終了日時を設定します。 |
| オフセット | サマータイム実施時に、通常の時刻から早める時間を設定します。 |

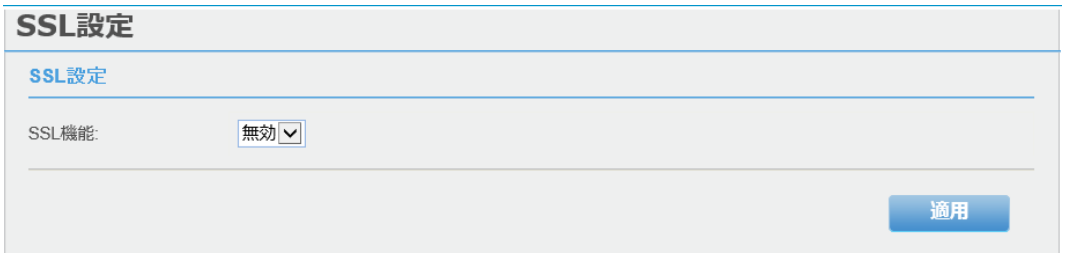
［適用］ボタンをクリックすると、変更が適用されます。

# 5.8. SSL

［SSL］ページでは、SSL 機能の設定を行います。
SSL 機能は通信を暗号化するための機能ですが、本スイッチでは管理画面のアクセスに対してのみ適用されます。SSL 機能が無効の場合には HTTP を、有効の場合には HTTPS を使用して管理画面にアクセスすることができます。初期状態では SSL 機能は無効です。

なお、本設定を変更した場合、使用するプロトコルの変更により管理画面へのセッションが切断されるため、プロトコルを変更して再度ログインする必要があります。

Note: 本スイッチの SSL 機能は TLS1.0 に対応し、証明書はプレインストールされた自己署名証明書を使用します。SSL 機能を有効にした場合、使用する Web ブラウザーの種類やバージョン、設定によっては、警告メッセージが表示されることや、管理画面にアクセスできないことがありますのでご注意ください。



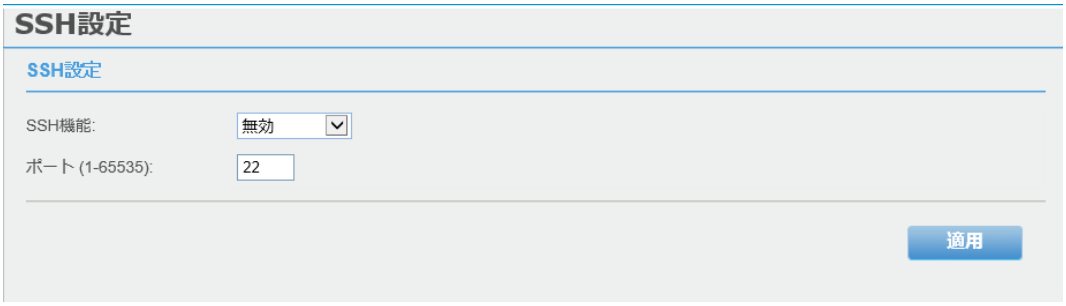

| SSL 設定 | |
|---|---|
| SSL 機能 | SSL 機能の状態（有効／無効）を選択します。（デフォルト：無効） |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 5.9. SSH

［SSH］ページでは、スイッチに対する SSH でのアクセス許可の設定を行います。
SSH はネットワーク経由でリモートホストと通信するためのプロトコルです。スイッチとホスト間で通信の暗号化を行います。

Note: SSH により提供されるセキュリティー強度は SSH のバージョンのほか、スイッチとホストがサポートする暗号化、鍵交換、メッセージ認証符号などでそれぞれ使用されるアルゴリズムによって異なります。使用するアルゴリズムはスイッチとホストの両方で対応する必要がありますので、ホストのターミナルソフトの種類やバージョン、設定によってはスイッチとの間に SSH 接続が確立できない場合があります。

Note: SSH 機能で提供するインターフェースは、たとえばネットワーク障害発生時の情報収集など、緊急時の対応用の内容であり、WEB ブラウザー用のインターフェースと同等の機能は備えていません。通常は無効にしてご使用ください。

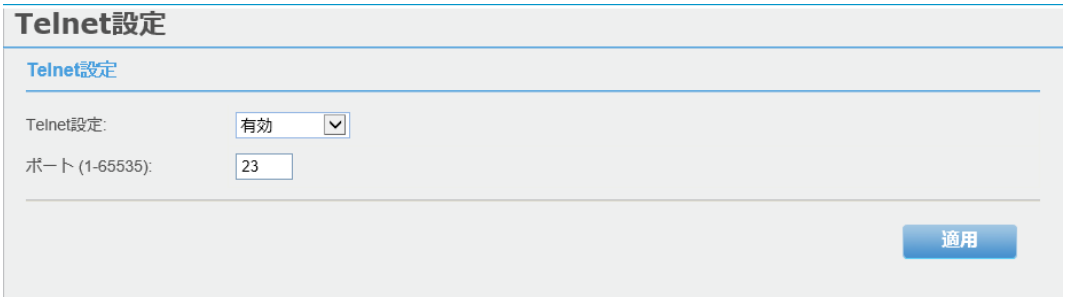



| SSH 設定 | |
|---|---|
| SSH 機能 | SSH 機能の状態（有効／無効）を選択します。（デフォルト：無効） |
| ポート（1-65535） | SSH 機能のサービスポートを 1～65535 の範囲で入力します。（デフォルト：22） |

# 5.10. Telnet

［Telnet］ページでは、スイッチに対する Telnet でのアクセス許可の設定を行います。
Telnet はネットワーク経由でリモートホストと通信するためのプロトコルです。スイッチとホスト間の通信は暗号化されず、パスワードを含め平文で送信します。

Note: Telnet 機能で提供するインターフェースは、たとえばネットワーク障害発生時の情報収集など、緊急時の対応用の内容であり、WEB ブラウザー用のインターフェースと同等の機能は備えていません。通常は無効にしてご使用ください。

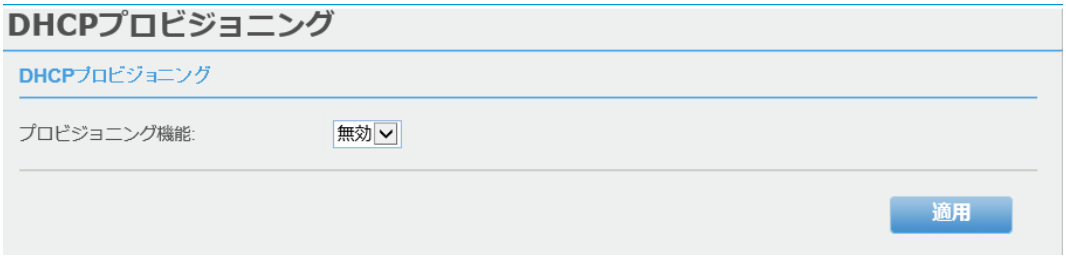



| Telnet 設定 | |
|---|---|
| Telnet 設定 | Telnet 設定の状態（有効／無効）を選択します。（デフォルト：無効） |
| ポート（1-65535） | Telnet のサービスポートを 1～65535 の範囲で入力します。（デフォルト：23） |

# 5.11. DHCP プロビジョニング

［DHCP プロビジョニング］ページでは、スイッチの DHCP 自動設定機能の設定を行います。
DHCP 自動設定機能を有効にすると、スイッチは DHCP クライアントとして動作し、Trivial File Transfer Protocol（以後、TFTP）サーバーから自動的に設定ファイルを取得します。

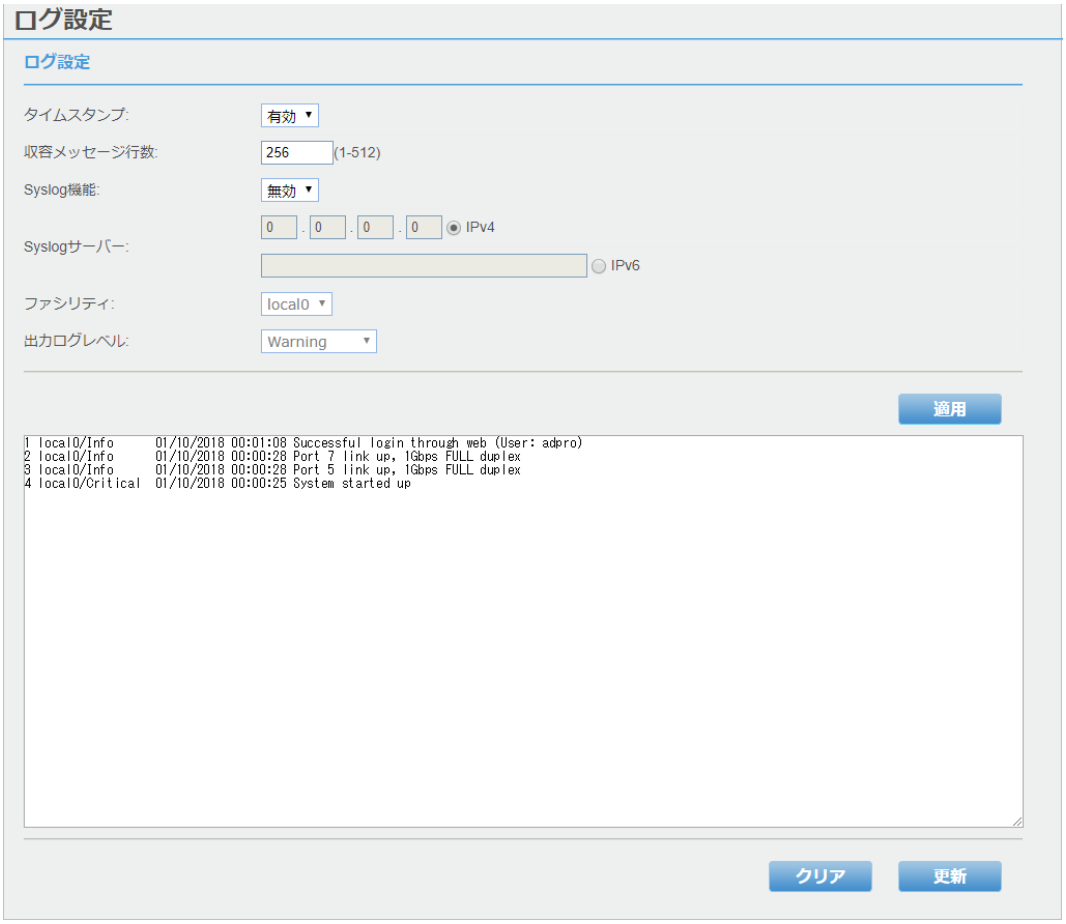
Note: プロビジョニングが有効に動作するためには、DHCP サーバーが TFTP サーバーの IP アドレスと設定ファイル名の情報を DHCP 応答パケットで配信する必要があります。また、TFTP サーバーでは、必要な設定ファイルをベースディレクトリーに格納し、スイッチからの要求に対して適切にファイルを提供する必要があります。




| DHCP プロビジョニング | |
|---|---|
| プロビジョニング機能 | 自動設定機能の状態（有効／無効）を選択します。(デフォルト：無効)<br>有効の場合、DHCP サーバーから IP アドレスを取得し、TFTP サーバーから設定ファイルを取得します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 5.12. ログ設定

［ログ設定］ページでは、システムログの設定やログの確認を行います。
システムログは、スイッチの動作を監視し、エラーなどの各種情報を記録します。システムに問題が発生した際に、解決に役立つ情報が得られることがあります。




| ログ設定 | |
|---|---|
| タイムスタンプ | ログのタイムスタンプの状態（有効／無効）を選択します。（デフォルト：有効） |
| 収容メッセージ行数 | 表示するログの行数を 1～512 の範囲で入力します。（デフォルト：256） |
| Syslog 機能 | リモートログサーバーへのログ送信の状態（有効／無効）を選択します。（デフォルト：無効） |
| Syslog サーバー | ［IPv4］または［IPv6］を選択し、ログ送信する Syslog サーバーの IP アドレスを入力します。 |
| ファシリティ | ログ送信に指定するファシリティ（local0～local7）を選択します。ファシリティ情報は、主に Syslog サーバー側で情報の整理のために使用されます。 |
| 出力ログレベル | ログの出力レベルを選択します。<br>出力レベルによって、送信されるログの内容が設定されます。 |

| | |
|---|---|
| | ・ Alert：緊急度が非常に高いイベント（Alert）のログを出力<br>・ Critical：重大なイベント（Critical 以上）のログを出力<br>・ Warning：警告レベル（Warning 以上）のログを出力<br>・ Info：情報レベル（Informational 以上）のログを出力 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［クリア］ボタン | ［クリア］ボタンをクリックすると、ログがクリアされます。 |
| ［更新］ボタン | ［更新］ボタンをクリックすると、ログメッセージが更新されます。 |

# 5.13. SNMP

SNMP は、スイッチ上の MIB 情報を使用して、スイッチを管理および監視するネットワーク運用管理プロトコルです。SNMP を使用する場合、管理者は SNMP マネージャーによりスイッチにアクセスします。

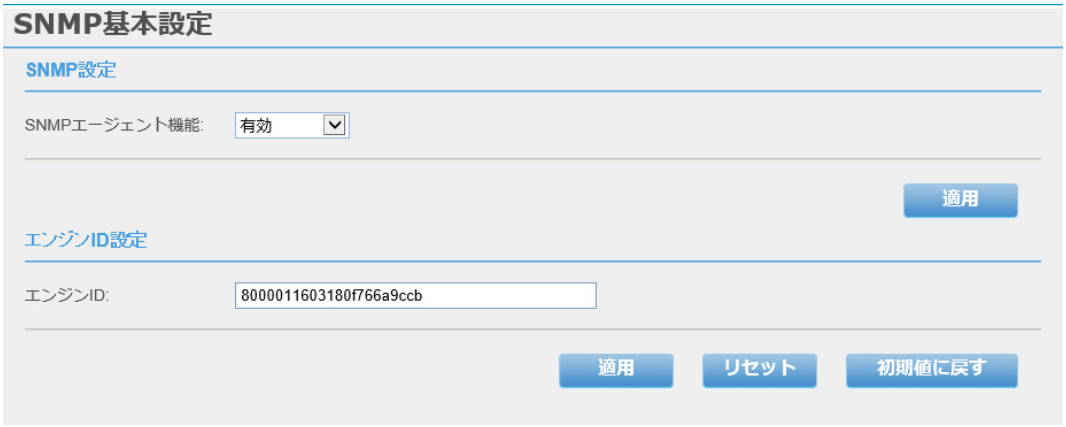
SNMP に対応したスイッチは、Management Information Base（MIB）というデータベースを作成し、機器の情報を収容します。MIB 情報は設定や状態に応じてスイッチが自動的に更新します。
SNMP マネージャーは、MIB 情報のオブジェクト識別子（OID)とインデックスによりアクセスする情報を指定し、読み取りや書き込みの操作を行います。

スイッチの SNMP エージェント機能は、SNMP マネージャーからの装置への MIB 情報のアクセスを制御する機能で、SNMP エージェント機能が無効の場合は MIB 情報へのアクセスを許可しません。
SNMP エージェントは、アクセスする SNMP マネージャーの身元や権限の確認を行い、権限に応じた操作を許可します。与えられる権限には、操作の権限（読み込み専用／読み書き可能）とアクセス範囲の権限の 2 種類があり、アクセス範囲の権限は SNMP ビューを用いて指定します。

Note: 本スイッチでは、サードパーティーの SNMP マネージャーツールによる設定を想定し、デフォルトで SNMP エージェント機能が有効になっています。SNMP 機能のデフォルト設定はアクセス上のリスクがあり、SNMP による管理を行わない場合、SNMP エージェント機能を無効にすることを推奨します。

## 5.13.1. 基本設定

［基本設定］ページでは、SNMP エージェント機能の設定を行うことができます。
SNMP による管理を行わない場合、SNMP エージェント機能を無効にすることを推奨します。




| SNMP 設定 | |
|---|---|
| SNMP エージェント機能 | SNMP エージェント機能の状態（有効／無効）を選択します。(デフォルト：有効) |
| ［適用］ボタン | ［適用］ボタンをクリックすると、SNMP エージェント機能の状態の変更が適用されます。 |

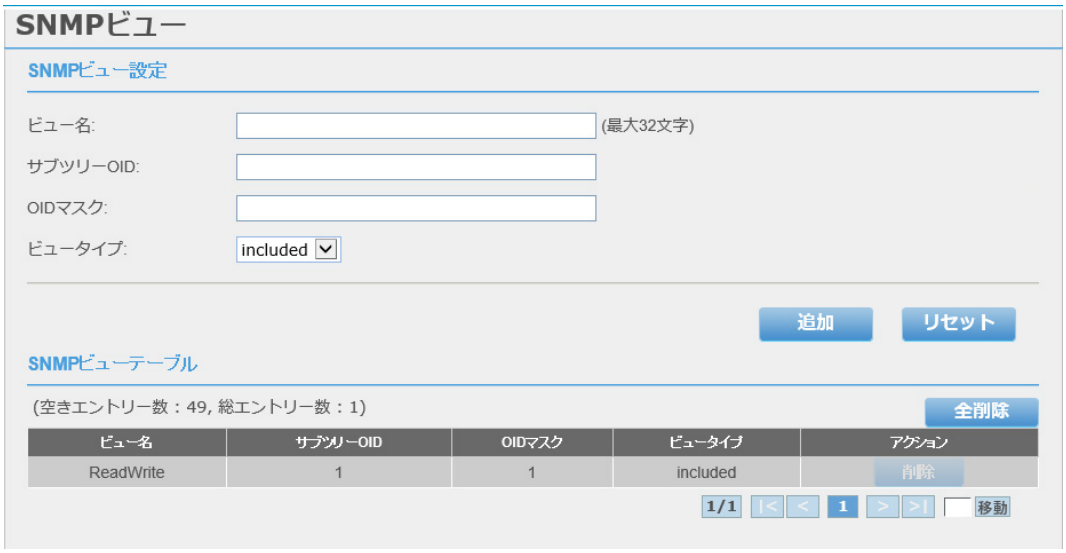
| エンジン ID 設定 | |
|---|---|
| エンジン ID | SNMP のエンジン ID が表示されます。<br>SNMP のエンジン ID は、スイッチで SNMPv3 エンジンを識別するための一意の識別子です。エンタープライズ ID と MAC アドレスから構成された 10～64 文字の範囲の 16 進数の文字列です。<br>デフォルトでは、RFC3411 標準に従っています。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、エンジン ID の変更が適用されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |
| ［初期値に戻す］ボタン | ［初期値に戻す］ボタンをクリックすると、初期値に戻ります。 |

## 5.13.2. ビュー

SNMP ビューは、SNMP マネージャーの各操作に対するアクセス範囲を指定した OID のリストです。
SNMP マネージャーからのアクセスは、［グループ］で登録するユーザーグループ単位で権限が定められます。読み込み、書き込みなどの各操作に対して SNMP ビューが指定された場合、該当するグループのユーザーはその操作に対して指定された OID の範囲でアクセスが可能になります。

MIB の管理項目（オブジェクト）はツリー状の階層構造で定義されており、上位オブジェクトは一個以上の下位オブジェクトを収容してサブツリーを構成します。オブジェクトの識別子である OID は複数の整数をピリオド（.）で区切った値で定義されますが、そのオブジェクトのツリー構造での位置も示し、例えば 1.3.6.1.2.1.2.2.1（ifEntry）は、1.3.6.1.2.1.2.2.1.1（ifIndex）や 1.3.6.1.2.1.2.2.1.8（ifOperStatus）の上位に該当します。

［ビュー］では、登録された SNMP ビューに対して OID とマスクを指定し、特定のオブジェクトに対するアクセス許可／除外のルールを作成します。ルールは下位オブジェクトに対しても適用されますが、別のルールが存在する場合はそれが優先されます。



| SNMP ビュー設定 | |
|---|---|
| ビュー名 | ビュー名を 32 文字以内の英数字で入力します。<br>ビュー名は、［SNMP］＞［グループ］ページで事前に作成しておく必要があります。 |
| サブツリーOID | SNMP ビューによるアクセス範囲の対象となる OID を 16 文字以内で「x.x.x.x.x」(x は数字)などの形式で入力します。<br>（「.」は文字数に含めません） |
| OID マスク | サブツリーOID のマスクを 16 文字以内で「x.x.x.x.x」(x は 0 もしくは 1)などの形式で入力します。<br>（「.」は文字数に含めません）<br>・ 1：該当する数字を一致条件で適用する<br>・ 0：該当する数字は一致条件で適用しない（ワイルドカード） |
| ビュータイプ | 指定した OID に対する操作権限（ビュータイプ）を選択します。<br>・ included：指定した OID をアクセス許可対象に含める<br>・ excluded：指定した OID をアクセス許可対象から除外する |
| ［追加］ボタン | ［追加］ボタンをクリックすると、SNMP ビューが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

入力例）

- ビュー名：ReadWrite
- サブツリーOID：1.3.6.1.2.1.11
- OID マスク：1.1.1.1.1.1.1
- ビュータイプ：excluded

上記の場合、ReadWrite ビューに対して OID が 1.3.6.1.2.1.11 のオブジェクト（snmp）をアクセス対象から除外するルールを定義します。このルールでは、例えば「SNMP マネージャーから SET（書き込み）要求を受信した回数を示す OID」（snmpInSetRequests:1.3.6.1.2.1.11.17）に対するアクセスは許可されません。

| SNMP ビューテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全エントリーが削除されます。<br>「ReadWrite」ビューのデフォルトエントリーは削除できません。 |
| ビュー名 | SNMP ビュー名が表示されます。デフォルトで「ReadWrite」ビューのデフォルトエントリーが登録されています。 |
| サブツリーOID | エントリーのサブツリーOID が表示されます。 |
| OID マスク | エントリーの OID マスクが表示されます。 |
| ビュータイプ | エントリーのビュータイプ（included／excluded）が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、エントリーが削除されます。<br>「ReadWrite」ビューのデフォルトエントリーは削除できません。 |

## 5.13.3. グループ

［グループ］ページでは、ユーザーグループに対して適用する SNMP ビューを指定します。
特定の操作に対して SNMP ビューが指定されていない場合、そのユーザーグループに所属するユーザーは該当する操作の権限が与えられません。

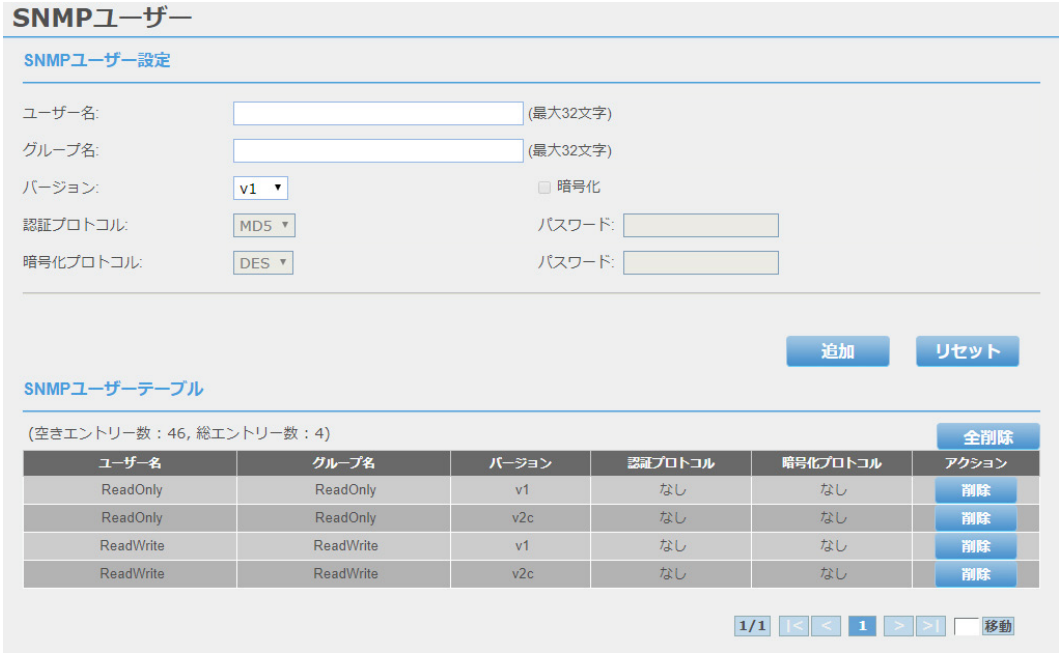

| SNMP グループアクセス設定 | |
|---|---|
| グループ名 | SNMP グループ名を 32 文字以内で入力します。<br>グループは、［SNMP］＞［ユーザー］ページで作成しておく必要があります。 |
| 読み出しビュー | グループに所属するユーザーの読み取りアクセス対象の SNMP ビューを 32 文字以内で指定します。未登録の SNMP ビューを指定した場合には新規にビューが作成されます。 |
| 書き込みビュー | グループに所属するユーザーの書き込みアクセス対象の SNMP ビュー名を 32 文字以内で指定します。未登録の SNMP ビューを指定した場合には新規にビューが作成されます。 |
| 受信ビュー | グループに所属するユーザーに通知する対象の SNMP ビュー名を 32 文字以内で指定します。未登録の SNMP ビューを指定した場合には新規にビューが作成されます。 |
| バージョン | 適用する SNMP グループの SNMP バージョンを選択します。 |
| セキュリティレベル | バージョンで［v3］を選択した場合のみ、セキュリティーレベルを選択します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、エントリーが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

| SNMP グループアクセステーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全エントリーが削除されます。<br>デフォルトエントリーは削除されません。 |
| グループ名 | SNMP グループ名が表示されます。<br>デフォルトで「ReadOnly」「ReadWrite」ユーザーグループについてのデフォルトエントリーが登録されています。 |
| 読み出しビュー | エントリーの読み出しビュー名が表示されます。 |
| 書き込みビュー | エントリーの書き込みビュー名が表示されます。 |
| 受信ビュー | エントリーの受信ビュー名が表示されます。 |
| バージョン | エントリーの SNMP のバージョンが表示されます。 |
| セキュリティレベル | エントリーのセキュリティーレベルが表示されます。 |
| アクション | ［削除］ボタンをクリックすると、エントリーが削除されます。<br>デフォルトエントリーは削除できません。<br>Note: エントリーを変更する場合は、エントリーを削除してから、もう一度入力してください。 |

## 5.13.4. ユーザー

［ユーザー］ページでは、SNMP マネージャーでアクセスするユーザー名と所属グループを登録します。SNMPv1 および v2c では、[コミュニティー]で設定する SNMP コミュニティー名でユーザーを識別し、SNMP マネージャーは SNMP コミュニティー名を宣言してスイッチにアクセスを行います。この時、SNMP マネージャーでは登録されたユーザー名を意識する必要はありません。

SNMPv3 では、SNMP マネージャーは登録されたユーザー名を直接指定してスイッチの操作を行います。



| SNMP ユーザー設定 | |
|---|---|
| ユーザー名 | SNMP ユーザー名を 32 文字以内で入力します。 |
| グループ名 | SNMP ユーザーの所属グループ名を 32 文字以内で入力します。<br>未登録のグループ名を指定した場合には新規にグループが作成されます。 |
| バージョン | SNMP のバージョン（v1／v2c／v3）を選択します。<br>［v3］を選択すると、［暗号化］のチェックボックスが選択可能になります。 |
| 認証プロトコル | バージョンで［v3］を選択して、［暗号化］をオンにした場合に、認証プロトコルを選択します。 |
| 暗号化プロトコル | バージョンで［v3］を選択して、［暗号化］をオンにした場合に、暗号化プロトコルを選択します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、ユーザーが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

| SNMP ユーザーテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、作成したすべてのユーザーエントリーが削除されます。<br>デフォルトエントリーは削除されません。 |
| ユーザー名 | SNMP ユーザー名が表示されます。 |
| グループ名 | SNMP ユーザーのグループ名が表示されます。 |
| バージョン | エントリーの SNMP のバージョンが表示されます。 |
| 認証プロトコル | エントリーの認証プロトコルが表示されます。 |
| 暗号化プロトコル | エントリーの暗号化プロトコルが表示されます。 |
| アクション | ［削除］ボタンをクリックすると、エントリーが削除されます。<br>デフォルトエントリーは削除できません。<br>Note: エントリーを変更する場合は、エントリーを削除してから、もう一度入力してください。 |

## 5.13.5. コミュニティー

［コミュニティー］ページでは、SNMPv1 および v2c で用いられる SNMP コミュニティー名を指定します。スイッチは、SNMP マネージャーが指定した SNMP コミュニティー名を元にユーザーを識別し、許可された権限に応じて処理を行います。
なお、SNMPv3 では SNMP コミュニティー名を使用しません。

Note: 本スイッチでは、デフォルトで「private」「public」という SNMP コミュニティー名が登録され、それぞれ「ReadWrite」「ReadOnly」というデフォルトユーザー名に紐づいています。これらのユーザーは、すべての OID に対するアクセス権限を持つため、運用管理上のセキュリティーリスクがあり

ます。SNMP による運用管理を行う場合は、SNMP コミュニティーのデフォルトエントリーを削除することを推奨します。


| SNMP コミュニティー設定 | |
|---|---|
| コミュニティー名 | SNMP コミュニティー名を 32 文字以内の英数字で入力します。(「"」は入力不可)<br>コミュニティー名は最大 10 個まで設定できます。 |
| ユーザー名 | SNMP ユーザー名を 32 文字以内で入力します。<br>ユーザー名は、[SNMP] > [ユーザー] ページで事前に作成しておく必要があります。 |
| [追加] ボタン | [追加] ボタンをクリックすると、コミュニティーが追加されます。 |
| [リセット] ボタン | [リセット] ボタンをクリックすると、入力がリセットされます。 |

| SNMP コミュニティーテーブル | |
|---|---|
| [全削除] ボタン | [全削除] ボタンをクリックすると、すべての SNMP コミュニティーエントリーが削除されます。 |
| コミュニティー名 | エントリーの SNMP コミュニティー名が表示されます。 |
| ユーザー名 | エントリーの SNMP ユーザー名が表示されます。 |
| アクション | [削除] ボタンをクリックすると、SNMP コミュニティーエントリーが削除されます。 |

## 5.13.6. トラップ

[トラップ] ページで、SNMP トラップ機能の設定を行います。
SNMP トラップ機能は、スイッチで何らかのイベント（例えばリンクアップやリンクダウンなど）が発生した場合に、SNMP を用いて所定の SNMP マネージャーに通知する機能です。通知するメッセージは MIB に基づき、OID で指定されます。

SNMP トラップ機能による通知を行う場合、SNMP マネージャーのホスト IP アドレスと、SNMP バージョン、使用するコミュニティー名もしくはユーザー名を設定します。


| SNMP トラップ設定 | |
|---|---|
| SNMP トラップ機能 | SNMP トラップ機能の状態（有効／無効）を選択します。（デフォルト：有効） |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| ホスト追加 | |
|---|---|
| ホスト IP アドレス | SNMP マネージャーのホスト IP アドレスを入力します。 |
| バージョン | SNMP のバージョンとセキュリティーレベル（v1／v2c／v3-ユーザー名のみ／v3-認証のみ／v3-認証及び暗号化）を選択します。 |
| コミュニティ名/ユーザー名 | コミュニティー名／ユーザー名を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、送信先ホストが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

| SNMP トラップホストテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全エントリーが削除されます。 |
| ホスト IP アドレス | ホスト IP アドレスが表示されます。 |
| バージョン | SNMP のバージョンやセキュリティーレベルが表示されます。 |
| コミュニティ名/ユーザー名 | コミュニティー名／ユーザー名が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、エントリーが削除されます。<br>Note: エントリーを変更する場合は、エントリーを削除してから、もう一度入力してください。 |

# 5.14. RMON

Remote network MONitoring（以後、RMON）は、SNMP の機能を利用して、ネットワークの監視とプロトコル解析をサポートします。

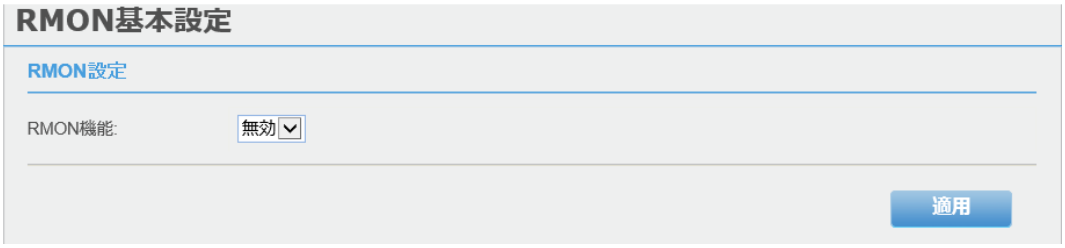
従来の SNMP を用いたネットワーク管理では、例えばスイッチの設定情報のような比較的変化の少ない情報やインシデントの管理などには適していますが、トラフィック量の経時的変化のようなダイナミックな情報に対するモニタリング、イベント発行（ログの通知など）にはあまり適していません。
RMON では、ネットワーク機器のトラフィック情報を収集するための RMON MIB が定義されており、トラフィックに関する様々な情報を集積し、ネットワーク管理に役立てることができます。

本スイッチの RMON 機能は、RMON MIB の「統計情報」「履歴管理」「アラーム」「イベント」グループに対応します。RMON 機能で収集する情報は各グループに対して登録したエントリー単位で識別・管理され、インデックスに対応した OID にアクセスすることで、収集した情報を SNMP マネージャーで取得することができます。また、トラフィック量の変動など、特定のネットワーク環境の変化に対して「アラーム」を登録して、「イベント」で設定したアクション（例えば SNMP トラップによる通知）を発生させることもできます。

Note: RMON 機能を使用する場合は、SNMP エージェント機能を有効にする必要があります。

## 5.14.1. 基本設定

［基本設定］ページでは、RMON 機能の設定を行います。




| RMON 設定 | |
|---|---|
| RMON 機能 | RMON 機能の状態（有効／無効）を選択します。（デフォルト：無効）<br>Note: RMON 機能を使用する場合は、SNMP エージェント機能を有効にする必要があります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 5.14.2. 統計情報

［統計情報］ページでは、RMON 統計情報グループの設定を行います。
RMON 統計情報グループは、監視対象のポートを指定し、パケット数やエラー数などの基本情報を収集します。


| 統計情報設定 | |
|---|---|
| Index | 統計情報インデックスを 1～65535 の範囲で入力します。 |
| ポート | RMON 統計情報を取得するポート番号を入力します。 |
| オーナー | オーナー情報を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、RMON 統計情報グループのエントリーが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

| 統計情報テーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、すべての RMON 統計情報グループのエントリーが削除されます。 |
| Index | エントリーのインデックスが表示されます。 |
| ポート | 対象となるポート番号が表示されます。 |
| ドロップイベント数 | 対象ポートのドロップイベント数が表示されます。 |
| オクテット数 | 対象ポートのオクテット数が表示されます。 |
| パケット数 | 対象ポートのパケット数が表示されます。 |
| ブロードキャストパケット数 | 対象ポートのブロードキャストパケット数が表示されます。 |
| マルチキャストパケット数 | 対象ポートのマルチキャストパケット数が表示されます。 |
| オーナー | オーナー情報が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、対象の RMON 統計情報グループのエントリーが削除されます。 |

## 5.14.3. 履歴

［履歴］ページでは、RMON 履歴管理グループの設定を行います。
RMON 履歴管理グループは、指定したポートの統計情報を一定のサンプリング間隔で取得したスナップショットを収集します。RMON 統計情報グループと比べて小さい負荷で管理を行うことができます。


| 履歴管理設定 | |
|---|---|
| Index | 履歴管理インデックスを 1～65535 の範囲で入力します。 |
| ポート | 履歴を取得するポート番号を入力します。 |
| 収集エントリー数 | スナップショットを保存する数を 1～50 の範囲で入力します。<br>バケットごとに RMON 統計情報のスナップショットを 1 つ保存できます。（エントリーによって、バケット数を変更できます） |
| 間隔 | スナップショットの取得間隔を 1～3600（秒）の範囲で入力します。 |
| オーナー | オーナーの情報を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、エントリーが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

| 履歴管理テーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、すべての RMON 履歴管理グループのエントリーが削除されます。 |
| Index | エントリーのインデックスが表示されます。 |
| ポート | エントリーの対象となるポート番号が表示されます。 |
| 収集エントリー数 | スナップショットを要求したバケット数が表示されます。 |
| 保存エントリー数 | スナップショットを保存したバケット数が表示されます。 |
| サンプリング間隔 | スナップショットを取得する間隔が表示されます。 |
| オーナー | オーナーの情報が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、対象の RMON 履歴管理グループのエントリーが削除されます。 |

## 5.14.4. アラーム

［アラーム］ページでは、RMON アラームグループの設定を行います。
RMON アラームグループは、特定の OID の MIB 情報をチェックし、登録したしきい値を超えた場合に、RMON イベントグループで設定したアクションを発生させます。


| アラーム設定 | |
|---|---|
| Index | アラームインデックスを 1～65535 の範囲で入力します。 |
| サンプリング間隔 | サンプリング間隔を 1～2147483647（秒）の範囲で入力します。 |
| モニタリング変数 | モニタリングする SNMP 変数の OID を入力します。<br>モニタリング可能な RMON 情報は 1.3.6.1.2.1.2.2.1.x.y の形式で指定する MIB 情報に限定されます。<br>変数 x は 10～13 もしくは 16～19 のいずれかの値を指定します。<br>10：対象ポートで受信した総オクテット数<br>11：対象ポートで受信したユニキャストパケット数<br>12：対象ポートで受信した非ユニキャストパケット数<br>13：対象ポートで受信時に破棄したパケット数<br>16：対象ポートから送信した総オクテット数<br>17：対象ポートから送信したユニキャストパケット数<br>18：対象ポートから送信した非ユニキャストパケット数<br>19：対象ポートで送信時に破棄したパケット数<br>変数 y はポート番号を指定します。 |
| モニタリング方式 | モニタリング方式を選択します。（デフォルト：絶対値）<br>・ 差分値：RMON 統計情報の前回値からの差分<br>・ 絶対値：RMON 統計情報の現在値 |

| | |
|---|---|
| 上昇閾値 | 上昇しきい値を 1～2147483647（秒）の範囲で入力します。<br>上昇しきい値を超えた場合にアラームイベントが発動します。 |
| 下降閾値 | 下降しきい値を 1～2147483647（秒）の範囲で入力します。<br>下降しきい値を下回った場合にアラームイベントが発動します。<br>Note: 下降しきい値は上昇しきい値よりも小さい値を設定する必要があります。 |
| 上昇イベント Index | 上昇しきい値を超えた場合に発生させるイベントのインデックスを入力します。<br>RMON アラームエントリーを追加する前に、[イベント] ページで対応するインデックスのイベントを登録しておく必要があります。 |
| 下降イベント Index | 下降しきい値を下回った場合に発生させるイベントのインデックスを入力します。<br>RMON アラームエントリーを追加する前に、[イベント] ページで対応するインデックスのイベントを登録しておく必要があります。 |
| オーナー | オーナーの情報を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、アラームが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

| **アラームテーブル** | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全アラームエントリーが削除されます。 |
| Index | インデックスが表示されます。 |
| サンプリング間隔 | サンプリング間隔が表示されます |
| モニタリング変数 | モニタリングする SNMP 変数の OID が表示されます |
| モニタリング方式 | モニタリング方式（差分値／絶対値）が表示されます。 |
| 上昇閾値 | 上昇しきい値が表示されます |
| 下降閾値 | 下降しきい値が表示されます |
| 上昇イベント Index | 上昇しきい値を超えた場合に発生させるイベントのインデックスが表示されます |
| 下降イベント Index | 下降しきい値を下回った場合に発生させるイベントのインデックスが表示されます |
| オーナー | オーナーの情報が表示されます |
| アクション | ［削除］ボタンをクリックすると、アラームエントリーが削除されます。 |

## 5.14.5. イベント

［イベント］ページでは、RMON イベントグループの設定を行います。
RMON イベントグループは、RMON アラームグループで登録された条件を満たした場合に発生するアクションを管理します。


| イベント設定 | |
|---|---|
| Index | イベントインデックスを 1～65535 の範囲で入力します。 |
| 説明 | イベントの説明を 32 文字以内で入力します。 |
| タイプ | イベントが発動したときのイベントタイプを選択します。<br>イベントログへの記録や SNMP マネージャーへの SNMP トラップによる通知、あるいは両方を行うように設定することができます。 |
| コミュニティー名 | SNMP トラップ通知を伴う場合、コミュニティー名を入力します。 |
| オーナー | オーナーの情報を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、イベントが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |

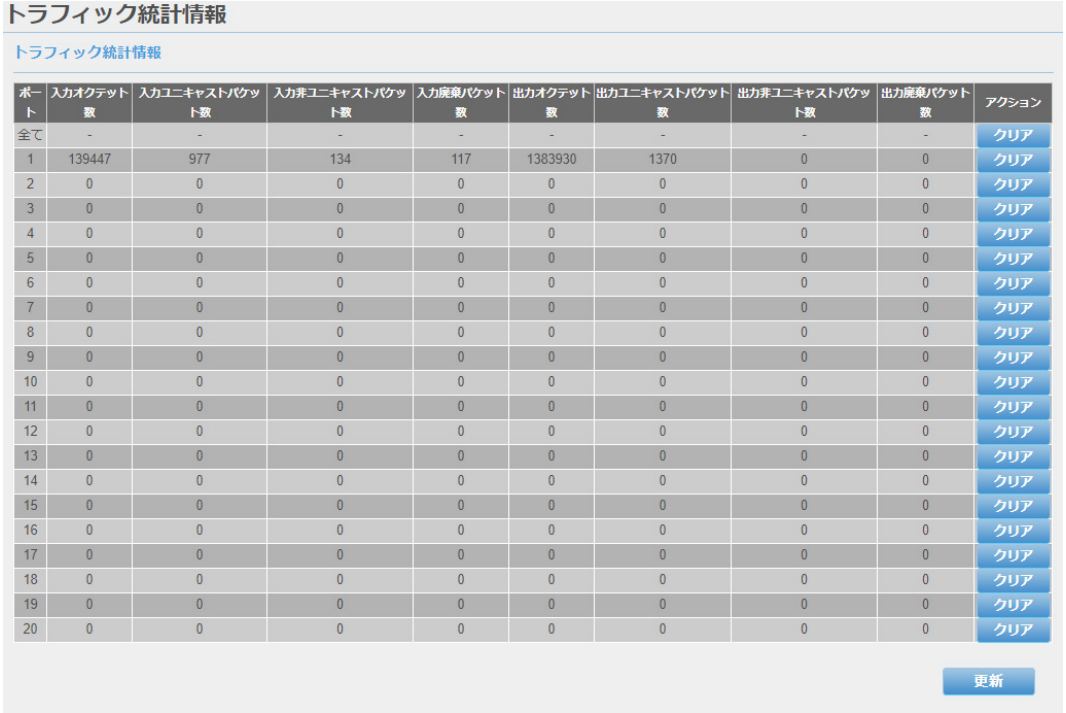
| イベントテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全エントリーが削除されます。 |
| Index | インデックスが表示されます。 |
| 説明 | イベントの説明が表示されます。 |
| タイプ | イベントタイプが表示されます。 |
| コミュニティー名 | SNMP トラップ通知で適用するコミュニティー名が表示されます。 |
| オーナー | オーナーの情報が表示されます。 |
| 最終発生時間 | 最後に実行されたイベントの日付と時刻が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、エントリーが削除されます。 |

# 5.15. 統計情報

スイッチの統計情報では、ポート単位でのトラフィック情報とエラー情報を確認できます。
ネットワークに問題がある場合などに、統計情報を確認して、トラブルシューティングに役立てることができます。

## 5.15.1. トラフィック

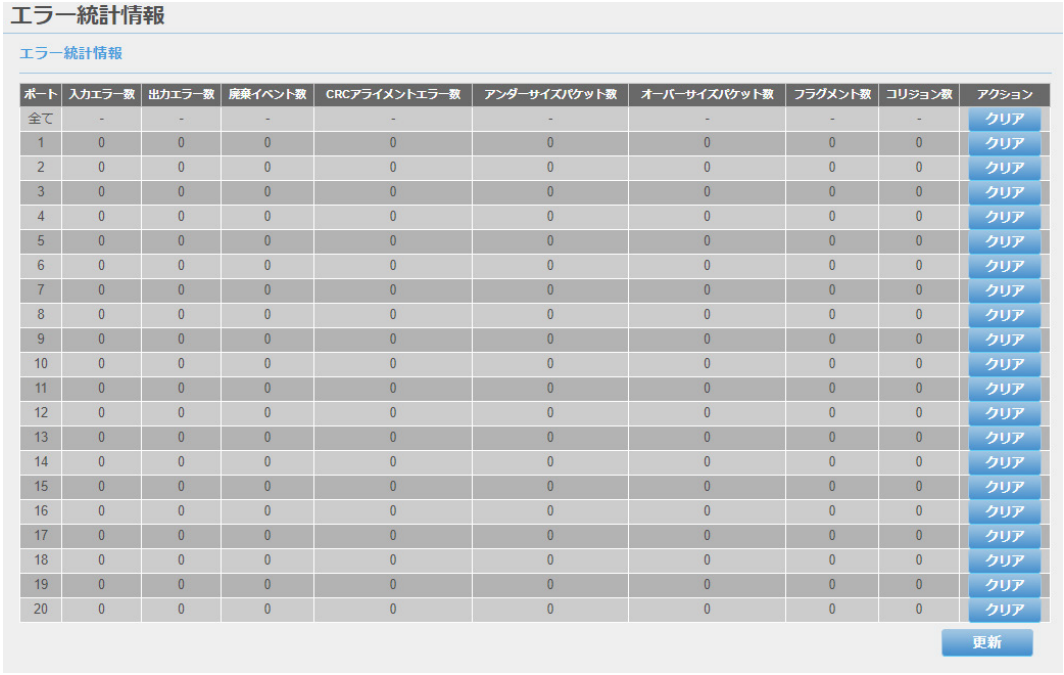
［トラフィック］ページでは、スイッチで正常に処理されたトラフィック情報を表示します。




| トラフィック統計情報 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 入力オクテット数 | ポートの入力オクテット数が表示されます。 |
| 入力ユニキャストパケット数 | ポートの入力ユニキャストパケット数が表示されます。 |
| 入力非ユニキャストパケット数 | ポートの入力非ユニキャストパケット数（ブロードキャストパケット／マルチキャストパケットなど）が表示されます。 |
| 入力廃棄パケット数 | ポートの入力廃棄パケット数が表示されます。 |
| 出力オクテット数 | ポートの出力オクテット数が表示されます。 |
| 出力ユニキャストパケット数 | ポートの出力ユニキャストパケット数が表示されます。 |
| 出力非ユニキャストパケット数 | ポートの出力非ユニキャストパケット数（ブロードキャストパケット／マルチキャストパケットなど）が表示されます。 |
| 出力廃棄パケット数 | ポートの出力廃棄パケット数が表示されます。 |
| アクション | ［クリア］ボタンをクリックすると、カウントがクリアされます。 |
| ［更新］ボタン | ［更新］ボタンをクリックすると、統計情報が更新されます。 |

## 5.15.2. エラー

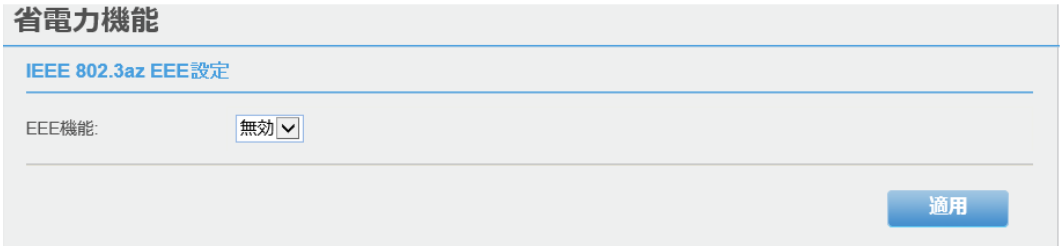
［エラー］ページでは、スイッチでエラーとして処理されたトラフィック情報を表示します。




| エラー統計情報 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 入力エラー数 | 入力エラーのパケット数が表示されます。 |
| 出力エラー数 | 出力エラーのパケット数が表示されます。 |
| 廃棄イベント数 | ドロップされたパケット数が表示されます。 |
| CRC アライメントエラー数 | CRC アライメントエラーのパケット数が表示されます。 |
| アンダーサイズパケット数 | 受信したアンダーサイズ（64 オクテット未満）のパケット数が表示されます。 |
| オーバーサイズパケット数 | 受信したオーバーサイズ（2000 オクテット超）のパケット数が表示されます。 |
| フラグメント数 | 受信したフラグメントパケット数（フレーム指示ビットを除き、FCS オクテットを含め 64 オクテット未満）が表示されます。 |
| コリジョン数 | 受信したコリジョンパケット数が表示されます。<br>ジャンボフレームが有効な場合は、ジャバーフレームのしきい値がジャンボフレームの最大サイズまで引き上げられます。 |
| アクション | ［クリア］ボタンをクリックすると、カウントがクリアされます。 |
| ［更新］ボタン | ［更新］ボタンをクリックすると、統計情報が更新されます。 |

# 5.16. 省電力機能

［省電力機能］ページでは、スイッチの省電力機能の状態を設定します。
省電力機能を有効にすると、ネットワークの使用率の低い期間に、スイッチで使用されるエネルギーを削減し、ネットワーク接続を中断させずに、スイッチを低電力状態にすることができます。
本機能を使用する際には、送信側と受信側ともに、IEEE 802.3az Energy Efficient Ethernet（以後、EEE）に対応している必要があります。

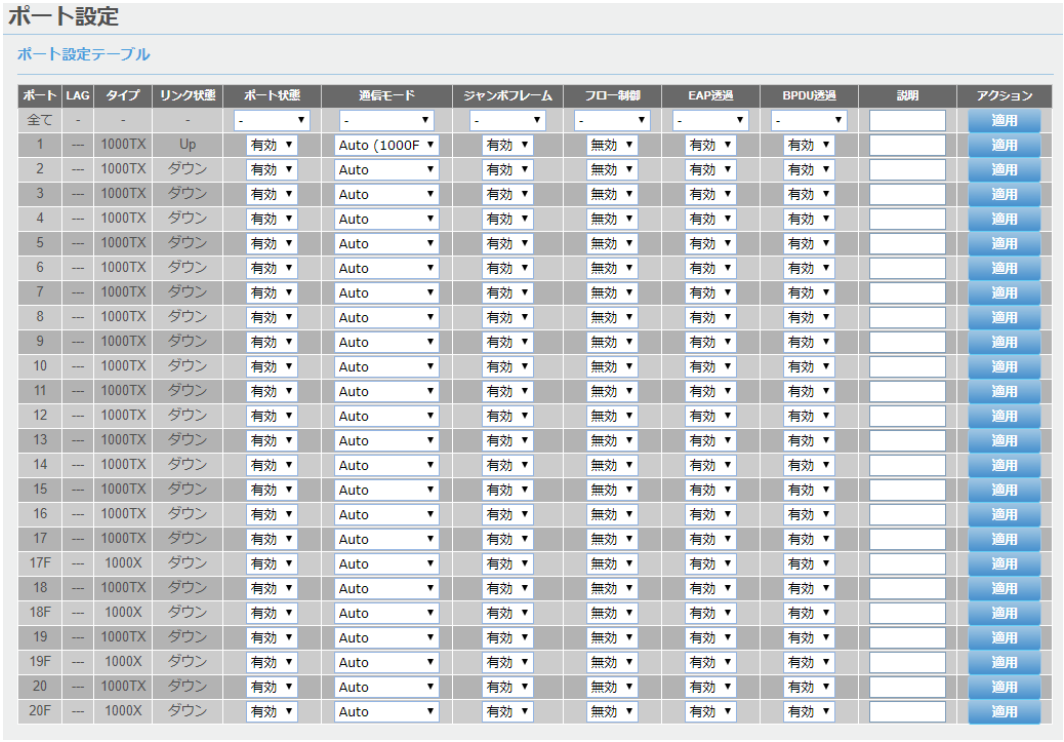



| IEEE 802.3az EEE 設定 | |
|---|---|
| EEE 機能 | EEE 機能の状態（有効／無効）を選択します。（デフォルト：無効） |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 6. ネットワーク

## 6.1. ポート設定

［ポート設定］ページで、ポート状態、通信モード、ジャンボフレーム、フロー制御、EAP 透過、BPDU 透過などの設定やリンクアグリゲーション（以後、LAG）、ポートタイプ、リンク状態の確認ができます。




| ポート設定テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。<br>なお、コンボポートでアクティブになるインターフェースはどちらか一方のみです。同時に使用した場合、SFP ポートが優先されます。 |
| LAG | LAG の状態とグループ番号が表示されます。 |
| タイプ | スイッチのポートタイプが表示されます。<br>・ 1000TX：10／100／1000Base-T イーサネットポート<br>・ 100FX または 1000X：SFP ポート |
| リンク状態 | ポートのネットワークリンクの状態が表示されます。<br>・ アップ：ポートと対向ノード間に有効なリンクが存在している<br>・ ダウン：ポートと対向ノード間に有効なリンクが存在していない |
| ポート状態 | ポートの状態を選択します。無効に設定されたポートは使用できなくなります。<br>・ 無効：イーサネットフレームを送受信しない<br>・ 有効：イーサネットフレームを送受信する（デフォルト設定） |

| | |
|---|---|
| 通信モード | ポートの通信モードを選択します。<br>・ Auto：オートネゴシエーションで動作（デフォルト設定）<br>対向ノードとのリンクを確立した後、通信モードがかっこ内に表示されます。(例えば1000 Mbpsの全二重モードならAuto(1000F))<br>・ 1G/F：1000 Mbpsの全二重通信モードで動作<br>・ 100M/F：100 Mbpsの全二重通信モードで動作<br>・ 10M/F：10 Mbpsの全二重通信モードで動作<br>・ 100M/H：100 Mbpsの半二重通信モードで動作<br>・ 10M/H：10 Mbpsの半二重通信モードで動作<br>**Note:** ポートがAutoに設定されている場合は、対向ノードもオートネゴシエーションに設定する必要があります。 |
| ジャンボフレーム | スイッチのジャンボフレーム機能の状態を選択します。<br>有効にした場合、最大ジャンボフレームサイズは10000 byteです。<br>・ 無効：ジャンボフレームを送受信しない<br>・ 有効：ジャンボフレームを送受信する（デフォルト設定）<br>**Note:** QoS機能が有効の場合、ジャンボフレームを有効にできません。 |
| フロー制御 | スイッチのフロー制御機能の状態を選択します。<br>・ 無効：フロー制御を無効にする（デフォルト設定）<br>・ 有効：フロー制御を有効にする |
| EAP透過 | ポートのEAP透過の状態を選択します。<br>EAP フレーム（EAPoL）は、ネットワークに接続するデバイスがIEEE802.1Xで認証を行う場合に送信します。認証デバイスとネットワーク装置の間に本スイッチがある場合、EAP 透過を有効にする必要があります。<br>・ 無効：EAPパケットを送受信しない<br>・ 有効：EAPパケットを送受信する（デフォルト設定） |
| BPDU透過 | ポートのBPDU透過の状態を選択します。<br>BDPUフレームは、スパニングツリープロトコルでネットワーク情報の配信に使用されます。STP 機能が有効なネットワーク機器間に本スイッチがあり、かつ本スイッチでSTP機能を使用しない場合、BDPU透過を有効にしないとSTPが正常に動作しない場合があります。<br>・ 無効：BPDUフレームを転送しない<br>・ 有効：BPDUフレームを転送する（デフォルト設定）<br>STP機能が有効の場合、スイッチはBPDUフレームを受信して処理する必要があるため、BPDU透過を有効にすることはできません。 |
| 説明 | ポートの説明を32文字以内で入力します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 6.2. スパニングツリー

スパニングツリープロトコル（STP）は、複数の到達可能なレイヤー2 通信経路が存在するネットワーク構成において、論理的なツリー状のトポロジーを自動的に構築するプロトコルです。STP を使用しない場合、複数の到達可能なレイヤー2 通信経路が存在するとループ構成になり、ブロードキャストフレームによる輻輳の発生などネットワークに悪影響があります。STP を使用すると、ネットワークトポロジーに応じてポートの状態を変えることで、ループ構成が解消されます。

STP 機能が有効なネットワーク機器では、BPDU フレームを使用してネットワーク情報を配信し、自動的に通信経路を算出します。有効な通信経路と判断されたポートはフォワーディング状態になり、そのポートでの転送処理が可能になります。通信経路として使用されないポートはブロッキング状態やディスカーディング状態になり、BPDU フレームの処理のみを行います。

本スイッチでは、スパニングツリープロトコルとして、802.1D STP、802.1w Rapid Spanning Tree Protocol（以後、RSTP）、802.1s Multiple Spanning Tree Protocol（以後、MSTP）の 3 つのバージョンをサポートします。
RSTP は STP を改善したプロトコルで、トポロジー変更が発生した際の遷移時間を STP よりも大幅に短縮することができます。ネットワークに導入する際は通常、STP よりも RSTP が用いられます。
MSTP は RSTP を拡張したプロトコルで、「リージョン」による機器グループ単位や「インスタンス」による VLAN グループ単位でのトポロジーを構築することができます。設定が煩雑化するため、多数のネットワーク機器や VLAN が存在する複雑な大規模ネットワーク向けのプロトコルです。

STP 機能を用いて冗長性のあるネットワークを構築するのは比較的容易で、たとえば 3 台のトライアングル構成のようなシンプルなネットワークであれば対象スイッチで RSTP を適用するだけで自動的に適切なトポロジーを構成します。ただし、さらに踏み込んだ詳細ネットワーク設計（パラメーターを調整して正常時および障害発生時の通信経路や切替時間などを制御）は難解で、規格書などで STP の詳細動作をご確認いただいた上で設計してください。
また、本スイッチは原則としてスモールビジネス向けネットワークでの利用を想定しており、その大部分は（VLAN が多数登録されていても）MSTP を必要とするような複雑な構成ではありません。MSTP は RSTP や STP よりも負荷が大きく、ネットワークの規模や複雑さによっては MSTP の処理が追いつかず期待した動作を行えない場合もありますので、本スイッチで MSTP を使用する際には事前に十分な検証を行ってください。

## 6.2.1. プロトコル

［プロトコル］ページで、STP 機能の状態、使用する STP プロトコル、および STP に使用する基本的なパラメーターを設定できます。


| STP 設定 | |
|---|---|
| STP 機能 | スイッチの STP 機能の状態（有効／無効）を選択します。（デフォルト：無効）<br>Note: STP 機能を有効にするには、［ネットワーク］＞［ポート設定］ページで BPDU 透過を無効にする必要があります。 |
| プロトコル | STP モードを選択します。（デフォルト：RSTP）<br>・ STP：スイッチで STP を有効にする<br>・ RSTP：スイッチで RSTP を有効にする<br>・ MSTP：スイッチで MSTP を有効にする |
| ブリッジ優先度 | ルートブリッジ選出に使用される優先度を 0～61440 の範囲(4096 の倍数）で選択します。（デフォルト：32768）<br>ルートブリッジは STP による論理的な L2 ネットワークトポロジーの基幹となる 1 台の機器を指し、ほかの機器はルートブリッジまでの経路情報を元にして使用する通信経路を導出します。<br>ルートブリッジの選出は規格により定められたルールにより自動的に行われますが、ネットワーク管理者がルートブリッジとなる機器を指定したい場合、ブリッジ優先度を低く設定することで優先的に選出されるようになります。 |
| BPDU エージング時間 | STP においてルートブリッジが送信する BPDU フレームの待ち時間を 6～40（秒）の範囲で入力します。 |

| | |
|---|---|
| | STP では、ルートブリッジが定期的に BPDU フレームを送信しますが、BPDU エージング時間を経過してもポートで BDPU フレームを受信しなかった場合、BPDU で配信された情報は削除され、トポロジー変更として処理されます。また、STP では実質的にルートブリッジからの最大距離（何台のスイッチを経由するか）を決定するパラメーターとして動作します。<br>RSTP では、STP を使用する機器を接続したポートにおいて参照されます。MSTP では、STP や RSTP を使用する機器が接続されているポートにおいて参照されます。 |
| BPDU 送信時間 | BPDU パケットを送信する間隔を 1～10（秒）の範囲で入力します。 |
| 状態遷移保留時間 | STP において、ポートの状態がフォワーディングになるまでの各状態における遷移保留時間を 4～30（秒）の範囲で入力します。<br>STP ではポートがブロッキング状態から変化する場合、リスニング状態からラーニング状態を経て、フォワーディング状態に移行します。状態遷移保留時間は、リスニング状態からラーニング状態、およびラーニング状態からフォワーディング状態に遷移するまでの保留時間を指します。<br>RSTP および MSTP では、STP を使用する機器や BPDU を送信しない機器を接続したポートにおいて参照されます。 |
| 転送保留カウント | スイッチが 1 秒あたりに送信可能な最大 BPDU 数を 1～10 の範囲で入力します。<br>連続してトポロジー変更が発生した場合、通知する BDPU フレーム数の増加に伴い、処理負荷が上昇することがありますので、最大 BPDU フレーム数を定めることで、負荷を抑制します。設定値を超えた場合は、次の BPDU パケットの送信を遅らせます。 |
| 最大ホップ数 | MSTP において、リージョン内での BPDU フレームの最大経由スイッチ台数を 6～40 の範囲で入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

Note: 設定時間は以下の式に従う必要があります。

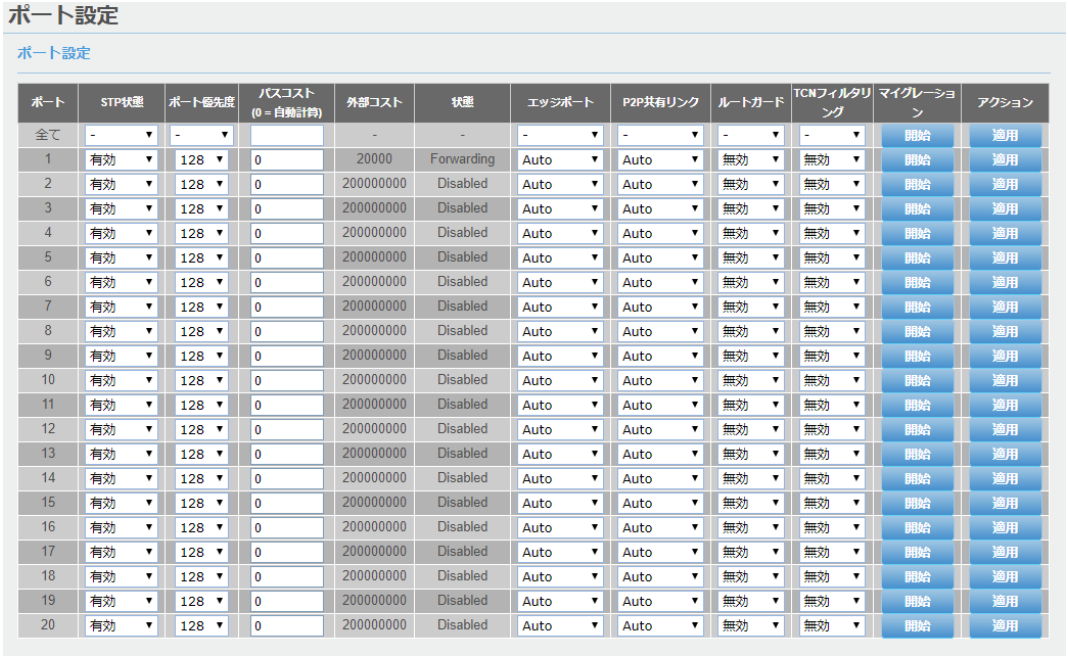
2×（状態遷移保留時間－1） ≧ BPDU エージング時間 ≧ 2×（BPDU 送信時間＋1）

| ルート情報 | |
|---|---|
| ルートブリッジ | ルートブリッジ ID が表示されます。 |
| ルートパスコスト | 受信した BPDU フレームから算出されるルートパスコスト（ルートブリッジまでの最短距離）が表示されます。ルートブリッジ自体のルートパスコストは 0 です。 |
| BPDU エージング時間 | BPDU エージング時間が表示されます。 |
| 状態遷移保留時間 | 状態遷移保留時間が表示されます。 |
| ルートポート | ルートポートとして割り当てられたポート番号が表示されます。 |

| | |
|---|---|
| | ルートポートは、スイッチの各ポートで受信した BPDU フレームから累積パスコストを算出した結果、ルートブリッジへの最短経路として選定されたポートです。STP ではルートブリッジを除き、各スイッチに各 1 ポート存在します。 |

## 6.2.2. ポート

［ポート］ページで、ポート単位での STP の設定を行います。




| ポート設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| STP 状態 | ポートの STP の状態（有効／無効）を選択します。 |
| ポート優先度 | ポート優先度を 0～240 の範囲（16 の倍数）で選択します。<br>ルートポート（ルートブリッジへの最短経路のポート）を選定する際に、複数のポートで累積パスコストが同一だった場合に優先するポートをポート優先度で指定することができます。ポート優先度が小さいポートが優先されます。<br>なお、パスコストもポート優先度も同一の場合、ポート番号が小さいポートが優先されます。 |
| パスコスト<br>(0＝自動計算) | ポートで加算されるパスコストを 0～200000000 の範囲で入力します。（デフォルト：0）<br>STP では、受信した BPDU フレームのルートパスコスト情報から各ポートの累積パスコストを計算し、比較することでルートパスコストを算出します。BDPU フレームを受信したポートは、累積パスコスト |

| | |
|---|---|
| | の計算の際に指定したパスコストを加算します。<br>0 を設定すると、802.1D の推奨値を使用して、物理リンク速度によってパスコストが自動で設定されます。<br>リンク速度と推奨値は以下のとおりです。<br>・ 10 Mbps：2000000<br>・ 100 Mbps：200000<br>・ 1 Gbps：20000<br>・ 10 Gbps：2000 |
| 外部コスト | ポートに対するパスコストを表示します。<br>［パスコスト］が 0 の場合、自動で設定された値が表示されます。 |
| 状態 | ポートの STP 遷移状態が表示されます。<br>Forwarding 状態のポートのみが通信の転送処理を行うことができます。 |
| エッジポート | ネットワークトポロジーのエッジデバイスに接続されているポート（エッジポート）の状態を設定します。（デフォルト：Auto）<br>エッジポート状態は、接続するデバイスに冗長となる経路が存在しない、すなわち BDPU フレームを受信しない前提のポートで、リンク状態の変化による Forwarding 状態への遷移が速やかに行われます。<br>・ Auto：<br>ポートが BDPU フレームの受信状態を確認し、エッジポート状態であるかどうかを自動的に判別します。<br>・ 該当：ポートをエッジポートとして割り当てます。エッジポートは通常、BPDU フレームを受信しませんが、BPDU パケットを受信した場合、自動的にエッジポート状態を解除します。<br>・ 非該当：<br>ポートがエッジポート状態ではないことを表します。 |
| P2P 共有リンク | ポートのリンクタイプを選択します。（デフォルト：Auto）<br>RSTP の高速収束は、RSTP を使用する機器がすべて直接接続されている（ポイントツーポイント（P2P）リンク状態）という前提で実現しており、たとえばリピーターハブによる間接的な接続が行われている場合、RSTP による高速状態遷移を行うと、ループ状態を発生させることがあります。P2P 接続形態ではないポートに対してリンク状態を共通リンク（P2P リンクではない状態）に指定しなければならない場合があります。なお、デュプレックスモードが半二重の場合、P2P リンク状態になることはできません。<br>・ Auto：<br>リンク状態は、ディプレックスモードから自動的に取得されます。全二重の場合は P2P リンク状態になり、半二重の場合は共通リンク状態になります。 |

| | |
|---|---|
| | ・ 該当：<br>P2P リンク状態を指定します。デュプレックスモードが半二重の場合、P2P リンク状態を維持できないため、共通リンクとして動作します。<br>・ 非該当：共有リンクを指定します。RSTP での高速収束は行わず、STP と同様の状態遷移を行います。 |
| ルートガード | ルートガードの状態（有効／無効）を選択します。（デフォルト：無効）<br>ルートガードが有効の場合、ルートポートの選定対象外になります。 |
| TCN フィルタリング | TCN は、ネットワークトポロジーの変化を通知する BPDU です。<br>TCN のフィルタリング状態（有効／無効）を選択します。（デフォルト：無効）<br>有効にした場合、ポートで受信した TCN をほかのポートへ配信しません。 |
| マイグレーション | ［開始］ボタンをクリックすると、RSTP および STP の BPDU を受け入れるように設定されたポートで STP 設定に関する情報を要求して、ほかのブリッジに BPDU パケットを送信します。<br>スイッチが RSTP 用に設定されている場合は、ポートは 802.1D STP から 802.1w RSTP に移行します。<br>マイグレーションでは、セグメントの全体やまたは一部で 802.1w RSTP にアップグレード可能なネットワークステーションやセグメントに接続されたポートで開始します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.2.3. トポロジー変更保護

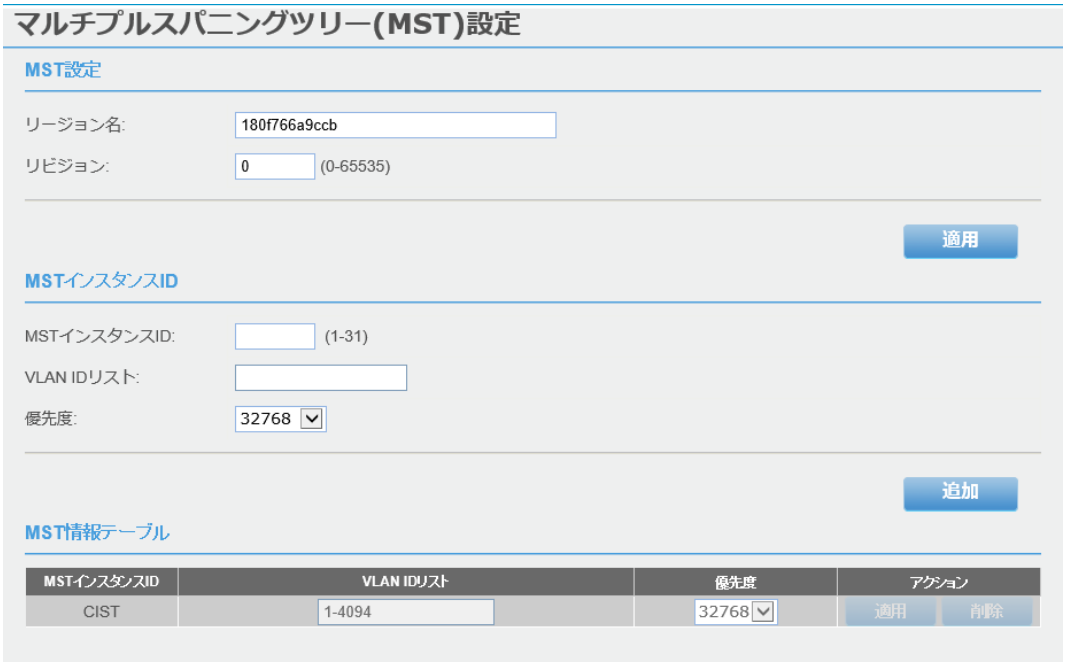
STP を使用したネットワークでは、トポロジー変更が発生するとトポロジー変更通知（TCN）の BDPU フレームにより情報を通知しますが、トポロジー変更が頻発する環境では、大量の TCN BPDU により処理負荷が増大することがあります。

［トポロジー変更保護］ページでは、トポロジー変更保護の設定を行います。トポロジー変更保護を有効にすると、一定期間でしきい値を上回る TCN BPDU を受信した際に無視します。

| MST 設定 | |
|---|---|
| TC 保護機能 | トポロジー変更保護の状態（有効／無効）を選択します。（デフォルト：無効） |
| TC 保護閾値 | トポロジー変更保護の周期のしきい値を 1～100（回）の範囲で入力します。（デフォルト：20 回） |
| TC 保護サイクル | トポロジー変更保護の周期を 1～10（秒）の範囲で入力します。（デフォルト：5 秒） |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

### 6.2.4. マルチプルスパニングツリー

［マルチプルスパニングツリー］ページで、リージョン名やリビジョンなどの MSTP に使用するパラメーターを設定します。また、VLAN ID と MST インスタンスのマッピングを設定することができます。




| MST 設定 | |
|---|---|
| リージョン名 | リージョン名を 32 文字以内で入力します。<br>リージョン名を設定しない場合は、MSTP を実行しているスイッチの MAC アドレスが入力されます。 |
| リビジョン | MST リビジョンを 0～65535 の範囲で入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| MST インスタンス ID | |
|---|---|
| MST インスタンス ID | MST インスタンス番号を 1～31 文字の範囲で入力します。 |
| VLAN ID リスト | MST インスタンスに関連付ける VLAN ID リストを入力します。 |
| 優先度 | ブリッジ優先度を 0～61440 の範囲（4096 の倍数）で選択します。 |

| | |
|---|---|
| ［追加］ボタン | ［追加］ボタンをクリックすると、MST インスタンスが追加されます。 |

| MST 情報テーブル | |
|---|---|
| MST インスタンス ID | MST インスタンス番号（あるいは CIST）が表示されます。 |
| VLAN ID リスト | MST インスタンスに関連付けられている VLAN ID が表示されます。 |
| 優先度 | ブリッジ優先度が表示されます。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。<br>［削除］ボタンをクリックすると、MST インスタンスが削除されます。 |

## 6.2.5. インスタンス

［インスタンス］ページで、MST インスタンスの情報を表示します。


| インスタンス情報 | |
|---|---|
| MSTI ID | MST インスタンス番号（あるいは CIST）が表示されます。 |
| 内部ルート | ルートブリッジへのパスコストが表示されます。 |
| ルートポート | ルートポートが表示されます。 |
| リージョナルルートブリッジ | リージョナルルートブリッジが表示されます。 |
| 指定ブリッジ | 指定ポートに接続されているスイッチが表示されます。 |
| インスタンス優先度 | インスタンスの優先度が表示されます。 |

## 6.2.6. MST ポート

［MST ポート］ページで、各ポートの MST インスタンス単位での状態を表示します。また、パスコストや優先度などを設定することができます。

| MST ポート | |
|---|---|
| ポート選択 | ポートを選択します。 |

| MST ポート情報 | |
|---|---|
| MSTI ID | MST インスタンス番号が表示されます。 |
| 指定ブリッジ | 指定ポートに接続されているスイッチが表示されます。 |
| 内部パスコスト | 指定ブリッジまでのパスコストが表示されます。 |
| パスコスト<br>(0＝自動) | ルートブリッジへのパスコストを計算する際に、MSTP で使用されるポートコストを 0～200000000 の範囲で入力します。（デフォルト：0） |
| 優先度 | 2 つのポートが同じポートコストの場合に、MSTP で使用されるポート優先度を 0～240 の範囲で入力します。（デフォルト：128） |
| 状態 | STP ポートの状態（有効／無効）が表示されます。 |
| 役割 | STP ポートの役割（ルートポート／指定ポート／バックアップポート／無効ポート）が表示されます。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 6.3. リンクアグリゲーション

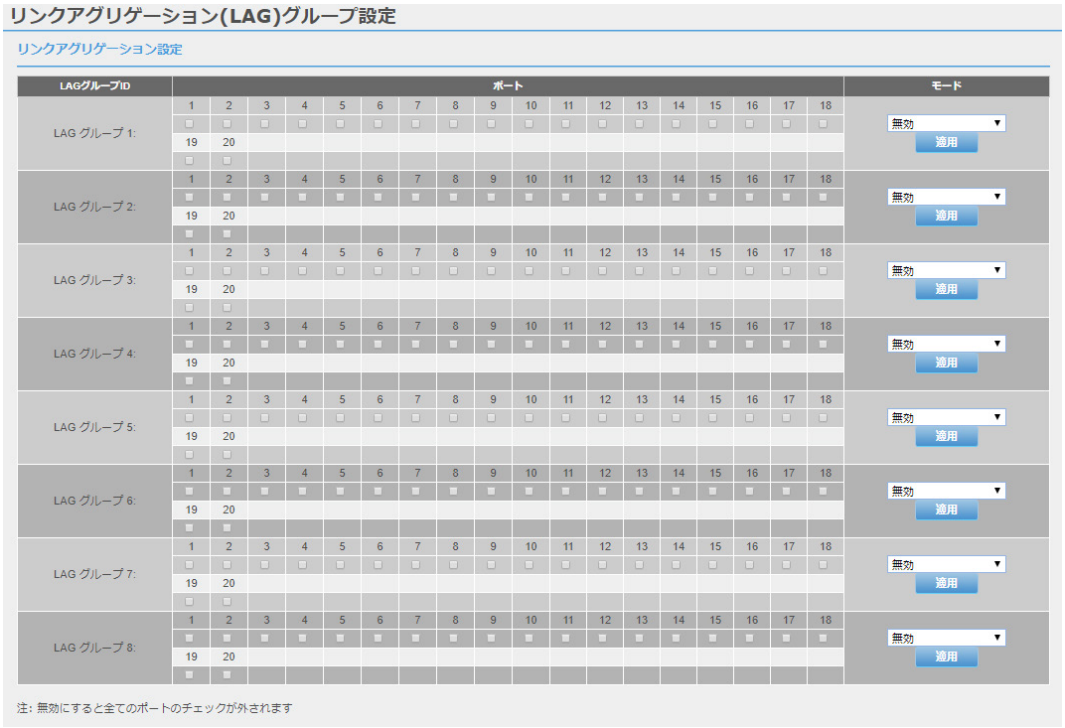
リンクアグリゲーション機能を使用すると、2 つ以上のリンクを統合して、合計帯域幅がより大きい単一の結合リンクを作成することができます。作成できる LAG グループ数は、機種によって異なります。

スタティック（手動）LAG グループでは 2～8 ポート、Link Aggregation Control Protocol（以後、LACP）（アクティブ／パッシブ）グループでは 2～10 ポートを同一グループとしてまとめることができます。LACP グループでは同時に最大 8 ポートまでが通信に使用されます。

## 6.3.1. グループ

［グループ］ページでは、LAG グループとして組み合わせるポートを選択して、グループの状態（モード）を指定します。

Note: スイッチと対向ノードの両方に LAG グループを設定した後に、機器間をケーブルで接続してください。先にケーブルを接続すると、ループ構成となりネットワークに悪影響を及ぼすことがあります。

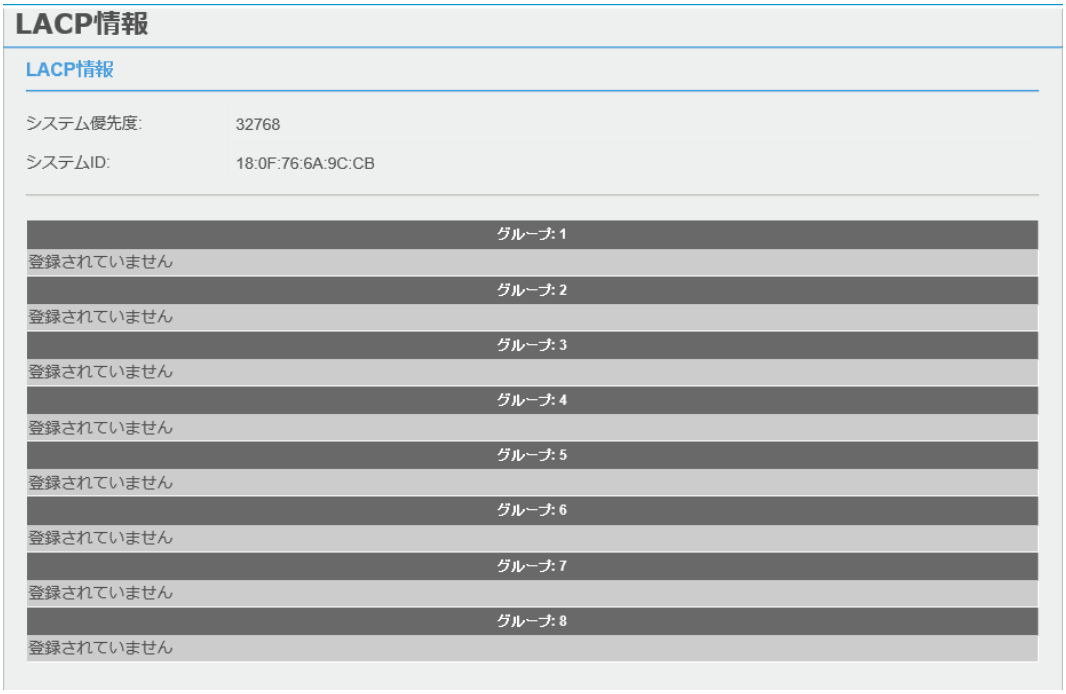



| リンクアグリゲーション設定 |
| --- |
| ポートを LAG グループとしてまとめることができます。<br>LAG グループごとにポート番号を選択し、LAG グループのモードを選択します。<br>・ LACP（アクティブ）：<br>同一 LAG グループに 2～10 個のポートを選択できます。<br>アクティブな LACP ポートでは、LACP 制御フレームを処理、送信します。 |

| |
|---|
| • LACP（パッシブ）：<br>同一 LAG グループに 2～10 個のポートを選択できます。<br>パッシブな LACP ポートでは、最初に LACP 制御フレームを送信しません。<br>• スタティック：<br>同一 LAG グループに 2～8 個のポートを選択できます。<br>• 無効：<br>LAG グループを解除し、選択したポートをクリアします。 |
| ［適用］ボタンをクリックすると、変更が適用されます。 |

### 6.3.2. LACP 情報

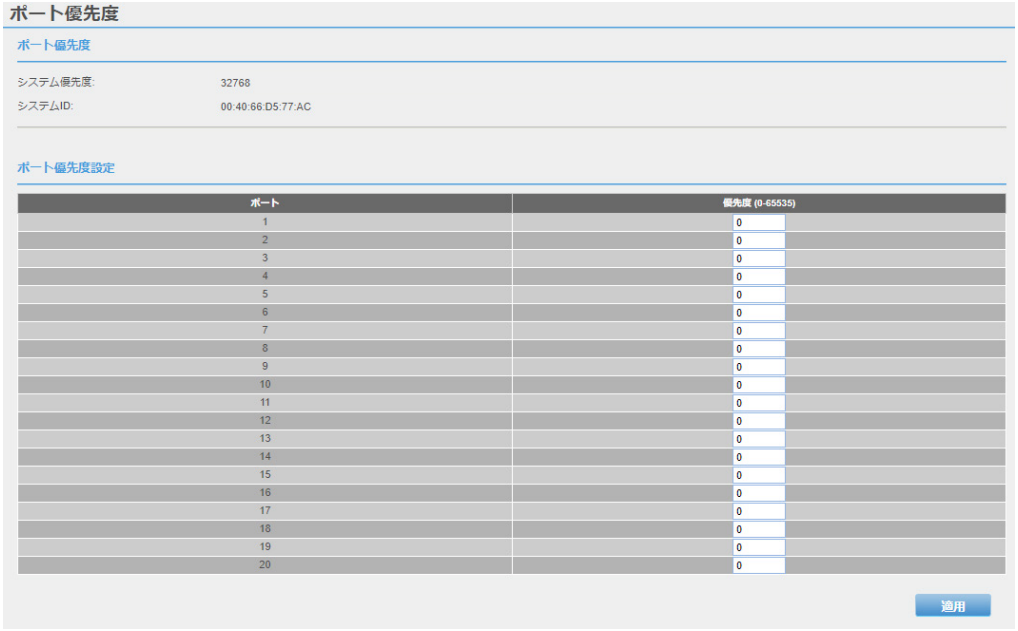
［グループ］ページでは、LACP の状態や設定情報を表示します。




| LACP 情報 | |
|---|---|
| システム優先度 | スイッチに割り当てられているシステム優先度が表示されます。<br>この値は変更できません。 |
| システム ID | スイッチに割り当てられている MAC アドレス値が表示されます。<br>この値は変更できません。 |
| グループ | グループ ID ごとの LACP 情報を表示します。<br>• アグリゲーター：LACP の識別 ID が表示されます。<br>• アクティブポート：LACP でアクティブ状態のポートが表示されます。<br>• スタンバイポート：LACP でスタンバイ状態のポートが表示されます。 |

## 6.3.3. ポート優先度

［ポート優先度］ページでは、LACP グループ内でのポートの優先度を表示します。

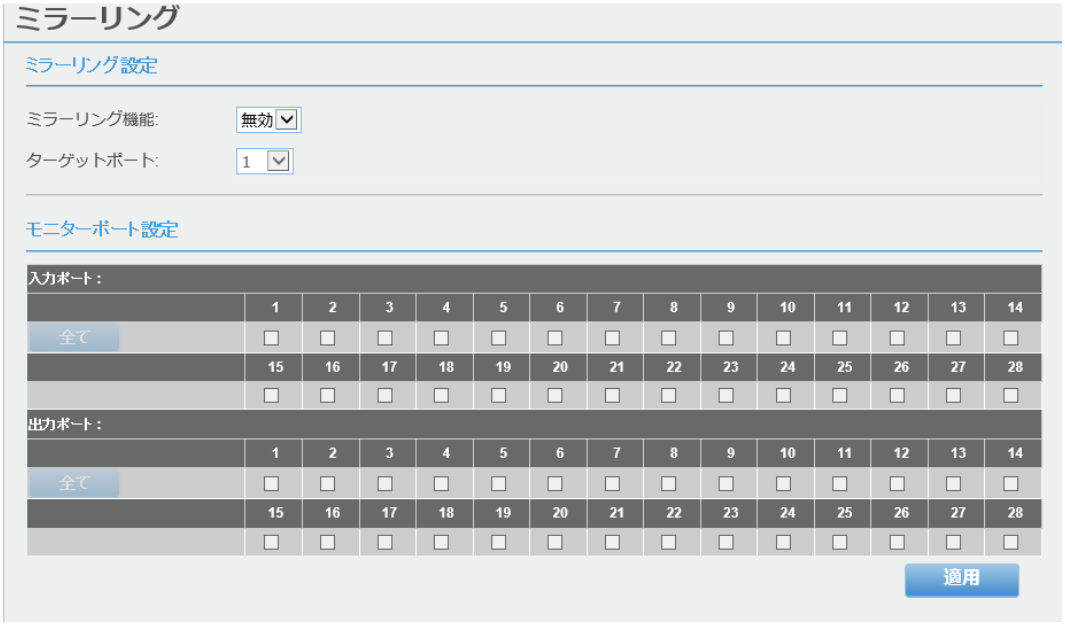



| ポート優先度 | |
|---|---|
| システム優先度 | LACP システム優先度（32768）が表示されます。 |
| システム ID | スイッチに割り当てられている MAC アドレスが表示されます。 |

| ポート優先度設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 優先度(0～65535) | ポート優先度によって、スタンバイになるポートが決まります。<br>1 つの LAG グループで、最大 8 個のポートがアクティブになります。トランクグループに優先度の高いポートを割り当てるには、該当のポート番号の優先度を 0～65535 の範囲で入力します。(デフォルト：0)<br>数値が低いほど優先度は高くなります。(65535 が最も低い優先度です。) |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 6.4. ミラーリング

［ミラーリング］ページでは、ポートミラーリングの設定を行います。
ポートミラーリングを行うと、モニターポートの入力（受信）パケットや出力（送信）パケットのコピーがターゲットポートに転送され、そこでネットワークトラフィックを監視できます。




| ミラーリング設定 | |
|---|---|
| ミラーリング機能 | ポートミラーリング機能の状態（有効／無効）を選択します。 |
| ターゲットポート | モニターポートの受信／送信パケットのコピーを受信するポートを選択します。 |

| モニターポート設定 | |
|---|---|
| 入力ポート | ポート番号を選択します。選択したポートの受信パケットがターゲットポートにコピーされます。<br>［全て］ボタンをクリックすると、ターゲットポートを除くすべてのポートが選択されます。 |
| 出力ポート | ポート番号を選択します。選択したポートの送信パケットがターゲットポートにコピーされます。<br>［全て］ボタンをクリックすると、ターゲットポートを除くすべてのポートが選択されます。 |

［適用］ボタンをクリックすると、変更が適用されます。

# 6.5. ループ検知

［ループ検知］ページでは、スイッチのループ検知機能の設定を行います。

ループ検知機能は、ネットワークでループ構成が発生した場合に検知し、ループ状態を解消するために対象ポートをブロックする機能です。
ループ検知が有効なポートでは、ループ検知用のフレームが定期的に送信されます。スイッチは、自身が送信したループ検知フレームを受信すると、ループ構成が発生したとみなします。
ループを検知したポートは自動的にブロックされます。自動復旧時間が経過すると、ループを検知したポートはブロックを解除します。

ループ構成を解消する方法としては他にスパニングツリープロトコル（STP）を用いる方法がありますが、STP は必然的にループ構成となる、冗長性のあるネットワークを構成した場合に、状況に応じた最適な論理経路を自動的に作成するために使用します。そのため、ネットワーク全体で STP を用いる必要があります。
ループ検知機能は、基本的なツリー構成のネットワークであってもなんらかの偶発的な要因によりループ構成となることがあり、その際にネットワーク全体への影響を最小限にするために用いられます。スイッチ単体でも効果は見込めますが、ネットワークトポロジーを考慮しないシンプルな機能のため、ポートをブロックしたとしてもネットワーク全体のループ構成が解消されない場合もあります。

Note: スパニングツリープロトコルが有効の場合は、ループ検知機能を有効にできません。


| ループ検知設定 | |
|---|---|
| ループ検知機能 | ループ検知機能の状態（有効／無効）を選択します。（デフォルト：無効） |

| ループ検知時間 | |
|---|---|
| 検知フレーム送信間隔 | ループをチェックする間隔を 1～32767（秒）の範囲で入力します。（デフォルト：2 秒） |
| 自動復旧時間 | ループを検知してポートがブロックされた場合の自動復旧時間を 0 または 60～1000000（秒）の範囲で入力します。（デフォルト：60 秒）0 を入力すると、自動復旧は行いません。 |

［適用］ボタンをクリックすると、変更が適用されます。

| ループ検知テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| ループ検知状態 | 各ポートのループ検知機能の状態を選択します。<br>［全て］から、すべてのポートをまとめて設定できます。<br>・ 有効：ループ検知機能を有効にする<br>・ 無効：ループ検知機能を無効にする |
| ループ状態 | 各ポートの現在のループ状態が表示されます。<br>・ 正常：正常に機能している（ループなし）<br>・ ループ検知：ループが検知されている |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 6.6. スタティックユニキャスト

［スタティックユニキャスト］ページで、MAC アドレス学習テーブルにユニキャスト MAC アドレスのスタティックエントリーを登録することができます。

MAC アドレス学習テーブルは、MAC アドレスとポートの対応を示す内部テーブルです。スイッチは受信フレームの宛先 MAC アドレス情報から、MAC アドレス学習テーブルの情報を参照して対象ポートに転送します。受信したフレームの宛先 MAC アドレスが MAC アドレス学習テーブル上に登録されていない場合には、スイッチは同一の VLAN インターフェースを持つすべてのポートに転送します（フラッディング）。

通常、MAC アドレス学習テーブルのエントリーは、ノードからの受信フレームにより自動的に登録されるため、管理者がスタティックのエントリーを意識する必要はありません。本機能は一部の限定的な条件で利用されます。


| スタティックユニキャスト登録 | |
|---|---|
| VLAN ID | VLAN ID を 1～4094 の範囲で入力します。指定する VLAN は、事前に設定されている必要があります。<br>Note: ［VLAN ID］は、［VLAN］＞［アドレス学習モード］ページで学習モードが IVL に設定されている場合のみ変更できます。 |
| MAC アドレス | スタティックエントリーの MAC アドレスを入力します。 |

| ポート設定 |
|---|
| ポートを選択し、VLAN ID と MAC アドレスを指定して、MAC アドレス学習テーブルのスタティックエントリーを作成できます。 |

［適用］ボタンをクリックすると、MAC アドレス学習アドレステーブルにスタティックエントリーが作成されます。

| スタティックユニキャストテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、作成したスタティックエントリーがすべて削除されます。 |
| VLAN | 作成したエントリーの VLAN ID が表示されます。<br>Note: 802.1Q VLAN の［VLAN］＞［アドレス学習モード］ページで学習モードが SVL に設定されている場合、［VLAN］は［N/A］と表示されます。 |
| MAC アドレス | 作成したエントリーの MAC アドレスが表示されます。 |
| ポート | スタティックユニキャストの MAC アドレスがマッピングされたポートが表示されます。 |
| アクション | ［修正］ボタンをクリックすると、作成したスタティックエントリーの設定情報を変更できます。<br>［削除］ボタンをクリックすると、作成したスタティックエントリーが削除されます。 |

# 6.7. スタティックマルチキャスト

［スタティックマルチキャスト］ページで、マルチキャストテーブルのスタティックエントリーを登録できます。
マルチキャストテーブルは、IP マルチキャスト通信で使用するグループ MAC アドレスとメンバーポートの対応を示した内部テーブルです。マルチキャストフィルタリング機能を有効にすると、スイッチはマルチキャストテーブルを参照し、該当するグループ MAC アドレスをメンバーに持つポートだけにマルチキャストトラフィックを転送します。

通常、マルチキャストテーブルは IGMP スヌーピング機能を使用して自動的に登録するように設定しますが、IGMP スヌーピングによる登録が行われていない場合にスタティックエントリーを登録することがあります。


| スタティックマルチキャスト登録 | |
|---|---|
| VLAN ID | VLAN ID を 1～4094 の範囲で入力します。VLAN は、事前に設定されている必要があります。<br>Note: ［VLAN ID］は、［VLAN］＞［アドレス学習モード］ページで学習モードが IVL に設定されている場合のみ変更できます。 |
| グループ MAC アドレス | スタティックエントリーのマルチキャスト MAC アドレスを入力します。 |

| グループメンバー |
|---|
| 複数のポートを選択し、マルチキャスト MAC アドレスを指定して、マルチキャストテーブルのスタティックエントリーを作成できます。<br>［全て］ボタンをクリックすると、すべてのポートが選択されます。 |

［適用］ボタンをクリックすると、マルチキャストテーブルにスタティックエントリーが作成されます。

| スタティックマルチキャストテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、作成したスタティックエントリーがすべて削除されます。 |
| VLAN ID | 作成したスタティックエントリーの VLAN ID が表示されます。<br>Note: 802.1Q VLAN の［VLAN］＞［アドレス学習モード］ページで学習モードが SVL に設定されている場合、［VLAN ID］は［N/A］（使用不可）と表示されます。 |
| MAC アドレス | 作成したスタティックエントリーのマルチキャスト MAC アドレスが表示されます。 |
| グループメンバー | スタティックエントリーのグループポートのメンバーリストが表示されます。 |
| アクション | ［修正］ボタンをクリックすると、作成したスタティックエントリーの設定情報を変更できます。<br>［削除］ボタンをクリックすると、作成したスタティックエントリーが削除されます。 |

# 6.8. IGMP スヌーピング

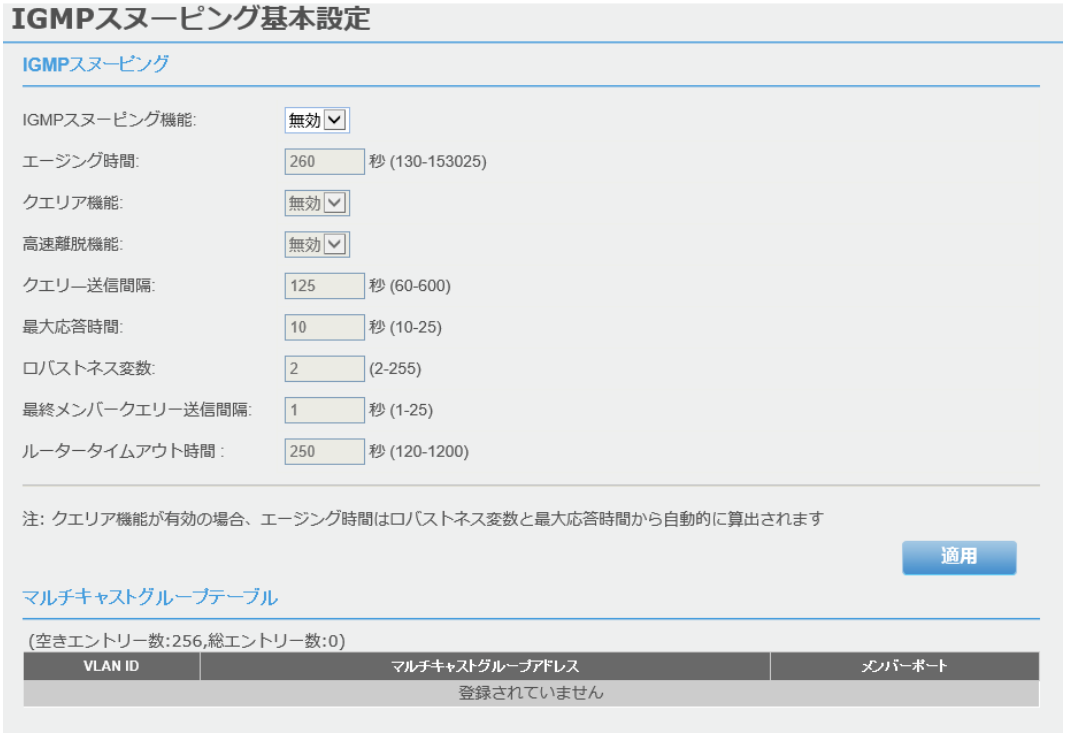
IGMP スヌーピング機能は、IPv4 マルチキャスト通信のグループ参加状況を通知する IGMP パケットをモニタリングして、マルチキャストテーブルを自動的に更新する機能です。

マルチキャストグループの参加状況の管理は、基本的に「IGMP メンバーシップレポート」と「IGMP クエリー」の 2 種類のパケットで行われます。
IGMP メンバーシップレポートはマルチキャストノードからマルチキャストルーターに参加状況を報告します。参加通知だけでなく、離脱、維持などの通知も行います。
IGMP クエリーは、原則としてマルチキャストルーターが送信するパケットで、マルチキャストノードの参加状況を調査するために用いられます。定期的に送信する IGMP ジェネラルクエリーと、一定条件で送信する IGMP スペシフィッククエリーがあり、IGMP クエリーに対するノードの応答を確認してマルチキャストトラフィックの転送先を制御します。

マルチキャストフィルタリング機能が有効の場合、スイッチが受信した IP マルチキャスト通信はマルチキャストテーブルに従って転送処理されます。IGMP スヌーピング機能はマルチキャストフィルタリングと併用して使用され、IGMP クエリーや IGMP メンバーシップレポートをモニタリングすることでマルチキャストルーターやノードが存在するポートを学習します。
IGMP スヌーピング機能を使用しない場合、マルチキャストフィルタリングが有効なポートでは、適切なスタティックエントリーが登録されていない限り IP マルチキャスト通信が転送されません。

## 6.8.1. 基本設定

［基本設定］ページでは、IGMP スヌーピング機能の一般的な設定を行います。



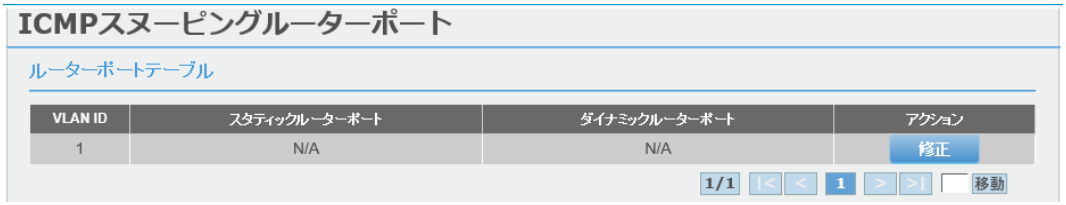
| IGMP スヌーピング | |
|---|---|
| IGMP スヌーピング機能 | IGMP スヌーピング機能の状態（有効／無効）を選択します。（デフォルト：無効） |
| エージング時間 | 学習した各メンバーポートのエージング時間を 130～153025（秒）の範囲で入力します。（デフォルト：260 秒）<br>エージング時間を経過するまでの間に特定のメンバーポートから IGMP メンバーシップレポートを受信しなかった場合、そのポートがメンバーから除外されます。<br>スイッチが代表クエリアの場合（クエリア機能が有効で、かつ優先的にクエリアになるデバイスがネットワーク上に存在しない場合）、エージング時間は設定値ではなく、以下の計算値を使用します。<br>エージング時間＝ロバストネス変数×クエリー送信間隔＋最大応答時間 |
| クエリア機能 | IGMP クエリーパケットを送信する機能の状態（有効／無効）を選択します。（デフォルト：無効）<br>IGMP クエリーは通常、マルチキャストルーターから送信されますが、同一ネットワーク内に送信ホストと受信ノードが存在し、マルチキャストルーターによる中継を必要としない構成の場合、クエリーを送信するデバイスがなく、IGMP スヌーピング機能を有効にしてもマルチキャストテーブルが適切に反映されないことがあります。この場合、クエリア機能を有効にしてください。 |
| 高速離脱機能 | 高速離脱機能の状態（有効／無効）を選択します。（デフォルト：無効）<br>高速離脱機能を有効にすると、メンバーポートから IGMP 離脱メッセージを受信した場合、受信したポートを即座にメンバーから除外します。 |
| クエリー送信間隔 | クエリア機能を有効にした場合の、IGMP ジェネラルクエリーの送信間隔を 60～600（秒）の範囲で入力します。（デフォルト：125 秒） |
| 最大応答時間 | IGMP クエリーに対する最大応答待ち時間を 10～25（秒）の範囲で入力します。（デフォルト：10 秒） |
| ロバストネス変数 | クエリア機能を有効にした場合の、クエリーの送信試行回数を 2～255 の範囲で入力します。（デフォルト：2） |
| 最終メンバークエリー送信間隔 | IGMP グループスペシフィッククエリーの送信間隔を 1～25（秒）の範囲で入力します。（デフォルト：1 秒）<br>グループスペシフィッククエリーは、マルチキャストルーターもしくは代表クエリアが IGMP 離脱メッセージを受信した際に、マルチキャストグループにほかの受信ホストが存在するかどうかを確認する目的で送信されます。応答がない場合は、学習したマルチキャストグループのエントリーが削除されます。 |

| | |
|---|---|
| ルータータイムアウト時間 | 学習済みルーターポートのタイムアウト時間を 120～1200（秒）の範囲で入力します。（デフォルト：250 秒）<br>タイムアウト時間を経過するまでの間に IGMP クエリーを受信しなかった場合、学習したルーターポートのエントリーが削除されます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| マルチキャストグループテーブル | |
|---|---|
| VLAN ID | VLAN ID が表示されます。 |
| マルチキャストグループアドレス | マルチキャストグループの MAC アドレスが表示されます。 |
| メンバーポート | マルチキャストグループのメンバーとして登録されているポートが表示されます。 |

## 6.8.2. ルーターポート

ルーターポートは、マルチキャストルーターが存在するポートです。IGMP スヌーピング機能では IGMP クエリーを受信して自動学習しますが、スタティックのエントリーを登録することもできます。




| ルーターポートテーブル | |
|---|---|
| VLAN ID | VLAN ID が表示されます。 |
| スタティックルーターポート | マルチキャストルーターに接続されるポートが表示されます。 |
| ダイナミックルーターポート | 学習されたダイナミックルーターポートが表示されます。 |
| アクション | ［変更］ボタンをクリックすると、ルーターポートの設定を変更できます。 |

ルーターポートテーブルの［変更］ボタンをクリックすると、エントリーの設定を変更できます。

| ルーターポート設定 | |
|---|---|
| VLAN ID | VLAN ID が表示されます。この ID で、ルーターポートの設定を変更する VLAN を識別します。 |

| スタティックルーターポート |
|---|
| マルチキャストルーターに接続されるポートを選択します。<br>［全て］ボタンをクリックすると、すべてのポートが選択されます。 |
| ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［元に戻す］ボタンをクリックすると、すべての選択がリセットされます。 |

# 6.9. MLD スヌーピング

MLD スヌーピング機能は、IPv6 マルチキャスト通信のグループ参加状況を通知する MLD パケットをモニタリングして、マルチキャストテーブルを自動的に更新する機能です。
IPv4 マルチキャスト通信での IGMP スヌーピング機能に相当します。

## 6.9.1. 基本設定

［基本設定］ページでは、MLD スヌーピング機能の一般的な設定を行います。


| MLD スヌーピング | |
|---|---|
| MLD スヌーピング機能 | MLD スヌーピング機能の状態（有効／無効）を選択します。（デフォルト：無効） |
| エージング時間 | 学習した各メンバーポートのエージング時間を 130～153025（秒）の範囲で入力します。（デフォルト：260 秒）<br>エージング時間を経過するまでの間に特定のメンバーポートから MLD メンバーシップレポートを受信しなかった場合、そのポートがメンバーから除外されます。<br>スイッチが代表クエリアの場合（クエリア機能が有効で、かつ優先的にクエリアになるデバイスがネットワーク上に存在しない場合）、エージング時間は設定値ではなく、以下の計算値を使用します。<br>エージング時間＝ロバストネス変数×クエリー送信間隔＋最大応答時間 |
| クエリア機能 | MLD クエリーパケットを送信する機能の状態（有効／無効）を選択します。（デフォルト：無効） |

| | |
|---|---|
| | MLD クエリーは、通常、マルチキャストルーターから送信されますが、同一ネットワーク内に送信ホストと受信ノードが存在し、マルチキャストルーターによる中継を必要としない構成の場合、クエリーを送信するデバイスがなく、MLD スヌーピング機能を有効にしてもマルチキャストテーブルが適切に反映されないことがあります。この場合、クエリア機能を有効にしてください。 |
| 高速離脱機能 | 高速離脱機能の状態（有効／無効）を選択します。（デフォルト：無効）<br>高速離脱機能を有効にすると、メンバーポートから MLD 離脱メッセージを受信した場合、受信したポートを即座にメンバーから除外します。 |
| クエリー送信間隔 | クエリア機能を有効にした場合の、MLD ジェネラルクエリーの送信間隔を 60～600（秒）の範囲で入力します。（デフォルト：125 秒） |
| 最大応答時間 | MLD クエリーに対する最大応答待ち時間を 10～25（秒）の範囲で入力します。（デフォルト：10 秒） |
| ロバストネス変数 | クエリア機能を有効にした場合の、クエリーの送信試行回数を 2～255 の範囲で入力します。（デフォルト：2） |
| 最終メンバークエリー送信間隔 | MLD グループスペシフィッククエリーの送信間隔を 1～25（秒）の範囲で入力します。（デフォルト：1 秒）<br>グループスペシフィッククエリーは、マルチキャストルーターもしくは代表クエリアが MLD 離脱メッセージを受信した際に、マルチキャストグループにほかの受信ホストが存在するかどうかを確認する目的で送信されます。応答がない場合は、学習したマルチキャストグループのエントリーが削除されます。 |
| ルータータイムアウト時間 | 学習済みルーターポートのタイムアウト時間を 120～1200（秒）の範囲で入力します。（デフォルト：250 秒）<br>ルータータイムアウト時間を経過するまでの間に MLD クエリーパケットを受信しなかった場合、学習したルーターポートのエントリーが削除されます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| **マルチキャストグループエントリ** | |
|---|---|
| VLAN ID | VLAN ID が表示されます。 |
| マルチキャストグループアドレス | マルチキャストグループの MAC アドレスが表示されます。 |
| メンバーポート | マルチキャストグループのメンバーとして登録されているポートが表示されます。 |

## 6.9.2. ルーターポート

ルーターポートは、マルチキャストルーターが存在するポートです。MLD スヌーピング機能では MLD クエリーを受信して自動学習しますが、スタティックのエントリーを登録することもできます。


| ルーターポートテーブル | |
|---|---|
| VLAN ID | VLAN ID が表示されます。 |
| スタティックルーターポート | マルチキャストルーターに接続されるポートが表示されます。 |
| ダイナミックルーターポート | 学習されたダイナミックルーターポートが表示されます。 |
| アクション | ［修正］ボタンをクリックすると、ルーターポートの設定を変更できます。 |

ルーターポートテーブルの［修正］ボタンをクリックすると、エントリーの設定を変更できます。


| ルーターポート設定 | |
|---|---|
| VLAN ID | VLAN ID が表示されます。この ID で、ルーターポートの設定を変更する VLAN を識別します。 |

| スタティックルーターポート |
|---|
| マルチキャストルーターに接続されるポートを選択します。<br>［全て］ボタンをクリックすると、すべてのポートが選択されます。 |
| ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［元に戻す］ボタンをクリックすると、すべての選択がリセットされます。 |

# 6.10. マルチキャスト VLAN

マルチキャスト VLAN 機能は、マルチキャスト通信サービスが存在するネットワークから、ほかのネットワークに対して片方向のマルチキャスト通信を提供する機能です。

たとえば、スイッチがマルチキャスト通信をメインとするクローズドネットワーク（カメラネットワークなど）と社内 LAN で共用されている場合、通常は両者のネットワークが完全に分離されているため、相互に通信することはできません。このような場合に、マルチキャスト VLAN という特殊な VLAN を登録し、配信側ポート（ソースポート）と受信側ポート（レシーバーポート）を指定することで、特定のマルチキャスト通信だけで動作する、ネットワーク跨ぎのマルチキャスト通信経路を確立することができます。この例では、業務用 PC からカメラネットワークの映像を確認する、といったことが実現できます。

## 6.10.1. 基本設定

［基本設定］ページから、マルチキャスト VLAN 機能の設定やマルチキャスト VLAN の作成、割り当てを行うことができます。


| マルチキャスト基本設定 | |
|---|---|
| IPv4 マルチキャスト機能 | IPv4 マルチキャスト VLAN の状態（有効／無効）を選択します。 |
| IPv6 マルチキャスト機能 | IPv6 マルチキャスト VLAN の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

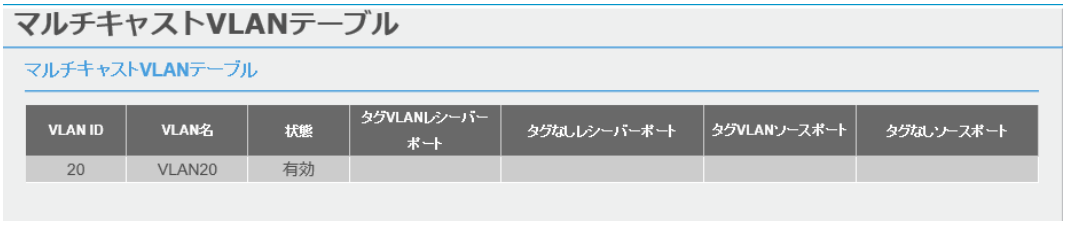
| マルチキャスト VLAN 設定 | |
|---|---|
| VLAN ID | 追加または削除するマルチキャスト VLAN ID を 2～4094 の範囲で入力します。 |
| VLAN 名 | 追加または削除するマルチキャスト VLAN の名前を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、［VLAN ID］と［VLAN 名］に入力 |

| | |
|---|---|
| | した VLAN がマルチキャスト VLAN エントリーに追加されます。 |
| ［削除］ボタン | ［VLAN ID］を入力して［削除］ボタンをクリックすると、対象となるマルチキャスト VLAN エントリーが削除されます。 |

| マルチキャスト VLAN ポート | |
|---|---|
| VLAN ID | マルチキャスト VLAN の ID が表示されます。 |
| VLAN 名 | マルチキャスト VLAN の名前が表示されます。 |
| 状態 | マルチキャスト VLAN の状態（有効／無効）を選択します。 |
| レシーバーポート | ［編集］ボタンをクリックすると、［マルチキャスト VLAN レシーバーポート設定］で、レシーバーポートに使用するポート番号を選択できます。 |
| ソースポート | ［編集］ボタンをクリックすると、［マルチキャスト VLAN ソースポート設定］で、ソースポートに使用するポート番号を選択できます。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.10.2. テーブル

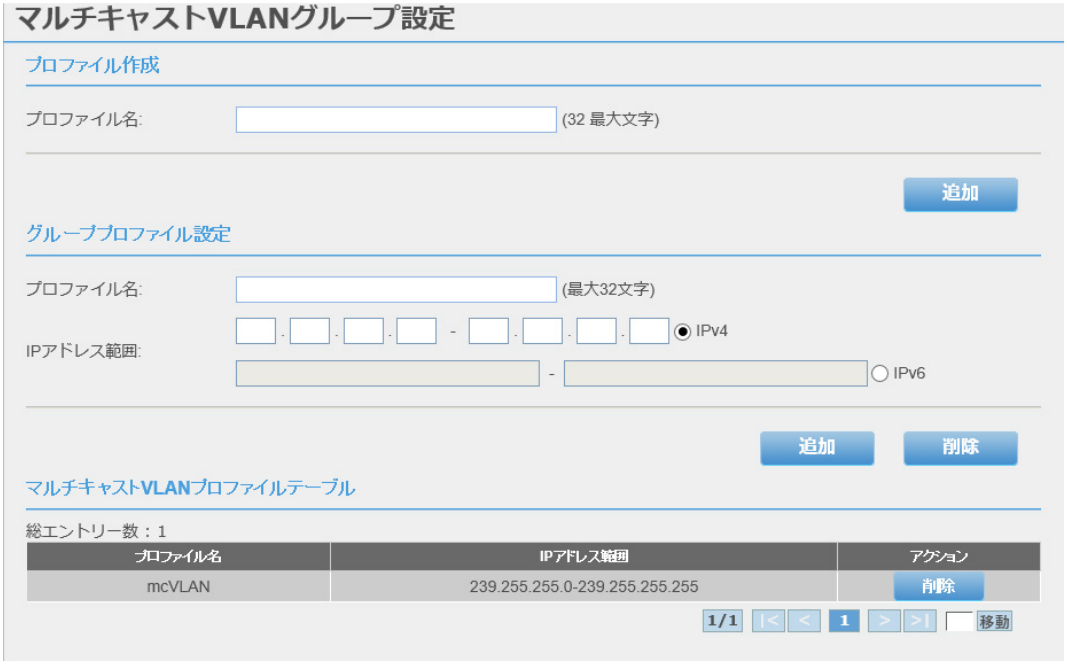
［テーブル］ページから、マルチキャスト VLAN の割り当てポートを確認することができます。




| マルチキャスト VLAN テーブル | |
|---|---|
| VLAN ID | マルチキャスト VLAN の ID が表示されます。 |
| VLAN 名 | マルチキャスト VLAN の名前が表示されます。 |
| 状態 | マルチキャスト VLAN の状態（有効／無効）が表示されます。 |
| タグ VLAN レシーバーポート | マルチキャスト VLAN に設定したタグ VLAN レシーバーポートが表示されます。 |
| タグなしレシーバーポート | マルチキャスト VLAN に設定したタグなしレシーバーポートが表示されます。 |
| タグ VLAN ソースポート | マルチキャスト VLAN に設定したタグ VLAN ソースポートが表示されます。 |
| タグなしソースポート | マルチキャスト VLAN に設定したタグなしソースポートが表示されます。 |

## 6.10.3. グループ

［グループ］ページで、マルチキャスト VLAN 機能で配信するマルチキャスト通信のプロファイルを設定します。




| プロファイル作成 | |
|---|---|
| プロファイル名 | マルチキャスト VLAN のプロファイルの名前を 32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、マルチキャスト VLAN グループが追加されます。 |

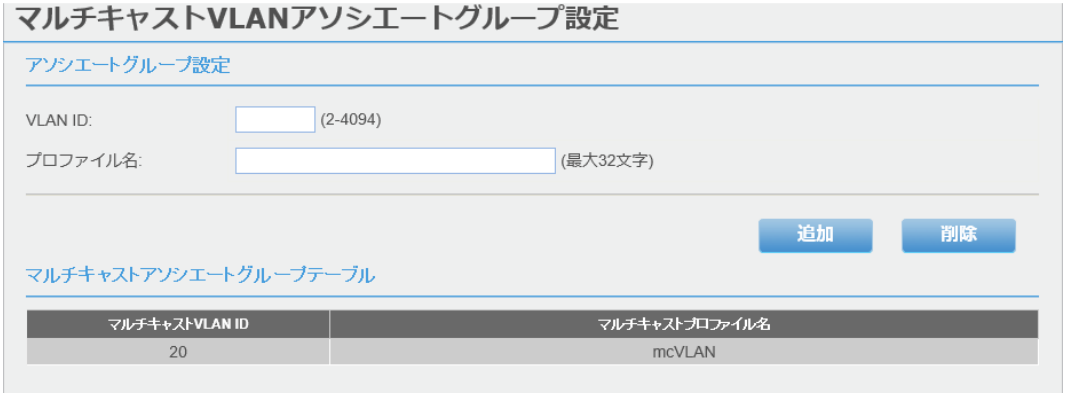
| グループプロファイル設定 | |
|---|---|
| プロファイル名 | 作成済みのマルチキャスト VLAN のプロファイル名を、32 文字以内で入力します。 |
| IP アドレス範囲 | ［IPv4］または［IPv6］を選択し、追加または削除するマルチキャストグループの IP アドレスの範囲を入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、［IP アドレス範囲］に入力したマルチキャストグループが、［プロファイル名］に入力したマルチキャスト VLAN のプロファイルに追加されます。 |
| ［削除］ボタン | ［削除］ボタンをクリックすると、［IP アドレス範囲］に入力したマルチキャストグループが、［プロファイル名］に入力したマルチキャスト VLAN のプロファイルから削除されます。 |

| マルチキャスト VLAN プロファイルテーブル | |
|---|---|
| プロファイル名 | 作成したマルチキャスト VLAN のプロファイルの名前が表示されます。 |

| | |
|---|---|
| IP アドレス範囲 | マルチキャスト VLAN に追加したマルチキャストグループの IP アドレスの範囲が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、マルチキャスト VLAN のプロファイルが削除されます。 |

## 6.10.4. アソシエートグループ

［アソシエートグループ］ページで、マルチキャスト VLAN に対して［グループ］ページで作成したプロファイルを割り当てます。




| アソシエートグループ設定 | |
|---|---|
| VLAN ID | マルチキャスト VLAN のプロファイルを追加または削除する VLAN ID を、2～4094 の範囲で入力します。 |
| プロファイル名 | 追加または削除するマルチキャスト VLAN のプロファイルの名前を、32 文字以内で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、マルチキャスト VLAN のプロファイルがマルチキャスト VLAN ID に関連付けられて登録されます。 |
| ［削除］ボタン | ［削除］ボタンをクリックすると、マルチキャスト VLAN のプロファイルが、マルチキャスト VLAN ID から削除されます。 |

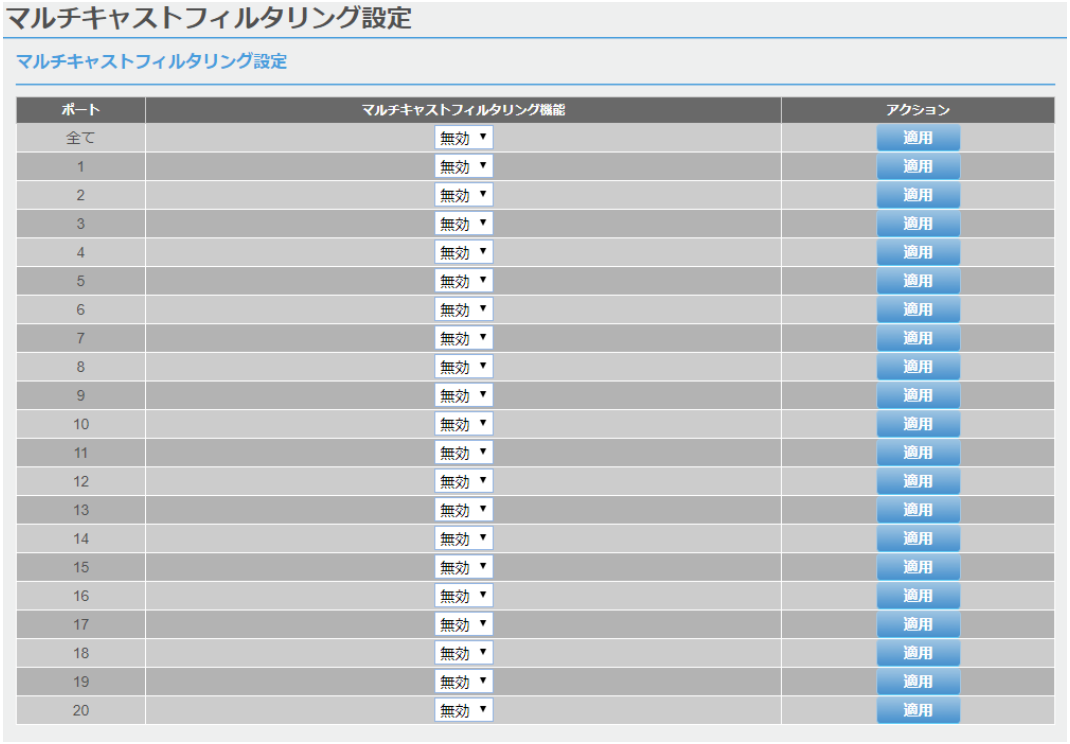
| マルチキャストアソシエートグループテーブル | |
|---|---|
| VLAN ID | マルチキャスト VLAN ID が表示されます。 |
| マルチキャストプロファイル名 | マルチキャスト VLAN ID に関連付けたマルチキャスト VLAN のプロファイルの名前が表示されます。 |

# 6.11. マルチキャストフィルタリング

［マルチキャストフィルタリング］ページで、IP マルチキャスト通信のフィルタリング制御を行うマルチキャストフィルタリング機能を設定します。

IP マルチキャスト通信は、送信ホストからマルチキャストルーターを経由し、末端のマルチキャストルーター（ラストホップルーター）でネットワーク内のノードに配信されます。マルチキャストフィルタリング機能を使用しない場合、スイッチはラストホップルーターからのマルチキャストトラフィックを全ポートに配信するため、ネットワーク帯域を消費します。

マルチキャストフィルタリング機能を使用すると、スイッチはマルチキャストテーブルを作成し、IGMP スヌーピング機能などと組み合わせてマルチキャストルーターやノードが存在するポートを学習します。IP マルチキャスト通信の転送はマルチキャストテーブルに登録されたポートに対して行われるため、トラフィックが効率化されます。




| マルチキャストフィルタリング設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| マルチキャストフィルタリング機能 | マルチキャストフィルタリング機能の状態（有効／無効）を選択します。［全て］から、すべてのポートをまとめて設定できます。<br>・ 無効：マルチキャストテーブルを参照しない<br>・ 有効：マルチキャストテーブルを参照して転送する |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

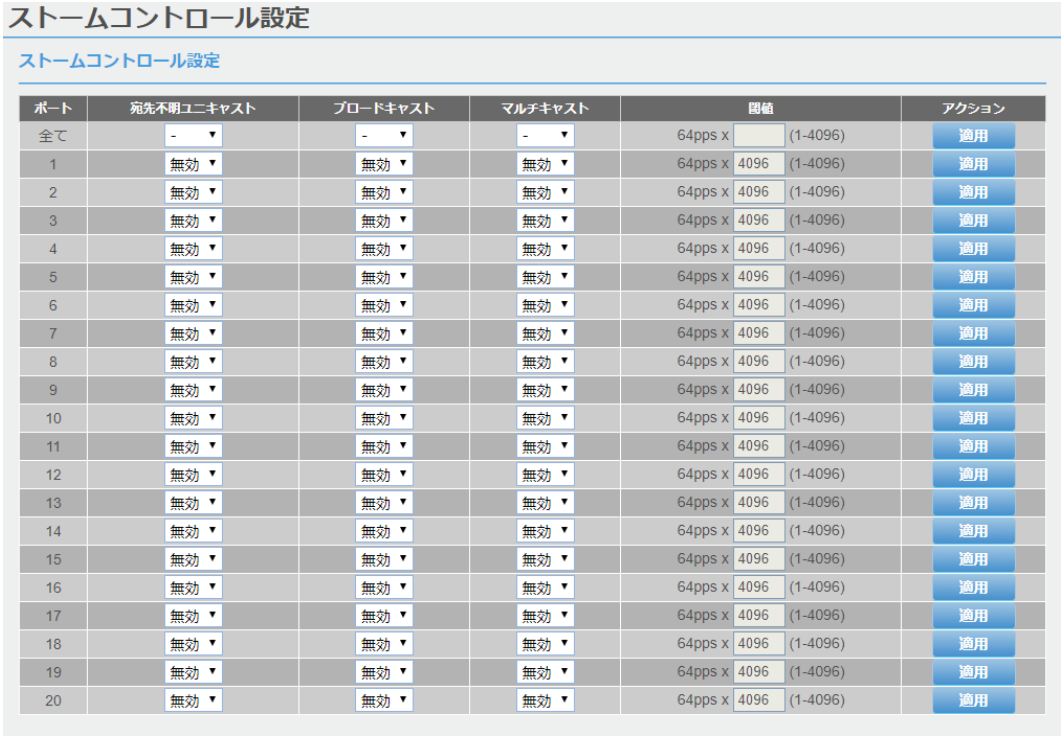
# 6.12. 帯域制御

帯域制御機能は、大量のトラフィックが発生した場合にスイッチやネットワークへの影響を最小限にするため、トラフィック制限値を設定して、しきい値を超えた場合に通信をブロックする機能です。

スイッチを含めたネットワーク全体に対して負荷がかかる Destination Lookup Failure（以後、DLF）、ブロードキャスト、マルチキャストに対して制限を行うストームコントロール機能と、ネットワーク全体の帯域を考慮してポート単位のトラフィック量を制限する入出力レート制限機能に大きく分類されます。

## 6.12.1. ストームコントロール

［ストームコントロール］ページで、DLF、ブロードキャスト、およびマルチキャストパケットの受信を制御できます。各パケットタイプで構成したしきい値を超えるトラフィックストームが検出されると、パケットはトラフィックストームが抑制されるまで破棄されます。




| ストームコントロール設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| 宛先不明ユニキャスト | DLF のストームコントロールの状態（有効／無効）を選択します。<br>Note: スイッチはパケットを受信するとフォワーディングデータベース（以後、FDB）から受信パケットの宛先 MAC アドレスを検索し、FDB に登録されているポートにパケットを転送します。FDB で宛先 MAC アドレスが見つからない場合は DLF であることを示します。 |

| | |
|---|---|
| ブロードキャスト | ブロードキャストストームコントロールの状態（有効／無効）を選択します。 |
| マルチキャスト | マルチキャストストームコントロールの状態（有効／無効）を選択します。 |
| 閾値 | デバイスが受信および転送する DLF、ブロードキャスト、およびマルチキャストのパケット量について、制限するしきい値の pps（1 秒あたりのパケット数）を 1～4096 の範囲で入力します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.12.2. 入力レート制限

［入力レート制限］ページで、各ポートでの入力トラフィックでの帯域制限を設定します。制限帯域を超えたトラフィックは破棄されます。


| 入力レート制限設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| 制限帯域 | 入力レート制限の値を入力します。 |
| 状態 | 入力レート制限の状態（有効／無効）を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.12.3. 出力レート制限

［出力レート制限］ページで、各ポートでの出力トラフィックでの帯域制限を設定します。制限帯域を超えたトラフィックは破棄されます。


| 出力レート制限設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| 制限帯域 | 出力レート制限の値を入力します。<br>**Note:** GE ポートの最大速度は、1000000 Kbps（64 Kbps×15625＝1000000 Kbps）です。 |
| 状態 | 出力レート制限の状態（有効／無効）を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

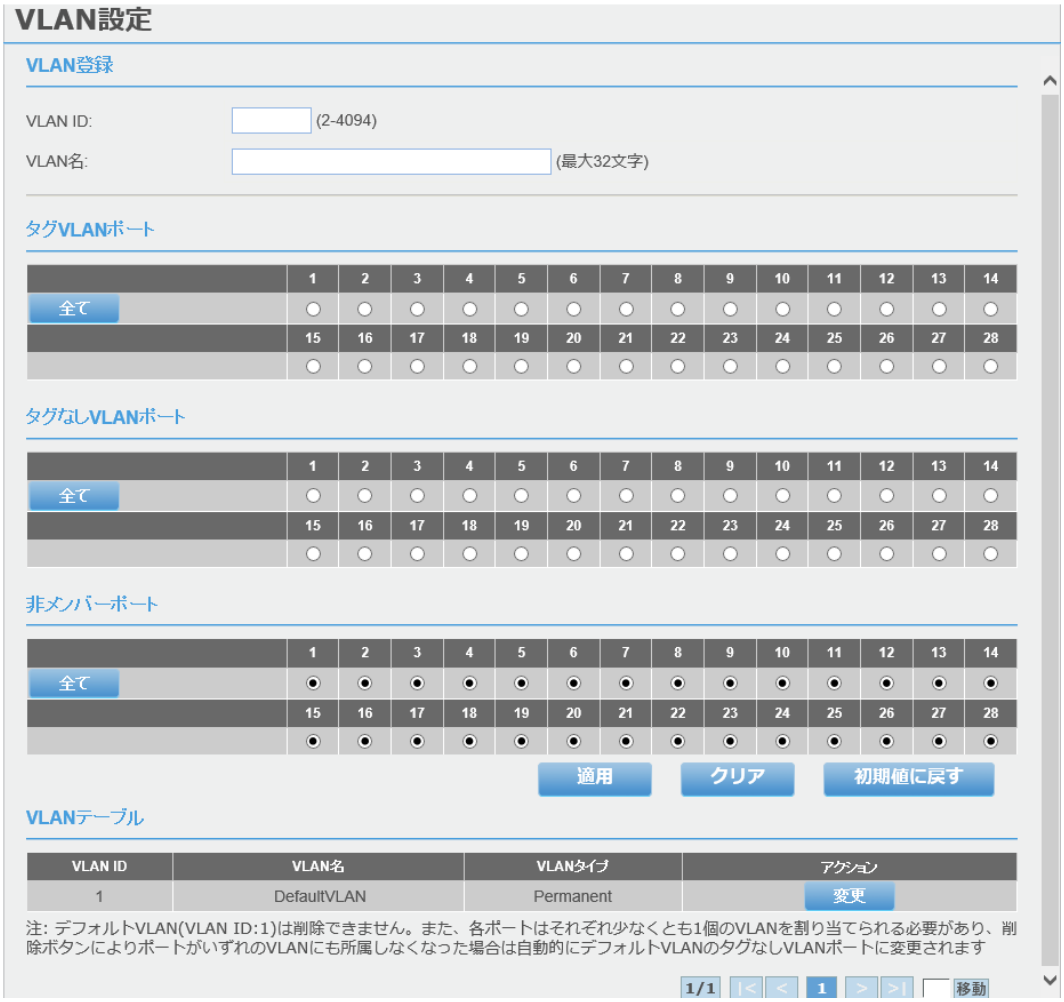
# 6.13. VLAN

VLAN を使用すると、ネットワークを論理的に異なるブロードキャストドメインに分割することができます。ネットワークを細分化することで、帯域を効率よく使用することができます。

本スイッチではデフォルトで、すべてのポートを「DefaultVLAN」という名前の VLAN にタグなしポートとして割り当てます。この「DefaltVLAN」の VLAN ID は「1」です。

## 6.13.1. VLAN 設定

［VLAN 設定］ページで、新しい VLAN を作成し、ポートに割り当てることができます。




| VLAN 登録 | |
|---|---|
| VLAN ID | VLAN ID を 2～4094 の範囲で入力します。<br>VLAN ID は、802.1Q により定められた VLAN 識別子です。VLAN ID は 12 ビットの長さで、4094 個の一意の VLAN を識別できます。<br>なお、スイッチは VLAN ID が 1 のデフォルト VLAN が登録されており、この VLAN を削除することはできません。 |
| VLAN 名 | VLAN の名前を 32 文字以内で入力します。 |

| タグ VLAN ポート |
| --- |
| タグ VLAN ポートは、複数の VLAN のメンバーとして含めることができます。タグ VLAN ポートと接続するコンピューターやそのほかのエッジデバイスは、デバイスのインターフェースでタグ VLAN を有効に設定しないと通信が成立しません。<br>［全て］ボタンをクリックすると、すべてのポートが選択されます。 |

| タグなし VLAN ポート |
| --- |
| タグなし VLAN ポートは、コンピューター、ラップトップ、プリンターなどのエッジデバイス（VLAN 非認識）を、指定された VLAN に接続するために使用されます。<br>一つのポートに複数のタグなし VLAN が設定されている場合、受信フレームはポートに設定した PVID の値と同じ VLAN として処理されます。PVID 設定は、［VLAN］＞［ポート設定］ページで設定します。<br>［全て］ボタンをクリックすると、すべてのポートが選択されます。 |

| 非メンバーポート |
| --- |
| VLAN のメンバーから除外するポートを指定します。<br>［全て］ボタンをクリックすると、すべてのポートが選択されます。 |

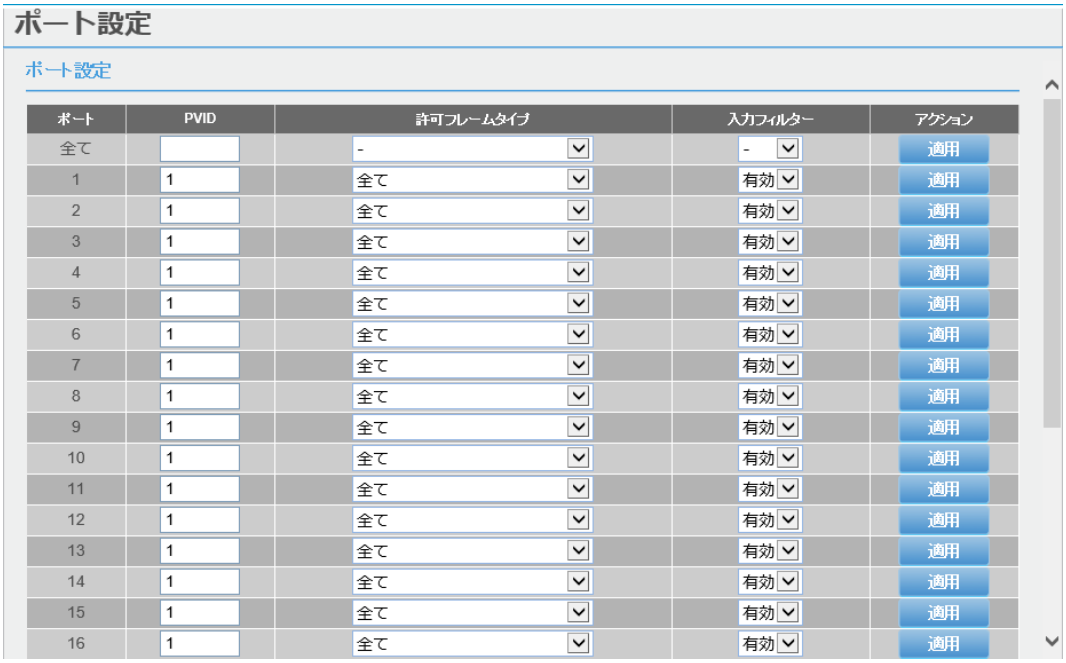
［適用］ボタンをクリックすると、VLAN が作成されます。
［クリア］ボタンをクリックすると、ポートの選択がクリアされます。
［初期値に戻す］ボタンをクリックすると、初期値に戻ります。

| VLAN テーブル | |
| --- | --- |
| VLAN ID | 登録されている VLAN の一覧が表示されます。マルチキャスト VLAN で作成された VLAN も含まれます。 |
| VLAN 名 | 各 VLAN の VLAN 名が表示されます。 |
| VLAN タイプ | 各 VLAN の VLAN タイプが表示されます。<br>・ Permanent：デフォルトの VLAN で、削除することはできません<br>・ Static：手動で作成した VLAN |
| アクション | ［修正］ボタンをクリックすると、VLAN の設定を変更できます。VLAN の名前を変更したり、各ポートをタグ VLAN ポート、タグなし VLAN ポート、または非メンバーポートに変更したりできます。<br>［削除］ボタンをクリックすると、VLAN が削除されます。マルチキャスト VLAN として作成された VLAN は、この画面では削除できません。 |

## 6.13.2. ポート設定

［ポート設定］ページで、PVID などフレーム受信時の VLAN の処理に関する設定を行います。
このページでは、主にポートの PVID の設定を行います。PVID は、複数のタグなし VLAN がポートに割り当

てられている場合に、タグなしのフレームを受信した際の VLAN ID を示します。

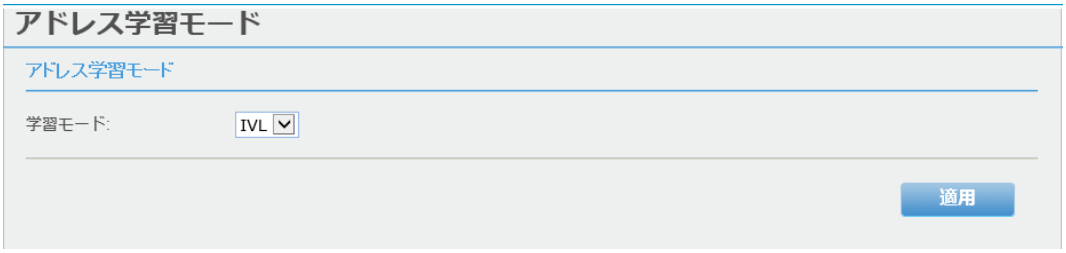



| ポート設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| PVID | 対象ポートの PVID を入力します。 |
| 許可フレームタイプ | 受け入れ可能なフレームのタイプを選択します。<br>・ 全て：<br>すべてのフレームを受け入れ可能です。<br>・ タグあり：<br>タグ付きフレームのみ受け入れ可能です。タグなしフレームは破棄されます。<br>・ タグなし及び優先度タグ付き：<br>タグなしフレームと、802.1p などの優先度情報のみのタグ付きフレームを受け入れ可能です。 |
| 入力フィルター | 入力フィルタリングの状態（有効／無効）を選択します。<br>Note: 音声 VLAN で自動検知機能を有効にするには、VLAN の入力フィルタリングを無効にする必要があります。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.13.3. アドレス学習モード

［アドレス学習］ページで、スイッチ内部の MAC アドレス学習テーブルの動作モードについて設定します。一般的なネットワークでは、デフォルト設定である IVL を使用してください。SVL は、例えば複数のタグなし VLAN が登録されているポートがあり、そのポートで受信したタグなしフレームと送信するタグなしフレ

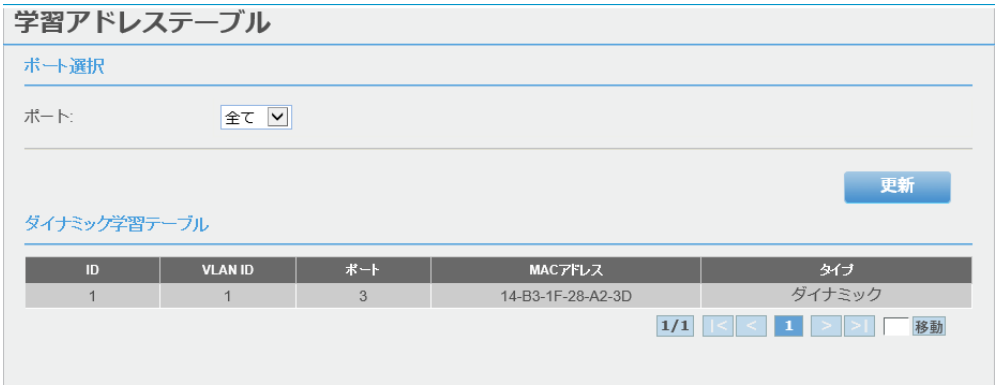
ームで VLAN が異なる（非対称 VLAN と呼ばれる構成）ような、特殊ネットワーク環境下で用いられます。




| アドレス学習モード | |
|---|---|
| 学習モード | スイッチを以下のいずれかの学習モードに構成できます。<br>・ IVL：<br>VLAN 単位で独立した MAC アドレス学習テーブルを持つモードです。ネットワークで非対称 VLAN 構成などの要件がなければ、IVL の使用を推奨します。<br>・ SVL：<br>VLAN によらず共通の MAC アドレス学習テーブルを持つモードです。非対称 VLAN の構成を行う場合に使用します。通常は IVL を使用してください。<br>Note: 学習モードを切り替えると、MAC アドレス学習テーブルやマルチキャストテーブルなど、各種テーブルの情報がクリアされます。また、IVL モードから SVL モードに切り替える前に、音声 VLAN を無効にする必要があります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.13.4. 学習アドレステーブル

［学習アドレステーブル］ページで、スイッチが学習した MAC アドレスとポート、VLAN の情報が表示されます。




| ポート選択 | |
|---|---|
| ポート | ポート番号を選択します。 |

| | |
|---|---|
| ［更新］ボタン | ［更新］ボタンをクリックすると、選択したポート番号のダイナミック学習テーブルが更新されます。 |

| ダイナミック学習テーブル | |
|---|---|
| ID | 学習アドレステーブルの ID が表示されます。 |
| VLAN ID | 該当する VLAN ID が表示されます。<br>学習モードが SVL の場合は［N/A］と表示されます。 |
| ポート | ポート番号が表示されます。 |
| MAC アドレス | MAC アドレスが表示されます。 |
| タイプ | 学習アドレステーブルのタイプが表示されます。 |

## 6.13.5. VLAN 情報

［VLAN 情報］ページでは、登録した VLAN と割り当てポートの情報が表示されます。


| VLAN データベース | |
|---|---|
| VLAN ID | VLAN ID が表示されます。 |
| VLAN 名 | VLAN 名が表示されます。 |
| VLAN FDB ID | MAC アドレス学習テーブル上で登録される VLAN ID が表示されます。<br>学習モードが SVL の場合は、［N/A］と表示されます。 |
| メンバーポート | 各 VLAN のメンバーポートが表示されます。 |
| タグなしポート | 各 VLAN のタグなしポートが表示されます。 |
| 状態 | 各 VLAN の状態が表示されます。 |

# 6.14. マンションモード

［マンションモード］ページでは、マンションモード（中継パス制限機能）の設定を行います。

マンションモードは、特定のポート（送信元ポート）からのトラフィックを転送するポート（転送先ポート）を限定する機能です。
たとえば、各ポートに接続する端末はそれぞれアップリンクポートとの通信を行いたいが、端末間での通信は禁止したい、といったネットワーク要件を簡単に実現することができます。


| マンションモード設定 | |
|---|---|
| マンションモード | マンションモードの状態を選択します。<br>・ 有効：マンションモードの設定を有効にする<br>・ 無効：マンションモードの設定を無効にする |

| ポート選択 | |
|---|---|
| 送信元ポート | 対象となる送信元ポートを選択します。 |
| 転送先ポート | 送信元ポートからのトラフィックを転送するポートを選択します。 |

| マンションモード転送テーブル | |
|---|---|
| ポート | 送信元ポートが表示されます。 |
| 転送先ポート | 送信元ポートに対して指定した転送先ポートが表示されます。 |

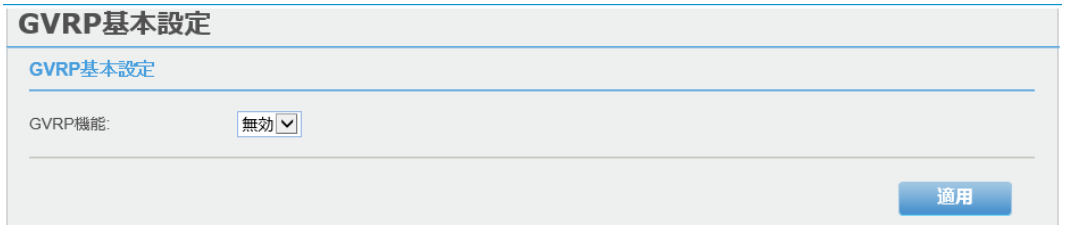
# 6.15. GVRP

GARP VLAN Registration Protocol（以後、GVRP）を有効にすると、GARP を使用してネットワークデバイス間で VLAN 情報を共有し、自動的にその情報を使用して新規の VLAN の作成やポート割り当てなどを行うことができます。これにより、複数のスイッチにまたがる VLAN を簡単に管理できます。

GVRP が正常に動作するには、送信側と受信側ともに GVRP に対応している必要があります。

## 6.15.1. 基本設定

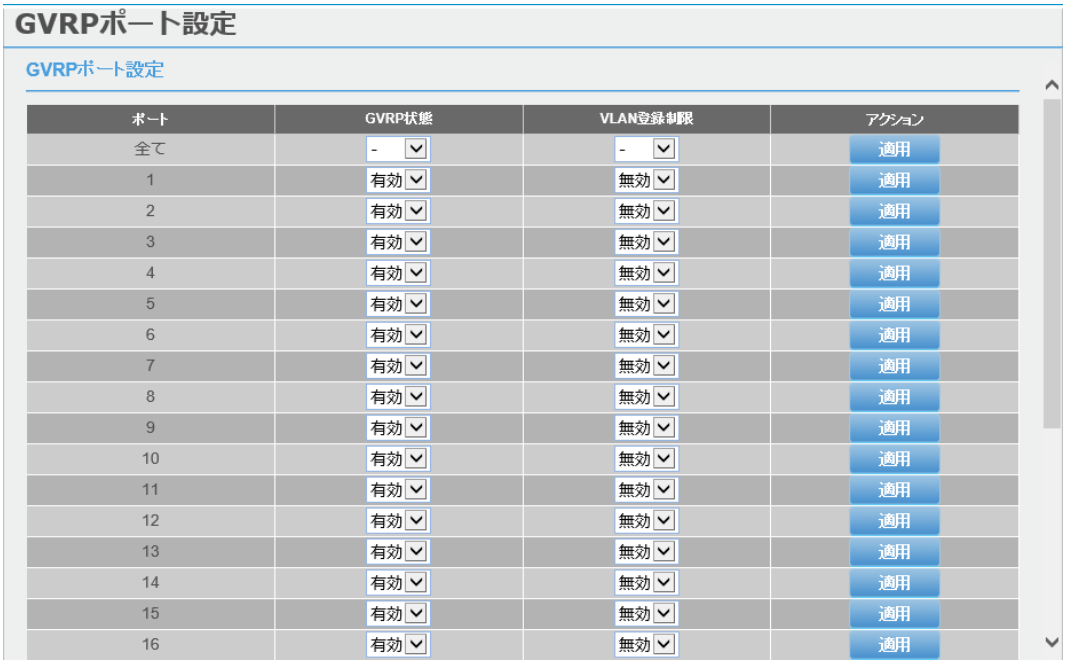
［基本設定］ページでは、GVRP 機能の設定を行います。




| GVRP 基本設定 | |
|---|---|
| GVRP 機能 | GVRP の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.15.2. ポート設定

［ポート設定］ページで、各ポートでの GVRP の有効／無効の設定、および VLAN 登録制限の有無を選択できます。



| GVRP ポート設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| GVRP 状態 | 各ポートの GVRP の状態を選択します。 |
| VLAN 登録制限 | 各ポートの VLAN 登録制限の状態を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.15.3. タイマー設定

［タイマー設定］ページで、各ポートに対して GARP の Join 時間、Leave 時間、Leave-All 時間を設定できます。

Note: GARP Leave 時間は「GARP Join タイマー×2＋10」より大きい必要があります。
GARP Leave-All 時間は「GARP Leave タイマー＋10」より大きい必要があります。

| GVRP タイマー設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| Join 時間<br>(10～1073741810)ミリ秒 | GARP Join タイマーを 10～1073741810（ミリ秒）の範囲で入力します。 |
| Leave-All 時間<br>(30～2147483630)ミリ秒 | GARP Leave-All タイマーを 30～2147483630（ミリ秒）の範囲で入力します。GARP Leave-All タイマーは以下の式に従い、GVRP Leave タイマーに応じて設定する必要があります。<br>GARP Leave-All タイマー＞（GARP Leave タイマー＋10） |
| Leave 時間<br>(40～2147483640)ミリ秒 | GARP Leave タイマーを 40～2147483640（ミリ秒）の範囲で入力します。GARP Leave タイマーは以下の式に従い、GVRP Join タイマーに応じて設定する必要があります。<br>GARP Leave タイマー≧（GARP Join タイマー×2＋10） |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

Note: ネットワークデバイス間の互換性を確保するには、ネットワークに参加しているすべての GVRP デバイスで、GARP Join タイマー、GARP Leave タイマー、GARP Leave-All タイマーに同じ値を設定した構成にする必要があります。

# 6.16. 音声 VLAN

音声 VLAN 機能を使用すると、登録された音声デバイスからの音声トラフィックを検知し、ポートが自動的に個別の VLAN を割り当てます。また、スイッチは音声トラフィックに対して Class of Service（以後、CoS）パラメーターを自動的に割り当て、音声トラフィックを制御することができます。

IP 電話などの音声デバイスの中には、音声用トラフィックを特定の VLAN タグつきフレームで、それ以外のトラフィックをタグなしフレームで送信する機能を持つものがあり、直結するスイッチから受信する LLDP フレームの LLDP-MED 情報などからタグつきフレームで送信する VLAN を決定しています。音声 VLAN 機能は、そのような音声デバイスを接続する際に使用します。

## 6.16.1. 設定

［設定］ページでは、音声 VLAN 機能や適用する VLAN、自動検知ポートなどを設定します。

自動検知ポートは、音声 VLAN 機能で音声デバイスを検知するポートです。検知された音声デバイスのトラフィックは、指定した音声 VLAN のフレームとして処理されます。
音声 VLAN に指定した VLAN が、すでにポートにタグ VLAN、またはタグなし VLAN として割り当てられている場合、そのポートを自動検知ポートにすることはできません。

また、学習モードが SVL の場合は、音声 VLAN を有効にすることはできません。


| 音声 VLAN | |
|---|---|
| 音声 VLAN 機能 | 音声 VLAN の状態（有効／無効）を選択します。（デフォルト：無効）<br>有効にすると、［音声 VLAN 設定］と［音声 VLAN テーブル］を構成できます。 |

| 音声 VLAN 設定 | |
|---|---|
| VLAN ID | 音声 VLAN に指定する VLAN ID を登録します。<br>Note: 音声 VLAN に指定する VLAN は、事前に［VLAN］ページで作成する必要があります。 |
| エージング時間 | ポートが音声 VLAN から除外されるエージング時間を 1～120（時間）の範囲で入力します。 |
| CoS 値 | 自動検知機能が有効な音声 VLAN のポートにおいて、受信した音声トラフィックに割り当てられる CoS 値を選択します。<br>Note: CoS 値による優先制御を有効にするには、QoS 機能が有効になっている必要があります。 |

［適用］ボタンをクリックすると、変更が適用されます。

| 音声 VLAN テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 自動検知 | 各ポートでの音声 VLAN の自動検知機能の状態を選択します。<br>［全て］から、すべてのポートをまとめて設定できます。<br>・ 有効：音声 VLAN の自動検知機能を有効にする<br>・ 無効：音声 VLAN の自動検知機能を無効にする<br>Note: 音声 VLAN がタグ VLAN またはタグなし VLAN で割り当てられているポートは、自動検知機能を有効にすることはできません。また、ポートでの音声 VLAN の自動検知機能を有効にする場合は、VLAN の入力フィルタリングを無効にする必要があります。VLAN の入力フィルタリングは、［VLAN］＞［ポート設定］ページで設定できます。 |
| 状態 | 自動検知ポートの状態が表示されます。<br>・ Static：<br>タグ VLAN またはタグなし VLAN で、音声 VLAN が割り当てられているポートです。自動検知機能を有効にすることはできません。<br>・ Dynamic：自動検知機能が有効で、登録された OUI デバイスから送信されたパケットが検知されているポートです。<br>・ None：<br>自動検知機能が無効なポート、または自動検知機能が有効で、登録された OUI デバイスから送信されたパケットが検知されていないポートです。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.16.2. OUI 登録

［OUI 登録］ページでは、音声 VLAN 機能で識別する音声デバイスの OUI 情報を登録します。

ネットワークデバイスのハードウェアアドレス（MAC アドレス）は、先頭 6 バイトにメーカー固有の識別子である Organizationally Unique Identifier（以後、OUI）が割り当てられています。デバイスの MAC アドレスの先頭 6 バイトが特定の OUI を含むかどうかによって、音声デバイスを絞り込むことができます。


| OUI 登録 | |
|---|---|
| 説明 | メーカーの OUI の説明を 20 文字以内で入力します。 |
| OUI | メーカーの OUI を含む MAC アドレスを入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、OUI エントリーが追加されます。 |

Note: ユーザー定義の OUI は最大 10 個まで指定できます。

| 音声 VLAN OUI テーブル | |
|---|---|
| ID | 手動で作成した OUI エントリーの ID が表示されます。 |
| 説明 | メーカーの OUI の説明が表示されます。 |
| OUI | メーカーの OUI が表示されます。 |
| OUI マスク | OUI マスクは、メーカーの OUI を作成するためにスイッチによって自動的に生成され適用されます。 |
| アクション | ［削除］ボタンをクリックすると、作成した OUI エントリーが削除されます。 |

# 6.17. LLDP

本スイッチでは、Link Layer Discovery Protocol（以後、LLDP）機能をサポートしています。LLDP を使用すると、スイッチと隣接する機器（ネイバー）が相互に LLDP 情報を通知し、ネイバーの情報を収集することができます。

LLDP では、使用する LLDP フレームのデータに TLV と呼ばれる所定の属性情報を加えることでネイバーに情報を通知します。TLV には、装置の基本情報を含んだ基本管理 TLV のほか、IEEE802.1 や IEEE802.3 で定められたネットワーク情報や、LLDP-MED で定められたアプリケーション情報などを含む TLV があり、LLDP を使用する機器はどの内容を通知するかを個別に設定することができます。

## 6.17.1. 設定

［設定］ページでは、LLDP 機能の状態や基本的なパラメーターなどの一般的な設定を行います。また、ポート単位で LLDP 機能の有効／無効や、有効時の動作（受信のみ／送信のみ／送受信）を設定することができます。

LLDP 機能の各パラメーターの調整を行うと LLDP の動作をきめ細かく指定することができますが、大部分のネットワークでは LLDP のパラメーター調整を考慮する必要はありません。LLDP 機能やポートの動作が行われれば、それ以外がデフォルト設定のままでも十分に期待した動作が見込まれます。


| LLDP 設定 | |
|---|---|
| LLDP 機能 | LLDP 機能の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、LLDP 機能の状態に関する設定変更が適用されます。 |

| LLDP 詳細設定 | |
|---|---|
| ファストスタート実行回数 | ファストスタート処理での LLDP フレームの送信回数を 1～10（回）の範囲で入力します。（デフォルト：3 回）<br>ファストスタート処理は、ネイバーが LLDP-MED 対応デバイスであると検知した際に、LLDP-MED 情報を通知するために直ちに LLDP フレームを送信する処理を指します。このとき、ネイバーに確実に LLDP-MED 情報を通知するため、LLDP フレームを複数回送信することができます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、LLDP 詳細設定の項目の設定変更が適用されます。 |

| LLDP パラメーター設定 | |
|---|---|
| ホールド乗数 | ホールド乗数を 2～10 の範囲で入力します。（デフォルト：2）<br>ホールドの乗数は LLDP で通知する情報の有効期限を示す TTL（Time To Live）を決定するために使用され、メッセージ送信間隔との乗算により算出されます。TTL は各 LLDP フレームで通知され、ネイバーは受信してから TTL が経過すると、その LLDP フレームで通知された情報を破棄します。 |
| メッセージ送信間隔 | スイッチが定期的に LLDP フレームを送信する間隔を 5～32768（秒）の範囲で入力します。（デフォルト：30 秒） |
| 再初期化保留時間 | ポートの LLDP 状態が無効になってから再初期化が実行されるまでの保留時間を 1～10（秒）の範囲で入力します。（デフォルト：2 秒） |
| 送信保留時間 | LLDP フレームの最小送信間隔を 1～8192（秒）の範囲で入力します。（デフォルト：2 秒）<br>例えば、定期的な LLDP フレームを送信した直後に通知すべき内容が変更されると、スイッチは直ちに LLDP フレームを発行して新たな情報を通知しようとしますが、送信保留時間が経過するまでは送信を保留します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、LLDP パラメーター設定の各項目の設定変更が適用されます。 |

Note: 設定値は以下の条件を満たす必要があります。
送信保留時間≦（0.25×メッセージ送信間隔）＋メッセージ送信間隔×ホールド乗数＜65535

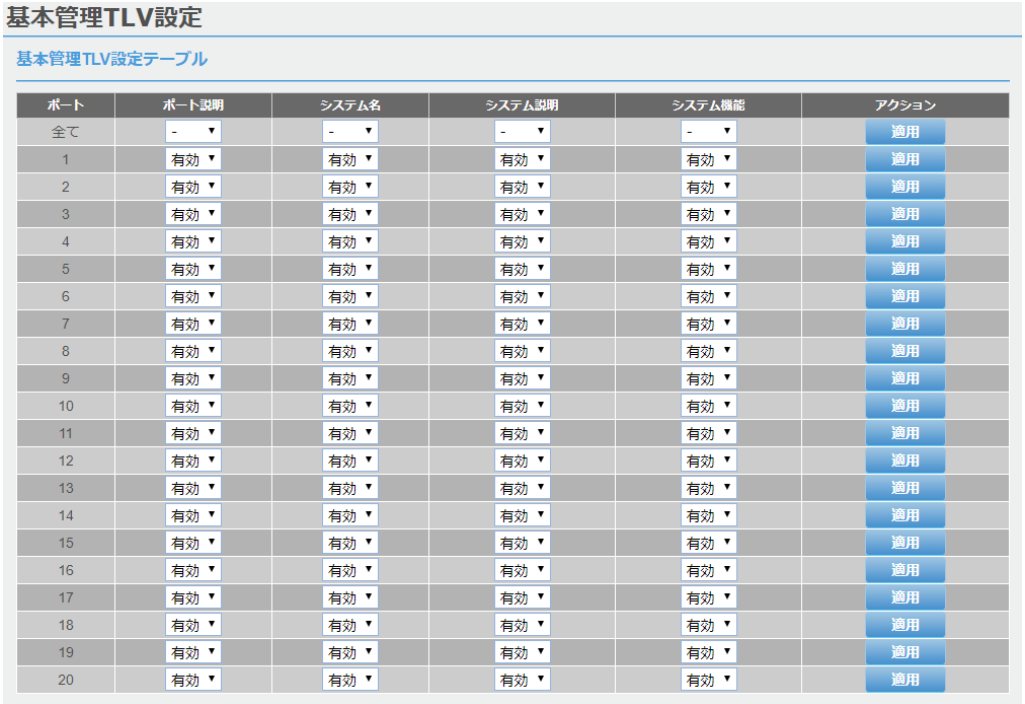
| LLDP システム情報 | |
|---|---|
| シャーシ ID サブタイプ | シャーシ ID のタイプが表示されます。 |
| シャーシ ID | シャーシ ID が表示されます。 |
| システム名 | デバイスのシステム名が表示されます。 |
| システム説明 | デバイスのシステムの説明が表示されます。 |

| LLDP-MED システム情報 | |
|---|---|
| デバイスクラス | デバイス LLDP-MED のデバイスクラスが表示されます。 |
| ハードウェアリビジョン | デバイスのハードウェアリビジョンが表示されます。 |
| ファームウェアリビジョン | デバイスのファームウェアリビジョンが表示されます。 |
| ソフトウェアリビジョン | デバイスのソフトウェアリビジョンが表示されます。 |
| シリアル番号 | デバイスのシリアル番号が表示されます。 |
| 製造者名 | デバイスのメーカー名が表示されます。 |
| 製品型式 | デバイスの製品型式が表示されます。 |
| 資産 ID | デバイスの LLDM-MED アセット ID が表示されます。 |

| LLDP ポート設定テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 状態 | 各ポートでの LLDP 機能の状態を選択します。<br>［全て］から、すべてのポートをまとめて設定できます。<br>・ 無効：<br>LLDP 機能を無効にします。<br>・ 送受信：<br>LLDP フレームを受信してネイバー情報を登録します。また、LLDP 情報を送信します。<br>・ 受信のみ：<br>LLDP フレームを受信してネイバー情報を登録しますが、LLDP 情報を送信しません。<br>・ 送信のみ：<br>LLDP 情報を送信しますが、LLDP フレームを受信してもネイバー情報を登録しません。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.17.2. 基本管理 TLV

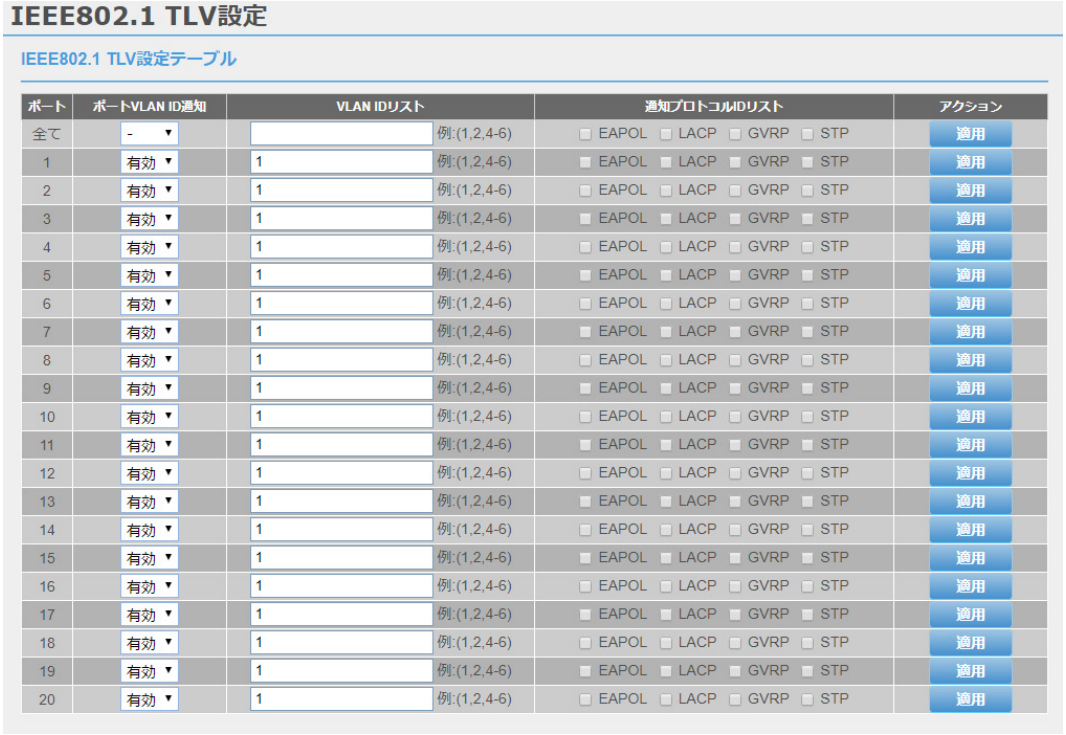
［基本管理 TLV］ページでは、装置の基本情報に関する基本管理 TLV の通知に関する設定を行います。




| 基本管理 TLV 設定テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| ポート説明 | ポート説明情報の通知状態（有効／無効）を選択します。 |
| システム名 | システム名の通知状態（有効／無効）を選択します。 |
| システム説明 | システム説明情報の通知状態（有効／無効）を選択します。 |
| システムサポート機能 | システムサポート機能の通知状態（有効／無効）を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.17.3. IEEE802.1 TLV

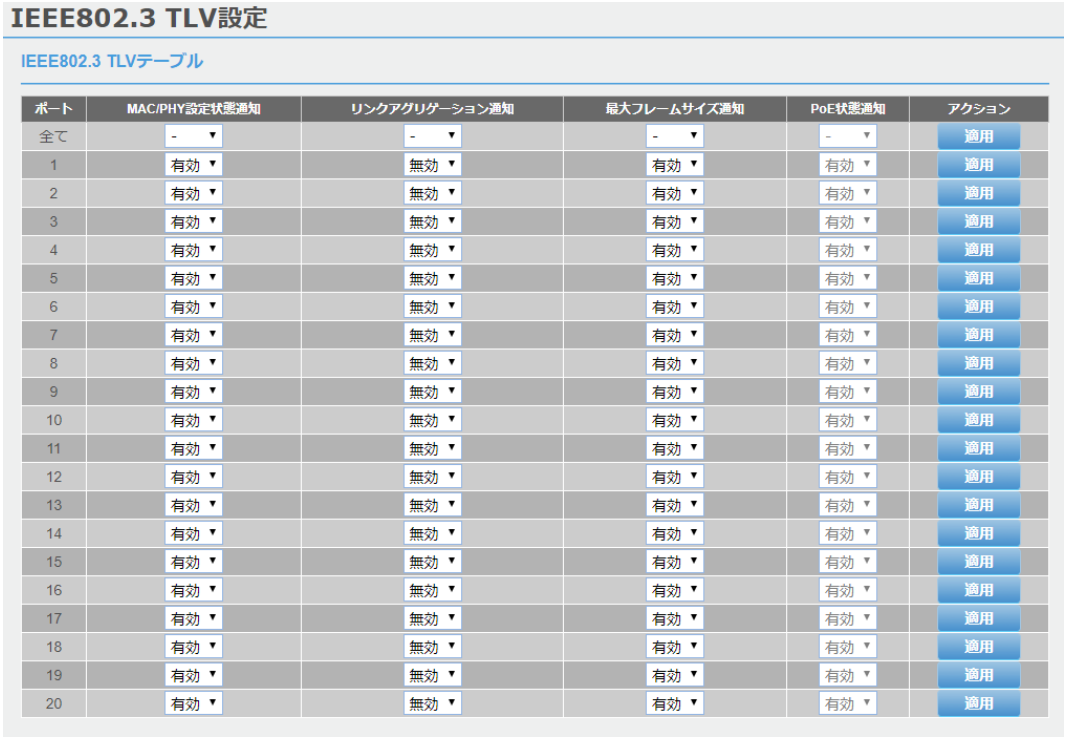
［IEEE802.1 TLV］ページでは、ネットワーク情報に関する IEEE802.1 TLV の通知設定を行います。




| IEEE802.1 TLV 設定テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| ポート VLAN ID 通知 | ポート VLAN ID の通知状態（有効／無効）を選択します。 |
| VLAN ID リスト | 通知する VLAN ID が表示されます。 |
| プロトコル ID | 通知するプロトコル（EAPOL／LACP／GVRP／STP）をそれぞれ選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.17.4. IEEE802.3 TLV

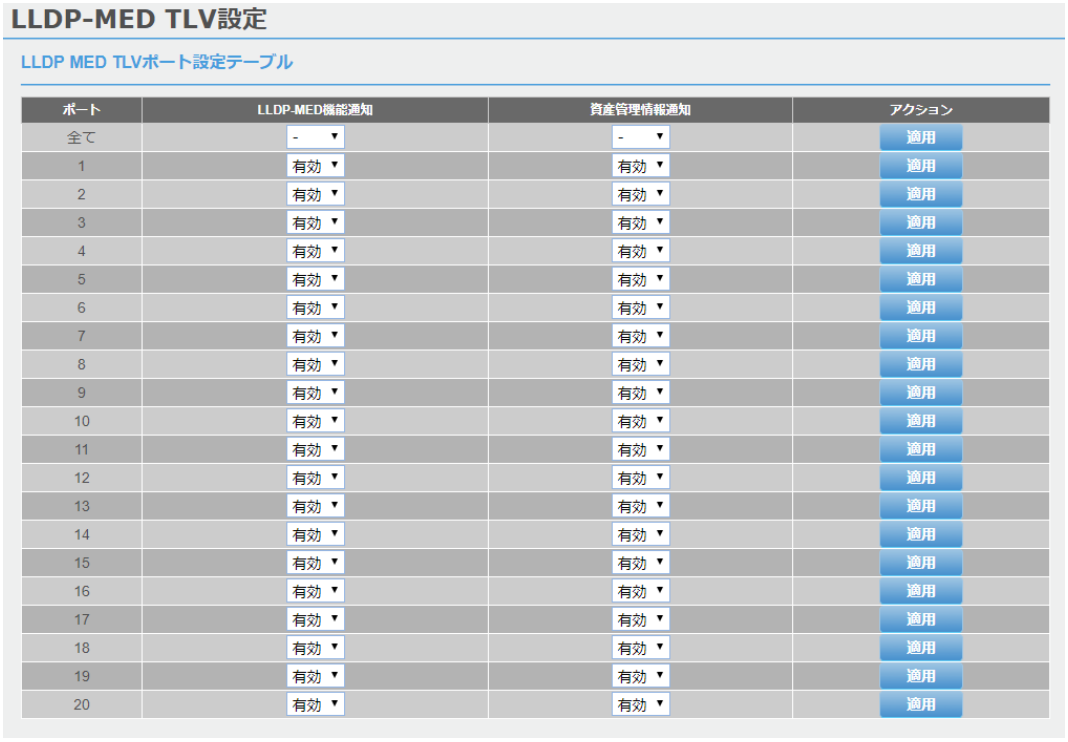
［IEEE802.3 TLV］ページでは、ネットワーク情報に関する IEEE802.3 TLV の通知設定を行います。




| IEEE802.3 TLV 設定テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| MAC/PHY 設定状態通知 | MAC/PHY 設定の通知状態（有効／無効）を選択します。 |
| リンクアグリゲーション通知 | LAG の通知状態（有効／無効）を選択します。 |
| 最大フレームサイズ通知 | 最大フレームサイズの通知状態（有効／無効）を選択します。 |
| PoE 状態通知 | PoE の通知状態（有効／無効）を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.17.5. LLDP-MED TLV

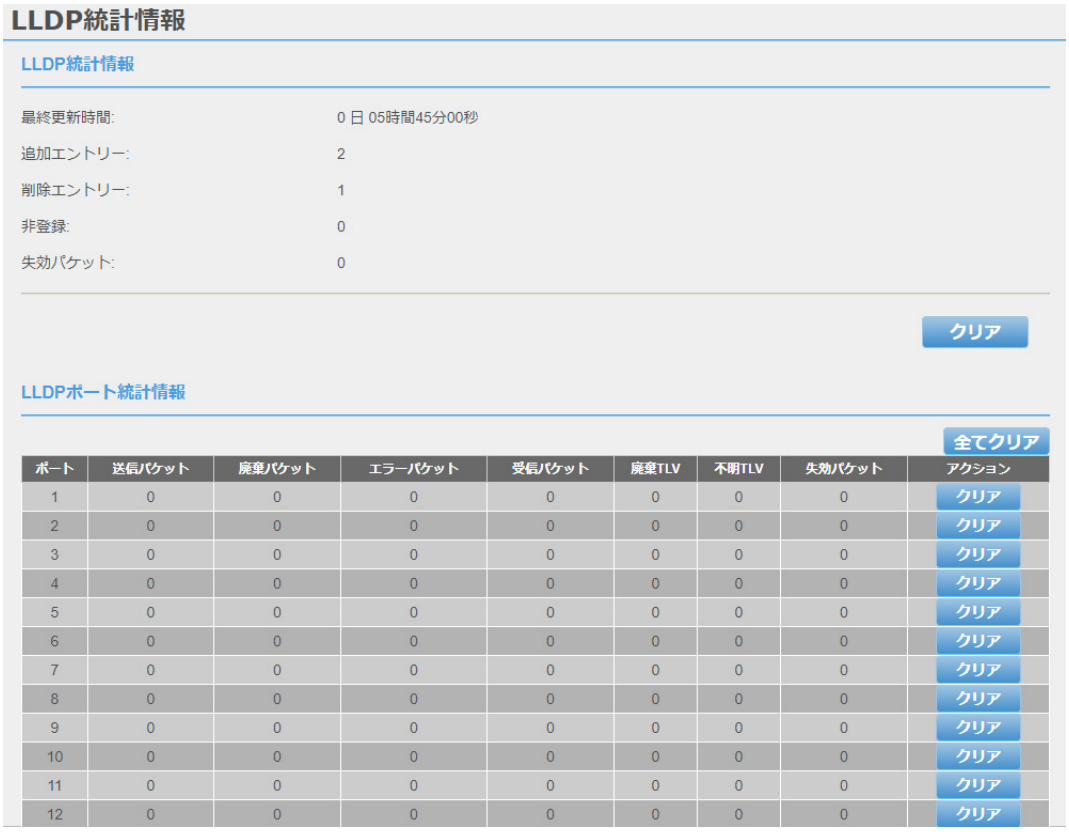
［LLDP-MED TLV］ページでは、アプリケーション情報に関する LLDP-MED TLV の通知設定を行います。




| LLDP-MED TLV ポート設定テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。<br>［全て］から、すべてのポートをまとめて設定できます。 |
| LLDP-MED 機能通知 | LLDP-MED 機能の通知状態（有効／無効）を選択します。 |
| 資産管理情報通知 | 資産管理情報の通知状態（有効／無効）を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 6.17.6. 統計情報

［統計情報］ページでは、すべての LLDP トラフィックの統計情報を確認できます。



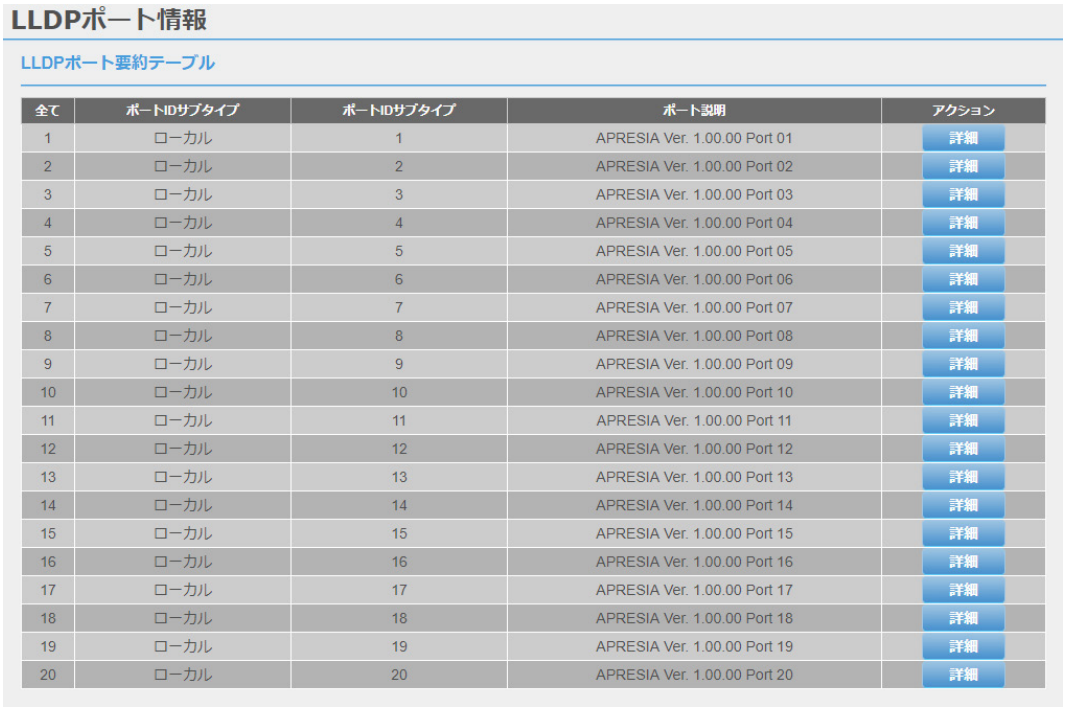

| LLDP 統計情報 | |
|---|---|
| 最終更新時間 | 最新の変更エントリーが追加または削除された日時が表示されます。 |
| 追加エントリー | 追加されたエントリーの数が表示されます。 |
| 削除エントリー | 削除されたエントリーの数が表示されます。 |
| 非登録 | 登録テーブルに空きがないために破棄された LLDP フレームの数が表示されます。 |
| 失効パケット | TTL の失効により削除されたエントリーの数が表示されます。 |
| ［クリア］ボタン | ［クリア］ボタンをクリックすると、［LLDP 統計情報］に表示されている情報がクリアされます。 |

| LLDP ポート統計情報 | |
|---|---|
| ［全てクリア］ボタン | ［全てクリア］ボタンをクリックすると、［LLDP ポート統計情報］に表示されているすべての情報がクリアされます。 |
| ポート | スイッチのポート番号が表示されます。 |
| 送信パケット | ポートから送信した LLDP フレームの数が表示されます。 |
| 廃棄パケット | ポートで受信した LLDP フレームのうち、廃棄された LLDP フレームの数が表示されます。 |

| | |
|---|---|
| エラーパケット | ポートで受信した LLDP フレームのうち、エラーフレームの数が表示されます。 |
| 受信パケット | ポートで受信した LLDP フレームの数が表示されます。 |
| 廃棄 TLV | 各 LLDP フレームで通知された TLV 情報のうち、フォーマットが誤っているために廃棄された TLV の数が表示されます。 |
| 不明 TLV | 各 LLDP フレームで通知された TLV 情報のうち、不明な値を持った TLV の数が表示されます。 |
| 失効パケット | 各 LLDP フレームは、LLDP の有効期限が設定されています。有効期限内に新しい LLDP フレームを受信しない場合、LLDP フレームは削除されます。<br>有効期限内に新しい LLDP フレームを受信しなかったために削除された LLDP フレームの数が表示されます。 |
| アクション | ［クリア］ボタンをクリックすると、ポートの統計情報がクリアされます。 |

## 6.17.7. ポート設定情報

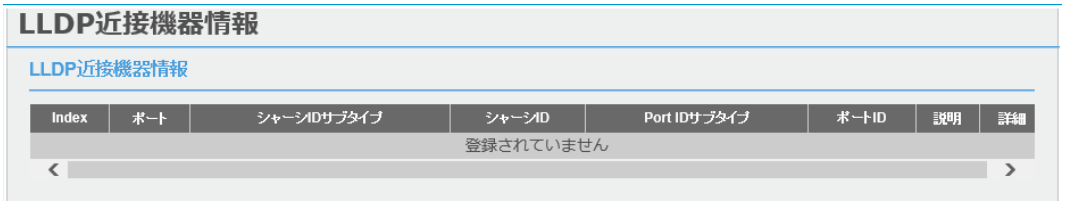
［ポート設定情報］ページでは、スイッチが LLDP で通知する情報を確認できます。




| LLDP ポート要約テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| ポート ID サブタイプ | LLDP で通知するポート ID サブタイプが表示されます。 |
| ポート ID | LLDP で通知するポート ID が表示されます。 |
| ポート説明 | LLDP で通知するポートの説明が表示されます。 |
| アクション | ［詳細］ボタンをクリックすると、ポートの LLDP 詳細情報が表示されます。 |

## 6.17.8. ネイバー情報

［ネイバー情報］ページでは、LLDP で取得したネイバー情報を確認できます。




| LLDP ネイバー情報 | |
|---|---|
| Index | 受信した LLDP 情報のネイバーのインデックス番号が表示されます。 |
| ポート | LLDP パケットを受信したポート番号が表示されます。 |
| シャーシ ID サブタイプ | ネイバーのシャーシ ID サブタイプが表示されます。 |
| シャーシ ID | ネイバーのシャーシ ID が表示されます。 |
| ポート ID サブタイプ | ネイバーのポート ID サブタイプが表示されます。 |
| ポート ID | ネイバーのポート ID が表示されます。 |
| 説明 | ネイバーのポートの説明が表示されます。 |
| 詳細 | ［詳細］ボタンをクリックすると、ネイバーの詳細情報が表示されます。 |

# 6.18. MAC VLAN

［MAC VLAN］ページでは、既存の任意の MAC アドレスを任意の VLAN にマッピングする MAC アドレスベース VLAN 機能の登録を行います。


| MAC VLAN 新規作成 | |
|---|---|
| MAC アドレス | VLAN にマッピングするホストの MAC アドレスを入力します。 |
| 説明 | MAC アドレスの説明を 8 文字以内で入力します。 |
| VLAN ID | MAC アドレスをマッピングする 802.1Q VLAN ID を 1～4094 の範囲で入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、VLAN にマッピングした MAC アドレスが追加されます。 |

| MAC VLAN テーブル | |
|---|---|
| MAC アドレス | VLAN にマッピングした MAC アドレスが表示されます。 |
| 説明 | MAC アドレスの説明が表示されます。 |
| VLAN ID | MAC アドレスをマッピングした VLAN ID が表示されます。 |
| アクション | ［修正］ボタンをクリックすると、MAC アドレスの説明、および VLAN ID を変更できます。<br>［削除］ボタンをクリックすると、作成した MAC VLAN のエントリーが削除されます。 |

# 6.19. プロトコル VLAN

プロトコル VLAN は、通信で使用するプロトコルごとに適用する VLAN を変更する機能です。主に、TCP/IP 通信以外のプロトコルを使用するデバイスが存在する場合に用いられます。

## 6.19.1. プロファイル

［プロファイル］ページでは、対象となるプロトコルを指定します。


| 追加 | |
|---|---|
| プロファイル ID | グループの ID 番号を 1～16 の範囲で入力します。 |
| フレームタイプ | 適用するフレームの形式（Ethernet II／SNAP／LLC）を選択します。 |
| イーサネットタイプ | 適用されるフレームのイーサネットタイプ番号を 16 進数 0000～FFFF の範囲で入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、プロトコル VLAN プロファイルが追加されます。 |

| プロファイルテーブル | |
|---|---|
| プロファイル ID | プロトコル VLAN のプロファイル ID が表示されます。 |
| フレームタイプ | プロトコル VLAN のフレームタイプが表示されます。 |
| イーサネットタイプ | プロトコル VLAN のイーサネットタイプ番号が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、プロトコル VLAN エントリーが削除されます。 |

## 6.19.2. プロファイルインターフェース

［プロファイルインターフェース］ページでは、作成したプロファイルをポートに適用し、合致した場合に適用する VLAN や優先度を決定します。


| プロファイルインターフェース作成 | |
|---|---|
| ポート | プロトコル VLAN を適用するポートを選択します。 |
| プロファイル ID | ポートにマップするプロファイル ID を選択します。 |
| VLAN ID | プロトコル VLAN で適用する VLANID を 1～4094 の範囲で入力します。 |
| 優先度 | プロトコル VLAN で適用する優先度を 0～7 の範囲で選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、プロトコル VLAN のポートエントリーが作成されます。 |

| プロファイルインターフェーステーブル | |
|---|---|
| ポート | ポート番号が表示されます。 |
| プロファイル ID | プロファイル ID が表示されます。 |
| VLAN ID | VLAN ID が表示されます。 |
| 優先度 | 優先度が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、プロトコル VLAN プロファイルインターフェースが削除されます。 |

# 7. QoS

QoS 機能を使用すると、安定した帯域を必要とする通信や、高い優先度を持つ重要な通信（遅延や時間に影響されやすいアプリケーションなど）のために、通信の優先制御を行うことができます。
QoS による優先制御は、受信したパケットをどの程度優先するかを判断する「クラシフィケーション」、ネットワーク上で同様の優先処理をするように識別情報を付加する「マーキング」、優先度付けしたパケットを各送信キューに振り分ける「キューイング」、送信キュー間でのパケット処理順番を決定する「スケジューリング」の 4 段階があります。ネットワーク要件に合致する QoS 優先制御を実現するためには、各段階に対して適切な設定を行う必要があります。
なお、「マーキング」は、主に ACL 機能を使用して設定します。

## 7.1. QoS 基本設定

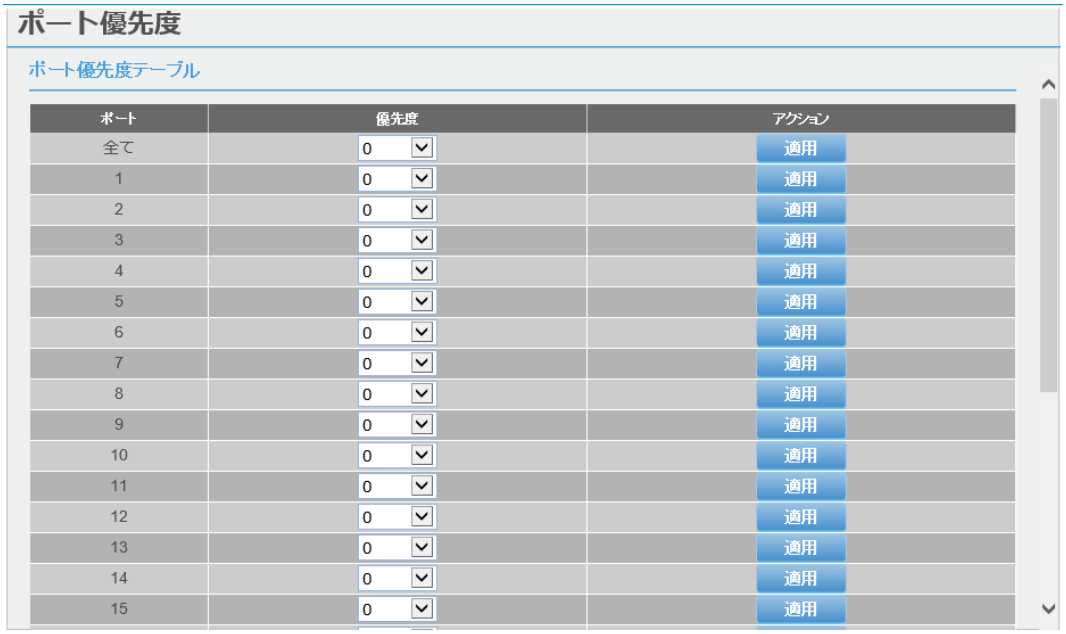
［QoS 基本設定］ページから、QoS 機能や優先度に対するキューの割り当てを設定することができます。
QoS 機能を有効にすると、各キューのパケットはスケジューリング方式に従って送信順番を制御されます。


| QoS 基本設定 | |
|---|---|
| QoS 機能 | QoS 機能の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| 優先度テーブル | |
|---|---|
| 優先度 | QoS 優先度が表示されます。 |
| キューID | QoS 機能を有効にすると、デフォルトではすべての優先度に対して［キューID］が 0 に割り当てられます。ネットワーク環境に基づいて、優先度とキューのマッピングを手動で変更してください。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 7.2. ポート優先度

［ポート優先度］ページでは、ポートに入力するタグなしパケットの QoS 優先度を指定します。




| ポート優先度テーブル | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 優先度 | 各ポートの QoS 優先度を変更する場合、優先度値（0～7）を選択します。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 7.3. DSCP マッピング

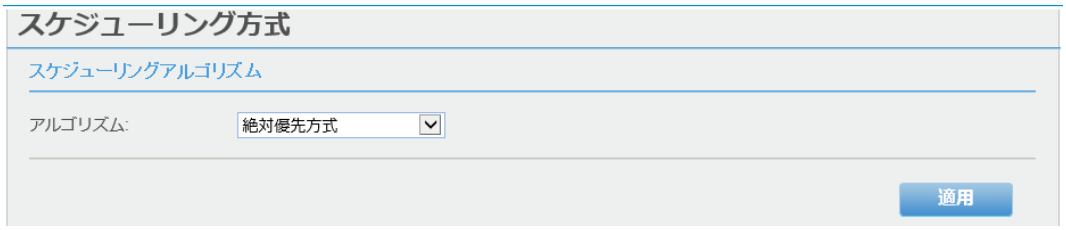
［DSCP マッピング］ページでは、パケットの DSCP 値に対する優先度割り当てを設定します。
使用するネットワークで DSCP による優先制御を行う場合、各 DSCP 値（0～63）について、QoS 優先度をマッピングします。すべての DSCP 値のデフォルト QoS 優先度は 0 です。


| DSCP 優先度マッピング | |
|---|---|
| DSCP マッピング機能 | DSCP マッピング機能の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| DSCP マッピングテーブル | |
|---|---|
| DSCP 値 | DSCP 値（0～63）が表示されます。 |
| 優先度 | 各 DSCP 値（0～63）に対して、QoS 優先度（0～7）を割り当てます。<br>［0-15］、［16-31］、［32-47］、［48-63］は、それぞれの範囲の DSCP 値に対して QoS 優先度をまとめて設定できます。<br>QoS 優先度を個別に設定する場合、［0-15］、［16-31］、［32-47］、［48-63］は［適用しない］を選択してください。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［初期値に戻す］ボタン | ［初期値に戻す］ボタンをクリックすると、初期値に戻ります。 |

# 7.4. スケジューリング方式

［スケジューリング方式］ページでは、キューに割り振られたパケットの送信順番を決定するアルゴリズムを設定します。




| スケジューリングアルゴリズム | |
|---|---|
| アルゴリズム | スケジューリングアルゴリズムを選択します。<br>・ 絶対優先方式：<br>ポートは優先度が高いキューのパケットをすべて送信してから、優先度が低いキューのパケットを送信します。<br>・ 重み付きラウンドロビン：<br>ポートは設定された数のパケットを各キューからラウンドロビン方式で送信します。各キューにトラフィックを送信する機会があります。<br>Note: QoS の重み付きラウンドロビンモードの比率は 1:2:4:8:16:32:64:127 です。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 7.5. IPv6 トラフィッククラス

［IPv6 トラフィッククラス］ページでは、IPv6 パケットのトラフィッククラスをベースとした優先度割り当てを設定します。IPv4 パケットでの DSCP 値をベースとした優先制御と同じような動作を行います。


| IPv6 トラフィッククラス設定 | |
|---|---|
| IPv6 トラフィッククラスマッピング機能 | IPv6 トラフィッククラスマッピング機能の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| IPv6 トラフィッククラスマッピング登録 | |
|---|---|
| IPv6 トラフィッククラス | IPv6 トラフィッククラスの値を 0～255 の範囲で入力します。 |
| キューID | キューID の値（0～7）を選択して、IPv6 トラフィッククラスからキューID へのマッピングを定義します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、IPv6 トラフィッククラスのエントリーが追加されます。 |

| IPv6 トラフィッククラスマッピングテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、IPv6 トラフィッククラスの全エントリーが削除されます。 |
| IPv6 トラフィッククラス | IPv6 トラフィッククラスの値が表示されます。 |
| キューID | IPv6 トラフィッククラスからマッピングしたキューID の値が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、IPv6 トラフィッククラスが削除されます。 |

# 8. セキュリティ

## 8.1. ポートアクセス制御

ポートアクセス制御機能は、スイッチのポートに接続するホストやデバイスを認証する機能です。
ポートアクセス制御が有効になると、スイッチはポートの認証状態により、各ポートのトラフィックの送受信を制御します。
各ポートの認証状態は、ローカルによる認証や RADIUS サーバーなどの外部認証による結果から自動的に制御されます。また、認証状態を固定で指定することも可能です。アップリンクポートや認証サーバーを接続するポート、または、ネットワークプリンターなどの待ち受けデバイスや、認証に対応しない端末を接続するポートに適用します。

Note: ポートアクセス制御機能による認証は、原則としてポートとデバイスが LAN ケーブルで直結している形態を想定しています。途中経路に別のスイッチングハブを配置することで、単一ポートで複数のデバイスを認証させることも可能ですが（サプリカントモード：マルチ）、中継するスイッチングハブによっては認証が動作しない場合があります。またデバイスのリンクダウンを検知できずに認証状態の不整合が発生するなど、想定とは異なる状態になる可能性がありますので、ご注意ください。なお、同時に認証登録が可能な最大デバイス数は 256 です。


| ポートアクセス制御 | |
|---|---|
| NAS ID | 本スイッチの Network Access Server ID（以後、NAS ID）を 16 文字以内で入力します。NAS ID により、スイッチにはすべてのポートに適用される 802.1X 識別子が割り当てられます。 |
| ポートアクセス制御機能 | ポートアクセス制御機能の状態（有効／無効）を選択します。（デフォルト：無効） |
| 認証方式 | スイッチが使用する認証方式を選択します。<br>・ RADIUS：<br>RADIUS サーバーを使用するリモート認証です。<br>・ TACACS+：<br>TACACS+サーバーを使用するリモート認証です。 |

| | |
|---|---|
| | ・ ローカル：スイッチ内部のデータベースを参照します。ローカル認証を行うには、ローカルユーザーを作成する必要があります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［設定］ボタン | ［設定］ボタンをクリックすると、［ポートアクセス設定］が表示されます。 |
| ［状態確認］ボタン | ［状態確認］ボタンをクリックすると、［ポートアクセス制御テーブル］が表示されます。 |

ポートアクセス制御の［設定］ボタンをクリックすると、［ポートアクセス設定］が表示されます。この画面から、ポートアクセス制御機能の詳細な設定を行います。


| **ポートアクセス設定** | |
|---|---|
| ポート | ポート番号を選択します。<br>［初期状態に戻す］ボタンをクリックすると、ポートの再認証が強制的に行われます。［初期状態に戻す］ボタンは、［ポート認証設定］でポートの制御モードを［Auto］に変更した後のみ使用できます。 |
| 認証モード | ポートの認証モード（802.1X 認証／MAC 認証）を選択します。<br>・ 802.1X 認証：<br>802.1X サプリカント機能を持つデバイスの認証を行います。<br>・ MAC 認証：<br>802.1X サプリカント機能を使用しないデバイスに対し、MAC アドレスをベースとした認証を行います。<br>Note: 802.1X 認証／MAC 認証いずれの場合にも、認証サーバーへの照会は EAP 認証タイプとして行われます。サーバーにユーザーを登録する場合は、認証タイプを整合させてください。 |

| | |
|---|---|
| ポート認証設定 | ポートの制御モード（非認証／Auto／認証）を選択します。（デフォルト：認証）<br>ポート認証を行う際は［Auto］に変更してください。<br>また、スイッチ管理画面のアクセスに使用しているポートを［認証］から変更すると、スイッチ管理画面にアクセスできなくなることがありますので、ご注意ください。 |
| 再認証 | ポートでの再認証機能の状態（有効／無効）を選択します。 |
| サプリカントモード | サプリカントモードを選択します。（デフォルト：シングル）<br>・ マルチ：1つのポートで複数のユーザーを認証できます。<br>・ シングル：<br>1つのポートで1つのユーザーのみ認証します。認証されたユーザー以外に対する動作は、ピギーバックモードによって異なります。 |
| ピギーバック | ピギーバックモードの状態（有効／無効）を選択します。<br>ピギーバックモードを有効にした場合、1つのクライアントが認証に成功すると、ほかのすべてのデバイスが認証なしでそのポート経由でパケットを転送できます。<br>**Note:** ピギーバックモードは、［サプリカントモード］が［シングル］に設定されているときのみ選択できます。 |
| ダイナミック VLAN | ダイナミック VLAN 機能の状態（有効／無効）を選択します。<br>ダイナミック VLAN 機能を有効にした場合、認証済みクライアントがログオンすると、スイッチはサーバーやローカルユーザーの情報に従って自動的に VLAN を割り当てます。<br>**Note:** 認証サーバーの情報から VLAN を自動的に割り当てる場合、ユーザー情報に以下の属性値を登録してください。<br>Tunnel-Type = 13,<br>Tunnel-Medium-Type = 6,<br>Tunnel-Private-Group-Id = <割り当てる VLAN ID> |
| セキュア VLAN | セキュア VLAN 機能の状態（有効／無効）を選択します。<br>セキュア VLAN 機能を有効にした場合、最初のクライアントが接続されて認証許可されると、認証許可されたクライアントとは異なる VLAN ID のクライアントは認証許可されません。<br>**Note:** セキュア VLAN モードは、［サプリカントモード］が［マルチ］に設定されているときのみ選択できます。 |
| ゲスト VLAN ID | ゲスト VLAN ID を入力します。認証に失敗すると、設定したゲスト VLAN が割り当てられます。 |
| 再送間隔 | 送信した EAP 要求（ID 要求）パケットに対するサプリカントからの応答を待機する時間を 1～65535（秒）の範囲で入力します。（デフォルト：30 秒） |

| | |
|---|---|
| 最大リクエスト回数 | 認証セッションをタイムアウトする前にサプリカントに EAP 要求パケットを送信する最大回数を 1～10 の範囲で入力します。(デフォルト：2) |
| ブロック期間 | クライアントの認証が失敗した後、認証を行わないブロック時間を 1～65535（秒）の範囲で入力します。(デフォルト：60 秒) |
| 再認証間隔 | クライアントに再認証を要求する時間を 1～65535（秒）の範囲で入力します。(デフォルト：3600 秒) |
| サプリカントタイムアウト | EAP 要求パケット送信後、サプリカントからの応答を待機する時間を 1～65535（秒）の範囲で入力します。(デフォルト：30 秒) |
| サーバータイムアウト | 認証サーバーからの応答を待機する時間を 1～65535（秒）の範囲で入力します。(デフォルト：30 秒) |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［取消］ボタン | ［取消］ボタンをクリックすると、変更が取り消されます。 |

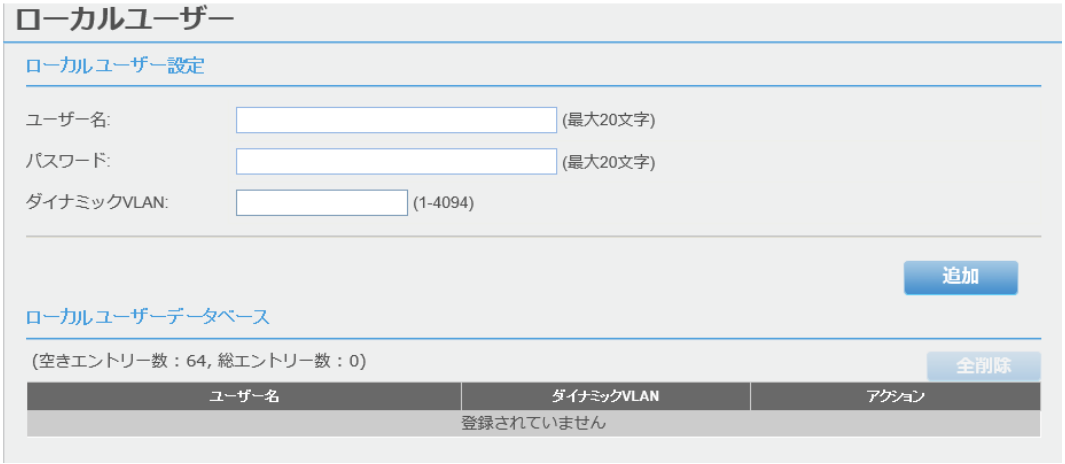
ポートアクセス制御の［状態確認］ボタンをクリックすると、［ポートアクセス制御テーブル］が表示されます。この画面から、各ポートの認証状態や設定を確認することができます。


| ポートアクセス制御テーブル | |
|---|---|
| NAS ID | 本スイッチの NAS ID が表示されます。 |
| 802.1X 認証 | ポートアクセス制御機能の状態が表示されます。 |
| 認証方式 | 認証方式が表示されます。 |
| ポート | スイッチのポート番号が表示されます。 |

| | |
|---|---|
| 認証モード | 各ポートに構成された認証モードが表示されます。 |
| ポート認証設定 | 各ポートに構成されたポート認証設定が表示されます。 |
| 認証状態 | 各ポートの現在の認証状態が表示されます。 |
| サプリカントモード | 各ポートのサプリカントモードが表示されます。 |
| ピギーバック | 各ポートのピギーバックモードの状態が表示されます。 |
| 認証 MAC アドレス | 認証済みクライアントの MAC アドレスが表示されます。<br>Note: 最初に認証されたクライアントの MAC アドレスのみ表示されます。 |
| VLAN | 認証済みクライアントの VLAN 情報が表示されます。 |

# 8.2. ローカルユーザー

［ローカルユーザー］ページでは、ポート認証で使用するユーザー情報をスイッチ内部に登録します。
ポートアクセス制御の認証方式がローカルの場合にはローカルユーザーデータベースが使用されます。




| ローカルユーザー設定 | |
|---|---|
| ユーザー名 | ローカルユーザーの名前を 20 文字以内で入力します。 |
| パスワード | ローカルユーザーのパスワードを 20 文字以内で入力します。 |
| ダイナミック VLAN | ダイナミック VLAN が有効の場合に、ローカルユーザーに適用する VLAN ID を入力します。<br>VLAN ID は、［ネットワーク］＞［VLAN］ページで作成した値を指定します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、ローカルユーザーのエントリーが追加されます。 |

| ローカルユーザーデータベース | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、作成したローカルユーザーの全エントリーが削除されます。 |
| ユーザー名 | ローカルユーザーの名前が表示されます。 |
| ダイナミック VLAN | ローカルユーザーをマッピングした VLAN ID が表示されます。 |
| アクション | ［変更］ボタンをクリックすると、作成したローカルユーザーのパラメーター（パスワードや VLAN ID）を変更できます。ユーザー名は変更できません。ユーザー名を変更する場合は、ユーザーを削除してから再作成してください。<br>［削除］ボタンをクリックすると、作成したローカルユーザーのエントリーが削除されます。 |

# 8.3. RADIUS サーバー

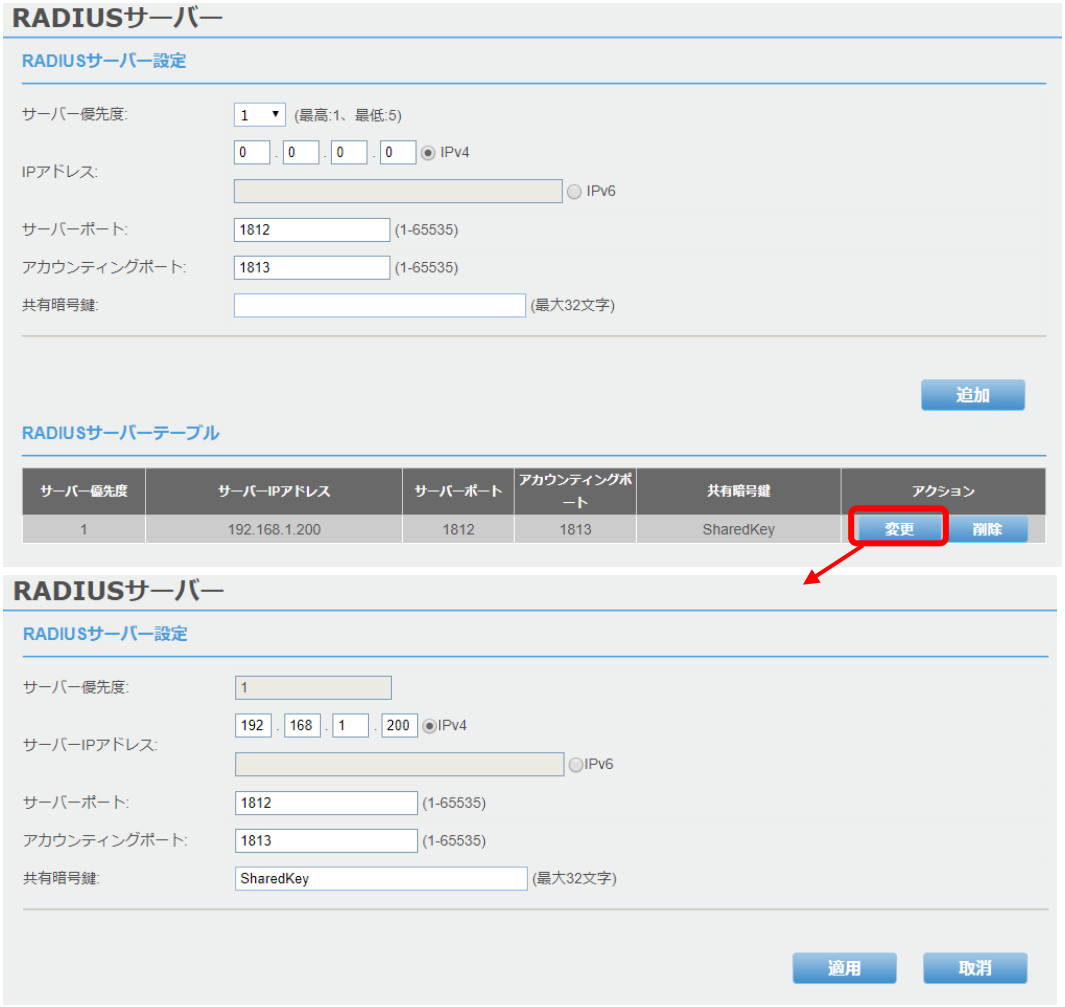
ポート認証でユーザー情報を参照する RADIUS サーバーを設定します。


| RADIUS サーバー設定 | |
|---|---|
| サーバー優先度 | 作成した RADIUS サーバーの優先度を選択します。<br>最高の優先度が 1、最低の優先度が 5 です。<br>Note: ［サーバー優先度］の各値は、1 つの RADIUS サーバーIP アドレスにのみ割り当てることができます。 |
| IP アドレス | ［IPv4］または［IPv6］を選択し、RADIUS サーバーの IP アドレスを入力します。 |
| サーバーポート | 認証メッセージを通信する RADIUS サーバー認証ポートを 1～65535 の範囲で入力します。（デフォルト：1812） |
| アカウンティングポート | アカウンティングメッセージを通信する RADIUS アカウンティングポートを 1～65535 の範囲で入力します。（デフォルト：1813） |
| 共有暗号鍵 | スイッチと RADIUS サーバーとの間の共有暗号鍵を入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、RADIUS サーバーのエントリーが追加されます。 |

| RADIUS サーバーテーブル | |
|---|---|
| サーバー優先度 | RADIUS サーバーに割り当てたサーバー優先度が表示されます。 |
| サーバーIP アドレス | RADIUS サーバーの IP アドレスが表示されます。 |
| サーバーポート | RADIUS サーバー認証のポート番号が表示されます。 |
| アカウンティングポート | RADIUS アカウンティングのポート番号が表示されます。 |
| 共有暗号鍵 | RADIUS サーバーの共有暗号鍵が表示されます。 |
| アクション | ［変更］ボタンをクリックすると、RADIUS サーバーのパラメーター |

| | |
|---|---|
| | を変更できます。<br>［削除］ボタンをクリックすると、RADIUS サーバーのエントリーが削除されます。 |

RADIUS サーバーテーブルの［変更］ボタンをクリックすると、RADIUS サーバーのパラメーターを変更できます。




| サーバー設定変更 | |
|---|---|
| サーバー優先度 | サーバー優先度は変更できません。 |
| IP アドレス | RADIUS サーバーの IP アドレスを変更できます。 |
| サーバーポート | RADIUS サーバーの認証ポートを変更できます。 |
| アカウンティングポート | RADIUS サーバーのアカウンティングポートを変更できます。 |
| 共有暗号鍵 | 共有暗号鍵の値を変更できます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［取消］ボタン | ［取消］ボタンをクリックすると、［RADIUS サーバー設定］ページに戻ります。 |

# 8.4. TACACS+サーバー

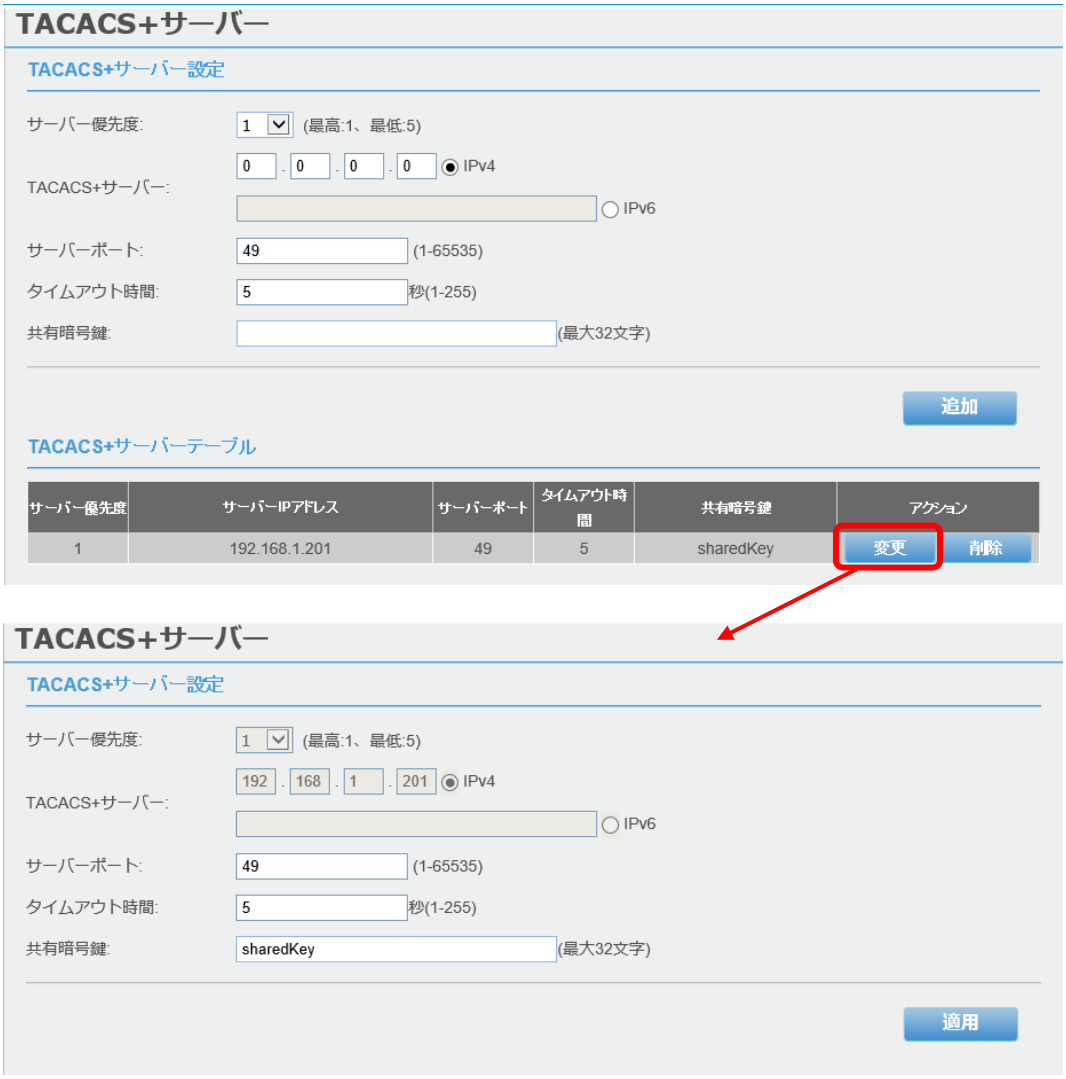
ポート認証でユーザー情報を参照する TACACS+サーバーを設定します。


| TACACS+サーバー設定 | |
|---|---|
| サーバー優先度 | 作成した TACACS+サーバーの優先度を選択します。<br>最高の優先度が 1、最低の優先度が 5 です。<br>Note: ［サーバー優先度］の各値は、1 つの TACACS+サーバーIP アドレスにのみ割り当てることができます。 |
| TACACS+サーバー | ［IPv4］または［IPv6］を選択し、TACACS+サーバーの IP アドレスを入力します。 |
| サーバーポート | TACACS+サーバーのポート番号を 1～65535 の範囲で入力します。(デフォルト：49) |
| タイムアウト時間 | スイッチが TACACS+サーバーからの応答を待機するタイムアウト値を 1～255（秒）の範囲で入力します。(デフォルト：5 秒) |
| 共有暗号鍵 | スイッチと TACACS+サーバーとの間の共有暗号鍵を入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、TACACS+サーバーのエントリーが追加されます。 |

| TACACS+サーバーテーブル | |
|---|---|
| サーバー優先度 | TACACS+サーバーに割り当てたサーバー優先度が表示されます。 |
| サーバーIP アドレス | TACACS+サーバーの IP アドレスが表示されます。 |
| サーバーポート | TACACS+サーバーのポート番号が表示されます。 |
| タイムアウト時間 | TACACS+サーバーのタイムアウト値が表示されます。 |
| 共有暗号鍵 | TACACS+サーバーの共有暗号鍵が表示されます。 |
| アクション | ［変更］ボタンをクリックすると、TACACS+サーバーの情報を変更できます。 |

| | |
|---|---|
| | ［削除］ボタンをクリックすると、TACACS+サーバーのエントリーが削除されます。 |

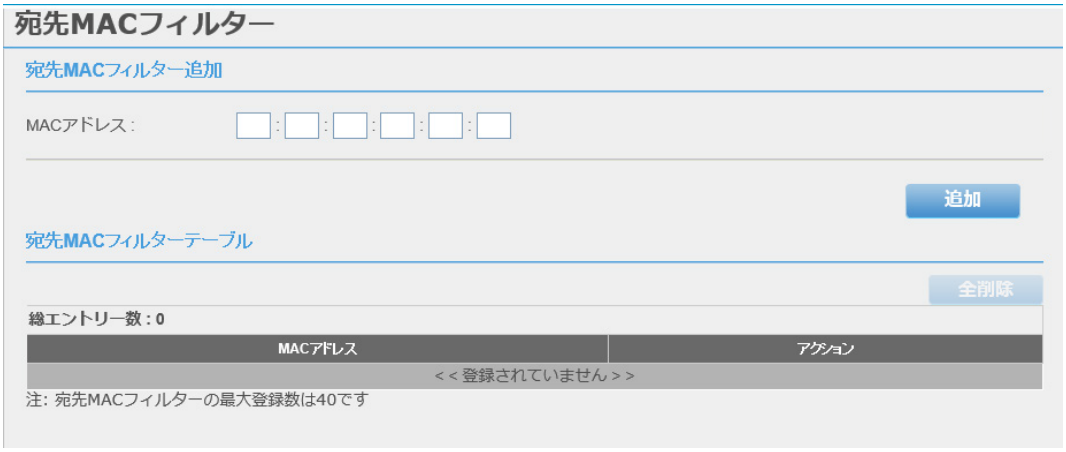
TACACS+サーバーテーブルの［変更］ボタンをクリックすると、TACACS+サーバーのパラメーターを変更できます。




| TACACS+サーバー設定 | |
|---|---|
| サーバー優先度 | サーバー優先度は変更できません。 |
| TACACS+サーバー | TACACS+サーバーの IP アドレスは変更できません。<br>TACACS+サーバーの IP アドレスを変更する場合は、エントリーを削除してから再作成してください。 |
| サーバーポート | TACACS+サーバーのポートを変更できます。 |
| タイムアウト時間 | タイムアウト値を変更できます。 |
| 共有暗号鍵 | 共有暗号鍵の値を変更できます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

# 8.5. 宛先 MAC フィルター

［宛先 MAC フィルター］ページでデバイスの MAC アドレスを追加すると、パケットの宛先 MAC アドレスがスイッチによりフィルタリングされます。登録された MAC アドレスと宛先 MAC アドレスが一致する場合、そのパケットは転送されずに破棄されます。



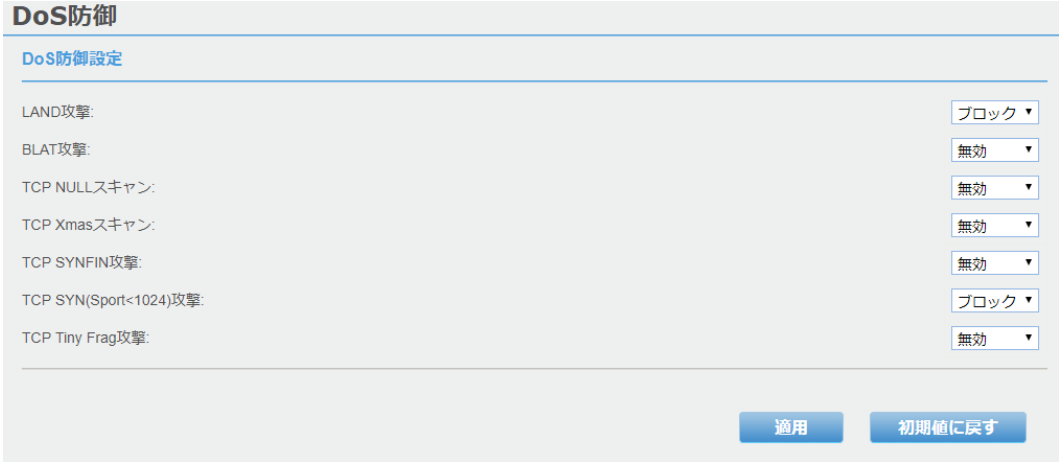

| 宛先 MAC フィルター追加 | |
|---|---|
| MAC アドレス | 宛先 MAC フィルターテーブルに追加する MAC アドレスを入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、宛先 MAC フィルターのエントリーが追加されます。 |

| 宛先 MAC フィルターテーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、作成した宛先 MAC フィルターの全エントリーが削除されます。 |
| MAC アドレス | 作成した宛先 MAC フィルターのエントリーが表示されます。 |
| アクション | ［削除］ボタンをクリックすると、作成した宛先 MAC フィルターのエントリーが削除されます。 |

# 8.6. DoS 防御

［DoS 防御］ページで、Denial of Service（以後、DoS）攻撃に対する防御機能を設定します。
以下の DoS 攻撃に対して防御機能を使用できます。

- LAND 攻撃
- BLAT 攻撃
- TCP NULL スキャン
- TCP Xmas スキャン
- TCP SYNFIN 攻撃
- TCP SYN(Sport<1024)攻撃
- TCP Tiny Frag 攻撃




| DoS 防御設定 | |
|---|---|
| LAND 攻撃 | LAND 攻撃では、対象デバイスに特殊なパケット（送信元／宛先の IP アドレスがデバイスの IP アドレスと同じパケット）を送信します。デバイスがそれらのパケットに返信を試みて、システムをロックする恐れがあります。 |
| BLAT 攻撃 | BLAT 攻撃では、対象デバイスに特殊なパケット（送信元ポートと宛先ポートが同じパケット）を送信します。デバイスがそれらのパケットに返信を試みて、システムをロックする恐れがあります。 |
| TCP NULL スキャン | TCP NULL スキャンでは、対象デバイスに TCP のシーケンス番号とすべての制御ビットがゼロのパケットを送信します |
| TCP Xmas スキャン | TCP Xmas スキャンでは、対象デバイスに TCP のシーケンス番号がゼロで、FIN、URG、PSH のビットが設定されているパケットを送信します。 |
| TCP SYNFIN 攻撃 | TCP SYNFIN 攻撃では、パケット内で SYN ビットと FIN ビットが設定されているパケットを対象デバイスに送信します。 |
| TCP SYN(Sport<1024)攻撃 | TCP SYN(Sport<1024)攻撃では、送信元ポート番号が 1024 未満の SYN パケットを対象デバイスに送信します。 |

| | |
|---|---|
| TCP Tiny Frag 攻撃 | TCP Tiny Frag 攻撃では、小さいフラグメントが送信されます。最終フラグメント以外で 400 バイト未満のフラグメントは、小さすぎると見なされる可能性があります。小さいフラグメントは、DoS 攻撃で使われたり、セキュリティー対策や検知をバイパスする試みで使われたりする可能性があります。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［初期値に戻す］ボタン | ［初期値に戻す］ボタンをクリックすると、初期値に戻ります。 |

デフォルトでは、すべて［無効］に設定されています。すべてのタイプのトラフィックがスイッチを通過できます。

Note: ルールを［ブロック］に設定すると、指定したタイプのトラフィックを拒否できます。セキュリティー強化のため、必要に応じてルールを［ブロック］に設定できます。

# 8.7. DHCP スヌーピング

DHCP スヌーピング機能はアクセス制御機能の一つで、DHCP サーバーから正常に IP アドレスを取得したデバイスのみ通信を許可する機能です。DHCP スヌーピング機能を有効にすると、スイッチはバインディングデータベースを構成し、バインディングデータベースやポートの信頼状態を元にトラフィック制御を行います。

バインディングデータベースには、クライアントと DHCP サーバーとの間で行われる DHCP での IP アドレス取得の通信をモニターし、自動学習した結果が登録されます。
各ポートの信頼状態は、DHCP スヌーピング機能によるトラフィック制御を行うかどうかを決定します。DHCP スヌーピング機能の制御は「信頼できないポート」に対して動作しますので、例えば不特定のノードが接続するポートは信頼できないポートに設定します。一方で、DHCP サーバーやネットワーク上流の機器などが存在するポートは「信頼ポート」に設定し、トラフィック制御の対象外とします。

## 8.7.1. 基本設定

［基本設定］ページで、DCHP スヌーピング機能の一般的な設定を行います。


| DHCP スヌーピング設定 | |
|---|---|
| DHCP スヌーピング機能 | DHCP スヌーピング機能の状態（有効／無効）を選択します。 |

| DHCP スヌーピング詳細設定 | |
|---|---|
| オプション 82 透過 | オプション 82 透過機能の状態を選択します。<br>・ 有効：<br>信頼できないポートでオプション 82 を含む DHCP 要求パケットを受信した場合でも、パケットを DHCP サーバーに転送します。<br>・ 無効：<br>信頼できないポートでオプション 82 を含む DHCP 要求パケットを受信した場合、パケットを転送しません。 |

| | |
|---|---|
| MAC アドレス検証 | MAC アドレス検証機能の状態を選択します。<br>・ 有効：<br>信頼できないポートで DHCP 要求パケットを受信したとき、DHCP パケット内のアドレスと送信元 MAC アドレスを照合します。一致しない場合、スイッチはパケットを破棄します。<br>・ 無効：<br>信頼できないポートで DHCP 要求パケットを受信したとき、DHCP パケット内のアドレスと送信元 MAC アドレスを照合しません。 |
| バックアップデータベース | データベースバックアップ機能の状態を選択します。<br>・ 有効：<br>スイッチは［データベース更新間隔］で指定された間隔でバインディングデータベースのバックアップを行います。<br>・ 無効：<br>バインディングデータベースのバックアップを行いません。 |
| データベース更新間隔 | バインディングデータベースのバックアップ更新間隔を 600～86400（秒）の範囲で入力します。 |
| オプション 82 挿入 | DHCP オプション 82 の挿入機能の状態を選択します。<br>・ 有効：<br>信頼できないポートで DHCP パケットを受信したとき、スイッチはオプション 82 の情報を挿入し、DHCP サーバーに転送します。DHCP サーバーは IP アドレスなどのパラメーターの割り当てポリシーのために、オプション 82 の情報を使用することがあります。<br>・ 無効：<br>信頼できないポートで DHCP パケットを受信したとき、スイッチはオプション 82 の情報を挿入しません。 |

［適用］ボタンをクリックすると、変更が適用されます。

## 8.7.2. VLAN 設定

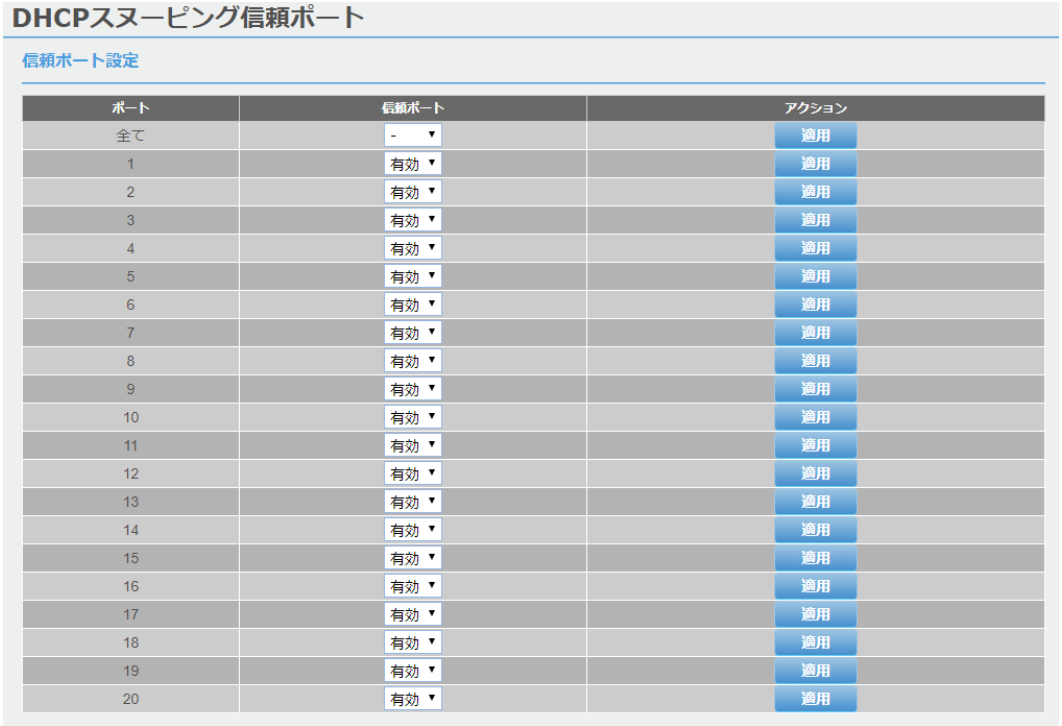
［VLAN 設定］ページで、DHCP スヌーピングを適用する VLAN を指定することができます。

| DHCP スヌーピング VLAN 登録 | |
|---|---|
| VLAN ID | DHCP スヌーピングを適用する既存の VLAN ID を入力します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、VLAN ID が追加されます。 |
| ［クリア］ボタン | ［クリア］ボタンをクリックすると、入力がクリアされます。 |

| DHCP スヌーピング VLAN テーブル | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全 VLAN ID が削除されます。 |
| VLAN ID | 追加した VLAN ID が表示されます。 |
| アクション | ［削除］ボタンをクリックすると、VLAN ID が削除されます。 |

## 8.7.3. 信頼ポート

［信頼ポート］ページで、DHCP スヌーピングのポートの信頼状態を設定します。




| 信頼ポート設定 | |
|---|---|
| ポート | スイッチのポート番号が表示されます。 |
| 信頼ポート | ポートの信頼状態（有効／無効）を選択します。（デフォルト：有効）<br>［全て］から、すべてのポートをまとめて設定できます。<br>［有効］を選択すると、そのポートは信頼ポートに設定されます。<br>［無効］を選択すると、そのポートは信頼できないポートに設定されます。 |
| アクション | ［適用］ボタンをクリックすると、変更が適用されます。 |

## 8.7.4. バインディングデータベース

［バインディングデータベース］ページで、バインディングデータベースの登録状況を確認することができます。また、エントリーの作成や、エントリーのタイプやポートの変更を行うことができます。


| バインディングデータベース編集 | |
|---|---|
| MAC アドレス | バインディングデータベースに登録するホストの MAC アドレスを入力します。 |
| IP アドレス | ［IPv4］または［IPv6］を選択し、デバイスまたはホストに割り当てられる IP アドレスを入力します。 |
| VLAN ID | ホストの VLAN ID を入力します。<br>Note: 事前に［DHCP スヌーピング］＞［VLAN 設定］ページで既存の VLAN ID を追加する必要があります。 |
| ポート | ホストが接続するポートを選択します。 |
| タイプ | バインディングデータベースのエントリーのタイプを選択します。<br>・ スタティック：<br>固定のエントリーで、リース時間は無限として扱われます。<br>・ ダイナミック：<br>DHCP での IP アドレス取得が正常に行われたと想定して追加するエントリーです。エントリーのリース時間を指定する必要があります。登録してから、リース時間を経過しても DHCP による IP アドレス再取得が行われない場合、エントリーは削除されます。 |
| リース時間 | ダイナミックエントリーを設定する場合の、リース時間の初期カウンター値を手動で入力します。<br>エントリーのリース時間のカウンターがゼロまで下がると、エントリーはスイッチから削除されます。 |

| | |
|---|---|
| ［追加］ボタン | ［追加］ボタンをクリックすると、バインディングデータベースのエントリーが追加されます。 |
| ［リセット］ボタン | ［リセット］ボタンをクリックすると、入力がリセットされます。 |
| ［クリア］ボタン | ［クリア］ボタンをクリックすると、バインディングデータベースの学習したエントリーがクリアされます。 |

| **バインディングデータベーステーブル** | |
|---|---|
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、学習または作成したバインディングデータベースの全エントリーが削除されます。 |
| MAC アドレス | バインディングデータベースのエントリーの MAC アドレスが表示されます。 |
| VLAN ID | バインディングデータベースのエントリーの VLAN ID が表示されます。 |
| IP アドレス | バインディングデータベースのエントリーの IP アドレスが表示されます。 |
| ポート | バインディングデータベースのエントリーのポート番号が表示されます。 |
| タイプ | バインディングデータベースのエントリーのタイプ（スタティック／ダイナミック）が表示されます。 |
| リース期間 | バインディングデータベースのエントリーのリース期間が表示されます。［スタティック］エントリーの場合は、［Infinite］が表示されます。 |
| アクション | ［検索］ボタンをクリックすると、特定の MAC アドレス、IP アドレス、VLAN ID、ポート番号、バインディングデータベースのタイプを検索して表示できます。<br>［変更］ボタンをクリックすると、［バインディングデータベース編集］ページにエントリーの情報が表示されます。<br>・ ダイナミックに学習したエントリーの場合：<br>エントリーのタイプを変更できます。<br>・ 手動で作成したエントリーの場合：<br>エントリーのポート番号やタイプを変更できます。<br>［削除］ボタンをクリックすると、学習または作成したバインディングデータベースのエントリーが削除されます。 |

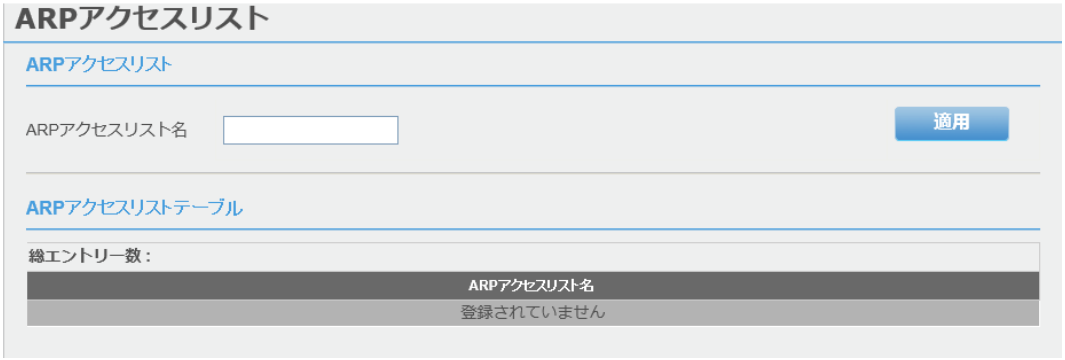
# 8.8. ダイナミック ARP 検査

ダイナミック ARP 検査はアクセス制御機能の一つで、受信した ARP パケットを検査し、設定した ARP アクセスリストや DHCP スヌーピングのバインディングデータベースを参照して処理を決定する機能です。
ARP パケットは TCP/IP 通信を行う前に、適切な送信先 MAC アドレスを探索するために使用します。ARP パケットのトラフィックを限定することで、ポリシーに合致しない通信を制限することができます。

ダイナミック ARP 検査は、各ポートの信頼状態と ARP 検査フィルターの設定を参照して実行されます。ARP 検査フィルターは、対象となる VLAN と適用するルール（ARP アクセスリスト）の組み合わせにより構成されます。ポートの信頼状態は、DHCP スヌーピングと同じように ARP パケットの制御を行うかどうかを決定し、「信頼できないポート」のみが ARP 検査フィルターの対象になります。

## 8.8.1. ARP アクセスリスト

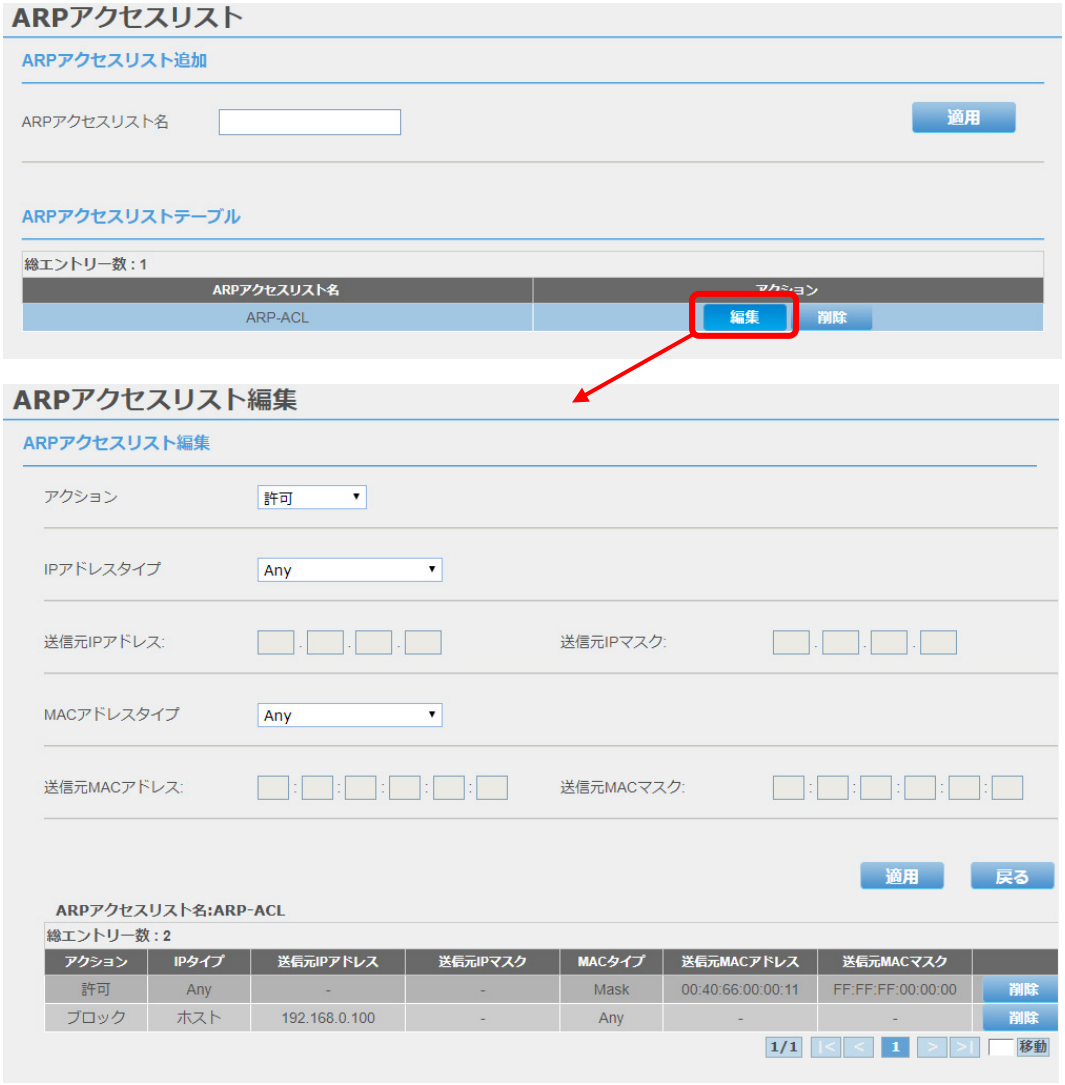
［ARP アクセスリスト］ページでは、ダイナミック ARP 検査の ARP アクセスリストを登録します。
ARP アクセスリストは、ダイナミック ARP 検査によって ARP パケットを許可またはブロックする対象とアクションを指定するためのプロファイルで、具体的な検査対象やアクションを定めたルールは ARP アクセスリスト上に登録されます。




| ARP アクセスリスト追加 | |
|---|---|
| APR アクセスリスト名 | 作成する ARP アクセスリストの名前を 32 文字以内で入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、ARP アクセスリストが追加されます。追加した ARP アクセスリストはルールが登録されていませんので、ルールを登録する場合は ARP アクセスリストテーブルから［編集］をクリックして追加してください。 |

| ARP アクセスリストテーブル | |
|---|---|
| APR アクセスリスト名 | ARP アクセスリストの名前が表示されます。 |
| アクション | ［編集］ボタンをクリックすると、ARP アクセスリストに適用するルールを編集できます。<br>［削除］ボタンをクリックすると、ARP アクセスリストが削除されます。 |

ARP アクセスリストテーブルの［編集］ボタンをクリックすると、ARP アクセスリストのルールを編集できます。




| ARP アクセスリスト編集 | |
|---|---|
| アクション | 追加するルールのアクションを指定します。<br>［許可］：該当する ARP パケットを明示的に許可します。<br>［ブロック］：該当する ARP パケットを明示的にブロックします。 |
| IP アドレスタイプ | ルールの適用対象となる送信元 IP アドレスを指定する方式を選択します。<br>・ Any：すべての IP アドレスを対象とします。<br>・ ホスト：指定した IP アドレスのみを対象とします。<br>・ IP マスク：ネットマスク範囲で対象 IP アドレスを指定します。 |
| 送信元 IP アドレス | ルールの適用対象となる送信元 IP アドレスを指定します。［Any］を選択した場合は設定できません。 |
| 送信元 IP マスク | ［IP マスク］を指定した場合のみ設定可能で、送信元 IP アドレスと組み合わせてネットワーク範囲を指定します。 |

| | |
|---|---|
| MAC アドレスタイプ | ルールの適用対象となる送信元 MAC アドレスを指定する方式を選択します。<br>・ Any：すべての MAC アドレスを対象とします。<br>・ ホスト：指定した MAC アドレスのみを対象とします。<br>・ MAC マスク：マスク指定により対象 MAC アドレスを指定します。 |
| 送信元 MAC アドレス | ルールの適用対象となる送信元 MAC アドレスを指定します。［Any］を選択した場合は設定できません。 |
| 送信元 MAC マスク | ［IP マスク］を指定した場合のみ設定可能で、送信元 MAC アドレスと組み合わせて MAC アドレス範囲を指定します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、ルールが追加されます。 |
| ［戻る］ボタン | ［戻る］ボタンをクリックすると、［ARP アクセスリスト］ページに戻ります。 |

登録したルールは、画面下部にテーブルで表示されます。
［削除］ボタンをクリックすると、対象のルールが削除されます。

## 8.8.2. 基本設定

［基本設定］ページでは、ダイナミック ARP 検査の基本的な動作について設定します。
［ARP 検査フィルタ］の設定項目で、検査対象の VLAN と適用する ARP アクセスリストのマッピングを行った ARP 検査フィルターを登録します。その以外の設定ではオプション機能やログ設定などを指定できます。

［ARP 検査設定］は、オプションの検査内容の設定を設定します。

| ARP 検査設定 | |
|---|---|
| 送信元 MAC | 送信元 MAC 検査の状態（有効／無効）を選択します。<br>送信元 MAC 検査はダイナミック ARP 検査のオプション機能で、送信元 MAC アドレスと ARP パケット内の送信元 MAC アドレス情報が一致するかをチェックします。<br>検査対象パケットは ARP 要求および ARP 応答パケットです。 |
| 宛先 MAC | 宛先 MAC 検査の状態（有効／無効）を選択します。<br>宛先 MAC 検査はダイナミック ARP 検査のオプション機能で、宛先 MAC アドレスと ARP パケット内の宛先 MAC アドレス情報が一致するかをチェックします。<br>検査対象パケットは ARP 応答パケットです。 |
| IP アドレス | IP アドレス検査の状態（有効／無効）を選択します。<br>IP アドレス検査はダイナミック ARP 検査のオプション機能で、ARP パケットの無効な IP アドレスや予期しない IP アドレスを検査します。また、ARP パケット内の IP アドレスの妥当性をチェックします。ARP 要求と ARP 応答の送信元 IP が ARP 応答の宛先 IP に対して検証されます。<br>宛先が IP アドレス 0.0.0.0、255.255.255.255、およびすべてのマルチキャストアドレスのパケットは廃棄されます。<br>送信元 IP アドレスはすべての ARP 要求と ARP 応答でチェックされ、宛先 IP アドレスは ARP 応答内のみチェックされます。 |

［ARP 検査ログ設定］は、ダイナミック ARP 検査が行われた際の ARP 検査ログの出力について設定します。［対象 VLAN］ページでダイナミック ARP 検査の対象に設定された VLAN の VLAN ID をインデックスとしたログ設定がテーブルに表示されます。検査対象 VLAN が登録されていない場合にはテーブルに表示されません。

| ARP 検査ログ設定 | |
|---|---|
| VLAN ID | ダイナミック ARP 検査対象 VLAN の VLAN ID が表示されます。 |
| ACL ログ | ARP アクセスリストを参照した場合の ARP 検査ログ出力の設定（ブロック／許可／全て／None）が表示されます。<br>・ ブロック：ARP アクセスリストでブロックした際に出力します。<br>・ 許可：ARP アクセスリストで許可された際に出力します。<br>・ 全て：ARP アクセスリストでブロック／許可された際に出力します。<br>・ None：ログを出力しません |
| DHCP ログ | バインディングデータベースを参照した場合の ARP 検査ログ出力の設定（ブロック／許可／全て／None）が表示されます。<br>・ ブロック：バインディングデータベースでブロックした際に出力します。 |

| | |
|---|---|
| | ・ 許可：バインディングデータベースで許可された際に出力します。<br>・ 全て：バインディングデータベースでブロック／許可された際に出力します。<br>・ None：ログを出力しません |
| アクション | ［編集］ボタンをクリックすると、ダイナミック ARP 検査対象 VLAN の ACL ログ、DHCP ログの設定を変更できます。 |

［ARP 検査フィルタ］では、ダイナミック ARP 検査で使用する ARP 検査フィルターを登録します。ARP 検査フィルターは VLAN と適用する ARP アクセスリストの組み合わせで構成され、ダイナミック ARP 検査の対象となった VLAN では、該当する ARP 検査フィルターやポートの信頼状態を元に ARP パケットの制御を行います。

| ARP 検査フィルタ | |
|---|---|
| ARP アクセスリスト名 | 追加または削除する ARP アクセスリストの名前を 32 文字以内で入力します。追加する ARP アクセスリストは、［ARP アクセスリスト］ページで設定されている必要があります。 |
| VLAN ID リスト | ARP アクセスリストを適用する、または削除する VLAN ID を入力します。 |
| スタティック ACL | ARP アクセスリストをスタティック ACL として使用するかどうか（対応／非対応）を選択します。<br>［対応］を選択すると、ARP アクセスリストで明示的に許可されていない場合はブロックされます。バインディングデータベースは参照しません。<br>［非対応］を選択すると、ARP アクセスリストで許可またはブロックされていない場合、バインディングデータベースを参照して処理を決定します。 |
| ［追加］ボタン | ［追加］ボタンをクリックすると、ARP アクセスリストが追加されます。 |
| ［削除］ボタン | ［削除］ボタンをクリックすると、追加した ARP アクセスリストが削除されます。 |

［ARP 検査フィルターテーブル］では、登録した ARP 検査フィルターが表示されます。

| ARP 検査フィルタテーブル | |
|---|---|
| VLAN ID | ARP アクセスリストを適用する VLAN ID が表示されます。 |
| ARP アクセスリスト名 | ARP アクセスリストの名前が表示されます。 |
| スタティック ACL | ARP アクセスリストのスタティック ACL の状態（対応／非対応）が表示されます。 |

## 8.8.3. ポート設定

［ポート設定］ページで、ダイナミック ARP 検査でのポートの信頼状態を設定します。


| ARP 検査ポート設定 | |
|---|---|
| ポート | スイッチのポート番号を選択します。 |
| 信頼ポート | 信頼ポートの状態（信頼する／信頼しない）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［初期値に設定］ボタン | ［初期値に設定］ボタンをクリックすると、各ポートの信頼ポートの設定が初期値に戻ります。 |

各ポートの信頼状態は、画面下部にテーブルで表示されます。

## 8.8.4. 対象 VLAN

［対象 VLAN］ページで、ダイナミック ARP 検査の対象 VLAN を設定します。

| ARP 検査対象 VLAN 設定 | |
|---|---|
| VLAN ID リスト | ダイナミック ARP 検査の対象にする VLAN ID を入力します。 |
| 状態 | ARP 検査対象 VLAN の状態（有効／無効）を選択します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| ARP 検査対象 VLAN リスト | |
|---|---|
| ARP 検査対象 VLAN | ARP 検査対象 VLAN に設定した VLAN ID が表示されます。 |

## 8.8.5. 統計情報

［統計情報］ページで、ダイナミック ARP 検査によるヒット件数の統計情報を表示します。


| ARP 検査統計情報 | |
|---|---|
| VLAN ID リスト | 統計情報をクリアする VLAN ID を入力します。 |
| ［クリア］ボタン | ［クリア］ボタンをクリックすると、入力した VLAN ID の統計情報がクリアされます。 |
| ［全てクリア］ボタン | ［全てクリア］ボタンをクリックすると、すべての統計情報がクリアされます。 |

| ARP 検査統計情報テーブル | |
|---|---|
| VLAN ID | ダイナミック ARP 検査対象の VLAN ID が表示されます。 |
| 転送 | 転送数が表示されます。 |
| 廃棄 | 廃棄数が表示されます。 |
| DHCP 廃棄数 | バインディングデータベース参照による廃棄数が表示されます。 |
| ACL 廃棄数 | ARP アクセスリスト参照による廃棄数が表示されます。 |
| DHCP 許可数 | バインディングデータベース参照による許可数が表示されます。 |
| ACL 許可数 | ARP アクセスリスト参照による許可数が表示されます。 |
| 送信元 MAC 廃棄数 | 送信元 MAC 検証による廃棄数が表示されます。 |
| 宛先 MAC 廃棄数 | 宛先 MAC 検証による廃棄数が表示されます。 |
| IP 廃棄数 | IP アドレス検証による廃棄数が表示されます。 |

## 8.8.6. ARP 検査ログ

［ARP 検査ログ］ページで、ダイナミック ARP 検査の ARP 検査ログを表示します。
ARP 検査ログは、［基本設定］ページの［ARP 検査ログ設定］に従って記録されます。


| ARP 検査ログ | |
|---|---|
| ログバッファ（1-1024） | ARP 検査ログの収容件数を 1～1024 の範囲で入力します。（デフォルト：32） |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |
| ［クリア］ボタン | ［クリア］ボタンをクリックすると、ARP 検査ログがクリアされます。 |

| ARP 検査ログテーブル | |
|---|---|
| ポート | ポート番号が表示されます。 |
| VLAN ID | VLAN ID が表示されます。 |
| 送信元 IP アドレス | 送信元 IP アドレスが表示されます。 |
| 送信元 MAC アドレス | 送信元 MAC アドレスが表示されます。 |
| 発生記録 | 発生状態が表示されます。 |

# 8.9. アクセスコントロールリスト

アクセスコントロールリスト（ACL）は、入力するパケットのヘッダー情報を参照し、転送やブロックなどの動作を決定する機能です。パケットが ACL ルールに定められた内容に合致すると、ACL ルールのアクションで定められた内容に従って処理します。

ACL には、大きく分類して「プロファイル」「ルール」の 2 種類の設定があります。
ACL プロファイルは、ACL 機能で入力パケットのどの部分とビットを参照するかというフィルター条件を定めたものです。ACL ルールは、具体的なフィルター内容やアクションを定めたものです。

ACL ルールは ACL プロファイル上に登録されますが、プロファイルのフィルター条件に該当しないルールは登録することができません。たとえば、宛先 MAC アドレスを参照しないフィルター条件のプロファイルを作成した場合、そのプロファイル上で宛先 MAC アドレスを指定するルールを登録することはできません。

## 8.9.1. ACL 設定ウィザード

［ACL 設定ウィザード］は、簡易な ACL ルールを自動的に作成するツールです。
必要な ACL プロファイルも自動的に作成されるため、プロファイルやルールの構成を意識することなく ACL 機能を使用することができます。
詳細な ACL ルールが必要な場合や、ルールを変更する場合は、［ACL 詳細設定］ページから設定してください。


| ACL ルール作成 | |
|---|---|
| タイプ選択 | ACL ルールのタイプ（L2 ルール／L3 ルール）を選択します。 |
| 送信元 | ACL ルールの対象とする送信元のタイプを選択します。 |
| 宛先 | ACL ルールの対象とする宛先のタイプを選択します。 |
| タイプ | ACL ルールでフィルタリングするサービスのタイプを選択します。 |
| アクション | すべての条件が満たされた場合、ACL ルールで実行するアクションを選択します。 |

| | |
|---|---|
| | • 許可：パケットを転送する<br>• ブロック：パケットを破棄する<br>• 帯域制限：レート制限を行う<br>• DSCP 変更： DSCP 値を割り当てる |
| ポート | 構成するポートまたはポートの範囲を入力します。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、ACL ルールが作成されます。 |
| ［取消］ボタン | ［取消］ボタンをクリックすると、入力がリセットされます。 |

## 8.9.2. ACL 詳細設定

［ACL 詳細設定］ページでは、ACL プロファイルおよび ACL ルールを作成することができます。
ACL 設定ウィザードでは設定できない細かいルールを指定する場合や、ルールを編集する場合に使用します。


| L2 プロファイルリスト／L3 プロファイルリスト | |
|---|---|
| ［新規作成］ボタン | ［新規作成］ボタンをクリックすると、ACL プロファイルを作成できます。 |
| ［全削除］ボタン | ［全削除］ボタンをクリックすると、全 ACL プロファイルが削除されます。 |
| プロファイル ID | プロファイル ID 番号が表示されます。 |
| タイプ | ACL プロファイルのタイプが表示されます。 |
| フィルター条件 | ACL プロファイルのフィルター条件の概要が表示されます。 |
| アクション | ［詳細］ボタンをクリックすると、ACL プロファイルの詳細情報が表示されます。<br>［ルール編集/作成］ボタンをクリックすると、ACL プロファイルの ACL ルールを作成または変更できます。<br>［削除］ボタンをクリックすると、ACL プロファイルが削除されます。 |

プロファイルリストテーブルの［ルール編集/作成］ボタンをクリックすると、ACL プロファイルの ACL ルールを作成または変更できます。


| ACL ルールテーブル | |
|---|---|
| プロファイル ID | ACL プロファイル ID 番号が表示されます。 |
| アクセス ID | ACL ルールのアクセス ID が表示されます。ルールを作成する際にアクセス ID を自動もしくは手動で割り当てます。<br>表示されたアクセス ID は ACL ルールにリンクしており、クリックすると、ルール内容の確認や修正を行うことができます。 |
| タイプ | ACL プロファイルのタイプが表示されます。 |
| フィルター条件 | ACL プロファイルのフィルター条件の概要が表示されます。 |
| アクション | ACL ルールで実行するアクションを表示します。 |
| ［削除］ボタン | ［削除］ボタンをクリックすると、ACL ルールを削除します。 |
| ［戻る］ボタン | ［戻る］ボタンをクリックすると、［ACL 詳細設定］ページに戻ります。 |
| ［ルール追加］ボタン | ［ルール追加］ボタンをクリックすると、ACL ルールを新たに作成することができます。 |

## 8.9.3. ACL ルール検索

［ACL ルール検索］ページでは、ACL ルールを検索して表示します。

例えば、特定のポートに適用されているすべての ACL ルールを探す場合、［ACL 詳細設定］ページから検索しようとすると、ACL プロファイル単位や ACL ルール単位で異なるページを調査する必要があり、多数のルールが登録されていると調査に時間がかかります。ACL ルール検索を使用すると、絞り込みを容易に行うことができます。


| ACL ルールテーブル | |
|---|---|
| タイプ | 検索する ACL ルールのタイプ（L2 ルール／L3 ルール）を選択します。 |
| プロファイル ID | プロファイル ID 番号を選択します。 |
| ポート | ACL ルールを検索するポート番号を入力します。 |
| ［検索］ボタン | ［検索］ボタンをクリックすると、指定したプロファイル ID 番号およびポート番号の ACL ルールを検索できます。 |

| テーブル | |
|---|---|
| プロファイル ID | プロファイル ID 番号が表示されます。 |
| アクセス ID | ACL ルールのアクセス ID が表示されます。<br>表示されたアクセス ID は ACL ルールにリンクしており、クリックすると、ルール内容の確認や修正を行うことができます。 |
| タイプ | ACL プロファイルのタイプが表示されます。 |
| フィルター対象 | ACL プロファイルのサマリーが表示されます。 |
| アクション | ACL プロファイルのステータスが表示されます。 |
| ［削除］ボタン | ［削除］ボタンをクリックすると、ACL プロファイルが削除されます。 |

# 9. ツール

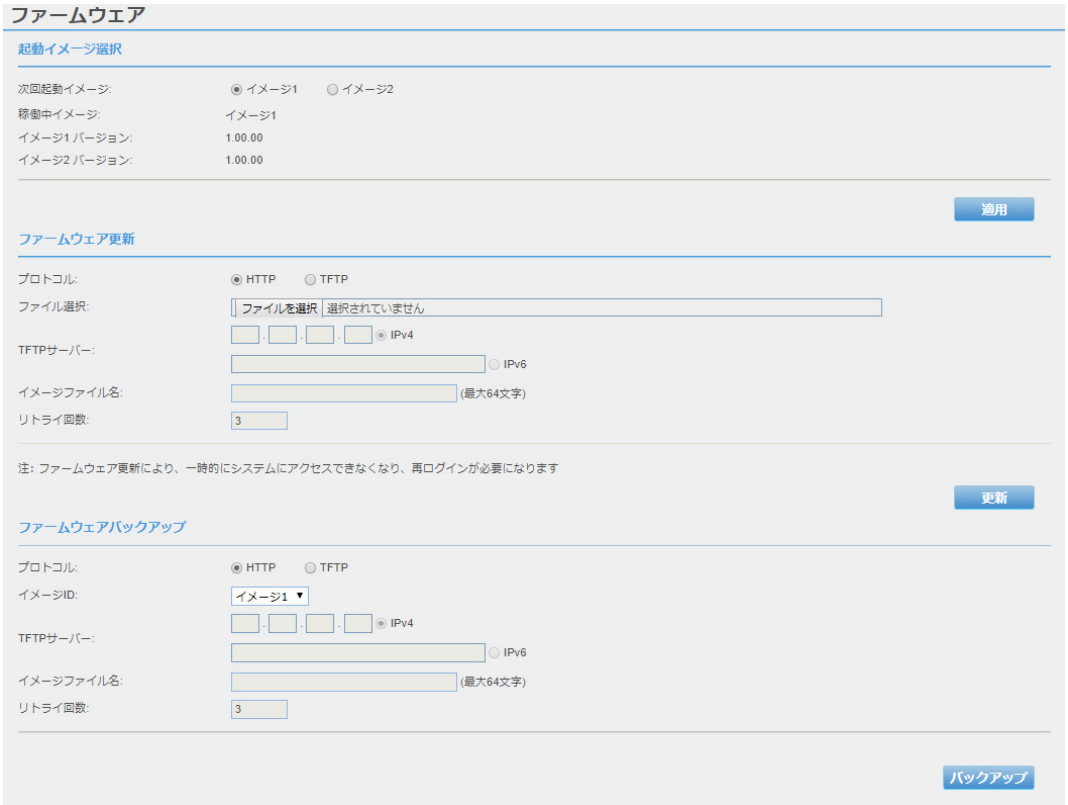
## 9.1. ファームウェア

［ファームウェア］ページで、スイッチのファームウェアを更新することができます。また、ファームウェアのバックアップや起動時のファームウェアの選択を行うことができます。

スイッチは内部に 2 個のファームウェア（イメージ）を格納可能で、そのうちの 1 個を起動時に適用するイメージとして指定します。
ファームウェアの更新は、稼働中のイメージとは別のイメージに対して行われます。ファームウェアの更新を実行した後、更新したイメージでスイッチを稼働させる場合は、次回起動イメージを変更して再起動する必要があります。

**重要な注意事項：**

- ファームウェアの更新プロセスを中断したり、更新プロセス中にリセットボタンを押したりしないでください。ファームウェアの更新プロセス中に中断が発生すると、スイッチが破損する可能性があります。




| 起動イメージ選択 | |
|---|---|
| 次回起動イメージ | スイッチの再起動後に使用するファームウェアイメージ（イメージ 1／イメージ 2）を選択します。 |
| 稼働中イメージ | スイッチが実行している現在のファームウェアイメージが表示されます。 |

| | |
|---|---|
| イメージ 1 バージョン | イメージ 1 のバージョンが表示されます。 |
| イメージ 2 バージョン | イメージ 2 のバージョンが表示されます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| ファームウェア更新 | |
|---|---|
| プロトコル | ファームウェア更新で使用するプロトコル（HTTP／TFTP）を指定します。 |
| ファイル選択 | プロトコルで HTTP を指定した場合に使用します。<br>［ファイルを選択］ボタンをクリックし、作業 PC 上のファームウェアファイル（*.hex）を選択します。 |
| TFTP サーバー | プロトコルで TFTP を指定した場合に使用します。<br>［IPv4］または［IPv6］を選択し、TFTP サーバーの IP アドレスを入力します。<br>Note: ファームウェアファイル（*.hex）は、TFTP サーバーのルートディレクトリーに配置してください。 |
| イメージファイル名 | プロトコルで TFTP を指定した場合に使用します。<br>TFTP サーバーのルートディレクトリーに配置したファームウェアのファイル名を、拡張子（.hex）付きで入力します。 |
| リトライ回数 | プロトコルで TFTP を指定した場合に使用します。<br>TFTP サーバーが要求に応答しない場合に、TFTP のリトライ回数を入力します。 |
| ［更新］ボタン | ［更新］ボタンをクリックすると、ファームウェアが更新されます。 |

| ファームウェアバックアップ | |
|---|---|
| プロトコル | ファームウェアバックアップで使用するプロトコル（HTTP／TFTP）を指定します。 |
| イメージ ID | バックアップするファームウェアイメージ（イメージ 1／イメージ 2）を選択します。 |
| TFTP サーバー | プロトコルで TFTP を指定した場合に使用します。<br>［IPv4］または［IPv6］を選択し、TFTP サーバーの IP アドレスを入力します。 |
| イメージファイル名 | プロトコルで TFTP を指定した場合に使用します。<br>バックアップした際のファームウェアのファイル名を入力します。 |
| ［バックアップ］ボタン | ［バックアップ］ボタンをクリックすると、選択したファームウェアイメージがバックアップされます。 |

# 9.2. 設定情報

変更した設定情報は、スイッチが継続して稼働している間は反映された状態になりますが、スイッチが再起動した後も反映させるためには設定情報を保存する必要があります。

スイッチの設定情報は設定ファイルとして保存されます。設定ファイルは、アクセスしている PC や TFTP サーバー上にバックアップすることができます。また、バックアップした設定ファイルを使用して設定情報をレストアすることも可能です。

スイッチは内部に 2 個の設定ファイルを格納可能で、そのうちの 1 個を起動時に適用する設定ファイルとして指定します。

## 9.2.1. バックアップ/レストア

［バックアップ/レストア］ページで、現在の設定ファイルをバックアップしたり、バックアップした設定ファイルをスイッチにレストアしたりすることができます。


| 起動時設定ファイル選択 | |
|---|---|
| 次回起動設定ファイル | スイッチの再起動後に使用する設定ファイル（設定 1／設定 2）を選択します。 |
| 稼働中設定ファイル | スイッチが実行している現在の設定ファイルが表示されます。 |
| ［適用］ボタン | ［適用］ボタンをクリックすると、変更が適用されます。 |

| 設定バックアップ | |
|---|---|
| プロトコル | 設定バックアップで使用するプロトコル（HTTP／TFTP）を指定します。 |

| | |
|---|---|
| 設定ファイル | バックアップする設定ファイルを選択します。<br>［次回起動時設定］がチェックされている場合、次回起動時設定に指定されている設定ファイルを自動的に選択します。 |
| TFTP サーバー | プロトコルで TFTP を指定した場合に使用します。<br>［IPv4］または［IPv6］を選択し、TFTP サーバーの IP アドレスを入力します。 |
| ファイル名 | プロトコルで TFTP を指定した場合に使用します。<br>バックアップした際の設定ファイルのファイル名を入力します。。 |
| ［バックアップ］ボタン | ［バックアップ］ボタンをクリックすると、指定した設定ファイルがバックアップされます。 |

| **設定レストア** | |
|---|---|
| プロトコル | 設定レストアで使用するプロトコル（HTTP／TFTP）を指定します。 |
| 設定ファイル | レストア先の設定ファイルを選択します。<br>［次回起動時設定］がチェックされている場合、次回起動時設定に指定されている設定ファイルを自動的に選択します。 |
| ファイル選択 | プロトコルで HTTP を指定した場合に使用します。<br>［ファイルを選択］ボタンをクリックし、作業 PC 上の設定ファイルを選択します。 |
| TFTP サーバー | プロトコルで TFTP を指定した場合に使用します。<br>［IPv4］または［IPv6］を選択し、TFTP サーバーの IP アドレスを入力します。<br>Note: 設定ファイルは、TFTP サーバーのルートディレクトリーに配置してください。 |
| ファイル名 | プロトコルで TFTP を指定した場合に使用します。<br>TFTP サーバーのルートディレクトリーに配置した設定ファイルのファイル名を入力します |
| ［レストア］ボタン | ［レストア］ボタンをクリックすると、選択した設定ファイルのすべての設定情報がスイッチにレストアされます。 |

## 9.2.2. 設定保存

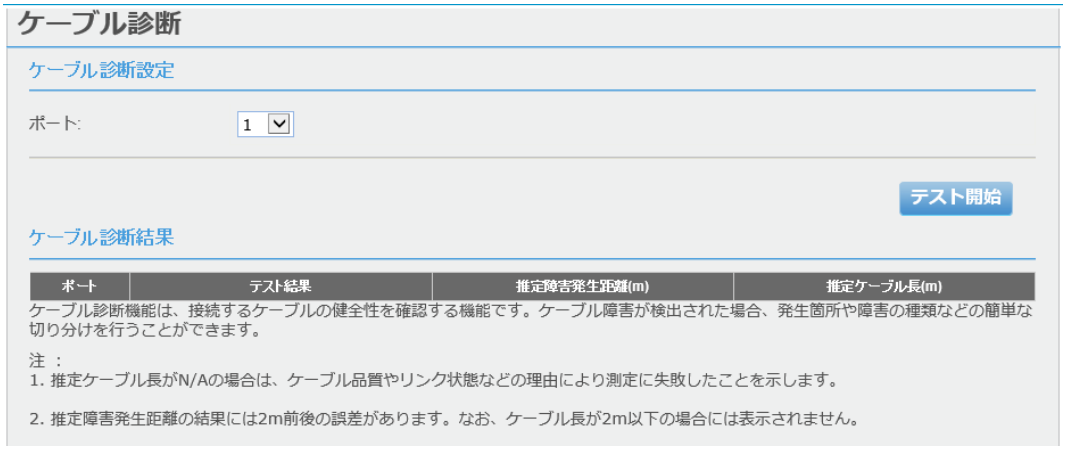
［設定保存］ページで、現在の設定情報を設定ファイルに反映します。


| 設定保存 | |
|---|---|
| 設定ファイル | 現在の設定情報を反映する設定ファイルを選択します。<br>［次回起動時設定］がチェックされている場合、次回起動時設定に指定されている設定ファイルを自動的に選択します。 |
| ［保存］ボタン | ［保存］ボタンをクリックすると、構成設定の変更がすべてフラッシュメモリーに保存されます。<br>Note: スイッチを再起動する前に設定保存を実行してください。事前に現在の設定を保存していないと、再起動後に設定変更情報がすべて失われます。<br>Info: 構成設定の保存には数秒間かかります。構成設定が保存されると、完了を示すダイアログボックスが表示されます。 |

# 9.3. ケーブル診断

［ケーブル診断］ページでは、ケーブル診断機能を実行することができます。
ケーブル診断機能を利用すると、ツイストペアケーブルのテストや検証を行うことができます。これにより、ケーブルの品質やエラーのタイプをすばやく特定できます。ケーブル診断機能は、対向デバイスと接続されている状態であれば、リンクが確立されていない状態でも動作します。

Note: テストではケーブルの問題発生場所も測定されます。問題発生場所は本スイッチからの距離で特定されます。



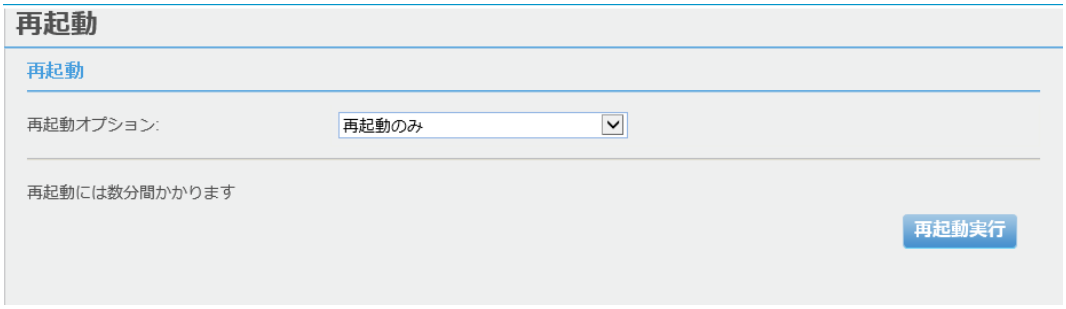

| ケーブル診断設定 | |
|---|---|
| ポート | テストするポートを選択します。 |
| ［テスト開始］ボタン | ［テスト開始］ボタンをクリックすると、診断処理が行われます。 |

| ケーブル診断結果 | |
|---|---|
| ポート | 選択したポート番号が表示されます。 |
| テスト結果 | 各ツイストペアケーブルの診断結果が表示されます。 |
| 推定障害発生距離(m) | ケーブルの問題位置がスイッチポートからの距離で表示されます。<br>ケーブルの問題位置の距離には±2 メートル程度の誤差があります。<br>そのため、使用されているケーブル長が 2 メートル未満の場合はテスト結果に表示されないことがあります。 |
| 推定ケーブル長(m) | テスト結果に［OK］と表示されている場合、スイッチポートに接続されているケーブルの合計長が表示されます。<br>Not Available（利用不可）を意味する［N/A］と表示される場合は、以下のいずれかの理由でケーブル長が特定されていません。<br>・ リンク速度が 1 Gbps 未満である<br>・ ケーブルが破損している<br>・ ケーブルが低品質である |

ケーブル診断結果の例は以下のとおりです。

# 9.4. 再起動

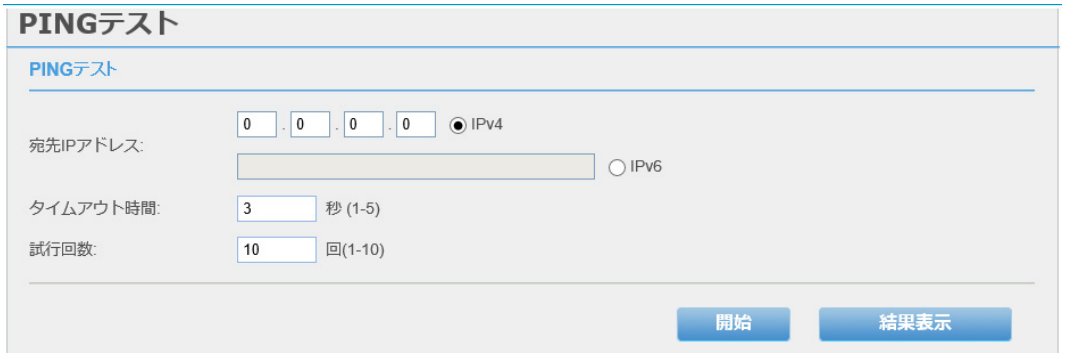
［再起動］ページで、スイッチを再起動することができます。
また、再起動オプションを指定して、再起動時に工場出荷時のデフォルト設定に戻すことも可能です。




| 再起動 | |
|---|---|
| 再起動オプション | 再起動のタイプを選択します。<br>・ 再起動のみ：<br>再起動の際、事前に構成を保存したことを確認してください。構成を保存していないと、変更は保持されません。スイッチを再起動する前に設定を保存してください。<br>・ 初期化して再起動：<br>再起動の際、設定がすべてリセットされます。<br>・ IP アドレス以外を初期化して再起動：<br>再起動の際、スイッチの IP アドレスの設定のみが保持され、ほかの設定はすべてリセットされます。 |
| ［再起動実行］ボタン | ［再起動実行］ボタンをクリックすると、スイッチが再起動します。 |

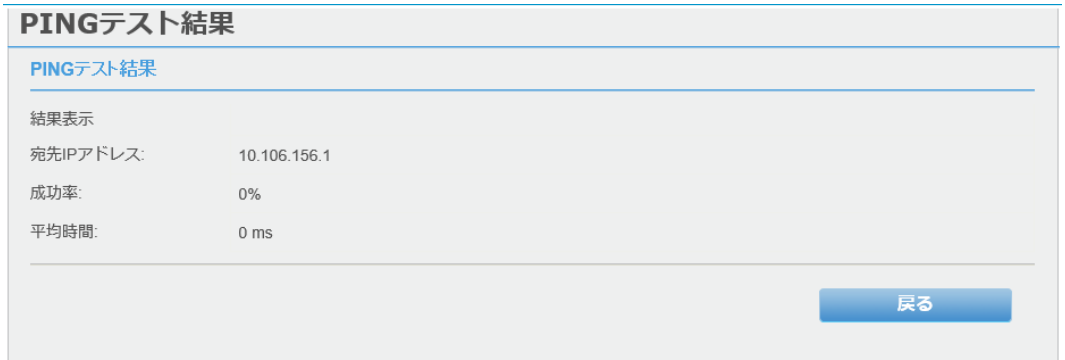
# 9.5. Ping

［Ping］ページで、スイッチから PING テストを実行することができます。




| PING テスト | |
|---|---|
| 宛先 IP アドレス | ［IPv4］または［IPv6］を選択し、ターゲットの IP アドレスを入力します。 |
| タイムアウト時間 | Ping が失敗したと判定する前にノードからの応答を待機する時間を 1～5（秒）の範囲で入力します。（デフォルト：3 秒） |
| 試行回数 | Ping の実行回数を 1～10（回）の範囲で入力します。（デフォルト：10 回） |
| ［開始］ボタン | ［開始］ボタンをクリックすると、Ping テストが実行されます。 |
| ［結果表示］ボタン | ［結果表示］ボタンをクリックすると、Ping テスト結果が表示されます。 |

Ping テスト結果の例は以下のとおりです。




| PING テスト結果 | |
|---|---|
| 宛先 IP アドレス | ［PING テスト］ページで指定した宛先 IP アドレスが表示されます。 |
| 成功率 | 成功率が%で表示されます。 |
| 平均時間 | Ping 応答を受信するまでの平均時間（ミリ秒）が表示されます。 |
| ［戻る］ボタン | ［戻る］ボタンをクリックすると、［PING テスト］ページに戻ります。 |

# Appendix A 標準 MIB の実装情報

本スイッチに実装する標準 MIB の情報を記載します。
各オブジェクトの説明は、関連する規格をご確認ください。

| SNMPv2-MIB | |
|---|---|
| system<br>(1.3.6.1.2.1.1) | sysDescr, sysObjectID, sysUpTime, sysContact, sysName,<br>sysLocation, sysServices, sysORLastChange, sysORIndex, sysORID,<br>sysORDescr, sysORUpTime |
| snmp<br>(1.3.6.1.2.1.11) | snmpInPkts, snmpOutPkts, snmpInBadVersions,<br>snmpInBadCommunityNames, snmpInBadCommunityUses,<br>snmpInASNParseErrs, snmpInTooBigs, snmpInNoSuchNames,<br>snmpInBadValues, snmpInReadOnlys, snmpInGenErrs,<br>snmpInTotalReqVars, snmpInTotalSetVars, snmpInGetRequests,<br>snmpInGetNexts, snmpInSetRequests, snmpInGetResponses,<br>snmpInTraps, snmpOutTooBigs, snmpOutNoSuchNames,<br>snmpOutBadValues, snmpOutGenErrs, snmpOutGetRequests,<br>snmpOutGetNexts, snmpOutSetRequests, snmpOutGetResponses,<br>snmpOutTraps, snmpEnableAuthenTraps, snmpSilentDrops,<br>snmpProxyDrops |

| IF-MIB | |
|---|---|
| interface<br>(1.3.6.1.2.1.2) | ifNumber, ifIndex, ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress,<br>ifAdminStatus, ifOperStatus, ifLastChange, ifInOctets,<br>ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifInErrors,<br>ifInUnknownProtos, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts,<br>ifOutDiscards, ifOutErrors, ifOutQLen, ifSpecific |
| ifMIB/ifMIBObjects<br>(1.3.6.1.2.1.31.1) | ifName, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts,<br>ifOutBroadcastPkts, ifHCInOctets, ifHCInUcastPkts,<br>ifHCInMulticastPkts, ifHCInBroadcastPkts, ifHCOutOctets,<br>ifHCOutUcastPkts, ifHCOutMulticastPkts, ifHCOutBroadcastPkts,<br>ifLinkUpDownTrapEnable, ifHighSpeed, ifPromiscuousMode,<br>ifConnectorPresent, ifAlias, ifCounterDiscontinuityTime,<br>ifStackHigherLayer, ifStackLowerLayer, ifStackStatus,<br>ifRcvAddressAddress, ifRcvAddressStatus, ifRcvAddressType,<br>ifTableLastChange, ifStackLastChange |

| IP-MIB | |
|---|---|
| ip<br>(1.3.6.1.2.1.4) | ipForwarding, ipDefaultTTL, ipInReceives, ipInHdrErrors,<br>ipInAddrErrors, ipForwDatagrams, ipInUnknownProtos, ipInDiscards, |

| | |
|---|---|
| | ipInDelivers, ipOutRequests, ipOutDiscards, ipOutNoRoutes, ipReasmTimeout, ipReasmReqds, ipReasmOKs, ipReasmFails, ipFragOKs, ipFragFails, ipFragCreates, ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask, ipAdEntBcastAddr, ipAdEntReasmMaxSize, ipRouteDest, ipRouteIfIndex, ipRouteMetric1, ipRouteMetric2, ipRouteMetric3, ipRouteMetric4, ipRouteNextHop, ipRouteType, ipRouteProto, ipRouteAge, ipRouteMask, ipRouteMetric5, ipRouteInfo, ipNetToMediaIfIndex, ipNetToMediaPhysAddress, ipNetToMediaNetAddress, ipNetToMediaType, ipRoutingDiscards |
| icmp (1.3.6.1.2.1.5) | icmpInMsgs, icmpInErrors, icmpInDestUnreachs, icmpInTimeExcds, icmpInParmProbs, icmpInSrcQuenchs, icmpInRedirects, icmpInEchos, icmpInEchoReps, icmpInTimestamps, icmpInTimestampReps, icmpInAddrMasks, icmpInAddrMaskReps, icmpOutMsgs, icmpOutErrors, icmpOutDestUnreachs, icmpOutTimeExcds, icmpOutParmProbs, icmpOutSrcQuenchs, icmpOutRedirects, icmpOutEchos, icmpOutEchoReps, icmpOutTimestamps, icmpOutTimestampReps, icmpOutAddrMasks, icmpOutAddrMaskReps |

| TCP-MIB | |
|---|---|
| tcp (1.3.6.1.2.1.6) | tcpRtoAlgorithm, tcpRtoMin, tcpRtoMax, tcpMaxConn, tcpActiveOpens, tcpPassiveOpens, tcpAttemptFails, tcpEstabResets, tcpCurrEstab, tcpInSegs, tcpOutSegs, tcpRetransSegs, tcpConnState, tcpConnLocalAddress, tcpConnLocalPort, tcpConnRemAddress, tcpConnRemPort, tcpInErrs, tcpOutRsts |

| UDP-MIB | |
|---|---|
| udp (1.3.6.1.2.1.7) | udpInDatagrams, udpNoPorts, udpInErrors, udpOutDatagrams, udpLocalAddress, udpLocalPort |

| EtherLike-MIB | |
|---|---|
| transmission/dot3 (1.3.6.1.2.1.10.3) | dot3StatsIndex, dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsSingleCollisionFrames, dot3StatsMultipleCollisionFrames, dot3StatsSQETestErrors, dot3StatsDeferredTransmissions, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors, dot3StatsCarrierSenseErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveErrors, dot3StatsEtherChipSet, dot3StatsSymbolErrors, |

| | |
|---|---|
| | dot3StatsDuplexStatus, dot3CollCount, dot3CollFrequencies, dot3ControlFunctionsSupported, dot3ControlInUnknownOpcodes, dot3PauseAdminMode, dot3PauseOperMode, dot3InPauseFrames, dot3OutPauseFrames |

| BRIDGE-MIB | |
|---|---|
| dot1dBridge/dot1dBase (1.3.6.1.2.1.17.1) | dot1dBaseBridgeAddress, dot1dBaseNumPorts, dot1dBaseType, dot1dBasePort, dot1dBasePortIfIndex, dot1dBasePortCircuit, dot1dBasePortDelayExceededDiscards, dot1dBasePortMtuExceededDiscards |
| dot1dBridge/dot1dStp (1.3.6.1.2.1.17.2) | dot1dStpProtocolSpecification, dot1dStpPriority, dot1dStpTimeSinceTopologyChange, dot1dStpTopChanges, dot1dStpDesignatedRoot, dot1dStpRootCost, dot1dStpRootPort, dot1dStpMaxAge, dot1dStpHelloTime, dot1dStpHoldTime, dot1dStpForwardDelay, dot1dStpBridgeMaxAge, dot1dStpBridgeHelloTime, dot1dStpBridgeForwardDelay, dot1dStpPort, dot1dStpPortPriority, dot1dStpPortState, dot1dStpPortEnable, dot1dStpPortPathCost, dot1dStpPortDesignatedRoot, dot1dStpPortDesignatedCost, dot1dStpPortDesignatedBridge, dot1dStpPortDesignatedPort, dot1dStpPortForwardTransitions, dot1dStpVersion, dot1dStpTxHoldCount, dot1dStpPathCostDefault, dot1dStpPortProtocolMigration, dot1dStpPortAdminEdgePort, dot1dStpPortOperEdgePort, dot1dStpPortAdminPointToPoint, dot1dStpPortOperPointToPoint |
| dot1dBridge/dot1dTp (1.3.6.1.2.1.17.4) | dot1dTpLearnedEntryDiscards, dot1dTpAgingTime |

| qBRIDGE-MIB | |
|---|---|
| dot1dBridge/qBridgeMIB /qBridgeMIBObjects /dot1qTp/dotTpFdbTable (1.3.6.1.2.1.17.7.1.2.2) | dot1qTpFdbAddress, dot1qTpFdbPort, dot1qTpFdbStatus |

| LLDP-MIB | |
|---|---|
| lldpNotifications /lldpNotificationPrefix (1.0.8802.1.1.2.0.0) | lldpRemTablesChange |

| | |
|---|---|
| lldpObjects<br>/lldpConfiguration<br>(1.0.8802.1.1.2.1.1) | lldpMessageTxInterval, lldpMessageTxHoldMultiplier,<br>lldpReinitDelay, lldpTxDelay, lldpNotificationInterval,<br>lldpPortConfigPortNum, lldpPortConfigAdminStatus,<br>lldpPortConfigNotificationEnable, lldpPortConfigTLVsTxEnable,<br>lldpConfigManAddrPortsTxEnable |
| lldpObjects<br>/lldpStatistics<br>(1.0.8802.1.1.2.1.2) | lldpStatsRemTablesLastChangeTime, lldpStatsRemTablesInserts,<br>lldpStatsRemTablesDeletes, lldpStatsRemTablesDrops,<br>lldpStatsRemTablesAgeouts, lldpStatsTxPortNum,<br>lldpStatsTxPortFramesTotal, lldpStatsRxPortNum,<br>lldpStatsRxPortFramesDiscardedTotal,<br>lldpStatsRxPortFramesErrors, lldpStatsRxPortFramesTotal,<br>lldpStatsRxPortTLVsDiscardedTotal,<br>lldpStatsRxPortTLVsUnrecognizedTotal,<br>lldpStatsRxPortAgeoutsTotal |
| lldpObjects<br>/lldpLocalSystemData<br>(1.0.8802.1.1.2.1.3) | lldpLocChassisIdSubtype, lldpLocChassisId, lldpLocSysName,<br>lldpLocSysDesc, lldpLocSysCapSupported, lldpLocSysCapEnabled,<br>lldpLocPortNum, lldpLocPortIdSubtype, lldpLocPortId,<br>lldpLocPortDesc, lldpLocManAddrSubtype, lldpLocManAddr,<br>lldpLocManAddrLen, lldpLocManAddrIfSubtype, lldpLocManAddrIfId,<br>lldpLocManAddrOID |
| lldpObjects<br>/lldpRemoteSystemsData<br>(1.0.8802.1.1.2.1.4) | lldpRemTimeMark, lldpRemLocalPortNum, lldpRemIndex,<br>lldpRemChassisIdSubtype, lldpRemChassisId, lldpRemPortIdSubtype,<br>lldpRemPortId, lldpRemPortDesc, lldpRemSysName, lldpRemSysDesc,<br>lldpRemSysCapSupported, lldpRemSysCapEnabled,<br>lldpRemManAddrSubtype, lldpRemManAddr, lldpRemManAddrIfSubtype,<br>lldpRemManAddrIfId, lldpRemManAddrOID, lldpRemUnknownTLVType,<br>lldpRemUnknownTLVInfo, lldpRemOrgDefInfoOUI,<br>lldpRemOrgDefInfoSubtype, lldpRemOrgDefInfoIndex,<br>lldpRemOrgDefInfo |
| lldpObjects/lldpExtensions<br>/lldpXdot3MIB<br>(1.0.8802.1.1.2.1.5.4623) | lldpXdot3PortConfigTLVsTxEnable , lldpXdot3Compliance,<br>lldpXdot3ConfigGroup, lldpXdot3LocSysGroup, lldpXdot3RemSysGroup |
| lldpObjects/lldpExtensions<br>/lldpXMedMIB<br>(1.0.8802.1.1.2.1.5.4795) | lldpXMedTopologyChangeDetected, lldpXMedLocDeviceClass,<br>lldpXMedPortCapSupported, lldpXMedPortConfigTLVsTxEnable,<br>lldpXMedPortConfigNotifEnable, lldpXMedFastStartRepeatCount,<br>lldpXMedLocMediaPolicyAppType, lldpXMedLocMediaPolicyVlanID,<br>lldpXMedLocMediaPolicyPriority, lldpXMedLocMediaPolicyDscp,<br>lldpXMedLocMediaPolicyUnknown, lldpXMedLocMediaPolicyTagged,<br>lldpXMedLocHardwareRev, lldpXMedLocFirmwareRev, |

| | |
|---|---|
| | lldpXMedLocSoftwareRev, lldpXMedLocSerialNum, lldpXMedLocMfgName, lldpXMedLocModelName, lldpXMedLocAssetID, lldpXMedLocLocationSubtype, lldpXMedLocLocationInfo, lldpXMedLocXPoEDeviceType, lldpXMedLocXPoEPSEPortPowerAv, lldpXMedLocXPoEPSEPortPDPriority, lldpXMedLocXPoEPSEPowerSource, lldpXMedLocXPoEPDPowerReq, lldpXMedLocXPoEPDPowerSource, lldpXMedLocXPoEPDPowerPriority, lldpXMedRemCapSupported, lldpXMedRemCapCurrent, lldpXMedRemMediaPolicyAppType, lldpXMedRemMediaPolicyVlanID, lldpXMedRemMediaPolicyPriority, lldpXMedRemMediaPolicyDscp, lldpXMedRemMediaPolicyUnknown, lldpXMedRemMediaPolicyTagged, lldpXMedRemHardwareRev, lldpXMedRemFirmwareRev, lldpXMedRemSoftwareRev, lldpXMedRemSerialNum, lldpXMedRemMfgName, lldpXMedRemModelName, lldpXMedRemAssetID, lldpXMedRemLocationSubtype, lldpXMedRemLocationInfo, lldpXMedRemXPoEDeviceType, lldpXMedRemXPoEPSEPowerAv, lldpXMedRemXPoEPSEPowerSource, lldpXMedRemXPoEPSEPowerPriority, lldpXMedRemXPoEPDPowerReq, lldpXMedRemXPoEPDPowerSource, lldpXMedRemXPoEPDPowerPriority, lldpXMedCompliance, lldpXMedConfigGroup, lldpXMedOptMediaPolicyGroup, lldpXMedOptInventoryGroup, lldpXMedOptLocationGroup, lldpXMedOptPoEPSEGroup, lldpXMedOptPoEPDGroup, lldpXMedRemSysGroup, lldpXMedNotificationsGroup |
| lldpObjects/lldpExtensions /lldpXdot1MIB (1.0.8802.1.1.2.1.5.32962) | lldpXdot1ConfigPortVlanTxEnable, lldpXdot1ConfigVlanNameTxEnable, lldpXdot1ConfigProtoVlanTxEnable, lldpXdot1ConfigProtocolTxEnable, lldpXdot1LocPortVlanId, lldpXdot1LocProtoVlanId, lldpXdot1LocProtoVlanSupported, lldpXdot1LocProtoVlanEnabled, lldpXdot1LocVlanId, lldpXdot1LocVlanName, lldpXdot1LocProtocolIndex, lldpXdot1LocProtocolId, lldpXdot1RemPortVlanId, lldpXdot1RemProtoVlanId, lldpXdot1RemProtoVlanSupported, lldpXdot1RemProtoVlanEnabled, lldpXdot1RemVlanId, lldpXdot1RemVlanName, lldpXdot1RemProtocolIndex, lldpXdot1RemProtocolId, lldpXdot1Compliance, lldpXdot1ConfigGroup, lldpXdot1LocSysGroup, lldpXdot1RemSysGroup |
| lldpConformance (1.0.8802.1.1.2.2) | lldpCompliance, lldpConfigGroup, lldpConfigRxGroup, lldpConfigTxGroup, lldpStatsRxGroup, lldpStatsTxGroup, lldpLocSysGroup, lldpRemSysGroup, lldpNotificationsGroup |

# Appendix B プライベート MIB の実装情報

本スイッチで実装するプライベート MIB に関する情報を記載します。
プライベート MIB に関する詳細な内容については、MIB 定義ファイルをご確認ください。

## n 実装するプライベート MIB について

ApresiaLightGS シリーズで実装するプライベート MIB の各オブジェクトは、以下の階層に割り当てられています。

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).hitachi-cable(278)

## n 製品オブジェクト識別子

ApresiLightGS シリーズの各製品に対して、以下の製品 OID が割り当てられています。

| シリーズ名称 | 製品名称 | sysObjectID |
|---|---|---|
| ApresiaLightGS シリーズ | ApresiaLightGS110GT-SS | 1.3.6.1.4.1.278.1.43.1 |
| | ApresiaLightGS120GT-SS | 1.3.6.1.4.1.278.1.43.2 |
| | ApresiaLightGS128GT-SS | 1.3.6.1.4.1.278.1.43.3 |
| | ApresiaLightGS152GT-SS | 1.3.6.1.4.1.278.1.43.4 |

# Appendix C システムログ一覧

本スイッチが出力するシステムログを以下に記載します。

| システム起動 | |
|---|---|
| ログ表示 | System started up |
| 重要度 | Critical |
| 説明 | スイッチが起動したことを示します。 |

| ファームウェア更新成功 | |
|---|---|
| ログ表示 | Firmware upgraded successfully. |
| 重要度 | Informational |
| 説明 | ファームウェアの更新に成功したことを示します。 |

| ファームウェア更新失敗（不正なイメージファイル） | |
|---|---|
| ログ表示 | Illegal file causes firmware upgrade failure. |
| 重要度 | Warning |
| 説明 | 不正なファイルの使用によってファームウェア更新に失敗したことを示します。 |

| ファームウェア更新失敗（チェックサムエラー） | |
|---|---|
| ログ表示 | Wrong file checksum causes firmware upgrade failure. |
| 重要度 | Warning |
| 説明 | チェックサムエラーによってファームウェア更新に失敗したことを示します。 |

| ファームウェア更新失敗（ファイル転送失敗） | |
|---|---|
| ログ表示 | File transfer failed during firmware upgrade. |
| 重要度 | Warning |
| 説明 | ファイル転送の失敗によってファームウェア更新に失敗したことを示します。 |

| 設定レストア成功 | |
|---|---|
| ログ表示 | Configuration successfully restored. |
| 重要度 | Informational |
| 説明 | 設定のレストアに成功したことを示します。 |

| 設定レストア失敗 | |
|---|---|
| ログ表示 | Configuration restore was unsuccessful! |
| 重要度 | Warning |
| 説明 | 設定のレストアに失敗したことを示します。 |

| 設定バックアップ成功 | |
|---|---|
| ログ表示 | Configuration successfully backup. |
| 重要度 | Informational |
| 説明 | 設定のバックアップに成功したことを示します。 |

| 設定バックアップ失敗 | |
|---|---|
| ログ表示 | Configuration backup was unsuccessful! |
| 重要度 | Warning |
| 説明 | 設定のバックアップに失敗したことを示します。 |

| 設定保存 | |
|---|---|
| ログ表示 | Configuration saved to flash |
| 重要度 | Informational |
| 説明 | 設定をフラッシュメモリーに保存したことを示します。 |

| ポートのリンクアップ | |
|---|---|
| ログ表示 | Port <portNum> link up, <link state> |
| 重要度 | Informational |
| 説明 | ポートがリンクアップしたことを示します。<br><portNum>にはポート番号が、<link state>には通信モードが表示されます。 |

| ポートのリンクダウン | |
|---|---|
| ログ表示 | Port <portNum> link down |
| 重要度 | Informational |
| 説明 | ポートがリンクダウンしたことを示します。<br><portNum>にはポート番号が表示されます。 |

| ポートアクセス認証失敗 | |
|---|---|
| ログ表示 | 802.1x Authentication failure from (Username: <username>, Port: <portNum>, MAC: <macaddr> ) |
| 重要度 | Warning |
| 説明 | ポートアクセス認証に失敗したことを示します。<br><portNum>にはポート番号が、<username>にはユーザー名が、<macaddr>にはアクセスした機器の MAC アドレスが表示されます。 |

| ポートアクセス認証成功 | |
|---|---|
| ログ表示 | 802.1x Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>) |
| 重要度 | Informational |
| 説明 | ポートアクセス認証に成功したことを示します。<br><portNum>にはポート番号が、<username>にはユーザー名が、<macaddr>にはアクセスした機器の MAC アドレスが表示されます。 |

| ポートアクセス認証（MAC 認証）成功 | |
|---|---|
| ログ表示 | 802.1x Authentication in MAC mode success from (Port: <portNum>, MAC: <macaddr>) |
| 重要度 | Informational |
| 説明 | ポートアクセス認証（MAC 認証）に成功したことを示します。<br><portNum>にはポート番号が、<macaddr>にはアクセスした機器の MAC アドレスが表示されます。 |

| ポートアクセス認証（MAC 認証）失敗 | |
|---|---|
| ログ表示 | 802.1x Authentication in MAC mode failure from ( Port: <portNum>, MAC: <macaddr>) |
| 重要度 | Informational |
| 説明 | ポートアクセス認証（MAC 認証）に失敗したことを示します。<br><portNum>にはポート番号が、<macaddr>にはアクセスした機器の MAC アドレスが表示されます。 |

| ポートアクセス認証失敗（エントリー競合） | |
|---|---|
| ログ表示 | 802.1x Authentication failure by adding a static entry ( Port: <portNum>, MAC: <macaddr>) because it had been added by { DHCP Binding Entries\| Static Unicast Address} with different information. |
| 重要度 | Warning |
| 説明 | バインディングデータベースやスタティックエントリーとの競合によってポートアクセス認証に失敗したことを示します。<br><portNum>にはポート番号が、<macaddr>にはアクセスした機器の MAC アドレスが表示されます。 |

| ポートアクセス認証失敗（エントリー上限） | |
|---|---|
| ログ表示 | 802.1x Authentication failure by adding a static entry ( Port: <portNum>, MAC: <macaddr>) because the entry size is approaching to mixiumum. |
| 重要度 | Informational |
| 説明 | エントリー上限によってポートアクセス認証）に失敗したことを示します。<br><portNum>にはポート番号が、<macaddr>にはアクセスした機器の MAC アドレスが表示されます。 |

| LAG ポートのリンクアップ | |
|---|---|
| ログ表示 | Trunk group <id> link up |
| 重要度 | Informational |
| 説明 | LAG ポートがリンクアップしたことを示します。<br><id>には LAG のグループ ID が表示されます。 |

| LAG ポートのリンクダウン | |
|---|---|
| ログ表示 | Trunk group <id> link down |
| 重要度 | Informational |
| 説明 | LAG ポートがリンクダウンしたことを示します。<br><id>には LAG のグループ ID が表示されます。 |

| トポロジー変更発生 | |
|---|---|
| ログ表示 | Topology changed [( port:< portNum>)] |
| 重要度 | Informational |
| 説明 | スパニングツリーでのトポロジー変更が発生したことを示します。<br><portNum>にはポート番号が表示されます。 |

| 新規ルートブリッジ選択 | |
|---|---|
| ログ表示 | New Root bridge selected (MAC: <macaddr> Priority :<value>) |
| 重要度 | Informational |
| 説明 | スパニングツリーで新規ルートブリッジが選択されたことを示します。<br><macaddr>には MAC アドレスが、<value>にはブリッジ優先度が表示されます。 |

| スパニングツリー有効化 | |
|---|---|
| ログ表示 | Spanning Tree Protocol is enabled |
| 重要度 | Informational |
| 説明 | STP 機能を有効にしたことを示します。 |

| スパニングツリー無効化 | |
|---|---|
| ログ表示 | Spanning Tree Protocol is disabled |
| 重要度 | Informational |
| 説明 | STP 機能を無効にしたことを示します。 |

| ログイン成功 | |
|---|---|
| ログ表示 | Successful login through web(User: <username>) |
| 重要度 | Informational |
| 説明 | スイッチへのログインが成功したことを示します。<br><username>にはユーザー名が表示されます。 |

| ログイン失敗 | |
|---|---|
| ログ表示 | Login failed through web |
| 重要度 | Alert |
| 説明 | スイッチへのログインが成功したことを示します。 |

| ログイン成功（HTTPS） | |
|---|---|
| ログ表示 | Successful login through web(SSL)(User: <username>) |
| 重要度 | Informational |
| 説明 | HTTPS によるスイッチへのログインが成功したことを示します。<br><username>にはユーザー名が表示されます。 |

| ログイン失敗（HTTPS） | |
|---|---|
| ログ表示 | Login failed through web(SSL) |
| 重要度 | Alert |
| 説明 | HTTPS によるスイッチへのログインが失敗したことを示します。 |

| ログイン成功（TELNET） | |
|---|---|
| ログ表示 | Successful login through telnet ( IPv4/Ipv6: <ipaddr> ) |
| 重要度 | Informational |
| 説明 | TELNET によるログインが成功したことを示します。<br><ipaddr>には接続した機器の IP アドレスが表示されます。 |

| ログイン失敗（TELNET） | |
|---|---|
| ログ表示 | Login failed through telnet ( IPv4/Ipv6: <ipaddr> ) |
| 重要度 | Warning |
| 説明 | TELNET によるログインが失敗したことを示します。<br><ipaddr>には接続した機器の IP アドレスが表示されます。 |

| ログアウト発生（TELNET） | |
|---|---|
| ログ表示 | Logout through telnet ( IPv4/Ipv6: <ipaddr> ) |
| 重要度 | Informational |
| 説明 | TELNET のログアウトが発生したことを示します。<br><ipaddr>には接続した機器の IP アドレスが表示されます。 |

| タイムアウト発生（TELNET） | |
|---|---|
| ログ表示 | Telnet timeout ( IPv4/Ipv6: <ipaddr> ) |
| 重要度 | Informational |
| 説明 | TELNET のタイムアウトが発生したことを示します。<br><ipaddr>には接続した機器の IP アドレスが表示されます。 |

| 不正なコミュニティー名による SNMP 要求 | |
|---|---|
| ログ表示 | SNMP request received with invalid community string! |
| 重要度 | Informational |
| 説明 | 不正なコミュニティー名を使用した SNMP 要求を受信したことを示します。 |

| パスワード変更 | |
|---|---|
| ログ表示 | Password was changed |
| 重要度 | Alert |
| 説明 | パスワードが変更されたことを示します。 |

| ログイン成功（SSH） | |
|---|---|
| ログ表示 | Successful login through Ssh(User: <username>, IP: <ipaddr>) |
| 重要度 | Informational |
| 説明 | SSH によるログインが成功したことを示します。<br><username>にはユーザー名が、<ipaddr>には接続した機器の IP アドレスが表示されます。 |

| ログイン失敗（SSH） | |
|---|---|
| ログ表示 | Login failed through Ssh (User: <username>, IP: <ipaddr>) |
| 重要度 | Warning |
| 説明 | SSH によるログインが失敗したことを示します。<br><username>には試行したユーザー名が、<ipaddr>には接続した機器の IP アドレスが表示されます。 |

| ログアウト発生（SSH） | |
|---|---|
| ログ表示 | Logout through Ssh(User: <username>, IP: <ipaddr>) |
| 重要度 | Informational |
| 説明 | SSH のログアウトが発生したことを示します。<br><ipaddr>には接続した機器の IP アドレスが表示されます。 |

| IP アドレス変更 | |
|---|---|
| ログ表示 | Interface {STRING} IP address was changed. New IP: {IPV4} |
| 重要度 | Informational |
| 説明 | IP アドレスが変更されたことを示します。<br>{STRING}にはインターフェース名が、{IPV4}には IP アドレスが表示されます。 |

| 信頼できないポートで DHCP サーバー応答を検知 | |
|---|---|
| ログ表示 | A DHCP Server frame is received from a distrust port ( <portNum>) |
| 重要度 | Warning |
| 説明 | 信頼できないポートで DHCP サーバーからの応答を受信したことを示します。<br><portNum>にはポート番号が表示されます。 |

| 信頼できないポートの DHCP クライアントが IP アドレス取得に成功 | |
|---|---|
| ログ表示 | A DHCP Client (<MacAddr>) gets IP Address (<ipaddr>) from DHCP server successfully from a distrust port ( <portNum>) |
| 重要度 | Warning |
| 説明 | 信頼できないポートの DHCP クライアントが IP アドレスを取得したことを示します。<br><MacAddr>には DHCP クライアントの MAC アドレスが、<ipaddr>には取得した IP アドレスが、<portNum>にはポート番号が表示されます。 |

| バインディングデータベースの失効 | |
|---|---|
| ログ表示 | A Dynamic/Learned binding entry with Mac (<MacAddr>), Port ( <portNum>), IP Address ( <ipv4addr/ipv6addr>) and VLAN ( <vid>) is expired |
| 重要度 | Warning |
| 説明 | バインディングデータベースのエントリーが失効したことを示します。<br><MacAddr>には MAC アドレスが、<portNum>にはポート番号が、<ipv4addr/ipv6addr>には IP アドレスが、<vid>には VLAN ID が表示されます。 |

| バインディングデータベースとの不整合を検知 | |
|---|---|
| ログ表示 | A DHCP Client (<MacAddr>) would like to get IP Address ( <ipv4addr/ipv6addr>) from a distrust port (<portNum>) but port is incorrect |
| 重要度 | Warning |
| 説明 | バインディングデータベースの登録とは異なるポートでクライアントの通信を検知したことを示します。<br><MacAddr>には MAC アドレスが、<ipv4addr/ipv6addr>には IP アドレスが、<portNum>にはポート番号が表示されます。 |

| バインディングデータベースのエントリー上限による登録失敗 | |
|---|---|
| ログ表示 | A DHCP Client {<VLAN>} {<ipv4addr/ipv6addr>} {<MacAddr>} from a distrust port ( <portNum>) would like to add a leant entry but the dhcp binding entry is full |
| 重要度 | Warning |
| 説明 | エントリーの登録上限により、バインディングデータベースへの登録が失敗したことを示します。<br><VLAN>には VLAN ID が、<ipv4addr/ipv6addr>には IP アドレスが、<MacAddr>には MAC アドレスが、<portNum>にはポート番号が表示されます。 |

# Appendix D SNMP トラップ一覧

本スイッチが出力する SNMP トラップを以下に記載します。
各トラップの説明は、関連する規格及び MIB 定義ファイルをご確認ください。

| SNMPv2-MIB | |
|---|---|
| coldStart | 1.3.6.1.6.3.1.1.5.1 |
| warmStart | 1.3.6.1.6.3.1.1.5.2 |
| authenticationFailure | 1.3.6.1.6.3.1.1.5.5 |

| IF-MIB | |
|---|---|
| linkDown | 1.3.6.1.6.3.1.1.5.3 |
| linkUp | 1.3.6.1.6.3.1.1.5.4 |

| RMON-MIB | |
|---|---|
| risingAlarm | 1.3.6.1.2.1.16.0.1 |
| fallingAlarm | 1.3.6.1.2.1.16.0.2 |

| プライベート MIB | |
|---|---|
| getIPFromUntrustPort | 1.3.6.1.4.1.278.108.1.4.5.2 |

ApresiaLightGS シリーズ ユーザーズガイド



2019 年　1 月 初版
2019 年　4 月 第 2 版

APRESIA Systems 株式会社
東京都中央区築地二丁目 3 番 4 号
築地第一長岡ビル
https://www.apresiasystems.co.jp/