Future X Communications

NS2010VPEL Management Guide

2019 年 9 月 Ver.1.0

FXC株式会社

本マニュアルについて

■ **本マニュアルでは、**NS2010VPEL **の各種設定およびシステムの管理手順について説明します。本製品の設定および管理、イーサネットポートに管理用の端末を接続して** Web **ブラウザにより設定を行います。**

この度は、お買い上げいただきましてありがとうございます。
製品を安全にお使いいただくため、必ず最初にお読みください。

・下記事項は、安全のために必ずお守りください。

●安全のための注意事項を守る
注意事項をよくお読みください。製品全般の注意事項が記載されています。

●故障したら使わない
すぐに販売店まで修理をご依頼ください。

●万一異常が起きたら
・ 煙が出たら
・ 異常な音、においがしたら
・ 内部に水・異物が入ったら
・ 製品を高所から落としたり、破損したとき
①電源を切る
②接続ケーブルを抜く
③販売店に修理を依頼する

・下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。

●電源ケーブルや接続ケーブルを傷つけない
・ 電源ケーブルを傷つけると火災や感電の原因となります。
・ 重いものをのせたり、引っ張ったりしない。
・ 加工したり、傷つけたりしない。
・ 熱器具の近くに配線したり、加熱したりしない。

●内部に水や異物を入れない
・ 火災や感電の原因となります。
・ 万一、水や異物が入ったときは、すぐに電源を切り、販売店に点検・修理をご依頼ください。

●内部をむやみに開けない
・ 本体をむやみに開けたり改造したりすると、火災や感電の原因となります。

●落雷が発生したらさわらない
・ 落雷の恐れがあるときは、本製品や接続ケーブルに触らないでください。
感電の原因になります。

●油煙、湯気、湿気、ほこりの多い場所には設置しない
・ 火災や感電の原因となります。

・

下記の注意事項を守らないとけがをしたり、周辺の物品に損害を与える原因となります。

●ぬれた手で触らない
・ 感電の原因となります。

●電源ケーブルは必ずΦ1.6mm またはΦ2.0mm の単線ケーブル（VVF など）を使用する（NS2010VPEL）
・ 規定のケーブルを使わないと、火災や感電の原因となります。

●指定の電圧で使う
・ NS2010VPEL の電源は AC100V（50/60Hz）で使用してください。

●コンセントや配線器具の定格を超えるような接続はしない
・ 発熱による火災の原因となります。

●通風孔をふさがない
・ 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。

●RJ45 ポートには電話線コネクタを差し込まない（NS2010VPEL）
・ RJ45 ポートが損傷する場合があります。

目次

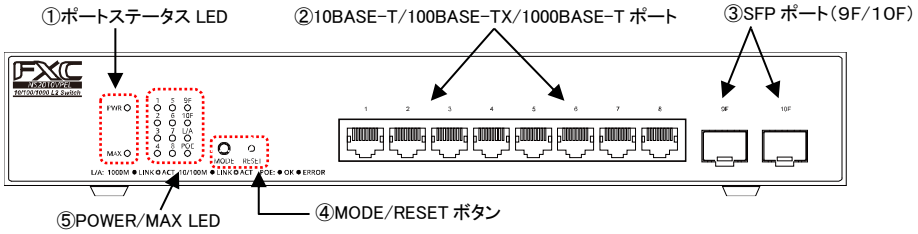
■ 1章 はじめに ■

1.1 特長

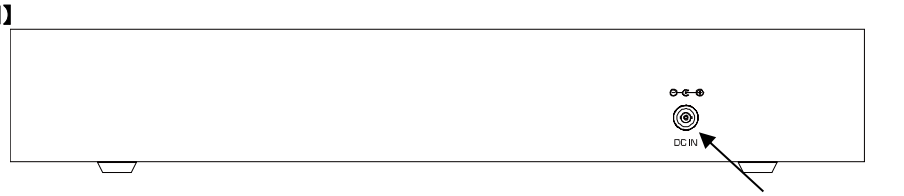
- ☐ 10/100/1000Mbps ギガビットイーサネットポート 8 ポート(PoE 給電機能付)
- ☐ 100/1000Mbps SFP スロットを 2 ポート搭載
- ☐ ジャンボフレーム(最大 10k bytes)に対応
- ☐ 8,192 個の MAC アドレスエントリーに対応
- ☐ WEB/GUI による管理画面操作に対応
- ☐ startup-config を 2 つ保存可能
- ☐ active/alternate による 2 面での firmware バックアップに対応
- ☐ IPv6 通信および IPv6 マネージメントに対応
- ☐ ファンレスによる静音設計
- ☐ IEEE802.3af/at に対応し、最大 75w 給電が可能
- ☐ PD スケジューリング機能に対応
- ☐ IEEE802.1q vlan, port-based vlan, private vlan, voice vlan に対応
- ☐ Spanning-tree Protocol (STP, RSTP)に対応
- ☐ unknown-unicast/broadcast/multicast 対応のストームコントロール機能に対応
- ☐ 検知フレームによる loop-detection 機能に対応
- ☐ MAC-based ACL , IPv4/IPv6-based ACL に対応
- ☐ 8 つの優先度キューおよび CoS/DSCP によるフロー制御に対応
- ☐ MAC-address filtering, multicast filtering などのパケットフィルタリング機能に対応
- ☐ IGMP snooping v1/v2/v3 に対応
- ☐ IEEE802.3az 準拠の EEE power-saving 機能に対応
- ☐ RoHS 準拠

1.2 各部の名称と働き

【前面図】



【背面図】



① ポートステータス LED
　各ポートの状態を示す LED ランプです。

LED 名称	色	状態	説明
Port LED (LINK/ACT)	緑	点灯	1000BASE-T リンク確立
		点滅	1000BASE-T 通信中
	橙	点灯	10/100BASE-TX リンク確立
		点滅	10/100BASE-TX 通信中
	-	消灯	接続無し
SFP Port LED (LINK/ACT)	緑	点灯	1000BASE-X リンク確立
		点滅	1000BASE-X 通信中
	橙	点灯	100BASE-FX リンク確立
		点滅	100BASE-FX 通信中
	-	消灯	接続無し
L/A、PoE	緑	L/A :点灯 PoE :消灯	各 Port LED は、リンク、通信状態を表示します。 ※MODE ボタンによりステータス表示を切り替え可能。
		L/A :消灯 PoE :点灯	各 Port LED は、PoE の給電状態を表示します。 ※MODE ボタンによりステータス表示を切り替え可能。

② 10BASE-T/100BASE-TX/1000BASE-T ポート
　10BASE-T/100BASE-TX/1000BASE-T の UTP ケーブルを接続するためのコネクタです。
　通信速度は自動的に認識されます。

③ SFP ポート（9F/10F）
　SFP モジュールの利用が可能です。

> **注意**
> **■SFP についてのご注意**
> 弊社取扱対象の SFP 製品以外については、動作保証いたしかねます。
> 対象製品情報については、弊社ホームページにてご確認ください。

④ MODE/RESET ボタン

各ボタンについて説明します。

ボタン	操作	説明
MODE	2～4 秒間長押し	ポート LED のステータス表示モードを切り替えます。 初期モード:L/A モード
RESET	1～5 秒間長押し	システムリブートを行います。
	6～10 秒間長押し	工場出荷状態にし、システムリブートを行います。

⑤ POWER/MAX LED

本体および PoE の電源の状態を示す LED ランプです。

LED 名称	色	状態	説明
POWER	緑	点灯	正常起動
		点滅	再起動
	–	消灯	電源オフ
MAX(PoE power)	橙	点灯	給電限界、追加給電停止
	–	消灯	給電可能

⑥ DC 入力ジャック

同梱の AC アダプタを接続するためのジャックです。

■ 本体の接続のしかた

1. AC アダプタを接続し、電源投入します。

DC プラグを本体背面の DC ジャックに挿し込み、AC アダプタをコンセントに挿し込みます。
アダプタコード抜け防止のために、同梱の結束バンドを下図の位置に取り付けてください。

2. DC 入力ジャックに同梱の AC アダプタを差し込んでください。

3. ネットワーク（UTP）ケーブルを接続する

UTP ケーブルを使って、UTP ポートと対向機器とを接続します。

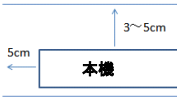
使用するケーブルは以下を参考にしてください。

規格	ケーブル
10BASE-T	100m 以内の UTP カテゴリ 3 以上
100BASE-TX	100m 以内の UTP カテゴリ 5 以上
1000BASE-T	100m 以内の UTP カテゴリ 5e 以上
SFP	使用する SFP に対応した光ファイバーケーブル

■ 設置場所について

警告　次のような環境での使用はしないでください。火災や感電、故障の原因となります。

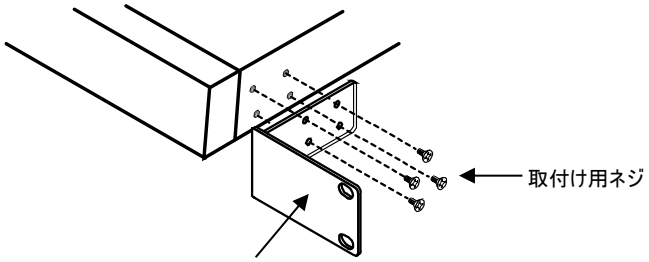
- 直射日光の当たる場所や熱器具の近くに設置しないでください。
- 振動の激しい場所や傾いた台の上など、不安定な場所に設置しないでください。
- 通風孔をふさいでしまうような場所に設置しないでください。
  （周囲に少なくとも左右 5cm、上部に 3cm 以上の放熱スペースが必要です）



- テレビ、ラジオ、コードレス電話機などのそばに設置しないでください。
- 急激な温度変化のある場所に設置しないでください。
- 湿度の多い場所や、水などの液体がかかる恐れのある場所に設置しないでください。
- ほこりの多い場所や、静電気障害の原因となるジュウタン床に設置しないでください。
- 腐食性ガスが発生するような場所に設置しないでください。

■19 インチラックへの取り付け

19 インチラック(EIA 規格)への取り付けの際は、付属のラックマウントキット取付け金具を次の図のように取り付けて下さい。



■ 通信モード

接続先ポートとして 10BASE-T/100BASE-TX ポートと通信する際、対向機器が IEEE802.3 規格対応の
オートネゴシエーション機能をサポートしていない場合は、本機の通信モードを対向機器の通信モードに
合わせて、設定してください。

■ ご使用にあたってのお願い

静電気注意
内部には静電気に敏感な電子部品を使用しています。
静電気を帯びた手でコネクタの接点部に直接触れると故障(静電破壊)の原因となります。

■ PoE 機能について

PoE(Power over Ethernet)とは、イーサネットの配線で利用されるカテゴリ 5 以上の
UTP ケーブル(より対線)を通じて電力を供給する技術の事で、IEEE 802.3at および IEEE 802.3af
として標準化されており、IEEE 802.3at は「最大 30 Watts」まで、IEEE 802.3af は「最大 15.4 Watts」
までサポートしています。

PoE には、PD への給電用の『PSE』と、PSE からの受電用の『PD』の 2 つのタイプがあります。
PD を PSE へ接続すると、PSE は初期設定時の電流クラスレベルを検知して、調整を行います。
接続が完了すると、PSE は PD への給電を開始します。
PoE に対応していない装置に接続する場合は、通常のスイッチとして機能し、給電は行いません。

以下の 3 つの状態では、PD への給電は行いませんのでご注意ください。

1. PoE 接続時の負荷がかかりすぎると、PD からの電流クラスレベルを検知し、スイッチは安全の
   ために自動的に PD への給電を停止します。

2. PoE のスイッチ全体への負荷が既に PD によって制御されている場合は、PD に新たに接続を
   行っても、スイッチからの給電は行いません。

3. スイッチはイーサネットケーブル用の TypeA(1、2、3、6 番のピン)に給電を行います。
   TypeB(4、5、7、8 番のピン)のみしかサポートしていない場合は、スイッチからの給電は行いません。

■ トラブルシューティング

●PWR LED が点灯しない
□ AC アダプタや DC プラグが外れていませんか？
⇒ 電源が正しく接続されていることを確認してください。

●UTP ケーブルを接続しても、LNK/ACT LED が点灯しない。
□ UTP ケーブルに異常はありませんか?
⇒ ケーブルが正しく接続されているか確認してください。
⇒ 断線確認のため、正常に通信できている他のケーブルと交換してみてください。

●PC との通信が不安定になったり、リンクダウンする。
□ Windows7、Windows8、Windows10 をお使いの場合、PC の NIC との相性により、 通信が不安定となる場合があります。
お使いの PC が同 OS の場合は、必ず、PC の「省電力イーサネット」を無効にしてご使用ください。

※省電力イーサネットを無効化にする方法については、PC によって異なります。
お使いの PC での無効化方法につきましては、PC のメーカーにお問い合わせください。

■ 2 章 WEB 設定 ■

2.1 本機との接続

本製品には HTTP Web エージェントが組み込まれているので、Web ブラウザを使用して、スイッチを設定し、統計値を確認してネットワークアクティビティを監視することができます。Web エージェントには、標準の Web ブラウザ（Chrome または Mozilla Firefox 2.0.0.0 以上）を使用して、ネットワーク上の任意のコンピュータからアクセスすることができます。

【注記】:本機では、すべて WEB インターフェースにより設定を行います。コマンドラインインターフェース（CLI）については、サポートしていません。

■動作環境

本製品の動作環境は、下記のとおりです。

❑ 本製品の対応 OS：
- Windows 10/8.1/8/7（32 ビット/64 ビット）

❑ 対応ブラウザー
- Internet Explorer 11 以降
- Chrome 53 以降
- Firefox 49 以降

※最新の対応情報は、当社ホームページをご確認ください。

■デフォルト設定値

IPアドレス	192.168.1.1
ユーザ名/パスワード	admin/admin

2.1.1 Web インターフェースへの接続

接続する PC の IP アドレスは、以下のとおり設定してください。

IP アドレス: 192.168.1.x(x:2-254)
サブネットマスク: 255.255.255.0

PC のインターフェースと本機の任意の LAN ポートをケーブルで接続します。

1. WEB ブラウザ(Internet Explorer/Chrome/Firefox)を開いて、「IP アドレス:192.168.1.1」を入力します。

【注記】:
本体のデフォルト設定の IP アドレスを変更した場合は、変更後の IP アドレスを入力してください。

2. アドレスバーに IP を入力して＜Enter＞キーを押すと、下記画面が表示されます。

3. ユーザ名とパスワードを入力後に<login>ボタンをクリックすると、本機のメイン画面が表示されます。
   ☞ デフォルト設定のユーザ名およびパスワードは「admin」です。

また、プルダウンメニューにより、言語の切り替え（日本語/英語）を選択することができます。

2.1.2 メイン画面の構成

メイン画面の構成については、以下のとおりです。

① メニューウィンドウ
本メニューは、上記の 7 つのメニュー（「機器情報」、「システム」、「ネットワーク」、「QoS」、「PoE」、「セキュリティ」、「ツール」）により構成されています。

② 言語の切り替え
プルダウンメニューにより、「日本語」と「英語」のいずれかに切り替えることができます。

③ ログアウト
クリックすると、現在のブラウザの接続が切断されます。
確認メッセージが表示されるため、ログアウトする場合は<OK>ボタン、そのまま設定を継続する場合は<キャンセル>ボタンを選択してください。

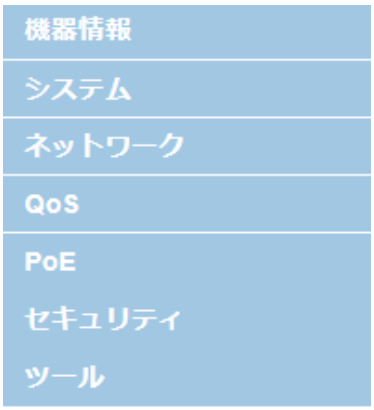
④ メインウィンドウ
メニューウインドウで選択したメニューに応じて、各機能の設定を行ったり、ステータス情報が表示されます。

■　3 章　本機の設定方法　■

ここでは、本機の設定方法について説明します。

ここでは、基本的なスイッチ機能について説明すると共に、Web ブラウザを使用して個々の機能を設定する方法を紹介します。

このセクションは、以下の章から設定されています



① 機器情報	本機に関する基本情報（ソフトウェア/ハードウェアのバージョンやシリアル番号など）が表示されます。
② システム	システム情報（IP アドレス、タイムアウト、管理者設定、SSL/SSH）の設定方法について説明します。
③ ネットワーク	本機の主な機能（スパニングツリー、リンクアグリゲーション、ミラーリング、ループ検知、VLAN）の設定方法について説明します。
④ QoS	QoS 機能の設定方法について説明します。 QoS を実装することで、ある特定の通信を優先して伝送させたり、帯域幅を確保することができます。
⑤ PoE	PoE の設定方法について説明します。
⑥ セキュリティ	ポートベースのセキュリティ機能とその設定手順について説明します。
⑦ ツール	本機のツール機能(ファームウェアの更新/バックアップ/リストア、設定情報のバックアップ/リストア、ケーブル診断、再起動、ping)の使用方法について説明します。

3.1 機器情報

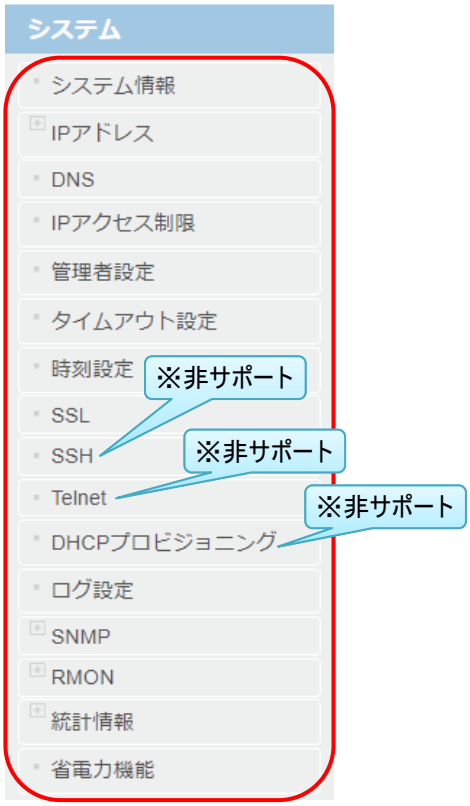
本章では、本機に関する基本情報（基本情報、システム情報、MAC アドレス/IP アドレス、IPv6 アドレス）が表示されます。

① 基本情報	起動時間:本機の起動時間が表示されます。 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:本機のシリアル番号が表示されます。
② ハードウェア	DRAM: RAMのメモリサイズが表示されます。 Flash フラッシュのメモリサイズが表示されます。
③ システム情報	システム名:本機のシステム名が表示されます。 ロケーション:本機の設置場所が表示されます。 連絡先:システム管理者の情報が表示されます。
④ MAC アドレス、IP アドレス	MACアドレス:本機のMACアドレスが表示されます。 IPアドレス:本機のIPv4アドレスが表示されます。 サブネットマスク:本機の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:本機の IPv4 デフォルトゲートウェイが表示されます。
⑤ Pv6 アドレス	IPv6アドレス/プレフィックス長:本機の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:本機の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:本機の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。
⑥ 自動設定機能	DHCPクライアント: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。

3.2 システム（※一部非サポートあり）

本章では、システム情報（IP アドレス、タイムアウト、管理者設定、SSL/SSH）の設定方法について説明します。
この情報は、同じローカルエリアネットワーク内の他のスイッチの中から特定の各スイッチを識別する際に役立ちます。

本メニューでは、以下の機能を設定することができます。



3.2.1 システム情報

デバイス名、設置場所、連絡先などの情報が表示されるため、システムを特定することができます。

「システム」→「システム情報」をクリックすると、以下の画面が表示されます。

■システム情報

❒システム説明:本機の製品名が表示されます。

❒システム OID:本機のネットワーク管理サブシステムの MIB II オブジェクト ID が表示されます。

❒システム名:本機にシステム名を入力します（15 文字以内）。

❒ロケーション:本機の設置場所を入力します（30 文字以内）。

❒連絡先:本機のシステム管理者を入力します。

上記設定を完了後、<適用>ボタンをクリックすることにより、エントリが反映されます。

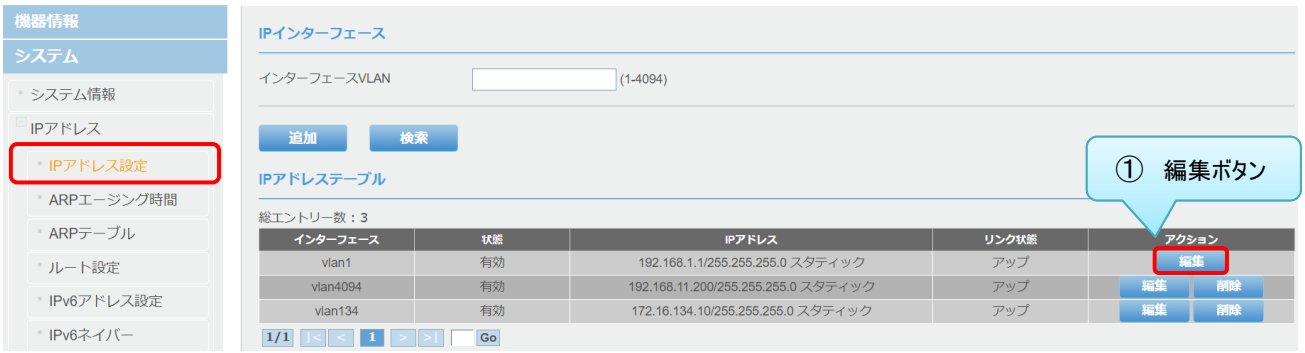
3.2.2 IP アドレス

ここでは、IPv4/IPv6 インターフェースの設定方法について説明します。

1. IP アドレス設定

VLAN インターフェースの VLAN ID を設定します。

「システム」→「IP アドレス」→「IP アドレス設定」をクリックすると、以下の画面が表示されます。



ここでは、IPv4 インターフェース上で VLAN の設定を行います。

■IP インターフェース VLAN
インターフェース VLAN を追加したい場合は<追加>ボタン、検索したい場合は<検索>ボタンをそれぞれクリックしてください(デフォルト設定:vlan 1)。

・<追加>ボタンをクリックすると、次の管理者テーブルに反映されます。
・<検索>ボタンをクリックすると、指定した VLAN ID の VLAN インターフェースが一番下の「IP アドレステーブル」上に表示されます。

■IP アドレステーブル
VLAN インターフェース名とその状態、IP アドレスおよびリンク状態等が表示されます。

登録されている VLAN インターフェースを編集したい場合は、アクションの① 編集 ボタンをクリックすると、以下の「IP アドレス詳細設定」画面が表示されます。

■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 アドレス設定を変更する場合、「有効」に設定してください。

■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。

・固定：IP アドレスを手動で設定します。

・DHCP：DHCP サーバーから IP アドレスを取得します。

❒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>ボタンをクリックすると、変更が適用されます。

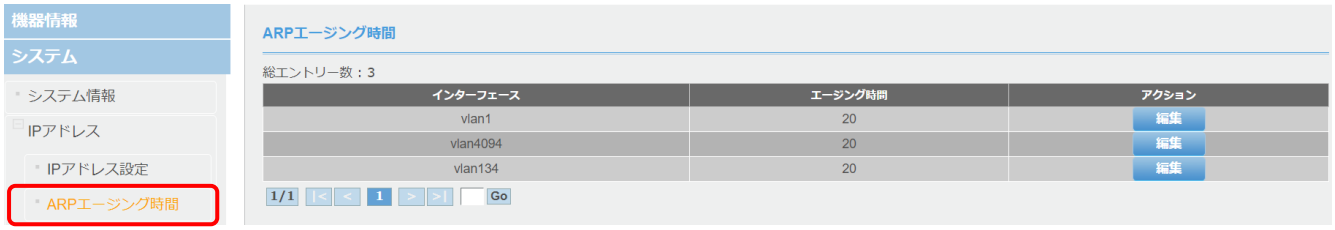
エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。

特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

2. ARP エージング時間

IP インターフェースの ARP エージング時間を個別に変更することができます。

「システム」→「IP アドレス」→「ARP エージング時間」をクリックすると、以下の画面が表示されます。



■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割り当てられている vlan 名が表示されます。

❒エージング時間:エージング時間が表示されます（デフォルト:20）。

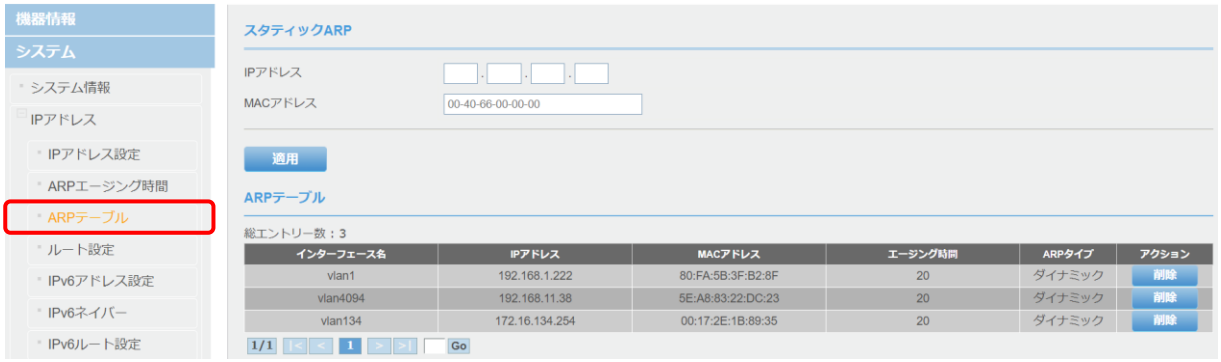
❒アクション:<編集>ボタンをクリックすると、エージング時間の値を変更することができます。

エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

3. ARP テーブル

ARP テーブルとは、イーサネット通信のために用いられる IP アドレスと MAC アドレスの対照表です。
ここでは、スタティック MAC アドレスを設定することができます。スタティックアドレスは、スイッチの特定のインターフェースに割り当てることができます。スタティックアドレスは、割り当てられたインターフェースにバインドされ、自動的に変更されることはありません。スタティックアドレスが他のインターフェースで検出された場合、そのアドレスは無視され、アドレステーブルには書き込まれません。

「システム」→「IP アドレス」→「ARP テーブル」をクリックすると、以下の画面が表示されます。



■スタティック ARP

❒IP アドレス: ARP の IP アドレスを入力します。

❒MAC アドレス: ARP の MAC アドレスを入力します。

・<適用>ボタンをクリックすると、次の表に反映されます。

■ARP テーブル

それぞれインターフェース名、IP アドレス、MAC アドレス、エージング時間、ARP タイプがそれぞれ表示されます。

4. ルート設定

管理者により宛先ネットワークへの最適なルートを手動にて設定します。
スタティックルートの情報は他のルータへ通知されることはありません。また、ネットワークの状態が変更された場合や他に有効な宛先ルートがある場合でも、自動的にそのルートに切り替わることはありません。

「システム」→「IP アドレス」→「ルート設定」をクリックすると、以下の画面が表示されます。

■ルート設定

❒IP アドレス:宛先ネットワーク、サブネットワーク、ホストのいずれかの IP アドレスを入力して下さい。
※アドレス「0.0.0.0」はルータのデフォルトゲートウェイを示します。

❒ネットマスク:関連付けられている IP サブネットのネットワークマスクを表します。このマスクは、個々のサブネットへのルーティングに使用されるホストのアドレスビットを表示します。

❒ネクストホップ:ルートのネクストホップ（またはゲートウェイ）の IP アドレスを表示します。

❒経緯順位:プルダウンメニューより、「プライマリー」または「バックアップ」のいずれかを選択してください。
障害発生時にプライマリールートに問題があった場合、その代替としてバックアップルートにパケットを転送します。

・<適用>ボタンをクリックすると、次の表に反映されます。

■ルートテーブル

上記エントリを設定すると、リスト表示されます。

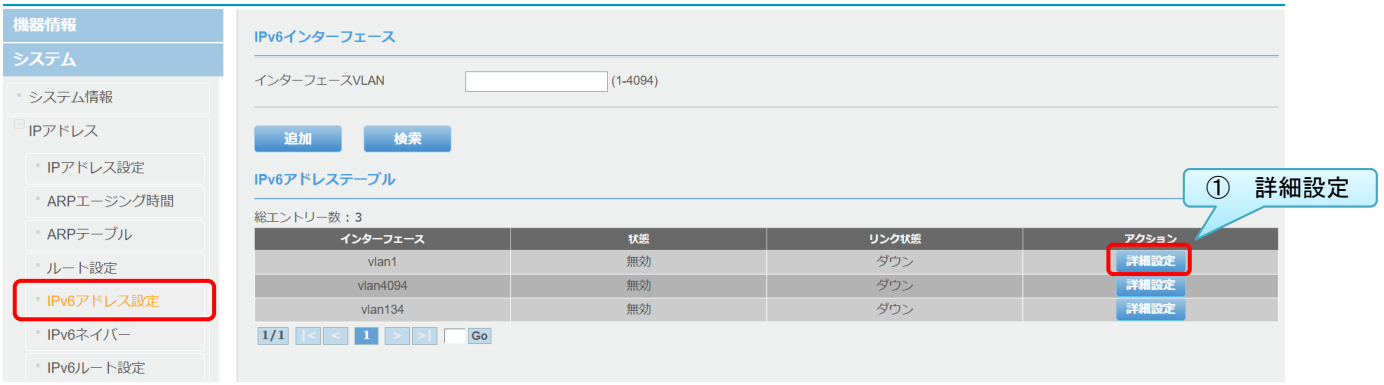
エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。

特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

5. IPv6 アドレス設定

ここでは、IPv6 インターフェース上で VLAN の設定を行います。

「システム」→「IP アドレス」→「IPv6 アドレス設定」をクリックすると、以下の画面が表示されます。



■IPv6 インターフェース

❒インターフェース VLAN: IPv6 インターフェース VLAN を設定します（有効範囲:1-4094）。

・<追加>ボタンをクリックすると、次の表に反映されます。
・<検索>ボタンをクリックすると、指定した VLAN ID の VLAN インターフェースが下の「IPv6 アドレステーブル」上に表示されます。

■IPv6 アドレステーブル

設定されている VLAN を変更、または削除したい場合は、<編集>ボタンをクリックして変更するか、<削除>ボタンをクリックしてアドレスを削除することができます。

詳細な設定を行いたい場合は、「IPv6 アドレステーブル」の① 詳細設定 ボタンをクリックすると、以下の画面が表示されます。

■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　インターフェースを有効/無効にします。

■IPv6 アドレス設定

❒DHCPv6 クライアント機能: DHCPv6　クライアントを有効/無効にします。

❒IPv6 アドレス/プレフィックス長: IPv6 インターフェースのローカルアドレスまたはプレフィックス長を手動で設定することができます。

■ネイバー要請

❒ネイバー要請(NS)送信間隔: NS メッセージの再送信間隔を入力します（有効範囲:1～3600（秒）、デフォルト:1　秒）

■IPv6 アドレステーブル

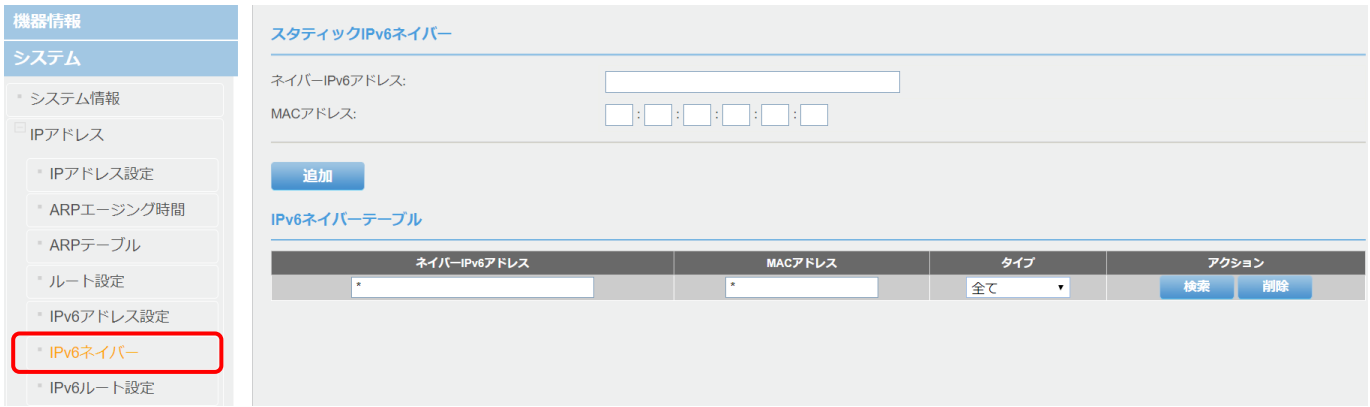
上記設定を完了後、<適用>ボタンをクリックすると、それぞれの値が表に反映されます。

エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページ)、<(前ページ)、>(次ページ)、>|(最後のページ)のいずれかをクリックして、画面を移行できます。
特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

6. IPv6 ネイバー

IPv6　管理が有効になっている場合、スイッチは接続されているリンク上の　IPv6 対応デバイスを識別します。
ネットワーク上で IPv6 対応のネイバーを手動で設定します。

「システム」→「IP アドレス」→「IPv6 ネイバー」をクリックすると、以下の画面が表示されます。



■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 アドレスを指定します。

❒MAC アドレス:MAC アドレスを指定します。

上記設定を完了後、<追加>ボタンをクリックすると、次の表にリスト表示されます。

■IPv6 ネイバーテーブル

❒ネイバーIPv6 アドレス、MAC アドレスがそれぞれ表示されます。

❒タイプ:　プルダウンメニューより「スタティック/ダイナミック/全て」のいずれかを選択してください（デフォルト設定:全て）。

❒アクション:特定のアドレスを入力後、<検索>ボタンをクリックして変更したいエントリを見つけるか、<削除>ボタンをクリックしてアドレスを削除することができます。

7. IPv6 ルート設定

ここでは、受信した IPv6 パケットを適切な経路に転送する機能です。

「システム」→「IP アドレス」→IPv6 ルート設定」をクリックすると、以下の画面が表示されます。

■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入力します。
※「デフォルトルート」に☑を入れると、すべてのネットワーク（::/0）を対象として指定します。
宛先ネットワークを指定する場合、「デフォルトルート」のチェックを外してください。

❒インターフェース VLAN: VLAN インターフェースの VLAN ID を入力します（有効範囲: 1-4094）。

❒IPv6 ネクストホップ:「IPv6 アドレス/プレフィックス長」で入力したネットワークの宛先パケットの転送先の IPv6 アドレスを指定します。

❒経路順位:プルダウンメニューにて、プライマリー、またはバックアップのいずれかを選択してください。
障害発生時に「プライマリー」ルートに問題があった場合、その代替として「バックアップ」ルートにパケットを転送します。

・<適用>ボタンをクリックすると、設定した値が反映されます。

■ルートテーブル

上記設定を完了後、<適用>ボタンをクリックすると、それぞれの値が表に反映されます。

3.2.3 DNS

ここでは、ホスト名を解決するために、IPv4/IPv6 DNS サーバーを設定します。
たとえば、SNTP サーバーの時間設定をドメイン名で指定した場合、本機の DNS サーバーを設定するまで、指定の SNTP ドメイン名を解決することはできません。

「システム」→「DNS」をクリックすると、以下の画面が表示されます。

フィールドに DNS の「IPv4 サーバーのアドレス」、または「IPv6 サーバーのアドレス」、あるいはその両方を入力します。

上記設定を完了後、<適用>ボタンをクリックすると、値が反映されます。

3.2.4 IP アクセス制限

ここでは、本機の管理画面へのアクセスを特定の IP アドレスのリストに制限することができます。

「システム」→「IP アクセス制限」をクリックすると、以下の画面が表示されます。

■IP アクセス制限

❒IP アクセス制限機能:管理画面へのアクセスを有効/無効にします（デフォルト設定:無効）。

【注記】:この機能を「有効」にすると、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。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

■IP アクセス認可 IP アドレス
❒IP アドレス:「IPv4　アドレス」または「IPv6 アドレス」のいずれかを入力します。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。

■IP アクセス制限リスト
上記の値がリスト表示されます。

3.2.5 管理者設定

ここでは、管理者パスワードを変更したり、追加したい管理ユーザーのアカウントを作成して、スイッチ管理画面へのアクセス方法について説明します。

「システム」→「管理者設定」をクリックすると、以下の画面が表示されます。

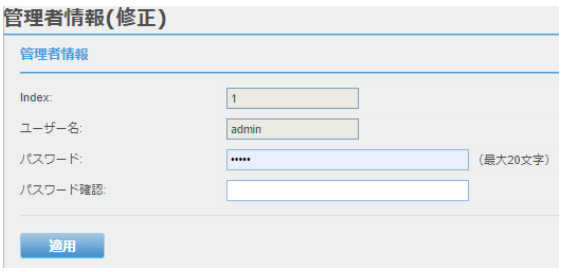
■管理者情報
新しい管理ユーザーカウントを作成するには、以下の手順に従ってください。
❒ユーザー名:新しいアカウントのユーザー名を入力します(20 文字以内の英数字で設定してください)。

❒パスワード:新しいドキュメントのパスワードを入力してください(20 文字以内の英数字で設定してください)。

❒パスワード確認: 確認のためにもう一度パスワードを入力してください。

・<追加>ボタンをクリックすると、次の管理者テーブルに反映されます。

■管理者テーブル
現在登録されている管理者情報が表示されます。
登録されているアカウントを変更する場合は、①変更ボタンをクリックすると、以下の画面が表示されるため、それぞれ値を入力してください。



■管理者情報
❒inex:新規アカウントのインデックス番号が表示されます。

❒ユーザ名:新規のユーザ名が表示されます。

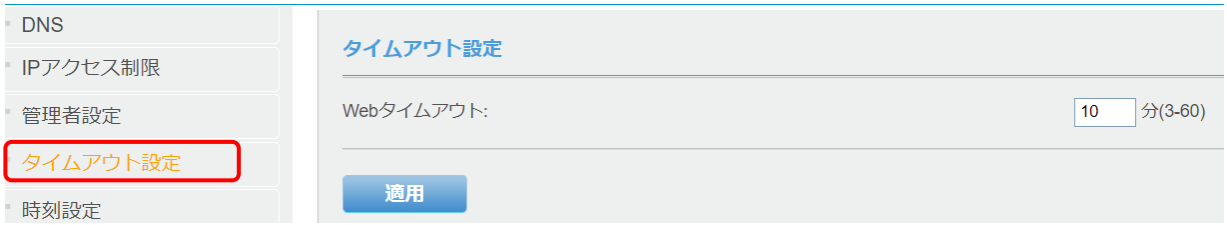
❒パスワード: パスワードは 20 文字以内の英数字で入力してください。

❒パスワード:確認のため、再度パスワードを入力してください。

3.2.6 タイムアウト設定

システムのタイムアウトの値を設定します。

「システム」→「タイムアウト設定」をクリックすると、以下の画面が表示されます。



■タイムアウト設定

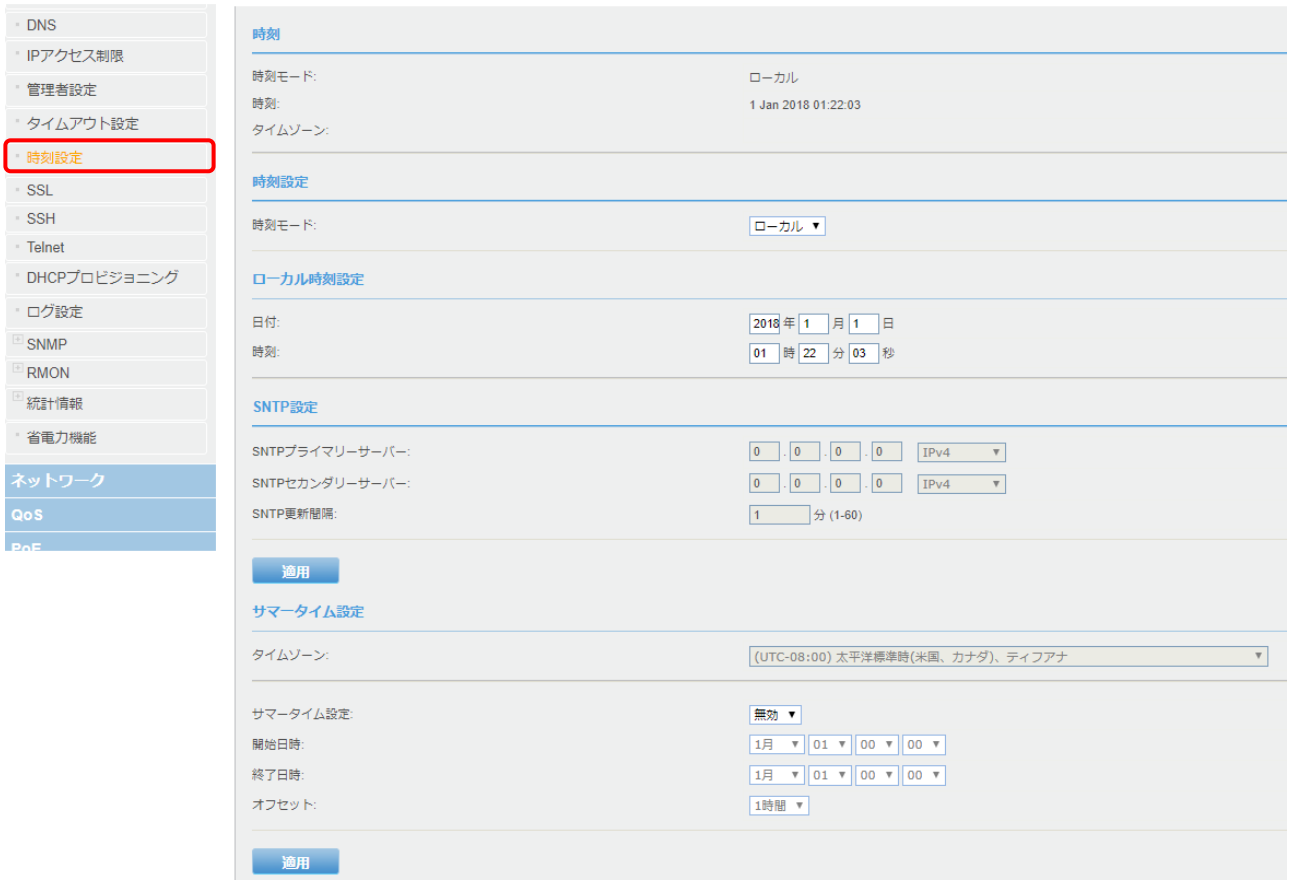
❒Web タイムアウト:管理画面から自動的にログアウトするアイドル時間を分単位で入力してください（有効範囲：3-60、フォルト値：10 分）。

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.7 時刻設定

SNTP（簡易ネットワークタイムプロトコル）を使用すると、スイッチの内部時刻がタイムサーバー（SNTP または NTP）からの定期的な更新情報に基づいて設定されるようにすることができます。スイッチの時刻が常に正確な時間に調整することで、イベントエントリの正確な日時がシステムログに記録されるようになります。

「システム」→「時刻設定」をクリックすると、以下の画面が表示されます。



■時刻

❒時刻モード:システムの日時が手動でローカル時間に設定されているか、ネットワークタイムサーバーの SNTP から自動的に取得されているかを表示します（デフォルト設定:ローカル）。

❒時刻:現在のシステム時刻と日付を表示します。

❒タイムゾーン:現在のシステムのタイムゾーンを表示します。

❒時刻モード:

・ローカルタイム:日時の設定を手動で設定します。

・SNTP:ネットワークタイムサーバーから日時の設定を自動的に取得します。

❒時刻設定:手動により時刻を設定できます。このオプションを選択した場合は、「ローカル時刻設定」にて日時の設定を手動で入力します。

❒日付:日付設定を入力します（年月日）。

❒時刻:時間設定を入力します（時間/分/秒）。

■SNMP 設定

SNTP:ネットワークタイムサーバーから自動的に日時の設定を取得できるように本機を設定できます。このオプションを選択する場合は、次の「SNTP の設定」画面で、タイムサーバーの設定を入力します。

【注記】:スイッチがインターネット SNTP タイムサーバーと通信するには、インターネットアクセス用のデフォルトゲートウェイアドレスを含む有効な IPv4/IPv6 アドレス設定が必要です。また、ドメイン名を使用している場合は、DNS サーバーによりホスト/ドメイン名を解決する必要があります。

❒SNTP プライマリサーバー:プライマリネットワークタイムサーバーの IPv4 アドレス、IPv6 アドレス、またはドメイン名を入力します。
❒SNTP セカンダリーサーバー:セカンダリネットワークタイムサーバーの IPv4 アドレス、IPv6 アドレス、またはドメイン名を入力します。
❒SNTP 更新間隔:タイムサーバーの日時設定を更新する間隔を入力します。
❒タイムゾーン:ドロップダウンリストにより、タイムゾーンを選択してください。ここでサマータイムを設定できます。

上記設定を完了後、<適用>ボタンをクリックしてください。

■サマータイム設定

ここでは、サマータイムの値を設定できます。
❒サマータイム設定：ドロップダウンリストによりサマータイムを有効/無効にします。
❒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:タイムゾーンに基づいてタイムオフセットを設定します。

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.8 SSL

SSL（Secure Sockets Layer）は、インターネット上でデータを暗号化して送受信するプロトコルです。
HTTPS/SSL 管理アクセスを有効にすると、安全な暗号化通信を使用してスイッチ管理画面にアクセスできるようになり、権限のないユーザーによるユーザー名とパスワードの資格情報を傍受するのを防ぎます。

通常、セキュリティの追加を必要としないシステム管理者のみローカルネットワークへのアクセスが可能です。他のネットワークまたはインターネット経由でスイッチ管理アクセスを有効にする場合は、この機能を有効にすることをお勧めします。

【注記】:SSL 管理アクセスを一旦有効にすると、HTTP 管理アクセスは無効になり、セキュアな暗号化通信のみ使用可能になるため、管理画面へのすべてのアクセスを強制的に無効にします。

「システム」→「SSL」をクリックすると、以下の画面が表示されます。

■SSL 設定

❒SSL 機能:

・有効:HTTPS/SSL 管理アクセスを有効にし、HTTP 非セキュアモードを有効にします。

・無効:HTTPS/SSL 管理アクセスを無効にし、HTTP 非セキュアモードを無効にします（デフォルト設定）。

【注記】:SSL 管理アクセスが無効な場合は「HTTP」、有効な場合は「HTTPS」を使用して管理画面にアクセスする必要があります。

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.9 SSH（※非サポート）

SSH（Secure Shell）は、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルです。パスワードなどの認証部分を含むすべてのネットワーク上の通信が暗号化されるため、ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視を行います。

「システム」→「SSH」をクリックすると、以下の画面が表示されます。

❒SSH 機能:
・有効:HTTPS/SSH 管理アクセスを有効にし、HTTP 非セキュアモードを無効にします。
・無効:HTTPS/SSH 管理アクセスを無効にし、HTTP 非セキュアモードを有効にします（初期設定）。

❒ポート(1～65535):
SSH 機能のサービスポートを入力します(有効範囲:1～65535)

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.10 Telnet（※非サポート）

ここでは、Telnet（つまり、仮想端末）を使用してネットワーク経由でオンボードの設定プログラムにアクセスすることができます。Telnet による管理アクセスは有効/無効にすることができます。

「システム」→「Telnet」を選択すると、以下の画面が表示されます。

■Telnet 設定
❒Telnet 設定:スイッチへの Telnet アクセスを有効/無効にします（デフォルト:有効）。
❒ポート(1～65535): Telnet のサービスポートを設定します(有効範囲:1～65535、デフォルト:23)。

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.11 DHCP プロビジョニング（※非サポート）

ここでは、DHCP 自動設定を有効/無効にすることができます。

リモートサーバーを介して設定ファイルを自動更新する場合、DHCP サーバーを介して DHCP 自動設定機能を利用できます。 この機能を DHCP サーバーと連携させるには、IP アドレス設定で DHCP クライアントを有効にする必要があります。

「システム」→「DHCP プロビジョニング」をクリックすると、以下の画面が表示されます。

■DHCP プロビジョニング

❒DHCP プロビジョニング機能を有効/無効にします（デフォルト：無効）。
本機能を有効にすると、DHCP サーバーから IP アドレスを取得し、設定ファイルを取得します。

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.12 ログ設定

ここでは、本機のログ情報を表示および設定することができます。
システムログは、通常の動作中にスイッチが生成するイベントメッセージを記録することによって、本機の動作を監視するように設計されています。これらのイベントは、システムの問題を識別し、解決する上で非常に有用です。

「システム」→「ログ設定」をクリックすると、以下の画面が表示されます。

■ログ設定

❒タイムスタンプ

ログに記録された各イベントメッセージへのタイムスタンプを有効/無効にします。

❒収容メッセージ行数:メッセージのバッファサイズを入力します（範囲:1～200、デフォルト設定:50）。

❒Syslog 機能:デバイスログを外部ログ（Syslog）サーバーに送信して、トラブルシューティングや監視を行います。
・有効:syslog を有効にし、Syslog サーバー IP セクションに、ロギングを送信するための外部 syslog サーバーの IPv4 または IPv6 アドレスを入力します。
・無効:syslog 機能を無効にします。

❒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:ドロップダウンリストにより、ロギングを保存するファシリティをクリックします（オプション:local0 - local7）。

【MEMO】:外部 syslog サーバーにロギングを保存する機能を定義できます。
これにより、デバイスごとに別々のログ記録セクションを確実に作成できます。

❒出力ログレベル:ドロップダウンリストをクリックして、ログに記録するイベントメッセージのレベルを選択してください。

レベル	重大度	説明
1	Alert	非常に緊急度の高いイベントであることを示します。
2	Critical	重大なイベントであることを示します。
3	Warning	警告レベルのイベントであることを示します。
4	Info	情報レベルのイベントであることを示します。

上記設定を完了後、<適用>ボタンをクリックしてください。

3.2.13 SNMP

1. 基本設定

ここでは、SNMP の設定方法について説明します。 SNMP を介してデバイス上の管理情報ベース（MIB）オブジェクトを設定して、本機を管理します。スイッチを管理するには、グループ名、スイッチの IP アドレス、および少なくとも 1 つ以上のコミュニティ文字列が最低限必要です。

【注記】:本機の SNMP エージェント機能を無効にすると、MIB を使用して SNMP 経由で管理できなくなります。

「システム」→「SNMP」→「基本設定」をクリックすると、以下の画面が表示されます。

■SNMP 設定

❒SNMP エージェント機能: SNMP を有効/無効にします（デフォルト設定:有効）。

・有効:SNMP エージェントが有効になります。SNMP ネットワーク管理ソフトウェアとスイッチのプライベート MIB を使用して管理することができます。

・無効：SNMP エージェントは無効になります。

上記設定を完了後、<適用>ボタンをクリックしてください。

■エンジン ID:設定

❒エンジン ID:ローカルデバイスのエンジン ID を入力します(64 文字以内の英数字(0～9 の数字および a～f の英字))。デフォルト設定では、RFC3411 規格に対応しています。

【注記】:SNMP を有効にするには、エンジン ID を定義する必要があります。

・<適用>ボタンをクリックすると、上記の設定した値が適用されます。

・<リセット>ボタンをクリックすると、入力した値がリセットされます。

・<削除>ボタンをクリックすると、表示されているエントリが削除されます。

2. ビュー

SNMP ビューテーブルを設定します。

SNMP ビューテーブルは、各ビュー名の MIB オブジェクトアクセス基準を指定します。ビュー名が指定されていない場合は、すべての MIB オブジェクトにアクセスできます。このテーブルのエントリに基づいてアクセス許可または拒否できる MIB の特定の領域を指定できます。ビューテーブルでエントリを作成および削除することができます。

「システム」→「SNMP」→「ビュー」をクリックすると、以下の画面が表示されます。

■SNMP ビュー設定

❒ビュー名：ビュー名を入力します（32 文字以内）
このエントリは「SNMP ユーザー/グループ」メニューで事前に定義する必要があります（次の項を参照ください）。

❒サブツリーOID:サブツリーOID を入力します。

❒OID マスク：OID マスクを選択します(デフォルト設定:1)。
1: 該当する数字を一致条件で適用します。
0: 該当する数字は一致条件で適用しません。

❒ビュータイプ:次のオプションのいずれかを選択して、<追加>ボタンをクリックします。
・Included:指定された MIB オブジェクトがビューに含まれます。
・Excluded:指定された MIB オブジェクトのビューをブロックします。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。
・<リセット>ボタンをクリックすると、入力した値がリセットされます。

■SNMP ビューテーブル

・<全削除>ボタンをクリックすると、統計情報のエントリーはすべて削除されます。
・<削除>ボタンをクリックすると、設定したエントリが削除されます。

エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

3. グループ

SNMP のグループアクセスを設定します。

「システム」→「SNMP」→「グループ」をクリックすると、以下の画面が表示されます。

■グループアクセス設定

❒SNMP ビュー名を作成する前に、「SNMP ユーザー/グループ」メニューでグループ名を定義する必要があります

❒グループ名:グループ名を入力します。

【注記】:このエントリは「SNMP ユーザー/グループ」メニューで事前に定義してください。

❒読み出しビュー:読み出しビュー名を入力します（32 文字以内）。

❒書き込みビュー:書き込みビュー名を入力します（32 文字以内）。

❒受信ビュー:受信ビュー名を入力します（32 文字以内）。

❒バージョン:プルダウンメニューより、「v3」を選択してください。

・v1: SNMP v1 はセキュリティ機能をサポートしません。

・v2c: SNMP v2c は、集中型、分散型どちらのネットワーク管理方法にも対応しています。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。

・v3:ネットワーク上で認証とパケットの暗号化を併用することでデバイスへの安全なアクセスを提供します。

❒セキュリティレベル:プルダウンメニューにより選択します。

・<追加>ボタンをクリックすると、上記に設定した値が次の表に反映されます。

・<リセット>ボタンをクリックすると、入力した値がリセットされます。

■SNMP グループアクセステーブル

エントリを変更する必要がある場合は、まずエントリを削除してから再入力してください。

SNMP ビュー名を削除する場合、表の右上の「アクション」メニューで削除したいビュー名を選択して、<削除>ボタンをクリックします。

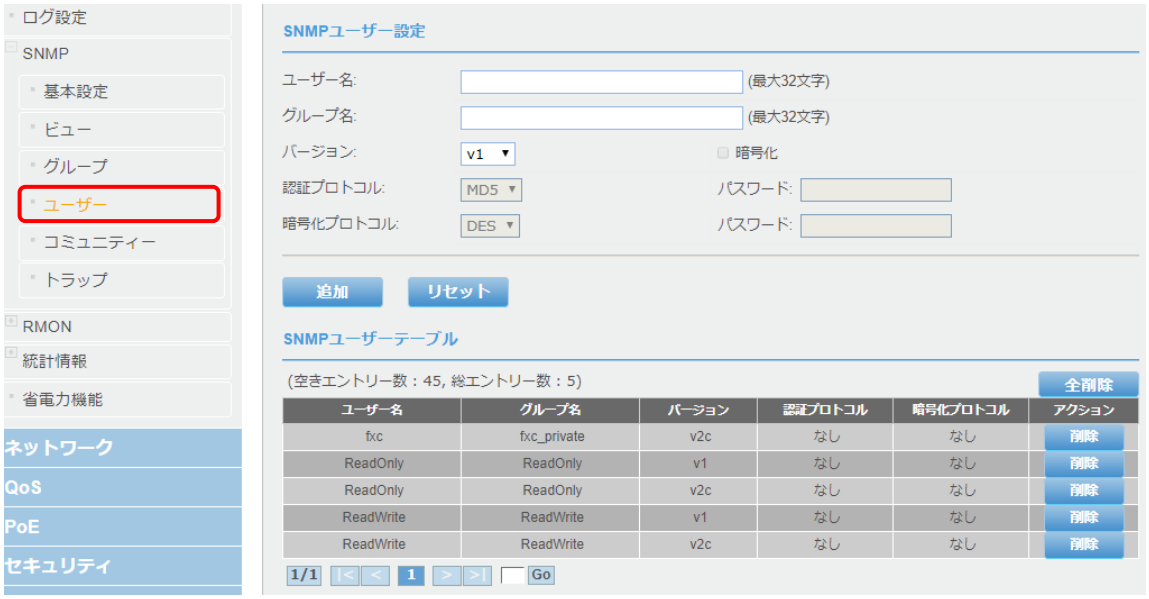
【注記】:

読み出しおよび書き込みグループ名に対応するビューはデフォルト値のため、削除することはできません。

4. ユーザー

SNMP ユーザー/グループをそれぞれ設定します。

「システム」→「SNMP」→「ユーザー」をクリックすると、以下の画面が表示されます。



■SNMP ユーザー設定

SNMP ユーザー名とグループ名の定義は、他のすべての SNMP テーブルの基本です。
SNMP ユーザー名およびグループ名の設定方法は、以下のとおりです。
【注記】:デフォルトでは、SNMP に定義されているユーザー名またはグループ名はありません。

❒ユーザー名:ユーザー名を入力します(32 文字以内)。
❒グループ名:新しいグループ名を入力します(32 文字以内)。
❒バージョン:プルダウンメニューにより「v3」を選択すると、暗号化チェックボックスがアクティブになります。
暗号化:チェックボックスを☑すると、「認証プロトコル」および「暗号化プロトコル」のパスワードフィールドが有効になります。
❒認証プロトコル:次のオプションのいずれかを選択して、認証プロトコルのパスワードを入力してください。
・MD5: MD5 認証プロトコル（メッセージを受信後に SNMP ユーザーは MD5 認証プロトコルで認証されます）。
・SHA: SHA 認証プロトコル（メッセージを受信後に、SNMP ユーザーは SHA 認証プロトコルで認証されます）。

❒暗号化プロトコル:次のいずれかのオプションを選択して、暗号化プロトコルのパスワードを入力してください。
・DES:データの情報が外部のオブザーバにより傍受されないように、DES 暗号化により SNMP データをスクランブルします。
・なし: SNMP データは暗号化されません。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。
・<リセット>ボタンをクリックすると、入力した値がリセットされます。

■SNMP ユーザー設定

登録されているユーザ名を削除したい場合は<削除>ボタンをそれぞれクリックしてください。

エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

5. コミュニティー

SNMP コミュニティーを設定します。
SNMP コミュニティーとは、SNMP で管理するネットワークシステムの範囲のことです。SNMP マネージャと SNMP エージェントとの間で、同じコミュニティー名にすることで情報を共有することができます。監視対象ごとに異なるコミュニティー名を設定することにより、効率的な管理とアクセス権限の分離を実現できます。

「システム」→「SNMP」→「コミュニティー」をクリックすると、以下の画面が表示されます。

■SNMP コミュニティーの設定:　SNMP コミュニティーの設定方法は、以下のとおりです。

❒コミュニティー名:新しいコミュニティー名を入力してください（32 文字以内）。

❒ユーザー名:事前に定義したユーザー名（ビューポリシー）を入力します（この名前は、「SNMP ユーザー/グループ」に
表示されているユーザー名のいずれかと一致する必要があります（32 文字以内）。

<追加>ボタンをクリックすると、新しいコミュニティー名とユーザー名の値が「SNMP コミュニティーテーブル」表示されます。

・<リセット>ボタンをクリックすると、入力した値がリセットされます。

【注記】:「SNMP ユーザー/グループ」画面に事前に定義されていないコミュニティー名を入力した場合、表にはリスト表示されますが、エージェント/マネージャ間の通信は不可となります。

■SNMP コミュニティーテーブル

登録されている VLAN ID を変更したい場合は<編集>ボタン、または削除したい場合は<削除>ボタンをそれぞれクリックしてください。

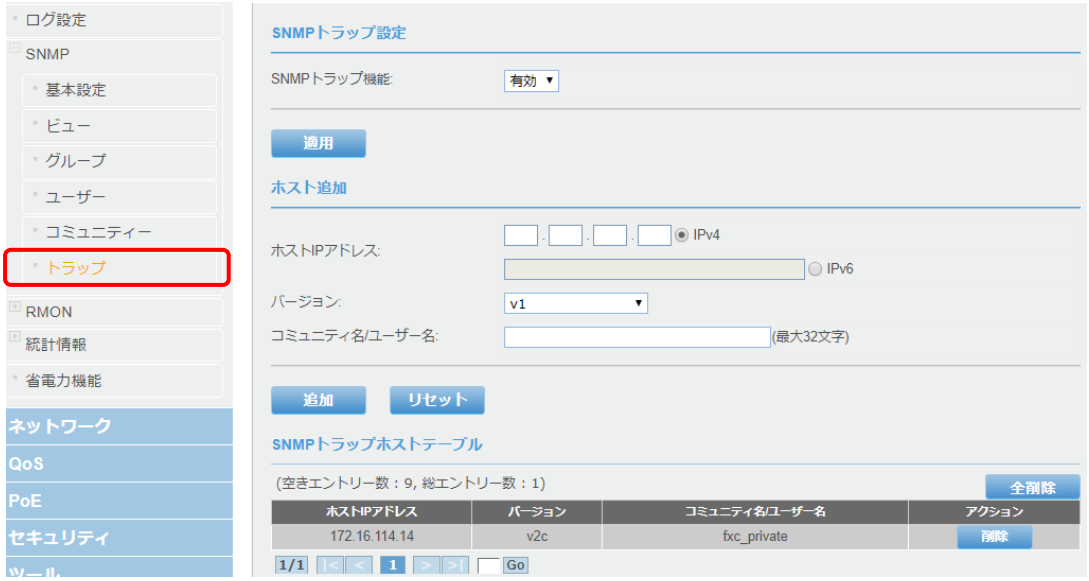
エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

6. トラップの設定

SNMP トラップ管理の設定方法について説明します。

ホストの IP アドレスは、SNMP トラップを受信する管理デバイスを指定するために使用されます。この IP アドレスは、本機のホストテーブルの SNMP バージョンと有効なコミュニティー名に関連付けられています。

「システム」→「SNMP」→「トラップの設定」をクリックすると、以下の画面が表示されます。



トラップホストテーブルエントリを作成するには、次の手順に従ってください。

■SNMP トラップ設定

❒SNMP トラップ機能:トラップ管理を有効にします(デフォルトでは「有効」)。

・<追加>ボタンをクリックすると、上記に設定したエントリが下の表に反映されます。

■ホスト追加

❒ホスト IP アドレス: SNMP トラップを受信する管理デバイスのホスト IP アドレスを入力します。

❒バージョン:ホスト管理デバイス用に設定されている SNMP バージョン（v1 または v2c）を入力します。

❒コミュニティー名/ユーザー名:以前に定義したコミュニティー名を入力します(最大 32 文字)。
コミュニティー名は、「SNMP トラップホストテーブル」画面に表示されるコミュニティー名と相関している必要があります。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。

・<リセット>ボタンをクリックすると、入力した値がリセットされます。

【注記】:事前に定義されていないコミュニティー名を入力した場合、表にはリスト表示されますが、エージェント/マネージャ間の通信は不可となります。

■SNMP トラップホストテーブル

登録されているホスト IP アドレスを削除したい場合は、<削除>ボタンをそれぞれクリックしてください。

エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

3.2.14 RMON

RMON を使用すると、リモートデバイスで情報を収集したり、指定したイベントに対して個別にアクションを実行できます。本製品は、RMON 対応デバイスであり、さまざまなタスクを個別に実行して、ネットワーク管理トラフィックを大幅に削減することができます。また、診断を継続的に実行し、ネットワークパフォーマンスに関する情報をログに記録することが可能です。イベントのトリガーとなる場合は、障害は自動的にネットワーク管理者に通知され、イベントの履歴情報が提供されます。本製品は、管理エージェントに接続できない場合には、指定されたタスクを引き続き実行し、次回、接続時にデータを管理ステーションに配信します。本製品は、mini-RMON をサポートしているため、各グループの統計情報、履歴、Event、およびアラームを設定することができます。RMON を有効にすると、システムによって物理インターフェースに関する情報が徐々に作成され、該当の RMON のデータベースグループに保存されます。管理エージェントは、SNMP プロトコルを使用して定期的に本機と通信します。 ただし、クリティカルなイベントが発生した場合、自動的にトラップメッセージを管理ステーションに送信し、管理エージェントは、そのイベントに対するアクションを実行します。

1. 設定

「システム」→「RMON」→「基本設定」を設定すると、以下の画面が表示されます。

■RMON 設定

❒RMON 設定:RMON を有効/無効にします（デフォルト設定:「無効」）。

上記設定を完了後、<適用>ボタンをクリックしてください。

2. 統計情報

RMON イーサネット統計のパラメータを設定します
SNMP の NMS ソフトウェアと MIB ツリーの RMON を使用して、個々のポートの統計情報をリモートで表示します。

「システム」→「RMON」→「統計情報」をクリックすると、以下の画面が表示されます。

■統計情報設定

❒索引:新しいグループの ID 番号を指定します（範囲:1～65535）。
❒ポート:イーサネットのトラフィックの統計情報の監視用のポートを指定します。
❒オーナー:エントリを作成したユーザーを識別するために使用されます。 これは主に複数の人が管理するスイッチを対象としており、オプションのフィールドです。

・<追加>ボタンをクリックすると、上記に設定した値が次の表に追加されます。
・<リセット>ボタンをクリックすると、入力した値がリセットされます。

■統計情報テーブル

ここでは、索引ごとに、ポート、ドロップイベント数、オクテット数、パケット数、ブロードキャストパケット数、マルチキャストパケット数、オーナー、アクションの値がそれぞれ表示されます。

・<全削除>ボタンをクリックすると、統計情報のエントリーはすべて削除されます。

3. 履歴

RMON 履歴制御設定のためのパラメータ設定

RMON 履歴では、ポート統計が事前に設定された間隔で取得され、スイッチのポート上の入力パケット数、タイプの情報またはパターンを識別するために使用できます。この情報は、MIB ツリーの RMON 部分の履歴グループを使用して、SNMP NMS ソフトウェアで表示されます。
履歴グループは各バケットに分けられ、それぞれポートの統計のスナップショットが 1 つずつ格納されています。グループは 1～50 のバケットを持ち、グループ内のバケット数が多いほど、保存可能なスナップショットも多くなります。

「システム」→「RMON」→「履歴」をクリックすると、以下の画面が表示されます。

■履歴管理設定

❒Index:新しいグループの ID 番号を指定します（範囲: 1～65535）。
❒ポート:イーサネットトラフィックの統計情報を監視するポートを指定します。
❒収集エントリー数:ポートの統計情報のスナップショット数を定義します。各バケットは RMON 統計のスナップショットを 1 つ保存可能です。異なるポートはそれぞれのバケットを持つことができます(範囲: 1～50 バケット)。
❒間隔:スイッチがポートの統計のスナップショットを取得する頻度を指定します(範囲: 1～3600 秒（1 時間））。
たとえば、スイッチがポート上で毎分 1 つのスナップショットを取得したい場合は、「60 秒」に設定します。
❒オーナー:エントリを作成したユーザーを入力します。これは主に複数の人が管理するスイッチを対象としており、オプションのフィールドです。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。
・<リセット>ボタンをクリックすると、入力した値がリセットされます。

■履歴管理テーブル

上記設定を完了後、表に値が反映されます。

4. アラーム

RMON アラームのパラメータを設定します
RMON アラームは、指定されたポートでのパケットアクティビティが指定されたしきい値を上回ったり下回ったりしたときにアラートメッセージを生成するために使用されます。アラートメッセージは、スイッチのイベントログに記録されたメッセージ、または SNMP NMS ソフトウェアに送信されるトラップ、あるいはその両方の形式をとることができます。
RMON アラームは 2 つのしきい値（上限しきい値と下限しきい値）で構成されています。のモニタ対象の指定ポーの RMON 統計値が上限しきい値を超えると、アラームのトリガーとなります。応答は、イベントログへのメッセージの入力、SNMP トラップの送信（またはその両方）です。監視対象の統計情報の値が下限しきい値を下回ると、アラームはリセットされます。
スイッチが実際の RMON 統計情報に対してアラームのしきい値をサンプリングする頻度は、時間間隔パラメータによって制御されます。アラームごとにモニタリング間隔を調整することが可能です。

RMON アラームを構成する 3 つのコンポーネントは次のとおりです。

- ❒RMON 統計グループ：アラームを発生させる場合は、ポートに RMON 統計グループを設定する必要があります。アラームを作成するときは、ポート番号ではなく、ポートの統計グループの ID 番号で割り当て先のポートを指定します。
- ❒RMON イベント：ポートでの入力パケットのアクティビティがアラームで定義された統計上のしきい値を超えたときのスイッチの動作を指定します。オプションは、スイッチのイベントログにメッセージを記録したり、SNMP ワークステーションに SNMP トラップを送信したり（またはその両方）します。
  設定可能なアクションは 3 つのみでイベントは複数のアラームで使用可能です。
- ❒アラーム：監視対象のポート統計情報と、スイッチがイベントのトリガーとなる上限および下限しきい値を定義します。アラームのしきい値は、同じイベントまたは異なるイベントを持つことができます。アラームは最大 8 つまでサポートします。

「システム」→「RMON」→「アラーム」をクリックすると、以下の画面が表示されます。

■アラーム設定

❒索引　新しいグループの ID 番号を指定します(有効範囲:1～65535)。

❒サンプリング間隔:　データがサンプリングされる時間（秒）を指定します(有効範囲: 1～2147483647 秒)。

❒モニタリング変数　イベントが監視している RMON MIB オブジェクトを指定します。

❒モニタリング方式　監視対象統計でアラームのトリガーとなるタイプを定義します。プルダウンメニューから 2 つのオプション(「デルタ値」と「絶対値」)があります。デルタ値設定は、しきい値を統計の現在値と前の値の差と比較します。絶対値設定は、しきい値を現在の統計値と比較します。

❒上昇しきい値　監視統計の特定の値またはしきい値のレベルを指定します。監視対象統計の値がこのしきい値を超えると、アラームイベントが発生します(有効範囲:1～2147483647）。

❒下降しきい値　監視対象統計の特定の値またはしきい値レベルを指定します。監視対象統計の値がこのしきい値レベルを下回ると、アラームイベントがトリガーされます（有効範囲:1～2147483647）。

❒下降イベント Index　上昇しきい値のイベントインデックスを指定します(有効範囲:1～65535)。このフィールドは必須であり、以前に「Events」に入力したイベントのインデックスと一致する必要があります

❒下降イベント Index　下限しきい値のイベントインデックスを指定します(有効範囲:1～65535)。このフィールドは必須であり、以前に「Events」に入力したイベントのインデックスと一致する必要があります。

❒オーナー　エントリを作成したユーザーを識別するために使用されます。これは主に複数の人が管理するスイッチを対象としており、オプションのフィールドです。

・<追加>ボタンをクリックすると、上記に設定した値が次の表に反映されます。

・<リセット>ボタンをクリックすると、入力した値がリセットされます。

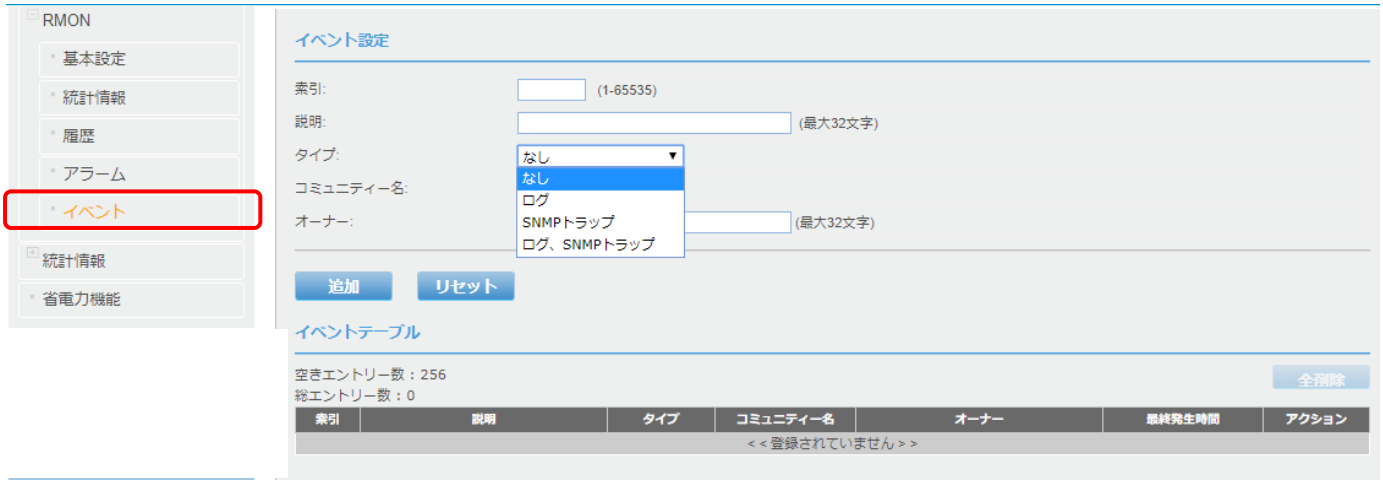
■アラーム設定テーブル

上記設定を完了後、表に値が反映されます。

5. イベント

RMON イベントの値を設定します。
デバイス上の特定の MIB オブジェクトを監視し、それらのいずれかが定義された範囲を超過すると、システム管理者へ警告を発することを目的としています。

「システム」→「RMON」→「イベント」をクリックすると、以下の画面が表示されます。



オプションとしては、スイッチのイベントログにメッセージを記録するか、SNMP ワークステーションに SNMP トラップを送信するか、またはその両方です。

■イベント設定

❒索引：新しいグループ ID 番号を指定します（有効範囲は 1～65535）。
❒説明：設定するイベントの内容を入力します（32 文字以内）。
❒タイプ：イベント発生時にイベントを記録する場所を指定します。
・ログ:スイッチのイベントログにメッセージを記録します。
・SNMP トラップ: SNMP トラップを SNMP　NMS ソフトウェアに送信します。
・ログ、SNMP トラップ：その両方（スイッチのイベントログにメッセージを記録し、SNMP トラップを SNMP　NMS ソフトウェアに送信します。
❒コミュニティー名：SNMP トラップを送信するコミュニティーを指定します。
❒オーナー：エントリを作成した人を識別するために使用されます。これは、主に複数の人が管理するスイッチを対象としており、オプションのフィールドです（32 文字以内）。

<追加>ボタンをクリックすると、新しく設定を追加したい場合にクリックしてください。
<リセット>ボタンをクリックすると、本体はリセットされますが、設定されている値はそのまま保持されます。

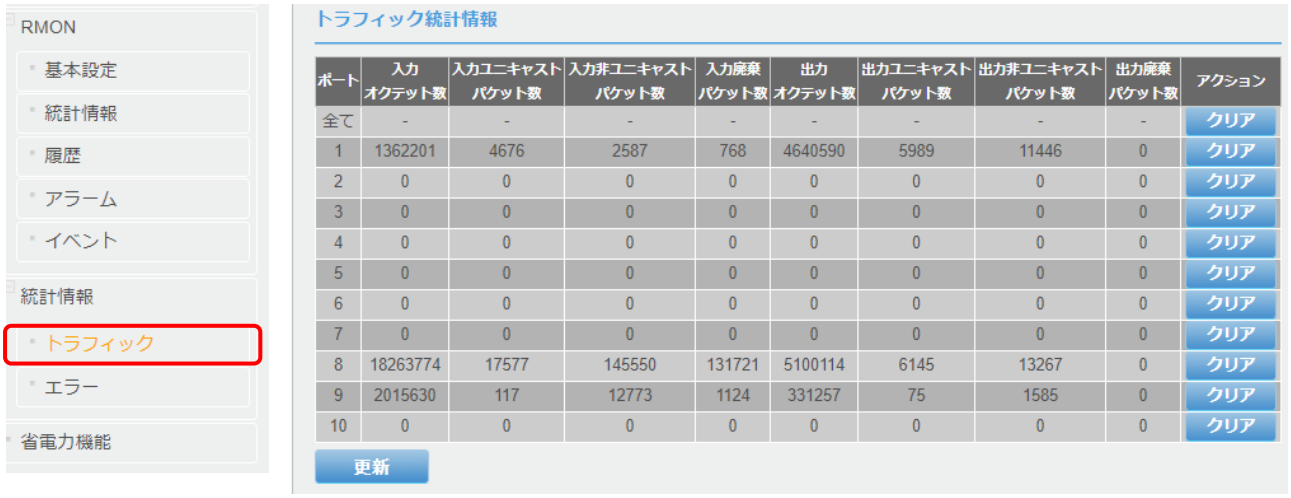
■イベントテーブル：上記で設定した値が表にそれぞれリスト表示されます。

・<全削除>ボタンをクリックすると、イベント情報はすべて削除されます。

3.2.15 統計情報

ポートに関する統計情報を収集します。それらの情報を使用して、一般的なネットワークエラーや全体的なトラフィックレートを監視することができます。
RMON は SNMP エージェントと連携して動作するため、RMON 機能を有効にするには SNMP エージェントを有効にする必要があります。

「システム」→「RMON」→「統計情報」を設定すると、以下の画面が表示されます。



ポート	入力オクテット数	入力ユニキャストパケット数	入力非ユニキャストパケット数	入力廃棄パケット数	出力オクテット数	出力ユニキャストパケット数	出力非ユニキャストパケット数	出力廃棄パケット数	アクション
全て	-	-	-	-	-	-	-	-	クリア
1	1362201	4676	2587	768	4640590	5989	11446	0	クリア
2	0	0	0	0	0	0	0	0	クリア
3	0	0	0	0	0	0	0	0	クリア
4	0	0	0	0	0	0	0	0	クリア
5	0	0	0	0	0	0	0	0	クリア
6	0	0	0	0	0	0	0	0	クリア
7	0	0	0	0	0	0	0	0	クリア
8	18263774	17577	145550	131721	5100114	6145	13267	0	クリア
9	2015630	117	12773	1124	331257	75	1585	0	クリア
10	0	0	0	0	0	0	0	0	クリア

■トラフィック統計情報

- ❒入力オクテット数（InOctets）：入力クテット（バイト/秒）、1 秒あたりのバイト単位の入力クテットビット数を表示します。
- ❒入力ユニキャストパケット数（InUcastPkts）：入力ユニキャストパケット数（Pkts）、1 秒あたりのパケット数で表した入力ユニキャストパケット数を表示します。
- ❒入力非ユニキャストパケット数（InNUcastPkts）：入力非ユニキャストパケット（Pkts）、1 秒あたりのパケット単位の入力非ユニキャストパケット（ブロードキャストおよびマルチキャストパケットなど）の数を表示します。
- ❒入力廃棄パケット数（InDiscards）：入力廃棄（Pkts）、1 秒あたりのパケット単位の入力廃棄パケットの数を表示します。
- ❒出力オクテット数（OutOctets）：出力オクテット（バイト/秒）、1 秒あたりのバイト数で表した出力クテットビットのレートを表示します。
- ❒出力ユニキャストパケット数（OutUcastPkts）：出力ユニキャストパケット（Pkts）、1 秒あたりのパケット数で表した出力ユニキャストパケットの数を表示します。
- ❒出力非ユニキャストパケット数（OutNUcastPkts）：出力非ユニキャストパケット（Pkts）、出力非ユニキャスト（ブロードキャストおよびマルチキャストパケットなど）パケットの数を表示します。
- ❒出力廃棄パケット数（OutDiscards）：出力廃棄（Pkts）、出力廃棄パケットの数を表示します。

3.2.16 省電力機能

IEEE 802.3(EEE)規格では、ネットワーク接続を中断せずにインターフェースを低電力状態に移行させることで、使用率が低い時間にネットワークリンクのエネルギーの消費を低減させることを目的とした方式とプロトコルが定義されています。

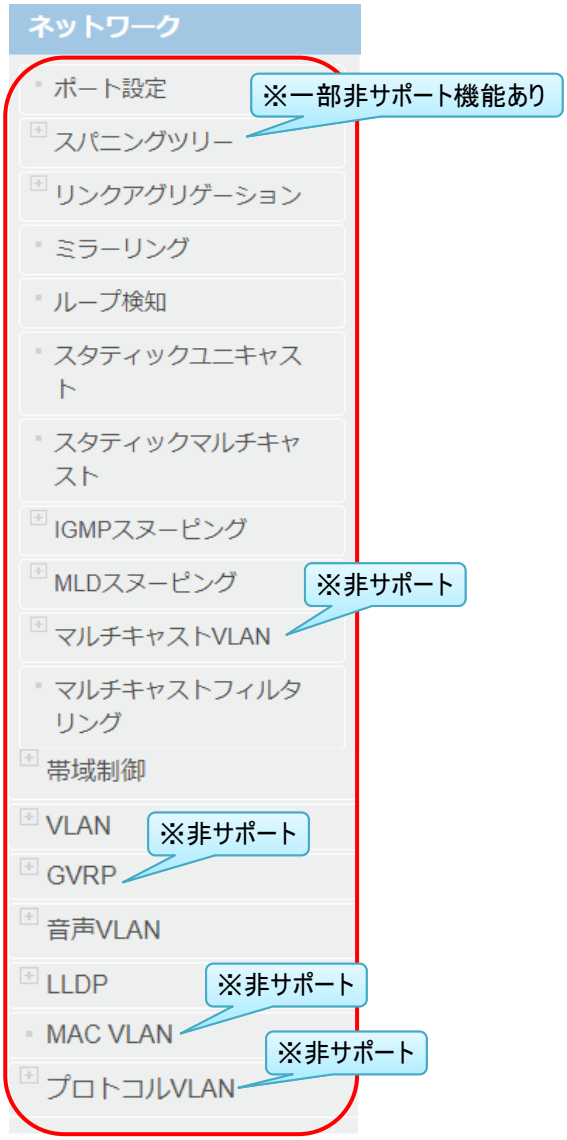
「システム」→「省電力機能」をクリックすると、以下の画面が表示されます。

■IEEE 802.3az　EEE 設定:デバイスの STP 状態を選択してください。この場合、送信側と受信側は省電力機能に準拠している必要があります（デフォルトでは、省電力機能は「無効」））。

3.3 ネットワーク（※一部非サポートあり）

本章では、本機の主な機能の設定方法について説明します。

本メニューは、以下の機能により構成されています。



3.3.1 ポート設定

ここでは、速度、デュプレックス、フロー制御、ジャンボフレームなどの物理ポートのパラメータを設定できます。また各ポートの現在のリンクステータスおよびネゴシエートされた速度/デュプレックスを表示します。また、BPDU ポートをスパニングツリー、EAP ポートを 802.1x ポートベース認証に設定できます。

「ネットワーク」→「ポート設定」をクリックすると、以下の画面が表示されます。

■ポート設定テーブル

❒ポート:ポート番号を指定します。
ポートの「全て」をプルダウンメニューにより「有効」にすると、ポート状態、通信モード、ジャンボフレーム、フロー制御、EAP、BPDU 設定をすべてのポートに同時に適用できます。

❒LAG:トランクグループ番号を表示します。この値により、スタティックまたはダイナミック 802.3ad LACP リンクアグリゲーションを使用してトランクに追加されたポートが表示されます。

❒タイプ:ポートの種類を表示します。スイッチのポートタイプは、10/100/1000Base-T ポート（1～20）の場合は「1000TX」、SFP ポート（17F～20F）の場合は「100FX」または「1000X」と表示されます。

❒ポート状態:ポートに接続されているエンドノード間のリンクのステータスを表示します。
設定可能な値は次のとおりです。
・Up:ポートとエンドノード間に有効なリンクが確立されていることを表示します。
・Down:ポートとエンドノード間に有効なリンクを確立していないことを表示します。

❒通信モード:ポートの動作ステータスを表示します。このパラメータを使用して、ポートを有効/無効にすることができます。ノードに接続されているノードまたはケーブルに問題が発生した場合は、ポートを無効にしてパケットが転送されないようにすることができます。問題が修正された後、ポートを有効にして通常の動作を再開できます。未使用のポートを無効にして、不正な接続から保護することもできます。設定可能な値は次のとおりです。
・ - :全てのポートに適用する場合、ダウンメニューにより「有効」を選択してください。
・有効:ポートがイーサネットフレームを送受信できることを表示します。
・無効:ポートがイーサネットフレームを送受信できないことを表示します。

❒通信モード:ポートの速度と二重モードの設定を表示します。このパラメータを使用して、ポートの速度と二重モードを設定できます。設定可能な設定は以下のとおりです。
・ - :全てのポートに適用する場合、ダウンメニューにより「有効」を選択してください。
・自動（:ポートがオートネゴシエーションを使用して動作速度と二重モードを設定していることを表示します。ポートがエンドノードとのリンクを確立した後、ポートの実際の動作速度とデュプレックスモードが括弧内に表示されます（たとえば、1000 Mbps 全二重モードの場合は「1000/F」）。
・自動（1000F）:ポートがオートネゴシエーションモードで「1000Mbps」に設定されていることを表示します。
・1G/F:ポートが全二重モードで「1000Mbps」に設定されていることを表示します。
・100M/F:ポートが全二重モードで「100Mbps」に設定されていることを表示します。
・10M/F:ポートが全二重モードで「10Mbps」に設定されていることを表示します。
・100M/H:ポートが半二重モードで「100Mbps」に設定されていることを表示します。
・10/H:ポートが半二重モードで「10Mbps」に設定されていることを表示します。

【注記】:
モード設定を選択すると、以下の点が適用されます。
UTPポートがオートネゴシエーションに設定されている場合、エンド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。
オートネゴシエーション対応のスイッチポートは、エンドノードがオートネゴシエーションに設定されていない場合、デフォルトで「半二重」になります。

❒ジャンボフレーム:ジャンボフレームをスイッチが受信可能かどうかを表示します。スイッチがビデオファイルとオーディオファイルを送信するときには、ジャンボフレームを有効にすることをお勧めします。設定可能な値は次のとおりです。
・ - :全てのポートに適用する場合、ダウンメニューにより「有効」を選択してください。
・有効:ポートのジャンボフレームの受信が有効であることを表示します。
・無効:ポートのジャンボフレームの受信が無効であることを表示します。

【注記】:ポートの QoS が有効になっている場合、ジャンボフレームは有効にできません。

❒フロー制御:ポートの現在のフロー制御設定を反映します。スイッチは特殊な一時停止パケットを使用して、特定の時間に送信を停止するようにエンドノードに通知します。
可能な値は次のとおりです。
・ - :全てのポートに適用する場合、ダウンメニューにより「有効」を選択してください。
・有効:フロー制御が有効であることを表示します。
・無効:フロー制御が無効であることを表示します。

❒EAP 透過:現在の拡張認証プロトコル（EAP）の設定状態を反映します。

❒BPDU 透過:ポートの現在の BPDU の設定状態を反映します。
可能な値は次のとおりです。
・ - :全てのポートに適用する場合、ダウンメニューにより「有効」を選択してください。
・有効:スイッチが BPDU フレームをスイッチに通過させ、他のすべてのポートにブロードキャストされることを表示します。
・無効:スイッチがスイッチを介して BPDU フレームを通過させないことを表示します。RSTP または STP が有効な場合、スイッチは BPDU フレームを受信し、スパニングツリープロトコルに従って処理されます。

3.3.2 スパニングツリー

【注記】:弊社では、本製品での MSTP 機能についてはサポートしておりません。

1. プロトコル

スパニングツリープロトコル（STP）は、ブリッジ/スイッチに対してネットワークトポロジを提供します。 また、ネットワーク上のエンドステーション間に単一のパスを提供することにより、ループを解消します。 ホスト間に代替ルートが存在すると、ループが発生します。 拡張ネットワークでループが発生すると、ブリッジはトラフィックを無期限に転送するため、トラフィックの増加により、ネットワークの効率が低下します。

「ネットワーク」→「スパニングツリー」→「プロトコル」をクリックすると、以下の画面が表示されます。

■STP 設定

STP 機能を有効にすると、各機能の設定が可能になります。

❒STP 機能:デバイスの STP 機能の有効/無効を選択してください（デフォルト:無効）。

❒プロトコル:有効にするスパニングツリープロトコル（STP）モードを指定します。

可能なフィールド値は次のとおりです。

・STP:デバイス上で STP 802.1d を有効にします。

・RSTP:デバイス上で Rapid STP 802.1w を有効にします（デフォルト）。

・MSTP:デバイス上で複数の STP 802.1s を有効にします。

❒ブリッジ優先度:ブリッジ優先度を設定します（有効範囲:0～61440（4096 単位）、デフォルト:32768）。ブリッジ優先度は、ルートブリッジを決定するためのパラメータです。ブリッジ優先度は値が小さいほど高い優先度になり，最も小さい値を設定した装置がルートブリッジになります。

❒BPDU エージング時間:ポートが STP/RSTP 情報を受信するまでの待機時間を定義します。マルチキャストスパニングツリーは、境界ポート上の STP/RSTP ドメインと通信時にこのパラメータを使用します（有効範囲:6～40 秒、デフォルト:20 秒）。

❒BPDU 送信時間:Hello タイムは、ルートブリッジによる BPDU の送信間隔を表します（有効範囲:1～10 秒）。

❒状態遷移保留時間:ブリッジがリスニング/ラーニング/フォワーディングへ遷移する際の保留時間を定義します（有効範囲:4～30 秒、デフォルト:2 秒）。

❒転送保留カウント:ブリッジが 1 秒間に送信できる BPDU の最大数を指定します(有効範囲:1～10、デフォルト:6)。

❒最大ホップ数:発信時に BPDU パケットに設定されるパラメータです。次のブリッジにより再送信されると、「1」つずつ減少します。ホップカウント値が「0」に達すると、ブリッジは BPDU パケットを破棄します（有効範囲: 6～40、デフォルト:20）。

【注記】: STP 機能を有効にすると、一時的に操作できなくなります。

■ルート情報

上記で設定したスパニングツリーのルート情報が表示されます。

2. ポート

スパニングツリープロトコルのポートの設定方法について説明します。

「ネットワーク」→「スパニングツリー」→「ポート」をクリックすると、以下の画面が表示されます。

■ポート設定

❒ポート:本機のポート番号が表示されます。

※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒STP 状態:スパニングツリープロトコルを有効/無効にします。

❒ポート優先度:ポートの優先順位を表示します（有効範囲: 0～240（16 の倍数））。2 つのパスコストが同じ値の場合に、そのプライオリティを選択する必要があります。ブリッジ優先度と同様に、ブリッジ優先度は値が小さいほど高い優先度になり、最も小さい値を設定した装置がルートポートになります。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。

ポート優先度の有効な値は、以下のとおりです。

レベル	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ポート優先度	0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240

❒パスコスト(0=自動計算):スパニングツリールートへのパスのパスコストに対して、管理上割り当てられた値です。値「0」を入力すると、自動で計算されたデフォルトのパスコスト値がポートに割り当てられます（デフォルト:0）。

❒外部コスト:指定されたポートリストにパケットを転送するための相対コストを示すメトリックを定義します。ポートコストは自動的に設定することも、メトリック値として設定することもできます。外部コストには「1～200000000」の間の値を定義してください。値が小さいほど、ポートがパケット転送用に選択される確率が高くなります（デフォルトのポートコストは「100Mbps ポート= 200000」、「Gigabit ポート= 20000」）。

❒状態:現在のポートスパニングツリーのステータスを表示します（デフォルト:無効）。

・ブロッキング:データの送受信をブロックし、MAC アドレスの学習も行いません。ただし 例外として BPDU の受信のみ許可します。ブロッキング(Blocking)状態はデフォルトで 20 秒経過するか BPDU を受信するとリスニング状態へ移行します。

・リスニング:データの送受信、また MAC アドレスの学習も行いません。この状態では BPDU の交換のみを行い、ルートブリッジの選択や最適経路の選択を行います。

・ラーニング: MAC アドレスの学習を許可されます。 ただしまだデータの送受信は出来ません。ポートは受信したフレームから送信元アドレスを学習し、それらをフィルタリング（スイッチング）データベースに追加します。

・フォワーディング:データの送受信が可能になります。STP は、ループを防ぐためにブロッキング状態のポートのモニタリングを継続します。
・無効　:ポートのスパニングツリーの機能が無効であることを表します（デフォルト設定）。

❒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の状態を設定します（デフォルト：自動）。エッジポートはスパニングツリーのトポロジー計算対象外となり、リンクアップ後直ちに通信可の状態になります。

❒P2P 共有リンク：P2P ポートはエッジポートと似ていますが、P2P ポートは全二重で動作する必要があります。（デフォルト：自動）。
また、エッジポートと同様に、P2P ポートは即時フォワーディング状態に移行するため、RSTP に影響を与えます。
ポートがこのステータスを維持できない場合（たとえば、ポートが半二重で強制設定されている場合）は、P2P リンク状態になりません。

❒ルートガード:パケットの制限付きの状態を有効/無効に切り替えます。「有効」に設定した場合、ポートはルートポートとして選択されることはありません（デフォルト：無効）。

❒TCN フィルタリング：パケットの制限付き TCN（トポロジ変更通知）のフィルタリングを有効/無効に切り替えます。TCN は、ブリッジがトポロジ変更を通知するためにルートポートに送信する BPDU です。「有効」に設定されている場合、ポートは受信した TCN を他のポートに伝播しません（デフォルト:無効）。

❒マイグレーション:ポートが RSTP および STP の BPDU に設定可能かどうかを表示します。

【注記】:この手順を実行すると、すべての設定変更が保存され、スイッチを再起動したり電源を入れ直した場合でも、設定の変更内容は適用されます。

3. トポロジ変更保護

トポロジの変更保護を設定します。

「ネットワーク」→「スパニングツリー」→「トポロジ変更保護」をクリックすると、以下の画面が表示されます。

■TC 保護

❒TC 保護機能: トポロジ変更保護機能を有効/無効にします（デフォルト:無効）。

❒TC 保護閾値: トポロジ変更保護機能の閾値を設定します（有効範囲:1-100 回、デフォルト値:20 回）。

❒TC 保護サイクル: トポロジ変更の実行サイクルを設定します（有効範囲:1-10 秒、デフォルト値:5 秒）。

上記設定を完了後、<適用>ボタンをクリックしてください。

4. マルチキャストスパニングツリー（※非サポート）

スパニングツリープロトコルの MST（マルチキャストスパニングツリー）設定について説明します。

「ネットワーク」→「スパニングツリー」→「マルチキャストスパニングツリー」をクリックすると、以下の画面が表示されます。

■MST 設定

❒リージョン名: MSTI（Multiple スパニングツリーインスタンス）を一意に識別するためにスイッチに設定されている設定名を設定します（32 文字以内）。リージョン名が設定されていない場合、このフィールドにはマルチキャストスパニングツリーを実行しているデバイスの MAC アドレスが表示されます。

❒リビジョン:この値は、設定名、および STP インスタンス ID にマッピングされた同一の VLAN とともに、スイッチに設定されている MST リージョンを識別します（有効範囲:0～65535、デフォルト設定:0）。

■MST インスタンス ID

❒MST インスタンス ID:VID リストに関連付けられている MSTI ID を表示します(有効範囲:1～31)。

❒VLAN ID リスト:VID リストを表示します（有効範囲:1- 4094）。
下の MST 情報テーブルに追加するには<追加>ボタンをクリックします。

❒優先度:新しい優先度を入力します（有効範囲:0～61440、デフォルト設定:32768)。

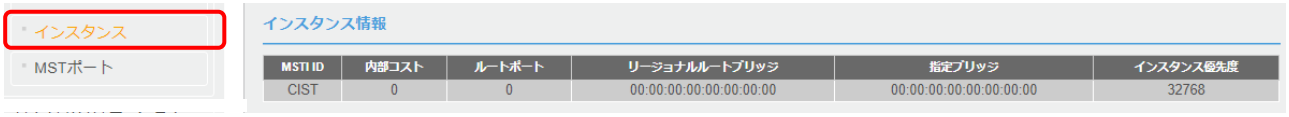
■MST 情報テーブル

上記の「MST インスタンス ID」で<追加>ボタンをクリックすると、新しいインスタンス ID の情報が表に追加されます。

5. インスタンス（※非サポート）

スパニングツリープロトコルのインスタンス情報（マルチキャストスパニングツリー）を表示します。

「ネットワーク」→「スパニングツリー」→「インスタンス」をクリックすると、以下の画面が表示されます。



■インスタンス情報

❒MSTI ID:VLAN が割り当てられているインスタンスを指定します。

❒内部コスト:STP インスタンス内でインターフェースが選択されている場合に、指定されたポートにパケットを転送するためのコストを表示します。

❒ルートポート:選択したインスタンスのルートポート番号を表示します。

❒リージョナルルートブリッジ:領域内のルートブリッジ ID を表示します。

❒指定ブリッジ:リンクまたは共有 LAN をルートに接続しているブリッジの ID を表示します。

❒インスタンス優先度:選択したスパニングツリーインスタンスデバイスの優先順位を指定します(範囲は「0～61440」、デフォルト値は「32768」)。

6. MST ポート（※非サポート）

スパニングツリープロトコルの MST ポート（マルチキャストスパニングツリーポート）のパスコストおよび優先度を設定します。

「ネットワーク」→「スパニングツリー」→「MST ポート」をクリックすると、以下の画面が表示されます。

■MST ポート

❒ポート選択：ドロップダウンメニューをクリックして、設定する MST ポートを選択してください。

■MST ポート情報

MST ポート情報画面では、マルチキャストスパニングツリーインターフェースを設定できます。

❒MSTI ID:VLAN が割り当てられているインスタンスを指定します。

❒指定ブリッジ:リンクまたは共有 LAN をルートに接続しているブリッジの ID を表示します。

❒内部コスト:STP インスタンス内でインターフェースが選択されている場合に、指定されたポートにパケットを転送するためのコストを表示します（デフォルト:200000000）。

❒パスコスト(0=自動):ルートブリッジへのパスコストを計算時にマルチキャストスパニングツリーによって使用されるポートコストです（デフォルト:0）。

❒優先度:スイッチ上の 2 つのポートのコストが同じ場合に、マルチキャストスパニングツリーによってパスコストの計算に使用されるポートの優先度を表します（デフォルト:128）。

❒状態:STP ポートの現在の状態が表示されます。

❒役割: STP ポートの役割が表示されます。

❒アクション: <適用>ボタンをクリックすると、それぞれ値が表に反映されます。

【注記】:この手順を実行すると、すべての設定変更が保存されるため、本機を再起動したり電源を入れ直した場合でも、設定の変更内容は適用されます。

3.3.3 リンクアグリゲーション

1. グループ

この機能により、2 つ以上のポートをカスケードして総帯域幅を増やすことができます。最大 4 つのトランクグループを作成でき、それぞれ最大 8 つのポートをサポートします。

【注記】:ポートトランクのケーブルをポートに接続してから、本機と対抗機の両方のポートを設定してください。ポートを設定する前にケーブルを接続すると、ネットワークトポロジにループが生じる可能性があります。
ループが発生するとブロードキャストストームが発生し、ネットワークの有効帯域幅が大幅に制限される可能性があります。

「ネットワーク」→「リンクアグリゲーション」→「グループ」をクリックすると、以下の画面が表示されます。

■リンクアグリゲーション設定

❒ポート:LAG グループの対象となるポート番号を選択してください。

❒モード:ドロップダウンリストにて、次のいずれかのオプションを選択してください。

・LACP(アクティブ):特定のアグリゲータは LACPDU（LACP Data Unit）パケットをブロードキャストして応答します。 この設定はトランクのための動的 LACP 機能を有効にします。同一のグループに、2～8 ポートまで選択可能です。
・LACP(パッシブ):特定のアグリゲータは応答しまが、LACPDU パケットをブロードキャストしません。この設定はトランクの LACP 機能を無効にします。同一のグループに、2～8 ポートまで選択可能です。
・スタティック:スタティックポートのトランキングを有効にし、トランクの LACP 機能を無効にします（スタティックリンクアグリゲーション）。同一のグループに、2～8 ポートまで選択可能です。
・無効:スタティックポートトランクおよび LACP 機能を無効にします。
【注記】:モードの「無効」を選択すると、全てのポートのチェックが外されます。

2. LACP 情報

LACP（Link Aggregation Control Protocol）とは、ネットワークの構成時に、機器間を接続する複数の物理リンクを束ねて 1 つの論理リンクとして扱う「リンクアグリゲーション」という技術で使われるプロトコルです。
グループ ID ごとに、登録されているメンバーポートのステータスが表示されます。

「ネットワーク」→「リンクアグリゲーション」→「LACP 情報」をクリックすると、以下の画面が表示されます。

■LACP 情報

❒システム優先度：この値はスイッチに適用されます。値は事前に割り当てられており、変更できません。

❒システム ID：個々のスイッチに割り当てられた MAC アドレス値を表示します。この値は変更できません。

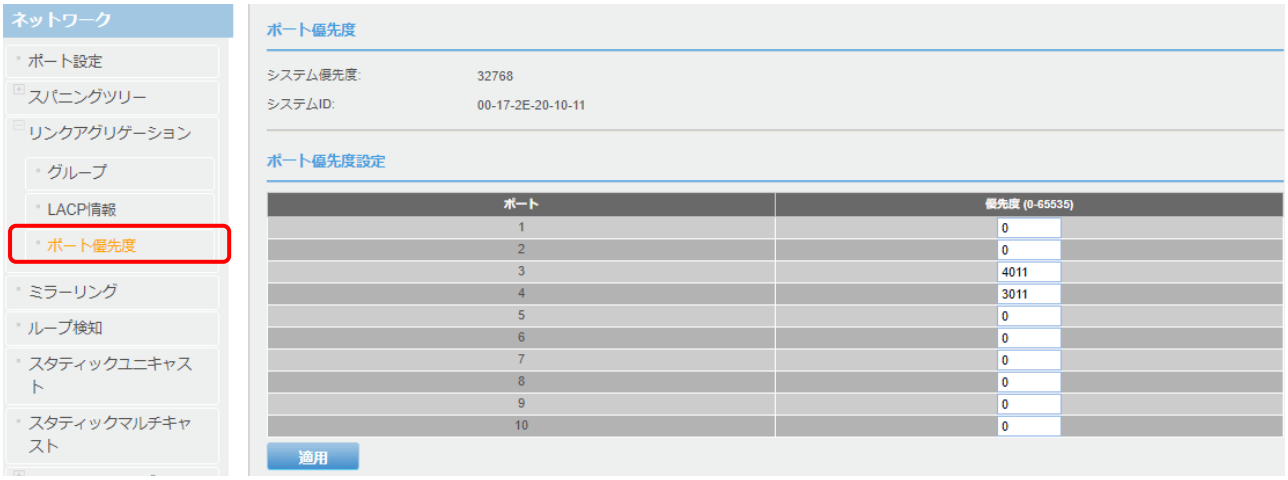
LAGグループID	メンバーポート	アクティブポート	スタンバイポート

❒LAG グループ ID＃：トランク（リンクアグリゲーショングループ）の ID 番号のステータスを表示します。
グループ ID ごとに登録されているポートの情報（メンバーポート、アクティブポート、スタンバイポート）がそれぞれ表示されます。

3. ポート優先度

ポートの優先度を指定します。値が小さいほど優先度が高くなります。

「ネットワーク」→「リンクアグリゲーション」→「ポート優先度」をクリックすると、以下の画面が表示されます。



■ポート優先度

❒システム優先度：この値はスイッチに事前に割り当てられた変更不可の値です

❒システム ID：個々のスイッチに割り当てられた MAC アドレス値を表示します。この値は変更できません。

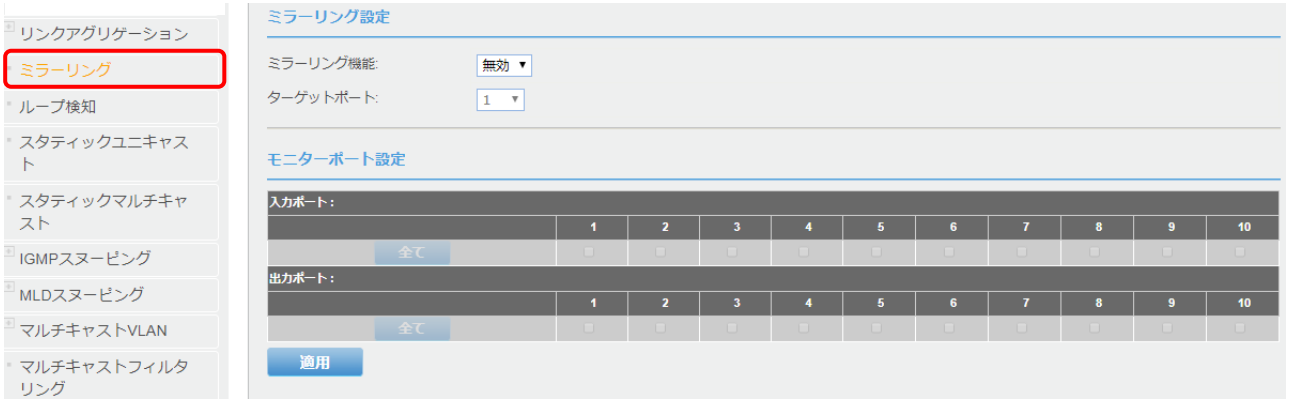
■ポート優先度設定
　それぞれのポートに対して優先度を割り当てることができます（有効範囲:0-65535）。

上記設定を完了後、<適用>ボタンをクリックすると、それぞれ値が表に反映されます。

3.3.4 ミラーリング

任意の送信元ポートからターゲットポートへのトラフィックをリアルタイム分析用にミラーリングすることができます。さら に、論理アナライザ、または RMON プローブをターゲットポートに接続して、送信元ポートで送受信されるトラフィックを、通信の妨げとならない方法で確認することができます。

「ネットワーク」→「ミラーリング」をクリックすると、以下の画面が表示されます。



■ミラーリング設定
　❒ミラーリング機能を有効/無効にします。

　❒ターゲットポート:ドロップダウンリストをクリックし、コピー対象の入力/出力パケット/データの送信先のポートを選択してください。（例:パケットキャプチャまたはデータ分析プログラムを備えたコンピュータまたは装置）

■モニターポート設定
　モニターポート設定にて、情報のモニタリング用の入力ポート、またはコピー先の出力ポートを選択してください。

　❒入力ポート:特定のポートでの受信パケットをコピーします。
　❒出力ポート:特定のポートでの送信パケットをコピーします。

　・<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、上記の設定したエントリが反映されます。

3.3.5 ループ検知

ループバック検出機能は、スイッチに直接接続されているアップリンクまたはダウンリンクスイッチで発生するループを検出したり、ループによる中断を事前に防止することができます。

「ネットワーク」→「ループ検知」をクリックすると、以下の画面が表示されます。

■ループ検知状態:ループバック検出機能の有効/無効を選択してください。

■ループ検知時間

❒検知フレーム送信間隔:ループのチェック間隔を定義します（有効範囲:1-32767 秒、デフォルト:2 秒）。

❒自動復旧時間: ループ検出によりブロック状態のポートへの接続が復旧されるまでの時間を定義します（有効範囲:60-1000000、デフォルト:60 秒）。ただし、自動復旧しない場合は、「0」に設定してください。

・有効:各ポートのループバック検出機能を有効にします。 この機能を選択したポートでアクティブにするには、事前にこの状態を画面上部の「Status」フィールドと共に有効にする必要があります。

・無効:選択したポートのループバック検出機能は無効となります。

【注記】:ループ検知機能を無効にすると、すべての値が初期値に戻ります。

上記設定を完了後、<適用>ボタンをクリックしてください。

■ループ検知テーブル

上記に設定したエントリが表に反映されます。

・ポートの「全て」をプルダウンメニューにより「有効」にすると、設定はすべてのポートに適用されます。

3.3.6 スタティックユニキャスト

ここでは、スタティックユニキャストエントリを設定に追加することができます。

「ネットワーク」→「スタティックユニキャスト」をクリックすると、以下の画面が表示されます。

■スタティックユニキャスト登録

❒VLAN　ID: MAC アドレスが常駐する VLAN ID を入力します（有効範囲:1-4094）。

【注記】:デフォルトでは、すべてのポートは「VLAN ID =1」です。

VLAN ID は、「VLAN」→「アドレス学習モード」の「学習モード」が「IVL」に設定されている場合のみ変更可能です。

❒MAC アドレス:追加するデバイスの MAC アドレスを入力します。

■ポート設定

MAC アドレスの登録先のポート番号を選択します。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

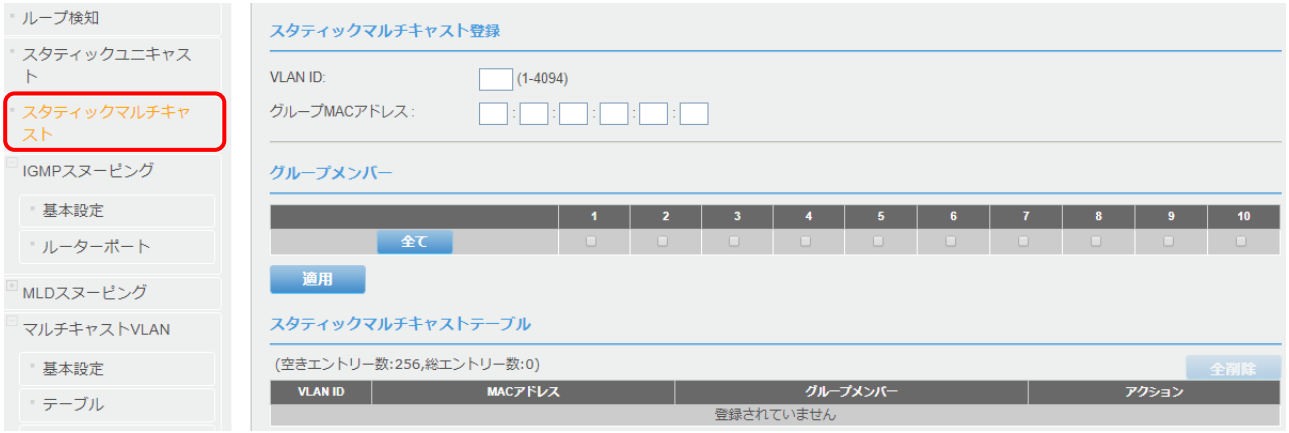
■スタティックユニキャストテーブル

・<全削除>ボタンをクリックすると、設定したスタティックエントリーはすべて削除されます。

3.3.7 スタティックマルチキャスト

ここでは、スタティックマルチキャストエントリを設定に追加することができます。

「ネットワーク」→「スタティックマルチキャスト」をクリックすると、以下の画面が表示されます。



■スタティックユニキャスト登録

❒VLAN　ID:マルチキャストグループの MAC アドレスが常駐する VLAN ID を入力します（有効範囲: 1-4094）。
【注記】:すべてのスイッチポートのデフォルトの VLAN ID は「1」です。

❒グループ MAC アドレス:マルチキャストグループの MAC アドレスを入力します。

■グループメンバー: MAC アドレスが常駐するポートを選択します。
指定のグループ MAC アドレスに対して、複数のグループメンバーを選択することができます。

・<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。

■スタティックユニキャストテーブル
上記設定を完了後、<適用>ボタンをクリックすると、それぞれエントリが表に反映されます。

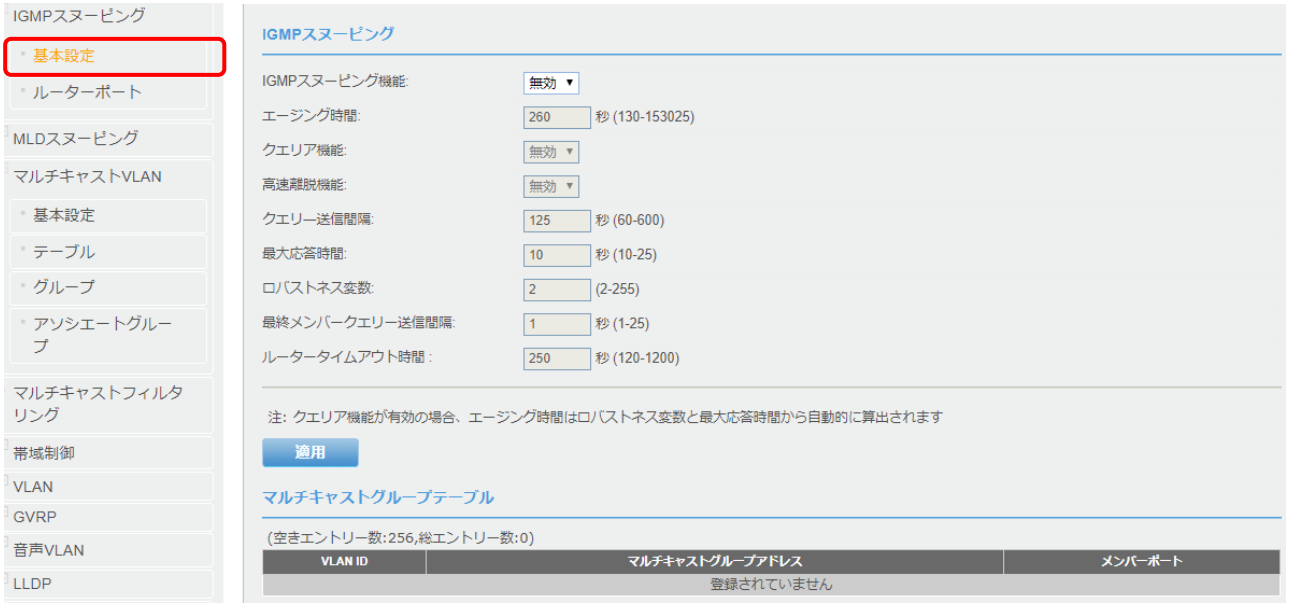
・<全削除>ボタンをクリックすると、設定したスタティックエントリーはすべて削除されます。

3.3.8 IGMP スヌーピング

IGMP スヌーピングは、マルチキャストフィルタリングをサポートするために必要な一連の機能の中核を成しています。マルチキャストクライアントからの IGMP サービス要求をパッシブに監視するため、マルチキャストトラフィックの転送が必要なスイッチポートを動的に設定するために使用されます。

1. 基本設定

「ネットワーク」→「IGMP スヌーピング」→「基本設定」をクリックすると、以下の画面が表示されます。



■IGMP スヌーピング

❒IGMP スヌーピング機能: IGMP スヌーピング機能を有効/無効にします。

❒エージング時間:スイッチが非アクティブの動的 MAC アドレスを消去するまでの待機時間を秒単位で入力します（有効範囲：130-153025，デフォルト値：260）。

❒クエリア機能:ドロップダウンリストをクリックし、クエリア機能を有効/無効にします（デフォルト:無効）。

❒クエリー送信間隔: IGMP クエリの送信時間を入力します(有効範囲:60-600，デフォルト値：125)。

❒最大応答時間:応答レポートを送信するまでの最大時間を指定します(有効範囲:10-25，デフォルト値：10)。

❒ロバストネス変数:サブネット上で予想されるパケット損失の変数を入力します。より高いパケット損失が予想される場合は、ロバストネス変数をより大きな値に設定する必要があります(有効範囲:2-255，デフォルト値：2)。

❒最終メンバークエリー送信間隔:メッセージを残すために応答して送信されたグループクエリの応答時間を設定します(有効範囲:1-25，デフォルト値：1)。

❒ルータータイムアウト時間:ルータがタイムアウトするまでの、ルータメッセージが表示される前の最大時間を入力します(有効範囲:120-1200，デフォルト値：250)。

【注記】:クエリア機能が有効の場合、エージング時間はロバストネス変数と最大応答時間から自動的に算出されます。

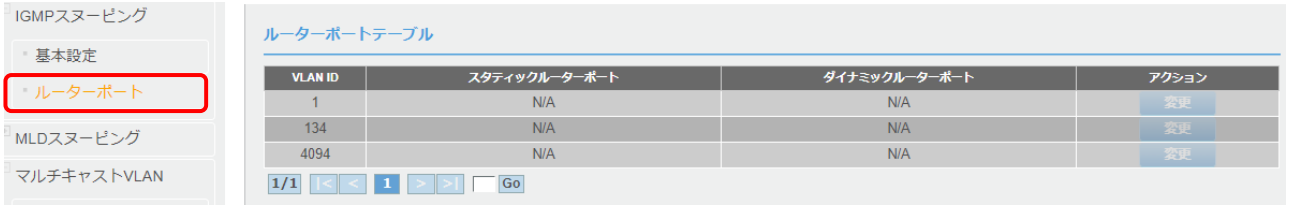
■マルチキャストグループテーブル

VLAN ID ごとに、登録されているマルチキャストグループアドレスとメンバーポートが表示されます。

2. ルーターポート

VLAN ID のルータポートリストでは、スタティックおよびダイナミックルータポートを設定できます。
手動で設定された IGMP スヌーピングルータポートはスタティックルータポートであり、動的ルータポートはクエリ制御メッセージを受信したときにスイッチによって動的に設定されます。

「ネットワーク」→「IGMP スヌーピング」→「ルーターポート」をクリックすると、以下の画面が表示されます。



■ルーターポートテーブル

VLAN ID ごとに、登録されている「スタティックポート」および「ダイナミックポート」が表示されています。
※ポートが登録されていない場合は、「N/A」と表示されます。

・<変更>ボタンをクリックすると、登録されている設定を変更できます。

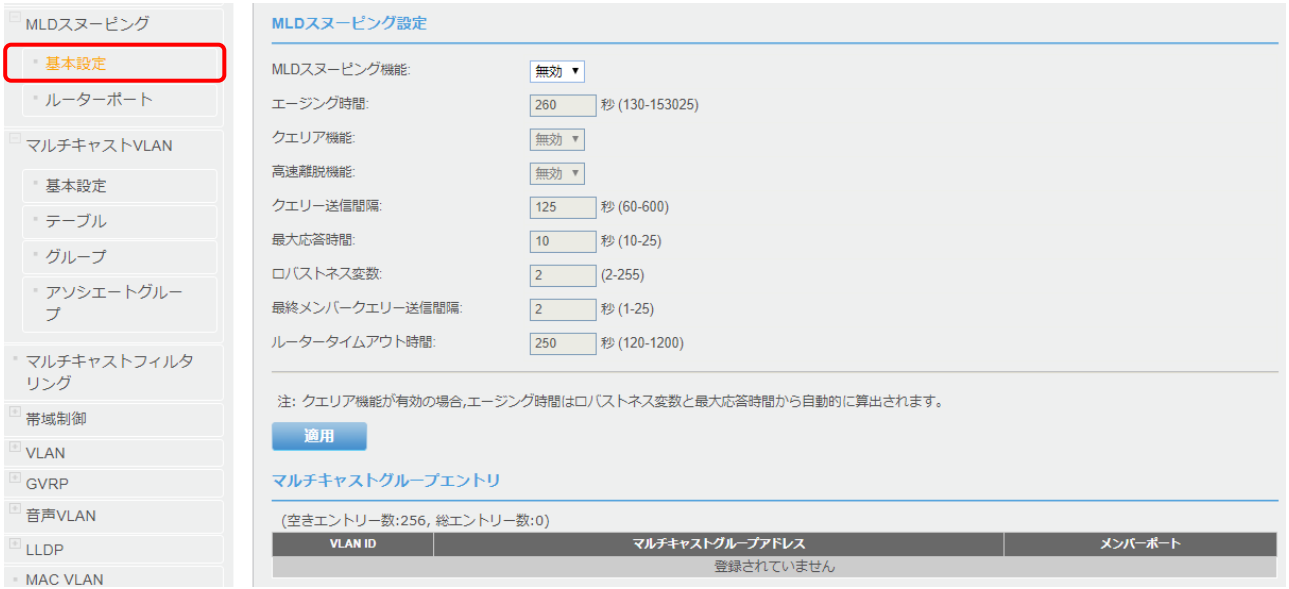
エントリが複数の画面にわたる場合は、「Page」フィールドでページ番号を指定して<Go>ボタンをクリックするか、|<(先頭のページへ)、<(前ページへ)、>(次ページへ)、>|(最後のページへ)のいずれかをクリックして、画面を移行できます。
特定のページに進みたい場合は、空欄に指定の数値を入力して、<GO>ボタンをクリックしてください。

3.3.9 MLD スヌーピング

1. 基本設定

IPv6 マルチキャストにおいてスイッチが各ポートの MLD メッセージを監視して、受信者のいるポートにのみマルチキャストトラフィックを転送します。MLD スヌーピングを使用すると、IPv6 マルチキャストデータは VLAN（仮想 LAN）内のすべてのポートにフラッディングされるのではなく、データを受信するポートのリストに転送されます。

「ネットワーク」→「MLD スヌーピング」→「基本設定」をクリックすると、以下の画面が表示されます



■MLD スヌーピング設定

❒MLD スヌーピング機能:ドロップダウンリストをクリックして、MLD スヌーピング機能を有効/無効にします。

❒エージング時間:スイッチが非アクティブの動的 MAC アドレスを消去するまでの待機時間を秒単位で入力します（有効範囲：130-153025，デフォルト値：260）。

❒クエリア機能:ドロップダウンリストをクリックし、クエリア機能を有効/無効にします。

❒クエリー送信間隔: IGMP クエリの送信時間を入力します(有効範囲:60-600，デフォルト値：125)。

❒最大応答時間:応答レポートを送信するまでの最大時間を指定します(有効範囲:10-25，デフォルト値：10)。

❒ロバストネス変数:サブネット上で予想されるパケット損失の変数を入力します。より高いパケット損失が予想される場合は、ロバストネス変数をより大きな値に設定する必要があります(有効範囲:2-255，デフォルト値：2)。

❒最終メンバークエリー送信間隔:メッセージを残すために応答して送信されたグループクエリの応答時間を設定します(有効範囲:1-25，デフォルト値：1)。

❒ルータータイムアウト時間:ルータがタイムアウトするまでの、ルータメッセージが表示される前の最大時間を入力します(有効範囲:120-1200，デフォルト値：250)。

【注記】:クエリア機能が有効の場合、エージング時間はロバストネス変数と最大応答時間から自動的に算出されます。

上記設定を完了後、<適用>ボタンをクリックすると、次の表に値が反映されます。

■マルチキャストグループエントリ

上記の設定が反映されます。

3.3.10 マルチキャスト VLAN（※非サポート）

MVR(Multicast VLAN Registration)は、マルチキャストトラフィック（TV チャネルやビデオオンデマンドのトラフィック）をサービスプロバイダーのネットワーク経由で送信する場合に最もよく使用されている単一のネットワーク VLAN に対するアクセスを制御するプロトコルです。VLAN 内のあらゆるマルチキャストトラフィックは、その VLAN に接続しているすべてのサブスクライバに送信されます。このプロトコルを使用すると、マルチキャスト VLAN の配信ツリーを動的に監視および確立するために必要な処理オーバーヘッドを大幅に削減することができます。
その結果、マルチキャストルーティングプロトコルを一切使用していない場合でも、一般的なマルチキャストサービスをネットワーク内の広い範囲でサポートすることが可能になります。MVR では、サブスクライバが属している他の VLAN のみにトラフィックを送信することにより、VLAN セグリゲーションで実現されるユーザーの分離とデータのセキュリティを確立します。共通のマルチキャストストリームは MVR VLAN から別々の VLAN グループに配信され、異なる IEEE 802.1Q VLAN 内のユーザーは、上位のルーティングサービスを使用しない限り、相互に情報を交換することはできません。

1. マルチキャスト VLAN の設定

「ネットワーク」→「マルチキャスト VLAN」→「基本設定」をクリックすると、以下の画面が表示されます

■マルチキャスト基本設定
　❒IPv4 マルチキャスト機能:有効/無効にします。
　❒IPv6 マルチキャスト機能:有効/無効にします。

　上記設定を完了後、<適用>ボタンをクリックしてください。

■マルチキャスト VLAN 設定
　❒VLAN ID:新規 VLAN の VLAN ID を入力します（有効範囲:2-4094）。
　❒VLAN 名: VLAN 名を入力します(32 文字以内)。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。
・<削除>ボタンをクリックすると、設定したエントリが削除されます。

■マルチキャスト VLAN ポート
　上記設定を完了すると、値が表に反映されます。

2. テーブル

マルチキャスト VLAN が割り当てられたポートが表示されます。

「ネットワーク」→「マルチキャスト VLAN」→「テーブル」をクリックすると、以下の画面が表示されます

■マルチキャスト VLAN テーブル

❒VLAN 名: VLAN 名を入力します。

❒状態: マルチキャスト VLAN の状態（有効/無効に）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 に対応しているタグ 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 に対応している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 に対応しているタグなし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 に対応しているタグなしソースポートが表示されます。

3. グループ

マルチキャスト VLAN のプロファイル名およびグループプロファイルの設定を行います。

「ネットワーク」→「マルチキャスト VLAN」→「基本設定」をクリックすると、以下の画面が表示されます

■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入力します(32 文字以内)。

・<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：登録済みのマルチキャスト VLAN のプロファイル名を入力します(32 文字以内)。

❒IP アドレス範囲: 「IPv4」または「IPv6」を選択し、追加または削除したい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>ボタンをクリックすると、上記に設定したエントリが次の表に追加されます。
・<削除>ボタンをクリックすると、設定したエントリが削除されます。

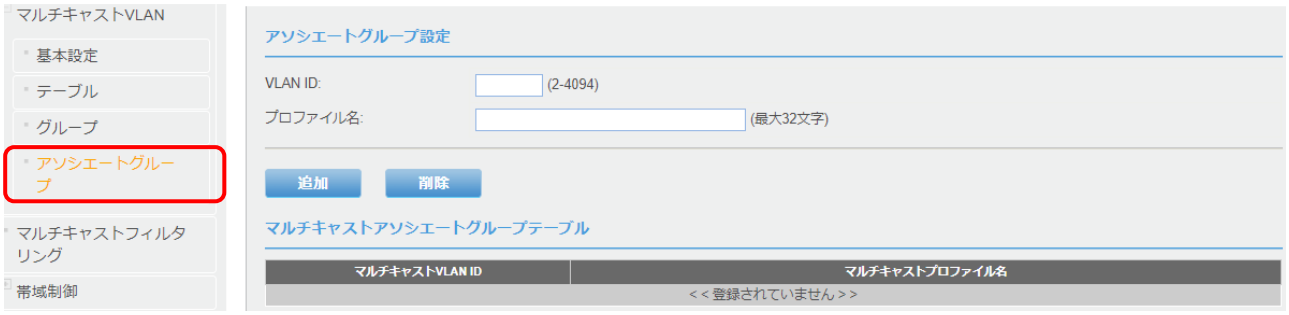
■マルチキャスト VLAN プロファイルテーブル

上記設定を完了すると、設定したマルチキャスト VLAN のプロファイル名が表示されます。

4. アソシエートグループ

前ページの「グループ」メニューで作成したマルチキャスト VLAN に対しプロファイルを割り当てます。

「ネットワーク」→「マルチキャスト VLAN」→「アソシエートグループ」をクリックすると、以下の画面が表示されます



■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 を入力します（有効範囲:2～4094）。

❒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入力します(32 文字以内)。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に追加されます。
・<削除>ボタンをクリックすると、表示されている値が削除されます。

■マルチキャストアソシエートグループテーブル

上記設定を完了すると、値が表に反映されます。

3.3.11 マルチキャストフィルタリング

ここでは、マルチキャストフィルタリングの設定を行います。

「ネットワーク」→「マルチキャスト VLAN」→「マルチキャストフィルタリング」をクリックすると、以下の画面が表示されます

■マルチキャストフィルタリング設定

❒ポート:本機のポート番号が表示されます。

※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒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を有効/無効にします。

・無効：マルチキャストテーブルを参照しません。

・有効：マルチキャストテーブルを参照して転送します。

❒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。

3.3.12 帯域幅制御

1. ストームコントロール

ここでは、各スイッチポートの宛先不明ユニキャスト、ブロードキャスト、マルチキャストのストームコントロールしきい値を設定することができます。ネットワーク上のデバイスが正常に動作していない場合や、アプリケーションプログラムが適切に設計または設定されていない場合にトラフィックストームが発生する可能性があります。また、ネットワークのトラフィックが過剰な場合、パフォーマンスが大幅に低下したり、すべての機能が完全に停止したりすることがあります。ブロードキャスト、マルチキャスト、または宛先不明ユニキャストのトラックのしきい値を設定することにより、ネットワークをトラフィックストームから保護することができます。

「ネットワーク」→「帯域幅制御」→「ストームコントロール」をクリックすると、以下の画面が表示されます。

■ストームコントロール設定

❒ポート:本機のポート番号が表示されます。

※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒宛先不明ユニキャスト: 宛先不明ユニキャストのストームコントロールを有効/無効にします。

❒ブロードキャスト:ブロードキャストのストームコントロールを有効/無効にします。

❒マルチキャスト:マルチキャストのストームコントロールを有効/無効にします。

❒閾値: 1 秒あたりのパケット数の閾値を入力します（64pps　x　値（有効範囲: 1-4096））。

❒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。

2. 入力レート制限

ここでは、各スイッチポートの入力レート制限設定を行います。

「ネットワーク」→「帯域幅制御」→「入力レート制限」をクリックすると、以下の画面が表示されます。

■入力レート制限設定

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒制限帯域:入力レートの制限値を入力して下さい。
※ポートの最大速度は、1,000,000Kbps（64Kbps × 15625）です。

❒状態:入力レートの制限を有効/無効にします。

❒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。

3.出力レート制限

ここでは、各スイッチポートの出力レートを設定します。

「ネットワーク」→「帯域幅制御」→「出力レート制限」をクリックすると、以下の画面が表示されます。

■出力レート制限設定

❒ポート:本機のポート番号が表示されます。

※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒制限帯域　出力レート制限の値を入力します。

※ポートの最大速度は、1,000,000Kbps（64Kbps × 15625）です。

❒状態:出力レート制限を有効/無効にします。

❒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。

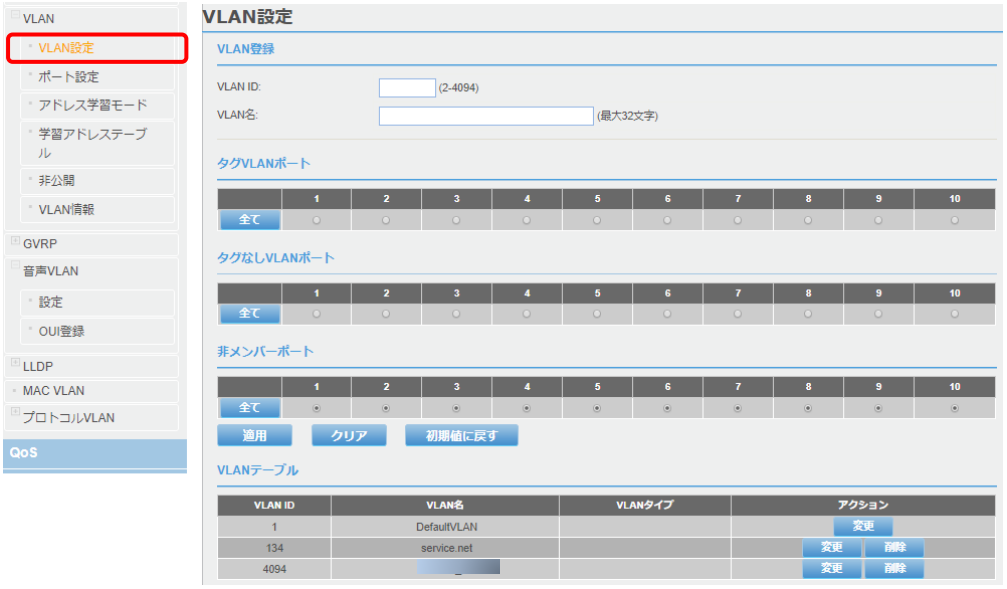
【注記】:無効にすると、設定値が初期値に戻ります

3.3.13 VLAN

1. VLAN 設定

タグ VLAN 機能では、物理的な接続を変更せずにデバイスを新しい VLAN を設定し、1 つの物理ポートに複数の VLAN のパケットを流せるようになります。

「ネットワーク」→「VLAN」→「VLAN 設定」をクリックすると、以下の画面が表示されます



■VLAN 登録

❒VLAN ID:新規 VLAN の VLAN ID を入力します。

❒VLAN 名: VLAN 名を入力します。

■タグ VLAN　ポート

タグ VLAN (Tag VLAN)とは、複数の VLAN を 1 本の LAN 接続だけで複数スイッチ間で共有できる技術です。
ポートでは、フレーム内のタグ情報を受信時に、そのフレームが特定のタグ付き VLAN のメンバーであるかどうかが判別されます。タグ付きの場合は、同じ VLAN の他のメンバーポートに切り替えることができます。フレームのタグがタグ付き VLAN に準拠していないと判断された場合、そのフレームは破棄されます。
また、タグ付き VLAN ポートは、複数の VLAN のメンバーとして設定できます。コンピュータや他のエッジデバイスは、通常、これらのデバイスのネットワークインターフェースが VLAN に対して有効でない限り、タグ付き VLAN ポートに接続されません

■タグなし VLAN　ポート

タグなし VLAN ポートは、VLAN を認識しないエッジデバイス（例:コンピュータ、ラップトップ、プリンタなど）を指定の VLAN に接続するために使用されます。
「ネットワーク」→「VLAN」→「ポート設定」により、タグなし VLAN ポートに応じて、ポートの VID 設定を修正する必要があります（たとえば、VLAN の VID が「2」の場合、PVID も「2」に設定してください。）。
新規 VLAN に追加するタグなしの VLAN ポートを選択してください。

■非メンバーVLAN ポート

VLAN　のメンバーに含めないポートを指定します。

■VLAN テーブル

【注記】:デフォルト VLAN(VLAN ID:1)は削除できません。また、各ポートはそれぞれ少なくとも 1 個の VLAN を割り当てられる必要があります。

・<変更>ボタンをクリックすると、登録されている設定を変更できます。

・<削除>ボタンをクリックすると、ポートがいずれの VLAN にも所属しなくなった場合は自動的にデフォルト VLAN のタグなし VLAN ポートに変更されます

2. ポート設定

ポートごとに、PVID、認可フレームタイプ、入力フィルターの設定を行います。

「ネットワーク」→「VLAN」→「ポート設定」をクリックすると、以下の画面が表示されます。

■ポート設定

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒PVID: ポートの PVID を入力します。

❒認可フレームタイプ:
受信可能なフレームのタイプを選択します。
・全て:すべてのフレームを受信可能です。
・タグあり:タグ付きフレームのみ受信し、タグなしフレームは破棄します。
・タグなし及び優先度タグ付き:タグなしフレーム、および 802.1p などの優先度情報をもつタグ付きフレームのみ受信します。

❒入力フィルター:フレームの処理方法（入力フィルター）の有効/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。

3. アドレス学習モード

ここでは、動的に生成された転送テーブルエントリを持つ VLAN 転送テーブルを表示します。

「ネットワーク」→「VLAN」→「アドレス学習モード」をクリックすると、以下の画面が表示されます。

❒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。

・IVL：IVL 方式とは、VLAN 毎に MAC アドレステーブルを保持する方式です（※推奨設定）。
そのため、機器全体で共通の MAC アドレステーブルを保持する SVL 方式とはスイッチング動作が異なります。

・SVL：SVL 方式とは、機器全体で MAC アドレステーブルを保持する方式です。そのため、VLAN 毎に MAC アドレステーブルを保持する IVL 方式とはスイッチング動作が異なります。
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
【注記】: SVL モードを使用している場合、音声 VLAN はサポートされません。

【注記】:アドレス学習モードを切り替える際は、以下の情報は消去されるため、注意してください。

・FDB（転送データベース）
・スタティックユニキャストアドレスエントリ/スタティックマルチキャストアドレスエントリ
・802.1X 認証レコード
・IGMP スヌーピングマルチキャストグループアドレス

4. 学習アドレステーブル

本機で学習された MAC アドレス、ポート番号、学習アドレステーブルのタイプが表示されます。

「ネットワーク」→「VLAN」→「学習アドレステーブル」をクリックすると、以下の画面が表示されます。

■ポート選択

ポート番号をプルダウンメニューにより選択してください。

■ダイナミック学習テーブル

上記の「ポート選択」メニューで選択したポート情報が表示されます。

❒索引: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。

【注記】:学習モードが「SVL」の場合は「N/A」と表示されます（IVL/SVL の切り替え方法については、前述の「3.アドレス学習モード」を参照してください）。

❒ポート ポート番号が表示されます。

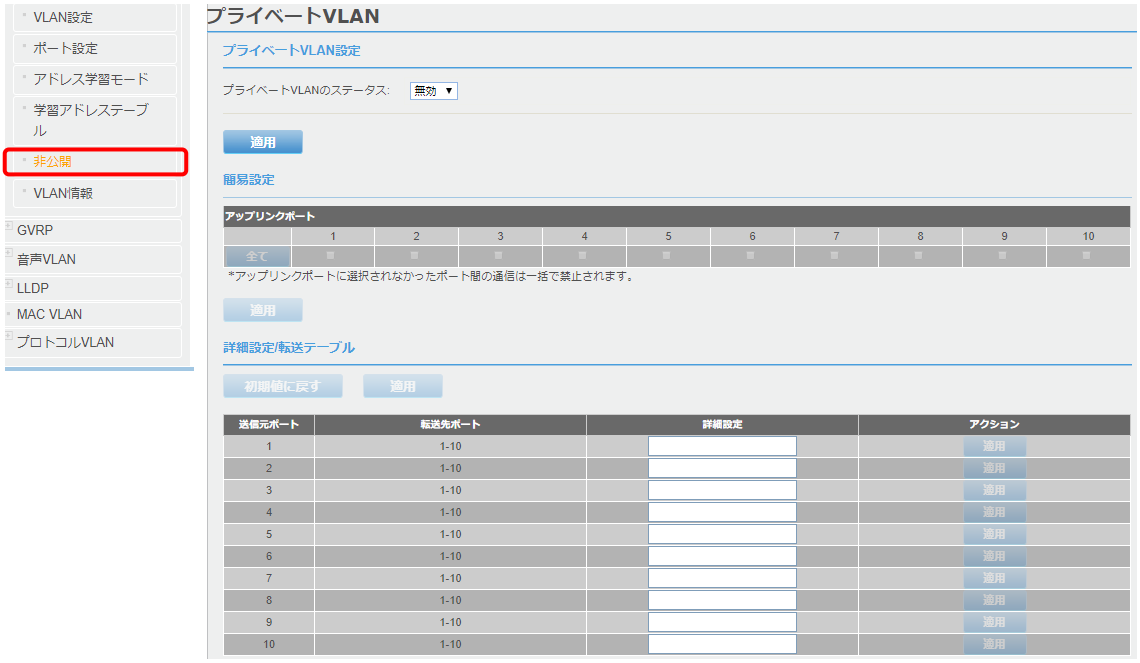
❒MAC アドレス:MAC アドレスが表示されます。

❒タイプ:学習アドレステーブルのタイプが表示されます

5. 非公開

非公開（プライベート）VLAN を設定します。
プライベート VLAN 機能を使用すると、メンバーから完全に分離され、他の VLAN と通信できない、より安全な VLAN を作成できます。プライベート VLAN は、VLAN のレイヤ 2 のブロードキャストドメインをサブドメインに分割して、スイッチ上のポートを互いに隔離できるようにします。

「ネットワーク」→「VLAN」→「非公開」をクリックすると、以下の画面が表示されます



■プライベート VLAN 設定
プライベート VLAN のステータス: プライベート VLAN のステータスを有効/無効にします。

■簡易設定
❒アップリンクポート:アップリンクポートを選択します。
【注記】:アップリンクポートに選択されなかったポート間の通信は一括で禁止されます。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

■詳細設定/転送テーブル
・<初期値に戻す>ボタンをクリックすると、設定されている値はすべてデフォルト値に戻ります
・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

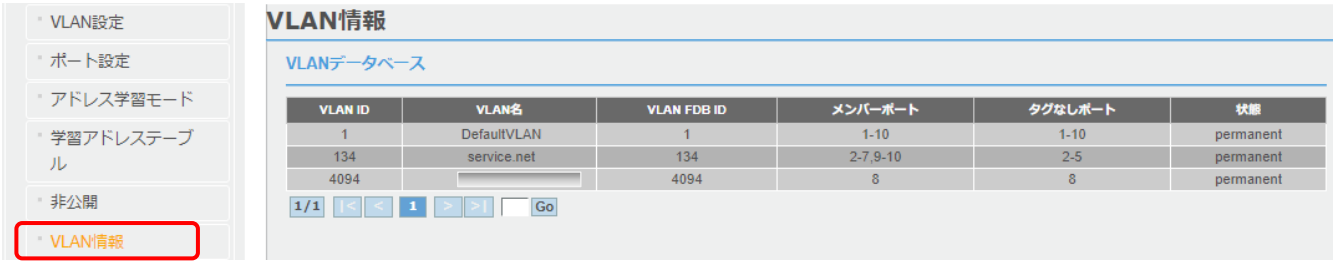
❒送信元ポート:送信元ポート(1～10 ポート)が表示されます。

❒転送先ポート:トラフィックの転送先のポートを選択します。

6. VLAN 情報

登録されている VLAN 情報が表示されます。

「ネットワーク」→「VLAN」→「VLAN 情報」をクリックすると、以下の画面が表示されます



■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に登録されている VLAN ID が表示されます。

【注記】:学習モードが「SVL」の場合は「N/A」と表示されます（IVL/SVL の切り替え方法については、前述の「3. アドレス学習モード」を参照してください）。

❒メンバーポート: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。

3.3.14 GVRP（※非サポート）

GVRP(GARP VLAN 登録プロトコル）を使用すると、ネットワーク機器は VLAN 情報を共有し、その情報を使用して既存の VLAN を変更したり、新しい VLAN を自動的に作成したりすることができます。これにより、複数のスイッチにまたがる VLAN を管理しやすくなります。GVRP を使用しない場合、VLAN のさまざまな部分が異なるスイッチ間で相互に通信できるように、手動で設定する必要があります。

1. 基本設定

「ネットワーク」→「GVRP」→「基本設定」をクリックすると、以下の画面が表示されます。

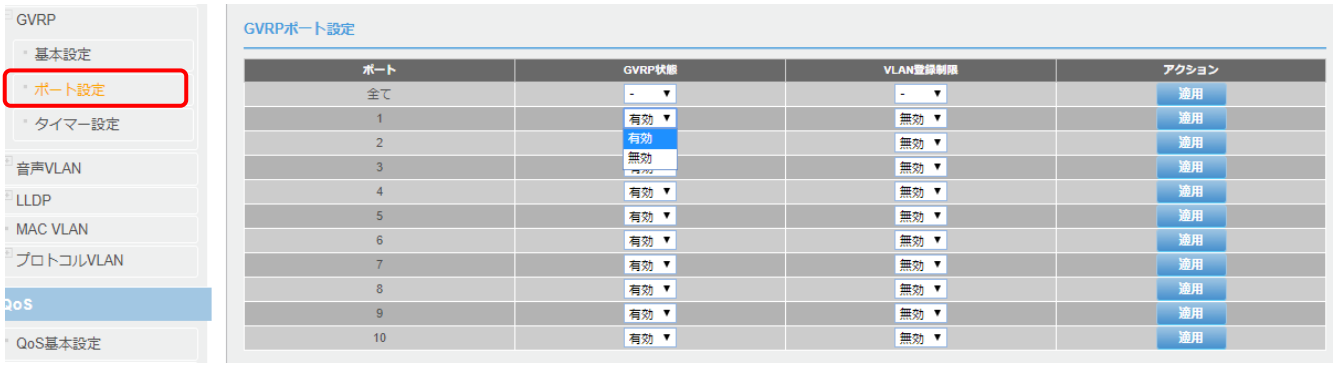
■GVRP 基本設定

❒GVRP 機能を有効/無効にします（デフォルト:無効）。

2. ポート設定

ここでは、どのポートに対して、GVRP を有効にするか、GVRP の使用を制限するかを選択できます。

「ネットワーク」→「GVRP」→「ポート設定」をクリックすると、以下の画面が表示されます。



■GVRP ポート設定

ホールド乗数:ホールドマルチプライヤ値を設定

❒GVRP 状態:ポートの GVRP 状態を有効/無効にします（デフォルト:無効）。

❒VLAN 登録制限:ポートへの VLAN 登録制限を有効/無効にします（デフォルト:無効）。

3. タイマー設定

ここでは、各ポートに対して GARP Join 時間、Leave 時間、および Leave　All 時間を設定します。

「ネットワーク」→「GVRP」→「タイマー設定」をクリックすると、以下の画面が表示されます。

■GVRP タイマー設定

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒Join 時間:GARP Join タイマーです（有効範囲:10 - 1073741810 ミリ秒、デフォルト:200)。

❒Leave 時間:GARP Leave タイマーです（有効範囲:30 - 2147483630 ミリ秒、デフォルト:600)。
このタイマーは、次の式に従って GVRP Join タイマーに基づいて設定する必要があります。
GARPLeave タイマー> =（GARPJoin タイマー　X 2）+ 10

❒Leave-A 時間:GARP Leave-A タイマーです（有効範囲:40 - 2147483630 ミリ秒、デフォルト:10000)。

【注記】:Leave 時間は、Join 時間の 2 倍よりも大きい値に設定する必要があります。また Leave-All 時間には leave 時間より大きい値を設定してください（各設定時間は 10 ミリ秒ごとに調整可能です。）

【注記】:ネットワーク機器間の互換性を確保するには、次の設定が必要です。
ネットワークに参加しているすべての GVRP デバイスに対して、GARP Join 時間、GARP Leave 時間、および GARP Leave-A 時間を同じ値を設定してください。

3.3.15 音声 VLAN

ここでは、スイッチの音声 VLAN 機能、および音声 VLAN 設定を作成、変更、削除する手順について説明します。
音声 VLAN 機能は、スイッチを介して高品質で中断のない音声トラフィックを維持できるように設計されています。
音声 VLAN 機能は次の要件を満たすために設定することができます。

❒音声 VLAN による CoS
音声VLAN CoSパラメータは、スイッチの入力ポートと出力ポート間の音声品質を維持します。音声VLAN CoS優先度を有効にするには、CoSを有効にする必要があります。設定したCoS優先度レベルは、音声VLANのすべてのポートの音声トラフィックに適用します。通常、ほとんどの（音声以外の）イーサネットトラフィックは、低次の出力キューを介してスイッチを通過します。音声データフローの遅延や中断を回避するには、音声VLANに割り当てられているCoS優先度レベルを上位キューにマッピングし、スケジューリングアルゴリズムをStrict優先度に設定する必要があります。これらの設定により、音声データパケットが他のタイプのデータよりも先に処理されるため、音声データがスイッチを通過するときに音声品質が維持されます。

❒組織固有 ID（OUI）

各IP電話の製造元は、1つ以上の組織固有識別子（OUI）によって識別できます。 OUIは3バイト長で、通常は16進形式で表されます。イーサネットネットワーク機器の各MACアドレスの最初の部分に埋め込まれています。 IP電話のOUIは、そのMACアドレスの最初の3バイトにあります。
通常、設置しているすべてのIP電話に同じOUIが共通していることがわかります。スイッチは、パケットの送信元MACアドレスのOUI情報と、最初に音声VLANを設定したときに設定したOUIテーブルを比較して、音声データパケットを識別します。これは、ポートの自動検出機能が動的音声VLANポートの場合に重要です。
音声VLANパラメータを設定するときは、少なくとも1台の音声VLANの完全なMACアドレスを入力する必要があります。製造元のOUIを生成するために、「OUI マスク」がWeb管理ユーティリティソフトウェアによって自動的に生成され適用されます。その製造元の残りの電話機のOUIが同じであれば、他の音声VLANのMACアドレスを設定に入力する必要はありません。
ただし、設置用のIP電話の中に、同じ製造元から複数のOUIがある場合や、IP電話が2つ以上の異なる製造元からのものである場合があります。その場合、製造元ごとに異なるOUIが表示されます。設置するIP電話の中で複数のOUIを識別している場合は、それぞれのOUIを表す1つのMACアドレスを音声VLANに設定する必要があります。合計10個のOUIを入力できます。

❒ダイナミック自動検出ポートとスタティックポート
音声VLANを設定する前に、音声VLAN設定の基礎となるタグ付きVLANを設定する必要があります。
VLANは、音声VLANのアップリンク/ダウンリンクとして機能する1つまたは複数のタグ付きまたはタグなしポートで設定する必要があります。デフォルトでは、タグ付きポートまたはタグなしポートはタグ付きVLANのスタティックメンバーです。動的自動検出ポートとして設定することを選択したポート
IP電話に直接接続する必要があります。音声VLAN設定用にタグ付きVLANのポートを最初に定義する場合は、それらのポートは「Not Member」ポートとして設定する必要があります。「Not Member」ポートは、送信元MACアドレスの定義済みOUIで音声データが検出されたときに音声VLANに動的に加入するのに適格です。
指定のタイムアウト時間が経過すると、ポートは音声VLANを解除します。このポートの設定は、音声VLAN自動検出機能で設定されています。
自動検出が機能するには、IP電話は、埋め込まれたVLAN IDタグを使用して802.1Qパケットを生成する必要があります。スイッチの音声VLAN IDと同じVLAN IDにIP電話を手動で設定する必要があります。「Not Member」ポートの1つで音声データが検出されると、IP電話からのパケットには音声VLAN IDが含まれるため、スイッチの音声VLAN内でスイッチングされます。
音声VLANの1つ以上のポートは、スタティックタグ付きまたはタグなしメンバーとして設定する必要があります。スタティックVLANメンバーは音声VLANの永続的なメンバーポートであり、ポートに接続されているデバイスの設定には依存しません。これらのポートは、他のイーサネットスイッチ、電話交換機、またはDHCPサーバーなどの他の音声VLANネットワークノードに接続されている可能性があります。音声VLAN自動検出機能は、スタティックタグ付きポートまたはタグ付きポートでは有効にできません。

【注記】:メディアエンドポイントデバイスのリンクレイヤディスカバリプロトコル（LLDP-MED）は、スイッチではサポートされていません。VLAN に対応している各音声 VLAN は、音声 VLAN ID と一致する VLAN ID に対して手動で設定する必要があります。 音声 VLAN に接続されている各音声 VLAN ポートは、タグ付き VLAN の「Not Member」ポートとして設定する必要があります。

1. 設定

【注記】:音声 VLAN を設定する前に、まずタグ付き VLAN を設定する必要があります。この VLAN は、音声 VLAN ベースで使用されます。

「ネットワーク」→「音声 VLAN」→「設定」をクリックすると、以下の画面が表示されます。

■音声 VLAN

❒音声 VLAN 機能：音声 VLAN 機能を有効/無効にします（デフォルト：無効）。
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(学習モードの設定については、「アドレス学習モード」を参照ください)。

【注記】:この機能を無効にすると、設定値が初期値に戻ります。

■音声 VLAN 設定

❒VLAN ID:「VLAN 設定」にて設定されているタグ付き VLAN ID です。音声 VLAN を有効にすると、VLAN ID は、プルダウンメニューより選択できます(デフォルト設定:1)。

【注記】: VLAN ID を音声 VLAN に指定する場合は、事前に設定する必要があります（VLAN ID の設定については、「VLAN 設定」を参照ください）。

❒エージング時間:音声 VLAN の OUI がポートで受信されてからの経過時間を時間単位で示します。
指定時間を経過すると、ポートは音声 VLAN から削除されます（有効範囲:1～120、デフォルト設定:1）。

❒CoS 値:各音声 VLAN ポートで受信された音声データパケットに割り当てられた CoS の優先順位レベルです（有効範囲:1-7、デフォルト値：7）。
【注記】:COS 優先度を有効にするには、QoS を有効にする必要があります（設定方法については、「QoS」??を参照ください）。

上記設定を完了後、<適用>ボタンをクリックすると、次の表に値が反映されます。

■音声 VLAN テーブル

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒自動検知:音声 VLAN の自動検出を有効/無効にします。

❒状態:　自動検知ポートの状態（なし/スタティック/ダイナミック）を表示します。

2. OUI 登録

音声 VLAN の OUI(Organization Unique Identifier)を設定方法について説明します。

「ネットワーク」→「音声 VLAN」→「OUI 登録」をクリックすると、以下の画面が表示されます。

■OUI 登録

❒ユーザー定義 OUI:「説明」フィールドに、製造元の OUI を識別するための説明を入力します（このパラメータの長さは「20 文字以内」）。

【注記】:ユーザー定義 OUI は最大 10 個まで登録可能です。

❒OUI:製造元の OUI を含む、音声 VLAN の MAC アドレスを入力します。

・<追加>ボタンをクリックすると、新しい OUI エントリが画面下の表に追加されます。

【注記】:設定する IP 電話に複数の OUI がある場合は、それぞれの OUI を表す MAC アドレスを 1 つ入力します（最大「10 個」まで OUI を入力可能）。

【注記】:この手順を実行すると、すべての設定変更が保存されるため、本機を再起動したり電源を入れ直した場合でも、設定の変更内容は適用されます。

■音声 VLAN OUI テーブル

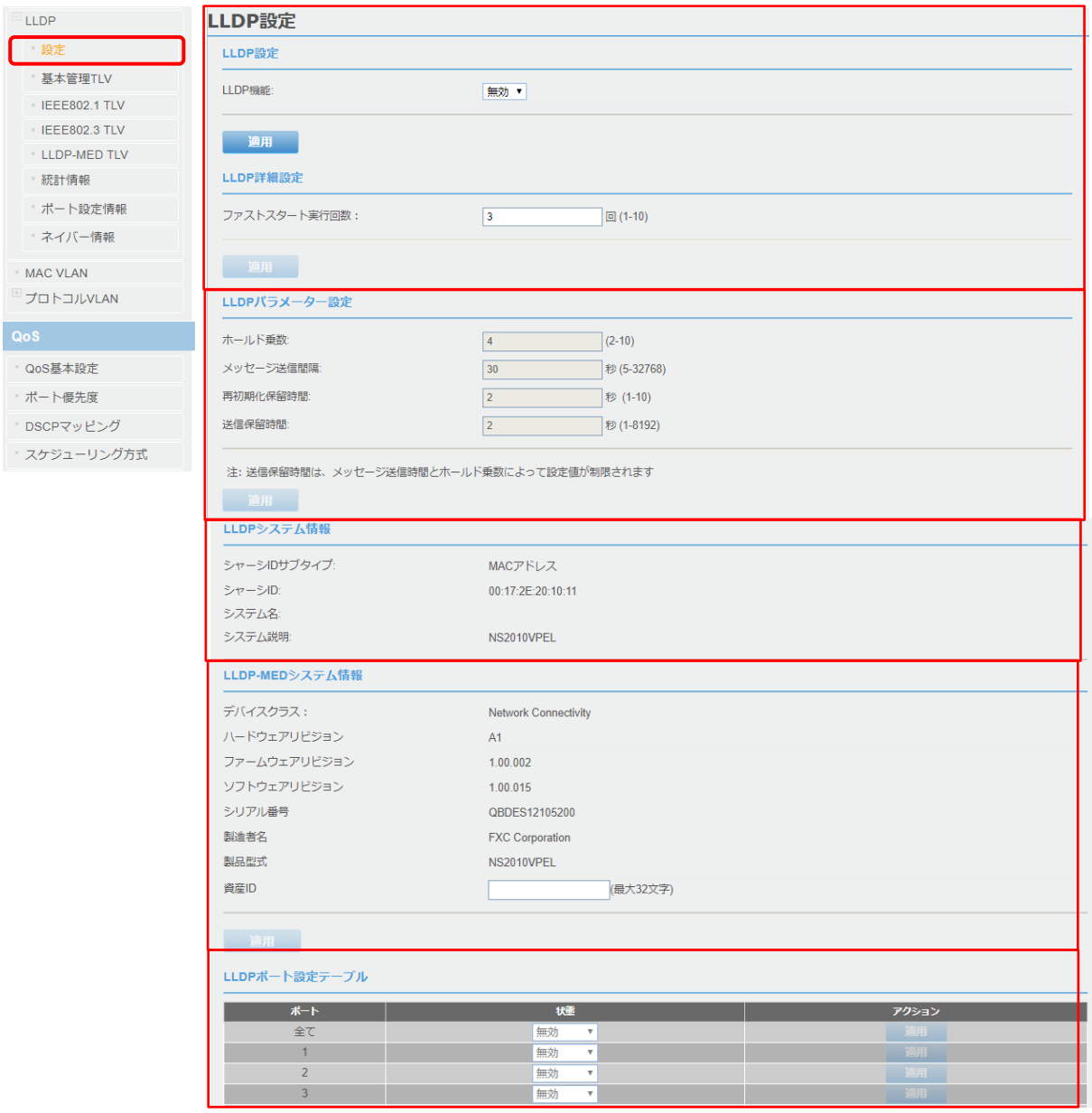
上記設定を完了後、<追記>ボタンをクリックすると、表に値が反映されます。

3.3.16 LLDP

LLDP (Link Layer Discovery Protocol)を使用すると、スイッチやルータなどのイーサネットネットワーク機器は、ネットワーク上で隣接する機器（ネイバー）との間で関連の情報を送受信し、ネイバー情報について学習したデータを保存できます。

1. 設定

「ネットワーク」→「LLDP」→「設定」をクリックすると、以下の画面が表示されます。



■LLDP 設定

❒LLDP 機能:LLDP 機能を有効/無効にします。

■LLDP詳細設定

❒ファストスタート実行回数：ファストスタートの実行回数を表示します（デフォルト値:3）。

■LLDP パラメーター設定

❒ホールド乗数:ホールドマルチプライヤ値を設定します。スイッチがネイバーにアドバタイズする TTooLs(Time To Live）を得るために、ホールドタイムの乗数に送信間隔を掛けます（有効範囲: 2～10、デフォルト値: 4）。

❒メッセージ送信間隔:送信間隔を設定します。これは、LLDP アドバタイズメントの通常の送信間隔です（有効範囲: 5～32768 秒、デフォルト値：30）。

❒再初期化保留時間:再初期化保留時間を設定します。これは、ポートで LLDP が無効になってから再初期化されるまでの秒数です(有効範囲:1～10 秒、デフォルト値:2)

❒送信保留時間:送信保留時間の値を設定します。これは、LLDP ローカル情報の変更に伴う LLDP アドバタイズメントの送信間の最小時間間隔です（有効範囲:1～8192 秒、デフォルト値:2）。

【注記】:送信保留時間は、メッセージ送信時間とホールド乗数によって設定値が制限されています。

■LLDP システム情報

❒シャーシIDサブシステム:「macAddress」であるシャーシ ID のサブタイプを記述します変更できません

❒シャーシ ID:スイッチの MAC アドレスをリストします（変更不可）。

❒システム名:スイッチのシステム名をリストします（変更不可）。

❒システム説明:スイッチの製品名が一覧表示されます。

■LLDP-MED システム情報

LLDP-MED システム情報（デバイスクラス，ハードウェアリビジョン，ファームウェアリビジョン,ソフトウェアリビジョン，シリアル番号，製造者名，製品型式，資産 ID）が表示されます。

■LLDP ポート設定テーブル

❒ポート:本機のポート番号が表示されます。

※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒状態:LLDP ポートの状態が表示されます。

各ポートで、ドロップダウンリストをクリックして、次のオプションから選択します。

・無効:LLDP は無効であることを表示します。ポートは LLDP データパケットを送受信できません。

・送受信:LLDP は有効、かつ LLDP データパケットの送受信ともに可能です。

・受信のみ:LLDP は有効ですが、LLDP データパケットの受信のみ可能です。

・送信のみ:LLDP は有効ですが、LLDP データパケットの送信のみ可能です。

❒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。

2. 基本管理 TLV

LLDP は、隣接機器（ネイバー）の検出に際して、“TLV”と呼ばれるタイプ（Type）、長さ（Length）、値（Value）の属性を使用してネイバーから情報を認識することができます。
本メニューでは、基本管理の通知設定を行います。

「ネットワーク」→「LLDP」→「基本設定 TLV」をクリックすると、以下の画面が表示されます。

■基本管理 TLV 設定テーブル
それぞれ、ポートごとに有効/無効を選択します。

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒ポート説明: ポート説明に関する通知を有効/無効にします（デフォルト:有効）。

❒システム名: システム名に関する通知を有効/無効にします（デフォルト:有効）。

❒システム説明:システム説明に関する通知を有効/無効にします（デフォルト:有効）。

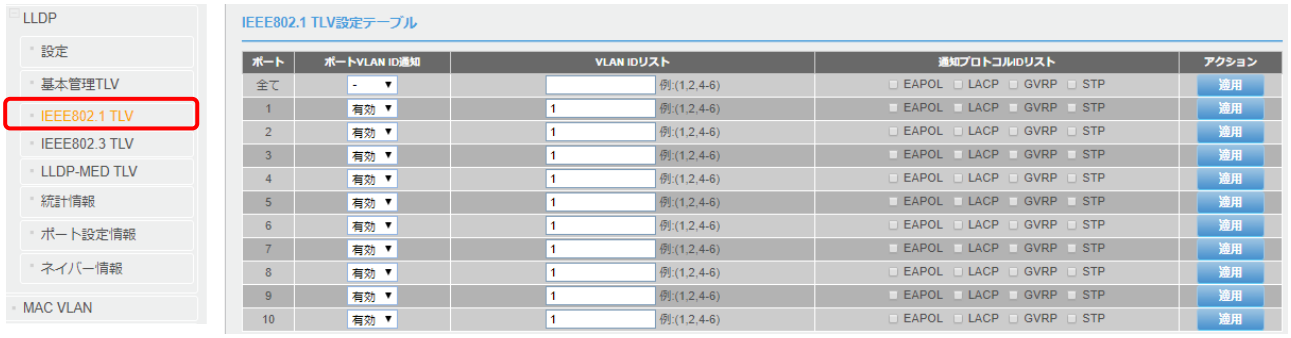
❒システム機能: システム名に関する通知を有効/無効にします（デフォルト:有効）。

❒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。

3. IEEE802.1 TLV の設定

LLDP は、隣接機器の検出に際して IEEE802.1 の TLV（タイプ（Type）、長さ（Length）、値（Value））の属性を使用してネイバーから情報を認識することができます。
本メニューでは、IEEE802.1 TLV の通知設定を行います。

「ネットワーク」→「LLDP」→「IEEE802.1 TLV」をクリックすると、以下の画面が表示されます。



■IEEE802.1 TLV 設定テーブル

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒ポート VLAN　ID 通知:　ポート VLAN ID の通知を有効/無効にします（デフォルト:有効）。

❒VLAN ID リスト:　通知する VLAN ID　が表示されます。

❒通知プロトコル ID リスト:
各プロトコル（EAPOL, LACP, GVRP,STP）のいずれかより選択してください。

❒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。

4. IEEE802.3 TLV の設定

LLDP は、隣接機器の検出に際して IEEE802.3 の TLV（タイプ（Type）、長さ（Length）、値（Value））の属性を使用してネイバーから情報を認識することができます。
本メニューでは、IEEE802.3 TLV の通知設定を行います。

「ネットワーク」→「LLDP」→「IEEE802.3 TLV の設定」をクリックすると、以下の画面が表示されます。

■IEEE802.3 TLV 設定テーブル

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒MAC/PHY 設定状態通知: MAC/PHY 設定状態通知を有効/無効にします（デフォルト設定：有効）。

❒リンクアグリゲーション通知: リンクアグリゲーション通知を有効/無効にします（デフォルト設定：有効）。

❒最大フレームサイズ通知: 最大フレームサイズ通知を有効/無効にします（デフォルト設定：有効）。

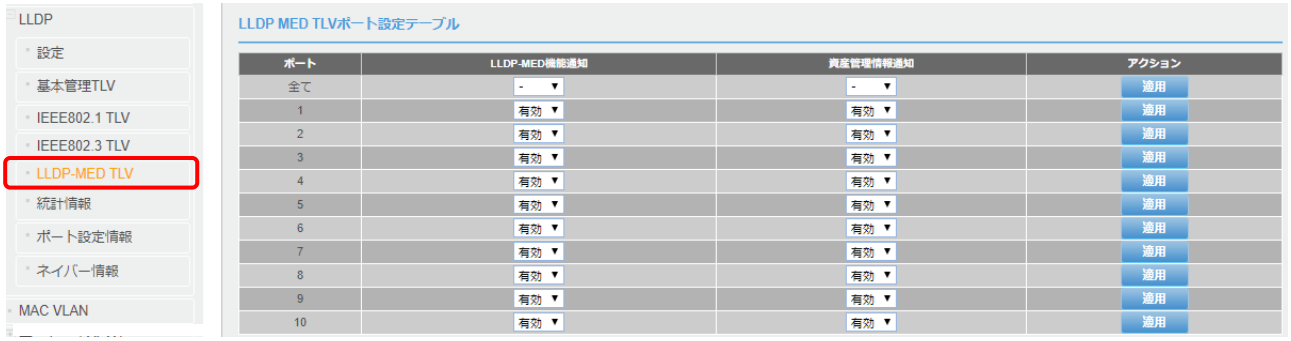
❒PoE 状態通知: PoE 状態通知を行います（デフォルト設定：無効）。

❒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。

5. LLDP-MED TLV の設定

LLDP-MED（LLDP for Media Endpoint Devices）は LLDP の拡張版であり、IP 電話などのエンドポイントデバイスとネットワークデバイス間で動作します。
本メニューでは、各ポートごとに、LLDP-MED 機能通知/資産管理情報通知を有効/無効にします。

「ネットワーク」→「LLDP」→「LLDP MED TLV の設定」をクリックすると、以下の画面が表示されます。



■IEEE802.1 TLV 設定テーブル

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒ LLDP-MED 機能通知: LLDP-MED 機能の通知を有効/無効にします（デフォルト:有効）。

❒資産管理情報通知: 通知する VLAN ID が表示されます。

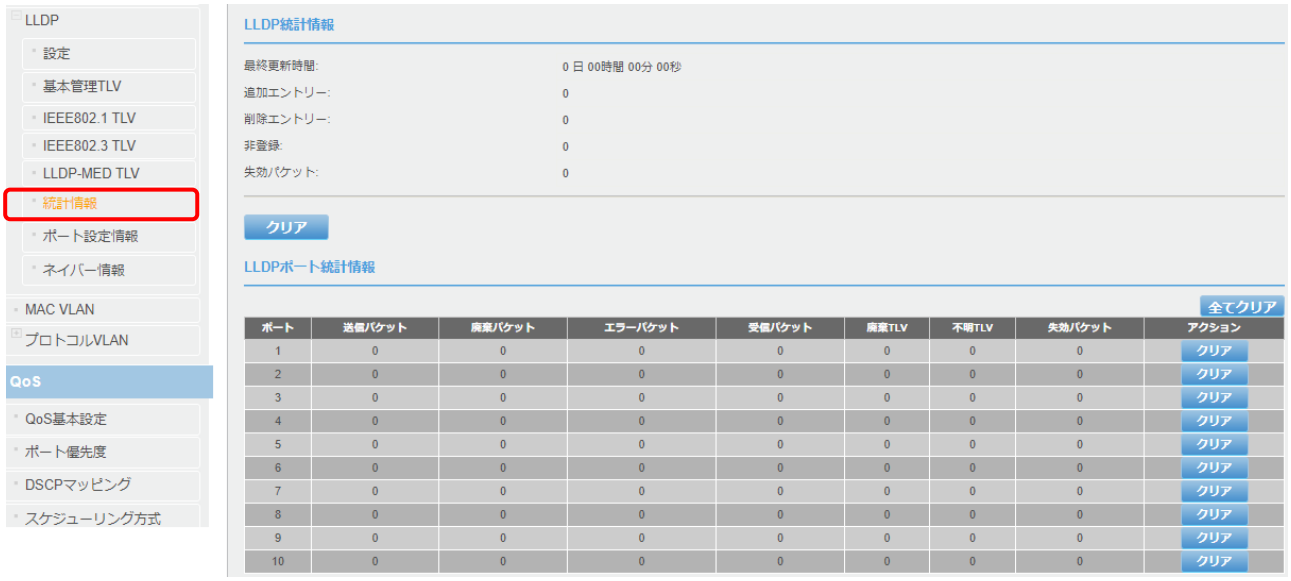
❒通知プロトコル ID リスト:
各プロトコル（EAPOL, LACP, GVRP,STP）のいずれかより選択してください。

❒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。

6. 統計情報

LLDP トラフィックの統計情報を表示します。

「ネットワーク」→「LLDP」→「統計情報」をクリックすると、以下の画面が表示されます。



■LLDP 統計情報

❒最終更新時間:最新のエントリの更新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数が表示されます。

❒非登録:登録されなかったエントリー数が表示されます。

❒失効パケット: 失効により削除されたパケット数が表示されます。

・<クリア>ボタンをクリックすると、上記の統計情報がクリアされます。

■LLDP ポート統計情報

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒送信パケット:ポートから送信した LLDP パケット数が表示されます。

❒廃棄パケット:受信した LLDP パケットのうち、廃棄された LLDP パケット数が表示されます。

❒エラーパケット:受信した LLDP パケットのうち、エラーパケット数が表示されます。

❒受信パケット:受信した LLDP パケット数が表示されます。

❒廃棄 TLV: LLDP パケットで通知された TLV 情報のうち、不正なフォーマットにより廃棄された TLV の数が表示されます。

❒不明 TLV:LLDP パケットで通知された TLV 情報のうち、不明な値の TLV の数が表示されます。

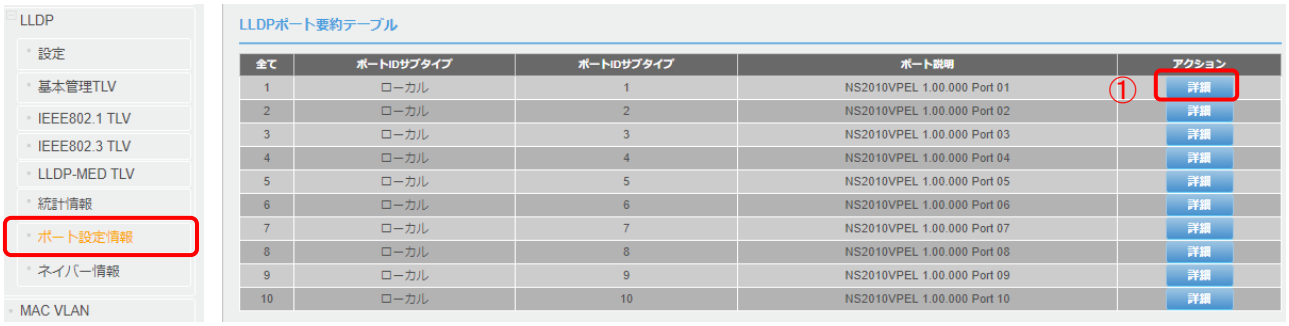
❒失効パケット:有効期限内に新しい LLDP パケットを受信しない場合、削除された LLDP パケット数が表示されます。

❒アクション ［クリア］ボタンをクリックすると、ポートの統計情報がクリアされます。

7. ポート設定情報

LLDP ポートの設定情報を表示します。

「ネットワーク」→「LLDP」→「ポート設定情報」をクリックすると、以下の画面が表示されます。



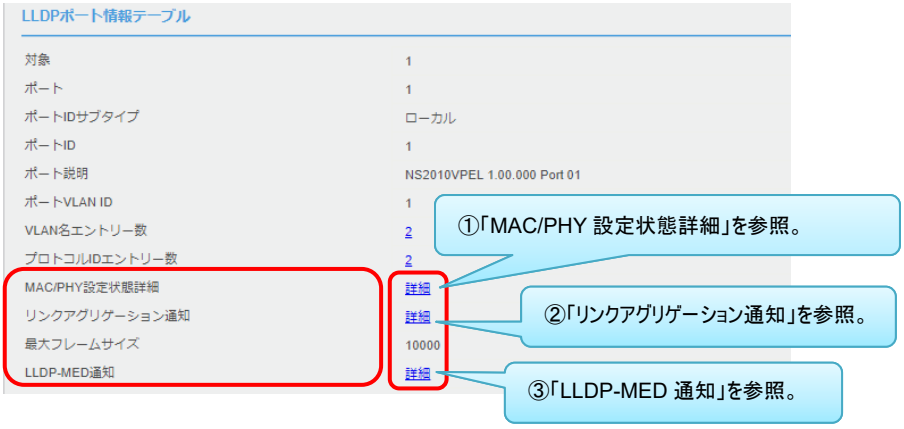
■LLDP ポート要約テーブル

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

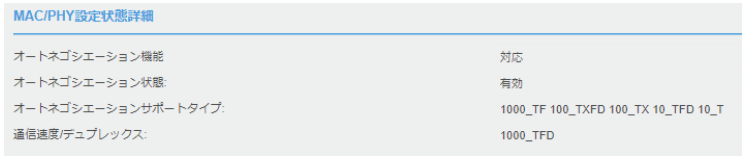
❒ポート ID サブタイプ: 通知するポート ID サブタイプが表示されます。

❒ポート説明: 通知するポート情報が表示されます。

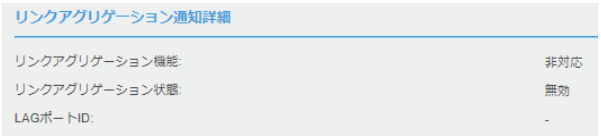
❒アクション: 詳細 ボタンをクリックすると、次のとおりポートごとに LLDP ポート設定情報が表示されます。



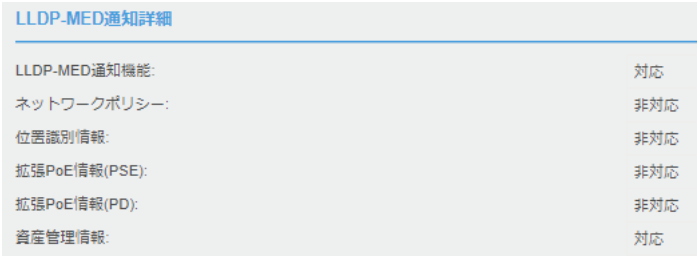
①MAC/PHY 設定状態詳細



②リンクアグリゲーション通知



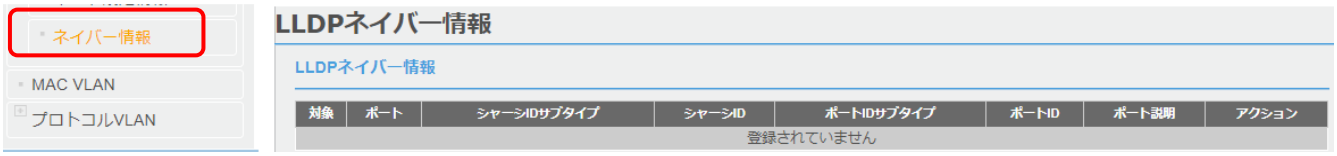
③LLDP-MED 通知



7. ネイバー情報

LLDP によるネイバー情報を表示します。

「ネットワーク」→「LLDP」→「ネイバー情報」をクリックすると、以下の画面が表示されます。



■LLDP ネイバー情報

❒対象:LLDP 情報を受信した順に、対象のネイバーに割り当てられた番号が表示されます。

❒ポート:LLDP 情報を受信した本機のポート番号が表示されます。

❒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。

❒ポート説明:ネイバーのポート情報が表示されます。

3.3.17 MAC VLAN（※非サポート）

MAC ベース VLAN は、送信元の MAC アドレス単位に VLAN のグループ分けを行います。

「ネットワーク」→「MAC VLAN」をクリックすると、以下の画面が表示されます。

■MAC VLAN 新規作成

❒MAC アドレス: VLAN に割り当てる MAC アドレスを入力します。
❒説明: MAC アドレスについて記述します（8 文字以下）。
❒VLAN ID: MAC アドレスを割り当てる VLAN ID を入力します（有効範囲:1-4094）。

・<追加>ボタンをクリックすると、次の表に反映されます。

■MAC VLAN テーブル

❒MAC アドレス:VLAN に割り当てられた MAC アドレスが表示されます。
❒説明: MAC アドレスの記述が表示されます。
❒VLAN ID:MAC アドレスが割り当てられた VLAN ID が表示されます。

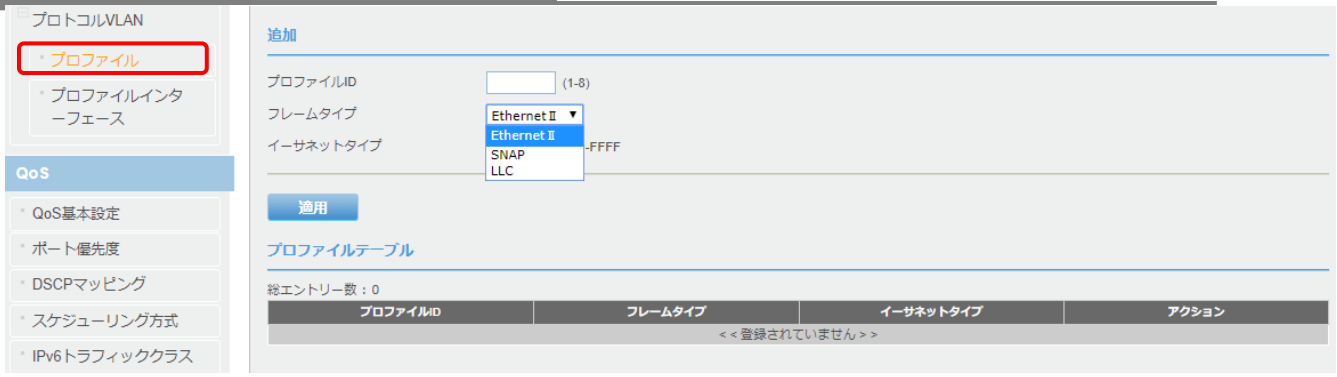
3.3.18 プロトコル VLAN（※非サポート）

複数のプロトコルをサポートしているネットワークデバイスでは、容易に共通の VLAN をグループ化することはできません。そのため特定のプロトコルをもつすべてのデバイスを取り込むために別々の VLAN 間でトラフィックを送信するために非標準デバイスが必要になる場合があります。このような設定の場合、セキュリティやアクセスの容易性といったユーザーにとって VLAN の基本的なメリットが損なわれます。これらの問題を回避するため、プロトコルベースの VLAN を使用することにより、物理ネットワークに必要なプロトコルに応じて論理 VLAN グループに分割することが可能です。ポートでフレームを受信すると、受信パケットで使用されているプロトコルタイプに応じて、フレームがどの VLAN に属しているかを判別することができます。

1. プロファイル

対象のプロトコルを選択します。

「ネットワーク」→「プロトコル VLAN」→「プロファイル」をクリックすると、以下の画面が表示されます。



■追加

❒プロファイル ID:プロファイル ID を入力します（有効範囲:1-8）。

❒フレームタイプ: フレームタイプをドラッグメニューより「Ethernet Ⅱ」、「SNAP」、「LLCP」のいずれかから選択します（デフォルト値：Ethernet Ⅱ）。

❒イーサネットタイプ:イーサネットタイプを入力します（有効範囲：0000-FFFF）。

・<適用>ボタンをクリックすると、 上記の設定したエントリが反映されます。

■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。

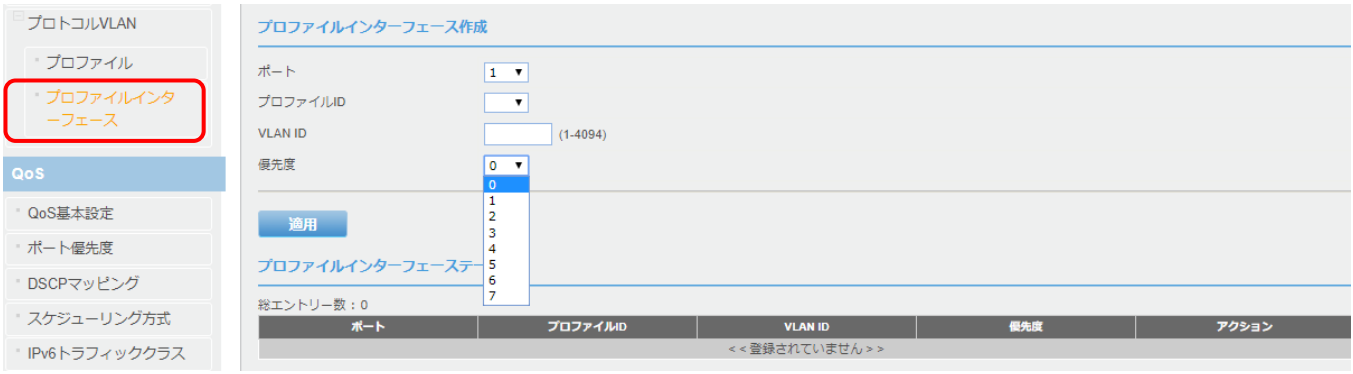
❒フレームタイプ:プロトコル VLAN のフレームタイプが表示されます。

❒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。

2. プロファイルインターフェース

ポートごとに、プロファイル ID、VLAN ID、優先度を割り当てます。

「ネットワーク」→「プロトコル VLAN」→「プロファイルインターフェース」をクリックすると、以下の画面が表示されます。



■プロファイルインターフェース作成

❒ポート：プルダウンメニューにより、設定するポート番号を選択します（有効範囲:1～10、デフォルト:1）

❒プロファイル ID: プロファイル ID を入力します。

❒VLAN ID: VLAN ID を入力します（有効範囲:1～4094）。

❒優先度:優先度を入力します（有効範囲:0～7、デフォルト:0）

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

■プロファイルインターフェーステーブル

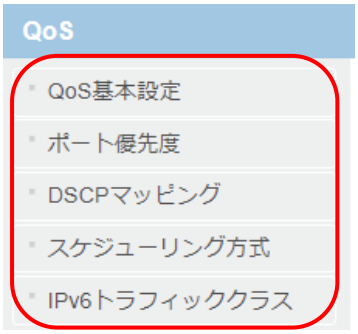
上記設定を完了後、表に値が反映されます。

3.4 QoS

本章では、QoS 機能の設定方法について説明します。
QoS を実装することで、ある特定の通信を優先して伝送させたり、帯域幅を確保することができます。

遅延に対して敏感な特定のトラフィック（例えば、音声伝送およびビデオ会議などのパケット遅延の影響を受ける可能性のあるもの）を他のパケットよりも高い優先順位を設定することで、スイッチを通過するトラフィックフローを管理できます。これは“トラフィックの優先順位付け”といいます。

本メニューは、以下の機能により構成されます。



3.4.1 QoS 基本設定

ここでは、CoS 優先度を設定します。

【注記】:CoS 優先度と出力キューをマッピングするには、各ポートのジャンボフレームパラメータを無効にする必要があります。
ジャンボフレームが有効になっていると、COS を有効にできません。

「QoS」→「QoS 基本設定」をクリックすると、以下の画面が表示されます。

■QoS 基本設定
❒QoS 機能 QoS 機能を有効/無効にします。
・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

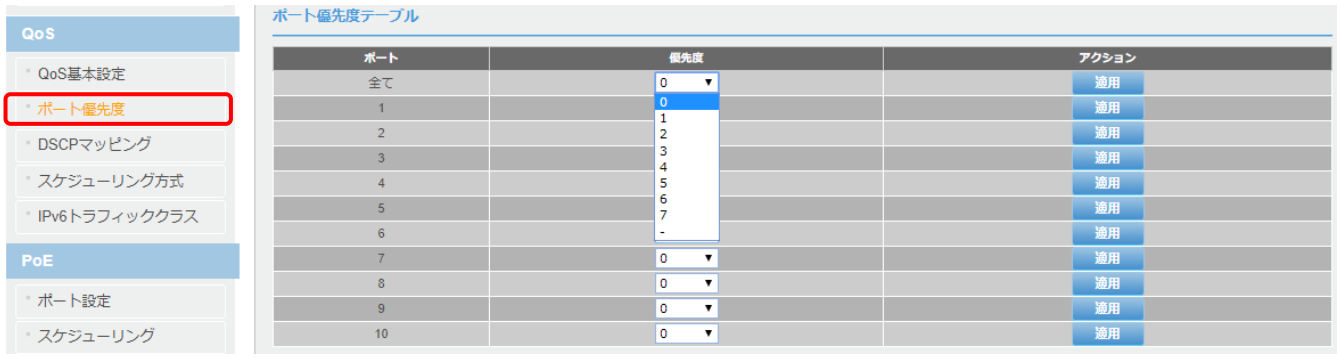
■優先度テーブル
❒優先度: QoS の優先度が表示されます。
❒キューID:ネットワーク環境に基づいて、優先度とキューID を手動にて設定してください。

【注記】:QoS 機能を無効にすると、キューIDの設定が初期値に戻ります。

3.4.2 ポート優先度

ポート優先度は、スイッチの内部処理のために入力時にタグなしフレームに割り当てられる値です。
ここでは、デフォルト時にポート優先度のマッピングをユーザーの優先度に変換します。

「QoS」→「ポート優先度」をクリックすると、以下の画面が表示されます。



■ポート優先度テーブル

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

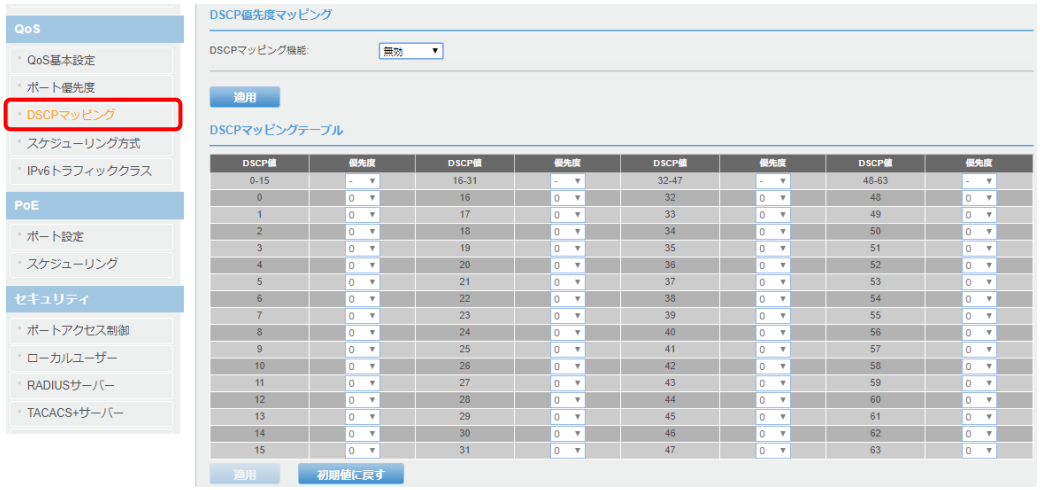
❒ポート優先度
各ポートの QoS 優先度を設定します（有効範囲:0～7）。

❒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。

3.4.3 DSCP マッピング

パケットの DSCP（Differentiated Services Code Point）クラスのマッピングを設定します。

「QoS」→「DSCP マッピング」をクリックすると、以下の画面が表示されます。



■DSCP マッピング機能: DSCP マッピング機能を有効/無効にします。

■DSCP マッピングテーブル

❒DSCP 値: DSCP　値が表示されます（有効範囲:0～63）。

❒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。
画面最上部に DSCP 値の範囲（0-15、16-31、32-47、48-63）が表示されています。
それぞれの範囲ごとに優先度（0～7）を適用することができます。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。
・<初期値に戻す>ボタンをクリックすると、設定されている値はすべてデフォルト値に戻ります。

3.4.4 スケジューリング方式

スケジューリング方式を設定する方法について説明します。

「QoS」→「スケジューリングアルゴリズム」をクリックすると、以下の画面が表示されます。

■スケジューリングアルゴリズム

❒絶対優先方式:ポートは、優先順位の低いキューを送信する前に、優先順位の高いキューからすべてのパケットを送信します。

❒重み付きラウンドロビン（Weighted Round Robin）:各キューからあらかじめ設定された一定数のパケットを重み付けで割り振ると、それぞれがトラフィックを送信することができます。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

3.4.5 IPv6 トラフィッククラス

IPv6 パケットのトラフィッククラスベースの優先度を割り当てます。

「QoS」→「IPv6 トラフィッククラス」をクリックすると、以下の画面が表示されます。

■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を有効/無効に設定します。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

■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 クラスの値を指定します(有効範囲:0-255)。

❒キューID: ポートに割り当てる優先順位を定義します(有効範囲:0-7)。

・<追加>ボタンをクリックすると、トラフィッククラス設定エントリをテーブルに追加します。

■IPv6 トラフィッククラスマッピングテーブル

上記設定を完了後、表にリスト表示されます。

・<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すべてのエントリーが削除されます。

3.5 PoE

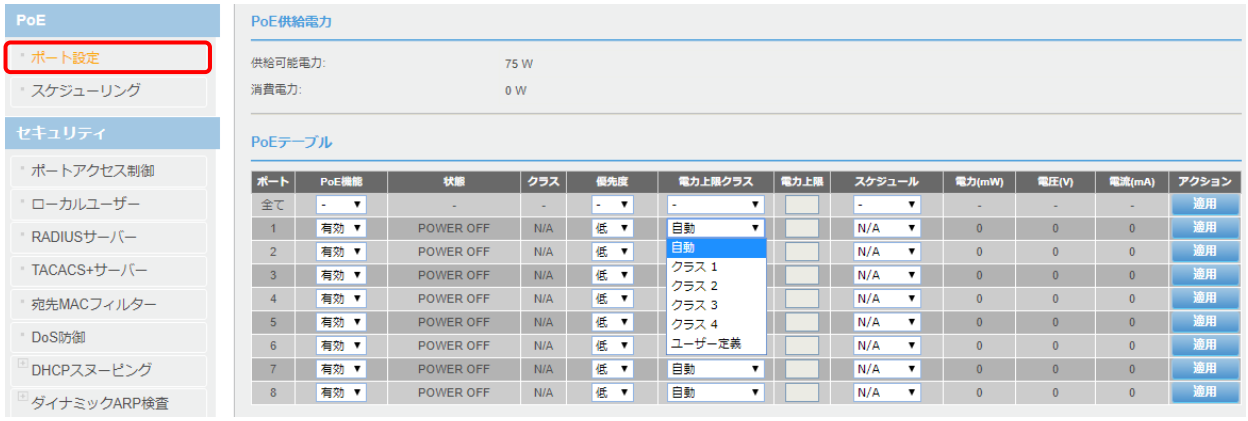
本メニューでは、PoE の設定方法について説明します。
ネットワーク装置の導入する上で配線する電源の場所によって制限される場合があります。
PoE を使用することにより、電源の場所を気にせずに、必要な場所に PoE 互換デバイスを設置することで、ネットワークを容易に設置することができます。
本製品は、ネットワークケーブルに DC 電力を供給し、他のネットワーク機器に対して電源として機能する PSE デバイスです。

本機能は、以下のメニューにより構成されています。

3.5.1 ポート設定

ここでは、PoE のポート設定について説明します。

「PoE」→「ポート設定」をクリックすると、以下の画面が表示されます。



■PoE 供給電力
❒供給可能電力:最大 PoE パワーバジェットをワットで表示します。
❒消費電力: PoE デバイスまたは PD（受電装置）に供給されている現在の PoE 電力をワット単位で表示します（デフォルト:0）。

■PoE テーブル
❒ポート:特定の PoE ステータスを持つポート番号を表示します。
【注記】: 設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒PoE 機能:特定のポートで PoE を有効/無効にします（デフォルト:無効）。

❒状態: PoE ポートのステータスは次のようになります。
・Power ON:PoE 電力が供給されています。
・Power OFF:PoE 電力は供給されていません。

❒クラス: PoE クラスは PD のクラスを表示します。ポートが電力を供給していない場合は、“N/A”と表示されます。

❒優先度:ポートの優先順位（高、中、低のいずれか）を表示します（デフォルト:低）。

優先度	説明
高	最上位の優先順位です。このレベルに設定されたポートは、他の優先度レベルに割り当てられたポートよりも先に電力を供給されます。
中	このレベルに設定されたポートは、高レベルに割り当てられたすべてのポートに対してすでに電力が供給されている場合にのみ受電可能です。
低	最下位の優先順位です。 このレベルに設定されたポートは、高レベルおよび中レベルに割り当てられたすべてのポートに対してすでに電力が供給されている場合にのみ受電可能です（デフォルト設定）。

❒電力上限クラス:クラス別の電力制限またはユーザーが定義した電力の上限を表示します（「自動」、「クラス1-4」、「ユーザー定義」、デフォルト設定：自動）。

❒電力上限:特定のポートの最大電力消費量を定義できます。
【注記】:ユーザー定義の電力制限は「1.0～30.0 ワット」です。

❒スケジュール:定義済みの PoE TimeRange を選択してください。時間範囲が設定されていない場合は、“N/A”と表示されます。

❒電力（mW）:PD に電力供給時の電力（mW）を表示します。

❒電圧（V）:PD に電力供給時のポートで測定される電圧(V)を表示します。

❒電流（mA）: PD に供給している電流（mA）を表示します。

❒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。

3.5.2 スケジューリング

新しい PoE のタイムレンジを設定します。

「PoE」→「スケジューリング」をクリックすると、以下の画面が表示されます。

■給電停止スケジュール

❒スケジュール名:新しい PoE のスケジュール名を入力します（32 文字以内）。

※毎日:「開始/終了曜日」がグレー表示され、開始/終了時間のみ指定可能となります。

❒開始曜日: PoE 給電の開始曜日を設定します。

❒開始時間（HH:MM）:PoE 給電の開始時間を設定します。

❒終了曜日:PoE 給電の終了曜日を設定します。

❒終了時間（HH:MM）:PoE 給電の終了時間を設定します。

・<適用>ボタンをクリックすると、上記の設定したエントリが反映されます。

【注記】:システム時間が PoE ポートに接続された時間範囲に達すると、PoE は無効になります。

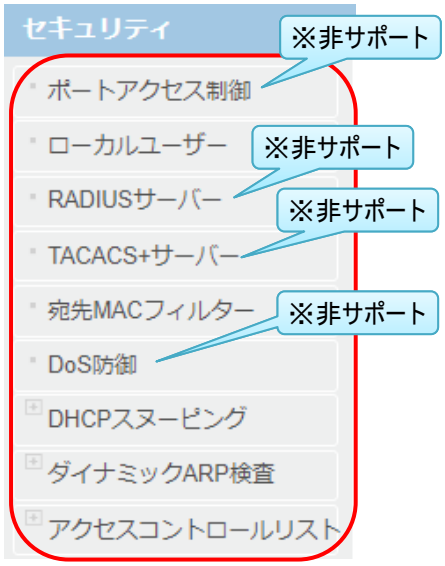
■PoE スケジューリングテーブル

上記設定を完了すると、表に値が反映されます。

3.6 セキュリティ（※一部非サポートあり）

ここでは、ポートベースのセキュリティ機能とその設定手順について説明します。

本機能は、以下のメニューにより構成されています。



3.6.1 ポートアクセス制御（※非サポート）

ポートベースのアクセス制御（IEEE 802.1x）は、スイッチポートを介してトラフィックの送受信可能なユーザーを制御することができます。この機能を使用すると、ユーザー名とパスワードを入力してログオンするまで、ポート経由でトラフィックを送受信できないようになります。
この機能により、ユーザー名とパスワードを割り当てたユーザーのみ、ネットワークへのアクセスが可能となるため、許可されていないユーザーによるコンピュータへのアクセスや、または無人のワークステーション経由のネットワークリソースへのアクセスを防ぐことができます。

この機能は、以下の 2 つの認証方法のいずれかで設定可能です。

❒ RADIUS 認証プロトコル:
ネットワーク上にリモート RADIUS サーバーが存在している必要があります。
RADIUS サーバーは、ユーザー名とパスワードの組みを介して認証を行います。

❒ ローカルユーザー（ローカル）認証:
外部サーバーなしでスイッチの内部で認証パラメータを設定できます。この場合、ユーザー名とパスワードの組み合わせは、
オプションの VLAN に関連付けられています。認証プロセスはこれらのエントリに基づいて標準の EAPOL（EAP over LAN）処理を介して Web 管理ユーティリティによってローカルで行われます。

【注記】:EAP(Extensible Authentication Protocol)を用いた RADIUS は、この機能でサポートされている唯一の認証サーバーです。

「セキュリティ」→「ポートアクセス制御」をクリックすると、以下の画面が表示されます。

■ポートアクセス制御

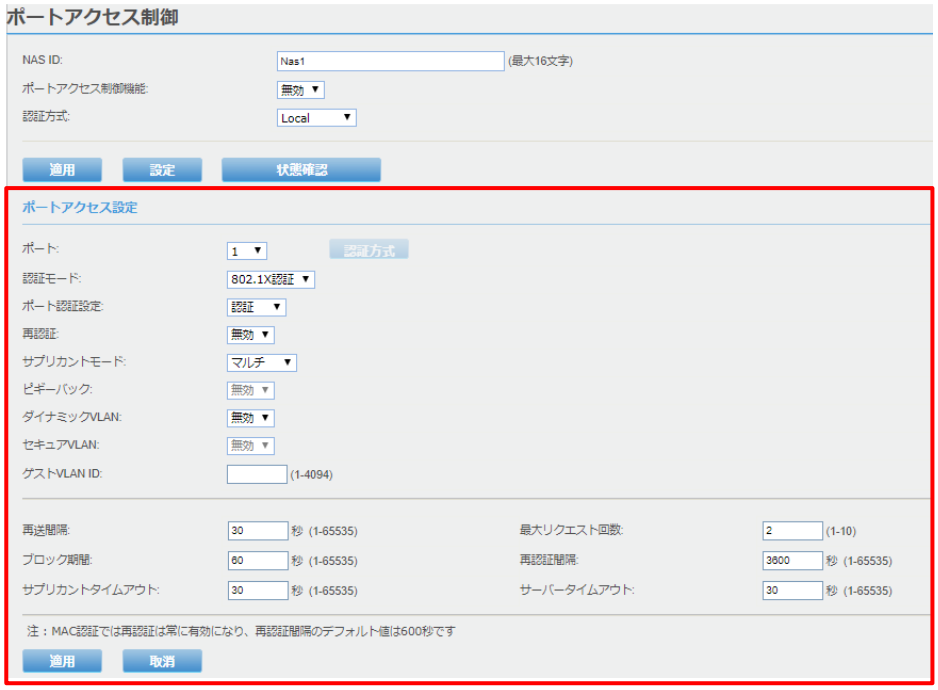
❒NAS ID:すべてのポートに適用されるスイッチに 802.1x 識別子を割り当てます（16 文字以内の英数字（大文字/小文字区別あり）でスペース使用可）。
※NAS ID の指定はオプションです。

❒ポートアクセス制御:ポートアクセス制御を有効/無効にします。

❒認証方式:スイッチで使用される認証方法を表示します。
次のいずれかを選択してください。
・RADIUS:リモート認証用のポートセキュリティを設定します。
・TACACS+:端末認証用のポートセキュリティを設定します。
・Local:ローカル認証用のポートセキュリティを設定します。ローカル認証を行うには、次項のローカルユーザーを設定する必要があります（「ローカルユーザー」を参照ください）。

・<適用>ボタンをクリックすると、次の表に値が反映されます。
・<設定>/<状態確認>ボタンをクリックすると、以下の画面が表示されます（下記参照）。

（ア） 設定 ボタンをクリックすると、下記のとおり、「ポートアクセス設定」画面が表示され、ポートごとにアクセスを行うための認証設定等を行うことができます。

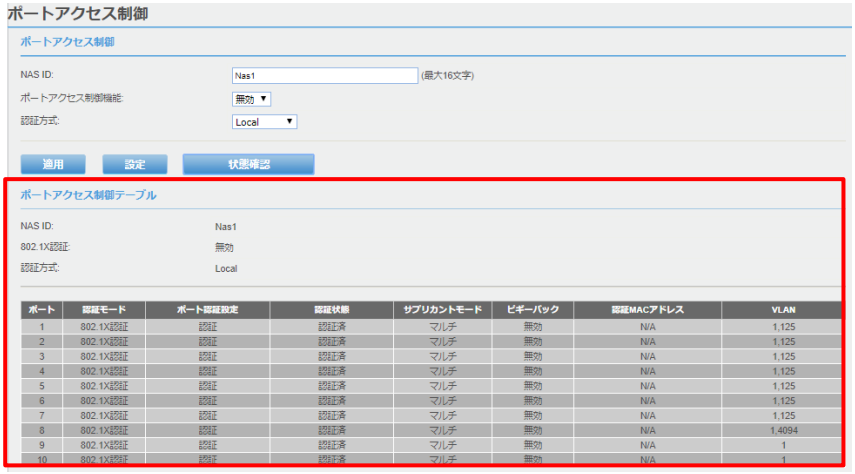


■ポートアクセス設定

❒ポート: ポート番号を選択します。
❒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（デフォルト：802.1X 認証）。
❒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）
ポート認証を行う場合は「自動」に変更してください。
❒再認証:ポートでの再認証機能を有効/無効にします。
❒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）。
・マルチ：1 つのポートに対して、複数のユーザーを認証できます。
・シングル：1 つのポートに対して、1 つのユーザーのみ認証します。
❒ピギーバック: ピギーバックモードを有効/無効にします。
ピギーバックモードを「有効」にすると、1 つのクライアントが認証にパスすると、他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可能になります。
【注記】:ピギーバックモードは、「サプリカントモード」が「シングル」に設定されている場合のみ選択できます。
❒ダイナミック VLAN ダイナミック VLAN 機能を有効/無効にします。
ダイナミック VLAN 機能を「有効」にすると、認証済みクライアントがログインすると、サーバーやローカルユーザーの情報に応じて自動的に VLAN を割り当てます。
❒セキュア VLAN:セキュア VLAN 機能を有効/無効にします。
セキュア VLAN 機能を「有効」にすると、一旦クライアントの認証が許可されると、そのクライアントとは異なる VLAN ID のクライアントの認証は許可されません。
【注記】: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可能です。
❒ゲスト VLAN ID:ゲスト VLAN ID を入力します。
※認証に失敗すると、ゲスト VLAN が割り当てられます。
❒再送間隔:プリカントからの応答を待機する時間を入力します(有効範囲:1～65535（秒）、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パケットを送信回数の上限を入力します（最大回数: 1-10、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入力します(有効範囲:1～65535（秒）、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入力します(有効範囲:1～65535（秒）、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つ時間を入力します(有効範囲:1～65535（秒）、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つ時間を入力します(有効範囲:1～65535（秒）、デフォルト：30 秒）。

【注記】:MAC 認証では再認証は常に有効になり、再認証間隔のデフォルト値は「600 秒」です

(イ) 状態確認 ボタンをクリックすると、下記のとおり「ポートアクセステーブル」の画面が表示されます。



■ポートアクセス制御テーブル

❒NAS ID: 本機の NAS ID が表示されます。
❒802.1X: 認証 802.1X 認証の状態が表示されます。
❒認証方式: 認証方式(RADIUS/TACACS+/Local)が表示されます（デフォルト: Local）

ポート	認証モード	ポート認証設定	認証状態	サプリカントモード	ピギーバック	認証MACアドレス	VLAN

❒ポート: 本機のポート番号が表示されます。
❒認証モード: 各ポートに設定された認証モードが表示されます。
❒ポート認証設定: 各ポートに設定された制御モードが表示されます。
❒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の設定が表示されます。
❒ピギーバック: 各ポートのピギーバックモードの設定が表示されます。
❒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。
❒VLAN: 認証済みクライアントの VLAN 情報が表示されます。

3.6.2 ローカルユーザー

ローカルユーザー機能は、リモート（RADIUS）サーバーが利用できない場合にポートセキュリティ用のローカル認証サーバーを提供します。
ローカルユーザー（ローカル）認証方式では、スイッチの内部で 802.1x 認証パラメータを設定できます。 この場合、ユーザー名とパスワードの組み合わせは、設定時にオプションの VLAN に関連づけられます。サプリカントの認証プロセスは、これらのエントリに基づいて標準の EAPOL（EAP over LAN）処理を介してスイッチ管理ユーティリティによってローカルで行われます。

「セキュリティ」→「ローカルユーザー」をクリックすると、以下の画面が表示されます。

■ローカルユーザー設定

❒ユーザー名:ユーザーの名前を入力します(20 文字以内)。

❒パスワード:ユーザーのパスワードを入力します(20 文字以内)。

❒ダイナミック VLAN: ユーザーにアクセスを許可する VLAN の VID を入力します(有効範囲:1-4094)。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に追加されます。

■ローカルユーザーデーターベース

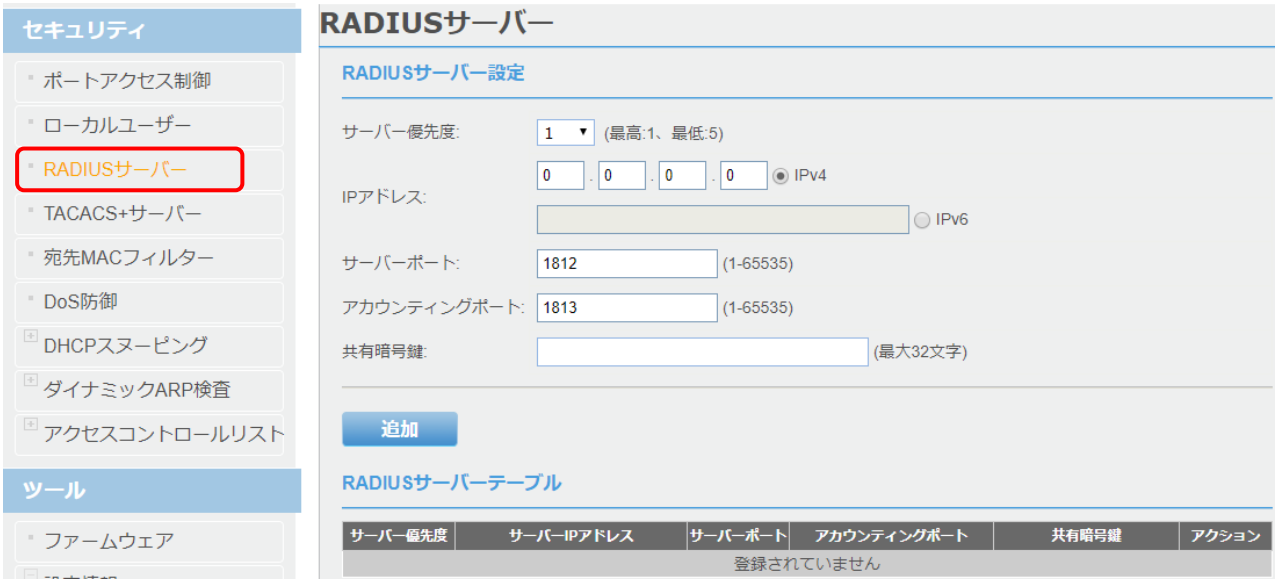
❒ローカルユーザーデーターベース:「ローカルユーザー設定」で設定した内容が反映されます。

・<全削除>ボタンをクリックすると、設定したデータベースはすべて削除されます。

3.6.3 RADIUS サーバー（※非サポート）

RADIUS サーバー（RADIUS 認証方式）を追加する手順について説明します。

「セキュリティ」→「RADIUS サーバー」をクリックすると、以下の画面が表示されます。



■RADIUS サーバー設定

❒サーバー優先度: RADIUS サーバーの優先順位を入力します（有効範囲:1～5、デフォルト:1）。
※1:最高優先度～5:最低優先度を表します。

❒IP アドレス:IPv4 または IPv6 を選択して RADIUS サーバーの IP アドレスを設定し、追加したい RADIUS サーバーの IP アドレスを入力します。

❒サーバーポート（1-65535）: RADIUS 認証サーバーの UDP ポートを設定します(有効範囲:1-65535、デフォルト値:1812)。

❒アカウンティングポート: RADIUS アカウントサーバーの UDP ポートを設定します(有効範囲:1-65535、デフォルト値: 1813)。

❒共有暗号鍵:本機と RADIUS サーバー間の RADIUS 通信用のデフォルトの認証および暗号化キーを入力します(32 文字以内)。

■RADIUS サーバーテーブル

「RADIUS サーバー設定」で設定した値が反映されます。

3.6.4 TACACS+サーバー（※非サポート）

TACACS +サーバー（TACACS +認証方法）の設定について説明します。

TACACS +(ターミナルアクセスコントローラアクセス制御システム）は、集中型セキュリティユーザークセス検証を提供します。本機は TACACS +サーバーを最大 5 台までサポートします。
TACACS +は、RADIUS や他の認証プロセスとの一貫性を保ち、集中型のユーザー管理システムを提供します。
TACACS +プロトコルは、クライアントと TACACS +サーバー間の暗号化されたプロトコル交換を介してネットワークの整合性を保証します。ユーザーにより割り当てられた TACACS +パラメータは、新しく設定された TACACS +サーバーに適用されます。値が定義されていない場合は、デフォルトの場合新しい TACACS +サーバーに適用されます。

「セキュリティ」→「TACACS+」をクリックすると、以下の画面が表示されます。

■TACACS +サーバー設定

❒サーバー優先度:TACACS +サーバーの優先順位を入力します（有効範囲：1～5、デフォルト:1）。
※1:最高優先度～5:最低優先度を表します。

❒サーバーIP アドレス: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 +セッションをもつポート番号を入力します(有効範囲:1-65535 秒、デフォルト値: 1812)。

❒タイムアウト時間:クエリーを再試行するか、次のサーバーに切り替えるまでに、デバイスが TACACS +サーバーからの応答を待つ時間を入力します（有効な値は:1～255 秒、デフォルト値: 5 秒）。

❒共有暗号鍵:本機と TACACS +サーバー間の TACACS +通信用のデフォルトの認証および暗号化キーを入力します（32 文字以内）。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に追加されます。

■TACACS+サーバーテーブル:
「TACACS +サーバー設定」で設定した値が反映されます。

3.6.5 宛先 MAC フィルター

ここでは、宛先 MAC フィルター機能とその設定手順について説明します。
宛先 MAC フィルター機能により、スイッチが特定のデバイスにパケットを転送するのを防ぎます。Web 管理ユーティリティソフトウェアの「宛先 MAC フィルター」画面で、フィルタリングしたいデバイスの MAC アドレスを入力します。

スイッチはパケットを受信すると、パケットの宛先 MAC アドレスをチェックし、宛先 MAC アドレスがフィルターに設定されている MAC アドレスと一致する場合、そのパケットの転送せずにドロップします。

「セキュリティ」→「宛先 MAC フィルター」をクリックすると、以下の画面が表示されます。

■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>ボタンをクリックすると、上記に設定したエントリが次の表に追加されます。

■宛先 MAC フィルターテーブル:

上記に設定したエントリが表に追加されます。

【注記】: 宛先 MAC フィルターの最大登録数は「40」です。

3.6.6 DoS 防御（※非サポート）

スイッチには DOS(Denial of Service)防止機能が組み込まれており、特定の種類のトラフィックに関連したネットワークへの DOS 攻撃を制限できます。

「セキュリティ」→「DoS 防御」をクリックすると、以下の画面が表示されます。

■DoS 防御設定

それぞれ、以下の攻撃に対して、無効/ブロックを設定してください（デフォルト:無効）。

❒AND 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:

・<適用>ボタンをクリックすると、上記の設定が適用されます。
・<初期値に戻す>ボタンをクリックすると、エンジン ID フィールドの値はすべてデフォルト値に戻ります。

3.6.7 DHCP スヌーピング

ここでは、DHCP スヌーピングを有効にする方法について説明します。

「セキュリティ」→「DHCP スヌーピング設定」→「基本設定」をクリックすると、以下の画面が表示されます。

■DHCP スヌーピング設定

❒DHCP スヌーピング機能: DHCP スヌーピング機能を有効/無効にします。

【注記】:「DHCP スヌーピング」→「VLAN 設定」で VLAN を指定する必要があります（「VLAN 設定」を参照してください」。

ネットワーク上のスタティック IP アドレスはすべて手動でバインディングデータベースに追加する必要があります。

■DHCP スヌーピング詳細設定

❒オプション 82 透過:プルダウンメニューから次のいずれかを選択してください（デフォルト:無効）。

・有効:オプション 82 パケットを変更せずにそのまま通過させることができます。

・無効:オプション 82 パケットがスイッチを通過するのをブロックします。

❒MAC アドレス検証:プルダウンメニューから次のいずれかを選択してください（デフォルト:有効）。

・有効:各 egress ARP パケットの MAC アドレスは、バインディングテーブルのエントリと比較して検証されます。無効な ARP パケットは破棄されます。

・無効:各 egress ARP パケットの MAC アドレスは、バインディングテーブルに対して検証を行いません。すべての ARP パケットは、パケットヘッダー内の IP および MAC アドレス情報に関係なく、スイッチを介して転送されます。

❒バックアップデータベース:次のいずれかを選択してください（デフォルト:無効）。

・有効: Web 管理ユーティリティソフトウェアは、指定された間隔（データベース更新間隔）で、バインディングテーブルのバックアップコピーをフラッシュに保存します。

・無効: Web 管理ユーティリティソフトウェアは、バインディングテーブルのバックアップのコピーをフラッシュに保存しません。

❒データベース更新間隔:データベース更新間隔を入力します（有効範囲: 600～86400 秒、デフォルト値：1200）。

❒DHCP オプション 82 挿入:プルダウンメニューから次のいずれかを選択してください（デフォルト:無効）。

・有効:Web 管理ユーティリティソフトウェアは DHCP option 82 情報を DHCP パケットに挿入します。

・無効:Web 管理ユーティリティソフトウェアは、DHCP option 82 情報を DHCP パケットに挿入しません。

上記設定を完了後、<適用>ボタンをクリックすると、それぞれの値が表に反映されます。

1. VLAN 設定

ここでは、DHCP スヌーピングを適用するために既存の VLAN を定義します。

「セキュリティ」→「DHCP スヌーピング」→「VLAN 設定」をクリックしてください。

■DHCP スヌーピング VLAN 登録

❒VLAN ID: DHCP スヌーピングを有効にする VLAN ID を登録します（有効範囲:1-4094）。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に追加されます。
・<クリア>ボタンをクリックすると、上記に設定したエントリはクリアされます。

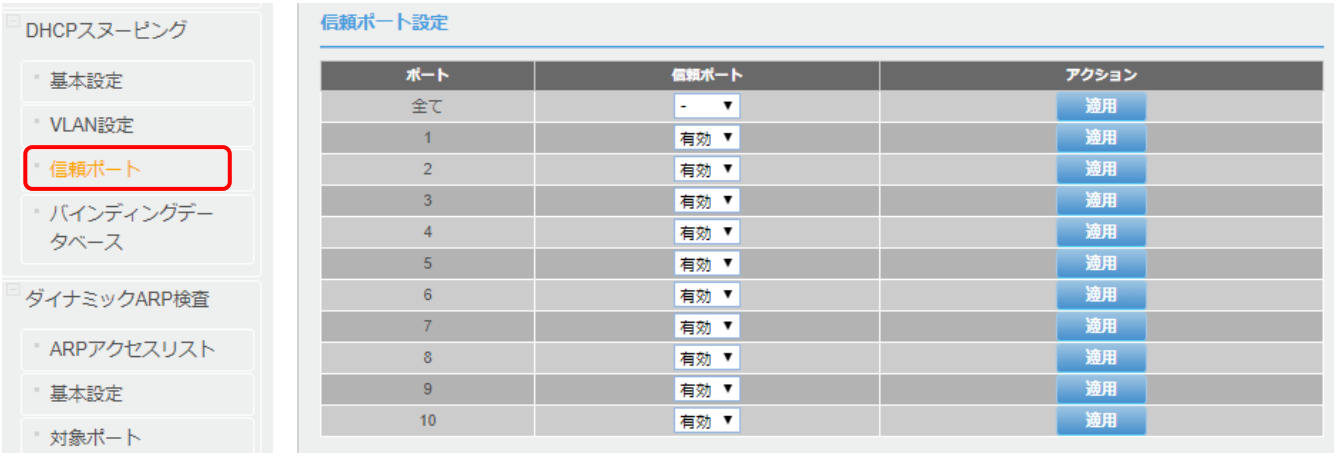
■DHCP スヌーピング VLAN テーブル

「DHCP スヌーピング VLAN 登録」で登録した VLAN ID がリストに表示されます。

2 信頼ポート設定

ここでは、trusted DHCP サーバーインターフェースの設定方法について説明します。

「セキュリティ」→「DHCP スヌーピング」→「信頼ポート設定」をクリックすると、以下の画面が表示されます。



【注記】:信頼ポートとして、以下の条件を確認してください。
・有効な信頼 DHCP サーバーに直接アクセスしている。
・信頼サーバーとの間で DHCP メッセージが中継されているネットワークデバイスである。
・DHCP スヌーピングが有効なスイッチなど、信頼できる送信元ポートである。

■信頼ポート設定

❒ポート:本機のポート番号が表示されます。
※設定をすべてのポートに適用する場合は、表の最上部のポートの「全て」の行を「有効」に設定してください。

❒信頼ポート設定
・無効:DHCP スヌーピング機能に対して非信頼ポートとして定義します。
・有効:DHCP スヌーピング機能に対して信頼ポートとして定義します。

❒アクション:<適用>ボタンをクリックすると、設定したエントリが反映されます。

3 バインディングデータベース

DHCP アドレスのバインディングデータベースの設定方法について説明します。
バインディングデータベースには、ローカルエリアネットワーク上の各ホストのダイナミック、またはスタティックに割り当てられた MAC アドレスと IP アドレス情報を設定することができます。

「セキュリティ」→「DHCP スヌーピング」→「バインディングデータベース編集」をクリックすると、以下の画面が表示されます。

■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」を選択して、ホストに割り当てられている 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(有効範囲:1-4094)。
【注記】:「DHCP スヌーピング」→「VLAN 設定」画面にて、あらかじめ VLAN ID 設定する必要があります（「VLAN 設定」を参照ください）。

❒ポート:プルダウンメニューにより、ホストが接続されているポート番号を選択します（デフォルト設定:1）。

❒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。
・スタティック：非信頼ポートに固定 IP アドレスを持つ部門サーバーなどを接続するときに利用します。
バインディングデータベースに端末情報を手動にて設定して、通信を行います。
スタティックエントリーの場合、エントリーのリース時間を指定する必要はありません。
・ダイナミック：DHCP サーバーから IP アドレスが配布された際に登録されます。
通常は，ダイナミック登録によって端末情報を登録します。
ダイナミックエントリーの場合、エントリーのリース時間を指定する必要があります

❒リース時間: ダイナミックエントリーに設定した場合、IP アドレスの割り当てが有効になる時間を設定します(有効範囲:10～4294967295 秒)。

・<追加>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。
・<リセット>ボタンをクリックすると、入力した値がリセットされます。
・<クリア>ボタンをクリックすると、設定した値がクリアになります。

■バインディングデータベース
　ダイナミックエントリーの場合、DHCP サーバーから動的に割り当てられた IP アドレスはサーバーによって割り当てられるため、テーブル上に自動的に入力されます。スタティックエントリーの場合、手動で割り当てられた IP アドレスは、ホストのアドレス情報を入力して<追加>ボタンをクリックして手動で入力します。

3.6.8 ダイナミック ARP 検査

ダイナミック ARP 検査とは、LAN 上で ARP パケットを検査するセキュリティ機能のことです。
本機能は、IP アドレスと MAC アドレスの関連付けを検証し、不正な ARP 応答を破棄して、正規の ARP 応答パケットのみを転送します。

1. APR アクセスリスト

APR アクセスリストを設定します。

「セキュリティ」→「ダイナミック ARP 検査」→「APR アクセスリスト」をクリックすると、以下の画面が表示されます。

■ARP アクセスリスト追加
　❒ARP アクセスリスト名：追加したい ARP アクセスリスト名を入力してください。

　・<適用>ボタンをクリックすると、設定したリスト名が反映されます。

■ARP アクセスリストテーブル
　❒「ARP アクセスリスト追加」で入力した ARP アクセスリスト名がリストに表示されます。

2. 基本設定

本章では、ダイナミック ARP 検査の基本設定を行います。

「セキュリティ」→「ダイナミック ARP 検査」→「基本設定」をクリックすると、以下の画面が表示されます。

■ARP 検査設定

❒送信元 MAC:送信元 MAC を有効/無効にします（デフォルト:無効）。
レイヤ 2 ヘッダに含まれる送信元 MAC アドレスと、ARP ヘッダに含まれる送信元 MAC アドレスが同一であることを検査します。ARP 要求および ARP 応答の両方に対して検査を行います。

❒宛先 MAC:宛先 MAC　検査を有効/無効にします（デフォルト:無効）。
レイヤ 2 ヘッダに含まれる宛先 MAC アドレス（Destination MAC）と，ARP ヘッダに含まれる宛先 MAC アドレスが同一であることを検査します。
ARP 応答に対してのみ検査を行います。

❒IP アドレス:IP アドレス検査を有効/無効にします（デフォルト:無効）。
ARP ヘッダに含まれる宛先 IP アドレスが次に示す範囲内であることを検査します。
・1.0.0.0 ～ 126.255.255.255
・128.0.0.0 ～ 223.255.255.255
ARP Reply に対してのみ検査を行います。

・<適用>ボタンをクリックすると、設定したエントリが反映されます。

■ARP 検査ログ設定

ARP 検査ログが表示されます。VLAN ID/ACL ログ/DHCP ログがそれぞれ表示されます。

■ARP 検査フィルタ

❒ARP アクセスリスト名: ARP アクセスリスト名を入力します（32 文字以内）。
【注記】:ARP アクセスリストを追加する場合、「ARP　アクセスリスト」画面で設定されている必要があります。

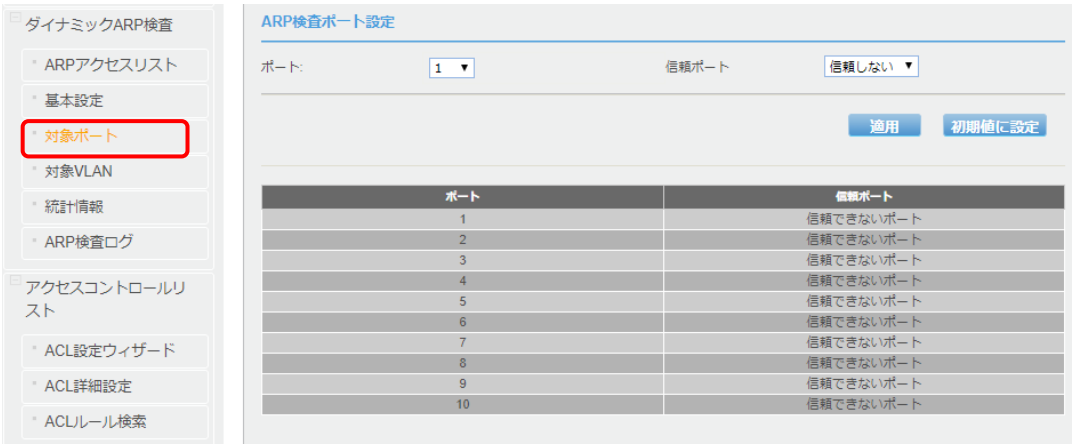
❒VLAN ID リスト:追加/削除したい VLAN ID を入力します。

❒スタティック ACL:　スタティック ACL を ARP アクセスリストに対応させるか、非対応とするか選択してください。
・対応：スタティック ACL で許可されてない場合はブロックします。バインディングデータベースは参照しません。
・非対応：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>ボタンをクリックすると、上記に設定したエントリが次の表に反映されます。
・<削除>ボタンをクリックすると、設定したエントリが削除されます。

3. 対象ポート

「セキュリティ」→「ダイナミック ARP 検査」→「対象ポート」をクリックすると、以下の画面が表示されます。



■ARP 検査ポート設定
対象ポートごとに、信頼ポートの可否を選択します。

❒信頼ポート
DHCP サーバーや部門サーバーなど，信頼済みの端末を接続するポートを“信頼ポート”と呼びます。
信頼ポートで受信した ARP パケットは監視されません。

❒信頼できないポート
DHCP クライアントなど、信頼されていない端末を接続するポートを“信頼できないポート”と呼びます。
DHCP サーバーには接続しません。

・<適用>ボタンをクリックすると、設定したエントリが反映されます。
・<初期値に設定>ボタンをクリックすると、デフォルト値に戻ります。

4. 対象 VLAN

ダイナミック ARP 検査対象の VLAN を設定します。

「セキュリティ」→「ダイナミック ARP 検査」→「対象 VLAN」をクリックすると、以下の画面が表示されます。

■ARP 検査統計情報

❒VLAN ID リスト: ダイナミック ARP 検査対象の VLAN ID を入力します。

・<クリア>ボタンをクリックすると、設定した VLAN ID の値がクリアになります。
・<全てクリア>ボタンをクリックすると、設定した VLAN ID の値がすべてクリアになります。

■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に応じて廃棄数が表示されます。
❒ACL 廃棄数:ARP アクセスリストベースの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に応じて許可数が表示されます。
❒ACL 許可数：ARP アクセスリストベースの許可数が表示されます。
❒送信元 MAC 廃棄数:送信元 MAC 検証ベースの廃棄数が表示されます。
❒宛先 MAC 廃棄数:宛先 MAC 検証ベースの廃棄数が表示されます。
❒IP 廃棄数:IP アドレス検証ベースの廃棄数が表示されます。

5. ARP 検査ログ

ダイナミック ARP 検査のログ情報が表示されます。

「セキュリティ」→「ダイナミック ARP 検査」→「ARP 検査ログ」をクリックすると、以下の画面が表示されます。

■ARP　検査ログ

❒ログバッファ（1-1024）: ARP 検査ログの件数を入力します（有効範囲:1-1024、デフォルト:32）

・<クリア>ボタンをクリックすると、設定したエントリがクリアになります。
・<適用>ボタンをクリックすると、設定したエントリが反映されます。

■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。

3.6.9 アクセス制御リスト

アクセス制御リスト（ACL）の設定方法について説明します。

アクセス制御設定を使用すると、イーサネットポートがスイッチポートに入り、スイッチを介して処理されるときに、イーサネットトラフィックのさまざまな側面を制御できます。入力ポートで特定のフィルター基準を設定することによって、スイッチを通過するトラフィックを許可/拒否します。イーサネットパケットのスイッチング優先順位を管理することもできます。これはすべて、フィルタリングと優先順位の動作を定義するポリシーを指定することによって行われます。

1. ACL 設定ウィザード

ACL 構成ウィザードは、簡単なアクセスプロファイルやルールを自動的に作成します。詳細な設定を行いたい場合、あるいは新規のプロファイルを作成したい場合は、次項の「ACL 詳細設定」にて設定してください。

「セキュリティ」→「アクセス制御リスト」→「アクセス制御リスト（ACL）構成ウィザード」をクリックすると、以下の画面が表示されます。

■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:アクセスパケットの送信元を定義します。

・Any:ACL アクションがあらゆる送信元からのパケットに対して行われることを表示します。
・MAC アドレス:指定された MAC アドレスからのパケットに対して ACL アクションが実行されることを表示します。
・IPv4 アドレス:指定された IPv4 送信元アドレスからのパケットに対して ACL アクションが実行されることを表示します。
・IPv6 アドレス:指定された IPv6 アドレスからのパケットに対して ACL アクションが実行されることを表示します。

❒宛先:アクセスパケットの宛先を定義します。

・Any:ACL アクションがあらゆる宛先へのパケットに対して行われることを表示します。
・MAC アドレス:指定された MAC アドレスへのパケットに対して ACL アクションが実行されることを表示します。
・IPv4 アドレス:指定された IPv4 宛先アドレスへのパケットに対して ACL アクションが実行されることを表示します。
・IPv6 アドレス:指定された IPv6 宛先アドレスへのパケットに対して ACL アクションが実行されることを表示します。

❒サービスタイプ:サービスタイプを定義します。

・Any:すべてのタイプのサービスのパケットに対して ACL アクションが実行されることを表示します。
・Ether タイプ:Ether タイプパケットフィルタリングを指定します。
・ICMP「全て」:ICMP パケットフィルタリングを指定します。

・IGMP:IGMP パケットフィルタリングを指定します。
・TCP 「全て」:TCP パケットフィルタリングを指定します。
・TCP Source　ポート:パケットを対応する TCP 送信元ポートに一致させます。
・TCP Destination　ポート:パケットを対応する TCP 宛先ポートに一致させます。
・UDP 「全て」:UDP パケットフィルタリングを指定します。
・UDP Source　ポート:パケットを対応する UDP Source　ポートに一致させます。
・UDP Destination　ポート:パケットを対応する UDP 宛先ポートに一致させます。

❒アクション:ルール基準にリンクしている ACL アクションを定義します。
※このフィールドはオプションです。
・許可:指定された ACL 基準に適合する入力パケットが許可されます。
・ブロック指定された ACL 基準に適合する入力パケットをドロップします。
・帯域制限:すべての ACL 基準が満たされている場合、レート制限を有効にします。
・DSCP 変更: DSCP レベルを表示します（有効範囲:0～63）。

❒ポート:設定するポートを定義します。

・<適用>ボタンをクリックすると、設定した値が反映されます。
・<取消>ボタンをクリックすると、設定した値が削除されます。

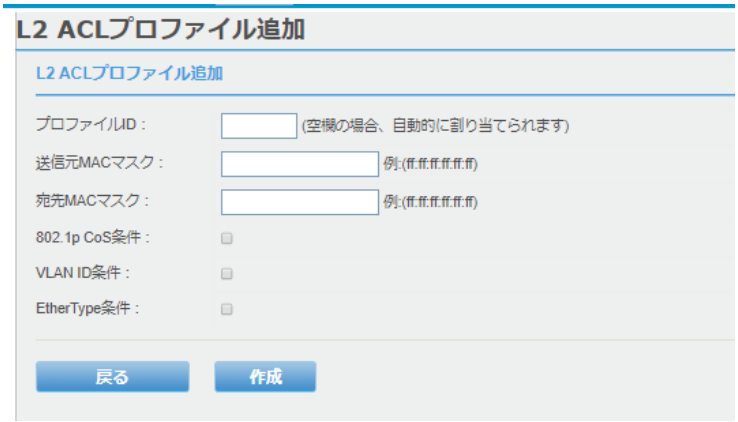
2. アクセス詳細設定

L2/L3 プロファイルリストをそれぞれ作成します。
ここでは、より詳細なフィルタリングルールを作成する場合に使用します。

「セキュリティ」→「アクセス制御リスト」→「アクセス詳細設定」をクリックすると、以下の画面が表示されます。

プロファイル数は「最大 150」まで、最大ルール数は「最大 256」まで設定可能です。

画面上の L2/ L3　ACL プロファイルリストの 新規作成 ボタンをクリックすると、以下の「ACL プロファイル追加」画面が表示されます。



それぞれ新しい ACL プロファイルの情報を入力してください。
・<戻る>ボタンをクリックすると、「ACL 詳細設定」画面に戻ります。
・<作成>ボタンをクリックすると、新しい ACL ルールを設定できます。

3. ACL ルール検索

各ポートに割り当てられている現在の L2/L3 ルールのポリシーをインデックスまたはシーケンスで表示できます。
ACL ルール検索機能を用いると、指定したポートに割り当てたルールを容易に検索することができます。

「セキュリティ」→「アクセス制御リスト」→「ACL ルール検索」をクリックすると、以下の画面が表示されます。

■ACL ルールテーブル
　❒タイプ　ID:L2 ルール/L3 ルールのいずれかを選択します（デフォルト:L2 ルール）。
　❒プロファイル ID:検索対象のプロファイル ID を選択します（デフォルト:Any）。
　❒ポート:検索対象のポート番号を入力します。

・<検索>ボタンをクリックすると、下記の表に検索結果が表示されます。

プロファイルID	アクセスID	タイプ	フィルター対象	状態	アクション

　❒プロファイル ID:プロファイル ID を表示します。
　❒アクセス ID:アクセス ID を表示します。
　❒タイプ:プロファイルの種類を表示します。
　❒フィルター対象:ACL ルールの要約を表示します。
　❒状態:ACL ルールの状態を表示します。

3.7 ツール

ここでは、本機のツール機能(ファームウェアの更新/バックアップ/リストア、設定情報のバックアップ/リストア、ケーブル診断、再起動、ping)の使用方法について説明します。

本機能は、以下のメニューより構成されています。

3.7.1 ファームウェア

ここでは、ファームウェアの更新方法について説明します。

本器で稼働中、または保存されているファームウェアのバージョンについては、「3.2.1 システム情報」メニューまたは、「ツール」→「ファームウェアの更新」をクリックしてご確認ください。

本機用のファームウェアのアップグレードバージョンが入手可能かどうかを確認するには、弊社ホームページ（https://www.fxc.jp/cgi-bin/certify/index.html）にて本製品のバージョンを確認してください。

「ツール」→「ファームウェア」をクリックすると、以下の画面が表示されます。

この場合、以下の点に注意してください。

- ファームウェアのアップグレードプロセスを中断しないでください。アップグレード中にデバイスの電源を切ったり、リセットボタンを押さないでください。
- ラップトップコンピュータを使用してファームウェアをアップグレードする場合は、ラップトップに電源が接続されていること、またはバッテリが完全に充電されていることを確認してください。
- ファームウェアのアップグレードプロセスを中断する可能性があるため、コンピュータのスリープモードを無効にします。
- ワイヤレス接続を使用してファームウェアをアップグレードしないでください。有線ネットワーク接続のみを使用してください。
- ファームウェアのアップグレードのプロセス中に中断されると、恒久的に損傷を受ける可能性があります。

① 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:現在動作しているファームウェアイメージが表示されます。

❒イメージ 1/2 バージョン:イメージ 1/2 のバージョンが表示されます。

・<適用>ボタンをクリックすると、設定したエントリが反映されます。

② ファームウェア更新

【注記】:現在ご使用のイメージ以外のファームウェアイメージが更新されます。

❒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。
<参照>ボタンをクリックし、お使いの PC 上のイメージファイルを選択します(拡張子:*.hex)。

❒TFTP サーバー:「IPv4/IPv6」のいずれかを選択して、「TFTP サーバー」の IP アドレスを入力します。
【注記】: 1. プロトコルで TFTP を指定した場合に使用します。
2. イメージファイル（*.hex）は、TFTP サーバーのルートディレクトリーに保存してください。

❒イメージファイル名：プロトコルで「TFTP」を指定した場合にのみ使用できます（64 文字以内）。
TFTP サーバーのルートディレクトリーに保存したイメージファイルの名前（***.hex）を入力します。

❒リトライ回数: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。
【注記】: プロトコルで TFTP を指定した場合にのみ設定可能です。

・<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。

【注記】:ファームウェア更新により、一時的にシステムにアクセスできなくなり、再ログインが必要になります
【注記】: TFTP を選択する場合、TFTP サーバーが必要になります。この機能に使用できるサードパーティの TFTP サーバーのアプリケーションをご使用ください。TFTP プロトコルに慣れていない場合は、HTTP を使用することをお勧めします。

③ ファームウェアのバックアップ

❒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。
❒イメージ ID：バックアップを行うイメージ ID を選択します。
❒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。
<ファイルを選択>ボタンをクリックし、お使いの PC 上の設定ファイルを選択します(拡張子:*.hex)。

❒TFTP サーバー:「IPv4/IPv6」のいずれかを選択して、「TFTP サーバー」の IP アドレスを入力します。
【注記】: プロトコルで TFTP を指定した場合に使用します。

❒イメージファイル名：プロトコルで「TFTP」を指定した場合にのみ使用できます（64 文字以内）。
バックアップ後のファイルの名前（***.hex）を入力します。

❒リトライ回数: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。
【注記】: プロトコルで TFTP を指定した場合にのみ設定可能です。

・<適用>ボタンをクリックすると、指定の設定ファイルがバックアップされます。

3.7.2 設定情報

1. 設定情報のバックアップ/レストア

本機の設定ファイルをバックアップしたり、バックアップしたファイルをレストアする方法について説明します。

「ツール」→「設定情報」→「バックアップ/レストア」をクリックすると、以下の画面が表示されます。

本機に多数のカスタマイズ設定を追加した場合やデフォルトにリセットする必要がある場合、カスタマイズ設定はすべて失われますが、すべての設定を手動で再設定することなく、バックアップファイルから簡単にレストアすることができます。

① 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:現在動作している設定ファイルが表示されます。

・<適用>ボタンをクリックすると、設定したエントリが反映されます。

② 設定のバックアップ

❒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。
<ファイルを選択>ボタンをクリックし、バックアップを行う設定ファイルを選択します。

❒TFTP サーバー:・「IPv4/IPv6」のいずれかを選択して、「TFTP サーバー」の IP アドレスを入力します。
【注記】: プロトコルで TFTP を指定した場合に使用します。

❒ファイル名：プロトコルで「TFTP」を指定した場合にのみ使用できます（64 文字以内）。
バックアップ後の設定ファイルの名前（***.bin）を入力します。

・<バックアップ>ボタンをクリックすると、指定の設定ファイルがバックアップされます。

③ 設定レストア

❒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。

❒設定ファイル：レストアの対象設定ファイルを選択します。

❒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。
<ファイルを選択>ボタンをクリックし、お使いの PC 上のレストアする設定ファイルを選択します(拡張子:*.hex)。

❒TFTP サーバー：・「IPv4/IPv6」のいずれかを選択して、「TFTP サーバー」の IP アドレスを入力します。
【注記】: 1. プロトコルで TFTP を指定した場合に使用します。
2. レストアする設定ファイル（*.hex）は、TFTP サーバーのルートディレクトリーに保存してください。

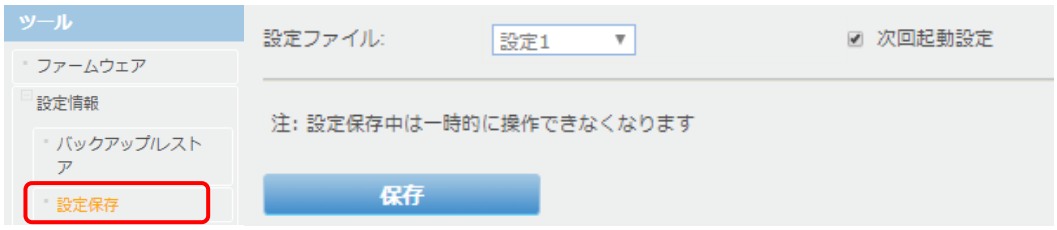
❒ファイル名：プロトコルで「TFTP」を指定した場合にのみ使用できます（64 文字以内）。
レストアする設定ファイルの名前（***.hex）を入力します。

・<レストア>ボタンをクリックすると、設定ファイルはレストアされます。

2. 設定保存

設定を変更した後の設定情報の保存方法について説明します。

「ツール」→「設定情報」→「設定保存」をクリックすると、以下の画面が表示されます。



❒設定ファイル：保存したい設定ファイルを選択してください。
※「次回起動時設定」が☑すると、次回起動時にこの設定ファイルが使用されるため、使用しない場合は☑を外してください。

・<保存>ボタンをクリックすると、変更した情報がすべてフラッシュメモリーに保存されます。

【注記】:設定を保存中は、一時的に操作できなくなります。
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、再起動後に変更した設定情報がすべて失われます。
また、設定の保存には数秒間かかります。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。

【注記】:設定保存中は一時的に操作できなくなります。

3.7.3 ケーブル診断

ケーブル長の推定距離を確認し、トラブルシューティング用の基本的なケーブル診断ツールを提供します。

「ツール」→「ケーブル診断」をクリックすると、以下の画面が表示されます。

ケーブル診断機能は、ポートごとに接続されたケーブルの健全性を確認する機能です。ケーブル障害が検出された場合、発生箇所や障害の種類などの簡単な切り分けを行うことができます。

【注記】:

1. 推定ケーブル長が「N/A」と表示される場合は、ケーブル品質やリンク状態などの理由により測定に失敗したことを示します。
2. 推定障害発生距離の結果には「2m」前後の誤差があります。なお、ケーブル長が「2m 以下」の場合には表示されません。

■ケーブル診断設定

❒ポート:ケーブル診断を実行するポートを選択し、 テスト開始 ボタンをクリックしてテストを実行します。

■ケーブル診断結果

❒テスト結果：ケーブルの各ペアの診断結果を表示します。次のいずれかのケーブルステータスパラメータが表示されます。

- ・OK:ケーブルに問題は検出されませんでした。
- ・Open in Cable：断線している可能性があります。
- ・Short in Cable：ペアのケーブルワイヤがショートしています。
- ・Cross talk in Cable：ケーブル内の別のペアとの間でクロストークが検出されました。

❒推定障害発生距離(m)：ポートからケーブルの障害箇所までの距離を指定します。

❒推定ケーブル長(m):ポートに接続されているケーブルの推定長を表示します。

3.7.4 再起動

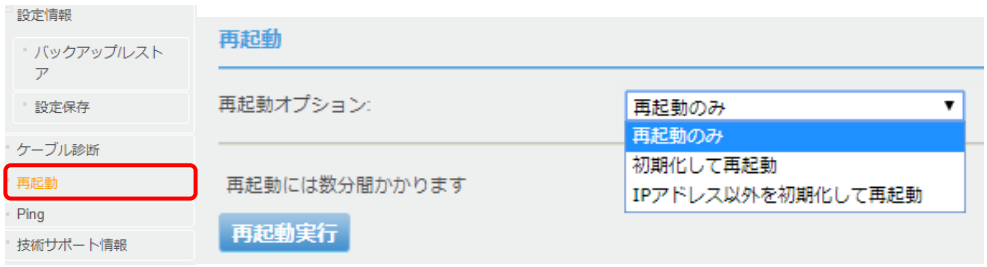
再起動/出荷時設定へのリセット方法について説明します。

本機に何らかの問題が発生し、トラブルシューティングを試みる場合は、まず本機を再起動することをお勧めします。
ただし、本機を再起動する場合、可能であればまず設定情報を保存してください（保存方法については、「2.設定保存」にてご確認ください。

本機を再起動する方法は 2 つあります。
- ❒ハードウェアによる再起動:本機の前面パネルにあるリセットボタンをクリップ等で「1～5」秒間押し続けてください（詳細については、「1.2 各部の名称と働き」にてご確認ください。
- ❒ソフトウェアによる再起動（以下参照ください。）

次に、ソフトウェアによる再起動について説明します。

「ツール」→「設定情報」→「再起動」をクリックすると、以下の画面が表示されます。



■再起動
- ❒再起動オプション:再起動の方法には、次のオプションがあります。
  - ・再起動のみ：再起動の際、事前に設定情報を保存したことを確認してください。設定情報を保存していない場合、変更は保持されないため、スイッチを再起動する前に必ず設定を保存してください。
  - ・初期化して再起動：再起動すると、設定がすべてリセットされます。
  - ・IP アドレス以外を初期化して再起動：再起動すると、スイッチの IP アドレスの設定のみが保持され、他の設定はすべてリセットされます。
  - 【注記】: ただし、IP アドレス設定が保持されるのは 「vlan 1」に設定されたアドレスのみとなります。

・上記のオプションを選択して、<再起動実行>ボタンをクリックしてください。
【注記】:再起動には、数分間かかります。

3.7.5 Ping(ネットワーク接続テスト)

ここでは、本機からネットワーク上のノードに ping を送信する手順について説明します。

「ツール」→「設定情報」→「Ping テスト」をクリックすると、以下の画面が表示されます。

■PING テスト

❒宛先 IP アドレス: IPv4/IPv6 のいずれかを選択し、対象の 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 の実行回数を入力します（有効範囲: 1～10（回）、デフォルト：10 回）

・<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 をクリックすると、次の「Ping テスト結果」画面が表示されます。

■PING テスト結果

❒結果表示

・宛先 IP アドレス:「PING テスト」画面で指定した宛先 IP アドレスが表示されます。

・成功率: PING テストの成功率（%）が表示されます。

・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>ボタンをクリックすると、「PING テスト」画面に戻ります。

3.7.6 技術サポート情報

技術サポート情報が表示されます。

「ツール」→「設定情報」→「技術サポート情報」をクリックすると、以下の画面が表示されます。

❒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。

❒TFTP サーバー：・「IPv4/IPv6」のいずれかを選択して、「TFTP サーバー」の IP アドレスを入力します。
【注記】: 1. 「プロトコル」で TFTP を指定した場合に使用します。
2. 設定ファイル（*.hex）は、TFTP サーバーのルートディレクトリーに保存してください。

❒ファイル名：プロトコルで「TFTP」を指定した場合にのみ使用できます（64 文字以内）。
TFTP サーバーのルートディレクトリーに保存した設定ファイルの名前（***.hex）を入力します。

NS2010VPEL Management Guide
(FXC19-DC-2000011-R1.0)

初版 2019 年 9 月

Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide
NS2010VPEL
Management Guide

FXC株式会社