Panasonic

L2 スイッチングハブ

WEB リファレンス

品番 ZLP28080/ZLP28080H/
ZLP28160/ZLP28160H/
ZLP28240/ZLP28240H/
ZLP28480

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
GA-EM8T	ZLP28080	1.0.0.01 以上
GA-EMi8T	ZLP28080H	1.0.0.01 以上
GA-EM16T	ZLP28160	1.0.0.01 以上
GA-EMi16T	ZLP28160H	1.0.0.01 以上
GA-EM24T	ZLP28240	1.0.0.01 以上
GA-EMi24T	ZLP28240H	1.0.0.01 以上
GA-EM48T	ZLP28480	1.0.0.01 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。

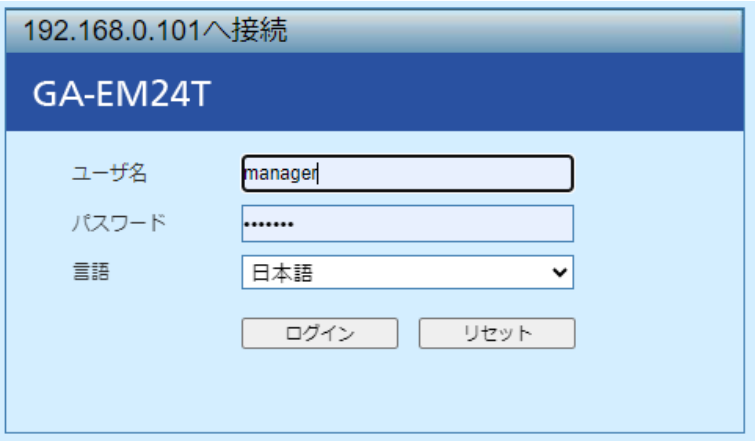

図 1-1　WEB ブラウザ　ログイン画面

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ユーザー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)
(ユーザー名 :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)

```
GA-EMxxT>enable
GA-EMxxT#configure terminal
GA-EMxxT(config)#interface vlan 1
GA-EMxxT(config-if)#ip address 192.168.0.101 255.255.255.0
GA-EMxxT(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

```
GA-EMxxT(config)#ip http server
```

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

CLI コマンド実行例 :

```
                              GA-EMxxT
                        Command Line Interface

                     Product Number: ZLP28xx0
                  Firmware Version: V1.0.0.00
                       MAC Address: xx:xx:xx:xx:xx:xx
                     Serial Number: xxxxxxxxxxx

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

GA-EMxxT>enable
GA-EMxxT#config
GA-EMxxT(config)#interface vlan 1
GA-EMxxT(config-if)#ip address 192.168.0.101 255.255.255.0
GA-EMxxT(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.0.101
GA-EMxxT(config-if)#exit
GA-EMxxT(config)#ip http server
GA-EMxxT(config)#
```

1.2 WEB 簡単設定ウィザード

WEB 設定を有効する場合、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 ユーザー名とパスワードを入力します。
(ユーザー名 :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 :

```
                                GA-EMxxT
                            Command Line Interface

                         Product Number: ZLP28xx0
                        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      :192.168.1.101
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。

[GA-EMxxT] をクリックして、以下のウィンドウを表示します。

図 2-1 デバイス情報

2.2 システム情報設定

このウィンドウを用いて、システム情報の設定を行い、設定値を表示します。

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

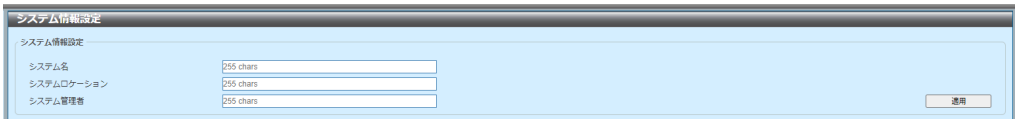

図 2-2 システム情報設定

設定パラメータ （[システム情報設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

2.3 ポートコンフィグレーション

2.3.1 ポート設定

このウィンドウを用いて、スイッチのポート設定を行い、設定値を表示します。

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

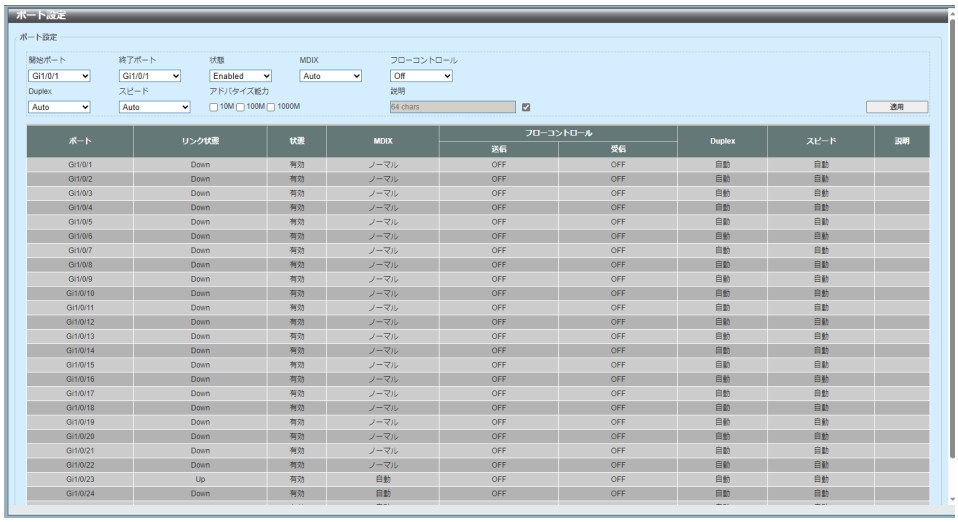

図 2-3 **ポート設定**

設定パラメータ （[ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	ポートの状態（**Enabled**/**Disabled**）を選択します。 (デフォルト : Enabled)
MDIX	MDIX（Medium Dependent Interface Crossover）のオプションを選択します。(デフォルト : 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。

パラメータ	概要
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。(デフォルト : Off)
Duplex	使用する二重モード（**Auto**/**Half**/**Full**）を選択します。 (デフォルト : Auto)
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。(デフォルト : 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** - 銅ポートの場合、オートネゴシエーションが開始して、スピードおよびフローコントロールをそのリンクパートナとネゴシエートします。ファイバポートの場合、オートネゴシエーションが開始して、クロックおよびフローコントロールをそのリンクパートナとネゴシエートします。 • **10M** - 10Mbps に強制します。（10Mbps の銅線接続にのみ利用できます） • **100M** - 100Mbps に強制します。（100Mbps の銅線接続にのみ利用できます） • **1000M** - 1000Mbps に強制します。 • **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。
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 (10M, 100M, 1000M) 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。（最大 : 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。

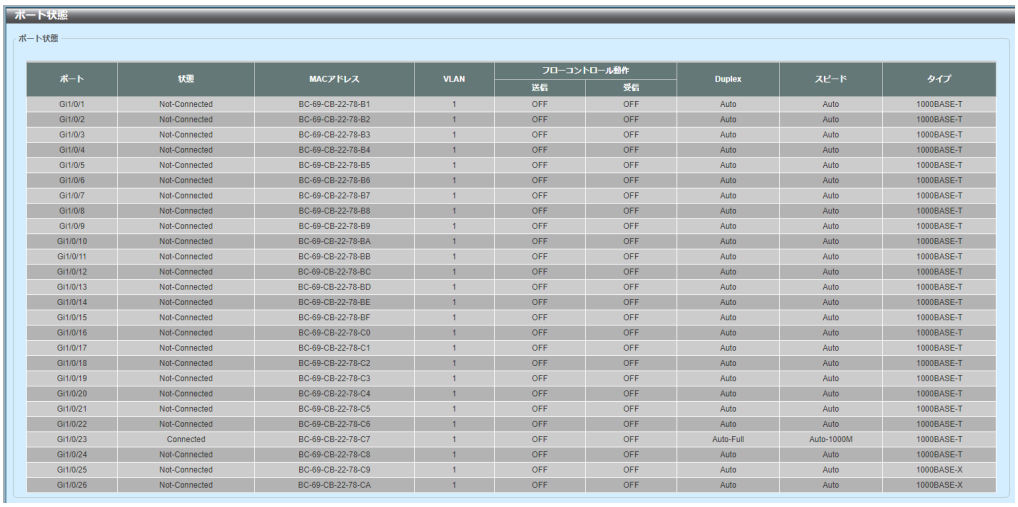

図 2-4 ポート状態

2.3.3 ポート GBIC

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

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

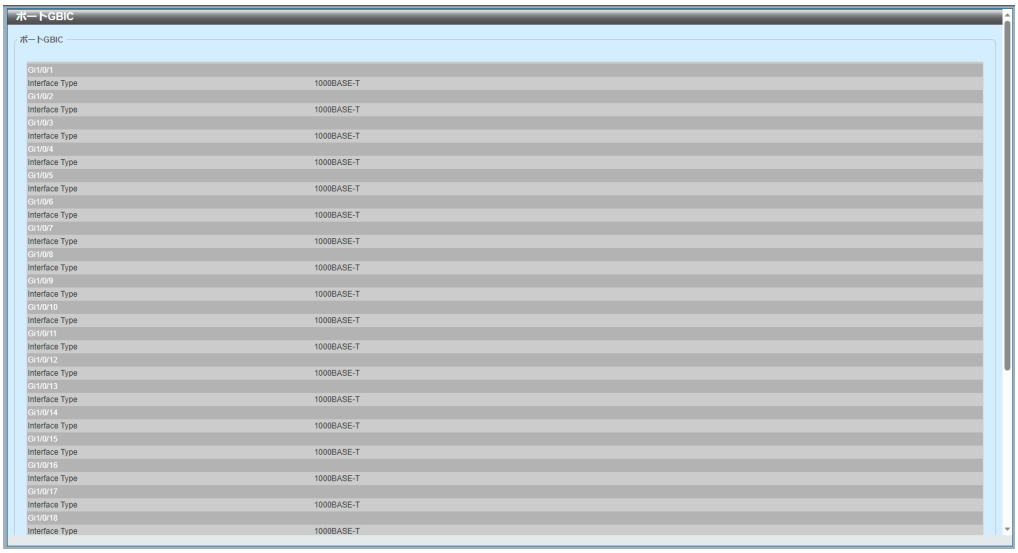

図 2-5 ポート GBIC

2.3.4 ポートオートネゴシエーション

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

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

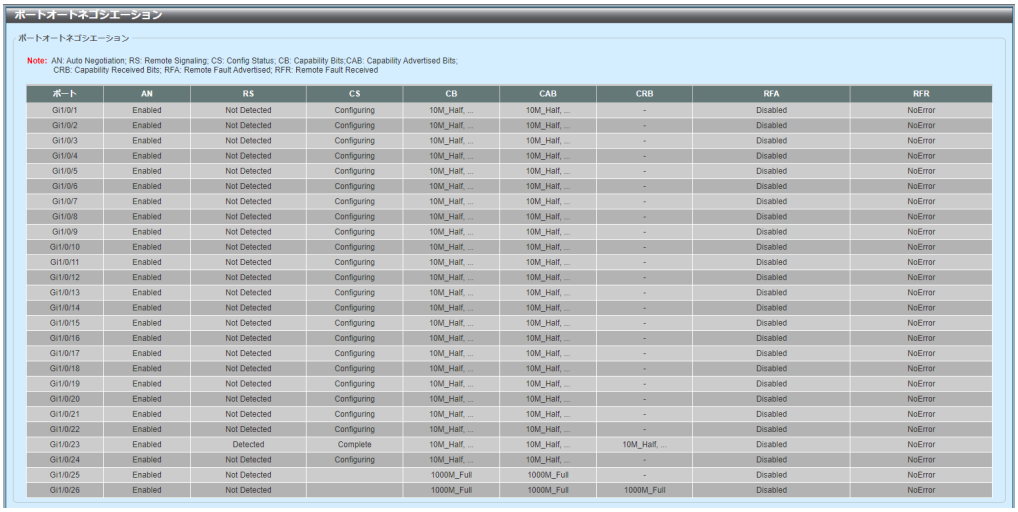

図 2-6 ポートオートネゴシエーション

2.3.5 Error Disable 設定

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

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

図 2-7 Error Disable 設定

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

パラメータ	概要
エラーディセーブル原因	設定対象のエラー閉塞（エラーディセーブル Error Disabled）原因を、**All** / **Port Security** / **Storm Control** / **Dynamic ARP Inspection** / **DHCP Snooping** 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 - **Dynamic ARP Inspection**：ARP レート制限 - **DHCP Snooping**：DHCP スヌーピング
状態	選択されたエラーディセーブル原因に対する自動復旧を有効化 / 無効化します。（**Disabled**：無効化、**Enabled**：有効化、デフォルト：**Disabled**）
間隔	選択されたエラーディセーブル原因によって生じたエラー閉塞状態からポートを自動復旧する迄の時間（秒）を入力します。（設定範囲：5 ～ 86400、デフォルト：300）
（設定更新）	上記各パラメータ値の設定後、[適用] ボタンをクリックして、Error Disable リカバリ設定を更新します。
（Error Disable リカバリ設定一覧）	Error Disable リカバリ設定値をエラーディセーブル原因毎の一覧表形式で表示します。
エラーディセーブル原因	**All** / **Port Security** / **Storm Control** / **Dynamic ARP Inspection** / **DHCP Snooping** ：エラー閉塞（Error Disabled）の原因を示します。
状態	**Enabled**（有効）/**Disabled**（無効）：エラーディセーブル原因に対する自動復旧の有効化 / 無効化状態を示します。

パラメータ	概要
間隔	時間：原因によって生じるエラー閉塞状態からポートを復旧する時間（秒）を示します（範囲：5 ～ 86400）。
（自動復旧までの残時間一覧）	エラー閉塞中のインターフェースの自動復旧までの残時間をインターフェース毎の一覧形式で表示します。
インターフェース	インターフェース ID：エラー閉塞中のインターフェース（イーサネット物理ポート）。
エラーディセーブル原因	**All** / **Port Security** / **Storm Control** /**Dynamic ARP Inspection** / **DHCP Snooping** ：エラー閉塞（Error Disabled）の原因を示します。
残り時間（秒）	残時間：原因によって生じるエラー閉塞状態からポートを自動復旧するまでの残時間（秒）を示します。（範囲：0 ～ 86400）。

[**適用**] ボタン - 設定内容を反映します。

2.3.6 ジャンボフレーム

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

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

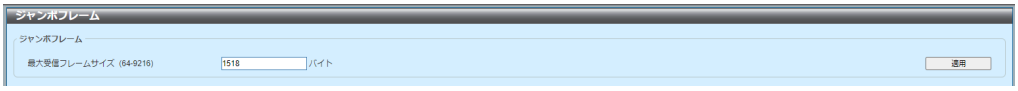

図 2-8 ジャンボフレーム

設定パラメータ （[ジャンボフレーム] セクション）

パラメータ	概要
最大受信フレームサイズ	最大受信フレームサイズ値（バイト）を入力します。 （デフォルト：1518、設定範囲：64-9216）

[**適用**] ボタン - 設定内容を反映します。

2.3.7 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 2-9 システムログ Discriminator 設定

設定パラメータ （[識別ログ設定] セクション）

パラメータ	概要
識別名	ディスクリミネータプロファイルの名前を入力します。 （最大：15 文字）
アクション	選択した動作に関連付けるファシリティ動作オプションおよびファシリティのタイプ（**Drops**/**Includes**）を選択します。各システムログについて、本リファレンスの 14 章を参照ください。
重大度	ログ記録する情報タイプの動作オプション（**Drops**/**Includes**）と重大度（**0**（緊急）/**1**（アラート）/**2**（クリティカル）/**3**（エラー）]/**4**（警告）/**5**（通知）/**6**（情報）/**7**（デバッギング））を選択します。

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

2.4 システムログ

2.4.1 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。

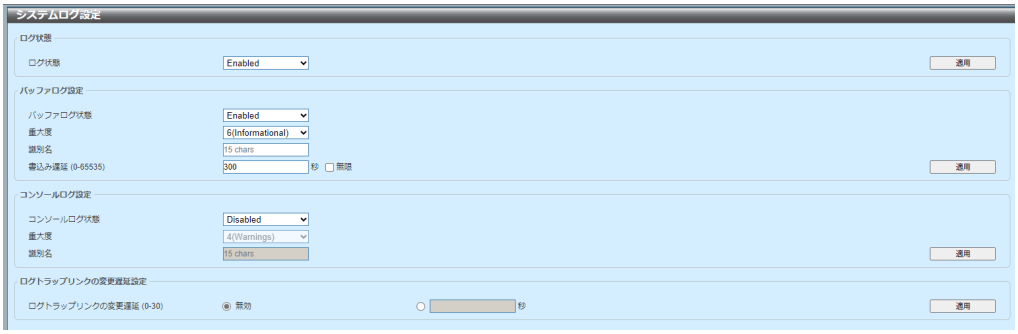

図 2-10 システムログ設定

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。 (デフォルト : Enabled)

[**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**）を選択します。 (デフォルト : Enabled)
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。 (デフォルト : 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。（最大：15 文字）
書込み遅延	ログの書き込み遅延値（秒）を入力します。 [**無限**] オプションを選択した場合、書き込み遅延機能は無効になります。（デフォルト：300、設定範囲：0-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[コンソールログ設定] セクション）

パラメータ	概要
コンソールログ状態	コンソールログ状態（**Enabled**/**Disabled**）を選択します。 (デフォルト : Disabled)
重大度	ログ記録する情報のタイプの（**0**（**Emergencies**/**1**（**Alerts**）/**2**（**Critical**）/**3**（**Errors**）]/**4**（**Warnings**）/**5**（**Notifications**）/**6**（**Informational**）/**7**（**Debugging**））を選択します。 (デフォルト : 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、コンソールログメッセージがフィルタリングされます。（最大：15 文字）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ログトラップリンクの変更遅延設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

2.4.2 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 2-11 システムログサーバ設定

設定パラメータ （[ログサーバ設定] セクション）

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

<table>
<tr><th>パラメータ</th><th colspan="3">概要</th></tr>
<tr><td>ファシリティ</td><td colspan="3">ログ記録するファシリティ番号を選択します。ファシリティ番号はそれぞれ特定のファシリティに関連付けられています。</td></tr>
<tr><td></td><td>ファシリティ番号</td><td>ファシリティ名</td><td>ファシリティの概要説明</td></tr>
<tr><td></td><td>1</td><td>user</td><td>ユーザレベルメッセージ</td></tr>
<tr><td></td><td>2</td><td>mail</td><td>メールシステム</td></tr>
<tr><td></td><td>3</td><td>daemon</td><td>システムデーモン</td></tr>
<tr><td></td><td>4</td><td>auth1</td><td>セキュリティ / 認証メッセージ</td></tr>
<tr><td></td><td>5</td><td>syslog</td><td>SYSLOG によって内部的に生成されるメッセージ</td></tr>
<tr><td></td><td>6</td><td>lpr</td><td>ラインプリンタサブシステム</td></tr>
<tr><td></td><td>7</td><td>news</td><td>ネットワークニュースサブシステム</td></tr>
<tr><td></td><td>8</td><td>uucp</td><td>UUCP サブシステム</td></tr>
<tr><td></td><td>9</td><td>clock1</td><td>クロックデーモン</td></tr>
<tr><td></td><td>10</td><td>auth2</td><td>セキュリティ / 認証メッセージ</td></tr>
<tr><td></td><td>11</td><td>ftp</td><td>FTP デーモン</td></tr>
<tr><td></td><td>12</td><td>ntp</td><td>NTP サブシステム</td></tr>
<tr><td></td><td>13</td><td>logaudit</td><td>ログ監査</td></tr>
<tr><td></td><td>14</td><td>logalert</td><td>ログアラート</td></tr>
<tr><td></td><td>15</td><td>clock2</td><td>クロックデーモン</td></tr>
<tr><td></td><td>16</td><td>local0</td><td>ローカル使用 0（local0）</td></tr>
<tr><td></td><td>17</td><td>local1</td><td>ローカル使用 1（local1）</td></tr>
<tr><td></td><td>18</td><td>local2</td><td>ローカル使用 2（local2）</td></tr>
<tr><td></td><td>19</td><td>local3</td><td>ローカル使用 3（local3）</td></tr>
<tr><td></td><td>20</td><td>local4</td><td>ローカル使用 4（local4）</td></tr>
<tr><td></td><td>21</td><td>local5</td><td>ローカル使用 5（local5）</td></tr>
<tr><td></td><td>22</td><td>local6</td><td>ローカル使用 6（local6）</td></tr>
<tr><td></td><td>23</td><td>local7</td><td>ローカル使用 7（local7）</td></tr>
<tr><td>識別名</td><td colspan="3">ログサーバに送信されるメッセージのフィルタリングに使用する、ディスクリミネータの名前を入力します。
(最大：15 文字)</td></tr>
<tr><td>ヘッダー情報</td><td colspan="3">ヘッダー情報を選択します。選択できるオプションは、IP、System Name、および None。</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。

2.4.3 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。

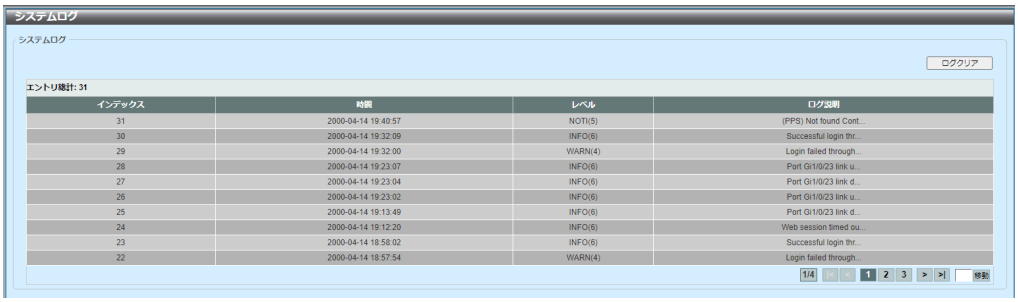

図 2-12 システムログ

[ログクリア] ボタン - ログエントリをクリアします。

2.4.4 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 2-13 システムアタックログ

[アタックログクリア] ボタン - アタックログエントリをクリアします。

2.4.5 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。

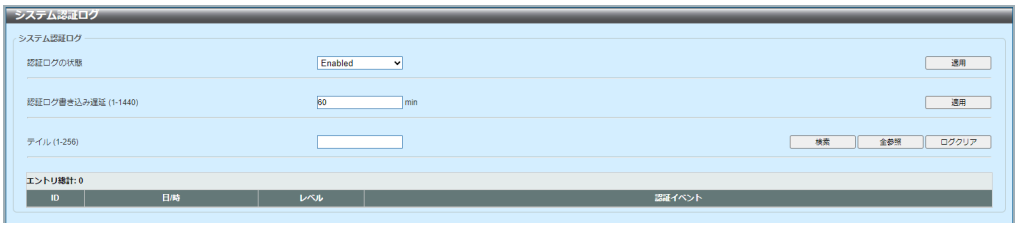

図 2-14 システム認証ログ

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。 (デフォルト : 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。 （設定範囲：1-1440, デフォルト : 60min）
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。

2.5 時間と SNTP（Simple Network Time Protocol）

2.5.1 時刻設定

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

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

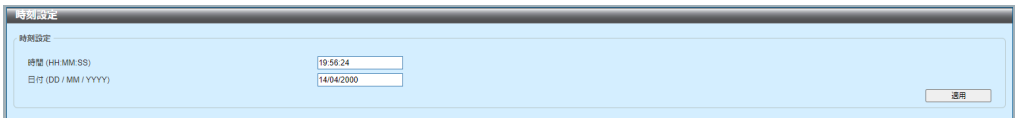

図 2-15 時刻設定

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。

2.5.2 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。

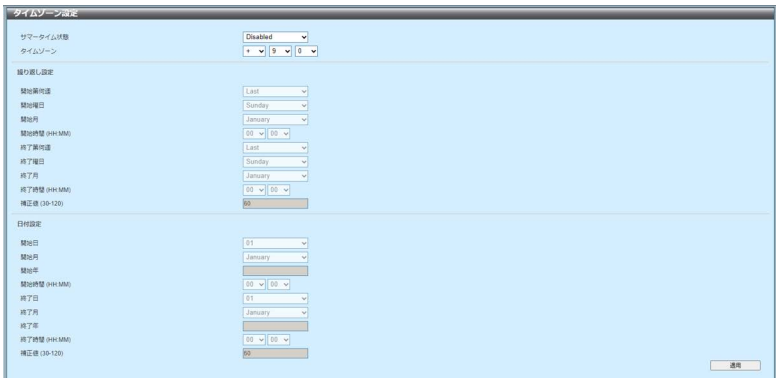

図 2-16 タイムゾーン設定

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。(デフォルト : 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。(デフォルト : +, 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。

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

設定パラメータ （[日付設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

2.5.3 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 2-17 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。 (デフォルト : Disabled)
ポール間隔	同期間隔（秒）を入力します。 （デフォルト：720、設定範囲：30-99999）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[SNTP サーバ設定] セクション）

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

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

3 マネジメント

3.1 コマンドログ収集コマンド

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

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

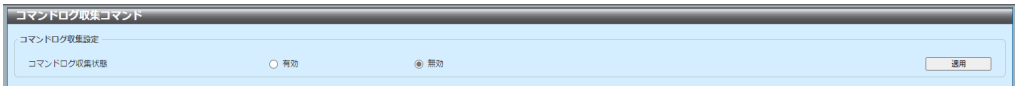

図 3-1 コマンドログ収集コマンド

設定パラメータ （[コマンドログ収集設定] セクション）

パラメータ	概要
コマンドログ収集状態	コマンドログ収集の状態（**有効** / **無効**）を選択します。 (デフォルト : 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。（最大 : 32 文字）
特権レベル	アカウントの特権レベルを入力します。（設定範囲 : 1-15）
パスワードタイプ	ユーザアカウントのパスワードタイプ（**None**/**Plain Text**/**Encrypted-SHA1**）を選択します。
パスワード	([パスワードタイプ] パラメータで [Plain Text]、または [Encrypted-SHA1] 選択時に設定可) ユーザアカウントのパスワードを入力します。 (最大文字数 : 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。

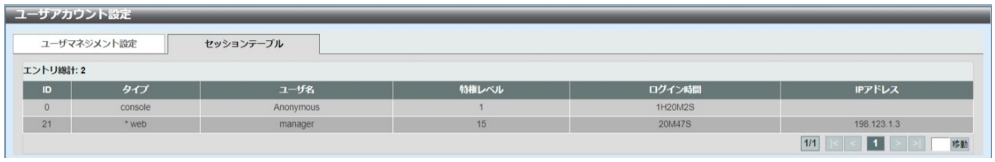

図 3-3 ユーザアカウント設定（セッションテーブル）

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。(デフォルト : 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。

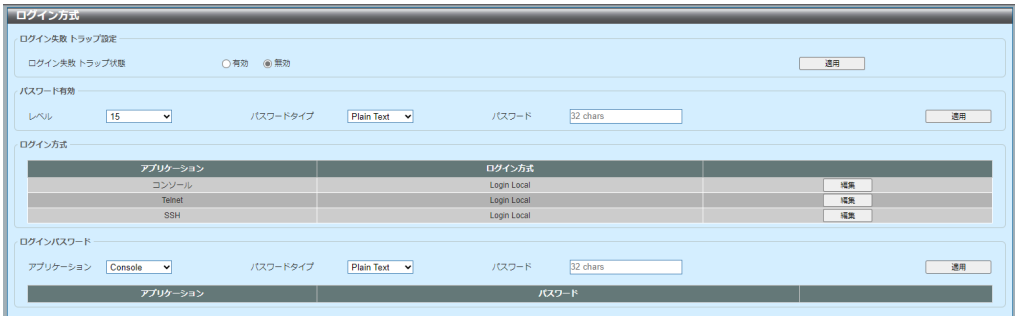

図 3-5 ログイン方式

次のパラメータは、[ログイン失敗トラップの設定] セクションで設定できます。

パラメータ	概要
ログイン失敗トラップ設定	ここでログイン失敗トラップの状態を有効または無効にする場合に選択します。 デフォルト状態の場合、無効になります。

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

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

設定パラメータ （[編集]>[ログイン方式] セクション）

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

設定パラメータ （[ログインパスワード] セクション）

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

[**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。

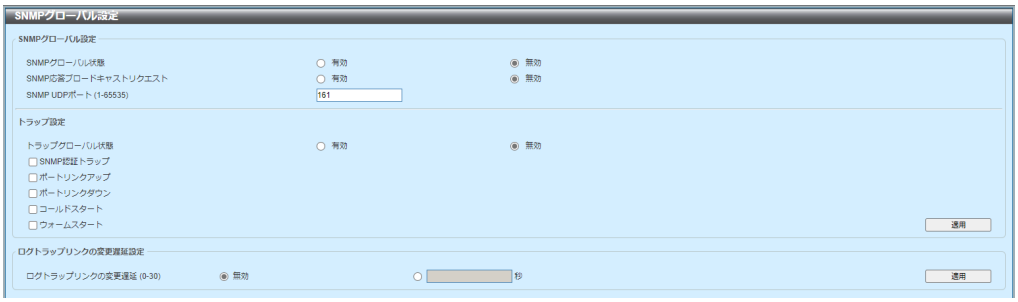

図 3-6 SNMP グローバル設定

設定パラメータ （[SNMP グローバル設定] セクション）

パラメータ	概要
SNMP グローバル状態	SNMP の状態（**有効** / **無効**）を選択します。デフォルト値は無効です。(デフォルト : 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。(デフォルト : 無効)
SNMP UDP ポート	SNMP UDP ポート番号を入力します。(設定範囲 : 1-65535, デフォルトポート番号 : 161)

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。(デフォルト : 無効)

パラメータ	概要
SNMP 認証トラップ	このオプションを選択した場合、SNMP 認証失敗通知の送信を制御します。正しく認証されていない SNMP メッセージを装置が受信すると、authenticationFailuretrap トラップが生成されます。認証方式は、使用されている SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、パケットに不正なコミュニティ文字列があると認証は失敗します。SNMPv3 の場合、パケットに不正な SHA/MD5 認証キーがあると認証は失敗します。
ポートリンクアップ	このオプションを選択した場合、ポートリンクアップ通知の送信を制御します。通信リンクの 1 つがアップ状態にあると装置が認識すると、linkUp トラップが生成されます。
ポートリンクダウン	このオプションを選択した場合、ポートリンクダウン通知の送信を制御します。通信リンクの 1 つがダウン状態にあると装置が認識すると、linkDown トラップが生成されます。
コールドスタート	このオプションを選択した場合、SNMP コールドスタート通知の送信を制御します。
ウォームスタート	このオプションを選択した場合、SNMP ウォームスタート通知の送信を制御します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ログトラップリンクの変更遅延設定] セクション）

パラメータ	概要
ログトラップリンクの変更遅延	物理ポートのリンク状態に関連するシステムログ及び SNMP トラップの発行遅延を有効にします。範囲は、0 ～ 30 秒 (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。 (デフォルト：無効)

[**適用**] ボタン - 設定内容を反映します。

3.5.2 SNMP リンクチェンジトラップ設定

このウィンドウを用いて、SNMP 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 3-7 SNMP リンクチェンジトラップ設定

設定パラメータ （[SNMP リンクチェンジトラップ設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

3.5.3 SNMP ビューテーブル設定

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

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

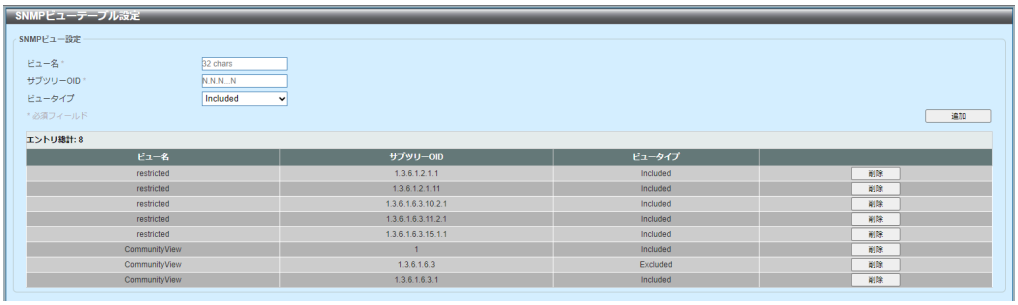

図 3-8 SNMP ビューテーブル設定

設定パラメータ （[SNMP ビュー設定] セクション）

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

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

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	1.3.6.1.2.1.1.11	**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 3-9 SNMP コミュニティテーブル設定

設定パラメータ （[SNMP コミュニティ設定] セクション）

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

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

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

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 3-10 SNMP グループテーブル設定

設定パラメータ （[SNMP グループ設定] セクション）

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

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

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

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。

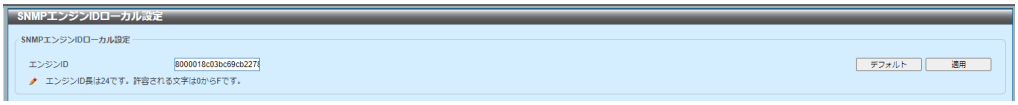

図 3-11 SNMP エンジン ID ローカル設定

設定パラメータ （[SNMP エンジン ID ローカル設定] セクション）

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

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

3.5.7 SNMP ユーザテーブル設定

このウィンドウを用いて、SNMP ユーザの設定を行い、設定値を表示します。

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

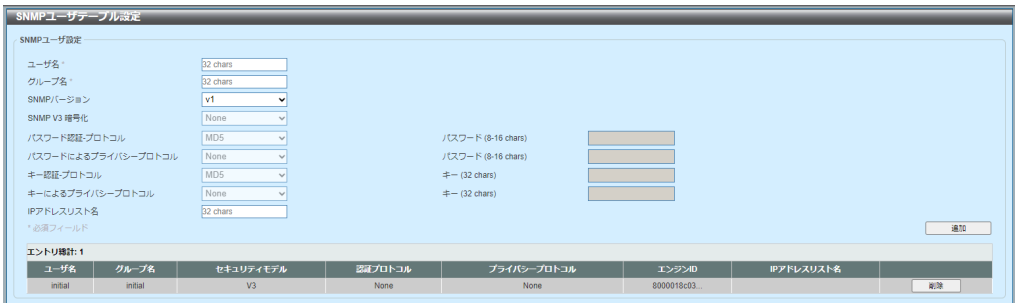

図 3-12 SNMP ユーザテーブル設定

設定パラメータ （[SNMP ユーザ設定] セクション）

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

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

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

3.5.8 SNMP ホストテーブル設定

このウィンドウを用いて、SNMP ホストの設定を行い、設定値を表示します。

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

図 3-13 SNMP ホストテーブル設定

設定パラメータ （[SNMP ホスト設定] セクション）

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

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

3.6 RMON（リモートモニタリング）

3.6.1 RMON グローバル設定

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

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

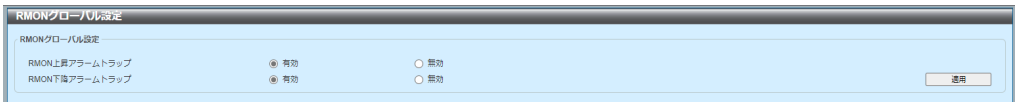

図 3-14 RMON グローバル設定

設定パラメータ （[RMON グローバル設定] セクション）

パラメータ	概要
RMON 上昇アラームトラップ	RMON 上昇アラームトラップの状態（**有効** / **無効**）を選択します。(デフォルト : 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。(デフォルト : 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 3-15 RMON 統計設定

設定パラメータ （[RMON 統計設定] セクション）

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

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

図 3-16 RMON 統計設定 (詳細参照)

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 3-17 RMON ヒストリ設定

設定パラメータ （[RMON ヒストリ設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
インデックス	ヒストリグループテーブルのエントリのインデックス番号を入力します。（設定範囲：1-65535）
パケット数	統計の RMON 収集ヒストリグループに指定したパケットの数を入力します。（デフォルト：50、設定範囲：1-65535）
間隔	各ポーリング周期の間隔時間（秒）を入力します。 （設定範囲：1-3600, デフォルト：1800 秒）
オーナー名	オーナー文字列を入力します。（最大：127 文字）

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

[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 3-18 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 3-19 RMON アラーム設定

設定パラメータ （[RMON アラーム設定] セクション）

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

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

3.6.5 RMON イベント設定

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

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

図 3-20 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。（設定範囲：1-127 文字）
オーナー名	オーナー文字列を入力します。（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。

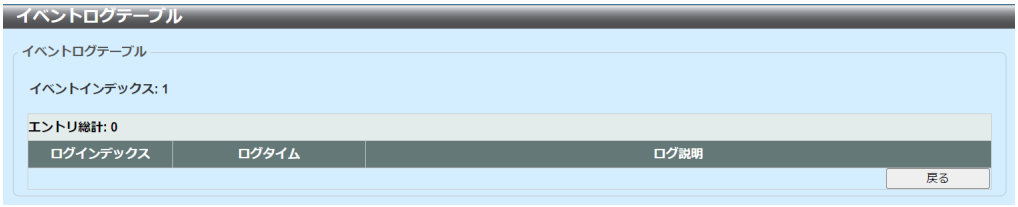

図 3-21 RMON イベント設定 (イベントログテーブル)

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。

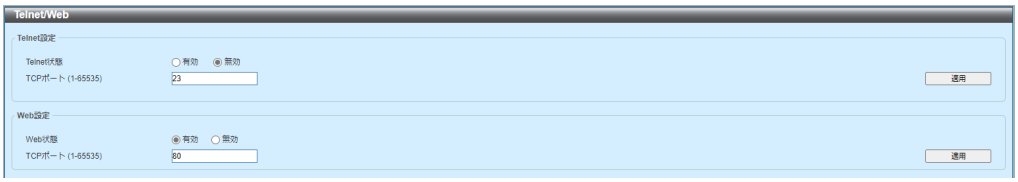

図 3-22 Telnet/WEB

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。 (デフォルト : 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。 （デフォルト：23、設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[WEB 設定] セクション）

パラメータ	概要
WEB 状態	WEB サーバの状態（**有効** / **無効**）を選択します。 (デフォルト : 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。 （デフォルト：80、設定範囲：1-65535）

[**適用**] ボタン - 設定内容を反映します。

3.8 セッションタイムアウト

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

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

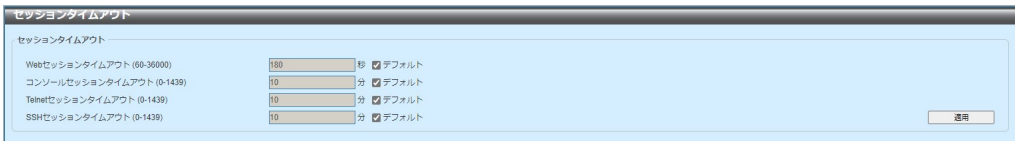

図 3-23 セッションタイムアウト

設定パラメータ （[セッションタイムアウト] セクション）

パラメータ	概要
WEB セッション タイムアウト	WEB セッションタイムアウトの時間（秒）を設定します。（デフォルト：180、設定範囲：60-36000）
コンソールセッション タイムアウト	コンソールセッションタイムアウトの時間（分）を設定します。0 を設定すると、タイムアウトが無効になります。（デフォルト：10、設定範囲：0-1439）
Telnet セッション タイムアウト	Telnet セッションタイムアウトの時間（分）を設定します。0 を設定すると、タイムアウトが無効になります。（デフォルト：10、設定範囲：0-1439）
SSH セッション タイムアウト	SSH セッションタイムアウトの時間（分）を設定します。0 を設定すると、タイムアウトが無効になります。（デフォルト：10、設定範囲：0-1439）

[**適用**] ボタン - 設定内容を反映します。

3.9 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。

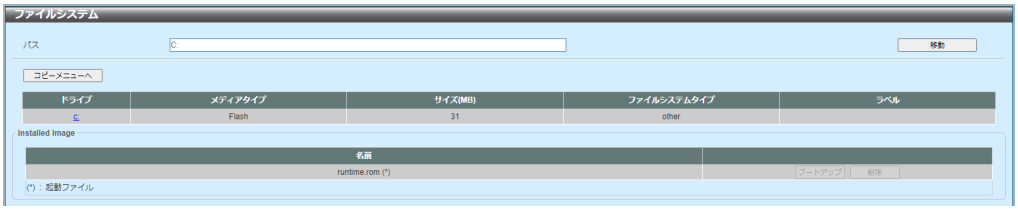

図 3-24 ファイルシステム

設定パラメータ ([パス] セクション)

パラメータ	概要
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。
[**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。
[**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。

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 3-25 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。

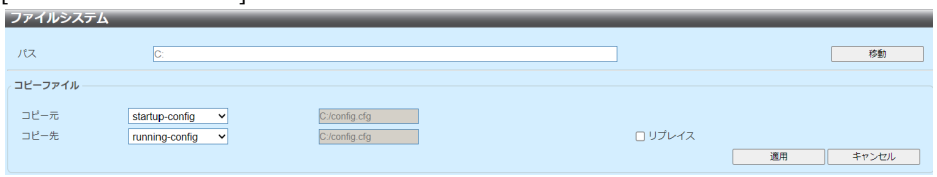

図 3-26 ファイルシステム（コピー）

設定パラメータ （[コピーファイル] セクション）

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

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

3.10 IP 簡単設定

3.10.1 IP 簡単設定プロトコル設定

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

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

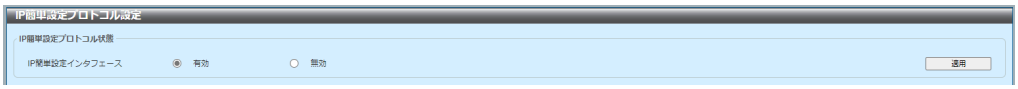

図 3-27 IP 簡単設定プロトコル設定

設定パラメータ （[IP 簡単設定プロトコル状態] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

4 PPS

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。

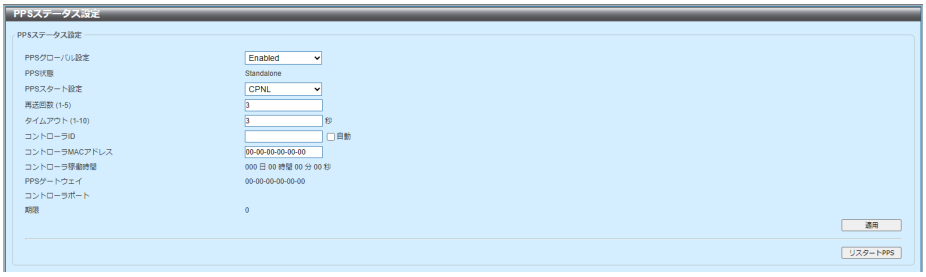

図 4-28 PPS ステータス設定

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。 (デフォルト : Enabled)
PPS スタート状態	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。 Note : 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。(設定範囲 : 1-5, デフォルト : 3)
タイムアウト	タイムアウトの値を入力します。 (設定範囲 : 1-10, デフォルト : 3)
コントローラー ID	コントローラ 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 ID と MAC アドレスを自動的に決定できるようになります。

パラメータ	概要
コントローラー **MAC** アドレス	コントローラーの MAC アドレスを入力します。

[**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。

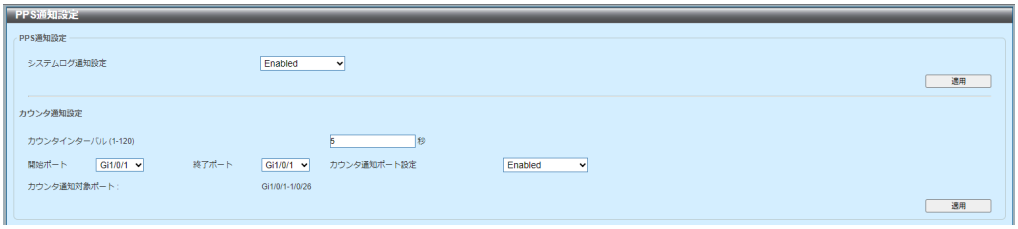

図 4-29 PPS 通知設定

設定パラメータ （[PPS 通知設定] セクション）

パラメータ	概要
システムログ通知設定	PPS のシステムログ通知の状態（**Enabled**/**Disabled**）を選択します。(デフォルト :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。 （設定範囲：1-120, デフォルト：5）
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。 (デフォルト :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。

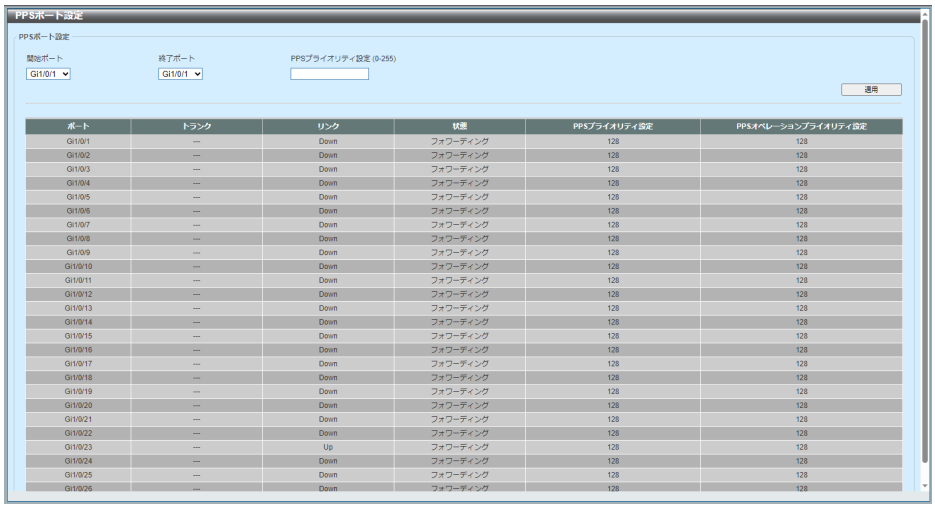

図 4-30 PPS ポート設定

設定パラメータ （[PPS ポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを設定します。
PPS プライオリティ設定	PPS プライオリティの値を設定します。 （設定範囲：0-255 デフォルト：128）

[**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 4-31 PPS コネクション設定

設定パラメータ （[PPS コネクション設定] セクション）

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

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

4.5 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。

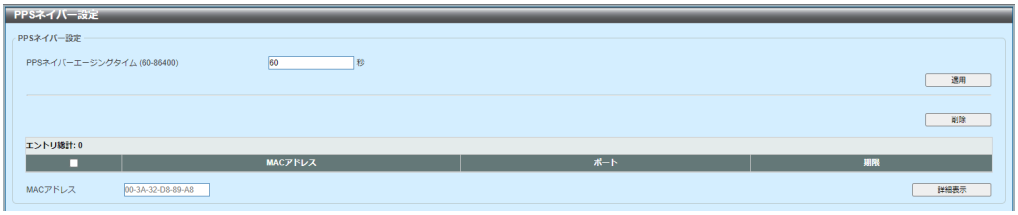

図 4-32 PPS ネイバー設定

設定パラメータ （[PPS ネイバー設定] セクション）

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

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

5 L2 機能

5.1 FDB（フォワーディングデータベース）

5.1.1 スタティック FDB

5.1.1.1 ユニキャストスタティック FDB

このウィンドウを用いて、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。

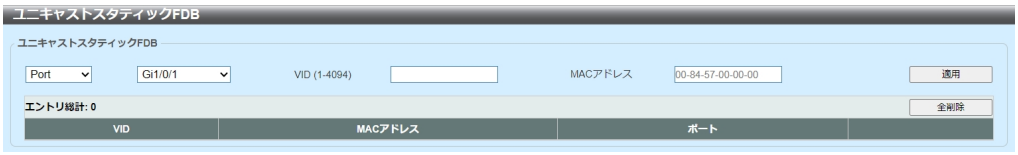

図 5-1 ユニキャストスタティック FDB

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。
ポートナンバー	([Port] 選択時に設定可）ポートを選択します。
VID	使用する VLAN ID を入力します。(設定範囲：1-4094)
MAC アドレス	パケットがスタティックに転送される MAC アドレスを入力します。このアドレスには、ユニキャスト MAC アドレスを指定してください。

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

5.1.1.2 マルチキャストスタティック FDB

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

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

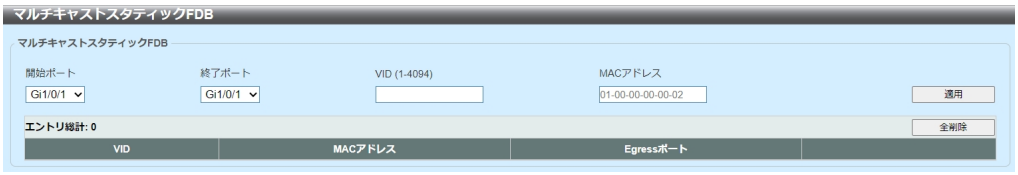

図 5-2 マルチキャストスタティック FDB

設定パラメータ （[マルチキャストスタティック FDB] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
MAC アドレス	マルチキャストパケット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。

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。 （デフォルト：300、設定範囲：0,10-1000000）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC アドレスポート学習設定] タブ）

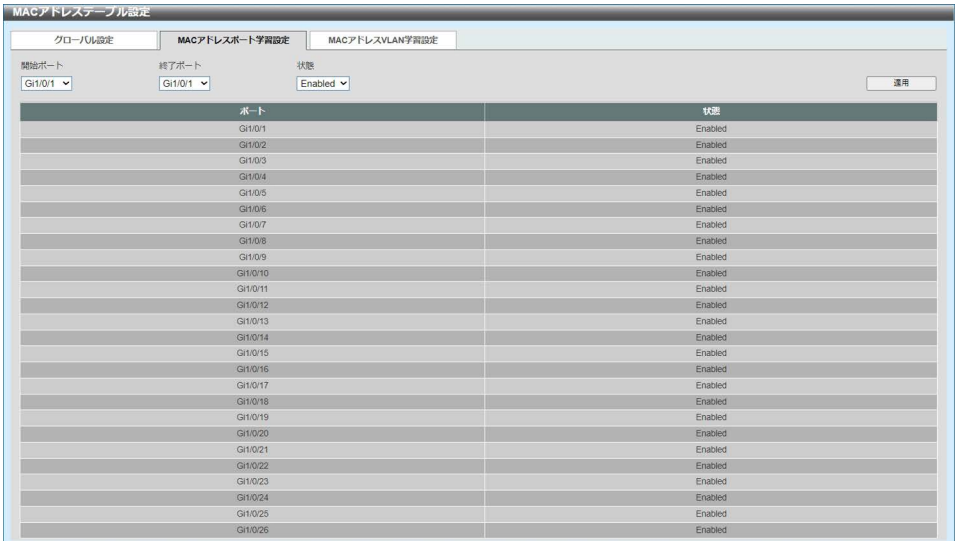

図 5-4 MAC アドレステーブル設定（MAC アドレスポート学習設定）

以下のパラメータを設定できます。

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

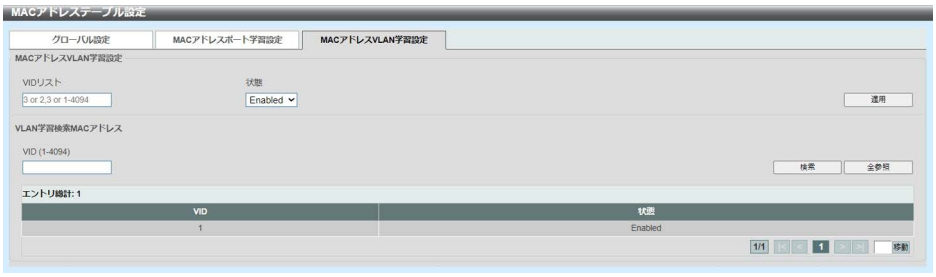

図 5-5 MAC アドレステーブル設定（MAC アドレス VLAN 学習設定）

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

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

[適用] ボタン - エントリを追加します。

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

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

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

5.1.3 MAC アドレステーブル

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

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

図 5-6 MAC アドレステーブル

設定パラメータ （[MAC アドレステーブル] セクション）

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

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

5.1.4 MAC 通知

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

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

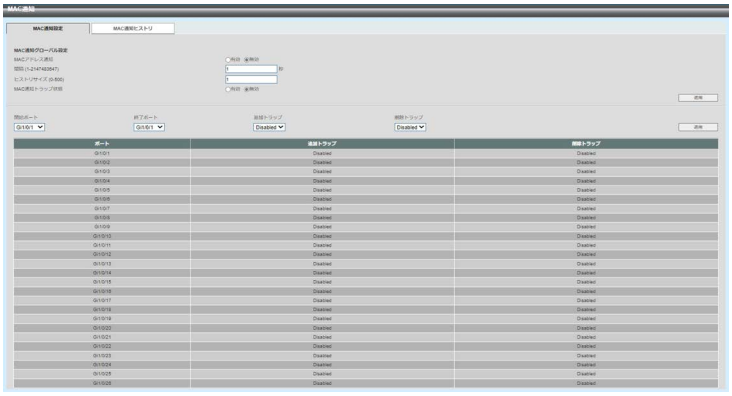

図 5-7 MAC 通知（MAC 通知設定）

設定パラメータ （[MAC 通知設定] タブ）

パラメータ	概要
MAC アドレス通知	MAC 通知状態（**有効** / **無効**）を選択します。 (デフォルト : 無効)
間隔	通知間隔の時間（秒）を入力します。 （デフォルト：1、設定範囲：1-2147483647）
ヒストリサイズ	通知に使用するヒストリログにリスト表示するエントリの最大数を入力します。（デフォルト：1、設定範囲：0-500）
MAC 通知トラップ状態	MAC 通知トラップ状態（**有効** / **無効**）を選択します。 (デフォルト : 無効)
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。 (デフォルト : 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。 (デフォルト : 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 通知ヒストリの表示します。

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

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

[検索 VLAN] セクションでは、以下のパラメータを設定できます。

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

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

5.2.2 802.1v プロトコル VLAN

5.2.2.1 プロトコル VLAN プロファイル

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

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

図 5-10 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：1-8)
フレームタイプ	フレームタイプのオプション（**Ethernet2**/**SNAP**/**LLC**）を選択します。この機能は、パケットヘッダ内のタイプオクテットを調べて、関連付けられたプロトコルのタイプを探索します。これにより、パケットをプロトコル定義の VLAN にマッピングします。
イーサタイプ	グループのイーサネットタイプ値を入力します。プロトコル値を用いて、指定したフレームタイプのプロトコルを識別します。フレームタイプに応じて、オクテット文字列が以下のいずれかの値を持ちます。 • Ethernet2 の場合 - 16 ビット（2 オクテット）の 16 進数値です。IPv4 は 0800、IPv6 は 86DD、ARP は 0806 など。 • SNAP の場合 - 16 ビット（2 オクテット）の 16 進数値です。 • LLC の場合 - 2 オクテットの IEEE 802.2 LSAP（Link Service Access Point）ペアです。最初のオクテットは DSAP（Destination Service Access Point）、2 番目のオクテットはソースです。

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

5.2.2.2 プロトコル VLAN プロファイルインタフェース

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

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

図 5-11 プロトコル VLAN プロファイルインタフェース

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

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

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

5.2.3 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 5-12 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。

5.2.4 VLAN インタフェース

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

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

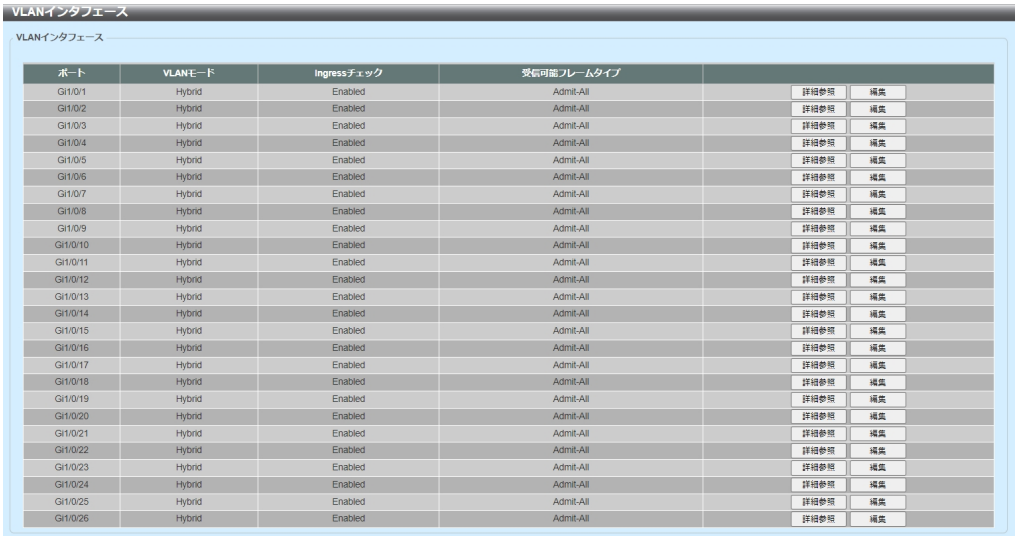

図 5-13 VLAN インタフェース

[**詳細参照**] ボタン - エントリの詳細情報を表示します。
[**編集**] ボタン - 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。

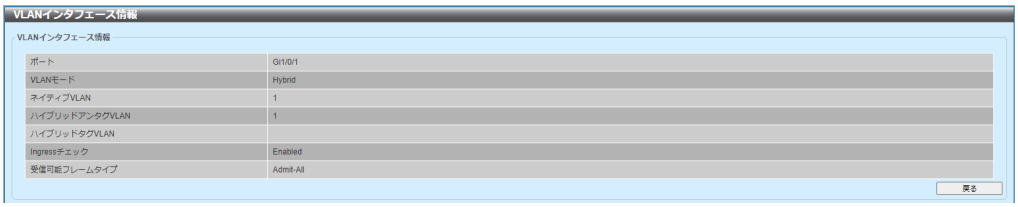

図 5-14 VLAN インタフェース (詳細参照)

[**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 [**アクセス**] を選択して、次のウィンドウを表示します。

図 5-15 VLAN インタフェース（編集、アクセス）

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

パラメータ	概要
VLAN モード	VLAN モードのオプション（**Access**/**Hybrid**/**Trunk**）を選択します。(デフォルト : Hybrid)
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。(デフォルト : 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。(デフォルト : 有効)
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）
クローン	クローンの有効、無効を選択します。
開始ポート／終了ポート	ポートを選択します。

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

[**ハイブリット**] 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 5-16 VLAN インタフェース (Edit, ハイブリット)

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

パラメータ	概要
VLAN モード	VLAN モードのオプション（**Access**/**Hybrid**/**Trunk**）を選択します。(デフォルト : Hybrid)
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。(デフォルト : Admit All)

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。 (デフォルト : 有効)
ネイティブ VLAN	ネイティブ VLAN の有効、無効を選択します。
VID	([ネイティブ VLAN] パラメータで [有効] 選択時に設定可) 使用する VLAN ID を入力します。(設定範囲 : 1-4094)
アクション	実行するアクション（**None**/**Add**/**Remove**/**Tagged**/ **Untagged**）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	許可 VLAN 範囲を入力します。(設定範囲 : 1-4094)
クローン	クローンの有効、無効を選択します。
開始ポート／終了ポート	ポートを選択します。

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

[トランク] ボタンをクリックして、以下のウィンドウを表示します。

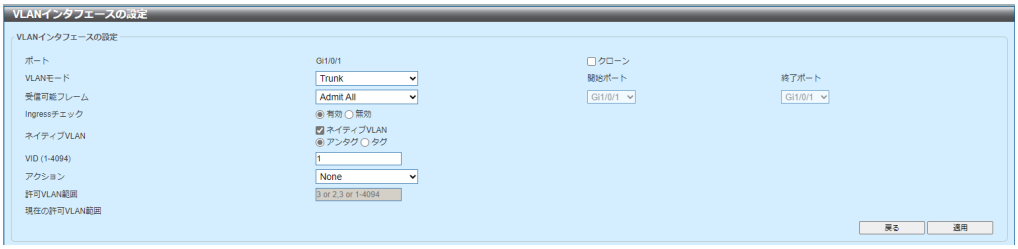

図 5-17 VLAN インタフェース (Edit, トランク)

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

パラメータ	概要
VLAN モード	VLAN モードのオプション（**Access**/**Hybrid**/**Trunk**）を選択します。(デフォルト : Hybrid)
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。 (デフォルト : 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。 (デフォルト : 有効)

パラメータ	概要
ネイティブ VLAN	([VLAN モード] パラメータで [Trunk] 選択時に設定可) ([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**/**Add**/**Remove**/**Tagged**/**Untagged**/**Except**/**Replace**）を選択します。
許可 VLAN 範囲	許可 VLAN 範囲を入力します。(設定範囲 :1-4094)
クローン	クローンの有効、無効を選択します。
開始ポート／終了ポート	ポートを選択します。

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

5.3 ループ検知・遮断

5.3.1 ループ検知・遮断の設定

このウィンドウを用いて、ループ検知・遮断の設定を行い、設定値を表示します。

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

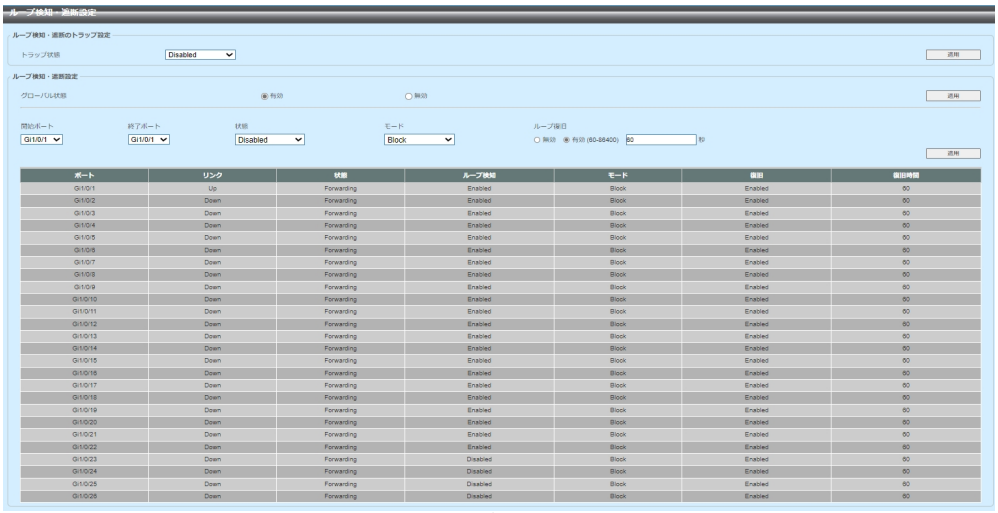

図 5-18 ループ検知・遮断設定

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。(デフォルト : 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。(デフォルト : 有効)
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの回線ループバックの状態（**Enabled**/**Disabled**）を選択します。(デフォルト : Disabled)

パラメータ	概要
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。 (デフォルト : 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。 (デフォルト : 有効 , 60)

[**適用**] ボタン - 設定内容を反映します。

5.3.2 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。

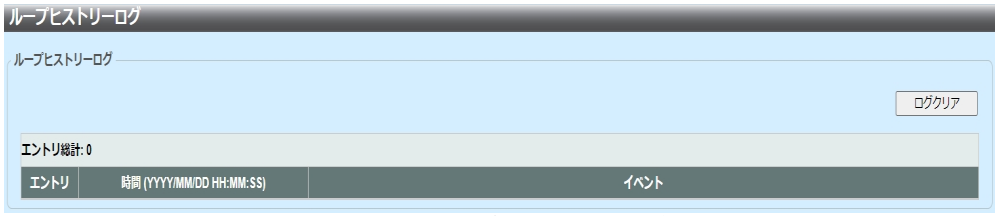

図 5-19 ループヒストリーログ

[ログクリア] ボタン - テーブルからログエントリをクリアします。

5.4 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。

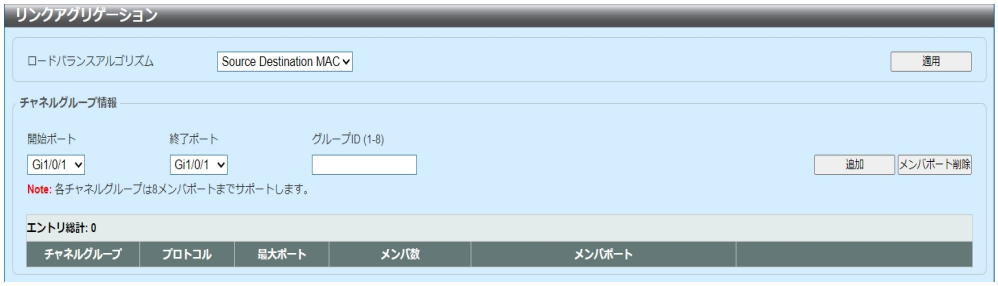

図 5-20 リンクアグリゲーション

設定パラメータ

パラメータ	概要
ロードバランス アルゴリズム	使用するロードバランスアルゴリズム（**Source MAC/ Destination MAC/Source Destination MAC/Source IP/Destination IP/Source Destination IP**）を選択します。（デフォルト：Source Destination MAC）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[チャネルグループ情報] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
グループ ID	チャネルグループ番号を入力します。 GA-EM(i)8T/16T/24T の場合、設定範囲は 1 から 8。GA-EM48T の場合、設定範囲は 1 から 16 です。 システムは、最初に物理ポートが作成されると、ポートチャネルを自動的に作成されます。 チャネル グループに参加します。インターフェイスは 1 つのチャネル グループにのみ参加できます。

[**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。
[**戻る**] ボタン - 前のウィンドウに戻ります。

[**詳細参照**] ボタン - エントリの詳細情報を表示します。

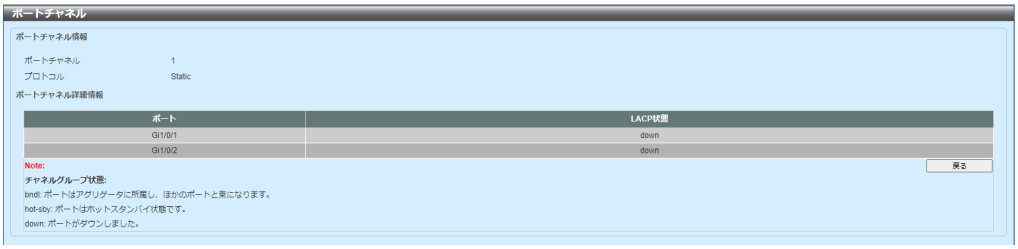

図 5-21 リンクアグリゲーション (詳細参照)

[**戻る**] ボタン - 前のウィンドウに戻ります。

5.5 L2 マルチキャスト制御

5.5.1 IGMP スヌーピングスタティックグループ設定

このウィンドウを用いて、マルチキャスト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 スヌーピングスタティックグループ設定] をクリックして、以下のウィンドウを表示します。

図 5-22 IGMP スヌーピンググループ設定

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

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

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

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

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

[**検索**] ボタン - 検索結果を表示します。

[**全参照**] ボタン - エントリをすべて表示します。

5.5.2 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。

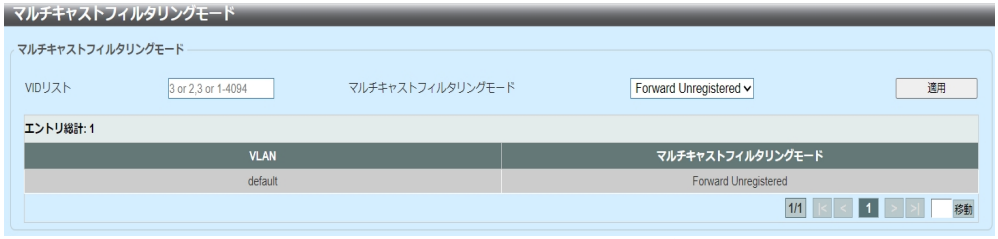

図 5-23 マルチキャストフィルタリングモード

設定パラメータ （[マルチキャストフィルタリングモード] セクション）

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

5.5.3 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。

[L2 機能] > [L2 マルチキャスト制御] > [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 5-24 IP マルチキャストフォワーディングキャッシュ

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

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

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

6 L3 機能

6.1 ARP （Address Resolution Protocol）

6.1.1 ARP エージング時間

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

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

図 6-1 ARP エージング時間

設定パラメータ （[ARP エージング時間検索] セクション）

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

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, デフォルト : 240)

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

6.1.2 スタティック ARP

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

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

図 6-2 スタティック ARP

設定パラメータ （[スタティック ARP 設定] セクション）

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

[**適用**] ボタン - スタティック ARP エントリを追加します。

設定パラメータ （[スタティック ARP 検索] セクション）

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

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

6.1.3 ARP テーブル

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

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

図 6-3 ARP テーブル

設定パラメータ （[ARP 検索] セクション）

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

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

6.2 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 6-4 IPv6 ネイバー

設定パラメータ （[IPv6 ネイバー設定] セクション）

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

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

6.3 インタフェース

6.3.1 IPv4 インタフェース

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

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

図 6-5 IPv4 インタフェース

設定パラメータ （[IPv4 インタフェース] セクション）

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

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

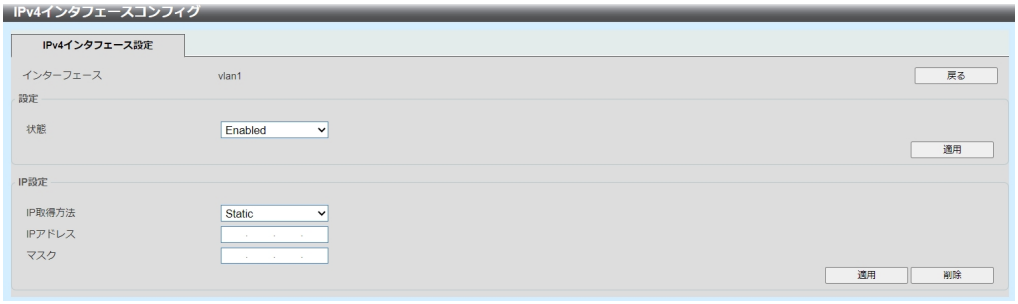

図 6-6 IPv4 インターフェイス (編集、IPv4 インターフェイスコンフィグ)

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

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

[**適用**] ボタン - 設定内容を反映します。

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

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

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

6.3.2 IPv6 インタフェース

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

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

図 6-7 IPv6 インタフェース

設定パラメータ （[IPv6 インタフェース] セクション）

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

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

[**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 6-8 IPv6 インタフェース (詳細参照、IPv6 インタフェース設定)

設定パラメータ （[詳細参照]>[IPv6 インタフェース設定] タブ）

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

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

設定パラメータ （[詳細参照]>[スタティック IPv6 アドレス設定] タブ）

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

[**適用**] ボタン - 設定内容を反映します。

[インタフェース IPv6 アドレス] タブ - インタフェース IPv6 アドレスのエントリ統計を表示します。

図 6-9 IPv6 インタフェース (詳細参照、インタフェース IPv6 アドレス)

[**削除**] ボタン - 指定したエントリを削除します。
[**移動**] ボタン - ページ番号を入力し、特定のページに移動します。

[**ネイバー探索**] タブ - ND 設定の詳細情報を表示します。

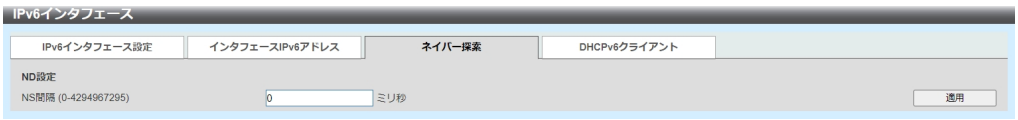

図 6-10 IPv6 インタフェース（詳細参照、ネイバー探索）

設定パラメータ （[詳細参照]>[ネイバー探索] タブ）

パラメータ	概要
NS 間隔	NS（Neighbor Solicitation）間隔の値（ミリ秒）を入力します。(設定範囲 : 0 - 4294967295, 1000 の倍数でのみ設定可能) 0 を設定した場合、ルータは 1 秒を使用します。

[**適用**] ボタン - エントリを追加します。

[**DHCPv6 クライアント**] タブ - DHCPv6 クライアント設定の詳細情報を表示します。

図 6-11 IPv6 インタフェース（詳細参照、DHCPv6 クライアント）

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

設定パラメータ （[詳細参照]>[DHCPv6 クライアント] タブ）

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

[**適用**] ボタン - 設定内容を反映します。

6.4 IPv4 デフォルトルート

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

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

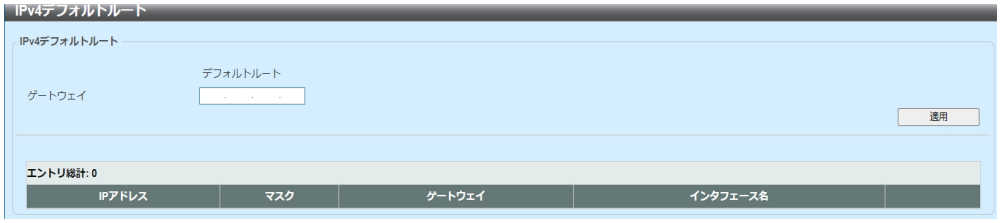

図 6-12 IPv4 デフォルトルート

設定パラメータ （[IPv4 デフォルトルート] セクション）

パラメータ	概要
ゲートウェイ	ゲートウェイアドレスを入力します。

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

6.5 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 6-13 IPv4 ルートテーブル

設定パラメータ ([IPv4 ルートテーブル設定] セクション)

パラメータ	概要
接続	接続されているルートのみが表示されます。
要約	スイッチのルートソースの概要と数を表示されます。

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

[**要約**] オプションと [**検索**] ボタンをクリックして、次のウィンドウを表示します。

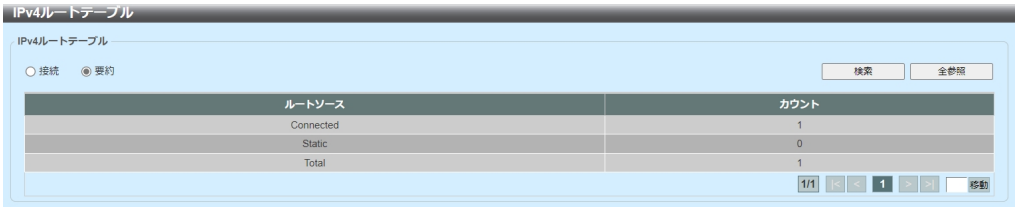

図 6-14 IPv4 ルートテーブル（要約）

6.6 IPv6 デフォルトルート

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

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

図 6-15 IPv6 デフォルトルート

設定パラメータ （[IPv6 デフォルトルート] セクション）

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

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

6.7 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 6-16 IPv6 ルートテーブル

設定パラメータ ([IPv6 ルートテーブル設定] セクション)

パラメータ	概要
接続	接続されているルートのみが表示されます。
データベース	ルーティング データベース内のすべての関連エントリが表示されます。
要約	スイッチのルートソースの概要と数を表示されます。

[**検索**] ボタン - 検索結果を表示します。
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。

[**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。

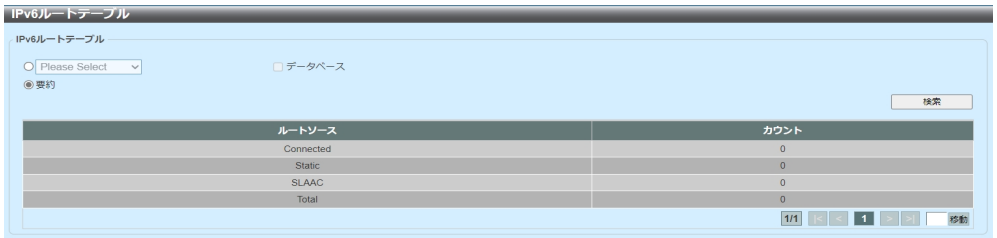

図 6-17 IPv6 ルートテーブル（要約）

7 QoS（Quality of Service）

7.1 基本設定

7.1.1 ポートデフォルト CoS

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

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

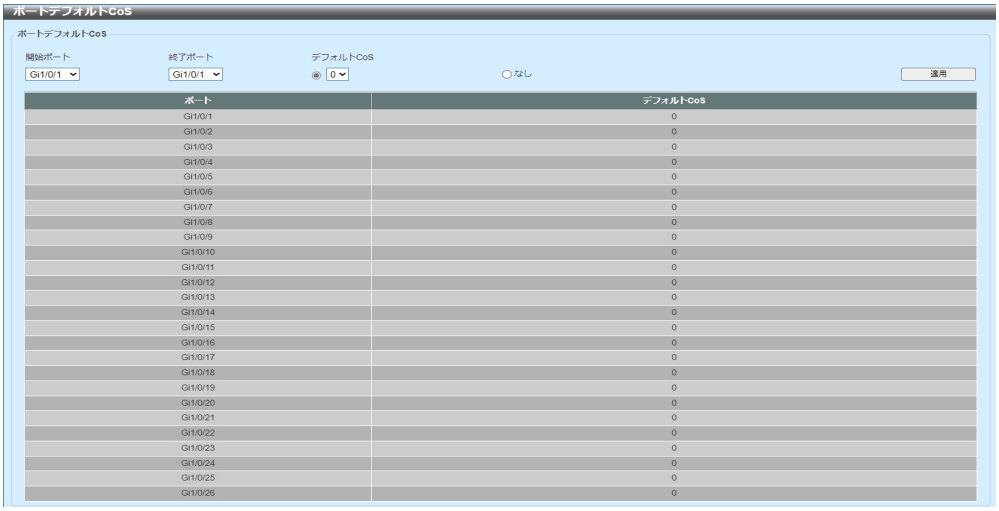

図 7-1 ポートデフォルト CoS

設定パラメータ （[ポートデフォルト CoS] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
デフォルト **CoS**	指定するポートのデフォルト CoS オプション（**0 ～ 7**）を選択します。デフォルト値は 0 です。 • **なし** - パケットがタグ付けされていればパケットの CoS が、タグ付けされていなければポートのデフォルト CoS が、それぞれパケットの CoS になります。

[**適用**] ボタン - 設定内容を反映します。

7.1.2 ポートスケジューラ方式

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

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

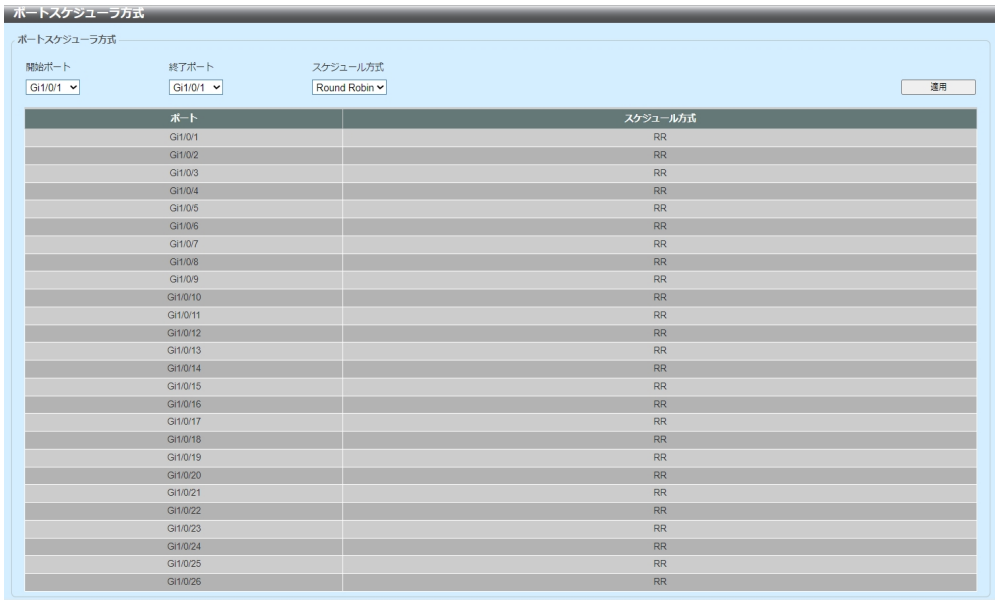

図 7-2 ポートスケジューラ方式

設定パラメータ （[ポートスケジューラ方式] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
スケジュール方式	指定したポートに適用するスケジューラ方式を選択します。（デフォルト：Round Robin） • **絶対優先（Strict Priority）** - すべてのキューで絶対優先スケジューリングを使用します。これは、CoS が最も高いキューから最も低いキューまでを実行する、絶対優先アクセスです。 • **ラウンドロビン（Round Robin）** - すべてのキューでラウンドロビンスケジューリングを使用します。これは、各キューで 1 つのパケットにサービスを提供したら次のキューに移動する、公平なアクセスです。

[**適用**] ボタン - 設定内容を反映します。

7.1.3 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。

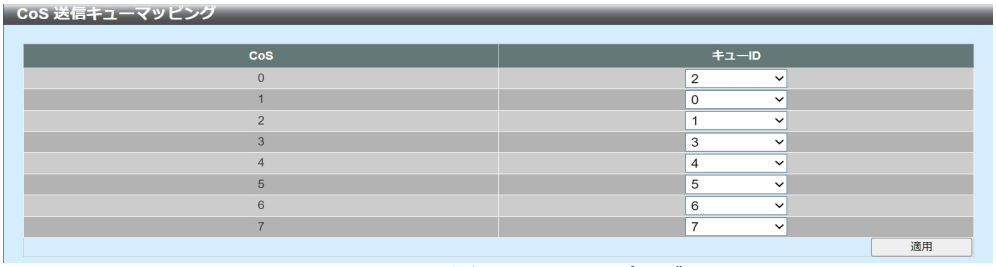

図 7-3 CoS 送信キューマッピング

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。

7.1.4 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。

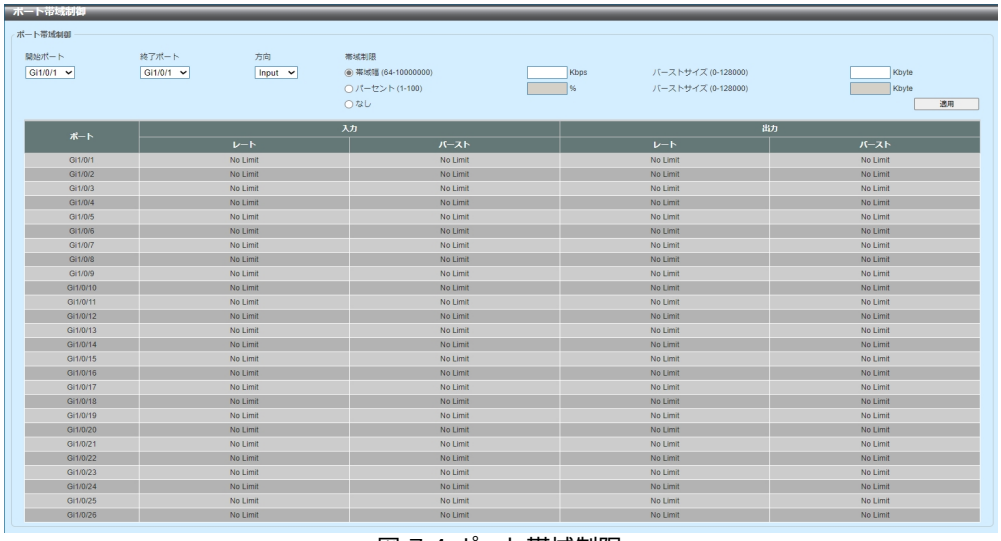

図 7-4 ポート帯域制限

設定パラメータ （[ポート帯域制限] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

7.2 高度な設定

7.2.1 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 7-5 クラスマップ

設定パラメータ

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

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

[適合] ボタンをクリックして、以下のウィンドウを表示します。

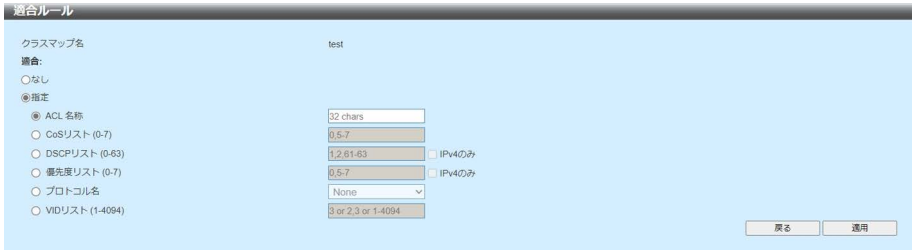

図 7-6 クラスマップ（適合）

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。

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

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

7.2.2 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。

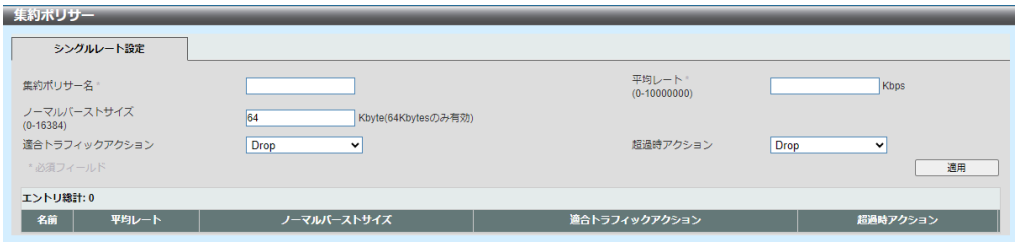

図 7-7 集約ポリサー（シングルレート設定）

設定パラメータ （[シングルレート設定] タブ）

パラメータ	概要
集約ポリサー名	集約ポリサー名を入力します。
平均レート	平均レート値を入力します。（設定範囲：0-10000000）
ノーマルバーストサイズ	ノーマルバーストサイズ値を入力します。 （64KBytes のみ設定できます。）
適合トラフィックアクション	確認アクションを選択します。確認アクションは、緑色のパケットに対して実行するアクションを指定します。 （Drop のみ使用できます。） • **Drop** - パケットを廃棄します。
超過時アクション	超過時アクションを選択します。超過時アクションは、帯域制限を超過したパケットに対して実行するアクションを指定します。（Drop のみ使用できます。） • **Drop** - パケットを廃棄します。

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

7.2.3 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 7-8 ポリシーマップ

設定パラメータ （[ポリシーマップ作成／削除] セクション）

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

[**適用**] ボタン - エントリを追加します。

設定パラメータ （[トラフィックポリシー] セクション）

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

[**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。

[**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。

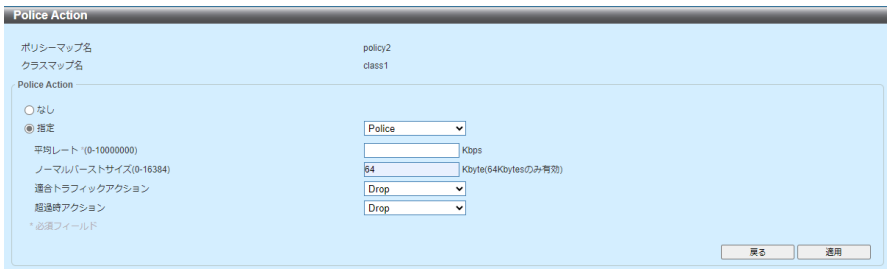

図 7-9 ポリシーマップ（ポリサー、Police）

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

パラメータ	概要
なし	このオプションを選択した場合、このエントリにポリサーは設定されません。
指定	適用するポリサー設定（**Police**）を選択します。
平均レート	平均レート値を入力します。（設定範囲：0-10000000）
ノーマルバーストサイズ	ノーマルバーストサイズ値を入力します。 （64KBytes のみ設定できます。）
適合トラフィック アクション	実行する適合トラフィックアクションを選択します。このアクションは、緑色のパケットに対して実行します。選択する値は以下です。(Drop のみ使用できます。) • **Drop** - パケットを廃棄します。
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黄色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 のみ使用できます。) • **Drop** - パケットを廃棄します。

[**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 7-10 ポリシーマップ（ポリサー、Police Aggregate）

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

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

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

[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 7-11 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)

[**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。

7.2.4 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。

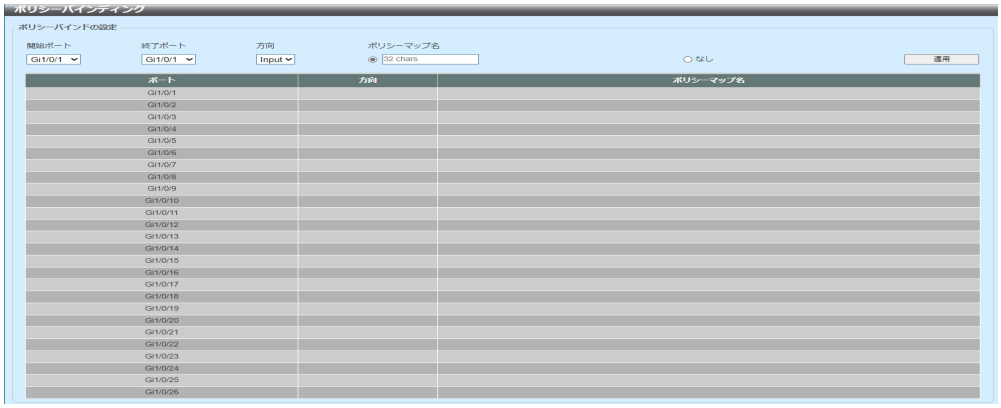

図 7-12 ポリシーバインディング

設定パラメータ （[ポリシーバインドの設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

8 ACL（Access Control List）

8.1 ACL 設定ウィザード

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

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

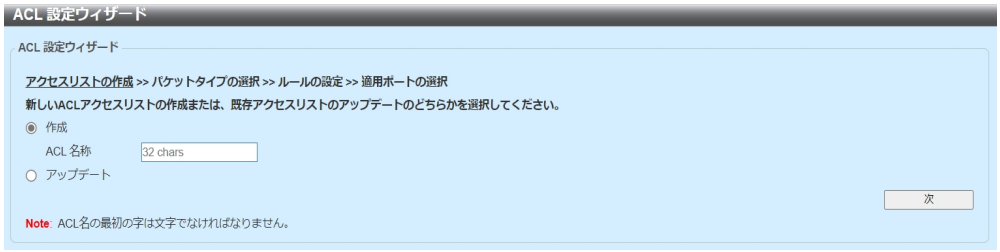

図 8-1 ACL 設定ウィザード（作成）

[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。（最大：32 文字）
アップデート	このオプションを選択した場合、既存の ACL アクセスリストをアップデートします。テーブルで既存の ACL を選択して、アップデートします。

[作成] >[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。

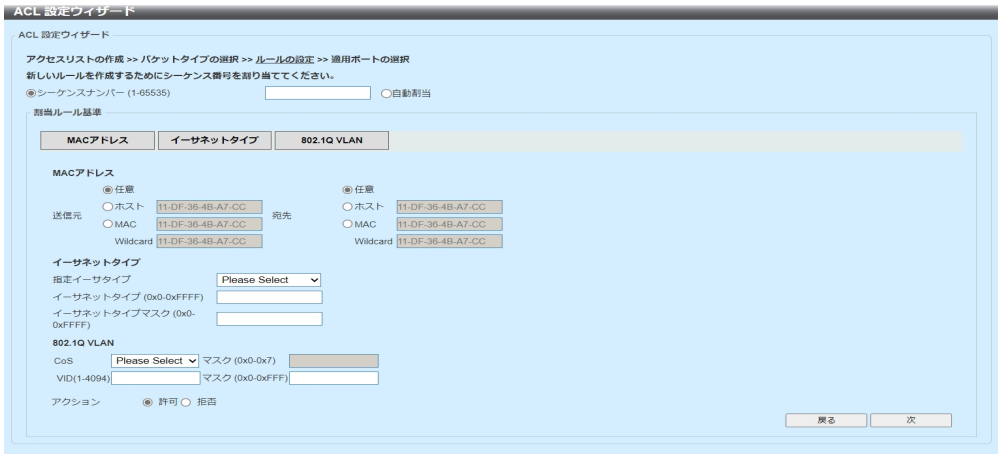

図 8-4 ACL 設定ウィザード（拡張 MAC ACL の設定）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。

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 **Wildcard** 値を表示された入力フィールドに入力します。
宛先	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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**/**decent-iv**/**etype-6000**/**etype-8042**/**lat**/**lavc-sca**/**mop-console**/**mop-dump**/**vines-echo**/**vines-ip**/**xns-idp**/**arp**）を選択します。
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。 (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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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)
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。

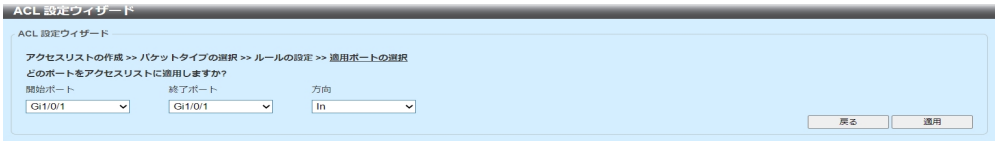

図 8-5 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

パラメータ	概要
方向	方向（**In**）を選択します。

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

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。

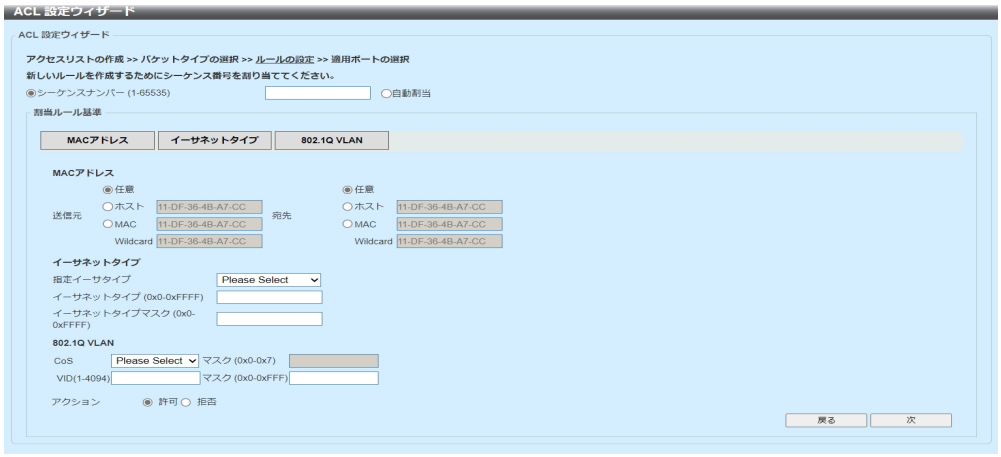

図 8-6 ACL 設定ウィザード（拡張 MAC ACL の設定）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。

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 **Wildcard** 値を表示された入力フィールドに入力します。

パラメータ	概要
宛先	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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**/**decent-iv**/**etype-6000**/**etype-8042**/**lat**/**lavc-sca**/**mop-console**/**mop-dump**/**vines-echo**/**vines-ip**/**xns-idp**/**arp**）を選択します。
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。 (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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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)
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。

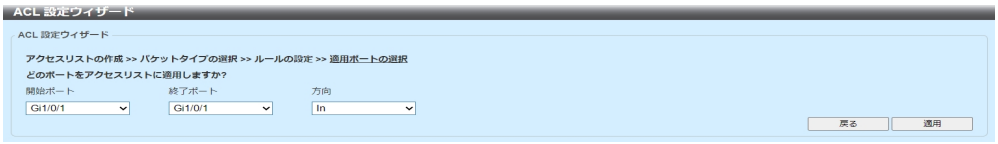

図 8-7 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

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

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

8.1.2 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。

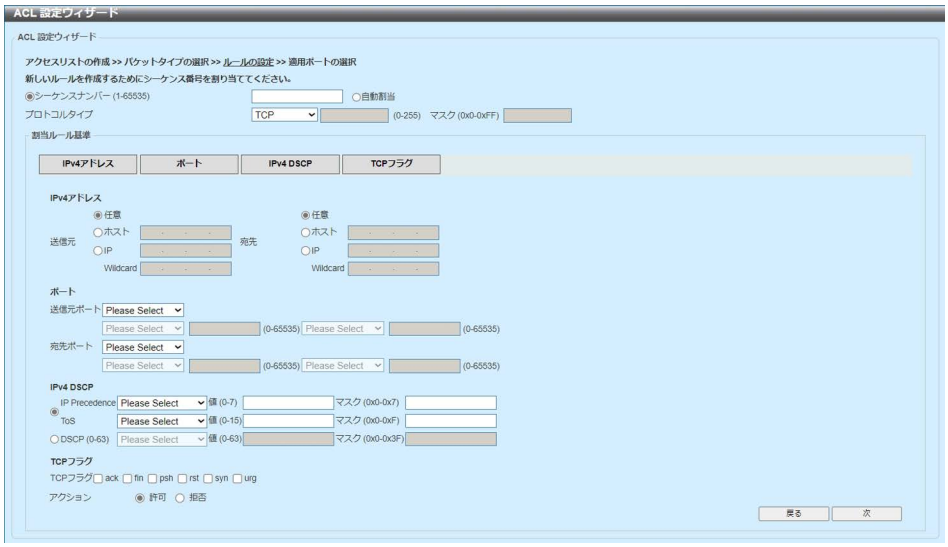

図 8-8 ACL 設定ウィザード（拡張 IP ACL の設定）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1 - 65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。
プロトコルタイプ	プロトコルタイプオプション（**TCP**/**UDP**/**ICMP**/**EIGRP**(88) /**ESP**（50）/**GRE**(47) /**IGMP**(2) /**OSPF**(89) /**PIM**（103）/**VRRP**(112) /**IP-in-IP**(94) /**PCP**（108）/**Protocol ID**/**None**）を選択します。 • **値** - プロトコル ID を手動で入力できます。 (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)

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** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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) • **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) • **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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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)

パラメータ	概要
DSCP	使用する DSCP 値を選択します。選択する値は、**[default]**（0）、**[af11]**（10）、**[af12]**（12）、**[af13]**（14）、**[af21]**（18）、**[af22]**（20）、**[af23]**（22）、**[af31]**（26）、**[af32]**（28）、**[af33]**（30）、**[af41]**（34）、**[af42]**（36）、**[af43]**（38）、**[cs1]**（8）、**[cs2]**（16）、**[cs3]**（24）、**[cs4]**（32）、**[cs5]**（40）、**[cs6]**（48）、**[cs7]**（56）、**[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。 (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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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。範囲は 0 ～ 255 です。**[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。
メッセージコード	([プロトコルタイプ] で [ICMP] 選択した場合に設定) **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[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。
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。

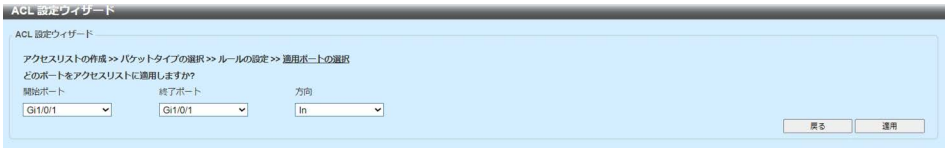

図 8-9 ACL 設定ウィザード（ポートと方向の選択）

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
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In**）を選択します。

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

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。

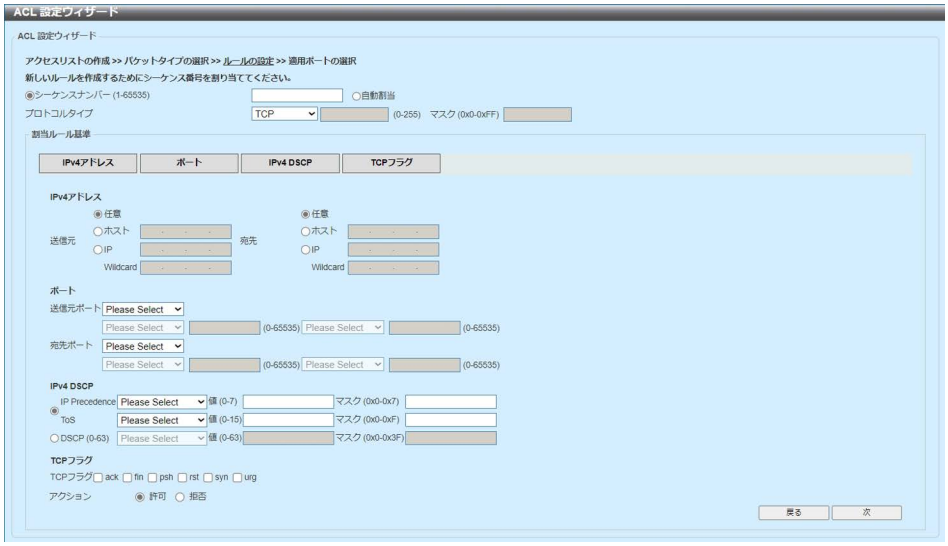

図 8-10 ACL 設定ウィザード（拡張 IP ACL の設定）

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。

パラメータ	概要
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）

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** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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) • **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] 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) • **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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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。

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] 選択した場合に設定) **[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[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] 選択した場合に設定) **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[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。
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。

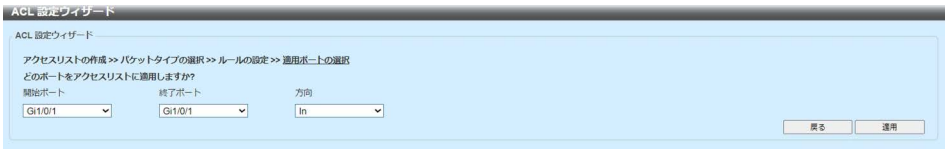

図 8-11 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

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

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

8.1.3 IPv6

[作成] > [IPv6] を選択すると、以下のウィンドウが表示されます。

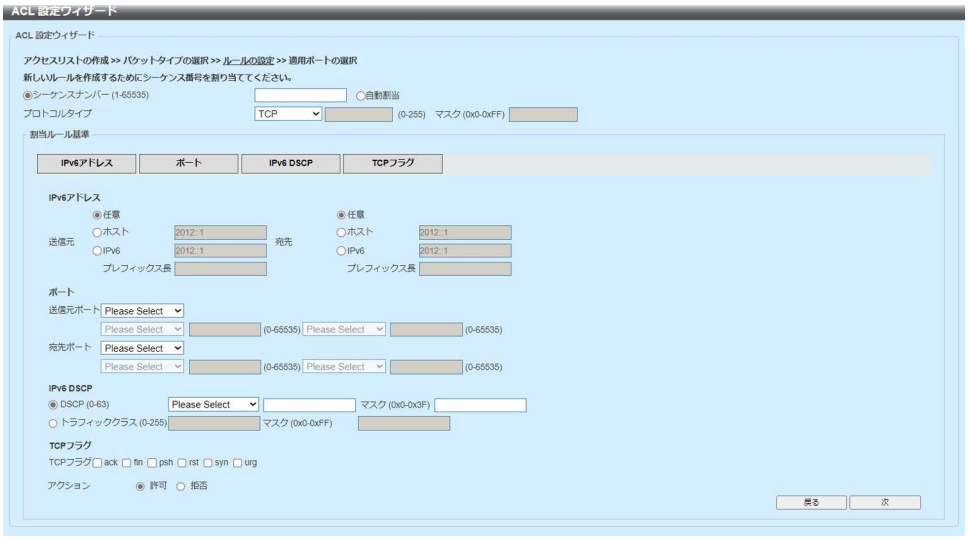

図 8-12 ACL 設定ウィザード (拡張 IPv6 ACL 設定)

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。
プロトコルタイプ	プロトコルタイプオプション（**TCP**/**UDP**/**ICMP**/**ESP**（50）/**PCP**（108）/**SCTP**（132）/**Protocol ID**/**None**）を選択します。 • **値** - プロトコル ID を手動で入力できます。 (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)

設定パラメータ （[IPv6 アドレス] セクション）

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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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) • **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) • **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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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値を選択および入力します。 (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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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] パラメータで [ICMP] 選択時に設定可) 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) [**指定 ICMP メッセージタイプ**] を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。 (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。
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。

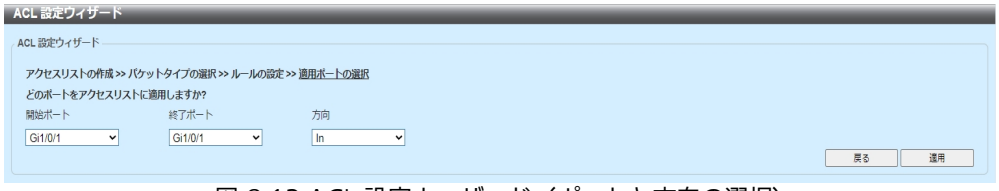

図 8-13 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

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

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

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。

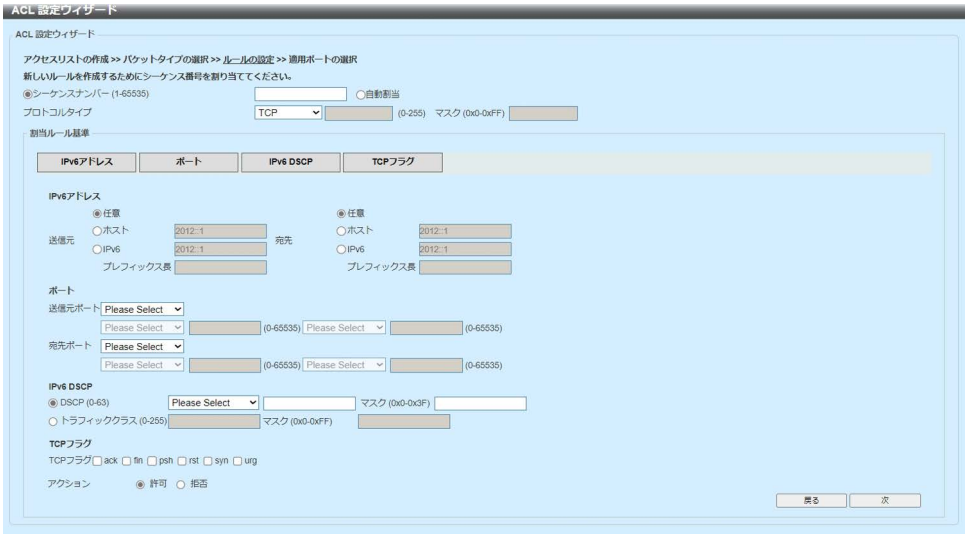

図 8-14 ACL 設定ウィザード (拡張 IPv6 ACL 設定)

設定パラメータ （[ACL 設定ウィザード] セクション）

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。（設定範囲：1-65535） [**自動割当**] を選択した場合、このエントリの ACL ルールナンバーを自動生成します。
プロトコルタイプ	プロトコルタイプオプション（**TCP**/**UDP**/**ICMP**/**ESP**（50）/**PCP**（108）/**SCTP**（132）/**Protocol ID**/**None**）を選択します。 • **値** - プロトコル ID を手動で入力できます。 (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)

設定パラメータ （[IPv6 アドレス] セクション）

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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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) • **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) • **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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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値を選択および入力します。(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)
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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。
アクション	実行するアクション（**許可** / **拒否**）を選択します。

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] パラメータで [ICMP] 選択時に設定可) 使用する ICMP メッセージタイプを選択します。
ICMP メッセージタイプ	([プロトコルタイプ] パラメータで [ICMP] 選択時に設定可) [**指定 ICMP メッセージタイプ**] を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。 (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。
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。

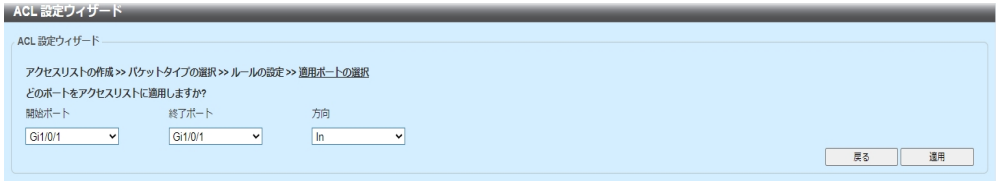

図 8-15 ACL 設定ウィザード（ポートと方向の選択）

設定パラメータ （[ACL 設定ウィザード] セクション）

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

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

8.2 ACL アクセスリスト

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

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

図 8-16 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（最大 : 32 文字）

[**検索**] ボタン - 検索結果を表示します。
[**ACL 追加**] ボタン - ACL プロファイルエントリを追加します。
[**編集**] ボタン - エントリの設定を編集します。
[**削除**] ボタン - ACL プロファイルのカウンタ情報を削除します。
[**ルールの設定**] 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 8-17 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。デフォルト値は 10 です。たとえば、増分（ステップ）値が 5、開始シーケンスナンバーが 20 である場合、それ以降のシーケンスナンバーは、25、30、35、40 のようになります。
注釈	この ACL に関連付けるオプションの注釈を入力します。

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

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

パラメータ	概要
ACL タイプ	作成する ACL タイプ（**Standard IP ACL**/**Extended IP ACL**/**Standard IPv6 ACL**/**Extended IPv6 ACL**/**Extended MAC ACL**/**Extended Expert ACL**）を選択します。
ID	ACL の ID を入力します。(設定範囲 : 1 - 1999)
ACL 名称	ACL の名前を入力します。（最大 : 32 文字）。

[**適用**] ボタン - ACL エントリを追加します。

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。

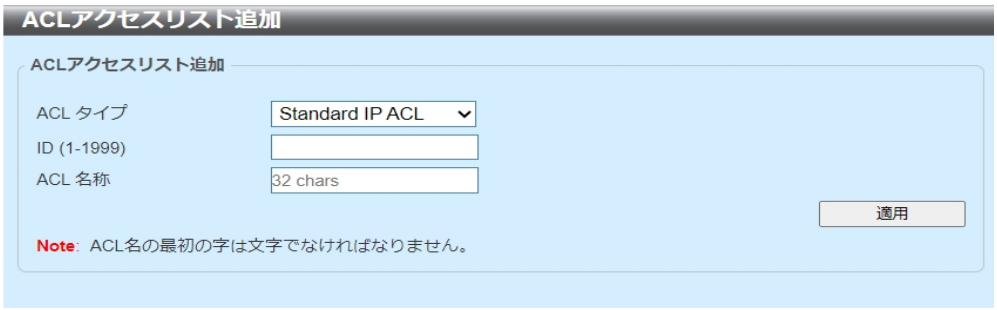

図 8-18 ACL アクセスリスト（ACL 追加、標準 IP ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

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

[**適用**] ボタン - ACL エントリを追加します。

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

図 8-19 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** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。

[**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 8-20 ACL アクセスリスト（ACL 追加、拡張 IP ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

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

[**適用**] ボタン - ACL エントリを追加します。

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

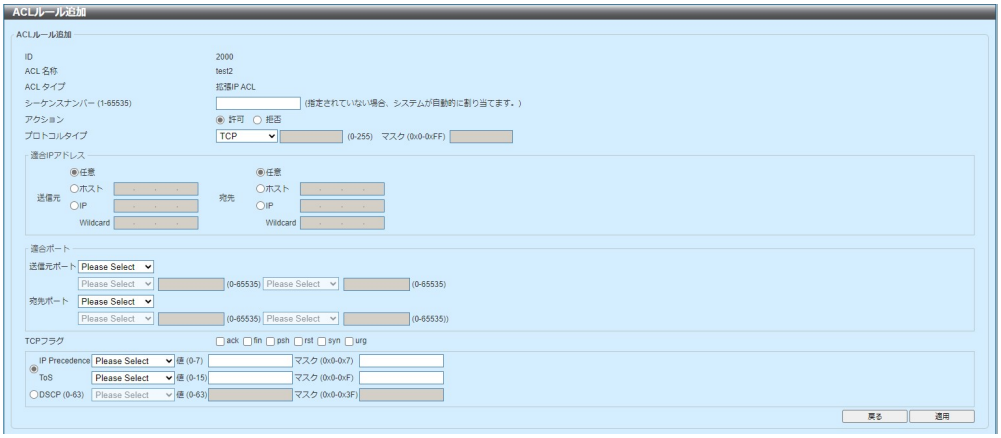

図 8-21 ACL アクセスリスト (ルール追加、拡張 IP ACL)

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** - 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。
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** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。

パラメータ	概要
送信元ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定）ソースポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。(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)
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)

[**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 8-22 ACL アクセスリスト（ACL 追加、標準 IPv6 ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

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

[**適用**] ボタン - ACL エントリを追加します。

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

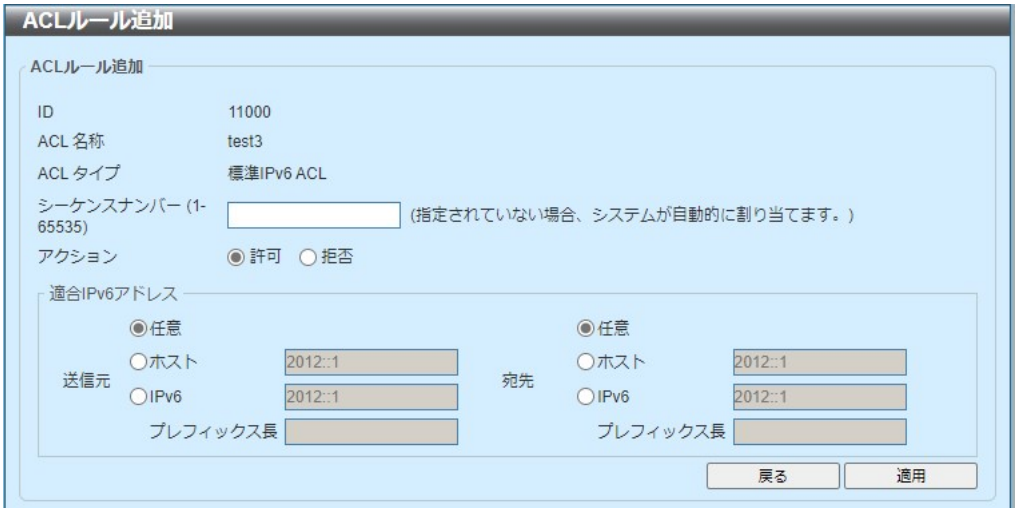

図 8-23 ACL アクセスリスト (ルール追加、標準 IPv6 ACL)

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。

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

8.2.4 拡張 IPv6 ACL

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

図 8-24 ACL アクセスリスト（ACL 追加、拡張 IPv6 ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

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

[**適用**] ボタン - ACL エントリを追加します。

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

図 8-25 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** - プロトコル ID を手動で入力できます。範囲は 0 ～ 255 です。 • **マスク** - **[Protocol ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。
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) • **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) • **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。範囲は 0 ～ 255 です。**[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。
メッセージコード	([プロトコルタイプ] で [ICMP] を選択した場合に設定） **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[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。
DSCP	使用する DSCP 値を選択します。選択する値は、**[default]**（0）、**[af11]**（10）、**[af12]**（12）、**[af13]**（14）、**[af21]**（18）、**[af22]**（20）、**[af23]**（22）、**[af31]**（26）、**[af32]**（28）、**[af33]**（30）、**[af41]**（34）、**[af42]**（36）、**[af43]**（38）、**[cs1]**（8）、**[cs2]**（16）、**[cs3]**（24）、**[cs4]**（32）、**[cs5]**（40）、**[cs6]**（48）、**[cs7]**（56）、**[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。範囲は 0 ～ 63 です。 • **マスク** - DSCP マスク値を入力します。範囲は 0x0 ～ 0x3F です。
トラフィッククラス	トラフィッククラス値を選択および入力します。範囲は 0 ～ 255 です。 • **マスク** - トラフィッククラスマスク値を入力します。範囲は 0x0 ～ 0xFF です。

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

8.2.5 拡張 MAC ACL

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

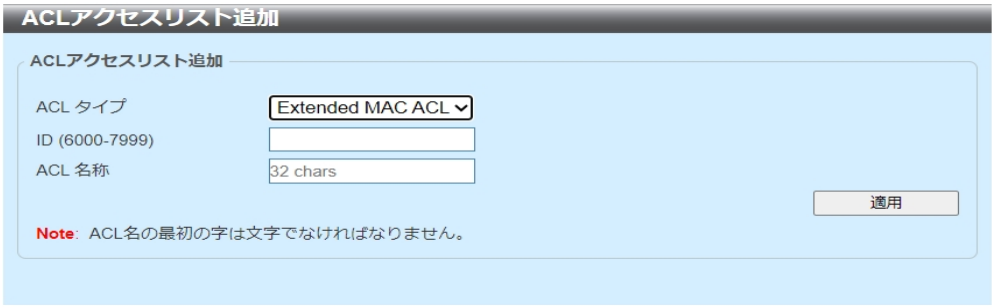

図 8-26 ACL アクセスリスト（ACL 追加、拡張 MAC ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

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

[**適用**] ボタン - ACL エントリを追加します。

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

図 8-27 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 **Wildcard** 値を表示された入力フィールドに入力します。
宛先	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
指定イーサタイプ	イーサネットタイプオプションを選択します。選択する値は、**[aarp]**、**[appletalk]**、**[decent-iv]**、**[etype-6000]**、**[etype-8042]**、**[lat]**、**[lavc-sca]**、**[mop-console]**、**[mop-dump]**、**[vines-echo]**、**[vines-ip]**、**[xns-idp]**、**[arp]** です。
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。 (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。範囲は 0 ～ 7 です。 • **マスク** - CoS マスク値を入力します。範囲は 0x0 ～ 0x7 です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 • **マスク** - VLAN ID マスク値を入力します。範囲は 0x0 ～ 0xFFF です。

[**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 8-28 ACL アクセスリスト（ACL 追加、Extended Expert ACL）

設定パラメータ （[ACL アクセスリスト追加] セクション）

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

[**適用**] ボタン - ACL エントリを追加します。

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

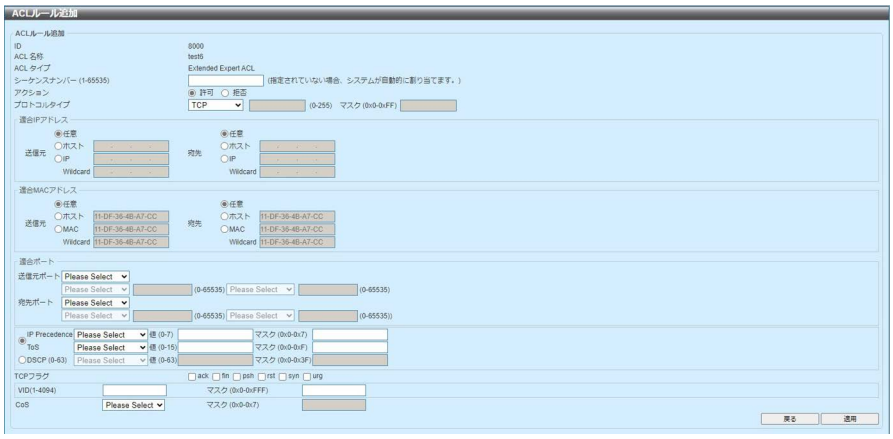

図 8-29 ACL アクセスリスト (ルール追加、Extended Expert ACL)

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** - プロトコル ID を手動で入力できます。範囲は 0 ～ 255 です。 • **マスク** - [**Protocol ID**] オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。
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** - **[Wildcard]** のビットマップを使用して、ソース IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
宛先（IP アドレス）	ディスティネーション情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
送信元（MAC アドレス）	ソース MAC アドレス情報を選択および入力します。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト MAC アドレスを入力します。 • **MAC** - ソース MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。

パラメータ	概要
宛先（MAC アドレス）	ディスティネーション MAC アドレス情報を選択および入力します。 • **任意** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト MAC アドレスを入力します。 • **MAC** - ディスティネーション MAC アドレスおよび **Wildcard** 値を表示された入力フィールドに入力します。
送信元ポート	([プロトコルタイプ] で [TCP]、[UDP] を選択した場合に設定) ソースポート値を選択および入力します。 • **=** - ACL は指定したポート番号のみ使用します。(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 です。) **[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。
メッセージコード	([プロトコルタイプ] で [ICMP] を選択した場合に設定) **[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[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。範囲は 0 ～ 7 です。 • **マスク** - IP Precedence マスク値を入力します。範囲は 0x0 ～ 0x7 です。
ToS	使用する ToS（Type-of-Service）値を選択します。選択する値は、**[normal]**（0）、**[min-monetary-cost]**（1）、**[max-reliability]**（2）、**[max-throughput]**（4）、**[min-delay]**（8）です。 • **値** - ToS 値を手動でも入力できます。範囲は 0 ～ 15 です。 • **マスク** - ToS マスク値を入力します。範囲は 0x0 ～ 0xF です。
DSCP	使用する DSCP 値を選択します。選択する値は、**[default]**（0）、**[af11]**（10）、**[af12]**（12）、**[af13]**（14）、**[af21]**（18）、**[af22]**（20）、**[af23]**（22）、**[af31]**（26）、**[af32]**（28）、**[af33]**（30）、**[af41]**（34）、**[af42]**（36）、**[af43]**（38）、**[cs1]**（8）、**[cs2]**（16）、**[cs3]**（24）、**[cs4]**（32）、**[cs5]**（40）、**[cs6]**（48）、**[cs7]**（56）、**[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。範囲は 0 ～ 63 です。 • **マスク** - DSCP マスク値を入力します。範囲は 0x0 ～ 0x3F です。
TCP フラグ	([プロトコルタイプ] で [TCP] を選択した場合に設定) この ACL で評価する TCP フラグを選択します。選択する値は、**[ack]**、**[fin]**、**[psh]**、**[rst]**、**[syn]**、**[urg]** です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 • **マスク** - VLAN ID マスク値を入力します。範囲は 0x0 ～ 0xFFF です。

パラメータ	概要
CoS	使用する CoS 値を選択します。範囲は 0 ～ 7 です。 • **マスク** - CoS マスク値を入力します。範囲は 0x0 ～ 0x7 です。

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

8.3 ACL インタフェースアクセスグループ

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

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

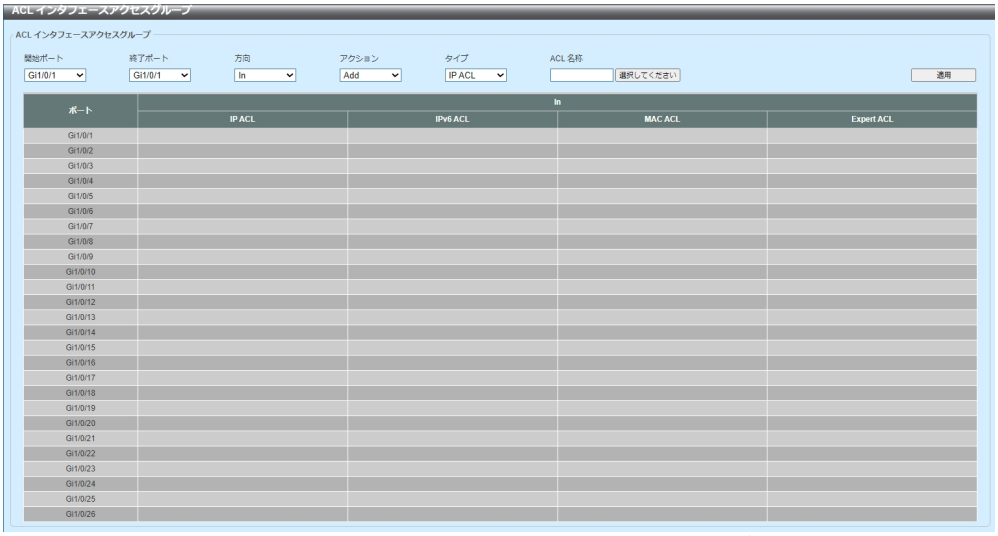

図 8-30 ACL インタフェースアクセスグループ

設定パラメータ （[ACL インタフェースアクセスグループ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
方向	方向（**In**）を選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	ACL タイプ（**IP ACL**/**IPv6 ACL**/**MAC ACL**/**Expert ACL**）を選択します。
ACL 名称	[**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 8-31 ACL インタフェースアクセスグループ（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。
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 8-32 ACL VLAN アクセスマップ

設定パラメータ （[ACL VLAN アクセスマップ] セクション）

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

[**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。
[**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 8-33 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	ここに、一致する IP アクセスリストが表示されます。
適合 IPv6 アクセスリスト	ここに、一致する IPv6 アクセスリストが表示されます。
適合 MAC アクセスリスト	ここに、一致する MAC アクセスリストが表示されます。

[**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。

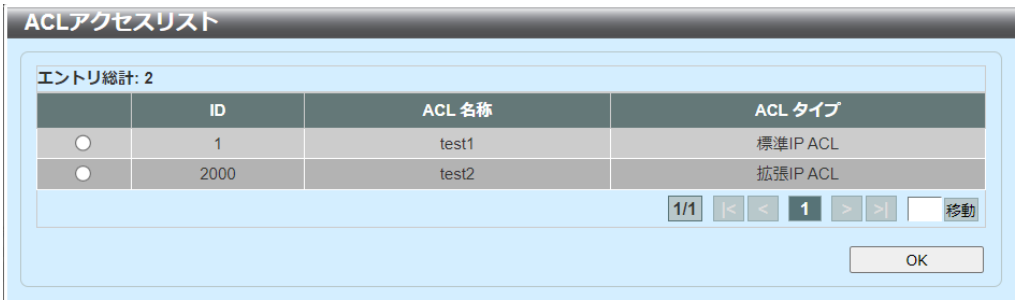

図 8-34 ACL VLAN アクセスマップ（バインディング , 選択してください）

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 8-35 ACL VLAN フィルタ

設定パラメータ （[ACL VLAN フィルタ] セクション）

パラメータ	概要
アクセスマップ名	アクセスマップ名を入力します。（最大：32 文字）
アクション	実行するアクション（**Add**/**Delete**）を選択します。
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。 [**全 VLAN 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。

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。

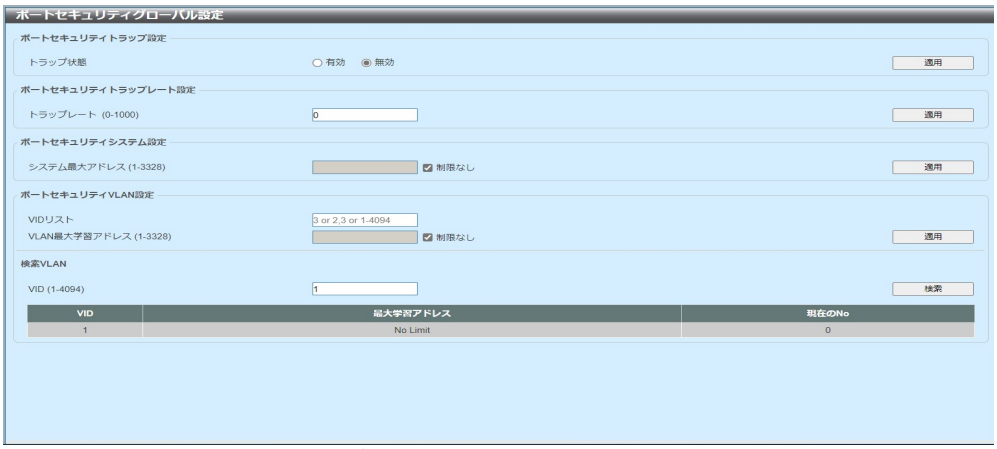

図 9-1 ポートセキュリティグローバル設定

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 トラップを有効または無効にする場合に選択します。デフォルト状態の場合、無効になります。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[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。 (デフォルト：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。 （デフォルト：制限なし、設定範囲：1-3328） **[制限なし]** を選択した場合、セキュアな MAC アドレスの最大数を許可します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ポートセキュリティ VLAN 設定] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）
VLAN 最大学習アドレス	指定した VLAN で学習可能な MAC アドレスの最大許可数を入力します。（設定範囲：1-3328） **[制限なし]** を選択した場合、セキュアな MAC アドレスの最大数を許可します。

[**適用**] ボタン - エントリを追加します。

[検索 VLAN] セクションでは、以下のパラメータを設定できます。

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

[**検索**] ボタン - 検索結果を表示します。

9.1.2 ポートセキュリティポート設定

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

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

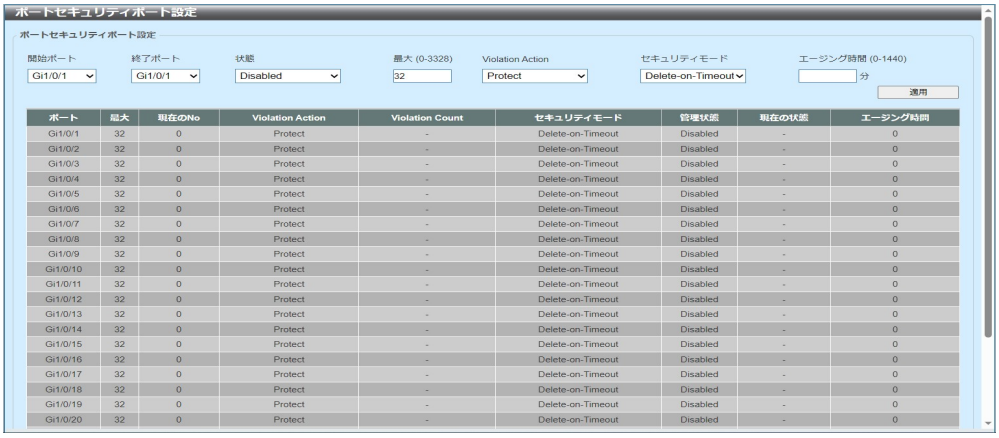

図 9-2 ポートセキュリティポート設定

設定パラメータ （[ポートセキュリティポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートのポートセキュリティ機能の (Enabled/Disabled) 設定します。
最大	指定したポートのセキュアな MAC アドレスの最大許可数を入力します。（デフォルト：32、設定範囲：0-3328）
Violation Action	実行する違反時アクションを選択します。 (デフォルト : 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。

パラメータ	概要
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。 (デフォルト : Delete - on - Timeout) • **Parmanent** - 学習されたすべての MAC アドレスは、ユーザがエントリを手動で削除した場合を除いて、クリアされません。 • **Delete-on-Timeout** - 学習されたすべての MAC アドレスは、エントリがエージアウトした場合、またはユーザがエントリを手動で削除した場合にクリアされます。
エージング時間	指定したポートで自動学習したセキュアなダイナミックアドレスに使用するエージング時間（分）を入力します。 (設定範囲：0-1440)

[**適用**] ボタン - 設定内容を反映します。

9.1.3 ポートセキュリティアドレスエントリ

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

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

図 9-3 ポートセキュリティアドレスエントリ

設定パラメータ （[ポートセキュリティアドレスエントリ] セクション）

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

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

9.2 802.1X

9.2.1 802.1X グローバル設定

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

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

図 9-4 802.1X グローバル設定

設定パラメータ （[802.1X グローバル設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[802.1X 認証ポート設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

9.2.2 802.1X 強制認証 MAC 設定

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

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

図 9-5 802.1X 強制認証 MAC 設定

設定パラメータ （[強制認証 MAC 設定] セクション）

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

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

9.2.3 802.1X 未認証 MAC 設定

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

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

図 9-6 802.1X 未認証 MAC 設定

設定パラメータ （[未認証 MAC アドレス設定] セクション）

パラメータ	概要
エージアウト時間	エージアウト時間値を入力します。この時間は、未認証のスタティックホストのエージアウトで使用します。 （設定範囲：0-65535, デフォルト：300）
ポート	ポートを選択します。
MAC アドレス	未認証ホストの MAC アドレスを入力します。
～で検索	• **MAC** - 未認証の設定済みダイナミックホストを検索します。 • **Port** - 指定したポートで未認証の設定済みダイナミックホストを検索します。

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

9.2.4 802.1X ポート設定

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

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

図 9-7 802.1X ポート設定（ポートベースアクセスコントロール）

設定パラメータ （[ポートベースアクセスコントロール] タブ）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
ポート制御	ポートの認証状態を選択します。 (デフォルト : 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。 (デフォルト : 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。 (設定範囲 : 1-65535, デフォルト : 60)
送信期間	送信期間を入力します。これは、スイッチがサプリカントからの EAP リクエスト /Identity フレームを待機する秒数です。この期間が経過すると、リクエストを再送信します。 (設定範囲 : 1-65535, デフォルト : 30)
サプリカントタイムアウト	サプリカントタイムアウト値を入力します。これは、サプリカントからの応答を待機する秒数です。この期間が経過すると、サプリカントメッセージがタイムアウトします。これは、EAP リクエスト ID には適用されません。 (設定範囲 : 1-65535, デフォルト : 30)

パラメータ	概要
サーバタイムアウト	サーバタイムアウト値を入力します。これは、認証サーバからの応答を待機する秒数です。この期間が経過すると、接続がタイムアウトします。 （設定範囲：1-65535, デフォルト：30）
再認証期間	再認証期間を入力します。これは、再認証試行間隔の秒数です。（設定範囲：1-65535, デフォルト：3600）
最大リクエスト	バックエンド認証マシンからの EAP リクエストの最大許可数を入力します。これを超過すると、認証プロセスがリスタートされます。（設定範囲：1-10, デフォルト：2）
ポート毎再認証	指定したポートの定期的な再認証の状態（**Enabled**/**Disabled**）を選択します。
再認証タイムローカル	タイマーによるセッション再認証におけるローカル設定の状態（**Enabled**/**Disabled**）を選択します。

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

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

図 9-8 802.1X ポート設定（MAC ベースアクセスコントロール）

設定パラメータ （[MAC ベースアクセスコントロール] タブ）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
サプリカント数	ポートの認証ユーザの最大許可数を入力します。 （設定範囲：1 - 384, デフォルト：384）
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。 (デフォルト : 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。 （設定範囲：1-65535, デフォルト：60）
送信期間	送信期間を入力します。これは、スイッチがサプリカントからの EAP リクエスト /Identity フレームを待機する秒数です。この期間が経過すると、リクエストを再送信します。 （設定範囲：1-65535, デフォルト：30）
サプリカントタイムアウト	サプリカントタイムアウト値を入力します。これは、サプリカントからの応答を待機する秒数です。この期間が経過すると、サプリカントメッセージがタイムアウトします。これは、EAP リクエスト ID には適用されません。 （設定範囲：1-65535, デフォルト：30）
サーバタイムアウト	サーバタイムアウト値を入力します。これは、認証サーバからの応答を待機する秒数です。この期間が経過すると、接続がタイムアウトします。 （設定範囲：1-65535, デフォルト：30）
再認証期間	再認証期間を入力します。これは、再認証試行間隔の秒数です。（設定範囲：1-65535, デフォルト：3600）

パラメータ	概要
最大リクエスト	バックエンド認証マシンからの EAP リクエストの最大許可数を入力します。これを超過すると、認証プロセスがリスタートされます。(設定範囲：1-10, デフォルト：2)
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。
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。
強制認証タイムアウト	強制認証タイムアウト値を入力します。これは、スイッチが強制認証 / 未認証への移行を待機する秒数です。この期間が経過すると、移行がタイムアウトします。移行がタイムアウトしないようにするには、0 を入力します。(設定範囲：0-65535, デフォルト：3600)

[**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
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。(デフォルト : 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。(デフォルト : 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
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。

9.3 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 9-12 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。 (デフォルト : 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。

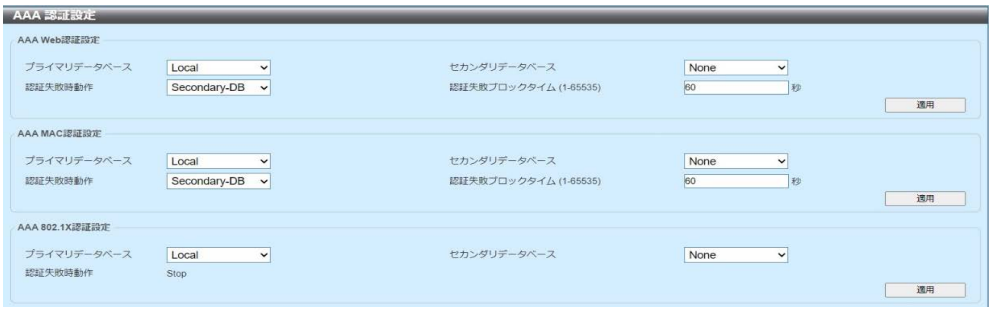

図 9-13 AAA 認証設定

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。(最大 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。 • **Local** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。 • **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。(最大 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。（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。(最大 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。 • **Local** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。 • **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。(最大 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。（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。(最大 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。 • **Local** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。

[**適用**] ボタン - 設定内容を反映します。

9.3.3 AAA 認証ユーザ設定

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

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

図 9-14 AAA 認証ユーザ設定

設定パラメータ （[AAA 認証ユーザ設定] セクション）

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

[**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、[**GO**] 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。

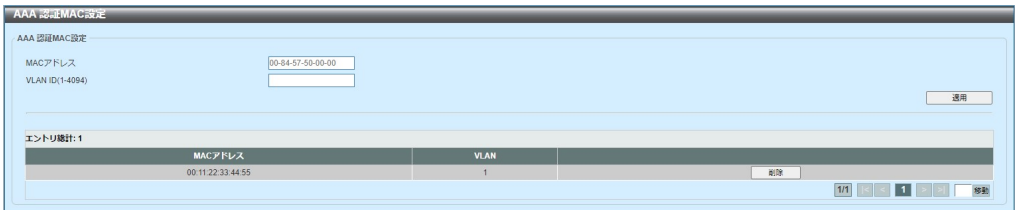

図 9-15 AAA 認証 MAC 設定

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）

[**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、[**GO**] 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。

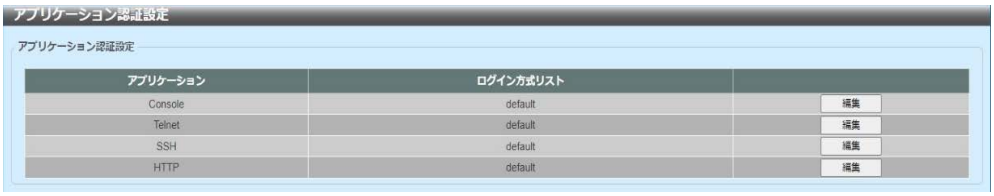

図 9-16 アプリケーション認証設定

[編集] クリックして、以下のウィンドウを表示します。

図 9-17 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 9-18 アプリケーションアカウンティング設定

図 9-19 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。 (最大: 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。 (最大 : 32 文字)

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

9.3.7 認証 EXEC の設定

このウィンドウを用いて、認証 EXEC の設定を行い、設定値を表示します。

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

図 9-20 認証 EXEC の設定

設定パラメータ （[AAA 認証有効] セクション）

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

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

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

9.3.8 アカウンティング設定

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

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

図 9-21 アカウンティング設定（AAA アカウンティングネットワーク）

設定パラメータ （[AAA アカウンティングネットワーク] タブ）

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

[**適用**] ボタン - 設定内容を反映します。

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

図 9-22 アカウンティング設定（AAA アカウンティングシステム）

設定パラメータ （[AAA アカウンティングシステム] タブ）

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

[**適用**] ボタン - 設定内容を反映します。

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

図 9-23 アカウンティング設定（AAA アカウンティング動作契機）

設定パラメータ （[AAA アカウンティング動作契機] タブ）

パラメータ	概要
リスト名	**[AAA アカウンティング動作契機]** オプションで使用する方式リスト名を入力します。(最大 : 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**/**RADIUS**）を選択します。 **[None]** オプションは、方式 1 でのみ利用可能です。

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

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

図 9-24 アカウンティング設定（AAA アカウンティングコマンド）

設定パラメータ （[AAA アカウンティングコマンド] タブ）

パラメータ	概要
レベル	使用する特権レベル（**1-15**）を選択します。
リスト名	**[AAA アカウンティングコマンド]** オプションで使用する方式リスト名を入力します。(最大 : 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**）を選択します。 **[None]** オプションは、方式 1 でのみ利用可能です。

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

9.4 認証

9.4.1 認証ダイナミック VLAN 設定

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

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

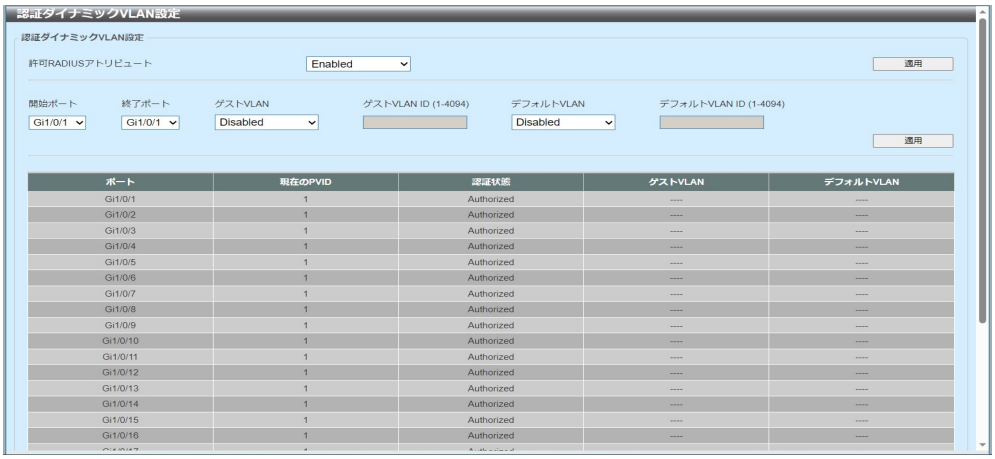

図 9-25 認証ダイナミック VLAN 設定

設定パラメータ （[認証ダイナミック VLAN 設定] セクション）

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

[**適用**] ボタン - 設定内容を反映します。

9.4.2 認証状態テーブル

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

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

図 9-26 認証状態テーブル

設定パラメータ （[認証状態テーブル] セクション）

パラメータ	概要
認証エージングタイム	MAC/WEB 認証セッションのタイムアウト値を入力します。 （設定範囲：0-65535, デフォルト：1440）
Sort By	• MAC - 認証セッションを MAC アドレス順に表示します。 • Port - 指定したポートの認証セッションを表示します。

[**適用**] ボタン - 設定内容を反映します。
[**検索**] ボタン - 検索結果を表示します。
[**削除**] ボタン - 認証済みホストを削除します。

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。

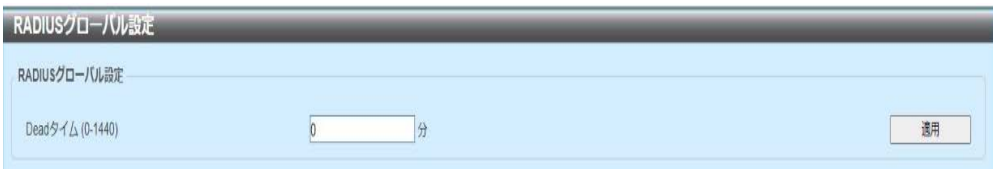

図 9-27 RADIUS グローバル設定

設定パラメータ （[RADIUS グローバル設定] セクション）

パラメータ	概要
Dead タイム	Dead タイム値を入力します。システムが認証サーバを使用して認証を実行する場合、サーバを 1 つずつ試行します。試行したサーバが応答しない場合は次のサーバを試行します。システムは、応答しないサーバを見つけると、そのサーバをダウンとしてマークして、Dead 時間タイマーを開始します。この状態のサーバは、Dead 時間が経過するまで、それ以降のリクエストの認証ではスキップされます。 このオプションが 0 の場合、応答しないサーバは Dead としてマークされません。この設定を用いて、応答しないサーバホストエントリをスキップする Dead タイムを設定することによって、認証処理時間を短縮できます。 （デフォルト：0、設定範囲：0-1440）

[**適用**] ボタン - 設定内容を反映します。

9.5.2 RADIUS サーバ設定

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

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

図 9-28 RADIUS サーバ設定

設定パラメータ （[RADIUS サーバ設定] セクション）

パラメータ	概要
IP アドレス	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 アドレス	RADIUS サーバの IPv6 アドレスを入力します。
認証ポート	使用する認証ポート番号を入力します。 認証を使用しない場合は、値 0 を使用します。 （デフォルト：1812、設定範囲：0 - 65535）
アカウンティングポート	使用するアカウンティングポート番号を入力します。 アカウンティングを使用しない場合は、値 0 を使用します。 （デフォルト：1813、設定範囲：0 - 65535）
再送信	再送信回数の値を入力します。 このオプションを無効にするには、値 0 を入力します。 （デフォルト：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。 （デフォルト：5、設定範囲：1 - 255）
キータイプ	使用するキータイプ（**Plain Text**/**Encrypted**）を選択します。
キー	RADIUS サーバとの通信に使用するキーを入力します。 （最大：32 文字）

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

9.5.3 RADIUS グループサーバ設定

このウィンドウを用いて、RADIUS グループサーバの設定を行い、設定値を表示します。

[セキュリティ] > [RADIUS] > [RADIUS グループサーバ設定] をクリックして、以下のウィンドウを表示します。
(注意) デフォルトで「radius」は設定されています。

図 9-29 RADIUS グループサーバ設定

設定パラメータ （[RADIUS グループサーバ設定] セクション）

パラメータ	概要
グループサーバ名	RADIUS グループサーバ名を入力します。名前は 32 文字までです。
IP アドレス	RADIUS グループサーバの IPv4 アドレスを入力します。
IPv6 アドレス	RADIUS グループサーバの IPv6 アドレスを入力します。

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

[**詳細参照**] をクリックして、以下のウィンドウを表示します。

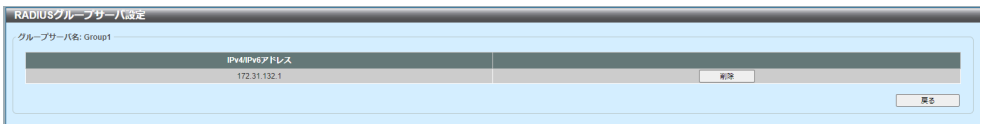

図 9-30 RADIUS グループサーバ設定 (詳細参照)

[**削除**] ボタン - エントリを削除します。
[**戻る**] ボタン - 前のウィンドウに戻ります。

9.5.4 RADIUS 統計

このウィンドウを用いて、RADIUS 統計情報を表示およびクリアします。

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

図 9-31 RADIUS 統計

設定パラメータ （[RADIUS 統計] セクション）

パラメータ	概要
グループサーバ名	このリストから RADIUS グループサーバ名を選択します。

[**クリア**] ボタン - 統計情報をクリアします。
[**全クリア**] ボタン - すべての統計情報をクリアします。

9.6 SAVI（Source Address Validation Improvements）

9.6.1 IPv4

9.6.1.1 DHCPv4 スヌーピング

9.6.1.1.1 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 9-32 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。(デフォルト : 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。(デフォルト : 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。(デフォルト : 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。(デフォルト : 無効)

パラメータ	概要
DHCP OPTION82 付与 **（注意）**	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、DHCP メッセージを転送する際、Option 82 付与の状態 (有効 / 無効) を選択します。 （デフォルト：無効） • **有効** - DHCP メッセージを送信する際、Option82 を挿入します。 • **無効** - DHCP メッセージを送信する際、Option82 を挿入しません。
リモート ID フォーマット	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、DHCP メッセージに Option 82 付与する際のリモート ID フォーマットを選択します。 （デフォルト：Default） • **Default** - スイッチングハブの MAC アドレスを設定します。 • **User Define** - ユーザーが指定した文字列を設定します。 • **None** - リモート ID を設定しません。
Circuit ID 付与 **（注意）**	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、DHCP メッセージを転送する際、Option 82 Circuit ID 付与の状態 (有効 / 無効) を選択します。 （デフォルト：有効） • **有効** - DHCP メッセージを送信する際、Option 82 の Circuit ID を挿入します。 • **無効** - DHCP メッセージを送信する際、Option 82 の Circuit ID を挿入しません。
DHCP OPTION82 **ポリシー** **（注意）**	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、Option 82 付与された DHCP メッセージを転送する際のポリシーを選択します。 （デフォルト：Replace） • **Drop** - Option 82 が付与されているパケットを破棄します。 • **Keep** - Option 82 が付与されているパケットを Option 82 の内容を変更せず、転送します。 • **Replace** - Option 82 が付与されているパケットの Option 82 の内容を変更し、送信します。

パラメータ	概要
DHCP OPTION82 リプライ確認（注意）	DHCP スヌーピング実行中に DHCP サーバーからの DHCP クライアントに対して、DHCP メッセージを転送する際、DHCP メッセージに付与されている Option 82 の情報（リモート ID）を確認する状態を選択します。 (デフォルト：無効) • **有効 -** DHCP メッセージに付与されている Option 82 の情報が一致した場合、Option 82 のみを削除して送信します。Option 82 の情報が一致しない場合、DHCP メッセージを Drop します。 • **無効 -** DHCP メッセージに付与されている Option 82 の内容を変更せず、転送します。

(注意)DHCP OPTION82 VLAN 設定で設定したパラメータを優先します。

[**適用**] ボタン - 設定内容を反映します。

9.6.1.1.2 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。

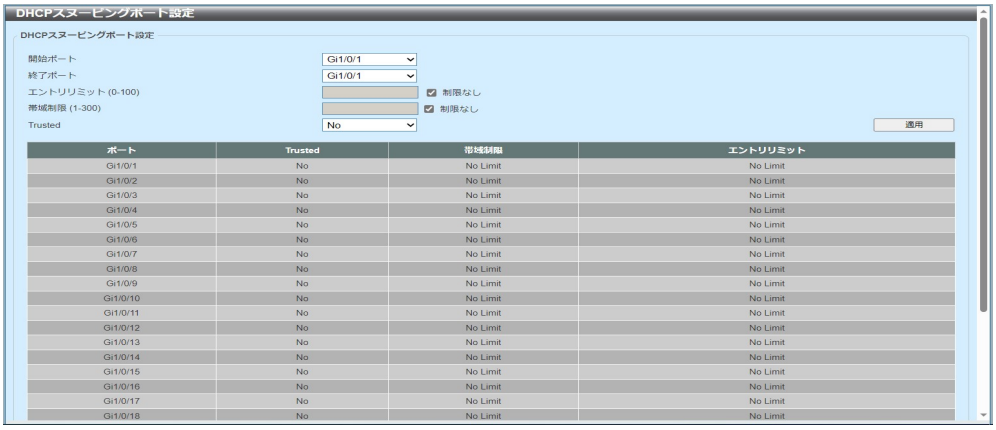

図 9-33 DHCP スヌーピングポート設定

設定パラメータ （[DHCP スヌーピングポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
エントリリミット	エントリリミット値を入力します。（設定範囲：0-100） **[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。(デフォルト：制限なし)
帯域制限	帯域制限値を入力します。（設定範囲：1-300（pps）） **[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。(デフォルト：制限なし)
Trusted	Trusted オプション（**Yes**/**No**）を選択します。 (デフォルト：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。

9.6.1.1.3 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 9-34 DHCP スヌーピング VLAN 設定

設定パラメータ （[DHCP スヌーピング VLAN 設定] セクション）

パラメータ	概要
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）
状態	DHCP スヌーピング VLAN の状態（**Enabled**/**Disabled**）を選択します。

[**適用**] ボタン - 設定内容を反映します。

9.6.1.1.4 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 9-35 DHCP スヌーピングデータベース

設定パラメータ （[DHCP スヌーピングデータベース] セクション）

パラメータ	概要
書込み遅延	書込み遅延時間を入力します。 （デフォルト：300 秒、設定範囲：60-86400 秒）

[**リセット**] ボタン - DHCP スヌーピングデータベースをリセットします。
[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[DHCP スヌーピングデータベースの保存] セクション）

パラメータ	概要
URL	ドロップダウンリストから場所（**TFTP**/**FTP**）を選択して、DHCP スヌーピングデータベースを保存する URL を入力します。

[**リセット**] ボタン - DHCP スヌーピングデータベースをリセットします。
[**適用**] ボタン - DHCP スヌーピングデータベースを保存します。

設定パラメータ （[DHCP スヌーピングデータベースの読み込み] セクション）

パラメータ	概要
URL	ドロップダウンリストから場所（**TFTP**/**FTP**）を選択して、DHCP スヌーピングデータベースを読み込む URL を入力します。

[**適用**] ボタン - DHCP スヌーピングデータベースを読み込みます。
[**クリア**] ボタン - カウンタ情報をクリアします。

9.6.1.1.5 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。

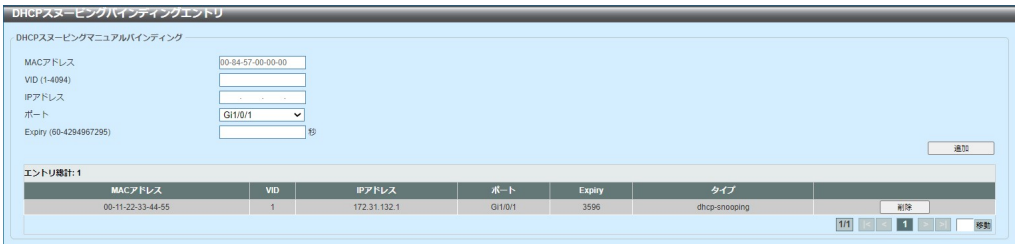

図 9-36 DHCP スヌーピングバインディングエントリ

設定パラメータ （[DHCP スヌーピングマニュアルバインディング] セクション）

パラメータ	概要
MAC アドレス	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
IP アドレス	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
ポート	ポートを選択します。
Expiry	使用する有効期限値（秒）を入力します。 （設定範囲：60-4294967295）

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

9.6.1.1.6 DHCP OPTION82 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 OPTION82 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 OPTION82 VLAN 設定] をクリックして、以下のウィンドウを表示します。

図 9-37 DHCP OPTION82 VLAN 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。

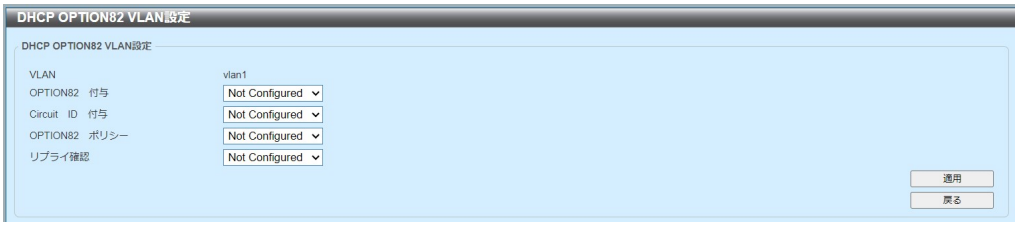

図 9-38 DHCP OPTION82 VLAN 設定 (編集)

設定パラメータ （[DHCP OPTION82 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）
OPTION82 付与	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、DHCP メッセージを転送する際、Option 82 付与の状態 (Not Configured/Disabled/Enabled) を選択します。（デフォルト：Not Configured） • **Not Configured** - DHCP スヌーピンググローバル設定で選択されたパラメータを参照します。 • **Disabled** - DHCP メッセージを送信する際、Option82 を挿入しません。 • **Enabled** - DHCP メッセージを送信する際、Option82 を挿入します。

パラメータ	概要
Circuit ID 付与	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、DHCP メッセージを転送する際、Option 82 Circuit ID 付与の状態 (Not Configured/Disabled/ Enabled) を選択します。(デフォルト：Not Configured) • **Not Configured** - DHCP スヌーピンググローバル設定で選択されたパラメータを参照します。 • **Disabled** - DHCP メッセージを送信する際、Option 82 の Circuit ID を挿入しません。 • **Enabled** - DHCP メッセージを送信する際、Option 82 の Circuit ID を挿入します。
OPTION82 ポリシー	DHCP スヌーピング実行中に DHCP クライアントから DHCP サーバーに対する、Option 82 付与された DHCP メッセージを転送する際のポリシーを選択します。(デフォルト：Not Configured) • **Not Configured** - DHCP スヌーピンググローバル設定で選択されたパラメータを参照します。 • **Drop** - Option 82 が付与されているパケットを破棄します。 • **Keep** - Option 82 が付与されているパケットを Option 82 の内容を変更せず、転送します。 • **Replace** - Option 82 が付与されているパケットの Option 82 の内容を変更し、送信します。
リプライ確認	DHCP スヌーピング実行中に DHCP サーバーからの DHCP クライアントに対して、DHCP メッセージを転送する際、DHCP メッセージに付与されている Option 82 の情報（リモート ID）を確認する状態を選択します。 (デフォルト：Not Configured) • **Not Configured** - DHCP スヌーピンググローバル設定で選択されたパラメータを参照します。 • **Disabled** - DHCP メッセージを転送する際、DHCP メッセージに付与されている Option 82 の情報を確認しません。DHCP メッセージに付与されている Option 82 の内容を変更せず、転送します。 • **Enabled** - DHCP メッセージを送信する際、DHCP メッセージに付与されている Option 82 の情報を確認します。DHCP メッセージに付与されている Option 82 の情報が一致した場合、Option 82 のみを削除して送信します。Option 82 の情報が一致しない場合、DHCP メッセージを Drop 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。

9.6.1.2 ダイナミック ARP 検査

9.6.1.2.1 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。

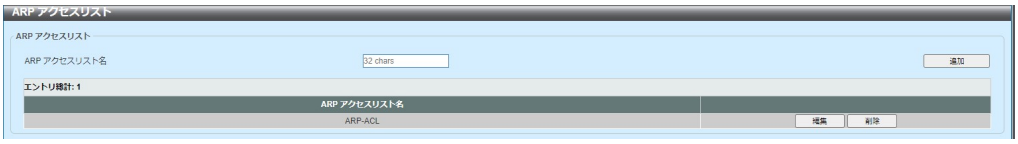

図 9-39 ARP アクセスリスト

設定パラメータ （[ARP アクセスリスト] セクション）

パラメータ	概要
ARP アクセスリスト名	使用する ARP アクセスリスト名を入力します。 (最大 : 32 文字)

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

[**編集**] をクリックして、以下のウィンドウを表示します。

図 9-40 ARP 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
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。

9.6.1.2.2 ARP 検査設定

このウィンドウを用いて、ダイナミック ARP 検査の設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [ダイナミック ARP 検査] > [ARP 検査設定] をクリックして、以下のウィンドウを表示します。

図 9-41 ARP 検査設定

設定パラメータ （[ARP 検査項目] セクション）

パラメータ	概要
ソース MAC	ソース MAC オプションの状態（**有効** / **無効**）を選択します。ARP リクエスト / 応答パケットをチェックして、イーサネットヘッダのソース MAC アドレスが ARP ペイロードのセンダー MAC アドレスと一致していることをチェックします。(デフォルト : 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。(デフォルト : 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。(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 （[ARP 検査 VLAN ログ収集] セクション）

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

[**適用**] ボタン - 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

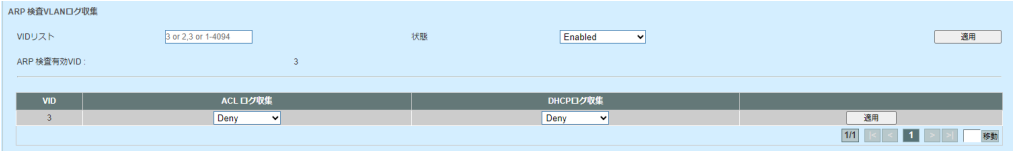

図 9-42 ARP 検査 VLAN ログ収集 (編集)

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を選択します。選択できるオプションは、[Deny]、[Permit]、[All]、[None] です。
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を選択します。選択できるオプションは、[Deny]、[Permit]、[All]、[None] です。

[**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。（最大：32 文字）
VID リスト	使用する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。（設定範囲：1-4094）

パラメータ	概要
スタティック **ACL**	スタティック ACL（Yes/No）を使用を選択します。

[**追加**] ボタン - エントリを追加します。
[**削除**] ボタン - エントリを削除します。
ページ番号を入力し、[**GO**] ボタンをクリックすると特定のページに移動します。

9.6.1.2.3 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。

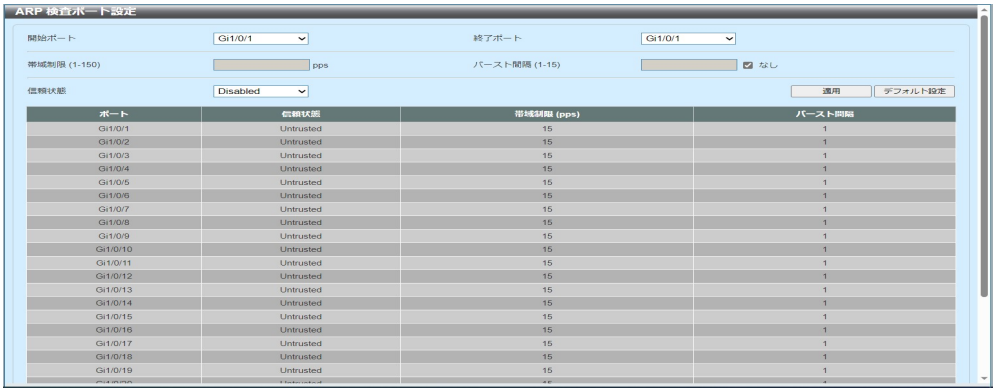

図 9-43 ARP 検査ポート設定

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
帯域制限	帯域制限値（pps）を入力します。**[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。 （選択範囲：1-150, デフォルト：15）
バースト間隔	バースト間隔値を入力します。（設定範囲：1-15） **[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。(デフォルト : 1)
信頼状態	信頼状態（**Enabled**/**Disabled**）を選択します。 (デフォルト : 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 - 信頼状態をデフォルト設定に設定します。

9.6.1.2.4 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 9-44 ARP 検査統計情報

設定パラメータ

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

[**VLAN 単位クリア**] ボタン - 指定した VLAN に関する統計情報をクリアします。
[**全クリア**] ボタン - すべての統計情報をクリアします。

9.6.1.2.5　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 9-45 ARP 検査ログ

設定パラメータ （[ARP 検査ログ] セクション）

パラメータ	概要
ログバッファ	ログバッファのサイズを入力します。 （デフォルト：32、選択範囲：1-1024） **[デフォルト]** オプションを選択した場合、デフォルト値を使用します。

[**適用**] ボタン - 設定内容を反映します。
[**ログクリア**] ボタン - ARP 検査ログをクリアします。

9.6.1.3 IP ソースガード

9.6.1.3.1 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 9-46 IP ソースガードポート設定

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの IP ソースガードの状態（**Enabled**/**Disabled**）を選択します。
検証	使用する検証方法を選択します。 • **IP** - 受信したパケットの IP アドレスをチェックします。 • **IP-MAC** - 受信したパケットの IP アドレスと MAC アドレスをチェックします。

[**適用**] ボタン - エントリを追加します。

9.6.1.3.2 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 9-47 IP ソースガードバインディング

設定パラメータ （[IP ソースバインディング設定] セクション）

パラメータ	概要
MAC アドレス	バインディングエントリの MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
IP アドレス	バインディングエントリの IP アドレスを入力します。
開始ポート／終了ポート	ポートを選択します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[IP ソースバインディングエントリ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
IP アドレス	バインディングエントリの IP アドレスを入力します。
MAC アドレス	バインディングエントリの MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。（設定範囲：1-4094）
タイプ	検索するバインディングエントリのタイプを選択します。 • **All** - すべての DHCP バインディングエントリを表示します。 • **DHCP-Snooping** - DHCP バインディングスヌーピングによって学習された IP ソースガードバインディングエントリを表示します。 • **Static** - 手動で設定された IP ソースガードバインディングエントリを表示します。

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

9.6.1.3.3 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 9-48 IP ソースガード HW エントリ

設定パラメータ

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。

9.7 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。

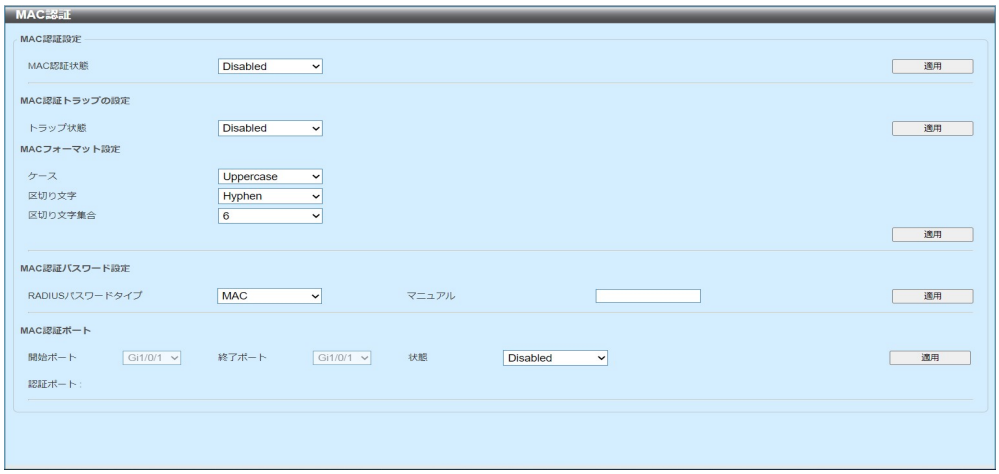

図 9-49 MAC 認証

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。(デフォルト : 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。(デフォルト : 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。たとえば、AA-BB-CC-DD-EE-FF となります。 • **Lowercase** - MAC アドレスに小文字形式を使用します。たとえば、aa-bb-cc-dd-ee-ff となります。
区切り文字	MAC アドレスで使用する区切り文字のタイプを選択します。 • **Hyphen** - MAC アドレスで区切り文字としてハイフンを使用します。たとえば、AA-BB-CC-DD-EE-FF となります。 • **Colon** - MAC アドレスで区切り文字としてコロンを使用します。たとえば、AA：BB：CC：DD：EE：FF となります。 • **Dot** - MAC アドレスで区切り文字としてドットを使用します。たとえば、AA.BB.CC.DD.EE.FF となります。 • **None** - MAC アドレスで区切り文字を使用しません。たとえば、AABBCCDDEEFF となります。
区切り文字集合	MAC アドレスで使用する区切り文字の数を選択します。 • **2** - MAC アドレスで区切り文字を 1 つ使用します。たとえば、AABBCC-DDEEFF となります。 • **4** - MAC アドレスで区切り文字を 2 つ使用します。たとえば、AABB-CCDD-EEFF となります。 • **6** - MAC アドレスで区切り文字を 5 つ使用します。たとえば、AA-BB-CC-DD-EE-FF となります。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC 認証パスワード設定] セクション）

パラメータ	概要
RADIUS パスワードタイプ	RADIUS パスワードタイプを選択します。 (デフォルト : MAC) • **MAC** - RADIUS パスワードとして MAC アドレスを使用します。 • **Manual** - RADIUS パスワードとしてマニュアル文字列を使用します。
マニュアル	MAC 認証アカウントの RADIUS パスワードを入力します。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[MAC 認証ポート] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの MAC 認証 (Enabled/Disabled) を設定します。(デフォルト : Disabled)

[**適用**] ボタン - 設定内容を反映します。

9.8 WEB 認証

9.8.1 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 9-50 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。(デフォルト : 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
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。(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 （[認証設定] セクション）

パラメータ	概要
仮想 IP	使用する仮想 IPv4 アドレスを入力します。すべての WEB 認証プロセスはこの仮想 IP アドレスと通信しますが、ICMP パケットまたは ARP リクエストに対してこの仮想 IP が応答することはありません。仮想 IPv4 アドレスとスイッチの IPv4 アドレスは、別々のサブネットを使用する必要があります。仮想 IPv4 アドレスは、WEB 認証の正常動作に欠かせないコンポーネントです。
HTTP ポート番号	HTTP TCP/UDP ポート番号を入力します。 （デフォルト：80、設定範囲：1-65535）
リダイレクト **URL**	リダイレクト URL を入力します。（最大：64 文字）

[**適用**] ボタン - 設定内容を反映します。

9.8.2 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。

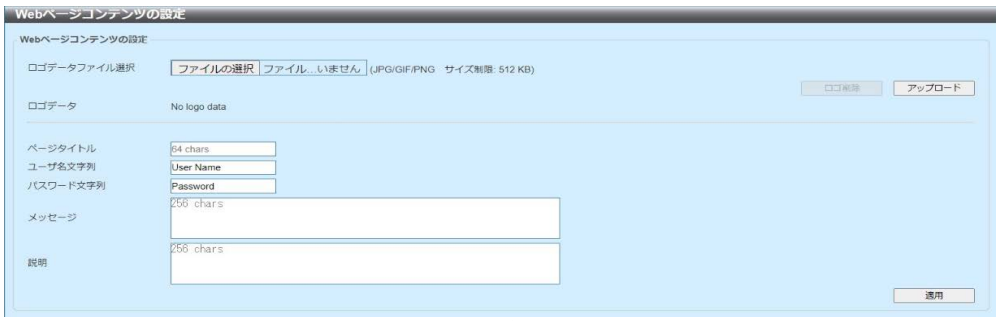

図 9-51 WEB ページコンテンツの設定

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）がある場所に移動します。
ロゴデータ	アップロードされているイメージファイル（使用中）が表示されます。512KB まで転送可能です。 **[ロゴ削除]** ボタンをクリックして、既存のイメージファイルを削除します。
ページタイトル	カスタムのページタイトルメッセージを入力します。 日本語入力が可能です。（最大：64 文字）
ユーザ名文字列	カスタムのユーザ名タイトルを入力します。 日本語入力が可能です。（最大：32 文字）
パスワード文字列	カスタムのパスワードタイトルを入力します。 日本語入力が可能です。（最大：32 文字）
メッセージ	カスタムのメッセージを入力します。（最大：256 文字） 日本語入力および以下の HTML タグが使用可能です。 以下の <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p>
説明	カスタムの説明メッセージを入力します。（最大：256 文字） 日本語入力および以下の HTML タグが使用可能です。 以下の <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p>

[アップロード] ボタン - 新しいロゴをアップロードします。

[**適用**] ボタン - 設定内容を反映します。
[**ロゴ削除**] ボタン - 既存の画像ファイルを削除します。

9.8.3 一時 DHCP サーバ設定

このウィンドウを用いて、一時 DHCP サーバ設定を行います。

[セキュリティ] > [WEB 認証] > [一時 DHCP サーバ設定] をクリックして、以下のウィンドウを表示します。

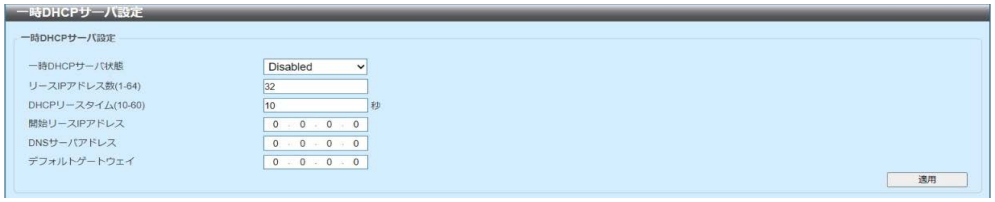

図 9-52 一時 DHCP サーバ設定

設定パラメータ （[一時 DHCP サーバ設定] セクション）

パラメータ	概要
一時 DHCP サーバ状態	一時利用 DHCP サーバの状態（**Enabled**/**Disabled**）を選択します。(デフォルト : Disabled)
リース IP アドレス数	リースする IP アドレス数を入力します。 （デフォルト：32、設定範囲：1-64）
DHCP リースタイム	IP アドレスのリース時間 （ 秒 ）を入力します。 （設定範囲：10-60, デフォルト：10）
開始リース IP アドレス	リースする IP アドレスの開始アドレスを入力します。
DNS サーバアドレス	DHCP で通知する DNS サーバアドレスの値を入力します。
デフォルトゲートウェイ	DHCP で通知するデフォルトゲートウェイアドレスの値を入力します。

[**適用**] ボタン - 設定内容を反映します。

9.9 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。

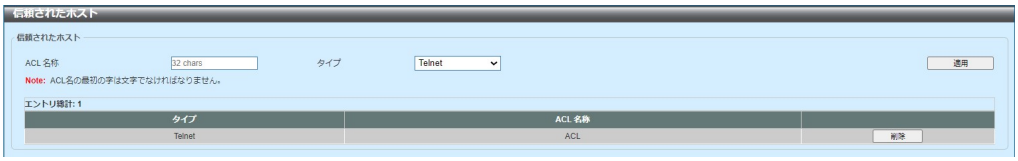

図 9-53 信頼されたホスト

設定パラメータ （[信頼されたホスト] セクション）

パラメータ	概要
ACL 名称	ACL の名前を入力します。（最大：32 文字）
タイプ	信頼されたホストのタイプ（**Telnet**/**SSH**/**Ping**/**HTTP**/**HTTPS**）を選択します。

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

9.10 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。

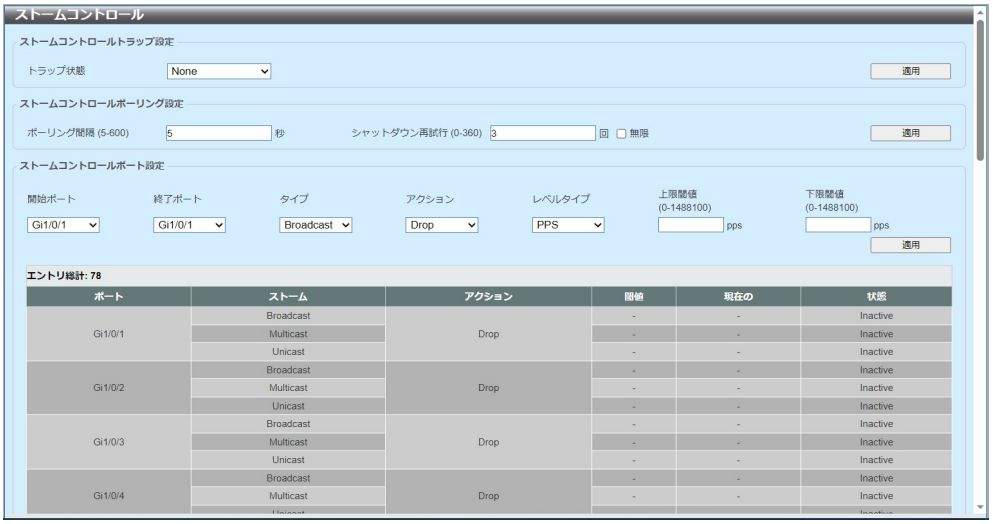

図 9-54 ストームコントロール（レベルタイプ、PPS）

設定パラメータ （[ストームコントロールトラップ設定] 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。(デフォルト : None) • **None** - トラップ状態を無効にするように指定します。 • **Storm Occur** - ストームイベントが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出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。 （デフォルト：5、設定範囲：5-600）
シャットダウン再試行	シャットダウン再試行回数の値を入力します。 （デフォルト：3、設定範囲：0-360） **[無限]** オプションをオンにした場合、この機能を無効にします。

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[ストームコントロールポート設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
タイプ	制御するストームアタックのタイプ（**Broadcast**/**Multicast**/**unicast**）を選択します。 **[アクション]** として **[Shutdown]** が設定されている場合、ユニキャストは、既知と未知の両方のユニキャストパケットを指します。すなわち、既知と未知のユニキャストパケット数が指定した閾値に達すると、ポートをシャットダウンします。それ以外の場合は、ユニキャストは未知のユニキャストパケットを指します。
アクション	実行するアクションを選択します。(デフォルト : 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。
レベルタイプ	レベルタイプオプション（**PPS**）を選択します。
上限閾値	PPS Rise 値を入力します。このオプションは、1 秒あたりのパケットカウントの上限レートを指定します。範囲は、1 秒あたり 0 ～ 1488100 パケットです。[下限閾値] の値を指定しない場合、指定した上限閾値の 80% の値がデフォルト値になります。
下限閾値	PPS Low 値を入力します。このオプションは、1 秒あたりのパケットカウントの下限レートを指定します。範囲は、1 秒あたり 0 ～ 1488100 パケットです。[下限閾値] の値を指定しない場合、指定した上限閾値の 80% の値がデフォルト値になります。

[**適用**] ボタン - 設定内容を反映します。

9.11 SSH（Secure Shell）

9.11.1 SSH グローバル設定

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

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

図 9-55 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。(デフォルト : 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。（デフォルト：22、設定範囲：1-65535）
認証タイムアウト	認証タイムアウト値を入力します。（デフォルト：120、設定範囲：30-600）
認証リトライ数	認証リトライ回数の値を入力します。（デフォルト：3、設定範囲：1-32）

[**適用**] ボタン - 設定内容を反映します。

9.11.2 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 9-56 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。

9.11.3 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 9-57 SSH サーバコネクション

9.11.4 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 9-58 SSH ユーザ設定

設定パラメータ （[SSH ユーザ設定] セクション）

パラメータ	概要
ユーザ名	SSH ユーザアカウントのユーザ名を入力します。 （最大：32 文字）
認証方式	SSH 認証方式（**Password**/**Public Key**/**Host-based**）を選択します。
キーファイル	（[認証方式] パラメータで [Public Key] または [Host-based] 選択時の設定可） 選択した場合に公開鍵を入力します。（最大：779 文字）
ホスト名	（[認証方式] パラメータで [Host-based] 選択時の設定可） ホスト名を入力します。（最大：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。

9.12 SSL（Secure Sockets Layer）

9.12.1 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 9-59 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。 (デフォルト : 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。（最大 : 32 文字）

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[インポートファイル] セクション）

パラメータ	概要
ファイル選択	アップロードするファイルタイプ（**証明書** / **プライベートキー**）を選択します。ファイルタイプを選択した後、**[ファイルの選択]** 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。（最大 : 32 文字）

[**適用**] ボタン - SSL ファイルをインポートします。

9.12.2 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 9-60 暗号化 PKI トラストポイント

設定パラメータ （[暗号化 PKI トラストポイント] セクション）

パラメータ	概要
トラストポイント	インポートした証明書とキーペアに関連付けるトラストポイントの名前を入力します。（最大：32 文字）
ファイルシステムパス	証明書とキーペアのファイルシステムパスを入力します。
パスワード	プライベートキーをインポートしたときに暗号化を解除するために使用する、暗号化されたパスワードフレーズを入力します。パスワードフレーズを指定しない場合、NULL 文字列を使用します。（最大：64 文字）
TFTP サーバパス	TFTP サーバパスを入力します。
タイプ	インポートする証明書のタイプを選択します。 • **Both** - CA（Certificate Authority）証明書と、ローカル証明書およびキーペアをインポートします。 • **CA** - CA 証明書のみをインポートします。 • **Local** - ローカル証明書とキーペアのみをインポートします。
概要	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割り当てます。このトラストポイントは、アプリケーションがどの認証 (CA) トラストポイントを明示的に指定していない場合、デフォルトのトラストポイント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。

9.12.3 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。

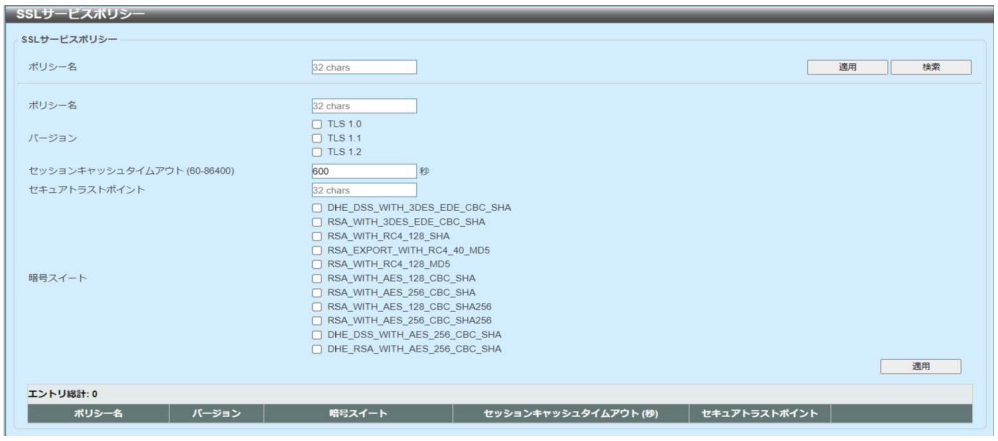

図 9-61 SSL サービスポリシー

[SSL サービスポリシー] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ポリシー名	SSL サービスポリシー名を入力します。（最大：32 文字）
バージョン	TLS のバージョン（**TLS1.0**/**TLS1.1**/**TLS1.2**）を選択します。
セッションキャッシュタイムアウト	セッションキャッシュのタイムアウト値（秒）を入力します。（デフォルト：600、設定範囲：60 - 86400）
セキュアトラストポイント	セキュアトラストポイント名を入力します。（最大：32 文字）
暗号スイート	このプロファイルに関連付ける暗号スイートを選択します。

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

9.13 ポートグループ設定

このウィンドウは、ポートグループ設定を行うために使用します。ポートグループは、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 9-62 ポートグループ設定

[ポートグループ設定] 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
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。(最大 :16 文字)
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 9-63 ポートグループ設定 (編集)

[ポートグループ設定] 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
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。

[適用] ボタン - エントリを追加します。

9.14 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。

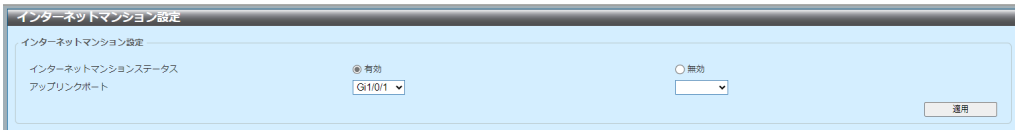

図 9-64 インターネットマンション設定

[インターネットマンション設定] 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
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) にする場合に選択します。 (デフォルト : 無効)
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。

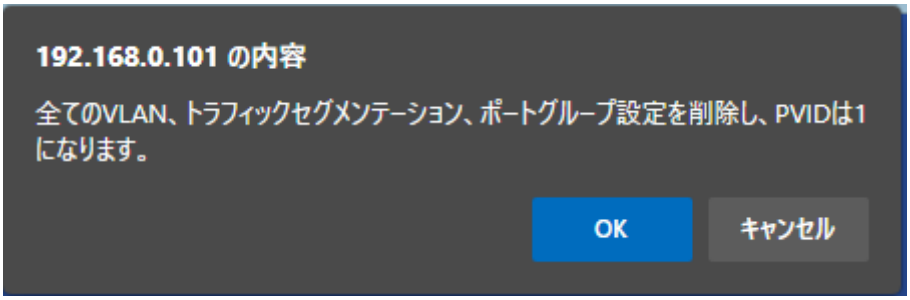

図 9-65 インターネットマンション設定 (確認プロンプト)

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
開始ポート／終了ポート	ポートを選択します。

[テスト] ボタン - ケーブル診断テストを開始します。
[全クリア] ボタン - すべてのケーブル診断結果をクリアします。
[クリア] ボタン - ケーブル診断結果をクリアします。

10.2 DDM（Digital Diagnostic Monitoring）

10.2.1 DDM 設定

このウィンドウを用いて、DDM 機能に関連付けられているグローバル設定および指定したポートの DDM シャットダウンの設定を行い、設定値を表示します。

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

図 10-2 DDM 設定

設定パラメータ （[DDM グローバル設定] セクション）

パラメータ	概要
トランシーバモニタリングトラップアラーム	トランシーバモニタリングアラームトラップ送信の状態（**有効** / **無効**）を選択します。(デフォルト：無効)
トランシーバモニタリングトラップ警告	トランシーバモニタリング警告トラップ送信の状態（**有効** / **無効**）を選択します。(デフォルト：無効)

[**適用**] ボタン - 設定内容を反映します。

設定パラメータ （[DDM シャットダウン設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	指定したポートの DDM の状態（**Enabled**/**Disabled**）を選択します。(デフォルト：Enabled)
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** - 設定されている警告閾値範囲を超えた場合にポートをシャットダウンします。 • **None** - 閾値範囲を超えたかどうかに関係なく、ポートをシャットダウンしません。これはデフォルトオプションです。

[**適用**] ボタン - 設定内容を反映します。

10.2.2 DDM 温度閾値設定

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

[DDM] > [DDM 温度閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-3 DDM 温度閾値設定

設定パラメータ （[DDM 温度閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	温度閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
値	閾値（摂氏）を入力します。（設定範囲：-128-127.996）

[**適用**] ボタン - 設定内容を反映します。

10.2.3 DDM 電圧閾値設定

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

[DDM] > [DDM 電圧閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-4 DDM 電圧閾値設定

設定パラメータ （[DDM 電圧閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	電圧閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
値	閾値（V）を入力します。（設定範囲：0-6.55）

[**適用**] ボタン - 設定内容を反映します。

10.2.4 DDM バイアス電流閾値設定

このウィンドウを用いて、指定したポートの DDM バイアス電流閾値の設定を行い、設定値を表示します。

[DDM] > [DDM バイアス電流閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-5 DDM バイアス電流閾値設定

設定パラメータ （[DDM バイアス電流閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	バイアス電流閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
値	閾値（mA）を入力します。（設定範囲：0-131）

[**適用**] ボタン - 設定内容を反映します。

10.2.5 DDM 送信パワー閾値設定

このウィンドウを用いて、指定したポートの DDM 送信パワー閾値の設定を行い、設定値を表示します。

[DDM] > [DDM 送信パワー閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-6 DDM 送信パワー閾値設定

設定パラメータ （[DDM 送信パワー閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	送信パワー閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
パワー単位	電力単位（**mW**/**dBm**）を選択します。
値	閾値（mW/dBm）を入力します。 • パワー単位が mW の場合 - （設定範囲：0-6.5535） • パワー単位が dBm の場合 - （設定範囲：-40-8.1647）

[**適用**] ボタン - 設定内容を反映します。

10.2.6 DDM 受信パワー閾値設定

このウィンドウを用いて、指定したポートの DDM 受信パワー閾値の設定を行い、設定値を表示します。

[DDM] > [DDM 受信パワー閾値設定] をクリックして、以下のウィンドウを表示します。

図 10-7 DDM 受信パワー閾値設定

設定パラメータ （[DDM 受信パワー閾値設定] セクション）

パラメータ	概要
ポート	ポートを選択します。
アクション	実行するアクション（**Add**/**Delete**）を選択します。
タイプ	受信パワー閾値のタイプ（**Low Alarm**/**Low Warning**/**High Alarm**/**High Warning**）を選択します。
パワー単位	電力単位（**mW**/**dBm**）を選択します。
値	閾値（mW/dBm）を入力します。 • パワー単位が mW の場合 - （設定範囲：0-6.5535） • パワー単位が dBm の場合 - （設定範囲：-40-8.1647）

[**適用**] ボタン - 設定内容を反映します。

10.2.7 DDM 状態テーブル

このウィンドウを用いて、DDM 状態テーブルと情報を表示します。

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

図 10-8 DDM 状態テーブル

11 モニタリング

11.1 使用率

11.1.1 ポート使用率

このウィンドウを用いて、ポート使用率テーブルと情報を表示します。

[モニタリング] > [使用率] > [ポート使用率] をクリックして、以下のウィンドウを表示します。

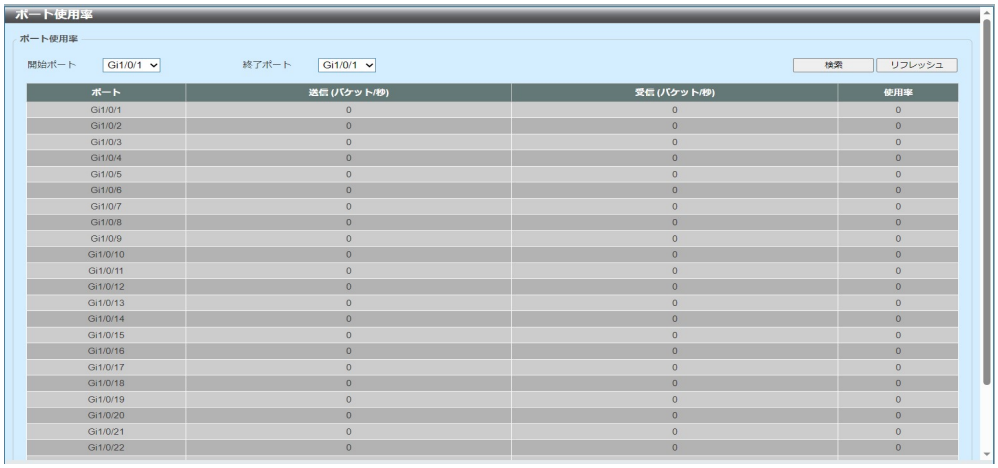

図 11-1 ポート使用率

設定パラメータ （[ポート使用率] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**リフレッシュ**] ボタン - テーブルに表示されている情報をリフレッシュします。

11.2 統計

11.2.1 ポート

このウィンドウを用いて、ポートの受信 / 送信統計と情報を表示します。

[モニタリング] > [統計] > [ポート] をクリックして、以下のウィンドウを表示します。

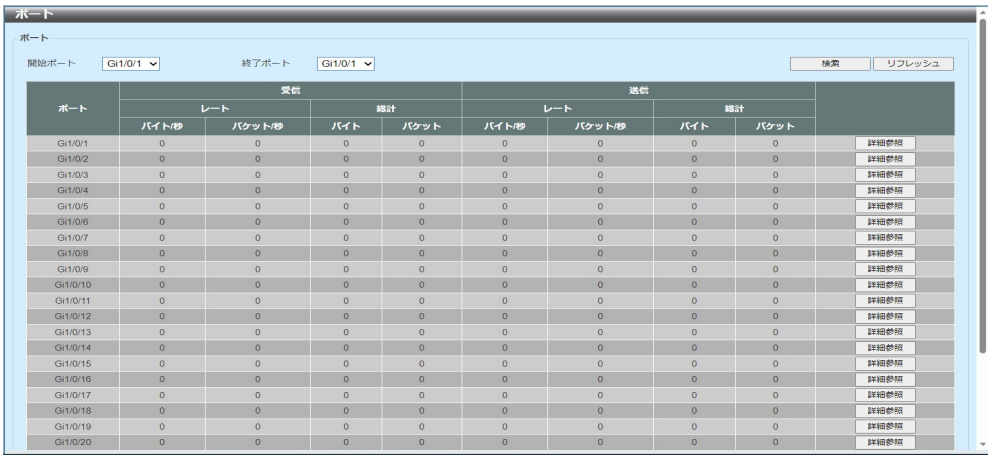

図 11-2 ポート

設定パラメータ （[ポート] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**リフレッシュ**] ボタン - テーブルに表示されている情報をリフレッシュします。
[**詳細参照**] ボタン - エントリの詳細情報を表示します。

[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。

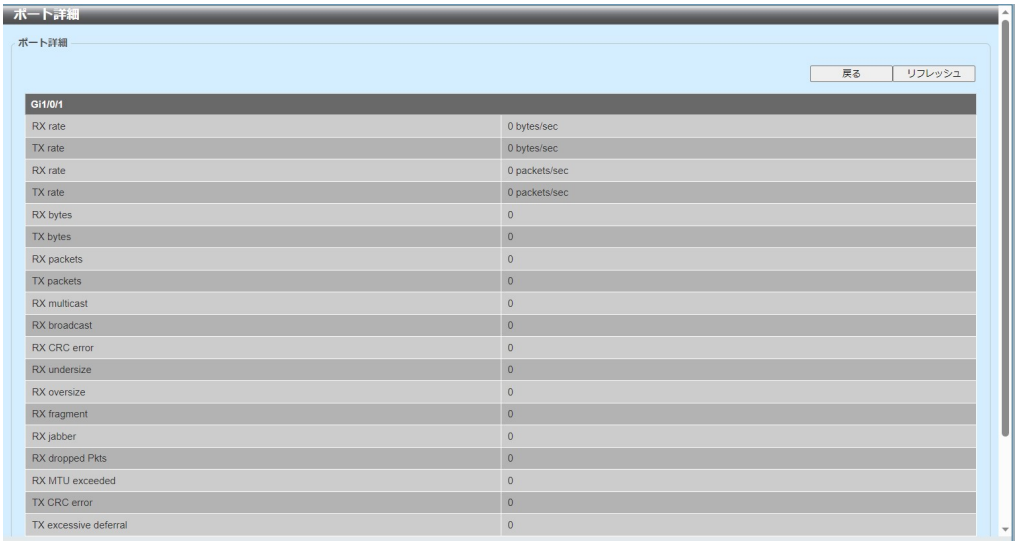

図 11-3 ポート (詳細参照)

[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 インタフェースカウンタ

このウィンドウを用いて、インタフェースカウンタ統計と情報を表示します。

[モニタリング] > [統計] > [インタフェースカウンタ] をクリックして、以下のウィンドウを表示します。

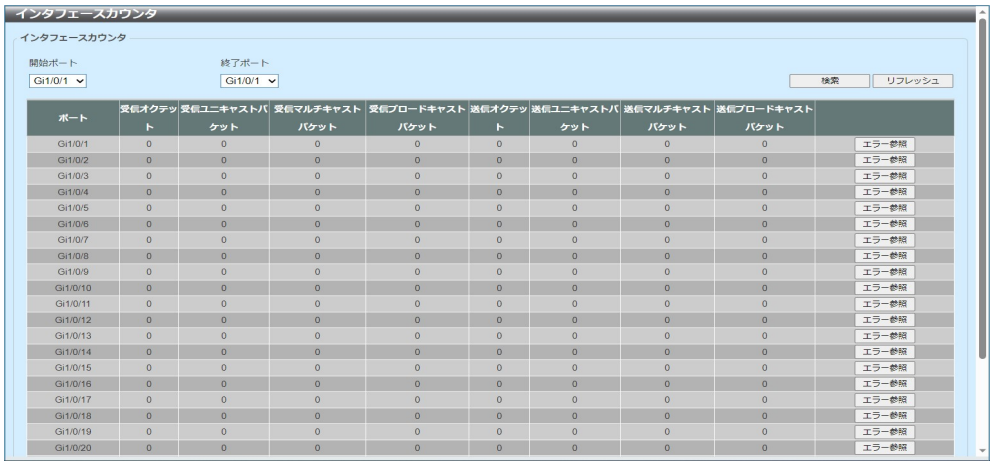

図 11-4 インタフェースカウンタ

設定パラメータ （[インタフェースカウンタ] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。

[**検索**] ボタン - 検索結果を表示します。
[**リフレッシュ**] ボタン - テーブルに表示されている情報をリフレッシュします。
[**エラー参照**] ボタン - 詳細エラー情報を表示します。

[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。

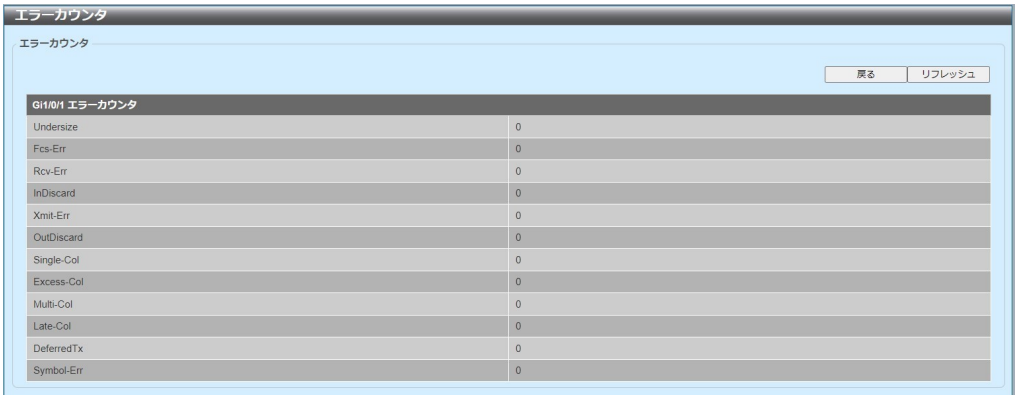

図 11-5 インタフェースカウンタ（エラー参照）

[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。

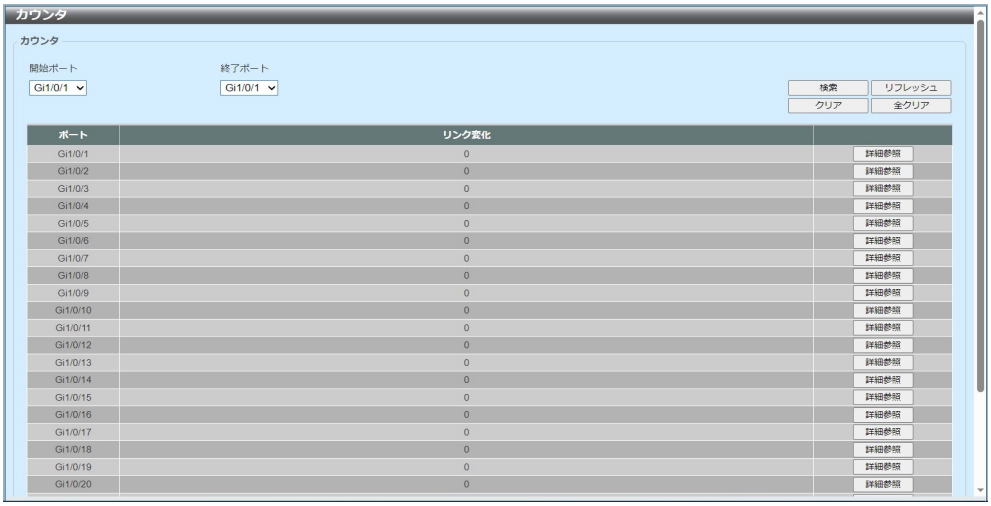

図 11-6 カウンタ

設定パラメータ （[カウンタ] セクション）

パラメータ	概要
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。

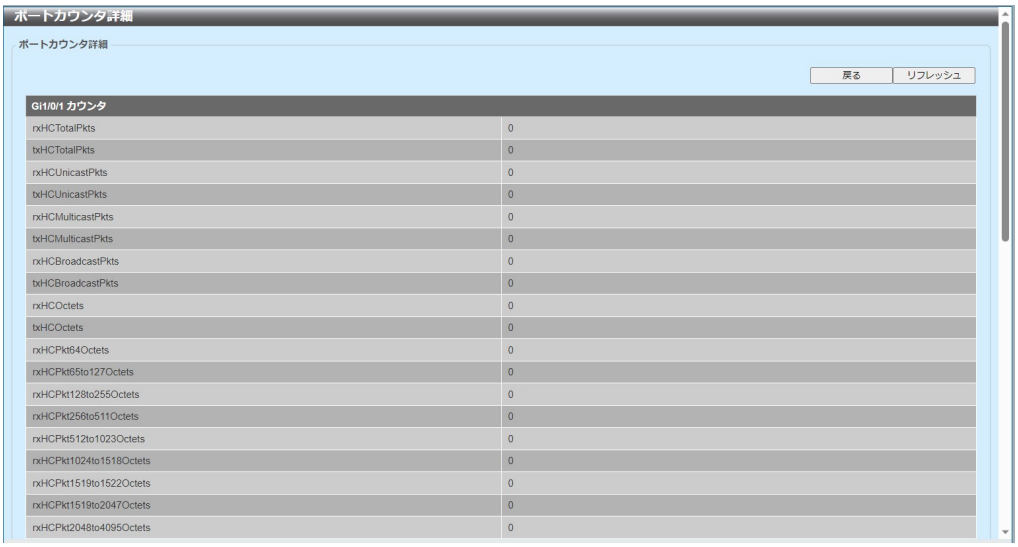

図 11-7 カウンタ (詳細参照)

[**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 （[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** ～ **2**）を選択します。
ディスティネーション	ポートミラーエントリのディスティネーション設定を選択および設定します。
ソース	([ソース] パラメータで [Port] 選択時に設定可) • **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。

[**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**）を選択します。 **[Session Number]** を選択した場合は、ドロップダウンからセッションナンバーを選択します。

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

[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。

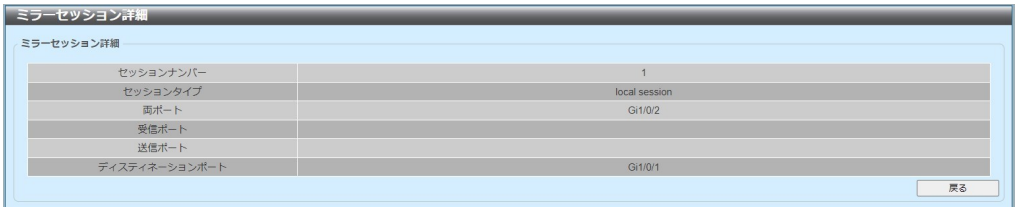

図 11-9 ミラー設定 (詳細参照)

[**戻る**] ボタン - 前のウィンドウに戻ります。

11.4 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。
(注意)GA-EM48T のみ、詳細 FAN 状態と詳細温度状態が表示されます。

[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 11-10 デバイス (GA-EM48T 以外の機種の場合)

図 11-11 デバイス (GA-EM48T の場合)

12 ECO モード

12.1 省電力

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

[ECO モード] > [省電力] をクリックして、以下のウィンドウを表示します。

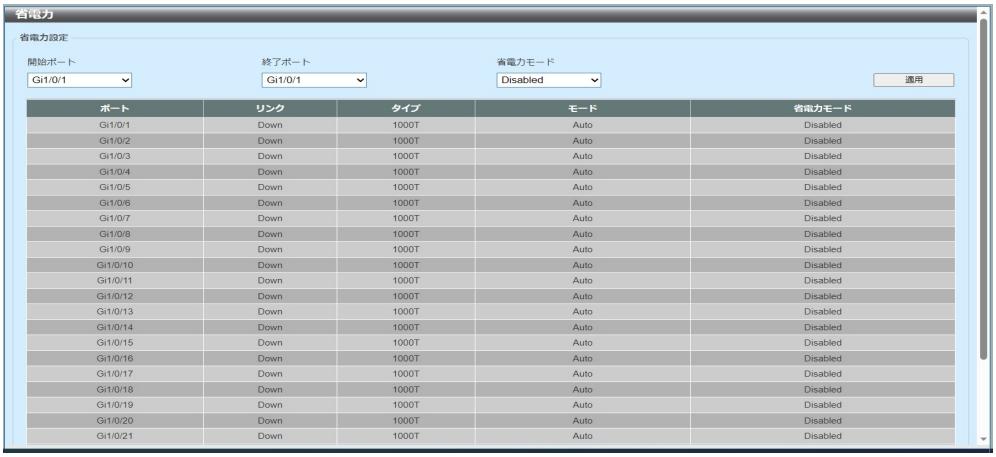

図 12-1 省電力

設定パラメータ （[省電力設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
省電力モード	指定したポートで使用する省電力モードを選択します。 (デフォルト : 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** - 省電力機能の能力を半分だけ使用します。これは、通常は、まったく使用しない場合と最大限に使用する場合の間であればすべて該当します。

[**適用**] ボタン - 設定内容を反映します。

12.2 EEE（Energy Efficient Ethernet）

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

[ECO モード] > [EEE] をクリックして、以下のウィンドウを表示します。

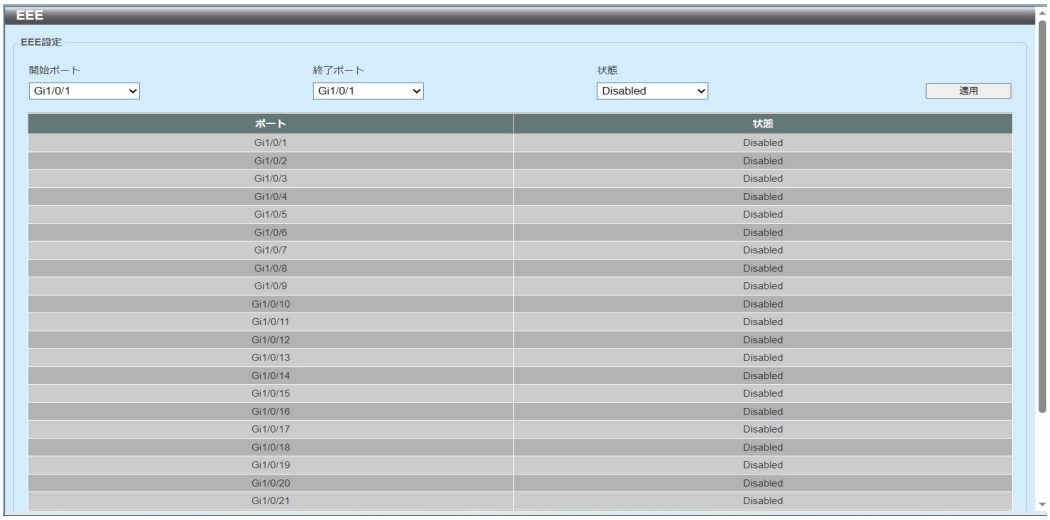

図 12-2 EEE

設定パラメータ （[EEE 設定] セクション）

パラメータ	概要
開始ポート／終了ポート	ポートを選択します。
状態	EEE の状態（**Enabled**/**Disabled**）を選択します。 (デフォルト : Disabled)

[**適用**] ボタン - 設定内容を反映します。

13 ツールバー

13.1 保存

13.1.1 コンフィグ保存

このウィンドウを用いて、実行中のコンフィグレーションをスタートアップコンフィグレーションとして保存します。これにより、電源故障時にコンフィグレーションが失われないようにします。

ツールバー >[保存] > [コンフィグ保存] をクリックして、以下のウィンドウを表示します。

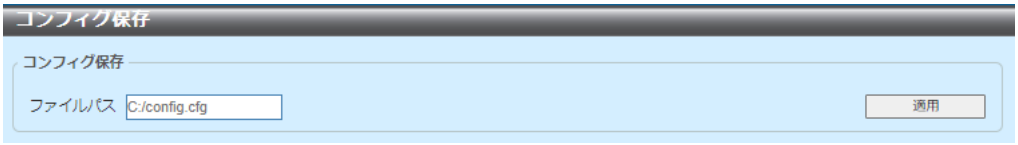

図 13-1 コンフィグ保存

設定パラメータ （[コンフィグ保存] セクション）

パラメータ	概要
ファイルパス	ファイル名とパスを表示された入力フィールドに入力します。

[**適用**] ボタン - コンフィグレーションを保存します。

13.2 ツール

13.2.1 ファームウェアアップグレード

13.2.1.1 HTTP サーバからファームウェアアップグレード

このウィンドウを用いて、ローカル PC から HTTP を使用してスイッチのファームウェアをアップグレードします。

(注意)[実行しました] と表示されましたら、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。

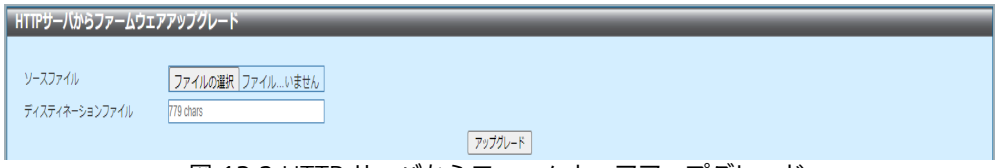

図 13-2 HTTP サーバからファームウェアアップグレード

設定パラメータ

パラメータ	概要
ソースファイル	**[ファイルの選択]** ボタンをクリックして、このアップグレードで使用するファームウェアファイル（ローカル PC 上）がある場所に移動します。
ディスティネーション ファイル	新しいファームウェアを保存するスイッチ上のディスティネーションパスと場所を入力します。(最大：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。

13.2.1.2 TFTP サーバからファームウェアアップグレード

このウィンドウを用いて、TFTP サーバからスイッチのファームウェアをアップグレードします。

(注意)[実行しました] と表示されましたら、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。

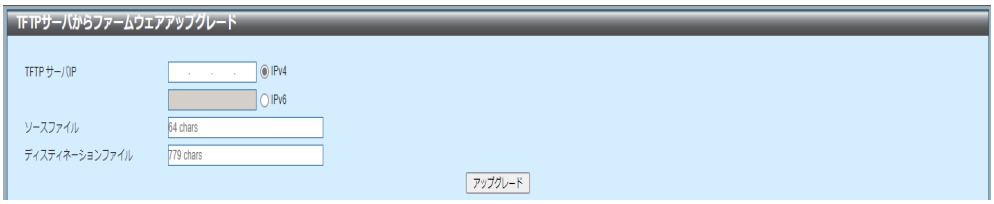

図 13-3 TFTP サーバからファームウェアアップグレード

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	TFTP サーバにあるファームウェアファイルのソースファイル名とパスを入力します。(最大 : 64 文字)
ディスティネーションファイル	新しいファームウェアを保存するスイッチ上のディスティネーションパスと場所を入力します。(最大 : 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。

13.2.2 コンフィグレーション復旧&バックアップ

13.2.2.1 HTTP サーバからコンフィグレーション復旧

このウィンドウを用いて、ローカル PC から HTTP を使用してスイッチにコンフィグレーションを復旧します。

ツールバー >[ツール] > [コンフィグレーション復旧&バックアップ] > [HTTP サーバからコンフィグレーション復旧] をクリックして、以下のウィンドウを表示します。

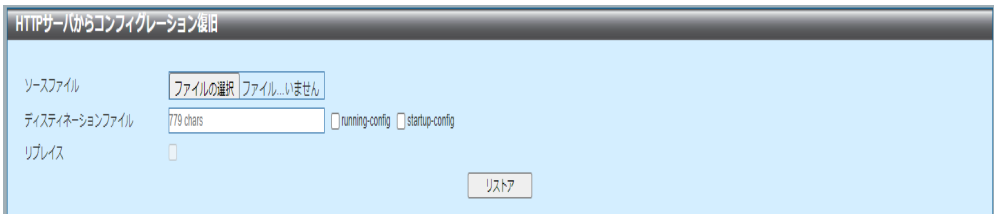

図 13-4 HTTP サーバからコンフィグレーション復旧

設定パラメータ

パラメータ	概要
ソースファイル	**[ファイルの選択]** ボタンをクリックして、この復旧で使用するコンフィグレーションファイル（ローカル PC 上）がある場所に移動します。
ディスティネーションファイル	コンフィグレーションファイルを保存するスイッチ上のディスティネーションパスと場所を入力します。 (最大：779 文字) • **running-config** - スイッチ上の実行中のコンフィグレーションファイルを復旧して上書きします。 • **startup-config** - スイッチ上のスタートアップコンフィグレーションファイルを復旧して上書きします。
リプレイス	このオプションを選択した場合、スイッチ上のコンフィグレーションファイルをこのファイルでリプレイスします。

[リストア] ボタン - リストアを開始します。

13.2.2.2 TFTP サーバからコンフィグレーション復旧

このウィンドウを用いて、TFTP サーバからスイッチのコンフィグレーションを復旧します。

ツールバーで **[ツール] > [コンフィグレーション復旧＆バックアップ] > [TFTP サーバからコンフィグレーション復旧]** をクリックして、以下のウィンドウを表示します。

図 13-5 TFTP サーバからコンフィグレーション復旧

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	TFTP サーバにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大：64 文字)
ディスティネーションファイル	コンフィグレーションファイルを保存するスイッチ上のディスティネーションパスと場所を入力します。 (最大：779 文字) • **running-config** - スイッチ上の実行中のコンフィグレーションファイルを復旧して上書きします。 • **startup-config** - オプションを選択した場合、スイッチ上のスタートアップコンフィグレーションファイルを復旧して上書きします。
リプレイス	このオプションを選択した場合、スイッチ上のコンフィグレーションファイルをこのファイルでリプレイスします。

[リストア]ボタン - リストアを開始します。

13.2.2.3 HTTP サーバへコンフィグレーションをバックアップ

このウィンドウを用いて、スイッチのコンフィグレーションのバックアップコピーを HTTP を使用してローカル PC に保存します。

ツールバーで **[ツール] > [コンフィグレーション復旧＆バックアップ] > [HTTP サーバへコンフィグレーションをバックアップ]** をクリックして、以下のウィンドウを表示します。

図 13-6 HTTP サーバへコンフィグレーションをバックアップ

設定パラメータ

パラメータ	概要
ソースファイル	スイッチにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大：64 文字) • **running-config** - スイッチから実行中のコンフィグレーションファイルをバックアップします。 • **startup-config** - スイッチからスタートアップコンフィグレーションファイルをバックアップします。

[**バックアップ**] ボタン - バックアップを開始します。

13.2.2.4 TFTP サーバへコンフィグレーションをバックアップ

このウィンドウを用いて、スイッチのコンフィグレーションのバックアップコピーを TFTP サーバに保存します。

ツールバーで **[ツール] > [コンフィグレーション復旧＆バックアップ] > [TFTP サーバへコンフィグレーションをバックアップ]** をクリックして、以下のウィンドウを表示します。

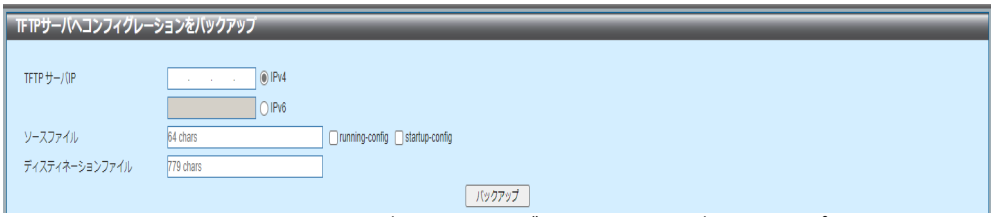

図 13-7 TFTP サーバへコンフィグレーションをバックアップ

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	スイッチにあるコンフィグレーションファイルのソースファイル名とパスを入力します。(最大：64 文字) • **running-config** - スイッチから実行中のコンフィグレーションファイルをバックアップします。 • **startup-config** - スイッチからスタートアップコンフィグレーションファイルをバックアップします。
ディスティネーションファイル	コンフィグレーションファイルを保存する TFTP サーバ上のディスティネーションパスと場所を入力します。 (最大：779 文字)

[バックアップ] ボタン - バックアップを開始します。

13.2.3 ログバックアップ

13.2.3.1 ログを HTTP サーバへバックアップ

このウィンドウを用いて、スイッチのシステムログまたは攻撃ログのコピーを HTTP を使用してローカル PC に保存します。

ツールバー >[ツール] > [ログバックアップ] > [ログを **HTTP** サーバへバックアップ] をクリックして、以下のウィンドウを表示します。

図 13-8 ログを HTTP サーバへバックアップ

設定パラメータ

パラメータ	概要
ログタイプ	HTTP を使用してローカル PC にバックアップするログタイプを選択します。 • **システムログ** - システムログをバックアップします。 • **攻撃ログ** - 攻撃ログをバックアップします。

[**バックアップ**] ボタン - バックアップを開始します。

13.2.3.2 ログを TFTP サーバへバックアップ

このウィンドウを用いて、スイッチのシステムログまたは攻撃ログのコピーを TFTP サーバに保存します。

ツールバー >[ツール] > [ログバックアップ] > [ログを TFTP サーバへバックアップ] をクリックして、以下のウィンドウを表示します。

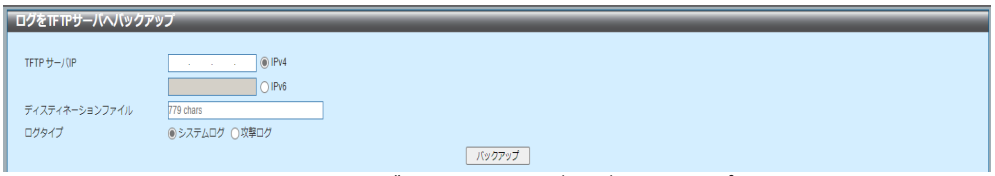

図 13-9 ログを TFTP サーバへバックアップ

設定パラメータ

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ディスティネーションファイル	ログファイルを保存する TFTP サーバ上のディスティネーションパスと場所を入力します。(最大：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。

13.2.4 Ping

このウィンドウを用いて、ディスティネーション IPv4/IPv6 アドレスまたはドメイン名に Ping して、ネットワーク接続をテストします。Ping リクエストには、アクセスリストを適用できます。

ツールバー >[ツール] > [Ping] をクリックして、以下のウィンドウを表示します。

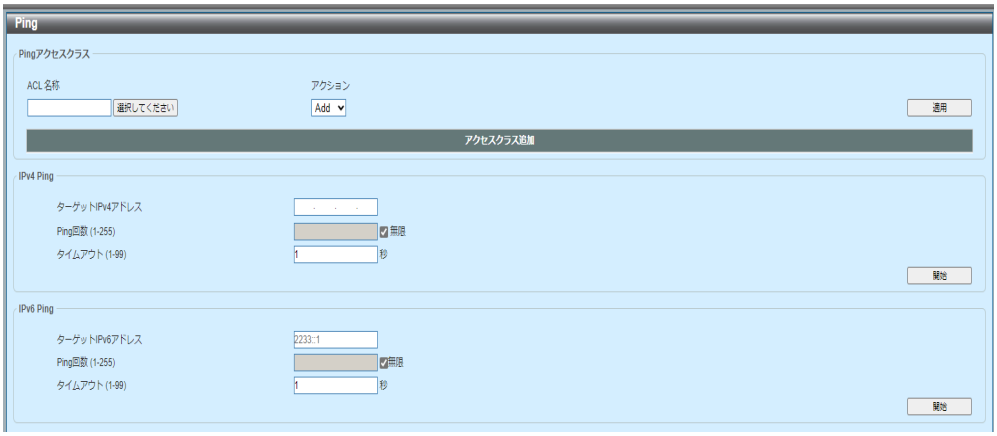

図 13-10 Ping

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。

[IPv4 Ping] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ターゲット IPv4 アドレス	ディスティネーション IPv4 アドレスを選択および入力します。
Ping 回数	このウィンドウで設定した IPv4 アドレスに Ping を試行する回数を入力します。範囲は 1 ～ 255 です。 **[無限]** チェックボックスをオンにした場合、プログラムを停止するまで、指定した IPv4 アドレスに ICMP Echo パケットを送信し続けます。
タイムアウト	Ping メッセージのタイムアウト時間を入力します。パケットがここで指定した時間内に IPv4 アドレスを検出できない場合、Ping パケットは廃棄されます。範囲は、1 ～ 99 秒です。

[開始] ボタンをクリックして、IPv4 Ping を開始します。

[IPv6 Ping] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ターゲット IPv6 アドレス	ディスティネーション IPv6 アドレスを選択および入力します。
Ping 回数	このウィンドウで設定した IPv6 アドレスに Ping を試行する回数を入力します。範囲は 1 ～ 255 です。 **[無限]** チェックボックスをオンにした場合、プログラムを停止するまで、指定した IPv6 アドレスに ICMP Echo パケットを送信し続けます。
タイムアウト	Ping メッセージのタイムアウト時間を入力します。パケットがここで指定した時間内に IPv6 アドレスを検出できない場合、Ping パケットは廃棄されます。範囲は、1 ～ 99 秒です。

[開始] ボタンをクリックして、IPv6 Ping を開始します。

[IPv4 Ping] パラメータを選択および入力し、**[開始]** ボタンをクリックして、以下のウィンドウを表示します。

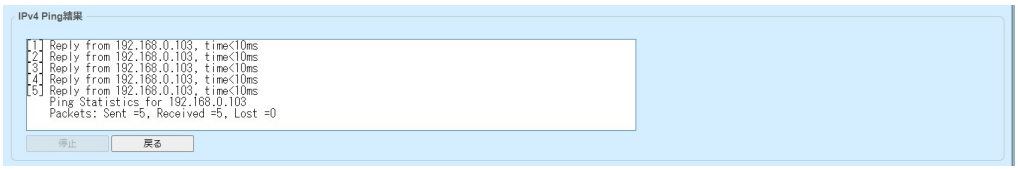

図 13-11 IPv4 Ping(結果)

[停止] ボタンをクリックして、Ping プロセスを停止します。
[戻る] ボタンをクリックして、前の [Ping] ウィンドウに戻ります。

[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。

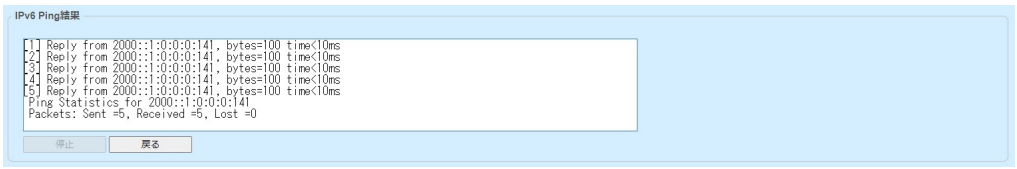

図 13-12 IPv6 Ping(結果)

[停止] ボタンをクリックして、Ping プロセスを停止します。
[戻る] ボタンをクリックして、前の [Ping] ウィンドウに戻ります。

[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。

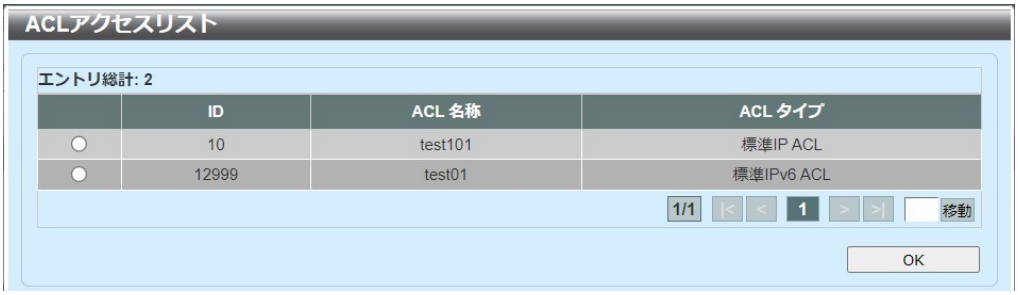

図 13-13 Ping (選択してください)

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

13.2.5 トレースルート

このウィンドウを用いて、ディスティネーション IPv4/IPv6 アドレスまたはドメイン名へのルートをトレースして、ネットワーク接続をテストします。

ツールバー >[ツール] > [トレースルート] をクリックして、以下のウィンドウを表示します。

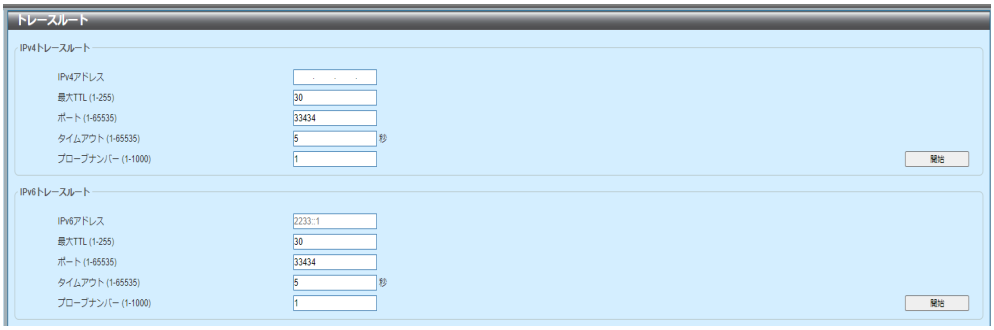

図 13-14 トレースルート

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。
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。(設定範囲 : 1 - 65535, デフォルト : 5)
プローブナンバー	プローブタイムの数を入力します。(設定範囲 : 1 - 1000, デフォルト : 1)

[**開始**] ボタン - IPv4 トレースルートを開始します。

設定パラメータ （[IPv6 トレースルート] セクション）

パラメータ	概要
IPv6 アドレス	ディスティネーション IPv6 アドレスを選択および入力します。

パラメータ	概要
最大 TTL	トレースルートリクエストの TTL の最大値を入力します。これは、トレースルートパケットが通過できるルータの最大数です。トレースルートオプションは、2 つの装置間のネットワークパスを探索するときに通過します。 (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。(設定範囲 : 1 - 65535, デフォルト : 5)
プローブナンバー	プローブタイムの数を入力します。 (設定範囲 : 1 - 1000, デフォルト : 1)

[**開始**] ボタン - IPv6 トレースルートを開始します。

[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。

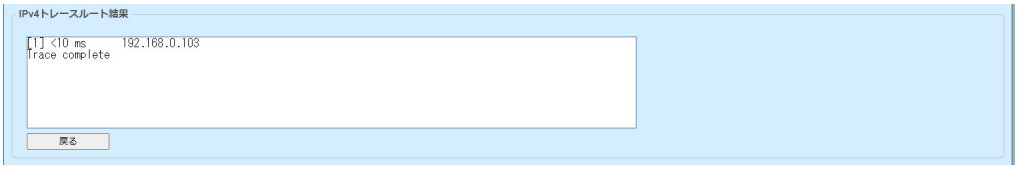

図 13-15 IPv4 トレースルート (結果)

[戻る] ボタンをクリックして、**[トレースルート]** 前の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。

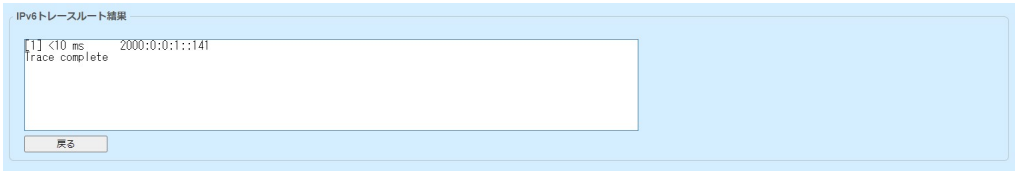

図 13-16 IPv6 トレースルート (結果)

[**戻る**] ボタン - 前のウィンドウに戻ります。

13.2.6 リセット

このウィンドウを用いて、スイッチのソフトウェアコンフィグレーションの工場出荷時の値へのリセットを開始します。

ツールバー >[ツール] > [リセット] をクリックして、以下のウィンドウを表示します。

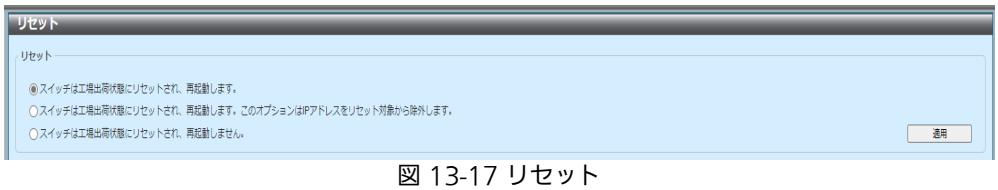

図 13-17 リセット

設定パラメータ

パラメータ	概要
リセット	以下のいずれかのリセットオプションを選択します。 • **スイッチは工場出荷状態にリセットされ、再起動します** • **スイッチは工場出荷状態にリセットされ、再起動します。このオプションは IP アドレスをリセット対象から除外します** • **スイッチは工場出荷状態にリセットされ、再起動しません**

[**適用**] ボタン - 工場出荷状態へのリセットを開始します。

13.2.7 システム再起動

このウィンドウを用いて、スイッチの再起動を開始します。最後の再起動または電源オン以降に行われた新しいコンフィグレーション変更は、保存されていなければ、失われます。

ツールバー >[ツール] > [システム再起動] をクリックして、以下のウィンドウを表示します。

図 13-18 システム再起動 (Normal)

[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。

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** - 指定された時刻および / 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]**を選択して、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]**を選択して、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。

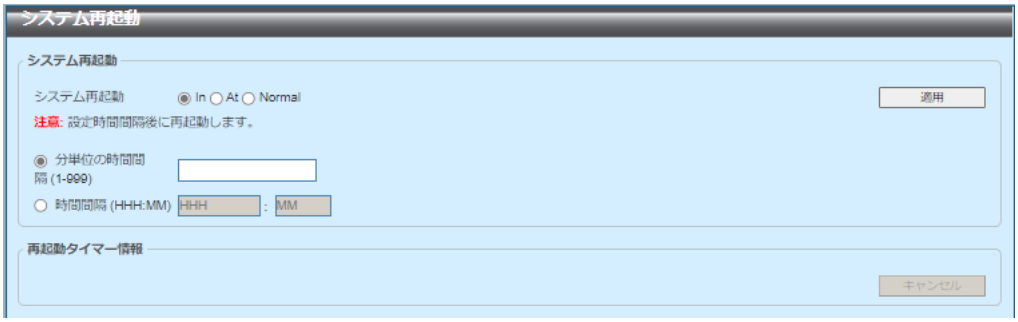

図 13-19 システム再起動 (In)

パラメータ	概要
分単位の時間間隔(1 - 999)	インターバル値を入力します。(設定範囲 :1-999 分)
時間間隔(HHH:MM)	タイムインターバルを選択します。時間(HHH)と分(MM)の値を選択します。

[**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。

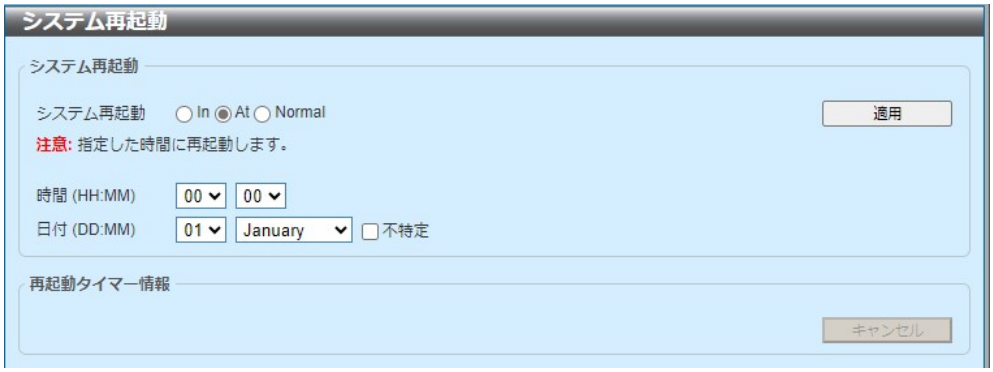

図 13-20 システム再起動 (At)

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(HH:MM)	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。
データ(オプション)	スイッチ再起動のデータを選択します。再起動を最大 24 日間遅らせることができます。月と日を選択します。

[**適用**] ボタン - 指定された時刻および / または日付が経過した後に再起動を開始します。

13.3 言語

WEB UI の言語は英語と日本語から選択できます。デフォルトは、日本語です。

プルダウンから言語を選択します。

図 13-21 言語

13.4 ログアウト

ツールバーで [**ログアウト**] オプションをクリックして、スイッチの WEB UI からログアウトします。

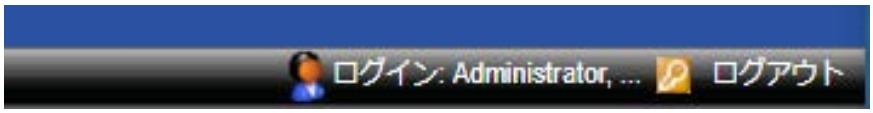

図 13-22 ログアウト

14 付録 - システムログ一覧

14.1 802.1X

ID	ログの概要	重大度
1.	イベントの概要：802.1X 認証に成功しました。 ログメッセージ：[802.1X]（<method>）Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	情報
2.	イベントの概要：802.1X 認証に失敗しました。 ログメッセージ：[802.1X]（<method>）Rejected user <username> (<macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
3.	イベントの概要：802.1X 認証テーブルがフルなので、新しいアドレスを認証できません。 ログメッセージ：[802.1X]Rejected <macaddr> on Port <portNum> （auth table was full） パラメータ概要： macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

14.2 AAA

ID	ログの概要	重大度
1.	イベントの概要：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	情報
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ーの場合の AAA サーバー IP アドレス username: 認証ユーザー名	情報
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ーの場合の AAA サーバー IP アドレス username: 認証ユーザー名	ワーニング
4.	イベントの概要：リモートサーバー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 サーバー IP アドレス username: 認証ユーザー名	ワーニング
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ーの場合、AAA サーバー IP アドレス username: 認証ユーザー名	情報

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ーの場合の AAA サーバー IP アドレス username: 認証ユーザー名	ワーニング
7.	イベントの概要：リモートサーバーが 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 サーバー IP アドレス username: 認証ユーザー名	ワーニング

14.3 ARP

ID	ログの概要	重大度
1.	イベントの概要：Gratuitous ARP で重複 IP を検出しました。 ログメッセージ：Conflict IP was detected with this device （IP：<ipaddr>, MAC：<macaddr>, Port <portNum>, Interface：<ipif_name>） パラメータ概要： ipaddr：使用中の装置と重複している IP アドレス。 macaddr：使用中の装置と重複する IP アドレスを持つ装置の MAC アドレス。 portNum：1. 整数値、2. 装置の論理ポート番号を表します。 ipif_name：競合 IP アドレスを持つスイッチのインタフェースの名前。	ワーニング

14.4 コマンド

ID	ログの概要	重大度
1.	イベントの概要：コマンドログ収集 ログメッセージ：”<command-str>” executed by <username> from <line>[, IP：<ip-address>] パラメータ概要： username：このコマンドを実行したアカウント名。 command-str：正常に実行され、スイッチのコンフィグレーションを変更したコマンド文字列。 line：このパラメータは、このコマンドを実行したラインモードを示します（console、telnet、SSH など）。 ip-address：（オプション）コマンドがリモート端末で入力された場合（telnet、SSH など）、このパラメータが必要です。	情報

14.5 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。	情報
2.	イベントの概要：ファームウェアのアップグレードに失敗しました。 ログメッセージ：Firmware upgraded by <session> unsuccessfully （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング
3.	イベントの概要：ファームウェアのアップロードに成功しました。 ログメッセージ：Firmware uploaded by <session> successfully （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
4.	イベントの概要：ファームウェアのアップロードに失敗しました。 ログメッセージ：Firmware uploaded by <session> unsuccessfully （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング

ID	ログの概要	重大度
5.	イベントの概要：コンフィグレーションのダウンロードに成功しました。 ログメッセージ：Configuration downloaded by <session> successfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
6.	イベントの概要：コンフィグレーションのダウンロードに失敗しました。 ログメッセージ：Configuration downloaded by <session> unsuccessfully.（Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング
7.	イベントの概要：コンフィグレーションのアップロードに成功しました。 ログメッセージ：Configuration uploaded by <session> successfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	情報
8.	イベントの概要：コンフィグレーションのアップロードに失敗しました。 ログメッセージ：Configuration uploaded by <session> unsuccessfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング

ID	ログの概要	重大度
9.	イベントの概要：未知のタイプのファイルのダウンロードに失敗しました。 ログメッセージ：Downloaded by <session> unsuccessfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>], Server IP：<serverIP>, File Name：<pathFile>） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。 serverIP：サーバ IP アドレス。 pathFile：サーバ上のパスとファイル名。	ワーニング
10.	イベントの概要：ログメッセージのアップロードに成功しました。 ログメッセージ：Log message uploaded by <session> successfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>]） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。	情報
11.	イベントの概要：ログメッセージのアップロードに失敗しました。 ログメッセージ：Log message uploaded by <session> unsuccessfully. （Username：<username>[, IP：<ipaddr>, MAC：<macaddr>]） パラメータ概要： session：ユーザのセッション。 username：現在のログインユーザを表します。 ipaddr：クライアント IP アドレスを表します。 macaddr：クライアント MAC アドレスを表します。	情報

14.6 DAD

ID	ログの概要	重大度
1.	イベントの概要：DUT が DAD 期間中に重複アドレスを持つ NS（Neighbor Solicitation）メッセージを受信したのでログを追加します。 ログメッセージ：Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Solicitation Messages パラメータ概要： ipv6address：ネイバー要請メッセージの IPv6 アドレス。 interface-id：ポートインタフェース ID。	ワーニング
2.	イベントの概要：DUT が DAD 期間中に重複アドレスを持つ NA（Neighbor Advertisement）メッセージを受信したのでログを追加します。 ログメッセージ：Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Advertisement Messages パラメータ概要： ipv6address：ネイバーアドバタイズメッセージの IPv6 アドレス。 interface-id：ポートインタフェース ID。	ワーニング

14.7 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"	ワーニング
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"	クリティカル

14.8 デバッグエラー

ID	ログの概要	重大度
1.	イベント概要：システムの致命的なエラーが発生したので、システムを再起動します。 ログメッセージ：System re-start reason：system fatal error	緊急
2.	イベントの概要：CPU 例外が発生したので、システムを再起動します。 ログメッセージ：System re-start reason：CPU exception	緊急

14.9 DHCPv6 クライアント

ID	ログの概要	重大度
1.	イベントの概要：DHCPv6 クライアントインタフェースの管理者の状態が変化しました。 ログメッセージ：DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] パラメータ概要： ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
2.	イベントの概要：DHCPv6 クライアントが DHCPv6 サーバから IPv6 アドレスを取得しました。 ログメッセージ：DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name> パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
3.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの更新を開始しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> starts renewing パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
4.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの更新に成功しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> renews success パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
5.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの再バインディングを開始しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
6.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスの再バインディングに成功しました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> rebinds success パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報
7.	イベントの概要：DHCPv6 サーバから取得した IPv6 アドレスが削除されました。 ログメッセージ：The IPv6 address < ipv6address > on interface <ipif-name> was deleted パラメータ概要： ipv6address：DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name：DHCPv6 クライアントインタフェースの名前。	情報

14.10 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。	ワーニング
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。	情報

14.11 ファン (GA-EM48T のみ)

ID	ログの概要	重大度
1.	イベントの概要：左ファンが機能していません。 ログメッセージ：Left Fan <value> failed パラメータ概要： value：ファン ID。	クリティカル
2.	2 イベントの概要：左ファンが復旧しました。 ログメッセージ：Left Fan <value> back to normal パラメータ概要： value：ファン ID。	クリティカル

14.12 インタフェース

ID	ログの概要	重大度
1.	イベントの概要：ポートがリンクアップしました。 ログメッセージ：Port <port> link up, <nway> パラメータ概要： port：論理ポート番号を表します。 nway：リンクのスピードと二重モードを表します。	情報
2.	イベントの概要：ポートがリンクダウンしました。 ログメッセージ：Port <port> link down パラメータ概要： port：論理ポート番号を表します。	情報

14.13 IP ソースガードの検証

ID	ログの概要	重大度
1.	イベントの概要：このメッセージは、DHCP スヌーピングエントリを IPSG テーブルに設定するハードウェアルールリソースが存在しないことを示します。 ログメッセージ：Failed to set IPSG entry due to no hardware rule resource. (IP：<ipaddr>, MAC：<macaddr>, VID：<vlanid>, Interface <interface-id>) パラメータ概要： ipaddr：IP アドレス macaddr：MAC アドレス vlanid：VLAN ID interface-id：インタフェースナンバー	ワーニング

14.14 LACP

ID	ログの概要	重大度
1.	イベントの概要：リンクアグリゲーショングループがリンクアップしました。 ログメッセージ：Link Aggregation Group < group_id > link up パラメータ概要： group_id：リンクアップしたアグリゲーショングループのグループ ID。	情報
2.	イベントの概要：リンクアグリゲーショングループがリンクダウンしました。 ログメッセージ：Link Aggregation Group < group_id > link down パラメータ概要： group_id：リンクダウンしたアグリゲーショングループのグループ ID。	情報
3.	イベントの概要：メンバポートがリンクアグリゲーショングループに所属しました。 ログメッセージ：<ifname> attach to Link Aggregation Group <group_id> パラメータ概要： ifname：アグリゲーショングループに所属したポートのインタフェース名。 group_id：ポートの所属先のアグリゲーショングループのグループ ID。	情報
4.	イベントの概要：メンバポートがリンクアグリゲーショングループへの所属を解除しました。 ログメッセージ：<ifname> detach from Link Aggregation Group <group_id> パラメータ概要： ifname：アグリゲーショングループへの所属を解除したポートのインタフェース名。 group_id：ポートが所属を解除したアグリゲーショングループのグループ ID。	情報

14.15 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ーを表す。	情報
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ーを表す。	ワーニング
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ーを表す。	情報
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ーを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	ワーニング
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報

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ーを表す。 ipaddr: クライアント IP アドレスを表す。	クリティカル
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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 ユーザーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	ワーニング
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報
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ーを表す。 ipaddr: クライアント IP アドレスを表す。	情報

14.16 ループ検知

ID	ログの概要	重大度
1.	イベントの概要：2 つのポートまたは 2 つの LACP インタフェースの間でループを検知しました。 ログメッセージ：The loop detected between port/port-channel <portNum> and <portNum> パラメータ概要： portNum：ポート番号または LACP インタフェース ID。	ワーニング
2.	イベントの概要：1 つのポートまたは 1 つの LACP インタフェースでループを検知しました。 ログメッセージ：The loop detected on port/port-channel <portNum> パラメータ概要： portNum：ポート番号または LACP インタフェース ID。	ワーニング
3.	イベントの概要：1 つのポートと 1 つの LACP インタフェースの間でループを検知しました。 ログメッセージ：The loop detected between port/port-channel <portNum> and port/port-channel <portNum> パラメータ概要： portNum：ポート番号またはポートチャネルナンバー。	ワーニング
4.	イベントの概要：ループしていたポートまたは LACP インタフェースが自動復旧しました。 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。	情報

14.17 MAC ベースアクセスコントロール

ID	ログの概要	重大度
1.	イベントの概要：MAC 認証に成功しました。 ログメッセージ：[MAC]（<method>）Authorized <macaddr> on Port <portNum> to VLAN <vid> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	情報
2.	イベントの概要：MAC 認証に失敗しました。 ログメッセージ：[MAC]（<method>）Rejected <macaddr> on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
3.	イベントの概要：MAC 認証テーブルがフルなので、新しいアドレスを認証できません。 ログメッセージ：[MAC]Rejected <macaddr> on Port <portNum>（auth table was full） パラメータ概要： macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

14.18 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。	ワーニング
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	ワーニング

14.19 PPS （Power to Progress SDN）

ID	ログの概要	重大度
1.	イベントの概要：コントローラが更新されました。 ログメッセージ：(PPS) New Controller （ID：<ControllerID>） パラメータ概要： ControllerID：PPS コントローラ ID	情報
2.	イベントの概要：コントローラポートが更新されました。 ログメッセージ：(PPS) New Controller Port （Port ：<PortNum>） パラメータ概要： PortNum：ポート番号	情報
3.	イベントの概要：ステータスを "Standalone" から "Controlled" に変更しました。 ログメッセージ：(PPS) Change Status from Standalone to Controlled	情報
4.	イベントの概要：ステータスを "Controlled" から "CPNL" に変更しました。 ログメッセージ：(PPS) Change Status from Controlled to CPNL	情報
5.	イベントの概要：ステータスを "CPNL" から "Controlled" に変更しました。 ログメッセージ：(PPS) Change Status from CPNL to Controlled	情報
6.	イベントの概要：コンフィグレーションモードで開始しました。 ログメッセージ：(PPS) Start Configuration Mode	情報
7.	イベントの概要：コンフィグレーションモードを停止しました。 ログメッセージ：(PPS) Stop Configuration Mode	情報
8.	イベントの概要："Commit" またはリクエスト（セーブ）を受信し、設定を変更しました。 ログメッセージ：(PPS) Configuration Changed	情報
9.	イベントの概要："Rollback" を受信し、設定を修復しました。 ログメッセージ：(PPS) Configuration Changed （Rollback）	情報
10.	イベントの概要：コントローラがポートの状態を "Forwarding" に変更しました。 ログメッセージ：(PPS) Controller change port status to Forwarding	情報
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	情報
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.	情報
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.	情報
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.	注意
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.	エラー
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	エラー

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.	エラー
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.	エラー
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.	情報
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.	情報
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.	情報
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.	注意

14.20 RADIUS

ID	ログの概要	重大度
1.	イベントの概要：このログは、RADIUS が有効な VLAN ID 属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned VID：<vid> to port <interface-id> （Username：<username>） パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 vid：RADIUS サーバが許可して割り当てた VLAN ID。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報

14.21 SNMP

ID	ログの概要	重大度
1.	イベントの概要：無効なコミュニティ文字列を含む SNMP リクエストを受信しました。 ログメッセージ：SNMP request received from <ipaddr> with invalid community string パラメータ概要： ipaddr：IP アドレス。	情報

14.22 SSH

ID	ログの概要	重大度
1.	イベントの概要：SSH サーバーが有効になりました。 ログメッセージ：SSH server is enabled	情報
2.	イベントの概要：SSH サーバーが無効になりました。 ログメッセージ：SSH server is disabled	情報

14.23 システム

ID	ログの概要	重大度
1.	イベントの概要：システムがスタートアップしました。 ログメッセージ：System started up	クリティカル
2.	イベントの概要：現在のコンフィグレーションがフラッシュに保存されました。 ログメッセージ：Configuration saved to flash by console （Username：<username>） パラメータ概要： username：ユーザー名。	情報
3.	イベントの概要：電源が落ちました。 ログメッセージ： Power <powerID> failed パラメータ概要： powerID：パワー ID。	クリティカル
4.	イベントの概要：: 電源が復旧する。 ログメッセージ：Power <powerID> back to normal パラメータ概要： powerID：パワー ID。	クリティカル
5.	イベントの概要：リモートからシステムコンフィグレーションを保存しました。 ログメッセージ：Configuration saved to flash （Username：<username>, IP：<ipaddr>） username：ユーザ名。 ipaddr：IP アドレス。	情報
6.	イベントの概要：システムの電源がオンになり、スタートアップしました。 ログメッセージ：System cold start	クリティカル
7.	イベントの概要：システムが再起動し、スタートアップしました。 ログメッセージ：System warm start	クリティカル

14.24 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 サーバへの IP アドレス	情報

14.25 Telnet

ID	ログの概要	重大度
1.	イベントの概要：Telnet によるログインに成功しました。 ログメッセージ：Successful login through Telnet （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	情報
2.	イベントの概要：Telnet によるログインに失敗しました。 ログメッセージ：Login failed through Telnet （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	ワーニング
3.	イベントの概要：Telnet によりログアウトしました。 ログメッセージ：Logout through Telnet （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	情報
4.	イベントの概要：Telnet セッションがタイムアウトしました。 ログメッセージ：Telnet session timed out （Username：<username>, IP：<ipaddr>） パラメータ概要： ipaddr：Telnet クライアントの IP アドレス。 username：Telnet サーバへのログインに使用したユーザ名。	情報

14.26 温度 (GA-EM48T のみ)

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：Sensor：<sensorID> detects abnormal temperature <temperature> パラメータ概要： sensorID：センサ ID temperature：センサの現在の温度。	クリティカル
2.	イベントの概要：通常の温度に回復しました。 ログメッセージ：Sensor：<sensorID> temperature back to normal パラメータ概要： sensorID：センサ ID	クリティカル

14.27 トラフィック制御

ID	ログの概要	重大度
1.	イベントの概要：ブロードキャスト、マルチキャスト、またはユニキャストのストームが発生しています。 ログメッセージ：<Broadcast | Multicast | Unicast> storm is occurring on <interface-id> パラメータ概要： interface-id：ストームが発生しているインタフェース ID。	ワーニング
2.	イベントの概要：ブロードキャスト、マルチキャスト、またはユニキャストのストームが解消されました。 ログメッセージ：<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> パラメータ概要： interface-id：ストームが解消されたインタフェース ID。	情報
3.	イベントの概要：パケットストームによりポートがシャットダウンされました。 ログメッセージ：<interface-id> is currently 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。	ワーニング

14.28 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。	注意
2.	イベントの概要：クライアントホストが認証に成功しました。 ログメッセージ：[WEB]（RADIUS/Local）Authorized user <string> (<macaddr>) on Port <portNum> to VLAN <vlanNum> パラメータ概要： string：ユーザ名。 macaddr：MAC アドレス。 portNum：ポート番号。 vlanNum：VLAN ナンバー。	情報
3.	イベントの概要：クライアントテーブルがフルです。 ログメッセージ：[WEB]Rejected <macaddr> on Port <portNum>（auth table was full） パラメータ概要： macaddr：MAC アドレス。 portNum：ポート番号。	注意

14.29 Web

ID	ログの概要	重大度
1.	イベントの概要：Web からのログインに成功しました。 ログメッセージ：Successful login through Web （Username：<username>, IP：<ipaddr>） パラメータ概要： username：ユーザ名。 ipaddr：Web からスイッチにアクセスしたユーザの IP アドレス。	情報
2.	イベントの概要：Web からのログインに失敗しました。 ログメッセージ：Login failed through Web （Username：<username>, IP：<ipaddr>） パラメータ概要： username：ユーザ名。 ipaddr：Web からスイッチにアクセスしたユーザの IP アドレス。	ワーニング
3.	イベントの概要：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。	情報
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。	ワーニング
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。	情報
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。	情報

15 付録 - システムトラップ一覧

15.1 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

15.2　ファン (GA-EM48T のみ)

ID	トラップ名	トラップの概要	OID
1.	mnoFanFailure	ファンが機能しなくなったときに、この通知が送信されます。	1.3.6.1.4.1.396.5.5.1.1
2.	mnoFanRecovery	ファンが復旧したときに、この通知が送信されます。	1.3.6.1.4.1.396.5.5.1.5

15.3 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

15.4 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

15.5 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

15.6 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

15.7 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

15.8 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

15.9 RMON

ID	トラップ名	トラップの概要	OID
1.	risingAlarm	アラームエントリがその上昇閾値を超えて、SNMP トラップを送信するように設定されているイベントが生成されたときに、この SNMP トラップが生成されます。 バインディングオブジェクト： (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
2.	fallingAlarm	アラームエントリがその下降閾値を超えて、SNMP トラップを送信するように設定されているイベントが生成されたときに、この SNMP トラップが生成されます。 バインディングオブジェクト： (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

15.10 SNMP 認証

ID	トラップ名	トラップの概要	OID
1.	authenticationFailure	authenticationFailure トラップは、エージェントロールで動作する SNMPv2 エンティティが、正しく認証されていないプロトコルメッセージを受信したことを示します。SNMPv2 のすべての実装にこのトラップを生成する機能が必要ですが、snmpEnableAuthenTraps オブジェクトは、このトラップが生成されるかどうかを示します。	1.3.6.1.6.3.1.1.5.5

15.11 システム

ID	トラップ名	トラップの概要	OID
1.	coldStart	coldStart トラップは、エージェントロールで動作する SNMPv2 エンティティが自身を再初期化していること、およびそのコンフィグレーションが変更されている可能性があることを示します。	1.3.6.1.6.3.1.1.5.1
2.	warmStart	warmStart トラップは、エージェントロールで動作する SNMPv2 エンティティが、コンフィグレーションが変更されないように自身を再初期化していることを示します。	1.3.6.1.6.3.1.1.5.2

15.12 温度 (GA-EM48T のみ)

ID	トラップ名	トラップの概要	OID
1.	mnoTemperatureRising Alarm	この通知は、現在の温度が上限閾値を超えているときに送信されます。	1.3.6.1.4.1.396.5.5.1.2.1
2.	mnoTemperatureFalling Alarm	この通知は、現在の温度が上限閾値から下回っているときに送信されます。	1.3.6.1.4.1.396.5.5.1.2.2

15.13 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

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/

P0524-3114