Panasonic

PoE 給電スイッチングハブ

WEB リファレンス

品番 ZLP880895/ZLP881695/
ZLP88160

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
XA-AML8TFPoE++	ZLP880895	1.0.0.00 以上
XA-AML16TFPoE++	ZLP881695	1.0.0.00 以上
XA-AM16T	ZLP88160	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 設定を有効にするには、次ページ以降の 2 つの内どちらかの設定が必要となります。
- 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。

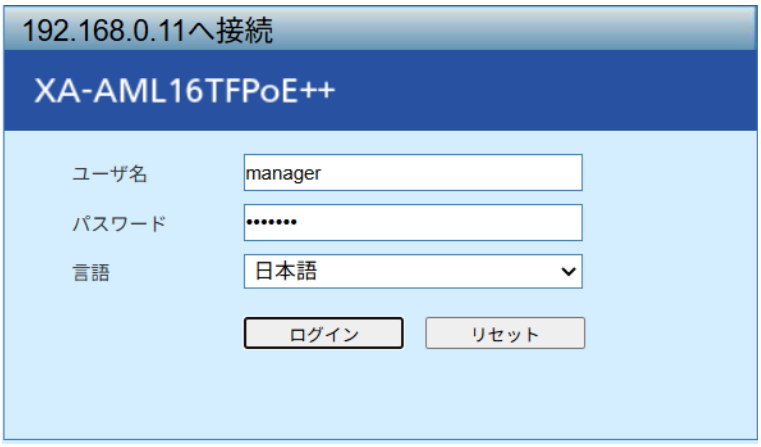

図 1-1　WEB ブラウザ　ログイン画面

1.1 CLI コマンド設定

WEB 設定を有効にする場合、本装置に事前に CLI コマンドで以下の設定が必要です。

①ユーザ名とパスワードを入力します。(以下はデフォルト設定です)
(ユーザ名 :manager, パスワード :manager)

```
UserName : manager
Password : manager
```

② IP アドレスとデフォルトゲートウェイを設定
(例 : IP アドレス : 192.168.0.101,
デフォルトゲートウェイ : 192.168.0.101)

```
XA-AML16TFPoE++>enable
XA-AML16TFPoE++#configure terminal
XA-AML16TFPoE++(config)#interface vlan 1
XA-AML16TFPoE++(config-if)#ip address 192.168.0.101 255.255.255.0
XA-AML16TFPoE++(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.0.101
```

③ http サーバ機能の有効化

```
XA-AML16TFPoE++(config)#ip http server
```

WEB ブラウザに②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。

CLI コマンド実行例 :

```
                    XA-AML16TFPoE++
                Command Line Interface

              Product Number: ZLP881695
            Firmware Version: V1.0.0.00
                 MAC Address: xx:xx:xx:xx:xx:xx
               Serial Number: xxxxxxxxxxx

UserName:manager
Password:*******

XA-AML16TFPoE++>enable
XA-AML16TFPoE++#configure
XA-AML16TFPoE++(config)#interface vlan1
XA-AML16TFPoE++(config-if)#ip address 192.168.0.101 255.255.255.0
XA-AML16TFPoE++(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.0.101
XA-AML16TFPoE++(config-if)#exit
XA-AML16TFPoE++(config)#ip http server
XA-AML16TFPoE++(config)#
```

1.2 WEB 簡単設定ウィザード

WEB 設定を有効にする場合、本装置に事前に 「WEB 簡単設定ウィザード」の以下設定が必要です。

(注意) WEB 簡単設定ウィザードは、工場出荷状態の config 未設定の時のみ使用可能です。

① ユーザ名とパスワードを入力します。
(ユーザ名 :manager, パスワード :websetup)

```
UserName : manager
Password : websetup
```

② IP アドレス、サブネット マスク、デフォルト ゲートウェイ アドレス、新しいユーザ名、新しいパスワードを入力します。

```
Enter IP address      :192.168.0.101
Enter Subnet mask     :255.255.255.0
Enter Default Gateway :192.168.0.101
Enter Username        :manager
Enter Password        :manager
```

③画面に構成した設定が表示されます。[Y] を入力して設定を適用します。

```
IP address      :192.168.0.101
Subnet mask     :255.255.255.0
Default Gateway :192.168.0.101
Username        :manager
Password        :manager
Web status      :Enable
Note : This configuration is not saved to startup-config. ( 注 1)
Apply this configuration?(Y/N) Y ( 注 1)
```

④確認後、ログイン画面に戻ります。

(注 1) Apply this configuration?(Y/N) で [Y] を選択した場合は、WEB 簡単設定ウィザードで設定した内容は、running-config として有効となります。ただし、startup-config に保存されません。

WEB ブラウザに②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。

CLI コマンド実行例 :

```
                          XA-AML16TFPoE++
                       Command Line Interface

                    Product Number: ZLP881695
                  Firmware Version: V1.0.0.00
                       MAC Address: xx:xx:xx:xx:xx:xx
                     Serial Number: xxxxxxxxxxx

UserName:manager
Password:********

Launched the Web Easy Setup Wizard.

Enter IP address      :192.168.0.101
Enter Subnet mask     :255.255.255.0
Enter Default Gateway :192.168.0.101
Enter Username        :manager
Enter Password        :manager

IP address      :192.168.0.101
Subnet mask     :255.255.255.0
Default Gateway :192.168.0.101
Username        :manager
Password        :manager
Web status      :Enable
Note:This configuration is not saved to startup-config.
Apply this configuration?(Y/N)y
```

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。

[XA-AML16TFPoE++] 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。

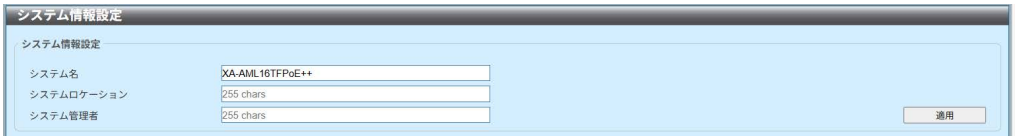

図 2-2 システム情報設定

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。(設定可能文字：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。(設定可能文字：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。(設定可能文字：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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
状態	ポートの状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)

パラメータ	概要
MDIX	MDIX（Medium Dependent Interface Crossover）のオプションを選択します。(初期値 : Auto) • **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。(初期値 : Off)
デュプレックス	使用する二重モード（**Auto**/**Half**/**Full**）を選択します。 (初期値 : Auto)

パラメータ	概要
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。(初期値 : Auto) 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** - ツイストペアポートの場合、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 のツイストペアケーブルのみ利用できます) • **1000M** - 1000Mbps に強制します。 • **1000M Master** - 1000Mbps 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。 • **1000M Slave** - 1000Mbps 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。 • **10G** - 10Gbps に強制します。 • **2500M** - 2.5Gbps に強制します。 • **5000M** - 5Gbps に強制します。 • **40G** - 40Gbps に強制します。
アドバタイズ能力	[スピード] を [AUTO] に設定すると、これらの機能がオートネゴシエーション時にアドバタイズされます。選択されていない場合は、すべての速度 (**100M, 1000M, 10G, 2500M, 5000M**) がアドバタイズされます
説明	ポートの説明を入力します。(設定可能文字 : 64 文字) [**説明**] テキストボックスを無効にするには、[**省略**] チェックボックスを選択します。

[**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。

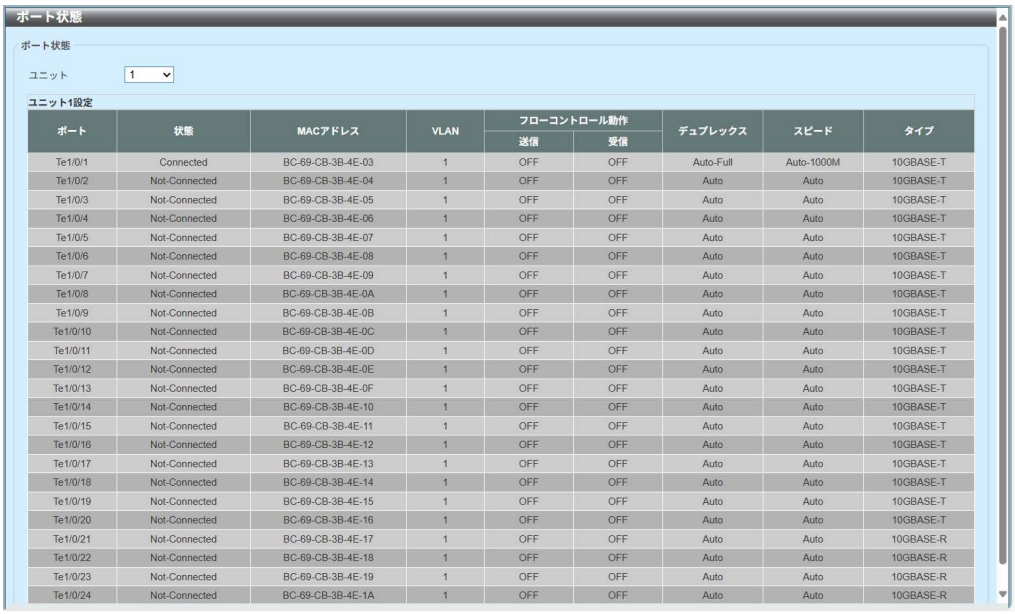

図 2-4 ポート状態

設定パラメータ （[ポート状態] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

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。

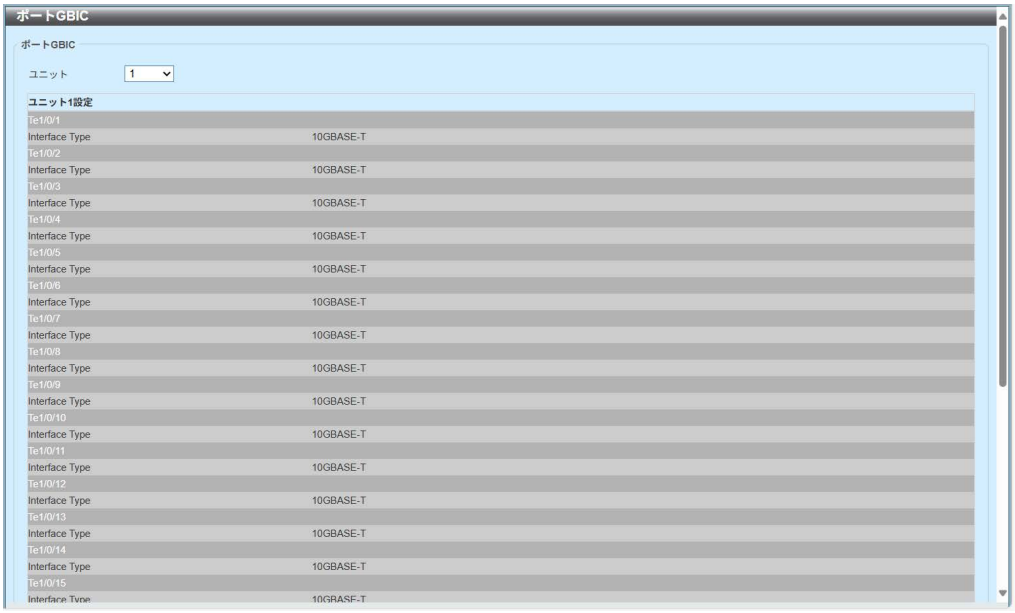

図 2-5 ポート GBIC

設定パラメータ （[ポート GBIC] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

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。

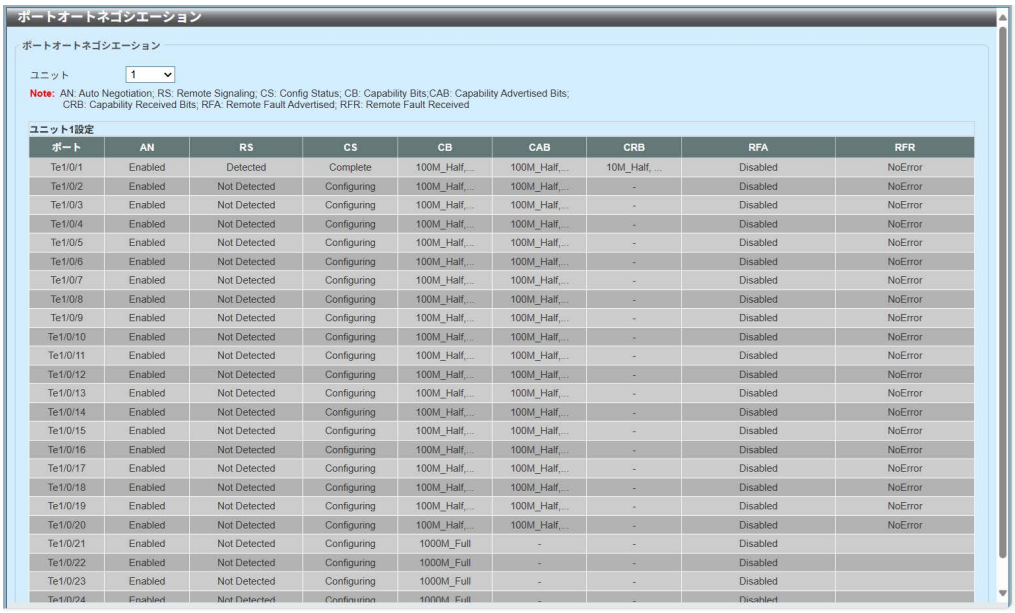

図 2-6 ポートオートネゴシエーション

設定パラメータ （[ポートオートネゴシエーション] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

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 攻撃保護 - **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** : UDL 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 / 無効**）します。（**Disabled** : 無効化、**Enabled** : 有効化、初期値 : **Disabled**）
間隔 (秒)	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。（初期値 : 300 秒 , 設定範囲 : 5 ～ 86400 秒）

[**適用**] ボタン - 設定内容を反映します。

以下は、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示します。

- **インターフェース** - 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) を示します。
- **エラーディセーブル原因** - エラー閉塞 (Error Disabled) の原因を示します。(原因：Port Security / Storm Control / BPDU Attack Protection / Dynamic ARP Inspection / DHCP Snooping / L2PT Guard / Detect-UDL)
- **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を秒単位で示します。(設定範囲：0 ～ 86400 秒)

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 （初期値：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

2.4.1 PoE グローバル設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] >[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。

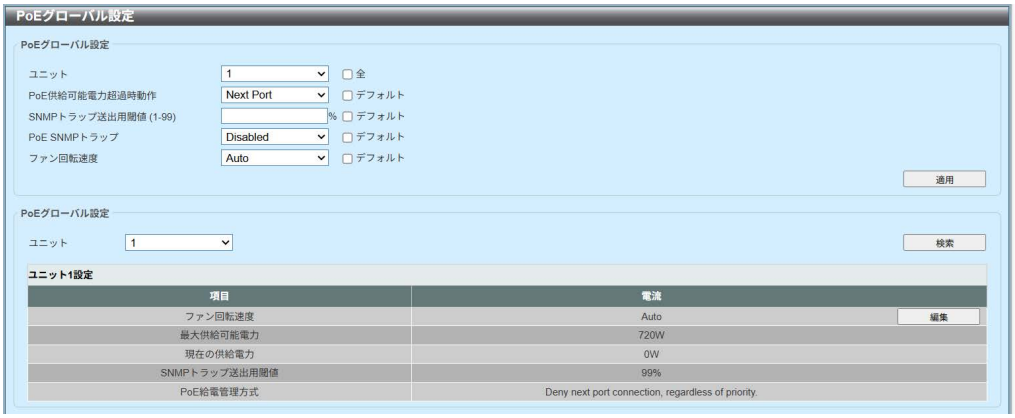

図 2-9 PoE グローバル設定

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
ユニット	ユニット ID を入力します。スタッキングした際に表示します。
PoE 供給可能電力超過時動作	給電電力が 最大給電電力 (Power Budget) を超えた際の電源給電の方法が表示されます。(初期値 : NextPort) • **NextPort** - 最大給電電力 (Power Budget) 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 トラップ送出用閾値	Trap を送信するための給電電力の閾値が表示されます。 (初期値 : 99, 設定範囲 : 1 ～ 99%)
PoE SNMP トラップ	PoE 給電トラップ（**Enabled/Disabled**）を選択します。 (Enabled : 有効化 , Disabled : 無効化 , 初期値 : Disabled)

パラメータ	概要
ファン回転速度	本装置が供給できる給電電力とファンの速度を選択します。 (初期値：Auto) • **Low** - 低速度で動作します。最大動作環境温度は 30 ℃、最大給電電力（PowerBudget）は 機種ごとで異なります。 ・XA-AML8TFPoE++ : 360W ・XA-AML16TFPoE++ : 720W • **Mid** - 中速度で動作します。最大動作環境温度は 40 ℃、最大給電電力（PowerBudget）は 機種ごとで異なります。 ・XA-AML8TFPoE++ : 360W ・XA-AML16TFPoE++ : 720W • **High** - 高速度で動作します。最大動作環境温度は 50 ℃、最大給電電力（PowerBudget）は 機種ごとで異なります。 ・XA-AML8TFPoE++ : 360W ・XA-AML16TFPoE++ : 720W • **Auto** - スイッチの動作環境温度と給電量、10G リンクアップ数に基づいてファン速度が自動的に調整しながら動作します。 各機種の動作環境と条件については下記、（補足）に記載します。

[適用] ボタン - 変更を反映します。
[電流] の下にある **[編集]** ボタンをクリックして、ファンの回転速度を設定します。

[電流] の下にある **[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。

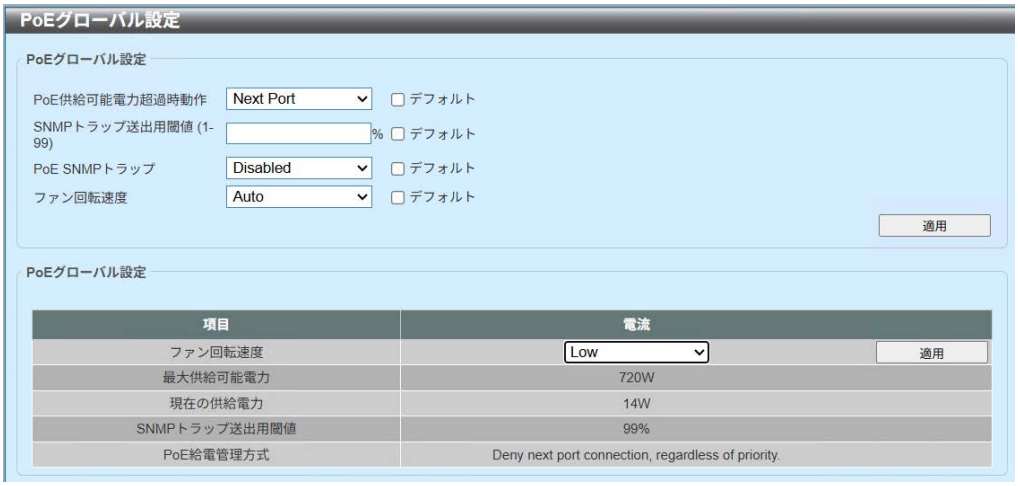

図 2-10 PoE グローバル設定 - 編集ボタン

設定パラメータ （[PoE グローバル設定 - 編集ボタン] セクション）

パラメータ	概要
ファンスピード	本装置が供給できる給電電力とファンの速度を選択します。 (初期値：Auto) • **Low** - 低速度で動作します。最大動作環境温度は 30 ℃、最大給電電力（PowerBudget）は 機種ごとで異なります。 ・XA-AML8TFPoE++ : 360W ・XA-AML16TFPoE++ : 720W • **Mid** - 中速度で動作します。最大動作環境温度は 40 ℃、最大給電電力（PowerBudget）は 機種ごとで異なります。 ・XA-AML8TFPoE++ : 360W ・XA-AML16TFPoE++ : 720W • **High** - 高速度で動作します。最大動作環境温度は 50 ℃、最大給電電力（PowerBudget）は 機種ごとで異なります。 ・XA-AML8TFPoE++ : 360W ・XA-AML16TFPoE++ : 720W • **Auto** - スイッチの動作環境温度と給電量、10G リンクアップ数に基づいてファン速度が自動的に調整しながら動作します。 各機種の動作環境と条件については下記、（補足）に記載します。

[適用] ボタン - 変更を反映します。

（補足）ファンの回転速度 (auto) を設定した場合の各機種の動作環境と条件は以下の表で表しております。

- XA-AML8TFPoE++

動作環境・条件		
動作環境温度	給電電力 （Power Budget）	10Gリンク数（最大）
50℃	360 W	8
	240 W	4
40℃	360 W	8
	240 W	4
30℃	360 W	8
	240 W	4

- XA-AML16TFPoE++

動作環境・条件		
動作環境温度	給電電力（Power Budget）	10Gリンク数（最大）
50℃	720 W	16
	540 W	12
	360 W	8
40℃	720 W	16
	540 W	12
	360 W	8
30℃	720 W	16
	540 W	12
	360 W	8

- XA-AM16T

動作環境・条件	
動作環境温度	10Gリンク数（最大）
50℃	16
	12
	8
40℃	16
	12
	8
30℃	16
	12
	8

（注意）XA-AM16T は、PoE 機能に対応していないため、PoE グローバル設定画面の詳細情報は表示されません。

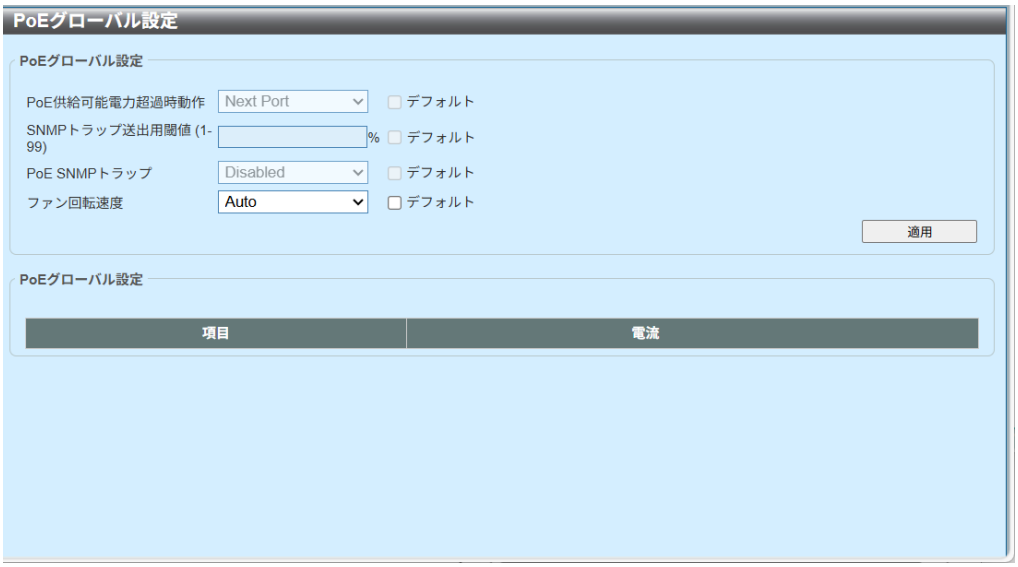

図 2-11 PoE グローバル設定（XA-AM16T）

2.4.2 PoE ポート設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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 2-12 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート - 終了ポート	設定するポートを選択します。
状態	ポートの給電 (**Enabled/Disabled**) を選択します。 [Enabled] を選択した場合、PoE ポートテーブルの給電設定では [UP] と表示され、[Disabled] を選択した場合、PoE ポートテーブルの給電設定では [DOWN] と表示されます。 (初期値 : Enable, PoE ポートテーブルの給電設定は Up)
最大供給電力	給電電力の上限を設定します。 (初期値 : Auto)
優先度	給電の優先順位を設定します。 選択する値は [Critical]、[High] および [Low] です。 (初期値 : Low)

[**適用**] ボタン - 変更を反映します。

設定パラメータ （[PoE ポートテーブル] セクション）

パラメータ	概要
開始ポート - 終了ポート	設定するポートを選択します。

[**検索**] ボタン - 指定したポートのPoE設定を検査して表示します。
[全参照]ボタン - PoE対応のすべてのポート設定を一覧で表示します。

2.4.3 PoE スケジュール

2.4.3.1 PoE スケジューラポートリスト設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] > [PoE スケジュール] > [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 2-13 PoE スケジューラポートリスト設定

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
ポートリスト番号	PoE スケジューラのポートリストのインデックス番号を設定します。
ポートメンバー	PoE スケジューラを動作させるポートを設定します。 各ポート番号はカンマ区切り (ex1,3 1.3 番ポート指定) もしくは、ハイフン (ex1-4 1-4 番ポート指定) で指定範囲を指定します。

[適用] ボタン - 変更を反映します。
[削除] ボタン - 該当項目を削除します。

2.4.3.2 PoE スケジューラ日付リスト設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

この 3 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] > [PoE スケジュール] > [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 2-14 PoE スケジューラ日付リスト設定

設定パラメータ （[PoE スケジューラ日付リスト設定] セクション）

パラメータ	概要
日付リスト番号	PoE スケジューラの日付リストのインデックス番号を設定します。(設定範囲：1 ～ 65535)
日付リスト名	PoE スケジューラの日付リストの名前を設定します。 (設定可能文字：30 文字)
年（2000-2099）	日付リストが実行される年を設定します。
月日 (MM/DD)	日付リストが実行される月日を設定します。 日付の形式は MM/DD です。 範囲を指定したい場合は、ハイフン (-) を使用します。 (ex1/10-1/15：1 月 10 日から 15 日までの範囲) 複数の日付や範囲を区切る場合は、カンマ (,) を使用します。 (ex1/23-1/25,1/27：1 月 23 日から 25 日、そして 27 日)

[適用] ボタン - 変更を反映し、PoE スケジューラ日付リストテーブルにエントリします。

2.4.3.3 PoE スケジューラ設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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 スケジュール] > [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。

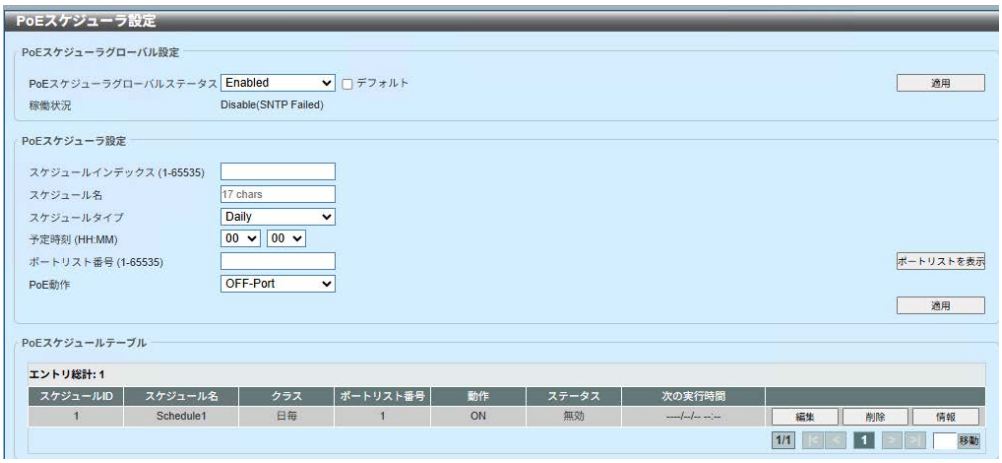

図 2-15 PoE スケジューラ設定

設定パラメータ（[PoE スケジュールグローバル設定] セクション）

パラメータ	概要
PoE スケジューラグローバルステータス	PoE スケジューラのグローバル設定 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[適用] ボタン - 変更を反映します。

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設定します。 (設定範囲：1 ～ 65535)
スケジュール名	PoE スケジュール名を設定します。(設定可能文字：17 文字)
スケジュールタイプ	PoE スケジュールのクラスを設定します。選択するオプションは以下です。 • **Monthly** - 指定した月の特定の日に PoE スケジュールを有効にします。月単位を選択した後、日付を入力します。複数の日を指定する場合は、カンマ区切り (ex 1,3 1.3 日指定) もしくは、ハイフン (ex 1-4 1-4 日指定) で範囲を指定します。(設定範囲：1 ～ 31) • **Weekly** - 指定した曜日に PoE スケジュールを有効にします。週単位を選択した後、曜日を選択します。選択肢は、月曜日から日曜日です。 • **Daily** - 毎日 PoE スケジュールを有効にします。 • **Date List** - 指定した日付リストの日に PoE スケジュールを有効にします。日付リストを選択した後、既存の日付リストの ID を入力します。(設定範囲：1 ～ 65535) もしくは、[日付リストを表示] ボタンをクリックし、使用したい既存のリストを選択します。
予定時刻	PoE スケジュールが実行される時間を設定します。
ポートリスト番号	PoE スケジュールが実行されるポートリストの番号を設定します。(設定範囲：1 ～ 65535)
PoE 動作	PoE スケジュールのアクションを表示します。選択するオプションは以下です。 • **[OFF-Port]** - PoE を無効にします。 • **[ON-Port]** - PoE を有効にします。 • **[OFF-ON-Port]** - 必要に応じて PoE を一時的に無効にしたり、有効にしたりします。

[**適用**] ボタン - 変更を反映します。

PoE スケジュールテーブルでは、以下の操作ができます。
[**編集**] ボタン - 指定した PoE スケジュールの状態を設定します。
[**削除**] ボタン - 指定した PoE スケジュールを削除します。
[**情報**] ボタン - 指定した PoE スケジュールの詳細情報を表示します。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

[ポートリストを表示] ボタンをクリックして、以下ののウィンドウを表示します。

図 2-16 PoE スケジューラ設定 _ ポートリストを表示

[**適用**] ボタン - エントリを反映します。

[**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 2-17 PoE スケジューラ設定 _ 編集ボタン押下

設定パラメータ（**[PoE スケジュールテーブル]** セクション）

パラメータ	概要
ステータス	PoE スケジュール（**有効 / 無効**）を選択します。

[**適用**] ボタン - 変更を反映します。

[**情報**] ボタンをクリックして、以下のウィンドウを表示します。

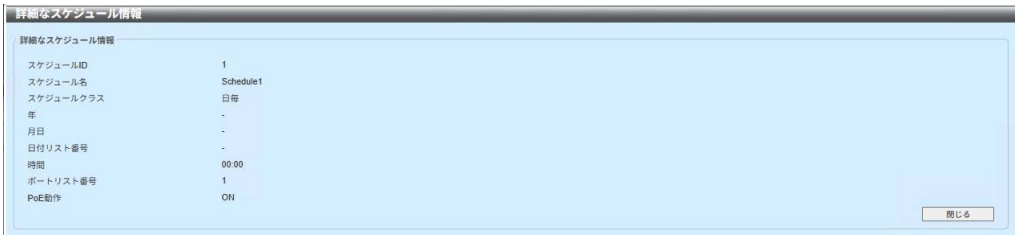

図 2-18 PoE スケジューラ設定 _ 情報

[閉じる] ボタン - ウィンドウを閉じます。

2.4.3.4 PoE スケジュールポートリストの設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

このウィンドウを用いて、PoE スケジュールポートリストの設定情報を表示します。

[システム] > [PoE] > [PoE スケジュール] > [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 2-19 PoE スケジュールポートリストの設定

設定パラメータ （[PoE スケジュールポートリストの設定] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
ポート	ポートを選択します。

[検索] ボタン - 指定したポートに関連する PoE 情報を表示します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

2.4.4 PoE オートリブート

2.4.4.1 PoE オートリブート LLDP 監視設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] > [PoE オートリブート] > [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。

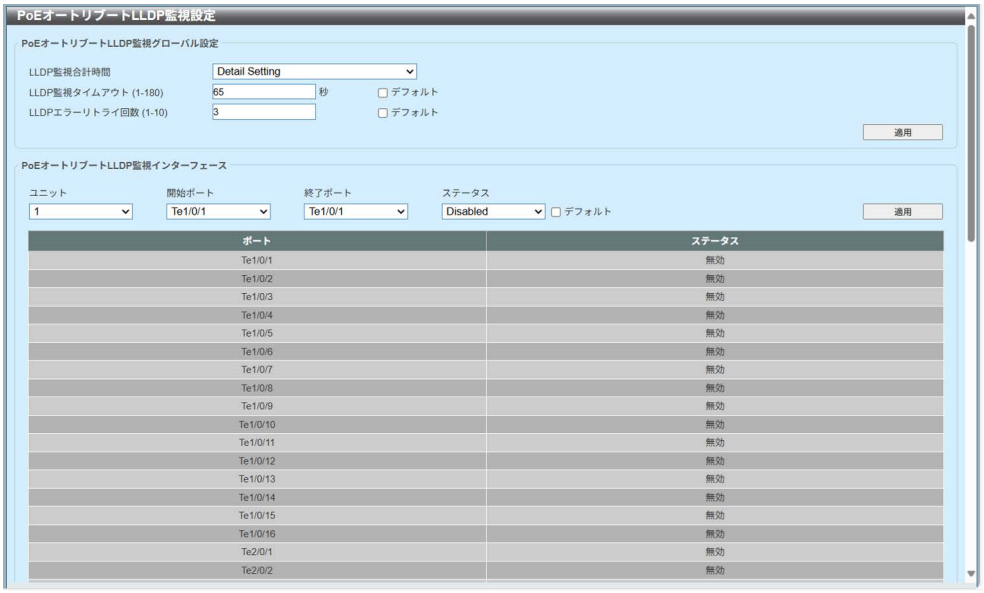

図 2-20 PoE スオートリブート LLDP 監視設定

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 監視合計時間	LLDP 監視の合計時間を設定します。 • **Detail Setting -** PoE オートリブート LLDP 監視グローバル設定の詳細設定 (LLDP 監視タイムアウト・LLDP エラーリトライ回数) をユーザ自身で設定できます。但し、Detail Setting を使用して設定した場合、LLDP 監視合計時間が表示されません。 • **360sec(LLDP Error Retry Times：6) -** LLDP 監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 360 秒後、PoE オートリブート機能が動作するように設定します。 • **480sec(LLDP Error Retry Times：8) -** LLDP 監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 480 秒後、PoE オートリブート機能が動作するように設定します。 • **600sec(LLDP Error Retry Times：10) -** LLDP 監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 600 秒後、PoE オートリブート機能が動作するように設定します。 (補足)「LLDP Error Retry Times：」はスイッチングハブに接続されている PoE デバイスの異常検知回数を表示しています。 (注意) LLDP 監視合計時間：Detail Setting で LLDP 監視合計時間：360 sec, 480 sec, 600 sec と同じ数値を適用した場合、適用後に LLDP 監視合計時間：360 sec, 480 sec, 600 sec を選択し、適用した場合、“ エラー : 個別の設定が監視時間設定と衝突しています。” というエラー文が表示され、適用されない場合がございます。
LLDP 監視タイムアウト	PoE 端末から送信される LLDP パケットを確認する時間 (秒) 設定します。(初期値：65, 設定範囲：1 ～ 180)
LLDP エラーリトライ回数	LLDP 監視の再監視回数を設定します。 (初期値：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 監視インターフェース] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート / 終了ポート	ポート番号の範囲を選択します。
ステータス	LLDP 監視のステータス（**Enabled/Disabled**）を設定します。（Enabled : 有効 , Disabled : 無効 , 初期値 : 無効）

[**適用**] ボタン - 設定内容を反映します。

2.4.4.2 PoE オートリブート Ping 監視設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] > [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。

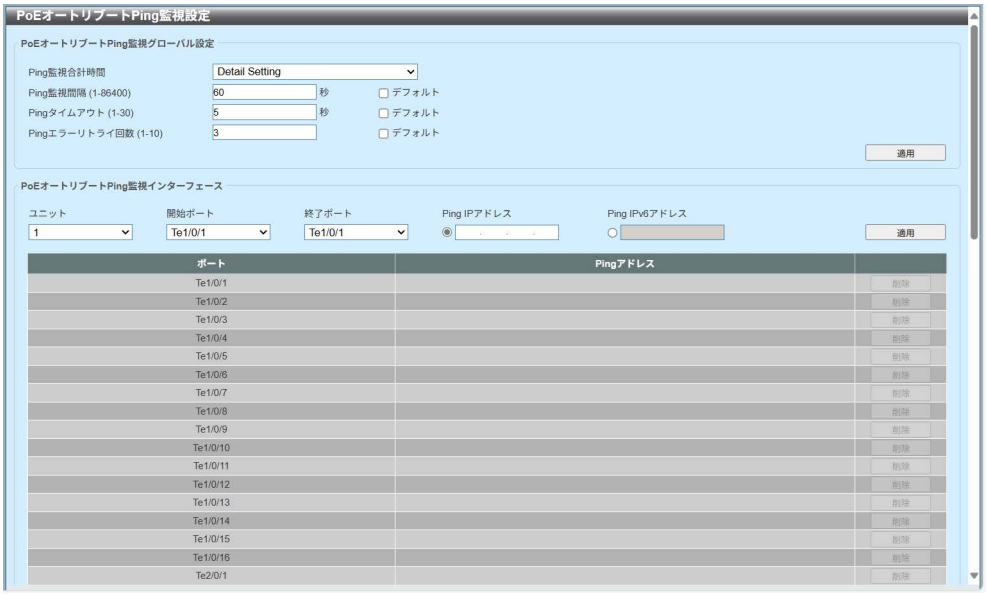

図 2-21 PoE オートリブート Ping 監視設定

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 監視合計時間	**Ping** 監視の合計時間を設定します。 • **Detail Setting -** PoE オートリブート Ping 監視グローバル設定の詳細設定 (Ping 監視間隔・Ping 監視タイムアウト・Ping エラーリトライ回数) をユーザ自身で設定できます。但し、Detail Setting を使用して設定した場合、Ping 監視合計時間が表示されません。 • **310sec(Ping Error Retry Times : 5) -** Ping 監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 310 秒後、PoE オートリブート機能が動作するように設定します。 • **490sec(Ping Error Retry Times : 8) -** Ping 監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 490 秒後、PoE オートリブート機能が動作するように設定します。 • **610sec(Ping Error Retry Times : 10) -** Ping 監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 610 秒後、PoE オートリブート機能が動作するように設定します。 (補足)「Ping Error Retry Times : 」はスイッチングハブに接続されている PoE デバイスの異常検知回数を表示しています。 (注意) Ping 監視合計時間 : Detail Setting で Ping 監視合計時間 : 310 sec, 490 sec, 610 sec と同じ数値を適用した場合、適用後に Ping 監視合計時間 : 310 sec, 490 sec, 610 sec を選択し、適用した場合、" エラー : 個別の設定が監視時間設定と衝突しています。" というエラー文が表示され、適用されない場合がございます。
Ping 監視間隔	PoE オートリブート Ping 監視の時間 (秒) を設定します。 （初期値 : 60, 設定範囲 : 1 ～ 86400）
Ping タイムアウト	スイッチングハブから PoE 端末に対して、Ping を送信し、PoE 端末からの応答を確認する時間 (秒) を設定します。 （初期値 : 5, 設定範囲 : 1 ～ 30）
Ping エラーリトライ回数	Ping 監視を実行し、PoE 端末の異常を検知した時の再監視実行回数を設定します。（初期値 : 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 監視インターフェース] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート / 終了ポート	ポート番号の範囲を選択します。
Ping IP アドレス	Ping 監視対象の IPv4 アドレスを設定します。 (設定範囲 : クラス D, E とループバックアドレス以外は設定可能です。 設定範囲の例として、 10.0.0.0 ～ 10.255.255.255, 172.16.0.0 ～ 172.31.255.255, 192.168.0.0 ～ 192.168.255.255 初期値 : なし)
Ping IPv6 アドレス	Ping 監視対象の IPv6 アドレスを設定します。 (設定範囲 : マルチキャストアドレス以外は設定可能です。 設定範囲の例として、 2000:: ～ 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF FE80:: ～ FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF FEC0:: ～ FEFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 初期値 : なし)

[**適用**] ボタン - 設定内容を反映します。
[**削除**] ボタン - 設定されている IPv4 または IPv6 アドレスをポートから削除します。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください :
例 : インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

2.4.4.3 PoE オートリブートトラフィック監視設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] > [PoE オートリブート] > [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。

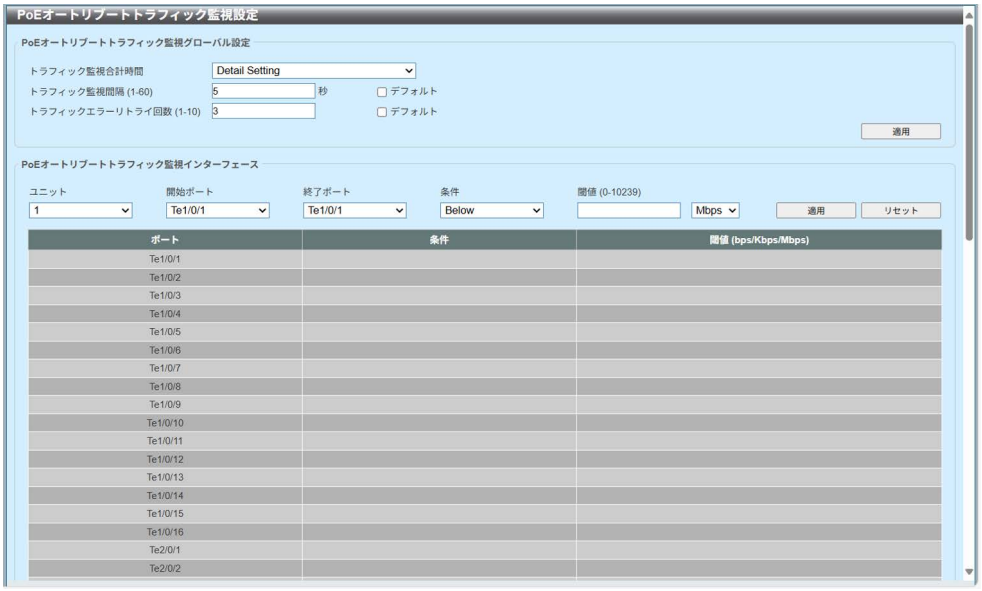

図 2-22 PoE オートリブートトラフィック監視設定

設定パラメータ
（**[PoE 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 合計時間	トラフィック監視の合計時間を設定します。 • **Detail Setting -** PoE オートリブートトラフィック監視グローバル設定の詳細設定 (トラフィック監視間隔・トラフィックエラーリトライ回数) をユーザ自身で設定できます。但し、Detail Setting を使用して設定した場合、トラフィック監視合計時間が表示されません。 • **360sec(Traffic Error Retry Times：6) -** トラフィック監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 360 秒後、PoE オートリブート機能が動作するように設定します。 • **480sec(Traffic Error Retry Times：8) -** トラフィック監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 480 秒後、PoE オートリブート機能が動作するように設定します。 • **600sec(Traffic Error Retry Times：10) -** トラフィック監視を動作させ、スイッチングハブに接続されている PoE デバイスに異常が発生して 600 秒後、PoE オートリブート機能が動作するように設定します。 (補足)「Traffic Error Retry Times：」はスイッチングハブに接続されている PoE デバイスの異常検知回数を表示しています。 (注意) トラフィック監視合計時間：Detail Setting でトラフィック監視合計時間：360 sec, 480 sec, 600 sec と同じ数値を適用した場合、適用後にトラフィック監視合計時間：360 sec, 480 sec, 600 sec を選択し、適用した場合、“ エラー：個別の設定が監視時間設定と衝突しています。” というエラー文が表示され、適用されない場合がございます。
トラフィック監視間隔	PoE 端末から受信したトラフィック量を測定し、平均値を算出する時間 (秒) を秒単位で設定します。 （初期値：5, 設定範囲：1 ～ 60）
トラフィックエラーリトライ回数	トラフィック監視の再監視回数を設定します。 (初期値：3, 設定範囲：1 ～ 10)

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ーフェース] セクション)

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート / 終了ポート	ポート番号の範囲を選択します。
条件	PoE 端末から受信したトラフィック量による PoE 端末異常判定（**Below/Over**）を設定します。 (Below：閾値以下 , Over：閾値以上 , 初期値：Below)
閾値	PoE 端末から受信したトラフィック量の平均値（トラフィック監視間隔における平均値）の閾値を設定します。閾値入力ボックスの隣に単位の選択ボックスがあり、ユーザが自由に単位を変更できます。 • **bps** - 閾値を bps で設定します。 (設定範囲：0 ～ 10737418239 bps) • **Kbps** - 閾値を Kbps で設定します。 (設定範囲：0 ～ 10485759 Kbps) • **Mbps** - 閾値を Mbps で設定します。この単位が初期値となります。 (設定範囲：0 ～ 10239 Mbps)

[**適用**] ボタン - 設定内容を反映します。
[**リセット**] ボタン - 設定内容を削除します。

2.4.4.4 PoE オートリブート SMTP 設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] > [PoE オートリブート] > [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 2-23 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]** 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設定します。(設定可能文字：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設定します。(設定可能文字：256 文字)

2.4.4.5 PoE オートリブートインターフェース設定 [XA-AML8TFPoE++/XA-AML16TFPoE++]

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] > [PoE オートリブート] > [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。

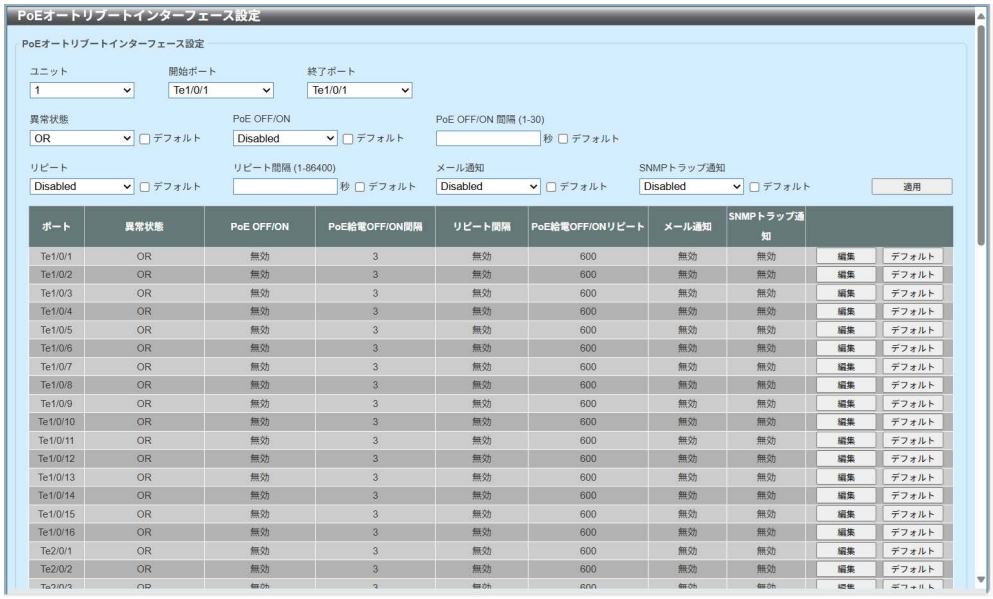

図 2-24 PoE オートリブートインターフェース設定

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

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート / 終了ポート	ポート番号の範囲を選択します。
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を設定します。以下のオプションから選択します。 • **OR** - いずれかの監視で異常判定します。このオプションが初期値となります。 • **And** - 全監視で異常判定します。
PoE OFF/ON	PoE 端末の異常時に実行する PoE 給電の OFF/ON 状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
PoE OFF/ON 間隔	PoE 端末の異常時に実行する PoE 給電の OFF/ON 実行時間を秒単位で設定します。 (初期値 : 3 秒 , 設定範囲 : 1 ～ 30 秒)

パラメータ	概要
リピート	PoE 端末の異常時に PoE 給電の OFF/ON を繰り返し実行する状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
リピート間隔	PoE 端末の異常時に PoE 給電の OFF/ON を繰り返し実行する間隔を秒単位で設定します。 (初期値 : 600 秒 , 設定範囲 : 1 ～ 86400 秒)
メール通知	PoE 端末の異常時に SMTP サーバを経由したメールの送信状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
SNMP トラップ通知	PoE 端末の異常時に SNMP トラップの送信状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)

[適用] ボタン - 設定内容を反映します。

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

図 2-25 PoE オートリブートインターフェース設定 (編集)

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

パラメータ	概要
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を設定します。以下のオプショから選択します。 • **OR** - いずれかの監視で異常判定をします。この設定が初期値となります。 • **AND** - 全監視で異常判定をします。
PoE OFF/ON	PoE 端末の異常時に実行する PoE 給電の OFF/ON 状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
PoE OFF/ON 間隔	PoE 端末の異常時に実行する PoE 給電の OFF/ON 実行時間を秒単位で設定します。 (初期値 : 3 秒 , 設定範囲 : 1 ～ 30 秒)

パラメータ	概要
リピート	PoE 端末の異常時に PoE 給電の OFF/ON を繰り返し実行する状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
リピート間隔	PoE 端末の異常時に PoE 給電の OFF/ON を繰り返し実行する間隔（秒）を設定します。 (初期値 : 600, 設定範囲 : 1 ～ 86400)
メール通知	PoE 端末の異常時に SMTP サーバを経由したメールの送信状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
SNMP トラップ通知	PoE 端末の異常時に SNMP トラップの送信状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)

(注意)
・編集ボタン押下後の画面では、個別に設定変更が可能です。
・適用ボタン押下後、図 2-24 PoE オートリブートインターフェース設定画面に移動します。
・移動後、ステータス一覧表には編集ボタン押下後の画面で設定した内容で表示されます。
[適用] ボタンをクリックして、変更を反映します。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - PoE オートリブートインターフェース設定画面に戻ります。

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

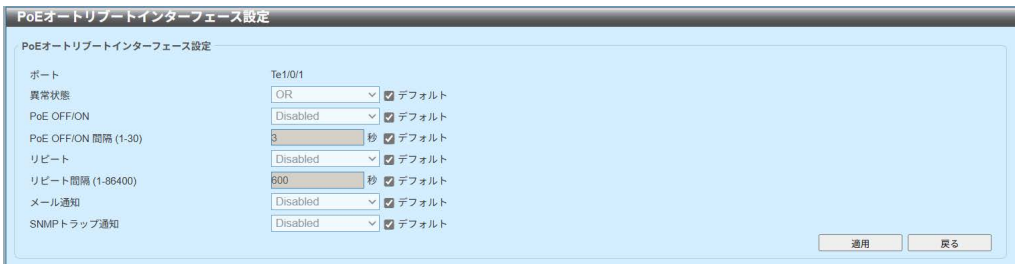

図 2-26 PoE オートリブートインターフェース設定 (デフォルト)

設定パラメータ (**[PoE オートリブートインターフェース設定 (デフォルト)]** セクション)

パラメータ	概要
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を設定します。以下のオプションから選択します。 • **OR** - いずれかの監視で異常判定をします。この設定が初期値となります。 • **AND** - 全監視で異常判定をします。

パラメータ	概要
PoE OFF/ON	PoE 端末の異常時に実行する PoE 給電の OFF/ON 状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
PoE OFF/ON 間隔	PoE 端末の異常時に実行する PoE 給電の OFF/ON 実行時間を秒単位で設定します。(初期値 : 3, 設定範囲 : 1 ～ 30)
リピート	PoE 端末の異常時に PoE 給電の OFF/ON を繰り返し実行する状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
リピート間隔	PoE 端末の異常時に PoE 給電の OFF/ON を繰り返し実行する間隔を秒単位で設定します。 (初期値 : 600 秒 , 設定範囲 : 1 ～ 86400 秒)
メール通知	PoE 端末の異常時に SMTP サーバを経由したメールの送信状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)
SNMP トラップ通知	PoE 端末の異常時に SNMP トラップの送信状態（**Enabled/Disabled**）を選択します。 (Enabled: 有効化 , Disabled: 無効化 , 初期値 : Disabled)

(注意)
・デフォルトボタン押下後の画面では、すべての設定でデフォルトチェックボックスがついた状態で表示されます。
・適用ボタン押下後、図 2-24PoE オートリブートインターフェース設定画面に移動します。移動後、ステータス一覧表にはすべての設定がデフォルト値で表示されます。
・デフォルトボタン押下後の画面でデフォルトのチャックボックスを外した場合、設定変更と変更した設定内容で適用することも可能です。移動後、ステータス一覧表には変更した設定内容で表示されます。

[**適用**] ボタン - 設定内容を反映します。
[**戻る**] ボタン - PoE オートリブートインターフェース設定画面に戻ります。

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。

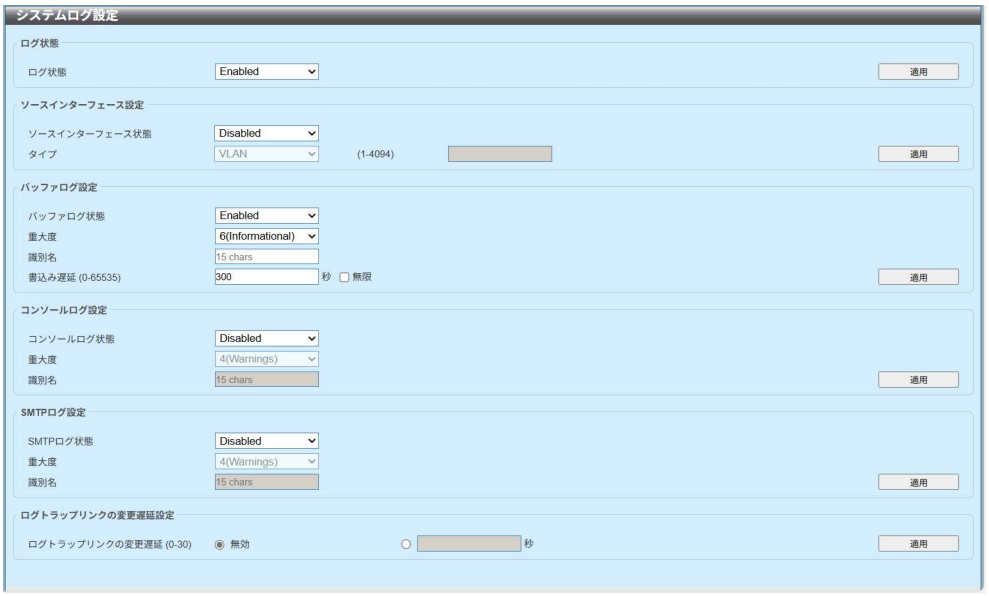

図 2-27 システムログ設定

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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ソースインターフェース設定] セクション）

パラメータ	概要
ソースインターフェース状態	ソースインターフェース状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
タイプ	インターフェースのタイプの（**Loopback** / **VLAN**）を選択します。(初期値 : VLAN)

[**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。「既定（Default)」を選択した場合、グローバルなバッファログの状態はシステムの既定の動作となります。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)
重大度	ログ記録する情報の重大度（**0**（**Emergencies**）/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。 (初期値 : 6 (Informational))
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。（設定可能文字：15 文字）
書込み遅延	ログの書き込み遅延値を秒単位で入力します。 [**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。（初期値：300 秒 , 設定範囲：0 ～ 65535 秒）

[**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**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
重大度	ログ記録する情報の重大度（**0**（**Emergencies**）/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。 (初期値 : 4 (Warnings))

パラメータ	概要
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。(設定可能文字：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**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
重大度	ログ記録する情報の重大度（**0**（**Emergencies**/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**)）を選択します。 (初期値 : 4 (Warnings))
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。 (設定可能文字：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 トラップの通知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。 (初期値：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 2-28 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。 (設定可能文字：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（**Drops**/**Includes**）およびファシリティのタイプを選択します。
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。 (Drops：破棄 , Includes：含む)

[**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 2-29 システムログサーバ設定

設定パラメータ （[ログサーバ] 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。 **（注意）**FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください： 例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。 FE80::200:FF:FE00%vlan1
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。 （初期値：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。 (初期値 : 4 (Warnings))

<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。
(設定可能文字：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。

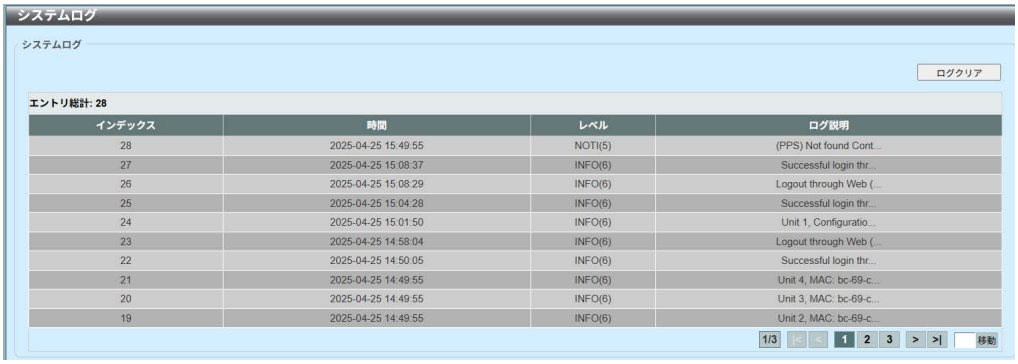

図 2-30 システムログ

[**ログクリア**] ボタン - ログエントリをクリアします。
複数のページがある場合は、ページ番号を入力して [**移動**] ボタンをクリックすることで、特定のページに移動できます。

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 2-31 システムアタックログ

設定パラメータ （[システムアタックログ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

[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。

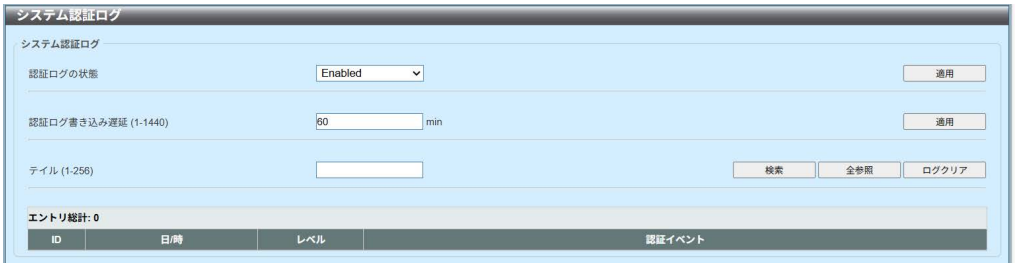

図 2-32 システム認証ログ

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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)
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。 （初期値 : 60min, 設定範囲：1 ～ 1440 分）
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、スイッチの時刻設定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。

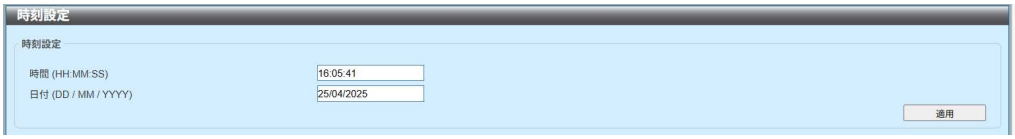

図 2-33 時刻設定

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。

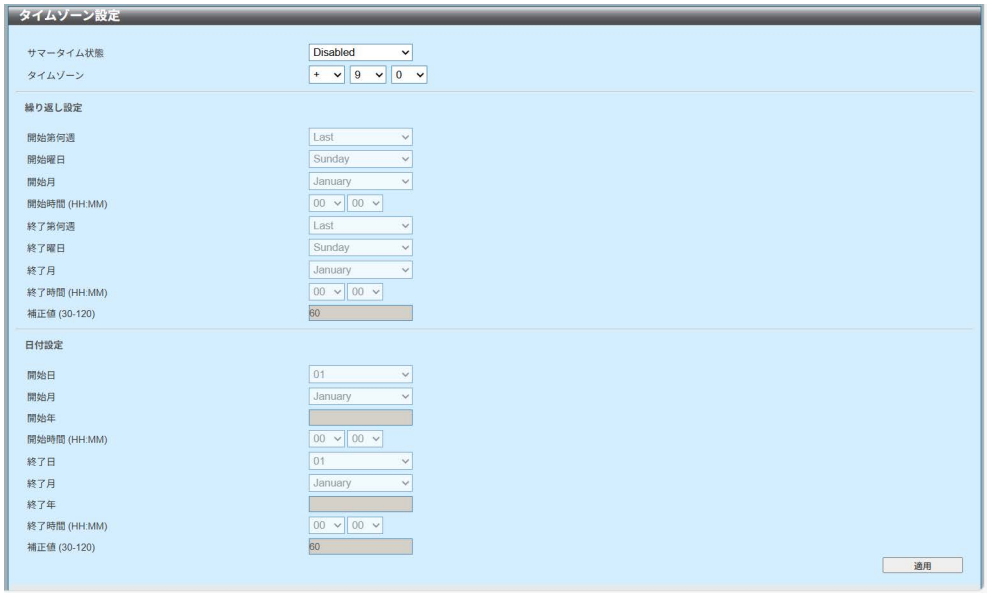

図 2-34 タイムゾーン設定

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。(初期値 : Disabled) • **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。(初期値 : +, 9, 0)

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。
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。 （初期値：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。 （初期値：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 2-35 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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
ポール間隔	同期間隔（秒）を入力します。 （初期値：720, 設定範囲：30 ～ 99999 秒）

[**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。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを
使用する場合は、以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

2.7 時間範囲

このウィンドウを用いて、時間範囲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 2-36 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	時間範囲プロファイルの名前を入力します。 (設定可能文字：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 - 範囲名プロファイルに紐づいた周期の設定 (開始週日以降) を個別に削除します。
[**削除**] ボタン - 範囲名プロファイル自体を削除します。

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。スイッチの設定変更を伴わないコマンド入力の場合、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。

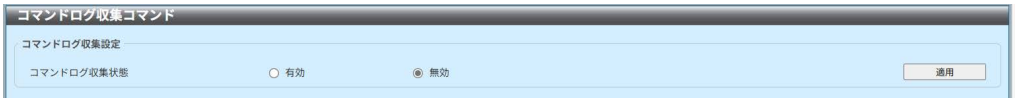

図 3-1 コマンドログ収集コマンド

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。 (初期値 : 無効)

[**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。(設定可能文字 : 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。 (設定可能文字 : Plain Text: 32 文字 , Encrypted - SHA1: 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。

[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）

複数のページがある場合は、ページ番号を入力して [**移動**] ボタンをクリックすることで、特定のページに移動できます。

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。 (初期値 : 無効)

[**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。

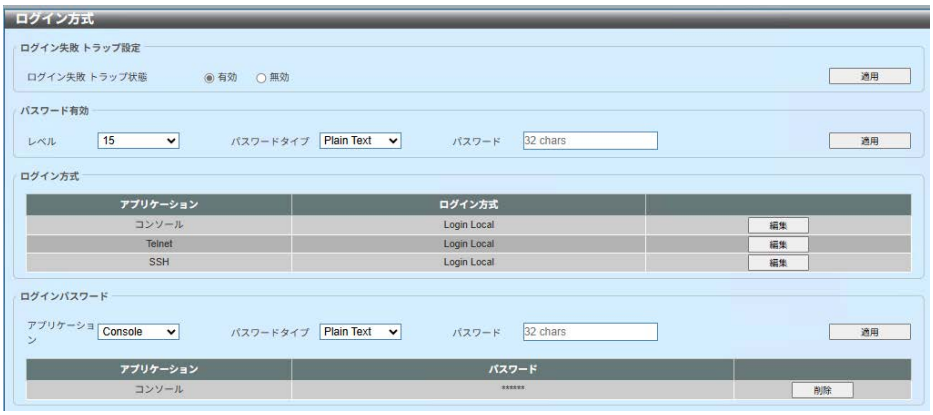

図 3-5 ログイン方式

設定パラメータ ([ログイン失敗 トラップ設定] セクション)

パラメータ	概要
ログイン失敗トラップ設定	ログイン失敗トラップの状態を (**有効 / 無効**) を選択します。 (初期値 : 無効)

[**適用**] ボタン - 設定内容を変更します。

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。 (初期値 : 15)
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。 (初期値 : 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。

パラメータ	概要
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** - 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。(設定可能文字：32 文字) • **Encrypted**- 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。(設定可能文字：35 文字)

[**適用**] ボタン - 設定内容を反映します。

[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 3-6 ログイン方式 (編集)

設定パラメータ （[ログイン方式]>[編集] 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。

[**編集**] ボタン - エントリの設定を編集できます。
[**適用**] ボタン - 変更を適用します。

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。(設定可能文字：32 文字) • **Encrypted -** 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。(設定可能文字：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、SNMP グローバル設定を行い、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。

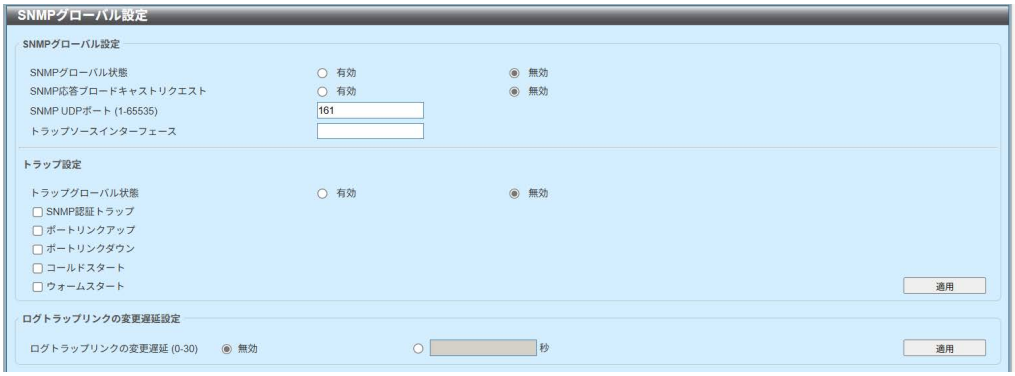

図 3-7 SNMP グローバル設定

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。 (初期値 : 無効)
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。 (初期値 : 無効)
SNMP UDP ポート	SNMP UDP ポート番号を入力します。 (初期値 : 161, 設定範囲 : 1 ～ 65535)
トラップソースインターフェース	SNMP トラップパケットを送信するためのソースアドレスとして使用される IP アドレスを持つインターフェースを入力します。

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	トラップパケットの送信の状態（**有効** / **無効**）を選択します。(初期値 : 無効)
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 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。
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 トラップの通知遅延を有効にします。範囲は、0 ～ 30 秒 (0 を設定すると無効になります) です。本製品でリンクアグリゲ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。 (初期値：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 リンクチェンジ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。

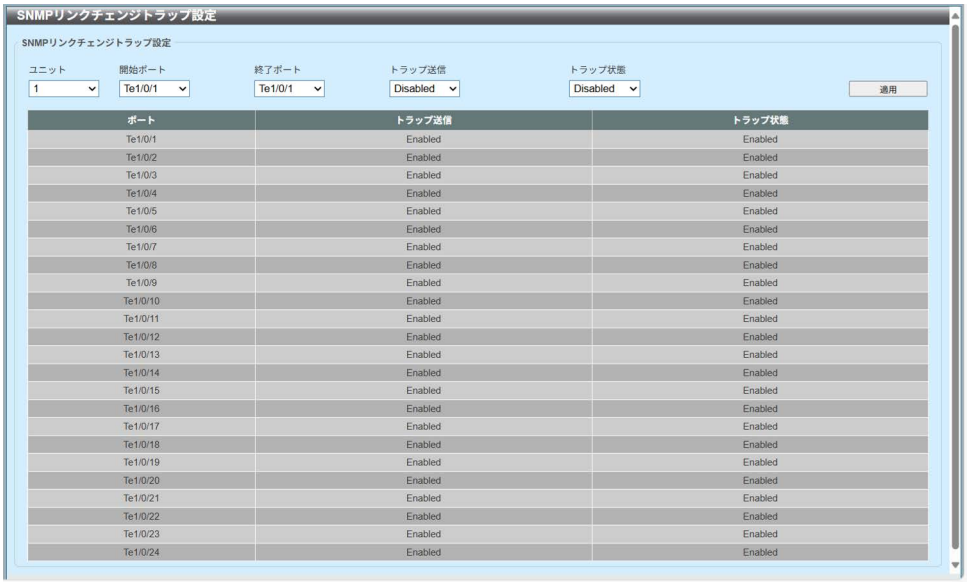

図 3-8 SNMP リンクチェンジトラップ設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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	システムで生成されたすべての SNMP 通知トラップ送信の状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 :Enabled)
トラップ状態	リンク状態の変化 (linkchange) に関する SNMP トラップの送信（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)

[**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 3-9 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。（設定可能文字：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。

SNMP ビュー (デフォルト エントリ)

ビュー名	サブツリー OID	ビュータイプ
restricted	1.3.6.1.2.1.1	**Included**
restricted	1.3.6.1.2.1.11	**Included**
restricted	1.3.6.1.6.3.10.2.1	**Included**
restricted	1.3.6.1.6.3.11.2.1	**Included**
restricted	1.3.6.1.6.3.15.1.1	**Included**
CommunityView	1	**Included**
CommunityView	1.3.6.1.6.3	**Excluded**
CommunityView	1.3.6.1.6.3.1	**Included**

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 3-10 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。（Plain Text を選択時は設定可能文字：32 文字 /Encrypted を選択時は設定可能文字：35 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。（設定可能文字：32 文字）
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。(設定可能文字：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。

コミュニティーテーブル (デフォルト)

コミュニティー名	ビュー名	アクセス権	IP アクセスリスト名
public	CommunityView	ro	-
private	CommunityView	rw	-

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 3-11 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。(設定可能文字：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。(設定可能文字 : 32 文字)
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。(設定可能文字：32 文字)

パラメータ	概要
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ないことを指定します。 • **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は暗号化されないことを指定します。 • **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は暗号化を指定します。
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通知できるオブジェクトを記述します。 (設定可能文字：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。 (設定可能文字：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。

SNMP グループ設定 (デフォルト)

グループ名	読み取りビュー名	ライタービュー名	通知ビュー名	セキュリティモデル	セキュリティレベル	IPアドレスリスト名
public	Community View	-	Community View	v1	-	-
public	Community View	-	Community View	v2c	-	-
initial	restricted	-	restricted	v3	NoAuthNoPriv	-
private	Community View	Community View	Community View	v1	-	-
private	Community View	Community View	Community View	v2c	-	-

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。

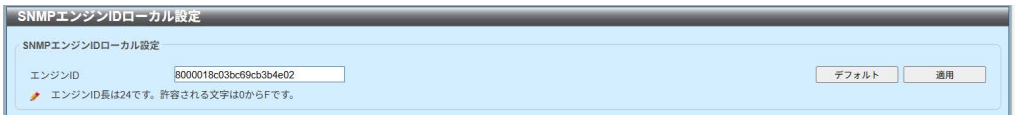

図 3-12 SNMP エンジン ID ローカル設定

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。 （設定可能文字：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 3-13 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。（設定可能文字：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。（設定可能文字：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。 • **SHA** - HMAC-SHA 認証プロトコルを使用します。
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）

パラメータ	概要
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。 • **SHA** - HMAC-SHA 認証プロトコルを使用します。
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)
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。 (設定可能文字 :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。

3.5.8 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 3-14 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。 （注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください： 例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。 FE80::200:FF:FE00%vlan1
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。

パラメータ	概要
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** - 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に対して、認証も暗号化も行いません。 • **AuthNoPriv** - 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に対して、認証は必要ですが、暗号化は行いません。 • **AuthPriv** - 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に対して、認証と暗号化の両方を行います。
UDP ポート	UDP ポート番号を入力します。 (初期値：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。(設定可能文字：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。

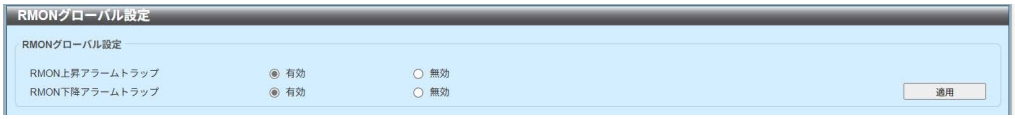

図 3-15 RMON グローバル設定

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。(初期値 : 有効)
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。(初期値 : 有効)

[**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。

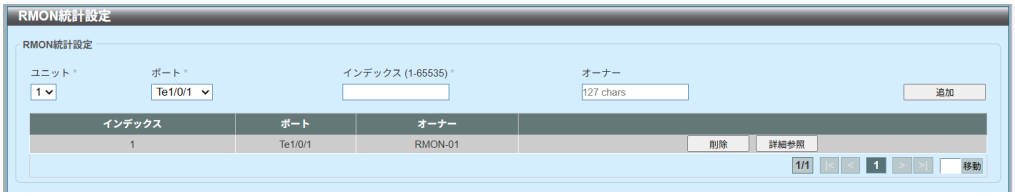

図 3-16 RMON 統計設定

設定パラメータ （[RMON 統計設定] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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	オーナーの名前を文字列で入力します。 （設定可能文字：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。

複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

[詳細参照] 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 3-17 RMON 統計設定 (詳細参照)

[**戻る**] ボタン - 前の画面に戻ります。

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。

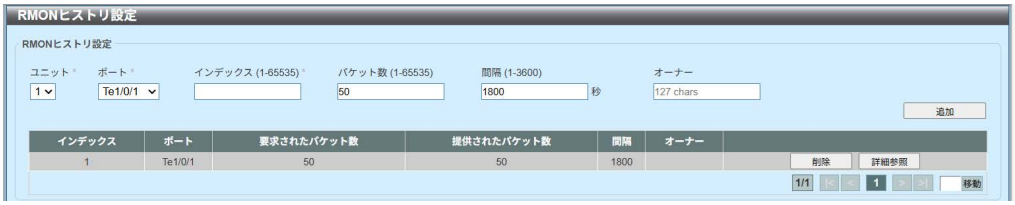

図 3-18 RMON ヒストリ設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 ヒストリで収集される統計データを保存するパケットの数を入力します。 （初期値：50, 設定範囲：1 ～ 65535）
間隔	各ポーリング周期の間隔時間を秒単位で入力します。 （初期値 : 1800 秒 , 設定範囲：1 ～ 3600 秒）
オーナー名	オーナーの名前を文字列で入力します。 （設定可能文字：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。

[詳細参照] をクリックして、以下のウィンドウを表示します。

図 3-19 RMON ヒストリ設定 (詳細参照)

[戻る] ボタン - 前のウィンドウに戻ります。

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 3-20 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。
上限閾値	上限閾値を入力します。（設定範囲：0 ～ 2147483647）
下限閾値	下限閾値を入力します。（設定範囲：0 ～ 2147483647）
上限超過時イベント No	上限閾値を超えた際に通知を行うためのイベントエントリのインデックスを入力します。このインデックスは、[RMON イベント設定] で事前に設定されたイベントエントリの番号を指定します。インデックスを指定しない場合、上限閾値を超えても通知などのアクションは実行されません。 （設定範囲：1 ～ 65535）
下限超過時イベント No	下限閾値を下回った際に通知を行うためのイベントエントリのインデックスを入力します。このインデックスは、[RMON イベント設定] で事前に設定されたイベントエントリの番号を指定します。インデックスを指定しない場合、下限閾値を下回っても、通知などのアクションは実行されません。 （設定範囲：1 ～ 65535）
オーナー名	オーナーの名前を文字列で入力します。 （設定範囲：1 ～ 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 3-21 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。 （設定範囲：1 ～ 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。[タイプ] パラメータで「Trap」または「Log and Trap」を選択した場合に入力します。（設定範囲：1 ～ 127 文字）
オーナー名	オーナーの名前を文字列で入力します。 （設定範囲：1 ～ 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。
[**ビューログ**] ボタン - エントリのイベントログテーブルを表示します。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

[ビューログ] ボタンをクリックして、以下のウィンドウを表示します。

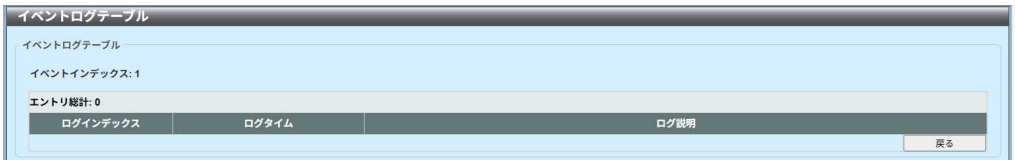

図 3-22 RMON イベント設定 (イベントログテーブル)

[戻る] ボタン - 前のウィンドウに戻ります。

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 3-23 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。 (初期値 : 無効)
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。 （初期値 : 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。 (初期値 : 無効)
TCP ポート	装置の WEB 管理に使用する TCP ポート番号を入力します。 （初期値 : 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。

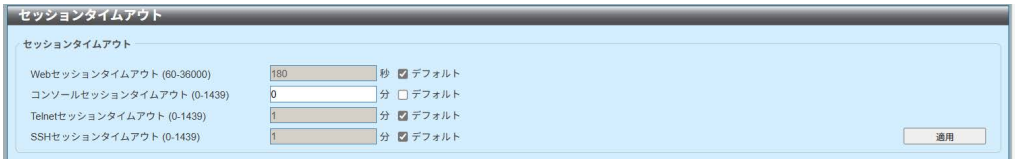

図 3-24 セッションタイムアウト

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。 （初期値：180, 設定範囲：60 ～ 36000 秒）
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。 （初期値：3 分 , 設定範囲：0 ～ 1439 分）
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。 （初期値：3 分 , 設定範囲：0 ～ 1439 分）
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。 （初期値：3 分 , 設定範囲：0 ～ 1439 分）

[**適用**] ボタン - 設定内容を反映します。

3.9 DHCP (Dynamic Host Configuration Protocol)

3.9.1 サービス DHCP

このウィンドウを用いて、DHCP および DHCPv6 のサービス機能を有効または無効にします。DHCPv6 は Dynamic Host Configuration Protocol Version 6 または Dynamic Host Configuration Protocol for IPv6 の略です。

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

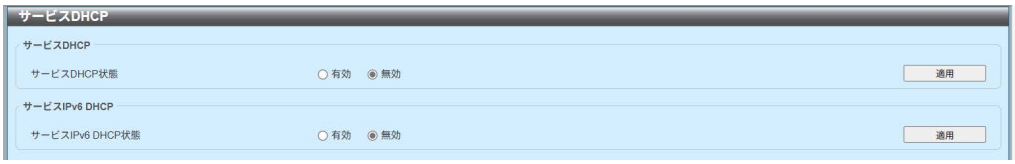

図 3-25 サービス DHCP

設定パラメータ （[サービス DHCP] セクション）

パラメータ	概要
サービス DHCP 状態	DHCP サービス状態 (**有効 / 無効**) を選択します。 (初期値 : 無効)

[適用] ボタン - 変更を反映します。

設定パラメータ （[サービス IPv6 DHCP] セクション）

パラメータ	概要
サービス IPv6 DHCP 状態	DHCPv6 サービス状態 (**有効 / 無効**) を選択します。 (初期値 : 無効)

[適用] ボタン - 変更を反映します。

3.9.2 DHCP クラス設定

このウィンドウを用いて、DHCP クラスの設定を行い、設定値を表示します。

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

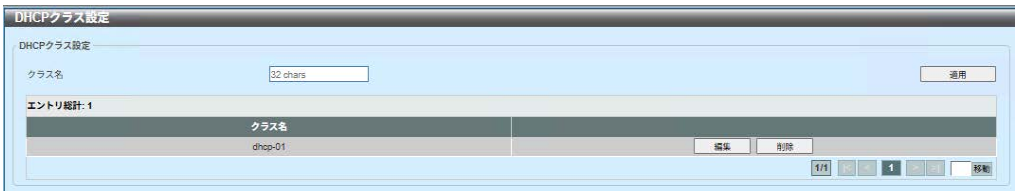

図 3-26 DHCP クラス設定

設定パラメータ （[DHCP クラス設定] セクション）

パラメータ	概要
クラス名	DHCP クラス名を入力します。 (設定可能文字 : 32 文字)

[適用] ボタン - 指定した情報に基づいて新しい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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[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 3-27 DHCP クラス設定（編集）

設定パラメータ （[DHCP クラスオプション設定] セクション）

パラメータ	概要
オプション	DHCP オプション番号を入力します。(設定範囲：1 ～ 254)
16 進数	指定した DHCP オプションの 16 進数パターンを入力します。チェックボックスをオンにした場合、オプションの残りのビットを無視します。
ビットマスク	パターンをマスクするビットマスクを 16 進数で入力します。マスクされたパターンのビットが照合されます。指定しない場合、**[16 進数]** フィールドに入力したすべてのビットがチェックされます。

[適用] ボタン - 指定した情報に基づいて新しい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。

3.9.3 DHCP プール設定

このウィンドウを用いて、DHCP プールの設定を行い、設定値を表示します。

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

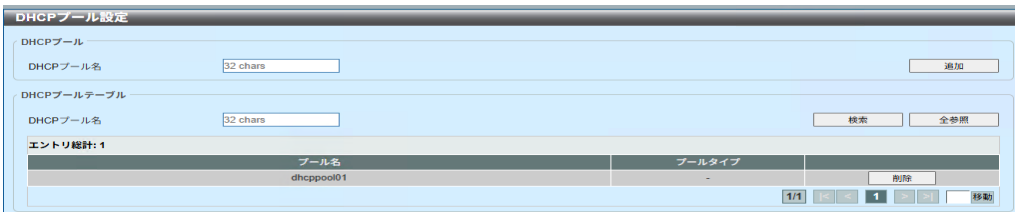

図 3-28 DHCP プール設定

設定パラメータ （[DHCP プール] セクション）

パラメータ	概要
DHCP プール名	DHCP プール名を入力します。 (設定可能文字：32 文字)

[追加] ボタン - 指定した情報に基づいて新しいエントリを追加します。

設定パラメータ （[DHCPプールテーブル]セクション）

パラメータ	概要
DHCP プール名	DHCP プール名を入力します。 (設定可能文字：32 文字)

[検索] - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
[削除] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

3.9.4 DHCP サーバ

3.9.4.1 DHCP サーバグローバル設定

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

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

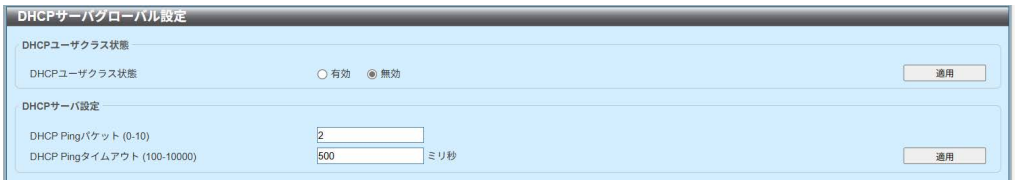

図 3-29 DHCP サーバグローバル設定

設定パラメータ （[DHCP ユーザクラス状態] セクション）

パラメータ	概要
DHCP ユーザクラス状態	DHCP ユーザクラス状態 (**有効 / 無効**) を選択します。有効にすると、DHCP サーバが DHCP クラスを用いてアドレスの割り当てを実行します。 (初期値 : 無効)

[適用] ボタン - 変更を反映します。

設定パラメータ （[DHCP サーバ設定] セクション）

パラメータ	概要
DHCP Ping パケット	割り当てる IP アドレスを含むネットワーク上でスイッチが送出する ping パケットの数を入力します。ping リクエストに応答がない場合、IP アドレスはローカルネットワークに一意であるとみなされ、リクエスト元のクライアントに割り当てられます。0 は、ping テストを実行しないことを意味します。 (初期値 : 2, 設定範囲は 0 ～ 10)
DHCP Ping タイムアウト	ping パケットがタイムアウトするまでに DHCP サーバが待機する時間を入力します。 (初期値 : 500, 設定範囲 : 100 ～ 10000 ミリ秒)

[適用] ボタン - 変更を反映します。

3.9.4.2 DHCP サーバプール設定

このウィンドウを用いて、DHCP サーバプール設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCP サーバ] > [DHCP サーバプール設定] をクリックして、以下のウィンドウを表示します。

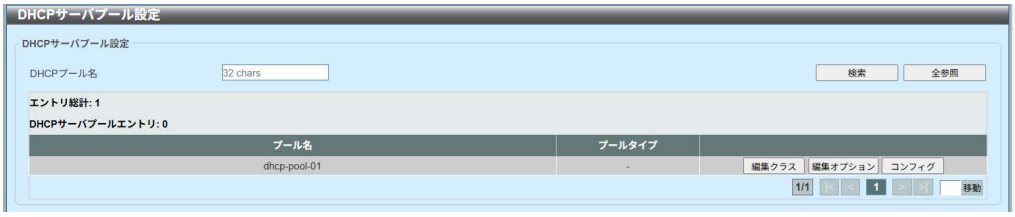

図 3-30 DHCP サーバプール設定

設定パラメータ （[DHCP サーバプール設定] セクション）

パラメータ	概要
DHCP プール名	DHCP サーバプール名を入力します。 (設定可能文字：32 文字)

[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
[編集クラス] ボタン - 指定したエントリに関連する DHCP クラスの設定を編集します。
[編集オプション] ボタン - 指定したエントリに関連する DHCP オプションの設定を編集します。
[コンフィグ] ボタン - 指定したエントリに関連する DHCP の設定を行います。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[編集クラス] 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 3-31 DHCP サーバプール設定（編集クラス）

設定パラメータ （[DHCP サーバプールクラス設定] セクション）

パラメータ	概要
クラス名	この DHCP プールに関連付ける既存の DHCP クラス名を選択します。
開始アドレス	DHCP プール内の DHCP クラスに関連付ける開始 IPv4 アドレスを入力します。実際に必要な操作としては、[DHCP サーバプールコンフィグ] セクションにて、以下パラメータを設定する必要があります。 • ネットワーク (IP/ マスク)
最終アドレス	DHCP プール内の DHCP クラスに関連付ける終了 IPv4 アドレスを入力します。実際に必要な操作としては、[DHCP サーバプールコンフィグ] セクションにて、以下パラメータを設定する必要があります。 • ネットワーク (IP/ マスク)

[適用] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[名前単位削除] ボタン - エントリを削除します。
[アドレス単位削除] ボタン - 設定済みの開始および終了アドレスをエントリから削除します。
[戻る] ボタン - 前のウィンドウに戻ります。

[編集オプション] 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 3-32 DHCP サーバプール設定（編集オプション）

設定パラメータ （[DHCP サーバプールオプション設定] セクション）

パラメータ	概要
オプション	DHCP オプション番号を入力します。(設定範囲 : 1 ～ 254)
タイプ	DHCP オプションのタイプを選択します。選択する値は以下のとおりです。 • **[ASCII]** - ASCII（American Standard Code for Information Interchange）文字列を表示された入力フィールドに入力します。(設定可能文字 : 255 文字) • **[HEX]** - 16 進数の文字列を表示された入力フィールドに入力します。(設定可能文字 : 254 文字) **[なし]** を選択した場合、長さ 0 の 16 進数文字列を指定します。 • **[IP]** - IPv4 アドレスを表示された入力フィールドに入力します。最大で 8 個の IPv4 アドレスを入力できます。

[適用] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[名前単位削除] ボタン - 該当の項目を削除します。
[アドレス単位削除] ボタン - 指定したエントリの開始アドレスと終了アドレスを削除します。
[戻る] ボタン - 前のウィンドウに戻ります。

[コンフィグ] ボタンをクリックして、以下のウィンドウを表示します。

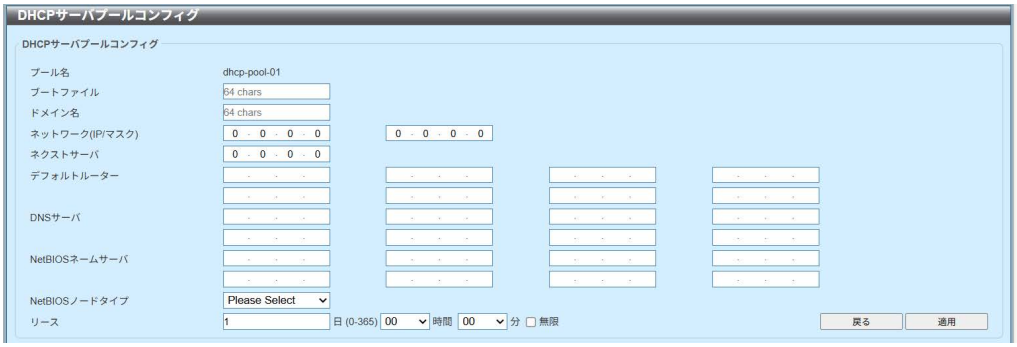

図 3-33 DHCP サーバプール設定（コンフィグ））

設定パラメータ （[DHCP サーバプールコンフィグ] セクション）

パラメータ	概要
ブートファイル	ブートファイル名を入力します。(設定可能文字 : 64 文字)
ドメイン名	DHCP クライアントのドメイン名を入力します。 (設定可能文字 : 64 文字)
ネットワーク **(IP/ マスク)**	DHCP クライアントのネットワーク IPv4 アドレスおよびサブネットマスクを入力します。

パラメータ	概要
ネクストサーバ	ネクストサーバの IPv4 アドレスを入力します。このサーバに起動イメージファイルが保存されます。この IP アドレスを使用して、DHCP クライアントが起動イメージファイルを取得できます。このサーバは、一般に TFTP（Trivial File Transfer Protocol）サーバです。指定できるネクストサーバの IP アドレスは 1 つだけです。
デフォルトルーター	DHCP クライアントのデフォルトルータの IPv4 アドレスを入力します。最大で 8 個の IPv4 アドレスを入力できます。ルータの IP アドレスは、クライアントと同一サブネット上に存在しなければなりません。ルータのリストは、優先度の順に指定します。
DNS サーバ	DHCP クライアントで使用される DNS（Domain Name System）サーバの IPv4 アドレスを入力します。最大で 8 個の IPv4 アドレスを入力できます。サーバのリストは、優先度の順に指定します。
NetBIOS ネームサーバ	DHCP クライアントの WINS（Windows Internet Name Service）ネームサーバの IPv4 アドレスを入力します。最大で 8 個の IPv4 アドレスを入力できます。サーバのリストは、優先度の順に指定します。NetBIOS は Network Basic Input/Output System の略です。
NetBIOS ノードタイプ	Microsoft DHCP クライアントの NetBIOS ノードタイプを選択します。ノードタイプは、NetBIOS が名前の登録と解決に使用する方法を決定します。選択する値は以下のとおりです。 • **[Broadcast]** - ブロードキャストシステムがブロードキャストを使用します。 • **[Peer To Peer]** - ピアツーピア（p-node）システムがネームサーバ（WINS）に対するポイントツーポイントの名前クエリのみを使用します。 • **[Mixed]** - 混合（m-node）システムがまずブロードキャストを実行し、次にネームサーバに対するクエリを実行します。 • **[Hybrid]** - ハイブリッド（h-node）システムがまずネームサーバに対するクエリを実行し、次にブロードキャストを実行します。ハイブリッドタイプを推奨します。
リース	アドレスプールから割り当てられる IPv4 アドレスのリース期間を入力および選択します。 • **[日]** に 0 ～ 365 の範囲で値を入力します。 • 時間と分をドロップダウンから選択します。 • あるいは、**[無限]** オプションをオンにして、リース期間が無制限になるよう指定することもできます。

[適用] ボタン - 変更を反映します。
[戻る] ボタン - 前のウィンドウに戻ります。

3.9.4.3 DHCP サーバ除外アドレス

このウィンドウを用いて、DHCP クライアントへの割り当てから除外する IPv4 アドレスの範囲を設定し、表示します。複数の IPv4 アドレスを除外できます。

[マネジメント] > [DHCP] > [DHCP サーバ] > [DHCP サーバ除外アドレス] をクリックして、以下のウィンドウを表示します。

図 3-34 DHCP サーバ除外アドレス

設定パラメータ （[DHCP サーバ除外アドレス] セクション）

パラメータ	概要
開始アドレス	除外するアドレス範囲の開始 IPv4 アドレスを入力します。
最終アドレス	除外するアドレス範囲の終了 IPv4 アドレスを入力します。

[適用] ボタン - 指定した情報に基づいて新しい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。

3.9.4.4 DHCP サーバマニュアルバインディング

このウィンドウを用いて、DHCP サーバのマニュアルバインディングの設定を行い、設定値を表示します。IP アドレスは、クライアント ID またはホストのハードウェアアドレスのどちらかにバインドできます。

[マネジメント] > [DHCP] > [DHCP サーバ] > [DHCP サーバマニュアルバインディング] をクリックして、以下のウィンドウを表示します。

図 3-35 DHCP サーバマニュアルバインディング

設定パラメータ （[DHCP サーバマニュアルバインディング] セクション）

パラメータ	概要
プール名	DHCP サーバプール名を入力します。 (設定可能文字：32 文字)
ホスト	DHCP ホストの IPv4 アドレスを入力します。
マスク	DHCP ホストネットワークのサブネットマスクを入力します。
ハードウェアアドレス	DHCP ホストの MAC アドレスを入力します。
クライアント識別子	DHCP ホストの識別子を 16 進数表記で入力します。クライアント識別子は、メディアタイプと MAC アドレスで構成されます。

[適用] ボタン - 指定した情報に基づいて新しい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。

3.9.4.5 DHCP サーバダイナミックバインディング

このウィンドウを用いて、DHCP サーバのダイナミックバインディングを表示およびクリアします。

[マネジメント] > [DHCP] > [DHCP サーバ] > [DHCP サーバダイナミックバインディング] をクリックして、以下のウィンドウを表示します。

図 3-36 DHCP サーバダイナミックバインディング

設定パラメータ （[DHCP サーバプダイナミックバインディング] セクション）

パラメータ	概要
IP アドレス	バインディングエントリの IPv4 アドレスを入力します。
プール名	クリアする DHCP サーバプール名を入力します。**[全指定]** オプションを選択した場合、すべてのプールのバインディングエントリをクリアします。(設定可能文字 : 32 文字)
バインディング IP アドレス	バインディングエントリの IPv4 アドレスを入力します。

[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[クリア] ボタン - 指定した条件に基づきテーブル内のエントリをクリアします。

3.9.4.6 DHCP サーバ IP 競合

このウィンドウを用いて、DHCP サーバデータベースから DHCP 競合エントリを表示およびクリアします。

[マネジメント] > [DHCP] > [DHCP サーバ] > [DHCP サーバ IP 競合] をクリックして、以下のウィンドウを表示します。

図 3-37 DHCP サーバ IP 競合

設定パラメータ （[DHCP サーバ IP 競合] セクション）

パラメータ	概要
IP アドレス	特定またはクリアする競合エントリの IPv4 アドレスを入力します。
プール名	クリアする DHCP サーバプール名を入力します。**[全指定]** オプションを選択した場合、すべてのプールの競合エントリをクリアします。(設定可能文字：32 文字)
競合 IP アドレス	特定またはクリアする競合エントリの IPv4 アドレスを入力します。

[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[クリア] ボタン - 指定した条件に基づきテーブル内のエントリをクリアします。

3.9.4.7 DHCP サーバ統計

このウィンドウを用いて、DHCP サーバ統計を表示します。

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

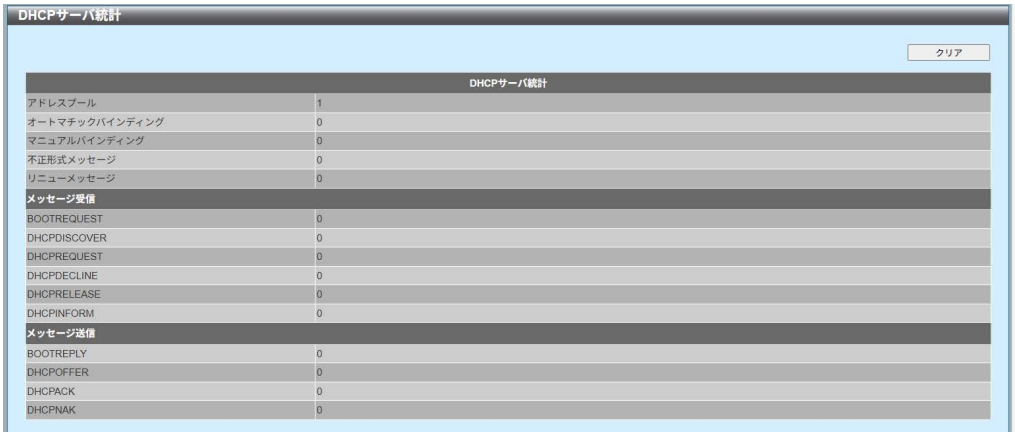

図 3-38 DHCP サーバ統計

[クリア] ボタン - 統計情報をクリアします。

3.9.5 DHCPv6 サーバ

3.9.5.1 DHCPv6 サーバプール設定

このウィンドウを用いて、DHCPv6 サーバのプール設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCPv6 サーバ] > [DHCPv6 サーバプール設定] をクリックして、以下のウィンドウを表示します。

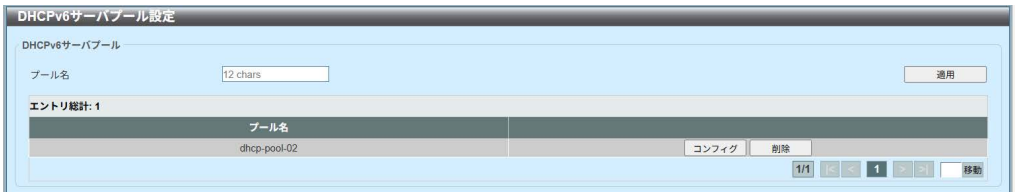

図 3-39 DHCPv6 サーバプール設定

設定パラメータ （[DHCPv6 サーバプール] セクション）

パラメータ	概要
プール名	DHCPv6 サーバプール名を入力します。 (設定可能文字：12 文字)

[適用] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[コンフィグ] ボタン - 指定したエントリに関連する設定を行います。
[削除] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[コンフィグ] 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 3-40 DHCPv6 サーバプール設定（コンフィグ）

[戻る] ボタン - 前のウィンドウに戻ります。

設定パラメータ（[DHCPv6 サーバプールコンフィグ] セクション）

パラメータ	概要
アドレスプレフィックス	DHCPv6 サーバプールの IPv6 ネットワークアドレスとプレフィックス長を選択および入力します（例：2015::0/64）。
プレフィックス委任プール	DHCPv6 サーバプールのプレフィックス委任名を選択および入力します。(設定可能文字：12 文字)
有効ライフタイム	有効ライフタイムの値を入力します。(設定範囲：60 ～ 4294967295 秒) 有効ライフタイムには、推奨ライフタイムより大きい値を指定する必要があります。[デフォルト] オプションを選択した場合、初期値の 2592000 秒（30 日）を使用します。
推奨ライフタイム	推奨ライフタイムの値を入力します。 (設定範囲：60 ～ 4294967295 秒) [デフォルト] オプションを選択した場合、初期値の 604800 秒（7 日）を使用します。
DNS サーバ	DHCPv6 クライアントに割り当てる DNS サーバの IPv6 アドレスを入力します。
ドメイン名	DHCPv6 クライアントに割り当てるドメイン名を入力します。(設定可能文字：253 文字)

[適用] ボタン - 変更を反映します。

設定パラメータ（[スタティックバインディング] セクション）

パラメータ	概要
スタティック バインディングアドレス	特定のクライアントに割り当てるスタティックバインディング IPv6 アドレスを入力します。
スタティック バインディング プレフィックス	スタティックバインディング IPv6 ネットワークアドレスとプレフィックス長を入力します。
クライアント DUID	クライアントの DUID（DHCP Unique Identifier）を入力します。(設定可能文字：28 文字)
IAID	IAID（Identity Association Identifier）を入力します。ここで指定する IAID は、クライアントに割り当てられた非臨時アドレス（IANA）の集合を一意に識別します。
有効ライフタイム	有効ライフタイムの値を入力します。有効ライフタイムには、推奨ライフタイムより大きい値を指定する必要があります。(設定範囲は、60 ～ 4294967295 秒)[デフォルト] オプションを選択した場合、初期値の 2592000 秒（30 日）を使用します。
推奨ライフタイム	推奨ライフタイムの値を入力します。(設定範囲：60 ～ 4294967295 秒)[デフォルト] オプションを選択した場合、初期値の 604800 秒（7 日）を使用します。

[適用] ボタン - 変更を反映します。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを
使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

3.9.5.2 DHCPv6 サーバローカルプール設定

このウィンドウを用いて、DHCPv6 サーバのローカルプール設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCPv6 サーバ] > [DHCPv6 サーバローカルプール設定] をクリックして、以下のウィンドウを表示します。

図 3-41 DHCPv6 サーバローカルプール設定

設定パラメータ （[DHCPv6 サーバローカルプール] セクション）

パラメータ	概要
プール名	DHCPv6 サーバプール名を入力します。 (設定可能文字：12 文字)
IPv6 アドレス / プレフィックス長	ローカルプールの IPv6 プレフィックスアドレスとプレフィックス長を入力します。 (注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください： 例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。 FE80::200:FF:FE00%vlan1
割当長	プールからユーザに委任するプレフィックス長を入力します。プレフィックス長より短い長さを割り当てることはできません。

[適用] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[ユーザ詳細] ボタン - 第 2 テーブルの指定したエントリに関連付けられているユーザ情報を表示します。
[削除] ボタン - エントリを削除します。

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

3.9.5.3 DHCPv6 サーバ除外アドレス

このウィンドウを用いて、DHCPv6 プールから除外する IPv6 アドレスを設定し、表示します。DHCPv6 プールから複数の IPv6 アドレスを除外できます。

[マネジメント] > [DHCP] > [DHCPv6 サーバ] > [DHCPv6 サーバ除外アドレス] をクリックして、以下のウィンドウを表示します。

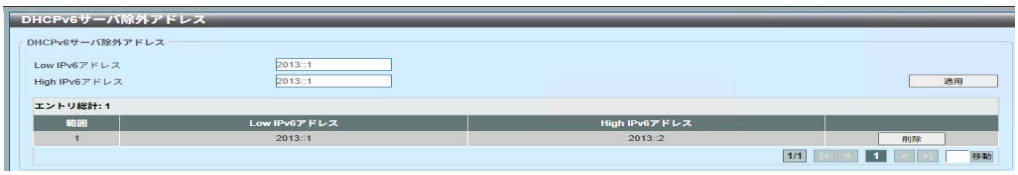

図 3-42 DHCPv6 サーバ除外アドレス

設定パラメータ （[DHCPv6 サーバ除外アドレス] セクション）

パラメータ	概要
Low IPv6 アドレス	除外する IPv6 アドレスまたは除外するアドレス範囲の開始 IPv6 アドレスを入力します。
High IPv6 アドレス	除外するアドレス範囲の終了 IPv6 アドレスを入力します。

[適用] ボタン - 指定した情報に基づいて新しい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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

（注意）
FE80から始まるIPv6のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1のIPv6 リンクローカル
アドレス "FE80::200:FF:FE00"を指定する。

FE80::200:FF:FE00%vlan1

3.9.5.4 DHCPv6 サーババインディング

このウィンドウを用いて、DHCPv6 サーババインディングエントリを表示およびクリアします。

[マネジメント] > [DHCP] > [DHCPv6 サーバ] > [DHCPv6 サーババインディング] をクリックして、以下のウィンドウを表示します。

図 3-43 DHCPv6 サーババインディング

設定パラメータ （[DHCPv6 サーババインディング] セクション）

パラメータ	概要
IPv6 アドレス	表示またはクリアするバインディングエントリの IPv6 アドレスを入力します。**[全指定]** オプションを選択した場合、すべての DHCPv6 クライアントプレフィックスのバインディングをバインディングテーブルに表示、またはテーブルからクリアされます。

[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[クリア] ボタン - 指定した条件に基づきテーブル内のエントリをクリアします。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

3.9.5.5 DHCPv6 サーバインターフェース設定

このウィンドウを用いて、DHCPv6 サーバに関連するインタフェースの設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCPv6 サーバ] > [DHCPv6 サーバ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 3-44 DHCPv6 サーバインターフェース設定

設定パラメータ （[DHCPv6 サーバインターフェース設定] 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)
プール名	DHCPv6 サーバプール名を入力します。
高速コミット	2 メッセージ交換 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値：Disabled)
優先度	優先度を入力します。**[デフォルト]** オプションを選択した場合、優先度 0 が使用され、**[Allow Hint]** オプションを選択した場合、ヒントが許可されます。 (設定範囲：0 ～ 255)
インターフェース名	インターフェース名を入力します。

[適用] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[削除] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

3.9.5.6 DHCPv6 サーバ操作情報

このウィンドウを用いて、DHCPv6 サーバの操作情報を表示します。

[マネジメント] > [DHCP] > [DHCPv6 サーバ] > [DHCPv6 サーバ操作情報] をクリックして、以下のウィンドウを表示します。

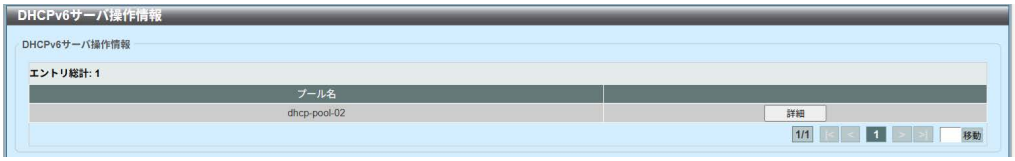

図 3-45 DHCPv6 サーバ操作情報

[詳細]ボタン - エントリの詳細を確認します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]**ボタンをクリックして特定のページに移動します。

[詳細]ボタンをクリックして、セッションテーブルを表示します。

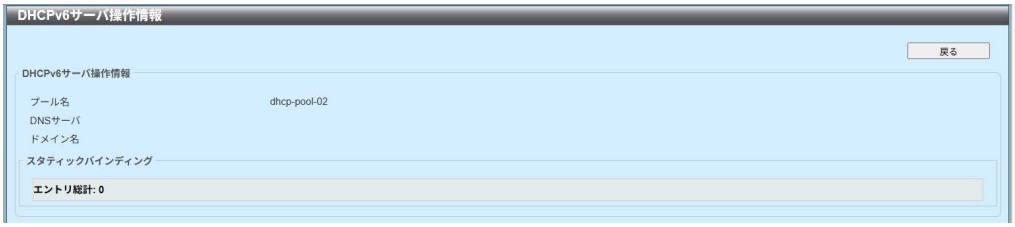

図 3-46 DHCPv6 サーバ操作情報 (詳細)

[戻る]ボタン - 前のウィンドウに戻ります。

3.9.6 DHCP リレー

3.9.6.1 DHCP リレーグローバル設定

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

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

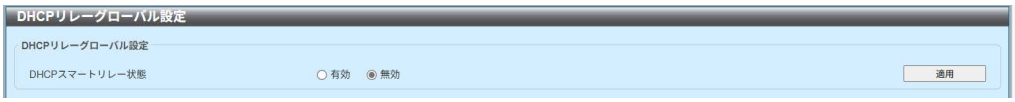

図 3-47 DHCP リレーグローバル設定

設定パラメータ （[DHCP リレーグローバル設定] セクション）

パラメータ	概要
DHCP スマートリレー状態	DHCP スマートリレー状態 (**有効 / 無効**) を選択します。(初期値：無効)

[適用] ボタン - 変更を反映します。

3.9.6.2 DHCP リレープール設定

このウィンドウを用いて、DHCP リレーエージェントに DHCP リレープールの設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCP リレー] > [DHCP リレープール設定] をクリックして、以下のウィンドウを表示します。

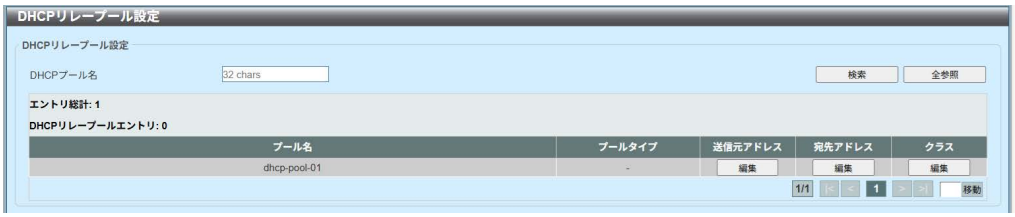

図 3-48 DHCP リレープール設定

設定パラメータ （[DHCP リレープール設定] セクション）

パラメータ	概要
DHCP プール名	DHCP プール名を入力します。 (設定可能文字：32 文字)

[検索] - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
[送信元アドレス] の下にある **[編集]** ボタンをクリックして、エントリに関連付けられている DHCP リレーソース設定を編集します。
[宛先アドレス] の下にある **[編集]** ボタンをクリックして、エントリに関連付けられている DHCP リレーディスティネーション設定を編集します。
[クラス] の下にある **[編集]** ボタンをクリックして、エントリに関連付けられている DHCP リレークラス設定を編集します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[送信元アドレス] の下にある **[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 3-49 DHCP リレープールソース設定

設定パラメータ （[DHCP リレープールソース設定] セクション）

パラメータ	概要
ソース IP アドレス	クライアントパケットのソースサブネットを入力します。
サブネットマスク	ソースサブネットのネットワークマスクを入力します。

[適用] ボタン - 指定した情報に基づいて新しい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。

[宛先アドレス] の下にある **[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 3-50 DHCP リレープールディスティネーション設定

設定パラメータ （[DHCP リレープールディスティネーション設定] セクション）

パラメータ	概要
リレーディスティネーション	DHCP リレーで使用されるディスティネーションサーバの IP アドレスを入力します。

[適用] ボタン - 指定した情報に基づいて新しい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。

[クラス] の下にある [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。

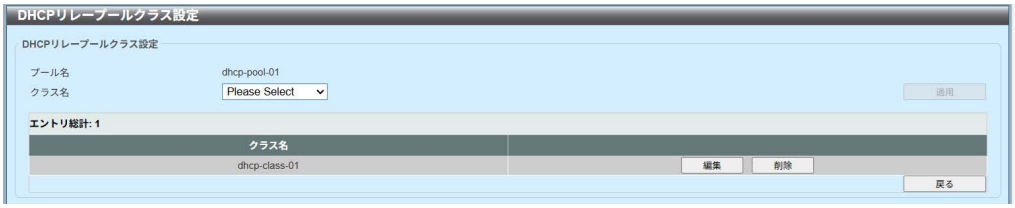

図 3-51 DHCP リレープールクラス設定

設定パラメータ （**[DHCP リレープールクラス設定]** セクション）

パラメータ	概要
クラス名	DHCP クラス名を選択します。

[適用] ボタン - 指定した情報に基づいて新しい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。
[戻る] ボタン - 前のウィンドウに戻ります。

[DHCP リレープールクラス設定] の **[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 3-52 DHCP リレープールクラスエディット設定

設定パラメータ （**[DHCP リレープールクラスエディット設定]** セクション）

パラメータ	概要
リレーターゲット	DHCP クラスで定義されているオプションの値パターンに一致するパケットをリレーする、DHCP リレーターゲットを指定します。

[適用] ボタン - 指定した情報に基づいて新しい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。

3.9.6.3 DHCP リレー情報設定

このウィンドウを用いて、DHCP リレー情報を設定し、表示します。

[マネジメント] > [DHCP] > [DHCP リレー] > [DHCP リレー情報設定] をクリックして、以下のウィンドウを表示します。

図 3-53 DHCP リレー情報設定

設定パラメータ （[DHCP リレー情報グローバル] セクション）

パラメータ	概要
全信頼情報	特定のインタフェースの IP DHCP リレー情報の信頼 (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)
情報確認	DHCP リレーエージェントによる受信 DHCP 応答パケットのリレーエージェント情報オプションの有効性確認 (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)
ポリシー情報	DHCP リレーエージェントの Option 82 再転送ポリシーを選択します。選択する値は以下のとおりです。 • **[Keep]** - すでにリレーオプションが設定されているパケットを保持します。パケットは変更されずにそのまま、DHCP サーバにリレーされます。 • **[Drop]** - すでにリレーオプションが設定されているパケットを破棄します。 • **[Replace]** - すでにリレーオプションが設定されているパケットを置き換えます。パケットは新しいオプションに置き換えられます。
オプション情報	DHCP リクエストパケットのリレーの際のリレーエージェント情報（Option 82）の挿入 (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

[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 3-54 DHCP リレー情報設定 (編集)

設定パラメータ （[DHCP リレー情報] セクション）

パラメータ	概要
信頼済み	DHCP リレーエージェントによるすべてのインタフェースの IP DHCP リレー情報の信頼 (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)
チェックリレー	DHCP リレーエージェントによる受信 DHCP 応答パケットのリレーエージェント情報オプションの有効性確認と削除 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)
ポリシーアクション	DHCP リレーエージェントの Option 82 再転送ポリシーを選択します。選択する値は以下のとおりです。 • **[Keep]** - すでにリレーオプションが設定されているパケットを保持します。パケットは変更されずにそのまま、DHCP サーバにリレーされます。 • **[Drop]** - すでにリレーオプションが設定されているパケットを破棄します。 • **[Replace]** - すでにリレーオプションが設定されているパケットを置き換えます。パケットは新しいオプションに置き換えられます。
オプション挿入	DHCP リクエストパケットのリレーの際のリレーエージェント情報（Option 82）の挿入 (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

3.9.6.4 DHCP リレー情報オプションフォーマット設定

このウィンドウを用いて、DHCP 情報フォーマットを設定し、表示します。

[マネジメント] > [DHCP] > [DHCP リレー] > [DHCP リレー情報オプションフォーマット設定] をクリックして、以下のウィンドウを表示します。

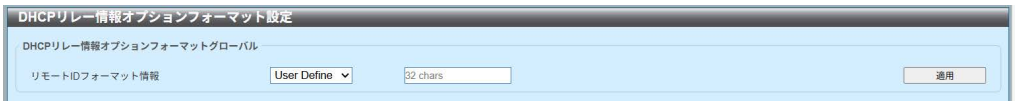

図 3-55 DHCP リレー情報オプションフォーマット設定

設定パラメータ （[DHCP リレー情報オプションフォーマットグローバル] セクション）

パラメータ	概要
リモート ID フォーマット情報	DHCP 情報リモート ID サブオプションを選択します。選択する値は以下のとおりです。 • **[Default]** - スイッチのシステム MAC アドレスをリモート ID として使用します。 • **[User Define]** - ユーザ定義のリモート ID を使用します。(設定可能文字：32 文字)

[適用] ボタン - 変更を反映します。

3.9.6.5 DHCP ローカルリレー VLAN

このウィンドウを用いて、VLAN または VLAN のグループのローカルリレー設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCP リレー] > [DHCP ローカルリレー VLAN] をクリックして、以下のウィンドウを表示します。

図 3-56 DHCP ローカルリレー VLAN

設定パラメータ （[DHCP ローカルリレー VLAN 設定] セクション）

パラメータ	概要
DHCP ローカルリレー 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。(設定範囲は 1 ～ 4094) **[全 VLAN 指定]** チェックボックスをオンにした場合、すべての VLAN を選択します。
状態	特定の VLAN で DHCP ローカルリレー (**Enabled/ Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

3.9.7 DHCPv6 リレー

3.9.7.1 DHCPv6 リレーグローバル設定

このウィンドウを用いて、グローバル DHCPv6 リレー設定を行い、設定値を表示します。この設定には、リモート ID とインタフェース ID の設定が含まれます。

[マネジメント] > [DHCP] > [DHCPv6 リレー] > [DHCPv6 リレーグローバル設定] をクリックして、以下のウィンドウを表示します。

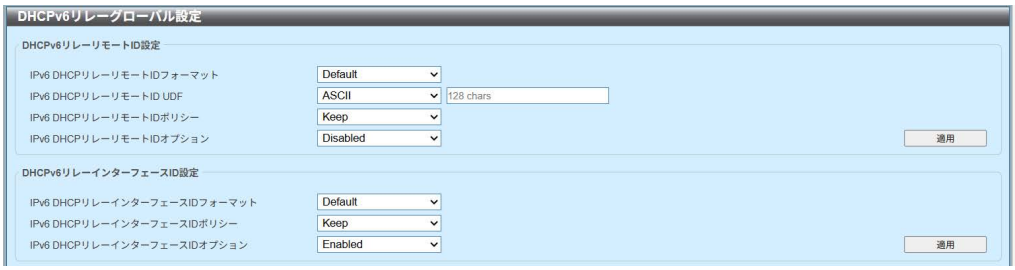

図 3-57 DHCPv6 リレーグローバル設定

設定パラメータ （[DHCPv6 リレーリモート ID 設定] セクション）

パラメータ	概要
IPv6 DHCP リレー リモート ID フォーマット	使用する IPv6 DHCP リレーのリモート ID フォーマットを選択します。選択する値は **[Default]**、**[CID With User Define]**、および **[User Define]** です。
IPv6 DHCP リレー リモート ID UDF	リモート ID の UDF（ユーザ定義フィールド）を選択します。選択する値は以下のとおりです。 • **[ASCII]** - ASCII 文字列をテキストボックスに最大 128 文字で入力します。 • **[HEX]** - 16 進数文字列をテキストボックスに最大 256 文字で入力します。
IPv6 DHCP リレー リモート ID ポリシー	DHCPv6 リレーエージェントの Option 37 再転送ポリシーを選択します。選択する値は以下のとおりです。 • **[Keep]** - すでにリレーエージェントのリモート ID オプションが設定されている DHCPv6 リクエストパケットを、変更しないでそのまま、DHCPv6 サーバにリレーします。 • **[Drop]** - すでにリレーエージェントのリモート ID（Option 37）が設定されているパケットを破棄します。
IPv6 DHCP リレー リモート ID オプション	DHCPv6 リクエストパケットのリレーの際のリレーエージェントのリモート ID（Option 37）の挿入 (**Enabled/ Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

設定パラメータ （[DHCPv6 リレーインターフェース ID 設定] セクション）

パラメータ	概要
IPv6 DHCP リレーインタフェース **ID** フォーマット	使用する IPv6 DHCP リレーのインタフェース ID フォーマットを選択します。選択する値は **[Default]**、**[CID]**、および **[Vendor1]** です。
IPv6 DHCP リレーインタフェース **ID** ポリシー	DHCPv6 リレーエージェントの Option 18 再転送ポリシーを選択します。選択する値は以下のとおりです。 • **[Keep]** - すでにリレーエージェントのインタフェース ID オプションが設定されている DHCPv6 リクエストパケットを、変更しないでそのまま、DHCPv6 サーバにリレーします。 • **[Drop]** - すでにリレーエージェントのインタフェース ID（Option 18）が設定されているパケットを破棄します。
IPv6 DHCP リレーインタフェース **ID** オプション	DHCPv6 リクエストパケットのリレーの際のリレーエージェントのインタフェース ID（Option 18）の挿入 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

3.9.7.2 DHCPv6 リレーインターフェース設定

このウィンドウを用いて、DHCPv6 リレーインターフェースの設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCPv6 リレー] > [DHCPv6 リレー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 3-58 DHCPv6 リレーインターフェース設定

設定パラメータ （[DHCPv6 リレーインターフェース設定] セクション）

パラメータ	概要
インターフェース VLAN	DHCPv6 リレーで使用するインターフェース VLAN ID を入力します。(設定範囲：1 ～ 4094)
宛先 IPv6 アドレス	DHCPv6 リレーのディスティネーションアドレスを入力します。
出力インターフェース VLAN	リレーディスティネーションの出力インターフェース VLAN ID を入力します。(設定範囲は 1 ～ 4094)

[適用] ボタン - 変更内容を反映します。
[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[削除] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

(注意)
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

3.9.7.3 DHCPv6 ローカルリレー VLAN

このウィンドウを用いて、DHCPv6 ローカルリレー VLAN の設定を行い、設定値を表示します。

[マネジメント] > [DHCP] > [DHCPv6 リレー] > [DHCPv6 ローカルリレー VLAN] をクリックして、以下のウィンドウを表示します。

図 3-59 DHCPv6 ローカルリレー VLAN

設定パラメータ （[DHCPv6 ローカルリレー VLAN] セクション）

パラメータ	概要
DHCPv6 ローカルリレー VID リスト	使用する VLAN ID を入力します。VLAN ID はカンマ区切り (ex1,3) もしくは、ハイフン (ex1-3) で設定することもできます。(設定範囲 : 1 ～ 4094) **[全 VLAN 指定]** を選択した場合、全 VLAN を指定できます。
状態	DHCPv6 ローカルリレー VLAN 状態 (**Enabled/Disabled**) を選択します。(Enabled : 有効化 , Disabled : 無効化)

[適用] ボタン - 変更内容を反映します。

3.10 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。

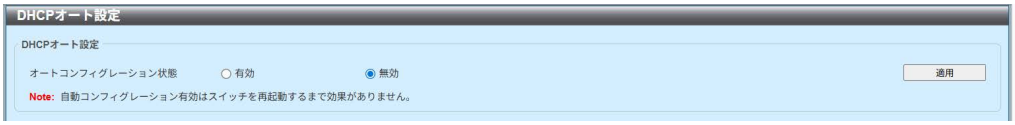

図 3-60 DHCP オート設定

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。 (初期値 : 無効)

[**適用**] ボタン - 設定内容を反映します。

3.11 DNS （Domain Name System）

3.11.1 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。

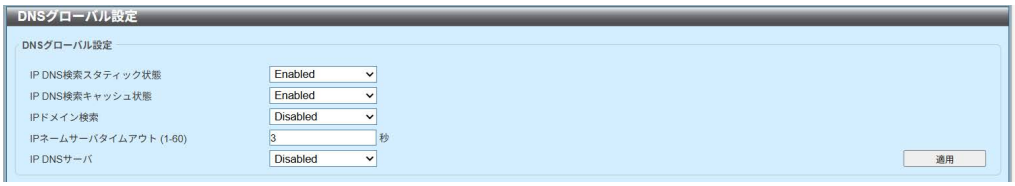

図 3-61 DNS グローバル設定

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。 (Enabled：有効化 , Disabled：無効化 , 初期値：Enabled)
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。 (Enabled：有効化 , Disabled：無効化 , 初期値：Enabled)
IP ドメイン検索	IP ドメイン検索状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値：Disabled)
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。（初期値：3, 設定範囲：1 ～ 60 秒）
IP DNS サーバ	DNS サーバの状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値：Disabled)

[**適用**] ボタン - 設定内容を反映します。

3.11.2 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。

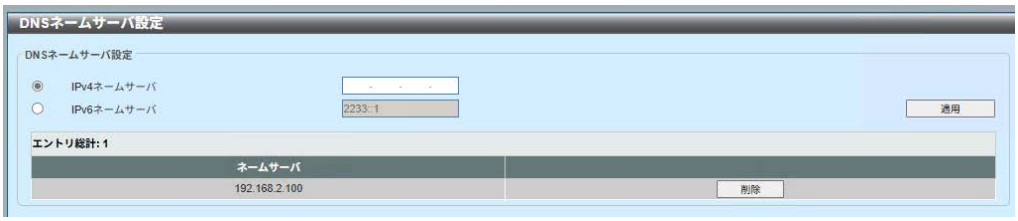

図 3-62 DNS ネームサーバ設定

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。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

3.11.3 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 3-63 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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

3.12 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 3-64 ファイルシステム

設定パラメータ ([パス] セクション)

パラメータ	概要
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。
[**コピーメニューへ**] 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。

ドライブリンク（c : ）を選択し、以下のウィンドウを表示します。

図 3-65 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。

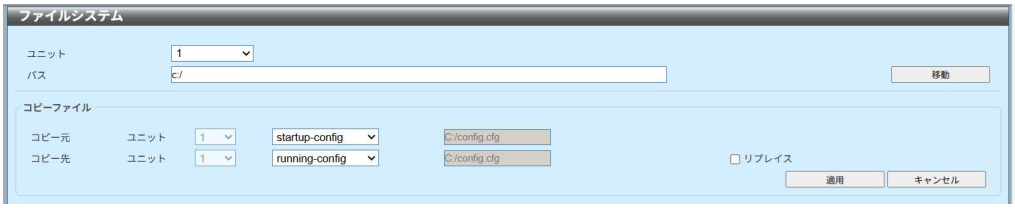

図 3-66 ファイルシステム（コピーメニュー）

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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。 **[runnning-config]** オプションを選択したときのみ、**[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、コピー元に設定されたファイルに置き換わります。

[**適用**] ボタン - コピー元の設定およびコピー先の設定を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。

3.12.1 ファイルシステム - USB ブート

USB ブートとは、USB メモリ内に格納されている設定ファイルやファームウェアを起動 (設定) させることができる機能です。

このウィンドウを用いて、USB メモリのフォーマット、および USB ブートの設定を行います。

(注意)
本設定を行う前に USB メモリを接続した状態で、以下設定を行います。
[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。

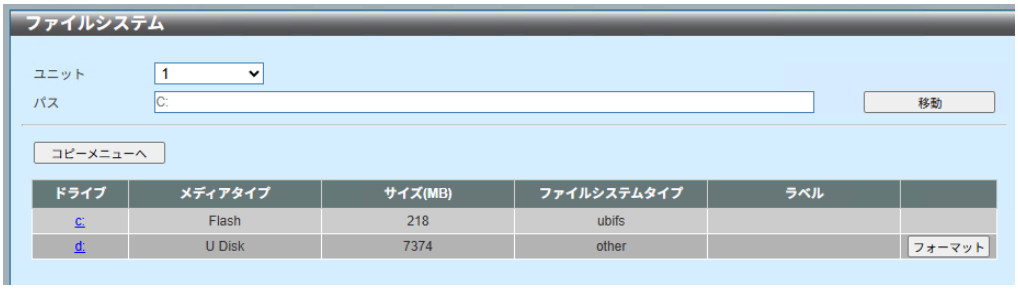

図 3-67 ファイルシステム (USB ブート)

設定パラメータ ([パス] セクション)

パラメータ	概要
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。
[**コピーメニューへ**] 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。
[**フォーマット**] ボタン - USB メモリのフォーマット設定画面に移動します。
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。
ドライブリンク（d : ）をクリックして、USB メモリに移動します。

[**フォーマット**] 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 3-68 ファイルシステム（フォーマット）

設定パラメータ （[フォーマットドライブ] セクション）

パラメータ	概要
ドライブ	d: - USB メモリを選択します。
タイプ	USB メモリのフォーマット形式は [FAT32] です。
ラベル	USB メモリの識別名を設定します。 (設定可能文字：11 文字)

[**適用**] ボタン - 設定内容を反映します。
[**キャンセル**] ボタン - フォーマット設定をキャンセルします。

(注意) フォーマット設定時のご注意

USB メモリは必ず FAT32 形式でフォーマットしてください。
Windows のデフォルトフォーマットツールでは FAT32 形式を選択できない場合があります。その場合は、FAT32 形式でのフォーマットに対応した専用ツールをご使用ください。

ドライブリンク（d：）を選択し、以下のウィンドウを表示します。

図 3-69 ファイルシステム（d：）

[**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。

(注意) USB ブートを行う時に下記点に注意して、設定をしてください。
1. [リネーム] の設定で下記の記号は設定できません。
- **"**
- *****
- **><**
- **?**

2. USB 内に FW が格納されている場合、PPS(Power to Progress SDN) から FW バージョンアップを
実行しても USB 内の FW が優先されます。

[**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。

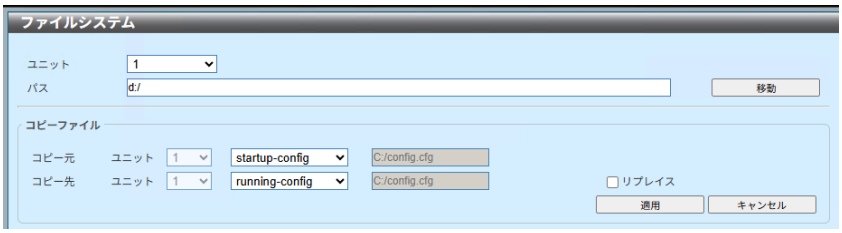

図 3-70 ファイルシステム（コピーメニュー）

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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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、コピー元で選択した設定ファイルに置き換わります。 (注意) **[リプレイス]** チェックボックスをオンにした場合、コピー先は running config を指定する必要がございます。

[**適用**] ボタン - コピーを実行します。
[**キャンセル**] ボタン - コピーをキャンセルします。

3.13 スタッキング

3.13.1 物理スタッキング

このウィンドウを用いて、スイッチの物理スタッキング機能に関連する設定を行い、設定値を表示します。スイッチを物理的にスタックするには、QSFP（Quad Small Form-factor Pluggable）トランシーバに接続された光ファイバケーブル、あるいは QSFP コネクタを備えた DAC（Direct Attached Cables）を使用します。
スタッキングが有効な場合、最後の 2 つの QSFP ポートがスタッキング専用になります。他の目的では使用できません。このポートは、スタッキングモードが有効な場合にのみスタッキングを実行できます。

[マネジメント] > [スタッキング] > [物理スタッキング] をクリックして、以下のウィンドウを表示します。

図 3-71 物理スタッキング

設定パラメータ（[物理スタッキング] セクション）

パラメータ	概要
スタッキングモード	スタッキングモード (**有効 / 無効**) を選択します。
スタックプリエンプト	優先度の高いユニットをスイッチに追加するときに、マスターの役割のプリエンプション (**有効 / 無効**) を選択します。
トラップ状態	スタッキングのトラップ状態 (**有効 / 無効**) を選択します。
現在のユニット ID	ユニット ID を選択します。
新ボックス ID	**[現在のユニット ID]** フィールドで選択したスイッチに対して、新しいボックス ID を選択します。ユーザは 1 ～ 4 の範囲の任意の数を指定して、スイッチスタック内のスイッチを識別できます。**[Auto]** を選択すると、スイッチスタック内のスイッチにボックス番号が自動的に割り当てられます。
優先度	スイッチスタッキングユニットの優先度を入力します。 (設定範囲：1 ～ 63)

[適用] ボタン - 変更内容を反映します。

3.14 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。

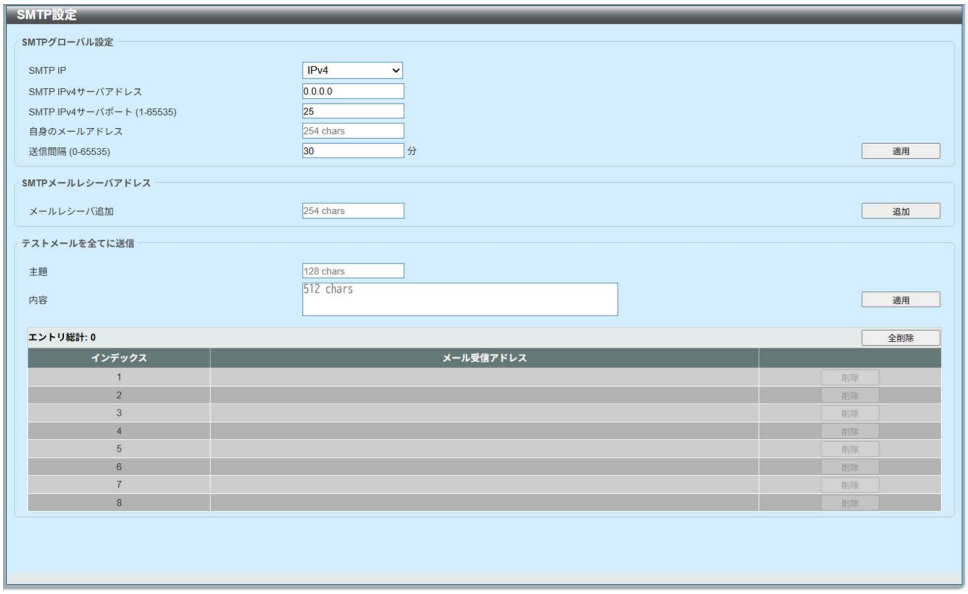

図 3-72 SMTP 設定

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	([SMTP 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	([SMTP 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	([SMTP 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。 (初期値：25, 設定範囲：1 ～ 65535)
SMTP IPv6 サーバポート	([SMTP 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。 (初期値：25, 設定範囲：1 ～ 65535)
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。 (設定可能文字：254 文字)

パラメータ	概要
送信間隔	送信間隔の値（分）を設定します。 （初期値：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。 （設定可能文字：254 文字）

[**追加**] ボタン - エントリを追加します。

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。（設定可能文字：128 文字）
内容	メールの本文を入力します。（設定可能文字：512 文字）

[**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。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

3.15 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 3-73 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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
[**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。
複数のページが存在する場合は、ページ番号を入力し、[移動] ボタンをクリックして特定のページに移動します。

3.16 IP 簡単設定

3.16.1 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ー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。

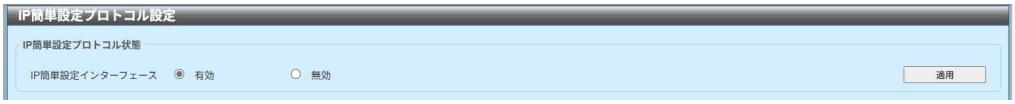

図 3-74 IP 簡単設定プロトコル設定

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 簡単設定インターフェース	IP 簡単設定インターフェース (**有効 / 無効**) を選択します。(初期値 : 有効)

[適用] ボタン - 変更を反映します。

3.16.2 IP 簡単設定プロトコルフォワード設定

このウィンドウを用いて、IP 簡単設定プロトコルフォワード設定を行い、設定値を表示します。

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

図 3-75 IP 簡単設定プロトコルフォワード設定

設定パラメータ
([IP 簡単設定プロトコルフォワードグローバル状態] セクション)

パラメータ	概要
IP 簡単設定プロトコルフォワード状態	IP 簡単設定プロトコルフォワード状態 (**有効 / 無効**) を選択します。

[適用] ボタン - 変更を反映します。

設定パラメータ ([センダー IP 設定] セクション)

パラメータ	概要
送信元 IP アドレス	送信元の IP アドレスを入力します。
宛先インターフェース名	宛先インターフェースの名前を入力します。

[追加] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[削除] ボタン - 指定した情報に基づいてエントリを削除します。
[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

設定パラメータ （[インターフェース設定] セクション）

パラメータ	概要
受信インターフェース	受信インターフェースの ID を入力します。 (設定範囲：1 ～ 4094)
宛先インターフェース名	宛先インタフェースの名前を選択および入力します。
ソース IP アドレス	ソースの IP 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 IP アドレス	ディスティネーションの IP アドレスを選択および入力します。

[追加] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[削除] ボタン - 指定した情報に基づいてエントリを削除します。
[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

4 PPS(Power to Progress SDN)

4.1 PPS ステータス設定

このウィンドウを用いて、PPS ステータス設定を表示します。

[PPS] > [PPS ステータス設定] をクリックして、以下のウィンドウを表示します。

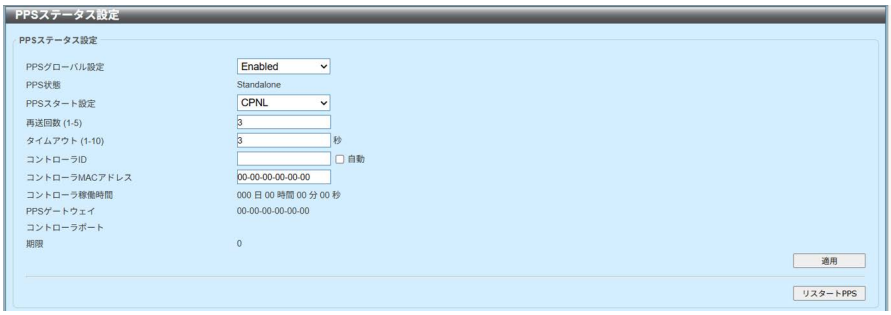

図 4-1 PPS ステータス設定

設定パラメータ （[PPS ステータス設定] セクション）

パラメータ	概要
PPS グローバル設定	PPS 機能（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)
PPS スタート設定	PPS スタート状態を表示します。選択できるオプションは以下の通りです。 • **Standalone** - PPS の開始ステータスとしてスタンドアロンモードを選択します。 • **CPNL** - PPS の開始ステータスとしてコントローラポートネイバー損失 (CPNL) モードを選択します。 （注意）コントローラ ID が存在しない場合は、CPNL を選択しても Standalone 状態になります
再送回数	再送回数の値を入力します。 (初期値 : 3, 設定範囲 : 1 ～ 5)
タイムアウト	タイムアウトの値（秒）を入力します。 (初期値 : 3, 設定範囲 : 1 ～ 10 秒)
コントローラ ID	スイッチ側で PPS コントローラを識別するための ID を入力します。**[自動]** オプションを選択すると、スイッチがコントローラを自動的に決定します。

パラメータ	概要
コントローラ **MAC** アドレス	スイッチが自身に登録した PPS コントローラの MAC アドレスを入力します。 この MAC アドレスから送信された PPSP のみ使用します。 **[コントローラ ID]** で **[自動]** オプションを選択すると、 MAC アドレスを自動的に決定します。

（補足）
以下は、スイッチにて PPS が格納されているデバイスを認識した時に、
自動的に登録されます。

- PPS 状態：
  - Controlled - PPS コントローラを認識し、有効な PPSP を受信している状態を示します。
  - CPNL - PPS コントローラを認識しているが、有効な PPSP を受信していない状態または、PPS コントローラを認識していないが、PPS コントローラの探索は行っている状態を示します。
  - Standalone - PPS コントローラを認識できていない状態。PPS コントローラの検出も停止している。

- コントローラポート
  スイッチが自身に登録した PPS コントローラが接続されているポートです。
  間にスイッチが複数ある場合は、PPSP を受信したポートが登録されます。

- 期限
  PPS コントローラの登録情報が削除されるまでの時間です。

[**適用**] ボタン - 変更を反映します。
[**リスタート PPS**] ボタン - PPS をリスタートします。

4.2 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 4-2PPS 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。 (Enabled：有効化 , Disabled：無効化 , 初期値 :Enabled)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[カウンタ通知設定] セクション）

パラメータ	概要
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。 （初期値 : 5, 設定範囲：1 ～ 120 秒）
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 :Enabled)

[**適用**] ボタン - 設定内容を反映します。

4.3 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 4-3 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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。 （初期値 : 128, 設定範囲 : 0 ～ 255 ）

[**適用**] ボタン - 設定内容を反映します。

4.4 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 4-4 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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。
複数のページが存在する場合は、ページ番号を入力し、[移動] ボタンをクリックして特定のページに移動します。

4.5 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。

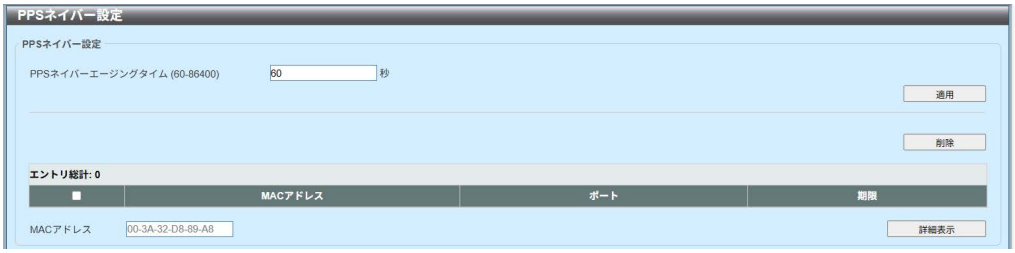

図 4-5 PPS ネイバー設定

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。（ 初期値 : 60, 設定範囲 : 60 ～ 86400 秒）
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。

4.6 PPS バーチャルリンク設定

このウィンドウを用いて、PPS バーチャルリンクの設定を行います。

[PPS] > [PPS バーチャルリンク設定] をクリックして、以下のウィンドウを表示します。

図 4-6 PPS バーチャルリンク設定

設定パラメータ （[PPS バーチャルリンク設定] セクション）

パラメータ	概要
ターゲット IPv4 アドレス	IPv4 アドレスを入力します。
ターゲット IPv6 アドレス	IPv6 アドレスを入力します。
送信元 VLAN インターフェース	送信元 VLAN インターフェースの 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。
[**削除**] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

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、ユニ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] > [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。

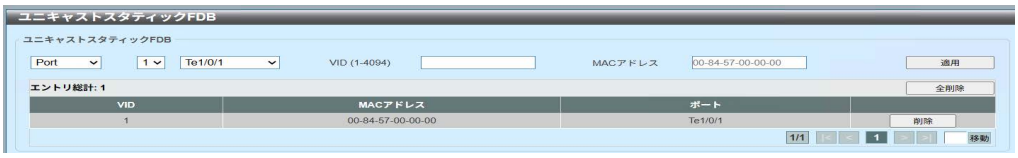

図 5-1 ユニキャストスタティック FDB

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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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。

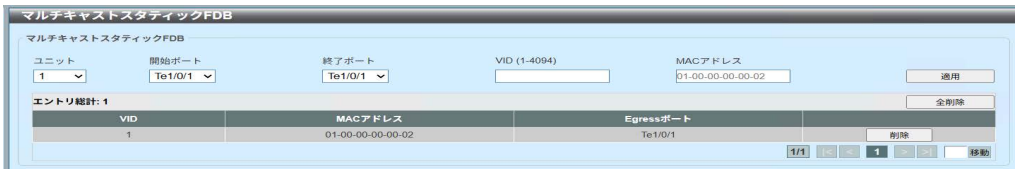

図 5-2 マルチキャストスタティック FDB

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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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、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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 0 を設定したとき、無効になります。 (初期値：300, 設定範囲：0,10 ～ 1000000 秒)
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 (**有効 / 無効**) を選択します。(初期値：無効)

[**適用**] ボタン - 設定内容を反映します。

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

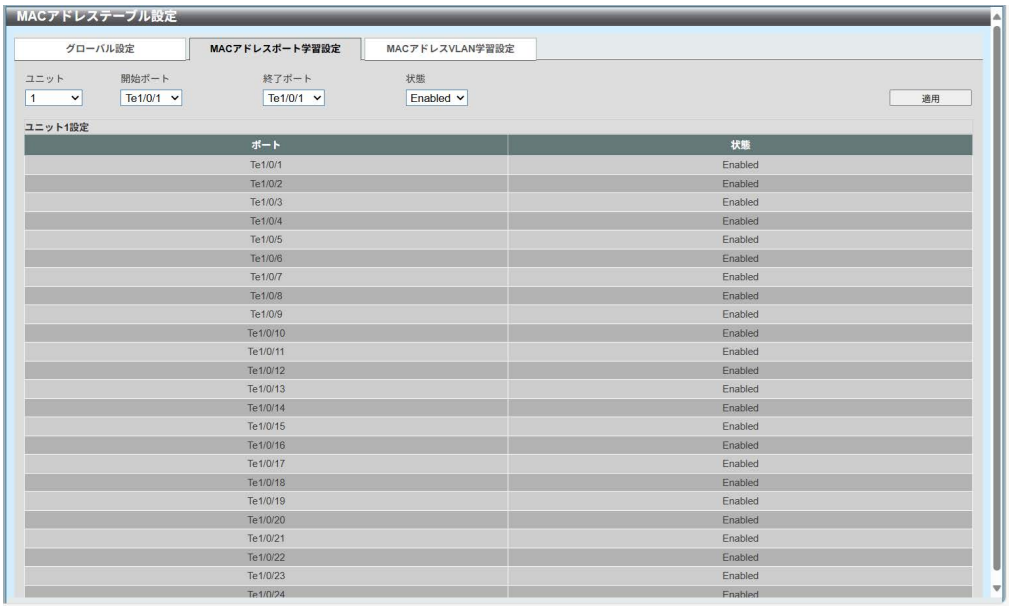

図 5-4 MAC アドレステーブル設定（MAC アドレスポート学習設定）

設定パラメータ （[MAC アドレスポート学習設定] セクション）

パラメータ	概要
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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 MAC アドレス学習の状態（**Enabled**/ **Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)

[**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。

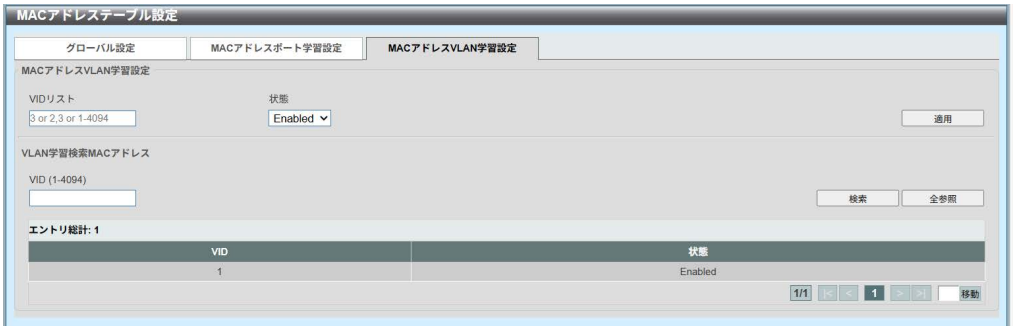

図 5-5 MAC アドレステーブル設定（MAC アドレス VLAN 学習設定）

設定パラメータ （[MAC アドレス VLAN 学習設定] 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。 (Enabled：有効化 , Disabled：無効化 , 初期値：Enabled)

[適用] ボタン - エントリを追加します。

設定パラメータ （[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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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	ユニット ID、ポートを選択します。 (注意) ユニット ID は、スタッキングした際に表示します。
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 エントリをポート指定でクリア**] 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 エントリを VLAN 指定でクリア**] 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 エントリを MAC 指定でクリア**] 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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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。

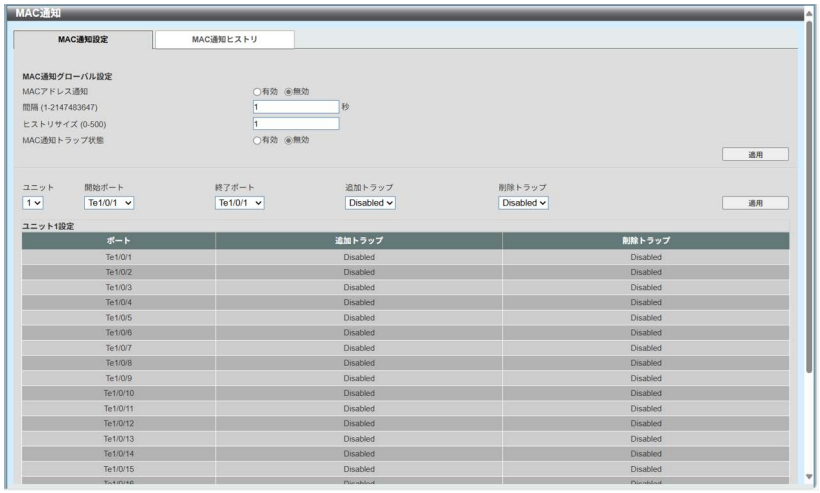

図 5-7 MAC 通知（MAC 通知設定）

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。 (初期値 : 無効)
間隔	通知間隔の時間（秒）を入力します。 （初期値：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。（初期値：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。 (初期値 : 無効)
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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 通知ヒストリを表示します。

図 5-8 MAC 通知 (MAC 通知ヒストリ)

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 5-9 802.1Q 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	使用する VLAN ID を入力します。VLAN ID はカンマ区切り (ex1,3) もしくは、ハイフン (ex1-3) で設定することもできます。（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 - VLAN 名を編集します。
[**削除**] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 5-10 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 ～ 12）
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 リンクサービスアクセスポイント (LSAP) ペアです。最初のオクテットは宛先サービスアクセスポイント (DSAP)、2 番目のオクテットは送信元です。

[**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ーフェース

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ー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ーフェース] をクリックして、以下のウィンドウを表示します。

図 5-11 プロトコル VLAN プロファイルインターフェース

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

パラメータ	概要
ポート	ユニット ID、ポートを選択します。 (注意) ユニット ID は、スタッキングした際に表示します。
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。

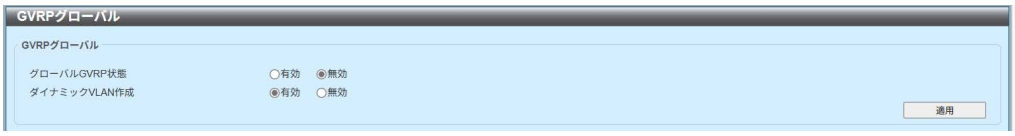

図 5-12 GVRP グローバル

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。 (初期値：無効)
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。 (初期値：有効)

[**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。

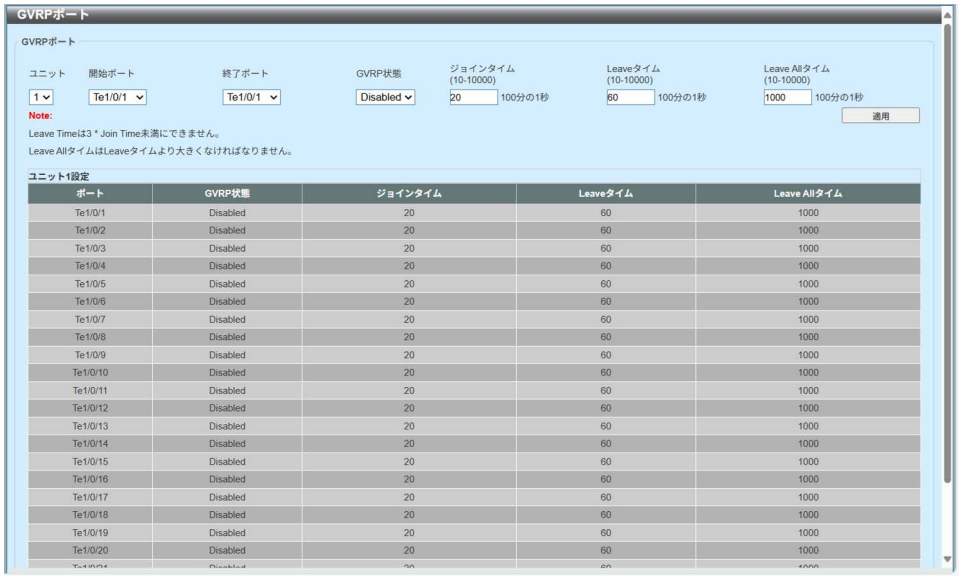

図 5-13 GVRP ポート

設定パラメータ （[GVRP ポート] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値：Disabled)
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。 (初期値：20, 設定範囲：10 ～ 10000 センチ秒)
Leave タイム	Leave タイム値（センチ秒）を入力します。 (初期値：60, 設定範囲：10 ～ 10000 センチ秒)
Leave All タイム	Leave All タイム値（センチ秒）を入力します。 (初期値：1000, 設定範囲：10 ～ 10000 センチ秒)

[**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 5-14 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 5-15 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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、すべての禁止 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：2 ～ 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 5-16 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

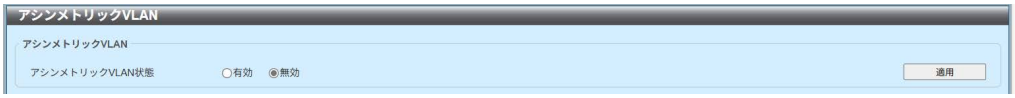

図 5-17 アシンメトリック VLAN

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。(初期値：無効)

[**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。

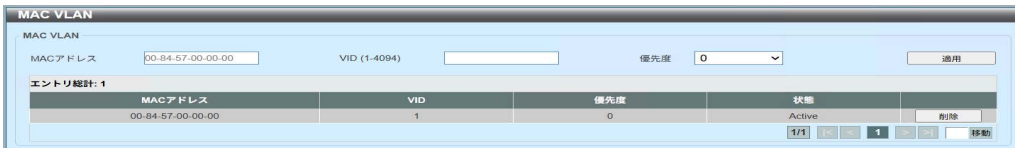

図 5-18 MAC VLAN

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	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 インターフェース

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

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

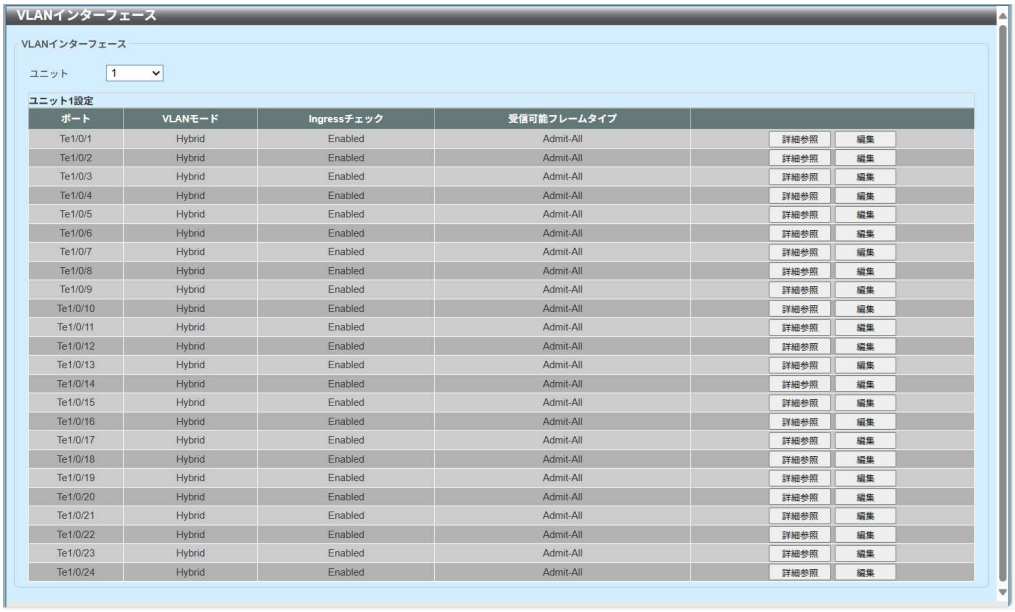

図 5-19 VLAN インターフェース

設定パラメータ （[VLAN インターフェース] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

[**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 - エントリの設定を編集します。

[**詳細参照**] ボタン選択し、以下のウィンドウを表示します。

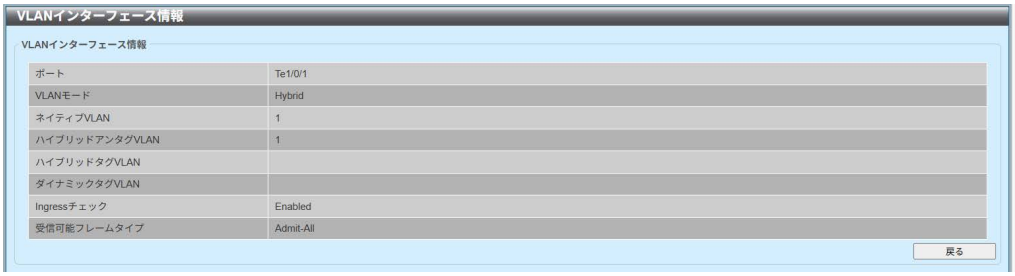

図 5-20 VLAN インターフェース (詳細参照)

[**戻る**] ボタン - 前のウィンドウに戻ります。

[**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。
VLAN モードとして [**Access**] を選択して、次のウィンドウを表示します。

図 5-21 VLAN インターフェース（編集、Access）

設定パラメータ （[Access]>[VLAN インターフェースの設定] 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]** 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。 (初期値 : Admit All)
Ingress チェック	Ingress チェックの状態（**有効** / **無効**）を選択します。 (初期値 : 有効)
VID	使用する VLAN ID を入力します。（設定範囲：1 ～ 4094）
クローン	チェックボックスでクローン機能を有効にします。 クローン機能を有効にすると、同じ設定内容が指定されたポートにコピーされます。
開始ポート／終了ポート	(**[クローン]** パラメータで **[有効]** 選択時に設定可) 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。

[**Hybrid**] 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 5-22 VLAN インターフェース (編集 , Hybrid)

設定パラメータ （[Hybrid]>[VLAN インターフェースの設定] 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 **[Hybrid]** 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。 (初期値 : Admit All)
Ingress チェック	Ingress チェックの状態（**有効** / **無効**）を選択します。 (初期値 : 有効)
ネイティブ VLAN	チェックボックスでネイティブ VLAN の有効にします。
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**）を選択します。
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	(**[アクション]** パラメータで **[None]** 以外を選択時に設定可) 許可 VLAN 範囲を入力します。(設定範囲 : 1 ～ 4094)
クローン	チェックボックスでクローン機能を有効にします。 クローン機能を有効にすると、同じ設定内容が指定されたポートにコピーされます。
開始ポート／終了ポート	(**[クローン]** パラメータで **[有効]** 選択時に設定可) 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。

[Trunk] 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 5-23 VLAN インターフェース (編集 , Trunk)

設定パラメータ （[Trunk]>[VLAN インターフェースの設定] 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 **[Trunk]** 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。 (初期値 : Admit All)
Ingress チェック	Ingress チェックの状態（**有効** / **無効**）を選択します。 (初期値 : 有効)
ネイティブ VLAN	(**[ネイティブ VLAN]** パラメータで **[有効]** 選択時に設定可) ネイティブ VLAN の有効、無効を選択します。 モード（**タグ / アンタグ**）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/All/Add/Remove/Except/ Replace**）を選択します。
許可 VLAN 範囲	(**[アクション]** パラメータで **[None/All]** 以外を選択時に設定可）許可 VLAN 範囲を入力します。(設定範囲 :1 ～ 4094)
クローン	チェックボックスでクローン機能を有効にします。 クローン機能を有効にすると、同じ設定内容が指定されたポートにコピーされます。
開始ポート／終了ポート	(**[クローン]** パラメータで **[有効]** 選択時に設定可) 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。

[VLAN モード] で **[Promiscuous]** を選択して、以下のウィンドウを表示します。

図 5-24 VLAN インターフェース（編集、Promiscuous）

設定パラメータ （[Promiscuous]>[VLAN インターフェースの設定] 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 **[Promiscuous]** 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を選択します。選択する値は（**Tagged Only**/**Untagged Only**/**Admit All**）です。
Ingress チェック	Ingress チェックの状態（**有効** / **無効**）を選択します。 (初期値 : 有効)
クローン	チェックボックスでクローン機能を有効にします。 クローン機能を有効にすると、同じ設定内容が指定されたポートにコピーされます。。
開始ポート - 終了ポート	(**[クローン]** パラメータで **[有効]** 選択時に設定可) 使用するポートを選択します。

[適用] ボタン - 変更を反映します。
[戻る] ボタン - 前のウィンドウに戻ります。

[VLAN モード] で **[Host]** を選択して、以下のウィンドウを表示します。

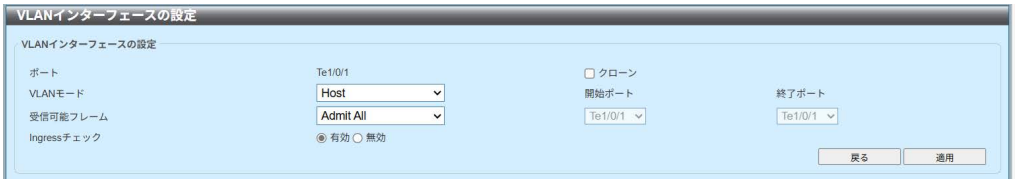

図 5-25 VLAN インターフェース（編集、Host）

設定パラメータ （[Host]>[VLAN インターフェースの設定] 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 **[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を選択します。選択する値は（**Tagged Only**/**Untagged Only**/**Admit All**）です。

パラメータ	概要
Ingress チェック	Ingress チェックの状態（**有効** / **無効**）を選択します。 (初期値 : 有効)
クローン	チェックボックスでクローン機能を有効にします。 クローン機能を有効にすると、同じ設定内容が指定されたポートにコピーされます。
開始ポート - 終了ポート	([クローン] パラメータで [**有効**] 選択時に設定可) 使用するポートを選択します。

[**適用**] ボタン - 変更を反映します。
[**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 5-26 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。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

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 5-27 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。 (初期値：無効)
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。(初期値：5)
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。 （初期値：720 分 , 設定範囲：1 ～ 65535 分）

[**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 5-28 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

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 Auto Tagged 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 Auto Untagged 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。

[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 5-29 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。（設定可能文字：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 5-30 音声 VLAN 装置

設定パラメータ （[音声 VLAN 装置テーブル] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

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 5-31 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 5-32 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）

パラメータ	概要
アクション	プライベート VLAN で実行するアクション（**Add**/**Remove**/**Disabled**）を選択します。
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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 5-33 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。 (初期値：無効)

[**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。 (初期値：RSTP)

[**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。（初期値：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。（初期値：20, 設定範囲：6 ～ 40 秒）
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。（初期値：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。（初期値：15, 設定範囲：4 ～ 30）
TX ホールド数	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。（初期値：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。（初期値：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。

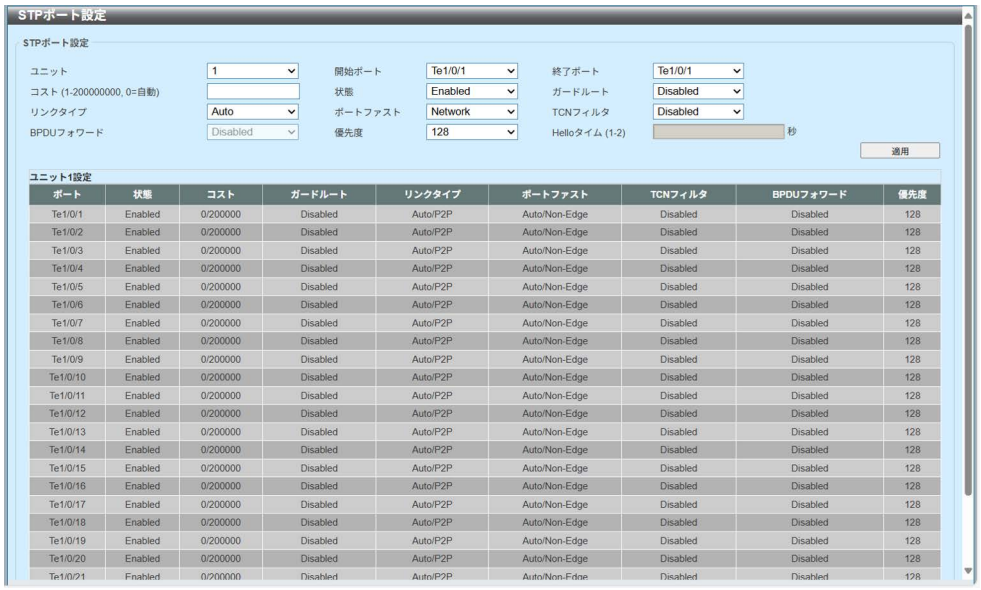

図 5-34 STP ポート設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 （初期値：0, 設定範囲：0 ～ 200000000）
状態	STP ポートの状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)

パラメータ	概要
ガードルート	ガードルートの状態（**Enabled**/**Disabled**）を選択します。(Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。（初期値：Auto）
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。 （初期値：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 (**Enabled**/**Disabled**) を選択します。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。（初期値：Disabled）
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。 Enabled を設定するためには、事前に状態：Disabled に変更しておく必要があります。 （Enabled：有効化 , Disabled：無効化 , 初期値：Disabled）
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。（初期値：128）
Hello タイム	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 秒）

[**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。

[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。

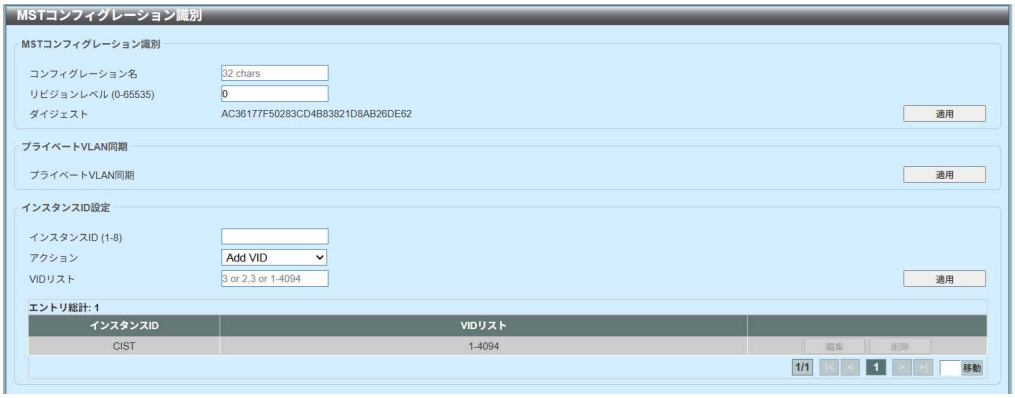

図 5-35 MST コンフィグレーション識別

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。（設定可能文字：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。（初期値：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 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。[**編集**] ボタンをクリックすると、編集するインスタンス ID が表示されます。アクションと VID リストを設定し、適用ボタンをクリックすることで、編集が可能となります。
[**削除**] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 5-36 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。(初期値 : 32768, 設定範囲 : 0 ～ 61440)

[**編集**] ボタン - エントリの設定を編集します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 5-37 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (設定範囲：0 ～ 200000000)
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。 （初期値：128, 設定範囲：0 ～ 240）

[**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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

5.4 ループ検知・遮断

5.4.1 ループ検知・遮断設定

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。

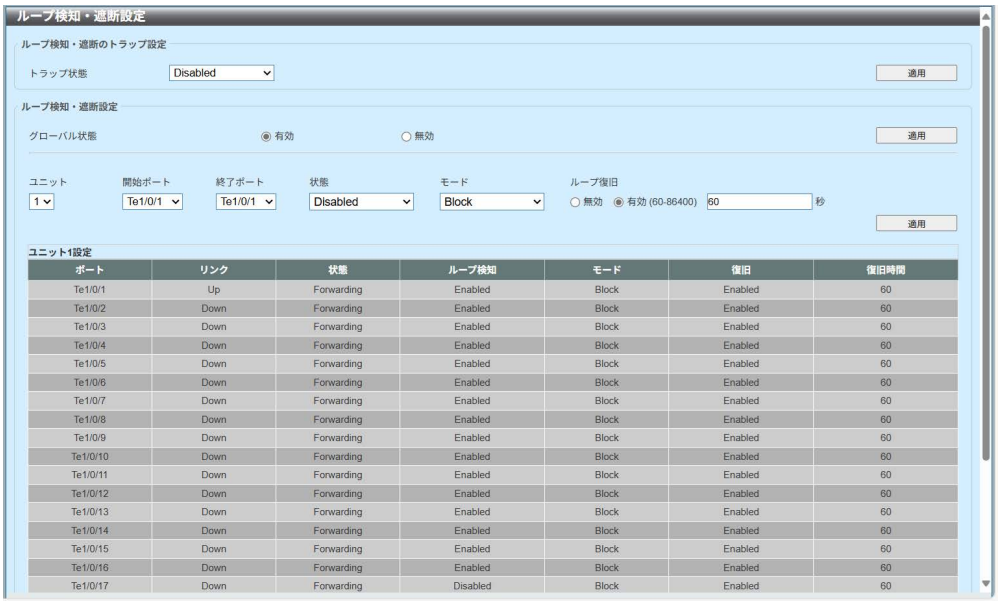

図 5-38 ループ検知・遮断設定

設定パラメータ ([ループ検知・遮断のトラップ設定] セクション)

パラメータ	概要
トラップ状態	ループ検知・遮断 トラップ状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

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（**有効** / **無効**）を選択します。 (初期値 : 有効)
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートのループ検知の状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 (初期値 : Block)
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。 (初期値 : 有効 , 60 秒 , 設定範囲 : 60 ～ 86400 秒)

[**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。

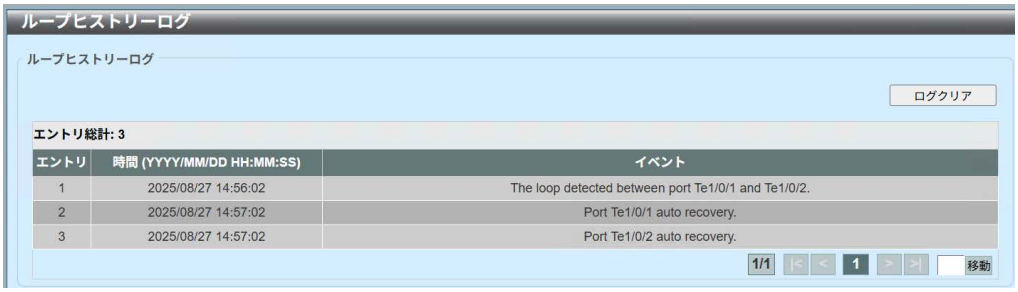

図 5-39 ループヒストリーログ

[**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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 5-40 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	システムプライオリティ値を入力します。 値が低いほど優先度が高くなります。複数のポートが同じプライオリティを持つ場合、ポート番号が小さいほど、優先度が高くなります。 (初期値 : 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/Source L4 Port/Destination L4 Port/Source Destination L4 Port**）を選択します。（初期値 : 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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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
グループ ID	チャネルグループ番号を入力します。 物理ポートが最初にチャネルグループに参加すると、システムが自動的にポートチャネルを作成します。また、インターフェースは 1 つのチャネル グループにのみ参加できます。 (設定範囲：1 ～ 40)
モード	モード (**Static**/**Active**/**Passive**) を選択します。「Static」を指定した場合、チャネルグループのタイプは静的になります。「Active」または「Passive」を指定した場合、チャネルグループのタイプはリンクアグリゲーション制御プロトコル（LACP）になります。一度チャネルグループのタイプが決定すると、他のタイプのインターフェースはそのチャネルグループに参加できなくなります。

[**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。

[**詳細参照**] ボタンをクリックすると、エントリの詳細情報を表示します。

図 5-41 リンクアグリゲーション (詳細参照)

[**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 5-42 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。(初期値：5)
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。 (初期値：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。

パラメータ	概要
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。
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。 トンネルプロトコルの初期値の MAC アドレス： • **GVRP** - 00-C0-8F-04-92-C1 • **STP** - 00-C0-8F-04-92-C0 • **01-00-0C-CC-CC-CC** - 00-C0-8F-04-92-C2 • **01-00-0C-CC-CC-CD** - 00-C0-8F-04-92-C3

[**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 5-43 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(設定範囲：1 ～ 4096)

[**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 5-44 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 スヌーピングをグローバルに (**有効 / 無効**) を選択します。(初期値：無効)
不明なデータ制限	不明な IGMP スヌーピングデータ制限値を入力します。初期値を使用するには「**デフォルト**」を選択します。 (初期値：128, 設定範囲：1 ～ 4094)
IGMP スヌーピング未知データ	クリアする未知の IGMP スヌーピングデータグループを選択します。 • **All** - すべての未知の IGMP スヌーピングデータグループをクリアすることを指定します。 • **VLAN** - 指定された VLAN に関連する未知の IGMP スヌーピングデータグループをクリアすることを指定します。 • **Group** - 指定された未知の IGMP スヌーピングデータグループをクリアすることを指定します。

パラメータ	概要
VID	[IGMP スヌーピング未知データ] で [VLAN] を選択すると、有効になります。 VLAN ID を入力します。(設定範囲：1 ～ 4094)
グループアドレス	[IGMP スヌーピング未知データ] で [Group] を選択すると、有効になります。 クリアする未知の IGMP スヌーピングデータグループのアドレスを入力します。

[適用] ボタン - 変更を反映します。
[クリア] ボタン - 未知の IGMP スヌーピングデータグループをクリアします。

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) 選択した VLAN ID で IGMP スヌーピング (**有効 / 無効**) を選択します。(初期値：無効)

[適用] ボタン - 指定した情報に基づいて新しい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 - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
[詳細参照] ボタン - このエントリに関する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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[**詳細参照**] ボタンをクリックして、以下のウィンドウを表示します。

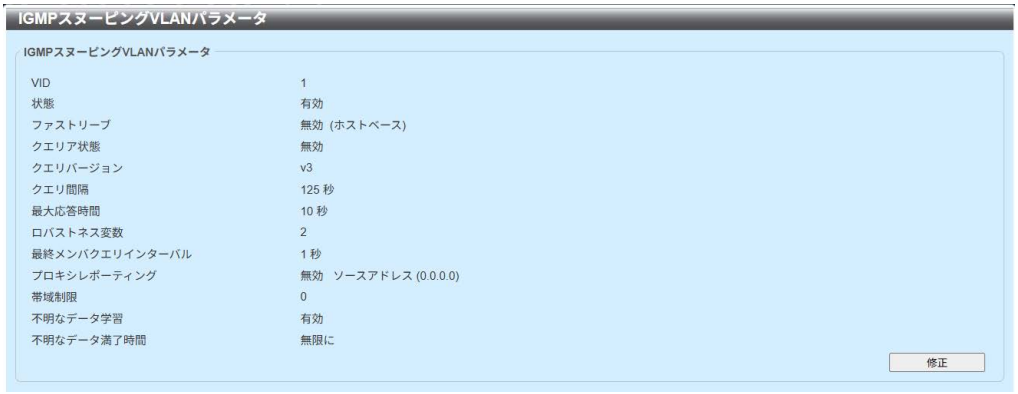

図 5-45 IGMP スヌーピング設定（詳細参照）

[**修正**] ボタン - 設定を編集します。
[**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 5-46 IGMP スヌーピング設定（編集、修正）

設定パラメータ （[IGMP スヌーピング VLAN 設定] セクション

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機能 (**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。 (初期値：無効)
クエリア状態	クエリア状態 (**有効 / 無効**) を選択します。 (初期値：無効)

パラメータ	概要
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を選択します。選択する値は **[1]**、**[2]**、および **[3]** です。 (初期値：3)
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。 (初期値：125, 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。 (初期値：10 秒 , 設定範囲：1 ～ 25 秒)
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。(初期値：2, 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。(初期値：1 秒 , 範囲は 1 ～ 25 秒)
プロキシレポーティング	プロキシレポート機能 (**有効 / 無効**) を選択します。 (初期値：無効)
ソースアドレス	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。このオプションは、**[プロキシレポーティング]** で **[有効]** を選択すると有効になります。
帯域制限	帯域制限値を入力します。(設定範囲：1 ～ 1000) 帯域制限値はパケット / 秒で指定します。 **[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。
不明なデータ学習	未知の IGMP スヌーピングデータの学習 (**有効 / 無効**) を選択します。 (初期値：有効)
不明なデータ満了時間	未知のデータの有効期限を入力します。**[無限に]** オプションを選択すると、有効期限が無効になります。 (設定範囲：1 ～ 65535 秒)

[適用] ボタン - 変更を反映します。

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 5-47 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。
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタン - 指定した情報に基づいて新しいエントリを追加します。
[削除] ボタン - 指定した情報に基づいて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、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 - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

設定パラメータ （[IGMP 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、IP マルチキャストグループアドレスを入力します。
詳細	IGMP グループの詳細情報を表示します。

[検索] ボタン - 指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、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 5-48 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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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） レートはパケット / 秒で指定します。 **[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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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 ～ 4094）
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** - Drop 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。
ACL 名を除外	標準 IP アクセスリストの名前を入力します。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。 （設定可能文字：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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。あるいは、**[選択してください]** ボタンをクリックして、このスイッチに設定されている既存のアクセスリストを選択します。 （設定可能文字：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
ユニット	スタッキングユニット ID を入力します。 スタッキングした際に表示します。
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。

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[詳細参照] 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 5-49 IGMP スヌーピングフィルタ設定（詳細参照）

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[戻る] ボタン - 前のウィンドウに戻ります。

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。

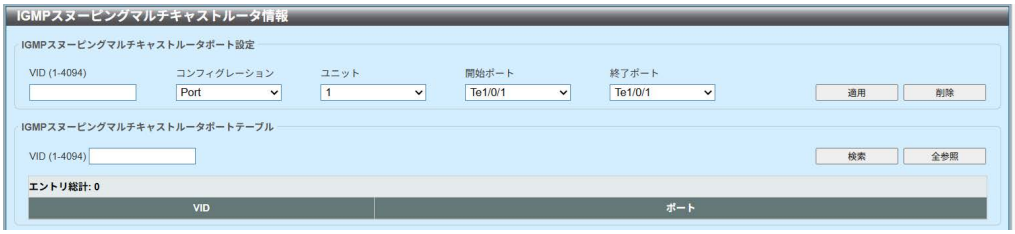

図 5-50 IGMP スヌーピングマルチキャストルータ情報

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。(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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 5-51 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）
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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）
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 5-52 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。 (初期値：無効)
不明なデータ制限	不明な MLD スヌーピングデータ制限値を入力します。 [デフォルト] を選択すると、初期値になります。 (初期値：128, 設定範囲：1 ～ 2048)
MLD スヌーピング不明データ	不明の MLD スヌーピングデータグループを選択します。 • **All** - すべての未知の MLD スヌーピングデータグループをクリアすることを指定します。 • **VLAN** - 指定された VLAN に関連する未知の MLD スヌーピングデータグループをクリアすることを指定します。 • **Group** - 指定された未知の MLD スヌーピングデータグループをクリアすることを指定します。
VID	[MLD スヌーピング不明データ] で [VLAN] を選択時に設定可能です。VLAN ID を入力します。(設定範囲：1 ～ 4094)
グループアドレス	[MLD スヌーピング不明データ] で [Group] を選択時に設定可能です。クリアする不明の MLD スヌーピングデータグループの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。

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。 （初期値：無効 , 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 - 設定を編集します。

[**詳細参照**] ボタンをクリックして、以下のウィンドウを表示します。

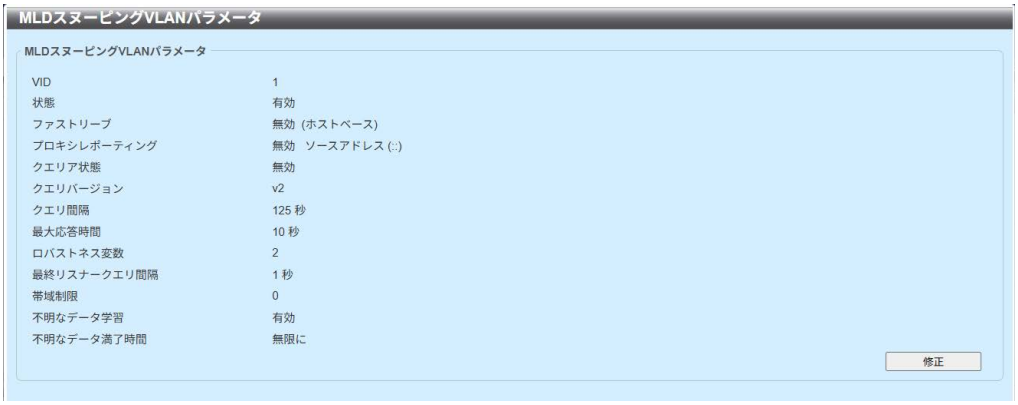

図 5-53 MLD スヌーピング設定（詳細参照）

[**修正**] ボタン - 設定を修正します。

[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 5-54 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
ファーストリーブ	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。 (初期値：無効)
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。 (初期値：無効)
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。 (初期値：無効)
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。(初期値：2)
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。 (初期値：125, 設定範囲：1 ～ 31744 秒)
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。 (初期値：10, 設定範囲：1 ～ 25 秒)
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。(初期値：2, 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。(初期値：1 秒 , 設定範囲：1 ～ 25)

パラメータ	概要
帯域制限	帯域制限値を入力します。(設定範囲：1 ～ 1000) レートはパケット / 秒で指定します。 **[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。
不明なデータ学習	不明なデータ学習 (**有効 / 無効**) を選択します。 (初期値：有効)
不明なデータ満了時間	不明なデータの有効期限を入力します。 **[無限に]** オプションをオンにした場合、有効期限が無効になります。(設定範囲：1 ～ 65535 秒)

[**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 5-55 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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 5-56 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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） レートはパケット / 秒を指定します。 **[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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 ～ 2048）
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** - Drop 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。
ACL 名を除外	標準 IP アクセスリストの名前を入力します。あるいは、**[選択してください]** ボタンをクリックして、このスイッチで設定されている既存のアクセスリストを選択します。 （設定可能文字：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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。あるいは、**[選択してください]** ボタンをクリックして、このスイッチで設定されている既存のアクセスリストを選択します。 （設定可能文字：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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

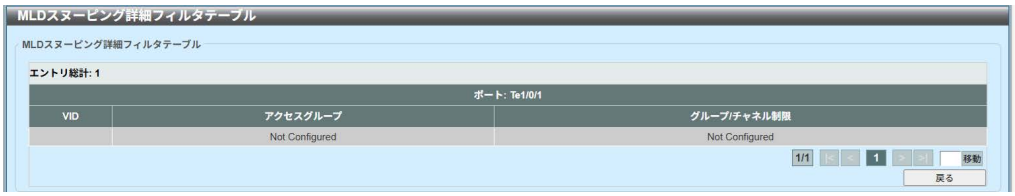

図 5-57 MLD スヌーピングフィルタ設定（詳細参照）

複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。
[戻る] ボタンをクリックして、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。

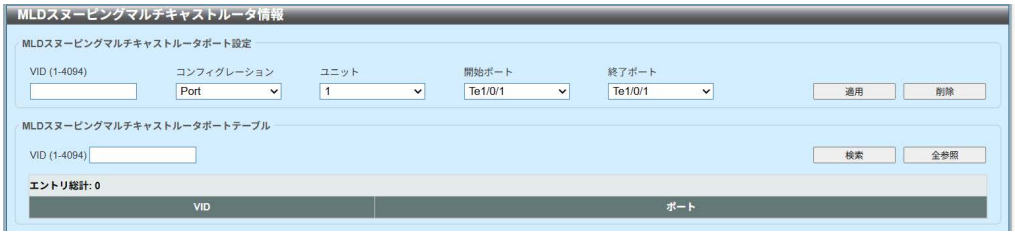

図 5-58 MLD スヌーピングマルチキャストルータ情報

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** - 設定する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** - 設定する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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 5-59 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）
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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）
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 5-60 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 (ex1,3)、またはハイフン区切り (ex1-3) 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。 • **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。 (デフォルト : Forward Unregistered)

[**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。

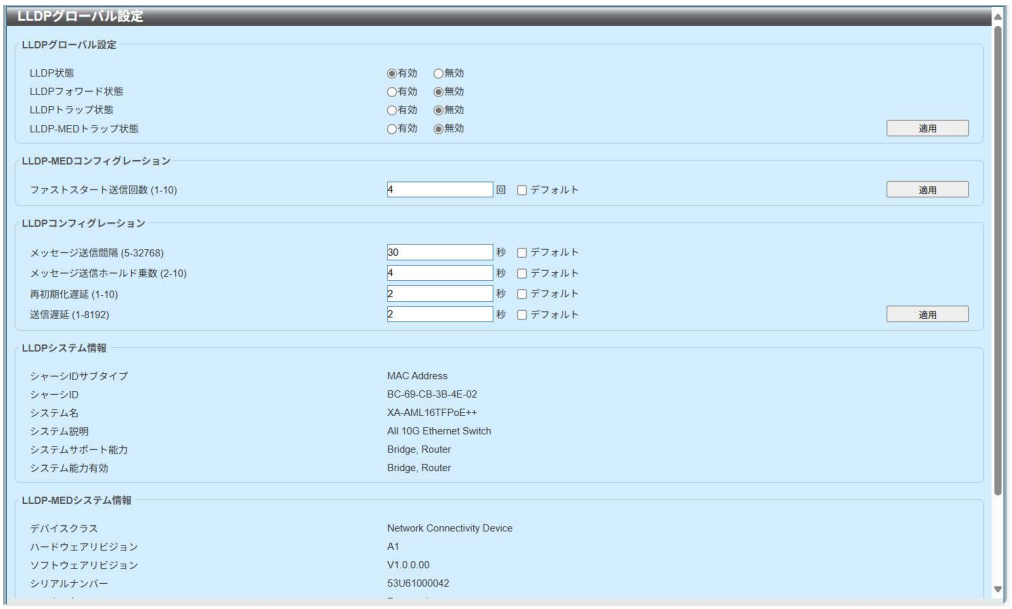

図 5-61 LLDP グローバル設定

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。 (初期値：有効)
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。(初期値：無効)
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。 (初期値：無効)
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。(初期値：無効)

[**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。[**デフォルト**] オプションを選択した場合、初期値を使用します。（初期値：4, 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 （[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。[**デフォルト**] オプションを選択した場合、初期値を使用します。（初期値：30, 設定範囲：5 ～ 32768 秒）
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。[**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。（初期値：4, 設定範囲：2 ～ 10 秒）
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。[**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。（初期値：2, 設定範囲：1 ～ 10 秒）
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。メッセージ送信間隔の値の 4 分の 1 を超えないようにしてください。[**デフォルト**] オプションを選択した場合、初期値を使用します。（初期値：2, 設定範囲：1 ～ 8192 秒）

[**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 5-62 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (初期値 : Disabled)
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。(初期値 : Local)

パラメータ	概要
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 5-63 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。

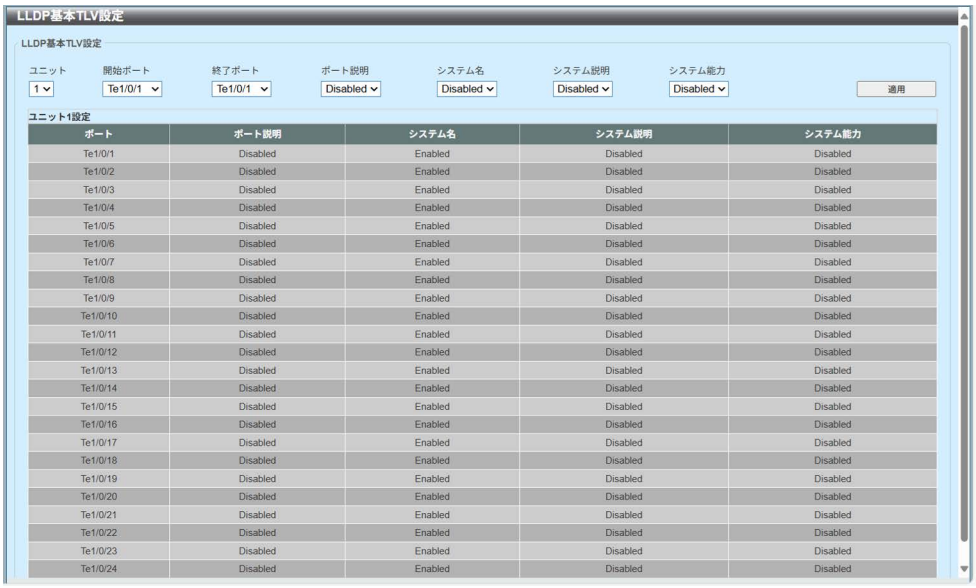

図 5-64 LLDP 基本 TLV 設定

[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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(初期値 : Disabled)
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。(初期値 : Enabled)
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。(初期値 : Disabled)
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。(初期値 : Disabled)

[**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。

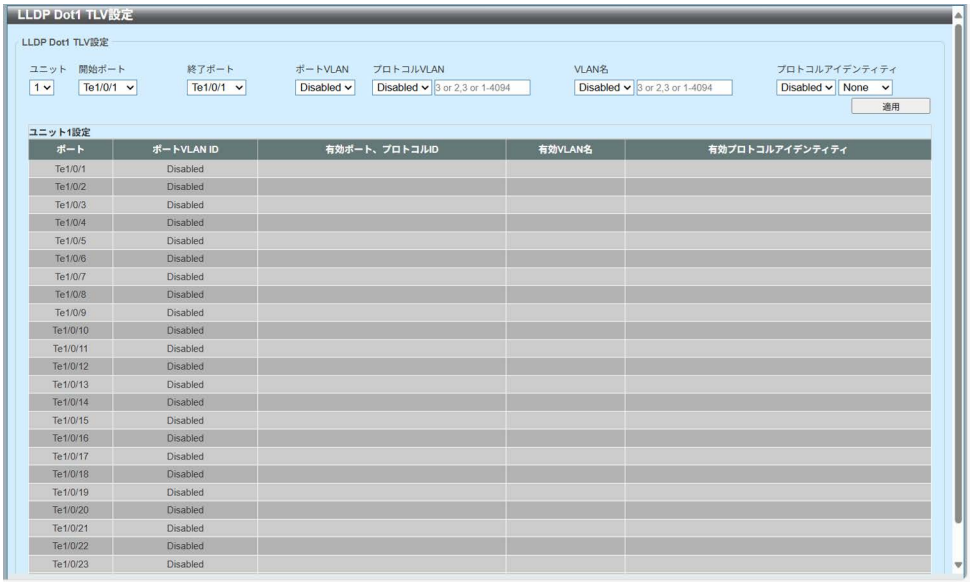

図 5-65 LLDP Dot1 TLV 設定

設定パラメータ （[LLDP Dot1 TLV 設定] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(初期値：Disabled)
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 5-66 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
MAC/PHY コンフィグレーション / 状態	MAC/PHY コンフィグレーション / 状態 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。(初期値 : Disabled)
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。(初期値 : Disabled)
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。(初期値 : Disabled)
Power Via MDI	Power via MDI TLV の送信の状態（**Enabled**/**Disabled**）を選択します。(初期値 : Enabled)
PoE 情報	Power via MDI 測定 TLV を送信の状態（**Enabled**/**Disabled**）を選択します。(初期値 : Enabled)

[**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。

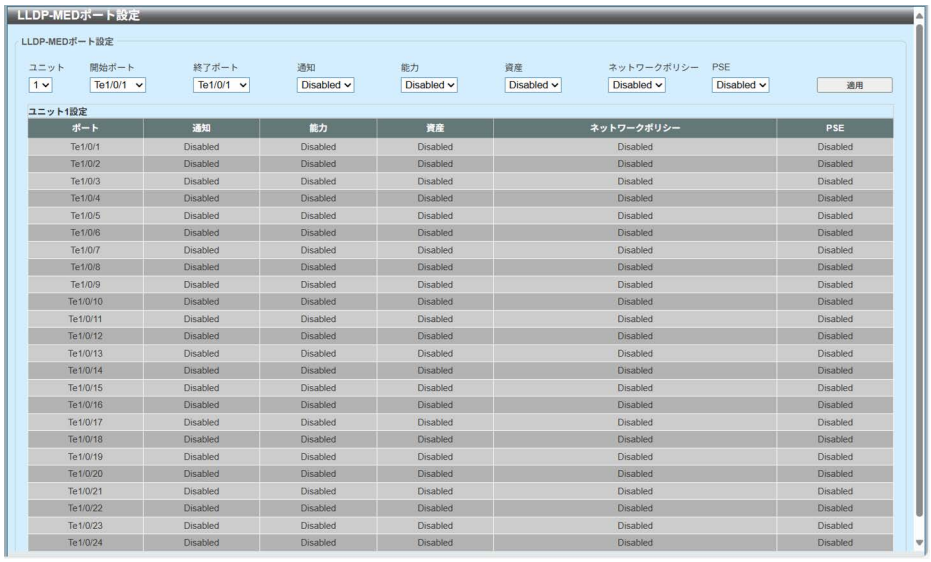

図 5-67 LLDP-MED ポート設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(初期値 : Disabled)
能力	LLDP-MED 能力 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。(初期値 : Disabled)
資産	LLDP-MED 資産管理 TLV の送信の状態（**Enabled**/**Disabled**）を選択します。(初期値 : Disabled)
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。(初期値 : Disabled)
PSE	LLDP-MED PSE（Power Sourcing Equipment）TLV の送信の状態（**Enabled**/**Disabled**）を選択します。 (初期値 : Disabled)

[**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。

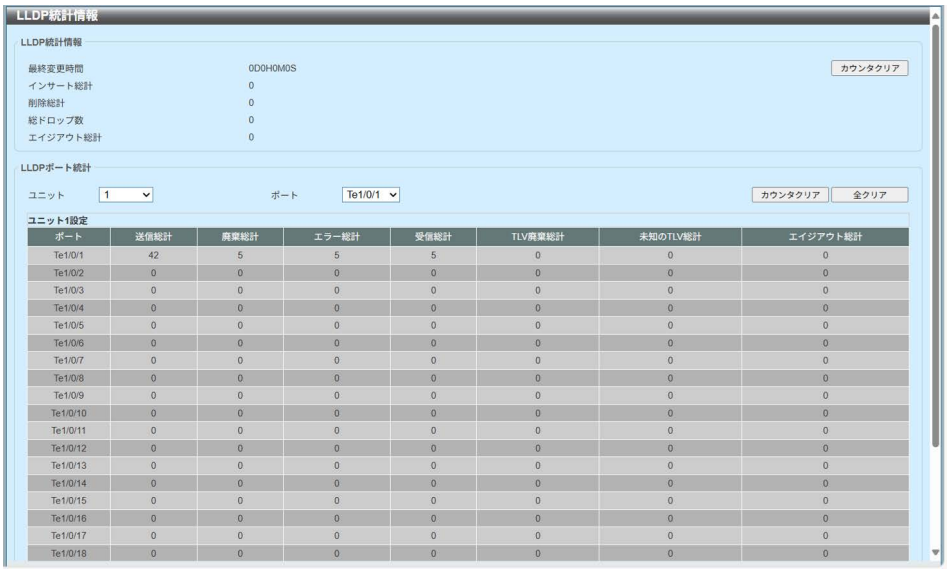

図 5-68 LLDP 統計情報

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
ポート	ポートを選択します。

[**カウンタクリア**] ボタン - カウンタ情報をクリアします。
[**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 5-69 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
[**詳細を表示**] ボタン - LLDP ローカルポート詳細情報を表示します。

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

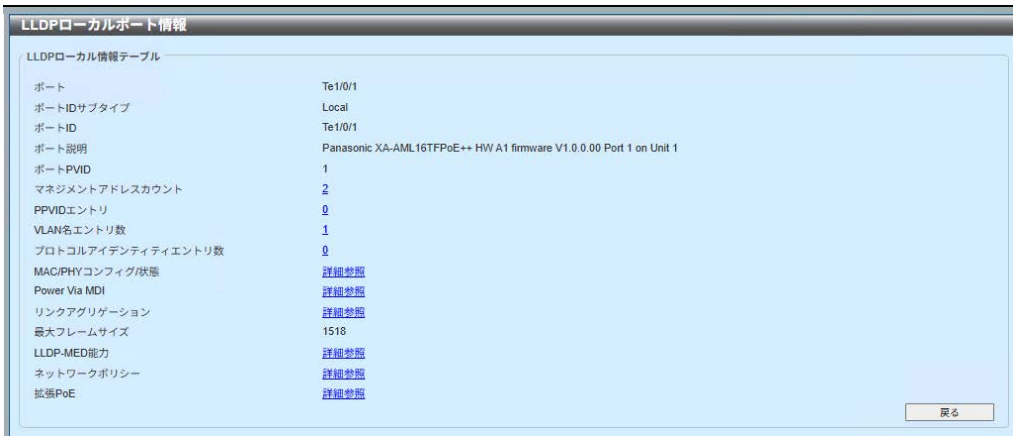

図 5-70 LLDP ローカルポート情報 (LLDP ローカル情報テーブル)

表内の各リンクをクリックして、該当機能に関する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 5-71 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 5-72 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 (**有効 / 無効**) を選択します。 （初期値：無効）
リンクフォールト検知状態	UDLD 機能 (**有効 / 無効**) を選択します。 （初期値：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。（初期値：5, 設定範囲：5 ～ 300） 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 (Enabled/Disabled) を選択します。 （**Disabled**：無効化 , **Enabled**：有効化 , 初期値：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 (Enabled/Disabled) を選択します。 （**Disabled**：無効化、**Enabled**：有効化、初期値：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。 「デフォルト」オプションを選択すると、**Passive** が適用されます。
（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	**Active**/**Passive**：インターフェースの EFM 動作モードを示します。
UDLD 状態	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。

（注意）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 5-73 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。 (初期値 : 無効)

[**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。(設定可能文字 : 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。

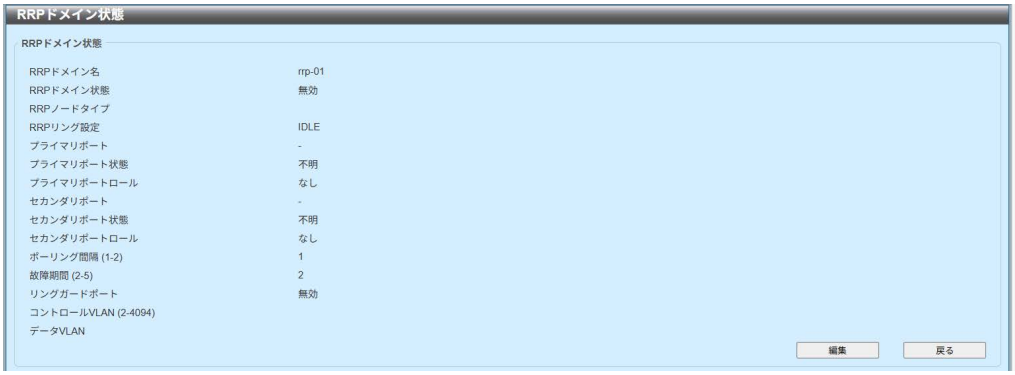

図 5-74 RRP（詳細参照）

[**編集**] ボタン - 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。

[**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。

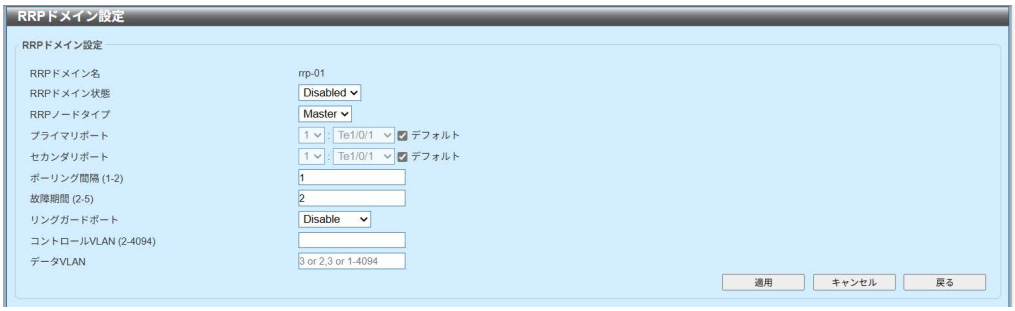

図 5-75 RRP（編集）

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。(Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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 ドメインに複数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。 （初期値：1, 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。（初期値：2, 設定範囲：2 ～ 5 秒）

パラメータ	概要
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、図 5-74 に戻ります。
[**戻る**] ボタン - 図 5-73 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 制御設定

このウィンドウを用いて、タイムアウト機能実行前の ARP リフレッシュを有効または無効にします。

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

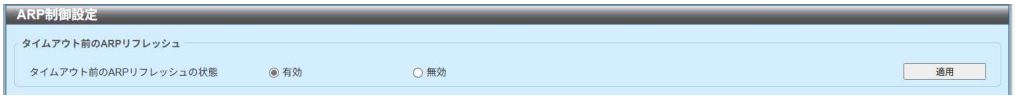

図 6-1 ARP 制御設定

設定パラメータ （[**タイムアウト前の ARP リフレッシュ**] セクション）

パラメータ	概要
タイムアウト前の ARP リフレッシュの状態	タイムアウト機能実行前の ARP リフレッシュ (**有効 / 無効**) を選択します。

[適用] ボタン - 変更を反映します。

6.1.2 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。

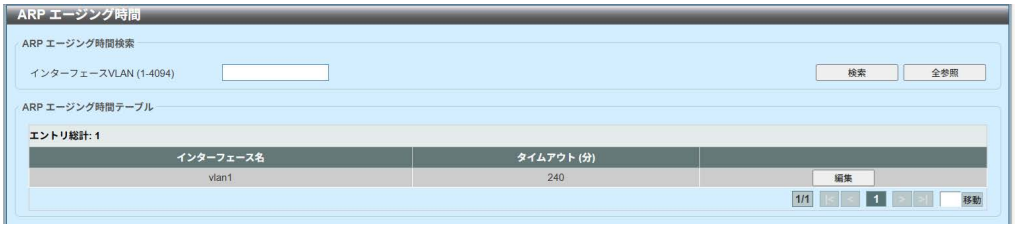

図 6-2 ARP エージング時間

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
インターフェース VLAN	VLAN ID を入力します。(設定範囲：1 ～ 4094)

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

設定パラメータ （[ARP エージング時間テーブル] セクション）

パラメータ	概要
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。(設定範囲：0 ～ 65535 分)

[編集] ボタン - エントリの設定を編集します。
[適用] ボタン - 変更を反映します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

6.1.3 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 6-3 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。
インターフェース 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。

設定パラメータ （[スタティック ARP テーブル] セクション）

パラメータ	概要
ハードウェアアドレス	エントリの MAC アドレスを入力します。

[**編集**] ボタン - エントリの設定を編集します。
[**適用**] ボタン - エントリの変更をします。
[**削除**] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

6.1.4 プロキシ ARP

このウィンドウを用いて、プロキシ ARP の設定を行い、設定値を表示します。プロキシ ARP では、IP アドレスと MAC アドレスを元の ARP レスポンダとして模倣することによって、スイッチは別の装置宛ての ARP リクエストに応答できるようになります。スイッチは、スタティックルートまたはデフォルトゲートウェイを追加せずに、意図したディスティネーションにパケットをルーティングできます。ホストは他の装置宛てのパケットに応答します。

[L3 機能] > [ARP] > [プロキシ 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 プロキシ ARP

設定パラメータ （[プロキシ ARP] セクション）

パラメータ	概要
プロキシ ARP 状態	**[編集]** ボタンをクリックした後、プロキシ ARP 状態 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)
ローカルプロキシ ARP 状態	**[編集]** ボタンをクリックした後、ローカルプロキシ ARP 状態 (**有効 / 無効**) を選択します。このローカルプロキシ ARP 機能により、ソース IP アドレスとディスティネーション IP アドレスが同じインタフェースにある場合、スイッチはプロキシ ARP に応答できます。

[編集] ボタン - エントリの設定を編集します。
[適用] ボタン - 新しいスタティック ARP エントリを追加します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

6.1.5 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 6-5 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
インターフェース **VLAN**	インターフェースの 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	タイプのオプションを選択します。選択する値は **[All]** および **[Dynamic]** です。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、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 - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 6-6 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。(初期値：無効)
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。(初期値：無効)
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。(初期値：無効)
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。(初期値：有効)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[Gratuitous ARP 送信間隔] 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 送信間隔時間を秒単位で入力します。 (初期値：0 秒 , 設定範囲：0 ～ 3600 秒)

[**編集**] ボタン - エントリの設定を編集します。
[適用] ボタン - 設定内容を反映します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 6-7 IPv6 ネイバー

設定パラメータ（[タイムアウト前の IPv6 ネイバーリフレッシュ] セクション）

パラメータ	概要
タイムアウト前の IPv6 ネイバーリフレッシュ状態	タイムアウト前の IPv6 ネイバーリフレッシュ状態（**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 （[IPv6 ネイバー設定] セクション）

パラメータ	概要
インターフェース VLAN	VLAN インターフェース 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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

```
FE80::200:FF:FE00%vlan1
```

6.4 インターフェース

6.4.1 IPv4 インターフェース

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

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

図 6-8 IPv4 インターフェース

設定パラメータ （[IPv4 インターフェース] セクション）

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

[適用] ボタン - 新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[編集] ボタン - 指定したエントリの設定を編集します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[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。

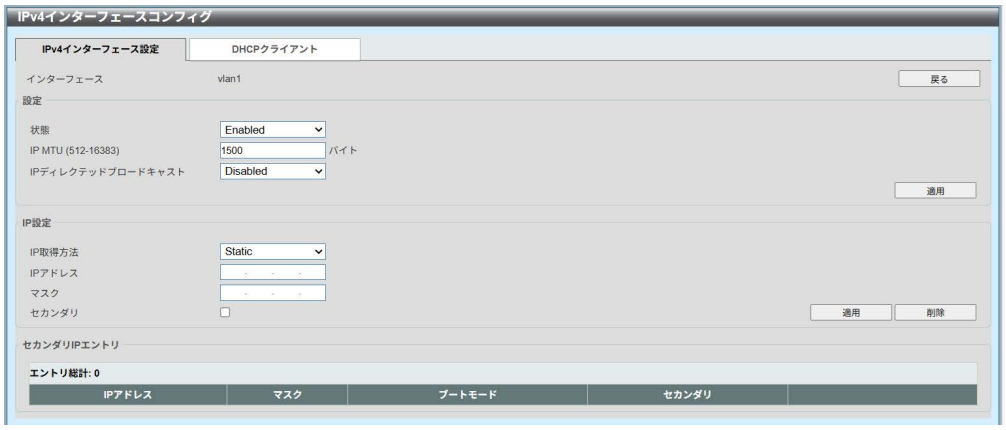

図 6-9 IPv4 インタフェース（編集、IPv4 インタフェース設定）

設定パラメータ （[設定] セクション）

パラメータ	概要
状態	IPv4 インタフェースのグローバル状態 (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)
IP MTU	MTU（Maximum Transmission Unit）値を入力します。(初期値：1500 バイト , 設定範囲：512 ～ 16383)
IP ディレクテッドブロードキャスト	IP ディレクテッドブロードキャスト機能 (**Enabled/Disabled**) を選択します。このパラメータを用いて、ディスティネーションネットワークがスイッチに直接接続されている場合に、インターフェースで受信した IP ディレクテッドブロードキャストの物理ブロードキャストへの変換を有効または無効にします。(Enabled：有効化 , Disabled：無効化)

[戻る] ボタン - 前のウィンドウに戻ります。
[適用] ボタン - 変更を反映します。

設定パラメータ （[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。選択する値は以下のとおりです。 • **[スタティック]** - 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]** - このインターフェースが、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	このインターフェースの IPv4 アドレスを入力します。
マスク	このインターフェースの IPv4 サブネットマスクを入力します。
セカンダリ	このオプションをオンにした場合、IPv4 アドレスとマスクをセカンダリインターフェース設定として使用します。

[適用] ボタン - 新しいエントリを追加します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[DHCP クライアント] タブをクリックして、以下のウィンドウを表示します。

図 6-10 IPv4 インタフェース（編集、DHCP クライアント）

設定パラメータ （[DHCP クライアント] セクション）

パラメータ	概要
DHCP クライアント クライアント ID	DHCP クライアント ID を入力します。(設定範囲 : 1 ～ 4094) このパラメータを用いて、discover メッセージで送信するクライアント ID としてその MAC アドレスの 16 進数表記を使用する VLAN インターフェースを指定します。
クラス ID 文字列	クラス ID の文字列を入力します。(設定可能文字 : 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。(設定可能文字 : 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。(設定可能文字 : 64 文字) 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。
リース	DHCP クライアントのリース期間を入力します。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 日) 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 - 変更を反映します。

6.4.2 IPv6 インターフェース

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

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

図 6-11 IPv6 インターフェース

設定パラメータ （[IPv6 インターフェース] セクション）

パラメータ	概要
インターフェース **VLAN**	IPv6 エントリに関連付ける VLAN インターフェース ID を入力します。

[適用] ボタン - 新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[詳細参照] ボタン - エントリに関する詳細情報を表示します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[詳細参照] 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 6-12 IPv6 インターフェース（詳細参照、IPv6 インターフェース設定）

設定パラメータ （[IPv6 インターフェース] セクション）

パラメータ	概要
IPv6 MTU	IPv6 MTU 値を入力します。(初期値：1500, 設定範囲：1280 ～ 65534 バイト) このパラメータを用いて、RA（ルータアドバタイズ）メッセージでアドバタイズする MTU を設定します。
IPv6 状態	IPv6 インターフェースのグローバル状態 (**Enabled/Disabled**) を選択します。(初期値：**Disabled**)

[戻る] ボタン - 前のウィンドウに戻ります。
[適用] ボタン - 変更を反映します。

設定パラメータ （[スタティック IPv6 アドレス設定] セクション）

パラメータ	概要
IPv6 アドレス	この IPv6 インターフェースの IPv6 アドレスを入力します。 • **[EUI-64]**（Extended Unique Identifier 64-bit）オプションを選択した場合、EUI-64 インターフェース ID を使用するインターフェースで IPv6 アドレスを設定します。 • **[リンクローカル]** オプションを選択した場合、IPv6 インター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 - 変更を反映します。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカル
アドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

[インターフェース IPv6 アドレス] タブをクリックして、
以下のウィンドウを表示します。

図 6-13 IPv6 インターフェース（詳細参照、インターフェース IPv6 アドレス）

[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[ネイバー探索] タブをクリックして、以下のウィンドウを表示します。

図 6-14 IPv6 インターフェース（詳細参照、ネイバー探索）

設定パラメータ （[ND 設定] セクション）

パラメータ	概要
管理コンフィグフラグ	**[管理コンフィグフラグ]** オプションを **[ON]** または **[OFF]** にします。ネイバーホストがフラグをオンにした RA を受信すると、そのホストはステートフルな設定プロトコルを用いて IPv6 アドレスを取得する必要があります。
Other Config フラグ	**[Other Config フラグ]** オプションを **[ON]** または **[OFF]** にします。他の設定フラグをオンにすると、ステートフル設定プロトコルを用いて IPv6 アドレス以外のオート設定情報を取得するよう、ルータは接続されているホストに指示します。
RA 最小間隔	RA 間隔時間の最小値を入力します。この値は、最大値を 0.75 倍した値よりも小さくなければなりません。 (設定範囲：3 ～ 1350 秒)
RA 最大間隔	RA 間隔時間の最大値を入力します。 (設定範囲：4 ～ 1800 秒)
RA ライフタイム	RA ライフタイムの値を入力します。RA のライフタイム値は、RA を受信したホストに、ルータをデフォルトルータとみなすライフタイム値を伝えます。(設定範囲：0 ～ 9000 秒)
RA 抑制	RA 抑制機能 (**Enabled/Disabled**) を選択します。
到達可能時間	到達可能時間を入力します。指定した時間が 0 の場合、ルータはインターフェースで 1200 秒を使用し、RA メッセージで 1200（未指定）をアドバタイズします。到達可能時間は、IPv6 ノードによるネイバーノードの到達可能性の判断に使用されます。(設定範囲：0 ～ 3600000 ミリ秒)
NS 間隔	NS（Neighbor Solicitation）間隔の値を入力します。指定した時間が 0 の場合、ルータは 1 秒を使用します。 (初期値：0, 設定範囲：0 ～ 3600000 ミリ秒（1000 の倍数）)
ホップリミット	ホップリミット値を入力します。システムで生成された IPv6 パケットは、この値を初期ホップリミットとしても使用します。(設定範囲：0 ～ 255)

[適用] - 新しいエントリを追加します。
[編集] - 指定したエントリの設定を編集します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[DHCPv6 クライアント] タブをクリックして、以下のウィンドウを表示します。

図 6-15 IPv6 インタフェース（詳細参照、DHCPv6 クライアント）

[リスタート] - DHCPv6 クライアント機能を再開します。

設定パラメータ （[DHCPv6 クライアント設定] セクション）

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 (**Enabled/Disabled**) を選択します。(Enabled : 有効化 , Disabled : 無効化) **[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。(初期値 : Disabled)

設定パラメータ （[DHCPv6 クライアント PD 設定] セクション）

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 (**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。 (Enabled : 有効化 , Disabled : 無効化 , 初期値 : Disabled)
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。 (設定可能文字 : 12 文字)
IPv6 DHCP クライアント **PD** ヒント	メッセージでヒントとして送信する IPv6 プレフィックスを入力します。

[適用] - 変更を反映します。

6.4.3 ループバックインターフェース

このウィンドウを用いて、ループバックインターフェースの設定を行い、設定値を表示します。

[L3 機能] > [インターフェース] > [ループバックインターフェース] をクリックして、以下のウィンドウを表示します。

図 6-16 ループバックインターフェース

設定パラメータ （[ループバックインターフェース] セクション)

パラメータ	概要
インターフェースループバック	ループバックインターフェース ID を入力します。 (設定範囲：1 ～ 8)

[適用] ボタン - 新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[編集] ボタン - 指定したエントリの設定を編集します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[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 6-17 ループバックインターフェース設定

[戻る] ボタン - 前のウィンドウに戻ります。
[適用] ボタン - 変更を反映します。

最初のセクションでは、以下のパラメータを設定できます。

パラメータ	概要
状態	ループバックインターフェース (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

設定パラメータ （[IPv4] セクション)

パラメータ	概要
IP アドレス	ループバックインターフェースに関連付けられている IPv4 アドレスを入力します。
マスク	ループバックインターフェースに関連付けられている IPv4 サブネットマスクを入力します。

[適用] ボタン - 変更を反映します。

設定パラメータ （[IPv6]セクション)

パラメータ	概要
IPv6 アドレス	ループバックインターフェースに関連付けられている IPv6 アドレスを入力します。[**リンクローカル**] オプションを選択すると、IPv6 インター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 - 変更を反映します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

（注意）FE80から始まるIPv6のリンクローカルアドレスを
使用する場合は、以下のように入力してください：
例：インターフェース VLAN 1のIPv6 リンクローカル
アドレス "FE80::200:FF:FE00"を指定する。

FE80::200:FF:FE00%vlan1

6.4.4 Null インターフェース

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

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

図 6-18 Null インターフェース

設定パラメータ （[Null インターフェース] セクション)

パラメータ	概要
インターフェース **Null**	Null インターフェース ID を入力します。この値は必ず 0 です。

[適用] ボタン - 新しいエントリを追加します。

6.5 IPv4 スタティック / デフォルトルート

このウィンドウを用いて、IPv4 スタティックルートおよび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 スタティック / 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 6-19 IPv4 スタティック / デフォルトルート

設定パラメータ ([IPv4 スタティック / デフォルトルート] セクション)

パラメータ	概要
IP アドレス	このルートの IPv4 アドレスを入力します。**[デフォルトルート]** オプションをオンにした場合、IPv4 アドレスとしてデフォルトルートを使用します。
マスク	このルートの IPv4 ネットワークマスクを入力します。
ゲートウェイ	このルートのゲートウェイアドレスを入力します。
Null インターフェース	NULL インターフェース (**Enabled/Disabled**) を選択します。(Enabled：有効化 , Disabled：無効化)
バックアップ状態	バックアップ状態のオプションを選択します。選択する値は以下のとおりです。 • **[Primary]** - ルートをディスティネーションへのプライマリルートとして指定します。 • **[Backup]** - ルートをディスティネーションへのバックアップルートとして指定します。

[適用] ボタン - 新しいエントリを追加します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 6-20 IPv4 ルートテーブル

設定パラメータ （[IPv4 ルートテーブル] セクション)

パラメータ	概要
IP アドレス	単一の IPv4 アドレスを選択および入力します。
ネットワークアドレス	IPv4 ネットワークアドレスを選択および入力します。1 つ目（左側）の入力フィールドにネットワークプレフィックスを入力し、2 つ目（右側）の入力フィールドにネットワークマスクを入力します。
RIP	このオプションを選択した場合、RIP ルートのみを表示します。
接続	このオプションを選択した場合、接続されたルートのみを表示します。
ハードウェア	このオプションを選択した場合、ハードウェアルートのみを表示します。ハードウェアルートは、ハードウェアチップに書き込まれたルートです。
要約	このオプションを選択した場合、このスイッチに設定されているルートソースの要約および数を表示します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[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。

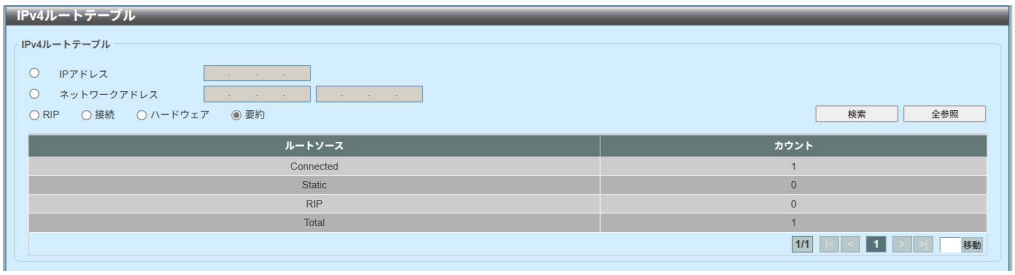

図 6-21 IPv4 ルートテーブル（要約）

6.7 IPv6 スタティック / デフォルトルート

このウィンドウを用いて、IPv6 スタティックルートまたは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 スタティック / 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 6-22 IPv6 スタティック / デフォルトルート

設定パラメータ （[**IPv6 スタティック / デフォルトルート**] セクション)

パラメータ	概要
IPv6 アドレス / プレフィックス長	このルートの IPv6 アドレスとプレフィックス長を入力します。[**デフォルトルート**] オプションをオンにした場合、このルートをデフォルトルートで使用します。
インターフェース名	このルートに関連付けるインターフェースの名前を入力します。(設定可能文字：12 文字)
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。
距離	スタティックルートの管理上の距離を入力します。値が小さいほど良いルートになります。指定しない場合、スタティックルートの管理上の距離は初期値になります。 (初期値：1, 設定範囲：1 ～ 254)
バックアップ状態	バックアップ状態のオプションを選択します。選択する値は以下のとおりです。 • **[Primary]** - ルートをディスティネーションへのプライマリルートとして指定します。 • **[Backup]** - ルートをディスティネーションへのバックアップルートとして指定します。

[適用] ボタン - 新しいエントリを追加します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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 6-23 IPv6 ルートテーブル

設定パラメータ （[**IPv6 ルートテーブル**] セクション)

パラメータ	概要
IPv6 Address	表示する IPv6 アドレスを選択および入力します。
IPv6 Address/ Prefix Length	表示する IPv6 アドレスとプレフィックス長を選択および入力します。**[より長いプレフィックス]** オプションを選択した場合、ルート、およびより具体的なすべてのルートを表示します。
Interface Name	表示するインターフェースの名前を選択および入力します。(設定可能文字：12 文字)
Connected	このオプションを選択した場合、接続されたルートのみを表示します。
データベース	このオプションを選択した場合、単なる最適ルートの代わりに、ルーティングデータベース内の関連するエントリをすべて表示します。
ハードウェア	このオプションを選択した場合、ハードウェアルートのみを表示します。ハードウェアルートは、ハードウェアチップに書き込まれたルートです。
要約	このオプションを選択した場合、このスイッチに設定されているルートソースの要約および数を表示します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

（注意）FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

[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。

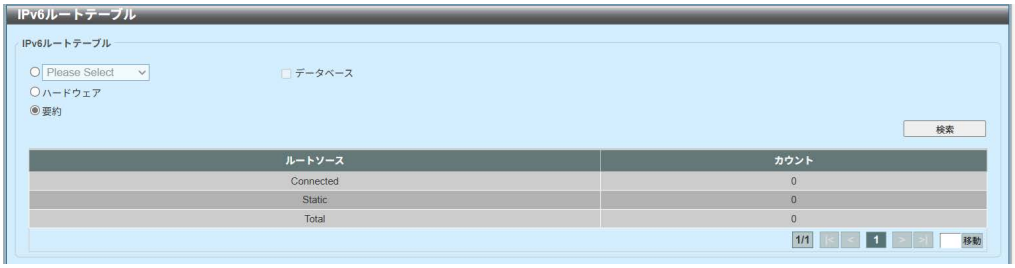

図 6-24 IPv6 ルートテーブル（要約）

6.9 ルートプリファレンス

このウィンドウを用いて、ルートプリファレンスの設定を行い、設定値を表示します。

[L3 機能] > [ルートプリファレンス] をクリックして、以下のウィンドウを表示します。

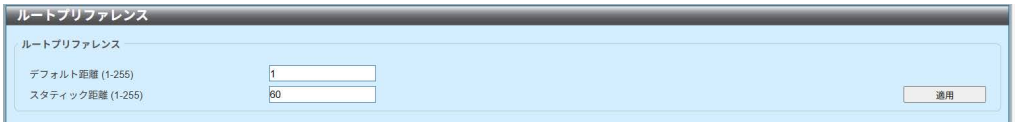

図 6-25 ルートプリファレンス

設定パラメータ （[**ルートプリファレンス**] セクション)

パラメータ	概要
デフォルト距離	デフォルトルートの管理上の距離を入力します。 (初期値：1, 設定範囲：1 ～ 255)
スタティック距離	スタティックデフォルトルートの管理上の距離を入力します。 (初期値：60, 設定範囲：1 ～ 255)

[適用] ボタン - 変更を反映します。

6.10 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 6-26 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
インターフェース VLAN	使用する VLAN インターフェース 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。 (設定可能文字 : 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 インター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 - 新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

(注意)
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください :

例 : インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

6.11 RIP（Routing Information Protocol）

6.11.1 RIP 設定

このウィンドウを用いて、RIP 設定を行い、設定値を表示します。

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

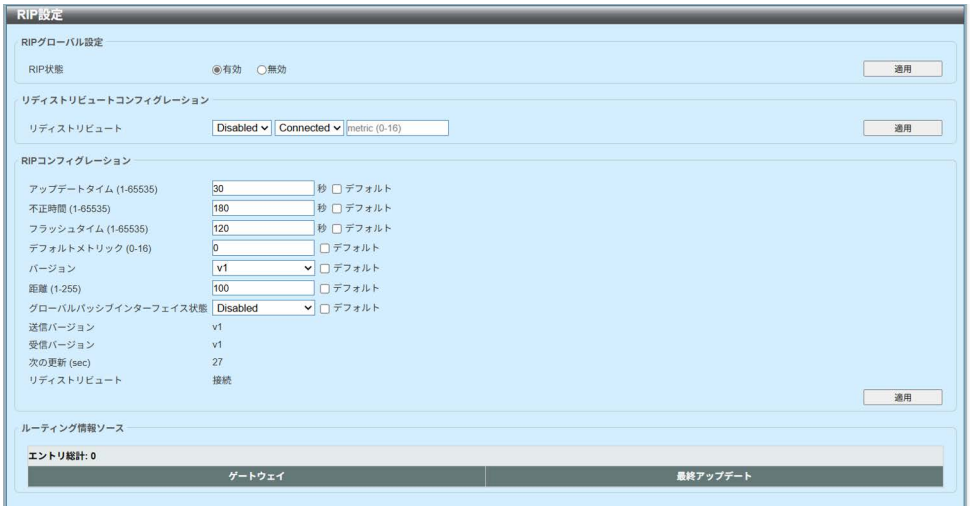

図 6-27 RIP 設定

設定パラメータ （[**RIP グローバル設定**] セクション

パラメータ	概要
RIP 状態	RIP 機能をグローバルに (**有効 / 無効**) を選択します。

[適用] ボタン - 変更を反映します。

設定パラメータ （[リディストリビュートコンフィグレーション] セクション）

パラメータ	概要
リディストリビュート	RIP 再配布機能 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化) RIP に再配布するルーティングプロトコル（ドメイン）を選択します。選択する値は **[Connected]**、**[Static]** です。 • **[Connected]** オプションは、インターフェースでの IP アドレス設定を通じて自動的に確立されるルートを示します。 • **[Static]** オプションは、IP スタティックルートの再配布を意味します。 再配布ルートのメトリック値を表示された入力フィールドに入力します。(設定範囲：0 ～ 16)

[適用] ボタン - 変更を反映します。

設定パラメータ（[RIP コンフィグレーション] セクション）

パラメータ	概要
アップデートタイム	アップデート間隔を秒単位で入力します。この間隔でアップデートメッセージが送信されます。**[デフォルト]** オプションを選択した場合、初期値を使用します。 (初期値：30 秒 , 設定範囲：1 ～ 65535 秒)
不正時間	不正時間の値を秒単位で入力します。**[デフォルト]** オプションを選択した場合、初期値を使用します。 (初期値：180 秒 , 設定範囲：1 ～ 65535 秒)
フラッシュタイム	フラッシュタイム値を秒単位で入力します。**[デフォルト]** オプションを選択した場合、初期値を使用します。 (初期値：120 秒 , 設定範囲：1 ～ 65535 秒)
デフォルトメトリック	デフォルトのメトリック値を入力します。デフォルトメトリックを用いて、他のルーティングプロトコルからルートを再配布します。再配布されているルートは他のプロトコルによって学習されるため、RIP ではメトリックの互換性がない可能性があります。メトリックの指定により、メトリックの同期が可能になります。**[デフォルト]** オプションを選択した場合、初期値を使用します。 (初期値：0, 設定範囲：0 ～ 16)
バージョン	すべてのインターフェースのデフォルトバージョンとして使用するグローバル RIP バージョンを選択します。選択する値は **[v1]**（RIPv1）および **[v2]**（RIPv2）です。**[デフォルト]** オプションを選択した場合、この機能ではデフォルト設定が使用されます。デフォルトでは、RIPv1 パケットと RIPv2 パケットが受信されますが、送信されるのは RIPv1 パケットのみです。

パラメータ	概要
距離	RIP の管理上の距離を入力します。値が小さいほど良いルートになります。[デフォルト] オプションを選択した場合、初期値を使用します。(初期値：100, 設定範囲：1 ～ 255)
グローバルパッシブインターフェース状態	パッシブインターフェース状態をグローバルに (**Enabled/Disabled**) を選択します。この機能を有効にすると、RIP ルーティングアップデートの送信がグローバルに無効化されます。[デフォルト] オプションを選択した場合、グローバルなパッシブインターフェースの状態は無効に設定されます。(Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

6.11.2 RIP インターフェース設定

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

[L3 機能] > [RIP] > [RIP 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 6-28 RIP インターフェース設定

設定パラメータ（[RIP インターフェース設定] セクション）

パラメータ	概要
ネットワーク	RIP が使用する IPv4 ネットワークアドレスを入力します。インターフェースに定義されているサブネットが指定したネットワークに属する場合、そのインターフェースは RIP で有効になります。

[追加] - 新しいエントリを追加します。
[削除] - 指定したエントリを削除します。
[編集] - 指定したエントリの設定を編集します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[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 6-29 RIP インターフェース設定（編集）

設定パラメータ（[RIP インターフェースの設定] セクション）

パラメータ	概要
送信バージョン	インターフェースで RIP パケットの送信に使用する RIP バージョンを選択します。選択する値は **[v1]**（RIP バージョン 1）および **[v2]**（RIP バージョン 2）です。
受信バージョン	インターフェースで RIP パケットの受信に使用する RIP バージョンを選択します。選択する値は **[v1]**（RIP バージョン 1）、**[v2]**（RIP バージョン 2）、および **[v1/v2]**（RIP バージョン 1 または 2）です。
v2-broadcast 送信	マルチキャストパケットではなくブロードキャストパケットとしての RIP バージョン 2 アップデートパケットの送信を有効または無効にします。
認証モード	認証モードを選択します。選択する値は **[Disabled]** および **[Text]** です。
認証テキストパスワード	認証テキストパスワードを選択および入力します。この値は最大 16 文字で指定でき、**[認証モード]** で **[Text]** を選択した場合にのみ入力可能です。
パッシブインターフェース	パッシブインターフェースオプション (**Enabled/Disabled**) を選択します。この機能を有効にすると、このインターフェースでの RIP ルーティングアップデートの送信が無効化されます。(Enabled : 有効化 , Disabled : 無効化)

[戻る] - 前のウィンドウに戻ります。
[適用] - 変更を反映します。

6.11.3 RIP データベース

このウィンドウを用いて、RIP ルーティングデータベースを表示します。

[L3 機能] > [RIP] > [RIP 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 6-30 RIP データベース

設定パラメータ（[RIP データベース] セクション）

パラメータ	概要
ネットワークアドレス	表示するネットワークのサブネットプレフィックスとプレフィックス長を入力します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

6.12 IP マルチキャストルーティングプロトコル

6.12.1 IGMP プロキシ

6.12.1.1 IGMP プロキシ設定

このウィンドウを用いて、IGMP プロキシの設定を行い、設定値を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [IGMP プロキシ] > [IGMP プロキシ設定] をクリックして、以下のウィンドウを表示します。

図 6-31 IGMP プロキシ設定

設定パラメータ（[IGMP プロキシグローバル設定] セクション）

パラメータ	概要
グローバル状態	IGMP プロキシ機能をグローバルに (**有効 / 無効**) を選択します。

[適用] ボタン - 変更を反映します。

設定パラメータ（[IGMP プロキシアップストリーム設定] セクション）

パラメータ	概要
インターフェース **VLAN**	VLAN インターフェース ID を入力します。 (設定範囲：1 ～ 4094)
アップストリーム	アップストリーム IGMP プロキシとしてインターフェース (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

設定パラメータ（[IGMP プロキシダウンストリーム設定] セクション）

パラメータ	概要
インターフェース **VLAN**	VLAN インターフェース ID を入力します。 (範囲：1 ～ 4094)
ダウンストリーム	ダウンストリーム IGMP プロキシとしてインターフェース (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

設定パラメータ（[IGMP プロキシ代表フォワーディング設定] セクション）

パラメータ	概要
インターフェース **VLAN**	VLAN インターフェース ID を入力します。 (範囲：1 ～ 4094)
代表フォワーディング	非クエリア IGMP プロキシダウンストリームインターフェースで、代表フォワーディング (**Enabled/Disabled**) を選択します。複数の IGMP ベースフォワーダによるダウンストリームリンクとみなされるリンクのローカルループや冗長トラフィックを回避するため、IGMP プロキシでは IGMP クエリアを用いて、LAN 上に単一のフォワーダを選定します。このオプションを用いて、非クエリア装置をフォワーダにすることができます。インターフェースがダウンストリームインターフェースとして設定されていない場合、あるいはアップストリームインターフェースとして設定されている場合、この機能は有効になりません。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

6.12.1.2 IGMP プロキシグループテーブル

このウィンドウを用いて、IGMP プロキシグループテーブルおよび情報を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [IGMP プロキシ] > [IGMP プロキシグループテーブル] をクリックして、以下のウィンドウを表示します。

図 6-32 IGMP プロキシグループテーブル

設定パラメータ（[IGMP プロキシグループテーブル] セクション）

パラメータ	概要
グループアドレス	IPv4 グループマルチキャストアドレスを入力します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

6.12.1.3 IGMP プロキシフォワーディングテーブル

このウィンドウを用いて、IGMP プロキシフォワーディングテーブルおよび情報を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [IGMP プロキシ] > [IGMP プロキシフォワーディングテーブル] をクリックして、以下のウィンドウを表示します。

図 6-33 IGMP プロキシフォワーディングテーブル

設定パラメータ（[IGMP プロキシ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	IPv4 グループマルチキャストアドレスを入力します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

6.12.2 MLD プロキシ

6.12.2.1 MLD プロキシ設定

このウィンドウを用いて、MLD プロキシの設定を行い、設定値を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [MLD プロキシ] > [MLD プロキシ設定] をクリックして、以下のウィンドウを表示します。

図 6-34 MLD プロキシ設定

設定パラメータ（[MLD プロキシグローバル設定] セクション）

パラメータ	概要
グローバル状態	MLD プロキシ機能 (**有効 / 無効**) を選択します。

[適用] ボタン - 変更を反映します。

設定パラメータ（[MLD プロキシアップストリーム設定] セクション）

パラメータ	概要
インターフェース **VLAN**	VLAN インターフェース ID を入力します。 (設定範囲：1 ～ 4094)
アップストリーム	アップストリーム MLD プロキシとしてのインターフェース (**Enabled/Disabled**) を選択します。この機能は、インターフェースに IPv6 アドレスが設定されている場合にのみ有効です。MLD プロキシ装置に存在可能なアップストリームインターフェースは 1 つだけです。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

設定パラメータ（**[MLD プロキシダウンストリーム設定]** セクション）

パラメータ	概要
インターフェース **VLAN**	VLAN インターフェース ID を入力します。 (設定範囲：1 ～ 4094)
ダウンストリーム	ダウンストリーム MLD プロキシとしてインターフェース (**Enabled/Disabled**) にします。この機能は、インターフェースに IPv6 アドレスが設定されている場合にのみ有効です。複数のダウンストリームインターフェースを 1 つの MLD プロキシ装置に設定できます。 (Enabled：有効化 , Disabled：無効化)

[適用] ボタン - 変更を反映します。

設定パラメータ（**[MLD プロキシ代表フォワーディング設定]** セクション）

パラメータ	概要
インターフェース **VLAN**	VLAN インターフェース ID を入力します。 (設定範囲：1 ～ 4094)
代表フォワーディング	非クエリア MLD プロキシダウンストリームインターフェースで、代表フォワーディングを有効または無効にします。複数の MLD ベースフォワーダによるダウンストリームリンクとみなされるリンクのローカルループや冗長トラフィックを回避するため、MLD プロキシでは MLD クエリアを用いて、LAN 上に単一のフォワーダを選定します。管理者はこのコマンドを用いて、非クエリア装置をフォワーダにすることができます。インターフェースがダウンストリームインターフェースとして設定されていない場合、あるいはアップストリームインターフェースとして設定されている場合、この機能は有効になりません。

[適用] ボタン - 変更を反映します。

6.12.2.2 MLD プロキシグループテーブル

このウィンドウを用いて、MLD プロキシグループテーブルおよび情報を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [MLD プロキシ] > [MLD プロキシグループテーブル] をクリックして、以下のウィンドウを表示します。

図 6-35 MLD プロキシグループテーブル

設定パラメータ（**[MLD プロキシグループテーブル]** セクション）

パラメータ	概要
グループアドレス	IPv6 グループマルチキャストアドレスを入力します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

6.12.2.3 MLD プロキシフォワーディングテーブル

このウィンドウを用いて、MLD プロキシフォワーディングテーブルおよび情報を表示します。

[L3 機能] > [IP マルチキャストルーティングプロトコル] > [MLD プロキシ] > [MLD プロキシフォワーディングテーブル] をクリックして、以下のウィンドウを表示します。

図 6-36 MLD プロキシフォワーディングテーブル

設定パラメータ（**[MLD プロキシ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	IPv6 グループマルチキャストアドレスを入力します。

[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

6.12.3 IPMC

6.12.3.1 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 6-37 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 - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

6.12.4 IPv6MC

6.12.4.1 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テーブル情報を表示します。

[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 6-38 IP 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 - 指定した検索条件に基づいてエントリを検索し、表示します。
[全参照] ボタン - 利用可能なエントリをすべて検索し、表示します。

6.13 VRRP 設定

このウィンドウを用いて、VRRP（Virtual Router Redundancy Protocol）の設定を行い、設定値を表示します。

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

図 6-39 VRRP 設定

設定パラメータ （**[VRRP 設定]** セクション）

パラメータ	概要
SNMP サーバトラップ VRRP ニューマスタ	新しい VRRP マスターに対応する SNMP サーバトラップ機能 (**有効 / 無効**) にします。有効にすると、装置がマスター状態に移行した後にトラップが送出されます。
SNMP サーバトラップ VRRP 認証失敗	認証の失敗に対応する SNMP サーバトラップ機能 (**有効 / 無効**) を選択します。有効にすると、パケットを受信したルータの認証キーまたは認証タイプがこのルータのものと競合する場合に、トラップが送出されます。
Non-owner-ping Response	Non-owner-ping Response 機能 (**有効 / 無効**) を選択します。この機能を用いて、この仮想ルータに関連付けられている非オーナー IP アドレスに対して、マスター状態の仮想ルータが ICMP（Internet Control Message Protocol）エコーリクエストに応答できるようにします。

[適用] ボタン - 変更を反映します。

設定パラメータ （**[仮想ルータ設定]** セクション）

パラメータ	概要
インターフェース VLAN	使用する VLAN インターフェース ID を入力します。 (設定範囲：1 ～ 4094)
VRID	使用する仮想ルータ ID を入力します。この ID を用いて、VRRP グループ内の仮想ルータを識別します。 (設定範囲：1 ～ 255)
仮想 IP アドレス	作成した仮想ルータグループの IPv4 アドレスを入力します。
VRRP 認証	チェックボックスをオンにした後、インターフェースでの VRRP 認証用にプレーンテキスト認証パスワードを入力します。この文字列は 8 文字までです。このインターフェースのすべての仮想ルータに認証が適用されます。同じ VRRP グループ内の装置には、同じ認証パスワードが必要です。
インターフェース名	使用するインターフェース名を入力し、検索します。 (設定可能文字：12 文字)

[適用] ボタン - 新しいエントリを追加します。
[検索] ボタン - 指定した検索条件に基づいてエントリを検索し、表示します。
[編集] ボタン - 指定したエントリの設定を編集します。
[削除] ボタン - 指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

[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 6-40 VRRP 設定（編集）

設定パラメータ （**[VRRP 仮想ルータ設定 (編集)]** セクション）

パラメータ	概要
アドバタイズ間隔	ここにアドバタイズの間隔の値を入力します。これは、マスタールータによる連続する VRRP アドバタイズの時間間隔です。(初期値：1 秒 , 設定範囲：1 ～ 255 秒)
プリエンプション	プリエンプション機能 (**Enabled/Disabled**) を選択します。この機能を用いて、現在のマスターよりも優先度の高いルータがマスターの役割を引き継げるようにします。
優先度	優先度値を入力します。(初期値：100, 設定範囲：1 ～ 254)
クリティカル IP アドレス	クリティカル IPv4 アドレスを入力します。1 つの仮想ルータにクリティカル IP アドレスを設定すると、クリティカル IP アドレスが到達不能な場合、その仮想ルータは有効になりません。1 つの VRRP グループが追跡できるのは、1 つのクリティカル IP アドレスだけです。
シャットダウン	シャットダウン機能 (**Enabled/Disabled**) を選択します。この機能を用いて、インターフェースの仮想ルータを無効にします。よくある誤りとして、他の非オーナールータをシャットダウンする前に IP アドレスオーナールータをシャットダウンしないでください。

[戻る] ボタン - 前のウィンドウに戻ります。
[適用] ボタン - 変更を反映します。

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、ポートインター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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(初期値 : 0) • **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 インターフェーススケジュール設定

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] > [インターフェーススケジュール設定] をクリックして、以下のウィンドウを表示します。

図 7-2 インターフェーススケジュール設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
プロファイル ID	プロファイル ID を選択します。 （初期値：1, 設定範囲：1 ～ 8）

[**適用**] ボタン - 設定内容を反映します。

7.1.3 スケジュールプロファイル設定

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] > [スケジュールプロファイル設定] をクリックして、以下のウィンドウを表示します。

図 7-3 スケジュールプロファイル設定

設定パラメータ （[スケジュール方式] セクション）

パラメータ	概要
プロファイル ID	スケジュール方式のプロファイル ID を選択します。 （設定範囲：1 ～ 8）
スケジュール方式	スケジュール方式からプロファイル ID に適用する方式を選択します。 • **SP** - すべてのキューに対して、優先度の厳密な制御を行います。 • **WRR** - フレーム数に基づいて重み付けされたラウンドロビン形式で処理を行います。 • **WDRR** - フレーム長に基づいて、全ポートのキューに対して重み付けされた不足分ラウンドロビン方式で処理を行います。 デフォルトを選択した場合、デフォルト値（WRR）を使用します。

設定パラメータ （[キュー設定] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
プロファイル ID	スケジュール方式のプロファイル ID を選択します。 （設定範囲：1 ～ 8）
キュー ID	キュー ID 値を入力します。（設定範囲：0 ～ 7）
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。

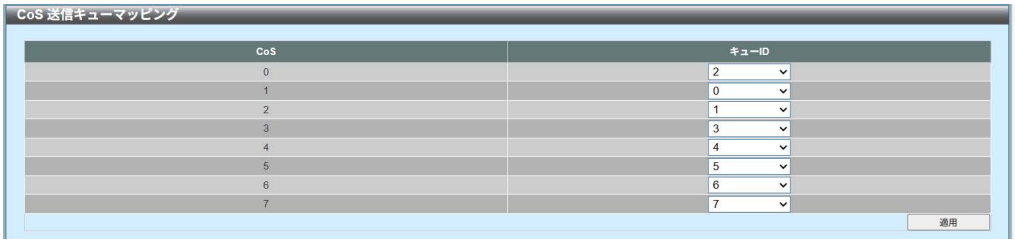

図 7-4 CoS 送信キューマッピング

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。(デフォルト “CoS とキュー ID”: 0 と 2, 1 と 0, 2 と 1, 3 と 3, 4 と 4, 5 と 5, 6 と 6, 7 と 7)

[**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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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：帯域幅 : 64 ～ 40000000Kbps, バーストサイズ : 0 ～ 128000Kbyte） • **[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：パーセント :1 ～ 100%, バーストサイズ : 0 ～ 128000Kbyte） • **[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ー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、入口でポーズ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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 • **[最大帯域]** - 帯域制限の最大帯域を入力します。最大帯域幅を設定すると、キューから送信されるパケットが最大帯域幅を超えることはありません。 （設定範囲：64 ～ 40000000Kbps） • **[最大パーセント]** - 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。（設定可能文字：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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。

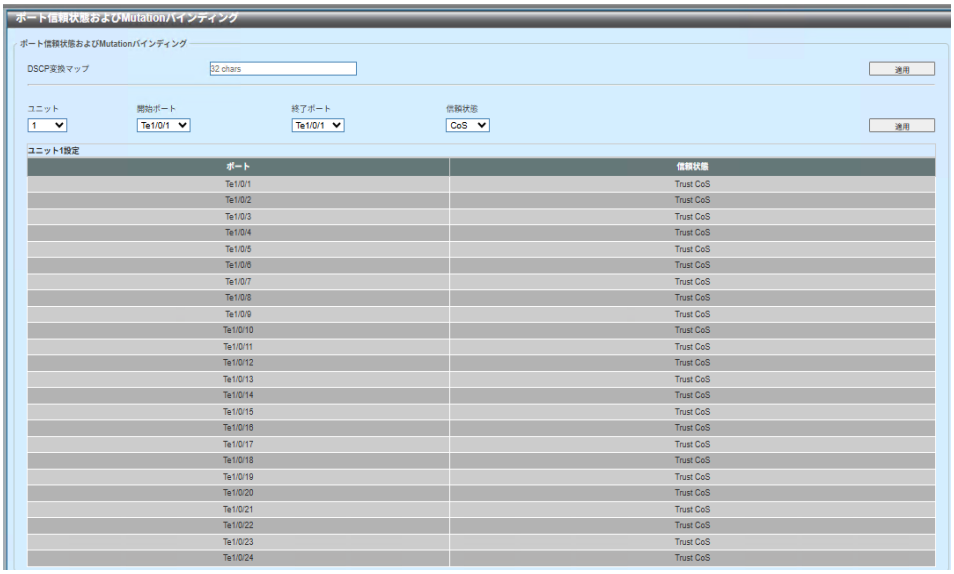

図 7-8 ポート信頼状態および Mutation バインディング

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (初期値 : CoS)
DSCP 変換マップ	DSCP 変換マップ名を入力します。(設定可能文字 : 32 文字)

[**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
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。

DSCP CoS マッピング設定のデフォルトエントリは以下の通りです。

CoS Value	0	1	2	3	4	5	6	7
DSCP List	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

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。

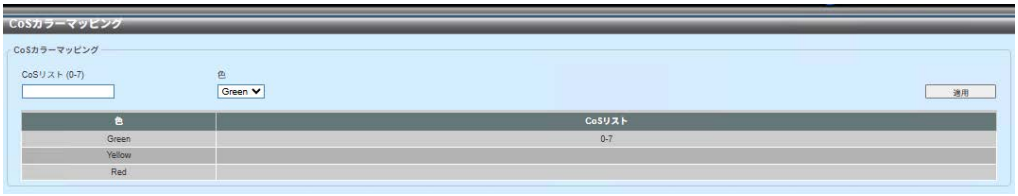

図 7-10 CoS カラーマッピング

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
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。(初期値 : Green)

[**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

設定パラメータ（**[DSCP カラーマッピング]** セクション）

パラメータ	概要
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。（初期値：Green）

[**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。（設定可能文字：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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

[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。

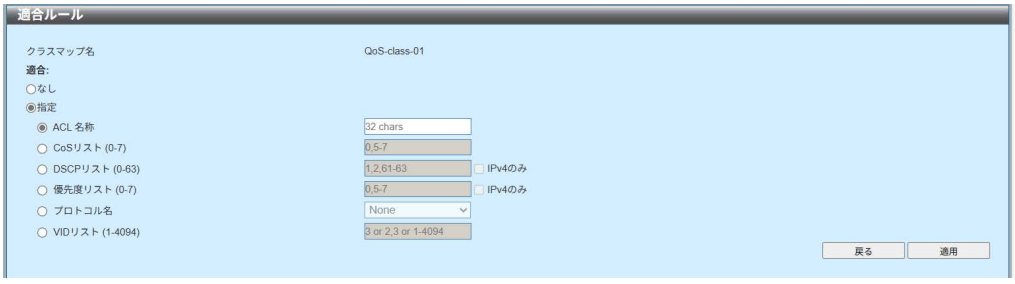

図 7-13 クラスマップ（適合）

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。（設定可能文字：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 (ex1,3)、またはハイフン区切り (ex1-3) 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 ～ 10000000Kbps）
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。設定しない場合の値は 12 になります。 （設定範囲：0 ～ 16384Kbyte）
最大バーストサイズ	最大バーストサイズを入力します。 (設定範囲：0 ～ 16384Kbyte)
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、カラーマッピングが Green のパケットに対して実行するアクションを指定します。指定しない場合、デフォルトのアクションを指定します。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。デフォルトのアクションです。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

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際にカラーマッピングが Yellow のパケットに対して実行するアクションを指定します。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。デフォルトのアクションです。 • **Set-DSCP-1P -** 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。
違反時アクション	違反時アクションを選択します。違反アクションは、単一レートポリシングのための通常および最大バーストサイズに違反した際にカラーマッピングが Red のパケットに対して実行するアクションを指定します。 デフォルトのアクションは超過時アクションと同じになります。 • **None** - 何もアクションを実行しないことを指定します。 • **Drop -** パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P -** 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

[**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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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	コミットされた情報レート (CIR) の値を入力します。 (設定範囲：0 ～ 10000000kbps)
バースト確認	CIR に対応する確認バーストサイズを入力します。 (設定範囲：0 ～ 16384kbyte)
PIR	ピーク情報レート (PIR) の値を入力します。 (設定範囲：0 ～ 10000000 kbps)
ピークバースト	ピークバースト値を入力します。 (設定範囲：0 ～ 16384Kbytes)
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、カラーマッピングが Green のパケットに対して実行するアクションを指定します。指定しない場合、デフォルトのアクションを指定します。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。デフォルトのアクションです。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

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際にカラーマッピングが Yellow のパケットに対して実行するアクションを指定します。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。デフォルトのアクションです。 • **Set-DSCP-1P -** 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。
違反時アクション	違反時アクションを選択します。違反アクションは、単一レートポリシングのための通常および最大バーストサイズに違反した際にカラーマッピングが Red のパケットに対して実行するアクションを指定します。 デフォルトのアクションは超過時アクションと同じになります。 • **Drop -** パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P -** 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

[**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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。 (設定可能文字：32 文字)

[**適用**] ボタン - エントリを追加します。

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。(設定可能文字：32 文字)
クラスマップ名	クラスマップ名を入力します。(設定可能文字：32 文字)

(注意) 該当のポリシーマップ名をクリックすると、トラフィックポリシーにクラスマップが表示されます。

[**アクション設定**] ボタン - エントリの Action 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、以下のウィンドウを表示します。

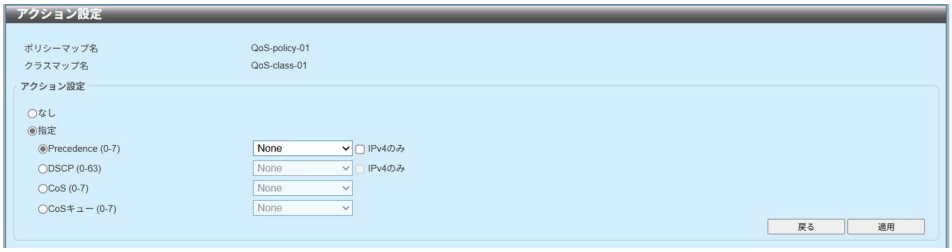

図 7-17 ポリシーマップ（アクション設定）

設定パラメータ （[アクション設定] 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れません。
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。選択するオプションは以下です。 • **Precedence** - このクラスマップと適合する Precedence 値を選択入力します。(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 Precedence になります。 • **DSCP** - このクラスマップと適合する DSCP 値を選択します。(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。 • **CoS** - このクラスマップと適合する CoS 値を選択入力します。(設定範囲：0 ～ 7) • **CoS キュー** - このクラスマップと適合する CoS キュー値を選択入力します。(設定範囲：0 ～ 7) ポリシーマップがインターフェースの送出方向のフローに適用されている場合は、CoS キュー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。
[**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。

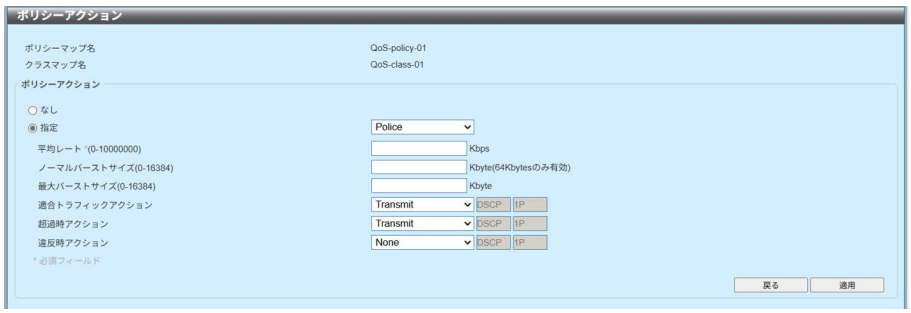

図 7-18 ポリシーマップ（ポリサー、Police）

設定パラメータ （[ポリサー]>[ポリシーアクション] 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 ～ 10000000Kbps）
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 ～ 16384Kbyte）
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 ～ 16384Kbyte）
適合トラフィック アクション	準拠アクションを選択します。確認アクションは、カラーマッピングが Green のパケットに対して実行するアクションを指定します。選択するオプションは以下です。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

パラメータ	概要
超過時アクション	ここで実行される超過アクションを選択します。このアクションは、レート制限を超えるカラーマッピングが Yellow のパケットに対して実行します。選択するオプションは以下です。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。
違反時アクション	ここで適用する違反時のアクションを選択します。このアクションはカラーマッピングが Red のパケットに対して実行されます。選択するオプションは以下です。 • **None** - 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** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

[**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。

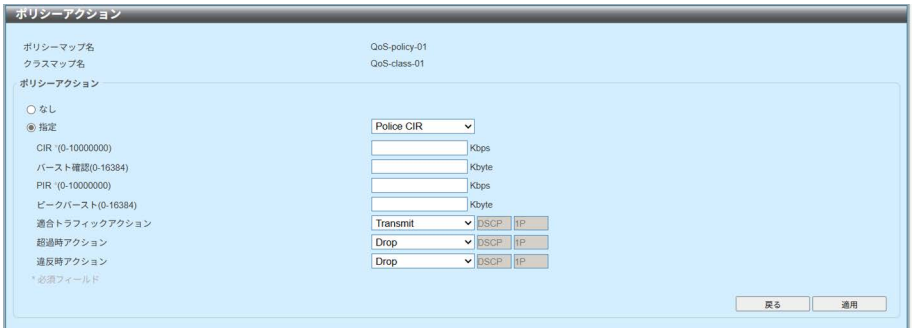

図 7-19 ポリシーマップ（ポリサー、Police CIR）

設定パラメータ （[ポリサー]>[ポリシーアクション] 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	設定情報レート値 (Committed Information Rate) を入力します。（設定範囲：0 ～ 10000000Kbps）
バースト確認	確認バースト値を入力します。 （設定範囲：0 ～ 16384Kbyte）
PIR	ピーク情報レート (PIR) 値を入力します。 （設定範囲：0 ～ 10000000Kbps）
ピークバースト	ピークバースト値を入力します。 （設定範囲：0 ～ 16384Kbyte）
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、カラーマッピングが Green のパケットに対して実行するアクションを指定します。選択するオプションは以下です。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

パラメータ	概要
超過時アクション	ここで実行される超過アクションを選択します。このアクションは、レート制限を超えるカラーマッピングが Yellow のパケットに対して実行します。選択するオプションは以下です。 • **Drop** - パケットを廃棄します。 • **Set-DSCP-Transmit** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。
違反時アクション	ここで適用する違反時のアクションを選択します。このアクションはカラーマッピングが Red のパケットに対して実行されます。選択するオプションは以下です。 • **None** - 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** - 新しい DSCP 値でパケットを設定し、送信します。指定されたスペースに DSCP 値を入力します。 • **Set-1P-Transmit** - 新しい IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに IEEE 802.1p 値を入力します。 • **Transmit** - パケットを変更せずに送信します。 • **Set-DSCP-1P** - 新しい DSCP および IEEE 802.1p 値でパケットを設定し、送信します。指定されたスペースに DSCP 値と IEEE 802.1p 値を入力します。

[**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]>[ポリシーアクション] 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	集約ポリサーの名前を入力します。 （設定可能文字：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。

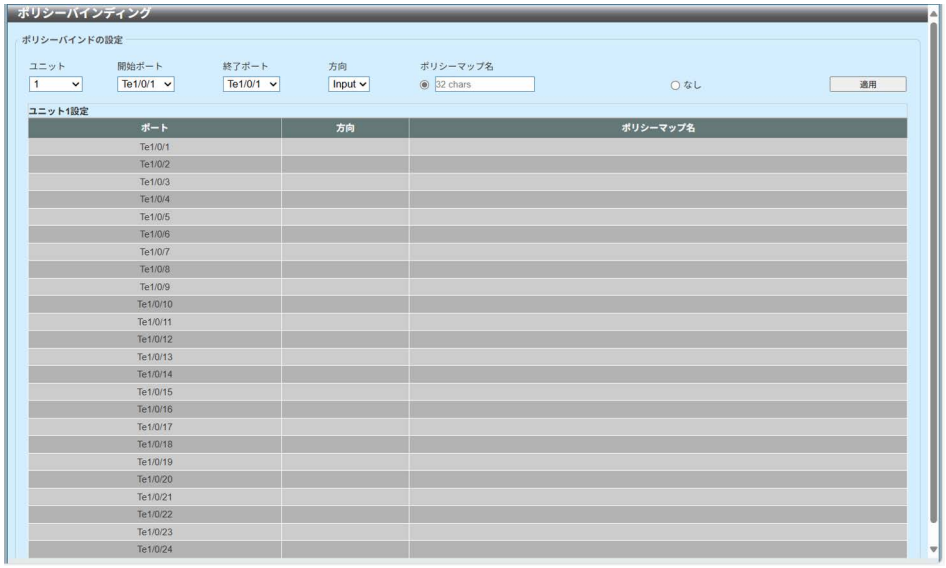

図 7-21 ポリシーバインディング

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：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。

7.3 WRED インターフェース

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

[QoS] > [WRED インターフェース] をクリックして、以下のウィンドウを表示します。

図 7-22 WRED インターフェース設定

設定パラメータ （[WRED インターフェース設定] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
WRED 状態	ポートの状態（**Enabled/Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[適用] ボタン - 変更内容を確認します。

7.4 出力バッファ設定

このウィンドウを用いて、出力バッファの閾値の設定を行い、指定した閾値を表示します。出力バッファの閾値はデフォルト設定での運用を推奨します。ポートの最大通信量を瞬間的に超えるトラフィックが多発する環境のみ High に変更します。

[QoS] > [出力バッファ設定] をクリックして、以下のウィンドウを表示します。

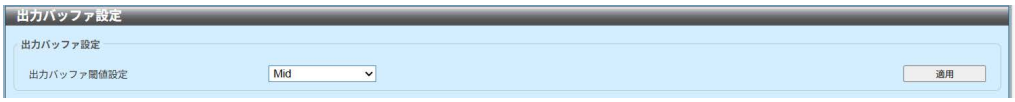

図 7-23 出力バッファ設定

設定パラメータ （[出力バッファ設定] セクション）

パラメータ	概要
出力バッファ閾値設定	出力バッファの閾値を選択します。 選択する値は以下になります。 • **High** - 出力ポートでより多くのセルが利用可能になるため、破棄する出力パケットを抑制します。 • **Mid** - 出力ポートでデフォルトのセルが利用可能になります。 • **Low** - 出力ポートで利用可能なセルが少なくなるため、より多くの出力パケットを破棄します。 (初期値 : Mid)

[適用] - 変更内容を確認します。

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）

[アップデート] 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 8-2 ACL 設定ウィザード（アップデート）

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。（設定可能文字：32 文字）

パラメータ	概要
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] >[ACL 名称] を入力 **> [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。
ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。

ACL の作成を選択して [**次**] ボタンをクリックすると、次のウィンドウが表示されます。

図 8-3 ACL 設定ウィザード（ACL タイプの選択）

設定パラメータ

パラメータ	概要
MAC	このオプションを選択した場合、MAC ACL を作成します。
IPv4	このオプションを選択した場合、IPv4 ACL を作成します。
IPv6	このオプションを選択した場合、IPv6 ACL を作成します。

[次] ボタン - ウィザードの次の手順に進みます。
[戻る] ボタン - ウィザードの前の手順に戻ります。

8.1.1 MAC ACL

[作成] > [MAC] を選択すると、以下のウィンドウが表示されます。

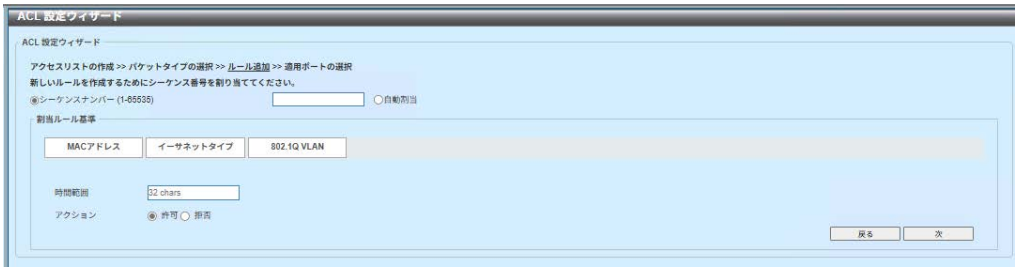

図 8-4 ACL 設定ウィザード (MAC 選択)

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
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。

[MAC アドレス] をクリックして、以下のウィンドウを表示します。

図 8-5 MAC ACL(MAC アドレス)

設定パラメータ （[MAC アドレス] セクション）

パラメータ	概要
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 アドレスおよびワイルドカード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 アドレスおよびワイルドカード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 ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字：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。

[イーサネットタイプ] をクリックして、以下のウィンドウを表示します。

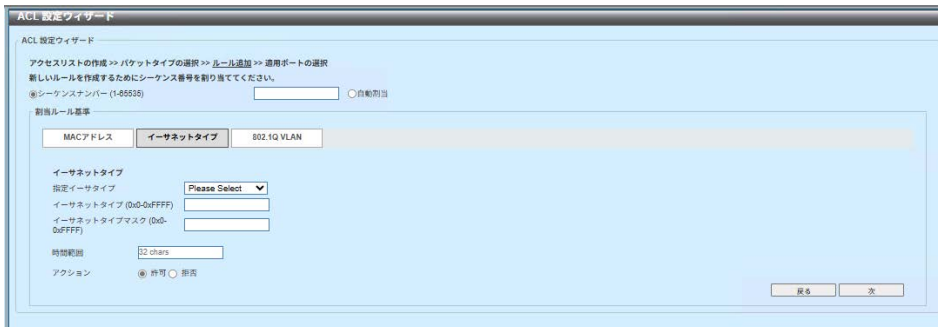

図 8-6 MAC ACL(イーサネットタイプ)

設定パラメータ （[イーサネットタイプ] セクション）

パラメータ	概要
指定イーサタイプ	イーサネットタイプオプション（**aarp**/**appletalk**/**decnet-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。

パラメータ	概要
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。 (設定範囲 : 0x600 ～ 0xFFFF) [**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。 (設定範囲 : 0x0 ～ 0xFFFF) [**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。
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

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

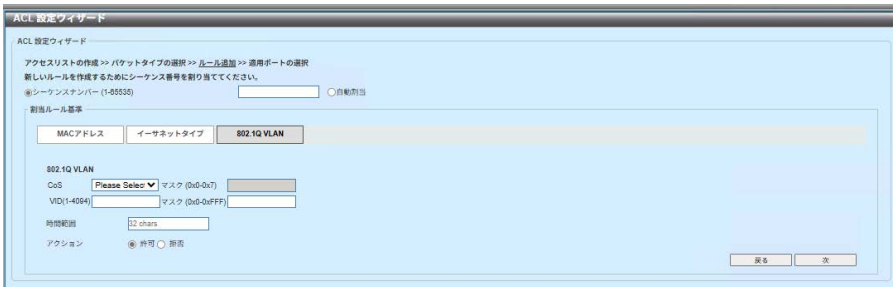

図 8-7 MAC ACL(802.1Q VLAN)

設定パラメータ （[802.1Q VLAN] セクション）

パラメータ	概要
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。 (設定範囲 : 0x0 ～ 0x7)
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。 (設定範囲 : 0x0 ～ 0xFFF)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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 - ウィザードの次のステップに進みます。

[**戻る**] ボタン - ウィザードの前のステップに戻ります。

[MAC アドレス / イーサネットタイプ /802.1Q VLAN] ボタン全てを選択すると、以下のウィンドウを表示します。

図 8-8 MAC ACL(全て選択)

[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 8-9 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In/Out**）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。

作成済みの拡張 ACL を編集する場合は、[ACL 設定ウィザード] > [アップデート] から拡張 ACL をエントリから選択し、[次] を選択すると、以下のウィンドウが表示され、編集を行えます。

図 8-10 ACL 設定ウィザード（拡張 MAC ACL の設定）

編集手順は、図 8-4 以降と同様です。

[**次**] ボタン - ウィザードの次のステップに進みます。
[**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

[作成] > [IPv4] を選択すると、以下のウィンドウが表示されます。

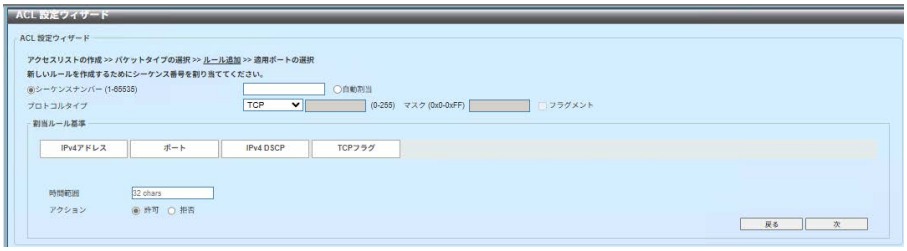

図 8-11 ACL 設定ウィザード（IPv4 選択）

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
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。 （設定範囲：0 ～ 255） • 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。 （設定範囲：0x0 ～ 0xFF） • フラグメント - このオプションを選択する場合、パケットフラグメントフィルタリングが含まれます。

[IPv4 アドレス] 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 8-12 IPv4 ACL(IPv4 アドレス)

設定パラメータ （[IPv4 アドレス] セクション）

パラメータ	概要
送信元	ソース IPv4 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 IP アドレスを使用および入力します。 • **IP** - **[ワイルドカード]** 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** - **[ワイルドカード]** 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 ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

[ポート] 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 8-13 IPv4 ACL(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
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または入力します。 • **=** - ACL は指定したポート番号のみ使用します。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)

パラメータ	概要
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または入力します。 • **=** - ACL は指定したポート番号のみ使用します。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

[IPv4 DSCP] をクリックして、以下のウィンドウを表示します。

図 8-14 IPv4 ACL(IPv4 DSCP)

設定パラメータ （[IPv4 DSCP] セクション）

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。(設定範囲 : 0 ～ 7) • **マスク** - IP Precedence マスク値を入力します。(設定範囲 : 0x0 ～ 0x7)
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。(設定範囲 : 0 ～ 15) • **マスク** - ToS マスク値を入力します。(設定範囲 : 0x0 ～ 0xF)
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。(設定範囲 : 0 ～ 63) • **マスク** - DSCP マスク値を入力します。(設定範囲 : 0x0 ～ 0x3F)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

[TCP フラグ] ボタンをクリックして、以下のウィンドウを表示します。

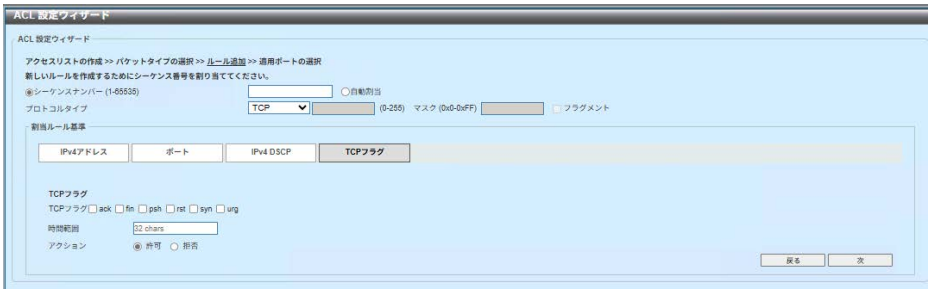

図 8-15 IPv4 ACL(TCP フラグ)

設定パラメータ （[TCP フラグ] セクション）

パラメータ	概要
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。
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字：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。

[IPv4 アドレス / ポート /IPv4DSCP/TCP フラグ] ボタン全てを選択すると、以下のウィンドウを表示します。

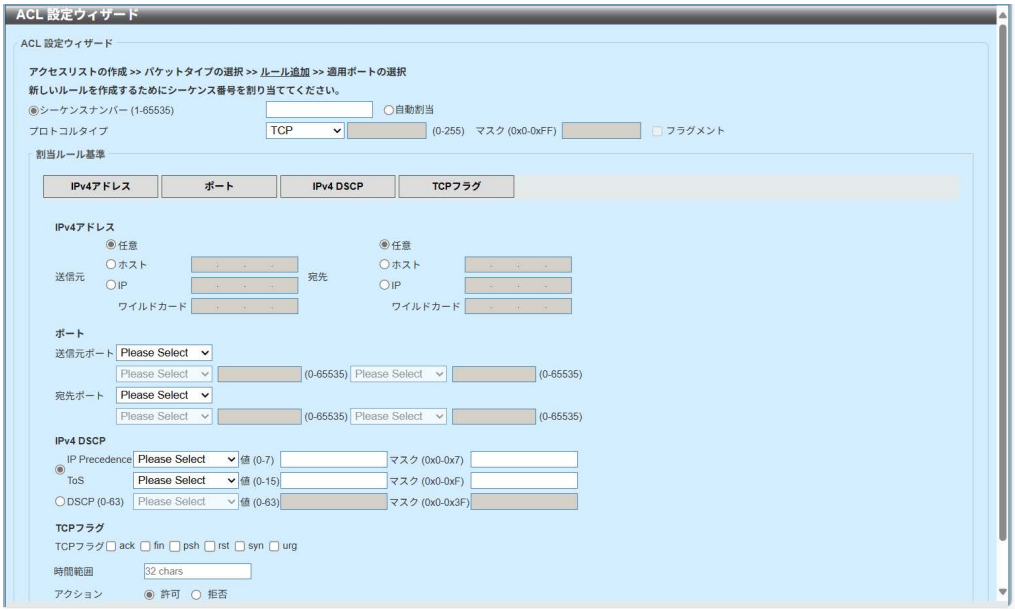

図 8-16 IPv4 ACL(全て選択)

[ICMP] ボタンをクリックして、以下のウィンドウを表示します。

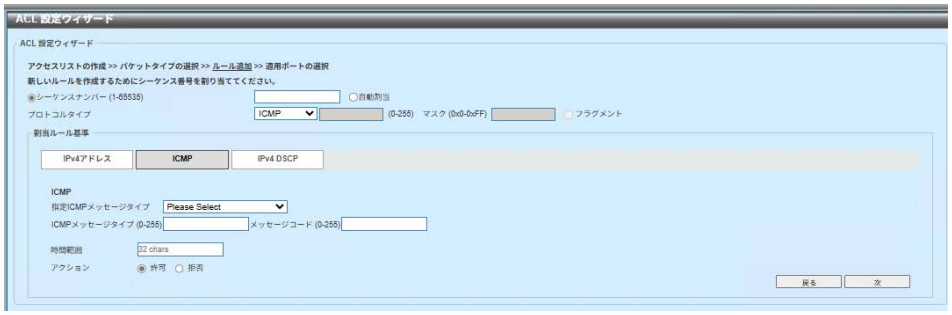

図 8-17 IPv4 ACL(ICMP)

設定パラメータ （[ICMP] セクション）

（注意）[プロトコルタイプ] で [ICMP] 選択した場合、設定可能です。

パラメータ	概要
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。**[指定 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。(設定範囲：0 ～ 255)
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。**[指定 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。(設定範囲：0 ～ 255)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字：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 - ウィザードの次のステップに進みます。
[**戻る**] ボタン - ウィザードの前のステップに戻ります。

[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 8-18 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In/Out**）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。
作成済みの拡張 ACL を編集する場合は、**[ACL 設定ウィザード]>[アップデート]** から拡張 ACL をエントリから選択し、**[次]** を選択すると、以下のウィンドウが表示され、編集が行えます。

図 8-19 ACL 設定ウィザード（拡張 IP ACL の設定）

編集手順は、図 8-7 以降と同様です。

[**次**] ボタン - ウィザードの次のステップに進みます。
[**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

[作成] > [IPv6] を選択すると、以下のウィンドウが表示されます。

図 8-20 ACL 設定ウィザード（IPv6 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
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**/**Protocol ID**/**ESP**（50）/**PCP**（108）/**SCTP**（132）/**None**）を選択します。 • **値** - [**Protocol ID**] オプションを選択した後、プロトコル ID を手動で入力できます。(設定範囲 : 0 ～ 255) • **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。 (設定範囲 : 0x0 ～ 0xFF)

[IPv6 アドレス] 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 8-21 IPv6 ACL(IPv6 アドレス)

設定パラメータ （[IPv6 アドレス] セクション）

[IPv6 アドレス] ボタンを押下することで、以下のパラメータが表示されます。

パラメータ	概要
送信元	ソース IPv6 アドレ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。
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 ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字：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。

（注意）

FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

[ポート] 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 8-22 IPv6 ACL(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
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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)

パラメータ	概要
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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

[IPv6 DSCP] 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 8-23 IPv6 ACL(IPv6 DSCP)

設定パラメータ （[IPv6 DSCP] セクション）

パラメータ	概要
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。(設定範囲 : 0 ～ 63) • **マスク** - DSCP マスク値を入力します。(設定範囲 : 0x0 ～ 0x3F)
トラフィッククラス	トラフィッククラスを選択し、値を入力します。(設定範囲 : 0 ～ 255) • **マスク** - トラフィッククラスマスク値を入力します。(設定範囲 : 0x0 ～ 0xFF)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

[TCP フラグ] 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 8-24 IPv6 ACL(TCP フラグ)

設定パラメータ （[TCP フラグ] セクション）

パラメータ	概要
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。
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字 : 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。

[フローラベル] 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 8-25 IPv6 ACL(フローラベル)

設定パラメータ （[フローラベル] セクション）

パラメータ	概要
フローラベル	フローラベルの値を入力します。 (設定範囲：0 ～ 1048575) フローラベルのマスクを入力します。 (設定範囲：0x0 ～ 0xFFFFF)
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字：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 - ウィザードの次のステップに進みます。
[**戻る**] ボタン - ウィザードの前のステップに戻ります。

[IPv6 アドレス / ポート /IPv6DSCP/TCP フラグ / フローラベル] ボタン全てを選択すると、以下のウィンドウを表示します。

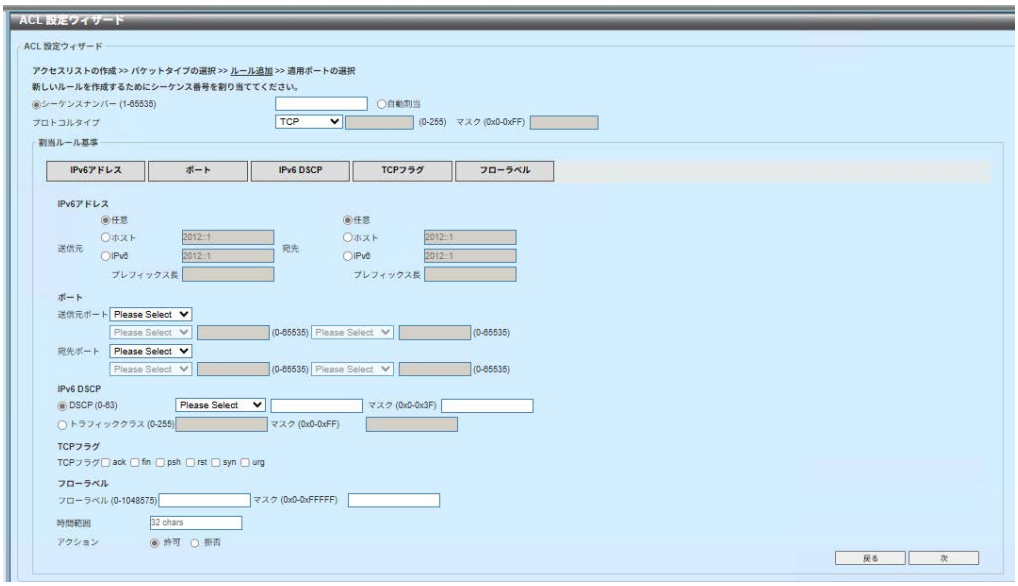

図 8-26 IPv6 ACL(全て選択)

[ICMP] ボタンをクリックして、以下のウィンドウを表示します。
（注意）[プロトコルタイプ] で [ICMP] 選択した場合、設定可能です。

図 8-27 IPv6 ACL(ICMP)

設定パラメータ （[ICMP] セクション）

パラメータ	概要
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。

パラメータ	概要
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。 (設定範囲：0 ～ 255) [**指定 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] 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。 (設定範囲：0 ～ 255) [**指定 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。
時間範囲	この ACL ルールで使用される時間範囲プロファイルの名前を入力します。(設定可能文字：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 8-28 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In/Out**）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。

作成済みの拡張 ACL を編集する場合は、**[ACL 設定ウィザード]>[アップデート]** から拡張 ACL をエントリから選択し、**[次]** を選択すると、以下のウィンドウが表示され、編集行えます。

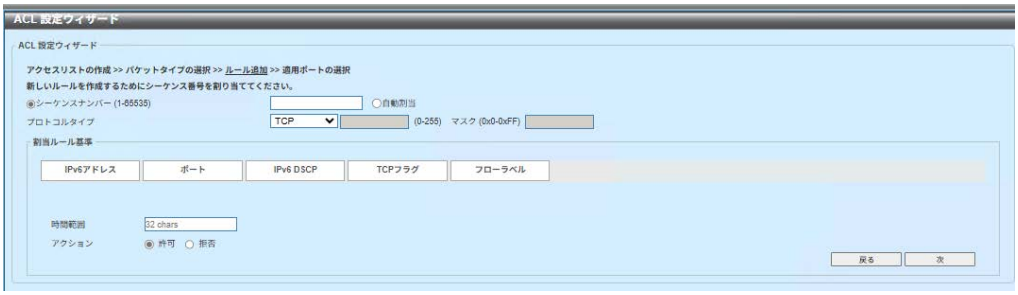

図 8-29 ACL 設定ウィザード (拡張 IPv6 ACL 設定)

編集手順は、図 8-10 以降と同様です。

[**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 8-30 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 ACL**/**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。 (設定範囲 : 1 ～ 14999)
ACL 名称	アクセスリスト名を選択および入力します。 (設定可能文字 : 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。
[**削除**] ボタン - 指定したエントリを削除します。
[**カウンタ全クリア**] ボタン - 全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 - 選択した ACL プロファイルに関連する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。
ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。

[**編集**] ボタンをクリックして、以下ウィンドウを表示します。

図 8-31 ACL アクセスリスト (編集)

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。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。 (初期値：10, 設定範囲：1 ～ 32)
カウンタ状態	カウンタ状態 (Enabled/Disable) を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値：Disabled)
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。

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 8-32 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。（設定可能文字：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 **[ルール追加]** 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。

図 8-33 ACL アクセスリスト (ルール追加、標準 IP ACL)

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。(設定範囲 : 1 ～ 65535)
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 IP 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 IP アドレスを使用および入力します。 • **IP** - **[ワイルドカード]** 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** - **[ワイルドカード]** 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	時間範囲プロファイルの名前を入力します。 (設定可能文字 : 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 8-34 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。（設定可能文字：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 **[ルール追加]** 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。

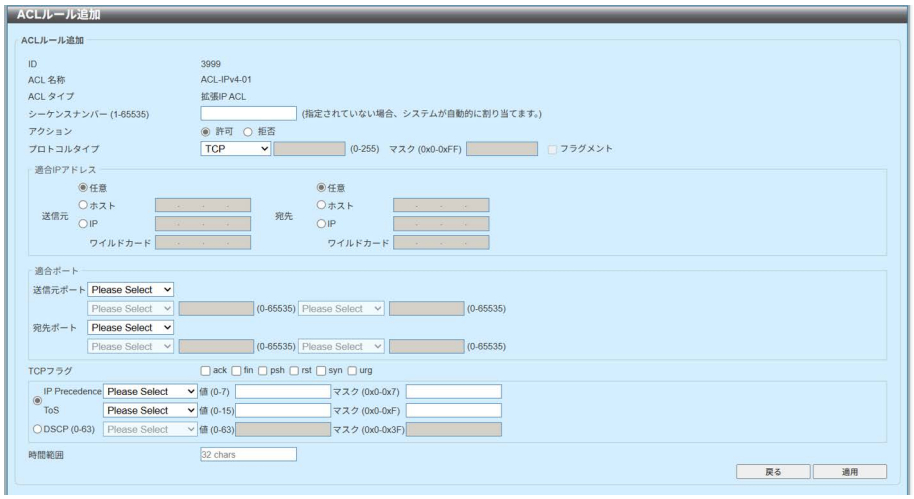

図 8-35 ACL アクセスリスト (ルール追加、拡張 IP ACL)

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。(設定範囲 : 1 - 65535)
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** - **[Protocol ID]** オプションを選択した後、プロトコル ID を入力します。(設定範囲：0 ～ 255) • **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。(設定範囲：0x0 ～ 0xFF) • **フラグメント** - パケットフラグメントのフィルタリングが含まれます。
送信元	ソース IP 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 IP アドレスを使用および入力します。 • **IP** - **[ワイルドカード]** 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** - **[ワイルドカード]** 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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)
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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)
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。 (設定範囲 : 0 ～ 255) **[指定 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] 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。 (設定範囲 : 0 ～ 255) **[指定 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。 (設定範囲 : 0 ～ 7) • **マスク** - IP Precedence マスク値を入力します。 (設定範囲 : 0x0 ～ 0x7)
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。 (設定範囲 : 0 ～ 15) • **マスク** - ToS マスク値を入力します。 (設定範囲 : 0x0 ～ 0xF)
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。 (設定範囲 : 0 ～ 63) • **マスク** - DSCP マスク値を入力します。 (設定範囲 : 0x0 ～ 0x3F)
時間範囲	時間範囲プロファイルの名前を入力します。 (設定可能文字 : 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 8-36 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。（設定可能文字：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 **[ルール追加]** 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。

図 8-37 ACL アクセスリスト (ルール追加、標準 IPv6 ACL)

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。(設定範囲 : 1 ～ 65535)
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 IPv6 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 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	時間範囲プロファイルの名前を入力します。 (設定可能文字 : 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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

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 8-38 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。（設定可能文字：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 **[ルール追加]** 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。

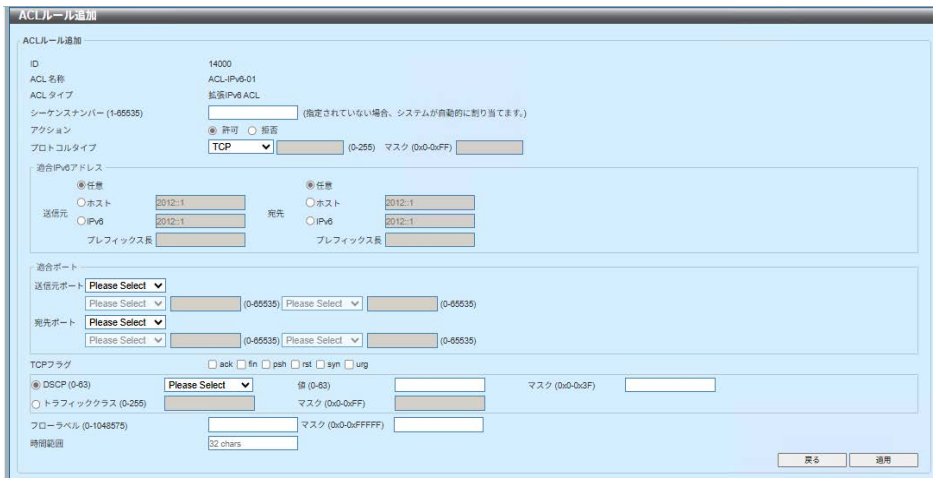

図 8-39 ACL アクセスリスト (ルール追加、拡張 IPv6 ACL)

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。(設定範囲 : 1 ～ 65535)
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** - **[Protocol ID]** オプションを選択した後、プロトコル ID を手動で入力できます。(設定範囲 : 0 ～ 255） • **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。(設定範囲 : 0x0 ～ 0xFF)
送信元	ソース IPv6 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 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。
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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • ≠ - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)

パラメータ	概要
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。(設定範囲：0 ～ 65535) • **>** - 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。(設定範囲：0 ～ 65535) • **<** - 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。(設定範囲：0 ～ 65535) • **≠** - ACL は指定されたポート番号を除くすべてのポートを使用します。(設定範囲：0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲：0 ～ 65535) • **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。(設定範囲：0x0 ～ 0xFFFF)
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] 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。**[指定 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。(設定範囲：0 ～ 255)
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。**[指定 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。(設定範囲：0 ～ 255)
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。

パラメータ	概要
トラフィッククラス	トラフィッククラス値を入力します。 (設定範囲：0 ～ 255) • **マスク** - トラフィッククラスマスク値を入力します。 (設定範囲 0x0 ～ 0xFF)
フローラベル	フローラベルの値を入力します。(設定範囲：0 ～ 1048575) • マスク - フローラベルのマスク値を入力します。 (設定範囲：0x0 ～ 0xFFFFF)
時間範囲	時間範囲プロファイルの名前を入力します。 (設定可能文字：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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

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 8-40 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。（設定可能文字：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 **[ルール追加]** 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。

図 8-41 ACL アクセスリスト (ルール追加、拡張 MAC ACL)

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。(設定範囲：1 ～ 65535)
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 アドレスおよびワイルドカード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 アドレスおよびワイルドカード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]**、**[decnet-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。 (設定範囲 : 0x0 ～ 0xFFFF) [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。 (設定範囲 : 0x0 ～ 0xFFFF) [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。(設定範囲：0 ～ 7) • **マスク** - CoS マスク値を入力します。 (設定範囲：0x0 ～ 0x7)
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。 (設定範囲：0x0 ～ 0xFFF)
時間範囲	時間範囲プロファイルの名前を入力します。 (設定可能文字：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 8-42 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。（設定可能文字：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 **[ルール追加]** 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。

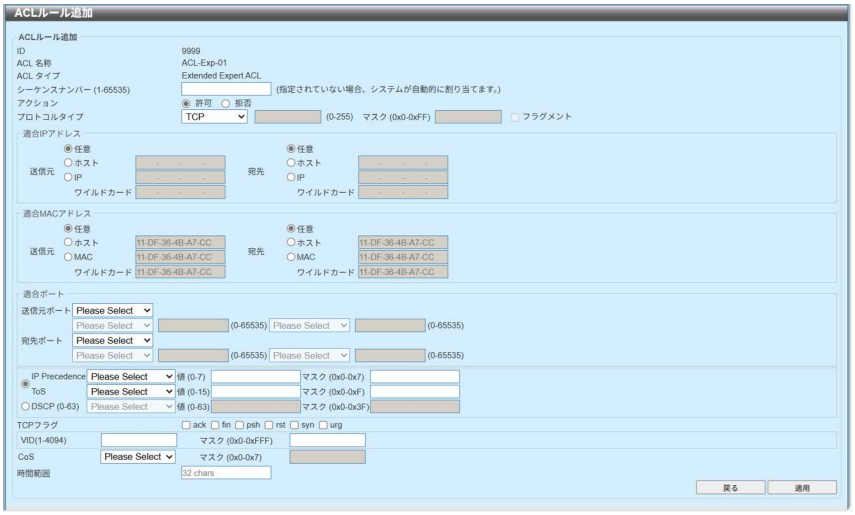

図 8-43 ACL アクセスリスト (ルール追加、Extended Expert ACL)

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。(設定範囲 : 1 ～ 65535)
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** - [**Protocol ID**] オプションを選択した後、プロトコル ID を手動で入力できます。(設定範囲 : 0 ～ 255) • **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 - パケットフラグメントフィルタリングを有効にします。
送信元（IP アドレス）	ソース IP 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 IP アドレスを使用および入力します。 • **IP** - **[ワイルドカード]** 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** - **[ワイルドカード]** 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 アドレスおよびワイルドカード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 アドレスおよびワイルドカード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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)
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。(設定範囲 : 0 ～ 65535) • **>** - 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。(設定範囲 : 0 ～ 65535) • **<** - 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。(設定範囲 : 0 ～ 65535) • **Range** - ACL は範囲内の指定されたポートを使用します。(設定範囲 : 0 ～ 65535) • **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。(設定範囲 : 0x0 ～ 0xFFFF)
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。

パラメータ	概要
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。 (設定範囲 : 0 ～ 255) **[指定 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。 (設定範囲 : 0 ～ 255) **[指定 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。 (設定範囲 : 0 ～ 7) • **マスク** - IP Precedence マスク値を入力します。 (設定範囲 : 0x0 ～ 0x7)
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。(設定範囲 : 0 ～ 15) • **マスク** - ToS マスク値を入力します。 (設定範囲 : 0x0 ～ 0xF)
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。 (設定範囲 : 0 ～ 63) • **マスク** - DSCP マスク値を入力します。 (設定範囲 : 0x0 ～ 0x3F)
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。

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) • **マスク** - VLAN ID マスク値を入力します。 (設定範囲：0x0 ～ 0xFFF)
CoS	使用する CoS 値を選択します。(設定範囲：0 ～ 7) • **マスク** - CoS マスク値を入力します。 (設定範囲：0x0 ～ 0x7)
時間範囲	時間範囲プロファイルの名前を入力します。 (設定可能文字：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 インター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 インター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 8-44 ACL インターフェースアクセスグループ

設定パラメータ （[ACL インターフェースアクセスグループ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In/Out**）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	[**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。

[選択してください] をクリックして、以下のウィンドウを表示します。

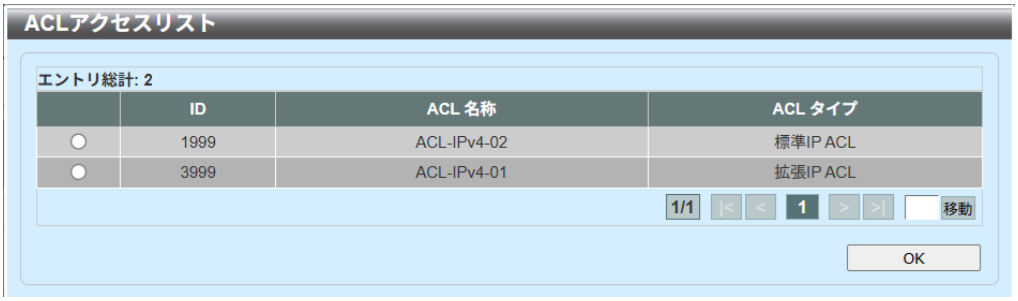

図 8-45 ACL インターフェースアクセスグループ（アクセスリスト選択画面）

ページ番号を入力し、[移動] ボタンをクリックすると、特定のページに移動します。
エントリを選択し、[OK] ボタンをクリックして、選択したアクセス制御リストを使用します。

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 8-46 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。（設定可能文字：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	カウンタの状態 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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 - カウンタ情報をクリアします。
[**カウンタクリア**] ボタン - 指定されたアクセスマップに関連する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。
ページ番号を入力し、[**移動**] ボタンをクリックすると、特定のページに移動します。

[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 8-47 ACL VLAN アクセスマップ（バインディング）

設定パラメータ （[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	[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 IP アクセスリストを選択します。
適合 IPv6 アクセスリスト	[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 IPv6 アクセスリストを選択します。
適合 MAC アクセスリスト	[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 MAC アクセスリストを選択します。

[**選択してください**] ボタン - 使用できる構成済みのアクセス制御リストが表示されます。
[**適用**] ボタン - 変更を受け入れます。
[**削除**] ボタン - 指定したバインディングを削除します。

[選択してください] をクリックして、以下のウィンドウを表示します。

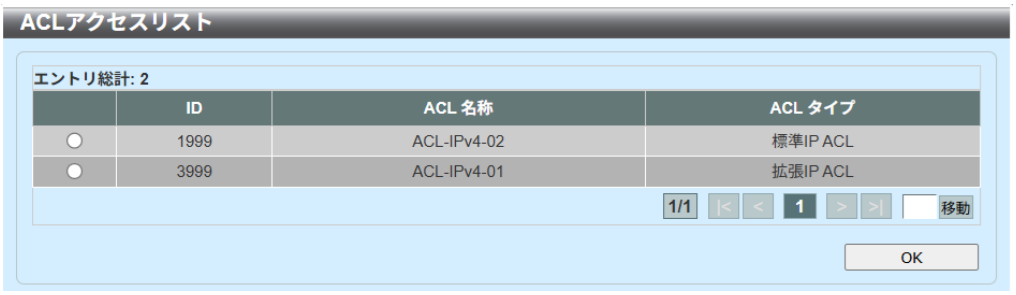

図 8-48 ACL VLAN アクセスマップ（バインディング , アクセスリスト選択画面）

エントリを選択し、[**OK**] ボタンをクリックして、選択したアクセス制御リストを使用します。
ページ番号を入力し、[**移動**] ボタンをクリックすると、特定のページに移動します。

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 8-49 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。（設定可能文字：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 指定**] 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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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トラップ設定] セクション）

パラメータ	概要
トラップ状態	ポート セキュリティ トラップ (**有効 / 無効**) を選択します。 (初期値 : 無効)

[**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トラップレート設定] セクション）

パラメータ	概要
トラップレート	ポート セキュリティ トラップのレートを入力します。 (初期値 : 0, 設定範囲 : 0 ～ 1000)

[**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。 （初期値：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）
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。（初期値：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 - エントリを追加します。

設定パラメータ （[検索 VLAN] 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。

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
状態	ポートの状態（**Enabled/Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。（初期値：32, 設定範囲：0 ～ 3328）

パラメータ	概要
違反アクション	実行する違反時アクションを選択します。 (初期値 : Protect) • **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。 (初期値：Delete - on - Timeout) • **Permanent** - 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。
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。 （初期値：0, 設定範囲：0 ～ 1440）

[**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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値：Disabled)
NAS ID	NAS（Network Access Server）の ID を入力します。半角のみ設定可能です。（初期値：nas1, 設定可能文字：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 秒）

[**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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。 （初期値：300 秒 , 設定範囲：0 ～ 65535 秒）
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
[**削除**] ボタン - エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。

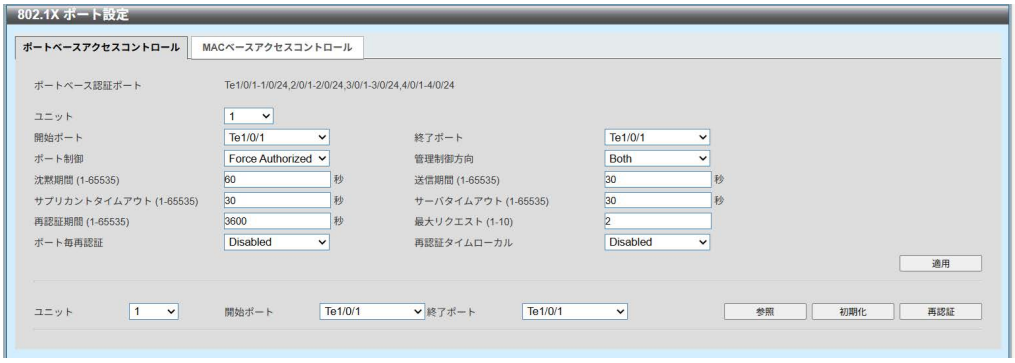

図 9-7 802.1X ポート設定（ポートベースアクセスコントロール）

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (初期値 : Force Authorized) • **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。 (初期値 : Both) • **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。 (初期値 : 60 秒 , 設定範囲 : 1 ～ 65535 秒)
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。 (初期値 : 30 秒 , 設定範囲 : 1 ～ 65535 秒)

パラメータ	概要
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。 (初期値：30 秒 , 設定範囲：1 ～ 65535 秒)
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。 (初期値：30 秒 , 設定範囲：1 ～ 65535 秒)
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。(初期値：3600 秒 , 設定範囲：1 ～ 65535 秒)
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。(初期値：2, 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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 ～ 1024）
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。 (初期値：Both) • **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。 （初期値：60 秒 , 設定範囲：1 ～ 65535 秒）
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。 （初期値：30 秒 , 設定範囲：1 ～ 65535 秒）
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。 （初期値：30 秒 , 設定範囲：1 ～ 65535 秒）
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。 （初期値：30 秒 , 設定範囲：1 ～ 65535 秒）

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。(初期値：3600 秒 , 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。(初期値：2, 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 (**Enabled/Disabled**) を設定します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
ポート毎再認証	指定したポートの定期的な再認証 (**Enabled/Disabled**) を設定します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 (初期値：3600 秒 , 設定範囲：0 ～ 65535 秒)

[**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。

[詳細参照] をクリックして、以下のウィンドウを表示します。

図 9-9 802.1x ポート設定 (MAC ベースアクセスコントロール、詳細参照)

[**編集**] ボタン - 指定したエントリの設定を編集します。
[**初期化**] ボタン - 指定したサプリカント MAC アドレス接続を開始します。
[**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。
[**削除**] ボタン - エントリを削除します。

ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。
[**戻る**] ボタン - 前の画面に戻ります。

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 9-10 EAP ポートコンフィグ

設定パラメータ

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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。

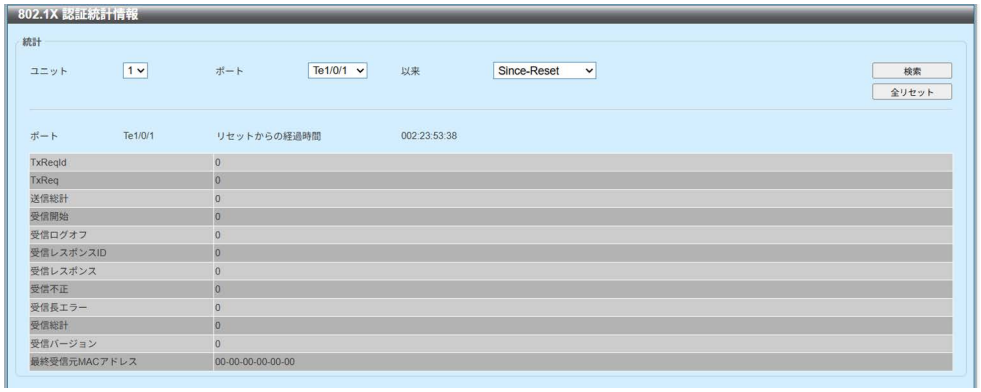

図 9-11 802.1X 認証統計情報

設定パラメータ （[統計] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 サプリカントのグローバル設定

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 9-12 802.1X 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。（設定可能文字：32 文字） [**ユーザ名の削除**] オプションを選択した場合、802.1X のサプリカントからユーザ名を削除します。
パスワード	サプリカントのパスワードを設定します。 （設定可能文字：32 文字） [**暗号化**] オプションを選択した場合、パスワードの暗号化を有効にします。これにより、パスワードは暗号化された形式で保存されます。 [**パスワードの削除**] オプションを選択した場合、802.1X のサプリカントからパスワードを削除します。
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。 (設定可能文字：56 文字)
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。

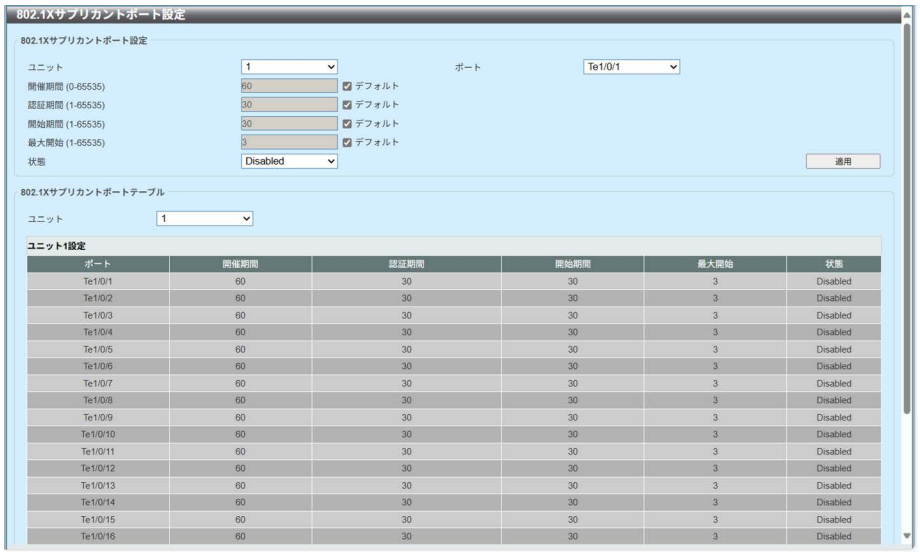

図 9-13 802.1X サプリカントポート設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（初期値：60 秒 , 設定範囲：0 ～ 65535 秒）
認証期間	Authenticator からのリクエストを待つ時間を設定します。 （初期値：30 秒 , 設定範囲：1 ～ 65535 秒）
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。 （初期値：30 秒 , 設定範囲：1 ～ 65535 秒）
最大開始	EAPOL-Start パケットを送信する最大数を設定します。 （初期値：3 回 , 設定範囲：1 ～ 65535 秒）
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。

設定パラメータ （[802.1X サプリカントポートテーブル] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。

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。

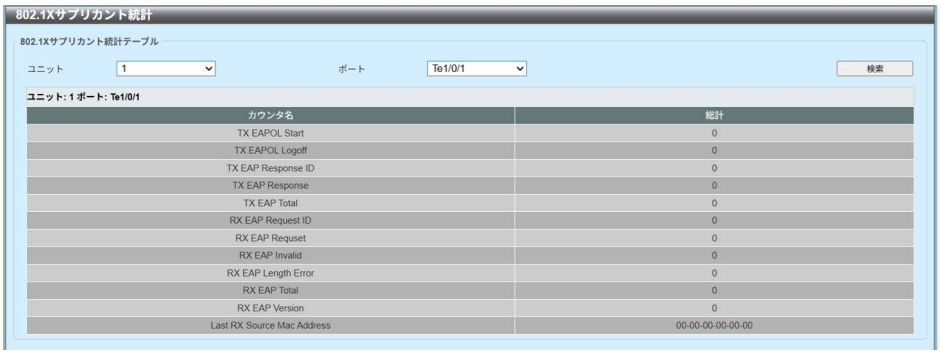

図 9-14 802.1X サプリカント統計情報

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

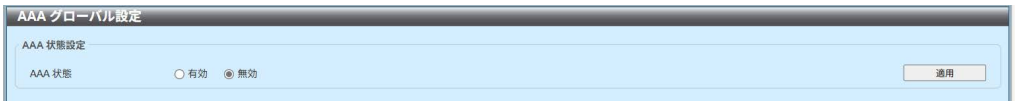

図 9-15 AAA グローバル設定

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。 (初期値 : 無効)

[**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。

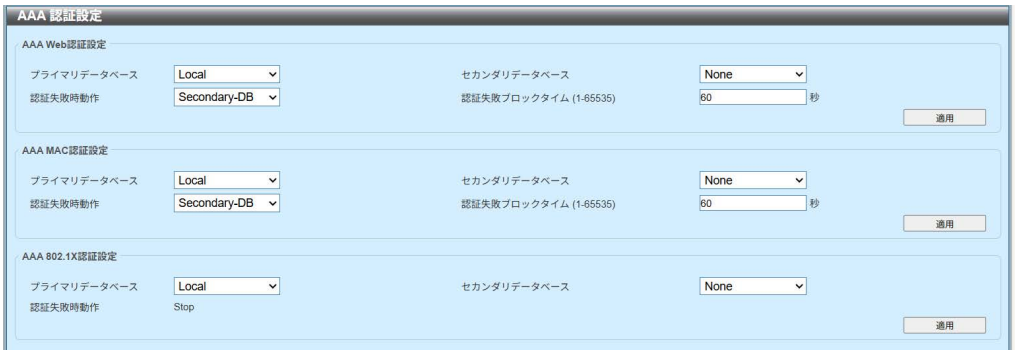

図 9-16 AAA 認証設定

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。 • **Group** - スイッチ上の RADIUS サーバグループをプライマリデータベースとして使用するように指定します。サーバ グループの名前を入力します。スペースを許可しない一般的な文字列を使用できます。(設定可能文字：32 文字)
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。 • **Group** - スイッチ上の RADIUS サーバグループをセカンダリデータベースとして使用するように指定します。サーバ グループの名前を入力します。スペースを許可しない一般的な文字列を使用できます。(設定可能文字：32 文字)

パラメータ	概要
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。（初期値：60 秒 , 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。 • **Group**- スイッチ上の RADIUS サーバグループをプライマリデータベースとして使用するように指定します。サーバ グループの名前を入力します。スペースを許可しない一般的な文字列を使用できます。(設定可能文字：32 文字)
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。 • **Group** - スイッチ上の RADIUS サーバグループをセカンダリデータベースとして使用するように指定します。サーバ グループの名前を入力します。スペースを許可しない一般的な文字列を使用できます。(設定可能文字：32 文字)

パラメータ	概要
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。（初期値：60 秒 , 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。 • **Group**- スイッチ上の RADIUS サーバグループをプライマリデータベースとして使用するように指定します。サーバ グループの名前を入力します。スペースを許可しない一般的な文字列を使用できます。(設定可能文字：32 文字)
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。

[**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 9-17 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。 (設定可能文字：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。
フィルター -ID	フィルター ID を入力します。フィルター ID はここで使用される ACL の番号です。特に指定しない場合は、初期値となります。(初期値：0, 設定範囲：1 ～ 14999)
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 (Enabled/Disabled) を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
2 段階目の認証	2 段階認証を有効にする場合、オプションを選択します。

[**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。
ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。

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 9-18 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)
フィルター -ID	フィルター ID を入力します。フィルター ID は、ここで使用するアクセスリスト (ACL) の番号です。 (初期値：0, 設定範囲：1 ～ 14999)
2 ステップ認証	ここで 2 段階認証を有効にするか無効にするかを選択します。選択肢は以下です。 • **No** - ローカル認証アカウントの 2 段階認証を無効にします。 • **Web** - 2 段階認証を有効にし、ウェブ認証を第 2 の認証方法として使用します。 • **802.1X** - 2 段階認証を有効にし、IEEE 802.1X 認証を第 2 の認証方法として使用します。 • **Any** - 2 段階認証を有効にし、IEEE 802.1X とウェブ認証の両方を第 2 の認証方法として使用します。

[**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。
ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。

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 9-19 アプリケーション認証設定

[編集] クリックして、以下のウィンドウを表示します。

図 9-20 アプリケーション認証設定 (編集)

設定パラメータ （[アプリケーション認証設定] セクション）

パラメータ	概要
ログイン方式リスト	ログイン方式リストの名前を入力します。

[**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 9-21 アプリケーションアカウンティング設定

図 9-22 アプリケーションアカウンティング設定 (編集)

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

パラメータ	概要
Exec方式リスト	Exec方式リストの名前を入力します。 (設定可能文字: 32文字)

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

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。 (設定可能文字 : 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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。

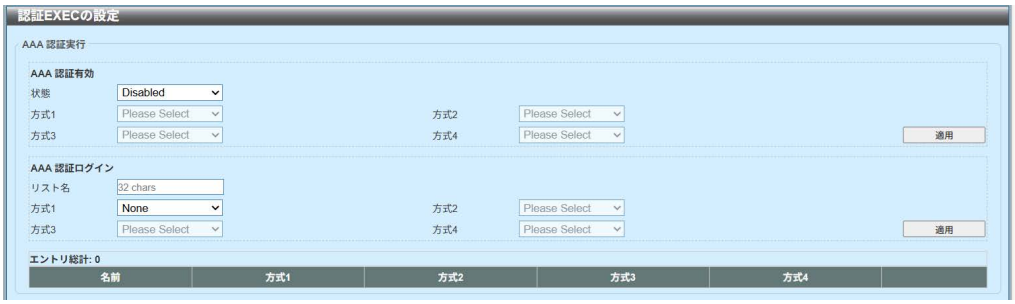

図 9-23 認証 EXEC の設定

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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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** - RADIUS グループサーバ設定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。(設定可能文字：32 文字) • **RADIUS** - RADIUS サーバ設定によって定義されているサーバを使用します。 • **TACACS+** - TACACS+ サーバ設定によって定義された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。(設定可能文字：32 文字)
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** - RADIUS グループサーバ設定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。（設定可能文字：32 文字） • **RADIUS** - RADIUS サーバ設定によって定義されているサーバを使用します。 • **TACACS+** - TACACS+ サーバ設定によって定義された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 9-24 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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 **[Group]** オプションを選択した場合は、指定されたスペースに AAA グループサーバの名前を入力します。 (設定可能文字：32 文字)

[**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 9-25 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 (**Enabled/Disabled**) を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 **[Group]** オプションを選択した場合は、指定されたスペースに AAA グループサーバの名前を入力します。 (設定可能文字：32 文字)

[**適用**] ボタン - 設定内容を反映します。

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

図 9-26 アカウンティング設定（AAA アカウンティング実行）

設定パラメータ （[AAA アカウンティング実行] タブ）

パラメータ	概要
リスト名	**[AAA アカウンティング実行]** オプションで使用する方式リスト名を入力します。(設定可能文字：32 文字)

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（**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。 **[Group]** オプションを選択した場合は、指定されたスペースに AAA グループサーバの名前を入力します。 (設定可能文字：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。

[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 9-27 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] タブ）

パラメータ	概要
レベル	ここで使用する特権レベルを選択します。 (設定範囲：1 ～ 15)
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。(設定可能文字 : 32 文字)
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**/**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。 **[Group]** オプションを選択した場合は、指定されたスペースに AAA グループサーバの名前を入力します。 (設定可能文字：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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。

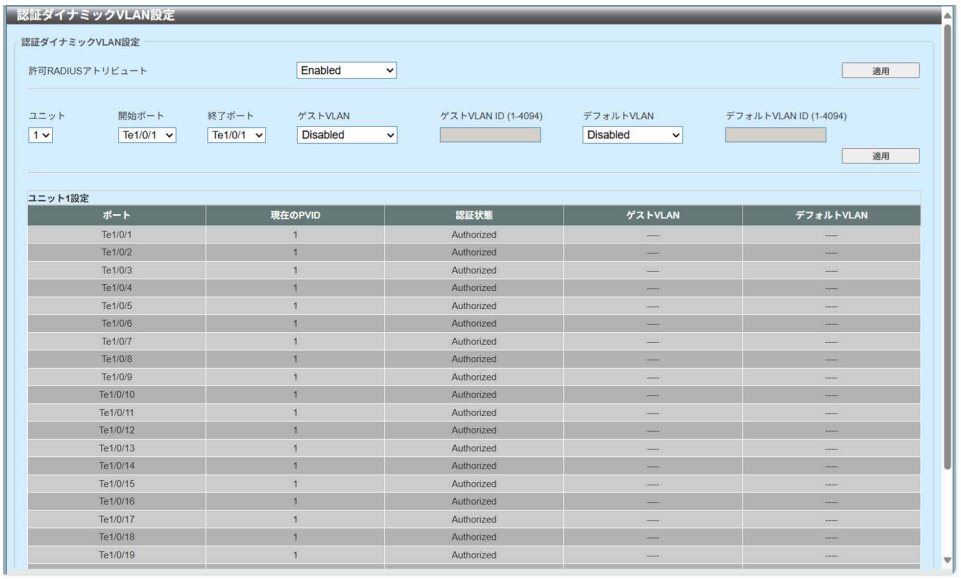

図 9-28 認証ダイナミック VLAN 設定

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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Enabled)
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
ゲスト VLAN ID	ゲスト VLAN ID を入力します。（設定範囲：1 ～ 4094）

パラメータ	概要
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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 9-29 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。（初期値：1440 分 , 設定範囲：0 ～ 65535 分）
Sort By MAC	認証セッションを MAC アドレス順に表示します。
Sort By Port	指定したポートの認証セッションを表示します。 • **ユニット** - ユニット ID を入力します。スタッキングした際に表示します。 • **開始ポート / 終了ポート** - 使用するポートをここで選択します。

[**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。
[**削除**] ボタン - 認証済みホストを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[移動]** ボタンをクリックして特定のページに移動します。

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。

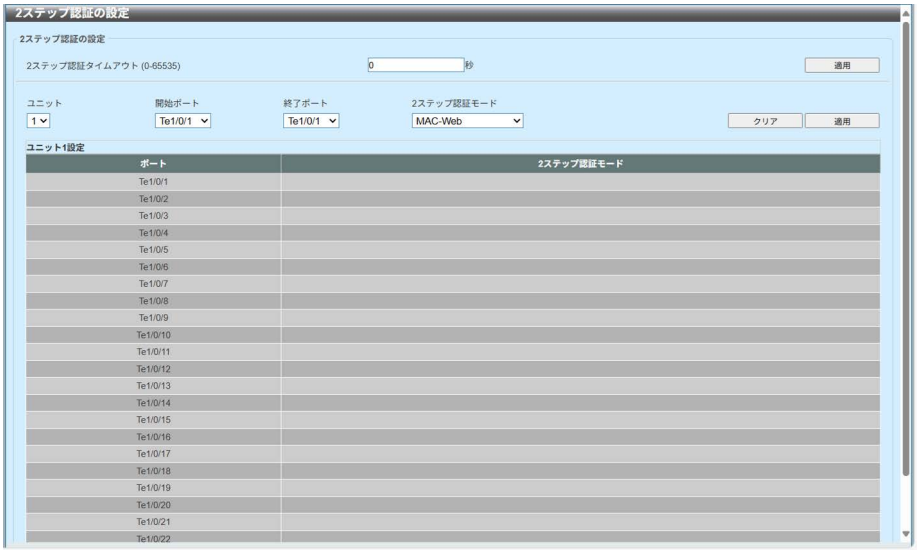

図 9-30 2 ステップ認証の設定

設定パラメータ （[**2 ステップ認証の設定**] セクション）

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。 （初期値：0, 設定範囲：0 ～ 65535）
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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** - 最初のステップで MAC 認証を、次に WEB 認証を使用します。 • **MAC-Dot1X** - 最初のステップで MAC 認証を、次に IEEE 802.1X 認証を使用します。 • **Dot1X-WEB** - 最初のステップで IEEE 802.1X 認証を、WEB 認証を使用します。

[**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。

(注意) 本設定は、AAA のグローバル設定を有効にしないと CLI 上では running-config に表示されません。

[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 9-31 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 タイムタイマーを開始します。この状態のサーバは、Dead タイムが経過するまで、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。 （初期値：0 分 , 設定範囲：0 ～ 1440 分）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[RADIUS グローバル IPv4 ソースインターフェース] セクション）

パラメータ	概要
IPv4 RADIUS ソースインターフェース	IPv4 RADIUS 送信元インターフェースのタイプ (**VLAN/Loopback**) を選択します。
インターフェース ID	インターフェースの ID を入力します。 • **VLAN** - 1 ～ 4094 で設定が可能です。 • **Loopback** - 1 ～ 8 で設定が可能です。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[RADIUS グローバル IPv6 ソースインターフェース] セクション）

パラメータ	概要
IPv6 RADIUS ソースインターフェース	IPv6 RADIUS 送信元インターフェースのタイプ (**VLAN/Loopback**) を選択します。
インターフェース ID	インターフェースの ID を入力します。 • **VLAN** - 1 ～ 4094 で設定が可能です。 • **Loopback** - 1 ～ 8 で設定が可能です。

[**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。

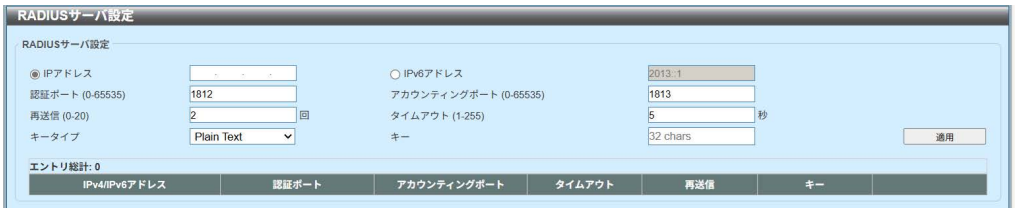

図 9-32 RADIUS サーバ設定

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。 （初期値：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。 （初期値：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。 （初期値：2, 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。 （初期値：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。 • **Plain Text** - パスワードの設定可能文字数は 32 文字です。 • **Encrypted(暗号化)** - パスワードの設定可能文字数は 64 文字です。

[**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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

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。
(注意) デフォルトで「radius」は設定されています。

図 9-33 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。 (設定可能文字：32 文字)
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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

[**詳細参照**] をクリックして、以下のウィンドウを表示します。

図 9-34 RADIUS グループサーバ設定 (詳細参照)

設定パラメータ （[RADIUS グループサーバ設定 > 詳細参照] セクション）

パラメータ	概要
IPv4 RADIUS ソースインターフェース	IPv4 RADIUS 送信元インターフェースのタイプ (**VLAN/Loopback**) を選択します。
インターフェース ID	インターフェースの ID を入力します。 • **VLAN** - 1 ～ 4094 で設定が可能です。 • **Loopback** - 1 ～ 8 で設定が可能です。
IPv6 RADIUS ソースインターフェース	IPv6 RADIUS 送信元インターフェースのタイプ (**VLAN/Loopback**) を選択します。
インターフェース ID	インターフェースの ID を入力します。 • **VLAN** - 1 ～ 4094 で設定が可能です。 • **Loopback** - 1 ～ 8 で設定が可能です。

[**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。
[**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 9-35 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。
複数のページが存在する場合は、ページ番号を入力し、[移動] ボタンをクリックして特定のページに移動します。
2 番目の [クリア] ボタン - テーブル内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+ グローバル設定

このウィンドウを用いて、TACACS+ 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] > [TACACS+] > [TACACS+ 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 9-36 TACACS+ グローバル設定

設定パラメータ
（[TACACS+ グローバル IPv4 ソースインターフェース] セクション）

パラメータ	概要
IPv4 TACACS+ ソースインターフェース名	IPv4 TACACS+ ソースインターフェースタイプ (**VLAN/Loopback**) を選択します。
インターフェース ID	インターフェースの ID を入力します。 • **VLAN** - 1 ～ 4094 で設定が可能です。 • **Loopback** - 1 ～ 8 で設定が可能です。

[適用] ボタン - 変更を反映します。

9.6.2 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。

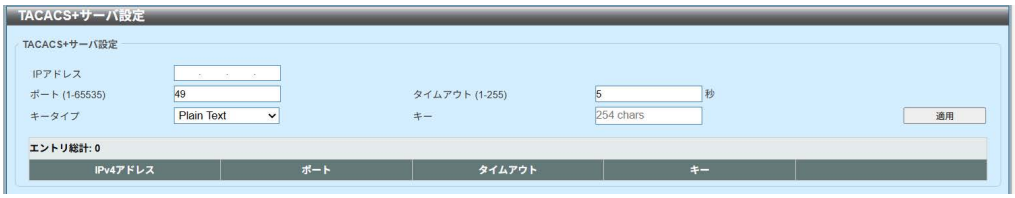

図 9-37 TACACS+ サーバ設定

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。 (初期値 : 49, 設定 : 1 ～ 65535)
タイムアウト	タイムアウト値を入力します。 (初期値 : 5 秒 , 設定 : 1 ～ 255 秒)
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	TACACS+ サーバとの通信に使用するキーを入力します。 • **Plain Text** - パスワードは 254 文字まで設定可能です。 • **Encrypted(暗号化)** - パスワードは 344 文字まで設定可能です。

[適用] ボタン - 新しいエントリを追加します。
[削除] ボタン - 指定したエントリを削除します。

9.6.3 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 9-38 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。 (設定可能文字：32 文字)
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。

[**詳細参照**] をクリックして、以下のウィンドウを表示します。

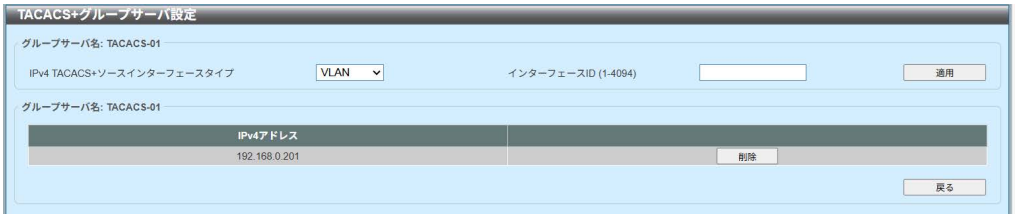

図 9-39 TACACS+ グループサーバ設定 (詳細参照)

設定パラメータ （[TACACS+ グループサーバ設定 > 詳細参照] セクション）

パラメータ	概要
IPv4 TACACS+ ソースインターフェース	IPv4 TACACS+ 送信元インターフェースのタイプ (**VLAN/Loopback**) を選択します。
インターフェース ID	インターフェースの ID を入力します。 • **VLAN** - 1 ～ 4094 で設定が可能です。 • **Loopback** - 1 ～ 8 で設定が可能です。

[**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。
[**戻る**] ボタン - 前のウィンドウに戻ります。

9.6.4 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 9-40 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。
2 番目の [クリア] ボタン - テーブル内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。

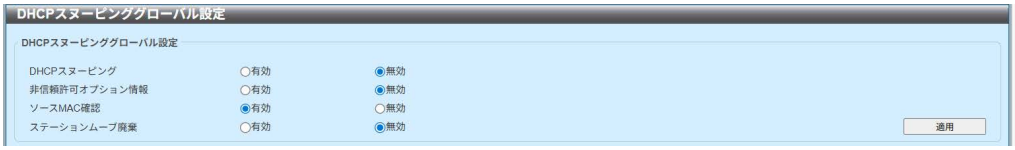

図 9-41 DHCP スヌーピンググローバル設定

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。(初期値：無効)
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。(初期値：無効)
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。(初期値：有効)
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。(初期値：無効)

[**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。

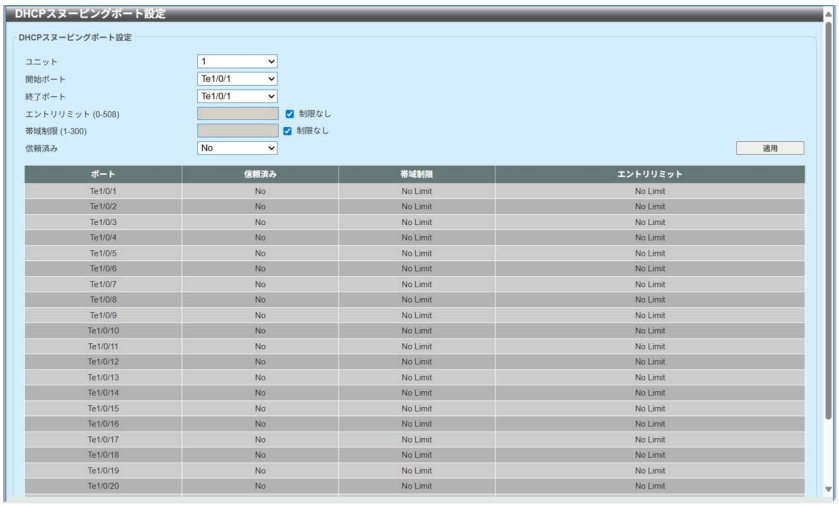

図 9-42 DHCP スヌーピングポート設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。**[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。 (初期値：制限なし , 設定範囲：0 ～ 508)
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、機能を無効にします。 (初期値：制限なし , 設定範囲：1 ～ 300)
信頼済み	Trusted オプション（**Yes**/**No**）を選択します。 (初期値：No) 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。

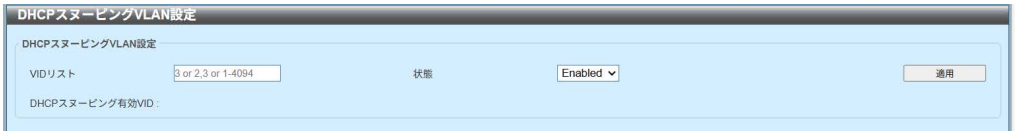

図 9-43 DHCP スヌーピング VLAN 設定

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 (ex1,2) で連続する VLAN ID を入力するか、またはハイフン区切り (ex1-5) 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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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 9-44 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。 （初期値：300 秒、設定範囲：60 ～ 86400 秒）

[**リセット**] ボタン - 書き込み遅延時間を初期値にリセットします。
[**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**/**Local**）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保存する URL 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**/**Local**）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 - 最終無視バインディング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 9-45 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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 秒）

[**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。
複数のページが存在する場合は、ページ番号を入力し、[移動] ボタンをクリックして特定のページに移動します。

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 9-46 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。 (設定可能文字：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。

[**編集**] をクリックして、以下のウィンドウを表示します。

図 9-47 ARP アクセスリスト (編集)

設定パラメータ（[ARP アクセスリスト (編集)] セクション）

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。

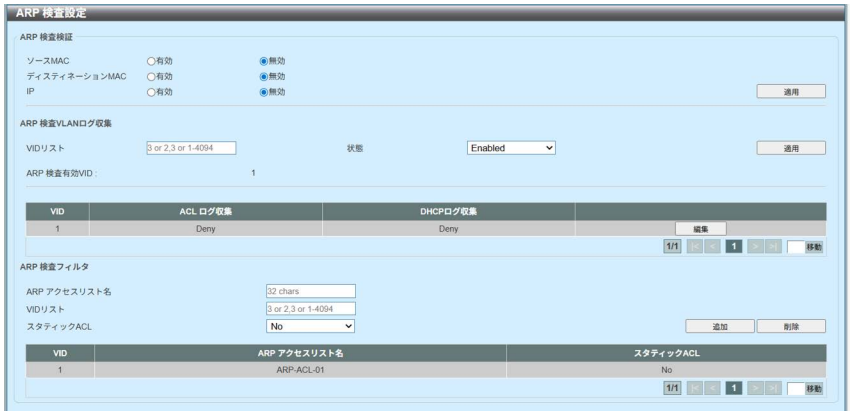

図 9-48 ARP 検査設定

設定パラメータ （[ARP 検査検証] 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。(初期値 : 無効)
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。(初期値 : 無効)
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。(初期値 : 無効)

[**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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**適用**] ボタン - 設定内容を反映します。
[**編集**] ボタン - 指定したエントリの設定を編集します。
ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。

[編集] クリックして、以下のウィンドウを表示します

図 9-49 ARP 検査 VLAN ログ収集 (編集)

設定パラメータ （[ARP 検査 VLAN ログ収集 (編集)] セクション）

パラメータ	概要
ACL ログ収集	ACL との一致に基づくパケットのログ収集基準 (**Deny**/**Permit**/**All**/**None**) を選択します。
DHCP ログ収集	DHCP との一致に基づくパケットのログ収集基準 (**Deny**/**Permit**/**All**/**None**) 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 （[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。 （設定可能文字：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 (ex1,2) で連続する VLAN ID を入力するか、またはハイフン区切り (ex1-5) 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**）の使用を選択します。

[**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。
ページ番号を入力し、[**移動**] ボタンをクリックすると特定のページに移動します。

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。

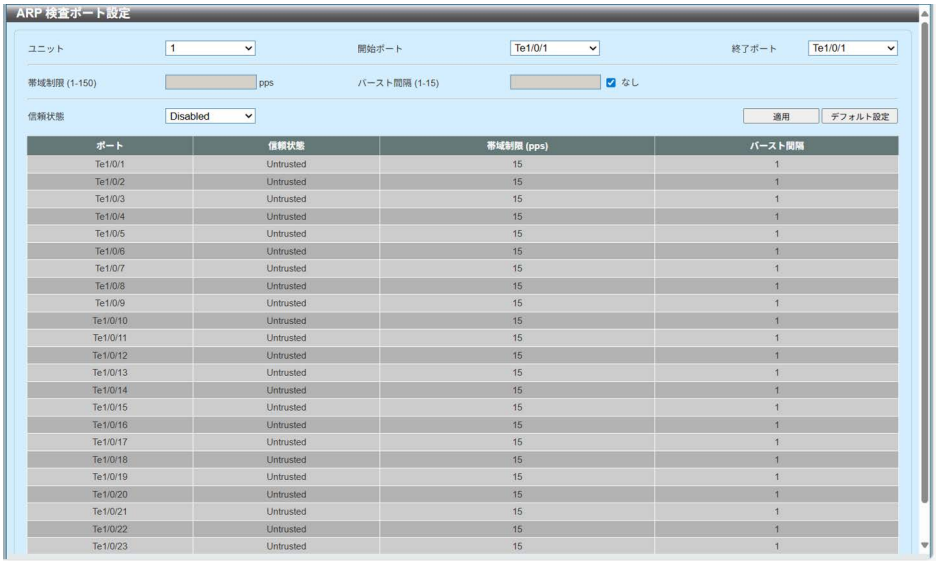

図 9-50 ARP 検査ポート設定

設定パラメータ

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。**[なし]** をオンにした場合、ARP パケットレートは制限されません。 （初期値：15, 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。**[帯域制限]** 機能有効時のみ、設定可能になり、無効時は設定不可になります。 **[なし]** を選択すると、その設定を無効にすることができます。(初期値：1, 設定範囲：1 ～ 15)
信頼状態	信頼状態（**Enabled**/**Disabled**）を選択します。 **[Enabled]** を選択すると、**[Trusted]** が表示されます。 **[Disabled]** を選択すると、**[Untrusted]** が表示されます。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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 - ARP 検査ポート設定をデフォルト設定にします。

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 9-51 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 (ex1,2) で連続する VLAN ID を入力するか、またはハイフン区切り (ex1-5) 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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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 9-52 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]** オプションを選択した場合、デフォルト値を使用します。(初期値 : 32, 選択範囲 : 1 ～ 1024)

[**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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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。

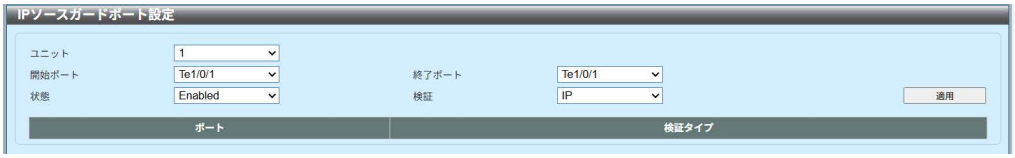

図 9-53 IP ソースガードポート設定

設定パラメータ

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 IP ソースガードの状態（**Enabled**/**Disabled**）を選択します。 (Enabled : 有効化 , Disabled : 無効化 , 初期値 : Disabled)
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。

（注意）
SAVI-IP ソースガードの設定を行う際は、以下の制限事項を必ずお守りください。

- 設定作業中は、IP ソースガード設定を行うポートに UTP ケーブルを接続しないでください。
- 上記の状態（UTP ケーブル接続中のポートに IP ソースガード設定を行うこと）では、以下の問題が発生します。
  - Web 設定画面が応答不能（フリーズ）となります。
  - 設定操作が正常に完了できません。

[**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 9-54 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。
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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 9-55 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

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 9-56 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。 (設定可能文字 : 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 - 新しいエントリを追加します。
[削除] ボタン - 指定したプロファイルから 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。 (初期値 : 32, 設定範囲 : 10 ～ 1024)

[適用]ボタン - 新しいエントリを追加します。
[ログクリア]ボタン - ログエントリをクリアします。

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。

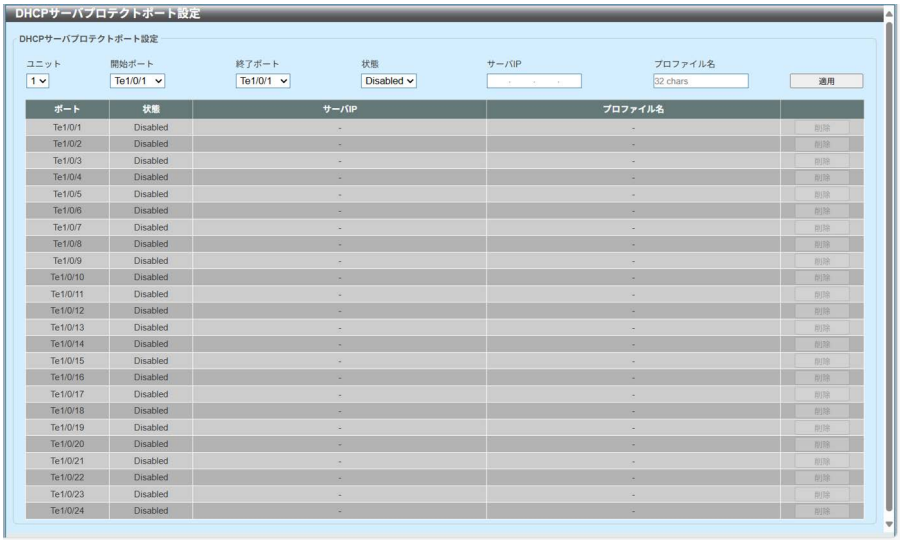

図 9-57 DHCP サーバプロテクトポート設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 DHCP サーバプロテクト機能の状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。(設定可能文字：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。

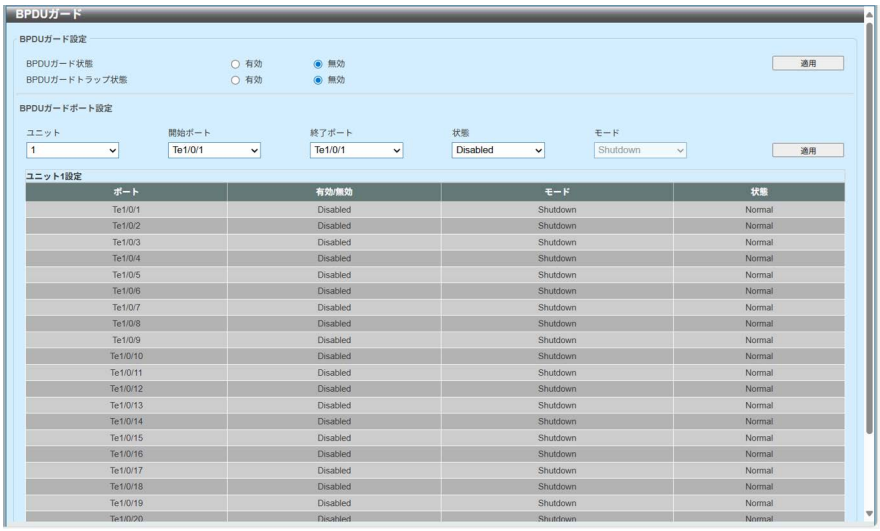

図 9-58 BPDU ガード

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。 (初期値：無効)
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。 (初期値：無効)

[**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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 BPDU ガードの状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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 9-59 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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。

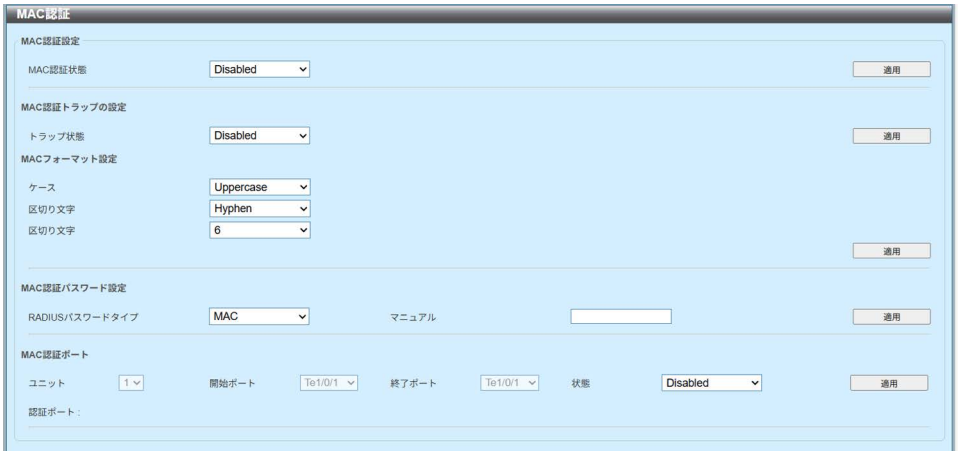

図 9-60 MAC 認証

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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC 認証トラップの設定] セクション）

パラメータ	概要
トラップ状態	MAC 認証トラップ機能の状態（**Enabled**/**Disabled**）を選択します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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。(ex AA-BB-CC-DD-EE-FF) • **Lowercase** - MAC アドレスに小文字形式を使用します。(ex aa-bb-cc-dd-ee-ff)
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。(ex AA-BB-CC-DD-EE-FF) • **Colon** - MAC アドレスで区切り文字としてコロンを使用します。(ex AA：BB：CC：DD：EE：FF) • **Dot** - MAC アドレスで区切り文字としてドットを使用します。(ex AA.BB.CC.DD.EE.FF) • **None** - MAC アドレスで区切り文字を使用しません。(ex AABBCCDDEEFF)
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。(ex AABBCC-DDEEFF) • **4** - MAC アドレスで区切り文字を 2 つ使用します。(ex AABB-CCDD-EEFF) • **6** - MAC アドレスで区切り文字を 5 つ使用します。(ex AA-BB-CC-DD-EE-FF)

[**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。 (初期値：: MAC)
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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 MAC 認証 (**Enabled/Disabled**) を設定します。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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。

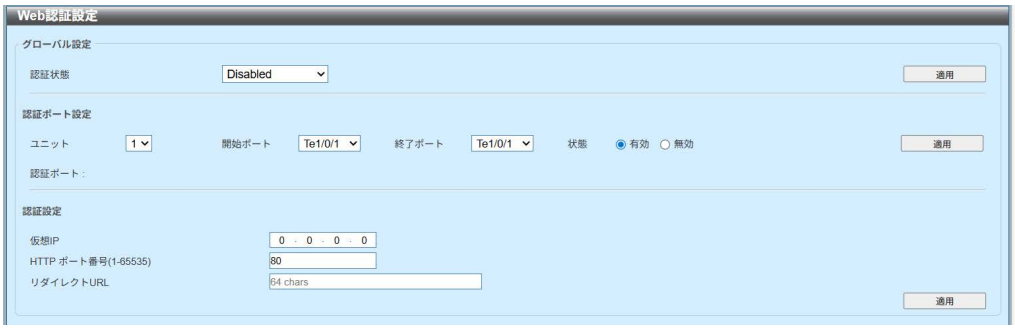

図 9-61 WEB 認証設定

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。(Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 WEB 認証機能の状態（**有効** / **無効**）を選択します。(初期値：無効)

[**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。 （初期値：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。（設定可能文字：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。

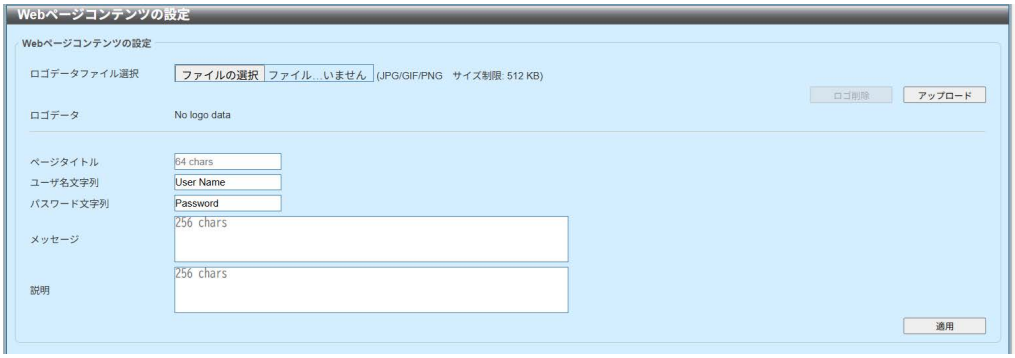

図 9-62 WEB ページコンテンツの設定

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	**[ファイルの選択]** 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）を選択します。 (ファイルのサイズ制限：512KB)
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。**[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。（設定可能文字：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。（設定可能文字：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。（設定可能文字：32 文字）
メッセージ	カスタムのメッセージを入力します。 （設定可能文字：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>

パラメータ	概要
説明	カスタムの説明メッセージを入力します。 (設定可能文字：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。
[**ロゴ削除**] ボタン - 既存の画像ファイルを削除します。

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 9-63 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。（設定可能文字：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 9-64 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
ユニット	ユニット ID を選択します。 スタッキングした際に表示します。
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。
フォワードユニット	ユニット ID を選択します。 スタッキングした際に表示します。
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。

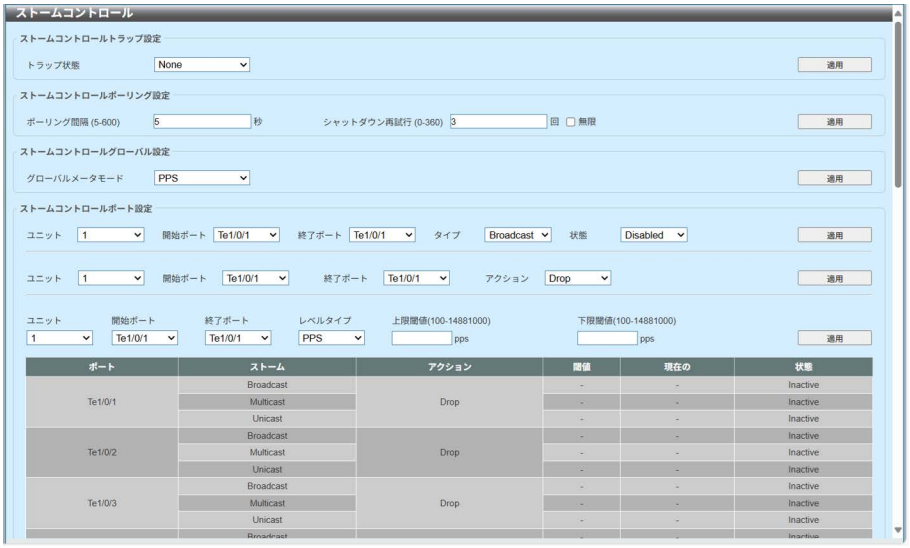

図 9-65 ストームコントロール

設定パラメータ （[ストームコントロールトラップ設定] セクション）

パラメータ	概要
トラップ状態	ストーム制御トラップの送信 (有効 / 無効) を選択します。オプションを以下から選択します。(初期値：None) • **None** - トラップ送信を無効にするように指定します。 • **Storm Occur** - ストームイベントを検知したときに通知を送信するように指定します。 • **Storm Clear** - ストームイベントがクリアされたときに通知を送信するように指定します。 • **Both** - ストームイベントが検知またはクリアされたときに通知を送信するように指定します。

[**適用**] ボタン - 設定内容を反映します

設定パラメータ （[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。 （初期値：5 秒 , 設定範囲：5 ～ 600 秒）
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。 （初期値：3 回 , 設定範囲：0 ～ 360 回） **[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グローバル設定] セクション）

パラメータ	概要
グローバルメータモード	グローバルメーターモードを選択します。選択できるオプションは以下です。 • **PPS** - パケット数を 1 秒あたりのカウントで測定します。 • **Kbps** - ビットレートを 1 秒あたりの速度で測定します。 • **Percentage** - 全帯域幅に対する割合として測定します。

[**適用**] ボタン - 設定内容を反映します

設定パラメータ （[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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
開始ポート／終了ポート	ポートを選択します。
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。
状態	ストームコントロール機能（**Enabled/Disabled**）を選択します。(Enabled：有効化 , Disabled：無効化)
アクション	実行するアクションを選択します。(初期値：Drop) • **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。

パラメータ	概要
レベルタイプ	レベルタイプオプションを選択します。 オプションは以下です。 • **PPS** - 閾値を 1 秒あたりのパケット数（PPS）で指定します。 • **Kbps** - 閾値を 1 秒あたりのビットレート（Kbps）を指定します。 • **Level** - 閾値を各ポートの総帯域幅に対するパーセンテージを指定します。
上限閾値	閾値の上限閾値を入力します。 • **PPS を選択した場合** - 1 秒あたりのパケット数（PPS）で閾値の上限値を入力します。 （設定範囲：100 ～ 14881000pps） • **Kbps を選択した場合 -** ポートで受信されるトラフィックのレートをキロビット毎秒（Kbps）で入力します。 （設定範囲：100 ～ 10000000Kbps） • **Level を選択した場合 -** ポートで受信されるトラフィックの閾値を、ポートの総帯域幅に対するパーセンテージで入力します。（設定範囲：1 ～ 100%）
下限閾値	閾値の下限閾値を入力します。 • **PPS を選択した場合** - 1 秒あたりのパケット数（PPS）で下限閾値を入力します。下限閾値を指定しない場合、デフォルトは指定した上限閾値の 80%となります。 （設定範囲：100 ～ 14881000pps） • **Kbps を選択した場合 -** ポートで受信されるトラフィックのレートをキロビット毎秒（Kbps）で入力します。下限閾値を指定しない場合は、上限閾値の 80%が初期値となります。（設定範囲：100 ～ 10000000Kbps） • **Level を選択した場合 -** ポートの総帯域幅に対するパーセンテージで下限閾値を入力します。指定しない場合は、上限閾値の 80%が初期値となります。 （設定範囲：1 ～ 100%）

[**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 9-66 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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)
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。 （初期値：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。 （初期値：120 秒 , 設定範囲：30 ～ 600 秒）
認証リトライ数	認証リトライ回数の値を入力します。 （初期値：3 回 , 設定範囲：1 ～ 32 回）

[**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 9-67 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。[キーモジュール] は [暗号化キータイプ] が RSA の場合のみ設定可能です。

[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。

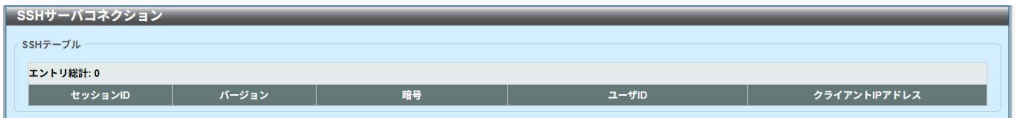

図 9-68 SSH サーバコネクション

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 9-69 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。 （設定可能文字：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。 （設定可能文字：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。（設定可能文字：255 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。
複数のページが存在する場合は、ページ番号を入力し、[**移動**] ボタンをクリックして特定のページに移動します。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

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 9-70 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。 (初期値：無効)
サービスポリシー	サービスポリシー名を入力します。（設定可能文字：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、**[ファイルの選択]** 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。（設定可能文字：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 9-71 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。（設定可能文字：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。（設定可能文字：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。
プライマリ	指定したトラストポイントをプライマリトラストポイントとして設定します。CA（Certificate Authority）のトラストポイントを明示的に指定していない場合、このトラストポイントが初期値として使用されます。

[**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。

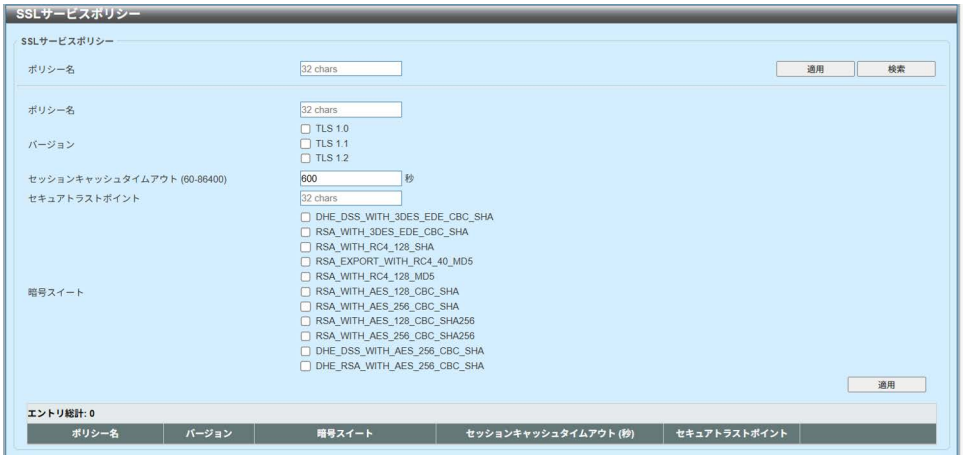

図 9-72 SSL サービスポリシー

設定パラメータ（**[SSL サービスポリシー]** セクション）

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。 (設定可能文字：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。 (初期値：600 秒 , 設定範囲：60 ～ 86400 秒)
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。 (設定可能文字：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。

9.18 ポートグルーピング設定

このウィンドウは、ポートグルーピング設定を行うために使用します。ポートグルーピングは、ホスト間の通信を分離するために使用されます。同じグループ内のホストのみが相互に通信でき、異なるグループ内のホストは通信できません。グループ内で定義されていないホストも相互に通信ができますが、グループ内のホストとは通信できなくなります。ポートは、複数のポートグループのメンバーになることができます。

[セキュリティ] > [ポートグルーピング設定] をクリックして、以下のウィンドウを表示します。

図 9-73 ポートグルーピング設定

設定パラメータ（**[ポートグループ設定]** セクション）

パラメータ	概要
グループ ID	グループ ID を入力します。(設定範囲 : 1 ～ 256)
グループ名	グループの名前を入力します。(設定可能文字 : 16 文字)
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
グループメンバー	グループメンバーのポートを選択します。

[**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。
[**削除**] ボタン - エントリを削除します。

[編集] セクションでは、以下のパラメータを設定できます。

図 9-74 ポートグループ設定 (編集)

設定パラメータ（[ポートグループ設定] セクション）

パラメータ	概要
状態	ポート グループ エントリのステータス (**Enabled/ Disabled**) にします。 (Enabled：有効化 , Disabled：無効化)

[**適用**] ボタン - エントリを追加します。

9.19 インターネットマンション設定

このウィンドウは、インターネットマンション設定を行います。アップリンク ポートのみにホストし、通信を制限するために使用されます。ダウンリンクポートに接続されているすべてのホストは互いに分離されており、アップリンクポートのみ通信できます。この機能を有効にすると、PPS、IEEE 802.1X、およびループ検出パケットは分離されません。

[セキュリティ] > [インターネットマンション設定] をクリックして、以下のウィンドウを表示します。

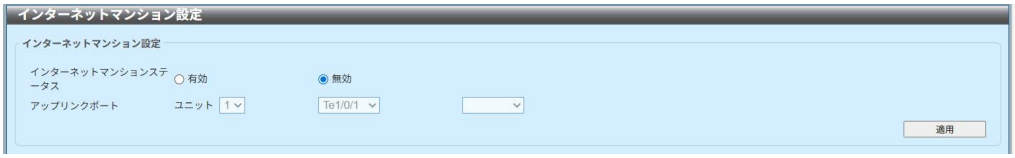

図 9-75 インターネットマンション設定

設定パラメータ（**[インターネットマンション設定]** セクション）

パラメータ	概要
インターネットマンションステータス	指定したポートでインターネットマンション機能 (**有効 / 無効**) を選択します。(初期値 : 無効)
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
アップリンクポート	アップリンクポートを選択します。

[**適用**] ボタン - エントリを追加します。

[**適用**] ボタンをクリックすると、次のプロンプトメッセージが表示されます。

図 9-76 インターネットマンション設定 (確認プロンプト)

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

[OAM] > [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。(初期値 : 無効)
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。(初期値 : 無効)

[**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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 DDM の状態（**Enabled**/**Disabled**）を選択します。(Enabled : 有効化 , Disabled : 無効化 , 初期値 : Enabled)

パラメータ	概要
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。

[OAM] > [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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 摂氏）

[**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。

[OAM] > [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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 ～ 6.55V）

[**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。

[OAM] > [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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 ～ 131mA）

[**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。

[OAM] > [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。

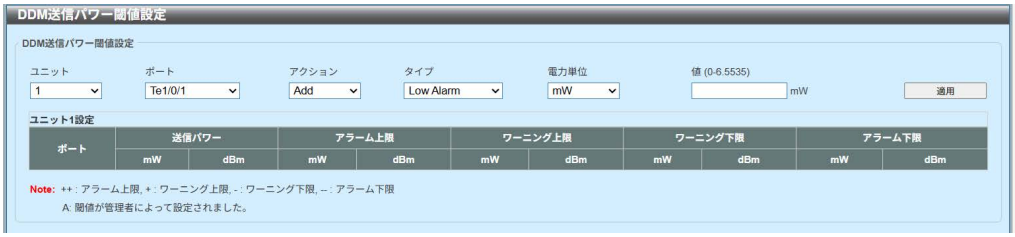

図 10-6 DDM 送信パワー閾値設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 - 0 ～ 6.5535mW で入力します。 • パワー単位が dBm の場合 - -40 ～ 8.1647dBm で入力します。

[**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。

[OAM] > [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。

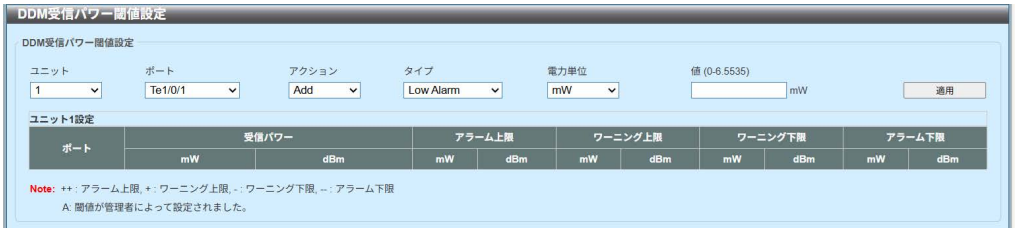

図 10-7 DDM 受信パワー閾値設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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 - 設定範囲は 0 ～ 6.5535mW です。 • パワー単位が dBm の場合 - 設定範囲は -40 ～ 8.1647dBm です。

[**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。

[OAM] > [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。

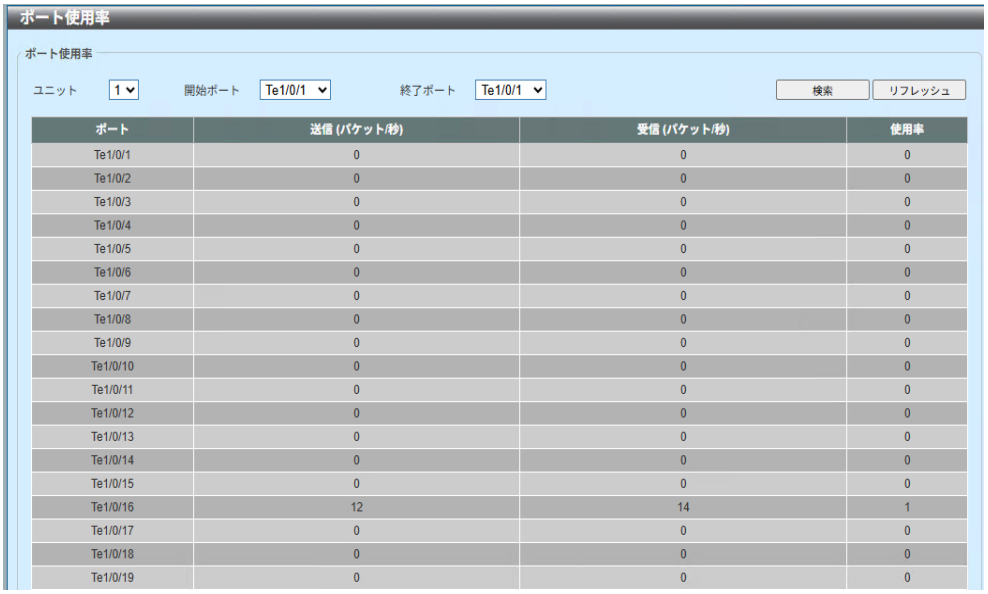

図 11-1 ポート使用率

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

[詳細参照] を選択すると、以下のウィンドウが表示されます。

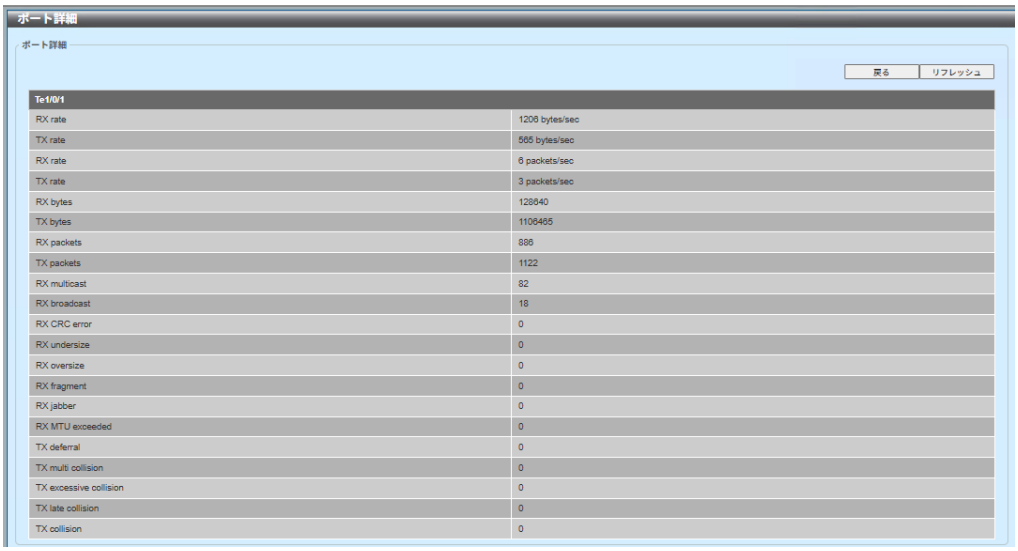

図 11-3 ポート (詳細参照)

[戻る]ボタン - 前のウィンドウに戻ります。
[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。

11.2.2 インターフェースカウンタ

このウィンドウを用いて、インター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] > [インターフェースカウンタ] をクリックして、以下のウィンドウを表示します。

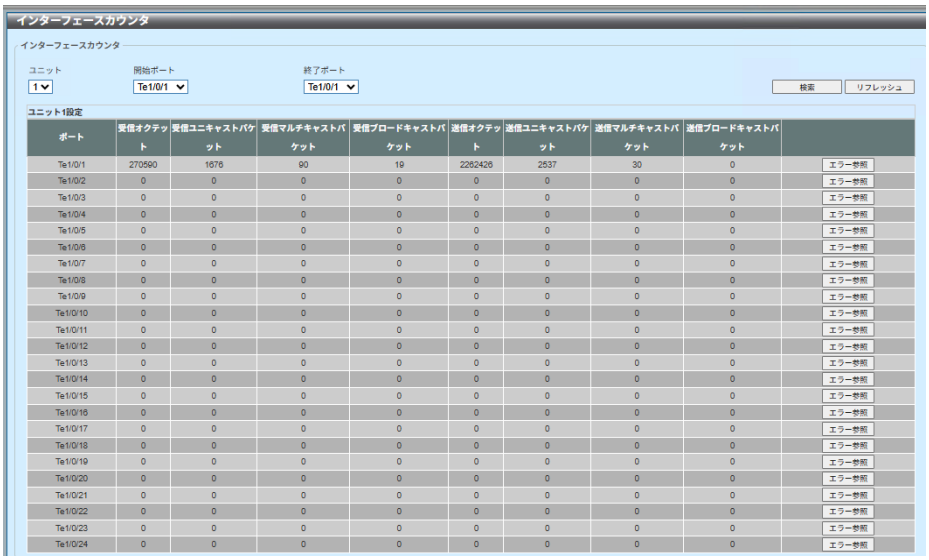

図 11-4 インターフェースカウンタ

設定パラメータ （[インターフェースカウンタ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

[エラー参照] を選択すると、以下のウィンドウが表示されます

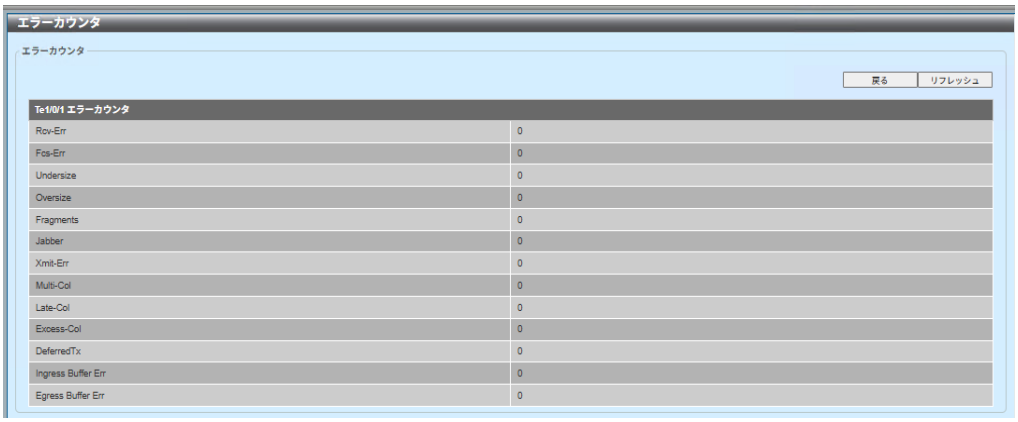

図 11-5 インターフェースカウンタ（エラー参照）

[戻る]ボタン - 前のウィンドウに戻ります。
[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。

11.2.3 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。

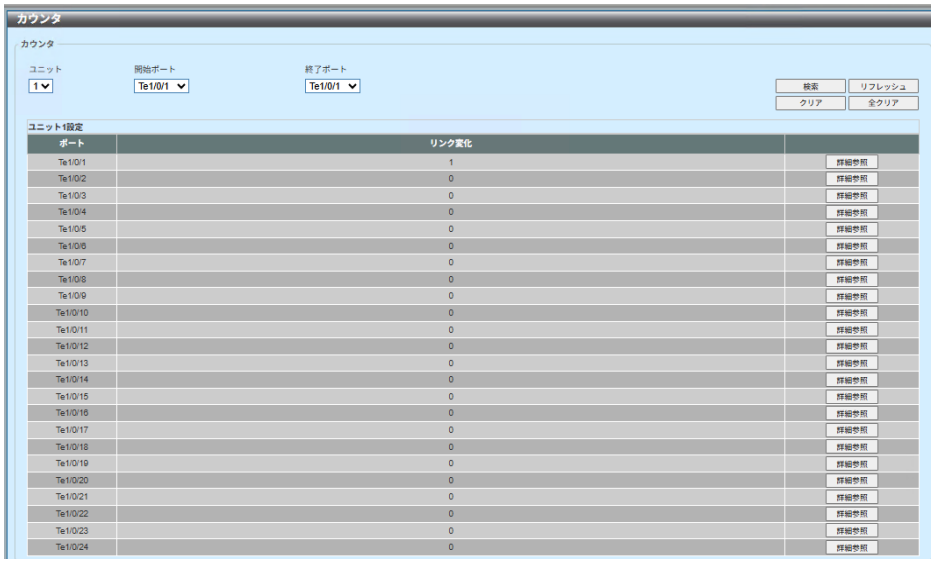

図 11-6 カウンタ

設定パラメータ （[カウンタ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

[**詳細参照**] を選択すると、以下のウィンドウが表示されます。

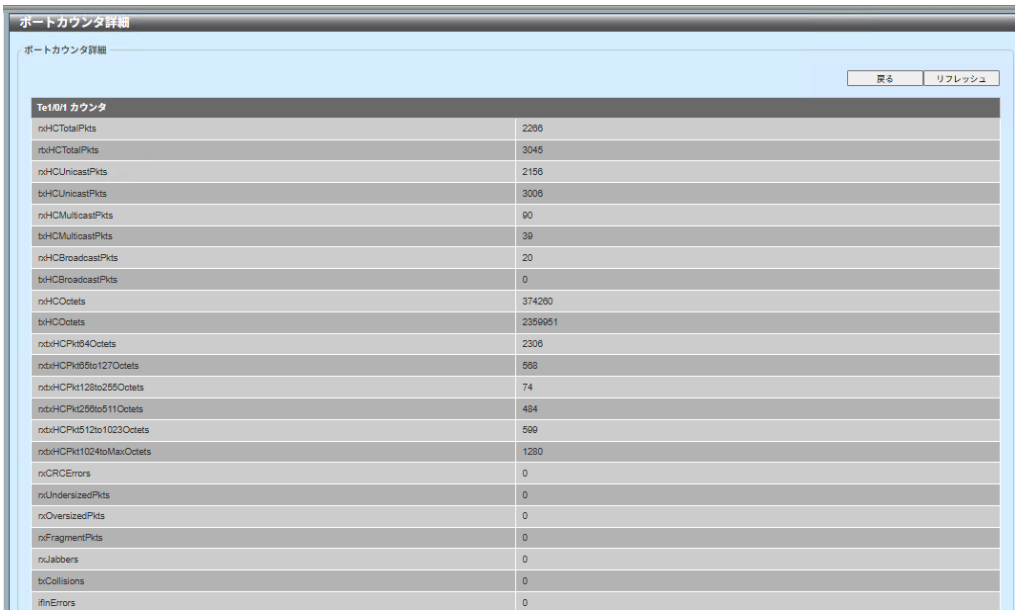

図 11-7 カウンタ (詳細参照)

[**戻る**] ボタン - 前のウィンドウに戻ります。
[**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。

11.3 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 11-8 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	VLAN ID を入力します。複数の VLAN ID を入力する場合はカンマで区切るか (ex 2,3)、範囲をハイフン (ex 2-5) でつなげて入力します。(設定範囲：2 ～ 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。

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宛先設定を選択および設定します。 • **Port** - ユニット ID と宛先のポート番号を選択します。 • **Remote VLAN** - ユニット ID と宛先のポート番号を選択します。VLAN ID（VID）を指定の欄に入力します。(VID 設定範囲：2 ～ 4094)

パラメータ	概要

ソース	• **Port** - [**開始ポート**]、[**終了ポート**] を選択します。
	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。
	• **ACL** - アクセスコントロールリスト（ACL）の名前を入力します。(設定可能文字：32 文字)
	• **VLAN** - VLAN ID または範囲を入力します。
	(設定範囲：2 ～ 4094)
	  • **RX** - 受信方向のみのトラフィックをミラーリングします。
	• **Remote VLAN** - VLAN ID を入力します。
	(設定範囲：2 ～ 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。

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。(設定範囲：1 ～ 4)

[**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。

[**詳細参照**] を選択すると、以下のウィンドウが表示されます。

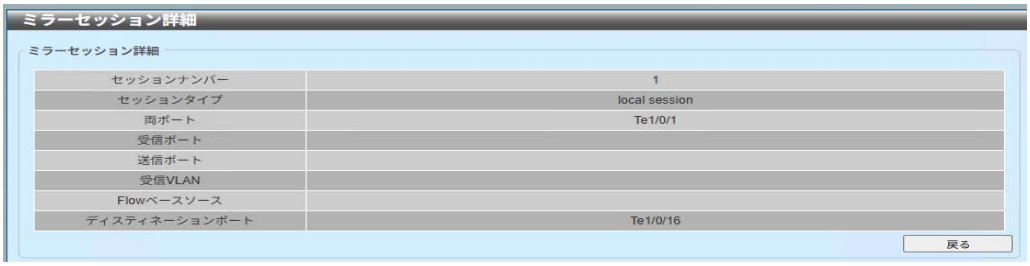

図 11-9 ミラー設定 (詳細参照)

[**戻る**] ボタン - 前のウィンドウに戻ります。

11.4 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。

11.4.1 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

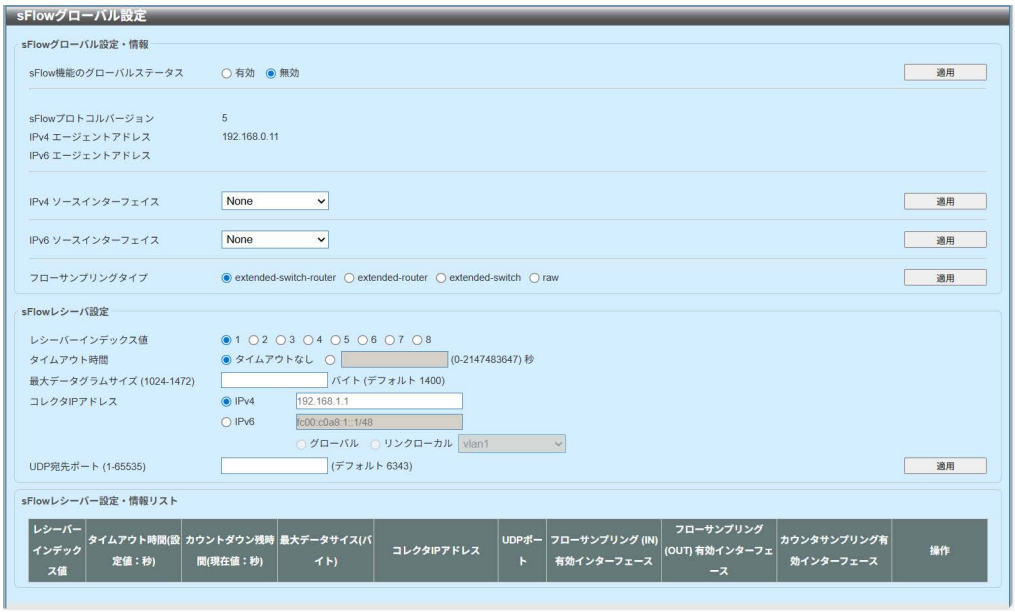

図 11-10 sFlow グローバル設定

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	**sFlow 機能 (有効 / 無効)** を選択します。 （デフォルト：無効）

[**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 アドレスを持つ VLAN を選択します。
IPv6 ソースインターフェース	IPv6 アドレスを持つ VLAN を選択します。
フローサンプリングタイプ	sFlow のフローサンプリングタイプを選択します。オプションは以下です。 • **extended-switch-router** - 拡張スイッチと拡張ルーターの両方の情報がサンプルヘッダーに含まれます。 • **extended-router** - 拡張ルータの情報のみがサンプルヘッダーに含まれます。 • **extended-switch** - 基本的な情報に加え、拡張スイッチの情報もサンプルヘッダーに含まれます。 • **raw** - フローサンプルが基本的な構成要素のみで構成されていることを示します。

[**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	レシーバーインデックス値を指定します。 (設定範囲：1 ～ 8)
タイムアウト時間	受信側の操作タイムアウト値を選択または入力します。 選択できるオプションは以下です。 • **タイムアウトなし** - 受信側の操作タイマーがタイムアウトしない設定です。デフォルトのオプションです。 • **タイムアウト時間** - 操作のタイムアウト時間 (秒) を入力します。(設定範囲：0 ～ 2147483647 秒)

パラメータ	概要
最大データグラムサイズ	最大のデータグラムサイズを入力します。 コレクタの IP アドレスによって設定範囲が異なります。 • IPv4 - 1024 バイト～ 1472 バイトの範囲で設定します • IPv6 - 1024 バイト～ 1452 バイトの範囲で設定します。 (初期値：1400 バイト)
コレクタ IP アドレス	sFlow データグラム送信先である sFlow コレクタの IP アドレス **(IPv4/IPv6)** を選択して入力します。**IPv6** アドレスを選択する場合は、以下のオプションを選択します。 • グローバル - グローバル IPv6 アドレスを使用します。 • リンクローカル - リンクローカル IPv6 アドレスを使用します。
UDP 宛先ポート	**sFlow** 接続の宛先 **TCP/UDP** ポート番号を入力します。 (初期値：6343, 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 （[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。 （設定範囲：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。 （指定範囲：0 ～ 2147483647（=2^{31}-1））。
最大データサイズ (バイト)	**1024 ～ 1472**：最大データサイズの値。
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。
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。

パラメータ	概要
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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

11.4.2 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 11-11 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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
設定インターフェース範囲 From/To	使用するポートまたはポート範囲を選択します。
レシーバーインデックスリスト	受信者のインデックス番号を選択します。
IN/OUT	サンプリング方向を選択します。 • **IN** - 受信したパケットを取得します。デフォルト設定です。 • **OUT** - 送信されるパケットを取得します。
サンプリングレート	パケットのサンプリングレートを入力します。 (初期値 : 1048576, 設定範囲 : 1024 ～ 16777216)
最大ヘッダサイズ	サンプリング時に許可される最大ヘッダサイズを入力します。 (初期値 : 128 バイト , 設定範囲 : 64 バイト～ 256 バイト)

[**適用**] ボタン - 設定内容を更新します。
[**削除**] ボタン - エントリを削除します。
[**編集**] ボタン - 設定内容を編集します。

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
エントリ総計	**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**：受信パケットがフローサンプリングの対象。 **OUT**：送信パケットがフローサンプリングの対象。
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}））。
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。

11.4.3 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。

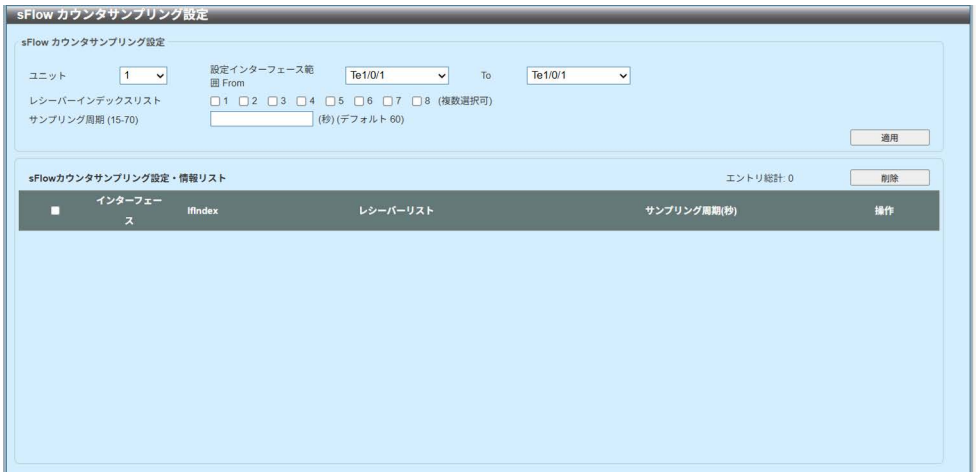

図 11-12 sFlow カウンタサンプリング設定

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
設定インターフェース範囲 From/To	使用するポートまたはポート範囲を選択します。
レシーバーインデックスリスト	受信者のインデックス番号を選択します。
サンプリング周期	サンプリング周期を入力します。 (初期値 : 60 秒 , 設定範囲 : 15 ～ 70 秒)

[**適用**] ボタン - 設定内容を更新します。
[**削除**] ボタン - エントリを削除します。
[**編集**] ボタン - 設定内容を編集します。

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
エントリ総計	**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 ～ 70 秒）。
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

11.4.4 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。

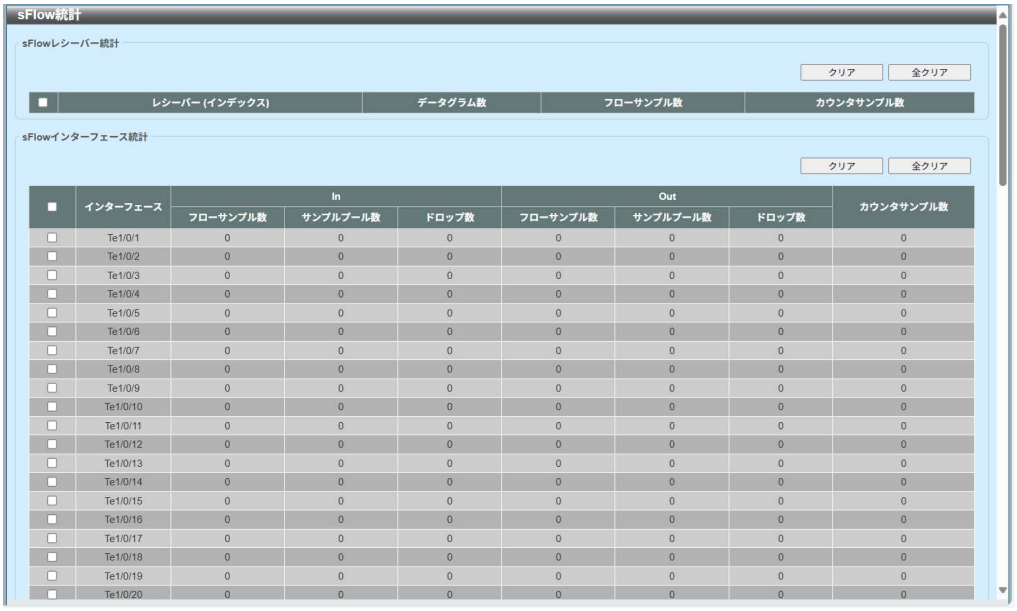

図 11-13 sFlow 統計

[**クリア**] ボタン - sFlow レシーバー統計情報をクリアします。
[**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 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。

11.5 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 11-14 デバイス

（注意）
* が状態コードを示しており、閾値を超えると * が表示されます。

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。

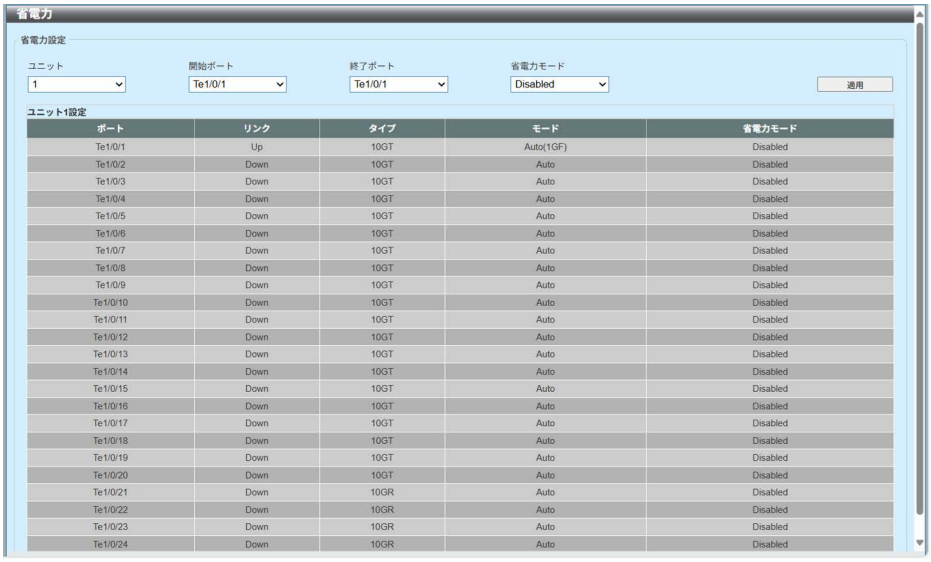

図 12-1 省電力

設定パラメータ （[省電力設定] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (初期値 : Disabled) • **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** - 省電力機能を有効にします。他機器との接続性を優先する省電力機能を利用する場合、こちらを設定します。

[**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。

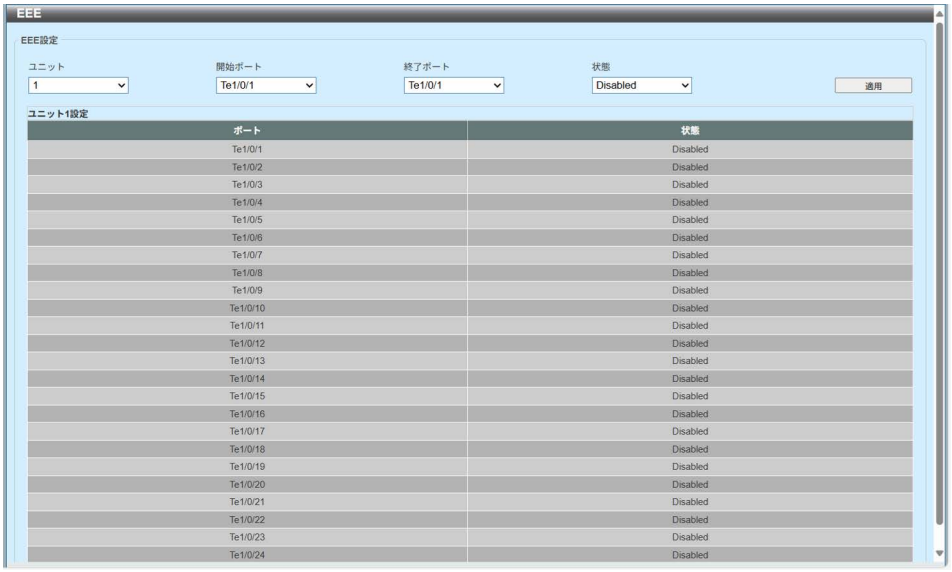

図 12-2 EEE

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。 (Enabled：有効化 , Disabled：無効化 , 初期値 : Disabled)

[**適用**] ボタン - 設定内容を反映します。

13 メンテナンスモード

13.1 メンテナンスモード設定

メンテナンスモードは、環境構築作業等で発生する Syslog や Trap を、他の端末やサーバへ送信しないように抑制する機能です。
対象は、コンソールライン ,Syslog サーバ , SMTP, SNMP, PPSP への通知です。

ご注意

- メンテナンスモード動作中はシステムログを内部バッファに記録し続けます。内部バッファが限界に達すると、もっとも古いログエントリが新しいログエントリで上書きされます。
- メンテナンスモードは、以下で終了します。
  - **時間満了**
  - **終了ボタンを選択し即時終了**
  - **Reboot(Normal) - 指定によるシステム再起動**
- メンテナンスモードを開始した時、以下設定は初期化されません。
  - **PoE オートリブート**
  - **PoE スケジュール**
- メンテナンスモードを開始した場合、下記、機能の設定は初期化されます。
  - **Reboot-in, at**

  （注意）メンテナンスモード動作中でも上記３つの機能は設定可能ですが、
  メンテナンスモード終了後に動作が開始となります。
- メンテナンスモード動作中に時刻が変更された場合 (SNTP 設定・時間設定)、変更された時刻に対応した「開始日時・終了日時」の表示を更新します。
- メンテナンスモードが設定されたことは running-config には残されません。

13.1.1 メンテナンスモード設定

このウィンドウを用いて、メンテナンスモード設定を行います。

[メンテナンスモード] > [メンテナンスモード設定] をクリックして、以下のウィンドウを表示します。

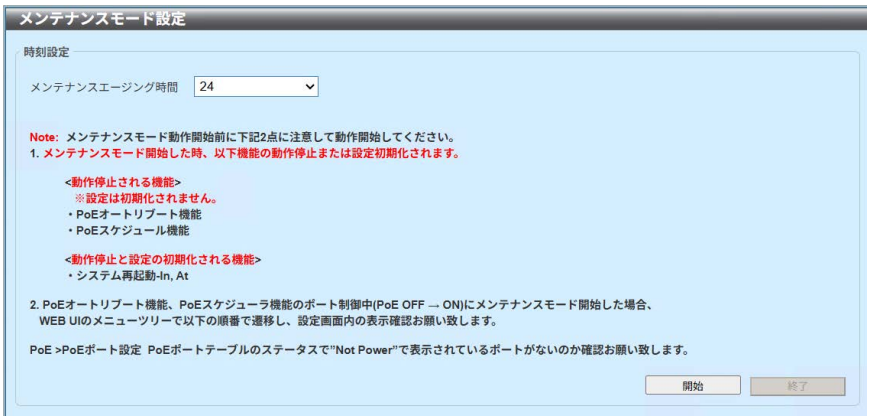

図 13-1 メンテナンスモード設定

設定パラメータ （[メンテナンスモード設定] セクション）

パラメータ	概要
メンテナンスエージング時間	メンテナンスモードの動作時間 (H) を指定します。 (初期値：24、設定範囲：1 ～ 24)

[**開始**] ボタン - メンテナンスモードを開始します。

[**開始**] ボタン押下後、Web UI の右上に以下の詳細情報を表示します。

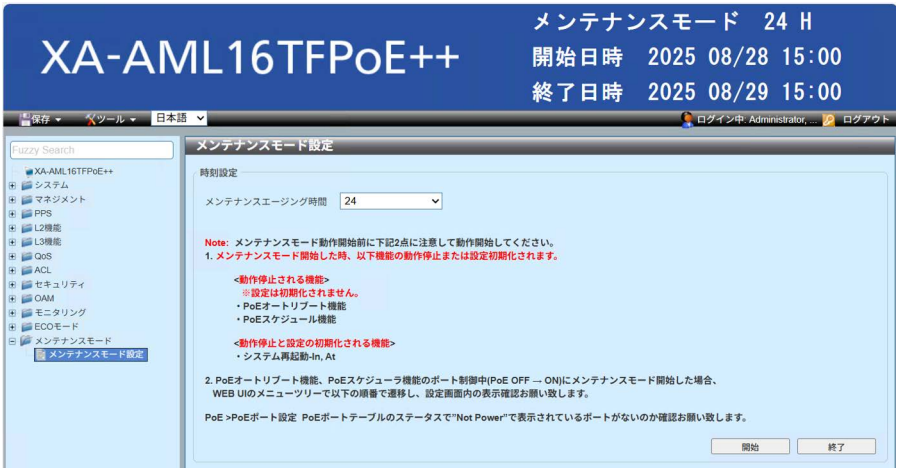

図 13-2 メンテナンスモード設定 - 詳細情報

設定パラメータ （[メンテナンスモード設定 - 詳細情報] セクション）

パラメータ	概要
メンテナンスモード	メンテナンスモードの動作時間を表示します。
開始日時	開始日時を表示します。
終了日時	終了日時を表示します。

メンテナンスモードの設定開始後に再度 **[開始]** を選択すると、メンテナンスモードの時間を上書きすることができます。上書きした時間で詳細情報表示も更新されます。メンテナンスモードの時間を上書きする際の設定パラメータに関しては、" 設定パラメータ (**[メンテナンスモード設定]** セクション)" を参照してください。

[終了] ボタン - メンテナンスモードを終了します。メンテナンスモードの詳細情報表示も消えます。

14 ツールバー

14.1 保存

14.1.1 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。

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。

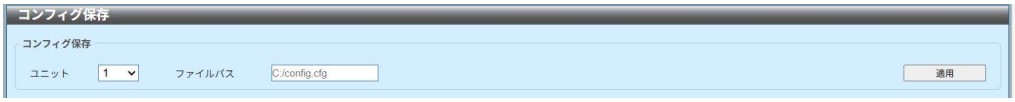

図 14-1 コンフィグ保存

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
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。

14.2 ツール

14.2.1 ファームウェアアップグレード&バックアップ

14.2.1.1 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。

(注意)
[実行しました] と表示されましたら、[マネジメント] > [ファイルシステム] で新しいファームウェアのファイルをブートアップに設定し、再起動します。

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 14-2 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（[HTTP サーバからファームウェアアップグレード] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (設定可能文字：779 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。

14.2.1.2 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。

(注意)
[実行しました] と表示されましたら、[マネジメント] > [ファイルシステム] で新しいファームウェアのファイルをブートアップに設定し、再起動します。

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 14-3 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（[TFTP サーバからファームウェアアップグレード] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(設定可能文字：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。 (設定可能文字：779 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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.1.3 FTP 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、FTP 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] > [FTP 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 14-4 FTP 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（[FTPサーバからファームウェアアップグレード]セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
FTP サーバ IP	FTP サーバの IP アドレスを入力します。 • **IPv4** - FTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - FTP サーバの IPv6 アドレスを選択および入力します。
ユーザ名	FTP 接続のユーザ名を入力します。(設定可能文字：32 文字)
パスワード	FTP 接続のパスワードを入力します。 (設定可能文字：15 文字)
ソースファイル	FTP 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。(設定可能文字：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。 (設定可能文字：779 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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.1.4 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 14-5 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（[RCP サーバからファームウェアアップグレード] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：16 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。（設定可能文字：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。 （設定可能文字：779 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。

14.2.1.5 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 14-6 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（[HTTP サーバへファームウェアバックアップ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：64 文字）

[バックアップ] ボタン - バックアップを開始します。

14.2.1.6 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 14-7 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（[TFTP サーバへファームウェアバックアップ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：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。 （設定可能文字：779 文字）

[**バックアップ**] ボタン - バックアップを開始します。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.1.7 FTP 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 FTP 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] > [FTP 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 14-8 FTP サーバへファームウェアバックアップ

設定パラメータ（[FTP サーバへファームウェアバックアップ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
FTP サーバ IP	FTP サーバの IP アドレスを入力します。 • **IPv4** - FTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - FTP サーバの IPv6 アドレスを選択および入力します。
TCP ポート	FTP 接続のポート番号を入力します。 (設定範囲：1 ～ 65535)
ユーザ名	FTP 接続のユーザ名を入力します。(設定可能文字：32 文字)
パスワード	FTP 接続のパスワードを入力します。 (設定可能文字：15 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。(設定可能文字：64 文字)
ディスティネーション ファイル	FTP 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。 (設定可能文字：779 文字)

[バックアップ] ボタン - バックアップを開始します。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.1.8 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 14-9 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（[RCP サーバへファームウェアバックアップ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字 : 16 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。（設定可能文字 : 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。 （設定可能文字 : 779 文字）

[**バックアップ**]ボタン - バックアップを開始します。

14.2.2 コンフィグレーション復旧＆バックアップ

14.2.2.1 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 14-10 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（[HTTP サーバからコンフィグレーション復旧] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。 (設定可能文字：779 文字) • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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	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。

14.2.2.2 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 > [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 14-11 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（[TFTP サーバからコンフィグレーション復旧] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：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。 （設定可能文字：779 文字） • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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	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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.2.3 FTP 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、FTP 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 > [ツール] > [コンフィグレーション復旧&バックアップ] > [FTP 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 14-12 FTP サーバからコンフィグレーション復旧

設定パラメータ（[FTP サーバからコンフィグレーション復旧] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
FTP 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 IPv4 アドレスを選択および入力します。
TCP ポート	FTP 接続の TCP ポート番号を入力します。 (設定範囲：1 ～ 65535)
ユーザ名	FTP 接続のユーザ名を入力します。(設定可能文字：32 文字)
パスワード	FTP 接続のパスワードを入力します。 (設定可能文字：15 文字)
ソースファイル	FTP 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。(設定可能文字：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。 (設定可能文字：779 文字) • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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	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。

14.2.2.4 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 > [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 14-13 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（[RCP サーバからコンフィグレーション復旧] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：16 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。（設定可能文字：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。 （設定可能文字：64 文字） • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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	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。

14.2.2.5 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 > [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 14-14 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（[HTTP サーバへコンフィグレーションをバックアップ] セクション）

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。（設定可能文字：64 文字） • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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。

14.2.2.6 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 > [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 14-15 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
([TFTP サーバへコンフィグレーションをバックアップ] セクション)

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(設定可能文字 : 64 文字) • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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。 (設定可能文字 : 779 文字)

[バックアップ] ボタン - バックアップを開始します。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.2.7 FTP 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 FTP サーバに保存します。

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] > [FTP 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。

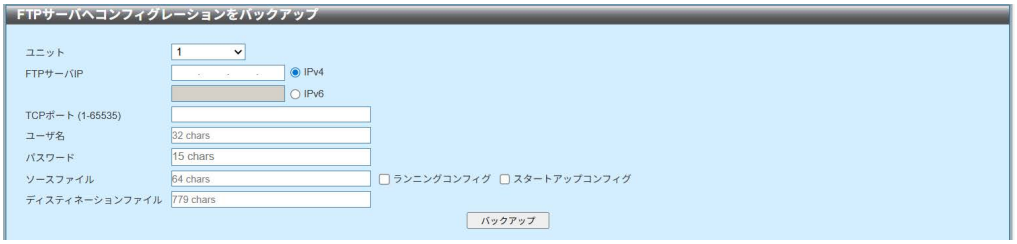

図 14-16 FTP サーバへコンフィグレーションをバックアップ

設定パラメータ
([FTP サーバへコンフィグレーションをバックアップ] セクション)

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
FTP サーバ IP	FTP サーバの IP アドレスを入力します。 • IPv4 - FTP サーバの IPv4 アドレスを選択および入力します。 • IPv6 - FTP サーバの IPv6 アドレスを選択および入力します。
TCP ポート	FTP 接続の TCP ポート番号を入力します。 (設定範囲 : 1 ～ 65535)
ユーザ名	FTP 接続のユーザ名を入力します。(設定可能文字 : 32 文字)
パスワード	FTP 接続のパスワードを入力します。 (設定可能文字 : 15 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。(設定可能文字 : 64 文字) • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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 FTP 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。 (設定可能文字 : 779 文字)

[**バックアップ**] ボタン - バックアップを開始します。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
 例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.2.8 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 > [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 14-17 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
([RCP サーバへコンフィグレーションをバックアップ] セクション)

パラメータ	概要
ユニット	ユニット ID を入力します。 スタッキングした際に表示します。
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。(設定可能文字 : 16 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。(設定可能文字 : 64 文字) • **ランニングコンフィグ** - 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。 • **スタートアップコンフィグ** - 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。 (設定可能文字 : 779 文字)

[**バックアップ**] ボタン - バックアップを開始します。

14.2.3 ログバックアップ

14.2.3.1 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 14-18 ログを HTTP サーバへバックアップ

設定パラメータ（[ログを HTTP サーバへバックアップ] セクション）

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。

14.2.3.2 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 14-19 ログを TFTP サーバへバックアップ

設定パラメータ（[ログを TFTP サーバへバックアップ] セクション）

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。（設定可能文字：779 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。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、以下のように入力してください：

例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス "FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.3.3 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 14-20 ログを RCP サーバへバックアップ

設定パラメータ（[ログを RCP サーバへバックアップ] セクション）

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。（設定可能文字：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。（設定可能文字：779 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。

14.2.4 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。

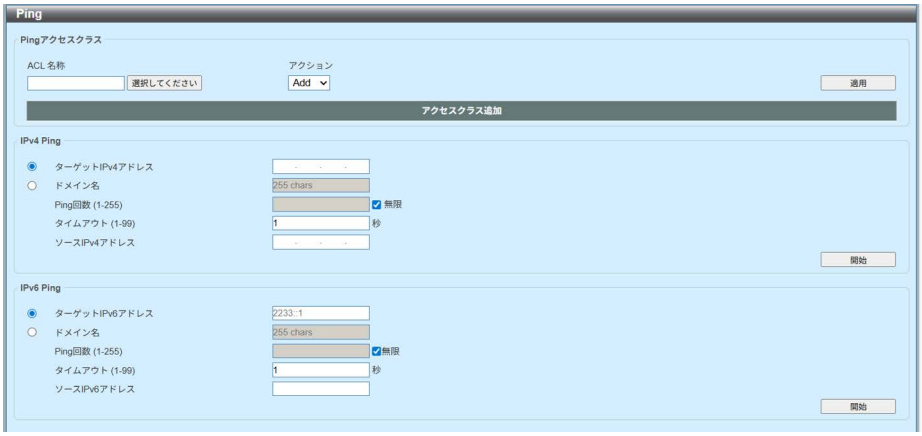

図 14-21 Ping

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	既存の ACL を選択します。[**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。

[選択してください] をクリックすると、次のウィンドウが表示されます。

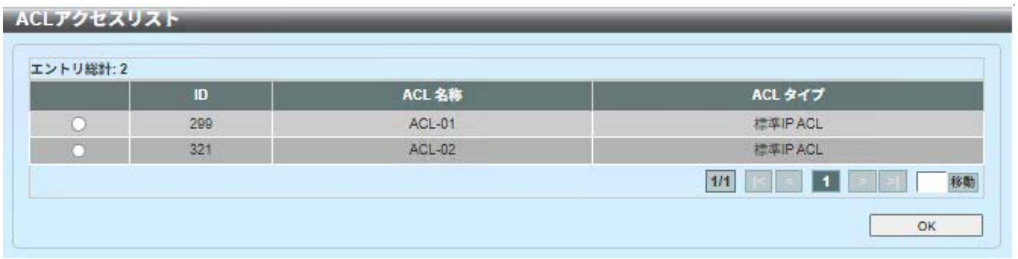

図 14-22 Ping (選択してください)

ページ番号を入力し、**[移動]** ボタンをクリックすると、特定のページに移動します。
[OK] ボタン - 選択したアクセス制御リストを使用します。

設定パラメータ（[IPv4 Ping] セクション）

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	宛先のドメイン名を入力します。 (設定可能文字：255 文字)
Ping 回数	このウィンドウで設定した IPv4 アドレスに ICMP Echo パケットを送信します。(初期値：[**無限**]) **[無限]** チェックボックスをオフにした場合、Ping を施行する回数を入力し、回数分送信します。(設定範囲：1 ～ 255)
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。(設定範囲：1 ～ 99 秒)
ソース **IPv4** アドレス	送信元の IPv4 アドレスを入力します。複数の IPv4 アドレスが設定されている場合、その中のいずれかを入力できます。この IPv4 アドレスは、リモートホストに送信されるパケットの送信元アドレスとして使用されます。

[開始] ボタン - IPv4 Ping を開始します。

設定パラメータ（[IPv6 Ping] セクション）

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	宛先のドメイン名を入力します。 (設定可能文字：255 文字)
Ping 回数	このウィンドウで設定した IPv6 アドレスに ICMP Echo パケットを送信します。(初期値：[**無限**]) **[無限]** チェックボックスをオフにした場合、Ping を施行する回数を入力し、回数分送信します。(設定範囲：1 ～ 255)
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。(設定範囲：1 ～ 99 秒)
ソース **IPv6** アドレス	送信元の IPv6 アドレスを入力します。複数の IPv6 アドレスが設定されている場合、その中のいずれかを入力できます。この IPv6 アドレスは、リモートホストに送信されるパケットの送信元アドレスとして使用されます。

[開始] ボタン - 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。

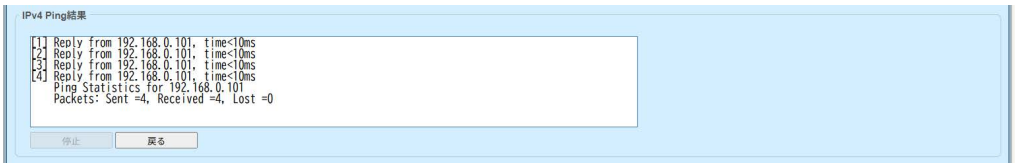

図 14-23 IPv4 Ping(結果)

[停止] ボタン - Ping プロセスを停止します。
[戻る] ボタン - 前の [Ping] ウィンドウに戻ります。

[IPv6 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。

図 14-24 IPv6 Ping(結果)

[停止] ボタン - Ping プロセスを停止します。
[戻る] ボタン - 前の [Ping] ウィンドウに戻ります。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.5 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。

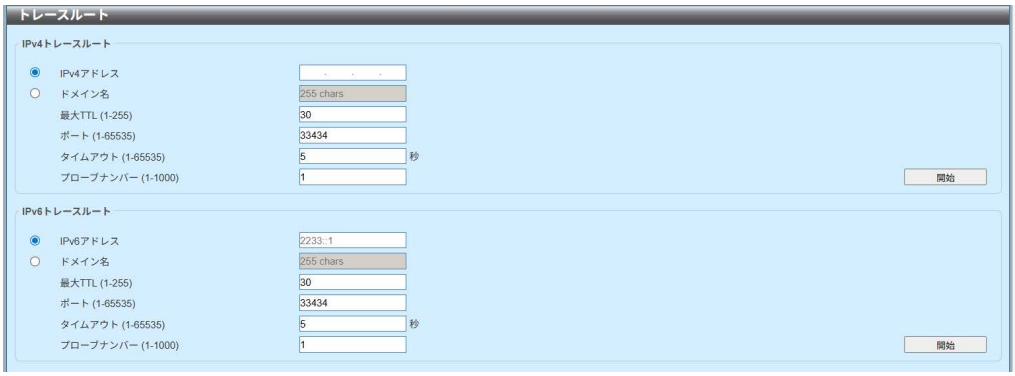

図 14-25 トレースルート

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	ドメイン名を入力します。(設定可能文字 : 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。(設定範囲 : 1 ～ 255)
ポート	ポート番号を入力します。(設定範囲 : 1 ～ 65535)
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。(初期値 : 5 秒 , 設定範囲 : 1 ～ 65535 秒）
プローブナンバー	プローブタイムの数を入力します。（初期値 : 1, 設定範囲 : 1 ～ 1000）

[**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	ドメイン名を入力します。(設定可能文字 : 255 文字)
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。 (設定範囲 : 1 ～ 255)
ポート	ポート番号を入力します。(設定範囲 : 1 ～ 65535)
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。（初期値 : 5, 設定範囲 : 1 ～ 65535）
プローブナンバー	プローブタイムの数を入力します。 （初期値 : 1, 設定範囲 : 1 ～ 1000）

[**開始**] ボタン - IPv6 トレースルートを開始します。

[IPv4 トレースルート] 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。

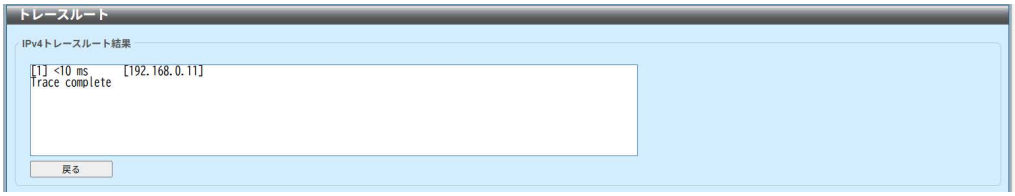

図 14-26 IPv4 トレースルート (結果)

[戻る] ボタン - 前の **[トレースルート]** ウィンドウに戻ります。

[IPv6 トレースルート] 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。

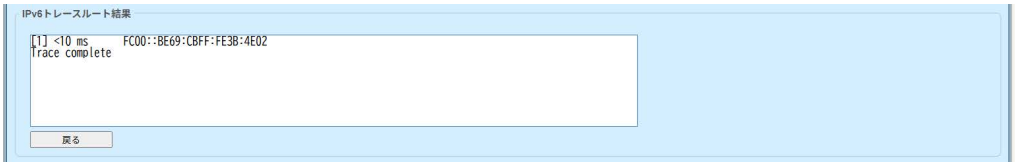

図 14-27 IPv6 トレースルート (結果)

[**戻る**] ボタン - 前の **[トレースルート]** ウィンドウに戻ります。

（注意）
FE80 から始まる IPv6 のリンクローカルアドレスを使用する場合は、
以下のように入力してください：
例：インターフェース VLAN 1 の IPv6 リンクローカルアドレス
"FE80::200:FF:FE00" を指定する。

FE80::200:FF:FE00%vlan1

14.2.6 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 14-28 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。このオプションはスタッキング情報をリセット対象から除外します。

[**適用**] ボタン - 工場出荷状態へのリセットを開始します。

14.2.7 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 14-29 システム再起動 (Normal)

設定パラメータ（[システム再起動 (Normal)] セクション）

パラメータ	概要
システム再起動	オプションを選択します。 • **In** - 一定時間が経過した後にスイッチを再起動するように指定します。コンフィグレーションは自動的には**保存されません。** • **At** - 指定された時刻または日付が経過した後にスイッチを再起動するように指定します。コンフィグレーションは自動的には**保存されません。** • **Normal** - スイッチが直ちに再起動するように指定します。
セーブ設定	**[はい]** - 再起動する前に現在のコンフィグレーションを保存します。 **[いいえ]** - 現在のコンフィグレーションを削除します。

[**適用**] ボタン - 指定した再起動オプションに従い、再起動を開始します。
[**キャンセル**] ボタン - 設定した再起動タイマーをキャンセルします。

[In] を選択後、以下のウィンドウを表示します。

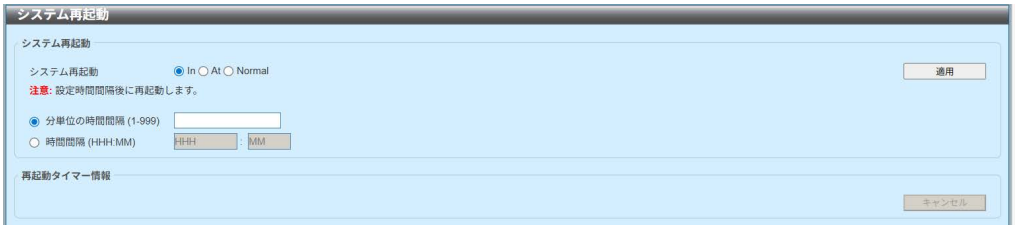

図 14-30 システム再起動 (In)

設定パラメータ （[システム再起動 (In)] セクション）

パラメータ	概要
分単位の時間間隔	インターバル値を入力します。(設定範囲 :1 ～ 999 分)
時間間隔	タイムインターバルを選択します。時間(HHH)と分(MM)の値を入力します。

[**適用**] ボタン - 一定時間経過後、再起動を開始します。

[At] を選択後、以下のウィンドウを表示します。

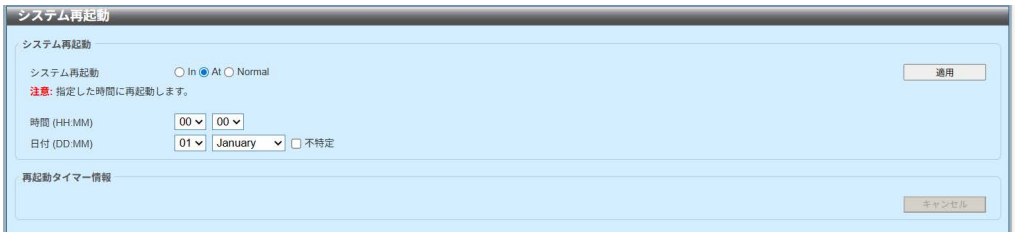

図 14-31 システム再起動 (At)

設定パラメータ （[システム再起動 (At)] セクション）

パラメータ	概要
時間	スイッチ再起動の時間を選択します。時間(HH)と分(MM)の値を選択します。
日付	スイッチ再起動の日付を選択します。 再起動は最大で24 日後まで遅らせることができます。

[**適用**] ボタン - 指定された時間または日付が経過した後に
再起動を開始します。

（注意）
システム再起動 - At を設定する際、最大許容期間は 24 日のため年間を通して設定することはできません。
例）現在時刻：2025 年 7 月 7 日 14:20 で「7 月 7 日 14:10」は
設定できません。

14.3 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 14-32 言語

14.4 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 14-33 ログアウト

15 付録 - システムログ一覧

15.1 802.1X

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。	Informational
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。	Notice
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。	Notice

15.2 802.1X サプリカント

ID	ログの概要	重大度
1.	イベントの概要：802.1X サプリカントの認証が成功しました。 ログメッセージ：802.1X Supplicant authorized	Informational
2.	イベントの概要：802.1X サプリカントの認証が失敗しました。 ログメッセージ：802.1X Supplicant rejected	Notice

15.3 AAA

ID	ログの概要	重大度
1.	イベントの概要：AAA グローバル状態が有効または無効になりました。 ログメッセージ：AAA is <status> パラメータ概要： status：AAA のステータス	Informational
2.	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 <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> <server-ip> (Username: <username>) パラメータ概要： exec-type：exec の種類。例：コンソール , telnet, SSH, WEB, WEB(SSL) client-ip：IP プロトコルで有効な場合のクライアント IP アドレス aaa-method：認証方法。　例 :none, local, server server-ip: 認証方法がリモートサーバの場合の AAA サーバ IP アドレス username: 認証ユーザ名	Informational
3.	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 <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> <server-ip> (Username: <username>) パラメータ概要： exec-type：exec の種類。例：コンソール , telnet, SSH, WEB, WEB(SSL) client-ip：IP プロトコルで有効な場合のクライアント IP アドレス aaa-method：認証方法　例：local, server server-ip: 認証方法がリモートサーバの場合の AAA サーバ IP アドレス username: 認証ユーザ名	Warning
4.	イベントの概要：リモートサーバがログイン認証のリクエストに応答がありませんでした。 ログメッセージ：Login failed through <exec-type> [from <client-ip>]due to AAA server <server-ip> timeout (Username: <username>) パラメータ概要： exec-type：exec の種類。例：コンソール , telnet, SSH, WEB, WEB(SSL) client-ip：IP プロトコルで有効な場合のクライアント IP アドレス server-ip: AAA サーバ IP アドレス username: 認証ユーザ名	Warning
5.	イベントの概要：特権の有効化に成功しました。 ログメッセージ：Successful enable privilege through <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> <server-ip> (Username: <username>) パラメータ概要： exec-type：exec の種類。例：コンソール , Telnet, SSH client-ip：IP プロトコルで有効な場合のクライアント IP アドレス aaa-method：認証方法。　例 : local, server server-ip: 認証方法がリモートサーバの場合、AAA サーバ IP アドレス username: 認証ユーザ名	Informational

ID	ログの概要	重大度
6.	イベントの概要：特権の有効化に失敗しました。 ログメッセージ：Enable privilege failed through <exec-type> [from <client-ip>]authenticated by AAA <aaa-method> <server-ip> (Username: <username>) パラメータ概要： exec-type：exec の種類。例：コンソール , Telnet, SSH client-ip：IP プロトコルで有効な場合のクライアント IP アドレス aaa-method：認証方法。例：local, server server-ip: 認証方法がリモートサーバの場合の AAA サーバ IP アドレス username: 認証ユーザ名	Warning
7.	イベントの概要：リモートサーバが enable パスワード認証に応答がありませんでした。 ログメッセージ:Enable privilege failed through <exec-type> [from <client-ip>]due to AAA server <server-ip> timeout (Username: <username>) パラメータ概要： exec-type：exec の種類。例：コンソール , Telnet, SSH client-ip：IP プロトコルで有効な場合のクライアントの IP アドレス server-ip: AAA サーバ IP アドレス username: 認証ユーザ名	Warning
8.	イベントの概要：RADIUS サーバが有効な VLAN ID を割り当てました。 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 vid：RADIUS サーバから割り当てられた VLAN ID interface-id: クライアントの認証されたポート番号 username: 認証ユーザ名	Informational
9.	イベントの概要：RADIUS サーバが帯域幅の制限を割り当てました。 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 direction：帯域幅の制御方向（例：ingress（受信）または egress（送信）） threshold：RADIUS サーバから割り当てられた帯域幅の上限値 interface-id: クライアントの認証されたポート番号 username: 認証ユーザ名	Informational
10.	イベントの概要：RADIUS サーバがデフォルトの 802.1p 優先度を割り当てました。 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 priority：RADIUS サーバから割り当てられた 802.1p の優先度 interface-id: クライアントの認証されたポート番号 username: 認証ユーザ名	Informational

ID	ログの概要	重大度
11.	イベントの概要：システムリソースが不足しているため、RADIUS サーバから割り当てられた ACL スクリプトの適用に失敗しました。 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 username: 認証ユーザ名 interface-id: クライアントの認証されたポート番号 acl-script：RADIUS サーバから割り当てられた ACL スクリプト	Warning

15.4 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。	Warning

15.5 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。	Informational
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。	Notice
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。	Notice
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。	Notice
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。	Notice

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。	Notice
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。	Notice

15.6 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：<interface-id> enter STP BPDU under protection state (mode: <mode>) パラメータ概要： interface-id：BPDU アタックを検知したインターフェース。 mode：BPDU の現在の状態。状態は drop、block または shutdown。	Informational
2.	イベントの概要：BPDU アタックから復旧しました。 ログメッセージ：<interface-id> recover from BPDU under protection state パラメータ概要： interface-id：BPDU アタックを検知したインターフェース。	Informational

15.7 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： 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。 username：このコマンドを実行したアカウント名。 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。	Informational

15.8 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：Firmware 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。	Informational
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。	Warning
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。	Informational
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。	Warning

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。	Informational
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。	Warning
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。	Informational
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。	Warning

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。	Warning
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。	Informational
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。	Informational

15.9 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。	Warning
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。	Warning

15.10 DDM

ID	ログの概要	重大度
1.	イベント概要：DDM が警告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"	Warning
2.	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"	Critical

15.11 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	Emergencies
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	Emergencies

15.12 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。	Informational
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。	Informational
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。	Informational
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。	Informational
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。	Informational
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。	Informational
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。	Informational

ID	ログの概要	重大度
8.	イベントの概要：DHCPv6PD クライアントのインターフェースの管理状態が変更されました。 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：DHCPv6PD クライアントのインタフェースの名前。	Informational
9.	イベントの概要：DHCPv6 クライアントの PD は、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 のプレフィックスです。 intf-name：DHCPv6PD クライアントのインタフェースの名前。	Informational
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プロセスが開始されました。 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 のプレフィックスです。 intf-name：DHCPv6PD クライアントのインタフェースの名前。	Informational
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が完了しました。 ログメッセージ： The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 のプレフィックスです。 intf-name：DHCPv6PD クライアントのインタフェースの名前。	Informational
12.	イベントの概要：委任ルータから取得した IPv6 プレフィックスのリバインド作業が開始されました。 ログメッセージ： The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 のプレフィックスです。 intf-name：DHCPv6PD クライアントのインタフェースの名前。	Informational
13.	イベントの概要：委任ルータから取得した IPv6 プレフィックスのリバインド作業が完了しました。 ログメッセージ： The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 のプレフィックスです。 intf-name：DHCPv6PD クライアントのインタフェースの名前。	Informational
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： ipv6networkaddr：委任ルータから取得した IPv6 のプレフィックスです。 intf-name：DHCPv6PD クライアントのインタフェースの名前。	Informational

15.13 DHCPv6 リレー

ID	ログの概要	重大度
1.	イベントの概要：特定のインタフェースの DHCPv6 リレーの管理者の状態が変化しました。 ログメッセージ：DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] パラメータ概要： ipif-name：DHCPv6 リレーエージェントインタフェースの名前。	Informational

15.14 DHCPv6 サーバ

ID	ログの概要	重大度
1.	イベントの概要：DHCPv6 サーバプール <pool-name> のアドレスを使い果たしました。 ログメッセージ：The address of the DHCPv6 Server pool <pool-name> is used up パラメータ概要： pool-name：DHCPv6 サーバプールの名前。	Informational
2.	イベントの概要：割り当て済みの IPv6 アドレスの数が 704 に等しくなりました。 ログメッセージ：The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 704	Informational

15.15 DNS リゾルバ

ID	ログの概要	重大度
1.	イベントの概要：重複するドメイン名キャッシュが追加されたため、ダイナミックドメイン名キャッシュが削除されます。 ログメッセージ：Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> パラメータ概要： domain name：ドメイン名文字列。 ipaddr：IP アドレス。	Informational

15.16 ダイナミック ARP Inspection

ID	ログの概要	重大度
1.	イベントの概要：このログは、DAI(Dynamic ARP Inspection) 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。	Warning
2.	イベントの概要：このログは、DAI(Dynamic ARP Inspection) 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。	Informational

15.17 ファン

ID	ログの概要	重大度
1.	イベントの概要：ファンが機能していません。 ログメッセージ：Unit <unitID>, LEFT Fan <value> failed パラメータ概要： unit ID：ユニット ID value：ファン ID	Critical
2.	イベントの概要：ファンが復旧しました。 ログメッセージ：Unit <unitID>, LEFT Fan <value> back to normal パラメータ概要： unit ID：ユニット ID value：ファン ID	Critical
3.	イベントの概要：ファンのモードを変更しました。 ログメッセージ：Unit <unitID>, Fan mode <value> パラメータ概要： unit ID：ユニット ID value：ファン ID	Critical

15.18 インターフェース

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。	Informational
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。	Informational

15.19 PoE [XA-AML8TFPoE++/XA-AML16TFPoE++]

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 On notification パラメータ概要： port：論理ポート番号を表します。	Informational
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 Off notification パラメータ概要： port：論理ポート番号を表します。	Informational
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	Notice
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	Informational
5.	イベントの概要：PoE がアラーム状態に入ります。 ログメッセージ：Uint <unitID> POE detects abnormal パラメータ概要： unitID：ユニット ID を表しております。	Critical
6.	イベントの概要：PoE IC が正常に復旧しました。 ログメッセージ：Uint <unitID> POE detects Normal パラメータ概要： unitID：ユニット ID を表しております。	Critical

15.20 PoE オートリブート [XA-AML8TFPoE++/XA-AML16TFPoE++]

ID	ログの概要	重大度
1.	イベントの概要：PoE 給電の ON を実行しました。 ログメッセージ：Execute PoE ON(< interface-id >) パラメータ概要： interface-id：ポート番号を表します。	Warning
2.	イベントの概要：PoE 給電の OFF を実行しました。 ログメッセージ：Execute PoE OFF(< interface-id >) パラメータ概要： interface-id：ポート番号を表します。	Warning
3.	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(<ipaddr>) パラメータ概要： ipaddr：PoE 端末の IP アドレスを表します。	Warning
4.	イベントの概要：Ping 監視が復旧しました。 ログメッセージ：Detect equipment recovery by ICMP(<ipaddr>) パラメータ概要： ipaddr：PoE 端末の IP アドレスを表します。	Informational
5.	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(< interface-id >) パラメータ概要： interface-id：ポート番号を表します。	Warning
6.	イベントの概要：LLDP 監視が復旧しました。 ログメッセージ：Detect equipment recovery by LLDP(< interface-id >) パラメータ概要： interface-id：ポート番号を表します。	Informational
7.	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(< interface-id >) パラメータ概要： interface-id：ポート番号を表します。	Warning
8.	イベントの概要：トラフィック監視が復旧しました。 ログメッセージ：Detect equipment recovery by traffic(< interface-id >) パラメータ概要： interface-id：ポート番号を表します。	Informational

15.21 PoE スケジューラ [XA-AML8TFPoE++/XA-AML16TFPoE++]

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 < interface-id > is changed to ON by PoE Scheduler. パラメータ概要： < interface-id >：ポート番号を表します。	Informational
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 < interface-id > is changed to OFF by PoE Scheduler. パラメータ概要： < interface-id >：ポート番号を表します。	Informational
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 < interface-id > is reset by PoE Scheduler. パラメータ概要： < interface-id >：ポート番号を表します。	Informational
4.	イベントの概要：SNTP 取得失敗してから、SNTP サーバへのアクセスが成功しました。 ログメッセージ：(PoE Scheduler) PoE status Auto Recover	Informational

15.22 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	Warning

15.23 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。	Informational
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。	Informational
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。	Informational
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。	Informational

15.24 Login/Logout

ID	ログの概要	重大度
1.	イベントの概要：コンソールから正常にログインしました。 ログメッセージ：Successful login through Console (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Informational
2.	イベントの概要：コンソールからログインに失敗しました。 ログメッセージ：Login failed through Console (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Warning
3.	イベントの概要：コンソールセッションからタイムアウトしました。 ログメッセージ：Console session timed out (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Informational
4.	イベントの概要：コンソールがログアウトしました。 ログメッセージ：Logout through Console (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Informational
5.	イベントの概要：telnet から正常にログインしました。 ログメッセージ：Successful login through Telnet (Username: <username>, IP: <ipaddr>) パラメータ概要： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Informational
6.	イベントの概要：telnet から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： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Warning
7.	イベントの概要：telnet セッションから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： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Informational
8.	イベントの概要：telnet が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： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Informational
9.	イベントの概要：SSH から正常にログインしました。 ログメッセージ：Successful login through SSH (Username: <username>, IP: <ipaddr>) パラメータ概要： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Informational

ID	ログの概要	重大度
10	イベントの概要：SSH からログインに失敗しました。 ログメッセージ：Login failed through SSH (Username: <username>, IP: <ipaddr>) パラメータ概要： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Critical
11	イベントの概要：SSH セッションからタイムアウトしました。 ログメッセージ：SSH session timed out (Username: <username>, IP: <ipaddr>) パラメータ概要： username：現在のログインユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Informational
12	イベントの概要：SSH がログアウトしました。 ログメッセージ：Logout through SSH(Username: <username>, IP: <ipaddr>) パラメータ概要： username：現在のログイン ユーザを表す。 ipaddr: クライアント IP アドレスを表す。	Informational
13	イベントの概要：PPS ターミナルから正常にログインしました。 ログメッセージ：Successful login through PPS Terminal(Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Informational
14	イベントの概要：PPS ターミナルからログインに失敗しました。 ログメッセージ：Login failed through PPS Terminal (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Warning
15	イベントの概要：PPS ターミナルセッションからタイムアウトしました。 ログメッセージ：PPS Terminal session timed out (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Informational
16	イベントの概要：PPS ターミナルがログアウトしました。 ログメッセージ：Logout through PPS Terminal (Username: <username>) パラメータ概要： username：現在のログインユーザを表す。	Informational

15.25 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。	Notice

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。	Notice

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。	Notice

15.26 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。	Critical
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。	Critical
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。	Critical
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復旧しました。 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。	Critical

15.27 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。	Informational
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。	Notice
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。	Notice

15.28 メンテナンスモード

ID	ログの概要	重大度
1.	イベントの概要：メンテナンスモードを開始しました。 ログメッセージ：maintenance mode start <HOURS> H End date and time: <DateTime> パラメータ概要： HOURS: メンテナンスモードの動作時間（時間単位） DateTime: メンテナンスモード終了日時を示します。 (表示形式 : 20xx MM/DD HH:mm.)	Informational
2.	イベントの概要：メンテナンスモードを終了しました。 ログメッセージ：maintenance mode end <factor> and <factor 2> パラメータ概要： factor：メンテナンスモードの終了トリガー • time expiration：時間経過 • time change：メンテナンスモードの動作時間変更 • force end：強制終了（終了ボタン押下や no コマンドの実行） • reboot：システム再起動 factor 2 ：メンテナンスモード動作中の設定変更と設定保存の有無 • configuration change：設定変更 • configuration save：設定保存 • configuration change/save：設定変更後、設定保存 • configuration save/change：設定保存後、設定変更	Informational

15.29 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。	Notice
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。	Notice
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	Informational
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	Informational
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。	Notice
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。	Notice
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_role：変化後のロール。	Informational
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。	Informational

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。	Informational
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。	Informational
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。	Informational
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。	Informational
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。	Informational
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。	Informational

15.30 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：ポート上の MAC アドレスがいっぱいです。 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： mac-address：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。	Warning
2.	イベントの概要：システム上の MAC アドレスがいっぱいです。 ログメッセージ：Limit on system entry number has been exceeded	Warning

15.31 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	Informational
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	Informational
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	Informational
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	Informational
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	Informational
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	Informational
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	Informational
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	Informational
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）	Informational
10.	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	Informational
11.	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	Informational
12.	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.	Informational
13.	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.	Informational
14.	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.	Warning
15.	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.	Error
16.	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	Error

ID	ログの概要	重大度
17.	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.	Error
18.	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.	Error
19.	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.	Informational
20.	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.	Informational
21.	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.	Informational
22.	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.	Warning

15.32 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。	Informational
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。	Informational
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。	Informational
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。	Warning
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。	Warning

15.33 リブートスケジュール

ID	ログの概要	重大度
1.	イベント概要：指定時間内にスイッチが再起動することについてのヒント ログメッセージ：5 分前になったときに “Reboot scheduled in 5 minutes” と表示されます。	Warning
2.	イベント概要：指定時間内にスイッチが再起動することについてのヒント ログメッセージ：1 分前になったときに “Reboot scheduled in 1 minutes” と表示されます。	Critical
3.	イベント概要：間隔指定のリブートスケジュールによる再起動後 ログメッセージ：System was restarted by schedule in an interval time.	Informational
4.	イベント概要：時刻指定のリブートスケジュールによる再起動後 ログメッセージ：System was restarted by schedule at specific time.	Informational

15.34 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	Notice
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	Warning
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	Informational
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	Warning
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	Notice
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	Informational
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：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。	Informational

15.35 sflow

ID	ログの概要	重大度
1.	イベントの概要：レシーバーの起動とタイマーカウントダウンを開始しました。 ログメッセージ：The sFlow Receiver <RECEIVER_INDEX> (collector: <COLLECTOR_IP_ADDRESS>) was activated, and its timer (<TIMEOUT_SECONDS> seconds) countdown just started パラメータ概要： RECEIVER_INDEX: レシーバー ID COLLECTOR_IP_ADDRESS: IPv4 または IPv6 アドレス TIMEOUT_SECONDS: タイマー値	Informational
2.	イベントの概要：レシーバーの起動と無期限タイマーを設定しました。 ログメッセージ：The sFlow Receiver <RECEIVER_INDEX> (collector: <COLLECTOR_IP_ADDRESS>) was activated, and its timer never expires パラメータ概要： RECEIVER_INDEX: レシーバー ID COLLECTOR_IP_ADDRESS: IPv4 または IPv6 アドレス	Informational
3.	イベントの概要：レシーバーのタイマー期限切れと非アクティブ化しました。 ログメッセージ：The sFlow Receiver <RECEIVER_INDEX> (collector: <COLLECTOR_IP_ADDRESS>) timer expired, and the Receiver was inactivated パラメータ概要： RECEIVER_INDEX: レシーバー ID COLLECTOR_IP_ADDRESS: IPv4 または IPv6 アドレス	Informational

15.36 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。	Informational

15.37 SSH

ID	ログの概要	重大度
1.	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	Informational
2.	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	Informational

15.38 スタッキング

ID	ログの概要	重大度
1.	イベントの概要：ホットインサートが発生しました。 ログメッセージ：Unit：<unitID>, MAC：<macaddr> Hot insertion パラメータ概要： unitID：ボックス ID。 Macaddr：MAC アドレス。	Informational
2.	イベントの概要：ホットリムーブが発生しました。 ログメッセージ：Unit：<unitID>, MAC：<macaddr> Hot removal パラメータ概要： unitID：ボックス ID。 Macaddr：MAC アドレス。	Informational
3.	イベントの概要：スタッキングトポロジが変化しました。 ログメッセージ：Stacking topology is <Stack_TP_TYPE>. Master（Unit <unitID>, MAC：<macaddr>） パラメータ概要： Stack_TP_TYPE：スタッキングトポロジタイプは以下のどちらかです。 1. Ring 2. Chain unitID：ボックス ID。 Macaddr：MAC アドレス。	Critical
4.	イベントの概要：バックアップマスターがマスターに変化しました。 ログメッセージ：Backup master changed to master. Master （Unit：<unitID>） パラメータ概要： unitID：ボックス ID。	Informational
5.	イベントの概要：スレーブがマスターに変化しました。 ログメッセージ：Slave changed to master. Master （Unit：<unitID>） パラメータ概要： unitID：ボックス ID。	Informational
6.	イベントの概要：ボックス ID が競合しています。 ログメッセージ：Hot insert failed, box ID conflict：Unit <unitID> conflict (MAC：<macaddr> and MAC：<macaddr>) パラメータ概要： unitID：ボックス ID。 macaddr：競合しているボックスの MAC アドレス。	Critical

15.39 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	Critical
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。	Informational
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。	Informational
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	Critical
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	Critical

15.40 SNTP

ID	ログの概要	重大度
1.	イベントの概要：SNTP の時刻同期が行われた IP アドレスを示します。 ログメッセージ：SNTP update from server (IP : <ipaddr>) パラメータ概要： ipaddr：SNTP サーバの IP アドレス	Informational
2.	イベントの概要：SNTP の時刻同期が失敗しました。 ログメッセージ：SNTP update failure	Warning

15.41 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： username：Telnet サーバへのログインに使用したユーザ名。 ipaddr：Telnet クライアントの IP アドレス。	Informational
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： username：Telnet サーバへのログインに使用したユーザ名。 ipaddr：Telnet クライアントの IP アドレス。	Warning
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： username：Telnet サーバへのログインに使用したユーザ名。 ipaddr：Telnet クライアントの IP アドレス。	Informational
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： username：Telnet サーバへのログインに使用したユーザ名。 ipaddr：Telnet クライアントの IP アドレス。	Informational

15.42 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：Uint <unitID> Sensor:<sensorID> detects abnormal temperature <temperature> パラメータ概要： unitID：ユニット ID sensorID：センサー ID temperature：センサーの現在の温度	Critical
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：Uint <unitID> Sensor:<sensorID> temperature back to normal パラメータ概要： unitID：ユニット ID sensorID：センサー ID	Critical
3.	イベントの概要：温度が許容範囲を超えました。 ログメッセージ：Uint <unitID> Sensor:<sensorID> temperature is over the acceptable limit パラメータ概要： unitID：ユニット ID sensorID：センサー ID	Critical
4.	イベントの概要：温度が許容範囲に回復しました。 ログメッセージ：Uint <unitID> Sensor:<sensorID> temperature recovers to the acceptable limit パラメータ概要： unitID：ユニット ID sensorID：センサー ID	Critical

15.43 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。	Warning
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。	Informational
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 shutdown 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。	Warning

15.44 UDLD

ID	ログの概要	重大度
1.	イベントの概要：ポート上で新規の UDLD ネイバーを検出しました。 ログメッセージ：(efm-oam detect-udl) Detected New Neighbor : XX-XX-XX-XX-XX-XX パラメータ概要： XX-XX-XX-XX-XX-XX：隣接装置の MAC アドレス	Informational
2.	イベントの概要：ポート上で単方向通信状態を検出しました。 ログメッセージ：(efm-oam detect-udl) Detected Unidirectional Link on TenGigabitEthernet1/0/XX パラメータ概要： XX: ポート番号	Warning
3.	イベントの概要：UDLD によるリンク状態の変更を検出しました。 ログメッセージ：(efm-oam detect-udl) Detected Link status was changed to <link Status> on TenGigabitEthernet1/0/XX パラメータ概要： <link Status>:UDLD 制御による、リンクの状態 ・Shutdown. XX: ポート番号	Informational

15.45 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。	Informational
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。	Informational
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：VLAN ID。	Informational

15.46 VRRP

ID	ログの概要	重大度
1.	イベントの概要：特定の仮想ルータの状態が Master になりました。 ログメッセージ：VR <vr-id> at interface <intf-name> switch to Master role パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Informational
2.	イベントの概要：特定の仮想ルータの状態が Backup になりました。 ログメッセージ：VR <vr-id> at interface <intf-name> switch to Backup state パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Informational
3.	イベントの概要：特定の仮想ルータの状態が Init になりました。 ログメッセージ：VR <vr-id> at interface <intf-name> switch to Init state パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Informational
4.	イベントの概要：受信した 1 つの VRRP アドバタイズメッセージの認証タイプが不一致です。 ログメッセージ：Authentication type mismatch on VR <vr-id> at interface <intf-name> パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Warning
5.	イベントの概要：受信した 1 つの VRRP アドバタイズメッセージの認証チェックに失敗しました。 ログメッセージ：Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。 auth-type：VRRP インターフェース認証タイプ。	Warning
6.	イベントの概要：受信した 1 つの VRRP アドバタイズメッセージにチェックサムエラーがあります。 ログメッセージ：Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Warning
7.	イベントの概要：受信した 1 つの VRRP アドバタイズメッセージの仮想ルータ ID が不一致です。 ログメッセージ：Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Warning

ID	ログの概要	重大度
8.	イベントの概要：受信した 1 つの VRRP アドバタイズメッセージのアドバタイズ間隔が不一致です。 ログメッセージ：Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> パラメータ概要： vr-id：VRRP 仮想ルータ ID。 intf-name：仮想ルータが存在するインターフェース名。	Warning
9.	イベントの概要：仮想 MAC アドレスがスイッチ L2 テーブルに追加されました。 ログメッセージ：Added a virtual MAC <vrrp-mac-addr> into L2 table パラメータ概要： vrrp-mac-addr：VRRP 仮想 MAC アドレス。	Notice
10.	イベントの概要：スイッチ L2 テーブルから仮想 MAC アドレスが削除されました。 ログメッセージ：Deleted a virtual MAC <vrrp-mac-addr> from L2 table パラメータ概要： vrrp-mac-addr：VRRP 仮想 MAC アドレス。	Notice
11.	イベントの概要：仮想 MAC アドレスがスイッチ L3 テーブルに追加されました。 ログメッセージ：Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。	Notice
12.	イベントの概要：スイッチ L3 テーブルから仮想 MAC アドレスが削除されました。 ログメッセージ：Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table. パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。	Notice
13.	イベントの概要：スイッチチップ L2 テーブルへの仮想 MAC の追加に失敗しました。 ログメッセージ：Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> パラメータ概要： vrrp-mac-addr：VRRP 仮想 MAC アドレス。 vrrp-errcode：VRRP プロトコル動作のエラーコード。	Error
14.	イベントの概要：スイッチチップ L2 テーブルからの仮想 MAC の削除に失敗しました。 ログメッセージ：Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> パラメータ概要： vrrp-mac-addr：VRRP 仮想 MAC アドレス。 vrrp-errcode：VRRP プロトコル動作のエラーコード。	Error
15.	イベントの概要：スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。L3 テーブルがフルです。 ログメッセージ：Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。	Error

ID	ログの概要	重大度
16.	イベントの概要：スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。 MAC を学習したポートが無効です。 ログメッセージ：Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。 mac-port：VRRP 仮想 MAC のポート番号。	Error
17.	イベントの概要：スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。 MAC を学習したインタフェースが無効です。 ログメッセージ：Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。 mac-intf：VRRP 仮想 MAC アドレスが存在するインタフェース ID。	Error
18.	イベントの概要：スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。 MAC を学習したボックスが無効です。 ログメッセージ：Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。 mac-box：VRRP 仮想 MAC のスタッキングボックスナンバー。	Error
19.	イベントの概要：スイッチチップ L3 テーブルへの仮想 MAC の追加に失敗しました。 ログメッセージ：Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。 vrrp-errcode：VRRP プロトコル動作のエラーコード。	Error
20	イベントの概要：スイッチチップ L3 テーブルからの仮想 MAC の削除に失敗しました。 ログメッセージ：Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> パラメータ概要： vrrp-ip-addr：VRRP 仮想 IP アドレス。 vrrp-mac-addr：VRRP 仮想 MAC アドレス。 vrrp-errcode：VRRP プロトコル動作のエラーコード。	Error

15.47 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。	Notice
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。	Informational
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。	Notice

15.48 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。	Informational
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。	Warning
3.	イベントの概要：SSL を使った 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（SSL）（Username：<username>, IP：<ipaddr>） パラメータ概要： username：ユーザ名。 ipaddr：SSL を使った Web からスイッチにアクセスしたユーザの IP アドレス。	Informational
4.	イベント概要：SSL を使った 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：SSL を使った Web からスイッチにアクセスしたユーザの IP アドレス。	Warning
5.	イベントの概要：Web からのセッションタイムアウト。 ログメッセージ：Web session timed out（Username：<username>, IP：<ipaddr>） 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。	Informational
6.	イベントの概要：SSL を使った Web からのセッションタイムアウト ログメッセージ：Web (SSL) session timed out (Username: <username>, IP: <ipaddr>) パラメータ概要： username：ユーザ名。 ipaddr：SSL を使った Web からスイッチにアクセスしたユーザの IP アドレス。	Informational
7.	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>) 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。	Informational

ID	ログの概要	重大度
8.	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>) 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。	Informational
9.	イベントの概要：WEB がログアウトしました。 ログメッセージ：Logout 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。	Informational
10.	イベントの概要：SSL を使った WEB がログアウトしました。 ログメッセージ：Logout through Web(SSL) (Username: <username>, IP: <ipaddr>) パラメータ概要： username：ユーザ名。 ipaddr: SSL を使った Web からスイッチにアクセスしたユーザの IP アドレス。	Informational

16 付録 - システムトラップ一覧

16.1 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

16.2 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、または通常状態に復旧したとき、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： (1) mnoDdmPort ポート番号 (2) mnoDdmThresholdType DDM 閾値タイプ temperature/voltage/bias/txpower/rxpower (3) 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 DDM 閾値を超えているか、または通常状態に復旧しているか	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、または通常状態に復旧したとき、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： (1) mnoDdmPort ポート番号 (2) mnoDdmThresholdType DDM 閾値タイプ temperature/voltage/bias/txpower/rxpower (3) 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 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

16.3 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

16.4 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

16.5　ファン

ID	トラップ名	トラップの概要	OID
1.	mnoFanNotificationAlarmDetected unit <unitID>, FANID(FANID)	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。	1.3.6.1.4.1.396.5.5.1.10.0.1
2.	mnoFanNotificationAlarmRecovered unit <unitID>, FANID(FANID)	ファンが復旧したときに、この通知が送信されます。	1.3.6.1.4.1.396.5.5.1.10.0.2
3.	mnoFanNotificationModeChanged Unit <unitID>, Fan mode <Fan mode>	ファンモードが変更された時に、この通知が送信されます。	1.3.6.1.4.1.396.5.5.1.10.0.3

16.6　ログイン失敗

ID	トラップ名	トラップの概要	OID
1.	authenticationFailure	ログイン失敗トラップ	1.3.6.1.6.3.1.1.5.5

16.7 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

16.8 LACP

ID	トラップ名	トラップの概要	OID
1.	linkup	通信リンクの状態 "ifOperStatus" オブジェクトが "down" 状態から別の状態（"notPresent" 状態を除く）に遷移したことを検知したことを示します。 具体的な状態は "ifOperStatus" の値によって示されます。 バインディングオブジェクト： (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2.	linkdown	通信リンクの状態 "ifOperStatus" オブジェクトが "notPresent" 以外の状態から "down" 状態に遷移しようとしていることを検知したことを示します。 遷移前の具体的な状態は "ifOperStatus" の値によって示されます。 バインディングオブジェクト： (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

16.9 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回復したことを示します。	1.3.6.1.4.1.396.5.5.2.2

16.10 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： (1) mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 (2) mnoMacBasedAuthInfoPortIndex ポートインタフェース。 (3) mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.1
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： (1) mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 (2) mnoMacBasedAuthInfoPortIndex ポートインタフェース。 (3) mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.2
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： (1) mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 (2) mnoMacBasedAuthInfoPortIndex 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

16.11 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： (1) 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

16.12 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。	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。	1.3.6.1.2.1.17.0.2

16.13 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： (1) mnoPortSecPortIndex ポートインタフェース。 (2) mnoL2PortSecurityViolationMac ホスト MAC アドレス。	1.3.6.1.4.1.396.5.5.3.3.0.1

16.14 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) ifAdminStatus (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) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

16.15 PoE [XA-AML8TFPoE++/XA-AML16TFPoE++]

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。 バインディングオブジェクト： (1) pethPsePortOnOffNotification (2) pethPsePortDetectionStatus	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。 バインディングオブジェクト： (1) pethMainPseConsumptionPower	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。 バインディングオブジェクト： (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
4.	mnoPethNotificationAlarmDetected Unit <unitID>	PoE 測定のアラームが発生したことを示します。	1.3.6.1.4.1.396.5.5.1.12.0.1
5.	mnoPethNotificationAlarmRecovered Unit <unitID>	PoE 測定の復旧したことを示します。	1.3.6.1.4.1.396.5.5.1.12.0.2

16.16 PoE オートリブート [XA-AML8TFPoE++/XA-AML16TFPoE++]

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

16.17 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

16.18 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

16.19 スタッキング

ID	トラップ名	トラップの概要	OID
1.	mnoUnitInsert	ユニットホットインサート通知。 バインディングオブジェクト： mnoUnitMgmtId ホットインサートした装置のボックス ID mnoUnitMgmtMacAddr ホットインサート装置の MAC アドレス	1.3.6.1.4.1.396.5.5.1.3.0.1
2.	mnoUnitRemove	ユニットホットリムーブ通知。 バインディングオブジェクト： mnoUnitMgmtId ホットリムーブした装置のボックス ID mnoUnitMgmtMacAddr ホットリムーブした装置の MAC アドレス	1.3.6.1.4.1.396.5.5.1.3.0.2
3.	mnoUnitFailure	ユニット故障通知。 バインディングオブジェクト： mnoUnitMgmtId 故障した装置のボックス ID	1.3.6.1.4.1.396.5.5.1.3.0.3
4.	mnoUnitTPChange	スタッキングトポロジ変化通知 バインディングオブジェクト： mnoStackTopologyType 変化後の現在のスタッキングトポロジ： チェーン（1） リング（2） mnoUnitMgmtId マスターのボックス ID mnoUnitMgmtMacAddr マスターの MAC アドレス	1.3.6.1.4.1.396.5.5.1.3.0.4
5.	mnoUnitRoleChange	スタッキングユニットロール変化通知 バインディングオブジェクト： mnoStackRoleChangeType スタッキングロールのタイプの変化： バックアップからマスターへ（1） スレーブからマスターへ（2） mnoUnitMgmtId マスターのボックス ID	1.3.6.1.4.1.396.5.5.1.3.0.5

16.20 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

16.21 温度

ID	トラップ名	トラップの概要	OID
1.	mnoTemperatureNotificationAbnormalDetected Unit <unitID>, SensorID <sensorID>	この通知は、温度センサーがアラーム状態に入ったときに送信されます。	1.3.6.1.4.1.396.5.5.1.11.0.1
2.	mnoTemperatureNotificationAbnormalRecovered <unitID>, SensorID <sensorID>	この通知は、温度センサーが回復したときに送信されます。	1.3.6.1.4.1.396.5.5.1.11.0.2
3.	mnoTemperatureRisingAlarm	この通知は、温度が許容範囲を超えた場合に送信されます。	1.3.6.1.4.1.396.5.5.1.2.1
4.	mnoTemperatureFallingAlarm	この通知は、温度が許容範囲に回復した場合に送信されます。	1.3.6.1.4.1.396.5.5.1.2.2

16.22 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ムが検出され、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： (1) 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： (1) 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： (1) mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.3

16.23 VRRP

ID	トラップ名	トラップの概要	OID
1.	vrrpTrapNewMaster	newMaster トラップは、送信エージェントがマスター状態に移行したことを示します。 バインディングオブジェクト： （1）vrrpOperMasterIpAddr	1.3.6.1.2.1.68.0.1
2.	vrrpTrapAuthFailure	vrrpAuthFailure トラップは、このルータの認証キーまたは認証タイプと競合する認証キーまたは認証タイプを持つルータからパケットを受信したことを示します。このトラップの実装はオプションです。 バインディングオブジェクト： （1）vrrpTrapPacketSrc （2）vrrpTrapAuthErrorType	1.3.6.1.2.1.68.0.2

16.24 UDLD

ID	トラップ名	トラップの概要	OID
1.	mnoEfmOamUdlDetectedBidirectionalLink	双方向通信を検出したことを示します。	1.3.6.1.4.1.396.5.5.3.8.0.1
2.	mnoEfmOamUdlDetectedUnidirectionalLink	片方向通信を検出したことを示します。	1.3.6.1.4.1.396.5.5.3.8.0.2

16.25 sFlow

ID	トラップ名	トラップの概要	OID
1.	mnoSFlowReceiverActivated	sFlow レシーバーが起動し、タイマーのカウントダウンが始まったことを示します。	1.3.6.1.4.1.396.5.5.3.9.0.1
2.	mnoSFlowReceiverExpired	sFlow レシーバーのタイマーが切れ、レシーバが非アクティブになったことを示します。	1.3.6.1.4.1.396.5.5.3.9.0.2

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/

P0126-0