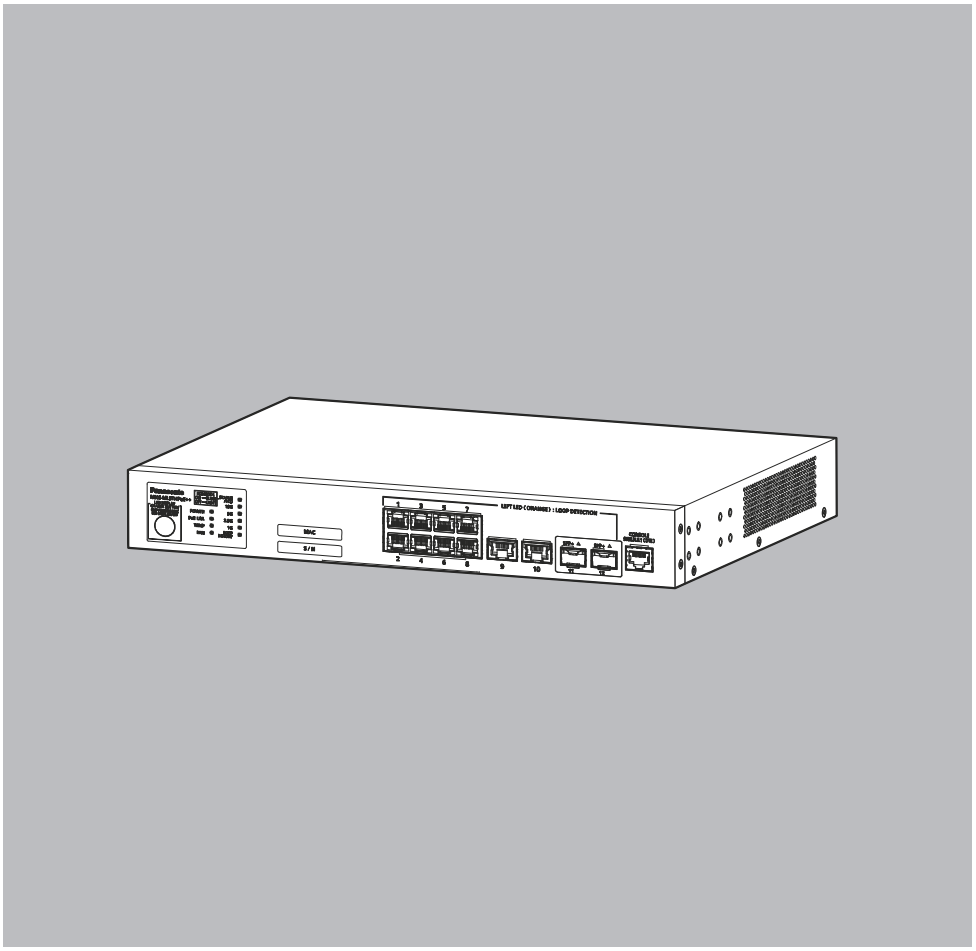
Panasonic

PoE 給電スイッチングハブ

WEB リファレンス

品番 ZLP290894



本 WEB リファレンスは、以下の機種を対象としております。

品名	品番	ファームウェアバージョン
MXG-ML8THPoE++	ZLP290894	1.0.0.00 以上

各機種の対応機能は、商品仕様書をご覧ください。

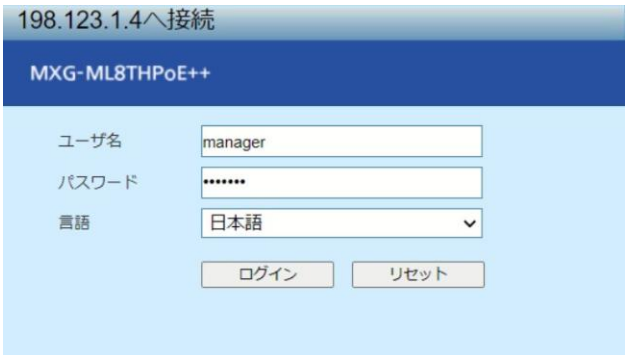
目次

1 はじめに

本装置は WEB で設定をすることが可能です。

- WEB 設定を使用する場合、本装置に事前に CLI コマンドで以下の設定が必要です。
  ① IP アドレスを設定（例：192.168.0.101）
  MXG-ML#configure terminal
  MXG-ML（config）#interface vlan 1
  MXG-ML（config-if）#ip address 192.168.0.101 255.255.255.0
  ② http サーバ機能の有効化
  MXG-ML（config）#ip http server

- WEB ブラウザに①で設定した IP アドレスを入力し、ユーザ名、パスワードを入力すると、本装置にログインできます。デフォルトのユーザ名とパスワードは「manager」です。



- 本リファレンスで使用している設定画面例は、実際の画面と異なる場合があります。

- 一部の画面は本リファレンスで説明していません。実際の画面の表示に従い、ご使用ください。

2 システム

2.1 デバイス情報

このウィンドウを用いて、一般的なスイッチ情報と使用率を表示します。

[MXG-ML8THPoE++] をクリックして、以下のウィンドウを表示します。

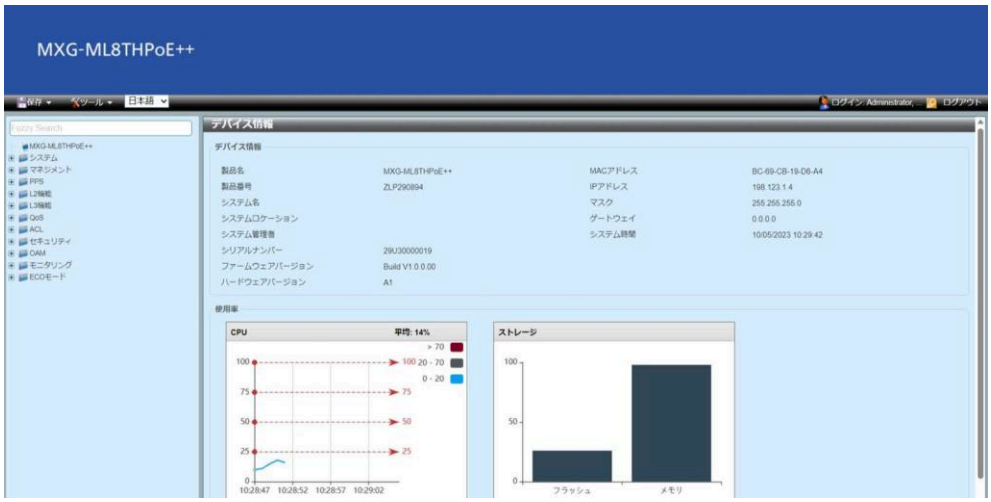


図 2-1 デバイス情報

2.2 システム情報設定

このウィンドウを用いて、システム情報の設定を行い、設定値を表示します。

[システム] > [システム情報設定] をクリックして、以下のウィンドウを表示します。

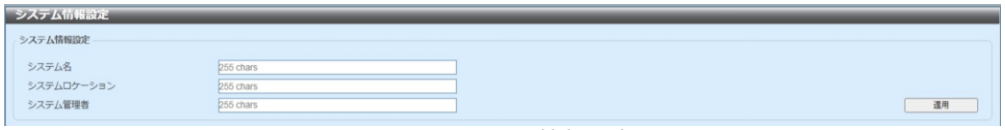


図 2-2 システム情報設定

設定パラメータ （[システム情報設定] セクション）

パラメータ	概要
システム名	スイッチのシステム名を入力します。この名前を用いて、ネットワーク内のスイッチを識別します。（最大：255 文字）
システムロケーション	スイッチの場所を入力します。（最大：255 文字）
システム管理者	スイッチの担当者名を入力します。一般に、スイッチの設定とメンテナンスを担当する人物または会社の名前となります。（最大：255 文字）

[**適用**] ボタン - 設定内容を反映します。

2.3 ポートコンフィグレーション

2.3.1 ポート設定

このウィンドウを用いて、スイッチのポート設定を行い、設定値を表示します。

[システム] > [ポートコンフィグレーション] > [ポート設定] をクリックして、以下のウィンドウを表示します。

図 2-3 **ポート設定**

設定パラメータ （[ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
メディアタイプ	ポートのメディアタイプ（**RJ45**/**SFP**）を選択します。
状態	ポートの状態（**Enabled**/**Disabled**）を選択します。
MDIX	MDIX（Medium Dependent Interface Crossover）のオプションを選択します。 • **Auto** - ケーブルの最適なタイプを自動的に感知します。 • **Normal** - 通常のケーブルの場合に選択します。このオプションを選択すると、ポートは MDIX モードになり、ストレートスルーケーブルで PC LAN アダプタに接続できます。あるいは、クロスオーバケーブルを使用して別のスイッチのポート（MDI モード）に接続できます。 • **Cross** - クロスオーバケーブルの場合に選択します。このオプションを選択すると、ポートは MDI モードになり、ストレートケーブルで別のスイッチのポート（MDIX モード）に接続できます。
フローコントロール	フローコントロール（**On**/**Off**）を選択します。 全二重に設定したポートでは 802.3x のフローコントロールを使用し、**自動**のポートでは 2 つのうち自動選択されたものを使用します。

パラメータ	概要
Duplex	使用する二重モード（**Auto**/**Half**/**Full**）を選択します。
スピード	ポートスピードのオプションを選択します。指定したスピードでのみ接続するよう、選択したポートに接続スピードを手動で強制設定します。 Master は二重通信、スピード、物理レイヤのタイプに関連する機能をポートでアドバタイズできるようになります。また、接続する 2 つの物理レイヤ間でのマスターとスレーブの関係も決定します。このマスターとスレーブの関係は、2 つの物理レイヤ間にタイミングコントロールを確立するうえで必要です。タイミングコントロールは、ローカルソースによってマスターの物理レイヤ上に設定されます。 Slave はループタイミングを用いています。この場合、タイミングはマスターから受信したデータストリームから得られます。1 つの接続をマスターに設定すると、もう一方の接続はスレーブに設定する必要があります。それ以外の設定を行うと、両方のポートで「リンクダウン」状態が発生します。 • **Auto** - 銅ポートの場合、オートネゴシエーションが開始して、スピードおよびフローコントロールをそのリンクパートナとネゴシエートします。ファイバポートの場合、オートネゴシエーションが開始して、クロックおよびフローコントロールをそのリンクパートナとネゴシエートします。 • **100M** - 100Mbps に強制します。（100Mbps の銅線接続にのみ利用できます） • **1000M** - 1000Mbps に強制します。（1Gbps のファイバ接続にのみ利用できます） • **1000M Master** - 1000MMbps に強制した上、Master として機能し送受信操作のタイミングを円滑にします。（1Gbps のファイバ接続にのみ利用できます） • **1000M Slave** - 1000MMbps に強制した上、Slave として機能し送受信操作のタイミングを円滑にします。（1Gbps のファイバ接続にのみ利用できます） • **2500M** - 2500Mbps に強制します。（2.5Gbps のファイバ接続にのみ利用できます） • **5000M** - 5000Mbps に強制します。（5Gbps のファイバ接続にのみ利用できます） • **10G** - 10Gbps に強制します。（10Gbps のファイバ接続にのみ利用できます）
アドバタイズ能力	([スピード] パラメータで [Auto] 選択時に設定可） オートネゴシエーション時にアドバタイズされる機能（**100M**/**1000M**/**10G**/**2500M**/**5000M**）を選択します。
説明	ポートの説明を入力します。（最大：64 文字）

[**適用**] ボタン - 設定内容を反映します。

2.3.2 ポート状態

このウィンドウを用いて、スイッチの物理ポートの状態および設定値を表示します。

[システム] > [ポートコンフィグレーション] > [ポート状態] をクリックして、以下のウィンドウを表示します。

図 2-4 ポート状態

2.3.3 ポート GBIC

このウィンドウを用いて、スイッチの物理ポートに接続されているトランシーバに関連する情報を表示します。GBIC は Gigabit Interface Converter の略です。

[システム] > [ポートコンフィグレーション] > [ポート GBIC] をクリックして、以下のウィンドウを表示します。

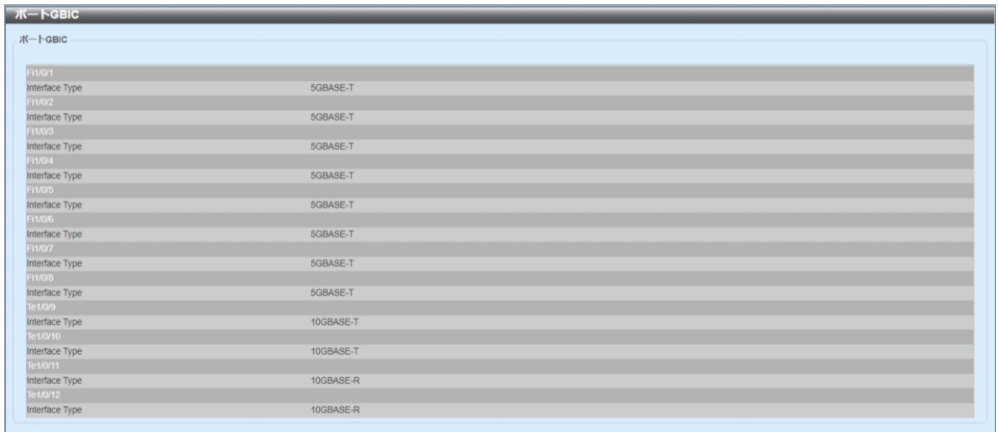


図 2-5 ポート GBIC

2.3.4 ポートオートネゴシエーション

このウィンドウを用いて、ポートのオートネゴシエーションテーブルおよび情報を表示します。

[システム] > [ポートコンフィグレーション] > [ポートオートネゴシエーション] をクリックして、以下のウィンドウを表示します。

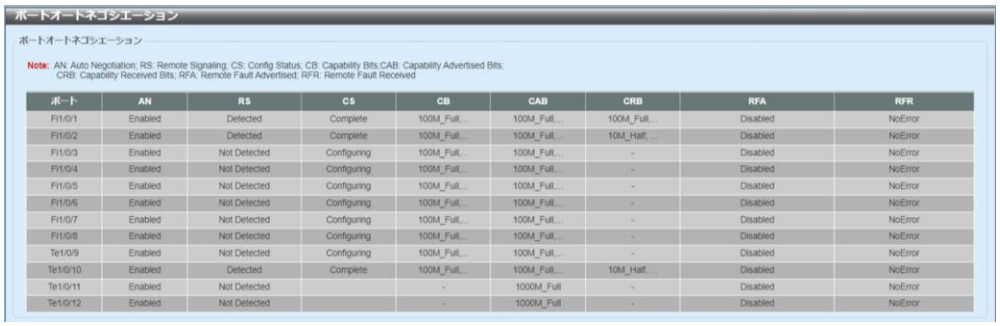


図 2-6 ポートオートネゴシエーション

2.3.5 Error Disable 設定

このウィンドウを用いて、Error Disable 機能に関連する設定を行い、設定値を表示します。

[システム] > [ポートコンフィグレーション] > [Error Disable 設定] をクリックして、以下のウィンドウを表示します。

図 2-7 Error Disable 設定

設定パラメータ （[Error Disable リカバリ設定] セクション）
原因毎に、エラー閉塞（Error Disabled）状態の自動復旧設定を行います。

パラメータ	概要
エラーディセーブル原因	設定対象のエラー閉塞（エラーディセーブル Error Disabled）原因を、**All** / **Port Security** / **Storm Control** / **BPDU Attack Protection** / **Dynamic ARP Inspection** / **DHCP Snooping** / **L2PT Guard** / **Detect UDL** から選択します。 - **All**：全ての原因を設定対象とする - **Port Security**：ポートセキュリティ違反 - **Storm Control** ：ストーム制御 - **BPDU Attack Protection**：BPDU ガード - **Dynamic ARP Inspection**：ARP レート制限 - **DHCP Snooping**：DHCP スヌーピング - **L2PT Guard**：L2PT ガード - **Detect UDL**：片方向リンク障害検知
状態	選択されたエラーディセーブル原因に対する自動復旧を有効化 / 無効化します。（**Disabled**：無効化、**Enabled**：有効化、デフォルト：**Disabled**）
間隔	選択されたエラーディセーブル原因によって生じたエラー閉塞状態からポートを自動復旧する迄の時間（秒）を入力します。（設定範囲：5 ～ 86400、デフォルト：300）

パラメータ	概要
（設定更新）	上記各パラメータ値の設定後、[適用] ボタンをクリックして、Error Disable リカバリ設定を更新します。
（Error Disable リカバリ設定一覧）	Error Disable リカバリ設定値をエラーディセーブル原因毎の一覧表形式で表示します。
エラーディセーブル原因	**All** / **Port Security** / **Storm Control** / **BPDU Attack Protection** / **Dynamic ARP Inspection** / **DHCP Snooping** / **L2PT Guard** / **Detect UDL**：エラー閉塞（Error Disabled）の原因を示します。
状態	**Enabled**（有効）/**Disabled**（無効）：エラーディセーブル原因に対する自動復旧の有効化 / 無効化状態を示します。
間隔	時間：原因によって生じるエラー閉塞状態からポートを復旧する時間（秒）を示します（範囲：5 ～ 86400）。
（自動復旧までの残時間一覧）	エラー閉塞中のインターフェースの自動復旧までの残時間をインターフェース毎の一覧形式で表示します。
インターフェース	インターフェース ID：エラー閉塞中のインターフェース（イーサネット物理ポート）。
エラーディセーブル原因	**All** / **Port Security** / **Storm Control** / **BPDU Attack Protection** / **Dynamic ARP Inspection** / **DHCP Snooping** / **L2PT Guard** / **Detect UDL**：エラー閉塞（Error Disabled）の原因を示します。
残り時間（秒）	残時間：原因によって生じるエラー閉塞状態からポートを自動復旧するまでの残時間（秒）を示します。 （範囲：0 ～ 86400）。

[**適用**] ボタン - 設定内容を反映します。

2.3.6 ジャンボフレーム

このウィンドウを用いて、ジャンボフレームの設定を行い、設定値を表示します。ジャンボフレームは、1518 バイト以上のペイロードを搭載するイーサネットフレームです。

[システム] > [ポートコンフィグレーション] > [ジャンボフレーム] をクリックして、以下のウィンドウを表示します。

図 2-8 ジャンボフレーム

設定パラメータ （[ジャンボフレーム] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
最大受信フレームサイズ	最大受信フレームサイズ値（バイト）を入力します。 （デフォルト：1518、設定範囲：64-9216）

[**適用**] ボタン - 設定内容を反映します。

2.4 PoE 設定

2.4.1 PoE グローバル設定

このウィンドウを用いて、PoE に関する装置共通の設定を行い、設定値を表示します。

[システム] >[PoE 設定] >[PoE グローバル設定] をクリックして、以下のウィンドウを表示します。

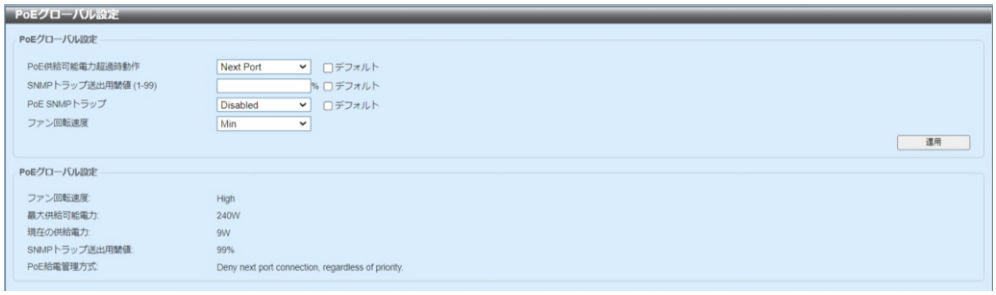


図 2-9 PoE グローバル設定

設定パラメータ （[PoE グローバル設定] セクション）

パラメータ	概要
PoE 供給可能電力超過時動作	給電電力が Power Budget を超えた際の電源給電の動作を選択します。（デフォルト：NextPort） • **Next Port** - 電源バジェットを超えた直前に接続されたポートの給電を停止します。 • **Low Priority** - 優先順位の一番低いポートの給電を停止します。優先順位が同じ場合はポート番号の大きいポートの給電が停止されます。
SNMP トラップ送出用量閾値	Trap を送信するための給電電力の閾値（%）を入力します。（デフォルト：50、設定範囲：1-99）
PoE SNMP トラップ	PoE 給電トラップを選択します。（デフォルト：Disabled）
ファン回転速度	供給できる給電電力とファン速度（**Min**/**Low2**/**Low1**/**High**）を選択します。 • **high** - 回転速度を高速に設定します。 • **low1** - 回転速度を低速に設定します。 • **low2** - 回転速度を低速に設定します。 • **min** - 回転を超低速に設定します。

[**適用**] ボタン - 設定内容を反映します。

2.4.2 PoE ポート設定

このウィンドウを用いて、ポート毎の給電設定を行います。

[システム] > [PoE] > [PoE ポート設定] をクリックして、以下のウィンドウを表示します。

図 2-10 PoE ポート設定

設定パラメータ （[PoE ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	PoE ポート状態（**Enabled**/**Disabled**）を選択します。
最大供給電力	給電電力の上限を入力します。 （デフォルト：オート、設定範囲：1000-95000）
優先度	給電の優先順位（**Critical**/**High**/**Low**）を選択します。 （デフォルト：Low）

[**適用**] ボタン - 設定内容を反映します。

2.4.3 PoE スケジューラポートリスト設定

このウィンドウを用いて、PoE スケジューラのポートリストの設定を行い、ポートリストの情報を表示します。

[システム] > [PoE 設定] > [PoE スケジューラポートリスト設定] をクリックして、以下のウィンドウを表示します。

図 2-11 PoE スケジュールポートリスト設定

設定パラメータ （[PoE スケジュールポートリスト設定] セクション）

パラメータ	概要
ポートリスト番号	ポートリストのインデックス番号を入力します。
ポートメンバー	動作させるポートを入力します。ポート番号はカンマ（,）区切り、またはハイフン（-）範囲指定します。

[**適用**] ボタン - 設定内容を反映します。

2.4.4 PoE スケジューラ日付リスト設定

このウィンドウを用いて、PoE スケジューラの日付リストの設定を行い、日付リストの情報を表示します。

[システム] > [PoE 設定] > [PoE スケジューラ日付リスト設定] をクリックして、以下のウィンドウを表示します。

図 2-12 PoE スケジューラ日付リスト設定

設定パラメータ （[PoE 日付リスト設定] セクション）

パラメータ	概要
日付リスト番号	日付リストのインデックス番号を入力します。 （設定範囲：1-65535）
日付リスト名	日付リストの名前を入力します。 （最大：30 文字）
年	日付リストが実行される年を入力します。 （設定範囲：2000-2099）
月日	日付リストが実行される月日（MM/DD）を入力します。

[**適用**] ボタン - 設定内容を反映します。

2.4.5 PoE スケジューラ設定

このウィンドウを用いて、PoE スケジューラの設定を行い、スケジュール情報を表示します。

[システム] > [PoE] > [PoE スケジューラ設定] をクリックして、以下のウィンドウを表示します。

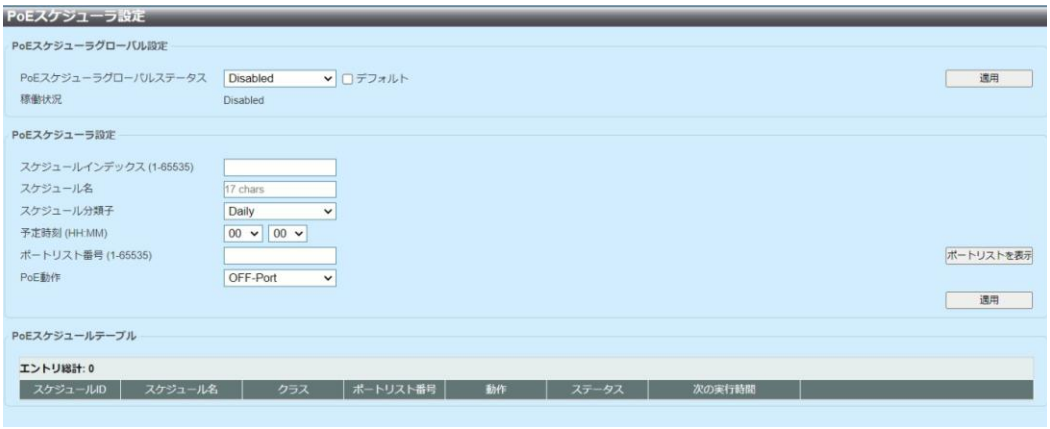


図 2-13 PoE スケジューラ設定

設定パラメータ （[PoE スケジューラグローバル設定] セクション）

パラメータ	概要
PoE スケジュールグローバルステータス	PoE スケジュール状態（**Enabled**/**Disabled**）を選択します。

設定パラメータ （[PoE スケジューラ設定] セクション）

パラメータ	概要
スケジュールインデックス	PoE スケジューラのインデックス番号を入力します。 （設定範囲：1-65535）
スケジュール名	PoE スケジュール名称を入力します。 （最大：17 文字）
スケジュール分類子	PoE スケジュールのクラス（**Daily**/**Weekly**/**Monthly**/**Date list**）を選択します。
予定時刻	PoE スケジュールの実行時刻を入力します。
ポートリスト番号	PoE スケジュールを実行するポートリスト番号を入力します。 （設定範囲：1-65535）
PoE 動作	PoE スケジュールアクション（**OFF-Port**/**ON-Port**/**OFF-ON-Port**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

2.4.6 PoE スケジュールポートリスト設定

このウィンドウを用いて、PoE スケジューラのポートリスト設定情報を表示します。

[システム] > [PoE 設定] > [PoE スケジュールポートリストの設定] をクリックして、以下のウィンドウを表示します。

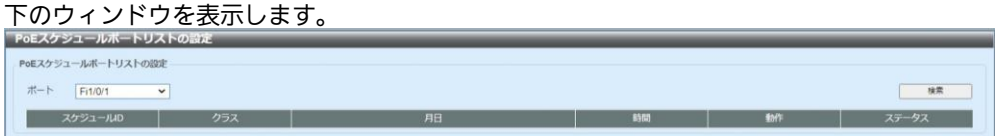


図 2-14 PoE スケジューラポートリストの設定

設定パラメータ （[PoE スケジューラポートリスト設定] セクション）

パラメータ	概要
ポート番号	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。

2.4.7 PoE オートリブート LLDP 監視設定

このウィンドウを用いて、PoE オートリブート LLDP 監視設定を行います。

[システム] > [PoE 設定] > [PoE オートリブート LLDP 監視設定] をクリックして、以下のウィンドウを表示します。

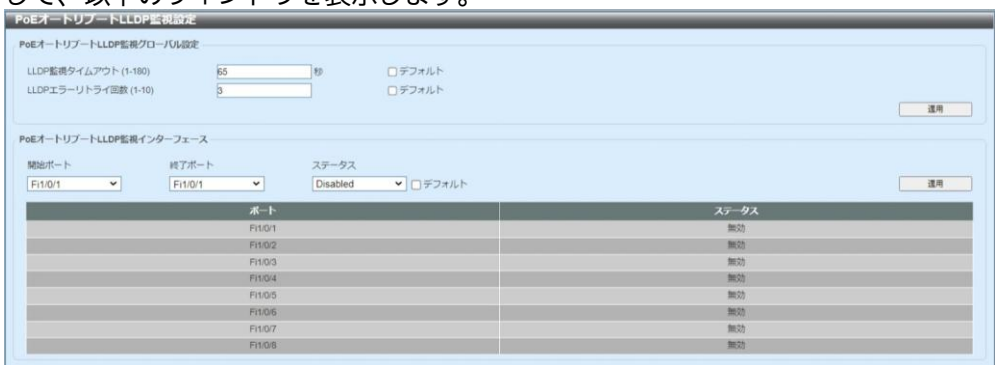


図 2-15 PoE スオートリブート LLDP 監視設定

設定パラメータ （[PoE オートリブート LLDP 監視グローバル設定] セクション）

パラメータ	概要
LLDP 監視タイムアウト	PoE オートリブートに使用するオートリブート LLDP 監視タイムアウト（秒）を入力します。 （デフォルト：65、設定範囲：1-180）
LLDP エラーリトライ回数	PoE オートリブートに使用するオートリブート LLDP 監視エラー時の再試行回数を入力します。 （デフォルト：3、設定範囲：1-10）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[PoE オートリブート LLDP 監視インタフェース] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
ステータス	PoE オートリブート LLDP 監視インタフェースの状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

2.4.8 PoE オートリブート Ping 監視設定

このウィンドウを用いて、PoE オートリブート Ping 監視設定を行います。

[システム] > [PoE] > [PoE オートリブート Ping 監視設定] をクリックして、以下のウィンドウを表示します。

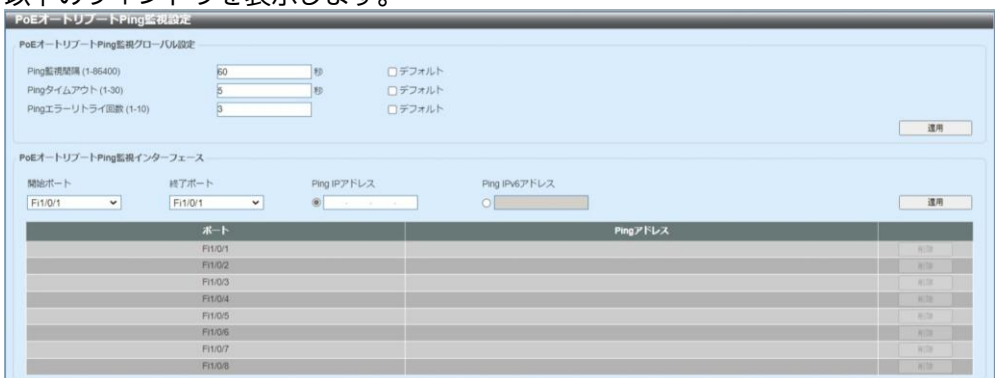


図 2-16 PoE オートリブート監視設定

設定パラメータ （[PoE オートリブート Ping 監視グローバル設定] セクション）

パラメータ	概要
Ping 監視間隔	PoE オートリブートでの Ping 監視 の間隔（秒）を入力します。（デフォルト：60、設定範囲：1-86400）
Ping タイムアウト	PoE オートリブートに使用する Ping 監視のタイムアウト（秒）を入力します。（デフォルト：5、設定範囲：1-30）
Ping エラーリトライ回数	PoE オートリブートに使用する Ping 監視のエラー発生時の再試行回数を入力します。（デフォルト：3、設定範囲：1-10）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[PoE オートリブート Ping 監視インタフェース] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
Ping IP アドレス	PoE オートリブートに使用する Ping の IP アドレスを入力します。
Ping IPv6 アドレス	PoE オートリブートに使用する Ping の IPv6 アドレスを入力します。

[**適用**] ボタン - 設定内容を反映します。

2.4.9 PoE オートリブートトラフィック監視設定

このウィンドウを用いて、PoE オートリブートトラフィック監視設定を行います。

[システム] > [PoE 設定] > [PoE オートリブートトラフィック監視設定] をクリックして、以下のウィンドウを表示します。

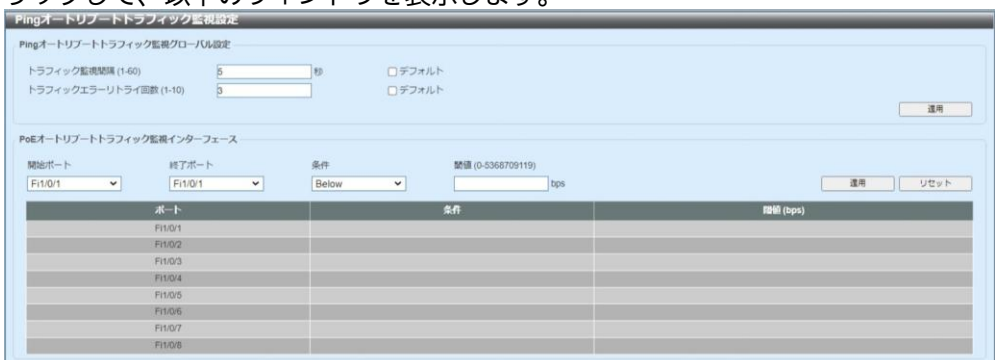


図 2-17 PoE スオートリブートトラフィック監視設定

設定パラメータ （[Ping オートリブートトラフィック監視グローバル設定] セクション）

パラメータ	概要
トラフィック監視間隔	トラフィック監視間隔（秒）を入力します。 （デフォルト：5、設定範囲：1-60）
トラフィックエラーリトライ回数	トラフィックエラー時の再試行回数を入力します。 （デフォルト：3、設定範囲：1-10）

[**適用**]ボタン - 設定内容を反映します。

設定パラメータ （[PoEオートリブートトラフィック監視インタフェース]セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
条件	通信料による PoE 端末異常判定（**Below**/**Over**）を選択します。
閾値	トラフィックの閾値（bps）を入力します。 （設定範囲：0-5368709119）

[**適用**]ボタン - 設定内容を反映します。

2.4.10 PoE オートリブート SMTP 設定

このウィンドウを用いて、PoE のオートリブート SMTP の設定を行います。
[システム] > [PoE 設定 **] > [PoE** オートリブート **SMTP** 設定 **]** をクリックして、以下のウィンドウを表示します。

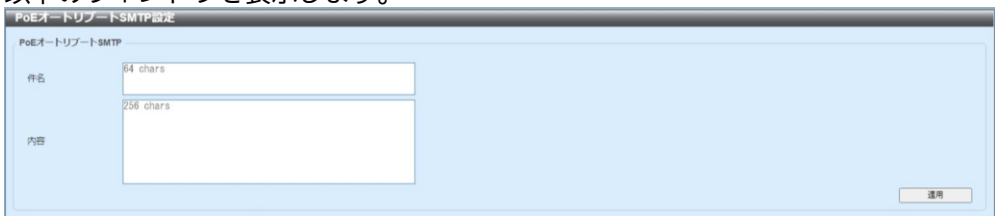


図 2-18 PoE オートリブート SMTP 設定

設定パラメータ （[PoE オートリブート SMTP 設定] セクション）

パラメータ	概要
件名	PoE オートリブートの SMTP によるメール通知を行う際の件名を入力します。（最大：64 文字）
内容	PoE オートリブートの SMTP によるメール通知を行う際の内容を入力します。 （最大：256 文字）

[**適用**]ボタン - 設定内容を反映します。

2.4.11 PoE オートリブートインターフェース設定

このウィンドウを用いて、PoE のオートリブートのインターフェースの設定を行います。

[システム] > [PoE 設定] > [PoE オートリブートインターフェース設定] をクリックして、以下のウィンドウを表示します。

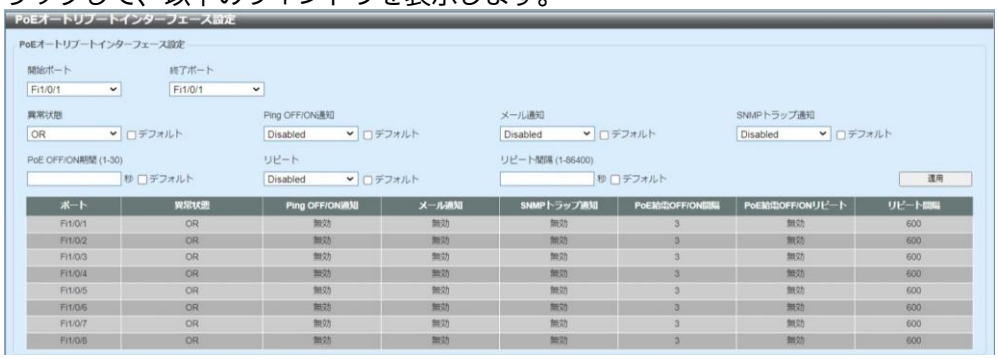


図 2-19 PoE オートリブートインターフェース設定

設定パラメータ （[PoE オートリブートインタフェース設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
異常状態	監視方式（Ping、LLDP、トラフィック）の異常判定を行うための条件（**OR**/**And**）を選択します。
Ping OFF/ON 通知	Ping OFF/ON 通知の状態（**Enabled**/**Disabled**）を選択します。（デフォルト：Disable）
メール通知	PoE オートリブートの Email 送信の状態（**Enabled**/**Disabled**）を選択します。（デフォルト：Disable）
SNMP トラップ通知	PoE オートリブートの SNMP トラップの状態（**Enabled**/**Disabled**）を選択します。（デフォルト：Disable）
PoE OFF/ON 期間	PoE オートリブート異常判定時の PoE 給電 OFF/ON 期間（秒）を入力します。（設定範囲：1-10）
リピート	PoE オートリブート異常判定時の PoE 給電 OFF/ON 繰り返し実行の状態（**Enabled**/**Disabled**）を選択します。
リピート間隔	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し間隔（秒）を入力します。（設定範囲：1-86400）

[**適用**] ボタン - 設定内容を反映します。

2.5 システムログ

2.5.1 システムログ設定

このウィンドウを用いて、システムログの設定を行い、設定値を表示します。

[システム] > [システムログ] > [システムログ設定] をクリックして、以下のウィンドウを表示します。

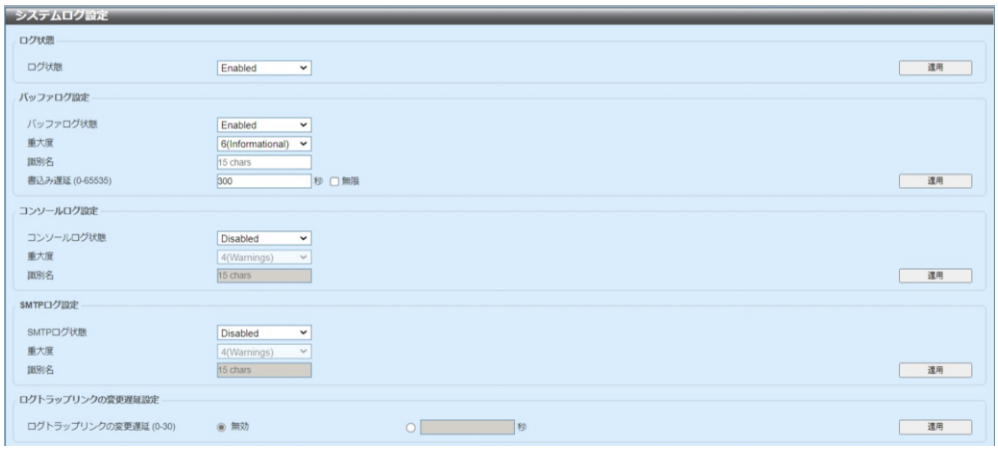


図 2-20 システムログ設定

設定パラメータ （[ログ状態] セクション）

パラメータ	概要
ログ状態	システムログ状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[バッファログ設定] セクション）

パラメータ	概要
バッファログ状態	バッファログ状態（**Enabled**/**Disabled**/**Default**）を選択します。
重大度	ログ記録する情報のタイプの重大度（**0**（**Emergencies**/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）]/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。
識別名	使用する識別名を入力します。ディスクリミネータプロファイルの名前を指定します。このプロファイルに規定したフィルタリング基準に基づき、バッファログメッセージがフィルタリングされます。（最大：15 文字）
書込み遅延	ログの書き込み遅延値（秒）を入力します。 [**無限**] オプションを選択した場合、書き込み遅延機能は無効になります。（デフォルト：300、設定範囲：0-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[コンソールログ設定] セクション）

パラメータ	概要
コンソールログ状態	コンソールログ状態（**Enabled**/**Disabled**/**Default**）を選択します。
重大度	ログ記録する情報のタイプの（**0**（**Emergencies**/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）]/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。
識別名	使用する識別名を入力します。ディスクリミネータプロファイルの名前を指定します。このプロファイルに規定したフィルタリング基準に基づき、コンソールログメッセージがフィルタリングされます。（最大：15 文字）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[SMTP ログ設定] セクション）

パラメータ	概要
SMTP ログ状態	SMTP ログ状態（**Enabled**/**Disabled**/**Default**）を選択します。
重大度	ログ記録する情報のタイプの重大度（**0**（**Emergencies**/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）]/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。
識別名	使用する識別名を入力します。ディスクリミネータプロファイルの名前を指定します。このプロファイルに規定したフィルタリング基準に基づき、SMTP ログメッセージがフィルタリングされます。（最大：15 文字）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ログトラップリンクの変更遅延設定] セクション）

パラメータ	概要
ログトラップリンクの変更遅延	物理ポートのリンク状態に関連するシステムログ及び SNMP トラップの発行遅延を有効にします。本製品でリンクアグリケーション使用時に物理ポートのリンク状態に関連するシステムログ及び SNMP トラップが、正常に送信できない場合は、本機能を使用することで問題を解決できることがあります。本機能を使用する場合の推奨値は 5 秒です。 （デフォルト：無効、設定範囲：0-30）

[**適用**] ボタン - 設定内容を反映します。

2.5.2 システムログ Discriminator 設定

このウィンドウを用いて、システムログで使用されるディスクリミネータの設定を行い、設定値を表示します。

[システム] > [システムログ] > [システムログ Discriminator 設定] をクリックして、以下のウィンドウを表示します。

図 2-21 システムログ Discriminator 設定

設定パラメータ （[識別ログ設定] セクション）

パラメータ	概要
識別名	ディスクリミネータプロファイルの名前を入力します。 （最大：15 文字）
アクション	選択した動作に関連付けるファシリティ動作オプションおよびファシリティのタイプ（**Drops**/**Includes**）を選択します。
重大度	ログ記録する情報タイプの動作オプション（**Drops**/**Includes**）と重大度（**0**（緊急）/**1**（アラート）/**2**（クリティカル）/**3**（エラー）]/**4**（警告）/**5**（通知）/**6**（情報）/**7**（デバッギング））を選択します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

2.5.3 システムログサーバ設定

このウィンドウを用いて、システムログで使用されるサーバの設定を行い、設定値を表示します。

[システム] > [システムログ] > [システムログサーバ設定] をクリックして、以下のウィンドウを表示します。

図 2-22 システムログサーバ設定

設定パラメータ （[ログサーバ設定] セクション）

パラメータ	概要
ホスト IPv4 アドレス	システムログサーバの IPv4 アドレスを入力します。
ホスト IPv6 アドレス	システムログサーバの IPv6 アドレスを入力します。
UDP ポート	システムログサーバの UDP ポート番号を入力します。 （デフォルト：514、設定範囲：514,1024-65535）
重大度	ログ記録する情報のタイプの重大度（**0**（**Emergencies**/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）]/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。

<table>
<tr><th>パラメータ</th><th colspan="3">概要</th></tr>
<tr><td>ファシリティ</td><td colspan="3">ログ記録するファシリティ番号を選択します。ファシリティ番号はそれぞれ特定のファシリティに関連付けられています。</td></tr>
<tr><td></td><td>ファシリティ番号</td><td>ファシリティ名</td><td>ファシリティの概要説明</td></tr>
<tr><td></td><td>1</td><td>user</td><td>ユーザレベルメッセージ</td></tr>
<tr><td></td><td>2</td><td>mail</td><td>メールシステム</td></tr>
<tr><td></td><td>3</td><td>daemon</td><td>システムデーモン</td></tr>
<tr><td></td><td>4</td><td>auth1</td><td>セキュリティ / 認証メッセージ</td></tr>
<tr><td></td><td>5</td><td>syslog</td><td>SYSLOG によって内部的に生成されるメッセージ</td></tr>
<tr><td></td><td>6</td><td>lpr</td><td>ラインプリンタサブシステム</td></tr>
<tr><td></td><td>7</td><td>news</td><td>ネットワークニュースサブシステム</td></tr>
<tr><td></td><td>8</td><td>uucp</td><td>UUCP サブシステム</td></tr>
<tr><td></td><td>9</td><td>clock1</td><td>クロックデーモン</td></tr>
<tr><td></td><td>10</td><td>auth2</td><td>セキュリティ / 認証メッセージ</td></tr>
<tr><td></td><td>11</td><td>ftp</td><td>FTP デーモン</td></tr>
<tr><td></td><td>12</td><td>ntp</td><td>NTP サブシステム</td></tr>
<tr><td></td><td>13</td><td>logaudit</td><td>ログ監査</td></tr>
<tr><td></td><td>14</td><td>logalert</td><td>ログアラート</td></tr>
<tr><td></td><td>15</td><td>clock2</td><td>クロックデーモン</td></tr>
<tr><td></td><td>16</td><td>local0</td><td>ローカル使用 0（local0）</td></tr>
<tr><td></td><td>17</td><td>local1</td><td>ローカル使用 1（local1）</td></tr>
<tr><td></td><td>18</td><td>local2</td><td>ローカル使用 2（local2）</td></tr>
<tr><td></td><td>19</td><td>local3</td><td>ローカル使用 3（local3）</td></tr>
<tr><td></td><td>20</td><td>local4</td><td>ローカル使用 4（local4）</td></tr>
<tr><td></td><td>21</td><td>local5</td><td>ローカル使用 5（local5）</td></tr>
<tr><td></td><td>22</td><td>local6</td><td>ローカル使用 6（local6）</td></tr>
<tr><td></td><td>23</td><td>local7</td><td>ローカル使用 7（local7）</td></tr>
<tr><td>識別名</td><td colspan="3">ログサーバに送信されるメッセージのフィルタリングに使用する、ディスクリミネータの名前を入力します。
（最大：15 文字）</td></tr>
</table>

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

2.5.4 システムログ

このウィンドウを用いて、システムログを表示およびクリアします。

[システム] > [システムログ] > [システムログ] をクリックして、以下のウィンドウを表示します。

図 2-23 システムログ

[ログクリア] ボタン - ログエントリをクリアします。

2.5.5 システムアタックログ

このウィンドウを用いて、システムアタックログを表示およびクリアします。

[システム] > [システムログ] > [システムアタックログ] をクリックして、以下のウィンドウを表示します。

図 2-24 システムアタックログ

[アタックログクリア] ボタン - アタックログエントリをクリアします。

2.5.6 システム認証ログ

このウィンドウを用いて、システム認証ログの設定を行い、設定値を表示します。

[システム] > [システムログ] > [システム認証ログ] をクリックして、以下のウィンドウを表示します。

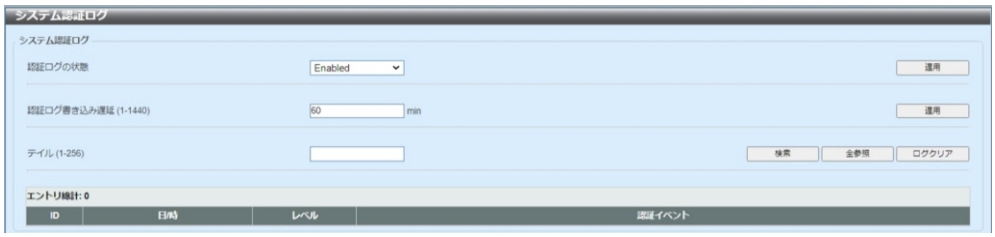


図 2-25 システム認証ログ

設定パラメータ （[システム認証ログ] セクション）

パラメータ	概要
認証ログの状態	認証ログ状態（**Enabled**/**Disabled**）を選択します。
認証ログ書き込み遅延	認証ログの書き込み遅延値（分）を入力します。 （設定範囲：1-1440）
テイル	表示する最新の認証ログエントリの数を入力します。 （設定範囲：1-256）

[**適用**] ボタン - 設定内容を反映します。
[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**ログクリア**] ボタン - ログエントリをクリアします。

2.6 時間と SNTP（Simple Network Time Protocol）

2.6.1 時刻設定

このウィンドウを用いて、スイッチの時間依存機能で使用される日時の設定を行い、設定値を表示します。

[システム] > [時間と SNTP] > [時刻設定] をクリックして、以下のウィンドウを表示します。

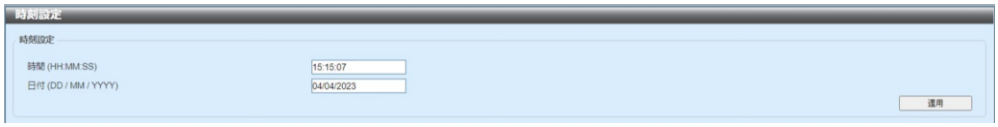


図 2-26 時刻設定

設定パラメータ （[時刻設定] セクション）

パラメータ	概要
時間	現在の時刻を時（HH）：分（MM）：秒（SS）で入力します。（例：19：20：20）
日付	現在の日（DD）：月（MM）：年（YYYY）を入力します。（例：25/04/2017）

[**適用**] ボタン - 設定内容を反映します。

2.6.2 タイムゾーン設定

このウィンドウを用いて、DST（サマータイム）およびタイムゾーンの設定を行い、設定値を表示します。

[システム] > [時間と SNTP] > [タイムゾーン設定] をクリックして、以下のウィンドウを表示します。

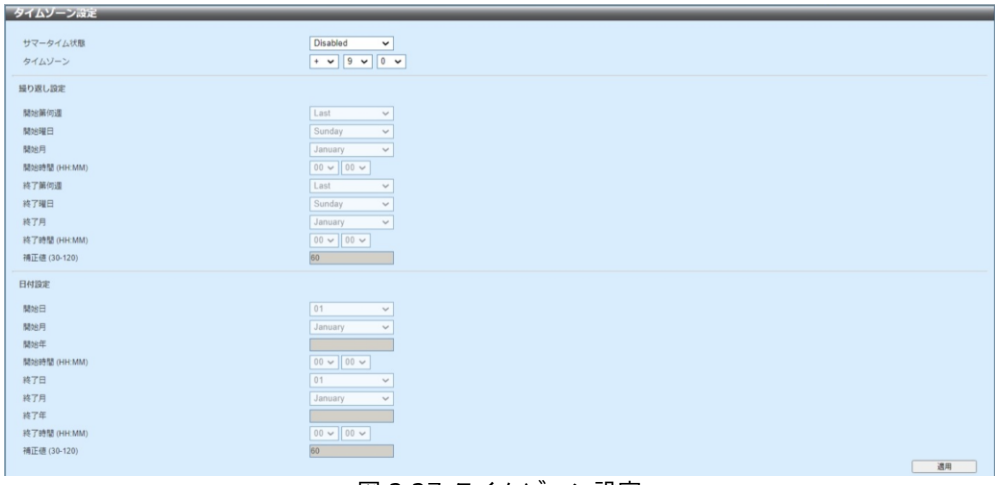


図 2-27 タイムゾーン設定

設定パラメータ

パラメータ	概要
サマータイム状態	サマータイムの設定を選択します。 • **Disabled** - サマータイム設定を無効にします。 • **Recurring Setting** - 指定した月の指定した曜日にサマータイムが開始および終了するよう設定します。 • **Date Setting** - 指定した月の指定した日にサマータイムが開始および終了するよう設定します。
タイムゾーン	UTC（協定世界時）からのローカルタイムゾーンのオフセットを選択します。

設定パラメータ （[繰り返し設定] セクション）

パラメータ	概要
開始第何週	サマータイムが開始する週を選択します。
開始曜日	サマータイムが開始する曜日を選択します。
開始月	サマータイムが開始する月を選択します。
開始時間	サマータイムが開始する時間を選択します。
終了第何週	サマータイムが終了する週を選択します。
終了曜日	サマータイムが終了する曜日を選択します
終了月	サマータイムが終了する月を選択します。
終了時間	サマータイムが終了する時間を選択します。

パラメータ	概要
補正値	サマータイム期間に加算する時間を分単位で入力します。 オフセットの範囲は 30、60、90、120 です。 （デフォルト：60、設定範囲：30-120）

設定パラメータ （[日付設定] セクション）

パラメータ	概要
開始日	サマータイムが開始する日を選択します。
開始月	サマータイムが開始する月を選択します。
開始年	サマータイムが開始する年を入力します。
開始時間	サマータイムが開始する時間を選択します。
終了日	サマータイムが終了する日を選択します。
終了月	サマータイムが終了する月を選択します。
終了年	サマータイムが終了する年を入力します。
終了時間	サマータイムが終了する時間を選択します。
補正値	サマータイム期間に加算する時間を分単位で入力します。 オフセットの範囲は 30、60、90、120 です。 （デフォルト：60、設定範囲：30-120）

[**適用**] ボタン - 設定内容を反映します。

2.6.3 SNTP 設定

このウィンドウを用いて、SNTP（Simple Network Time Protocol）の設定を行い、設定値を表示します。SNTP を用いて、スイッチの日時設定と SNTP サーバによってホストされる設定との間で、自動的かつ周期的に同期を取ります。

[システム] > [時間と SNTP] > [SNTP 設定] をクリックして、以下のウィンドウを表示します。

図 2-28 SNTP 設定

設定パラメータ （[SNTP グローバル設定] セクション）

パラメータ	概要
SNTP 状態	SNTP 状態（**Enabled**/**Disabled**）を選択します。
ポール間隔	同期間隔（秒）を入力します。 （デフォルト：720、設定範囲：30-99999）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[SNTP サーバ設定] セクション）

パラメータ	概要
IPv4 アドレス	SNTP サーバの IPv4 アドレスを入力します。
IPv6 アドレス	SNTP サーバの IPv6 アドレスを入力します。

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

2.7 時間範囲

このウィンドウを用いて、タイムレンジプロファイルの設定を行い、設定値を表示します。

[システム] > [時間範囲] をクリックして、以下のウィンドウを表示します。

図 2-29 時間範囲

設定パラメータ （[時間範囲] セクション）

パラメータ	概要
範囲名	タイムレンジプロファイルの名前を入力します。 （最大：32 文字）
From：週 ~To：週	このタイムプロファイルに使用する開始曜日と終了曜日を選択します。**[日毎]** オプションをオンにした場合、すべての曜日にこのタイムプロファイルを使用します。**[最終週日]** オプションをオンにした場合、週の開始曜日から週の末日までこのタイムプロファイルを使用します。
開始時間 ~ 終了時間	このタイムプロファイルに使用する開始時刻と終了時刻を選択します。1 つ目（左側）のドロップダウンメニューで時間を選択し、2 つ目（右側）のドロップダウンメニューで分を選択します。

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[全参照] ボタン - エントリをすべて表示します。
[**周期削除**] ボタン - 周期エントリを削除します。
[**削除**] ボタン - エントリを削除します。

2.8 PTP（Precision Time Protocol）

PTP（Precision Time Protocol）は、マイクロ秒（百万分の一秒）単位の高精度な時刻同期を実現する機能です。この機能を用いて、パケットベースネットワークで時刻同期させることが可能です。

ご注意

- End to End（E2E）の Transparent Clock（TC）モードのみ対応しています。
- グローバルコンフィグレーションモードの PTP 設定とインターフェースコンフィグレーションモードの PTP 設定の両方を有効にする必要があります。
- 本機能はシステム内の他装置と連携して端末に要求される時刻同期を保証します。本機種・本機能のみで時刻同期を保証するものではありません。事前にシステム検証を行う必要があります。

2.8.1 PTP 設定

このウィンドウを用いて、PTP 機能の設定を行い、設定値を表示します。

[システム] > [**PTP**] > [**PTP 設定**] をクリックして、以下のウィンドウを表示します。

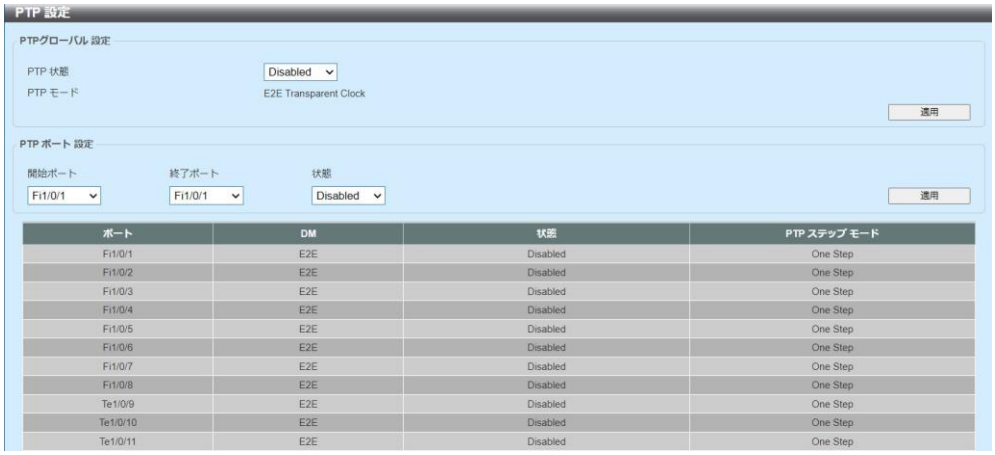


図 2-30 PTP 設定

設定パラメータ （[PTP グローバル設定] セクション）

パラメータ	概要
PTP 状態	PTP 機能の状態（**Enabled**/**Disabled**）を選択します。

設定パラメータ （[PTP ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	使用するポートを選択します。
状態	指定したポートの PTP 機能の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3 マネジメント

3.1 コマンドログ収集コマンド

このウィンドウを用いて、コマンドログ収集機能を有効または無効にします。この機能を用いて、CLI コマンドをログ記録します。スイッチの設定を変更しなかったコマンドはログ記録されません。

[マネジメント] > [コマンドログ収集コマンド] をクリックして、以下のウィンドウを表示します。

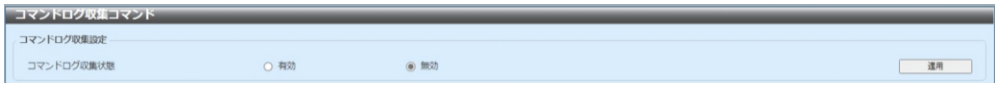


図 3-1 コマンドログ収集コマンド

設定パラメータ （[コマンドログ収集設定] セクション）

パラメータ	概要
コマンドログ収集状態	コマンドログ収集の状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3.2 ユーザアカウント設定

このウィンドウを用いて、ユーザアカウントの設定を行い、設定値を表示します。このユーザアカウントを用いて、スイッチのソフトウェア設定にログインします。

[マネジメント] > [ユーザアカウント設定] をクリックして、以下のウィンドウを表示します。

図 3-2 ユーザアカウント設定（ユーザマネジメント設定）

設定パラメータ （[ユーザマネジメント設定] タブ）

パラメータ	概要
ユーザ名	ユーザアカウント名を入力します。（最大：32 文字）
特権レベル	アカウントの特権レベルを入力します。（設定範囲：1-15）
パスワードタイプ	ユーザアカウントのパスワードタイプ（**None**/**Plain Text**/**Encrypted--SHA1**）を選択します。
パスワード	([パスワードタイプ] パラメータで [Plain Text]、または [Encrypted-SHA1] 選択時に設定可) ユーザアカウントのパスワードを入力します。

[**適用**] ボタン - エントリを追加します。

[セッションテーブル] タブをクリックして、セッションテーブルを表示します。

図 3-3 ユーザアカウント設定（セッションテーブル）

3.3 ユーザアカウント暗号化

このウィンドウを用いて、ユーザアカウントの暗号化を有効または無効にします。

[マネジメント] > [ユーザアカウント暗号化] をクリックして、以下のウィンドウを表示します。

図 3-4 ユーザアカウント暗号化

設定パラメータ （[ユーザアカウント暗号化] セクション）

パラメータ	概要
ユーザアカウント暗号化状態	ユーザアカウント暗号化状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3.4 ログイン方式

このウィンドウを用いて、スイッチでサポートされている各ログインアプリケーションのログイン方法を設定し、表示します。

[マネジメント] > [ログイン方式] をクリックして、以下のウィンドウを表示します。

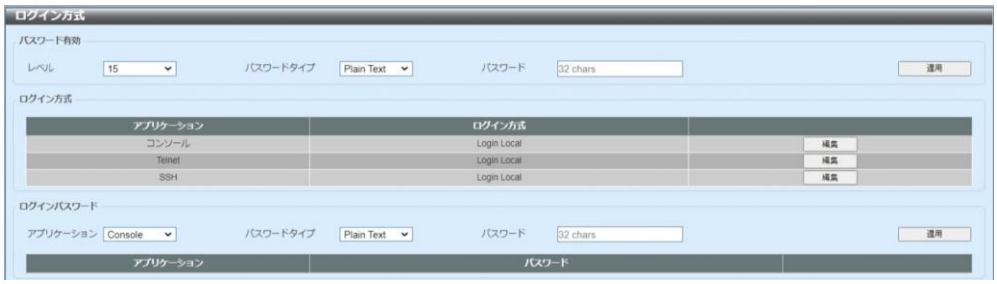


図 3-5 ログイン方式

設定パラメータ （[パスワード有効] セクション）

パラメータ	概要
レベル	ユーザアカウントの特権レベル（**1 ～ 15**）を選択します。
パスワードタイプ	ユーザのパスワードタイプを選択します。 （デフォルト：Plain Text） • **Plain Text** - プレーンテキスト形式にします。 • **Encrypted** - SHA-1 に基づいてパスワードを暗号化します。
パスワード	ユーザアカウントのパスワードを入力します。 • **Plain Text** の場合 - 大文字と小文字は区別され、スペースを含めることができます。（最大：32 文字） • **Encrypted** の場合 - 大文字と小文字は区別されます。（最大：35 文字）

[**適用**] ボタン - 設定内容を反映します。
[**編集**] ボタン - エントリの設定を編集できます。

設定パラメータ （[編集]>[ログイン方式] セクション）

パラメータ	概要
ログイン方式	指定したアプリケーションのログイン方式を選択します。 • **No Login** - 指定したアプリケーションへのアクセスにログイン認証は必要ありません。 • **Login** - 指定したアプリケーションにアクセスしようとするとパスワードの入力を求められます。 • **Login Local** - 指定したアプリケーションにアクセスするために、ユーザ名とパスワードの入力を求められます。

設定パラメータ （[ログインパスワード] セクション）

パラメータ	概要
アプリケーション	設定するアプリケーション（**Console**/**Telnet**/**SSH**）を選択します。
パスワードタイプ	使用するパスワード暗号化タイプ（**Plain Text**/**Encrypted**）を選択します。
パスワード	([ログイン方式] パラメータで [Login] 選択時に設定可) 選択したアプリケーションのパスワードを入力します。 • **Plain Text -** 大文字と小文字は区別され、スペースを含めることができます。（最大：32 文字） • **Encrypted -** 大文字と小文字は区別されます。 • （最大：35 文字）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

3.5 SNMP（Simple Network Management Protocol）

3.5.1 SNMP グローバル設定

このウィンドウを用いて、グローバル SNMP 設定を行い、設定値を表示します。

[マネジメント] > [SNMP] > [SNMP グローバル設定] をクリックして、以下のウィンドウを表示します。

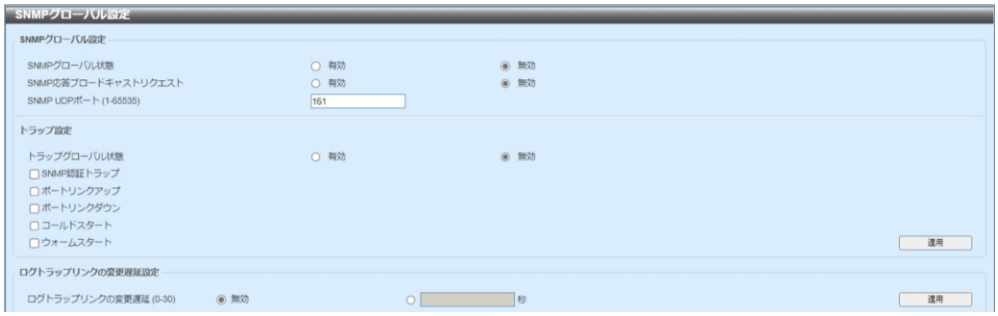


図 3-6 SNMP グローバル設定

設定パラメータ （[SNMP グローバル設定] セクション）

パラメータ	概要
SNMP グローバル状態	SNMP の状態（**有効** / **無効**）を選択します。
SNMP 応答ブロードキャストリクエスト	サーバによるブロードキャスト SNMP GetRequest パケットへの応答の状態（**有効** / **無効**）を選択します。
SNMP UDP ポート	SNMP UDP ポート番号を入力します。（設定範囲：1-65535）

設定パラメータ （[トラップ設定] セクション）

パラメータ	概要
トラップグローバル状態	すべてまたは特定の SNMP 通知の送信の状態（**有効** / **無効**）を選択します。
SNMP 認証トラップ	このオプションを選択した場合、SNMP 認証失敗通知の送信を制御します。正しく認証されていない SNMP メッセージを装置が受信すると、authenticationFailuretrap トラップが生成されます。認証方式は、使用されている SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、パケットに不正なコミュニティ文字列があると認証は失敗します。SNMPv3 の場合、パケットに不正な SHA/MD5 認証キーがあると認証は失敗します。

パラメータ	概要
ポートリンクアップ	このオプションを選択した場合、ポートリンクアップ通知の送信を制御します。通信リンクの 1 つがアップ状態にあると装置が認識すると、linkUp トラップが生成されます。
ポートリンクダウン	このオプションを選択した場合、ポートリンクダウン通知の送信を制御します。通信リンクの 1 つがダウン状態にあると装置が認識すると、linkDown トラップが生成されます。
コールドスタート	このオプションを選択した場合、SNMP コールドスタート通知の送信を制御します。
ウォームスタート	このオプションを選択した場合、SNMP ウォームスタート通知の送信を制御します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ログトラップリンクの変更遅延設定] セクション）

パラメータ	概要
ログトラップリンクの変更遅延	物理ポートのリンク状態に関連するシステムログ及び SNMP トラップの発行遅延を有効にします。範囲は、0 ～ 30 秒です。本製品でリンクアグリケーション使用時に物理ポートのリンク状態に関連するシステムログ及び SNMP トラップが、正常に送信できない場合は、本機能を使用することで問題を解決できることがあります。推奨値は 5 秒です。 （デフォルト：無効）

[**適用**] ボタン - 設定内容を反映します。

3.5.2 SNMP リンクチェンジトラップ設定

このウィンドウを用いて、SNMP Linkchange トラップの設定を行い、設定値を表示します。

[マネジメント] > [SNMP] > [SNMP リンクチェンジトラップ設定] をクリックして、以下のウィンドウを表示します。

図 3-7 SNMP リンクチェンジトラップ設定

設定パラメータ （[SNMP リンクチェンジトラップ設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
トラップ送信	システムによって生成された SNMP 通知トラップ送信の状態（**Enabled**/**Disabled**）を選択します。
トラップ状態	SNMP linkChange トラップの状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3.5.3 SNMP ビューテーブル設定

このウィンドウを用いて、SNMP ビューテーブルの設定を行い、設定値を表示します。この SNMP ビューエントリで、リモート SNMP マネージャがアクセス可能な MIB（Management Information Base）オブジェクトを定義します。SNMP Subtree OID（オブジェクト識別子）によって、SNMP ユーザを SNMP ビューにマッピングします。

[マネジメント] > [SNMP] > [SNMP ビューテーブル設定] をクリックして、以下のウィンドウを表示します。

図 3-8 SNMP ビューテーブル設定

設定パラメータ （[SNMP ビュー設定] セクション）

パラメータ	概要
ビュー名	SNMP ビュー名を入力します。このビュー名で、作成中の新しい SNMP ビューを識別します。（最大：32 文字）
サブツリー OID	ビューのサブツリー OID を入力します。OID は、SNMP マネージャによるアクセスに含まれる、またはアクセスから除外されるオブジェクトツリー（MIB ツリー）を識別します。
ビュータイプ	ビュータイプを選択します。 • **Included** - SNMP マネージャがアクセス可能なオブジェクトのリストに、このオブジェクトを含めます。 • **Excluded** - SNMP マネージャがアクセス可能なオブジェクトのリストから、このオブジェクトを除外します。

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

3.5.4 SNMP コミュニティテーブル設定

このウィンドウを用いて、SNMP マネージャと SNMP エージェントとの関係を定義する SNMP コミュニティ文字列の設定を行い、設定値を表示します。
SNMP コミュニティ文字列はパスワードのように機能して、スイッチの SNMP エージェントへのアクセスを許可します。
コミュニティ文字列には、以下の機能を関連付けることができます。

- SNMP マネージャの IP アドレスを掲載したアクセスリスト。SNMP マネージャは、コミュニティ文字列を使用して、スイッチの SNMP エージェントにアクセスすることが許可されています。
- MIB ビュー。SNMP コミュニティにアクセス可能な MIB オブジェクトのサブセットが定義されています。
- リードライトまたはリードオンリー権限。SNMP コミュニティにアクセス可能な MIB オブジェクトに対する権限です。

[マネジメント] > [SNMP] > [SNMP コミュニティテーブル設定] をクリックして、以下のウィンドウを表示します。

図 3-9 SNMP コミュニティテーブル設定

設定パラメータ （[SNMP コミュニティ設定] セクション）

パラメータ	概要
キータイプ	SNMP コミュニティのキータイプ（**Plain Text**/ **Encrypted**）を選択します。
コミュニティ名	SNMP コミュニティ名を入力します。このコミュニティ名で、SNMP コミュニティのメンバを識別します。この文字列は、スイッチの SNMP エージェントにある MIB オブジェクトに、リモート SNMP マネージャがアクセスするためのパスワードのように使用されます。（最大：32 文字）
ビュー名	SNMP ビュー名を入力します。このビュー名を用いて、リモート SNMP マネージャがスイッチでアクセスを許可されている MIB オブジェクトのグループを識別します。ビュー名は、SNMP ビューテーブルに存在している必要があります。（最大：32 文字）

パラメータ	概要
アクセス権	アクセス権を選択します。 • **Read Only** - 作成済みのコミュニティ文字列を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみできます。 • **Read Write** - 作成済みのコミュニティ文字列を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りと書き込みができます。
IP アクセスリスト名	このコミュニティ文字列を用いて SNMP エージェントにアクセス可能なユーザを制限する、標準アクセスリストの名前を入力します。

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

3.5.5 SNMP グループテーブル設定

このウィンドウを用いて、SNMP グループテーブルの設定を行い、設定値を表示します。SNMP グループは SNMP ユーザを SNMP ビューにマッピングします。

[マネジメント] > [SNMP] > [SNMP グループテーブル設定] をクリックして、以下のウィンドウを表示します。

図 3-10 SNMP グループテーブル設定

設定パラメータ （[SNMP グループ設定] セクション）

パラメータ	概要
グループ名	SNMP グループ名を入力します。（最大：32 文字）
リードビュー名	グループのユーザがアクセスできるリードビュー名を入力します。
ユーザベース セキュリティモデル	セキュリティモデルを選択します。 • **SNMPv1** - グループに SNMPv1 セキュリティモデルの使用を許可します。 • **SNMPv2c** - グループに SNMPv2c セキュリティモデルの使用を許可します。 • **SNMPv3** - グループに SNMPv3 セキュリティモデルの使用を許可します。
書込みビュー名	グループのユーザがアクセスできる書き込みビュー名を入力します。（最大：32 文字）
セキュリティレベル	([ユーザベースセキュリティモデル] で [SNMPv3] を選択時に設定可） セキュリティレベルを選択します。 • **NoAuthNoPriv** - 認証が行われず、スイッチとリモート SNMP マネージャとの間で送信されるパケットの暗号化も行われません。 • **AuthNoPriv** - 認証は必要ですが、スイッチとリモート SNMP マネージャとの間で送信されるパケットの暗号化は行われません。 • **AuthPriv** - 認証が必要で、スイッチとリモート SNMP マネージャとの間で送信されるパケットの暗号化も行われます。

パラメータ	概要
通知ビュー名	グループのユーザがアクセスできる通知ビュー名を入力します。通知ビューは、トラップパケットを通じて状態をグループユーザに報告できるオブジェクトを記述します。 (最大：32 文字)
IP アドレスリスト名	グループに関連付ける標準 IP ACL を入力します。 (最大：32 文字)

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

3.5.6 SNMP エンジン ID ローカル設定

このウィンドウを用いて、ローカル SNMP エンジン ID を設定し、表示します。エンジン ID はスイッチ固有であり、SNMPv3（SNMP バージョン 3）の実装で使用されます。

[マネジメント] > [SNMP] > [SNMP エンジン ID ローカル設定] をクリックして、以下のウィンドウを表示します。

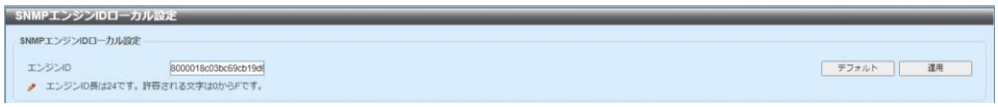


図 3-11 SNMP エンジン ID ローカル設定

設定パラメータ （[SNMP エンジン ID ローカル設定] セクション）

パラメータ	概要
エンジン ID	SNMP エンジン ID の文字列を入力します。（最大：24 文字）

[**デフォルト**] ボタン - デフォルトのエンジン ID を使用します。
[**適用**] ボタン - 設定内容を反映します。

3.5.7 SNMP ユーザテーブル設定

このウィンドウを用いて、SNMP ユーザの設定を行い、設定値を表示します。

[マネジメント] > [SNMP] > [SNMP ユーザテーブル設定] をクリックして、以下のウィンドウを表示します。

図 3-12 SNMP ユーザテーブル設定

設定パラメータ （[SNMP ユーザ設定] セクション）

パラメータ	概要
ユーザ名	SNMP ユーザ名を入力します。このユーザ名を用いて、SNMP ユーザを識別します。（最大：32 文字）
グループ名	ユーザの SNMP グループ名を入力します。スペースは使用できません。（最大：32 文字）
SNMP バージョン	SNMP バージョン（**v1**/**v2c**/**v3**）を選択します。
SNMP v3 暗号化	([SNMP バージョン] で [v3] 選択時に設定可) SNMPv3 の暗号化タイプ（**None**/**Password**/**Key**）を選択します。
パスワード認証 - プロトコル	([SNMPv3 暗号化] で [Password] 選択時に設定可) パスワードの認証プロトコルを選択します。 • **MD5** - HMAC-MD5-96 認証レベルを使用します。このフィールドにはパスワードまたはキーを入力する必要があります。 • **SHA** - HMAC-SHA 認証プロトコルを使用します。このフィールドにはパスワードまたはキーを入力する必要があります。
パスワード	認証プロトコルのパスワードを入力します。 • **MD5** - パスワードは 8 ～ 16 文字です。 • **SHA** - パスワードは 8 ～ 20 文字です。

パラメータ	概要
パスワードによるプライバシープロトコル	([SNMPv3 暗号化] で [Password] 選択時に設定可) パスワードのプライベートプロトコルを選択します。 • **None** - 認証プロトコルを使用しません。 • **DES56** - DES（データ暗号化標準規格）の 56 ビット暗号化を使用します（CBC-DES（DES-56）規格に基づく）。このフィールドにはパスワードまたはキーを入力する必要があります。
パスワード	プライベートプロトコルのパスワードを入力します。 • **None** - このフィールドは無効になります。 • **DES56** - のパスワードは 8 ～ 16 文字です。
キー認証 - プロトコル	([SNMPv3 暗号化] で [Key] 選択時に設定可) キーの認証プロトコルを選択します。 • **MD5** - HMAC-MD5-96 認証レベルを使用します。このフィールドにはパスワードまたはキーを入力する必要があります。 • **SHA** - HMAC-SHA 認証プロトコルを使用します。このフィールドにはパスワードまたはキーを入力する必要があります。
キー	認証プロトコルのキーを入力します。 • **MD5** - キーは 32 文字です。 • **SHA** - キーは 40 文字です。
キーによるプライバシープロトコル	([SNMPv3 暗号化] で [Key] 選択時に設定可) キーのプライベートプロトコルを選択します。 • **None** - 認証プロトコルを使用しません。 • **DES56]**- DES（データ暗号化標準規格）の 56 ビット暗号化を使用します（CBC-DES（DES-56）規格に基づく）。このフィールドにはパスワードまたはキーを入力する必要があります。
キー	プライベートプロトコルのキーを入力します。 • **None** - このフィールドは無効になります。 • **DES56** - のパスワードは 32 文字です。
IP アドレスリスト名	ユーザに関連付ける標準 IP ACL を入力します。

[**追加**] ボタン - エントリを追加します。

[**削除**] ボタン - エントリを削除します。

3.5.8 SNMP ホストテーブル設定

このウィンドウを用いて、SNMP ホストの設定を行い、設定値を表示します。

[マネジメント] > [SNMP] > [SNMP ホストテーブル設定] をクリックして、以下のウィンドウを表示します。

図 3-13 SNMP ホストテーブル設定

設定パラメータ （[SNMP ホスト設定] セクション）

パラメータ	概要
ホスト IPv4 アドレス	SNMP 通知ホストの IPv4 アドレスを入力します。
ホスト IPv6 アドレス	SNMP 通知ホストの IPv6 アドレスを入力します。
ユーザベース セキュリティモデル	セキュリティモデルを選択します。 • **SNMPv1** - グループユーザに SNMPv1 セキュリティモデルの使用を許可します。 • **SNMPv2c** - グループユーザに SNMPv2c セキュリティモデルの使用を許可します。 • **SNMPv3** - グループユーザに SNMPv3 セキュリティモデルの使用を許可します。
セキュリティレベル	([ユーザベースセキュリティモデル] パラメータで [SNMPv3] 選択時に設定可) セキュリティレベルを選択します。 • **NoAuthNoPriv** - 認証が行われず、スイッチとリモート SNMP マネージャとの間で送信されるパケットの暗号化も行われません。 • **AuthNoPriv** - 認証は必要ですが、スイッチとリモート SNMP マネージャとの間で送信されるパケットの暗号化は行われません。 • **AuthPriv** - 認証が必要で、スイッチとリモート SNMP マネージャとの間で送信されるパケットの暗号化も行われます。
UDP ポート	UDP ポート番号を入力します。 (デフォルト：162、設定範囲：1-65535)
コミュニティ文字列 / SNMPv3 ユーザ名	通知パケットとともに送信するコミュニティ文字列を入力します。(最大：32 文字)

[**追加**] ボタン - エントリを追加します。

[**削除**] ボタン - エントリを削除します。

3.6 RMON（リモートモニタリング）

3.6.1 RMON グローバル設定

このウィンドウを用いて、RMON の上昇アラームおよび下降アラームのトラップ状態を有効または無効にします。

[マネジメント] > [RMON] > [RMON グローバル設定] をクリックして、以下のウィンドウを表示します。

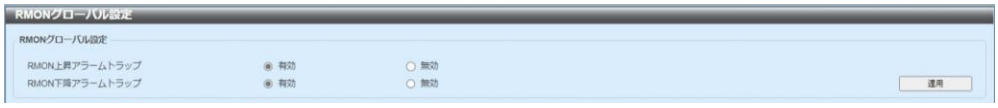


図 3-14 RMON グローバル設定

設定パラメータ （[RMON グローバル設定] セクション）

パラメータ	概要
RMON 上昇アラームトラップ	RMON 上昇アラームトラップの状態（**有効** / **無効**）を選択します。
RMON 下降アラームトラップ	RMON 下降アラームトラップの状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3.6.2 RMON 統計設定

このウィンドウを用いて、指定したポートの RMON 統計の設定を行い、設定値を表示します。

[マネジメント] > [RMON] > [RMON 統計設定] をクリックして、以下のウィンドウを表示します。

図 3-15 RMON 統計設定

設定パラメータ （[RMON 統計設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
インデックス	RMON テーブルインデックスを入力します。 （設定範囲：1-65535）
オーナー名	オーナー文字列を入力します。（最大：127 文字）

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

3.6.3 RMON ヒストリ設定

このウィンドウを用いて、指定したポートの RMON ヒストリの設定を行い、設定値を表示します。

[マネジメント] > [RMON] > [RMON ヒストリ設定] をクリックして、以下のウィンドウを表示します。

図 3-16 RMON ヒストリ設定

設定パラメータ （[RMON ヒストリ設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
インデックス	ヒストリグループテーブルのエントリのインデックス番号を入力します。（設定範囲：1-65535）
パケット数	統計の RMON 収集ヒストリグループに指定したパケットの数を入力します。（デフォルト：50、設定範囲：1-65535）
間隔	各ポーリング周期の間隔時間（秒）を入力します。 （設定範囲：1-3600）
オーナー名	オーナー文字列を入力します。（最大：127 文字）

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

3.6.4 RMON アラーム設定

このウィンドウを用いて、RMON アラームの設定を行い、設定値を表示します。

[マネジメント] > [RMON] > [RMON アラーム設定] をクリックして、以下のウィンドウを表示します。

図 3-17 RMON アラーム設定

設定パラメータ （[RMON アラーム設定] セクション）

パラメータ	概要
インデックス	アラームインデックスを入力します。（設定範囲：1-65535）
間隔	変数のサンプリングおよび閾値との照合の間隔（秒）を設定します。（設定範囲：1-2147483647）
値	サンプリングする変数のオブジェクト ID を入力します。
タイプ	モニタリングタイプ（**Absolute**/**Delta**）を選択します。
上昇閾値	上昇閾値を入力します。（設定範囲：0-2147483647）
下降閾値	下降閾値を入力します。（設定範囲：0-2147483647）
上限超過時イベント No	上昇閾値を超過するイベントの通知に使用するイベントエントリのインデックスを入力します。指定しない場合、上昇閾値を超過するときにアクションは必要ありません。（設定範囲：1–65535）
下限超過時イベント No	下降閾値を超過するイベントの通知に使用するイベントエントリのインデックスを入力します。指定しない場合、下降閾値を超過するときにアクションは必要ありません。（設定範囲：1-65535）
オーナー名	オーナー文字列を入力します。（最大：127 文字）

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

3.6.5 RMON イベント設定

このウィンドウを用いて、RMON イベントの設定を行い、設定値を表示します。

[マネジメント] > [RMON] > [RMON イベント設定] をクリックして、以下のウィンドウを表示します。

図 3-18 RMON イベント設定

設定パラメータ （[RMON イベント設定] セクション）

パラメータ	概要
インデックス	アラームエントリのインデックス値を入力します。 （設定範囲：1-65535）
説明	RMON イベントエントリの概要説明を入力します。 （最大：127 文字）
タイプ	RMON イベントエントリのタイプ（**None**/**Log**/**Trap**/**Log and Trap**）を選択します。
コミュニティ	コミュニティ文字列を入力します。（最大：127 文字）
オーナー名	オーナー文字列を入力します。（最大：127 文字）

[**追加**] ボタン - エントリを追加します。

3.7 Telnet/Web

このウィンドウを用いて、スイッチの Telnet および Web の設定を行い、設定値を表示します。

[マネジメント] > [Telnet/Web] をクリックして、以下のウィンドウを表示します。

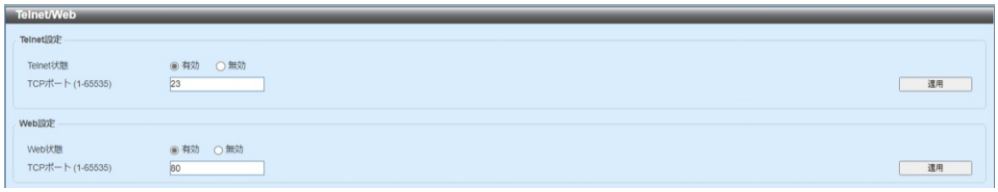


図 3-19 Telnet/Web

設定パラメータ （[Telnet 設定] セクション）

パラメータ	概要
Telnet 状態	Telnet の状態（**有効** / **無効**）を選択します。
TCP ポート	装置の Telnet 管理に使用する TCP ポート番号を入力します。（デフォルト：23、設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[Web 設定] セクション）

パラメータ	概要
Web 状態	Web サーバの状態（**有効** / **無効**）を選択します。
TCP ポート	装置の Telnet 管理に使用する TCP ポート番号を入力します。（デフォルト：80、設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

3.8 セッションタイムアウト

このウィンドウを用いて、Web、コンソール、Telnet、SSH 接続のセッションタイムアウトの設定を行い、設定値を表示します。

[マネジメント] > [セッションタイムアウト] をクリックして、以下のウィンドウを表示します。

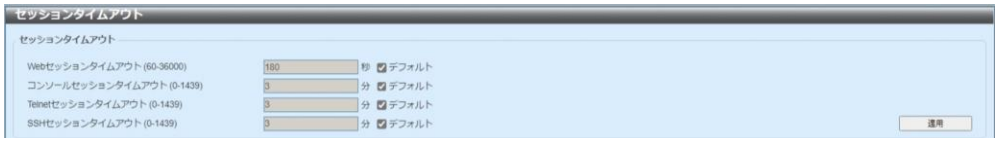


図 3-20 セッションタイムアウト

設定パラメータ （[セッションタイムアウト] セクション）

パラメータ	概要
Web セッション タイムアウト	Web セッションタイムアウトの時間（秒）を設定します。（デフォルト：180、設定範囲：60-36000）
コンソールセッション タイムアウト	コンソールセッションタイムアウトの時間（分）を設定します。0 を設定すると、タイムアウトが無効になります。（デフォルト：3、設定範囲：0-1439）
Telnet セッション タイムアウト	Telnet セッションタイムアウトの時間（分）を設定します。0 を設定すると、タイムアウトが無効になります。（デフォルト：3、設定範囲：0-1439）
SSH セッション タイムアウト	SSH セッションタイムアウトの時間（分）を設定します。0 を設定すると、タイムアウトが無効になります。（デフォルト：3、設定範囲：0-1439）

[**適用**] ボタン - 設定内容を反映します。

3.9 DHCP オート設定

このウィンドウを用いて、DHCP オート設定機能を有効または無効にします。

[マネジメント] > [DHCP オート設定] をクリックして、以下のウィンドウを表示します。

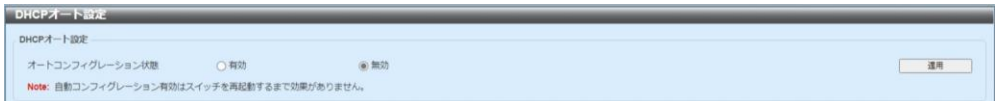


図 3-21 DHCP オート設定

設定パラメータ （[DHCP オート設定] セクション）

パラメータ	概要
オートコンフィグレーション状態	DHCP オートの状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3.10 DNS （Domain Name System）

3.10.1 DNS グローバル設定

このウィンドウを用いて、グローバル DNS 設定を行い、設定値を表示します。

[マネジメント] > [DNS] > [DNS グローバル設定] をクリックして、以下のウィンドウを表示します。

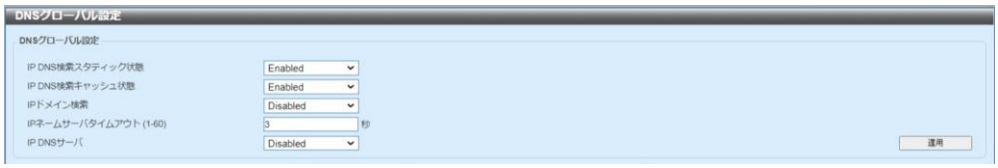


図 3-22 DNS グローバル設定

設定パラメータ （[DNS グローバル設定] セクション）

パラメータ	概要
IP DNS 検索スタティック状態	IP DNS 検索スタティックの状態（**Enabled**/**Disabled**）を選択します。
IP DNS 検索キャッシュ状態	IP DNS 検索キャッシュの状態（**Enabled**/**Disabled**）を選択します。
IP ドメイン検索	IP ドメイン検索状の態（**Enabled**/**Disabled**）を選択します。
IP ネームサーバタイムアウト	指定したネームサーバからの応答を待つ最大時間（秒）を設定します。（設定範囲：1-60）
IP DNS サーバ	DNS サーバの状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

3.10.2 DNS ネームサーバ設定

このウィンドウを用いて、DNS ネームサーバの設定を行い、設定値を表示します。

[マネジメント] > [DNS] > [DNS ネームサーバ設定] をクリックして、以下のウィンドウを表示します。

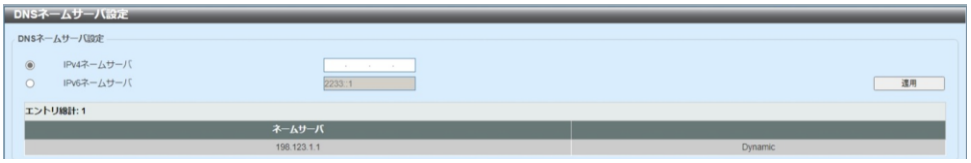


図 3-23 DNS ネームサーバ設定

設定パラメータ （[DNS ネームサーバ設定] セクション）

パラメータ	概要
IPv4 ネームサーバ	DNS サーバの IPv4 アドレスを選択および入力します。
IPv6 ネームサーバ	DNS サーバの IPv6 アドレスを選択および入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

3.10.3 DNS ホスト設定

このウィンドウを用いて、DNS ホストの設定を行い、設定値を表示します。

[マネジメント] > [DNS] > [DNS ホスト設定] をクリックして、以下のウィンドウを表示します。

図 3-24 DNS ホスト設定

設定パラメータ （[スタティックホスト設定] セクション）

パラメータ	概要
ホスト名	DNS ホストの名前を入力します。
IP アドレス	DNS ホストの IPv4 アドレスを選択および入力します。
IPv6 アドレス	DNS ホストの IPv6 アドレスを選択および入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
[**全クリア**] ボタン - テーブルからすべてのダイナミックエントリをクリアします。

3.11 ファイルシステム

このウィンドウを用いて、スイッチのファイルシステムの設定を行い、設定値を表示します。

[マネジメント] > [ファイルシステム] をクリックして、以下のウィンドウを表示します。

図 3-25 ファイルシステム

設定パラメータ

パラメータ	概要
パス	パス文字列を入力します。

[**移動**] ボタン - 入力したパスに移動します。
[**コピー**] ボタン - 特定のファイルをファイルシステムにコピーします。

ドライブリンク（c：）をクリックして、C：ドライブに移動します。

図 3-26 ファイルシステム（c：）

[**1 つ上に移動**] ボタン - 前のウィンドウに戻ります。
[**ディレクトリ作成**] ボタン - ファイルシステムにディレクトリを作成します。
[**ブートアップ**] ボタン - ファイルを起動シーケンスに使用します。起動シーケンスには、1 つの設定ファイルと 1 つのファームウェアファイルのみを使用できます。
[**リネーム**] ボタン - 特定のファイル名をリネームします。
[**削除**] ボタン - ファイルまたはフォルダをファイルシステムから削除します。

[コピーメニューへ] ボタンをクリックして、以下のウィンドウを表示します。

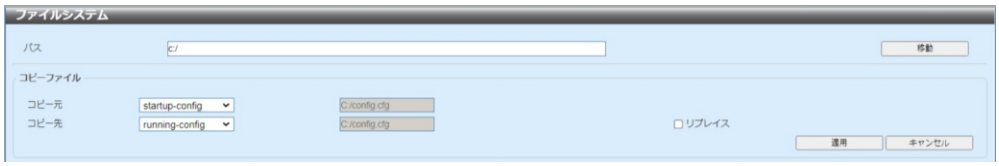


図 3-27 ファイルシステム（コピー）

設定パラメータ （[コピーファイル] セクション）

パラメータ	概要
コピー元	コピー元のファイルのタイプ（**startup-config**/**Source File**）を選択します。 **[Source File]** を選択したときのみ、ソースファイルのパスとファイル名を、表示された入力フィールドに入力できます。
コピー先	コピー先のファイルのタイプ（**startup-config**/**running-config**/**Destination File**）を選択します。 **[Destination File]** オプションを選択したときのみ、ディスティネーションファイルのパスとファイル名を、表示された入力フィールドに入力できます。 **[リプレイス]** チェックボックスをオンにすると、現在実行中の設定が、表示された設定ファイルに置き換わります。

[**適用**] ボタン - コピー元の設定／ファイルをコピー先の設定／ファイルにコピーします。
[**キャンセル**] ボタン - コピーをキャンセルします。

3.12 SMTP 設定

このウィンドウを用いて、SMTP（Simple Mail Transfer Protocol）の設定を行い、設定値を表示します。
[マネジメント] > [SMTP 設定] をクリックして、以下のウィンドウを表示します。

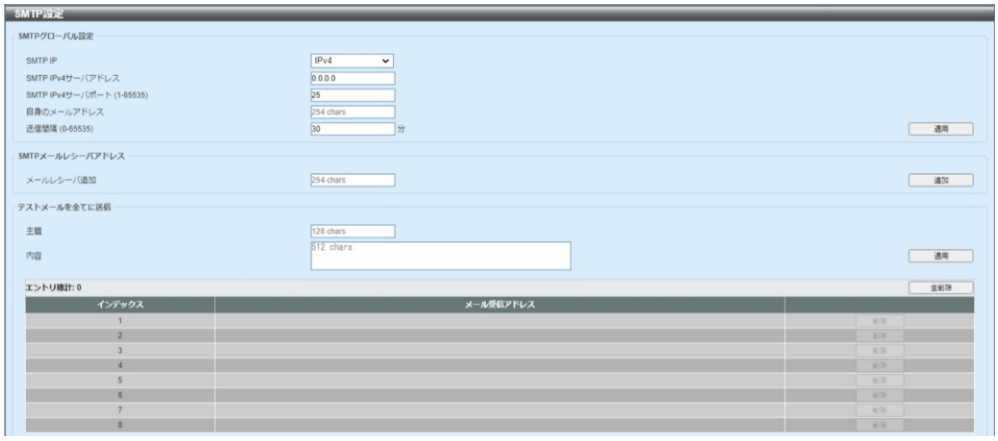


図 3-28 SMTP 設定

設定パラメータ （[SMTP グローバル設定] セクション）

パラメータ	概要
SMTP IP	SMTP サーバの IP アドレスタイプ（**IPv4**/**IPv6**）を選択します。
SMTP IPv4 サーバアドレス	([SNMP IP] で [IPv4] 選択時に設定可) SMTP サーバの IPv4 アドレスを入力します。
SMTP IPv6 サーバアドレス	([SNMP IP] で [IPv6] 選択時に設定可) SMTP サーバの IPv6 アドレスを入力します。
SMTP IPv4 サーバポート	([SNMP IP] で [IPv4] 選択時に設定可) SMTP サーバのポート番号を入力します。 (デフォルト：25、設定範囲：1-65535)
SMTP IPv6 サーバポート	([SNMP IP] で [IPv6] 選択時に設定可) SMTP サーバのポート番号を入力します。(デフォルト：25)
自身のメールアドレス	スイッチを表すメールアドレスを入力します。 (最大：254 文字)
送信間隔	送信間隔の値（分）を設定します。 (デフォルト：30、設定範囲：0-65535)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[SMTP メールレシーバアドレス] セクション）

パラメータ	概要
メールレシーバ追加	レシーバのメールアドレスを入力します。（最大：254 文字）

設定パラメータ （[テストメールをすべてに送信] セクション）

パラメータ	概要
主題	メールの件名を入力します。（最大：128 文字）
内容	メールの本文を入力します。（最大：512 文字）

[**追加**] ボタン - エントリを追加します。
[**適用**] ボタン - 設定内容を反映します。
[**全削除**] ボタン - すべてのレシーバメールアドレスを削除します。
[**削除**] ボタン - レシーバメールアドレスを削除します。

3.13 NLB FDB 設定

このウィンドウを用いて、指定したポートの NLB（ネットワーク負荷分散）FDB（ファイルデータベース）の設定を行い、設定値を表示します。

[マネジメント] > [NLB FDB 設定] をクリックして、以下のウィンドウを表示します。

図 3-29 NLB FDB 設定

設定パラメータ （[NLB FDB 設定] セクション）

パラメータ	概要
NLB タイプ	NLB タイプ（**Unicast**/**Multicast**）を選択します。
VID	([NLB タイプ] で [Multicast] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲：1-4094)
MAC アドレス	エントリのユニキャストまたはマルチキャスト MAC アドレスを入力します。受信したパケットのディスティネーション MAC アドレスが、指定した MAC アドレスと一致する場合、そのパケットは指定したインタフェースに転送されます。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - 設定内容を反映します。
[**全削除**] ボタン - すべてのエントリを削除します。
[**削除**] ボタン - エントリを削除します。

3.14 IP 簡単設定

3.14.1 IP 簡単設定プロトコル設定

このウィンドウを用いて、IP セットアップインタフェース機能を有効または無効にします。

[マネジメント] > [IP 簡単設定] > [IP 簡単設定プロトコル設定] をクリックして、以下のウィンドウを表示します。

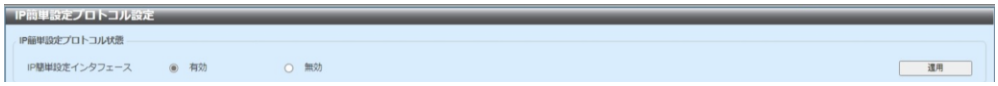


図 3-30 IP 簡単設定プロトコル設定

設定パラメータ （[IP 簡単設定プロトコル状態] セクション）

パラメータ	概要
IP 簡単設定インタフェース	IP 簡単設定インタフェースの状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

4 PPS

4.1 PPS 通知設定

このウィンドウを用いて、PPS の通知設定を行います。

[PPS] > [PPS 通知設定] をクリックして、以下のウィンドウを表示します。

図 4-31 PPS 通知設定

設定パラメータ （[PPS 通知設定] セクション）

パラメータ	概要
システムログ通知設定	PPS のシステムログ通知の状態（**Enabled**/**Disabled**）を選択します。
カウンタインターバル	カウンタインターバルの値（秒）を設定します。 （設定範囲：1-120）
開始ポート／終了ポート	ポートを設定します。
カウンタ通知ポート設定	カウンタ通知ポートの状態（**Enabled**/**Disabled**）を選択します。設定すると対象のカウンタ通知ポートが表示されます。

[**適用**] ボタン - 設定内容を反映します。

4.2 PPS ポート設定

このウィンドウを用いて、PPS のポート設定を行います。

[PPS] > [PPS ポート設定] をクリックして、以下のウィンドウを表示します。

図 4-32 PPS ポート設定

設定パラメータ （[PPS ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを設定します。
PPS プライオリティ設定	PPS プライオリティの値を設定します。 （設定範囲：0-255）

[**適用**] ボタン - 設定内容を反映します。

4.3 PPS コネクション設定

このウィンドウを用いて、PPS コネクションテーブルの設定を行います。

[PPS] > [PPS コネクション設定] をクリックして、以下のウィンドウを表示します。

図 4-33 PPS コネクション設定

設定パラメータ （[PPS コネクション設定] セクション）

パラメータ	概要
ポート	PPS コネクションに追加するスイッチのポート番号を選択します。
PPS 宛先 MAC アドレス	PPS コネクションに追加する PPS 宛先 MAC アドレスを入力します。
PPS ゲートウェイ MAC アドレス	PPS コネクションに追加する PPS ゲートウェイ MAC アドレスを入力します。
VLAN ID	VLAN ID を入力します。（設定範囲：1-4094）
タグ	ゲートウェイに送信するパケットへのタグ付加（**Yes**/**No**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**削除**] ボタン - エントリを削除します。
[**リスタートコネクション**] ボタン - 再度 PPS コネクションを行います。

4.4 PPS ネイバー設定

このウィンドウを用いて、PPS ネイバーテーブルの設定を行います。

[PPS] > [PPS ネイバー設定] をクリックして、以下のウィンドウを表示します。

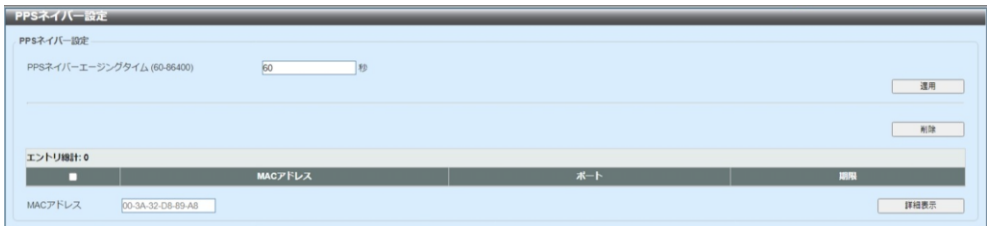


図 4-34 PPS ネイバー設定

設定パラメータ （[PPS ネイバー設定] セクション）

パラメータ	概要
PPS ネイバーエージングタイム	PPS 近接装置のエントリ保有時間（秒）を入力します。（設定範囲：60-86400）
MAC アドレス	PPS 近接装置の MAC アドレスを入力します。設定するとその MAC アドレスの情報が表示されます。

[**適用**] ボタン - 設定内容を反映します。
[**削除**] ボタン - エントリを削除します。
[**詳細表示**] ボタン - PPS ネイバー情報の詳細を表示します。

5 L2 機能

5.1 FDB（フォワーディングデータベース）

5.1.1 スタティック FDB

5.1.1.1 ユニキャストスタティック FDB

このウィンドウを用いて、スタティックユニキャストフォワーディングの設定を行い、設定値を表示します。

[L2 機能] > [FDB] > [スタティック FDB] > [ユニキャストスタティック FDB] をクリックして、以下のウィンドウを表示します。

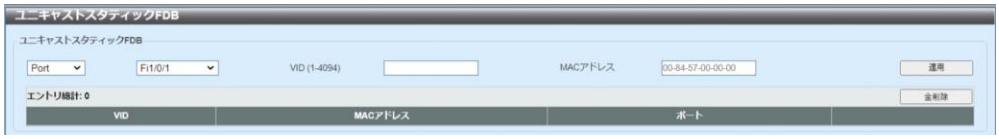


図 5-1 ユニキャストスタティック FDB

設定パラメータ （[ユニキャストスタティック FDB] セクション）

パラメータ	概要
Port/Drop	• **[Port]** - 入力した MAC アドレスが存在するポートを使用します。 • **[Drop]** - ユニキャストスタティック FDB から MAC アドレスをドロップします。
ポートナンバー	([Port] 選択時に設定可）ポートを選択します。
VID	使用する VLAN ID を入力します。(設定範囲：1-4094)
MAC アドレス	パケットがスタティックに転送される MAC アドレスを入力します。このアドレスには、ユニキャスト MAC アドレスを指定してください。

[**適用**] ボタン - エントリを追加します。
[**全削除**] ボタン - すべてのエントリを削除します。
[**削除**] ボタン - エントリを削除します。

5.1.1.2 マルチキャストスタティック FDB

このウィンドウを用いて、マルチキャストスタティック FDB の設定を行い、設定値を表示します。

[L2 機能] > [FDB] > [スタティック FDB] > [マルチキャストスタティック FDB] をクリックして、以下のウィンドウを表示します。

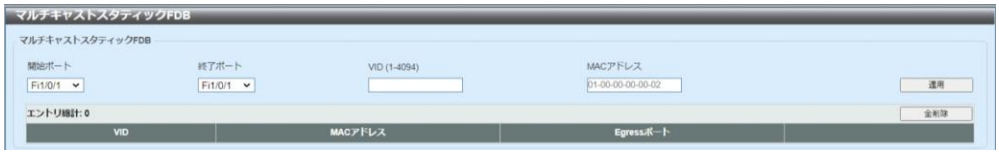


図 5-2 マルチキャストスタティック FDB

設定パラメータ （[マルチキャストスタティック FDB] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
MAC アドレス	マルチキャストパケットのスタティックディスティネーション MAC アドレスを入力します。このアドレスには、マルチキャスト MAC アドレスを指定してください。

[**適用**] ボタン - エントリを追加します。
[**全削除**] ボタン - すべてのエントリを削除します。
[**削除**] ボタン - エントリを削除します。

5.1.2 MAC アドレステーブル設定

このウィンドウを用いて、MAC アドレステーブルの設定を行い、設定値を表示します。

[L2 機能] > [FDB] > [MAC アドレステーブル設定] をクリックして、以下のウィンドウを表示します。

図 5-3 MAC アドレステーブル設定（グローバル設定）

設定パラメータ （[グローバル設定] タブ）

パラメータ	概要
エージング時間	MAC アドレステーブルのエージング時間（秒）を入力します。MAC アドレスのエージングは無効になります。（デフォルト：300、設定範囲：0,10-1000000）
エージングディスティネーションヒット	エージングディスティネーションヒットの状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC アドレスポート学習設定] タブ）

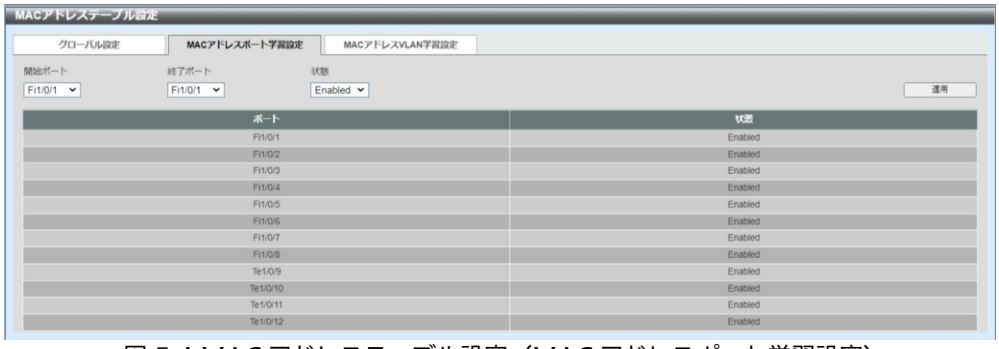


図 5-4 MAC アドレステーブル設定（MAC アドレスポート学習設定）

以下のパラメータを設定できます。

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの MAC アドレス学習の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

[MAC アドレス VLAN 学習設定] タブをクリックして、以下のウィンドウを表示します。

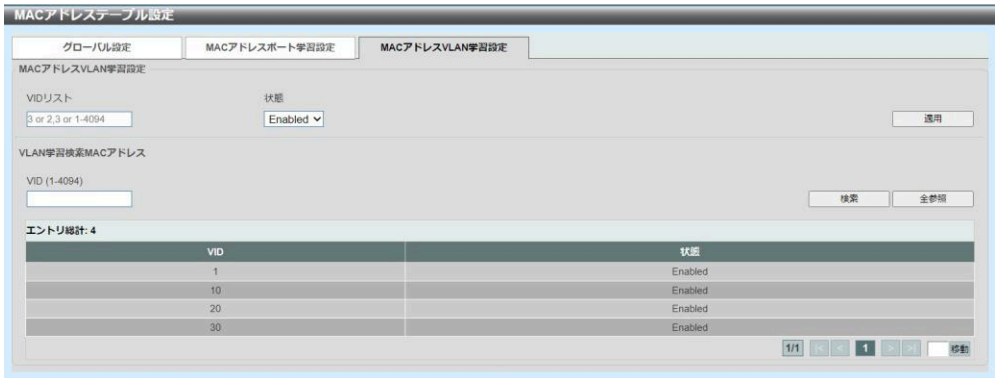


図 5-5 MAC アドレステーブル設定（MAC アドレス VLAN 学習設定）

設定パラメータ （[MAC アドレス VLAN 学習設定] タブ >[MAC アドレス VLAN 学習設定] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 （設定範囲：1-4094）
状態	指定した VLAN の MAC アドレス学習状態（**Enabled**/**Disabled**）を選択します。

[適用] ボタン - エントリを追加します。

設定パラメータ （[MAC アドレス VLAN 学習設定] タブ >[VLAN 学習検索 MAC アドレス] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.1.3 MAC アドレステーブル

このウィンドウを用いて、MAC アドレステーブルのエントリを表示およびクリアします。

[L2 機能] > [FDB] > [MAC アドレステーブル] をクリックして、以下のウィンドウを表示します。

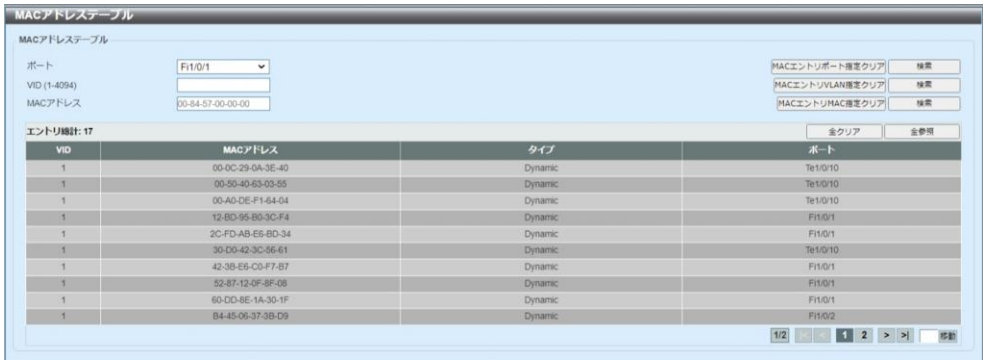


図 5-6 MAC アドレステーブル

設定パラメータ （[MAC アドレステーブル] セクション）

パラメータ	概要
ポート	ポートを選択します。
VID	使用する VLAN ID を入力します。（設定範囲：(1-4094)）
MAC アドレス	この設定に使用する MAC アドレスを入力します。

[**MAC エントリポート指定クリア**] ボタン - 指定したポートに関連付けられているダイナミック MAC アドレスをテーブルからクリアします。
[**MAC エントリ VLAN 指定クリア**] ボタン - 指定した VLAN に関連付けられているダイナミック MAC アドレスをクリアします。
[**MAC エントリ MAC 指定クリア**] ボタン - 指定したダイナミック MAC アドレスをテーブルからクリアします。
[**検索**] ボタン - 検索結果を表示します。
[**全クリア**] ボタン - すべてのエントリをテーブルからクリアします。
[**全参照**] ボタン - エントリをすべて表示します。

5.1.4 MAC 通知

このウィンドウを用いて、グローバル MAC 通知設定および指定したポートの MAC 通知設定を行い、設定値を表示します。

[L2 機能] > [FDB] > [MAC 通知] をクリックして、以下のウィンドウを表示します。

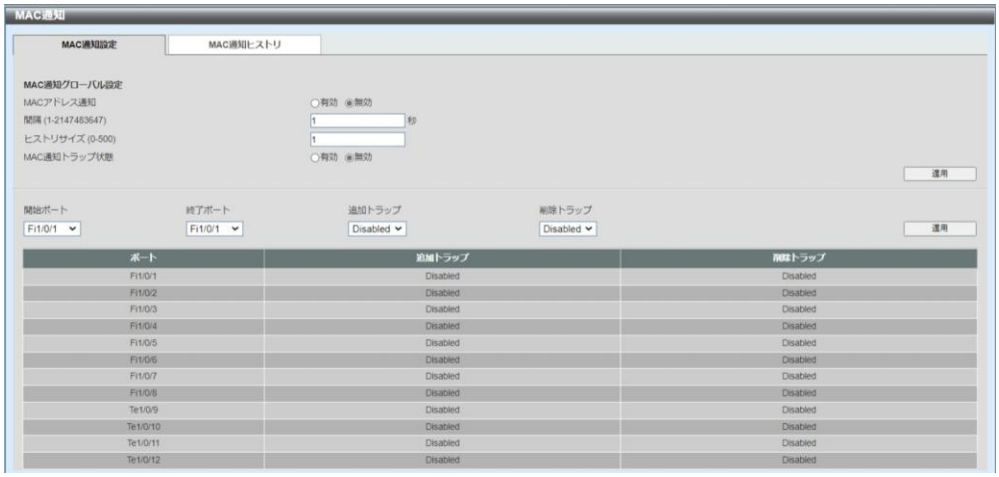


図 5-7 MAC 通知（MAC 通知設定）

設定パラメータ （[MAC 通知設定] タブ）

パラメータ	概要
MAC アドレス通知	MAC 通知状態（**有効** / **無効**）を選択します。
間隔	通知間隔の時間（秒）を入力します。 （デフォルト：1、設定範囲：1-2147483647）
ヒストリサイズ	通知に使用するヒストリログにリスト表示するエントリの最大数を入力します。（デフォルト：1、設定範囲：0-500）
MAC 通知トラップ状態	MAC 通知トラップ状態（**有効** / **無効**）を選択します。
開始ポート／終了ポート	ポートを選択します。
追加トラップ	選択したポートへのトラップ追加状態（**Enabled**/ **Disabled**）を選択します。
削除トラップ	選択したポートからのトラップ削除状態（**Enabled**/ **Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

[**MAC 通知ヒストリ**] タブをクリックして、MAC 通知ヒストリの表示します。

5.2 VLAN （Virtual Local Area Network）

5.2.1 802.1Q VLAN

このウィンドウを用いて、IEEE 802.1Q VLAN の設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [802.1Q VLAN] をクリックして、以下のウィンドウを表示します。

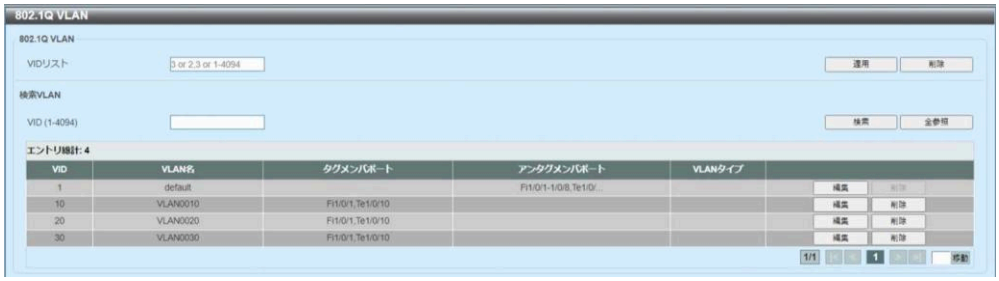


図 5-8 802.1Q VLAN

設定パラメータ （[802.1Q VLAN] セクション）

パラメータ	概要
VID リスト	作成または削除する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

[検索 VLAN] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**編集**] ボタン - エントリの設定を編集します。
[**削除**] ボタン - エントリを削除します。

5.2.2 802.1v プロトコル VLAN

5.2.2.1 プロトコル VLAN プロファイル

このウィンドウを用いて、IEEE 802.1v プロトコル VLAN の設定を行い、設定値を表示します。各プロトコルでは複数の VLAN がサポートされています。同じ物理ポート上の異なるプロトコルに、アンタグポートを設定できます。

[L2 機能] > [VLAN] > [802.1v プロトコル VLAN] > [プロトコル VLAN プロファイル] をクリックして、以下のウィンドウを表示します。

図 5-9 プロトコル VLAN プロファイル

設定パラメータ （[プロトコル VLAN プロファイル追加] セクション）

パラメータ	概要
プロファイル **ID**	802.1v プロトコル VLAN のプロファイル ID を入力します。（設定範囲：1-16）
フレームタイプ	フレームタイプのオプション（**Ethernet2**/**SNAP**/**LLC**）を選択します。この機能は、パケットヘッダ内のタイプオクテットを調べて、関連付けられたプロトコルのタイプを探索します。これにより、パケットをプロトコル定義の VLAN にマッピングします。
イーサタイプ	グループのイーサネットタイプ値を入力します。プロトコル値を用いて、指定したフレームタイプのプロトコルを識別します。フレームタイプに応じて、オクテット文字列が以下のいずれかの値を持ちます。 • Ethernet2 の場合 - 16 ビット（2 オクテット）の 16 進数値です。IPv4 は 0800、IPv6 は 86DD、ARP は 0806 など。 • SNAP の場合 - 16 ビット（2 オクテット）の 16 進数値です。 • LLC の場合 - 2 オクテットの IEEE 802.2 LSAP（Link Service Access Point）ペアです。最初のオクテットは DSAP（Destination Service Access Point）、2 番目のオクテットはソースです。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

5.2.2.2 プロトコル VLAN プロファイルインタフェース

このウィンドウを用いて、プロトコル VLAN プロファイルインタフェースの設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [802.1v プロトコル VLAN] > [プロトコル VLAN プロファイルインタフェース] をクリックして、以下のウィンドウを表示します。

図 5-10 プロトコル VLAN プロファイルインタフェース

設定パラメータ （[新プロトコル VLAN インタフェース追加] セクション）

パラメータ	概要
ポート	ポートを選択します。
プロファイル ID	802.1v プロトコル VLAN のプロファイル ID を選択します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
優先度	使用する優先度の値（**0** ～ **7**）を選択します。このパラメータを指定することによって、スイッチにあらかじめ設定されている 802.1p デフォルト優先度を書き換えます。この優先度により、パケット転送先の CoS（Class of Service）キューが決定します。このフィールドを指定した後は、この優先度に一致するパケットをスイッチが受信すると、そのパケットはあらかじめ設定された CoS キューに転送されます。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

5.2.3 GVRP

5.2.3.1 GVRP グローバル

このウィンドウを用いて、GVRP（GARP VLAN Registration Protocol）のグローバル設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [GVRP] > [GVRP グローバル] をクリックして、以下のウィンドウを表示します。

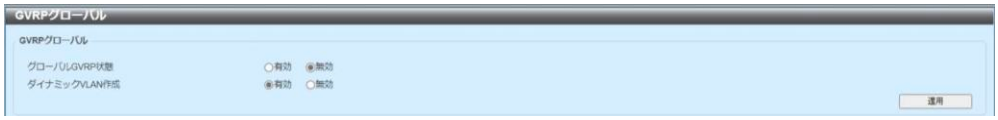


図 5-11 GVRP グローバル

設定パラメータ （[GVRP グローバル] セクション）

パラメータ	概要
グローバル **GVRP 状態**	グローバル GVRP 状態（**有効** / **無効**）を選択します。
ダイナミック VLAN 作成	ダイナミック VLAN 作成状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

5.2.3.2 GVRP ポート

このウィンドウを用いて、GVRP ポートの設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [GVRP] > [GVRP ポート] をクリックして、以下のウィンドウを表示します。

図 5-12 GVRP ポート

設定パラメータ （[GVRP ポート] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
GVRP 状態	GVRP ポート状態（Enabled/Disabled）を選択します。 これにより、ポートがダイナミックに VLAN のメンバになることができます。（デフォルト：無効）
ジョインタイム	ジョインタイム値（センチ秒）を入力します。 （デフォルト：20、設定範囲：10-10000）
Leave タイム	Leave タイム値（センチ秒）を入力します。 （デフォルト：60、設定範囲：10-10000）
Leave All タイム	Leave All タイム値（センチ秒）を入力します。 （デフォルト：1000、設定範囲：10-10000）

[**適用**] ボタン - 設定内容を反映します。

5.2.3.3 GVRP アドバタイズ VLAN

このウィンドウを用いて、GVRP アドバタイズ VLAN の設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [GVRP] > [GVRP アドバタイズ VLAN] をクリックして、以下のウィンドウを表示します。

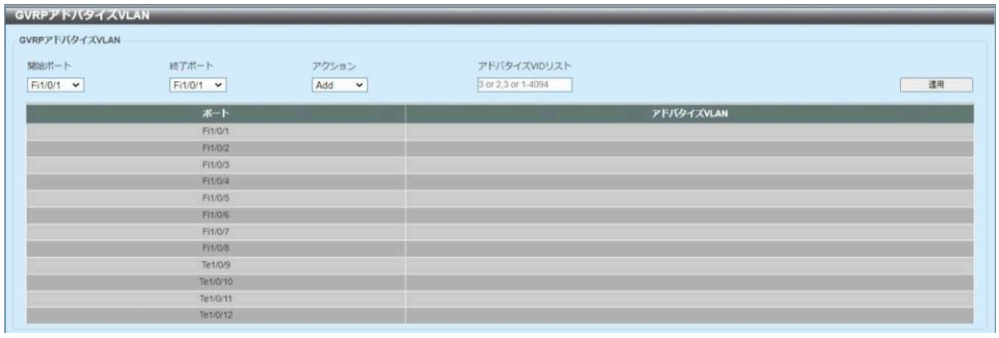


図 5-13 GVRP アドバタイズ VLAN

設定パラメータ （[GVRP アドバタイズ VLAN] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
アクション	ポートマッピングアクションに使用するアドバタイズ VLAN（**All**/**Add**/**Remove**/**Replace**）を選択します。 **[All]** を選択すると、すべてのアドバタイズ VLAN が使用されます。
アドバタイズ VID リスト	アドバタイズする VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。

5.2.3.4 GVRP 禁止 VLAN

このウィンドウを用いて、GVRP 禁止 VLAN の設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [GVRP] > [GVRP 禁止 VLAN] をクリックして、以下のウィンドウを表示します。

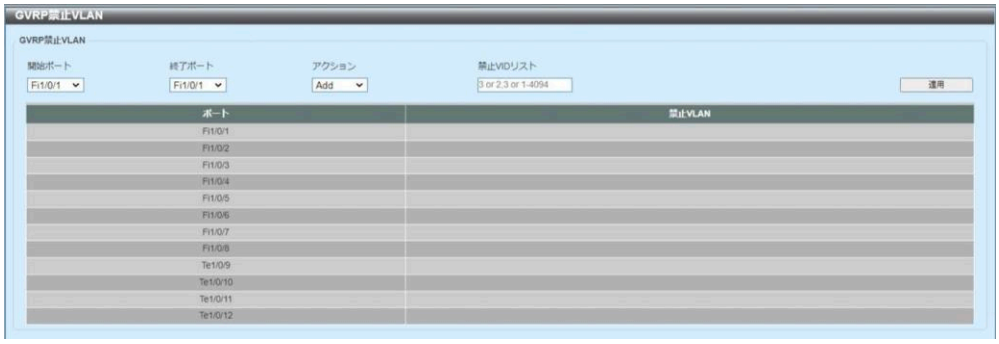


図 5-14 GVRP 禁止 VLAN

設定パラメータ （[GVRP 禁止 VLAN] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
アクション	ポートマッピングアクションに使用する禁止 VLAN（**All**/**Add**/**Remove**/**Replace**）を選択します。**[All]** を選択すると、禁止されたすべての VLAN が使用されます。
禁止 VID リスト	禁止する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 （設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。

5.2.3.5 GVRP 統計テーブル

このウィンドウを用いて、GVRP 統計を表示およびクリアします。

[L2 機能] > [VLAN] > [GVRP] > [GVRP 統計テーブル] をクリックして、以下のウィンドウを表示します。

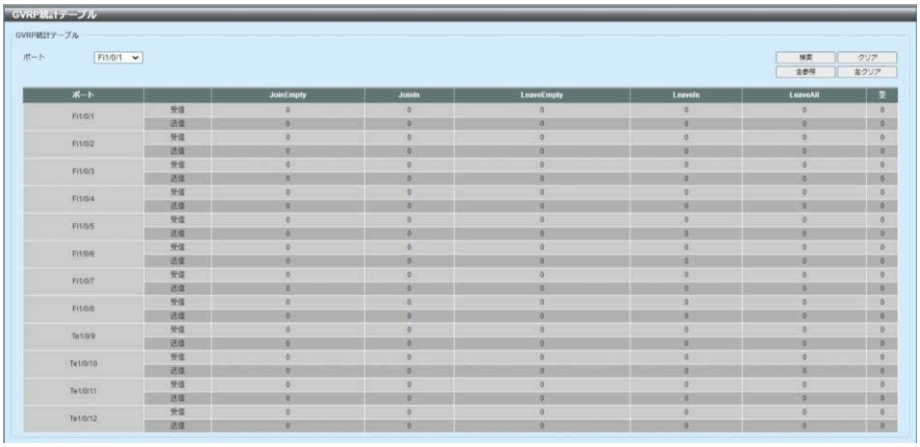


図 5-15 GVRP 統計テーブル

設定パラメータ （[GVRP 統計テーブル] セクション）

パラメータ	概要
ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**クリア**] ボタン - 指定したポートから統計情報をクリアします。
[**全参照**] ボタン - エントリをすべて表示します。
[**全クリア**] ボタン - すべての統計情報をクリアします。

5.2.4 アシンメトリック VLAN

このウィンドウを用いて、アシンメトリック VLAN の設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [アシンメトリック VLAN] をクリックして、以下のウィンドウを表示します。

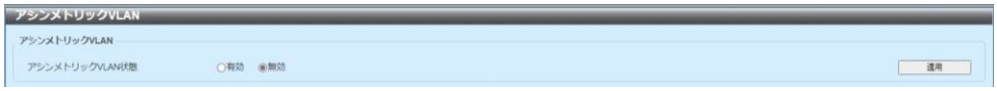


図 5-16 アシンメトリック VLAN

設定パラメータ （[アシンメトリック VLAN] セクション）

パラメータ	概要
アシンメトリック VLAN 状態	アシンメトリック VLAN 状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

5.2.5 MAC VLAN

このウィンドウを用いて、MAC ベース VLAN の設定を行い、設定値を表示します。スタティック MAC ベース VLAN エントリが設定され、あるポートに関連付けられている場合、そのポート上で動作している VLAN は変わります。

[L2 機能] > [VLAN] > [MAC VLAN] をクリックして、以下のウィンドウを表示します。

図 5-17 MAC VLAN

設定パラメータ （[MAC VLAN] セクション）

パラメータ	概要
MAC アドレス	Enter ユニキャスト MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
優先度	アンタグパケットに割り当てる優先度（**0** ～ **7**）を選択します。

[適用] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

5.2.6 VLAN インタフェース

このウィンドウを用いて、VLAN インタフェースの設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [VLAN インタフェース] をクリックして、以下のウィンドウを表示します。

図 5-18 VLAN インタフェース

[**詳細参照**] ボタン - エントリの詳細情報を表示します。

[編集] ボタンをクリックして、以下のウィンドウを表示します。

図 5-19 VLAN インタフェース（編集、アクセス）

設定パラメータ （[編集]>[VLAN インタフェースの設定] セクション）

パラメータ	概要
VLAN モード	VLAN モードのオプション（**Access**/**Hybrid**/**Trunk**/**Promiscuous**/**Host**）を選択します。
受信可能フレーム	受信可能フレームの動作オプション（**Tagged Only**/**Untagged Only**/**Admit All**）を選択します。
Ingress チェック	Ingress チェックの状態（**有効** / **無効**）を選択します。
VLAN Precedence	VLAN Precedence のオプション（**MAC-based VLAN**/**Subnet-based VLAN**）を選択します。
ネイティブ VLAN	ネイティブ VLAN の有効、無効を選択します。
VID	([ネイティブ VLAN] パラメータで [有効] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲：1-4094)
アクション	実行するアクション（**None**/**Add**/**Remove**/**Tagged**/**Untagged**/**Except**/**Replace**）を選択します。
許可 VLAN 範囲	許可 VLAN 範囲を入力します。

パラメータ	概要
モード追加	([VLAN モード] パラメータで [Hybrid] 選択時に設定可) ([アクション] パラメータで [Add] 選択時に設定可) モード（**タグ** / **アンタグ**）を選択します。
許可 VLAN 範囲	許可 VLAN 範囲を入力します。
クローン	クローンの有効、無効を選択します。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

5.2.7 サブネット VLAN

このウィンドウを用いて、サブネット VLAN の設定を行い、設定値を表示します。アンタグ IP パケットまたは優先度タグ IP パケットをポートで受信すると、そのソース IP アドレスを用いて、サブネット VLAN エントリと照合します。ソース IP がエントリのサブネットに含まれる場合は、パケットが、このサブネットに定義された VLAN に分類されます。

[L2 機能] > [VLAN] > [サブネット VLAN] をクリックして、以下のウィンドウを表示します。

図 5-20 サブネット VLAN

設定パラメータ （[サブネット VLAN] セクション）

パラメータ	概要
IPv4 ネットワークプレフィックス / プレフィックス長	サブネット VLAN の IPv4 アドレスとプレフィックス長の値を選択および入力します。
IPv6 ネットワークプレフィックス / プレフィックス長	サブネット VLAN の IPv6 アドレスとプレフィックス長の値を選択および入力します。
VID	使用するサブネット VLAN ID を入力します。 （設定範囲：1-4094）
優先度	使用する優先度の値（**0 ～ 7**）を選択します。 値が小さいほど、優先度が高くなります。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

5.2.8 音声 VLAN

5.2.8.1 音声 VLAN グローバル

このウィンドウを用いて、グローバル音声 VLAN の設定を行い、設定値を表示します。音声 VLAN 機能をグローバルに有効または無効にし、スイッチの音声 VLAN を指定します。スイッチに指定できる音声 VLAN は 1 つだけです。

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN グローバル] をクリックして、以下のウィンドウを表示します。

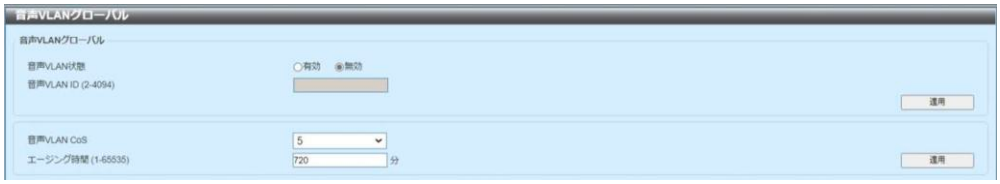


図 5-21 音声 VLAN グローバル

設定パラメータ （[音声 VLAN グローバル] セクション）

パラメータ	概要
音声 VLAN 状態	音声 VLAN の状態（**有効** / **無効**）を選択します。
音声 VLAN ID	音声 VLAN の VLAN ID を入力します。設定前に、音声 VLAN として指定する VLAN がすでに存在している必要があります。（設定範囲：2-4094）
音声 VLAN CoS	音声 VLAN の CoS（**0 ～ 7**）を選択します。音声 VLAN 対応ポートに到着する音声パケットは、CoS 指定済みとしてマークされます。CoS パケットの注釈を付けることにより、音声 VLAN トラフィックを QoS（Quality of Service）のデータトラフィックと区別できるようになります。
エージング時間	エージング時間（分）を入力します。自動的に学習された音声装置をエージアウトするためのエージング時間、および音声 VLAN 情報を設定します。ポートに接続されている最後の音声装置がトラフィック送信を停止し、この音声装置の MAC アドレスが FDB からエージアウトすると、音声 VLAN のエージングタイマーが始動します。音声 VLAN のエージングタイマーの期限が切れると、ポートが音声 VLAN から削除されます。エージングタイム中に音声トラフィックが再開すると、エージングタイマーがキャンセルされます。 （設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

5.2.8.2 音声 VLAN ポート

このウィンドウを用いて、音声 VLAN インタフェースの設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN ポート] をクリックして、以下のウィンドウを表示します。

図 5-22 音声 VLAN ポート

設定パラメータ （[音声 VLAN ポート] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの音声 VLAN 状態（**Enabled**/**Disabled**）を選択します。ポートで音声 VLAN を有効にすると、受信した音声パケットが音声 VLAN で転送されます。受信したパケットは、そのパケットのソース MAC アドレスが OUI アドレスに適合する場合に、音声パケットと判断されます。

パラメータ	概要
モード	モードを選択します。 • **[Auto Untagged]** - 音声 VLAN のアンタグメンバシップが自動的に学習されます。 • **[Auto Tagged]** - 音声 VLAN のタグメンバシップが自動的に学習されます。 • **[Manual]** - 音声 VLAN メンバシップを手動で設定します。 自動学習が有効の場合、ポートが音声 VLAN メンバとして自動的に学習されます。このメンバシップは自動的にエージアウトします。ポートがオートタグモードで動作し、装置の OUI を通じて音声装置をキャプチャする場合、そのポートはタグメンバとして自動的に音声 VLAN に参加します。音声装置がタグパケットを送信すると、スイッチがその優先度を変更します。音声装置がアンタグパケットを送信すると、PVID（ポート VLAN ID）で転送されます。 ポートがオートアンタグモードで動作し、装置の OUI を通じて音声装置をキャプチャする場合、そのポートはアンタグメンバとして自動的に音声 VLAN に参加します。音声装置がタグパケットを送信すると、スイッチがその優先度を変更します。音声装置がアンタグパケットを送信すると、音声 VLAN で転送されます。 スイッチは LLDP-MED（LLDP Media Endpoint Discovery）パケットを受信すると、VLAN ID、タグフラグ、優先度フラグをチェックします。スイッチはタグフラグと優先度設定に従います。

[**適用**] ボタン - 設定内容を反映します。

5.2.8.3 音声 VLAN OUI

このウィンドウを用いて、音声 VLAN の OUI の設定を行い、設定値を表示します。ユーザ定義の OUI を音声 VLAN に関連付けることができます。受信したパケットのソース MAC アドレスが任意の OUI パターンに一致する場合、受信したパケットは音声パケットと判断されます。デフォルトの OUI は、削除することも重複して指定することもできません。

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN OUI] をクリックして、以下のウィンドウを表示します。

図 5-23 音声 VLAN OUI

設定パラメータ （[音声 VLAN OUI] セクション）

パラメータ	概要
OUI アドレス	音声 VLAN OUI の MAC アドレスを入力します。
マスク	音声 VLAN OUI の MAC アドレスに対する一致ビットマスクを入力します。
説明	ユーザ定義 OUI の MAC アドレスに対する概要説明を入力します。(文字列 : 32 文字)

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

5.2.8.4 音声 VLAN 装置

このウィンドウを用いて、音声 VLAN 装置テーブルおよび情報を表示します。

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN 装置] をクリックして、以下のウィンドウを表示します。

図 5-24 音声 VLAN 装置

5.2.8.5 音声 VLAN LLDP-MED 装置

このウィンドウを用いて、音声 VLAN LLDP-MED 装置テーブルおよび情報を表示します。

[L2 機能] > [VLAN] > [音声 VLAN] > [音声 VLAN LLDP-MED 装置] をクリックして、以下のウィンドウを表示します。

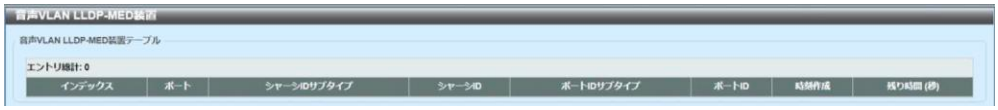


図 5-25 音声 VLAN LLDP-MED 装置

5.2.9 プライベート VLAN

このウィンドウを用いて、プライベート VLAN の設定を行い、設定値を表示します。

[L2 機能] > [VLAN] > [プライベート VLAN] をクリックして、以下のウィンドウを表示します。

図 5-26 プライベート VLAN

設定パラメータ （[プライベート VLAN] セクション）

パラメータ	概要
VID リスト	使用するプライベート VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 （設定範囲：1-4094）
状態	プライベート VLAN 状態（**Enabled**/**Disabled**）を選択します。
タイプ	作成するプライベート VLAN のタイプ（**Community**/**Isolated**/**Primary**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[プライベート VLAN アソシエーション] セクション）

パラメータ	概要
VID リスト	使用するプライベート VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 （設定範囲：1-4094）
アクション	プライベート VLAN で実行するアクション（**Add**/**Remove**/**Disable**）を選択します。

パラメータ	概要
セカンダリ VID リスト	使用するセカンダリプライベート VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 (設定範囲：1-4094)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[プライベート VLAN ホストアソシエーション] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
プライマリ VID	使用するプライマリ VLAN ID を入力します。 (設定範囲：1-4094)
セカンダリ VID	使用するセカンダリ VLAN ID を入力します。 (設定範囲：1-4094) **[関連付け削除]** オプションをオンにした場合、この設定は有効になりません。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[プライベート VLAN マッピング] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
プライマリ VID	使用するプライマリ VLAN ID を入力します。 (設定範囲：1-4094)
アクション	• **Add** - 入力した情報に基づいてエントリを追加します。 • **Remove** - 入力した情報に基づいてエントリを削除します。
セカンダリ VID リスト	使用するセカンダリ VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 (設定範囲：1-4094) **[マッピング削除]** オプションをオンにした場合、この設定は有効になりません。

[**適用**] ボタン - 設定内容を反映します。

5.3 STP （Spanning Tree Protocol）

5.3.1 STP グローバル設定

このウィンドウを用いて、グローバル STP 設定を行い、設定値を表示します。

[L2 機能] > [STP] > [STP グローバル設定] をクリックして、以下のウィンドウを表示します。

図 5-27 STP グローバル設定

設定パラメータ （[STP 状態] セクション）

パラメータ	概要
STP 状態	STP 状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[STP モード] セクション）

パラメータ	概要
STP モード	使用する STP モード（**MSTP**/**RSTP**/**STP**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[STP 優先度] セクション）

パラメータ	概要
優先度	STP 優先度値（**0 ～ 61440**）を選択します。値が小さいほど、優先度が高くなります。（デフォルト：32768）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[STP コンフィグレーション] セクション）

パラメータ	概要
ブリッジ最大エイジ	ブリッジ最大エイジ値（秒）を入力します。最大エイジ値を設定することにより、古い情報がネットワーク内で冗長パスを通って無限に循環することがなくなり、新しい情報の有効な伝搬が妨げられることもありません。この値はルートブリッジで設定されているため、スイッチのスパニングツリー設定値がブリッジ LAN の他の装置のものと同じであると判断するのに役立ちます。（デフォルト：20、設定範囲：6-40）
ブリッジハロータイム	([STP モード] パラメータで [RSTP] または [STP] 選択時に設定可) ブリッジのハロータイム値（秒）を入力します。実際にルートブリッジであることを他のすべてのスイッチに伝えるために、ルートブリッジが 2 回の BPDU（Bridge Protocol Data Unit）パケットを送信する間隔です。このフィールドは、STP バージョンとして STP または RSTP（Rapid Spanning Tree Protocol）を選択した場合にのみ表示されます。MSTP の場合、ハロータイムはポート単位で設定する必要があります。（デフォルト：2、設定範囲：1-2）
ブリッジフォワードタイム	ブリッジフォワードタイム値（秒）を入力します。 スイッチのすべてのポートがブロッキング状態からフォワーディング状態に移るときの、リスニング状態の時間です。 （デフォルト：15、設定範囲：4-30）
TX ホールドカウント	送信ホールドカウント値（回）を入力します。この値を用いて、所定の間隔で送信されるハローパケットの最大数を設定します。（デフォルト：6、設定範囲：1-10）
最大ホップ	許可する最大ホップ数を入力します。この値を用いて、スイッチによって送信された BPDU（Bridge Protocol Data Unit）パケットが破棄される前の、スパニングツリー領域内にある装置間のホップ数を設定します。値が 0 に到達するまで、スイッチの通過ごとにホップカウントが 1 つ減ります。その後、スイッチは BDPU パケットを破棄し、そのポートに保持されている情報はエージアウトします。 （デフォルト：20、設定範囲：1-40）

[**適用**] ボタン - 設定内容を反映します。

5.3.2 STP ポート設定

このウィンドウを用いて、STP ポートの設定を行い、設定値を表示します。

[L2 機能] > [STP] > [STP ポート設定] をクリックして、以下のウィンドウを表示します。

図 5-28 STP ポート設定

設定パラメータ （[STP ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
コスト	コスト値を入力します。この値は、指定したポートリストへのフォワーディングパケット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、自動的にあるいはメトリック値として設定できます。外部コストに 0 を設定すると、最適効率のリストにおいて、指定したポートへのフォワーディングパケットのスピードが自動的に設定されます。100Mbps ポートのデフォルトポートコストは 200000、Gigabit ポートは 20000 です。数が小さくなるほど、ポートがパケットを転送するよう選択される可能性が高くなります。 （デフォルト：0、設定範囲：0-200000000）
状態	STP ポーの ト状態（**Enabled**/**Disabled**）を選択します。
ガードルート	ガードルートの状態（**Enabled**/**Disabled**）を選択します。
リンクタイプ	リンクタイプオプション（**Auto**/**P2P**/**Shared**）を選択します。全二重ポートは P2P（ポイントツーポイント）接続があるものとみなされます。一方、半二重ポートは共有接続があるものとみなされます。リンクタイプを [Shared] に設定すると、ポートはフォワーディング状態に迅速に移行できません。 （デフォルト：Auto）

パラメータ	概要
ポートファスト	ポートファストポートファストオプションを選択します。 （デフォルト：Network） • **[Network]** - ポートは 3 秒間、non-port-fast 状態のままになります。BPDU を受信しない場合、ポートは port-fast 状態になり、フォワーディング状態に変わります。後から BPDU を受信すると、ポートは non-port-fast 状態に変化します。 • **[Disabled]** - ポートは常に non-port-fast 状態になります。フォワーディング状態になるまでに常に待機し、フォワードタイム遅延が発生します。 • **[Edge]** - リンクアップが生じると、フォワードタイム遅延まで待機せずに、ポートは直接 spanning-tree forwarding 状態に遷移します。後からインタフェースが BPDU を受信すると、その動作状態が non-port-fast 状態に変化します。
TCN フィルタ	TCN（トポロジ変更通知）フィルタのオプションを有効または無効にします。ポートを TCN フィルタモードに設定すると、ポートが受信する TC イベントは無視されます。 （デフォルト：無効）
BPDU フォワード	BPDU フォワード状態（**Enabled**/**Disabled**）を選択します。**[Enabled]** にすると、受信した STP BPDU がすべての VLAN メンバポートにアンタグ形式で転送されます。 （デフォルト：無効）
優先度	優先度値（**0 ～ 240**）を選択します。値が小さいほど、優先度が高くなります。（デフォルト：128）
Hello タイム	ここにハロータイムの値（秒）を入力します。この値により、各設定メッセージの周期的な送信の間に代表ポートが待機する間隔を指定します。（設定範囲：1-2）

[**適用**] ボタン - 設定内容を反映します。

5.3.3 MST コンフィグレーション識別

このウィンドウを用いて、MST コンフィグレーション ID の設定を行い、設定値を表示します。この設定によって、スイッチに設定されている MSTI（Multiple Spanning Tree Instance）を識別します。デフォルトの CIST（Common Internal Spanning Tree）は変更できますが、削除できません。また、MSTI ID は変更できません。

[L2 機能] > [STP] > [MST コンフィグレーション識別] をクリックして、以下のウィンドウを表示します。

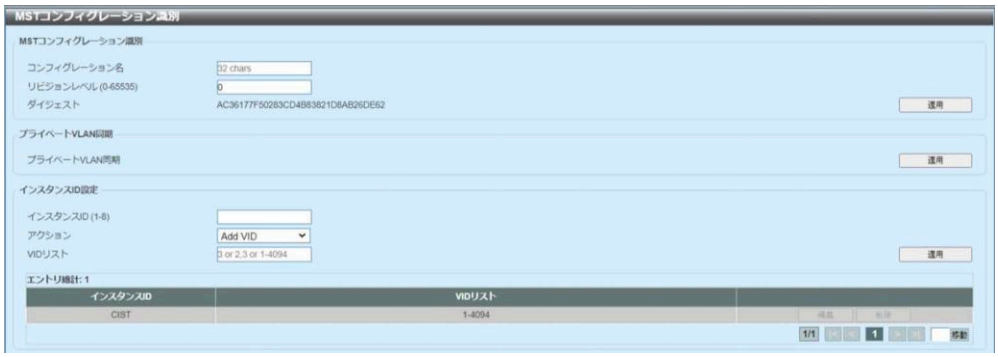


図 5-29 MST コンフィグレーション識別

設定パラメータ （[MST コンフィグレーション識別] セクション）

パラメータ	概要
コンフィグレーション名	MST を入力します。この名前は MSTI を一意に識別します。コンフィグレーション名を設定しない場合、このフィールドには MSTP を実行している装置への MAC アドレスが表示されます。（最大：32 文字）
リビジョンレベル	リビジョンレベル値を入力します。この値はコンフィグレーション名とともに、スイッチに設定されている MSTP 領域を識別します。（デフォルト：0、設定範囲：0-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[インスタンス ID 設定] セクション）

パラメータ	概要
インスタンス ID	インスタンス ID を入力します。（設定範囲：1-8）
アクション	実行するアクション（**Add**/**Add VID**/**Remove VID**）を選択します。
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。
[**編集**] ボタン - エントリの設定を編集します。
[**削除**] ボタン - エントリを削除します。

5.3.4 STP インスタンス

このウィンドウを用いて、STP インスタンスの設定を行い、設定値を表示します。

[L2 機能] > [STP] > [STP インスタンス] をクリックして、以下のウィンドウを表示します。

図 5-30 STP インスタンス

設定パラメータ （[STP インスタンス] セクション）

パラメータ	概要
インスタンス優先度	**[編集]** ボタンをクリックした後、インスタンス優先度の値を入力します。

[**編集**] ボタン - エントリの設定を編集します。

5.3.5 MSTP ポートインフォメーション

このウィンドウを用いて、MSTP ポートインフォメーションを設定し、表示します。

[L2 機能] > [STP] > [MSTP ポートインフォメーション] をクリックして、以下のウィンドウを表示します。

図 5-31 MSTP ポートインフォメーション

設定パラメータ （[MSTP ポートインフォメーション] セクション）

パラメータ	概要
ポート	ポートを選択します。
コスト	**[編集]** ボタンをクリックした後、コスト値を入力します。
優先度	**[編集]** ボタンをクリックした後、優先度の値を入力します。値が小さいほど、優先度が高くなります。（デフォルト：128）

[**検知プロトコルクリア**] ボタン - 検出されたプロトコルの関連付けを指定のポートから削除します。
[**検索**] ボタン - 検索結果を表示します。
[**編集**] ボタン - エントリの設定を編集します

5.4 ループ検知・遮断

5.4.1 ループ検知・遮断の設定

このウィンドウを用いて、ループ検知・遮断の設定を行い、設定値を表示します。

[L2 機能] > [ループ検知・遮断] > [ループ検知・遮断設定] をクリックして、以下のウィンドウを表示します。

図 5-32 ループ検知・遮断設定

設定パラメータ （[ループ検知・遮断設定] セクション）

パラメータ	概要
グローバル状態	ループ検知・遮断状態（**Enabled**/**Disabled**）を選択します。
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの回線ループバックの状態（**有効** / **無効**）を選択します。
モード	指定したポートで使用するループ検知・遮断モードを選択します。 • **Shutdown** - ループ発生時に、ポートをまずシャットダウン状態に設定し、その後でブロッキング状態に設定します。 • **Block** - ループ発生時に、ポートを直接ブロッキング状態に設定します。
ループ復旧	ループ復旧の状態（**有効** / **無効**）を選択します。有効にすると、タイムアウト値が期限切れになった後にポートは正常状態に回復します。タイムアウト値を表示された入力フィールドに入力します。

[**適用**] ボタン - 設定内容を反映します。

5.4.2 ループヒストリーログ

このウィンドウを用いて、ループヒストリーログを表示およびクリアします。

[L2 機能] > [ループ検知・遮断] > [ループヒストリーログ] をクリックして、以下のウィンドウを表示します。

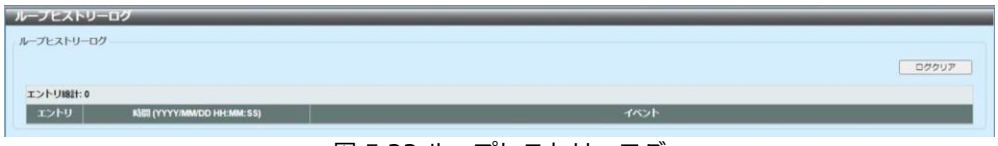


図 5-33 ループヒストリーログ

[ログクリア] ボタン - テーブルからログエントリをクリアします。

5.5 リンクアグリゲーション

このウィンドウを用いて、リンクアグリゲーションの設定を行い、設定値を表示します。

[L2 機能] > [リンクアグリゲーション] をクリックして、以下のウィンドウを表示します。

図 5-34 リンクアグリゲーション

設定パラメータ

パラメータ	概要
システム優先度	使用するシステム優先度の値を入力します。システム優先度によって、ポートチャネルに参加可能なポート、およびスタンドアロンモードになるポートが決定します。値が小さいほど、優先度が高くなります。同じ優先度を持つポートが 2 つ以上ある場合、ポート番号によって優先度が決まります。（デフォルト：32768、設定範囲：1-65535）
ロードバランス アルゴリズム	使用するロードバランスアルゴリズム（**Source MAC**/**Destination MAC**/**Source Destination MAC**/**Source IP**/**Destination IP**/**Source Destination IP**）を選択します。（デフォルト：Source Destination MAC）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[チャネルグループ情報] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
グループ **ID**	チャネルグループ番号を入力します。物理ポートが初めてチャネルグループに参加すると、自動的にポートチャネルが作成されます。1 つのインタフェースが参加できるチャネルグループは 1 つだけです。（設定範囲：1-6）

パラメータ	概要
モード	モードのオプション（**Static**/**Active**/**Passive**）を選択します。**[Static]** モードを指定した場合、チャネルグループタイプはスタティックです。**[Active]** モードまたは **[Passive]** モードを指定した場合、チャネルグループタイプは LACP（Link Aggregation Control Protocol）です。1 つのチャネルグループを構成するのは、スタティックメンバまたは LACP メンバのいずれかのみとなります。チャネルグループのタイプが決定した後は、他のタイプのインタフェースはそのチャネルグループに参加できません。

[**追加**] ボタン - エントリを追加します。
[**メンバポート削除**] ボタン - メンバポートを削除します。
[**チャネル削除**] ボタン - エントリを削除します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**編集**] ボタン - エントリの設定を編集します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

5.6 L2 プロトコルトンネル

このウィンドウを用いて、レイヤ 2 プロトコルトンネルの設定を行い、設定値を表示します。

[L2 機能] > [L2 プロトコルトンネル] をクリックして、以下のウィンドウを表示します。

図 5-35 L2 プロトコルトンネル（L2 プロトコルトンネルグローバル設定）

設定パラメータ （[L2 プロトコルトンネルグローバル設定] タブ）

パラメータ	概要
カプセル化パケット CoS	カプセル化パケットの CoS 値（**0 ～ 7**）を選択します。 **[デフォルト]** オプションを選択した場合、デフォルト値を使用します。
廃棄閾値	廃棄閾値を入力します。レイヤ 2 プロトコルパケットのトンネリングでは、パケットの暗号化、復号、転送に CPU の処理能力が消費されます。このオプションを用いて、CPU の処理帯域幅の消費量を制限します。システムで処理可能なすべてのレイヤ 2 プロトコルパケットの数に対して、閾値を指定します。パケットの最大数を超過したプロトコルパケットは破棄されます。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。 （デフォルト：0、設定範囲：100-20000）
アクション	実行するアクション（**Add**/**Delete**）を選択します。 これにより、L2PT（Layer 2 Protocol Tunneling）のトンネリングマルチキャストアドレスを、指定したプロトコルに追加、あるいは指定したプロトコルから削除します。
トンネルプロトコル	トンネルプロトコルを選択します。 • **GVRP** - 設定済みのアドレスに GVRP パケットがトンネリングされます。 • **STP** - 設定済みのアドレスに STP パケットがトンネリングされます。 • **MAC** - 指定したディスティネーションアドレスを持つプロトコルパケットが、設定したアドレスにトンネリングされます。 • **All** - 設定済みのアドレスにすべてのパケットがトンネリングされます。

パラメータ	概要
プロトコル MAC	([トンネルプロトコル] パラメータで [MAC] 選択時に設定可) 設定したアドレスにトンネリングされるディスティネーションアドレス（**01-00-0C-CC-CC-CC**/**01-00-0C-CC-CC-CD**）を選択します。
MAC アドレス	指定したプロトコルのトンネリング先の MAC アドレスを入力します。この MAC アドレスには、他のプロトコルで予約または使用されているアドレスは指定できません。

[**適用**] ボタン - 設定内容を反映します。

[L2 プロトコルトンネルポート設定] タブをクリックして、以下のウィンドウを表示します。

図 5-36 L2 プロトコルトンネル（L2 プロトコルトンネルポート設定）

設定パラメータ （[L2 プロトコルトンネルポート設定] タブ）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
アクション	アクションを選択します。 • **Add** - 入力した情報に基づいてエントリを追加します。 • **Delete -** 入力した情報に基づいてエントリを削除します。
タイプ	タイプのオプション（**None**/**Shutdown**/**Drop**）を選択します。
トンネルプロトコル	トンネルプロトコルのオプション（**GVRP**/**STP**/**Protocol MAC**/**All**）を選択します。
プロトコル MAC	([トンネルプロトコル] パラメータで [プロトコル MAC] 選択時に設定可) プロトコル MAC のオプション（**01-00-0C-CC-CC-CC**/**01-00-0C-CC-CC-CD**）を選択します。
閾値	([タイプ] パラメータで [Shutdown] または [Drop] 選択時に設定可) 閾値を入力します。

[**適用**] ボタン - エントリを追加します。
[**全クリア**] ボタン - すべてのエントリから情報をクリアします。
[**クリア**] ボタン - エントリから情報をクリアします。

5.7 L2 マルチキャスト制御

5.7.1 IGMP スヌーピング

5.7.1.1 IGMP スヌーピング設定

このウィンドウを用いて、IGMP（Internet Group Management Protocol）スヌーピングの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [IGMP スヌーピング] > [IGMP スヌーピング設定] をクリックして、以下のウィンドウを表示します。

図 5-37 IGMP スヌーピング設定

設定パラメータ （[グローバル設定] セクション）

パラメータ	概要
グローバル状態	IGMP スヌーピング状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[VLAN 状態設定] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[適用] ボタン - エントリを追加します。

設定パラメータ （[IGMP スヌーピングテーブル] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

[編集] ボタンまたは [修正] ボタンをクリックして、以下のウィンドウを表示します。

図 5-38 IGMP スヌーピング設定（編集、修正）

設定パラメータ （[編集]/[修正]）

パラメータ	概要
ファストリーブ	IGMP スヌーピング高速脱退状態（**有効** / **無効**）を選択します。有効にした場合、システムで IGMP 脱退メッセージを受信すると、ただちにメンバを脱退させます。
クエリア状態	クエリア状態（**有効** / **無効**）を選択します。
クエリバージョン	IGMP スヌーピングクエリアが送信する一般的なクエリパケットバージョン（**1**/**2**/**3**）を選択します。
クエリ間隔	IGMP の一般的なクエリメッセージを IGMP スヌーピングクエリアが周期的に送信する間隔を入力します。 （設定範囲：1-31744）
最大応答時間	IGMP スヌーピングクエリでアドバタイズされている最大応答時間（秒）を入力します。（設定範囲：1-25）
ロバストネス変数	IGMP スヌーピングで使用するロバストネス変数を入力します。（設定範囲：1-7）
最終メンバクエリインターバル	IGMP スヌーピングクエリアによる、IGMP グループ固有またはグループソース固有の（チャネル）クエリメッセージの送信間隔を入力します。（設定範囲：1-25）
プロキシレポーティング	プロキシレポート状態（**有効** / **無効**）を選択します。
ソースアドレス	([プロキシレポーティング] パラメータで [有効] 選択時に設定可) プロキシレポーティングのソース IP アドレスを入力します。
帯域制限	帯域制限値を入力します。 **[制限なし]** オプションをオンにした場合、このプロファイルに帯域制限を適用しません。

[**適用**] ボタン - 設定内容を反映します。

5.7.1.2 IGMP スヌーピンググループ設定

このウィンドウを用いて、IGMP スヌーピンググループの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [IGMP スヌーピング] > [IGMP スヌーピンググループ設定] をクリックして、以下のウィンドウを表示します。

図 5-39 IGMP スヌーピンググループ設定

設定パラメータ （IGMP スヌーピングスタティックグループ設定 [] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
グループアドレス	IP マルチキャストグループアドレスを入力します。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[IGMP スヌーピングスタティックグループテーブル] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
グループアドレス	IP マルチキャストグループアドレスを入力します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.7.1.3 IGMP スヌーピングフィルタ設定

このウィンドウを用いて、IGMP スヌーピングフィルタの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [IGMP スヌーピング] > [IGMP スヌーピングフィルタ設定] をクリックして、以下のウィンドウを表示します。

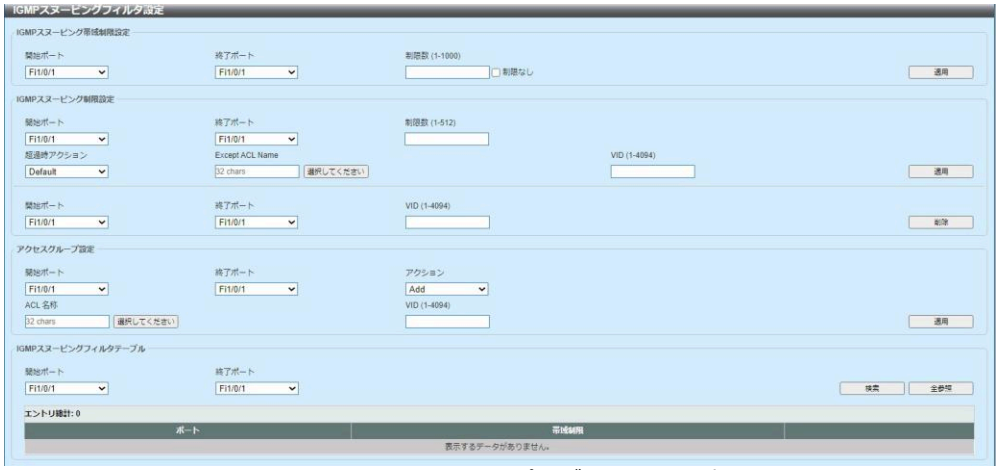


図 5-40 IGMP スヌーピングフィルタ設定

設定パラメータ （[IGMP スヌーピング帯域制限設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
制限数	制限数を入力します。特定のインタフェース上でスイッチが処理できる IGMP 制御パケットのレートを設定します。 （設定範囲：1-1000） **[制限なし]** オプションを選択した場合、制限を取り除きます。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[IGMP スヌーピング制限設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
制限数	制限数を入力します。このパラメータを用いて、作成可能な IGMP キャッシュエントリの数を制限します。 （設定範囲：1-512）
超過時アクション	超過時アクションを選択します。このパラメータを用いて、制限超過時に新たに認識されるグループを処理するための動作を指定します。 • **Default** - デフォルトのアクションが実行されます。 • **Drop** - 新しいグループがドロップされます。 • **Replace** - 新しいグループが最も古いグループと置き換わります。
Except ACL Name	標準 IP アクセスリストの名前を入力します。アクセスリストで許可されているグループ（*,G）またはチャネル（S,G）は、制限から除外されます。チャネルを許可するには、アクセスリストエントリのソースアドレスのフィールドに「S」と指定し、ディスティネーションアドレスのフィールドに「G」と指定します。グループを許可するには、アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。あるいは、**[選択してください]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。（最大：32 文字）
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[アクセスグループ設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
アクション	アクションを選択します。 • **Add** - 入力した情報に基づいてエントリを追加します。 • **Delete** - 入力した情報に基づいてエントリを削除します。
ACL 名称	標準 IP アクセスリストの名前を入力します。このパラメータを用いて、ユーザにグループ（*, G）への参加を許可します。アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。あるいは、**[選択してください]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。（最大：32 文字）
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[IGMP スヌーピングフィルタテーブル] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

5.7.1.4 IGMP スヌーピングマルチキャストルータ情報

このウィンドウを用いて、IGMP スヌーピングマルチキャストルータの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [IGMP スヌーピング] > [IGMP スヌーピングマルチキャストルータ情報] をクリックして、以下のウィンドウを表示します。

図 5-41 IGMP スヌーピングマルチキャストルータ情報

設定パラメータ （[IGMP スヌーピングマルチキャストルータポート設定] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（最大：32 文字）
コンフィグレーション	ポートコンフィグレーションを選択します。 • **Port** - 設定したポートをスタティックマルチキャストルータポートにします。 • **Forbidden Port** - 設定したポートをマルチキャストルータポートにしません。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[**IGMP スヌーピングマルチキャストルータポートテーブル**] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.7.1.5 IGMP スヌーピング統計設定

このウィンドウを用いて、IGMP スヌーピング統計を表示およびクリアします。

[L2 機能] > [L2 マルチキャスト制御] > [IGMP スヌーピング] > [IGMP スヌーピング統計設定] をクリックして、以下のウィンドウを表示します。

図 5-42 IGMP スヌーピング統計設定

設定パラメータ （[IGMP スヌーピング統計設定] セクション）

パラメータ	概要
統計	インタフェース（**All**/**VLAN**/**Port**）を選択します。
VID	([統計] パラメータで [VLAN] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲：1-4094)
開始ポート／終了ポート	([統計] パラメータで [Port] 選択時に設定可) ポートを選択します。

[クリア] ボタン - 指定した条件に基づいて統計情報をクリアします。

設定パラメータ （[IGMP スヌーピング統計テーブル] セクション）

パラメータ	概要
検索タイプ	インタフェースのタイプ（**VLAN**/**Port**）を選択します。
VID	([検索タイプ] パラメータで [VLAN] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲：1-4094)
開始ポート／終了ポート	([検索タイプ] パラメータで [Port] 選択時に設定可) ポートを選択します。

[**検索**] ボタン - 指定した情報に基づいた検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.7.2 MLD スヌーピング

5.7.2.1 MLD スヌーピング設定

このウィンドウを用いて、MLD（Multicast Listener Discovery）スヌーピングの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [MLD スヌーピング] > [MLD スヌーピング設定] をクリックして、以下のウィンドウを表示します。

図 5-43 MLD スヌーピング設定

設定パラメータ （[グローバル設定] セクション）

パラメータ	概要
グローバル状態	MLD スヌーピング状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[VLAN 状態設定] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - エントリを追加します。

設定パラメータ （[MLD スヌーピングテーブル] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

[**編集**] ボタンまたは [**修正**] ボタンをクリックして、以下のウィンドウを表示します。

図 5-44 MLD スヌーピング設定（編集、修正）

設定パラメータ （[編集]>[IGMP スヌーピング VLAN 設定] セクション）

パラメータ	概要
Fast Leave	MLD スヌーピング高速脱退状態（**有効** / **無効**）を選択します。有効にした場合、システムで MLD 脱退メッセージを受信すると、ただちにメンバを脱退させます。
プロキシレポーティング	プロキシレポート状態（**有効** / **無効**）を選択します。
ソースアドレス	([プロキシレポーティング] パラメータで [有効] 選択時に設定可) プロキシレポーティングのソース IP アドレスを入力します。
クエリア状態	クエリア状態（**有効** / **無効**）を選択します。
クエリバージョン	MLD スヌーピングクエリアが送信する一般的なクエリパケットバージョン（**1**/**2**）を選択します。
クエリ間隔	MLD の一般的なクエリメッセージを MLD スヌーピングクエリアが周期的に送信する間隔を入力します。 (設定範囲：1-31744)
最大応答時間	MLD スヌーピングクエリでアドバタイズされている最大応答時間（秒）を入力します。(設定範囲：1-25)
ロバストネス変数	MLD スヌーピングで使用するロバストネス変数を入力します。(設定範囲：1-7)
最終リスナークエリ間隔	MLD スヌーピングクエリアによる、MLD グループ固有またはグループソース固有の（チャネル）クエリメッセージの送信間隔を入力します。(設定範囲：1-25)
帯域制限	帯域制限値を入力します。(設定範囲：1-1000) **[制限なし]** オプションをオンにした場合、このプロファイルに帯域制限を適用しません。

[**適用**] ボタン - 設定内容を反映します。

5.7.2.2 MLD スヌーピンググループ設定

このウィンドウを用いて、MLD スヌーピンググループの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [MLD スヌーピング] > [MLD スヌーピンググループ設定] をクリックして、以下のウィンドウを表示します。

図 5-45 MLD スヌーピンググループ設定

設定パラメータ （[MLD スヌーピングスタティックグループ設定] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
グループアドレス	IPv6 マルチキャストグループアドレスを入力します。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[MLD スヌーピングスタティックグループテーブル] セクション）

パラメータ	概要
VID	使用する VLAN ID を選択および入力します。 （設定範囲：1-4094）
グループアドレス	ラジオボタンをクリックし、IPv6 マルチキャストグループアドレスを入力します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

設定パラメータ （[MLD スヌーピンググループテーブル] セクション）

パラメータ	概要
VID	使用する VLAN ID を選択および入力します。 （設定範囲：1-4094）
グループアドレス	ラジオボタンをクリックし、IPv6 マルチキャストグループアドレスを入力します。
詳細	このオプションを選択した場合、MLD グループの詳細情報を表示します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.7.2.3 MLD スヌーピングフィルタ設定

このウィンドウを用いて、MLD スヌーピングフィルタの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [MLD スヌーピング] > [MLD スヌーピングフィルタ設定] をクリックして、以下のウィンドウを表示します。

図 5-46 MLD スヌーピングフィルタ設定

設定パラメータ （[MLD スヌーピング帯域制限設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
制限数	制限数を入力します。この制限数を用いて、特定のインタフェース上でスイッチが処理できる MLD 制御パケットのレートを設定します。（設定範囲：1-1000） **[制限なし]** オプションを選択した場合、制限を取り除きます。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MLD スヌーピング制限設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
制限数	制限数を入力します。このパラメータを用いて、作成可能な MLD キャッシュエントリの数を制限します。 （設定範囲：1-512）
超過時アクション	超過時アクションを選択します。このパラメータを用いて、制限超過時に新たに認識されるグループを処理するための動作を指定します。 • **Default** - デフォルトのアクションが実行されます。 • **Drop** - 新しいグループがドロップされます。 • **Replace** - 新しいグループが最も古いグループと置き換わります。
Except ACL Name	標準 IP アクセスリストの名前を入力します。アクセスリストで許可されているグループ（*,G）またはチャネル（S,G）は、制限から除外されます。チャネルを許可するには、アクセスリストエントリのソースアドレスのフィールドに「S」と指定し、ディスティネーションアドレスのフィールドに「G」と指定します。グループを許可するには、アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。あるいは、**[選択してください]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。（最大：32 文字）
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[アクセスグループ設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
アクション	アクションを選択します。 • **Add** - 入力した情報に基づいてエントリを追加します。 • **Delete** - 入力した情報に基づいてエントリを削除します。
ACL 名称	標準 IP アクセスリストの名前を入力します。このパラメータを用いて、ユーザにグループ（*, G）への参加を許可します。アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。あるいは、**[選択してください]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。（最大：32 文字）
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MLD スヌーピングフィルタテーブル] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

5.7.2.4 MLD スヌーピングマルチキャストルータ情報

このウィンドウを用いて、MLD スヌーピングマルチキャストルータの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [MLD スヌーピング] > [MLD スヌーピングマルチキャストルータ情報] をクリックして、以下のウィンドウを表示します。

図 5-47 MLD スヌーピングマルチキャストルータ情報

設定パラメータ （[MLD スヌーピングマルチキャストルータポート設定] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
コンフィグレーション	ポートコンフィグレーションを選択します。 • **Port** - 設定済みポートがマルチキャスト対応ルータに接続しているものとします。 • **Forbidden Port** - 設定済みポートがマルチキャスト対応ルータに接続していないものとします。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[MLD スヌーピングマルチキャストルータポートテーブル] セクション）

パラメータ	概要
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.7.2.5 MLD スヌーピング統計設定

このウィンドウを用いて、MLD スヌーピング統計を表示およびクリアします。

[L2 機能] > [L2 マルチキャスト制御] > [MLD スヌーピング] > [MLD スヌーピング統計設定] をクリックして、以下のウィンドウを表示します。

図 5-48 MLD スヌーピング統計設定

設定パラメータ （[MLD スヌーピング統計設定] セクション）

パラメータ	概要
統計	インタフェース（**All**/**VLAN**/**Port**）を選択します。
VID	([統計] パラメータで [VLAN] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲：1-4094)
開始ポート／終了ポート	([統計] パラメータで [Port] 選択時に設定可) ポートを選択します。

[クリア] ボタン - 指定した条件に基づいて統計情報をクリアします。

設定パラメータ （[MLD スヌーピング統計テーブル] セクション）

パラメータ	概要
検索タイプ	インタフェースのタイプ（**VLAN**/**Port**）を選択します。
VID	([検索タイプ] パラメータで [VLAN] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲：1-4094)
開始ポート／終了ポート	([検索タイプ] パラメータで [port] 選択時に設定可) ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

5.7.3 マルチキャストフィルタリングモード

このウィンドウを用いて、マルチキャストフィルタリングモードの設定を行い、設定値を表示します。

[L2 機能] > [L2 マルチキャスト制御] > [マルチキャストフィルタリングモード] をクリックして、以下のウィンドウを表示します。

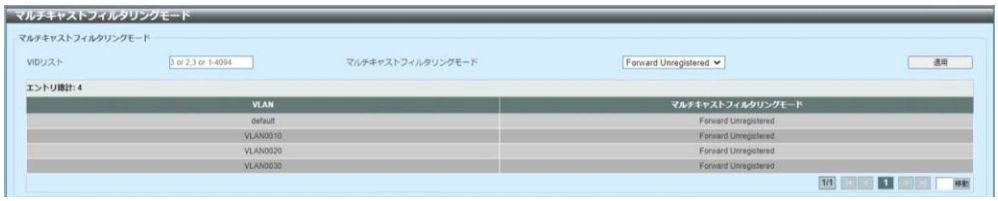


図 5-49 マルチキャストフィルタリングモード

設定パラメータ （[マルチキャストフィルタリングモード] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）
マルチキャストフィルタモード	マルチキャストフィルタモードを選択します。 • **Forward Unregistered** - 登録済みのマルチキャストパケットがフォワーディングテーブルに基づいて転送され、すべての未登録マルチキャストパケットが VLAN ドメインに基づいてフラッディングされます。 • **Forward All** - すべてのマルチキャストパケットが VLAN ドメインに基づいてフラッディングされます。 • **Filter Unregistered** - 登録済みのパケットがフォワーディングテーブルに基づいて転送され、すべての未登録マルチキャストパケットがフィルタリングされます。

[**適用**] ボタン - エントリを追加します。

5.8 LLDP （Link Layer Discovery Protocol）

5.8.1 LLDP グローバル設定

このウィンドウを用いて、グローバル LLDP 設定を行い、設定値を表示します。

[L2 機能] > [LLDP] > [LLDP グローバル設定] をクリックして、以下のウィンドウを表示します。

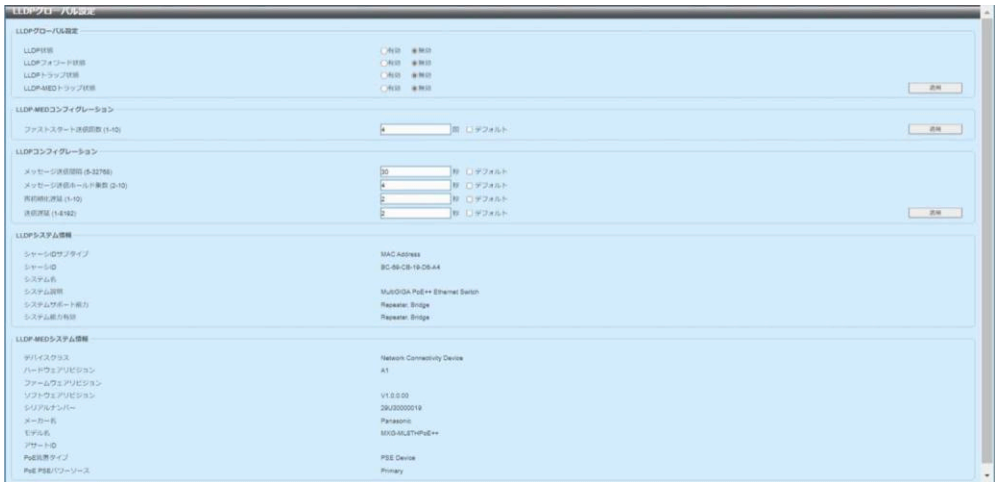


図 5-50 LLDP グローバル設定

設定パラメータ （[LLDP グローバル設定] セクション）

パラメータ	概要
LLDP 状態	LLDP の状態（**有効** / **無効**）を選択します。
LLDP フォワード状態	LLDP フォワードの状態（**有効** / **無効**）を選択します。 **[LLDP 状態]** を無効にし、**[LLDP フォワード状態]** を有効にすると、受信した LLDPDU（LLDP Data Unit）パケットが転送されます。
LLDP トラップ状態	LLDP トラップの状態（**有効** / **無効**）を選択します。
LLDP-MED トラップ状態	LLDP-MED（LLDP Media Endpoint Discovery）トラップの状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[LLDP-MED コンフィグレーション] セクション）

パラメータ	概要
ファストスタート送信回数	LLDP-MED ファストスタート送信回数の値を入力します。（設定範囲：1-10） [**デフォルト**] オプションを選択した場合、デフォルト値を使用します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[LLDP コンフィグレーション] セクション）

パラメータ	概要
メッセージ送信間隔	各物理インタフェースでの連続する LLDP アドバタイズメント送信の間隔（秒）を入力します。（設定範囲：5-32768） [**デフォルト**] オプションを選択した場合、デフォルト値を使用します。
メッセージ送信ホールド乗数	LLDPDU の TTL（Time-To-Live）値の計算に使用する、LLDPDU 送信間隔の乗数を入力します。（設定範囲：2-10） [**デフォルト**] オプションを選択した場合、デフォルト値を使用します。
再初期化遅延	インタフェースでの LLDP 初期化の遅延時間（秒）を入力します。（設定範囲：1-10） [**デフォルト**] オプションを選択した場合、デフォルト値を使用します。
送信遅延	インタフェースでの連続する LLDPDU の送信に対する遅延時間（秒）を入力します。送信間隔タイマーの値の 4 分の 1 を超えないようにしてください。（設定範囲：1-8192） [**デフォルト**] オプションを選択した場合、デフォルト値を使用します。

[**適用**] ボタン - 設定内容を反映します。

5.8.2 LLDP ポート設定

このウィンドウを用いて、LLDP ポートの設定を行い、設定値を表示します。

[L2 機能] > [LLDP] > [LLDP ポート設定] をクリックして、以下のウィンドウを表示します。

図 5-51 LLDP ポート設定

設定パラメータ （[LLLD ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
通知	通知の状態（**Enabled**/**Disabled**）を選択します。
サブタイプ	LLDP TLV（Type-Length-Value）のサブタイプ（**MAC Address**/**Local**）を選択します。
管理状態	ローカル LLDP エージェントを選択し、ポートでの LLDP フレームの送受信を許可します。（デフォルト：TX and RX） • **TX** - ローカル LLDP エージェントは LLDP フレームの送信のみ可能です。 • **RX** - ローカル LLDP エージェントは LLDP フレームの受信のみ可能です。 • **TX and RX**- ローカル LLDP エージェントは LLDP フレームの送受信が可能です。 • **Disabled** - ローカル LLDP エージェントは LLDP フレームの送信も受信もできません。
IP サブタイプ	送信する IP アドレス情報のタイプ（**Default**/**IPv4**/**IPv6**）を選択します。
アクション	実行するアクション（**Remove**/**Add**）を選択します。
アドレス	送信する IP アドレスを入力します。

[**適用**] ボタン - 設定内容を反映します。

5.8.3 LLDP マネジメントアドレスリスト

このウィンドウを用いて、LLDP マネジメントアドレスリストおよび情報を表示します。

[L2 機能] > [LLDP] > [LLDP マネジメントアドレスリスト] をクリックして、以下のウィンドウを表示します。

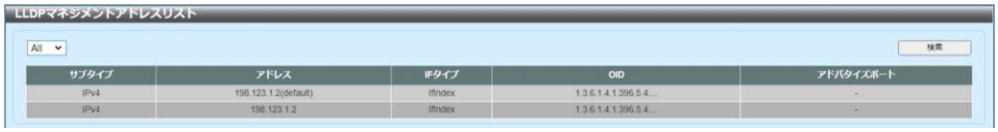


図 5-52 LLDP マネジメントアドレスリスト

設定パラメータ

パラメータ	概要
サブタイプ	サブタイプ（**All**/**IPv4**/**IPv6**）選択します。

[**検索**] ボタン - 検索結果を表示します。

5.8.4 LLDP 基本 TLV 設定

このウィンドウを用いて、LLDP TLV の基本設定を行い、設定値を表示します。

[L2 機能] > [LLDP] > [LLDP 基本 TLV 設定] をクリックして、以下のウィンドウを表示します。

図 5-53 LLDP 基本 TLV 設定

[LLDP 基本 TLV 設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
ポート説明	ポート説明 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
システム名	システム名 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
システム説明	システム説明 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
システム能力	システム能力 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

5.8.5 LLDP Dot1 TLV 設定

このウィンドウを用いて、IEEE 802.1 LLDP TLV の設定を行い、設定値を表示します。

[L2 機能] > [LLDP] > [LLDP Dot1 TLV 設定] をクリックして、以下のウィンドウを表示します。

図 5-54 LLDP Dot1 TLV 設定

設定パラメータ （[LLDP Dot1 TLV 設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
ポート VLAN	ポート VLAN ID TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
プロトコル VLAN	PPVID（ポートとプロトコル VLAN ID）TLV の送信の状態（**Enabled**/**Disabled**）を選択した上、VLAN ID を入力します。（設定範囲：1-4094）
VLAN 名	VLAN 名 TLV 送信の状態（**Enabled**/**Disabled**）を選択した上、VLAN ID を入力します。（設定範囲：1-4094）
プロトコルアイデンティティ	プロトコルアイデンティティ TLV 送信の状態（**Enabled**/**Disabled**）を選択した上、アイデンティティ（**None**/**EAPOL**/**LACP**/**GVRP**/**STP**/**All**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

5.8.6 LLDP Dot3 TLV 設定

このウィンドウを用いて、IEEE 802.3 LLDP TLV の設定を行い、設定値を表示します。

[L2 機能] > [LLDP] > [LLDP Dot3 TLV 設定] をクリックして、以下のウィンドウを表示します。

図 5-55 LLDP Dot3 TLV 設定

設定パラメータ （[LLDP Dot3 TLV 設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
MAC/PHY コンフィグ / 状態	MAC/PHY コンフィグ / 状態 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
リンクアグリゲーション	リンクアグリゲーション TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
最大フレームサイズ	最大フレームサイズ TLV の送信の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

5.8.7 LLDP-MED ポート設定

このウィンドウを用いて、LLDP-MED ポートの設定を行い、設定値を表示します。

[L2 機能] > [LLDP] > [LLDP-MED ポート設定] をクリックして、以下のウィンドウを表示します。

図 5-56 LLDP-MED ポート設定

設定パラメータ （[LLDP-MED ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
通知	LLDP-MED 通知 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
能力	LLDP-MED 能力 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
資産	LLDP-MED 資産管理 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。
ネットワークポリシー	LLDP-MED ネットワークポリシー TLV の送信の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

5.8.8 LLDP 統計情報

このウィンドウを用いて、LLDP 統計を表示およびクリアします。

[L2 機能] > [LLDP] > [LLDP 統計情報] をクリックして、以下のウィンドウを表示します。

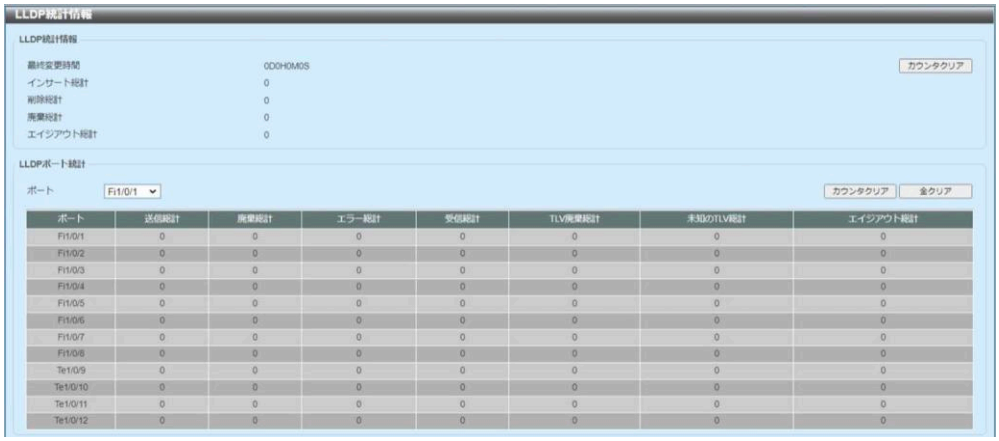


図 5-57 LLDP 統計情報

設定パラメータ （[LLDP ポート統計] セクション）

パラメータ	概要
ポート	ポートを選択します。

[クリア] ボタン - カウンタ情報をクリアします。
[全クリア] ボタン - すべてのポートのカウンタ情報をクリアします。

5.8.9 LLDP ローカルポート情報

このウィンドウを用いて、ローカル LLDP ポート情報を表示します。

[L2 機能] > [LLDP] > [LLDP ローカルポート情報] をクリックして、以下のウィンドウを表示します。

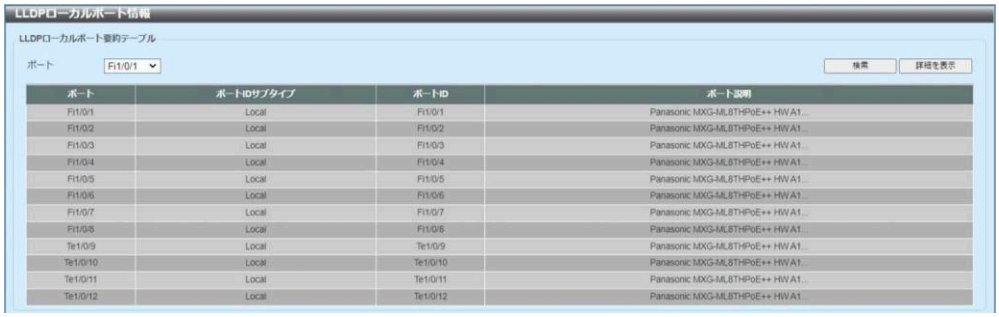


図 5-58 LLDP ローカルポート情報

設定パラメータ （[LLDP ローカルポート要約テーブル] セクション）

パラメータ	概要
ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**詳細参照**] ボタン - LLDP ローカルポート詳細情報を表示します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

5.8.10 LLDP ネイバーポート情報

このウィンドウを用いて、ネイバーの LLDP ポート情報を表示します。

[L2 機能] > [LLDP] > [LLDP ネイバーポート情報] をクリックして、以下のウィンドウを表示します。

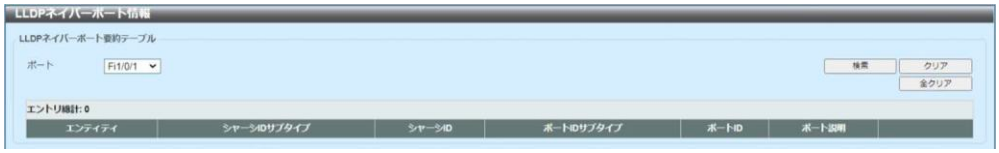


図 5-59 LLDP ネイバーポート情報

設定パラメータ （[LLDP ネイバーポート要約テーブル] セクション）

パラメータ	概要
ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**クリア**] ボタン - LLDP ネイバーポート情報をクリアします。
[**全クリア**] ボタン - すべての LLDP ネイバーポート情報をクリアします。

5.9 UDLD （Unidirectional Link Detection）

UDLD はインターフェースの誤動作やケーブル誤配線、回線障害、メディアコンバータ障害等によって引き起こされる片方向リンク障害の検知を契機に、インターフェースをエラー閉塞（error disabled）状態にする機能です。
本装置ではイーサネット物理インターフェース（ポート）を検知対象としており、IEEE802.3ah（Ethernet in the First Mile; EFM 機能）の Information OAMPDU フレーム（以降、EFM フレームと呼称）を対向装置間で送受信し、片方向リンク障害を検知します。
片方向リンク障害の検知は、UDLD 機能が有効化されているインターフェースにおいて、アクティブモードにて EFM 機能の初期状態で片方向リンク障害検知時間の間、対向装置より EFM フレームの受信がない場合と、対向装置より EFM リンクフォールト（受信リンク障害）通知を 5 秒間継続して受信した場合となります。

このウィンドウを用いて、UDLD 機能の設定を行い、設定値と情報を表示します。

[L2 機能] > [UDLD] をクリックして、以下のウィンドウを表示します。

図 5-60 UDLD

設定パラメータ （[UDLD グローバル設定] セクション）

パラメータ	概要
EFM OAM グローバル状態	EFM 機能が本装置で有効化 / 無効化されていることを示します。**有効** / **無効**ボタンを選択し、[適用] ボタンをクリックして、本装置の EFM 機能を有効化 / 無効化します。 （デフォルト：無効）
リンクフォールト検知状態	UDLD 機能が本装置で有効化 / 無効化されていることを示します。**有効** / **無効**ボタンを選択し、[適用] ボタンをクリックして、本装置の UDLD 機能を有効化 / 無効化します。 （デフォルト：無効）
リンクフォールト検知タイマー	本装置の片方向リンク障害検知時間（秒）を示します。 時間入力するか、[デフォルト] ボタンをチェックし、[適用] ボタンをクリックして、本装置の片方向リンク障害検知時間を設定します。（設定範囲：5 ～ 300、デフォルト適用時：5） EFM 機能の初期状態で、指定した片方向リンク障害検知時間の間、対向装置より EFM フレームの受信がない場合、片方向リンク障害を検知したと判断し、当該インターフェースを片方向リンク障害検知（EFM OAM Detect-UDL）要因でエラー閉塞（error disabled）状態にします。

設定パラメータ （[UDLD ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	EFM 機能、UDLD 機能を設定するインターフェース（イーサネット物理ポート）の範囲を開始ポート、終了ポートで指定します。
EFM 状態	インターフェースの EFM 機能を有効化 / 無効化します。 （**Disabled**：無効化、**Enabled**：有効化、デフォルト：Disabled） 有効化された場合、本装置の EFM 機能が有効化されていれば、当該インターフェースで、EFM 機能動作（EFM フレームの送受信）を開始します。
EFM OAM UDLD 状態	インターフェースの UDLD 機能を有効化 / 無効化します。 （**Disabled**：無効化、**Enabled**：有効化、デフォルト：Disabled） インターフェースの UDLD 機能を有効化するには、本装置で UDLD 機能が有効化されていることが必要です。

パラメータ	概要
モード	インターフェースの EFM 動作モードを選択します。 • **Active** - EFM 機能の初期状態では、EFM フレームを対向装置に周期的に送信し、対向装置より EFM フレームの受信を待ちます。 • **Passive** - EFM 機能の初期状態では、アクティブモードの対向装置より EFM フレームの受信を待ち、その EFM フレームを受信してから、対向装置に EFM フレームを送信します。
（設定更新）	上記各パラメータ値の設定後、[適用] ボタンをクリックして、当該インターフェースの UDLD ポート設定を更新します
（UDLD ポート設定・情報一覧）	UDLD ポート設定値と状態情報を一覧表形式で表示します。
インタフェース	インターフェース ID：EFM 機能、UDLD 機能が有効化されているインターフェース（イーサネット物理ポート）。
リンク	**Up**/**Down**/**Shutdown**：インターフェースのリンク状態。 **Up**：リンクアップ状態。 **Down**：リンクダウン状態。 **Shutdown**：設定にてシャットダウンされた（Shutdown）状態、あるいは、障害検知にてエラー閉塞された（Error Disabled）状態。
EFM 状態	**有効** / **無効**：インターフェースの EFM 状態。 インターフェースの EFM 機能が有効化 / 無効化されていることを示します。
モード	**アクティブ** / **パッシブ**：インターフェースの EFM 動作モードを示します。
UDLD 状態	Bidirectional/Unidirectional/（表示なし）：インターフェースの UDLD 状態を示します。Bidirectional：対向装置間で双方向通信が行えている状態。（双方向のリンクがどちらも正常に動作） Unidirectional：対向装置間で片方向リンク障害を検出した状態。（リンクはエラー閉塞） （表示なし）：対向装置間通信の状態が不明。（Unknown：Bidirectional か Unidirectional かまだ判断がつかない状態）
ネイバー MAC アドレス	MAC アドレス値：対向装置の MAC アドレス。
ネイバーホスト名	文字列：対向装置のホスト名（例：MXGML8THPoE++_1）。
ネイバーポート	インターフェース ID：EFM 通信における対向装置側の送受信イーサネット物理ポート番号。

[**適用**] ボタン - 設定内容を反映します。

NOTE 本機能（EFM 機能ベースの UDLD 機能）は当社製品でのみご使用いただけます。

5.10 RRP （Ring Redundant Protocol）

このウィンドウを用いて、RRP 設定を行い、設定値を表示します。

[L2 機能] > [RRP] をクリックして、以下のウィンドウを表示します。

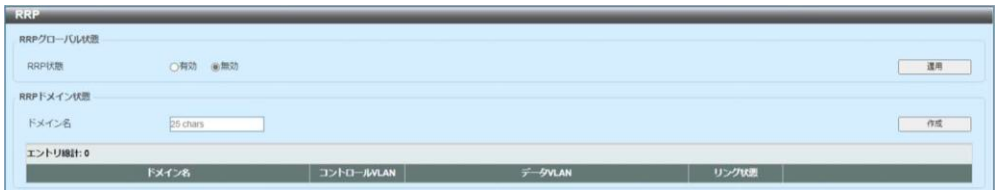


図 5-61 RRP

設定パラメータ （[RRP グローバル状態] セクション）

パラメータ	概要
RRP 状態	RRP 状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[RRP ドメイン状態] セクション）

パラメータ	概要
ドメイン名	RRP ドメイン名を入力します。（最大 : 25 文字） このドメインは物理リングを表します。

[**作成**] ボタン - 新しい RRP ドメインを作成します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

[**詳細参照**]>[**編集**] ボタンをクリックして、以下のウィンドウを表示します。

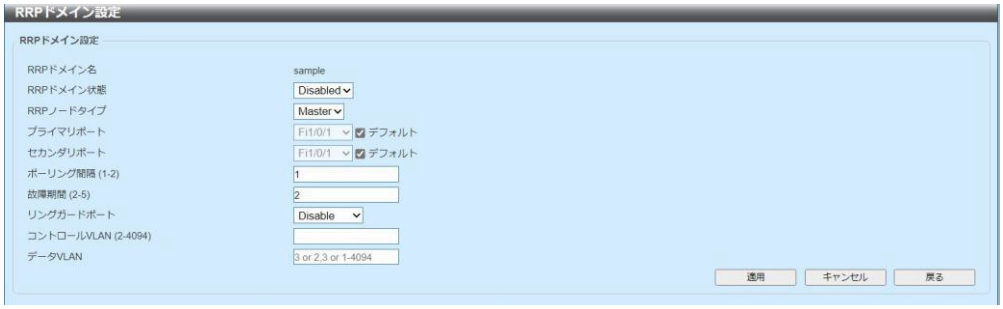


図 5-62 RRP（編集）

設定パラメータ （[編集]>[RRP ドメイン設定] セクション）

パラメータ	概要
RRP ドメイン状態	RRP ドメイン状態（**Enabled**/**Disabled**）を選択します。
RRP ノードタイプ	RRP ノードのタイプを選択します。 • **Master** - ノードをドメイン内のマスターノードとして指定します。1 つの RRP ドメインに指定できるマスターノードは 1 つだけです。マスターノードの役割には、リングポーリングとリング回復が含まれます。 • **Transit** - ノードをドメイン内のトランジットノードとして指定します。1 つの RRP ドメインに多くのトランジットノードを指定できます。トランジットノードの役割にはリンクダウンアラートが含まれます。
プライマリポート	プライマリポートを選択します。このポートが RRP ドメイン内の 1 つ目のポートになります。 [**デフォルト**] オプションを選択した場合、現在の設定をクリアします。
セカンダリポート	セカンダリスポートを選択します。このポートが RRP ドメイン内の 2 つ目のポートになります。 [**デフォルト**] オプションを選択した場合、現在の設定をクリアします。
ポーリング間隔	ハローパケットのポーリング間隔（秒）を入力します。ポーリング間隔は故障期間よりも短くしてください。 （設定範囲：1-2）
故障期間	故障期間（秒）を入力します。故障期間はポーリング間隔よりも長くしてください。（設定範囲：2-5）
リングガードポート	RRP リングのガードポートの状態を選択します。 • **Primary** - リングガード対応ポートとしてプライマリポートを指定します。 • **Secondary** - リングガード対応ポートとしてセカンダリポートを指定します。 • **Both** - リングガード対応ポートとしてプライマリポートとセカンダリポートの両方を指定します。 • **Disable** - この機能を無効にします。
コントロール VLAN	コントロール VLAN の ID を入力します。 （設定範囲：2-4094）
データ VLAN	データ VLAN の ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。
[**キャンセル**] ボタン - 変更を破棄します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

6 L3 機能

6.1 ARP （Address Resolution Protocol）

6.1.1 ARP エージング時間

このウィンドウを用いて、ARP エージング時間の設定を行い、設定値を表示します。

[L3 機能] > [ARP] > [ARP エージング時間] をクリックして、以下のウィンドウを表示します。

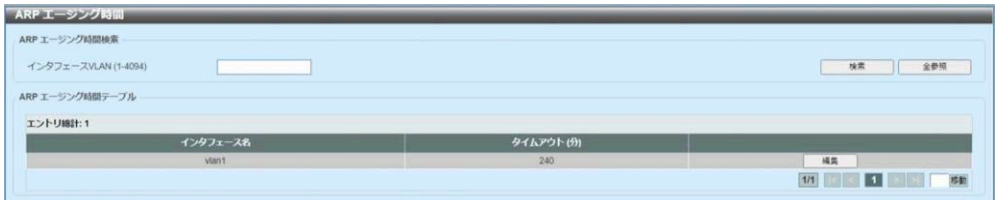


図 6-1 ARP エージング時間

設定パラメータ （[ARP エージング時間検索] セクション）

パラメータ	概要
インタフェース VLAN	VLAN ID を入力します。（設定範囲：1-4094）
タイムアウト	**[編集]** ボタンをクリックした後、タイムアウト値を入力します。

[検索] ボタン - 検索結果を表示します。
[全参照] ボタン - エントリをすべて表示します。
[**編集**] ボタン - エントリの設定を編集します。

6.1.2 スタティック ARP

このウィンドウを用いて、スタティック ARP の設定を行い、設定値を表示します。

[L3 機能] > [ARP] > [スタティック ARP] をクリックして、以下のウィンドウを表示します。

図 6-2 スタティック ARP

設定パラメータ （[スタティック ARP 設定] セクション）

パラメータ	概要
IP アドレス	MAC アドレスに関連付ける IP アドレスを入力します。
ハードウェアアドレス	IP アドレスに関連付ける MAC アドレスを入力します。

[**適用**] ボタン - スタティック ARP エントリを追加します。

設定パラメータ （[スタティック ARP 検索] セクション）

パラメータ	概要
IP アドレス	エントリの IP アドレスを選択および入力します。
IP ネットワークマスク	IP アドレスのサブネットマスクを選択および入力します。
ハードウェアアドレス	エントリの MAC アドレスを選択および入力します。
インタフェース VLAN	VLAN ID を選択および入力します。（設定範囲：1-4094）

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**編集**] ボタン - エントリの設定を編集します。
[**削除**] ボタン - エントリを削除します。

6.1.3 ARP テーブル

このウィンドウを用いて、テーブル内の ARP エントリを表示およびクリアします。

[L3 機能] > [ARP] > [ARP テーブル] をクリックして、以下のウィンドウを表示します。

図 6-3 ARP テーブル

設定パラメータ （[ARP 検索] セクション）

パラメータ	概要
インタフェース **VLAN**	インタフェースの VLAN ID を選択および入力します。 （設定範囲：1-4094）
IP アドレス	表示する IP アドレスを選択および入力します。
マスク	IP アドレスのサブネットマスクを選択および入力します。
ハードウェアアドレス	表示する MAC アドレスを選択および入力します。
タイプ	タイプ（**All**/**Dynamic**）を選択します。

[検索] ボタン - 検索結果を表示します。
[**全クリア**] ボタン - すべてのエントリをテーブルからクリアします。
[クリア] ボタン - エントリをクリアします。

6.2 Gratuitous ARP

このウィンドウを用いて、Gratuitous ARP の設定を行い、設定値を表示します。Gratuitous ARP リクエストパケットは、ソースとディスティネーションの IP アドレスが両方とも送信装置の IP アドレスに設定され、ディスティネーション MAC アドレスがブロードキャストアドレスである、ARP リクエストパケットです。
装置は Gratuitous ARP リクエストパケットを使用して、IP アドレスが他のホストと重複しているかどうかを明らかにします。あるいは、インタフェースに接続されているホストの ARP キャッシュエントリをあらかじめ読み込むか再設定します。

[L3 機能] > [Gratuitous ARP] をクリックして、以下のウィンドウを表示します。

図 6-4 Gratuitous ARP

設定パラメータ （[Gratuitous ARP グローバル設定] セクション）

パラメータ	概要
IP Gratuitous ARP 状態	Gratuitous ARP リクエストパケットの送信の状態（**有効** / **無効**）を選択します。
Gratuitous ARP トラップ状態	Gratuitous ARP 機能のトラップの状態（**有効** / **無効**）を選択します。
IP Gratuitous ARP Dad-Reply 状態	IP Gratuitous ARP Dad-Reply の状態（**有効** / **無効**）を選択します。
Gratuitous ARP 学習状態	Gratuitous ARP 学習の状態（**有効** / **無効**）を選択します。通常、システムは ARP リクエストパケットからの ARP エントリ、またはスイッチの IP アドレスの MAC アドレスを要求する通常の ARP リクエストパケットからの ARP エントリのみを学習します。このオプションを用いて、受信した Gratuitous ARP パケットに基づく ARP エントリの学習を有効または無効にします。Gratuitous ARP パケットはソース IP アドレスによって送信され、パケットがクエリしている IP アドレスと同一になります。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[Gratuitous ARP グローバル設定] セクション）

パラメータ	概要
間隔時間	**[編集]** ボタンをクリックした後、Gratuitous ARP 送信間隔時間（秒）を入力します。

[**編集**] ボタン - エントリの設定を編集します。

6.3 IPv6 ネイバー

このウィンドウを用いて、IPv6 ネイバーの設定を行い、設定値を表示します。

[L3 機能] > [IPv6 ネイバー] をクリックして、以下のウィンドウを表示します。

図 6-5 IPv6 ネイバー

設定パラメータ （[IPv6 ネイバー設定] セクション）

パラメータ	概要
インタフェース VLAN	VLAN インタフェース ID を入力します。 （設定範囲：1-4094）
IPv6 アドレス	IPv6 アドレスを入力します。
MAC アドレス	MAC アドレスを入力します。

[**適用**] ボタン - エントリを追加します。
[検索] ボタン - 検索結果を表示します。
[クリア] ボタン - 指定した情報に基づいた情報をクリアします。
[**全クリア**] ボタン - すべてのダイナミックエントリをクリアします。
[**削除**] ボタン - エントリを削除します。

6.4 インタフェース

6.4.1 IPv4 インタフェース

このウィンドウを用いて、IPv4 インタフェースの設定を行い、設定値を表示します。

[L3 機能] > [インタフェース] > [IPv4 インタフェース] をクリックして、以下のウィンドウを表示します。

図 6-6 IPv4 インタフェース

設定パラメータ （[IPv4 インタフェース] セクション）

パラメータ	概要
インタフェース **VLAN**	インタフェース VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[**編集**] ボタン - エントリの設定を編集します。

設定パラメータ（[編集]>[IPv4 インタフェース設定] タブ >[設定] セクション）

パラメータ	概要
状態	IPv4 インタフェース状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ（[編集]>[IPv4 インタフェース設定] タブ >[IP 設定] セクション）

パラメータ	概要
IP 取得方法	IP アドレスの取得方法を選択します。 • **Static** - このインタフェースの IPv4 アドレス設定を表示された入力フィールドに手動で入力します。 • **DHCP** - このインタフェースが、ローカルネットワークにある DHCP サーバから自動的に IPv4 設定を取得します。
IP アドレス	このインタフェースの IPv4 アドレスを入力します。
マスク	このインタフェースの IPv4 サブネットマスクを入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ（[編集]>[DHCP クライアント] タブ）

パラメータ	概要
クラス ID 文字列	クラス ID の文字列を入力します。（最大：32 文字） [**16 進数**] オプションを選択した場合、クラス ID の文字列を 16 進数形式で入力します。（最大：64 文字） このパラメータを用いて、DHCP discover メッセージの Option 60 の値として使用するベンダクラス ID を指定します。
ホスト名	ホスト名を入力します。このパラメータを用いて、DHCP discover メッセージで送信するホスト名オプションの値を指定します。（最大：64 文字）
リース	DHCP クライアントのリース期間を入力します。必要に応じて選択することもできます。テキストボックスには、リース期間を日数で入力できます。（設定範囲：0-10000） 必要に応じて、[**時間**] と [**分**] を選択することもできます。

[**適用**] ボタン - 設定内容を反映します。

6.4.2 IPv6 インタフェース

このウィンドウを用いて、IPv6 インタフェースの設定を行い、設定値を表示します。

[L3 機能] > [インタフェース] > [IPv6 インタフェース] をクリックして、以下のウィンドウを表示します。

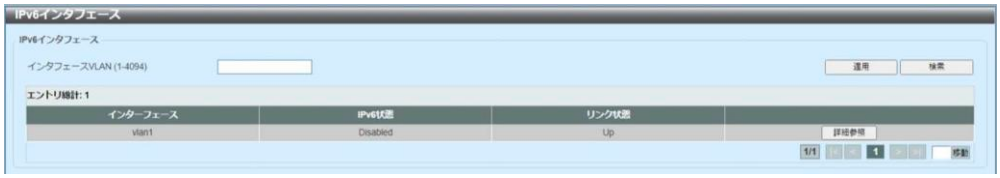


図 6-7 IPv6 インタフェース

設定パラメータ （[IPv6 インタフェース] セクション）

パラメータ	概要
インタフェース VLAN	IPv6 エントリに関連付ける VLAN インタフェース ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

設定パラメータ （[詳細参照]>[IPv6 インタフェース設定] タブ）

パラメータ	概要
IPv6 状態	IPv6 インタフェース状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[詳細参照]>[IPv6 インタフェース設定] タブン）

パラメータ	概要
IPv6 アドレス	この IPv6 インタフェースの IPv6 アドレスを入力します。 • **EUI-64** - EUI-64（Extended Unique Identifier 64-bit）インタフェース ID を使用するインタフェースで IPv6 アドレスを設定します。 • **リンクローカル** - IPv6 インタフェースのリンクローカルアドレスを設定します。

[**適用**] ボタン - 設定内容を反映します。

[インタフェース IPv6 アドレス] タブをクリックして、インタフェース IPv6 アドレスのエントリ統計を表示します。

設定パラメータ （[詳細参照]>[ネイバー探索] タブ）

パラメータ	概要
NS 間隔	NS（Neighbor Solicitation）間隔の値（ミリ秒）を入力します。0 を設定した場合、ルータは 1 秒を使用します。

[**適用**] ボタン - エントリを追加します。
[**編集**] ボタン - エントリの設定を編集します。

設定パラメータ （[詳細参照]>[DHCPv6 クライアント] タブ）

パラメータ	概要
クライアント状態	DHCPv6 クライアントサービス状態（**Enabled/Disabled**）を選択します。 [**高速コミット**] オプションを選択した場合、アドレス委任の 2 メッセージ交換を続行します。高速コミットオプションは Solicit メッセージに含まれ、2 メッセージハンドシェイクを要求します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[詳細参照]>[DHCPv6 クライアント] タブ）

パラメータ	概要
クライアント PD 状態	指定したインタフェース経由で PD（プレフィックス委任）を要求する DHCPv6 クライアントプロセス状態（**Enabled/Disabled**）を選択します。 [**高速コミット**] オプションを選択した場合、プレフィックス委任の 2 メッセージ交換を続行します。高速コミットオプションは Solicit メッセージに含まれ、2 メッセージハンドシェイクを要求します。
ジェネラル プレフィックス名	IPv6 ジェネラルプレフィックス名を入力します。 (最大：12 文字)

[**適用**] ボタン - 設定内容を反映します。

[**リスタート**]ボタン - DHCPv6クライアント機能を再開します。

6.5 IPv4 デフォルトルート

このウィンドウを用いて、IPv4 デフォルトルートの設定を行い、設定値を表示します。

[L3 機能] > [IPv4 デフォルトルート **]** をクリックして、以下のウィンドウを表示します。

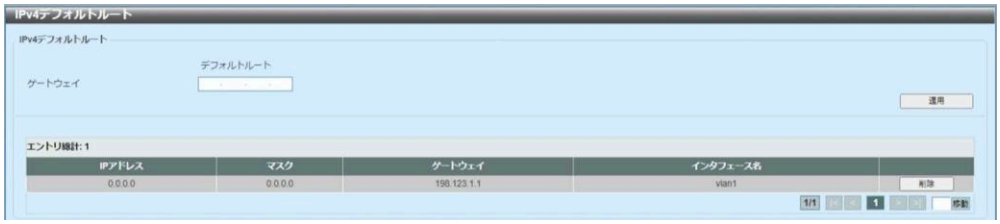


図 6-8 IPv4 デフォルトルート

設定パラメータ （[IPv4 デフォルトルート] セクション）

パラメータ	概要
ゲートウェイ	ゲートウェイアドレスを入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

6.6 IPv4 ルートテーブル

このウィンドウを用いて、IPv4 ルートテーブルおよび情報を表示します。

[L3 機能] > [IPv4 ルートテーブル] をクリックして、以下のウィンドウを表示します。

図 6-9 IPv4 ルートテーブル

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

6.7 IPv6 デフォルトルート

このウィンドウを用いて、IPv6 デフォルトルートの設定を行い、設定値を表示します。

[L3 機能] > [IPv6 デフォルトルート] をクリックして、以下のウィンドウを表示します。

図 6-10 IPv6 デフォルトルート

設定パラメータ （[IPv6 デフォルトルート] セクション）

パラメータ	概要
インタフェース名	このルートに関連付けるインタフェースの名前を入力します。
ネクストホップ **IPv6** アドレス	ネクストホップの IPv6 アドレスを入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

6.8 IPv6 ルートテーブル

このウィンドウを用いて、IPv6 ルートテーブルおよび情報を表示します。

[L3 機能] > [IPv6 ルートテーブル] をクリックして、以下のウィンドウを表示します。

図 6-11 IPv6 ルートテーブル

[**検索**] ボタン - 検索結果を表示します。

[要約] オプションをクリックして、以下のウィンドウを表示します。

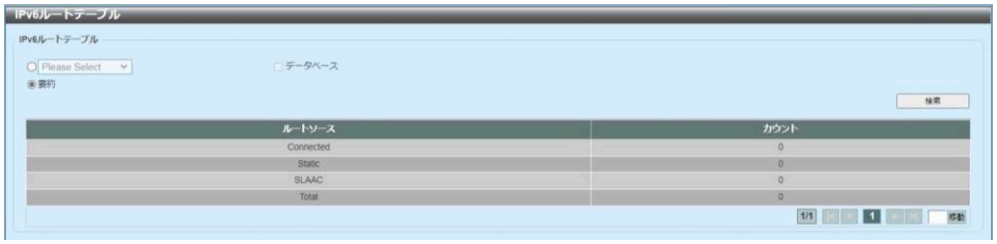


図 6-12 IPv6 ルートテーブル（要約）

[**検索**] ボタン - 検索結果を表示します。

6.9 IPv6 ジェネラルプレフィックス

このウィンドウを用いて、IPv6 ジェネラルプレフィックスの設定を行い、設定値を表示します。

[L3 機能] > [IPv6 ジェネラルプレフィックス] をクリックして、以下のウィンドウを表示します。

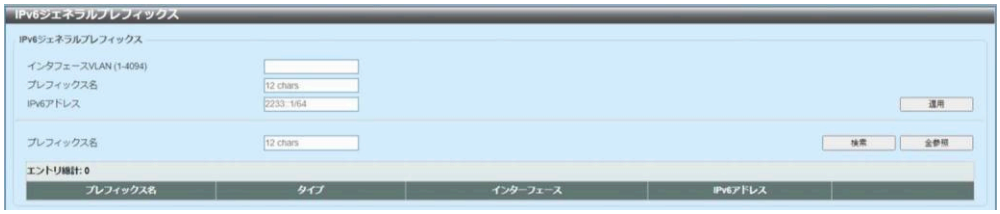


図 6-13 IPv6 ジェネラルプレフィックス

設定パラメータ （[IPv6 ジェネラルプレフィックス] セクション）

パラメータ	概要
インタフェース VLAN	使用する VLAN インタフェース ID を入力します。 （設定範囲：1-4094）
プレフィックス名	IPv6 ジェネラルプレフィックスエントリ名を入力します。 （最大：12 文字）
IPv6 アドレス	IPv6 アドレスとプレフィックス長を入力します。IPv6 アドレスのプレフィックス長は、VLAN インタフェースのローカルサブネットでもあります。

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。
[**削除**] ボタン - エントリを削除します。

6.9.0.1 IP マルチキャストフォワーディングキャッシュ

このウィンドウを用いて、IP マルチキャストフォワーディングキャッシュ情報を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [IPMC] > [IP マルチキャストフォワーディングキャッシュ] をクリックして、以下のウィンドウを表示します。

図 6-14 IP マルチキャストフォワーディングキャッシュ

設定パラメータ （[IP マルチキャストフォワーディングテーブル] セクション）

パラメータ	概要
グループアドレス	マルチキャストグループ IP アドレスを入力します。
ソースアドレス	マルチキャストソース IP アドレスを入力します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**] ボタン - エントリをすべて表示します。

6.9.0.2 IPv6 マルチキャストルーティングフォワーディング キャッシュテーブル

このウィンドウを用いて、IPv6 マルチキャストルーティングフォワーディング キャッシュ情報を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [IPv6MC] > [IPv6 マルチキャストルーティングフォワーディングキャッシュテーブル] をクリックして、以下のウィンドウを表示します。

図 6-15 IPv6 マルチキャストルーティングフォワーディングキャッシュテーブル

設定パラメータ （[IPv6 マルチキャストルーティングフォワーディングキャッシュテーブル] セクション）

パラメータ	概要
グループ **IPv6** アドレス	マルチキャストグループ IPv6 アドレスを入力します。
ソース **IPv6** アドレス	マルチキャストソース IPv6 アドレスを入力します。

[**検索**] ボタン - 検索結果を表示します。
[**全参照**]ボタン - エントリをすべて表示します。

7 QoS（Quality of Service）

7.1 基本設定

7.1.1 ポートデフォルト CoS

このウィンドウを用いて、ポートインタフェースごとにデフォルト CoS（Class of Service）の設定を行い、設定値を表示します。

[QoS] > [基本設定] > [ポートデフォルト CoS] をクリックして、以下のウィンドウを表示します。

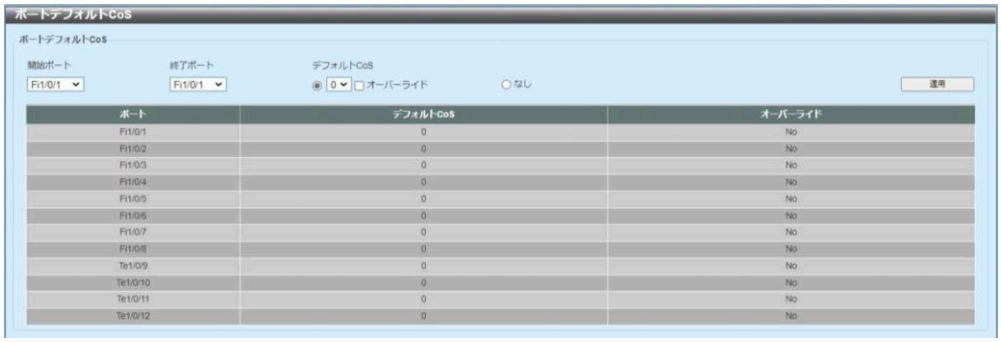


図 7-1 ポートデフォルト CoS

設定パラメータ （[ポートデフォルト CoS] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
デフォルト **CoS**	指定するポートのデフォルト CoS オプション（**0 ～ 7**）を選択します。 • **オーバーライド** - パケットの CoS が無視されます。デフォルト CoS が、ポートで受信されるすべての着信パケット（タグ / アンタグ）に適用されます。 • **なし** - パケットがタグ付けされていればパケットの CoS が、タグ付けされていなければポートのデフォルト CoS が、それぞれパケットの CoS になります。

[**適用**] ボタン - 設定内容を反映します。

7.1.2 ポートスケジューラ方式

このウィンドウを用いて、スケジューラ機能に関する方式の設定を行い、設定値を表示します。

[QoS] > [基本設定] > [ポートスケジューラ方式] をクリックして、以下のウィンドウを表示します。

図 7-2 ポートスケジューラ方式

設定パラメータ （[ポートスケジューラ方式] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

パラメータ	概要
スケジューラ方式	指定したポートに適用するスケジューラ方式を選択します。（デフォルト：Weighted Round Robin） • **絶対優先（Strict Priority）** - すべてのキューで絶対優先スケジューリングを使用します。これは、CoS が最も高いキューから最も低いキューまでを実行する、絶対優先アクセスです。 • **ラウンドロビン（Round Robin）** - すべてのキューでラウンドロビンスケジューリングを使用します。これは、各キューで 1 つのパケットにサービスを提供したら次のキューに移動する、公平なアクセスです。 • **加重ラウンドロビン（Weighted Round Robin）** - 許可されたパケットをラウンドロビンの順番に送信キューに送ることによって動作します。最初に、各キューは設定可能な重み付けに重さを設定します。優先度の高い CoS キューからパケットが送信されるたびに、対応する重み付けが 1 だけ差し引かれ、次に低い CoS キューのパケットがサービスを受けます。CoS キューの重み付けが 0 に到達すると、キューが補充されるまでキューのサービスは停止します。すべての CoS キューの重み付けが 0 に到達すると、その時点で重み付けは補充されます。 • **加重不足ラウンドロビン（Weighted Deficit Round Robin）** - ラウンドロビンの順番に、送信キューに蓄積されている未処理クレジットに対してサービスを提供します。最初に、各キューは設定可能なクォンタム値にクレジットカウンタを設定します。CoS キューからのパケットが送信されるたびに、パケットのサイズが対応するクレジットカウンタから差し引かれ、次に低い CoS キューにサービス権が渡されます。クレジットカウンタが 0 を下回る場合、クレジットが補充されるまでキューのサービスは停止します。すべての CoS キューのクレジットカウンタが 0 に到達すると、その時点でクレジットカウンタは補充されます。クレジットカウンタが 0 またはマイナスになり、最後のパケットが完全に送信されるまで、すべてのパケットにサービスが提供されます。この状態が発生すると、クレジットは補充されます。クレジットが補充されると、クレジットのクォンタムが各 CoS キューのクレジットカウンタに追加されます。各 CoS キューのクォンタムはユーザのコンフィグレーションによって異なる場合があります。 特定の CoS キューを SP モードに設定するには、それより優先度の高いすべての CoS キューも絶対優先モードでなければなりません。

[**適用**] ボタン - 設定内容を反映します。

7.1.3 キュー設定

このウィンドウを用いて、QoS キューの設定を行い、設定値を表示します。

[QoS] > [基本設定] > [キュー設定] をクリックして、以下のウィンドウを表示します。

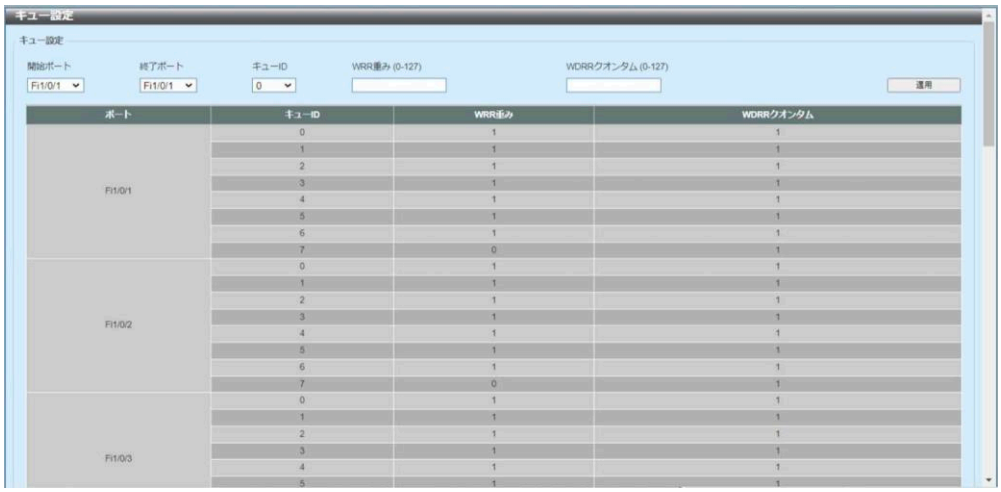


図 7-3 キュー設定

設定パラメータ （[キュー設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
キュー ID	キュー ID 値を入力します。
WRR 重み	WRR 重み値を入力します。（設定範囲：0-127） EF（Expedited Forwarding）の動作要件を満たすために、PHB（Per-hop Behavior）EF によって最も高いキューを常に選択します。また、このキューのスケジュールモードを絶対優先スケジューリングに指定する必要があります Differentiate Service がサポートされている限り、最後のキューの重み付けは 0 でなければなりません。
WDRR クオンタム	WDRR クオンタム値を入力します。（設定範囲：0-127）

[**適用**] ボタン - 設定内容を反映します。

7.1.4 CoS 送信キューマッピング

このウィンドウを用いて、CoS 送信キューマッピングの設定を行い、設定値を表示します。

[QoS] > [基本設定] > [CoS 送信キューマッピング] をクリックして、以下のウィンドウを表示します。

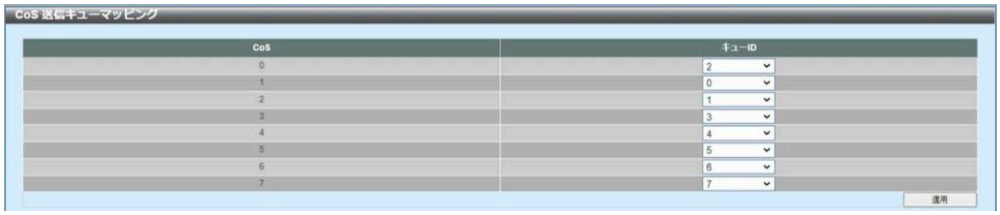


図 7-4 CoS 送信キューマッピング

設定パラメータ

パラメータ	概要
キュー ID	対応する CoS 値にマッピングするキュー ID（**0 ～ 7**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

7.1.5 ポート帯域制限

このウィンドウを用いて、ポート帯域制限の設定を行い、設定値を表示します。

[QoS] > [基本設定] > [ポート帯域制限] をクリックして、以下のウィンドウを表示します。

図 7-5 ポート帯域制限

設定パラメータ （[ポート帯域制限] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向オプションを選択します。 • **Input** - 入口パケットの帯域制限を設定します。 • **Output** - 出口パケットの帯域制限を設定します。
帯域制限	帯域制限値を選択および入力します。 • **[帯域幅]** - 使用する入力／出力帯域幅とバーストサイズ値を入力します。（設定範囲：64-10000000） • **[パーセント]** - 使用する入力／出力帯域幅とバーストサイズ値を入力します。（設定範囲：1-100） • **[なし]** - 指定したポートの帯域制限は削除されます。指定した制限が、指定したインタフェースの最高速度を超過することはありません。入口帯域幅の制限の場合、受信トラフィックが制限を超えると、入口で pause フレームまたはフロー制御フレームが送信されます。

[**適用**] ボタン - 設定内容を反映します。

7.1.6 キュー帯域制限

このウィンドウを用いて、キュー帯域制限の設定を行い、設定値を表示します。

[QoS] > [基本設定] > [キュー帯域制限] をクリックして、以下のウィンドウを表示します。

図 7-6 キュー帯域制限

設定パラメータ （[キュー帯域制限] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
キュー ID	設定するキュー ID（**0** ～ **7**）を選択します。
帯域制限	キューの帯域制限設定を選択および入力します。 • **[最小帯域]** - 帯域制限の最小帯域と帯域制限の最大帯域を入力します。最小の帯域幅を設定すると、キューから送信されるパケットが保証されます。最大の帯域幅を設定すると、帯域幅が利用可能な場合でも、キューから送信されるパケットが最大の帯域幅を超えることはありません。最小帯域幅を設定する場合、設定する最小帯域幅のアグリゲートはインタフェース帯域幅の 75% 未満でなければなりません。これにより、設定する最小帯域幅を保証します。絶対優先キューに最低保証帯域幅を設定する必要はありません。これは、すべてのキューの最小帯域幅を満たす場合に、このキューのトラフィックにまずサービスが提供されるからです。このコマンドのコンフィグレーションは物理ポートにのみアタッチされ、ポートチャネルにはアタッチされません。これは、1 つの CoS の最低保証帯域幅であり、物理ポート全体では使用できません。（設定範囲：64-10000000） • **[最小パーセント]** - 最小帯域のパーセント値と最大パーセント値を入力します。（設定範囲：1-100） • **[なし]** - 指定したポートに帯域制限は割り当てられません。

[**適用**] ボタン - 設定内容を反映します。

7.2 高度な設定

7.2.1 DSCP 変換マップ

このウィンドウを用いて、DSCP（Differentiated Services Code Point）変換マップの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [DSCP 変換マップ] をクリックして、以下のウィンドウを表示します。

図 7-7 DSCP 変換マップ

設定パラメータ （[DSCP 変換マップ] セクション）

パラメータ	概要
ミューテーション名	DSCP 変換マップ名を入力します。（最大：32 文字）
入力 DSCP リスト	入力 DSCP リスト値を入力します。（設定範囲：0-63）
出力 DSCP リスト	出力 DSCP 値を入力します。（設定範囲：0-63）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

7.2.2 ポート信頼状態および Mutation バインディング

このウィンドウを用いて、ポート信頼状態およびミューテーションのバインディングの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [ポート信頼状態および Mutation バインディング] をクリックして、以下のウィンドウを表示します。

図 7-8 ポート信頼状態および Mutation バインディング

設定パラメータ （[ポート信頼状態および Mutation バインディング] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
信頼状態	ポート信頼状態（**CoS**/**DSCP**）を選択します。。
DSCP 変換マップ	DSCP 変換マップ名を入力します。（最大：32 文字） **[なし]** オプションを選択した場合、DSCP 変換マップをポートに割り当てません。

[**適用**] ボタン - 設定内容を反映します。

7.2.3 DSCP CoS マッピング

このウィンドウを用いて、DSCP CoS マッピングの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [DSCP CoS マッピング] をクリックして、以下のウィンドウを表示します。

図 7-9 DSCP CoS マッピング

設定パラメータ （[DSCP CoS マッピング] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
CoS	DSCP リストにマッピングする CoS 値（**0 ～ 7**）を選択します。
DSCP リスト	CoS 値にマッピングする DSCP リスト値（**0 ～ 63**）を入力します。

[**適用**] ボタン - 設定内容を反映します。

7.2.4 CoS カラーマッピング

このウィンドウを用いて、CoS カラーマッピングの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [CoS カラーマッピング] をクリックして、以下のウィンドウを表示します。

図 7-10 CoS カラーマッピング

設定パラメータ （[CoS カラーマッピング] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
CoS リスト	色にマッピングする CoS 値を入力します。（設定範囲：0-7）
色	CoS 値にマッピングする色（**Green**/**Yellow**/**Red**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

7.2.5 DSCP カラーマッピング

このウィンドウを用いて、DSCP カラーマッピングの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [DSCP カラーマッピング] をクリックして、以下のウィンドウを表示します。

図 7-11 DSCP カラーマッピング

[DSCP カラーマッピング] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
DSCP リスト	色にマッピングする DSCP リスト値を入力します。 （設定範囲：0-63）
色	DSCP 値にマッピングする色（**Green**/**Yellow**/**Red**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

7.2.6 クラスマップ

このウィンドウを用いて、クラスマップの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [クラスマップ] をクリックして、以下のウィンドウを表示します。

図 7-12 クラスマップ

設定パラメータ

パラメータ	概要
クラスマップ名	クラスマップ名を入力します。（最大：32 文字）
複数適合基準	複数適合基準オプション（**Match All**/**Match Any**）を選択します。

[**適用**] ボタン - エントリを追加します。
[**適合**] ボタン - エントリの適合ルールを設定します。
[**削除**] ボタン - エントリを削除します。

[**適合**] ボタンをクリックして、以下のウィンドウを表示します。

図 7-13 クラスマップ（適合）

設定パラメータ （[適合]>[適合ルール] セクション）

パラメータ	概要
なし	このオプションを選択した場合、このクラスマップには何も適合させません。
指定	このオプションを選択した場合、以下のいずれかをこのクラスマップと適合させます。
ACL 名称	このクラスマップと適合するアクセスリスト名を選択および入力します。（最大：32 文字）
CoS リスト	このクラスマップと適合する CoS リスト値を選択および入力します。（設定範囲：0-7）
DSCP リスト	このクラスマップと適合する DSCP リスト値を選択および入力します。（設定範囲：0-63） **[IPv4 のみ]** オプションをオンにした場合、IPv4 パケットのみ適合します。指定しない場合、IPv4 と IPv6 の両方のパケットを対象とした照合になります。
優先度リスト	このクラスマップと適合する優先度リスト値を選択および入力します。（設定範囲：0-7） **[IPv4 のみ]** オプションをオンにした場合、IPv4 パケットのみ適合します。指定しない場合、IPv4 と IPv6 の両方のパケットを対象とした照合になります。IPv6 パケットの場合、IPv6 ヘッダのトラフィッククラスの最上位 3 ビットが優先度になります。
プロトコル名	このクラスマップと適合するプロトコル名（**ARP**/**BGP**/**DHCP**/**DNS**/**EGP**/**FTP**/**IPv4**/**IPv6**/**NetBIOS**/**NFS**/**NTP**/**OSPF**/**PPPoE**/**RIP**/**RTSP**/**SSH**/**Telnet**/**TFTP**）を選択します。
VID リスト	クラスマップと適合する VLAN ID を選択および入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

7.2.7 集約ポリサー

このウィンドウを用いて、集約ポリサーの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [集約ポリサー] をクリックして、以下のウィンドウを表示します。

図 7-14 集約ポリサー（シングルレート設定）

設定パラメータ （[シングルレート設定] タブ）

パラメータ	概要
集約ポリサー名	集約ポリサー名を入力します。
平均レート	平均レート値を入力します。（設定範囲：0-10000000）
ノーマルバーストサイズ	ノーマルバーストサイズ値を入力します。 （設定範囲：0-16384）
最大バーストサイズ	最大バーストサイズ値を入力します。（設定範囲：0-16384）
適合トラフィックアクション	確認アクションを選択します。確認アクションは、緑色のパケットに対して実行するアクションを指定します。 （デフォルト：Transmit） • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

パラメータ	概要
超過時アクション	超過時アクションを選択します。超過時アクションは、帯域制限を超過したパケットに対して実行するアクションを指定します。（デフォルト：Drop） • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
違反時アクション	違反時アクションを選択します。違反時アクションは、シングルレートポリシングの通常および最大のバーストサイズに違反するパケットに対して実行するアクションを指定します。CIR と PIR の両方に適合しなかったパケットに対して実行するアクションを指定します。シングルレートポリサーでは、違反時アクションを指定しない場合にシングルレート 2 カラーポリサーが作成されます。ツーレートポリサーでは、違反時アクションを指定しない場合のデフォルトアクションは超過時アクションになります。 • **None** - 何もアクションを実行しません。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
Color Aware	Color Aware 機能の有効、無効を設定します。 • **有効** - ポリサーは Color Aware モードで動作します。 • **無効** - ポリサーは Color Blind モードで動作します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

[2 レート設定] タブをクリックして、以下のウィンドウを表示します。

図 7-15 集約ポリサー（2 レート設定）

設定パラメータ （[2 レート設定] タブ）

パラメータ	概要
集約ポリサー名	集約ポリサー名を入力します。
CIR	CIR（Committed Information Rate）値を入力します。 認定パケットレートは、ツーレートメータリングの最初のトークンバケットです。（設定範囲：0-10000000）
バースト確認	バースト確認値を入力します。バースト確認値は、最初のトークンバケットのバーストサイズ（キロバイト）を指定します。（設定範囲：0-16384）
PIR	PIR（Peak Information Rate）値を入力します。 ピーク情報レートは、ツーレートメータリングの 2 番目のトークンバケットです。（設定範囲：0-10000000）
ピークバースト	ピークバースト値を入力します。ピークバースト値は、2 番目のトークンバケットのバーストサイズ（キロバイト）です。 （設定範囲：0-16384）
適合トラフィックアクション	確認アクションを選択します。確認アクションは、緑色のパケットに対して実行するアクションを指定します。 （デフォルト：Transmit） • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

パラメータ	概要
超過時アクション	超過時アクションを選択します。超過時アクションは、帯域制限を超過したパケットに対して実行するアクションを指定します。（デフォルト：Drop） • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
違反時アクション	違反時アクションを選択します。違反時アクションは、シングルレートポリシングの通常および最大のバーストサイズに違反するパケットに対して実行するアクションを指定します。CIR と PIR の両方に適合しなかったパケットに対して実行するアクションを指定します。シングルレートポリサーでは、違反時アクションを指定しない場合にシングルレート 2 カラーポリサーが作成されます。ツーレートポリサーでは、違反時アクションを指定しない場合のデフォルトアクションは超過時アクションになります。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
Color Aware	Color Aware 機能の有効、無効を設定します。 • **有効** - ポリサーは Color Aware モードで動作します。 • **無効** - ポリサーは Color Blind モードで動作します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

7.2.8 ポリシーマップ

このウィンドウを用いて、ポリシーマップの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [ポリシーマップ] をクリックして、以下のウィンドウを表示します。

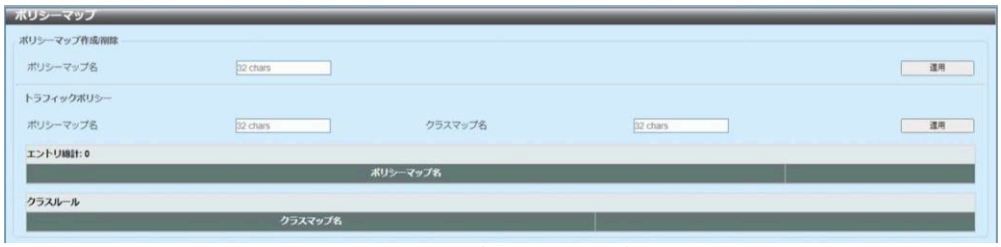


図 7-16 ポリシーマップ

設定パラメータ （[ポリシーマップ作成／削除] セクション）

パラメータ	概要
ポリシーマップ名	作成または削除するポリシーマップ名を入力します。 （最大：32 文字）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[トラフィックポリシー] セクション）

パラメータ	概要
ポリシーマップ名	ポリシーマップ名を入力します。（最大：32 文字）
クラスマップ名	クラスマップ名を入力します。（最大：32 文字）

[**適用**] ボタン - エントリを追加します。
[**アクション設定**] ボタン - エントリのアクションを設定します。
[**ポリサー**] ボタン - エントリの Police Action を設定します。
[**削除**] ボタン - エントリを削除します。

[アクション設定] ボタンをクリックして、以下のウィンドウを表示します。

図 7-17 ポリシーマップ（アクション設定）

設定パラメータ （[アクション設定]>[アクション設定] パラメータ）

パラメータ	概要
なし	このオプションを選択した場合、何もアクションを実行しません。
指定	このオプションを選択した場合、コンフィグレーションに基づいてアクションを実行します。
Precedence	パケットの新優先度値（**0 ～ 7**）を選択します。 **[IPv4 のみ]** オプションを選択した場合、IPv4 の優先度のみマークされます。選択しない場合、IPv4 と IPv6 の両方の優先度がマークされます。IPv6 パケットの場合、IPv6 ヘッダのトラフィッククラスの最上位 3 ビットが優先度になります。
DSCP	パケットの新 DSCP 値（**0 ～ 63**）を選択します。 **[IPv4 のみ]** オプションを選択した場合、IPv4 の DSCP のみマークされます。選択しない場合、IPv4 と IPv6 の両方の DSCP がマークされます。
CoS	パケットの CoS 値（**0 ～ 7**）を選択します。
ハードウェアキュー	パケットのハードウェアキュー値（**0 ～ 7**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

[ポリサー] ボタンをクリックし、[**指定**] パラメーターで [**Police**] を選択し、以下のウィンドウを表示します。

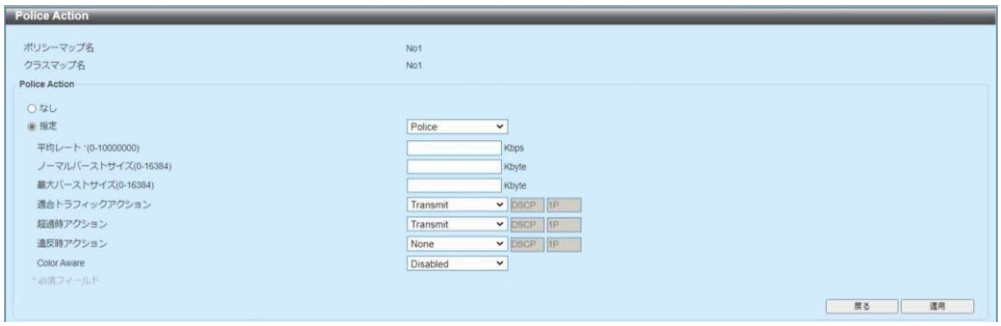


図 7-18 ポリシーマップ（ポリサー、Police）

設定パラメータ （[ポリサー]>[Police Action] セクション）

パラメータ	概要
なし	このオプションを選択した場合、このエントリにポリサーは設定されません。
指定	適用するポリサー設定（**Police**）を選択します。
平均レート	平均レート値を入力します。（設定範囲：0-10000000）
ノーマルバーストサイズ	ノーマルバーストサイズ値を入力します。 （設定範囲：0-16384）
最大バーストサイズ	最大バーストサイズ値を入力します。（設定範囲：0-16384）
適合トラフィック アクション	実行する適合トラフィックアクションを選択します。このアクションは、緑色のパケットに対して実行します。選択する値は以下のとおりです。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

パラメータ	概要
超過時アクション	実行する超過時アクションを選択します。このアクションは、帯域制限を超過する黄色のパケットに対して実行します。選択する値は以下のとおりです。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
違反時アクション	実行する違反時アクションを選択します。このアクションは、赤色のパケットに対して実行します。選択する値は以下のとおりです。 • **None** - 何も違反時アクションを実行しません。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
Color Aware	Color Aware の状態（**Enabled**/**Disabled**）を選択します。 • **Enabled** - Color Aware モードで動作します。 • **Disabled** - Color Blind モードで動作します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

[ポリサー] ボタンをクリックし、[**指定**] パラメーターで [**Police CIR**] を選択し、以下のウィンドウを表示します。

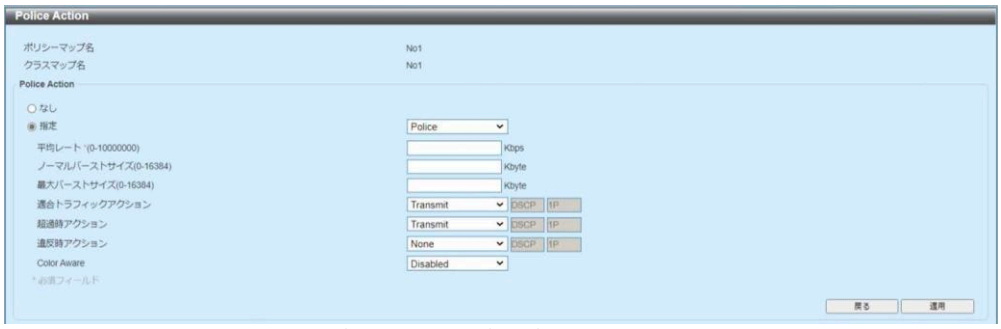


図 7-19 ポリシーマップ（ポリサー、Police CIR）

設定パラメータ （[ポリサー]>[Police Action] セクション）

パラメータ	概要
なし	このオプションを選択した場合、このエントリにポリサーは設定されません。
指定	適用するポリサー設定（**Police CIR**）を選択します。
CIR	CIR（Committed Information Rate）値を入力します。これは、ツーレートメータリングの最初のトークンバケットです。 （設定範囲：0-10000000）
バースト確認	バースト確認値を入力します。これは、最初のトークンバケットのサイズです。（設定範囲：0-16384）
PIR	PIR（Peak Information Rate）値を入力します。これは、ツーレートメータリングの 2 番目のトークンバケットです。 （設定範囲：0-10000000）
ピークバースト	ピークバースト値を入力します。これは、2 番目のトークンバケットのサイズです。 （設定範囲：0-16384）
適合トラフィックアクション	実行する適合トラフィックアクションを選択します。このアクションは、緑色のパケットに対して実行します。選択する値は以下のとおりです。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

パラメータ	概要
超過時アクション	実行する超過時アクションを選択します。このアクションは、帯域制限を超過する黄色のパケットに対して実行します。選択する値は以下のとおりです。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **Transmit** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
違反時アクション	実行する違反時アクションを選択します。このアクションは、赤色のパケットに対して実行します。選択する値は以下のとおりです。 • **None** - 何も違反時アクションを実行しません。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
Color Aware	Color Aware の状態（**Enabled**/**Disabled**）を選択します。 • **Enabled** - Color Aware モードで動作します。 • **Disabled** - Color Blind モードで動作します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

[ポリサー] ボタンをクリックし、[**指定**] パラメーターで [**Police Aggregate**] を選択し、以下のウィンドウを表示します。

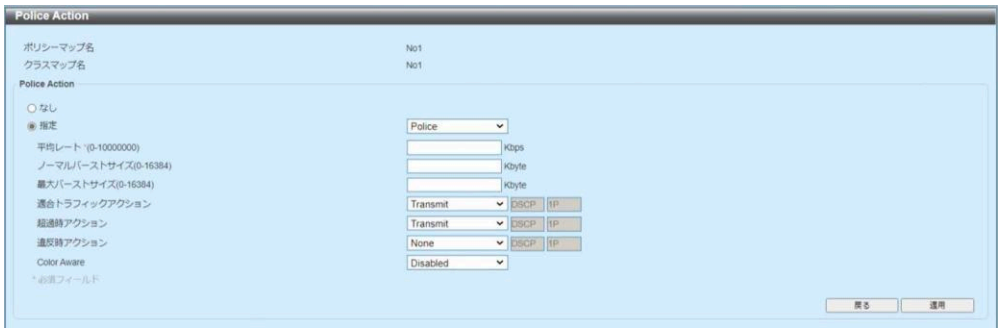


図 7-20 ポリシーマップ（ポリサー、Police Aggregate）

設定パラメータ （[ポリサー]>[Police Action] セクション）

パラメータ	概要
なし	このオプションを選択した場合、このエントリにポリサーは設定されません。
指定	適用するポリサー設定（**Police Aggregate**）を選択します。
集約ポリサー名	集約ポリシングルールの名前を入力します。（最大：32 文字）

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

7.2.9 ポリシーバインディング

このウィンドウを用いて、ポリシーバインディングの設定を行い、設定値を表示します。

[QoS] > [高度な設定] > [ポリシーバインディング] をクリックして、以下のウィンドウを表示します。

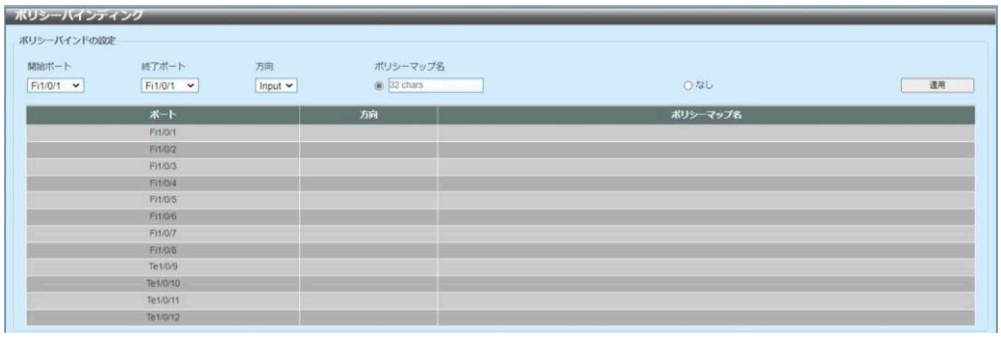


図 7-21 ポリシーバインディング

設定パラメータ （[ポリシーバインドの設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向（**Input**）を選択します。
ポリシーマップ名	ポリシーマップ名を入力します。（最大：32 文字） **[なし]** オプションを選択した場合、このエントリにポリシーマップを関連付けません。

[**適用**] ボタン - 設定内容を反映します。

8 ACL（Access Control List）

8.1 ACL 設定ウィザード

このウィンドウを用いて、[ACL 設定ウィザード] で新規および既存の ACL を設定します。

[ACL] > [ACL 設定ウィザード] をクリックして、以下のウィンドウを表示します。

図 8-1 ACL 設定ウィザード（作成）

設定パラメータ

パラメータ	概要
作成	このオプションを選択した場合、設定ウィザードを使用して新しい ACL アクセスリストを作成します。
ACL 名称	新しい ACL 名称を入力します。（最大：32 文字）
アップデート	このオプションを選択した場合、既存の ACL アクセスリストをアップデートします。テーブルで既存の ACL を選択して、アップデートします。

[作成] > [次] ボタンをクリックして、ウィザードの次のステップに進みます。

8.1.1 MAC ACL

[MAC] を選択すると、以下のウィンドウが表示されます。

図 8-2 ACL 設定ウィザード（MAC ACL の設定）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。
送信元	ソース MAC アドレス情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト MAC アドレスを入力します。 • **MAC** - ソース MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
宛先	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
指定イーサタイプ	イーサネットタイプオプション（**aarp/appletalk/decent-iv/etype-6000/etype-8042/lat/lavc-sca/mop-console/mop-dump/vines-echo/vines-ip/xns-idp/arp**）を選択します。
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。 [**指定イーサタイプ**] ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。

パラメータ	概要
イーサネットタイプ マスク	イーサネットタイプマスクを 16 進数値で入力します。[**指定イーサタイプ**] ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
CoS	使用する CoS 値（**0 ～ 7**）を選択します。 • **マスク** - CoS マスク値を入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094） • **マスク** - VLAN ID マスク値を入力します。
時間範囲	使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）
アクション	実行するアクション（**許可** / **拒否**）を選択します。

[次] ボタンをクリックすると、以下のウィンドウが表示されます。

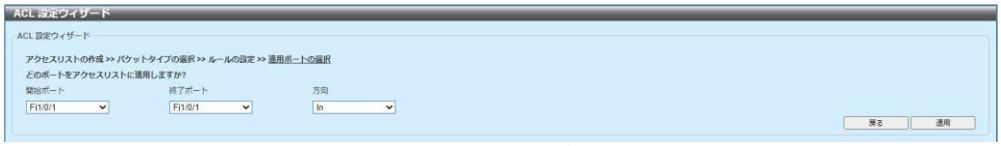


図 8-3 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

8.1.2 IPv4

[IPv4] を選択すると、以下のウィンドウが表示されます。

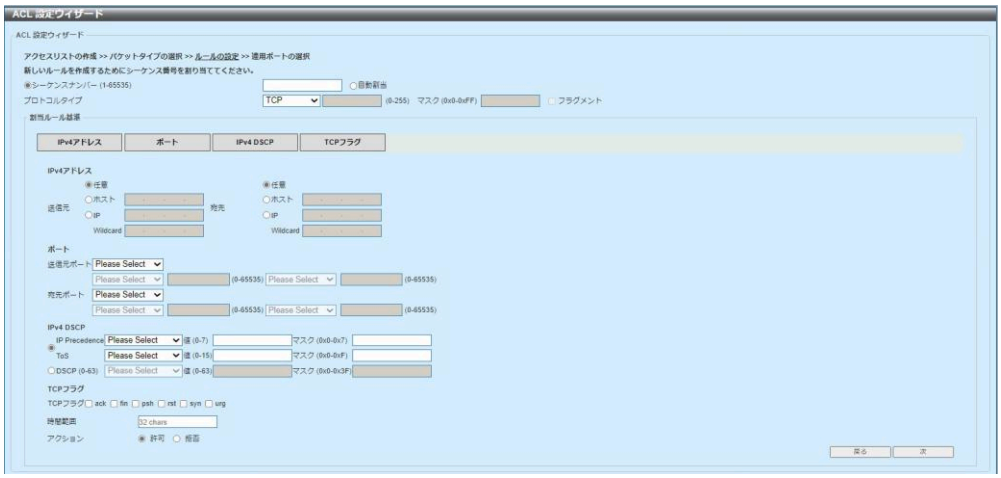


図 8-4 ACL 設定ウィザード（IPv4 ACL の設定）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。
プロトコルタイプ	プロトコルタイプオプション（**TCP**/**UDP**/**ICMP**/**EIGRP**（88）/**ESP**（50）/**GRE**（47）/**IGMP**（2）/**OSPF**（89）/**PIM**（103）/**VRRP**（112）/**IP-in-IP**（94）/**PCP**（108）/**Protocol ID**/**None**）を選択します。 • **値** - プロトコル ID を手動で入力できます。 • **マスク** - [**Protocol ID**] オプションを選択した後、手動でプロトコルマスク値を入力します。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
送信元	ソース情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。

パラメータ	概要
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
送信元ポート	([プロトコルタイプ] パラメータで [TCP] または [UDP] 選択時に設定可) • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。
宛先ポート	([プロトコルタイプ] パラメータで [TCP] または [UDP] 選択時に設定可) ディスティネーションポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。
指定 ICMP メッセージタイプ	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) [**指定 ICMP メッセージタイプ**] を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。 [**ICMP メッセージタイプ**] を選択した場合、メッセージタイプの数値が自動入力されます。

パラメータ	概要
メッセージコード	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) [**指定 ICMP メッセージタイプ**] を選択しない場合、使用するメッセージコードの数値を入力します。 [**ICMP メッセージタイプ**] を選択した場合、メッセージタイプの数値が自動入力されます。
IP Precedence	使用する IP Precedence 値（**routine**（0）/**priority**（1）/**immediate**（2）/**flash**（3）/**flash-override**（4）/**critical**（5）/**internet**（6）/**network**（7））を選択します。 • **値** - IP Precedence 値を手動でも入力できます。 • **マスク** - IP Precedence マスク値を入力します。
ToS	使用する ToS 値（**normal**（0）/**min-monetary-cost**（1）/**max-reliability**（2）/**max-throughput**（4）/**min-delay**（8））を選択します。 • **値** - ToS 値を手動でも入力できます。 • **マスク** - ToS マスク値を入力します。
DSCP	使用する DSCP 値（**default**（0）/**af11**（10）/**af12**（12）/**af13**（14）/**af21**（18）/**af22**（20）/**af23**（22）/**af31**（26）/**af32**（28）/**af33**（30）/**af41**（34）/**af42**（36）/**af43**（38）/**cs1**（8）/**cs2**（16）/**cs3**（24）/**cs4**（32）/**cs5**（40）/**cs6**（48）/**cs7**（56）/**ef**（46））を選択します。 • **値** - DSCP 値を手動でも入力できます。 • **マスク** - DSCP マスク値を入力します。
TCP フラグ	([プロトコルタイプ] パラメータで [TCP] 選択時に設定可) この ACL で評価する TCP フラグ（**ack**/**fin**/**psh**/**rst**/**syn**/**urg**）を選択します。
時間範囲	使用する時間範囲プロファイルの名前を入力します。 (最大：32 文字)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

[次] ボタンをクリックすると、以下のウィンドウが表示されます。

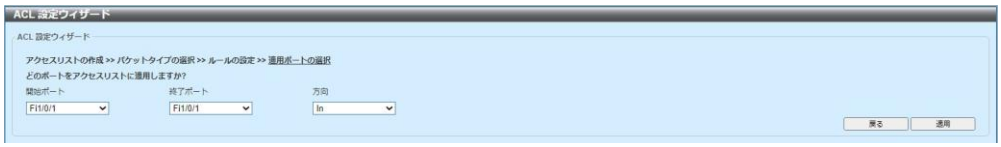


図 8-5 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

8.1.3 IPv6

[IPv6] を選択すると、以下のウィンドウが表示されます。

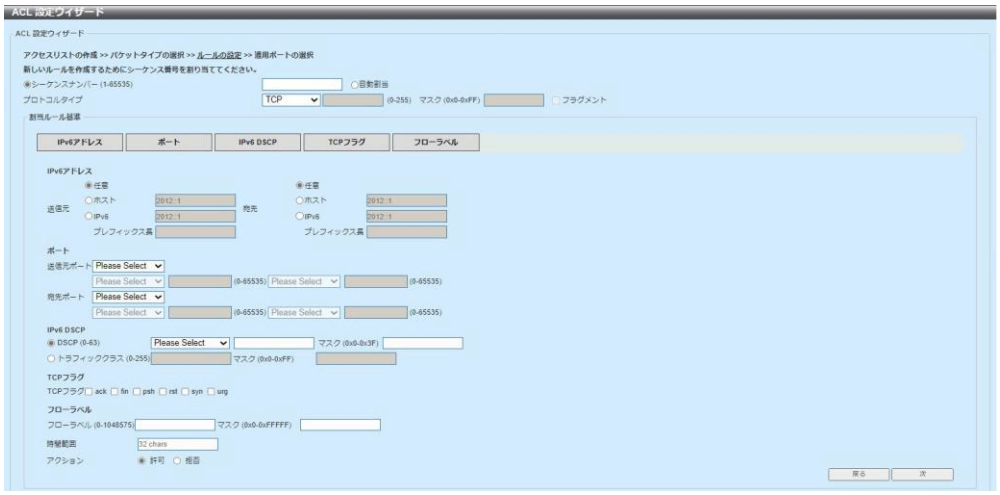


図 8-6 ACL 設定ウィザード（IPv6ACL の設定）

以下のパラメータを設定できます。

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。
プロトコルタイプ	プロトコルタイプオプション（**TCP**/**UDP**/**ICM**/**ESP**（50）/**PCP**（108）/**SCTP**（132）/**Protocol ID**/**None**）を選択します。 • **値** - プロトコル ID を手動で入力できます。 • **マスク** - [**Protocol ID**] オプションを選択した後、手動でプロトコルマスク値を入力します。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
送信元	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ソース IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。

パラメータ	概要
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ディスティネーション IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
送信元ポート	([プロトコルタイプ] パラメータで [TCP] または [UDP] 選択時に設定可) ソースポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。
宛先ポート	([プロトコルタイプ] パラメータで [TCP] または [UDP] 選択時に設定可) ディスティネーションポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。
指定 ICMP メッセージタイプ	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) [**指定 ICMP メッセージタイプ**] を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。 [**ICMP メッセージタイプ**] を選択した場合、メッセージタイプの数値が自動入力されます。

パラメータ	概要
メッセージコード	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) [**指定 ICMP メッセージタイプ**] を選択しない場合、使用するメッセージコードの数値を入力します。 [**ICMP メッセージタイプ**] を選択した場合、メッセージタイプの数値が自動入力されます。
DSCP	使用する DSCP 値（**default**（0）/**af11**（10）/**af12**（12）/**af13**（14）/**af21**（18）/**af22**（20）/**af23**（22）/**af31**（26）/**af32**（28）/**af33**（30）/**af41**（34）/**af42**（36）/**af43**（38）/**cs1**（8）/**cs2**（16）/**cs3**（24）/**cs4**（32）/**cs5**（40）/**cs6**（48）/**cs7**（56）/**ef**（46））を選択します。 • **値** - DSCP 値を手動でも入力できます。 • **マスク** - DSCP マスク値を入力します。
トラフィッククラス	トラフィッククラス値を選択および入力します。範囲は 0 ～ 255 です。 • **マスク** - トラフィッククラスマスク値を入力します。
TCP フラグ	([プロトコルタイプ] で [TCP] を選択した場合に設定) この ACL で評価する TCP フラグ（**ack**/**fin**/**psh**/**rst**/**syn**/**urg**）を選択します。
フローラベル	フローラベル値を入力します。 • **マスク** - フローラベルマスクを入力します。
時間範囲	使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）
アクション	実行するアクション（**許可** / **拒否**）を選択します。

[次] ボタンをクリックすると、以下のウィンドウが表示されます。

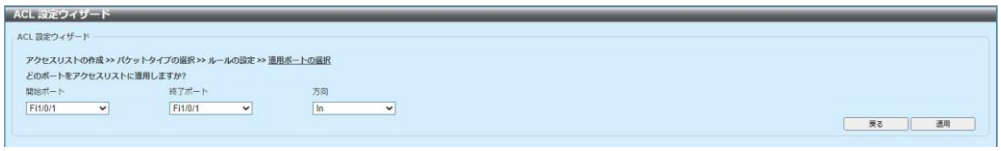


図 8-7 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

8.2 ACL アクセスリスト

このウィンドウを用いて、ACL および ACL ルールの設定を行い、設定値を表示します。

[ACL] > [ACL アクセスリスト] をクリックして、以下のウィンドウを表示します。

図 8-8 ACL アクセスリスト

設定パラメータ （[ACL アクセスリスト] セクション）

パラメータ	概要
ACL タイプ	検索する ACL タイプ（**All**/**IP ACL**/**IPv6 ACL**/**MAC AC**/**Expert ACL**）を選択します。
ID	アクセスリスト ID を選択および入力します。
ACL 名称	アクセスリスト名を選択および入力します（最大：32 文字）

[**検索**] ボタン - 検索結果を表示します。
[**ACL 追加**] ボタン - ACL プロファイルエントリを追加します。
[**編集**] ボタン - エントリの設定を編集します。
[**カウンタ全クリア**] ボタン - すべてのカウンタ情報をクリアします。
[**カウンタクリア**] ボタン - ACL プロファイルのカウンタ情報をクリアします。
[**ルール追加**] ボタン - ACL ルールエントリを追加します。
[**編集**] ボタン - エントリの設定を編集します。

設定パラメータ （[編集]）

パラメータ	概要
開始シーケンスナンバー	開始シーケンスナンバーを入力します。
ステップ	シーケンスナンバーのステップを入力します。これは、シーケンスナンバーのステップ数を指定します。デフォルト値は 10 です。たとえば、増分（ステップ）値が 5、開始シーケンスナンバーが 20 である場合、それ以降のシーケンスナンバーは、25、30、35、40 のようになります。
カウンタ状態	カウンタの状態（**Enabled**/**Disabled**）を選択します。
注釈	この ACL に関連付けるオプションの注釈を入力します。

[**適用**] ボタン - 設定内容を反映します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[ACL 追加]>[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	作成する ACL タイプ（**Standard IP ACL**/**Extended IP ACL**/**Standard IPv6 ACL**/**Extended IPv6 ACL**/**Extended MAC ACL**/**Extended Expert ACL**）を選択します。
ID	標準 IP ACL の ID を入力します。
ACL 名称	ACL の名前を入力します。（最大：32 文字）。

[**適用**] ボタン - ACL エントリを追加します。

8.2.1 標準 IP ACL

[ACL 追加] ボタン（**[ACL アクセスリスト]** ウィンドウ）をクリックして、以下のウィンドウを表示します。

図 8-9 ACL アクセスリスト（ACL 追加、標準 IP ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	選択する値は **[Standard IP ACL]** です。
ID	標準 IP ACL の ID を入力します。（設定範囲：1-1999）
ACL 名称	ACL の名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL エントリを追加します。

標準 IP ACL エントリを選択して **[ルールの設定]** ボタンをクリックして、[ACL ルール追加] ウィンドウを表示します。

設定パラメータ （[ルールの設定]>[ACL ルール追加] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。このナンバーは、指定しない場合、自動生成されます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。
送信元	ソース情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL プロファイルを追加します。
[**戻る**]ボタン - 前のウィンドウに戻ります。

8.2.2 拡張 IP ACL

[ACL 追加] ボタン（**[ACL アクセスリスト]** ウィンドウ）をクリックして、以下のウィンドウを表示します。

図 8-10 ACL アクセスリスト（ACL 追加、拡張 IP ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	選択する値は、**[Extended IP ACL]** です。
ID	拡張 IP ACL の ID を入力します。（設定範囲：2000-3999）
ACL 名称	ACL の名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL エントリを追加します。

拡張 IP ACL エントリを選択して **[ルールの設定]** ボタンをクリックして、[ACL ルール追加] ウィンドウを表示します。

設定パラメータ （[ルールの設定]>[ACL ルール追加] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。このナンバーは、指定しない場合、自動生成されます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。
プロトコルタイプ	プロトコルタイプオプションを選択します。選択する値は、**[TCP]**、**[UDP]**、**[ICMP]**、**[EIGRP]**（88）、**[ESP]**（50）、**[GRE]**（47）、**[IGMP]**（2）、**[OSPF]**（89）、**[PIM]**（103）、**[VRRP]**（112）、**[IP-in-IP]**（94）、**[PCP]**（108）、**[Protocol ID]**、**[None]** です。 • **値** - プロトコル ID を手動で入力できます。範囲は 0 ～ 255 です。 • **マスク** - **[Protocol ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
送信元	ソース情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。

パラメータ	概要
送信元ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定）ソースポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。
宛先ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定）ディスティネーションポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。
TCP フラグ	([プロトコルタイプ] で [TCP] 選択した場合に設定） この ACL で評価する TCP フラグを選択します。選択する値は、**[ack]**、**[fin]**、**[psh]**、**[rst]**、**[syn]**、**[urg]** です。
指定 ICMP メッセージタイプ	([プロトコルタイプ] で [ICMP] 選択した場合に設定） 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] で [ICMP] 選択した場合に設定） **[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。
メッセージコード	([プロトコルタイプ] で [ICMP] 選択した場合に設定） **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。

パラメータ	概要
IP Precedence	使用する IP Precedence 値を選択します。選択する値は、**[routine]**（0）、**[priority]**（1）、**[immediate]**（2）、**[flash]**（3）、**[flash-override]**（4）、**[critical]**（5）、**[internet]**（6）、**[network]**（7）です。 • **値** - IP Precedence 値を手動でも入力できます。範囲は 0 ～ 7 です。 • **マスク** - IP Precedence マスク値を入力します。範囲は 0x0 ～ 0x7 です。
ToS	使用する ToS（Type-of-Service）値を選択します。選択する値は、**[normal]**（0）、**[min-monetary-cost]**（1）、**[max-reliability]**（2）、**[max-throughput]**（4）、**[min-delay]**（8）です。 • **値** - ToS 値を手動でも入力できます。範囲は 0 ～ 15 です。 • **マスク** - ToS マスク値を入力します。範囲は 0x0 ～ 0xF です。
DSCP	使用する DSCP 値を選択します。選択する値は、**[default]**（0）、**[af11]**（10）、**[af12]**（12）、**[af13]**（14）、**[af21]**（18）、**[af22]**（20）、**[af23]**（22）、**[af31]**（26）、**[af32]**（28）、**[af33]**（30）、**[af41]**（34）、**[af42]**（36）、**[af43]**（38）、**[cs1]**（8）、**[cs2]**（16）、**[cs3]**（24）、**[cs4]**（32）、**[cs5]**（40）、**[cs6]**（48）、**[cs7]**（56）、**[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。範囲は 0 ～ 63 です。 • **マスク** - DSCP マスク値を入力します。範囲は 0x0 ～ 0x3F です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL プロファイルを追加します。
[**戻る**]ボタン - 前のウィンドウに戻ります。

8.2.3 標準 IPv6 ACL

[ACL 追加] ボタン（**[ACL アクセスリスト]** ウィンドウ）をクリックして、以下のウィンドウを表示します。

図 8-11 ACL アクセスリスト（ACL 追加、標準 IPv6 ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	選択する値は、**[Standard IPv6 ACL]** です。
ID	標準 IPv6 ACL の ID を入力します。 （設定範囲：11000-12999）
ACL 名称	ACL の名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL エントリを追加します。

標準 IPv6 ACL エントリを選択して **[ルールの設定]** ボタンをクリックして、[ACL ルール追加] ウィンドウを表示します。

設定パラメータ （[ルールの設定]>[ACL ルール追加] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。このナンバーは、指定しない場合、自動生成されます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。
送信元	ソース情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ソース IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ディスティネーション IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL プロファイルを追加します。
[**戻る**]ボタン - 前のウィンドウに戻ります。

8.2.4 拡張 IPv6 ACL

[ACL 追加] ボタン（**[ACL アクセスリスト]** ウィンドウ）をクリックして、以下のウィンドウを表示します。

図 8-12 ACL アクセスリスト（ACL 追加、拡張 IPv6 ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	選択する値は、**[Extended IPv6 ACL]** です。
ID	拡張 IPv6 ACL の ID を入力します。 （設定範囲：13000-14999）
ACL 名称	ACL の名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL エントリを追加します。

拡張 IPv6 ACL エントリを選択して **[ルールの設定]** ボタンをクリックして、[ACL ルール追加] ウィンドウを表示します。

設定パラメータ （[ルールの設定]>[ACL ルール追加] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。このナンバーは、指定しない場合、自動生成されます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。
プロトコルタイプ	プロトコルタイプオプションを選択します。選択する値は、**[TCP]**、**[UDP]**、**[ICMP]**、**[Protocol ID]**、**[ESP]**（50）、**[PCP]**（108）、**[SCTP]**（132）、**[None]** です。 • **値** - プロトコル ID を手動で入力できます。範囲は 0 ～ 255 です。 • **マスク** - **[Protocol ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
送信元	ソース情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ソース IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ディスティネーション IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。

パラメータ	概要
送信元ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定）ソースポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。
宛先ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定）ディスティネーションポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。
TCP フラグ	この ACL で評価する TCP フラグを選択します。選択する値は、**[ack]**、**[fin]**、**[psh]**、**[rst]**、**[syn]**、**[urg]** です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** を選択した場合のみ利用可能です。
指定 ICMP メッセージタイプ	([プロトコルタイプ] で [ICMP] を選択した場合に設定） 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] で [ICMP] を選択した場合に設定） **[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。
メッセージコード	([プロトコルタイプ] で [ICMP] を選択した場合に設定） **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。

パラメータ	概要
DSCP	使用する DSCP 値を選択します。選択する値は、**[default]**（0）、**[af11]**（10）、**[af12]**（12）、**[af13]**（14）、**[af21]**（18）、**[af22]**（20）、**[af23]**（22）、**[af31]**（26）、**[af32]**（28）、**[af33]**（30）、**[af41]**（34）、**[af42]**（36）、**[af43]**（38）、**[cs1]**（8）、**[cs2]**（16）、**[cs3]**（24）、**[cs4]**（32）、**[cs5]**（40）、**[cs6]**（48）、**[cs7]**（56）、**[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。範囲は 0 ～ 63 です。 • **マスク** - DSCP マスク値を入力します。範囲は 0x0 ～ 0x3F です。
トラフィッククラス	トラフィッククラス値を選択および入力します。範囲は 0 ～ 255 です。 • **マスク** - トラフィッククラスマスク値を入力します。範囲は 0x0 ～ 0xFF です。
フローラベル	フローラベル値を入力します。範囲は 0 ～ 1048575 です。 • **マスク** - フローラベルマスクを入力します。範囲は 0x0 ～ 0xFFFFF です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL プロファイルを追加します。
[**戻る**]ボタン - 前のウィンドウに戻ります。

8.2.5 拡張 MAC ACL

[ACL 追加] ボタン（**[ACL アクセスリスト]** ウィンドウ）をクリックして、以下のウィンドウを表示します。

図 8-13 ACL アクセスリスト（ACL 追加、拡張 MAC ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	選択する値は、**[Extended MAC ACL]** です。
ID	拡張 MAC ACL の ID を入力します。 （設定範囲：6000-7999）
ACL 名称	ACL の名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL エントリを追加します。

拡張 MAC ACL エントリを選択して **[ルールの設定]** ボタンをクリックして、[ACL ルール追加] ウィンドウを表示します。

設定パラメータ （[ルールの設定]>[ACL ルール追加] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。このナンバーは、指定しない場合、自動生成されます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。
送信元	ソース MAC アドレス情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト MAC アドレスを入力します。 • **MAC** - ソース MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
宛先	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
指定イーサタイプ	イーサネットタイプオプションを選択します。選択する値は、**[aarp]**、**[appletalk]**、**[decent-iv]**、**[etype-6000]**、**[etype-8042]**、**[lat]**、**[lavc-sca]**、**[mop-console]**、**[mop-dump]**、**[vines-echo]**、**[vines-ip]**、**[xns-idp]**、、**[arp]** です。
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。範囲は 0x600 ～ 0xFFFF です。[指定イーサタイプ] ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
イーサネットタイプマスク	イーサネットタイプマスクを 16 進数値で入力します。範囲は 0x0 ～ 0xFFFF です。[指定イーサタイプ] ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
CoS	使用する CoS 値を選択します。範囲は 0 ～ 7 です。 • **マスク** - CoS マスク値を入力します。範囲は 0x0 ～ 0x7 です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 • **マスク** - VLAN ID マスク値を入力します。範囲は 0x0 ～ 0xFFF です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL プロファイルを追加します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

8.2.6 Extended Expert ACL

[ACL 追加] ボタン（**[ACL アクセスリスト]** ウィンドウ）をクリックして、以下のウィンドウを表示します。

図 8-14 ACL アクセスリスト（ACL 追加、Extended Expert ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

パラメータ	概要
ACL タイプ	選択する値は、**[Extended Expert ACL]** です。
ID	Extended Expert ACL の ID を入力します。 （設定範囲：8000-9999）
ACL 名称	ACL の名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL エントリを追加します。

Extended Expert ACL エントリを選択して **[ルールの設定]** ボタンをクリックして、[ACL ルール追加] ウィンドウを表示します。

設定パラメータ （[ルールの設定]>[ACL ルール追加] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。このナンバーは、指定しない場合、自動生成されます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。
プロトコルタイプ	プロトコルタイプオプションを選択します。選択する値は、**[TCP]**、**[UDP]**、**[ICMP]**、**[EIGRP]**（88）、**[ESP]**（50）、**[GRE]**（47）、**[IGMP]**（2）、**[OSPF]**（89）、**[PIM]**（103）、**[VRRP]**（112）、**[IP-in-IP]**（94）、**[PCP]**（108）、**[Protocol ID]**、**[None]** です。 • **値** - プロトコル ID を手動で入力できます。範囲は 0 ～ 255 です。 • **マスク** - [**Protocol ID**] オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
送信元（IP アドレス）	ソース情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先（IP アドレス）	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
送信元（MAC アドレス）	ソース MAC アドレス情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト MAC アドレスを入力します。 • **MAC** - ソース MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。

パラメータ	概要
宛先（MAC アドレス）	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
送信元ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定) ソースポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。
宛先ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定) ディスティネーションポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • ≠ - ACL は指定したポート番号を除くすべてのポートを使用します。 • **Range** - ACL は範囲内の指定されたポートを使用します。 • **Mask** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。
指定 ICMP メッセージタイプ	([プロトコルタイプ] で [ICMP] を選択した場合に設定) 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] で [ICMP] を選択した場合に設定) **[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。

パラメータ	概要
メッセージコード	([プロトコルタイプ] で [ICMP] を選択した場合に設定) **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。
IP Precedence	使用する IP Precedence 値を選択します。選択する値は、**[routine]**（0）、**[priority]**（1）、**[immediate]**（2）、**[flash]**（3）、**[flash-override]**（4）、**[critical]**（5）、**[internet]**（6）、**[network]**（7）です。 • **値** - IP Precedence 値を手動でも入力できます。範囲は 0 ～ 7 です。 • **マスク** - IP Precedence マスク値を入力します。範囲は 0x0 ～ 0x7 です。
ToS	使用する ToS（Type-of-Service）値を選択します。選択する値は、**[normal]**（0）、**[min-monetary-cost]**（1）、**[max-reliability]**（2）、**[max-throughput]**（4）、**[min-delay]**（8）です。 • **値** - ToS 値を手動でも入力できます。範囲は 0 ～ 15 です。 • **マスク** - ToS マスク値を入力します。範囲は 0x0 ～ 0xF です。
DSCP	使用する DSCP 値を選択します。選択する値は、**[default]**（0）、**[af11]**（10）、**[af12]**（12）、**[af13]**（14）、**[af21]**（18）、**[af22]**（20）、**[af23]**（22）、**[af31]**（26）、**[af32]**（28）、**[af33]**（30）、**[af41]**（34）、**[af42]**（36）、**[af43]**（38）、**[cs1]**（8）、**[cs2]**（16）、**[cs3]**（24）、**[cs4]**（32）、**[cs5]**（40）、**[cs6]**（48）、**[cs7]**（56）、**[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。範囲は 0 ～ 63 です。 • **マスク** - DSCP マスク値を入力します。範囲は 0x0 ～ 0x3F です。
TCP フラグ	([プロトコルタイプ] で [TCP] を選択した場合に設定) この ACL で評価する TCP フラグを選択します。選択する値は、**[ack]**、**[fin]**、**[psh]**、**[rst]**、**[syn]**、**[urg]** です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 • **マスク** - VLAN ID マスク値を入力します。範囲は 0x0 ～ 0xFFF です。
CoS	使用する CoS 値を選択します。範囲は 0 ～ 7 です。 • **マスク** - CoS マスク値を入力します。範囲は 0x0 ～ 0x7 です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。（最大：32 文字）

[**適用**] ボタン - ACL プロファイルを追加します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

8.3 ACL インタフェースアクセスグループ

このウィンドウを用いて、指定したポートの ACL アクセスグループの設定を行い、設定値を表示します。

[ACL] > [ACL インタフェースアクセスグループ] をクリックして、以下のウィンドウを表示します。

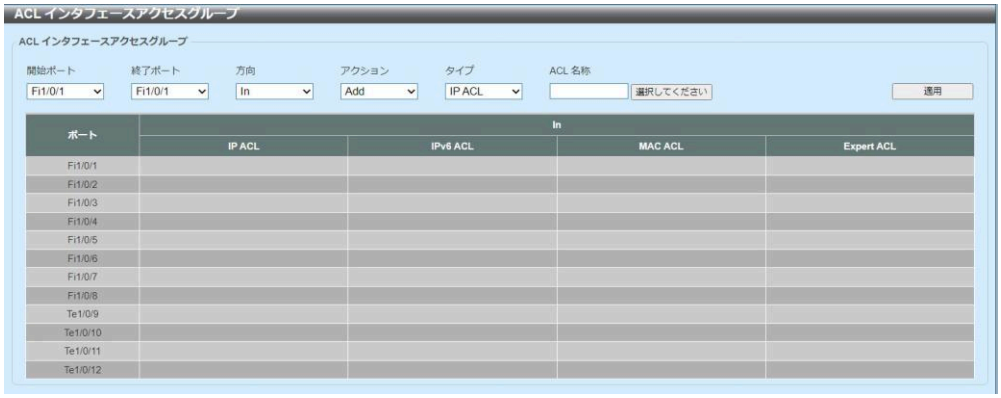


図 8-15 ACL インタフェースアクセスグループ

設定パラメータ （[ACL インタフェースアクセスグループ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In**）を選択します。。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	ACL タイプ（**IP ACL**/**IPv6 ACL**/**MAC ACL**/**Expert ACL**）を選択します。
ACL 名称	ACL 名称を入力します。（最大：32 文字） [**選択してください**] ボタンをクリックして、リストから既存の ACL を選択します。

[**適用**] ボタン - 設定内容を反映します。

8.4 ACL VLAN アクセスマップ

このウィンドウを用いて、ACL VLAN アクセスマップの設定を行い、設定値を表示します。

[ACL] > [ACL VLAN アクセスマップ] をクリックして、以下のウィンドウを表示します。

図 8-16 ACL VLAN アクセスマップ

設定パラメータ （[ACL VLAN アクセスマップ] セクション）

パラメータ	概要
アクセスマップ名	アクセスマップ名を入力します。（最大：32 文字）
サブマップナンバー	サブマップナンバーを入力します。（設定範囲：1-65535）
アクション	実行するアクション（**Forward**/**Drop**/**Redirect**）を選択します。 **[Redirect]** オプションを選択した場合、ドロップダウンリストでリダイレクト先インタフェースを選択します。
カウンタ状態	カウンタ状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - エントリを追加します。
[**カウンタ全クリア**] ボタン - すべてのカウンタ情報をクリアします。
[**カウンタクリア**] ボタン - カウンタ情報をクリアします。
[**検索**] ボタン - 検索結果を表示します。
[**バインディング**] ボタン - バインディングを設定します。
[**削除**] ボタン - エントリを削除します。

[バインディング] ボタンをクリックして、適合アクセスリストウィンドウを表示します。

設定パラメータ （[バインディング]>[適合アクセスリスト] セクション）

パラメータ	概要
適合 IP アクセスリスト	適合する IP アクセスリストが表示されます。
適合 IPv6 アクセスリスト	適合する IPv6 アクセスリストが表示されます。
適合 MAC アクセスリスト	適合する MAC アクセスリストが表示されます。

[**適用**] ボタン - 設定内容を反映します。
[**削除**] ボタン - バインディングを削除します。

8.5 ACL VLAN フィルタ

このウィンドウを用いて、ACL VLAN フィルタの設定を行い、設定値を表示します。

[ACL] > [ACL VLAN フィルタ] をクリックして、以下のウィンドウを表示します。

図 8-17 ACL VLAN フィルタ

設定パラメータ （[ACL VLAN フィルタ] セクション）

パラメータ	概要
アクセスマップ名	アクセスマップ名を入力します。（最大：32 文字）
アクション	実行するアクション（**Add**/**Delete**）を選択します。
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 [**全 VLAN**] オプションを選択した場合、このスイッチで設定されているすべての VLAN にこのコンフィグレーションを適用します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9 セキュリティ

9.1 ポートセキュリティ

9.1.1 ポートセキュリティグローバル設定

このウィンドウを用いて、グローバルポートセキュリティの設定を行い、設定値を表示します。

[セキュリティ] > [ポートセキュリティ] > [ポートセキュリティグローバル設定] をクリックして、以下のウィンドウを表示します。

図 9-1 ポートセキュリティグローバル設定

設定パラメータ （[ポートセキュリティシステム設定] セクション）

パラメータ	概要
システム最大アドレス	セキュアな MAC アドレスの最大許可数を入力します。 （デフォルト：制限なし、設定範囲：1 ～ 3328） **[制限なし]** を選択した場合、セキュアな MAC アドレスの最大数を許可します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ポートセキュリティ VLAN 設定] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）

パラメータ	概要
VLAN 最大学習アドレス	指定した VLAN で学習可能な MAC アドレスの最大許可数を入力します。(設定範囲：1-3328) **[制限なし]** を選択した場合、セキュアな MAC アドレスの最大数を許可します。

[**適用**] ボタン - エントリを追加します。

[検索 VLAN] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VID	使用する VLAN ID を入力します。(設定範囲：1-4094)

[**検索**] ボタン - 検索結果を表示します。

9.1.2 ポートセキュリティポート設定

このウィンドウを用いて、指定したポートのポートセキュリティの設定を行い、設定値を表示します。

[セキュリティ] > [ポートセキュリティ] > [ポートセキュリティポート設定] をクリックして、以下のウィンドウを表示します。

図 9-2 ポートセキュリティポート設定

設定パラメータ （[ポートセキュリティポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートのポートセキュリティ機能の有効、無効を設定します。
最大	指定したポートのセキュアな MAC アドレスの最大許可数を入力します。（デフォルト：32、設定範囲：0-3328）
Violation Action	実行する違反時アクションを選択します。 • **Protect** - ポートセキュリティプロセスレベルでセキュアではないホストからのすべてのパケットを廃棄しますが、セキュリティ違反カウントは増やしません。 • **Restrict** - ポートセキュリティプロセスレベルでセキュアではないホストからのすべてのパケットを廃棄します。セキュリティ違反カウントを増やし、システムログに記録します。 • **Shutdown** - セキュリティ違反が発生した場合、ポートをシャットダウンし、システムログに記録します。
セキュリティモード	セキュリティモードオプションを選択します。 • **Parmanent** - 学習されたすべての MAC アドレスは、ユーザがエントリを手動で削除した場合を除いて、クリアされません。 • **Delete-on-Timeout** - 学習されたすべての MAC アドレスは、エントリがエージアウトした場合、またはユーザがエントリを手動で削除した場合にクリアされます。

パラメータ	概要
エージング時間	指定したポートで自動学習したセキュアなダイナミックアドレスに使用するエージング時間（分）を入力します。 (設定範囲：0-1440)
エージングタイプ	エージングタイプを選択します。 • **Absolute** - このポートのセキュアアドレスはすべて、指定した時間が過ぎるとただちにエージアウトし、セキュアアドレスリストから削除されます。これがデフォルトのタイプです。 • **Inactivity** - このポートのセキュアアドレスがエージアウトするのは、指定した期間にセキュアなソースアドレスからのデータトラフィックがない場合のみです。

[**適用**] ボタン - 設定内容を反映します。

9.1.3 ポートセキュリティアドレスエントリ

このウィンドウを用いて、ポートセキュリティの MAC アドレスエントリの設定を行い、設定値を表示します。

[セキュリティ] > [ポートセキュリティ] > [ポートセキュリティアドレスエントリ] をクリックして、以下のウィンドウを表示します。

図 9-3 ポートセキュリティアドレスエントリ

設定パラメータ （[ポートセキュリティアドレスエントリ] セクション）

パラメータ	概要
ポート	ポートを選択します。
MAC アドレス	MAC アドレスを入力します。**不変**オプションを選択した場合、学習されたすべての MAC アドレスは、ユーザがエントリを手動で削除した場合を除いて、クリアされません。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
[**ポート単位クリア**] ボタン - 指定したポートに対してセキュアなすべての MAC アドレスを削除します。
[**MAC 単位クリア**] ボタン - 任意のポートに対してセキュアな MAC アドレスのうち、指定したアドレスを削除します。
[**全クリア**] ボタン - ポートに対してセキュアなすべての MAC アドレスを削除します。

9.2 802.1X

9.2.1 802.1X グローバル設定

このウィンドウを用いて、グローバル IEEE 802.1X の設定を行い、設定値を表示します。

[セキュリティ] > [802.1X] > [802.1X グローバル設定] をクリックして、以下のウィンドウを表示します。

図 9-4 802.1X グローバル設定

設定パラメータ （[802.1X グローバル設定] セクション）

パラメータ	概要
システム認証制御	システム認証制御の状態（**Enabled**/**Disabled**）を選択します。この機能は、未認証ホストによるネットワークへのアクセスを制限します。
NAS ID	NAS（Network Access Server）の ID を入力します。半角のみ設定可能です。（最大：16 文字）
EAP リクエスト間隔	EAP（Extensible Authentication Protocol）リクエスト間隔（秒）を入力します。（設定範囲：1-3600）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[802.1X 認証ポート設定] セクション）

パラメータ	概要
認証ポートモード	指定したポートで使用する認証モード（**Port-Based**]/**MAC-Based**）を選択します。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - 設定内容を反映します。

9.2.2 802.1X 強制認証 MAC 設定

このウィンドウを用いて、IEEE 802.1X 強制認証 MAC の設定を行い、設定値を表示します。

[セキュリティ] > [802.1X] > [802.1X 強制認証 MAC 設定] をクリックして、以下のウィンドウを表示します。

図 9-5 802.1X 強制認証 MAC 設定

設定パラメータ （[強制認証 MAC 設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
MAC アドレス	サプリカントの MAC アドレスを入力します。
マスク長	MAC マスクビット長を入力します。（設定範囲：0-48）
認証状態	認証状態を選択します。 • **Authorized** - このオプションを選択した場合、強制的に認証済み状態にします。 • **Unauthorized** - このオプションを選択した場合、強制的に未認証状態にします。

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[**削除**] ボタン - エントリを削除します。

9.2.3 802.1X 未認証 MAC 設定

このウィンドウを用いて、IEEE 802.1X 未認証 MAC の設定を行い、設定値を表示します。

[セキュリティ] > [802.1X] > [802.1X 未認証 MAC 設定] をクリックして、以下のウィンドウを表示します。

図 9-6 802.1X 未認証 MAC 設定

設定パラメータ （[未認証 MAC アドレス設定] セクション）

パラメータ	概要
エージアウト時間	エージアウト時間値を入力します。この時間は、未認証のスタティックホストのエージアウトで使用します。 （設定範囲：0-65535）
ポート	ポートを選択します。
MAC アドレス	未認証ホストの MAC アドレスを入力します。
～で検索	• **MAC** - 未認証の設定済みダイナミックホストを検索します。 • **Port** - 指定したポートで未認証の設定済みダイナミックホストを検索します。

[**適用**] ボタン - 設定内容を反映します。
[**検索**] ボタン - 検索結果を表示します。

9.2.4 802.1X ポート設定

このウィンドウを用いて、指定したポートの IEEE 802.1X のポートベース /MAC ベースアクセスコントロールの設定を行い、設定値を表示します。

[セキュリティ] > [802.1X] > [802.1X ポート設定] をクリックして、以下のウィンドウを表示します。

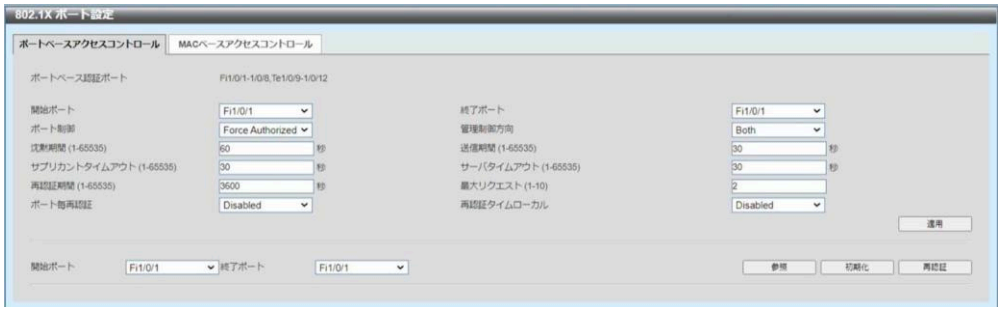


図 9-7 802.1X ポート設定（ポートベースアクセスコントロール）

設定パラメータ （[ポートベースアクセスコントロール] タブ）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
ポート制御	ポートの認証状態を選択します。 • **Auto** - ポートの IEEE 802.1X 認証を有効にします。 • **Force Authorized** - 強制的にポートを認証状態にします。 • **Force Unauthorized** - 強制的にポートを未認証状態にします。
管理制御方向	ポートのトラフィック制御方向を選択します。 • **Both** - 双方向のトラフィックを制御します。 • **In** - Inbound 方向のみのトラフィックを制御します。
沈黙期間	沈黙期間を入力します。これは、失敗した認証プロセスの後でスイッチが沈黙状態を維持する秒数です。 （設定範囲：1-65535）
送信期間	送信期間を入力します。これは、スイッチがサプリカントからの EAP リクエスト /Identity フレームを待機する秒数です。この期間が経過すると、リクエストを再送信します。 （設定範囲：1-65535）
サプリカントタイムアウト	サプリカントタイムアウト値を入力します。これは、サプリカントからの応答を待機する秒数です。この期間が経過すると、サプリカントメッセージがタイムアウトします。これは、EAP リクエスト ID には適用されません。 （設定範囲：1-65535）
サーバタイムアウト	サーバタイムアウト値を入力します。これは、認証サーバからの応答を待機する秒数です。この期間が経過すると、接続がタイムアウトします。（設定範囲：1-65535）

パラメータ	概要
再認証期間	再認証期間を入力します。これは、再認証試行間隔の秒数です。(設定範囲：1-65535)
最大リクエスト	バックエンド認証マシンからの EAP リクエストの最大許可数を入力します。これを超過すると、認証プロセスがリスタートされます。(設定範囲：1-10)
ポート毎再認証	指定したポートの定期的な再認証の状態（**Enabled**/**Disabled**）を選択します。
再認証タイムローカル	タイマーによるセッション再認証におけるローカル設定の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**参照**] ボタン - 指定されたポートに関連付けられているポートベースアクセスコントロール設定を表示します。
[**初期化**] ボタン - 指定されたポートのポートベースアクセスコントロール設定を初期化します。
[**再認証**] ボタン - 指定したポートへの接続をすべて再認証します。

[MAC ベースアクセスコントロール] タブをクリックして、以下のウィンドウを表示します。

図 9-8 802.1X ポート設定（MAC ベースアクセスコントロール）

設定パラメータ （[MAC ベースアクセスコントロール] タブ）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
サプリカント数	ポートの認証ユーザの最大許可数を入力します。 （設定範囲：1-512）
管理制御方向	ポートのトラフィック制御方向を選択します。選択する値は以下のとおりです。 • **Both** - 双方向のトラフィックを制御します。 • **In** - Inbound 方向のみのトラフィックを制御します。
沈黙期間	沈黙期間を入力します。これは、失敗した認証プロセスの後でスイッチが沈黙状態を維持する秒数です。 （設定範囲：1-65535）
送信期間	送信期間を入力します。これは、スイッチがサプリカントからの EAP リクエスト /Identity フレームを待機する秒数です。この期間が経過すると、リクエストを再送信します。 （設定範囲：1-65535）
サプリカントタイムアウト	サプリカントタイムアウト値を入力します。これは、サプリカントからの応答を待機する秒数です。この期間が経過すると、サプリカントメッセージがタイムアウトします。これは、EAP リクエスト ID には適用されません。 （設定範囲：1-65535）
サーバタイムアウト	サーバタイムアウト値を入力します。これは、認証サーバからの応答を待機する秒数です。この期間が経過すると、接続がタイムアウトします。（設定範囲：1-65535）
再認証期間	再認証期間を入力します。これは、再認証試行間隔の秒数です。（設定範囲：1-65535）
最大リクエスト	バックエンド認証マシンからの EAP リクエストの最大許可数を入力します。これを超過すると、認証プロセスがリスタートされます。（設定範囲：1-10）
再認証タイムローカル	タイマーによるセッション再認証におけるローカル設定の使用の有効、無効を設定します。

パラメータ	概要
ポート毎再認証	指定したポートの定期的な再認証の有効、無効を設定します。
強制認証タイムアウト	強制認証タイムアウト値を入力します。これは、スイッチが強制認証 / 未認証への移行を待機する秒数です。この期間が経過すると、移行がタイムアウトします。移行がタイムアウトしないようにするには、0 を入力します。 (設定範囲：0-65535)

[**適用**] ボタン - 設定内容を反映します。
[**参照**] ボタン - 指定されたポートに関連付けられているポートベースアクセスコントロール設定を表示します。
[**初期化**] ボタン - 指定されたポートのポートベースアクセスコントロール設定を初期化します。
[**再認証**] ボタン - 指定したポートへの接続をすべて再認証します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**編集**] ボタン - 再認証機能を有効または無効にします。

9.2.5 EAP ポートコンフィグ

このウィンドウを用いて、指定したポートの EAP の設定を行い、設定値を表示します。

[セキュリティ] > [802.1X] > [EAP ポートコンフィグ] をクリックして、以下のウィンドウを表示します。

図 9-9 EAP ポートコンフィグ

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
EAP リクエスト	指定したポートの EAP リクエスト機能の状態（**Enabled**/**Disabled**）を選択します。
EAP フォワード	指定したポートの EAP フォワード機能の状態（**Enabled**/**Disabled**）を選択します。これは、IEEE 802.1X PDU（Protocol Data Unit）のフォワーディングを有効 / 無効にするために使用します。

[**適用**] ボタン - 設定内容を反映します。

9.2.6 802.1X 認証統計情報

このコマンドを用いて、指定したポートの IEEE 802.1X 認証統計情報を表示およびクリアします。

[セキュリティ] > [802.1X] > [802.1X 認証統計情報] をクリックして、以下のウィンドウを表示します。

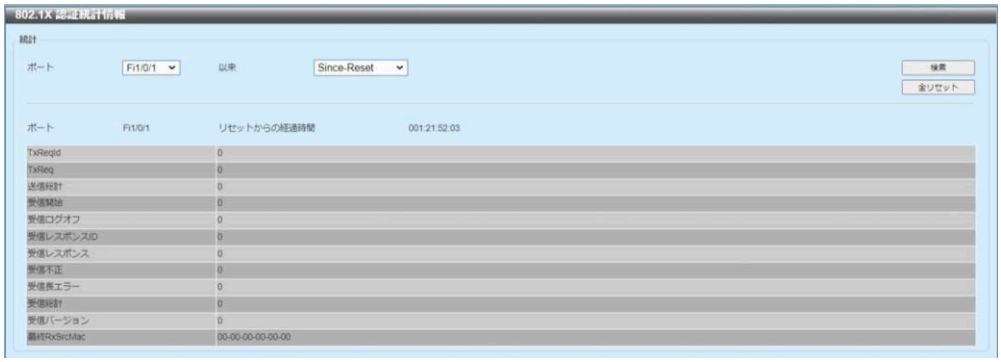


図 9-10 802.1X 認証統計情報

設定パラメータ （[統計] セクション）

パラメータ	概要
ポート	ポートを選択します。
以来	時間範囲を選択します。 • **Since-Reset** - 最後のスイッチリセット以来の統計を表示します。 • **Since-Up** - 最後のスイッチブートアップ以来の統計を表示します。

[**検索**] ボタン - 検索結果を表示します。
[**全リセット**] ボタン - すべての統計情報をリセットします。

9.2.7 802.1X サプリカントグローバル設定

スイッチングハブをサプリカントとして動作させるためにユーザ名、パスワードを設定します。802.1X サプリカント機能を使用することで、上位のスイッチングハブで IEEE802.1X 機能（ポートベース認証）を設定したポートに本装置を接続することが可能となり、不正アクセスの強化が図れます。

[セキュリティ] > [802.1X] > [802.1X サプリカントのグローバル設定] をクリックして、以下のウィンドウを表示します。

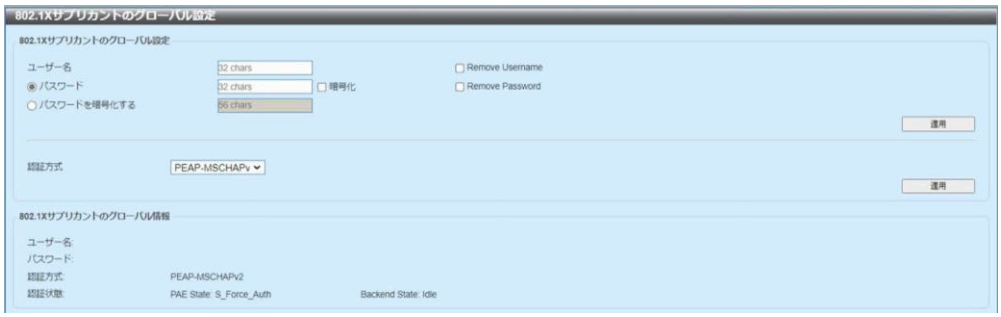


図 9-11 802.1X サプリカントグローバル設定

設定パラメータ （[802.1X サプリカントのグローバル設定] セクション）

パラメータ	概要
ユーザー名	サプリカントのユーザ名を設定します。半角のみ設定可能です。（最大：32 文字）
パスワード	サプリカントのパスワードを設定します。（最大：32 文字）
暗号化済みパスワード	暗号化されたパスワードを設定する際に利用します。
認証方式	認証方式（**MD5**/**PEAP-MSCHAPv2**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

9.2.8 802.1X サプリカントポート設定

指定したポートの IEEE 802.1X サプリカント機能の設定および状態を表示します。

[セキュリティ] > [802.1X] > [802.1X サプリカントポート設定] をクリックして、以下のウィンドウを表示します。

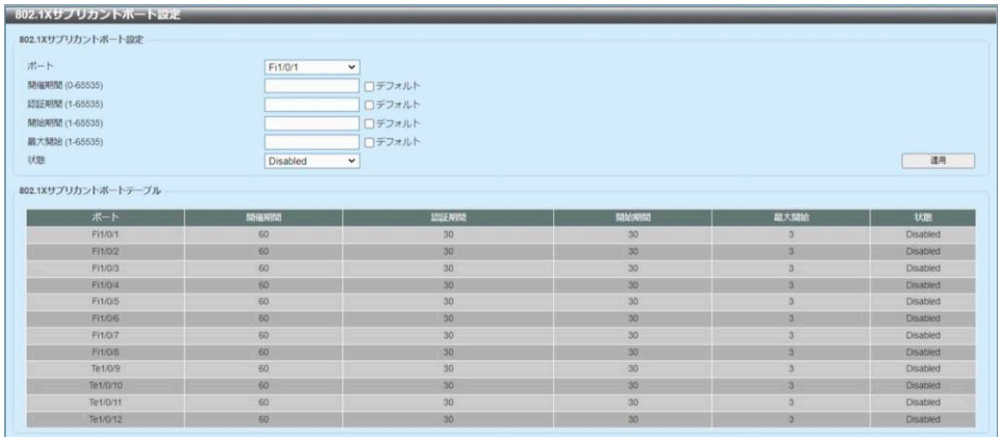


図 9-12 802.1X サプリカントポート設定

設定パラメータ （[802.1X サプリカントポート設定] セクション）

パラメータ	概要
ポート	設定するポートを選択します。
開催期間	サプリカントが認証を失敗した際に、次の認証まで待つ時間を設定します。（デフォルト：60 秒、設定範囲：0-65535）
認証期間	Authenticator からのリクエストを待つ時間を設定します。（デフォルト：30 秒、設定範囲：0-65535）
開始期間	認証を開始する際の EAPOL の送信間隔を設定します。（デフォルト：30 秒、設定範囲：0-65535）
最大開始	EAPOL-Start パケットを送信する最大数を設定します。（デフォルト：3 回、設定範囲：0-65535）
状態	ポートのサプリカント機能の有効、無効を設定します。 • **Disabled** - 最後のスイッチリセット以来の統計を表示します。 • **Enabled** - 最後のスイッチブートアップ以来の統計を表示します。

[**適用**] ボタン - 設定内容を反映します。

9.2.9 802.1X サプリカント統計情報

指定したポートの IEEE 802.1X サプリカント統計情報を表示します。

[セキュリティ] > [802.1X] > [802.1X サプリカント統計] をクリックして、以下のウィンドウを表示します。

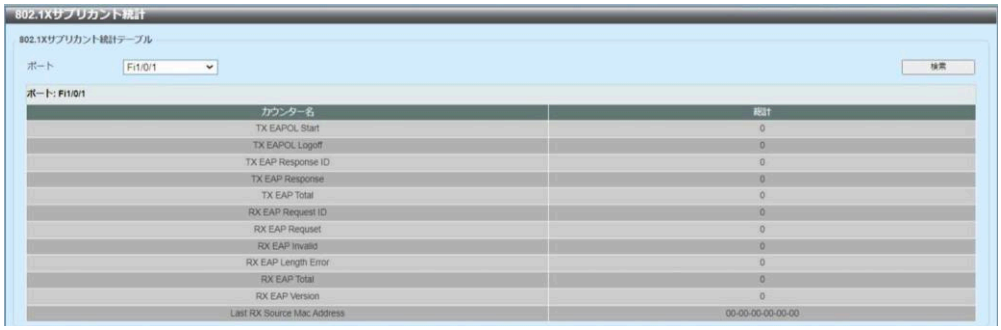


図 9-13 802.1X サプリカント統計情報

設定パラメータ （[802.1X サプリカント統計テーブル] セクション）

パラメータ	概要
ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。

9.3 AAA（Authentication, Authorization, and Accounting）

9.3.1 AAA グローバル設定

このウィンドウを用いて、AAA 機能をグローバルに有効または無効にします。

[セキュリティ] > [AAA] > [AAA グローバル設定] をクリックして、以下のウィンドウを表示します。

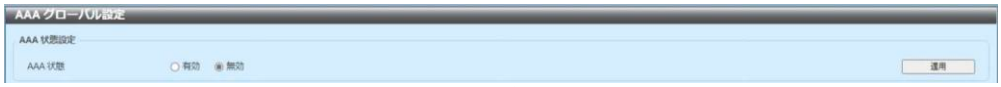


図 9-14 AAA グローバル設定

設定パラメータ （[AAA 状態設定] セクション）

パラメータ	概要
AAA 状態	AAA 機能の状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

9.3.2 AAA 認証設定

このウィンドウを用いて、AAA 認証の設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [AAA 認証設定] をクリックして、以下のウィンドウを表示します。

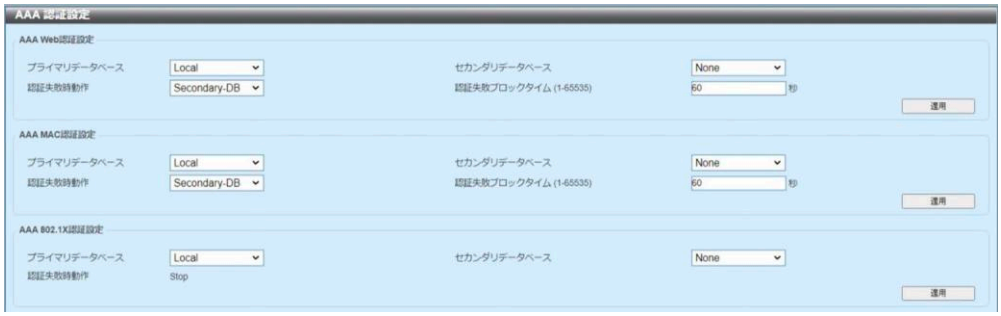


図 9-15 AAA 認証設定

設定パラメータ （[AAA Web 認証設定] セクション）

パラメータ	概要
プライマリデータベース	Web 認証に使用するプライマリデータベースを選択します。 • **RADIUS** - RADIUS サーバ上のデータベースをプライマリデータベースとして使用します。 • **Local** - スイッチ上のローカルデータベースをプライマリデータベースとして使用します。
セカンダリデータベース	Web 認証に使用するセカンダリデータベースを選択します。 • **None** - 認証が成功した扱いとなります。 • **RADIUS** - RADIUS サーバ上のデータベースをセカンダリデータベースとして使用します。 • **Local** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。
認証失敗時動作	Web 認証が失敗した場合に実行するアクションを選択します。選択する値は以下のとおりです。 • **Stop** - プライマリデータベースを使用して Web 認証が失敗した場合、認証を停止します。 この設定の場合でも、プライマリデータベースの RADIUS サーバと通信ができない場合、セカンダリデータベースの設定に従った動作となります。 • **Secondary-DB** - プライマリデータベースを使用して Web 認証が失敗した場合、セカンダリデータベースを使用して認証を開始します。
認証失敗ブロックタイム	Web 認証が失敗した場合にホストをブロックする秒数を入力します。（設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[AAA MAC 認証設定] セクション）

パラメータ	概要
プライマリデータベース	MAC 認証に使用するプライマリデータベースを選択します。 • **RADIUS** - RADIUS サーバ上のデータベースをプライマリデータベースとして使用します。 • **Local**- スイッチ上のローカルデータベースをプライマリデータベースとして使用します。
セカンダリデータベース	MAC 認証に使用するセカンダリデータベースを選択します。 • **None** - 認証が成功した扱いとなります。 • **RADIUS** - RADIUS サーバ上のデータベースをセカンダリデータベースとして使用します。 • **Local** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。
認証失敗時動作	MAC 認証が失敗した場合に実行するアクションを選択します。 • **Stop** - プライマリデータベースを使用して MAC 認証が失敗した場合、認証を停止します。 この設定の場合でも、プライマリデータベースの RADIUS サーバと通信ができない場合、セカンダリデータベースの設定に従った動作となります。 • **Secondary-DB** - プライマリデータベースを使用して MAC 認証が失敗した場合、セカンダリデータベースを使用して認証を開始します。
認証失敗ブロックタイム	MAC 認証が失敗した場合にホストをブロックする秒数を入力します。（設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[AAA 802.1X 認証設定] セクション）

パラメータ	概要
プライマリデータベース	IEEE 802.1X 認証に使用するプライマリデータベースを選択します。 • **RADIUS** - RADIUS サーバ上のデータベースをプライマリデータベースとして使用します。 • **Local** - スイッチ上のローカルデータベースをプライマリデータベースとして使用します。
セカンダリデータベース	IEEE 802.1X 認証に使用するセカンダリデータベースを選択します。 • **None** - セカンダリデータベースを使用しません。 • **Local** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。

[**適用**] ボタン - 設定内容を反映します。

9.3.3 AAA 認証ユーザ設定

このウィンドウを用いて、AAA 認証ユーザの設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [AAA 認証ユーザ設定] をクリックして、以下のウィンドウを表示します。

図 9-16 AAA 認証ユーザ設定

設定パラメータ （[AAA 認証ユーザ設定] セクション）

パラメータ	概要
ユーザ名	ローカル認証アカウントのユーザ名を入力します。 （最大：32 文字）
VLAN ID	ローカル認証アカウントのターゲット VLAN ID を入力します。（設定範囲：1-4094）
パスワード	ローカル認証アカウントの平文パスワードを選択および入力します。 **[暗号化]** オプションを選択した場合、このアカウントのパスワード暗号化を有効にします。平文パスワードは、スイッチ上で暗号化形式で保存されます。
暗号化パスワード	ローカル認証アカウントの暗号化パスワードを選択および入力します。
認証タイプ	認証タイプを選択します。 • **Both** - ローカル認証アカウントを IEEE 802.1X 認証と Web 認証の両方で使用します。 • **Web** - ローカル認証アカウントを Web 認証のみで使用します。 • **Dot1X** - ローカル認証アカウントを IEEE 802.1X 認証のみで使用します。
2 ステップ認証	2 ステップ認証の状態（**Enabled**/**Disabled**）を選択します。
2 段階目の認証	2 ステップ認証の 2 段階目の認証アカウントであることを指定します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.3.4 AAA 認証 MAC 設定

このウィンドウを用いて、AAA 認証 MAC の設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [AAA 認証 MAC 設定] をクリックして、以下のウィンドウを表示します。

図 9-17 AAA 認証 MAC 設定

設定パラメータ （[AAA 認証 MAC 設定] セクション）

パラメータ	概要
MAC アドレス	ローカル認証アカウントの MAC アドレスを入力します。これは、MAC 認証で使用します。
VLAN ID	ローカル認証アカウントのターゲット VLAN ID を入力します。（設定範囲：1-4094）
2 ステップ認証	2 ステップ認証を有効または無効にします。 • **No** - ローカル認証アカウントの 2 ステップ認証を無効にします。 • **Web** - 2 ステップ認証を有効にして、2 番目の認証方式として Web 認証を使用します。 • **802.1X** - 2 ステップ認証を有効にして、2 番目の認証方式として IEEE 802.1X 認証を使用します。 • **Any** - 2 ステップ認証を有効にして、2 番目の認証方式として IEEE 802.1X 認証と Web 認証を使用します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.3.5 アプリケーション認証設定

このウィンドウを用いて、アプリケーション認証の設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [アプリケーション認証設定] をクリックして、以下のウィンドウを表示します。

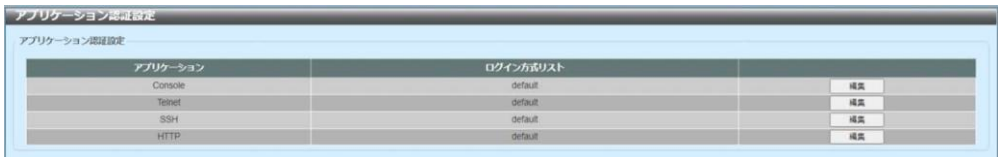


図 9-18 アプリケーション認証設定

[**編集**] ボタン - ログイン方式リストの名前を入力します。
[**適用**] ボタン - 設定内容を反映します。

9.3.6 アプリケーションアカウンティング設定

このウィンドウを用いて、アプリケーションアカウンティングの設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [アプリケーションアカウンティング設定] をクリックして、以下のウィンドウを表示します。

図 9-19 アプリケーションアカウンティング設定

[**編集**] ボタン - Exec 方式リストの名前を入力します。
[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[アプリケーションアカウンティングコマンド方式リスト] セクション）

パラメータ	概要
アプリケーション	使用するアプリケーション（**Console**/**Telnet**/**SSH**）を選択します。
レベル	使用する特権レベル（**1-15**）を選択します。
コマンド方式リスト	使用するコマンド方式リストの名前を入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.3.7 認証 EXEC の設定

このウィンドウを用いて、認証 EXEC の設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [認証 EXEC の設定] をクリックして、以下のウィンドウを表示します。

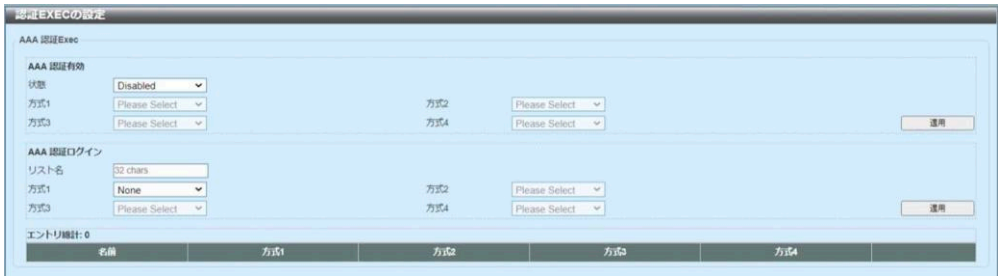


図 9-20 認証 EXEC の設定

設定パラメータ （[AAA 認証有効] セクション）

パラメータ	概要
状態	AAA 認証の状態（**Enabled**/**Disabled**）を選択します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リストを選択します。 • **None** - ユーザは、1 つ前の方式の認証で拒否されていなければ、認証されます。この方法は、通常は、リストの最後の方式として指定します。 • **Enable** - 認証にローカルイネーブルパスワードを使用します。 • **Group** - aaa group server コマンドによって定義されているサーバグループを使用します。AAA グループサーバ名を表示された入力フィールドに入力します。（最大：32 文字） • **RADIUS** - radius server host コマンドによって定義されているサーバを使用します。 • **TACACS+** - tacacs+ server host コマンドによって定義されているサーバを使用します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[AAA 認証ログイン] セクション）

パラメータ	概要
リスト名	**[AAA 認証ログイン]** オプションで使用する方式リスト名を入力します。

パラメータ	概要
方式 1 ～方式 4	このコンフィグレーションに使用する方式リストを選択します。 • **None** - ユーザは、1 つ前の方式の認証で拒否されていなければ、認証されます。この方法は、通常は、リストの最後の方式として指定します。 • **Local** - 認証にローカルデータベースを使用します。 • **Group** - aaa group server コマンドによって定義されているサーバグループを使用します。AAA グループサーバ名を表示された入力フィールドに入力します。(最大：32 文字) • **RADIUS** - radius server host コマンドによって定義されているサーバを使用します。 • **TACACS+** - tacacs+ server host コマンドによって定義されているサーバを使用します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.3.8 アカウンティング設定

このウィンドウを用いて、AAA アカウンティングの設定を行い、設定値を表示します。

[セキュリティ] > [AAA] > [アカウンティング設定] をクリックして、以下のウィンドウを表示します。

図 9-21 アカウンティング設定（AAA アカウンティングネットワーク）

設定パラメータ （[AAA アカウンティングネットワーク] タブ）

パラメータ	概要
デフォルト	デフォルト方式リスト使用の状態（**Enabled**/**Disabled**）を選択します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リスト（**None**/**Group**/**RADIUS**/**TACACS+**）を選択します。 **[None]** オプションは、方式 1 でのみ利用可能です。

[**適用**] ボタン - 設定内容を反映します。

[AAA アカウンティングシステム] タブをクリックして、以下のウィンドウを表示します。

図 9-22 アカウンティング設定（AAA アカウンティングシステム）

設定パラメータ （[AAA アカウンティングシステム] タブ）

パラメータ	概要
デフォルト	デフォルト方式リスト使用の有効、無効を設定します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リスト（**None**/**Group**/**RADIUS**/**TACACS+**）を選択します。 **[None]** オプションは、方式 1 でのみ利用可能です。

[**適用**] ボタン - 設定内容を反映します。

[AAA アカウンティング動作契機] タブをクリックして、以下のウィンドウを表示します。

図 9-23 アカウンティング設定（AAA アカウンティング動作契機）

設定パラメータ （[AAA アカウンティング動作契機] タブ）

パラメータ	概要
リスト名	**[AAA アカウンティング動作契機]** オプションで使用する方式リスト名を入力します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リスト（**None**/**Group**/**RADIUS**/**TACACS+**）を選択します。 **[None]** オプションは、方式 1 でのみ利用可能です。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

[AAA アカウンティングコマンド] タブをクリックして、以下のウィンドウを表示します。

図 9-24 アカウンティング設定（AAA アカウンティングコマンド）

設定パラメータ （[AAA アカウンティングコマンド] セクション）

パラメータ	概要
レベル	使用する特権レベル（**1-15**）を選択します。
リスト名	**[AAA アカウンティングコマンド]** オプションで使用する方式リスト名を入力します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リスト（**None**/**Group**/**RADIUS**/**TACACS+**）を選択します。**[TACACS+]** です。**[None]** オプションは、方式 1 でのみ利用可能です。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.4 認証

9.4.1 認証ダイナミック VLAN 設定

このウィンドウを用いて、認証に使用するダイナミック VLAN の設定を行い、設定値を表示します。

[セキュリティ] > [認証] > [認証ダイナミック VLAN 設定] をクリックして、以下のウィンドウを表示します。

図 9-25 認証ダイナミック VLAN 設定

設定パラメータ （[認証ダイナミック VLAN 設定] セクション）

パラメータ	概要
許可 RADIUS アトリビュート	RADIUS アトリビュートの受け入れの状態（**Enabled**/**Disabled**）を選択します。
開始ポート／終了ポート	ポートを選択します。
ゲスト VLAN	ゲスト VLAN の状態（**Enabled**/**Disabled**）を選択します。有効にした場合、ホストからゲスト VLAN への認証不要アクセスが許可されます。
ゲスト VLAN ID	ゲスト VLAN ID を入力します。（設定範囲：1-4094）
デフォルト VLAN	デフォルト VLAN の状態（**Enabled**/**Disabled**）を選択します。正常に認証されたホストは、ダイナミック VLAN 機能が無効な場合またはホストのターゲット VLAN が無効な場合は、デフォルト VLAN に割り当てられます。
デフォルト VLAN ID	デフォルト VLAN ID を入力します。（設定範囲：1-4094）

[**適用**] ボタン - 設定内容を反映します。

9.4.2 認証状態テーブル

このウィンドウを用いて、認証状態テーブルと情報を表示します。また、このウィンドウで認証エージングタイムも設定できます。

[セキュリティ] > [認証] > [認証状態テーブル] をクリックして、以下のウィンドウを表示します。

図 9-26 認証状態テーブル

設定パラメータ （[認証状態テーブル] セクション）

パラメータ	概要
認証エージングタイム	MAC/Web 認証セッションのタイムアウト値を入力します。（設定範囲：0-65535）
Sort By	• MAC - 認証セッションを MAC アドレス順に表示します。 • Port - 指定したポートの認証セッションを表示します。

[**適用**] ボタン - 設定内容を反映します。
[**検索**] ボタン - 検索結果を表示します。

9.4.3 2 ステップ認証の設定

このウィンドウを用いて、指定したポートの 2 ステップ認証の設定を行い、設定値を表示します。

[セキュリティ] > [認証] > [2 ステップ認証の設定] をクリックして、以下のウィンドウを表示します。

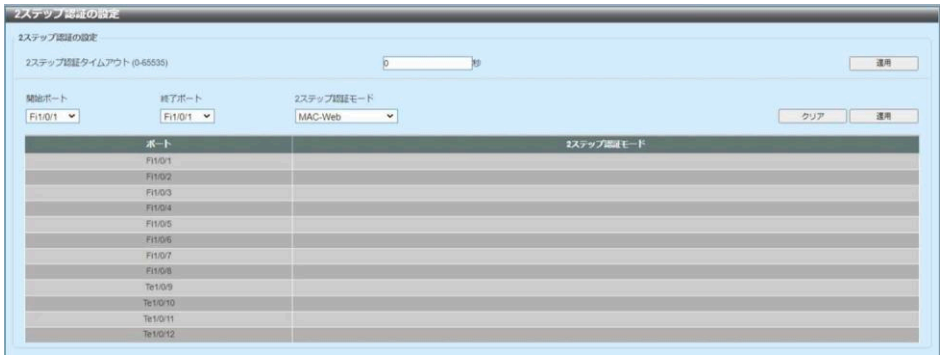


図 9-27 2 ステップ認証の設定

[2 ステップ認証の設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
2 ステップ認証タイムアウト	タイムアウト値を入力します。この時間が経過すると、認証の第 2 段階を試行します。(設定範囲：0-65535)
開始ポート／終了ポート	ポートを選択します。
2 ステップ認証モード	2 ステップ認証モードを選択します。 • **MAC-Web** - 2 ステップ認証方式の最初のステップで MAC 認証と Web 認証の両方を使用します。 • **MAC-Dot1X** - 2 ステップ認証方式の最初のステップで MAC 認証と IEEE 802.1X 認証の両方を使用します。 • **Dot1X-Web** - 2 ステップ認証方式の最初のステップで IEEE 802.1X 認証と Web 認証の両方を使用します。

[**適用**] ボタン - 設定内容を反映します。
[クリア] ボタン - 指定した条件に基づいて情報をクリアします。

9.5 RADIUS（Remote Authentication Dial-In User Service）

9.5.1 RADIUS グローバル設定

このウィンドウを用いて、RADIUS 機能に関連付けられているグローバル設定を行い、設定値を表示します。

[セキュリティ] > [RADIUS] > [RADIUS グローバル設定] をクリックして、以下のウィンドウを表示します。

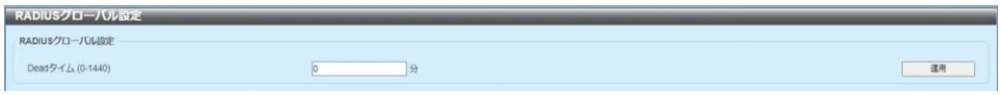


図 9-28 RADIUS グローバル設定

設定パラメータ （[RADIUS グローバル設定] セクション）

パラメータ	概要
Dead タイム	Dead タイム値を入力します。システムが認証サーバを使用して認証を実行する場合、サーバを 1 つずつ試行します。試行したサーバが応答しない場合は次のサーバを試行します。システムは、応答しないサーバを見つけると、そのサーバをダウンとしてマークして、Dead 時間タイマーを開始します。この状態のサーバは、Dead 時間が経過するまで、それ以降のリクエストの認証ではスキップされます。 このオプションが 0 の場合、応答しないサーバは Dead としてマークされません。この設定を用いて、応答しないサーバホストエントリをスキップする Dead タイムを設定することによって、認証処理時間を短縮できます。 （デフォルト：0、設定範囲：0-1440）

[**適用**] ボタン - 設定内容を反映します。

9.5.2 RADIUS サーバ設定

このウィンドウを用いて、RADIUS サーバの設定を行い、設定値を表示します。

[セキュリティ] > [RADIUS] > [RADIUS サーバ設定] をクリックして、以下のウィンドウを表示します。

図 9-29 RADIUS サーバ設定

設定パラメータ （[RADIUS サーバ設定] セクション）

パラメータ	概要
IP アドレス	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 アドレス	RADIUS サーバの IPv6 アドレスを入力します。
認証ポート	使用する認証ポート番号を入力します。 認証を使用しない場合は、値 0 を使用します。 （デフォルト：1812、設定範囲：0-65535）
アカウンティングポート	使用するアカウンティングポート番号を入力します。 アカウンティングを使用しない場合は、値 0 を使用します。 （デフォルト：1813、設定範囲：0-65535）
再送信	再送信回数の値を入力します。 このオプションを無効にするには、値 0 を入力します。 （デフォルト：3、設定範囲：0-20）
タイムアウト	使用するタイムアウト値を入力します。 （デフォルト：5、設定範囲：1-255）
キータイプ	使用するキータイプ（**Plain Text**/**Encrypted**）を選択します。
キー	RADIUS サーバとの通信に使用するキーを入力します。 （最大：32 文字）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.5.3 RADIUS グループサーバ設定

このウィンドウを用いて、RADIUS グループサーバの設定を行い、設定値を表示します。

[セキュリティ] > [RADIUS] > [RADIUS グループサーバ設定] をクリックして、以下のウィンドウを表示します。

図 9-30 RADIUS グループサーバ設定

設定パラメータ （[RADIUS グループサーバ設定] セクション）

パラメータ	概要
グループサーバ名	RADIUS グループサーバ名を入力します。名前は 32 文字までです。
IP アドレス	RADIUS グループサーバの IPv4 アドレスを入力します。
IPv6 アドレス	RADIUS グループサーバの IPv6 アドレスを入力します。

[**追加**] ボタン - エントリを追加します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**削除**] ボタン - エントリを削除します。
[**詳細参照**] ボタン - 詳細参照画面を表示します。

設定パラメータ （[詳細参照]）

パラメータ	概要
IPv4 RADIUS ソースインタフェース名	IPv4 RADIUS ソースインタフェースの名前を入力します。
IPv6 RADIUS ソースインタフェース名	IPv6 RADIUS ソースインタフェースの名前を入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

9.5.4 RADIUS 統計

このウィンドウを用いて、RADIUS 統計情報を表示およびクリアします。

[セキュリティ] > [RADIUS] > [RADIUS 統計] をクリックして、以下のウィンドウを表示します。

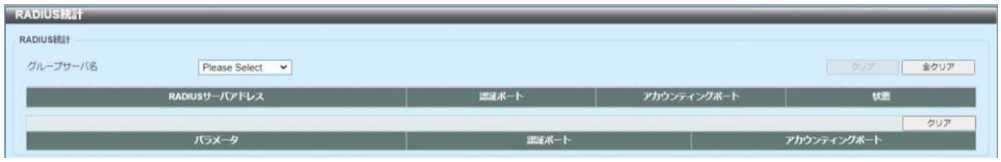


図 9-31 RADIUS 統計

設定パラメータ （[RADIUS 統計] セクション）

パラメータ	概要
グループサーバ名	このリストから RADIUS グループサーバ名を選択します。

[クリア] ボタン - 統計情報をクリアします。
[全クリア] ボタン - すべての統計情報をクリアします。

9.6 TACACS+（Terminal Access Controller Access-Control System Plus）

9.6.1 TACACS+ サーバ設定

このウィンドウを用いて、TACACS+ サーバの設定を行い、設定値を表示します。

[セキュリティ] > [TACACS+] > [TACACS+ サーバ設定] をクリックして、以下のウィンドウを表示します。

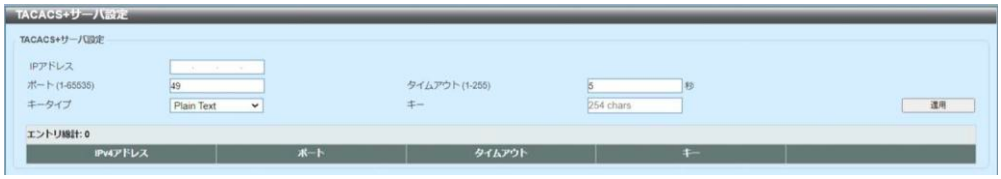


図 9-32 TACACS+ サーバ設定

設定パラメータ （[TACACS+ サーバ設定] セクション）

パラメータ	概要
IP アドレス	TACACS+ サーバの IPv4 アドレスを入力します。
ポート	使用するポート番号をここに入力します。 （デフォルト：49、設定範囲：1-65535）
タイムアウト	タイムアウト値（秒）を入力します。 （デフォルト：5、設定範囲：1-255）
キータイプ	使用するキータイプ（**Plain Text**/**Encrypted**）を選択します。です。
キー	TACACS+ サーバとの通信に使用するキーを入力します。 （最大：254 文字）

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.6.2 TACACS+ グループサーバ設定

このウィンドウを用いて、TACACS+ グループサーバの設定を行い、設定値を表示します。

[セキュリティ] > [TACACS+] > [TACACS+ グループサーバ設定] をクリックして、以下のウィンドウを表示します。

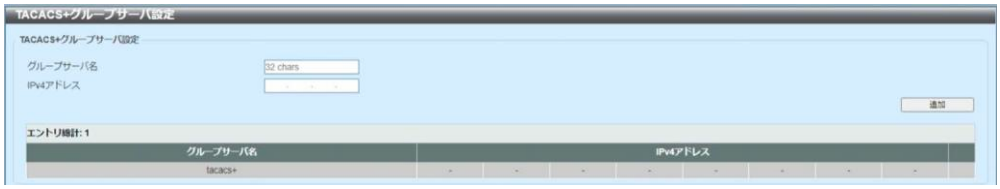


図 9-33 TACACS+ グループサーバ設定

設定パラメータ （[TACACS+ グループサーバ設定] セクション）

パラメータ	概要
グループサーバ名	TACACS+ グループサーバ名を入力します。名前は 32 文字までです。
IPv4 IP アドレス	TACACS+ グループサーバの IPv4 アドレスを入力します。

[**追加**] ボタン - エントリを追加します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[詳細参照]>[TACACS+ グループサーバ設定] セクション）

パラメータ	概要
IPv4 TACACS+ ソースインタフェース名	IPv4 TACACS+ ソースインタフェースの名前を入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

9.6.3 TACACS+ 統計

このウィンドウを用いて、TACACS+ 統計情報を表示およびクリアします。

[セキュリティ] > [TACACS+] > [TACACS+ 統計] をクリックして、以下のウィンドウを表示します。

図 9-34 TACACS+ 統計

設定パラメータ （[TACACS+ 統計] セクション）

パラメータ	概要
グループサーバ名	このリストから TACACS+ グループサーバ名を選択します。

[クリア] ボタン - 指定した条件に基づいて統計情報をクリアします。
[全クリア] ボタン - すべての統計情報をクリアします。

9.7 SAVI（Source Address Validation Improvements）

9.7.1 IPv4

9.7.1.1 DHCPv4 スヌーピング

9.7.1.1.1 DHCP スヌーピンググローバル設定

このウィンドウを用いて、DHCP スヌーピング機能に関連付けられているグローバル設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピンググローバル設定] をクリックして、以下のウィンドウを表示します。

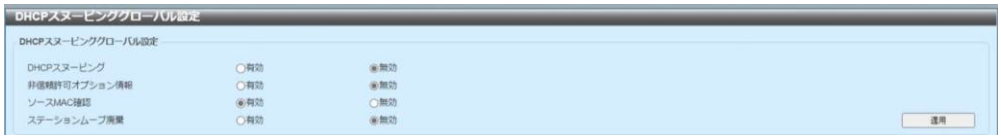


図 9-35 DHCP スヌーピンググローバル設定

設定パラメータ （[DHCP スヌーピンググローバル設定] セクション）

パラメータ	概要
DHCP スヌーピング	DHCP スヌーピングの状態（**有効** / **無効**）を選択します。
非信頼許可オプション情報	非信頼インタフェースでリレー Option 82 が設定されている DHCP パケットを許可するオプションの状態（**有効** / **無効**）を選択します。
ソース MAC 確認	DHCP パケットのソース MAC アドレスがクライアントのハードウェアアドレスと適合することの検証の状態（**有効** / **無効**）を選択します。
ステーションムーブ廃棄	DHCP スヌーピングステーションムーブの状態（**有効** / **無効**）を選択します。DHCP スヌーピングステーションムーブが有効な場合、特定のポートで同じ VLAN ID と MAC アドレスを持つダイナミック DHCP スヌーピングバインディングエントリは、同じ VLAN ID と MAC アドレスを使用する新しい DHCP プロセスを検出した場合に別のポートに移動できます。

[**適用**] ボタン - 設定内容を反映します。

9.7.1.1.2 DHCP スヌーピングポート設定

このウィンドウを用いて、指定したポートの DHCP スヌーピングの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピングポート設定] をクリックして、以下のウィンドウを表示します。

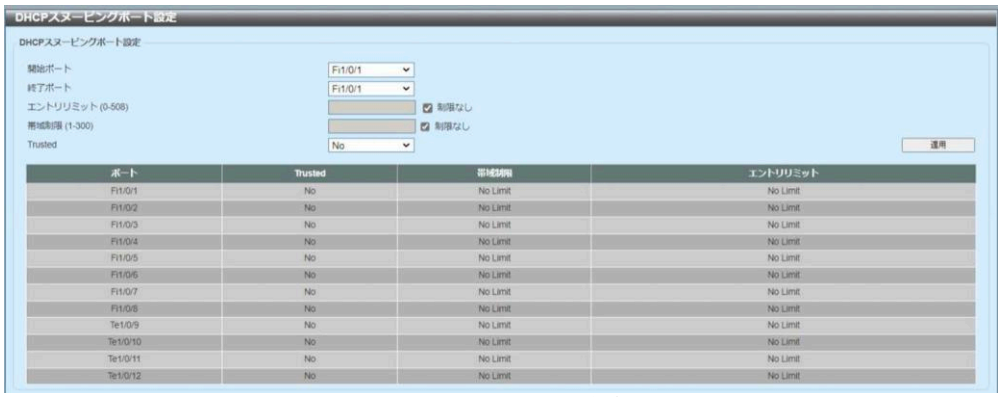


図 9-36 DHCP スヌーピングポート設定

設定パラメータ （[DHCP スヌーピングポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
エントリリミット	エントリリミット値を入力します。（設定範囲：0-508） **[制限なし]** オプションをオンにした場合、機能を無効にします。
帯域制限	帯域制限値を入力します。（設定範囲：1-300） **[制限なし]** オプションをオンにした場合、機能を無効にします。
Trusted	Trusted オプション（**Yes**/**No**）を選択します。 DHCP サーバまたは他のスイッチに接続しているポートは、Trusted インタフェースとして設定する必要があります。 DHCP クライアントに接続しているポートは、非信頼インタフェースとして設定する必要があります。DHCP スヌーピングは、非信頼インタフェースと DHCP サーバの間でファイアウォールとして動作します。

[**適用**] ボタン - 設定内容を反映します。

9.7.1.1.3 DHCP スヌーピング VLAN 設定

このウィンドウを用いて、指定した VLAN の DHCP スヌーピングの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピング VLAN 設定] をクリックして、以下のウィンドウを表示します。

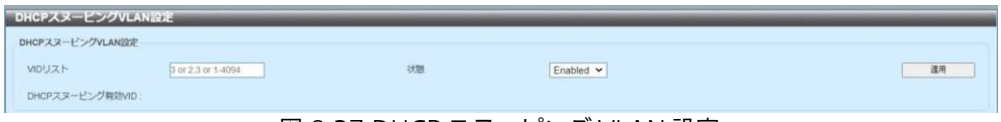


図 9-37 DHCP スヌーピング VLAN 設定

設定パラメータ （[DHCP スヌーピング VLAN 設定] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）
状態	DHCP スヌーピング VLAN の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

9.7.1.1.4 DHCP スヌーピングデータベース

このウィンドウを用いて、DHCP スヌーピングデータベースの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピングデータベース] をクリックして、以下のウィンドウを表示します。

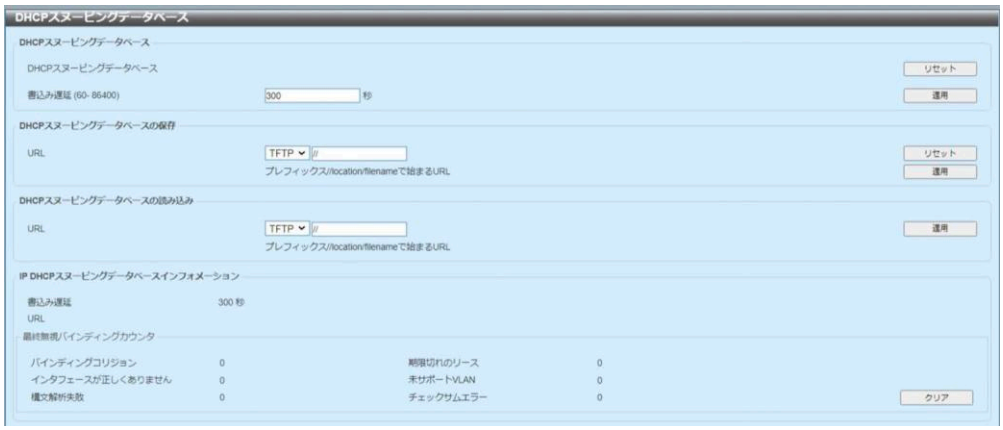


図 9-38 DHCP スヌーピングデータベース

設定パラメータ （[DHCP スヌーピングデータベース] セクション）

パラメータ	概要
書込み遅延	書込み遅延時間を入力します。 （デフォルト：300、設定範囲：60-86400）

[**リセット**] ボタン - DHCP スヌーピングデータベースをリセットします。
[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[DHCP スヌーピングデータベースの保存] セクション）

パラメータ	概要
URL	ドロップダウンリストから場所（**TFTP**/**FTP**）を選択して、DHCP スヌーピングデータベースを保存する URL を入力します。

[**リセット**] ボタン - DHCP スヌーピングデータベースをリセットします。
[**適用**] ボタン - DHCP スヌーピングデータベースを保存します。

設定パラメータ （[DHCP スヌーピングデータベースの読み込み] セクション）

パラメータ	概要
URL	ドロップダウンリストから場所（**TFTP**/**FTP**）を選択して、DHCP スヌーピングデータベースを読み込む URL を入力します。

[**適用**] ボタン - DHCP スヌーピングデータベースを読み込みます。
[**クリア**] ボタン - カウンタ情報をクリアします。

9.7.1.1.5 DHCP スヌーピングバインディングエントリ

このウィンドウを用いて、DHCP スヌーピングバインディングエントリの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピングバインディングエントリ] をクリックして、以下のウィンドウを表示します。

図 9-39 DHCP スヌーピングバインディングエントリ

設定パラメータ （[DHCP スヌーピングマニュアルバインディング] セクション）

パラメータ	概要
MAC アドレス	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
IP アドレス	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
ポート	ポートを選択します。
Expiry	使用する有効期限値（秒）を入力します。 （設定範囲：60-4294967295）

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.7.1.2 ダイナミック ARP 検査

9.7.1.2.1 ARP アクセスリスト

このウィンドウを用いて、ダイナミック ARP 検査に使用する ARP アクセスリストの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [ダイナミック ARP 検査] > [ARP アクセスリスト] をクリックして、以下のウィンドウを表示します。

図 9-40 ARP アクセスリスト

設定パラメータ （[ARP アクセスリスト] セクション）

パラメータ	概要
ARP アクセスリスト名	使用する ARP アクセスリスト名を入力します。 (最大：32 文字)

[**追加**] ボタン - エントリを追加します。
[**編集**] ボタン - エントリの設定を編集します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[編集]）

パラメータ	概要
アクション	実行するアクション（**Permit**/**Deny**）を選択します。
IP	使用するセンダー IP アドレスのタイプ（**Any**/**Host**/**IP with Mask**）を選択します。
センダー IP	([IP] パラメータで [Host] または [IP with Mask] 選択時の設定可) 使用するセンダー IP アドレスを入力します。
センダー IP マスク	([IP] パラメータで [IP with Mask] 選択時の設定可) 使用するセンダー IP マスクを入力します。
MAC	使用するセンダー MAC アドレスのタイプ（**Any**/**Host**/**MAC with Mask**）を選択します。
センダー MAC	([MAC] パラメータで [Host] または [MAC with Mask] 選択時の設定可) 使用するセンダー MAC アドレスを入力します。
センダー MAC マスク	([MAC] パラメータで [MAC with Mask] 選択時の設定可) 使用するセンダー MAC マスクを入力します。

[**適用**] ボタン - エントリを追加します。
[**戻る**] ボタン - 前のウィンドウに戻ります。
[**削除**] ボタン - エントリを削除します。

9.7.1.2.2 ARP 検査設定

このウィンドウを用いて、ダイナミック ARP 検査の設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [ダイナミック ARP 検査] > [ARP 検査設定] をクリックして、以下のウィンドウを表示します。

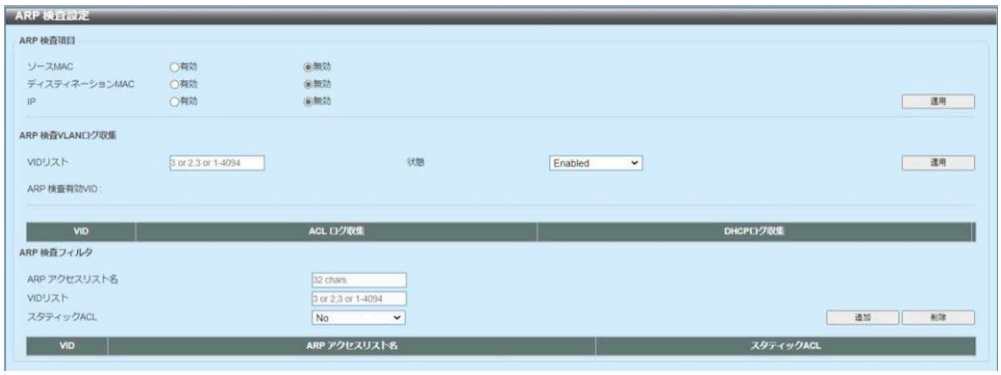


図 9-41 ARP 検査設定

設定パラメータ （[ARP 検査項目] セクション）

パラメータ	概要
ソース MAC	ソース MAC オプションの状態（**有効** / **無効**）を選択します。ARP リクエスト / 応答パケットをチェックして、イーサネットヘッダのソース MAC アドレスが ARP ペイロードのセンダー MAC アドレスと一致していることをチェックします。
ディスティネーション MAC	ディスティネーション MAC オプションの状態（**有効** / **無効**）を選択します。ARP 応答パケットをチェックして、イーサネットヘッダのディスティネーション MAC アドレスが ARP ペイロードのターゲット MAC アドレスと一致していることをチェックします。
IP	IP オプションの状態（**有効** / **無効**）を選択します。ARP ボディで無効な IP アドレスや予期しない IP アドレスをチェックします。また、ARP ペイロードの IP アドレスの有効性をチェックします。ARP リクエスト / 応答の両方のセンダー IP と ARP 応答のターゲット IP を検証します。IP アドレス 0.0.0.0 と 255.255.255.255、およびすべての IP マルチキャストアドレスをディスティネーションとするパケットは、廃棄されます。センダー IP アドレスは、すべての ARP リクエスト / 応答でチェックされます。ターゲット IP アドレスは、ARP 応答でのみチェックされます。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （ARP 検査 VLAN ログ収集] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。(設定範囲：1-4094)
状態	指定した VLAN の ARP 検査 VLAN ログ収集の状態 (**Enabled**/**Disabled**) を選択します。

[**適用**] ボタン - エントリを追加します。
[**編集**] ボタン - エントリの設定を編集します。

設定パラメータ ([ARP 検査フィルタ] セクション)

パラメータ	概要
ARP アクセスリスト名	使用する ARP アクセスリスト名を入力します。(最大：32 文字)
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。(設定範囲：1-4094)
スタティック ACL	スタティック ACL (Yes/No) を使用を選択します。

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.7.1.2.3 ARP 検査ポート設定

このウィンドウを用いて、指定したポートのダイナミック ARP 検査の設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [ダイナミック ARP 検査] > [ARP 検査ポート設定] をクリックして、以下のウィンドウを表示します。

図 9-42 ARP 検査ポート設定

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
帯域制限	帯域制限値（pps）を入力します。 （選択範囲：1-150）
バースト間隔	バースト間隔値を入力します。（設定範囲：1-15） **[なし]** オプションをオンにした場合、オプションを無効にします。
信頼状態	信頼状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。
[**デフォルト設定**] ボタン - 信頼状態をデフォルト設定に設定します。

9.7.1.2.4 ARP 検査統計情報

このウィンドウを用いて、ダイナミック ARP 検査統計情報を表示およびクリアします。

[セキュリティ] > [SAVI] > [IPv4] > [ダイナミック ARP 検査] > [ARP 検査統計情報] をクリックして、以下のウィンドウを表示します。

図 9-43 ARP 検査統計情報

設定パラメータ

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。(設定範囲：1-4094)

[**VLAN 単位クリア**] ボタン - 指定した VLAN に関する統計情報をクリアします。
[**全クリア**] ボタン - すべての統計情報をクリアします。

9.7.1.2.5 ARP 検査ログ

このウィンドウを用いて、ダイナミック ARP 検査ログ情報を表示およびクリアします。また、このウィンドウでログバッファ値も設定できます。

[セキュリティ] > [SAVI] > [IPv4] > [ダイナミック ARP 検査] > [ARP 検査ログ] クリックして、以下のウィンドウを表示します。

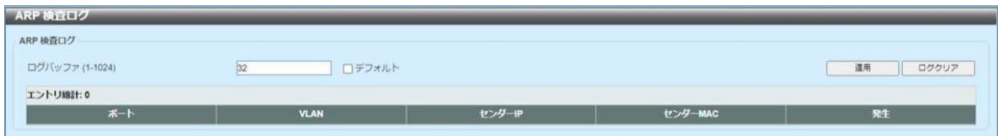


図 9-44 ARP 検査ログ

設定パラメータ （[ARP 検査ログ] セクション）

パラメータ	概要
ログバッファ	ログバッファのサイズを入力します。 （デフォルト：32、選択範囲：1-1024） **[デフォルト]** オプションを選択した場合、デフォルト値を使用します。

[**適用**] ボタン - 設定内容を反映します。
[**ログクリア**] ボタン - ARP 検査ログをクリアします。

9.7.1.3 IP ソースガード

9.7.1.3.1 IP ソースガードポート設定

このウィンドウを用いて、指定したポートの IP ソースガードの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [IP ソースガード] > [IP ソースガードポート設定] をクリックして、以下のウィンドウを表示します。

図 9-45 IP ソースガードポート設定

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの IP ソースガードの状態（**Enabled**/**Disabled**）を選択します。
検証	使用する検証方法を選択します。 • **IP** - 受信したパケットの IP アドレスをチェックします。 • **IP-MAC** - 受信したパケットの IP アドレスと MAC アドレスをチェックします。

[**適用**] ボタン - エントリを追加します。

9.7.1.3.2 IP ソースガードバインディング

このウィンドウを用いて、IP ソースガードバインディングの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [IP ソースガード] > [IP ソースガードバインディング] をクリックして、以下のウィンドウを表示します。

図 9-46 IP ソースガードバインディング

設定パラメータ （[IP ソースバインディング設定] セクション）

パラメータ	概要
MAC アドレス	バインディングエントリの MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
IP アドレス	バインディングエントリの IP アドレスを入力します。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[IP ソースバインディングエントリ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
IP アドレス	バインディングエントリの IP アドレスを入力します。
MAC アドレス	バインディングエントリの MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
タイプ	検索するバインディングエントリのタイプを選択します。 • **All** - すべての DHCP バインディングエントリを表示します。 • **DHCP-Snooping** - DHCP バインディングスヌーピングによって学習された IP ソースガードバインディングエントリを表示します。 • **Static** - 手動で設定された IP ソースガードバインディングエントリを表示します。

[**検索**] ボタン - 検索結果を表示します。
[**削除**] ボタン - エントリを削除します。

9.7.1.3.3 IP ソースガード HW エントリ

このウィンドウを用いて、指定したポートの IP ソースガードハードウェアエントリを表示します。

[セキュリティ] > [SAVI] > [IPv4] > [IP ソースガード] > [IP ソースガード HW エントリ] をクリックして、以下のウィンドウを表示します。

図 9-47 IP ソースガード HW エントリ

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。

9.8 DHCP サーバプロテクト

9.8.1 DHCP サーバプロテクトグローバル設定

このウィンドウを用いて、DHCP サーバプロテクト機能に関連付けられているグローバル設定を行い、設定値を表示します。

[セキュリティ] > [DHCP サーバプロテクト] > [DHCP サーバプロテクトグローバル設定] をクリックして、以下のウィンドウを表示します。

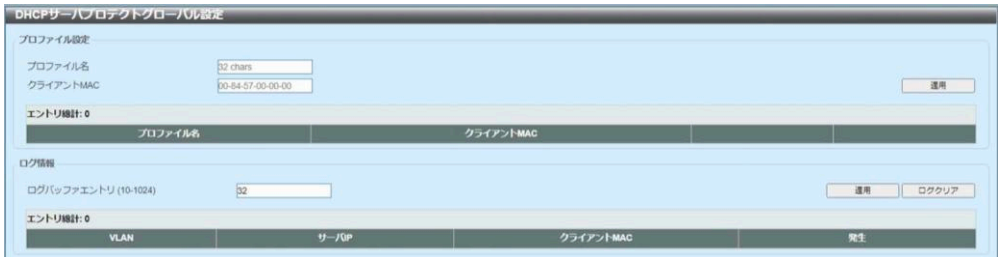


図 9-48 DHCP サーバプロテクトグローバル設定

設定パラメータ （[プロファイル設定] セクション）

パラメータ	概要
プロファイル名	DHCP サーバプロテクトプロファイル名を入力します。 （最大：32 文字）
クライアント MAC	使用する MAC アドレスを入力します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - プロファイルから MAC アドレスを削除します。
[**プロファイル削除**] ボタン - プロファイルを削除します。

設定パラメータ （[ログ情報] セクション）

パラメータ	概要
ログバッファエントリ	ログに記録するエントリ数を入力します。 （デフォルト：32、設定範囲：10-1024）

9.8.2 DHCP サーバプロテクトポート設定

このウィンドウを用いて、指定したポートの DHCP サーバプロテクトの設定を行い、設定値を表示します。

[セキュリティ] > [DHCP サーバプロテクト] > [DHCP サーバプロテクトポート設定] をクリックして、以下のウィンドウを表示します。

図 9-49 DHCP サーバプロテクトポート設定

設定パラメータ （[DHCP サーバプロテクトポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの DHCP サーバプロテクト機能の状態（**Enabled**/**Disabled**）を選択します。
サーバ IP	DHCP サーバの IP アドレスを入力します。
プロファイル名	指定したポートで使用する DHCP サーバプロテクトプロファイルを入力します。（最大：32 文字）

[**適用**] ボタン - 設定内容を反映します。
[**削除**] ボタン - 指定したポートからサーバ IP アドレスとプロファイル名を削除します。

9.9 BPDU ガード

このウィンドウを用いて、指定したポートの BPDU ガード機能の状態および BPDU ガードの設定を行い、設定値を表示します。

[セキュリティ] > [BPDU ガード] をクリックして、以下のウィンドウを表示します。

図 9-50 BPDU ガード

設定パラメータ （[BPDU ガード設定] セクション）

パラメータ	概要
BPDU ガード状態	BPDU ガード機能の状態（**有効** / **無効**）を選択します。
BPDU ガードトラップ状態	BPDU ガードトラップの状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[BPDU ガードポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの BPDU ガードの状態（**Enabled**/ **Disabled**）を選択します。
モード	指定したポートに適用する BPDU ガードモードを選択します。 • **Drop** - ポートでアタックを検出した場合に、受信したすべての BPDU パケットを廃棄します。 • **Block** - ポートでアタックを検出した場合に、（BPDU および正常なパケットを含む）すべてのパケットを廃棄します。 • **Shutdown** - ポートでアタックを検出した場合に、ポートをシャットダウンします。

[**適用**] ボタン - 設定内容を反映します。

9.10 NetBIOS フィルタリング

このウィンドウを用いて、指定したポートの NetBIOS フィルタリングの設定を行い、設定値を表示します。

[セキュリティ] > [NetBIOS フィルタリング] をクリックして、以下のウィンドウを表示します。

図 9-51 NetBIOS フィルタリング

設定パラメータ （[NetBIOS フィルタリング] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
NetBIOS フィルタリング状態	指定したポートの NetBIOS フィルタリングの状態（**Enabled**/**Disabled**）を選択します。これを用いて、物理ポートで NetBIOS パケットを許可または拒否します。
広域 NetBIOS フィルタリング状態	指定したポートの広域 NetBIOS フィルタリングの状態（**Enabled**/**Disabled**）を選択します。これを用いて、物理ポートで 802.3 フレームを介した NetBIOS パケットを許可または拒否します。

[**適用**] ボタン - 設定内容を反映します。

9.11 MAC 認証

このウィンドウを用いて、MAC 認証の設定を行い、設定値を表示します。

[セキュリティ] > [MAC 認証] をクリックして、以下のウィンドウを表示します。

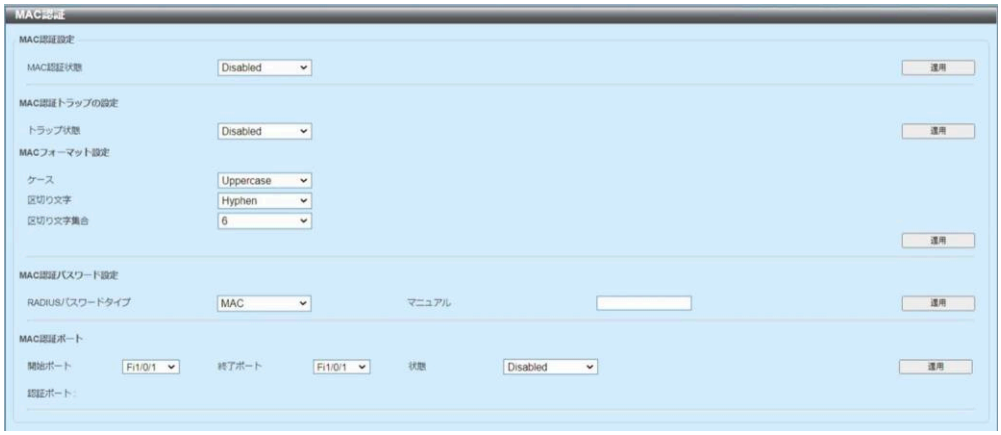


図 9-52 MAC 認証

設定パラメータ （[MAC 認証設定] セクション）

パラメータ	概要
MAC 認証状態	MAC 認証機能の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC フォーマット設定] セクション）

パラメータ	概要
ケース	MAC アドレスで使用する文字の形式を選択します。 • **Uppercase** - MAC アドレスに大文字形式を使用します。たとえば、AA-BB-CC-DD-EE-FF となります。 • **Lowercase** - MAC アドレスに小文字形式を使用します。たとえば、aa-bb-cc-dd-ee-ff となります。
区切り文字	MAC アドレスで使用する区切り文字のタイプを選択します。 • **Hyphen** - MAC アドレスで区切り文字としてハイフンを使用します。たとえば、AA-BB-CC-DD-EE-FF となります。 • **Colon** - MAC アドレスで区切り文字としてコロンを使用します。たとえば、AA：BB：CC：DD：EE：FF となります。 • **Dot** - MAC アドレスで区切り文字としてドットを使用します。たとえば、AA.BB.CC.DD.EE.FF となります。 • **None** - MAC アドレスで区切り文字を使用しません。たとえば、AABBCCDDEEFF となります。
区切り文字集合	MAC アドレスで使用する区切り文字の数を選択します。 • **2** - MAC アドレスで区切り文字を 1 つ使用します。たとえば、AABBCC-DDEEFF となります。 • **4** - MAC アドレスで区切り文字を 2 つ使用します。たとえば、AABB-CCDD-EEFF となります。 • **6** - MAC アドレスで区切り文字を 5 つ使用します。たとえば、AA-BB-CC-DD-EE-FF となります。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC 認証パスワード設定] セクション）

パラメータ	概要
RADIUS パスワードタイプ	RADIUS パスワードタイプを選択します。 • **MAC** - RADIUS パスワードとして MAC アドレスを使用します。 • **Manual** - RADIUS パスワードとしてマニュアル文字列を使用します。
マニュアル	MAC 認証アカウントの RADIUS パスワードを入力します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC 認証ポート] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの MAC 認証の有効、無効を設定します。

[**適用**] ボタン - 設定内容を反映します。

9.12 Web 認証

9.12.1 Web 認証設定

このウィンドウを用いて、Web 認証の設定を行い、設定値を表示します。

[セキュリティ] > [Web 認証] > [Web 認証設定] をクリックして、以下のウィンドウを表示します。

図 9-53 Web 認証設定

設定パラメータ （[グローバル設定] セクション）

パラメータ	概要
認証状態	Web 認証機能の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[認証ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの Web 認証機能の状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[認証設定] セクション）

パラメータ	概要
仮想 IP	使用する仮想 IPv4 アドレスを入力します。すべての Web 認証プロセスはこの仮想 IP アドレスと通信しますが、ICMP パケットまたは ARP リクエストに対してこの仮想 IP が応答することはありません。仮想 IPv4 アドレスとスイッチの IPv4 アドレスは、別々のサブネットを使用する必要があります。仮想 IPv4 アドレスは、Web 認証の正常動作に欠かせないコンポーネントです。
HTTP ポート番号	HTTP TCP/UDP ポート番号を入力します。 （デフォルト：80、設定範囲：1-65535）
リダイレクト **URL**	リダイレクト URL を入力します。（最大：64 文字）

[**適用**] ボタン - 設定内容を反映します。

9.12.2 Web ページコンテンツの設定

このウィンドウを用いて、Web ページコンテンツの設定を行い、設定値を表示します。

[セキュリティ] > [Web 認証] > [Web ページコンテンツの設定] をクリックして、以下のウィンドウを表示します。

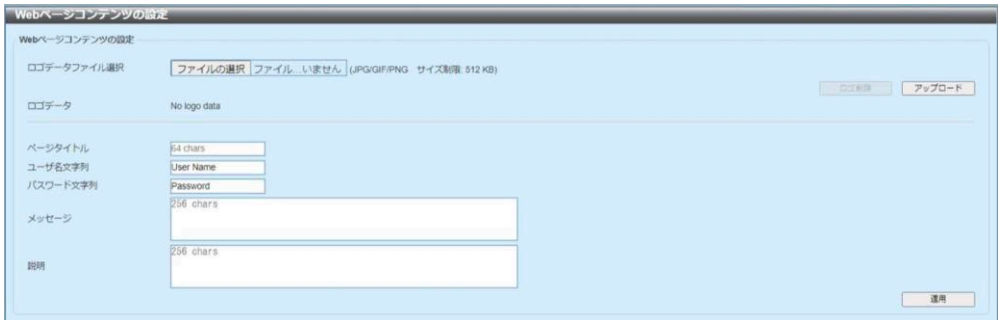


図 9-54 Web ページコンテンツの設定

設定パラメータ （[Web ページコンテンツの設定] セクション）

パラメータ	概要
ロゴデータファイル選択	**[ファイルを選択]** ボタンをクリックして、アップロードするイメージファイル（JPG/GIF/PNG）がある場所に移動します。
ロゴデータ	アップロードされているイメージファイル（使用中）が表示されます。512KB まで転送可能です。 **[ロゴ削除]** ボタンをクリックして、既存のイメージファイルを削除します。
ページタイトル	カスタムのページタイトルメッセージを入力します。 日本語入力が可能です。（最大：64 文字）
ユーザ名文字列	カスタムのユーザ名タイトルを入力します。 日本語入力が可能です。（最大：32 文字）
パスワード文字列	カスタムのパスワードタイトルを入力します。 日本語入力が可能です。（最大：32 文字）
メッセージ	カスタムのメッセージを入力します。（最大：256 文字） 日本語入力および以下の HTML タグが使用可能です。 以下の <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p>
説明	カスタムの説明メッセージを入力します。（最大：256 文字） 日本語入力および以下の HTML タグが使用可能です。 以下の <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p>

[アップロード] ボタン - 新しいロゴをアップロードします。

[**適用**] ボタン - 設定内容を反映します。

9.12.3 一時 DHCP サーバ設定

このウィンドウを用いて、一時 DHCP サーバ設定を行います。

[セキュリティ] > [Web 認証] > [一時 DHCP サーバ設定] をクリックして、以下のウィンドウを表示します。

図 9-55 一時 DHCP サーバ設定

設定パラメータ （[一時 DHCP サーバ設定] セクション）

パラメータ	概要
一時 DHCP サーバ状態	一時利用 DHCP サーバの状態（**Enabled**/**Disabled**）を選択します。
リース IP アドレス数	リースする IP アドレス数を入力します。 （デフォルト：32、設定範囲：1-64）
DHCP リースタイム	IP アドレスのリース時間 （ 秒 ）を入力します。 （設定範囲：10-60）
開始リース IP アドレス	リースする IP アドレスの開始アドレスを入力します。
DNS サーバアドレス	DHCP で通知する DNS サーバアドレスの値を入力します。
デフォルトゲートウェイ	DHCP で通知するデフォルトゲートウェイアドレスの値を入力します。

[**適用**] ボタン - 設定内容を反映します。

9.13 信頼されたホスト

このウィンドウを用いて、信頼されたホストのの設定を行い、設定値を表示します。

[セキュリティ] > [信頼されたホスト] をクリックして、以下のウィンドウを表示します。

図 9-56 信頼されたホスト

設定パラメータ （[信頼されたホスト] セクション）

パラメータ	概要
ACL 名称	ACL の名前を入力します。（最大：32 文字）
タイプ	信頼されたホストのタイプ（**Telnet**/**SSH**/**Ping**/**HTTP**/**HTTPS**）を選択します。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.14 トラフィックセグメンテーション設定

このウィンドウを用いて、指定したポートのトラフィックセグメンテーションの設定を行い、設定値を表示します。

[セキュリティ] > [トラフィックセグメンテーション設定] をクリックして、以下のウィンドウを表示します。

図 9-57 トラフィックセグメンテーション設定

設定パラメータ （[トラフィックセグメンテーション設定] セクション）

パラメータ	概要
開始ポート／終了ポート	パケットを受信するポートを選択します。
開始フォワードポート - 終了フォワードポート	パケットを転送するポートを選択します。

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

9.15 ストームコントロール

このウィンドウを用いて、ストームコントロールの設定を行い、設定値を表示します。

[セキュリティ] > [ストームコントロール] をクリックして、以下のウィンドウを表示します。

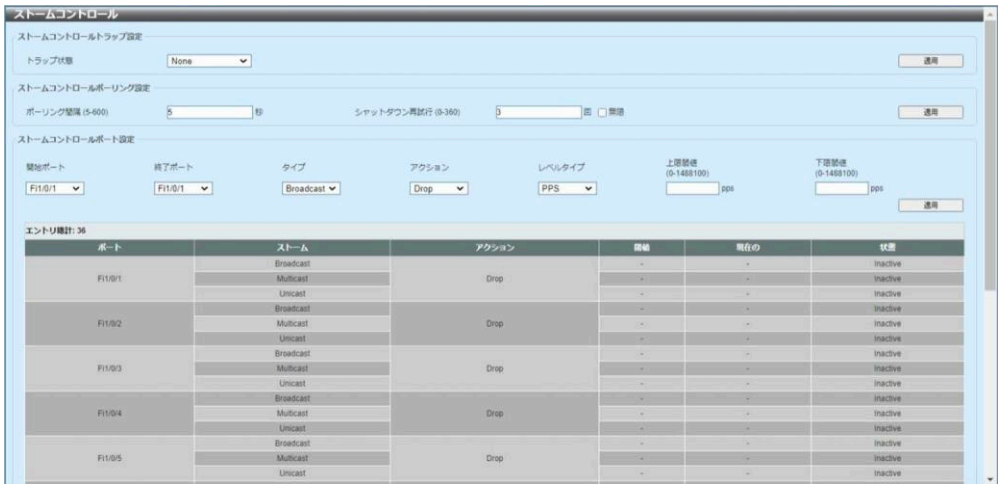


図 9-58 ストームコントロール（レベルタイプ、PPS）

設定パラメータ （[ストームコントロールポーリング設定] セクション）

パラメータ	概要
ポーリング間隔	使用するポーリング間隔値（秒）を入力します。 （デフォルト：5、設定範囲：5-600）
シャットダウン再試行	シャットダウン再試行回数の値を入力します。 （デフォルト：3、設定範囲：0-360） **[無限]** オプションをオンにした場合、この機能を無効にします。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ストームコントロールポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

パラメータ	概要
タイプ	制御するストームアタックのタイプ（**Broadcast**/**Multicast**/**unicast**）を選択します。 **[** アクション **]** として **[Shutdown]** が設定されている場合、ユニキャストは、既知と未知の両方のユニキャストパケットを指します。すなわち、既知と未知のユニキャストパケット数が指定した閾値に達すると、ポートをシャットダウンします。それ以外の場合は、ユニキャストは未知のユニキャストパケットを指します。
アクション	実行するアクションを選択します。 • **None** - ストームパケットをフィルタリングしません。 • **Shutdown** - 上昇閾値に指定した値に達した場合、ポートをシャットダウンします。 • **Drop** - 上昇閾値を超えるパケットを廃棄します。
レベルタイプ	レベルタイプオプション（**PPS**/**Kbps**/**Level**）を選択します。
上限閾値	PPS Rise 値を入力します。このオプションは、1 秒あたりのパケットカウントの上限レートを指定します。範囲は、1 秒あたり 1 ～ 255000 パケットです。[PPS Low] の値を指定しない場合、指定した上昇 PPS の 80% の値がデフォルト値になります。
下限閾値	PPS Low 値を入力します。このオプションは、1 秒あたりのパケットカウントの下限レートを指定します。範囲は、1 秒あたり 1 ～ 255000 パケットです。[PPS Low] の値を指定しない場合、指定した上昇 PPS の 80% の値がデフォルト値になります。

[**適用**] ボタン - 設定内容を反映します。

9.16 SSH（Secure Shell）

9.16.1 SSH グローバル設定

このウィンドウを用いて、SSH 機能に関連付けられているグローバルの設定を行い、設定値を表示します。

[セキュリティ] > [SSH] > [SSH グローバル設定] をクリックして、以下のウィンドウを表示します。

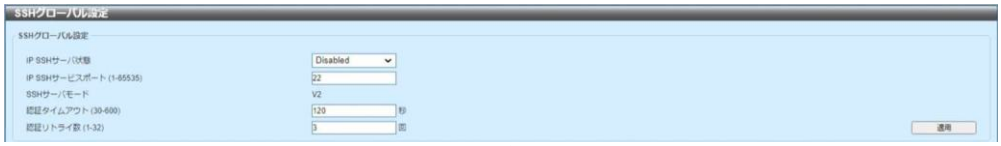


図 9-59 SSH グローバル設定

設定パラメータ （[SSH グローバル設定] セクション）

パラメータ	概要
IP SSH サーバ状態	SSH サーバの状態（**Enabled**/**Disabled**）を選択します。
IP SSH サービスポート	使用する SSH サービスポート番号を入力します。 （デフォルト：22、設定範囲：1-65535）
認証タイムアウト	認証タイムアウト値を入力します。 （デフォルト：120、設定範囲：30-600）
認証リトライ数	認証リトライ回数の値を入力します。 （デフォルト：3、設定範囲：1-32）

[**適用**] ボタン - 設定内容を反映します。

9.16.2 ホストキー

このウィンドウを用いて、SSH ホストキーの設定を行い、設定値を表示します。

[セキュリティ] > [SSH] > [ホストキー] をクリックして、以下のウィンドウを表示します。

図 9-60 ホストキー

設定パラメータ （[ホストキーマネジメント] セクション）

パラメータ	概要
暗号化キータイプ	使用する暗号化キータイプ（**RSA**/**DSA**）を選択します。
キーモジュール	キーモジュール値（**360**/**512**/**768**/**1024**/**2048**）を選択します。

[生成] ボタン - 選択内容に基づいてホストキーを生成します。
[削除] ボタン - 選択内容に基づいてホストキーを削除します。

設定パラメータ （[ホストキー] セクション）

パラメータ	概要
暗号化キータイプ	使用する暗号化キータイプ（**RSA**/**DSA**）を選択します。

9.16.3 SSH サーバコネクション

このウィンドウを用いて、SSH サーバコネクションテーブルと情報を表示します。

[セキュリティ] > [SSH] > [SSH サーバコネクション] をクリックして、以下のウィンドウを表示します。

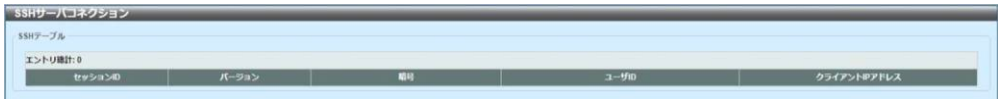


図 9-61 SSH サーバコネクション

9.16.4 SSH ユーザ設定

このウィンドウを用いて、SSH ユーザの設定を行い、設定値を表示します。

[セキュリティ] > [SSH] > [SSH ユーザ設定] をクリックして、以下のウィンドウを表示します。

図 9-62 SSH ユーザ設定

設定パラメータ （[SSH ユーザ設定] セクション）

パラメータ	概要
ユーザ名	SSH ユーザアカウントのユーザ名を入力します。 （最大：32 文字）
認証方式	SSH 認証方式（**Password**/**Public Key**/**Host-based**）を選択します。
キーファイル	（[認証方式] パラメータで [Public Key] または [Host-based] 選択時の設定可） 選択した場合に公開鍵を入力します。（最大：779 文字）
ホスト名	（[認証方式] パラメータで [Host-based] 選択時の設定可） ホスト名を入力します。（最大：225 文字）
IPv4 アドレス	（[認証方式] パラメータで [Host-based] 選択時の設定可） SSH ユーザアカウントの IPv4 アドレスを入力します。
IPv6 アドレス	（[認証方式] パラメータで [Host-based] 選択時の設定可） SSH ユーザアカウントの IPv6 アドレスを入力します。

[**適用**] ボタン - エントリを追加します。

9.17 SSL（Secure Sockets Layer）

9.17.1 SSL グローバル設定

このウィンドウを用いて、SSL 機能に関連付けられているグローバル設定を行い、設定値を表示します。

[セキュリティ] > [SSL] > [SSL グローバル設定] をクリックして、以下のウィンドウを表示します。

図 9-63 SSL グローバル設定

設定パラメータ （[SSL グローバル設定] セクション）

パラメータ	概要
SSL 状態	SSL 機能の状態（**有効** / **無効**）を選択します。
サービスポリシー	サービスポリシー名を入力します。（最大：32 文字）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[インポートファイル] セクション）

パラメータ	概要
ファイル選択	アップロードするファイルタイプ（**証明書** / **プライベートキー**）を選択します。ファイルタイプを選択した後、**[ファイルを選択]** ボタンを押して、ローカルコンピュータに存在するファイルを参照します。
インポート先ファイル名	使用するファイル名を入力します。（最大：32 文字）

[**適用**] ボタン - SSL ファイルをインポートします。

9.17.2 暗号化 PKI トラストポイント

このウィンドウを用いて、SSL 暗号化 PKI（Public Key Infrastructure）トラストポイントの設定を行い、設定値を表示します。

[セキュリティ] > [SSL] > [暗号化 PKI トラストポイント] をクリックして、以下のウィンドウを表示します。

図 9-64 暗号化 PKI トラストポイント

設定パラメータ （[暗号化 PKI トラストポイント] セクション）

パラメータ	概要
トラストポイント	インポートした証明書とキーペアに関連付けるトラストポイントの名前を入力します。（最大：32 文字）
ファイルシステムパス	証明書とキーペアのファイルシステムパスを入力します。
パスワード	プライベートキーをインポートしたときに暗号化を解除するために使用する、暗号化されたパスワードフレーズを入力します。パスワードフレーズを指定しない場合、NULL 文字列を使用します。（最大：64 文字）
TFTP サーバパス	TFTP サーバパスを入力します。
タイプ	インポートする証明書のタイプを選択します。 • **Both** - CA（Certificate Authority）証明書と、ローカル証明書およびキーペアをインポートします。 • **CA** - CA 証明書のみをインポートします。 • **Local** - ローカル証明書とキーペアのみをインポートします。

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[**削除**] ボタン - エントリを削除します。

9.17.3 SSL サービスポリシー

このウィンドウを用いて、SSL サービスポリシーの設定を行い、設定値を表示します。

[セキュリティ] > [SSL] > [SSL サービスポリシー] をクリックして、以下のウィンドウを表示します。

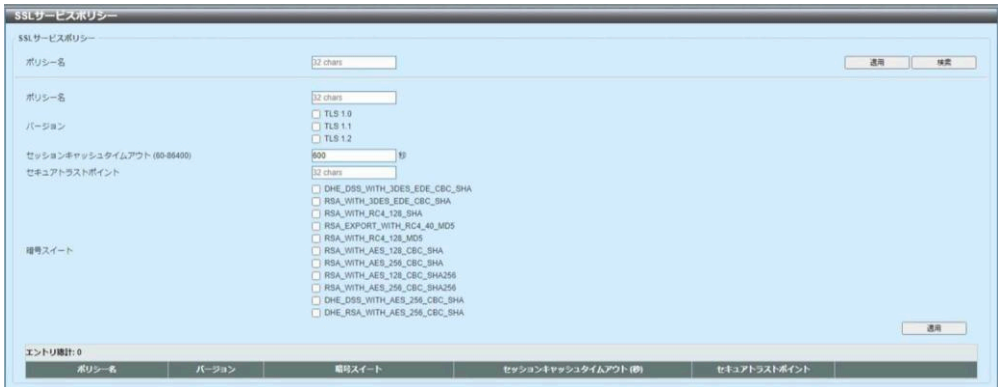


図 9-65 SSL サービスポリシー

[SSL サービスポリシー] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ポリシー名	SSL サービスポリシー名を入力します。（最大：32 文字）
バージョン	TLS のバージョン（**TLS1.0**/**TLS1.1**/**TLS1.2**）を選択します。
セッションキャッシュタイムアウト	セッションキャッシュのタイムアウト値（秒）を入力します。（デフォルト：600、設定範囲：60 ～ 86400）
セキュアトラストポイント	セキュアトラストポイント名を入力します。（最大：32 文字）
暗号スイート	このプロファイルに関連付ける暗号スイートを選択します。

[**適用**] ボタン - エントリを追加します。
[**検索**] ボタン - 検索結果を表示します。
[**編集**] ボタン - エントリの設定を編集します。
[**削除**] ボタン - エントリを削除します。

10 OAM（Operations, Administration & Management）

10.1 ケーブル診断

このウィンドウを用いて、指定したポートのケーブル診断テストを開始し、結果を表示します。ケーブル診断を実施する際は管理者（特権レベル 15）でログインが必要となります。

[OAM] > [ケーブル診断] をクリックして、以下のウィンドウを表示します。

図 10-1 ケーブル診断

設定パラメータ （[ケーブル診断] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[テスト] ボタン - ケーブル診断テストを開始します。
[全クリア] ボタン - すべてのケーブル診断結果をクリアします。
[クリア] ボタン - ケーブル診断結果をクリアします。

10.2 DDM（Digital Diagnostic Monitoring）

10.2.1 DDM 設定

このウィンドウを用いて、DDM 機能に関連付けられているグローバル設定および指定したポートの DDM シャットダウンの設定を行い、設定値を表示します。

[DDM] > [DDM 設定] をクリックして、以下のウィンドウを表示します。

図 10-2 DDM 設定

設定パラメータ （[DDM グローバル設定] セクション）

パラメータ	概要
トランシーバモニタリングトラップアラーム	トランシーバモニタリングアラームトラップ送信の状態（**有効** / **無効**）を選択します。
トランシーバモニタリングトラップワーニング	トランシーバモニタリングワーニングトラップ送信の状態（**有効** / **無効**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[DDM シャットダウン設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの DDM の状態（**Enabled**/**Disabled**）を選択します。
シャットダウン	シャットダウン動作を選択します。 • **Alarm** - 設定されているアラーム閾値範囲を超えた場合にポートをシャットダウンします。 • **Warning** - 設定されているワーニング閾値範囲を超えた場合にポートをシャットダウンします。 • **None** - 閾値範囲を超えたかどうかに関係なく、ポートをシャットダウンしません。これはデフォルトオプションです。

[**適用**] ボタン - 設定内容を反映します。

10.2.2 DDM 温度閾値設定

このウィンドウを用いて、指定したポートの DDM 温度閾値の設定を行い、設定値を表示します。

[DDM] > [DDM 温度閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-3 DDM 温度閾値設定

設定パラメータ （[DDM 温度閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	温度閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
値	閾値（摂氏）を入力します。（設定範囲：-128-127.996）

[**適用**] ボタン - 設定内容を反映します。

10.2.3 DDM 電圧閾値設定

このウィンドウを用いて、指定したポートの DDM 電圧閾値の設定を行い、設定値を表示します。

[DDM] > [DDM 電圧閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-4 DDM 電圧閾値設定

設定パラメータ （[DDM 電圧閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	電圧閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
値	閾値（V）を入力します。（設定範囲：0-6.55）

[**適用**] ボタン - 設定内容を反映します。

10.2.4 DDM バイアス電流閾値設定

このウィンドウを用いて、指定したポートの DDM バイアス電流閾値の設定を行い、設定値を表示します。

[DDM] > [DDM バイアス電流閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-5 DDM バイアス電流閾値設定

設定パラメータ （[DDM バイアス電流閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	バイアス電流閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
値	閾値（mA）を入力します。（設定範囲：0-131）

[**適用**] ボタン - 設定内容を反映します。

10.2.5 DDM 送信パワー閾値設定

このウィンドウを用いて、指定したポートの DDM 送信パワー閾値の設定を行い、設定値を表示します。

[DDM] > [DDM 送信パワー閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-6 DDM 送信パワー閾値設定

設定パラメータ （[DDM 送信パワー閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	送信パワー閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
パワー単位	電力単位（**mW**/**dBm**）を選択します。
値	閾値（mW/dBm）を入力します。 • パワー単位が mW の場合 - （設定範囲：0-6.5535） • パワー単位が dBm の場合 - （設定範囲：-40-8.1647）

[**適用**] ボタン - 設定内容を反映します。

10.2.6 DDM 受信パワー閾値設定

このウィンドウを用いて、指定したポートの DDM 受信パワー閾値の設定を行い、設定値を表示します。

[DDM] > [DDM 受信パワー閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-7 DDM 受信パワー閾値設定

設定パラメータ （[DDM 受信パワー閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	受信パワー閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
パワー単位	電力単位（**mW**/**dBm**）を選択します。
値	閾値（mW/dBm）を入力します。 • パワー単位が mW の場合 - （設定範囲：0-6.5535） • パワー単位が dBm の場合 - （設定範囲：-40-8.1647）

[**適用**] ボタン - 設定内容を反映します。

10.2.7 DDM 状態テーブル

このウィンドウを用いて、DDM 状態テーブルと情報を表示します。

[DDM] > [DDM 状態テーブル] をクリックして、以下のウィンドウを表示します。

図 10-8 DDM 状態テーブル

11 モニタリング

11.1 使用率

11.1.1 ポート使用率

このウィンドウを用いて、ポート使用率テーブルと情報を表示します。

[モニタリング] > [使用率] > [ポート使用率] をクリックして、以下のウィンドウを表示します。

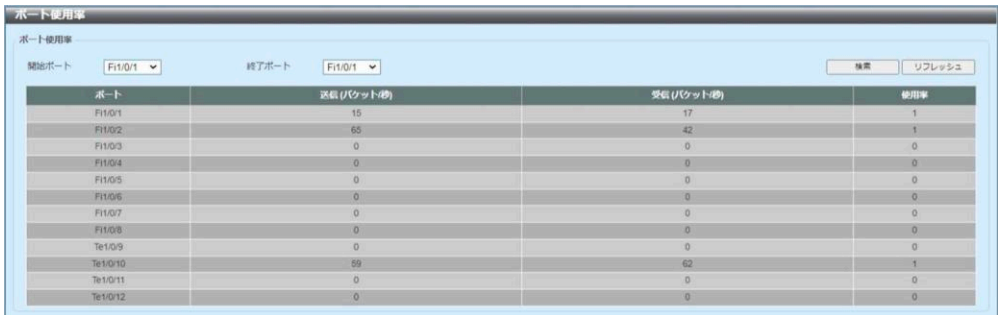


図 11-1 ポート使用率

設定パラメータ （[ポート使用率] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[リフレッシュ] ボタン - テーブルに表示されている情報をリフレッシュします。

11.2 統計

11.2.1 ポート

このウィンドウを用いて、ポートの受信 / 送信統計と情報を表示します。

[モニタリング] > [統計] > [ポート] をクリックして、以下のウィンドウを表示します。

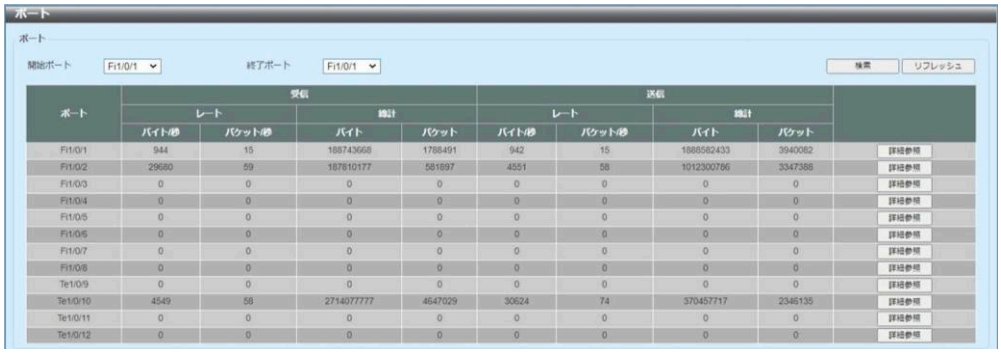


図 11-2 ポート

設定パラメータ （[ポート] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**リフレッシュ**] ボタン - テーブルに表示されている情報をリフレッシュします。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

11.2.2 インタフェースカウンタ

このウィンドウを用いて、インタフェースカウンタ統計と情報を表示します。

[モニタリング] > [統計] > [インタフェースカウンタ] をクリックして、以下のウィンドウを表示します。

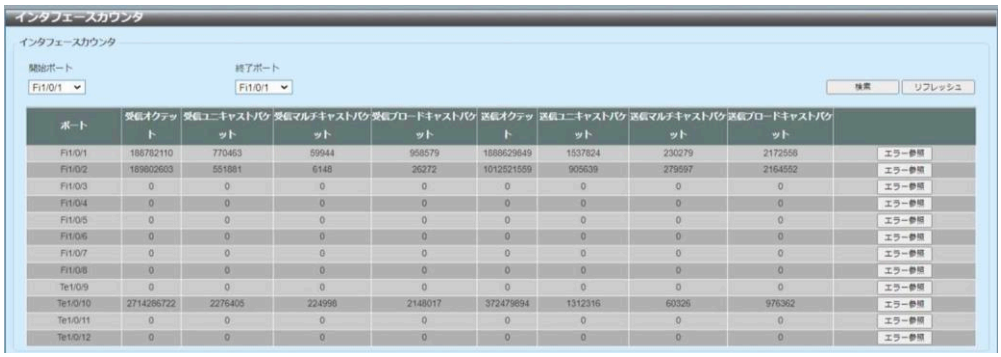


図 11-3 インタフェースカウンタ

設定パラメータ （[インタフェースカウンタ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**リフレッシュ**] ボタン - テーブルに表示されている情報をリフレッシュします。
[**エラー参照**] ボタン - 詳細エラー情報を表示します。

11.2.3 カウンタ

このウィンドウを用いて、指定したポートのリンクチェンジカウンタを表示およびクリアします。

[モニタリング] > [統計] > [カウンタ] をクリックして、以下のウィンドウを表示します。

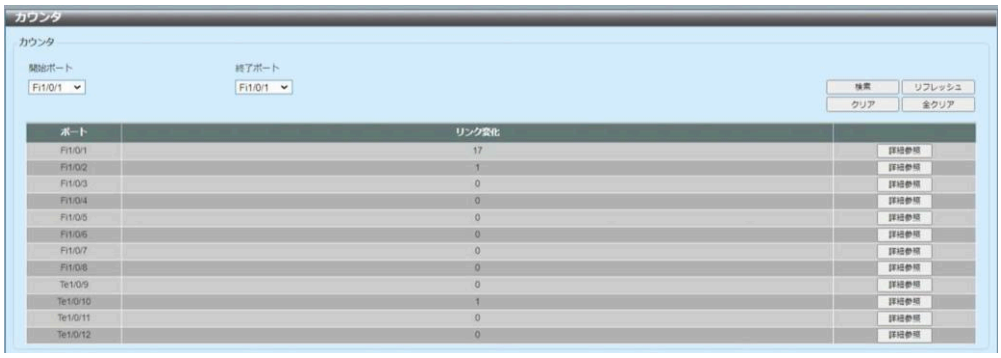


図 11-4 カウンタ

設定パラメータ （[カウンタ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**リフレッシュ**] ボタン - テーブルに表示されている情報をリフレッシュします。
[**クリア**] ボタン - リンクチェンジカウンタ情報をクリアします。
[**全クリア**] ボタン - すべてのリンクチェンジカウンタ情報をクリアします。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

11.3 ミラー設定

このウィンドウを用いて、ポートミラーの設定を行い、設定値を表示します。

[モニタリング] > [ミラー設定] をクリックして、以下のウィンドウを表示します。

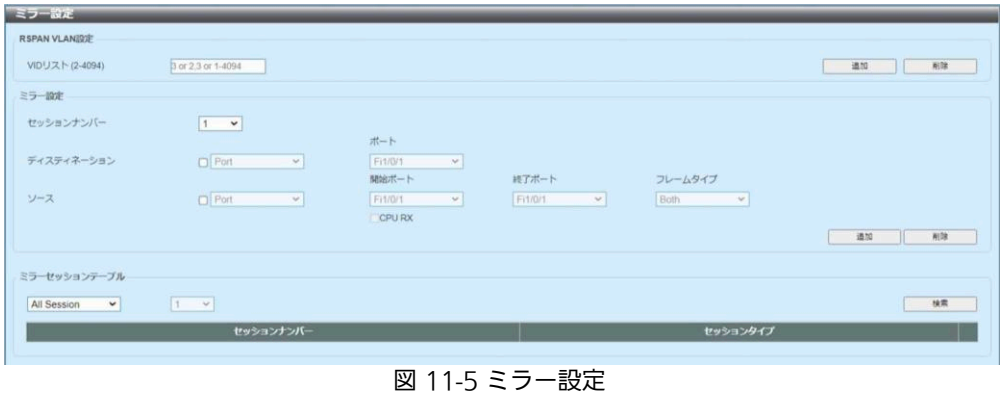


図 11-5 ミラー設定

設定パラメータ （[RSPAN VLAN 設定] セクション）

パラメータ	概要
VID リスト	使用する RSPAN VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[ミラー設定] セクション）

パラメータ	概要
セッションナンバー	ミラーセッションナンバー（**1 ～ 4**）を選択します。
ディスティネーション	ポートミラーエントリのディスティネーション設定を選択および設定します。 • **Port** - ディスティネーションポート番号を選択します。 • **Remote VLAN** - リモート VLAN ID を入力します。
ソース	ポートミラーエントリのソース設定を選択および設定します。 • **Port** - [**開始ポート**]、[**終了ポート**]、[**フレームタイプ**] を選択します。 • **ACL** - ACL 名を入力します。（最大：32 文字） • **Remote VLAN** - リモート VLAN ID を入力します。
フレームタイプ	([ソース] パラメータで [Port] 選択時に設定可) フレームタイプを選択します。 • **Both** - 受信方向と送信方向の両方のトラフィックがミラーリングされます。 • **RX** - 受信方向のみのトラフィックがミラーリングされます。 • **TX** - 送信方向のみのトラフィックがミラーリングされます。 • **CPU RX** - CPU RX トラフィックをモニタリングします。

[**適用**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。

設定パラメータ （[ミラーセッションテーブル] セクション）

パラメータ	概要
セッションタイプ	表示する情報のミラーセッションタイプ（**All Session**/**Session Number**/**Remote Session**/**Local Session**）を選択します。 **[Session Number]** を選択した場合は、ドロップダウンからセッションナンバーを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

11.4 デバイス

このウィンドウを用いて、スイッチの現在の温度測定値、ファン状態、および電源モジュール状態を表示します。

[モニタリング] > [デバイス] をクリックして、以下のウィンドウを表示します。

図 11-6 デバイス

11.5 sFlow

sFlow はスイッチネットワークを流れるトラフィックフローをモニタする機能で、sFlow エージェント（スイッチ等のネットワーク装置）が、フローサンプル（指定レートの頻度で収集したパケット情報）とカウンタサンプル（指定周期で収集した統計情報）を sFlow データグラムとして sFlow コレクタに送信し、sFlow コレクタにてネットワークのトラフィック特性を分析します。
本装置ではイーサネット物理インターフェース（ポート）を収集対象としており、sFlow version5 仕様準拠で実装しています。

11.5.1 sFlow グローバル設定

このウィンドウを用いて、sFlow 機能のグローバルな（装置単位）設定を行い、設定値と情報を表示します。

[モニタリング] > [sFlow] > [sFlow グローバル設定] をクリックして、以下のウィンドウを表示します

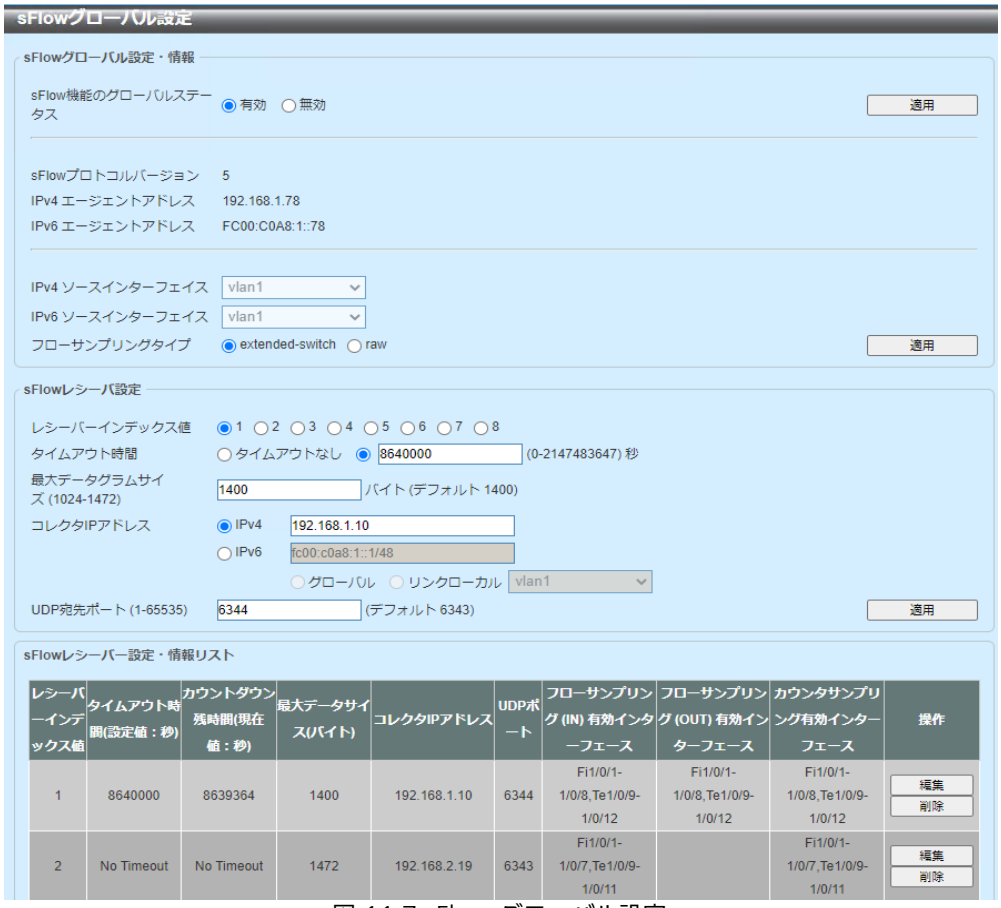


図 11-7 sFlow グローバル設定

設定パラメータ （[sFlow グローバル設定・情報] セクション）

パラメータ	概要
sFlow 機能のグローバルステータス	**有効 / 無効**：ラジオボタン（択一）。 本装置の sFlow 機能が有効化 / 無効化されていることを示します。（デフォルト：無効） **有効 / 無効**ボタンを選択し、[**適用**] ボタンをクリックして、本装置の sFlow 機能を有効化 / 無効化します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[sFlow グローバル設定・情報] セクション）

パラメータ	概要
sFlow プロトコルバージョン	5（固定値）
IPv4 エージェントアドレス	コレクタへの sFlow IPv4 通信で送信元アドレスとして使用される、送信元インタフェースの IPv4 アドレスです。
IPv6 エージェントアドレス	コレクタへの sFlow IPv6 通信で送信元アドレスとして使用される、送信元インタフェースの IPv6 アドレスです。
IPv4 ソースインターフェース	**IPv4 送信元インターフェース ID**：プルダウンリスト。 インターフェース ID の選択後、[**適用**] ボタンをクリックして、IPv4 送信元インターフェースを指定します。 デフォルト：コレクタ宛 IPv4 通信の送信インターフェースが送信元インターフェースとして使用されます。
IPv6 ソースインターフェース	**IPv6 送信元インターフェース ID**：プルダウンリスト。 インターフェース ID の選択後、[**適用**] ボタンをクリックして、IPv6 送信元インターフェースを指定します。 デフォルト：コレクタ宛 IPv6 通信の送信インターフェースが送信元インターフェースとして使用されます。

パラメータ	概要
フローサンプリングタイプ	**extended-switch/raw**：ラジオボタン（択一）。 **extended-switch/raw** ボタンを選択し、[**適用**] ボタンをクリックして、本装置のフローサンプリングに適用されるフローサンプリングタイプを指定します。 **extended-switch**：フローサンプルの構成要素として、基本構成要素であるサンプルヘッダーの他に、拡張スイッチ情報を付加します。（デフォルト） **raw**：フローサンプルの構成要素を基本構成要素であるサンプルヘッダーのみとします。フローサンプルパケットはイーサネットフレーム（プリアンブル、インターフェースギャップ、FCS 除く）であり、その先頭から指定されたバイト数（最大ヘッダーサイズ）が抜き出され、サンプルヘッダーデータとなります。 （参考）拡張スイッチ情報 • **Src VLAN**（オクテット数：4）- 受信 VLAN ID (802.1Q tag) • **Src Priority**（オクテット数：4）- 受信優先度（802.1p） • **Dst VLAN**（オクテット数：4）- 送信 VLAN ID（802.1Q tag） • **Dst Priority**（オクテット数：4）- 送信優先度（802.1p） 拡張スイッチ情報の詳細は、MXG-ML8THPoE++ CLI リファレンス 6.3.5 の使用ガイドラインを参照して下さい。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[sFlow レシーバ設定] セクション）

パラメータ	概要
レシーバーインデックス値	**1/2/3/4/5/6/7/8**：ラジオボタン（択一）。 レシーバーインデックス値を指定します。 本装置では最大 8 台のコレクタに sFlow データグラムの送信が可能で、コレクタ毎にレシーバー設定を行います。各レシーバーはインデックス値（1 ～ 8）で識別します。
タイムアウト時間	**タイムアウトなし / 時間**：ラジオボタン（択一）。 **タイムアウトなし**：レシーバーはタイムアウトせず、動作を継続します。（デフォルト） 時間：入力フィールド。レシーバー動作タイマー値（秒）を指定します（範囲：0 ～ 2147483647（=2^{31}-1））。 タイマーのカウントダウンはレシーバー設定適用時に開始し、タイマーが期限切れ（0）になった時点でレシーバー動作が停止します。期限切れ後、レシーバー動作を再始動したい場合は、タイマー値を再設定します。タイマー値として、0 を指定した場合は、レシーバーは動作を停止します。

パラメータ	概要
最大データグラムサイズ	**データグラムサイズ**：入力フィールド。 コレクタに送信する sFlow データグラム（UDP ペイロード部分に相当）の最大サイズ（バイト）を指定します（範囲：1024 ～ 1472（IPv4 通信時）、1024 ～ 1452（IPv6 通信時））。（デフォルト：1400）
コレクタ IP アドレス	**IPv4/IPv6**：ラジオボタン（択一）。 **IPv4**：入力フィールド。sFlow データグラム送信先である sFlow コレクタの IPv4 アドレス値を指定します。IPv4 UDP 通信で送信されます。もし、0.0.0.0 が指定された場合は、どのコレクタにも送信しません。 **IPv6**：入力フィールド、及び、グローバル / リンクローカル：ラジオボタン（択一）。 入力フィールドでは sFlow データグラム送信先である sFlow コレクタの IPv6 アドレス値を指定します。IPv6 UDP 通信で送信されます。もし、:: が指定された場合は、どのコレクタにも送信しません。ラジオボタンでは、アドレス種別を指定します。リンクローカルを選択した場合は、更に送信インターフェース ID をプルダウンリストから選択します。
UDP 宛先ポート	**UDP ポート番号**：入力フィールド。（範囲：1 ～ 65535）。（デフォルト：6343） コレクタとの UDP 通信ポート番号を指定します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[sFlow レシーバー設定・情報リスト] セクション）

パラメータ	概要
レシーバーインデックス	**1 ～ 8**：レシーバーインデックス値。
タイムアウト時間（設定値：秒）	**No Timeout**：レシーバーはタイムアウトせず、動作を継続します。 **時間**（秒）：レシーバー動作タイマー設定値（範囲：0 ～ 2147483647（=2^{31}-1））。
カウントダウン残時間（現在値：秒）	**No Timeout**：レシーバーはタイムアウトせず、動作を継続します。 **時間**（秒）：レシーバー動作タイマー残時間（範囲：0 ～ 2147483647（=2^{31}-1））。
コレクタ IP アドレス	**IPv4 アドレス**：sFlow データグラム送信先である sFlow コレクタの IPv4 アドレス値。 **IPv6 アドレス**：sFlow データグラム送信先である sFlow コレクタの IPv6 アドレス値。リンクローカルアドレスの場合は、末尾に送信インターフェース ID が %（デリミタ）を介して付与されます。

パラメータ	概要
UDP ポート	**UDP ポート番号**：コレクタとの UDP 通信ポート番号。 （範囲：1 ～ 65535）
フローサンプリング（IN）有効インターフェース	**インターフェース ID リスト**：当該レシーバー用に受信側のフローサンプリングが有効化されたインターフェース（イーサネット物理ポート）の ID リスト。
フローサンプリング（OUT）有効インターフェース	**インターフェース ID リスト**：当該レシーバー用に送信側のフローサンプリングが有効化されたインターフェース（イーサネット物理ポート）の ID リスト。
カウンタサンプリング有効インターフェース	**インターフェース ID リスト**：当該レシーバー用にカウンタサンプリングが有効化されたインターフェース（イーサネット物理ポート）の ID リスト。
操作	[**編集**] ボタンのクリックにより、当該行のレシーバー設定が［sFlow レシーバー設定］セクションに表示されるので、［sFlow レシーバー設定］セクションにてレシーバー設定の再編集を行います。 [**削除**] ボタンのクリックにより、当該行のレシーバー設定を削除します。

11.5.2 sFlow フローサンプリング設定

このウィンドウを用いて、sFlow フローサンプリング設定を行い、設定値と情報を表示します。

[モニタリング] > [sFlow] > [sFlow フローサンプリング設定] をクリックして、以下のウィンドウを表示します。

図 11-8 sFlow フローサンプリング設定

設定パラメータ （[sFlow フローサンプリング設定] セクション）

パラメータ	概要
設定インターフェース範囲 From/To	**インターフェース ID（From, To）**：プルダウンリスト。フローサンプリングを有効化、及び、設定するインターフェース（イーサネット物理ポート）の範囲を **From, To** で指定します。
レシーバーインデックスリスト	**1,2,3,4,5,6,7,8**：チェックボックス（複数選択可）。 フローサンプリングで得られたフローサンプルを送信するコレクタに対応するレシーバーのインデックスを指定します。
IN/OUT	**IN/OUT**：ラジオボタン（択一）。 **IN**：インターフェースの受信パケットをフローサンプリングします。（デフォルト） **OUT**：インターフェースの送信パケットをフローサンプリングします。

パラメータ	概要
サンプリングレート	**サンプリングレート**：入力フィールド。 フローサンプリングの平均サンプリングレートを指定します（範囲：1024 ～ 16777216（=2^{24}））。 （デフォルト：1048576（=2^{20}））。 実際のサンプリングレートは 1/RATE で算出され、サンプリング対象の受信 / 送信パケットがフローサンプルパケットとして選定される確率となります。受信 / 送信された RATE 数個のパケットに対して、1 個のパケットがフローサンプルパケットとして選定される確率に相当します。どのパケットがフローサンプルパケットとして選定されるかはランダムに決定されます。
最大 ヘッダーサイズ	**ヘッダーサイズ**：入力フィールド。 フローサンプルパケットからフローサンプルとして抜き出す最大ヘッダーサイズ（バイト）を指定します（範囲：64 ～ 256）。（デフォルト：128） 本装置では、フローサンプルパケットはイーサネットフレーム（プリアンブル、インターフェースギャップ、FCS 除く）であり、その先頭から指定された最大ヘッダーサイズが抜き出され、フローサンプルの基本構成要素であるサンプルヘッダーデータとなります。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[sFlow フローサンプリング設定・情報リスト] セクション）

パラメータ	概要
合計エントリ数	**設定数**：現在のフローサンプリング設定数（= 設定行数）。
☑（チェックボックス）	**チェックボックス**（複数行選択可）：[**削除**] ボタンのクリックにより、チェックボックスで選択されている行のフローサンプリング設定を一括で削除します。
インターフェース	**インターフェース ID**：フローサンプリング対象のインターフェース（イーサネット物理ポート）。
IfIndex	**IfIndex 値**：上記インターフェースの IfIndex 値（範囲 1 ～ 16777215（=2^{24}-1））。
IN/OUT	**IN**：フローサンプリング対象が受信パケット。 **OUT**：フローサンプリング対象が送信パケット。
レシーバーリスト	**レシーバーインデックスリスト**：フローサンプリングで得られたフローサンプルを送信するコレクタに対応するレシーバーのインデックスリスト。（インデックス値範囲：1 ～ 8）
サンプリングレート	**サンプリングレート値**：フローサンプリングの平均サンプリングレート（ 範囲：1/1024 ～ 1/16777216（=2^{24}））。

パラメータ	概要
最大ヘッダーサイズ（バイト）	**ヘッダーサイズ値**：フローサンプルパケットからフローサンプルとして抜き出す最大ヘッダーサイズ（バイト） （範囲：64 ～ 256）。
操作	[**編集**] ボタンのクリックにより、当該行のフローサンプリング設定が［sFlow フローサンプリング設定］セクションに表示されるので、［sFlow フローサンプリング設定］セクションにてフローサンプリング設定の再編集を行います。

11.5.3 sFlow カウンタサンプリング設定

このウィンドウを用いて、sFlow カウンタサンプリング設定を行い、設定値と情報を表示します。

[モニタリング] > [sFlow] > [sFlow カウンタサンプリング設定] をクリックして、以下のウィンドウを表示します。

図 11-9 sFloe カウンタサンプリング設定

設定パラメータ （[sFlow カウンタサンプリング設定] セクション）

パラメータ	概要
設定インターフェース範囲 From/To	**インターフェース ID（From, To）**：プルダウンリスト。カウンタサンプリングを有効化、及び、設定するインターフェース（イーサネット物理ポート）の範囲を **From, To** で指定します。
レシーバーインデックスリスト	**1,2,3,4,5,6,7,8**：チェックボックス（複数選択可）。カウンタサンプリングで得られたカウンタサンプルを送信するコレクタに対応するレシーバーのインデックスを指定します。
サンプリング周期	**サンプリング周期**：入力フィールド。カウンタサンプリング周期（秒）を指定します（設定範囲：15 ～ 280）。（デフォルト：60） 本周期でインターフェースの 2 種類のカウンタ情報（汎用インターフェースカウンタ、イーサネットインターフェースカウンタ）をカウンタサンプルとして採取します。

[**適用**] ボタン - 設定内容を更新します。

設定パラメータ （[sFlow カウンタサンプリング設定・情報リスト] セクション）

パラメータ	概要
合計エントリ数	**設定数**：現在のカウンタサンプリング設定数（= 設定行数）。
☑（チェックボックス）	**チェックボックス**（複数行選択可）：[**削除**] ボタンのクリックにより、チェックボックスで選択されている行のカウンタサンプリング設定を一括で削除します。
インターフェース	**インターフェース ID**：カウンタサンプリング対象のインターフェース（イーサネット物理ポート）。
IfIndex	**IfIndex 値**：上記インターフェースの IfIndex 値（範囲 1 ～ 16777215（=2^{24}-1））。
レシーバーリスト	**レシーバーインデックスリスト**：カウンタサンプリングで得られたカウンタサンプルを送信するコレクタに対応するレシーバーのインデックスリスト。（インデックス値範囲：1 ～ 8）
サンプリング周期（秒）	**サンプリング周期**：カウンタサンプリング周期（秒）（設定範囲：15 ～ 280）。
操作	[**編集**] ボタンのクリックにより、当該行のカウンタサンプリング設定が［sFlow カウンタサンプリング設定］セクションに表示されるので、［sFlow カウンタサンプリング設定］セクションにてカウンタサンプリング設定の再編集を行います。

（参考）汎用インターフェースカウンタ

カウンタ名	オクテット数	説明
ifIndex	4	インターフェースインデックス値（本装置では、範囲：1 ～ 16777215（=2^{24}-1））
ifType	4	IANAifType: 固定値 6（ethernetCsmacd）
ifSpeed	8	回線スピード（bit/s）（64bit）
ifDirection	4	Unknown=1, full-duplex=1, half-duplex=2
ifStatus	4	bit 0 = ifAdminStatus (0 = down, 1 = up), bit 1 = ifOperStatus (0 = down, 1 = up)
ifInOctets	8	受信オクテット数（64bit）
ifInUcastPkts	4	受信ユニキャストパケット数
ifInMulticastPkts	4	受信マルチキャストパケット数
ifInBroadcastPkts	4	受信ブロードキャストパケット数
ifInDiscards	4	受信廃棄パケット数
ifInErrors	4	受信エラーパケット数
ifInUnknownProtos	4	受信不明プロトコルパケット数
ifOutOctets	8	送信オクテット数（64bit）
ifOutUcastPkts	4	送信ユニキャストパケット数
ifOutMulticastPkts	4	送信マルチキャストパケット数
ifOutBroadcastPkts	4	送信ブロードキャストパケット数
ifOutDiscards	4	送信廃棄パケット数
ifOutErrors	4	送信エラーパケット数

カウンタ名	オクテット数	説明
ifPromiscuousMode	4	固定値 2（本装置宛のパケット / フレームのみを受け付ける）

（参考）イーサネットインターフェースカウンタ

カウンタ名	オクテット数	説明
dot3StatsAlignmentErrors	4	受信フレームアラインメントエラー数
dot3StatsFCSErrors	4	受信フレーム FCS エラー数
dot3StatsSingleCollisionFrames	4	単一衝突送信フレーム数（全二重では加算されません）
dot3StatsMultipleCollisionFrames	4	複数衝突送信フレーム数（全二重では加算されません）
dot3StatsSQETestErrors	4	SQE テストエラー数（10M 超、全二重では加算されません）
dot3StatsDeferredTransmissions	4	（メディアビジーによる）送信遅延回数（全二重では加算されません）
dot3StatsLateCollisions	4	送信時遅延衝突回数（全二重では加算されません）
dot3StatsExcessiveCollisions	4	衝突回数超過送信失敗フレーム数（全二重では加算されません）
dot3StatsInternalMacTransmitErrors	4	内部 MAC サブレイヤ送信エラーによる送信失敗フレーム数
dot3StatsCarrierSenseErrors	4	送信中キャリアセンスエラー数（全二重では加算されません）
dot3StatsFrameTooLongs	4	フレーム長超過受信エラー数
dot3StatsInternalMacReceiveErrors	4	内部 MAC サブレイヤ受信エラーによる受信失敗フレーム数
dot3StatsSymbolErrors	4	受信時シンボルエラー数

11.5.4 sFlow 統計

このウィンドウを用いて、sFlow 統計情報の表示とクリアを行います。

[モニタリング] > [sFlow] > [sFlow 統計] をクリックして、以下のウィンドウを表示します。

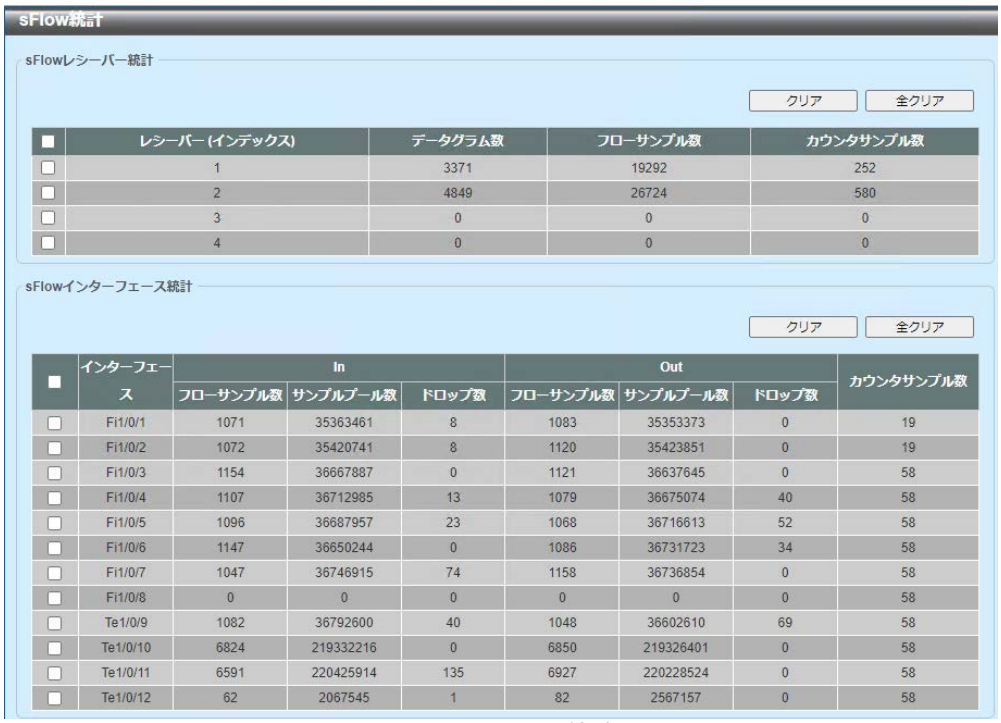


図 11-10 sFlow 統計

設定パラメータ （[sFlow レシーバー統計] セクション）

パラメータ	概要
☑（チェックボックス）	チェックボックス（複数行選択可）: [クリア] ボタンのクリックにより、チェックボックスで選択されている行の sFlow レシーバー統計情報を一括でクリアします。
レシーバー（インデックス）	**1 ～ 8**：レシーバーインデックス値。
データグラム数	レシーバーに対応するコレクタに送信された総 sFlow データグラム数。（32bit）
フローサンプル数	レシーバーに対応するコレクタに送信された総 sFlow フローサンプル数。（32bit）
カウンタサンプル数	レシーバーに対応するコレクタに送信された総 sFlow カウンタサンプル数。（32bit）

[**全クリア**] ボタン - sFlow レシーバー統計情報を全てクリアします。

設定パラメータ （[sFlow インターフェース統計] セクション）

パラメータ		概要
☑（チェックボックス）		チェックボックス（複数行選択可）: [クリア] ボタンのクリックにより、チェックボックスで選択されている行の sFlow レシーバー統計情報を一括でクリアします。
インターフェース		インターフェース ID：フローサンプリング、あるいは、カウンタサンプリングが有効化されたインターフェースの ID。
IN	フローサンプル数	有効化されたインターフェースの受信側フローサンプリングで得られた総フローサンプル数。（32bit）
	サンプルプール数	有効化されたインターフェースの受信側フローサンプリング実施中の総受信パケット数。（32bit）
	ドロップ数	有効化されたインターフェースの受信側フローサンプリングで得られたフローサンプルが（送信できずに）廃棄された合計回数。（32bit）
OUT	フローサンプル数	有効化されたインターフェースの送信側フローサンプリングで得られた総フローサンプル数。（32bit）
	サンプルプール数	有効化されたインターフェースの送信側フローサンプリング実施中の総送信パケット数。（32bit）
	ドロップ数	有効化されたインターフェースの送信側フローサンプリングで得られたフローサンプルが（送信できずに）廃棄された合計回数。（32bit）
カウンタサンプル数		有効化されたインターフェースのカウンタサンプリングで得られた総カウンタサンプル数。（32bit）

[全クリア] ボタン - sFlow インターフェース統計情報を全てクリアします。

12 ECO モード

12.1 省電力

このウィンドウを用いて、指定したポートの省電力の設定を行い、設定値を表示します。

[ECO モード] > [省電力] をクリックして、以下のウィンドウを表示します。

図 12-1 省電力

設定パラメータ （[省電力設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
省電力モード	指定したポートで使用する省電力モードを選択します。 • **Disabled** - 省電力機能を無効にします。 • **Full** - 省電力機能の能力を最大限に使用します。 • **Half** - 省電力機能の能力を半分だけ使用します。これは、通常は、まったく使用しない場合と最大限に使用する場合の間であればすべて該当します。

[**適用**] ボタン - 設定内容を反映します。

12.2 EEE（Energy Efficient Ethernet）

このウィンドウを用いて、指定したポートの EEE の設定を行い、設定値を表示します。

[ECO モード] > [EEE] をクリックして、以下のウィンドウを表示します。

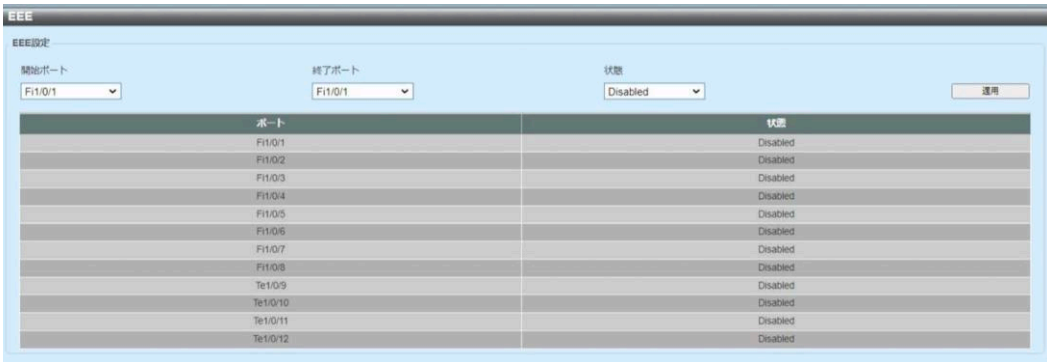


図 12-2 EEE

設定パラメータ （[EEE 設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	EEE の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

13 ツールバー

13.1 保存

13.1.1 コンフィグ保存

このウィンドウを用いて、実行中のコンフィグレーションをスタートアップコンフィグレーションとして保存します。これにより、電源故障時にコンフィグレーションが失われないようにします。

ツールバー >[保存] > [コンフィグ保存] をクリックして、以下のウィンドウを表示します。

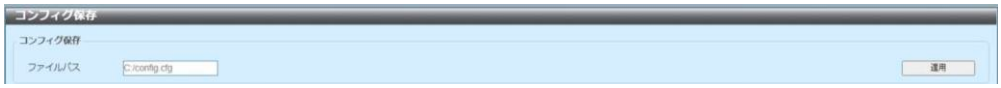


図 13-1 コンフィグ保存

設定パラメータ （[コンフィグ保存] セクション）

パラメータ	概要
ファイルパス	ファイル名とパスを表示された入力フィールドに入力します。

[**適用**] ボタン - コンフィグレーションを保存します。

13.2 ツール

13.2.1 ファームウェアアップグレード & バックアップ

13.2.1.1 HTTP サーバからファームウェアアップグレード

このウィンドウを用いて、ローカル PC から HTTP を使用してスイッチのファームウェアをアップグレードします。

ツールバー >[ツール] > [ファームウェアアップグレード & バックアップ] > [HTTP サーバからファームウェアアップグレード] をクリックして、以下のウィンドウを表示します。

図 13-2 HTTP サーバからファームウェアアップグレード

設定パラメータ

パラメータ	概要
ソースファイル	**[ファイルの選択]** ボタンをクリックして、このアップグレードで使用するファームウェアファイル（ローカル PC 上）がある場所に移動します。
ディスティネーションファイル	新しいファームウェアを保存するスイッチ上のディスティネーションパスと場所を入力します。（最大：64 文字）

[アップグレード] ボタン - アップグレードを開始します。

13.2.1.2 TFTP サーバからファームウェアアップグレード

このウィンドウを用いて、TFTP サーバからスイッチのファームウェアをアップグレードします。

ツールバー >[ツール] > [ファームウェアアップグレード & バックアップ] > [TFTP サーバからファームウェアアップグレード] をクリックして、以下のウィンドウを表示します。

図 13-3 TFTP サーバからファームウェアアップグレード

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	TFTP サーバにあるファームウェアファイルのソースファイル名とパスを入力します。(最大 : 64 文字)
ディスティネーションファイル	新しいファームウェアを保存するスイッチ上のディスティネーションパスと場所を入力します。(最大 : 64 文字)

[アップグレード] ボタン - アップグレードを開始します。

13.2.1.3 RCP サーバからファームウェアアップグレード

このウィンドウを用いて、RCP サーバからスイッチのファームウェアをアップグレードします。

ツールバー >[ツール] > [ファームウェアアップグレード & バックアップ] > [RCP サーバからファームウェアアップグレード] をクリックして、以下のウィンドウを表示します。

図 13-4 RCP サーバからファームウェアアップグレード

設定パラメータ

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。(最大 : 32 文字)
ソースファイル	RCP サーバにあるファームウェアファイルのソースファイル名とパスを入力します。(最大 : 64 文字)
ディスティネーションファイル	新しいファームウェアを保存するスイッチ上のディスティネーションパスと場所を入力します。(最大 : 64 文字)

[アップグレード] ボタン - アップグレードを開始します。

13.2.1.4 HTTP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを HTTP を使用してローカル PC に保存します。

ツールバー >[ツール] > [ファームウェアアップグレード & バックアップ] > [HTTP サーバへファームウェアバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-5 HTTP サーバへファームウェアバックアップ

設定パラメータ

パラメータ	概要
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。(最大 : 64 文字)

[**バックアップ**] ボタン - バックアップを開始します。

13.2.1.5 TFTP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを TFTP サーバに保存します。

ツールバー >[ツール] > [ファームウェアアップグレード & バックアップ] > [TFTP サーバへファームウェアバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-6 TFTP サーバへファームウェアバックアップ

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。(最大：64 文字)
ディスティネーションファイル	TFTP サーバにバックアップするファームウェアファイルのディスティネーションファイル名とパスを入力します。(最大：64 文字)

[バックアップ] ボタン - バックアップを開始します。

13.2.1.6 RCP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを RCP サーバに保存します。

ツールバー >[ツール] > [ファームウェアアップグレード & バックアップ] > [RCP サーバへファームウェアバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-7 RCP サーバへファームウェアバックアップ

設定パラメータ

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。(最大 : 32 文字)
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。(最大 : 64 文字)
ディスティネーション ファイル	RCP サーバにバックアップするファームウェアファイルのディスティネーションファイル名とパスを入力します。(最大 : 64 文字)

[**バックアップ**]ボタン - バックアップを開始します。

13.2.2 コンフィグレーション復旧&バックアップ

13.2.2.1 HTTP サーバからコンフィグレーション復旧

このウィンドウを用いて、ローカル PC から HTTP を使用してスイッチにコンフィグレーションを復旧します。

ツールバー >[ツール] > [コンフィグレーション復旧&バックアップ] > [HTTP サーバからコンフィグレーション復旧] をクリックして、以下のウィンドウを表示します。

図 13-8 HTTP サーバからコンフィグレーション復旧

設定パラメータ

パラメータ	概要
ソースファイル	**[ファイルの選択]** ボタンをクリックして、この復旧で使用するコンフィグレーションファイル（ローカル PC 上）がある場所に移動します。
ディスティネーションファイル	コンフィグレーションファイルを保存するスイッチ上のディスティネーションパスと場所を入力します。（最大：64 文字） • **running-config** - スイッチ上の実行中のコンフィグレーションファイルを復旧して上書きします。 • **startup-config** - スイッチ上のスタートアップコンフィグレーションファイルを復旧して上書きします。
リプレイス	このオプションを選択した場合、スイッチ上のコンフィグレーションファイルをこのファイルでリプレイスします。

[リストア] ボタン - リストアを開始します。

13.2.2.2 TFTP サーバからコンフィグレーション復旧

このウィンドウを用いて、TFTP サーバからスイッチのコンフィグレーションを復旧します。

ツールバーで **[ツール] > [コンフィグレーション復旧&バックアップ] > [TFTP サーバからコンフィグレーション復旧]** をクリックして、以下のウィンドウを表示します。

図 13-9 TFTP サーバからコンフィグレーション復旧

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	TFTP サーバにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大 : 64 文字)
ディスティネーションファイル	コンフィグレーションファイルを保存するスイッチ上のディスティネーションパスと場所を入力します。(最大 : 64 文字) • **running-config** - スイッチ上の実行中のコンフィグレーションファイルを復旧して上書きします。 • **startup-config** - オプションを選択した場合、スイッチ上のスタートアップコンフィグレーションファイルを復旧して上書きします。
リプレイス	このオプションを選択した場合、スイッチ上のコンフィグレーションファイルをこのファイルでリプレイスします。

[リストア]ボタン - リストアを開始します。

13.2.2.3 RCP サーバからコンフィグレーション復旧

このウィンドウを用いて、RCP サーバからスイッチのコンフィグレーションを復旧します。

ツールバーで **[ツール] > [コンフィグレーション復旧&バックアップ] > [RCP サーバからコンフィグレーション復旧]** をクリックして、以下のウィンドウを表示します。

図 13-10 RCP サーバからコンフィグレーション復旧

設定パラメータ

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。(最大 : 32 文字)
ソースファイル	RCP サーバにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大 : 64 文字)
ディスティネーションファイル	コンフィグレーションファイルを保存するスイッチ上のディスティネーションパスと場所を入力します。(最大 : 64 文字) • **running-config** - スイッチ上の実行中のコンフィグレーションファイルを復旧して上書きします。 • **startup-config** - スイッチ上のスタートアップコンフィグレーションファイルを復旧して上書きします。
リプレイス	このオプションを選択した場合、スイッチ上のコンフィグレーションファイルをこのファイルでリプレイスします。

[**リストア**]ボタン - リストアを開始します。

13.2.2.4 HTTP サーバへコンフィグレーションをバックアップ

このウィンドウを用いて、スイッチのコンフィグレーションのバックアップコピーを HTTP を使用してローカル PC に保存します。

ツールバーで **[ツール] > [コンフィグレーション復旧&バックアップ] > [HTTP サーバへコンフィグレーションをバックアップ]** をクリックして、以下のウィンドウを表示します。

図 13-11 HTTP サーバへコンフィグレーションをバックアップ

設定パラメータ

パラメータ	概要
ソースファイル	スイッチにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大 : 64 文字) • **running-config** - スイッチから実行中のコンフィグレーションファイルをバックアップします。 • **startup-config** - スイッチからスタートアップコンフィグレーションファイルをバックアップします。

[**バックアップ**] ボタン - バックアップを開始します。

13.2.2.5 TFTP サーバへコンフィグレーションをバックアップ

このウィンドウを用いて、スイッチのコンフィグレーションのバックアップコピーを TFTP サーバに保存します。

ツールバーで **[ツール] > [コンフィグレーション復旧&バックアップ] > [TFTP サーバへコンフィグレーションをバックアップ]** をクリックして、以下のウィンドウを表示します。

図 13-12 TFTP サーバへコンフィグレーションをバックアップ

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	スイッチにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大 : 64 文字) • **running-config** - スイッチから実行中のコンフィグレーションファイルをバックアップします。 • **startup-config** - スイッチからスタートアップコンフィグレーションファイルをバックアップします。
ディスティネーションファイル	コンフィグレーションファイルを保存する TFTP サーバ上のディスティネーションパスと場所を入力します。 (最大 : 64 文字)

[バックアップ] ボタン - バックアップを開始します。

13.2.2.6 RCP サーバへコンフィグレーションをバックアップ

このウィンドウを用いて、スイッチのコンフィグレーションのバックアップコピーを RCP サーバに保存します。

ツールバーで **[ツール] > [コンフィグレーション復旧&バックアップ] > [RCP サーバへコンフィグレーションをバックアップ]** をクリックして、以下のウィンドウを表示します。

図 13-13 RCP サーバへコンフィグレーションをバックアップ

設定パラメータ

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。(最大 : 32 文字)
ソースファイル	スイッチにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大 : 64 文字) • **running-config** - スイッチから実行中のコンフィグレーションファイルをバックアップします。 • **startup-config** - スイッチからスタートアップコンフィグレーションファイルをバックアップします。
ディスティネーションファイル	コンフィグレーションファイルを保存する RCP サーバ上のディスティネーションパスと場所を入力します。 (最大 : 64 文字)

[**バックアップ**] ボタン - バックアップを開始します。

13.2.3 ログバックアップ

13.2.3.1 ログを HTTP サーバへバックアップ

このウィンドウを用いて、スイッチのシステムログまたは攻撃ログのコピーを HTTP を使用してローカル PC に保存します。

ツールバー >[ツール] > [ログバックアップ] > [ログを HTTP サーバへバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-14 ログを HTTP サーバへバックアップ

設定パラメータ

パラメータ	概要
ログタイプ	HTTP を使用してローカル PC にバックアップするログタイプを選択します。 • **システムログ** - システムログをバックアップします。 • **攻撃ログ** - 攻撃ログをバックアップします。

[**バックアップ**] ボタン - バックアップを開始します。

13.2.3.2 ログを TFTP サーバへバックアップ

このウィンドウを用いて、スイッチのシステムログまたは攻撃ログのコピーを TFTP サーバに保存します。

ツールバー >[ツール] > [ログバックアップ] > [ログを TFTP サーバへバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-15 ログを TFTP サーバへバックアップ

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ディスティネーションファイル	ログファイルを保存する TFTP サーバ上のディスティネーションパスと場所を入力します。(最大 : 64 文字)
ログタイプ	TFTP サーバにバックアップするログタイプを選択します。 • **システムログ** - システムログをバックアップします。 • **攻撃ログ** - 攻撃ログをバックアップします。

[**バックアップ**] ボタン - バックアップを開始します。

13.2.3.3 ログを RCP サーバへバックアップ

このウィンドウを用いて、スイッチのシステムログまたは攻撃ログのコピーを RCP サーバに保存します。

ツールバー >[ツール] > [ログバックアップ] > [ログを RCP サーバへバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-16 ログを RCP サーバへバックアップ

設定パラメータ

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。(最大 : 32 文字)
ディスティネーション ファイル	ログファイルを保存する RCP サーバ上のディスティネーションパスと場所を入力します。(最大 : 64 文字)
ログタイプ	RCP サーバにバックアップするログタイプを選択します。 • **システムログ** - システムログをバックアップします。 • **攻撃ログ** - 攻撃ログをバックアップします。

[**バックアップ**] ボタン - バックアップを開始します。

13.2.4 Ping

このウィンドウを用いて、ディスティネーション IPv4/IPv6 アドレスまたはドメイン名に Ping して、ネットワーク接続をテストします。Ping リクエストには、アクセスリストを適用できます。

ツールバー >[ツール] > [Ping] をクリックして、以下のウィンドウを表示します。

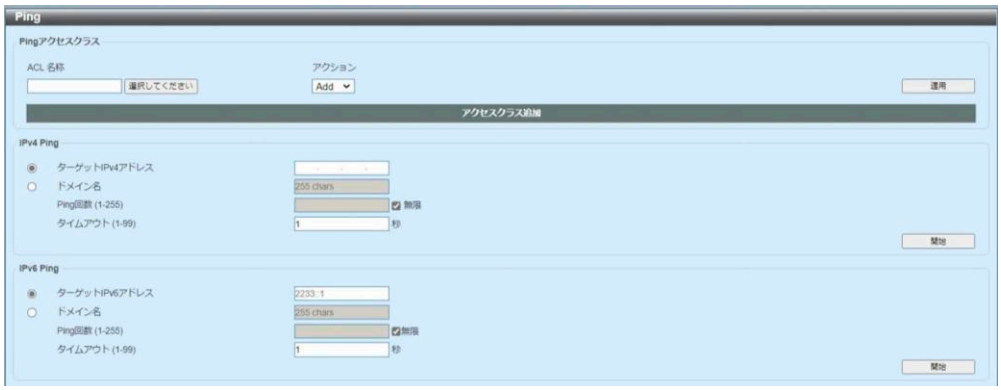


図 13-17 Ping

設定パラメータ （[Ping アクセスクラス] セクション）

パラメータ	概要
ACL 名称	使用する ACL の名前を入力します。（最大 : 32 文字） [**選択してください**] ボタンをクリックして、リストから既存の ACL を選択します。
アクション	実行するアクション（**Add**/**Clear**）を選択します。

[**適用**] ボタン - 選択したアクセスコントロールリストを使用します。

[IPv4 Ping] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ターゲット **IPv4** アドレス	ディスティネーション IPv4 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。これは 255 文字までです。
Ping 回数	このウィンドウで設定した IPv4 アドレスに Ping を試行する回数を入力します。範囲は 1 ～ 255 です。 **[無限]** チェックボックスをオンにした場合、プログラムを停止するまで、指定した IPv4 アドレスに ICMP Echo パケットを送信し続けます。
タイムアウト	Ping メッセージのタイムアウト時間を入力します。パケットがここで指定した時間内に IPv4 アドレスを検出できない場合、Ping パケットは廃棄されます。範囲は、1 ～ 99 秒です。

[開始] ボタンをクリックして、IPv4 Ping を開始します。

[IPv6 Ping] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ターゲット **IPv6** アドレス	ディスティネーション IPv6 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。これは 255 文字までです。
Ping 回数	このウィンドウで設定した IPv6 アドレスに Ping を試行する回数を入力します。範囲は 1 ～ 255 です。 **[無限]** チェックボックスをオンにした場合、プログラムを停止するまで、指定した IPv6 アドレスに ICMP Echo パケットを送信し続けます。
タイムアウト	Ping メッセージのタイムアウト時間を入力します。パケットがここで指定した時間内に IPv6 アドレスを検出できない場合、Ping パケットは廃棄されます。範囲は、1 ～ 99 秒です。

[開始] ボタンをクリックして、IPv6 Ping を開始します。

[IPv4 Ping] パラメータを選択および入力し、**[開始]** ボタンをクリックして、以下のウィンドウを表示します。
[Stop] ボタンをクリックして、Ping プロセスを停止します。
[戻る] ボタンをクリックして、前の [Ping] ウィンドウに戻ります。

13.2.5 トレースルート

このウィンドウを用いて、ディスティネーション IPv4/IPv6 アドレスまたはドメイン名へのルートをトレースして、ネットワーク接続をテストします。

ツールバー >[ツール] > [トレースルート] をクリックして、以下のウィンドウを表示します。

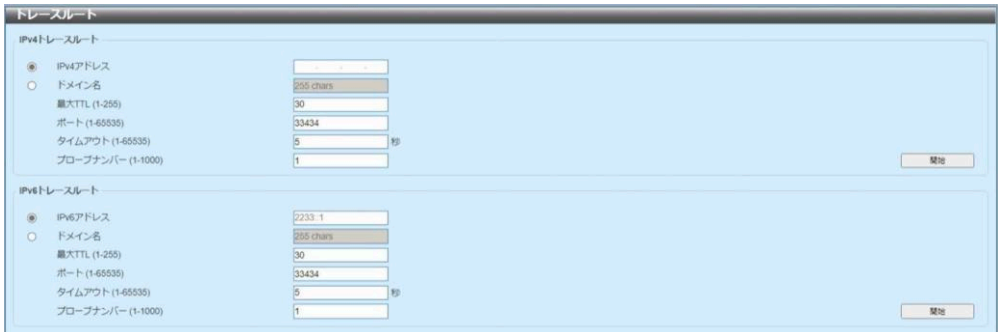


図 13-18 トレースルート

設定パラメータ （[IPv4 トレースルート] セクション）

パラメータ	概要
IPv4 アドレス	ディスティネーション IPv4 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。（最大：255 文字）
最大 TTL	トレースルートリクエストの TTL（Time-To-Live）の最大値を入力します。これは、トレースルートパケットが通過できるルータの最大数です。トレースルートオプションは、2 つの装置間のネットワークパスを探索するときに通過します。
ポート	ポート番号を入力します。
タイムアウト	リモート装置からの応答を待つ際のタイムアウト期間（秒）を入力します。（デフォルト：5）
プローブナンバー	プローブタイムの数を入力します。（デフォルト：1）

[**開始**] ボタン - IPv4 トレースルートを開始します。

設定パラメータ （[IPv6 トレースルート] セクション）

パラメータ	概要
IPv6 アドレス	ディスティネーション IPv6 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。（最大：255 文字）

パラメータ	概要
最大 TTL	トレースルートリクエストの TTL の最大値を入力します。これは、トレースルートパケットが通過できるルータの最大数です。トレースルートオプションは、2 つの装置間のネットワークパスを探索するときに通過します。
ポート	ポート番号を入力します。
タイムアウト	リモート装置からの応答を待つ際のタイムアウト期間（秒）を入力します。（デフォルト：5）
プローブナンバー	プローブタイムの数を入力します。（デフォルト：1）

[**開始**] ボタン - IPv6 トレースルートを開始します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

13.2.6 リセット

このウィンドウを用いて、スイッチのソフトウェアコンフィグレーションの工場出荷時の値へのリセットを開始します。

ツールバー >[ツール] > [リセット] をクリックして、以下のウィンドウを表示します。

図 13-19 リセット

設定パラメータ

パラメータ	概要
リセット	以下のいずれかのリセットオプションを選択します。 • **スイッチは工場出荷状態にリセットされ、再起動します** • **スイッチは工場出荷状態にリセットされ、再起動します。このオプションは IP アドレスをリセット対象から除外します** • **スイッチは工場出荷状態にリセットされ、再起動しません**

[**適用**] ボタン - 工場出荷状態へのリセットを開始します。

13.2.7 システム再起動

このウィンドウを用いて、スイッチの再起動を開始します。最後の再起動または電源オン以降に行われた新しいコンフィグレーション変更は、保存されていなければ、失われます。

ツールバー >[ツール] > [システム再起動] をクリックして、以下のウィンドウを表示します。

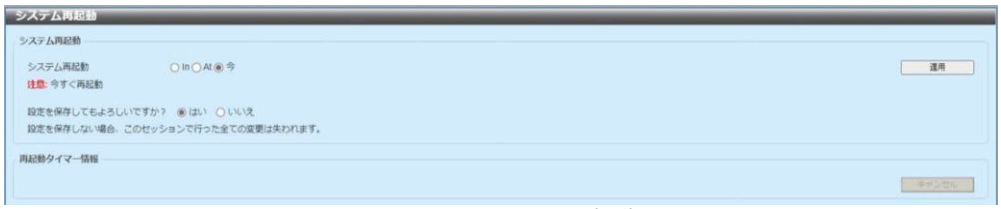


図 13-20 システム再起動

[**適用**] ボタン - 再起動を開始します。

13.3 言語

Web UI の言語は英語と日本語から選択できます。デフォルトは、日本語です。

プルダウンから言語を選択します。

図 13-21 言語

13.4 ログアウト

ツールバーで [**ログアウト**] オプションをクリックして、スイッチの Web UI からログアウトします。

図 13-22 ログアウト

14 付録 - システムログ一覧

14.1 802.1X

ID	ログの概要	重大度
1.	イベントの概要：802.1X 認証に成功しました。 ログメッセージ：[802.1X]（<method>）Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	情報
2.	イベントの概要：802.1X 認証に失敗しました。 ログメッセージ：[802.1X]（<method>）Rejected user <username> (<macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
3.	イベントの概要：802.1X 認証テーブルがフルなので、新しいアドレスを認証できません。 ログメッセージ：[802.1X]Rejected <macaddr> on Port <portNum> （auth table was full） パラメータ概要： macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

14.2 AAA

ID	ログの概要	重大度
1.	イベントの概要：ログインに成功しました。 ログメッセージ：Successful login through <Console | Telnet | SSH> (Username：<username>, IP：<ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	情報
2.	イベントの概要：ログインに失敗しました。 ログメッセージ：Login failed through <Console | Telnet | SSH> (Username：<username>, IP：<ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	ワーニング
3.	イベントの概要：ログアウトしました。 ログメッセージ：Logout through <Console | Telnet | SSH> （Username：<username>, IP：<ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	情報
4.	イベントの概要：セッションがタイムアウトしました。 ログメッセージ：<Console | Telnet > session timed out （Username：<username>, IP：<ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	情報
5.	イベントの概要：SSH サーバが有効になりました。 ログメッセージ：SSH server is enabled	情報
6.	イベントの概要：SSH サーバが無効になりました。 ログメッセージ：SSH server is disabled	情報
7.	イベントの概要：認証ポリシーが有効になりました。 ログメッセージ：Authentication Policy is enabled （Module：AAA）	情報
8.	イベントの概要：認証ポリシーが無効になりました。 ログメッセージ：Authentication Policy is disabled （Module：AAA）	情報
9.	イベントの概要：AAA サーバタイムアウトまたは不適切なコンフィグレーションのためにログインに失敗しました。 ログメッセージ:Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration （Username：<username>) パラメータ概要： ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング

ID	ログの概要	重大度
10.	イベントの概要：AAA のローカル認証で、認証なしで、またはサーバ認証で、管理者権限の移行が成功しました。 ログメッセージ：Successful Enable Admin through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | none | server <ipaddr | ipv6address>> （Username：<username>） パラメータ概要： local：AAA ローカル認証により管理者権限を移行します。 none：AAA 認証なしで管理者権限を移行します。 server：AAA サーバ認証により管理者権限を移行します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	情報
11.	イベントの概要：AAA サーバタイムアウトまたは不適切なコンフィグレーションのために管理者権限の移行に失敗しました。 ログメッセージ：Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration （Username：<username>） パラメータ概要： ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング
12.	イベントの概要：AAA ローカル認証または AAA サーバ認証による管理者権限の移行に失敗しました。 ログメッセージ：Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA < local | server <ipaddr | ipv6address>> （Username：<username>） パラメータ概要： local：AAA ローカル認証により管理者権限を移行します。 server：AAA サーバ認証により管理者権限を移行します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング
13.	イベントの概要：AAA のローカル認証で、認証なしで、またはサーバ認証で、ログインに成功しました。 ログメッセージ：Successful login through <Console | Telnet | SSH> from < ipaddr | ipv6address > authenticated by AAA <local | none | server <ipaddr | ipv6address>> （Username：<username>） パラメータ概要： local：AAA ローカル認証を指定します。 none：認証なしを指定します。 server：AAA サーバ認証を指定します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	情報

ID	ログの概要	重大度
14.	イベントの概要：AAA ローカル認証または AAA サーバ認証によるログインに失敗しました。 ログメッセージ:Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | server <ipaddr | ipv6address>> （Username：<username>） パラメータ概要： local：AAA ローカル認証を指定します。 server：AAA サーバ認証を指定します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング

14.3 ARP

ID	ログの概要	重大度
1.	イベントの概要：Gratuitous ARP で重複 IP を検出しました。 ログメッセージ：Conflict IP was detected with this device （IP：<ipaddr>, MAC：<macaddr>, Port <portNum>, Interface：<ipif_name>） パラメータ概要： ipaddr：使用中の装置と重複している IP アドレス。 macaddr：使用中の装置と重複する IP アドレスを持つ装置の MAC アドレス。 portNum：1. 整数値、2. 装置の論理ポート番号を表します。 ipif_name：競合 IP アドレスを持つスイッチのインタフェースの名前。	ワーニング

14.4 認証（2 ステップ）

ID	ログの概要	重大度
1.	イベントの概要：2 ステップ認証に成功しました。 ログメッセージ：[<step-mode>] （<method>）Authorized user <username> （<macaddr>）on Port <portNum> to VLAN <vid> パラメータ概要： step-mode：2 ステップ認証モードを示します。 method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	情報
2.	イベントの概要：MAC-WEB 認証に失敗しました。 ログメッセージ：[MAC-WEB] （<method>）Rejected at MAC auth <macaddr>）on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
3.	イベントの概要：MAC-WEB 認証に失敗しました。 ログメッセージ：[MAC-WEB] （<method>）Rejected at WEB auth user <username> （<macaddr>）on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
4.	イベントの概要：MAC-802.1X 認証に失敗しました。 ログメッセージ：[MAC-802.1X] （<method>）Rejected at MAC auth <macaddr>）on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
5.	イベントの概要：MAC-802.1X 認証に失敗しました。 ログメッセージ：[MAC-802.1X] （<method>）Rejected at 802.1X auth user <username> （<macaddr>）on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

ID	ログの概要	重大度
6.	イベントの概要：802.1X-WEB 認証に失敗しました。 ログメッセージ：[802.1X-WEB] （<method>）Rejected at 802.1X auth user <username> （<macaddr>）on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
7.	イベントの概要：802.1X-WEB 認証に失敗しました。 ログメッセージ：[802.1X-WEB] （<method>）Rejected at WEB auth user <username> （<macaddr>）on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

14.5 BPDU ガード

ID	ログの概要	重大度
1.	イベントの概要：BPDU アタックが発生しました。 ログメッセージ：Port<portNum> enter BPDU under attacking state（mode : drop / block / shutdown） パラメータ概要： portNum：ポート番号。 mode：BPDU の現在の状態。	情報
2.	イベントの概要：BPDU アタックから自動回復しました。 ログメッセージ：Port <portNum> recover from BPDU under attacking state automatically パラメータ概要： portNum：ポート番号。	情報
3.	イベントの概要：BPDU アタックからマニュアル回復しました。 ログメッセージ：Port<portNum> recover from BPDU under attacking state manually パラメータ概要： portNum：ポート番号。	情報

14.6 コマンド

ID	ログの概要	重大度
1.	イベントの概要：コマンドログ収集 ログメッセージ：“<command-str>” executed by <username> from <line>[, IP：<ip-address>] パラメータ概要： username：このコマンドを実行したアカウント名。 command-str：正常に実行され、スイッチのコンフィグレーションを変更したコマンド文字列。 line：このパラメータは、このコマンドを実行したラインモードを示します（console、telnet、SSH など）。 ip-address：（オプション）コマンドがリモート端末で入力された場合（telnet、SSH など）、このパラメータが必要です。	情報

14.7 コンフィグレーション / ファームウェア

ID	ログの概要	重大度
1.	イベントの概要：ファームウェアのアップグレードに成功しました。 ログメッセージ：irmware upgraded by <session> successfully （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
2.	イベントの概要：ファームウェアのアップグレードに失敗しました。 ログメッセージ：Firmware upgraded by <session> unsuccessfully （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング
3.	イベントの概要：ファームウェアのアップロードに成功しました。 ログメッセージ：Firmware uploaded by <session> successfully （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
4.	イベントの概要：ファームウェアのアップロードに失敗しました。 ログメッセージ：Firmware uploaded by <session> unsuccessfully （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング

ID	ログの概要	重大度
5.	イベントの概要：コンフィグレーションのダウンロードに成功しました。 ログメッセージ：Configuration downloaded by <session> successfully. （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
6.	イベントの概要：コンフィグレーションのダウンロードに失敗しました。 ログメッセージ：Configuration downloaded by <session> unsuccessfully. （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング
7.	イベントの概要：コンフィグレーションのアップロードに成功しました。 ログメッセージ：Configuration uploaded by <session> successfully. （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
8.	イベントの概要：コンフィグレーションのアップロードに失敗しました。 ログメッセージ：Configuration uploaded by <session> unsuccessfully. （Username : <username>[, IP : <ipaddr>, MAC : <macaddr>], Server IP : <serverIP>, File Name : <pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング

ID	ログの概要	重大度
9.	イベントの概要：未知のタイプのファイルのダウンロードに失敗しました。 ログメッセージ：Downloaded by <session> unsuccessfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング
10.	イベントの概要：ログメッセージのアップロードに成功しました。 ログメッセージ：Log message uploaded by <session> successfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>]） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。	情報
11.	イベントの概要：ログメッセージのアップロードに失敗しました。 ログメッセージ：Log message uploaded by <session> unsuccessfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>]） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。	情報

14.8 DAD

ID	ログの概要	重大度
1.	イベントの概要：DUT が DAD 期間中に重複アドレスを持つ NS（Neighbor Solicitation）メッセージを受信したのでログを追加します。 ログメッセージ：Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Solicitation Messages パラメータ概要： ipv6address：ネイバー要請メッセージの IPv6 アドレス。 interface-id：ポートインタフェース ID。	ワーニング
2.	イベントの概要：DUT が DAD 期間中に重複アドレスを持つ NA（Neighbor Advertisement）メッセージを受信したのでログを追加します。 ログメッセージ：Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Advertisement Messages パラメータ概要： ipv6address：ネイバーアドバタイズメッセージの IPv6 アドレス。 interface-id：ポートインタフェース ID。	ワーニング

14.9 DDM

ID	ログの概要	重大度
1.	イベント概要：DDM がアラーム閾値を超えたまたは復旧しました ログメッセージ：Port <portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] alarm threshold パラメータ概要： portNum：ポート番号 thresholdType：DDM 閾値タイプ。値は温度、供給電圧、バイアス電流、送信パワー、受信パワーのいずれか。 exceedType：閾値を超えたまたは通常状態に復旧。"recover from"、"exceeded" thresholdsubType：DDM 閾値サブタイプ。値は "high" または "low"	クリティカル
2.	イベント概要：DDM がワーニング閾値を超えたまたは復旧しました ログメッセージ：Port <portNum> SFP [thresholdType] [exceedType] the [thresholdSubType] warning threshold パラメータ概要： portNum：ポート番号 thresholdType：DDM 閾値タイプ。値は温度、供給電圧、バイアス電流、送信パワー、受信パワーのいずれか。 exceedType：閾値を超えたまたは通常状態に復旧。"recover from"、"exceeded" thresholdsubType：DDM 閾値サブタイプ。値は "high" または "low"	ワーニング

14.10 デバッグエラー

ID	ログの概要	重大度
1.	イベント概要：システムの致命的なエラーが発生したので、システムを再起動します。 ログメッセージ：System re-start reason：system fatal error	緊急
2.	イベントの概要：CPU 例外が発生したので、システムを再起動します。 ログメッセージ：System re-start reason：CPU exception	緊急

14.11 DHCPv6 クライアント

ID	ログの概要	重大度
1.	イベントの概要：DHCPv6 クライアントインタフェースの管理者の状態が変化しました。 ログメッセージ：DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] パラメータ概要： <ipif-name>：DHCPv6 クライアントインタフェースの名前。	情報
2.	イベントの概要：DHCPv6 クライアントが DHCPv6 サーバから IPv6 アドレスを取得しました。 ログメッセージ：DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name> パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
3.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの更新を開始しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> starts renewing パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
4.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの更新に成功しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> renews success パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
5.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの再バインディングを開始しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
6.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの再バインディングに成功しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> rebinds success パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
7.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスが削除されました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> was deleted パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報

ID	ログの概要	重大度
8.	イベントの概要：DHCPv6 クライアント PD インタフェースの管理者の状態が変化しました。 ログメッセージ：DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> パラメータ概要： intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
9.	イベントの概要：DHCPv6 クライアント PD が委任ルータから IPv6 プレフィックスを取得しました。 ログメッセージ：DHCPv6 client PD obtains an ipv6 prefix <ipv6networkaddr> on interface <intf-name> パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
10.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの更新を開始しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
11.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの更新に成功しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success パラメータ概要： ipv6anetworkaddr：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
12.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの再バインディングを開始しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding パラメータ概要： ipv6address：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
13.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの再バインディングに成功しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success パラメータ概要： ipv6address：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
14.	イベントの概要：委任ルータから取得した IPv6 プレフィックスが削除されました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted パラメータ概要： ipv6address：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報

14.12 ダイナミック ARP

ID	ログの概要	重大度
1.	イベントの概要：このログは、DAI が無効な ARP パケットを検出した場合に生成されます。 ログメッセージ：Illegal ARP <type> packets （IP：<ip-address>, MAC：<mac-address>, VLAN <vlan-id>, on <interface-id>） パラメータ概要： type：ARP パケットのタイプ。ARP パケットが ARP リクエストまたは ARP 応答のどちらであるかを示します。 ip-address：IP アドレス。 mac-address：MAC アドレス。 vlan-id：VLAN ID。 interface-id：インタフェースナンバー。	ワーニング
2.	イベントの概要：このログは、DAI が有効な ARP パケットを検出した場合に生成されます。 ログメッセージ：Legal ARP <type> packets （IP：<ip-address>, MAC：<mac-address>, VLAN <vlan-id>, on <interface-id>） パラメータ概要： type：ARP パケットのタイプ。ARP パケットが ARP リクエストまたは ARP 応答のどちらであるかを示します。 ip-address：IP アドレス。 mac-address：MAC アドレス。 vlan-id：VLAN ID。 interface-id：インタフェースナンバー。	情報

14.13 インタフェース

ID	ログの概要	重大度
1.	イベントの概要：ポートがリンクアップしました。 ログメッセージ：Port <port> link up, <nway> パラメータ概要： port：論理ポート番号を表します。 nway：リンクのスピードと二重モードを表します。	情報
2.	イベントの概要：ポートがリンクダウンしました。 ログメッセージ：Port <port> link down パラメータ概要： port：論理ポート番号を表します。	情報

14.14 PoE

ID	ログの概要	重大度
1.	イベントの概要：ポートの給電が ON になりました。 ログメッセージ：Port-<port> Power OFF notification パラメータ概要： port：論理ポート番号を表します。	情報
2.	イベントの概要：ポートの給電が OFF になりました。 ログメッセージ：Port-<port> Power On notification パラメータ概要： port：論理ポート番号を表します。	情報
3.	イベントの概要：PoE の給電電力が閾値を超えました。 ログメッセージ：Usage power is above the threshold	情報
4.	イベントの概要：PoE の給電電力が閾値を超えた後に閾値未満へ下がりました。 ログメッセージ：Usage power is below the threshold	情報
5.	イベントの概要：PoE IC の初期化が失敗しました。 ログメッセージ：PoE IC Reinit Fail	情報
6.	イベントの概要：PoE IC がリセットしました。 ログメッセージ：PoE IC Reset	情報

14.15 PoE オートリブート

ID	ログの概要	重大度
1.	イベントの概要：PoE 給電の OFF/ON を実行しました。 ログメッセージ：Execute PoE OFF/ON Port-<port> パラメータ概要： port：論理ポート番号を表します。	情報
2.	イベントの概要：Ping 監視により PoE 端末の異常を検知しました。 ログメッセージ：Detect equipment failure by ICMP <IP> パラメータ概要： IP：IP アドレスを表します。	情報
3.	イベントの概要：LLDP 監視により PoE 端末の異常を検知しました。 ログメッセージ：Detect equipment failure by LLDP Port-<port> パラメータ概要： port：論理ポート番号を表します。	情報
4.	イベントの概要：トラフィック監視により PoE 端末の異常を検知しました。 ログメッセージ：Detect equipment failure by Traffic Port-<port> パラメータ概要： port：論理ポート番号を表します。	情報

14.16 PoE スケジューラ

ID	ログの概要	重大度
1.	イベントの概要：PoE スケジューラにより PoE 給電を ON にしました。 ログメッセージ：(PoE) PoE port is changed to ON by PoE Scheduler. パラメータ概要： port：論理ポート番号を表します。	ワーニング
2.	イベントの概要：PoE スケジューラにより PoE 給電を OFF にしました。 ログメッセージ：(PoE) PoE port is changed to OFF by PoE Scheduler. パラメータ概要： port：論理ポート番号を表します。	ワーニング
3.	イベントの概要：PoE スケジューラにより PoE 給電を OFF/ON しました。 ログメッセージ：(PoE) PoE port is reset by PoE Scheduler.	ワーニング

14.17 IP ソースガードの検証

ID	ログの概要	重大度
1.	イベントの概要：このメッセージは、DHCP スヌーピングエントリを IPSG テーブルに設定するハードウェアルールリソースが存在しないことを示します。 ログメッセージ：Failed to set IPSG entry due to no hardware rule resource. (IP：<IPADDR>, MAC：<MACADDR>, VID：<VLANID>, Interface <INTERFACE-ID>) パラメータ概要： IPADDR：IP アドレス。 MACADDR：MAC アドレス。 VLANID：VLAN ID。 INTERFACE-ID：インタフェースナンバー。	ワーニング

14.18 LACP

ID	ログの概要	重大度
1.	イベントの概要：リンクアグリゲーショングループがリンクアップしました。 ログメッセージ：Link Aggregation Group < group_id > link up パラメータ概要： group_id：リンクアップしたアグリゲーショングループのグループ ID。	情報
2.	イベントの概要：リンクアグリゲーショングループがリンクダウンしました。 ログメッセージ：Link Aggregation Group < group_id > link down パラメータ概要： group_id：リンクダウンしたアグリゲーショングループのグループ ID。	情報
3.	イベントの概要：メンバポートがリンクアグリゲーショングループに所属しました。 ログメッセージ：<ifname> attach to Link Aggregation Group <group_id> パラメータ概要： ifname：アグリゲーショングループに所属したポートのインタフェース名。 group_id：ポートの所属先のアグリゲーショングループのグループ ID。	情報
4.	イベントの概要：メンバポートがリンクアグリゲーショングループへの所属を解除しました。 ログメッセージ：<ifname> detach from Link Aggregation Group <group_id> パラメータ概要： ifname：アグリゲーショングループへの所属を解除したポートのインタフェース名。 group_id：ポートが所属を解除したアグリゲーショングループのグループ ID。	情報

14.19 LLDP-MED

ID	ログの概要	重大度
1.	イベントの概要：LLDP-MED トポロジの変化を検出しました。 ログメッセージ：LLDP-MED topology change detected （on port <portNum>. chassis id：<chassisType>, <chassisID>, port id：<portType>, <portID>, device class：<deviceClass>） パラメータ概要： portNum：ポート番号。 chassisType：シャーシ ID サブタイプ。 値リスト： 1. chassisComponent（1） 2. interfaceAlias（2） 3. portComponent（3） 4. macAddress（4） 5. networkAddress（5） 6. interfaceName（6） 7. local（7） chassisID：シャーシ ID。 portType：ポート ID サブタイプ。 値リスト： 1. interfaceAlias（1） 2. portComponent（2） 3. macAddress（3） 4. networkAddress（4） 5. interfaceName（5） 6. agentCircuitId（6） 7. local（7） portID：ポート ID。 deviceClass：LLDP-MED デバイスタイプ。	注意

ID	ログの概要	重大度
2.	イベントの概要：競合する LLDP-MED デバイスタイプを検出しました。 ログメッセージ：Conflict LLDP-MED device type detected （ on port <portNum >, chassis id：< chassisType>, <chassisID>, port id：< portType>, <portID>, device class：<deviceClass>） パラメータ概要： portNum：ポート番号。 chassisType：シャーシ ID サブタイプ。 値リスト： 1. chassisComponent（1） 2. interfaceAlias（2） 3. portComponent（3） 4. macAddress（4） 5. networkAddress（5） 6. interfaceName（6） 7. local（7） chassisID：シャーシ ID。 portType：ポート ID サブタイプ。 値リスト： 1. interfaceAlias（1） 2. portComponent（2） 3. macAddress（3） 4. networkAddress（4） 5. interfaceName（5） 6. agentCircuitId（6） 7. local（7） portID：ポート ID。 deviceClass：LLDP-MED デバイスタイプ。	注意

ID	ログの概要	重大度
3.	イベントの概要：互換性のない LLDP-MED TLV セットを検出しました。 ログメッセージ：Incompatible LLDP-MED TLV set detected （ on port <portNum >, chassis id：< chassisType>, <chassisID>, port id：< portType>, <portID>, device class：<deviceClass>） パラメータ概要： portNum：ポート番号。 chassisType：シャーシ ID サブタイプ。 値リスト： 1. chassisComponent（1） 2. interfaceAlias（2） 3. portComponent（3） 4. macAddress（4） 5. networkAddress（5） 6. interfaceName（6） 7. local（7） chassisID：シャーシ ID。 portType：ポート ID サブタイプ。 値リスト： 1. interfaceAlias（1） 2. portComponent（2） 3. macAddress（3） 4. networkAddress（4） 5. interfaceName（5） 6. agentCircuitId（6） 7. local（7） portID：ポート ID。 deviceClass：LLDP-MED デバイスタイプ。	注意

14.20 ループ検知

ID	ログの概要	重大度
1.	イベントの概要：2 つのポートまたは 2 つの LACP インタフェースの間でループを検知しました。 ログメッセージ：The loop detected between port/port-channel <portNum> and <portNum> パラメータ概要： portNum：ポート番号または LACP インタフェース ID。	ワーニング
2.	イベントの概要：1 つのポートまたは 1 つの LACP インタフェースでループを検知しました。 ログメッセージ：The loop detected on port/port-channel <portNum> パラメータ概要： portNum：ポート番号または LACP インタフェース ID。	ワーニング
3.	イベントの概要：1 つのポートと 1 つの LACP インタフェースの間でループを検知しました。 ログメッセージ：The loop detected between port/port-channel <portNum> and port/port-channel <portNum> パラメータ概要： portNum：ポート番号またはポートチャネルナンバー。	ワーニング
4.	イベントの概要：ループしていたポートまたは LACP インタフェースが自動回復しました。 ログメッセージ：Port/Port-channel <portNum> auto recovery パラメータ概要： portNum：ポート番号または LACP インタフェース ID。	情報

14.21 MAC ベースアクセスコントロール

ID	ログの概要	重大度
1.	イベントの概要：MAC 認証に成功しました。 ログメッセージ：[MAC]（<method>）Authorized <macaddr> on Port <portNum> to VLAN <vid> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	情報
2.	イベントの概要：MAC 認証に失敗しました。 ログメッセージ：[MAC]（<method>）Rejected <macaddr> on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
3.	イベントの概要：MAC 認証テーブルがフルなので、新しいアドレスを認証できません。 ログメッセージ：[MAC]Rejected <macaddr> on Port <portNum>（auth table was full） パラメータ概要： macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

14.22 MSTP デバッグ拡張機能

ID	ログの概要	重大度
1.	イベントの概要：トポロジが変化しました。 ログメッセージ：Topology changed （Instance ：<Instance-id>,<interface-id>, MAC：<macaddr> ） パラメータ概要： Instance-id：インスタンス ID。 interface-id：ポート ID。 macaddr：MAC アドレス。	注意
2.	イベントの概要：スパニングツリーの新しいルートブリッジです。 ログメッセージ：[CIST | CIST Regional | MSTI Regional] New Root bridge selected （[Instance：<Instance-id>] MAC：<macaddr> Priority ：<priority>） パラメータ概要： Instance-id：インスタンス ID。 macaddr：MAC アドレス。 priority：優先度値。	注意
3.	イベントの概要：スパニングツリープロトコルが有効になりました。 ログメッセージ：Spanning Tree Protocol is enabled	情報
4.	イベントの概要：スパニングツリープロトコルが無効になりました。 ログメッセージ：Spanning Tree Protocol is disabled	情報
5.	イベントの概要：新しいルートポートです。 ログメッセージ：New root port selected （Instance：<instance-id>, <interface-id >） パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。	注意
6.	イベントの概要：スパニングツリーポート状態が変化しました。 ログメッセージ：Spanning Tree port status change （Instance ：< instance-id>, <interface-id>）<old-status> -> <new-status> パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。 old_status：変化前のステータス。 new_status：変化後のステータス。	注意
7.	イベントの概要：スパニングツリーポートロールが変化しました。 ログメッセージ：Spanning Tree port role change （Instance ：< instance-id>, <interface-id>）<old-role> -> <new-role> パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。 old_role：変化前のロール。 new_status：変化後のロール。	情報
8.	イベントの概要：スパニングツリーインスタンスが作成されました。 ログメッセージ：Spanning Tree instance created. （Instance ：< instance-id>） パラメータ概要： instance-id：インスタンス ID。	情報

ID	ログの概要	重大度
9.	イベントの概要：スパニングツリーインスタンスが削除されました。 ログメッセージ：Spanning Tree instance deleted. （Instance ：< instance-id >） パラメータ概要： instance-id：インスタンス ID。	情報
10.	イベントの概要：スパニングツリーバージョンが変化しました。 ログメッセージ：Spanning Tree version change （new version ：< new-version>） パラメータ概要： new_version：変化後の STP バージョン。	情報
11.	イベントの概要：スパニングツリー MST コンフィグレーション ID 名とリビジョンレベルが変化しました。 ログメッセージ：Spanning Tree MST configuration ID name and revision level change （name ：< name>, revision level <revision-level>） パラメータ概要： name：変化後の名前。 revision_level：変化後のリビジョンレベル。	情報
12.	イベントの概要：スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが削除されました。 ログメッセージ：Spanning Tree MST configuration ID VLAN mapping table change（instance：< instance-id > delete vlan <startvlanid> [- <endvlanid>]） パラメータ概要： instance-id：インスタンス ID。 startvlanid-endvlanid：VLAN リスト。	情報
13.	イベントの概要：スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが追加されました。 ログメッセージ：Spanning Tree MST configuration ID VLAN mapping table change （instance：< instance-id > add vlan <startvlanid> [- <endvlanid>]） パラメータ概要： instance-id：インスタンス ID。 startvlanid-endvlanid：VLAN リスト。	情報
14.	イベントの概要：ガードルート機能によりスパニングツリーロールが変化しました。 ログメッセージ：Spanning Tree port role change （Instance ：< instance-id >, <interface-id>）to alternate port due to the guard root パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。	情報

14.23 ポートセキュリティ

ID	ログの概要	重大度
1.	イベントの概要：ポートでアドレスがフルです。 ログメッセージ：MAC address <mac-address> causes port security violation on <interface-id> パラメータ概要： macaddr：違反 MAC アドレス。 interface-id：違反が発生しているインタフェース。	ワーニング
2.	イベントの概要：システムでアドレスがフルです。 ログメッセージ：Limit on system entry number has been exceeded	ワーニング

14.24 RADIUS

ID	ログの概要	重大度
1.	イベントの概要：このログは、RADIUS が有効な VLAN ID 属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned VID：<vid> to port <interface-id> （Username：<username>） パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 vid：RADIUS サーバが許可して割り当てた VLAN ID。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報
2.	イベントの概要：このログは、RADIUS が有効な帯域幅属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned <direction> bandwidth：<threshold> to port < interface-id> （Username：<username>） パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 direction：帯域制御の方向（入口または出口など）を示します。 threshold：RADIUS サーバが許可して割り当てた帯域幅閾値。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報
3.	イベントの概要：このログは、RADIUS が有効な優先度属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned 802.1p default priority：<priority> to port < interface-id> （Username：<username>） パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 priority：RADIUS サーバが許可して割り当てた優先度。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報
4.	イベントの概要：このログは、RADIUS が ACL スクリプトを割り当てたが、リソース不足のためにシステムに適用できなかった場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigns <username> ACL failure at port < interface-id> （<acl-script>） パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 username：認証するユーザ名を示します。 interface-id：認証されたクライアントのポート番号。 acl-script：RADIUS サーバが許可して割り当てた ACL スクリプト。	ワーニング
5.	イベントの概要：このログは、アクセスリストナンバーの割り当てに失敗した場合に生成されます。 ログメッセージ：Local assigns [USERNAME] filter-id ID failure at port INTERFACE-ID パラメータ概要： username：認証するユーザ名を示します。 filter-id：アクセスリストナンバーを示します。 interface-id：認証されたクライアントのポート番号。	ワーニング

14.25 RRP

ID	ログの概要	重大度
1.	イベントの概要：マスターノードの状態が "Failed" から "Complete" に変化しました。 ログメッセージ：Ring topology was recovered to complete	注意
2.	イベントの概要：マスターノードの状態が "Complete" から "Failed" に変化しました。 ログメッセージ：Ring topology was failed	ワーニング
3.	イベントの概要：マスターノードまたはトランジットノードが、RRP パケットまたはステートマシンに基づいて、そのフォワーディングデータベースをフラッシュしました。 ログメッセージ：FDB was flushed	情報
4.	イベントの概要：トランジットノードの RRP 状態が "Link-Up" に変化しました。 ログメッセージ：RRP ring status was changed to Link-Up	ワーニング
5.	イベントの概要：トランジットノードの RRP 状態が "Link-Down" に変化しました。 ログメッセージ：RRP ring status was changed to Link-Down	注意
6.	イベントの概要：トランジットノードの RRP 状態が "Pre-Forwarding" に変化しました。 ログメッセージ：RRP ring status was changed to Pre-Forwarding	情報
7.	イベントの概要：特定のドメインとポートでリングガード機能が有効になりました。 ログメッセージ：Ring Guard was activated on “<domain-name>” domain at port <port> パラメータ概要： <domain name>：ターゲットドメイン名。 <port num>：リングガード機能が有効になったターゲットポート番号。	情報

14.26 SNMP

ID	ログの概要	重大度
1.	イベントの概要：無効なコミュニティ文字列を含む SNMP リクエストを受信しました。 ログメッセージ：SNMP request received from <ipaddr> with invalid community string パラメータ概要： ipaddr：IP アドレス。	情報

14.27 システム

ID	ログの概要	重大度
1.	イベントの概要：システムがスタートアップしました。 ログメッセージ：System started up	クリティカル
2.	イベントの概要：現在のコンフィグレーションがフラッシュに保存されました。 ログメッセージ：Configuration saved to flash by console （Username：<username>） パラメータ概要： username：ユーザ名。	情報
3.	イベントの概要：リモートからシステムコンフィグレーションを保存しました。 ログメッセージ：Configuration saved to flash （Username：<username>, IP：<ipaddr>） username：ユーザ名。 ipaddr：IP アドレス。	情報
4.	イベントの概要：システムの電源がオンになり、スタートアップしました。 ログメッセージ：System cold start	クリティカル
5.	イベントの概要：システムが再起動し、スタートアップしました。 ログメッセージ：System warm start	クリティカル

14.28 Telnet

ID	ログの概要	重大度
1.	イベントの概要：Telnet によるログインに成功しました。 ログメッセージ：Successful login through Telnet （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	情報
2.	イベントの概要：Telnet によるログインに失敗しました。 ログメッセージ：Login failed through Telnet （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	ワーニング
3.	イベントの概要：Telnet によりログアウトしました。 ログメッセージ：Logout through Telnet （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	情報
4.	イベントの概要：Telnet セッションがタイムアウトしました。 ログメッセージ：Telnet session timed out （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	情報

14.29 温度

ID	ログの概要	重大度
1.	イベントの概要：温度センサがアラーム状態に移行しました。 ログメッセージ：Unit <unitID> Sensor：<sensorID> detects abnormal temperature <temperature> パラメータ概要： unitID：ユニット ID。 sensorID：センサ ID。 temperature：センサの現在の温度。	クリティカル
2.	イベントの概要：通常の温度に回復しました。 ログメッセージ：Unit <unitID> Sensor：<sensorID> temperature back to normal パラメータ概要： unitID：ユニット ID。 sensorID：センサ ID。 temperature：温度。	クリティカル

14.30 トラフィック制御

ID	ログの概要	重大度
1.	イベントの概要：ブロードキャスト、マルチキャスト、またはユニキャストのストームが発生しています。 ログメッセージ：Broadcast | Multicast | Unicast> storm is occurring on <interface-id> パラメータ概要： interface-id：ストームが発生しているインタフェース ID。	ワーニング
2.	イベントの概要：ブロードキャスト、マルチキャスト、またはユニキャストのストームが解消されました。 ログメッセージ：<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> パラメータ概要： interface-id：ストームが解消されたインタフェース ID。	情報
3.	イベントの概要：パケットストームによりポートがシャットダウンされました。 ログメッセージ：<interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm パラメータ概要： Interface-id：ストームにより error-disabled に移行したインタフェース ID。	ワーニング

14.31 UDLD

ID	ログの概要	重大度
1.	イベントの概要：このポートで単方向リンクを検出しました。 ログメッセージ：Unidirectional link detection on <INTERFACE-ID> パラメータ概要： INTERFACE-ID：インタフェース名。	ワーニング

14.32 音声 VLAN

ID	ログの概要	重大度
1.	イベントの概要：インタフェースで新しい音声装置を検出しました。 ログメッセージ：New voice device detected （<interface-id>, MAC：< mac-address >） パラメータ概要： interface-id：インタフェース名。 mac-address：音声装置の MAC アドレス。	情報
2.	イベントの概要：自動音声 VLAN モードのインタフェースが音声 VLAN に参加しました。 ログメッセージ：< interface-id > add into voice VLAN <vid > パラメータ概要： interface-id：インタフェース名。 vid：VLAN ID。	情報
3.	イベントの概要：このログメッセージは、インタフェースが音声 VLAN を脱退し、さらにそのインタフェースのエージング期間内に音声装置を検出しなかった場合に、送信されます。 ログメッセージ：< interface-id > remove from voice VLAN <vid > パラメータ概要： interface-id：インタフェース名。 vid：LAN ID。	情報

14.33 PPS （Power to Progress SDN）

ID	ログの概要	重大度
1.	イベントの概要：コントローラが更新されました。 ログメッセージ：(PPS) New Controller （ID：<ControllerID>） パラメータ概要： ControllerID：PPS コントローラ ID	情報
2.	イベントの概要：コントローラポートが更新されました。 ログメッセージ：(PPS) New Controller Port （Port ：<PortNum>） パラメータ概要： PortNum：ポート番号	情報
3.	イベントの概要：ステータスを “Standalone” から “Controlled” に変更しました。 ログメッセージ：(PPS) Change Status from Standalone to Controlled	情報
4.	イベントの概要：ステータスを “Controlled” から “CPNL” に変更しました。 ログメッセージ：(PPS) Change Status from Controlled to CPNL	情報
5.	イベントの概要：ステータスを “CPNL” から “Controlled” に変更しました。 ログメッセージ：(PPS) Change Status from CPNL to Controlled	情報
6.	イベントの概要：コンフィグレーションモードで開始しました。 ログメッセージ：(PPS) Start Configuration Mode	情報
7.	イベントの概要：コンフィグレーションモードを停止しました。 ログメッセージ：(PPS) Stop Configuration Mode	情報
8.	イベントの概要：“Commit” またはリクエスト（セーブ）を受信し、設定を変更しました。 ログメッセージ：(PPS) Configuration Changed	情報
9.	イベントの概要：“Rollback” を受信し、設定を修復しました。 ログメッセージ：(PPS) Configuration Changed （Rollback）	情報
10.	イベントの概要：“Shared key” または “Specific key”, その両方を消失しました。 ログメッセージ：(PPS) Lost Authentication Key	ワーニング
11.	イベントの概要：コントローラ再送信時にタイムアウトしました。 ログメッセージ：(PPS) No response from Controller	注意
12.	イベントの概要：コネクションテーブルが更新されました。 ログメッセージ：(PPS) Overwrite connection table	情報
13.	イベントの概要：コントローラがポートの状態を “Forwarding” に変更しました。 ログメッセージ：(PPS) Controller change port status to Forwarding	情報
14.	イベントの概要：コントローラがポートの状態を “Blocking” に変更しました。 ログメッセージ：(PPS) Controller change port status to Blocking	情報
15.	イベントの概要：起動時に SDN 情報 2（Backup）が破損し、SDN 情報 1（Main）を SDN 情報 2（Backup）にコピーしました。 ログメッセージ：(PPS) Copied PPS information 1 to 2.	情報
16.	イベントの概要：起動時に SDN 情報 1（Main）が破損し、SDN 情報 2（Backup）を SDN 情報 1（Main）にコピーしました。 ログメッセージ：(PPS) Copied PPS information 2 to 1.	情報
17.	イベントの概要：起動時に SDN 情報 1（Main）と 2（Backup）が破損し、SDN 情報をデフォルトにリセットしました。 ログメッセージ：(PPS) Reset PPS information 1 & 2 to default.	注意

ID	ログの概要	重大度
18.	イベントの概要：起動時に SDN 情報 1（Main）から 2（Backup）へのコピーに失敗しました。 ログメッセージ：(PPS) Copy PPS information 1 to 2 is failed.	エラー
19.	イベントの概要：起動時に SDN 情報 2（Backup）から 1（Main）へのコピーに失敗しました。 ログメッセージ：(PPS) Copy PPS information 2 to 1 is failed	エラー
20.	イベントの概要：SDN 情報 1 （Main）の保存に失敗しました。 * 起動時にコントローラ情報を更新してください ログメッセージ：(PPS) Save of PPS information 1 is failed.	エラー
21.	イベントの概要：SDN 情報 2（Backup）の保存に失敗しました。 ログメッセージ：(PPS) Save of PPS information 2 is failed.	エラー
22.	イベントの概要：コントローラから設定ファイルを受信しました。 ログメッセージ：(PPS) Configuration file download.	情報
23.	イベントの概要：コントローラに設定ファイルを送信しました。 ログメッセージ：(PPS) Configuration file upload.	情報
24.	イベントの概要：コントローラからファームウェアが変更されました。 ログメッセージ：(PPS) Runtime code changes.	情報
25.	イベントの概要：Standalone 装置がコントローラと 60 分間通信不可なことを表します。PPS 機能を自動的に停止したことを表します。 ログメッセージ：(PPS) Not found Controller. Stop PPS function.	注意

14.34 WAC

ID	ログの概要	重大度
1.	イベントの概要：クライアントホストが認証に失敗しました。 ログメッセージ：[WEB]（RADIUS/Local）Rejected user <string> (<macaddr>) on Port <portNum> パラメータ概要： string：ユーザ名。 macaddr：MAC アドレス。 portNum：ポート番号。	ワーニング
2.	イベントの概要：クライアントホストが認証に成功しました。 ログメッセージ：[WEB]（RADIUS/Local）Authorized user <string> (<macaddr>) on Port <portNum> to VLAN <vlanNum> パラメータ概要： string：ユーザ名。 macaddr：MAC アドレス。 portNum：ポート番号。 vlanNum：VLAN ナンバー。	情報
3.	イベントの概要：クライアントテーブルがフルです。 ログメッセージ：[WEB]Rejected <macaddr> on Port <portNum>（auth table was full） パラメータ概要： macaddr：MAC アドレス。 portNum：ポート番号。	注意

14.35 Web

ID	ログの概要	重大度
1.	イベントの概要：Web からのログインに成功しました。 ログメッセージ："Successful login through Web （Username：<username>, IP：<ipaddr>）" パラメータ概要： username：ユーザ名。 ipaddr：Web からスイッチにアクセスしたユーザの IP アドレス。	情報
2.	イベントの概要：Web からのログインに失敗しました。 ログメッセージ：Login failed through Web （Username：<username>, IP：<ipaddr>）" パラメータ概要： username：ユーザ名。 ipaddr：Web からスイッチにアクセスしたユーザの IP アドレス。	ワーニング
3.	イベントの概要：HTTPS からのログインに成功しました。 ログメッセージ：Successful login through Web（SSL）（Username：<username>, IP：<ipaddr>） パラメータ概要： username：ユーザ名。 ipaddr：セキュア Web からスイッチにアクセスしたユーザの IP アドレス。	情報
4.	イベント概要：セキュア Web からのログインに失敗しました。 ログメッセージ：Login failed through Web（SSL）（Username：<username>, IP：<ipaddr>） パラメータ概要： username：ユーザ名。 ipaddr：セキュア Web からスイッチにアクセスしたユーザの IP アドレス。	ワーニング
5.	イベントの概要：ログのアップロードに成功しました。 ログメッセージ：Log message uploaded by WEB successfully. （Username：<username>, IP：<ipaddr>, MAC：<macaddr>, Server IP：<ipaddr>, File Name：<filename>） パラメータ概要： username：ユーザ名。 ipaddr：スイッチにアクセスしたユーザの IP アドレス。 macaddr：クライアントの MAC アドレス。 server IP：TFTP サーバ IP アドレス。 filename：ログファイル名。	情報
6.	イベントの概要：ログのアップロードに失敗しました。 ログメッセージ：Log message uploaded by WEB unsuccessfully. （Username：<username>, IP：<ipaddr>, MAC：<macaddr>, Server IP：<ipaddr>, File Name：<filename>） パラメータ概要： username：ユーザ名。 ipaddr：スイッチにアクセスしたユーザのアクセス元の IP アドレス。 macaddr：クライアントの MAC アドレス。 server IP：TFTP サーバ IP アドレス。 filename：ログファイル名。	情報

15 付録 - システムトラップ一覧

15.1 BPDU ガード

ID	トラップ名	トラップの概要	OID
1.	mnoBpduProtectionUnderAttackingTrap	BPDU アタックが発生し、廃棄 / ブロック / シャットダウンモードに移行します。 バインディングオブジェクト： mnoBpduProtectionPortIndex ポートインタフェース。 （2）mnoBpduProtectionPortMode 廃棄 / ブロック / シャットダウンモード。	1.3.6.1.4.1.396.5.5.3.4.0.1
2.	mnoBpduProtectionRecoveryTrap	BPDU アタックから自動回復しました。 バインディングオブジェクト： mnoBpduProtectionPortIndex ポートインタフェース。 mnoBpduProtectionRecoveryMethod 自動 / マニュアル回復。	1.3.6.1.4.1.396.5.5.3.4.0.2

15.2 DDM

ID	トラップ名	トラップの概要	OID
1.	mnoDdmAlarmTrap	トラップアクションのコンフィグレーションに応じて、パラメータ値がアラーム閾値を超えたとき、または通常状態に回復したとき、このトラップが送信されます。 バインディングオブジェクト： mnoDdmPort ポート番号 mnoDdmThresholdType DDM 閾値タイプ temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType 超えた閾値がアラーム上限閾値またはアラーム下限閾値のどちらであるか (4) mnoDdmThresholdExceedOrRecover GBIC が DDM 閾値を超えているか、または通常状態に回復しているか	1.3.6.1.4.1.396.5.5.1.4.0.1
2.	mnoDdmWarningTrap	トラップアクションのコンフィグレーションに応じて、パラメータ値がワーニング閾値を超えたとき、または通常状態に回復したとき、このトラップが送信されます。 バインディングオブジェクト： mnoDdmPort ポート番号 mnoDdmThresholdType DDM 閾値タイプ temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType 超えた閾値がワーニング上限閾値またはワーニング下限閾値のどちらであるか (4) mnoDdmThresholdExceedOrRecover GBIC が DDM 閾値を超えているか、または通常状態に回復しているか	1.3.6.1.4.1.396.5.5.1.4.0.2

15.3 DHCP サーバプロテクト

ID	トラップ名	トラップの概要	OID
1.	mnoFilterDetectedTrap	不正な DHCP サーバが検出されたときに、このトラップが送信されます。検出した不正な DHCP サーバの IP アドレスは、ログ停止未認証期間中に 1 回のみトラッププレシーバに送信されます。 バインディングオブジェクト： mnoFilterDetectedIP 不正な DHCP サーバの IP アドレス。 mnoFilterDetectedport ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.7.0.1

15.4 Gratuitous ARP

ID	トラップ名	トラップの概要	OID
1.	mnoAgentGratuitousARPTrap	IP アドレスが競合したときに、このトラップが送信されます。 バインディングオブジェクト： agentGratuitousARPIpAddr Gratuitous ARP で受信した競合 IP アドレス。 agentGratuitousARPMacAddr Gratuitous ARP パケットのセンダー MAC アドレス。 agentGratuitousARPPortNumber Gratuitous ARP パケットを受信したスイッチのポート番号。 agentGratuitousARPInterfaceName Gratuitous ARP を受信したスイッチの IP インタフェース名。	1.3.6.1.4.1.396.5.5.3.6.0.1

15.5　ファン

ID	トラップ名	トラップの概要	OID
1.	mnoFanFailure	ファンが機能しなくなったときに、この通知が送信されます。	1.3.6.1.4.1.396.5.5.1.1
2.	mnoFanRecovery	ファンが復旧したときに、この通知が送信されます。	1.3.6.1.4.1.396.5.5.1.5

15.6 LLDP-MED

ID	トラップ名	トラップの概要	OID
1.	lldpRemTablesChange	lldpStatsRemTableLastChangeTime の値が変化したときに、lldpRemTablesChange 通知が送信されます。 バインディングオブジェクト： (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2.	lldpXMedTopologyChangeDetected	トポロジの変化を検出したローカル装置によって生成され、新しいリモート装置がローカルポートに接続されたこと、リモート装置が切断されたこと、またはリモート装置がポート間で移動されたことを示す通知。 バインディングオブジェクト： (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

15.7 ループ検知

ID	トラップ名	トラップの概要	OID
1.	mnoLoopDetectNotification	ネットワークループが発生したことを示します。	1.3.6.1.4.1.396.5.5.2.1
2.	mnoLoopRecoveryNotification	ネットワークループが消滅したことを示します。	1.3.6.1.4.1.396.5.5.2.2

15.8 MAC ベースアクセスコントロール

ID	トラップ名	トラップの概要	OID
1.	mnoMacBasedAccessControlLoggedSuccess	MAC ベースアクセスコントロールホストへのログインに成功すると、このトラップが送信されます。 バインディングオブジェクト： mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 mnoMacBasedAuthInfoPortIndex ポートインタフェース。 mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.1
2.	mnoMacBasedAccessControlLoggedFail	MAC ベースアクセスコントロールホストへのログインに失敗すると、このトラップが送信されます。 バインディングオブジェクト： mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 mnoMacBasedAuthInfoPortIndex ポートインタフェース。 mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.2
3.	mnoMacBasedAccessControlAgesOut	MAC ベースアクセスコントロールホストがエージアウトすると、このトラップが送信されます。 バインディングオブジェクト： mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 （2）mnoMacBasedAuthInfoMacIndex ポートインタフェース。 （3）mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.3

15.9 MAC 通知

ID	トラップ名	トラップの概要	OID
1.	mnoL2macNotification	このトラップは、アドレステーブルの MAC アドレスに変化があることを示します。 バインディングオブジェクト： mnoL2macNotifyInfo 装置の MAC アドレスの変更情報。詳細情報には、以下が含まれます。 操作コード + MAC アドレス + ボックス ID + インタフェース ID + ゼロ。 操作コード：1、2 1 は新しい MAC アドレスを学習したことを意味します。 2 は古い MAC アドレスを削除したことを意味します。 ボックス ID：スイッチのボックス ID インタフェース ID：ボックスで学習または削除したインタフェース ID。 ゼロ：各メッセージの区切りに使用します（操作コード + MAC アドレス + ボックス ID + ポート番号）。	1.3.6.1.4.1.396 .5.5.3.1.0.1

15.10 MSTP

ID	トラップ名	トラップの概要	OID
1.	newRoot	トラップは、送信エージェントがスパニングツリーの新しいルートになったことを示します。このトラップは、新しいルートとして選定された直後（トポロジ変化タイマーの期限切れ直後、選定の直後など）にブリッジにより送信されます。このトラップの実装はオプションです。	1,3,6,1,2,1,17.0.1
2.	topologyChange	トラップは、設定されているポートのいずれかが学習状態からフォワーディング状態に移行したとき、またはフォワーディング状態からブロッキング状態に移行したとき、ブリッジにより送信されます。そのような移行の際に newRoot トラップが送信された場合、それと同じ移行に関してこのトラップが送信されることはありません。このトラップの実装はオプションです。	1,3,6,1,2,1,17.0.2

15.11 ポートセキュリティ

ID	トラップ名	トラップの概要	OID
1.	mnoL2PortSecurityViolationTrap	ポートセキュリティトラップが有効な場合、事前定義されているポートセキュリティコンフィグレーションに違反する新しい MAC アドレスは、トラップメッセージ送信をトリガーします。 バインディングオブジェクト： mnoPortSecPortIndex ポートインタフェース。 mnoL2PortSecurityViolationMac ホスト MAC アドレス。	1.3.6.1.4.1.396.5.5.3.3.0.1

15.12 ポート

ID	トラップ名	トラップの概要	OID
1.	linkUp	この通知は、ポートがリンクアップしたときに生成されます。 バインディングオブジェクト： (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2.	linkDown	この通知は、ポートがリンクダウンしたときに生成されます。 バインディングオブジェクト： (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

15.13 PoE

ID	トラップ名	トラップの概要	OID
1.	pethPsePortOnOffNotification	PoE ポートの給電を開始・停止したことを示します。	1.3.6.1.2.1.105.0.1
2.	pethMainPowerUsageOnNotification	給電容量が設定した給電閾値を越えたことを示します。	1.3.6.1.2.1.105.0.2
3.	pethMainPowerUsageOffNotification	給電容量が設定した給電閾値を下回ったことを示します。	1.3.6.1.2.1.105.0.3

15.14 PoE オートリブート

ID	トラップ名	トラップの概要	OID
1.	EventFailureNotification	PoE オートリブートで端末を異常判定したことを示します。	1.3.6.1.4.1.396.5.5.1.9.1
2.	EventRecoverNotification	PoE オートリブートで端末を正常判定したことを示します。	1.3.6.1.4.1.396.5.5.1.9.2

15.15 RMON

ID	トラップ名	トラップの概要	OID
1.	risingAlarm	アラームエントリがその上昇閾値を超えて、SNMP トラップを送信するように設定されているイベントが生成されたときに、この SNMP トラップが生成されます。 バインディングオブジェクト： (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2.	fallingAlarm	アラームエントリがその下降閾値を超えて、SNMP トラップを送信するように設定されているイベントが生成されたときに、この SNMP トラップが生成されます。 バインディングオブジェクト： (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

15.16 SNMP 認証

ID	トラップ名	トラップの概要	OID
1.	authenticationFailure	authenticationFailure トラップは、エージェントロールで動作する SNMPv2 エンティティが、正しく認証されていないプロトコルメッセージを受信したことを示します。SNMPv2 のすべての実装にこのトラップを生成する機能が必要ですが、snmpEnableAuthenTraps オブジェクトは、このトラップが生成されるかどうかを示します。	1.3.6.1.6.3.1.1.5.5

15.17 システム

ID	トラップ名	トラップの概要	OID
1.	coldStart	coldStart トラップは、エージェントロールで動作する SNMPv2 エンティティが自身を再初期化していること、およびそのコンフィグレーションが変更されている可能性があることを示します。	1.3.6.1.6.3.1.1.5.1
2.	warmStart	warmStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、コンフィグレーションが変更されないように自身を再初期化していることを示します。	1.3.6.1.6.3.1.1.5.2

15.18 温度

ID	トラップ名	トラップの概要	OID
1.	mnoTemperatureRising Alarm	この通知は、現在の温度が上限閾値を超えているときに送信されます。	1.3.6.1.4.1.396.5.5.1.2.1
2.	mnoTemperatureFalling Alarm	この通知は、現在の温度が上限閾値から下降しているときに送信されます。	1.3.6.1.4.1.396.5.5.1.2.2

15.19 トラフィック制御

ID	トラップ名	トラップの概要	OID
1.	mnoPktStormOccurred	パケットストームメカニズムによりパケットストープが検出され、アクションとしてシャットダウンを実行する場合。 バインディングオブジェクト： mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.1
2.	mnoPktStormCleared	パケットストームが解消された場合。 バインディングオブジェクト： mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.2
3.	mnoPktStormDisablePort	パケットストームメカニズムによりポートが無効になった場合。 バインディングオブジェクト： mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.3

パナソニックEWネットワークス株式会社

〒105-0021　東京都港区東新橋 2 丁目 12 番 7 号　住友東新橋ビル 2 号館 4 階
TEL 03-6402-5301 / FAX 03-6402-5304
URL：https：//panasonic.co.jp/ew/pewnw/

P1023-0