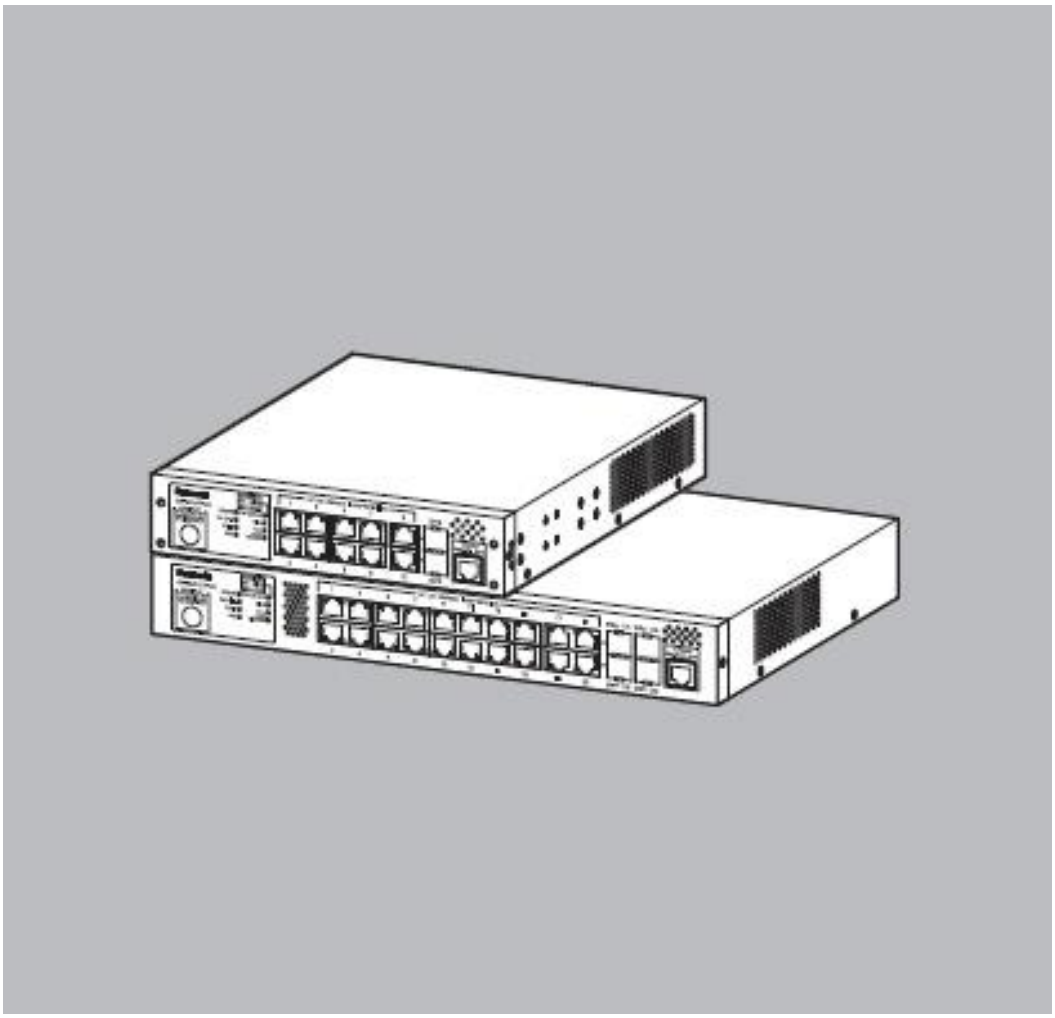
Panasonic

レイヤ２スイッチングハブ

WEB リファレンス

品番 PN260893D/PN261693D



本リファレンスは、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-MLD8TPoE+	PN260893D	3.0.0.08 以上
GA-MLD16TPoE+	PN261693D	3.0.0.08 以上

各機種の対応機能は、商品仕様書をご覧ください。

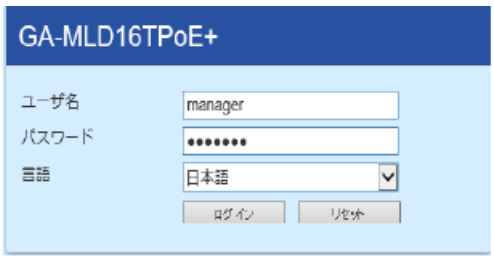
目次

1 はじめに

本装置は WEB で設定をすることが可能です。

- WEB 設定を使用する場合、本装置に事前に CLI コマンドで以下①②の設定が必要です。
  ① IP アドレスを設定。(192.168.0.101 は例です。)
  GA-MLD#configure terminal
  GA-MLD(config)#interface vlan 1
  GA-MLD(config-if)#ip address 192.168.0.101 255.255.255.0
  ② http サーバ機能を有効化。
  GA-MLD(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。ユーザ名、パスワードのデフォルトは「manager」です。



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

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

2 システム

2.1 デバイス情報

このウィンドウを用いて、一般的なスイッチ情報と使用率を表示します。このウィンドウは、スイッチの Web UI にログインすると最初に表示されます。

[GA-MLxxTPoE] リンク（フレーム A 内）をクリックして、以下のウィンドウを表示します。

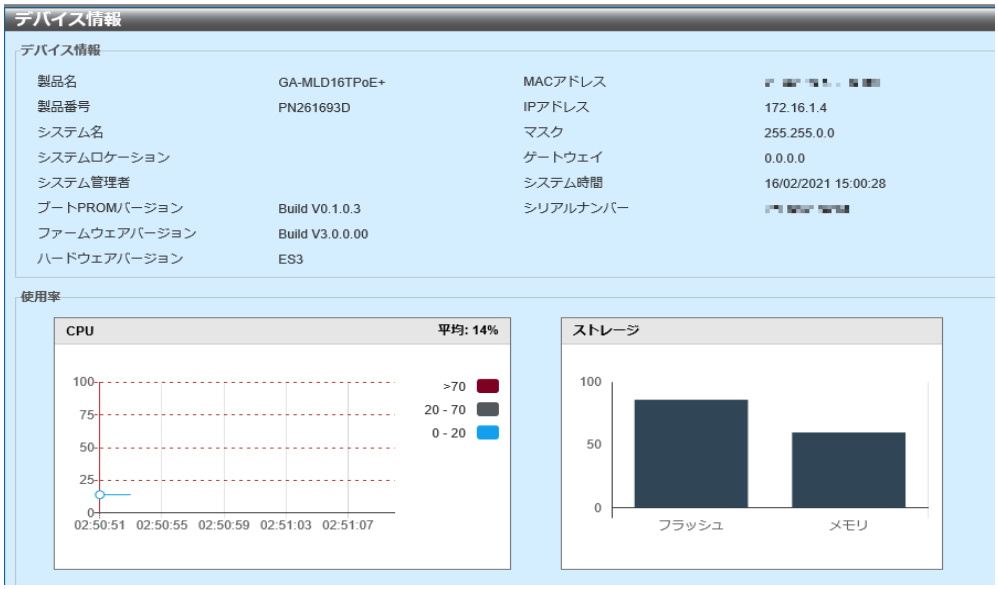


図 2-1 デバイス情報

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。

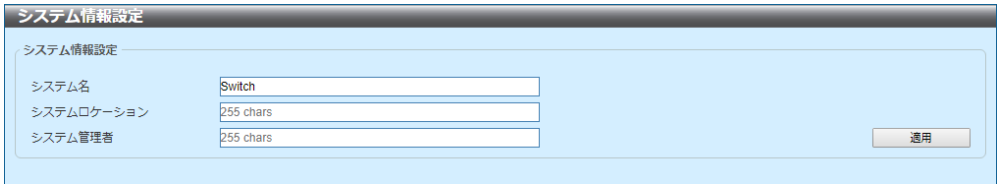


図 2-2 システム情報設定

[システム情報設定] 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
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できます。
システムロケーション	スイッチの場所の概要説明を入力します。
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。

[適用] ボタンをクリックして、変更を反映します。

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。

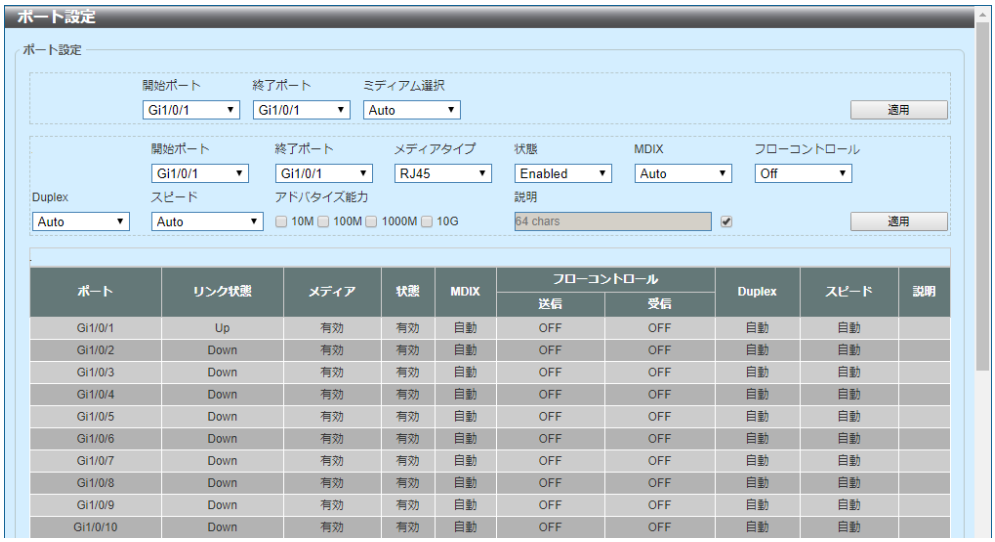


図 2-3 ポート設定

[ポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
メディア選択	ポートのメディアタイプを選択します。選択する値は **[自動]**、**[RJ45]**、および **[SFP]** です。SFP は Small Form-factor Pluggable の略です。
メディアタイプ	ポートのメディアタイプを選択します。選択する値は **[RJ45]** および **[SFP]** です。
状態	物理ポートを有効または無効にします。

パラメータ	概要
MDIX	MDIX（Medium Dependent Interface Crossover）のオプションを選択します。選択する値は以下のとおりです。 • **[自動]** - ケーブルの最適なタイプを自動的に感知します。 • **[ノーマル]** - 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。 • **[クロス]** - クロスオーバケーブルの場合に選択します。このオプションを選択すると、ポートは MDI モードになり、ストレートケーブルで別のスイッチのポート（MDIX モード）に接続できます。
フローコントロール	フローコントロールを **[ON]** または **[OFF]** にします。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。
二重	使用する二重モードを選択します。選択する値は **[自動]** と **[フル]** です。
スピード	ポートスピードのオプションを選択します。このオプションは、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。 **マスター**設定を行うと、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。 **スレーブ**設定に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。

パラメータ	概要
スピード	選択する値は以下のとおりです。 • **[自動]** - 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]** - ポートスピードを強制的に 10Mbps に設定します。このオプションは、10Mbps の銅線接続にのみ利用できます。 • **[100M]** - ポートスピードを強制的に 100Mbps に設定します。このオプションは、100Mbps の銅線接続にのみ利用できます。 • **[1000M]** - ポートスピードを強制的に 1Gbps に設定します。このオプションは、1Gbps のファイバ接続にのみ利用できます。 • **[1000M マスタ]** - ポートスピードを強制的に 1Gbps に設定します。また、マスターとして機能し、送受信操作のタイミングを円滑にします。このオプションは、1Gbps の銅線接続にのみ利用できます。 • **[1000M スレーブ]** - ポートスピードを強制的に 1Gbps に設定します。また、スレーブとして機能し、送受信操作のタイミングを円滑にします。このオプションは、1Gbps の銅線接続にのみ利用できます。
アドバタイズ能力	[スピード] を [自動] 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。
概要	対応するポートの概要説明を入力します。文字列は 64 文字までです。

[適用] ボタンをクリックして、変更を反映します。

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。

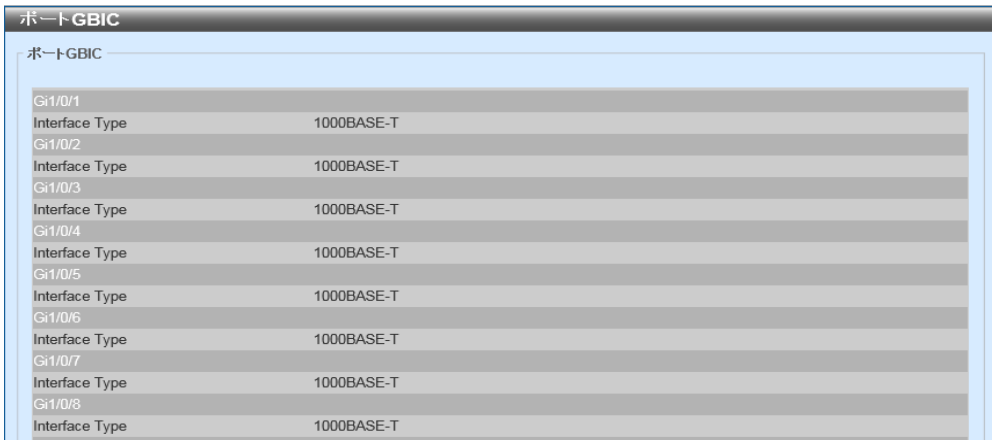
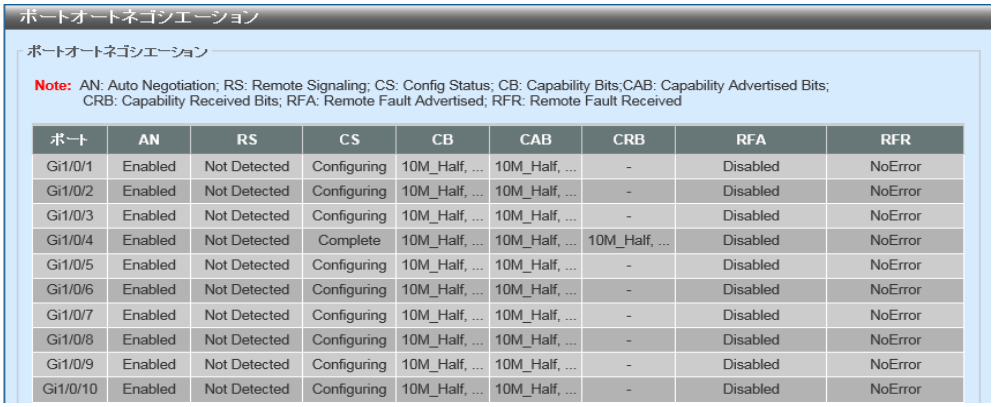


図 2-5 ポート GBIC

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。



ポート	AN	RS	CS	CB	CAB	CRB	RFA	RFR
Gi1/0/1	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/2	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/3	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/4	Enabled	Not Detected	Complete	10M_Half, ...	10M_Half, ...	10M_Half, ...	Disabled	NoError
Gi1/0/5	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/6	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/7	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/8	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/9	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError
Gi1/0/10	Enabled	Not Detected	Configuring	10M_Half, ...	10M_Half, ...	-	Disabled	NoError

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

[Error Disable リカバリ設定] 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
ErrDisable 原因	error-disabled 状態の原因を選択します。選択する値は **[全]**、**[ポートセキュリティ]**、**[ストームコントロール]**、**[BPDU アタックプロテクション]**、**[ダイナミック ARP 検査]**、**[DHCP スヌーピング]**、および **[L2PT ガード]** です。
状態	Error Disable リカバリ機能を有効または無効にします。
間隔	指定したモジュールが原因で発生するエラー状態からポートを復旧する時間（秒）を入力します。範囲は 5 ～ 86400 です。

[適用] ボタンをクリックして、変更内容を反映します。

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

[ジャンボフレーム] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
最大受信フレームサイズ	最大受信フレームサイズ値を入力します。範囲は 64 ～ 9216 バイトです。デフォルトでは、この値は 1518 バイトです。

[適用] ボタンをクリックして、変更を反映します。

2.3.7 ポートグルーピング設定

このウィンドウを用いて、ポートグルーピングの設定を行い、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] > [ポートグルーピング設定] をクリックして、以下のウィンドウを表示します。

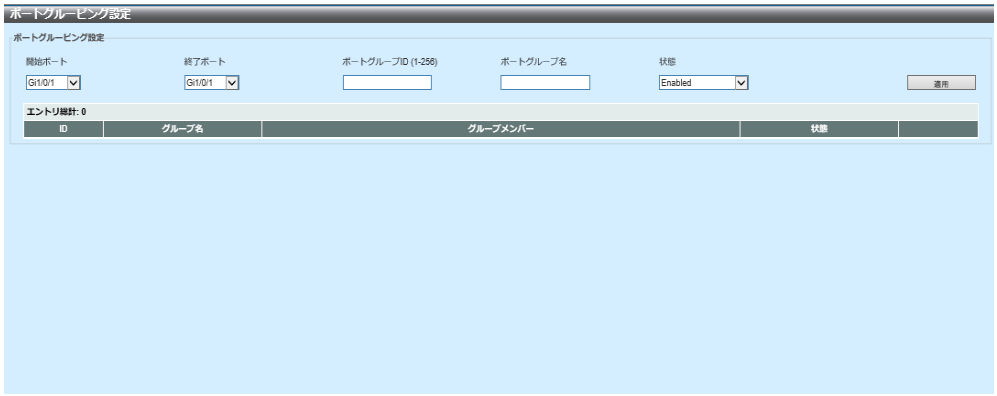


図 2-9 ポートグルーピング設定

[ポートグルーピング設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	ポート番号の範囲を選択します。
ポートグループ ID (1-256)	ポートグループの ID を設定します。
ポートグループ名	ポートグループの名前を設定します。
状態	ポートグルーピング設定を有効または無効に設定します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。

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。

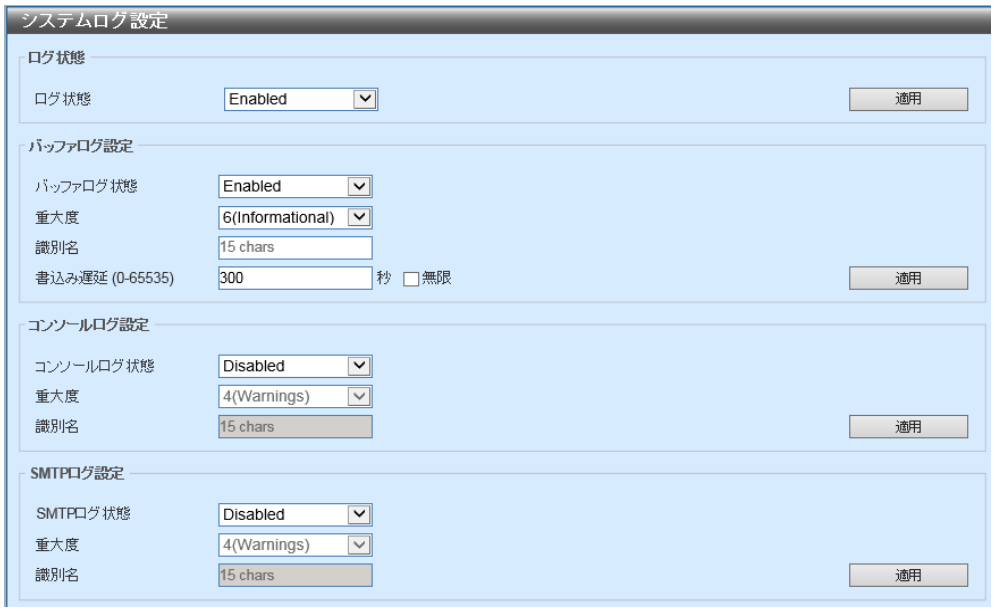


図 2-10 システムログ設定

[ログ状態] 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
ログ状態	グローバルシステムログ状態を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[バッファログ設定] 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
バッファログ状態	グローバルバッファログ状態を有効または無効にします。選択する値は **[有効]**、**[無効]**、および **[デフォルト]** です。**[デフォルト]** オプションを選択すると、グローバルバッファログ状態がデフォルト動作に従います。

パラメータ	概要
重大度	ログ記録する情報のタイプの重大度を選択します。選択する値は **[0(緊急)]**、**[1(警告)]**、**[2(クリティカル)]**、**[3(エラー)]**、**[4(警告)]**、**[5(通知)]**、**[6(情報)]**、および **[7(デバッギング)]** です。
識別名	使用する識別名を入力します。名前は 15 文字までです。Discriminator 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。
書込み遅延	ログの書き込み遅延値を入力します。範囲は、0 ～ 65535 秒です。デフォルトでは、この値は 300 秒です。**[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。

[適用] ボタンをクリックして、変更を反映します。

[コンソールログ設定] 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
コンソールログ状態	グローバルコンソールログ状態を有効または無効にします。
重大度	ログ記録する情報のタイプの重大度を選択します。選択する値は **[0(緊急)]**、**[1(警告)]**、**[2(クリティカル)]**、**[3(エラー)]**、**[4(警告)]**、**[5(通知)]**、**[6(情報)]**、および **[7(デバッギング)]** です。
識別名	使用する識別名を入力します。名前は 15 文字までです。Discriminator 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。

[適用] ボタンをクリックして、変更を反映します。

[SMTP ログ設定] 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
SMTP ログ状態	グローバル SMTP（Simple Mail Transfer Protocol）ログ状態を有効または無効にします。
重大度	ログ記録する情報のタイプの重大度を選択します。選択する値は **[0(緊急)]**、**[1(警告)]**、**[2(クリティカル)]**、**[3(エラー)]**、**[4(警告)]**、**[5(通知)]**、**[6(情報)]**、および **[7(デバッギング)]** です。
識別名	使用する識別名を入力します。名前は 15 文字までです。Discriminator プロファイルの名前を指定します。このプロファイルに規定したフィルタリング基準に基づき、SMTP ログメッセージがフィルタリングされます。

[適用] ボタンをクリックして、変更を反映します。

2.4.2 システムログ Discriminator 設定

このウィンドウを用いて、システムログで使用される Discriminator 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。

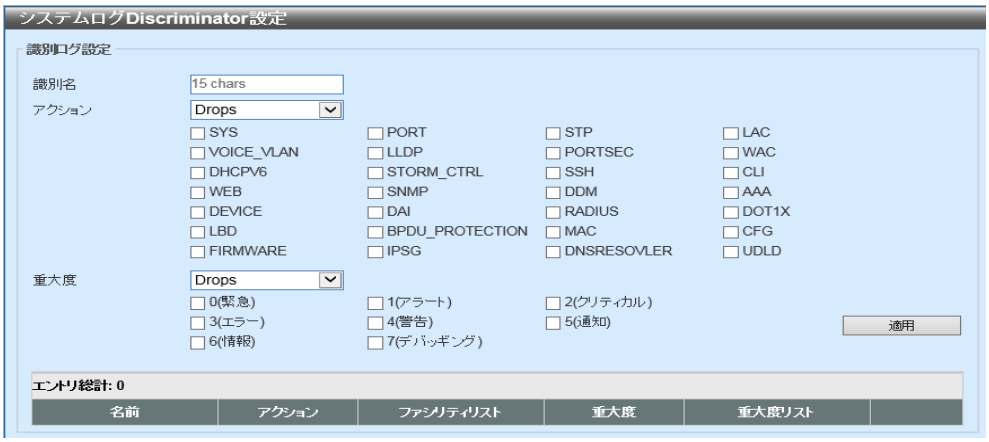


図 2-11 システムログ Discriminator 設定

[識別ログ設定] 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
識別名	Discriminator プロファイルの名前を入力します。名前は 15 文字までです。
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を選択します。動作オプションとして選択する値は **[廃棄]** および **[含む]** です。
重大度	ログ記録する情報のタイプの動作オプションと重大度を選択します。動作オプションとして選択する値は **[廃棄]** および **[含む]** です。選択する重大度の値は **[0(緊急)]**、**[1(警告)]**、**[2(クリティカル)]**、**[3(エラー)]**、**[4(警告)]**、**[5(通知)]**、**[6(情報)]**、および **[7(デバッギング)]** です。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

2.4.3 システムログサーバ設定

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

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

図 2-12 システムログサーバ設定

[ログサーバ] 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
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（User Datagram Protocol）ポート番号を入力します。この値は、514 とするか、1024 ～ 65535 の範囲で指定します。デフォルトでは、この値は 514 です。
重大度	ログ記録する情報のタイプの重大度を選択します。選択する値は **[0(緊急)]**、**[1(警告)]**、**[2(クリティカル)]**、**[3(エラー)]**、**[4(警告)]**、**[5(通知)]**、**[6(情報)]**、および **[7(デバッギング)]** です。

<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。範囲は 0 ～ 23 です。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。以下の表をご覧ください。</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、Discriminator の名前を入力します。名前は 15 文字までです。</td></tr>
</table>

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

2.4.4 システムログ

このウィンドウを用いて、システムログを表示およびクリアします。

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

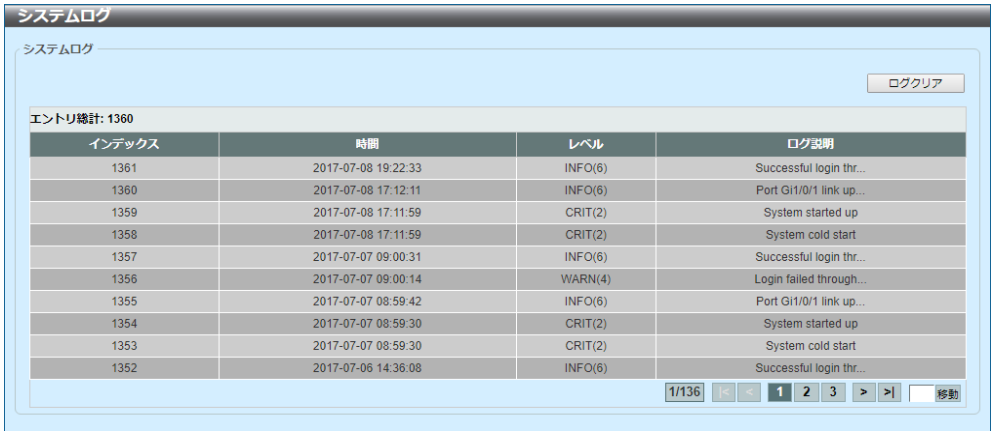


図 2-13 システムログ

[ログクリア] ボタンをクリックして、テーブルからログエントリをクリアします。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

2.4.5 システムアタックログ

このウィンドウを用いて、システムアタックログを表示およびクリアします。

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

図 2-14 システムアタックログ

[アタックログクリア] ボタンをクリックして、テーブルからアタックログのエントリをクリアします。

2.4.6 システム認証ログ

このウィンドウを用いて、システム認証ログの設定を行い、設定値を表示します。

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

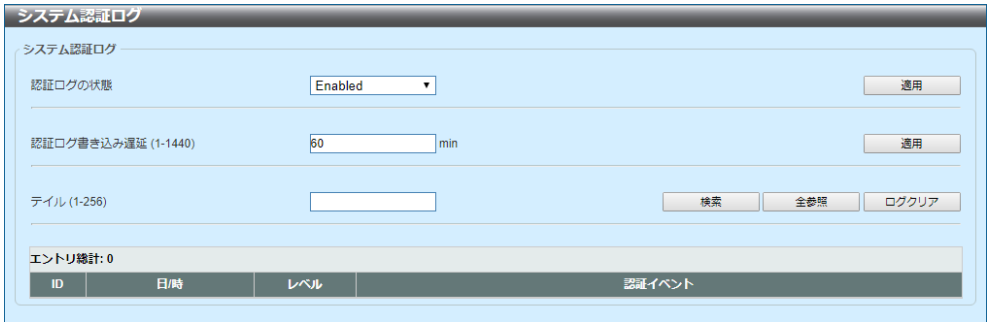


図 2-15 システム認証ログ

[システム認証ログ] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
認証ログの状態	認証ログを有効または無効にします。
認証ログ書き込み遅延	認証ログの書き込み遅延値を入力します。範囲は、1 ～ 1440 分です。
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。範囲は 1 ～ 256 です。

[適用] ボタンをクリックして、変更内容を反映します。
[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。
[ログクリア] ボタンをクリックして、テーブルから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 2-16 時刻設定

[時刻設定] 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
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 (DD / MM / YYYY)	現在の日（DD）、月（MM）、年（YYYY）を入力します（例：25/04/2017）。

[適用] ボタンをクリックして、変更内容を反映します。

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。

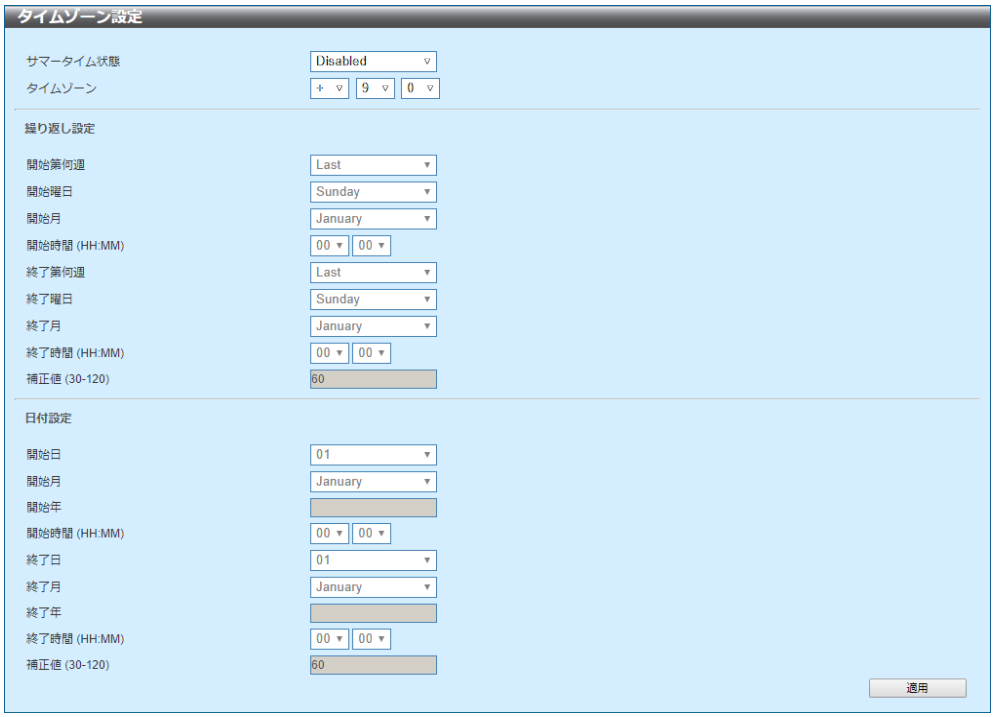


図 2-17 タイムゾーン設定

最初のセクションでは、以下のパラメータを設定できます。

パラメータ	概要
サマータイム状態	サマータイムの設定を選択します。選択する値は以下のとおりです。 • **[無効]** - サマータイム設定を無効にします。 • **[繰り返し設定]** - 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。 • **[日付設定]** - 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指定します。

[繰り返し設定] 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
From: 月週	サマータイムが開始する週を選択します。
From: 週日	サマータイムが開始する曜日を選択します。
From: 月	サマータイムが開始する月を選択します。
From: 時間	サマータイムが開始する時間を選択します。
To: 月週	サマータイムが終了する週を選択します。
To: 週日	サマータイムが終了する曜日を選択します
To: 月	サマータイムが終了する月を選択します。
To: 時間	サマータイムが終了する時間を選択します。
オフセット	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。デフォルト値は 60 です。このオフセットの範囲は 30、60、90、120 です。

[日付設定] 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
From: 月日	サマータイムが開始する日を選択します。
From: 月	サマータイムが開始する月を選択します。
From: 年	サマータイムが開始する年を入力します。
From: 時間	サマータイムが開始する時間を選択します。
To: 月日	サマータイムが終了する日を選択します。
To: 月	サマータイムが終了する月を選択します。
To: 年	サマータイムが終了する年を入力します。
To: 時間	サマータイムが終了する時間を選択します。
オフセット	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。デフォルト値は 60 です。このオフセットの範囲は 30、60、90、120 です。

[適用] ボタンをクリックして、変更を反映します。

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 2-18 SNTP 設定

[SNTP グローバル設定] 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
SNTP 状態	SNTP をグローバルに有効または無効にします。
ポール間隔	同期間隔を秒で入力します。値の範囲は 30 ～ 99999 秒です。デフォルトの間隔は 720 秒です。

[適用] ボタンをクリックして、変更を反映します。

[SNTP サーバ設定] 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
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] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

2.6 時間範囲

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

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

図 2-19 時間範囲

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

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

2.7 PoE 設定

2.7.1 PoE グローバル設定

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

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

図 2-20 PoE グローバル設定

[PoE グローバル設定] 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	
電源バジェット / ファンスピード	本装置が供給できる給電電力とファンの速度を選択します。	
送信トラップの電力使用量しきい値	Trap を送信するための給電電力の閾値が表示されます。 工場出荷時は「50%」に設定されています。	
電源管理方法	給電電力が Power Budget を超えた際の電源給電の方法が表示されます。工場出荷時は「次のポート接続を拒否」に設定されています。	
	次のポート接続を拒否	電源バジェットを超えた直前に接続されたポートの給電を停止します。
	低優先度ポートはシャットダウンされます	優先順位の一番低いポートの給電を停止します。 優先順位が同じ場合はポート番号の大きいポートの給電が停止されます。
SNMP トラップ	PoE 給電トラップを設定します。 工場出荷時は「無効」に設定されています。	

[適用] ボタンをクリックして、変更を反映します。

2.7.2 PoE ポート構成

このウィンドウを用いて、ポート毎の給電設定を行います。

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

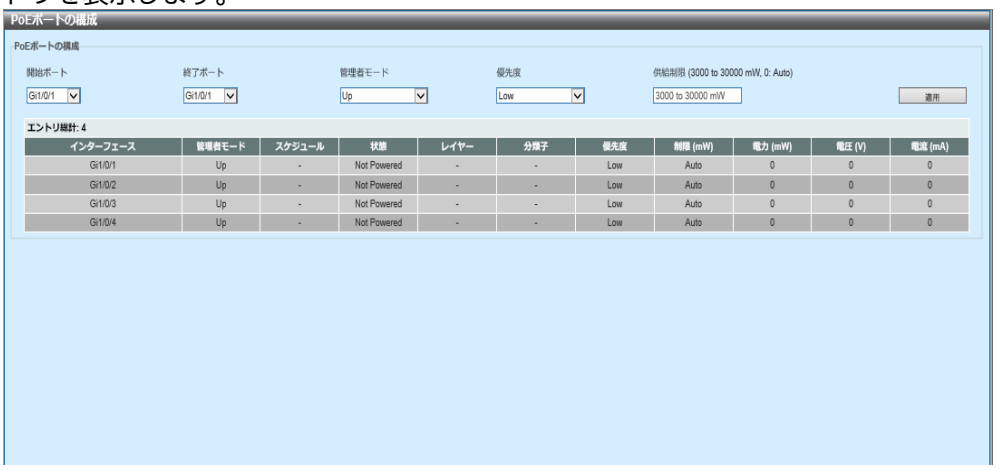


図 2-21 PoE ポート構成

[PoE ポートの構成] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	設定するポートを選択します。
管理者モード	ポートの給電を有効または無効に設定します。選択する値は [Up] および [Down] です。工場出荷時は「Up」に設定されています。
優先度	給電の優先順位を設定します。選択する値は [Crit.]、[High] および [Low] です。工場出荷時は「Low」に設定されています。
供給制限	給電電力の上限を設定します。(200mW 単位) 工場出荷時は「Auto」に設定されています。

[適用] ボタンをクリックして、変更を反映します。

2.7.3 PoE スケジュール設定

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

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

図 2-22 PoE スケジュール設定

[PoE スケジュール設定] 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
PoE スケジュールグローバルステータス	PoE スケジューラのグローバル設定を有効または無効に設定します。
インデックス	PoE スケジューラのインデックス番号を設定します。
状態	インデックス毎の PoE スケジュール機能の状態を有効または無効に設定します。
名前	PoE スケジュール名称を設定します。
分類子	PoE スケジュールのクラスを設定します。選択する値は **[Daily]**、**[Weekly]**、**[Monthly]** および **[Datelist]** です。
時間	PoE スケジュールが実行される時間を設定します。
日付	PoE スケジュールが実行される日付または曜日を設定します。
ポートリストインデックス	PoE スケジュールが実行されるポートリストの番号を設定します。
日付リストインデックス	PoE スケジュールが実行される日付リストの番号を表示します。
PoE アクション	PoE スケジュールのアクションを表示します。選択する値は **[OFF]**、**[ON]** および **[OFF/ON]** です。

パラメータ	概要
表示順	PoE スケジューラの表示順を設定します。選択する値は **[Index]** および **[Next Execution Time]** です。
インタフェースによるフィルター	PoE スケジューラの表示を選択したインターフェースでフィルタします。

[適用] ボタンをクリックして変更を反映します。

2.7.4 PoE スケジュールポートリスト構成

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

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

図 2-23 PoE スケジュールポートリストの構成

[PoE スケジュールポートリストの構成] 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
インデックス	PoE スケジューラのポートリストのインデックス番号を設定します。
ポートリスト	PoE スケジューラを動作させるポートを設定します。

[適用] ボタンをクリックして、変更を反映します。

2.7.5 PoE 日付リスト設定

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

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

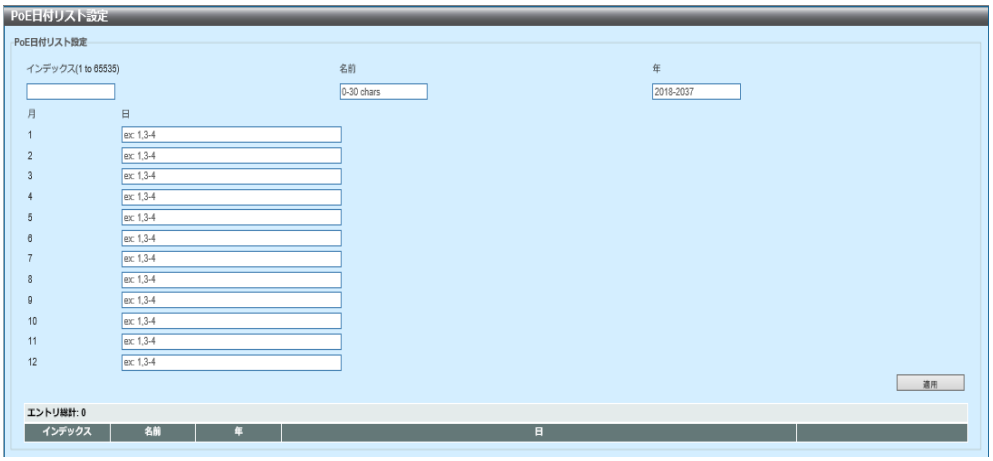


図 2-24 PoE 日付リスト設定

[PoE 日付リスト設定] 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
インデックス	PoE スケジューラの日付リストのインデックス番号を設定します。
名前	PoE スケジューラの日付リストの名前を設定します。
年	日付リストが実行される年を設定します。
日	日付リストが実行される日を月ごとに設定します。

[適用] ボタンをクリックして、変更を反映します。

2.7.6 PoE オートリブート設定

このウィンドウを用いて、PoE オートリブート設定を行います。

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

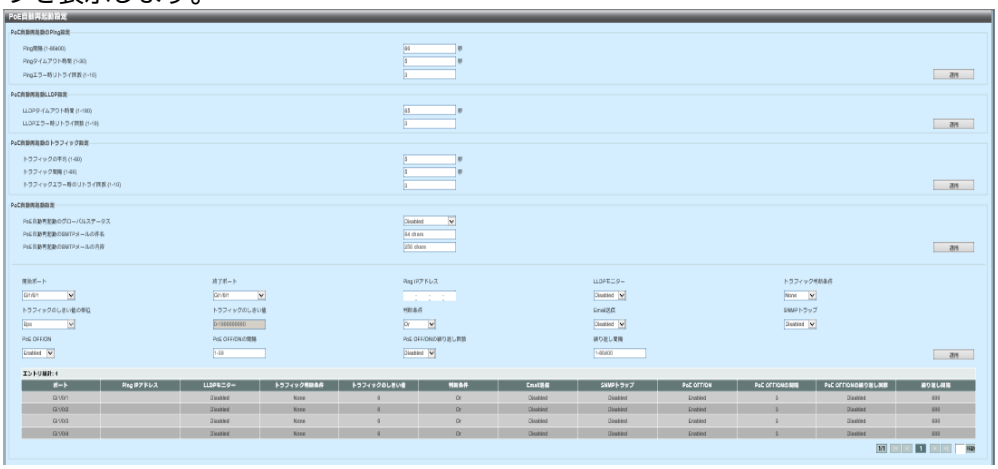


図 2-25 PoE オートリブート設定

Parameter	Overview
Ping 間隔 (1-86400)	PoE オートリブートに使用する Ping 監視 の間隔を秒単位で設定します。(工場出荷設定 60)
Ping タイムアウト (1-30)	PoE オートリブートに使用する Ping 監視のタイムアウトを秒単位で設定します。(工場出荷設定 5)
Ping エラーリトライ回数 (1-10)	PoE オートリブートに使用する Ping 監視のエラー発生時の再試行回数を設定します。(工場出荷設定 3)
LLDP タイムアウト (1-180)	PoE オートリブートに使用するオートリブート LLDP 監視タイムアウトを秒単位で設定します。(工場出荷設定 65)
LLDP エラーリトライ回数 (1-10)	PoE オートリブートに使用するオートリブート LLDP 監視エラー時の再試行回数を設定します。(工場出荷設定 3)
トラフィックの平均 (1-60)	装置内部のトラフィック平均値算出間隔を設定します。(工場出荷設定 5)
トラフィック間隔 (1-60)	トラフィック監視間隔を秒単位で設定します。(工場出荷設定 5)
トラフィックエラー時のリトライ回数 (1-10)	トラフィックエラー時の再試行回数を設定します。(工場出荷設定 3)
PoE 自動再起動のグローバルステータス	PoE オートリブートのグローバル設定を有効または無効に設定します。
PoE 自動再起動の SMTP メールの件名	PoE オートリブートの SMTP によるメール通知を行う際の件名を設定します。

Parameter	Overview
PoE 自動再起動の SMTP メールの内容	PoE オートリブートの SMTP によるメール通知を行う際の内容を設定します。
開始ポート / 終了ポート	ポート番号の範囲を選択します。
Ping IP アドレス	PoE オートリブートに使用する Ping の IP アドレスを設定します。
LLDP モニター	PoE オートリブート LLDP 監視設定を有効または無効に設定します。
トラフィック判断条件	通信料による PoE 端末異常判定を設定します。選択する値は [None]、[Below] および [Over] です。
トラフィックのしきい値の単位	トラフィックのしきい値の単位を設定します。
トラフィックのしきい値	トラフィックのしきい値を設定します。
判断条件	監視方式（Ping、LLDP、トラフィック）の異常判定を行うための条件を設定します。選択する値は [Or]、および [And] です。
Email 送信	PoE オートリブートの Email 送信設定を有効または無効に設定します。
SNMP トラップ	PoE オートリブートの SNMP トラップ設定を有効または無効に設定します。
PoE OFF/ON	PoE オートリブート異常判定時の PoE OFF/ON 実行を有効または無効に設定します。
PoE OFF/ON 間隔	PoE オートリブート異常判定時の PoE 給電 OFF/ON の間隔を設定します。
PoE OFF/ON リピート	PoE オートリブート異常判定時の PoE 給電 OFF/ON 繰り返し実行を有効または無効に設定します。
PoE OFF/ON リピート間隔	PoE オートリブート異常判定時の PoE OFF/ON 繰り返し間隔を設定します。

[適用] ボタンをクリックして、変更を反映します。

2.8 PTP（Precision Time Protocol）

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

ご注意

- GA-ML48TCPoE+（PN264892）のみ本機能に非対応となります。
- End to End（E2E）の Transparent Clock（TC）モードのみ対応しています。
- グローバルコンフィグレーションモードの PTP 設定とインターフェースコンフィグレーションモードの PTP 設定の両方を有効にする必要があります。
- 本機能はシステム内の他装置と連携して端末に要求される時刻同期を保証します。本機種・本機能のみで時刻同期を保証するものではありません。事前にシステム検証を行う必要があります。

2.8.1 PTP 設定

このウィンドウを用いて、PTP 機能の設定を行い、設定値を表示します。

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

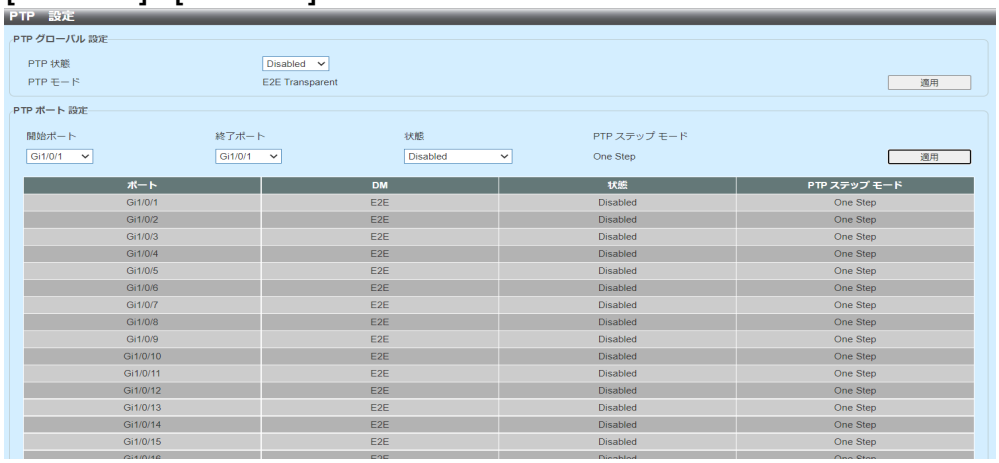


図 2-26 PTP 設定

[PTP グローバル設定] 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
PTP 状態	PTP 機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[PTP ポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの PTP 機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

3 マネジメント

3.1 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 3-27 ユーザアカウント設定（ユーザマネジメント設定）

[ユーザマネジメント設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ユーザ名	ユーザアカウント名を入力します。名前は 32 文字までです。
特権	このアカウントの特権レベルを入力します。範囲は 1 ～ 15 です。
パスワードタイプ	このユーザアカウントのパスワードタイプを選択します。選択する値は **[なし]**、**[プレーンテキスト]**、および **[SHA1 暗号化]** です。SHA は Secure Hash Algorithm の略です。
パスワード	**[プレーンテキスト]** または **[SHA1 暗号化]** をパスワードタイプとして選択した後、このユーザアカウントのパスワードを入力します。

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

[セッションテーブル] タブをクリックして、以下のウィンドウを表示します。

図 3-28 ユーザアカウント設定（セッションテーブル）

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

3.2 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。

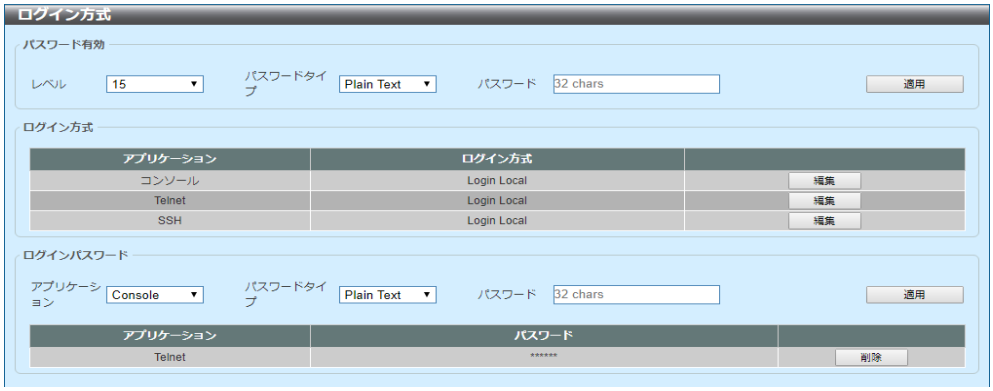


図 3-29 ログイン方式

[パスワード有効] 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
レベル	ユーザアカウントの特権レベルを選択します。範囲は 1 ～ 15 です。
パスワードタイプ	ユーザのパスワードタイプを選択します。選択する値は以下のとおりです。 • **[プレーンテキスト]** - パスワードをプレーンテキスト形式にします。これはデフォルトオプションです。 • **[暗号化]** - SHA-1 に基づいてパスワードを暗号化します。
パスワード	ユーザアカウントのパスワードを入力します。 • プレーンテキスト形式のパスワードは最大 32 文字で入力します。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。 • 暗号化形式のパスワードは最大 35 バイトで入力します。大文字と小文字は区別されます。

[適用] ボタンをクリックして、変更を反映します。
[編集] ボタンをクリックして、エントリの設定を編集します。

[ログイン方式] 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
ログイン方式	このパラメータは、[編集] ボタンをクリックすると設定可能になります。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。選択する値は以下のとおりです。 • [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。 • [ログイン] - 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。 • [ログインローカル] - 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。

[ログインパスワード] 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
アプリケーション	設定するアプリケーションを選択します。選択する値は [コンソール]、[Telnet]、および [SSH]（Secure Shell）です。
パスワードタイプ	使用するパスワード暗号化タイプを選択します。選択する値は [プレーンテキスト] および [暗号化] です。
パスワード	選択したアプリケーションのパスワードを入力します。このパスワードは、指定したアプリケーションの [ログイン方式] の設定が [ログイン] の場合に使用されます。 • プレーンテキスト形式のパスワードは最大 32 文字で入力します。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。 • 暗号化形式のパスワードは最大 35 バイトで入力します。大文字と小文字は区別されます。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.2.1 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 3-30 SNMP ビューテーブル設定

[SNMP ビュー設定] 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
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。指定可能な文字列は 32 文字までです。
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。選択する値は以下のとおりです。 • **[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] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.2.2 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 3-31 SNMP グループテーブル設定

[SNMP 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
グループ名	SNMP グループ名を入力します。名前は 32 文字までです。スペースは使用できません。
リードビュー名	グループのユーザがアクセスできるリードビュー名を入力します。
ユーザベース セキュリティモデル	セキュリティモデルを選択します。選択する値は以下のとおりです。 • **[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。

パラメータ	概要
セキュリティレベル	[ユーザベースセキュリティモデル] で **[SNMPv3]** を使用するよう選択した後、セキュリティレベルを選択します。選択する値は以下のとおりです。 • **[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。
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。
IP アドレスリスト名	グループに関連付ける標準 IP ACL（アクセスコントロールリスト）を入力します。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.2.3 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。

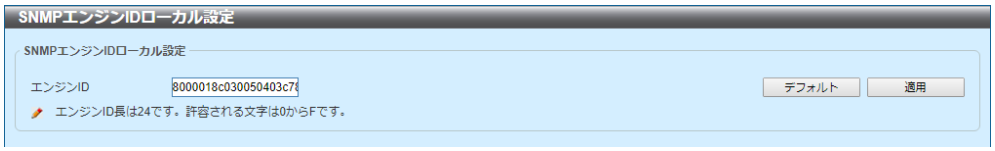


図 3-32 SNMP エンジン ID ローカル設定

[SNMP エンジン ID ローカル設定] 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
エンジン ID	SNMP エンジン ID の文字列を入力します。この文字列は 24 文字までです。

[デフォルト] ボタンをクリックして、デフォルトのエンジン ID を使用します。
[適用] ボタンをクリックして、変更を反映します。

3.2.4 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。

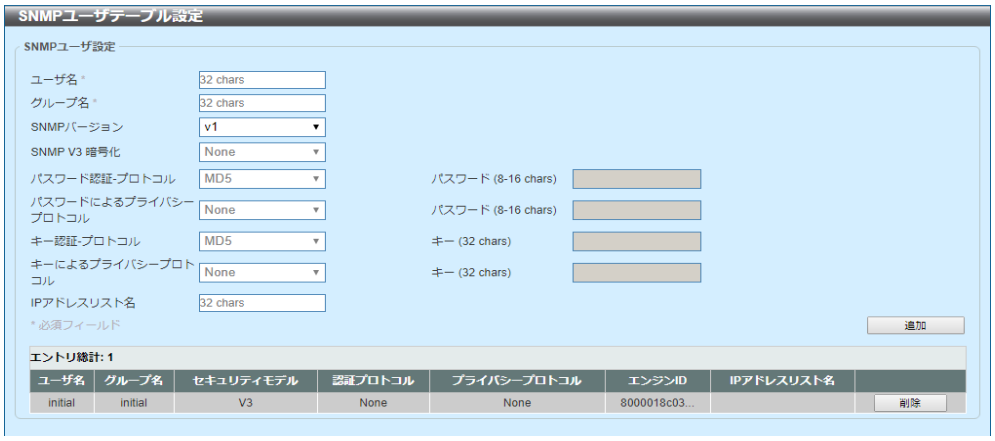


図 3-33 SNMP ユーザテーブル設定

[SNMP ユーザ設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ユーザ名	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。名前は 32 文字までです。
グループ名	ユーザの SNMP グループ名を入力します。名前は 32 文字までです。スペースは使用できません。
SNMP バージョン	SNMP バージョンを選択します。選択する値は **[v1]**、**[v2c]**、および **[v3]** です。
SNMP V3 暗号化	**[SNMP バージョン]** で **[v3]** を選択した後、SNMPv3 の暗号化タイプを選択します。選択する値は **[なし]**、**[パスワード]**、および **[キー]** です。
パスワード認証 - プロトコル	**[SNMP バージョン]** で **[v3]**、**[SNMP V3 暗号化]** で **[パスワード]** を選択した後、パスワードの認証プロトコルを選択します。選択する値は以下のとおりです。 • **[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 のパスワードは 8 ～ 16 文字です。 • SHA のパスワードは 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	**[SNMP バージョン]** で **[v3]**、**[SNMP V3 暗号化]** で **[パスワード]** を選択した後、パスワードのプライベートプロトコルを選択します。選択する値は以下のとおりです。 • **[なし]** - 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。 • **[なし]** を選択した場合、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	**[SNMP バージョン]** で **[v3]**、**[SNMP V3 暗号化]** で **[キー]** を選択した後、キーの認証プロトコルを選択します。選択する値は以下のとおりです。 • **[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 のキーは 32 文字です。 • SHA のキーは 40 文字です。
キーによるプライバシープロトコル	**[SNMP バージョン]** で **[v3]**、**[SNMP V3 暗号化]** で **[キー]** を選択した後、キーのプライベートプロトコルを選択します。選択する値は以下のとおりです。 • **[なし]** - 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。 • **[なし]** を選択した場合、このフィールドは無効になります。 • DES56 のキーは 32 文字です。
IP アドレスリスト名	ユーザに関連付ける標準 IP ACL を入力します。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.2.5 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 3-34 SNMP ホストテーブル設定

[SNMP ホスト設定] 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
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。選択する値は以下のとおりです。 • **[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]** で **[SNMPv3]** を選択した後、セキュリティレベルを選択します。選択する値は以下のとおりです。 • **[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。デフォルトのポート番号は 162 です。範囲は 1 ～ 65535 です。ポート番号によっては、他のプロトコルと競合する場合があります。

パラメータ	概要
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。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.3 RMON（リモートモニタリング）

3.3.1 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 3-35 RMON グローバル設定

[RMON グローバル設定] 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
RMON 上昇アラームトラップ	RMON 上昇アラームトラップ機能を有効または無効にします。
RMON 下降アラームトラップ	RMON 下降アラームトラップ機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

3.3.2 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。

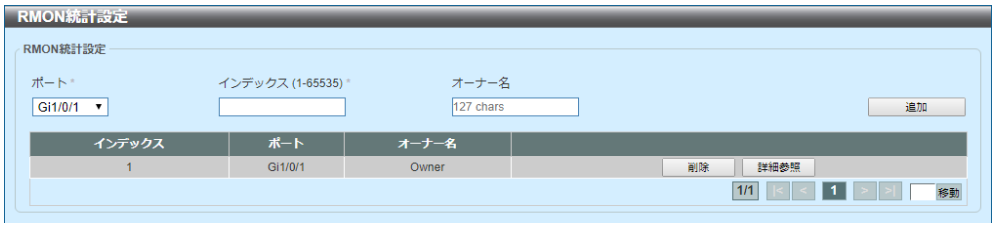


図 3-36 RMON 統計設定

[RMON 統計設定] 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
ポート	使用する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。値の範囲は 1 ～ 65535 です。
オーナー	オーナー文字列を入力します。文字列は 127 文字までです。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

図 3-37 RMON 統計設定（詳細参照）

[戻る] ボタンをクリックして、前のウィンドウに戻ります。

3.3.3 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 3-38 RMON ヒストリ設定

[RMON ヒストリ設定] 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
ポート	使用する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。範囲は 1 ～ 65535 です。
パケット数	統計の RMON 収集ヒストリグループに指定したバケットの数を入力します。範囲は 1 ～ 65535 です。デフォルト値は 50 です。
間隔	各ポーリング周期の間隔時間を入力します。範囲は、1 ～ 3600 秒です。
オーナー	オーナー文字列を入力します。文字列は 127 文字までです。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

[**詳細参照**] ボタンをクリックして、以下のウィンドウを表示します。

図 3-39 RMON ヒストリ設定（詳細参照）

[**戻る**] ボタンをクリックして、前のウィンドウに戻ります。

3.3.4 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 3-40 RMON アラーム設定

[RMON アラーム設定] 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
インデックス	アラームインデックスを入力します。範囲は 1 ～ 65535 です。
間隔	変数のサンプリングおよび閾値との照合の間隔を秒単位で入力します。有効な範囲は 1 ～ 2147483648 秒です。
変数	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を選択します。選択する値は **[アブソリュート]** および **[差分]** です。
上昇閾値	上昇閾値を 0 ～ 2147483647 の範囲で入力します。
下降閾値	下降閾値を 0 ～ 2147483647 の範囲で入力します。
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。有効な範囲は 1 ～ 65535 です。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。
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。有効な範囲は 1 ～ 65535 です。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。
オーナー	オーナー文字列を最大 127 文字で入力します。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.3.5 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 3-41 RMON イベント設定

[RMON イベント設定] 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。範囲は 1 ～ 65535 です。
概要	RMON イベントエントリの概要説明を入力します。文字列は 127 文字までです。
タイプ	RMON イベントエントリのタイプを選択します。選択する値は **[なし]**、**[ログ]**、**[トラップ]**、および **[ログとトラップ]** です。
コミュニティ	コミュニティ文字列を入力します。文字列は 127 文字までです。
オーナー	オーナー文字列を入力します。文字列は 127 文字までです。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。
[ビューログ] ボタンをクリックして、指定したエントリに関連付けられているログエントリを表示します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

[ビューログ] ボタンをクリックして、以下のウィンドウを表示します。

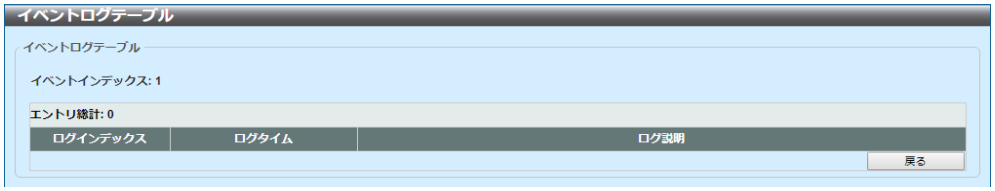


図 3-42 RMON イベント設定（ビューログ）)

[戻る] ボタンをクリックして、前のウィンドウに戻ります。

3.4 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。

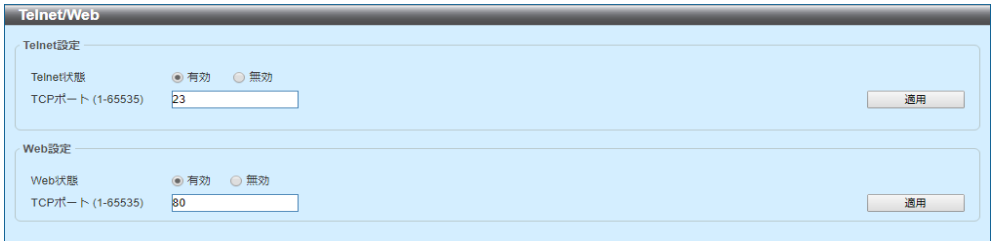


図 3-43 Telnet/Web

[Telnet 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
Telnet 状態	Telnet サーバ機能を有効または無効にします。
ポート	装置の Telnet 管理に使用する TCP（Transmission Control Protocol）ポート番号を入力します。Telnet プロトコルで通常利用する TCP ポートは 23 です。

[適用] ボタンをクリックして、変更を反映します。

[Web 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
Web 状態	Web を介した設定を有効または無効にします。
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。Telnet プロトコルで通常利用する TCP ポートは 80 です。

[適用] ボタンをクリックして、変更を反映します。

3.5 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 3-44 セッションタイムアウト

[セッションタイムアウト] 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
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を秒単位で入力します。**[デフォルト]** チェックボックスをオンにした場合、デフォルト値に戻ります。値の範囲は 60 ～ 36000 秒です。デフォルト値は 180 秒です。
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を分単位で入力します。**[デフォルト]** チェックボックスをオンにした場合、デフォルト値に戻ります。値の範囲は 0 ～ 1439 分です。0 を入力すると、タイムアウトが無効になります。デフォルト値は 3 分です。
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を分単位で入力します。**[デフォルト]** チェックボックスをオンにした場合、デフォルト値に戻ります。値の範囲は 0 ～ 1439 分です。0 を入力すると、タイムアウトが無効になります。デフォルト値は 3 分です。
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を分単位で入力します。**[デフォルト]** チェックボックスをオンにした場合、デフォルト値に戻ります。値の範囲は 0 ～ 1439 分です。0 を入力すると、タイムアウトが無効になります。デフォルト値は 3 分です。

[適用] ボタンをクリックして、変更を反映します。

3.6 DHCP オート設定

このウィンドウを用いて、DHCP オート設定機能を有効または無効にします。

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

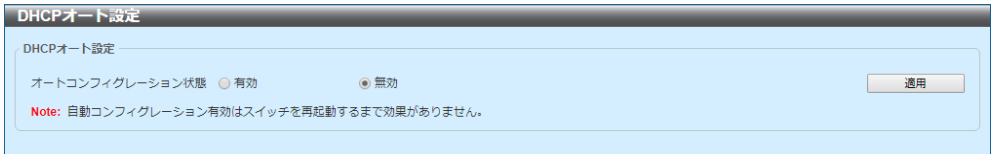


図 3-45 DHCP オート設定

[DHCP オート設定] 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
オートコンフィグレーション状態	DHCP オート設定機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

3.7 DNS (Domain Name System)

3.7.1 DNS グローバル設定

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

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

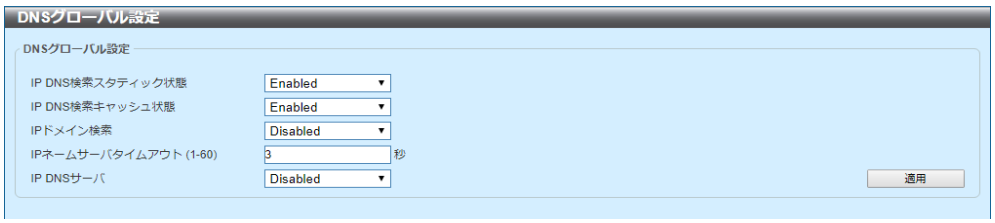


図 3-46 DNS グローバル設定

[DNS グローバル設定] 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
IP DNS 検索スタティック状態	IP DNS 検索スタティック状態を有効または無効にします。
IP DNS 検索キャッシュ状態	IP DNS 検索キャッシュ状態を有効または無効にします。
IP ドメイン検索	IP ドメイン検索状態を有効または無効にします。
IP ネームサーバタイムアウト	指定したネームサーバからの応答を待つ最大時間を入力します。この値は、1 ～ 60 秒の範囲で指定します。
IP DNS サーバ	DNS サーバ機能をグローバルに有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

3.7.2 DNS ネームサーバ設定

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

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

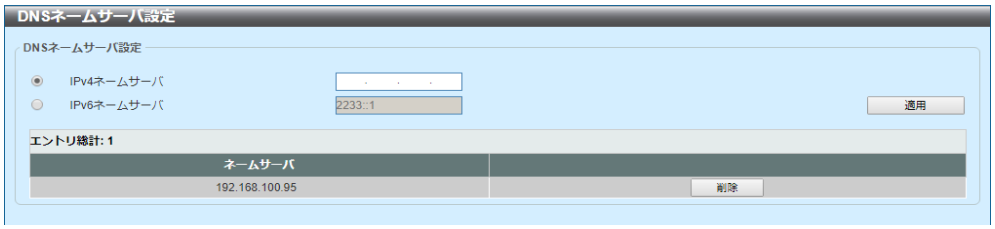


図 3-47 DNS ネームサーバ設定

[DNS ネームサーバ設定] 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
IPv4 ネームサーバ	DNS サーバの IPv4 アドレスを選択および入力します。
IPv6 ネームサーバ	DNS サーバの IPv6 アドレスを選択および入力します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

3.7.3 DNS ホスト設定

このウィンドウを用いて、DNS ホストの設定を行い、設定値を表示します。

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

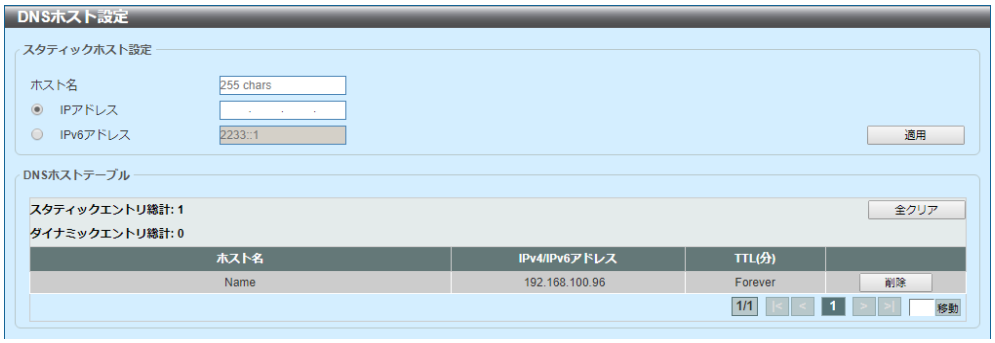


図 3-48 DNS ホスト設定

[スタティックホスト設定] 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
ホスト名	DNS ホストの名前を入力します。
IP アドレス	DNS ホストの IPv4 アドレスを選択および入力します。
IPv6 アドレス	DNS ホストの IPv6 アドレスを選択および入力します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[全クリア] ボタンをクリックして、テーブルからすべてのダイナミックエントリをクリアします。
[削除] ボタンをクリックして、エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

3.8 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 3-49 ファイルシステム

以下のパラメータを設定できます。

パラメータ	概要
パス	パス文字列を入力します。

[移動] ボタンをクリックして、入力したパスに移動します。
[コピー] ボタンをクリックして、特定のファイルをファイルシステムにコピーします。
ドライブリンク（c:）をクリックして、C: ドライブに移動します。

ドライブリンク（c:）をクリックして、以下のウィンドウを表示します。

図 3-50 ファイルシステム（c:）

[以前の] ボタンをクリックして、前のウィンドウに戻ります。
[ディレクトリ作成] ボタンをクリックして、ファイルシステムに新しいディレクトリを作成します。

[ブートアップ] ボタンをクリックして、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] ボタンをクリックして、特定のファイル名をリネームします。
[削除] ボタンをクリックして、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] ボタンをクリックして、以下のウィンドウを表示します。

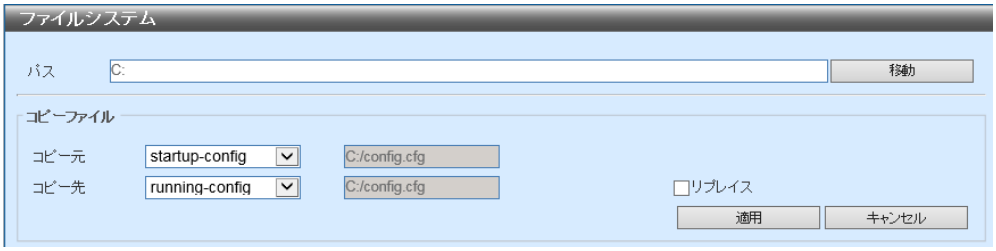


図 3-51 ファイルシステム（コピー）

以下のパラメータを設定できます。

パラメータ	概要
コピー元	コピー元のファイルのタイプを選択します。選択する値は [startup-config] および [Source File] です。[Source File] オプション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を選択します。選択する値は [startup-config]、[running-config]、および [Destination File] です。[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] ボタンをクリックして、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] ボタンをクリックして、コピーをキャンセルします。

3.9 SMTP 設定

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

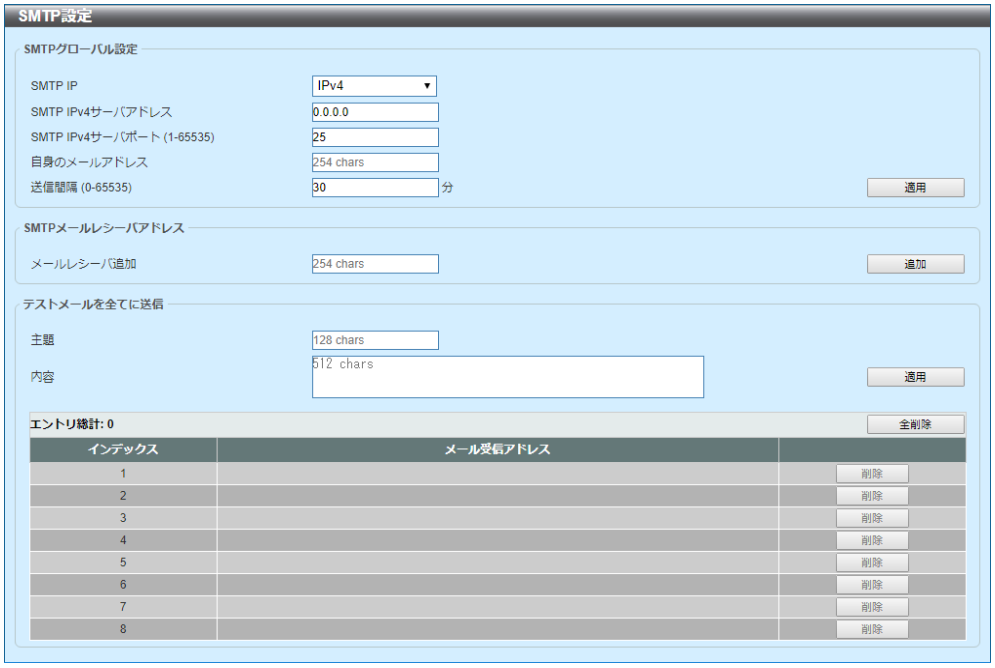


図 3-52 SMTP 設定

[SMTP グローバル設定] 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
SMTP IP	SMTP サーバの IP アドレスタイプを選択します。選択する値は **[IPv4]** および **[IPv6]** です。
SMTP IPv4 サーバアドレス	**[SMTP IP]** で **[IPv4]** を選択した後、SMTP サーバの IPv4 アドレスを入力します。
SMTP IPv6 サーバアドレス	**[SMTP IP]** で **[IPv6]** を選択した後、SMTP サーバの IPv6 アドレスを入力します。
SMTP IPv4 サーバポート	**[SMTP IP]** で **[IPv4]** を選択した後、SMTP サーバのポート番号を入力します。範囲は 1 ～ 65535 です。デフォルトでは、この値は 25 です。
SMTP IPv6 サーバポート	**[SMTP IP]** で **[IPv6]** を選択した後、SMTP サーバのポート番号を入力します。範囲は 1 ～ 65535 です。デフォルトでは、この値は 25 です。
自身のメールアドレス	スイッチを表すメールアドレスを入力します。この文字列は 254 文字までです。

パラメータ	概要
送信間隔	送信間隔の値を入力します。範囲は、0 ～ 65535 分です。デフォルトでは、この値は 30 分です。

[適用] ボタンをクリックして、変更を反映します。

[SMTP メールレシーバアドレス] 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
メールレシーバ追加	レシーバのメールアドレスを入力します。この文字列は 254 文字までです。

[テストメールを全てに送信] 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
件名	メールの件名を入力します。この文字列は 128 文字までです。
内容	メールの本文を入力します。この文字列は 512 文字までです。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[適用] ボタンをクリックして、変更を反映します。
[全削除] ボタンをクリックして、すべてのエントリからすべてのレシーバメールアドレスを削除します。
[削除] ボタンをクリックして、指定したエントリからレシーバメールアドレスを削除します。

3.10 NLB FDB 設定

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

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

図 3-53 NLB FDB 設定

[NLB FDB 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
NLB タイプ	NLB タイプを選択します。選択する値は **[ユニキャスト]** および **[マルチキャスト]** です。
VID	**[NLB タイプ]** で **[マルチキャスト]** を選択した後、使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
MAC アドレス	エントリのユニキャストまたはマルチキャスト MAC アドレスを入力します。受信したパケットのディスティネーション MAC アドレスが、指定した MAC アドレスと一致する場合、そのパケットは指定したインタフェースに転送されます。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更内容を反映します。
[全削除] ボタンをクリックして、すべてのエントリを削除します。
[削除] ボタンをクリックして、エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

3.11 IP アドレス簡単設定機能

3.11.1 IP 簡単設定プロトコル設定

このウィンドウを用いて、IP アドレス簡単設定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。

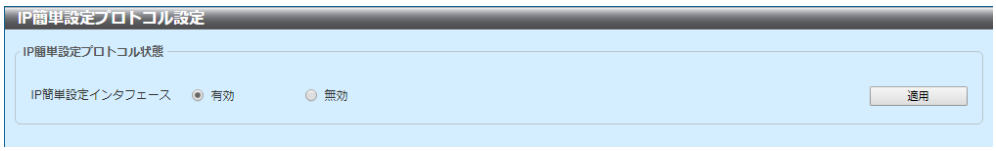


図 3-54 IP 簡単設定プロトコル設定

[IP 簡単設定プロトコル状態] 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
IP 簡単設定インタフェース	IP アドレス簡単設定機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

4 L2 機能

4.1 FDB（フォワーディングデータベース）

4.1.1 スタティック FDB

4.1.1.1 ユニキャストスタティック FDB

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

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

図 4-1 ユニキャストスタティック FDB

[ユニキャストスタティック FDB] 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
ポート / 廃棄	**[ポート]** オプションを選択した場合、入力した MAC アドレスが存在するポートを使用します。 **[廃棄]** オプションを選択した場合、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	**[ポート]** オプションを選択した後、使用するポートを選択します。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
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] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[全削除] ボタンをクリックして、すべてのエントリを削除します。

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

4.1.1.2 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。

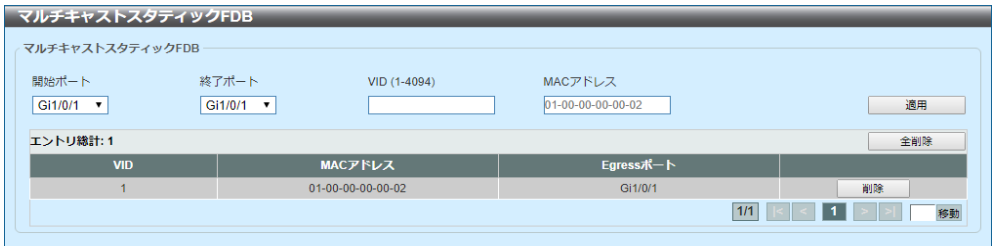


図 4-2 マルチキャストスタティック FDB

[マルチキャストスタティック FDB] セクションでは、以下のパラメータを設定できます。

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

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[全削除] ボタンをクリックして、すべてのエントリを削除します。
[削除] ボタンをクリックして、エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

4.1.2 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 4-3 MAC アドレステーブル設定（グローバル設定）

[グローバル設定] 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
エージング時間	MAC アドレステーブルのエージング時間を入力します。範囲は、10 ～ 1000000 秒です。0 を入力すると、MAC アドレスのエージングは無効になります。デフォルトでは、この値は 300 秒です。
エージングディスティネーションヒット	エージングディスティネーションヒット機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

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

図 4-4 MAC アドレステーブル設定（MAC アドレスポート学習設定）

[MAC アドレスポート学習設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの MAC アドレス学習機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

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

図 4-5 MAC アドレステーブル設定（MAC アドレス VLAN 学習設定）

[MAC アドレス VLAN 学習設定] 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
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。範囲は 1 ～ 4094 です。
状態	指定した VLAN の MAC アドレス学習機能を有効または無効にします。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。

[VLAN 学習検索 MAC アドレス] 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。範囲は 1 ～ 4094 です。

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

4.1.3 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。

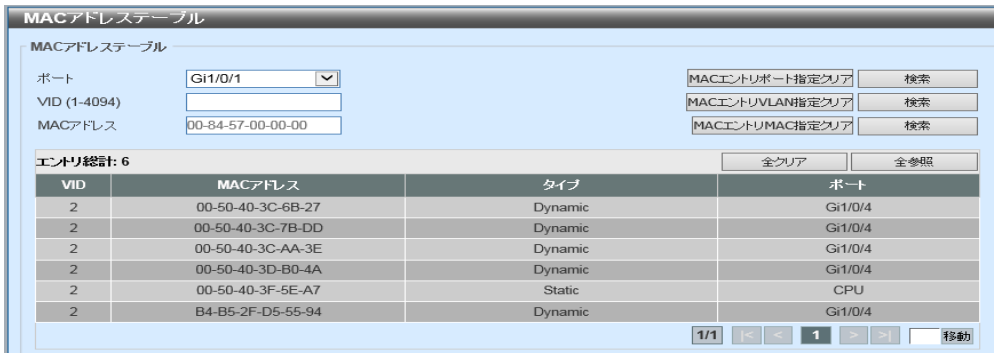


図 4-6 MAC アドレステーブル

[MAC アドレステーブル] 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
ポート	設定するポート番号を選択します。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
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。

[ポート単位ダイナミッククリア] ボタンをクリックして、指定したポートに関連付けられているすべてのダイナミック MAC アドレスをクリアします。
[VLAN 単位ダイナミッククリア] ボタンをクリックして、指定した VLAN に関連付けられているすべてのダイナミック MAC アドレスをクリアします。
[MAC 単位ダイナミッククリア] ボタンをクリックして、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] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全クリア] ボタンをクリックして、すべてのエントリをテーブルからクリアします。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

4.1.4 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 4-7 MAC 通知（MAC 通知設定）

[MAC 通知グローバル設定] 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
MAC アドレス通知	MAC 通知をスイッチ上でグローバルに有効または無効にします。
間隔	通知間隔の時間を入力します。範囲は、1 ～ 2147483647 秒です。デフォルトでは、この値は 1 秒です。
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。範囲は 0 ～ 500 です。デフォルトでは、この値は 1 です。
MAC 通知トラップ状態	MAC 通知トラップ状態を有効または無効にします。
開始ポート - 終了ポート	使用するポートを選択します。
追加トラップ	選択したポートへのトラップ追加を有効または無効にします。
削除トラップ	選択したポートからのトラップ削除を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[MAC 通知ヒストリ] タブをクリックして、以下のウィンドウを表示します。

図 4-8 MAC 通知（MAC 通知ヒストリ）

4.2 VLAN (Virtual Local Area Network)

4.2.1 802.1Q 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 4-9 802.1Q VLAN

[802.1Q 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 List	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。範囲は 1 ～ 4094 です。
インターネットマンション	インターネットマンション設定を有効または無効に設定します。
アップリンクポート	インターネットマンションの有効時、アップリンクポートを最大 2 ポートまで指定します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいて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。範囲は 1 ～ 4094 です。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。

[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。
[編集] ボタンをクリックして、エントリの設定を編集します。
[削除] ボタンをクリックして、エントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

4.2.2 802.1v プロトコル VLAN

4.2.2.1 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。

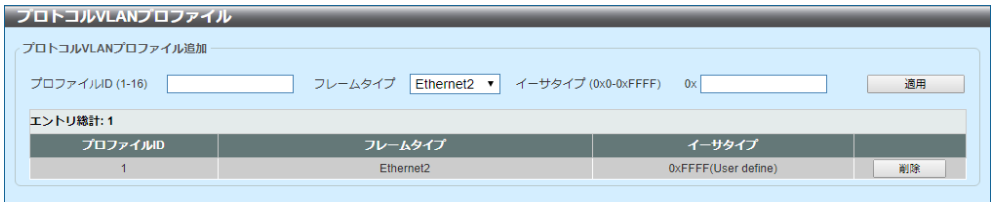


図 4-10 プロトコル VLAN プロファイル

[プロトコル VLAN プロファイル追加] 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
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。範囲は 1 ～ 16 です。
フレームタイプ	フレームタイプのオプションを選択します。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。選択する値は **[イーサネット 2]**、**[SNAP]**、および **[LLC]** です。SNAP は Subnetwork Access Protocol の略です。LLC は Logical Link Control の略です。
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。範囲は 0x0 ～ 0xFFFF です。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。 • イーサネット 2 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。 • IEEE802.3 SNAP の場合、16 ビット（2 オクテット）の 16 進数値です。 • IEEE802.3 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] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

4.2.2.2 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 4-11 プロトコル VLAN プロファイルインタフェース

[新プロトコル VLAN インタフェース追加] 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
ポート	設定するスイッチのポート番号を選択します。
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。範囲は 1 ～ 4094 です。
優先度	使用する優先度の値を選択します。この値は、0 ～ 7 の範囲で指定します。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] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

4.2.3 GVRP

4.2.3.1 GVRP グローバル

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

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

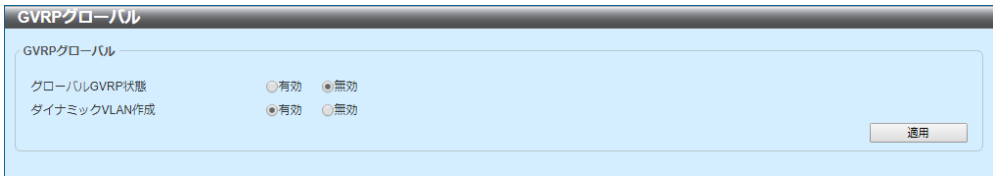


図 4-12 GVRP グローバル

[GVRP グローバル] 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
グローバル GVRP 状態	グローバル GVRP 状態を有効または無効にします。
ダイナミック VLAN 作成	ダイナミック VLAN 作成機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

4.2.3.2 GVRP ポート

このウィンドウを用いて、GVRP ポートの設定を行い、設定値を表示します。

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

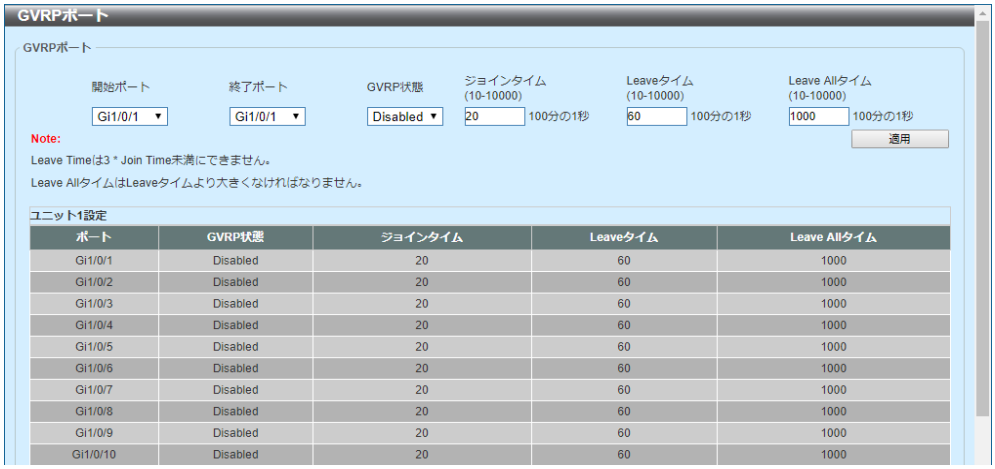


図 4-13 GVRP ポート

[GVRP ポート] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
GVRP 状態	GVRP ポート状態を有効または無効にします。これにより、ポートがダイナミックに VLAN のメンバになることができます。デフォルトでは、このオプションは無効です。
ジョインタイム	ジョインタイム値を入力します。範囲は 10 ～ 10000 センチ秒です。デフォルトでは、この値は 20 センチ秒です。
Leave タイム	Leave タイム値を入力します。範囲は 10 ～ 10000 センチ秒です。デフォルトでは、この値は 60 センチ秒です。
Leave All タイム	Leave All タイム値を入力します。範囲は 10 ～ 10000 センチ秒です。デフォルトでは、この値は 1000 センチ秒です。

[適用] ボタンをクリックして、変更を反映します。

4.2.3.3 GVRP アドバタイズ VLAN

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

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

図 4-14 GVRP アドバタイズ VLAN

[GVRP アドバタイズ 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
開始ポート - 終了ポート	使用するポートを選択します。
アクション	ポートマッピングアクションに使用するアドバタイズ VLAN を選択します。選択する値は **[全]**、**[追加]**、**[削除]**、および **[リプレイス]** です。**[全]** を選択すると、すべてのアドバタイズ VLAN が使用されます。
アドバタイズ VID リスト	アドバタイズする VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、変更を反映します。

4.2.3.4 GVRP 禁止 VLAN

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

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

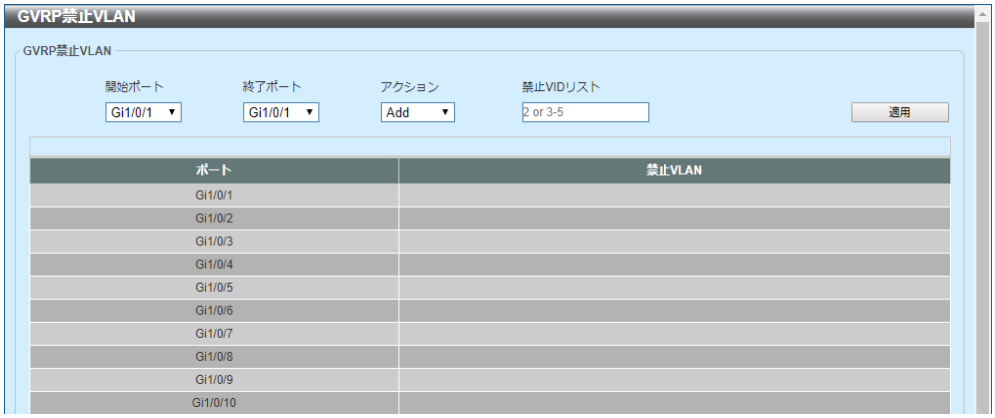


図 4-15 GVRP 禁止 VLAN

[GVRP 禁止 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
開始ポート - 終了ポート	使用するポートを選択します。
アクション	ポートマッピングアクションに使用する禁止 VLAN を選択します。選択する値は **[全]**、**[追加]**、**[削除]**、および **[リプレイス]** です。**[全]** を選択すると、禁止されたすべての VLAN が使用されます。
禁止 VID リスト	禁止する VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、変更を反映します。

4.2.3.5 GVRP 統計テーブル

このウィンドウを用いて、GVRP 統計を表示およびクリアします。

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

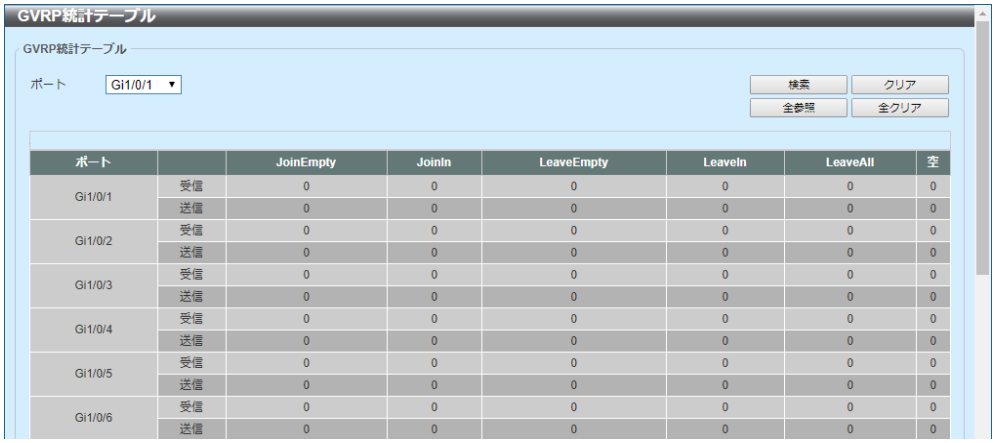


図 4-16 GVRP 統計テーブル

[GVRP 統計テーブル] 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
ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[クリア] ボタンをクリックして、指定したポートから統計情報をクリアします。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。
[全クリア] ボタンをクリックして、すべてのポートからすべての統計情報をクリアします。

4.2.4 アシンメトリック VLAN

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

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

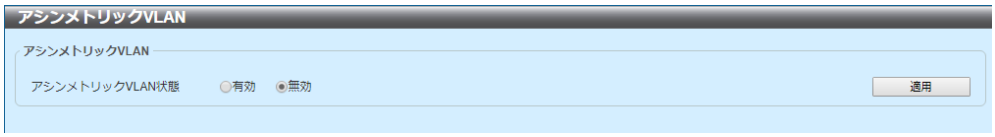


図 4-17 アシンメトリック VLAN

[アシンメトリック 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
アシンメトリック VLAN 状態	アシンメトリック VLAN 機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

4.2.5 MAC VLAN

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

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

図 4-18 MAC VLAN

[MAC 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
MAC アドレス	Enter ユニキャスト MAC アドレスを入力します。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
優先度	アンタグパケットに割り当てる優先度を選択します。この値は、0 ～ 7 の範囲で指定します。

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

4.2.6 VLAN インタフェース

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

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

図 4-19 VLAN インタフェース

[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。
[編集] ボタンをクリックして、エントリの設定を編集します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

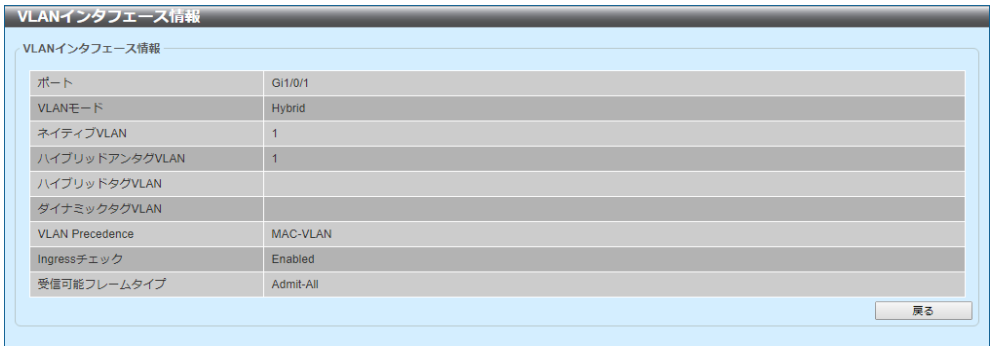


図 4-20 VLAN インタフェース（詳細参照）

[戻る] ボタンをクリックして、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。

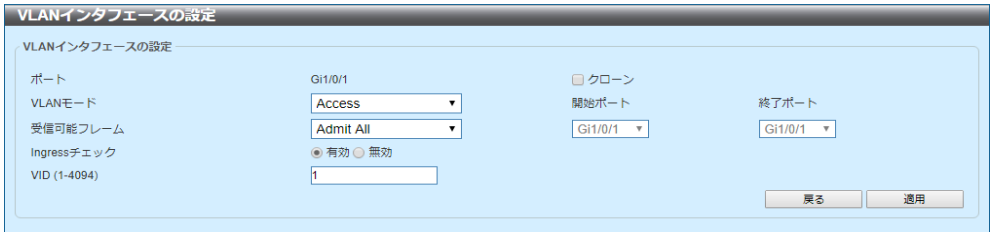


図 4-21 VLAN インタフェース（編集、アクセス）

[VLAN インタフェースの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VLAN モード	VLAN モードのオプションを選択します。選択する値は [アクセス]、[ハイブリッド]、[Trunk]、[プロミスキャス]、および [ホスト] です。
受信可能フレーム	受信可能フレームの動作オプションを選択します。選択する値は [タグのみ]、[アンタグのみ]、および [全受付] です。
Ingress チェック	Ingress チェック機能を有効または無効にします。
VLAN ID	この設定に使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
クローン	このオプションを選択した場合、クローン機能を有効にします。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更を反映します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

[VLAN モード] で [ハイブリッド] を選択して、以下のウィンドウを表示します。

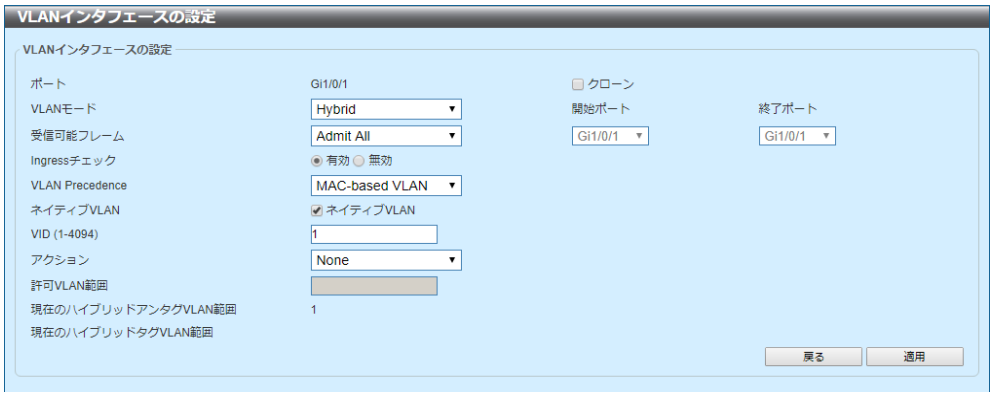


図 4-22 VLAN インタフェース（編集、ハイブリッド）

[VLAN インタフェースの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VLAN モード	VLAN モードのオプションを選択します。選択する値は **[アクセス]**、**[ハイブリッド]**、**[Trunk]**、**[プロミスキャス]**、および **[ホスト]** です。
受信可能フレーム	受信可能フレームの動作オプションを選択します。選択する値は **[タグのみ]**、**[アンタグのみ]**、および **[全受付]** です。
Ingress チェック	Ingress チェック機能を有効または無効にします。
VLAN Precedence	VLAN Precedence のオプションを選択します。選択する値は **[MAC ベース VLAN]** および **[サブネットベース VLAN]** です。
ネイティブ VLAN	このオプションをオンにした場合、ネイティブ VLAN 機能が有効になります。
VID	このパラメータは、**[ネイティブ VLAN]** オプションをオンにすると利用可能になります。 使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
アクション	実行するアクションを選択します。選択する値は **[なし]**、**[追加]**、**[削除]**、**[タグ]**、および **[アンタグ]** です。
モード追加	**[アンタグ]** と **[タグ]** のどちらのパラメータを追加するかを選択します。
許可 VLAN 範囲	許可 VLAN 範囲を入力します。
クローン	このオプションを選択した場合、クローン機能を有効にします。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更を反映します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

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

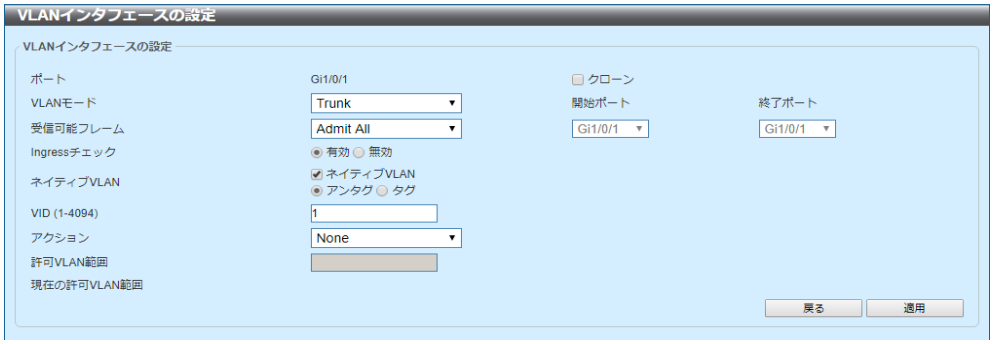


図 4-23 VLAN インタフェース（編集、Trunk）

[VLAN インタフェースの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VLAN モード	VLAN モードのオプションを選択します。選択する値は **[アクセス]**、**[ハイブリッド]**、**[Trunk]**、**[プロミスキャス]**、および **[ホスト]** です。
受信可能フレーム	受信可能フレームの動作オプションを選択します。選択する値は **[タグのみ]**、**[アンタグのみ]**、および **[全受付]** です。
Ingress チェック	このパラメータは、**[VLAN モード]** で **[Trunk]** を選択すると利用可能になります。Ingress チェック機能を有効または無効にします。
ネイティブ VLAN	このオプションをオンにした場合、ネイティブ VLAN 機能が有効になります。また、この VLAN でサポートするフレームとして **[アンタグ]** か **[タグ]** を選択します。
VID	このパラメータは、**[ネイティブ VLAN]** オプションをオンにすると利用可能になります。 使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
アクション	実行するアクションを選択します。選択する値は **[なし]**、**[全]**、**[追加]**、**[削除]**、**[Except]**、および **[リプレイス]** です。
許可 VLAN 範囲	許可 VLAN 範囲を入力します。
クローン	このオプションを選択した場合、クローン機能を有効にします。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更を反映します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

[VLAN モード] で **[プロミスキャス]** を選択して、以下のウィンドウを表示します。

図 4-24 VLAN インタフェース（編集、プロミスキャス）

[VLAN インタフェースの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VLAN モード	VLAN モードのオプションを選択します。選択する値は **[アクセス]**、**[ハイブリッド]**、**[Trunk]**、**[プロミスキャス]**、および **[ホスト]** です。
受信可能フレーム	受信可能フレームの動作オプションを選択します。選択する値は **[タグのみ]**、**[アンタグのみ]**、および **[全受付]** です。
Ingress チェック	Ingress チェック機能を有効または無効にします。
クローン	このオプションを選択した場合、クローン機能を有効にします。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更を反映します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

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

図 4-25 VLAN インタフェース（編集、ホスト）

[VLAN インタフェースの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
VLAN モード	VLAN モードのオプションを選択します。選択する値は **[アクセス]**、**[ハイブリッド]**、**[Trunk]**、**[プロミスキャス]**、および **[ホスト]** です。
受信可能フレーム	受信可能フレームの動作オプションを選択します。選択する値は **[タグのみ]**、**[アンタグのみ]**、および **[全受付]** です。
Ingress チェック	Ingress チェック機能を有効または無効にします。
クローン	このオプションを選択した場合、クローン機能を有効にします。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更を反映します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

4.2.7 サブネット VLAN

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

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

図 4-26 サブネット VLAN

[サブネット 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
IPv4 ネットワークプレフィックス / プレフィックス長	サブネット VLAN の IPv4 アドレスとプレフィックス長の値を選択および入力します。
IPv6 ネットワークプレフィックス / プレフィックス長	サブネット VLAN の IPv6 アドレスとプレフィックス長の値を選択および入力します。
VID	使用するサブネット VLAN ID を入力します。範囲は 1 ～ 4094 です。
優先度	使用する優先度の値を選択します。この値は、0 ～ 7 の範囲で指定します。値が小さいほど、優先度が高くなります。

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

4.2.8 音声 VLAN

4.2.8.1 音声 VLAN グローバル

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

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

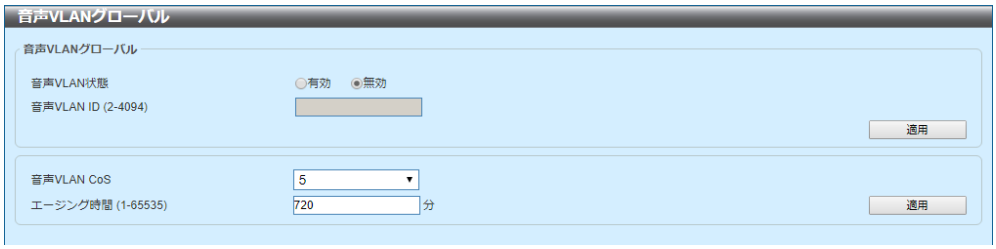


図 4-27 音声 VLAN グローバル

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

[適用] ボタンをクリックして、変更を反映します。

4.2.8.2 音声 VLAN ポート

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

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

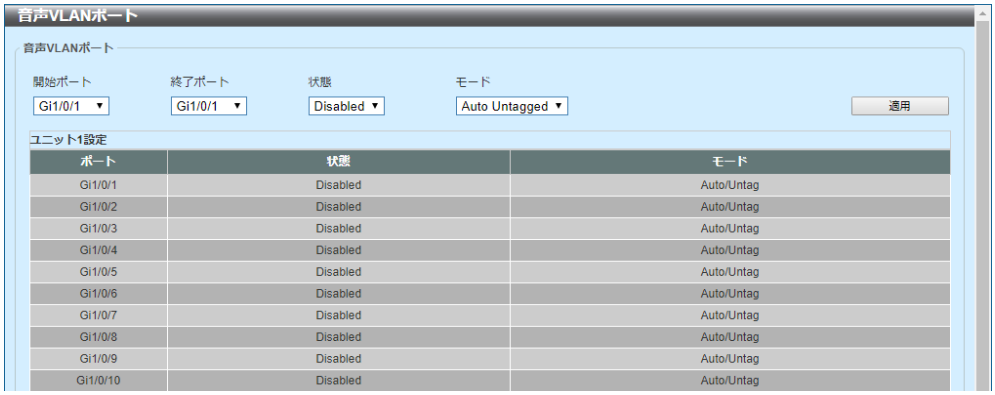


図 4-28 音声 VLAN ポート

[音声 VLAN ポート] セクションでは、以下のパラメータを設定できます。

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

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

[適用] ボタンをクリックして、変更を反映します。

4.2.8.3 音声 VLAN OUI

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

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

図 4-29 音声 VLAN OUI

[音声 VLAN OUI] 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
OUI アドレス	音声 VLAN OUI の MAC アドレスを入力します。
マスク	音声 VLAN OUI の MAC アドレスに対する一致ビットマスクを入力します。
概要	ユーザ定義 OUI の MAC アドレスに対する概要説明を入力します。この文字列は 32 文字までです。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、エントリを削除します。

4.2.8.4 音声 VLAN 装置

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

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

図 4-30 音声 VLAN 装置

4.2.8.5 音声 VLAN LLDP-MED 装置

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

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

図 4-31 音声 VLAN LLDP-MED 装置

4.2.9 プライベート VLAN

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

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

図 4-32 プライベート VLAN

[プライベート 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 リスト	使用するプライベート VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。範囲は 1 ～ 4094 です。
状態	プライベート VLAN 状態を有効または無効にします。
タイプ	作成するプライベート VLAN のタイプを選択します。選択する値は **[コミュニティ]**、**[Isolated]**、および **[プライマリ]** です。

[適用] ボタンをクリックして、変更を反映します。

[プライベート **VLAN** アソシエーション] 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 リスト	使用するプライベート VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。範囲は 1 ～ 4094 です。
アクション	プライベート VLAN で実行するアクションを選択します。選択する値は **[追加]**、**[削除]**、および **[無効]** です。
セカンダリ **VID** リスト	使用するセカンダリプライベート VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、変更を反映します。

[プライベート **VLAN** ホストアソシエーション] セクションでは、以下のパラメータを設定できます。

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

[適用] ボタンをクリックして、変更を反映します。

[プライベート **VLAN** マッピング] セクションでは、以下のパラメータを設定できます。

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

[適用] ボタンをクリックして、変更を反映します。

4.3 STP (Spanning Tree Protocol)

4.3.1 STP グローバル設定

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

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

図 4-33 STP グローバル設定

[STP 状態] 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
STP 状態	グローバル STP 状態を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[STP モード] 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
STP モード	使用する STP モードを選択します。選択する値は **[MSTP]**、**[RSTP]**、および **[STP]** です。 MSTP は Multiple Spanning Tree Protocol の略です。 RSTP は Rapid Spanning Tree Protocol の略です。 STP は Spanning Tree Protocol の略です。

[適用] ボタンをクリックして、変更を反映します。

[STP 優先度] 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
優先度	STP 優先度値を選択します。この値は、0 ～ 61440 の範囲で指定します。デフォルトでは、この値は 32768 です。値が小さいほど、優先度が高くなります。

[適用] ボタンをクリックして、変更を反映します。

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

[適用] ボタンをクリックして、変更を反映します。

4.3.2 STP ポート設定

このウィンドウを用いて、STP ポートの設定を行い、設定値を表示します。

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

図 4-34 STP ポート設定

[STP ポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
コスト	コスト値を入力します。範囲は 1 ～ 200000000 です。この値は、指定したポートリストへのフォワーディングパケットの相対コストを示すメトリックを定義します。ポートコストは、自動的にあるいはメトリック値として設定できます。デフォルト値は [0]（自動）です。外部コストに 0 を設定すると、最適効率のリストにおいて、指定したポートへのフォワーディングパケットのスピードが自動的に設定されます。100Mbps ポートのデフォルトポートコストは 200000、Gigabit ポートは 20000 です。数が小さくなるほど、ポートがパケットを転送するよう選択される可能性が高くなります。
状態	STP ポート状態を有効または無効にします。
ガードルート	ガードルート機能を有効または無効にします。
リンクタイプ	リンクタイプオプションを選択します。選択する値は **[自動]**、**[P2P]**、および **[シェア]** です。全二重ポートは P2P（ポイントツーポイント）接続があるものとみなされます。一方、半二重ポートは共有接続があるものとみなされます。リンクタイプを **[シェア]** に設定すると、ポートはフォワーディング状態に迅速に移行できません。デフォルトでは、このオプションは **[自動]** です。

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

[適用] ボタンをクリックして、変更を反映します。

4.3.3 MST コンフィグレーション識別

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

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

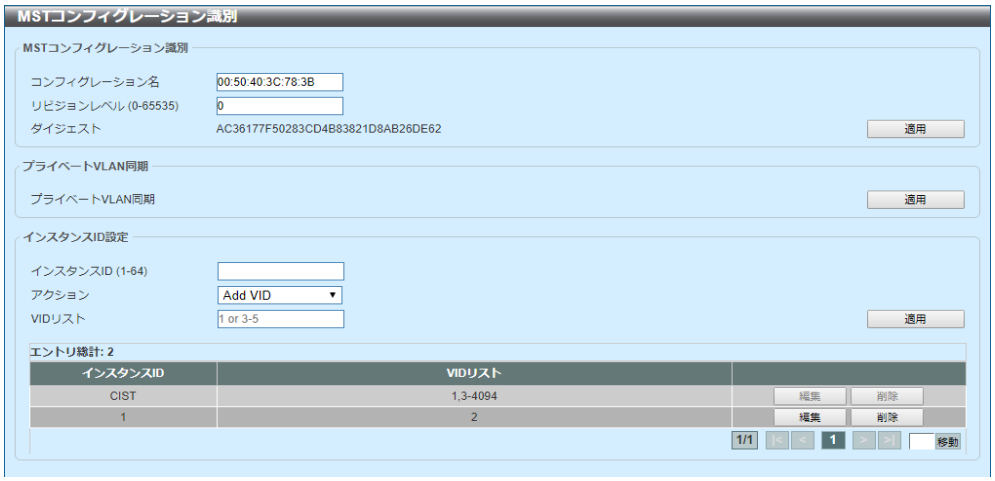


図 4-35 MST コンフィグレーション識別

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

[適用] ボタンをクリックして、変更を反映します。

[インスタンス ID 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
インスタンス ID	インスタンス ID を入力します。範囲は 1 ～ 64 です。
アクション	実行するアクションを選択します。選択する値は **[VID 追加]** および **[VID 削除]** です。
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。範囲は 1 ～ 4094 です。

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

4.3.4 STP インスタンス

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

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

図 4-36 STP インスタンス

[STP インスタンス] 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
インスタンス優先度	**[編集]** ボタンをクリックした後、インスタンス優先度の値を入力します。範囲は 0 ～ 61440 です。

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

4.3.5 MSTP ポートインフォメーション

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

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

図 4-37 MSTP ポートインフォメーション

[MSTP ポートインフォメーション] 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
ポート	使用するポートを選択します。
コスト	**[編集]** ボタンをクリックした後、コスト値を入力します。範囲は 1 ～ 200000000 です。
優先度	**[編集]** ボタンをクリックした後、優先度の値を入力します。選択する値の範囲は **[0]** ～ **[240]** です。デフォルトでは、このオプションは 128 です。値が小さいほど、優先度が高くなります。

[検知プロトコルクリア] ボタンをクリックして、検出されたプロトコルの関連付けを指定のポートから削除します。
[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[編集] ボタンをクリックして、エントリの設定を編集します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

4.4 ループ検知・遮断

4.4.1 ループ検知・遮断の設定

このウィンドウを用いて、ループ検知・遮断の設定を行い、設定値を表示します。

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

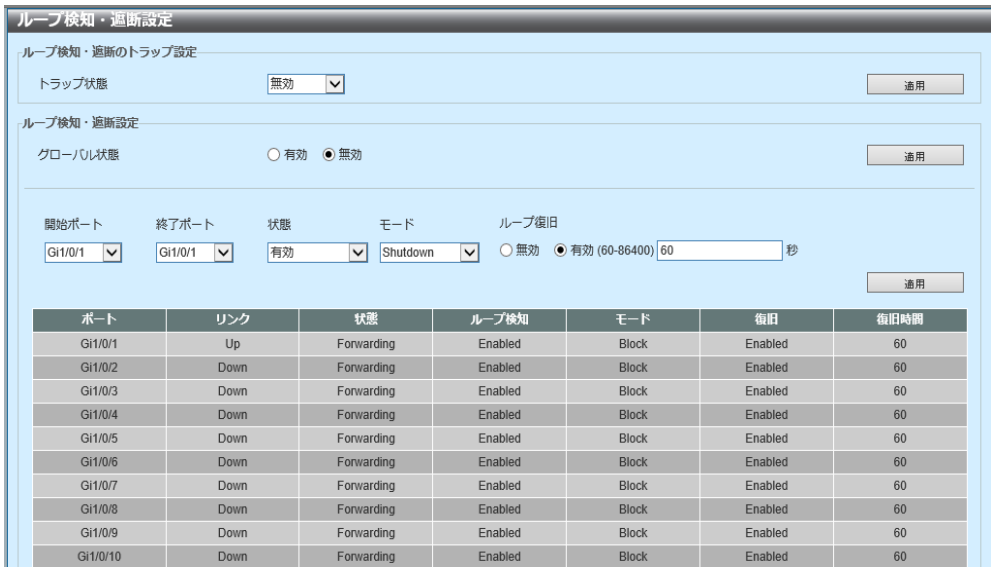


図 4-38 ループ検知・遮断設定

[ループ検知・遮断設定] 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
グローバル状態	ループ検知・遮断機能をグローバルに有効または無効にします。
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの回線ループバック機能を有効または無効にします。
モード	指定したポートで使用するループ検知・遮断モードを選択します。選択する値は以下のとおりです。: • **[シャットダウン]** - 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。 • **[ブロック]** - ループ発生時に、ポートを直接ブロッキング状態に設定します。
ループ復旧	ループ復旧機能を有効または無効にします。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。範囲は、60 ～ 86400 秒です。

[適用] ボタンをクリックして、変更を反映します。

4.4.2 ループヒストリーログ

このウィンドウを用いて、ループヒストリーログを表示およびクリアします。

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

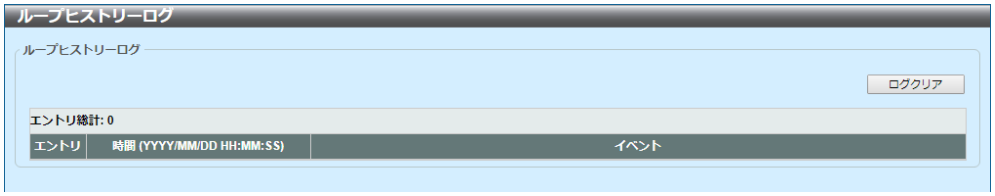


図 4-39 ループヒストリーログ

[ログクリア] ボタンをクリックして、テーブルからログエントリをクリアします。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

4.5 リンクアグリゲーション

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

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

図 4-40 リンクアグリゲーション

最初のセクションでは、以下のパラメータを設定できます。

パラメータ	概要
システム優先度	使用するシステム優先度の値を入力します。範囲は 1 ～ 65535 です。デフォルトでは、この値は 32768 です。システム優先度によって、ポートチャネルに参加可能なポート、およびスタンドアロンモードになるポートが決定します。値が小さいほど、優先度が高くなります。同じ優先度を持つポートが 2 つ以上ある場合、ポート番号によって優先度が決まります。
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を選択します。選択する値は **[ソース MAC]**、**[ディスティネーション MAC]**、**[ソースディスティネーション MAC]**、**[ソース IP]**、**[ディスティネーション IP]**、**[ソースディスティネーション IP]**、**[ソース L4 ポート]**、**[ディスティネーション L4 ポート]**、および **[ソースディスティネーション L4 ポート]** です。デフォルトでは、このオプションは **[ソースディスティネーション MAC]** です。

[適用] ボタンをクリックして、変更を反映します。

[チャネルグループ情報] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。範囲は 1 ～ 32 です。物理ポートが初めてチャネルグループに参加すると、自動的にポートチャネルが作成されます。1 つのインタフェースが参加できるチャネルグループは 1 つだけです。
モード	モードのオプションを選択します。選択する値は **[スタティック]**、**[アクティブ]**、および **[パッシブ]** です。**[スタティック]** モードを指定した場合、チャネルグループタイプはスタティックです。**[アクティブ]** モードまたは **[パッシブ]** モードを指定した場合、チャネルグループタイプは LACP（Link Aggregation Control Protocol）です。1 つのチャネルグループを構成するのは、スタティックメンバまたは LACP メンバのいずれかのみとなります。チャネルグループのタイプが決定した後は、他のタイプのインタフェースはそのチャネルグループに参加できません。

[追加] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[メンバポート削除] ボタンをクリックして、指定したポートチャネルからメンバポートを削除します。
[チャネル削除] ボタンをクリックして、エントリを削除します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

図 4-41 リンクアグリゲーション（詳細参照）

[編集] ボタンをクリックして、エントリの設定を編集します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

4.6 L2 プロトコルトンネル

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

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

図 4-42 L2 プロトコルトンネル（L2 プロトコルトンネルグローバル設定）

[L2 プロトコルトンネルグローバル設定] 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
カプセル化パケット CoS	カプセル化パケットの CoS 値を選択します。この値は、0 ～ 7 の範囲で指定します。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。
廃棄閾値	廃棄閾値を入力します。範囲は 100 ～ 20000 です。デフォルトでは、この値は 0 です。レイヤ 2 プロトコルパケットのトンネリングでは、パケットの暗号化、復号、転送に CPU の処理能力が消費されます。このオプションを用いて、CPU の処理帯域幅の消費量を制限します。システムで処理可能なすべてのレイヤ 2 プロトコルパケットの数に対して、閾値を指定します。パケットの最大数を超過したプロトコルパケットは破棄されます。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。これにより、L2PT（Layer 2 Protocol Tunneling）のトンネリングマルチキャストアドレスを、指定したプロトコルに追加、あるいは指定したプロトコルから削除します。

パラメータ	概要
トンネルプロトコル	トンネルプロトコルを選択します。選択する値は以下のとおりです。 • **[GVRP]** - 設定済みのアドレスに GVRP パケットがトンネリングされます。 • **[STP]** - 設定済みのアドレスに STP パケットがトンネリングされます。 • **[MAC]** - 指定したディスティネーションアドレスを持つプロトコルパケットが、設定したアドレスにトンネリングされます。 • **[全]** - 設定済みのアドレスにすべてのパケットがトンネリングされます。
プロトコル MAC	**[トンネルプロトコル]** として **[MAC]** オプションを選択した後、設定したアドレスにトンネリングされるディスティネーションアドレスを選択します。選択する値は **[01-00-0C-CC-CC-CC]** と **[01-00-0C-CC-CC-CD]** です。
MAC アドレス	指定したプロトコルのトンネリング先の MAC アドレスを入力します。この MAC アドレスには、他のプロトコルで予約または使用されているアドレスは指定できません。

[適用] ボタンをクリックして、変更を反映します。

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

図 4-43 L2 プロトコルトンネル（L2 プロトコルトンネルポート設定）

[L2 プロトコルトンネルポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
アクション	**[追加]** を選択して、入力した情報に基づいて新しいエントリを追加します。 **[削除]** を選択して、入力した情報に基づいてエントリを削除します。
タイプ	タイプのオプションを選択します。選択する値は **[なし]**、**[シャットダウン]**、および **[廃棄]** です。

パラメータ	概要
トンネルプロトコル	トンネルプロトコルのオプションを選択します。選択する値は **[GVRP]**、**[STP]**、**[プロトコル MAC]**、および **[全]** です。
プロトコル MAC	**[トンネルプロトコル]** として **[プロトコル MAC]** オプションを選択すると、以下のオプションが有効になります。プロトコル MAC のオプションを選択します。選択する値は **[01-00-0C-CC-CC-CC]** と **[01-00-0C-CC-CC-CD]** です。
閾値	このパラメータは、**[タイプ]** フィールドで **[シャットダウン]** または **[廃棄]** オプションを選択すると利用可能になります。閾値を入力します。範囲は 1 ～ 4096 です。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[全クリア] ボタンをクリックして、すべてのエントリから情報をクリアします。
[クリア] ボタンをクリックして、エントリから情報をクリアします。

4.7 L2 マルチキャスト制御

4.7.1 IGMP スヌーピング

4.7.1.1 IGMP スヌーピング設定

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

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

図 4-44 IGMP スヌーピング設定

[グローバル設定] 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
グローバル状態	IGMP スヌーピングをグローバルに有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[VLAN 状態設定] 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
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。

[IGMP スヌーピングテーブル] 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。範囲は 1 ～ 4094 です。

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

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

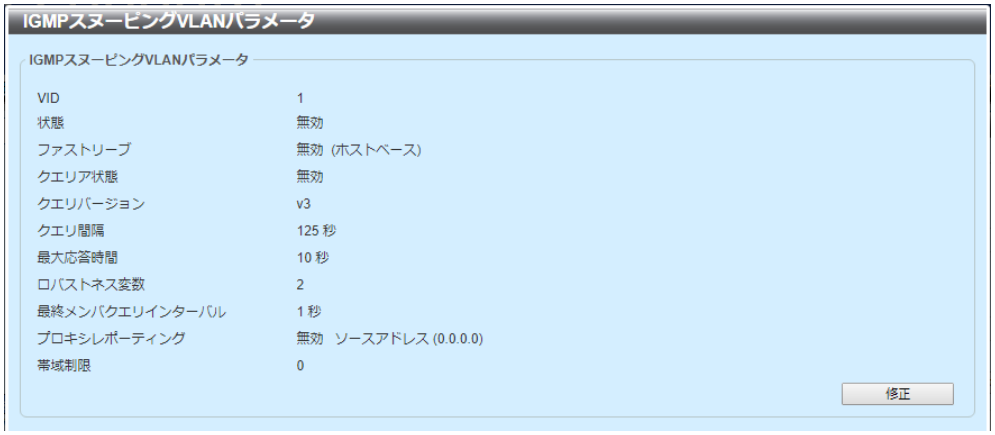


図 4-45 IGMP スヌーピング設定（詳細参照）

[編集] ボタンをクリックして、設定を編集します。

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

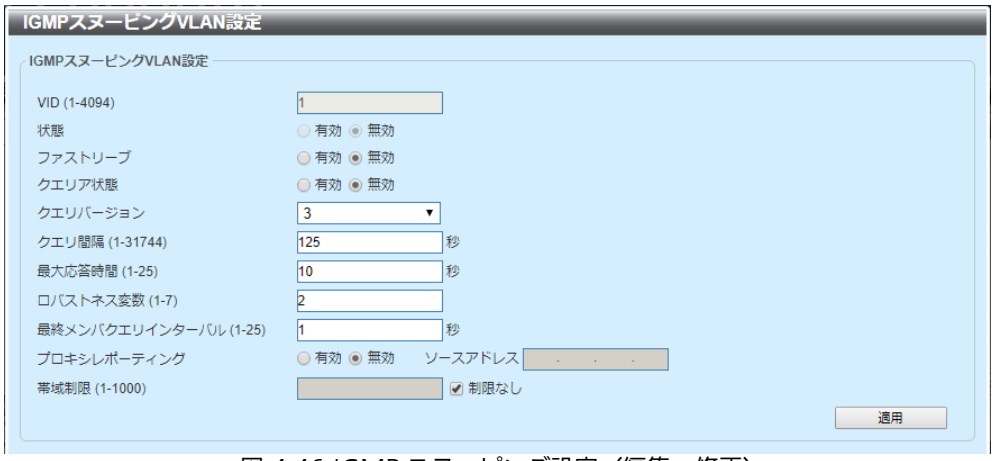


図 4-46 IGMP スヌーピング設定（編集、修正）

[IGMP スヌーピング VLAN 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
ファストリーブ	IGMP スヌーピング高速脱退機能を有効または無効にします。有効にした場合、システムで IGMP 脱退メッセージを受信すると、ただちにメンバを脱退させます。
クエリア状態	クエリア状態を有効または無効にします。
クエリバージョン	IGMP スヌーピングクエリアが送信する一般的なクエリパケットバージョンを選択します。選択する値は **[1]**、**[2]**、および **[3]** です。
クエリ間隔	IGMP の一般的なクエリメッセージを IGMP スヌーピングクエリアが周期的に送信する間隔を入力します。範囲は 1 ～ 31744 です。
最大応答時間	IGMP スヌーピングクエリでアドバタイズされている最大応答時間（秒）を入力します。範囲は 1 ～ 25 です。
ロバストネス変数	IGMP スヌーピングで使用するロバストネス変数を入力します。範囲は 1 ～ 7 です。
最終メンバクエリインターバル	IGMP スヌーピングクエリアによる、IGMP グループ固有またはグループソース固有の（チャネル）クエリメッセージの送信間隔を入力します。範囲は 1 ～ 25 です。
プロキシレポーティング	プロキシレポート機能を有効または無効にします。
ソースアドレス	プロキシレポーティングのソース IP アドレスを入力します。このオプションは、**[プロキシレポーティング]** で **[有効]** を選択すると有効になります。
帯域制限	帯域制限値を入力します。範囲は 1 ～ 1000 です。 **[制限なし]** オプションをオンにした場合、このプロファイルに帯域制限を適用しません。

[適用] ボタンをクリックして、変更を反映します。

4.7.1.2 IGMP スヌーピンググループ設定

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

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

図 4-47 IGMP スヌーピンググループ設定

[IGMP スヌーピングスタティックグループ設定] 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
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
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	使用するポートを選択します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[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 を選択および入力します。範囲は 1 ～ 4094 です。
グループアドレス	ラジオボタンをクリックし、IP マルチキャストグループアドレスを入力します。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。

[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。

[IGMP スヌーピンググループテーブル] 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 を選択および入力します。範囲は 1 ～ 4094 です。
グループアドレス	ラジオボタンをクリックし、IP マルチキャストグループアドレスを入力します。
詳細	IGMP グループの詳細情報を表示します。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。

4.7.1.3 IGMP スヌーピングフィルタ設定

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

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

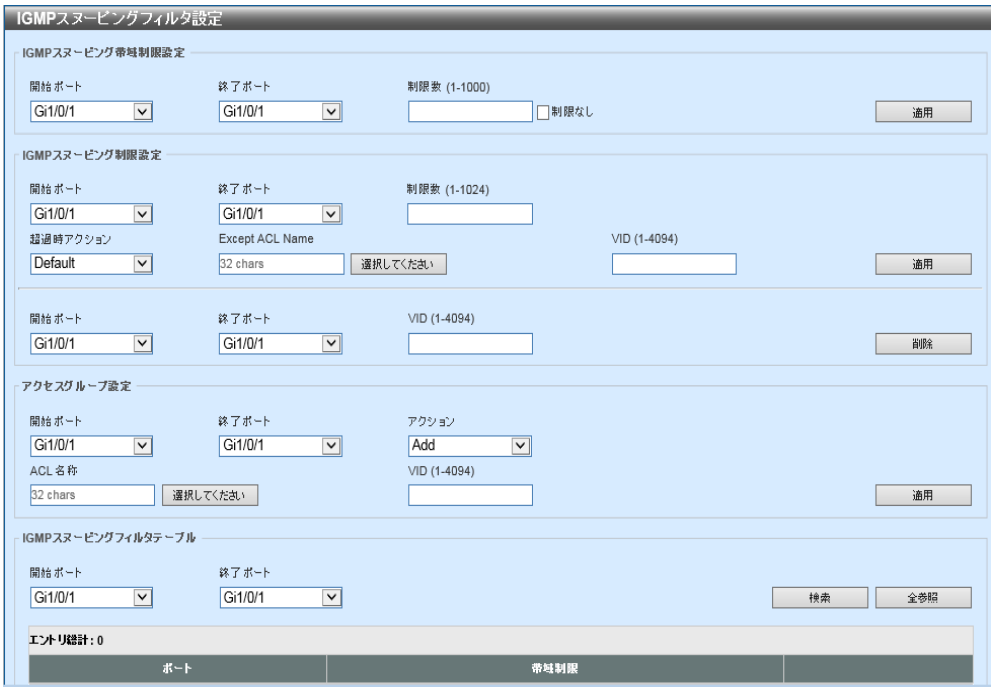


図 4-48 IGMP スヌーピングフィルタ設定

[IGMP スヌーピング帯域制限設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。これは、**[ポート]** オプションを以下のアクションとして選択した場合にのみ利用可能です。
制限数	制限数を入力します。特定のインタフェース上でスイッチが処理できる IGMP 制御パケットのレートを設定します。範囲は 1 ～ 1000 パケット / 秒です。**[制限なし]** オプションを選択した場合、制限を取り除きます。

[適用] ボタンをクリックして、変更を反映します。

[IGMP スヌーピング制限設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
制限数	制限数を入力します。このパラメータを用いて、作成可能な IGMP キャッシュエントリの数を制限します。範囲は 1 ～ 4096 です。
超過時アクション	超過時アクションを選択します。このパラメータを用いて、制限超過時に新たに認識されるグループを処理するための動作を指定します。選択する値は以下のとおりです。 • **[デフォルト]** - デフォルトのアクションが実行されます。 • **[廃棄]** - 新しいグループがドロップされます。 • **[リプレイス]** - 新しいグループが最も古いグループと置き換わります。
Except ACL Name	標準 IP アクセスリストの名前を入力します。アクセスリストで許可されているグループ（*,G）またはチャネル（S,G）は、制限から除外されます。チャネル（S,G）を許可するには、アクセスリストエントリのソースアドレスのフィールドに「S」と指定し、ディスティネーションアドレスのフィールドに「G」と指定します。グループ（*,G）を許可するには、アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。名前は 32 文字までです。あるいは、**[選択してください。]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

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

[適用] ボタンをクリックして、変更を反映します。

[IGMP スヌーピングフィルタテーブル] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

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

[**詳細参照**] ボタンをクリックして、以下のウィンドウを表示します。

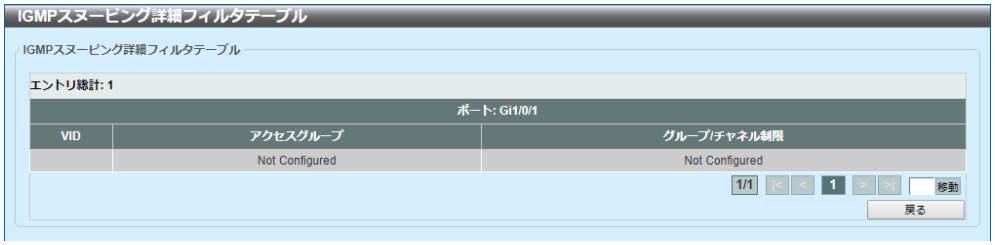


図 4-49 IGMP スヌーピングフィルタ設定（詳細参照）

複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。
[**戻る**] ボタンをクリックして、前のウィンドウに戻ります。

4.7.1.4 IGMP スヌーピングマルチキャストルータ情報

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

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

図 4-50 IGMP スヌーピングマルチキャストルータ情報

[IGMP スヌーピングマルチキャストルータポート設定] セクションでは、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。範囲は 1 ～ 4094 です。
コンフィグレーション	ポートコンフィグレーションを選択します。選択する値は以下のとおりです。 • **[ポート]** - 設定したポートをスタティックマルチキャストルータポートにします。 • **[禁止ポート]** - 設定したポートをマルチキャストルータポートにしません。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[IGMP スヌーピングマルチキャストルータポートテーブル] セクションでは、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。範囲は 1 ～ 4094 です。

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

4.7.1.5 IGMP スヌーピング統計設定

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

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

図 4-51 IGMP スヌーピング統計設定

[IGMP スヌーピング統計設定] 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
統計	インタフェースを選択します。選択する値は **[全]**、**[VLAN]**、および **[ポート]** です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。このオプションは、**[統計]** ドロップダウンリストで **[VLAN]** を選択した場合に利用可能です。
開始ポート - 終了ポート	使用するポートを選択します。このオプションは、**[統計]** ドロップダウンリストで **[ポート]** を選択した場合に利用可能です。

[クリア] ボタンをクリックして、指定した条件に基づいて統計情報をクリアします。

[IGMP スヌーピング統計テーブル] 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
検索タイプ	インタフェースのタイプを選択します。選択する値は **[VLAN]** および **[ポート]** です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 このオプションは、**[検索タイプ]** ドロップダウンリストで **[VLAN]** を選択した場合に利用可能です。
開始ポート - 終了ポート	使用するポートを選択します。 このオプションは、**[検索タイプ]** ドロップダウンリストで **[ポート]** を選択した場合に利用可能です。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。

4.7.2 MLD スヌーピング

4.7.2.1 MLD スヌーピング設定

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

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

図 4-52 MLD スヌーピング設定

[グローバル設定] 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
グローバル状態	MLD スヌーピングのグローバル状態を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[VLAN 状態設定] 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
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。

[MLD スヌーピングテーブル] 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。範囲は 1 ～ 4094 です。

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

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

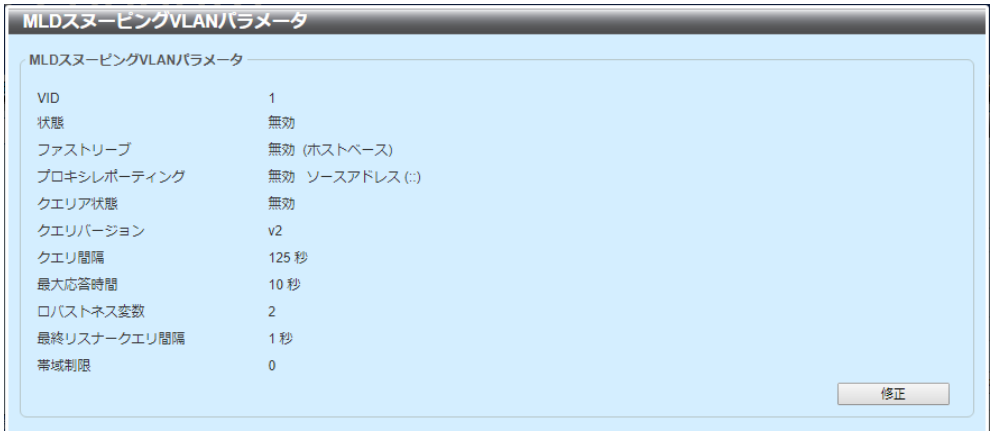


図 4-53 MLD スヌーピング設定（詳細参照）

[編集] ボタンをクリックして、設定を編集します。

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

図 4-54 MLD スヌーピング設定（編集、修正）

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

[適用] ボタンをクリックして、変更を反映します。

4.7.2.2 MLD スヌーピンググループ設定

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

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

図 4-55 MLD スヌーピンググループ設定

[MLD スヌーピングスタティックグループ設定] 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
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。
グループアドレス	IPv6 マルチキャストグループアドレスを入力します。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[MLD スヌーピングスタティックグループテーブル] セクションでは、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 を選択および入力します。範囲は 1 ～ 4094 です。
グループアドレス	ラジオボタンをクリックし、IPv6 マルチキャストグループアドレスを入力します。

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

[MLD スヌーピンググループテーブル] 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 を選択および入力します。範囲は 1 ～ 4094 です。
グループアドレス	ラジオボタンをクリックし、IPv6 マルチキャストグループアドレスを入力します。
詳細	このオプションを選択した場合、MLD グループの詳細情報を表示します。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。

4.7.2.3 MLD スヌーピングフィルタ設定

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

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

図 4-56 MLD スヌーピングフィルタ設定

[MLD スヌーピング帯域制限設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。これは、**[ポート]** オプションを以下のアクションとして選択した場合にのみ利用可能です。
制限数	制限数を入力します。この制限数を用いて、特定のインタフェース上でスイッチが処理できる MLD 制御パケットのレートを設定します。範囲は 1 ～ 1000 パケット / 秒です。**[制限なし]** オプションを選択した場合、制限を取り除きます。

[適用] ボタンをクリックして、変更を反映します。

[MLD スヌーピング制限設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
制限数	制限数を入力します。このパラメータを用いて、作成可能な MLD キャッシュエントリの数を制限します。範囲は 1 ～ 2048 です。
超過時アクション	超過時アクションを選択します。このパラメータを用いて、制限超過時に新たに認識されるグループを処理するための動作を指定します。選択する値は以下のとおりです。 • **[デフォルト]** - デフォルトのアクションが実行されます。 • **[廃棄]** - 新しいグループがドロップされます。 • **[リプレイス]** - 新しいグループが最も古いグループと置き換わります。
Except ACL Name	標準 IP アクセスリストの名前を入力します。アクセスリストで許可されているグループ（*,G）またはチャネル（S,G）は、制限から除外されます。チャネル（S,G）を許可するには、アクセスリストエントリのソースアドレスのフィールドに「S」と指定し、ディスティネーションアドレスのフィールドに「G」と指定します。グループ（*,G）を許可するには、アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。名前は 32 文字までです。あるいは、**[選択してください。]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[アクセスグループ設定] 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
開始ポート - 終了ポート	使用するポートを選択します。
アクション	**[追加]** を選択して、入力した情報に基づいて新しいエントリを追加します。 **[削除]** を選択して、入力した情報に基づいてエントリを削除します。

パラメータ	概要
ACL 名称	標準 IP アクセスリストの名前を入力します。このパラメータを用いて、ユーザにグループ（*, G）への参加を許可します。アクセスリストエントリのソースアドレスのフィールドに「any」を指定し、ディスティネーションアドレスのフィールドに「G」と指定します。名前は 32 文字までです。あるいは、**[選択してください。]** ボタンをクリックして、この設定に使用するスイッチで設定されている既存のアクセスリストを検索し、選択します。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、変更を反映します。

[MLD スヌーピングフィルタテーブル] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

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

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

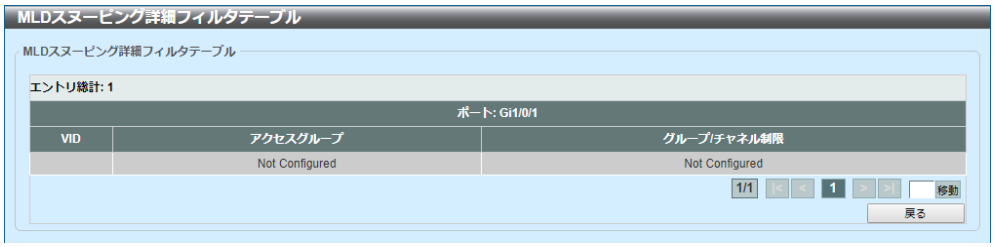


図 4-57 MLD スヌーピングフィルタ設定（詳細参照）

複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

4.7.2.4 MLD スヌーピングマルチキャストルータ情報

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

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

図 4-58 MLD スヌーピングマルチキャストルータ情報

[MLD スヌーピングマルチキャストルータポート設定] セクションでは、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。範囲は 1 ～ 4094 です。
コンフィグレーション	ポートコンフィグレーションを選択します。選択する値は以下のとおりです。 • **[ポート]** - 設定済みポートがマルチキャスト対応ルータに接続しているものとします。 • **[禁止ポート]** - 設定済みポートがマルチキャスト対応ルータに接続していないものとします。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[MLD スヌーピングマルチキャストルータポートテーブル] セクションでは、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。範囲は 1 ～ 4094 です。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。

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

4.7.2.5 MLD スヌーピング統計設定

このウィンドウを用いて、MLD スヌーピング統計を表示およびクリアします。

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

図 4-59 MLD スヌーピング統計設定

[MLD スヌーピング統計設定] 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
統計	インタフェースを選択します。選択する値は **[全]**、**[VLAN]**、および **[ポート]** です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 このオプションは、**[統計]** ドロップダウンリストで **[VLAN]** を選択した場合に利用可能です。
開始ポート - 終了ポート	使用するポートを選択します。 このオプションは、**[統計]** ドロップダウンリストで **[ポート]** を選択した場合に利用可能です。

[クリア] ボタンをクリックして、指定した条件に基づいて統計情報をクリアします。

[MLD スヌーピング統計テーブル] 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
検索タイプ	インタフェースのタイプを選択します。選択する値は **[VLAN]** および **[ポート]** です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 このオプションは、**[検索タイプ]** ドロップダウンリストで **[VLAN]** を選択した場合に利用可能です。
開始ポート - 終了ポート	使用するポートを選択します。 このオプションは、**[検索タイプ]** ドロップダウンリストで **[ポート]** を選択した場合に利用可能です。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。
[全参照] ボタンをクリックして、利用可能なエントリをすべて検索し、表示します。

4.7.3 マルチキャストフィルタリングモード

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

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

図 4-60 マルチキャストフィルタリングモード

[マルチキャストフィルタリングモード] 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 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。範囲は 1 ～ 4094 です。
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。選択する値は以下のとおりです。 • **[未登録フォワード]** - 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。 • **[全フォワード]** - すべてのマルチキャストパケットが VLAN ドメインに基づいてフラッディングされます。 • **[未登録フィルタ]** - 登録済みのパケットがフォワーディングテーブルに基づいて転送され、すべての未登録マルチキャストパケットがフィルタリングされます。

[適用] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。

4.8 LLDP (Link Layer Discovery Protocol)

4.8.1 LLDP グローバル設定

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

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

図 4-61 LLDP グローバル設定

[LLDP グローバル設定] 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
LLDP 状態	LLDP 機能を有効または無効にします。
LLDP フォワード状態	LLDP フォワード状態を有効または無効にします。**[LLDP 状態]** を無効にし、**[LLDP フォワード状態]** を有効にすると、受信した LLDPDU（LLDP Data Unit）パケットが転送されます。
LLDP トラップ状態	LLDP トラップ状態を有効または無効にします。
LLDP-MED トラップ状態	LLDP-MED（LLDP Media Endpoint Discovery）トラップ状態を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[LLDP-MED コンフィグレーション] 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
ファストスタート送信回数	LLDP-MED ファストスタート送信回数の値を入力します。範囲は 1 ～ 10 です。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。

[適用] ボタンをクリックして、変更を反映します。

[LLDP コンフィグレーション] 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
メッセージ送信間隔	各物理インタフェースでの連続する LLDP アドバタイズメント送信の間隔を入力します。範囲は、5 ～ 32768 秒です。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。
メッセージ送信ホールド乗数	LLDPDU の TTL（Time-To-Live）値の計算に使用する、LLDPDU 送信間隔の乗数を入力します。範囲は 2 ～ 10 です。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。
再初期化遅延	インタフェースでの LLDP 初期化の遅延時間を入力します。範囲は、1 ～ 10 秒です。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。
TX 遅延	インタフェースでの連続する LLDPDU の送信に対する遅延時間を入力します。有効な値の範囲は 1 ～ 8192 秒です。送信間隔タイマーの値の 4 分の 1 を超えないようにしてください。**[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] ボタンをクリックして、変更を反映します。

4.8.2 LLDP ポート設定

このウィンドウを用いて、LLDP ポートの設定を行い、設定値を表示します。

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

図 4-62 LLDP ポート設定

[LLD ポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
通知	通知機能を有効または無効にします。
サブタイプ	LLDP TLV（Type-Length-Value）のサブタイプを選択します。選択する値は **[MAC アドレス]** および **[ローカル]** です。
管理状態	ローカル LLDP エージェントを選択し、ポートでの LLDP フレームの送受信を許可します。選択する値は以下のとおりです。 • **[TX]** - ローカル LLDP エージェントは LLDP フレームの送信のみ可能です。 • **[RX]** - ローカル LLDP エージェントは LLDP フレームの受信のみ可能です。 • **[TX と RX]**- ローカル LLDP エージェントは LLDP フレームの送受信が可能です。 • **[無効]** - ローカル LLDP エージェントは LLDP フレームの送信も受信もできません。 デフォルトのオプションは **[TX と RX]** です。
IP サブタイプ	送信する IP アドレス情報のタイプを選択します。選択する値は **[デフォルト]**、**[IPv4]**、および **[IPv6]** です。
アクション	実行するアクションを選択します。選択する値は **[削除]** および **[追加]** です。
アドレス	送信する IP アドレスを入力します。

[適用] ボタンをクリックして、変更を反映します。

4.8.3 LLDP マネジメントアドレスリスト

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

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

図 4-63 LLDP マネジメントアドレスリスト

以下のパラメータを設定できます。

パラメータ	概要
サブタイプ	サブタイプ選択します。選択する値は **[全]**、**[IPv4]**、および **[IPv6]** です。 • **[IPv4]** オプションを選択した後、IPv4 アドレスを表示された入力フィールドに入力します。 • **[IPv6]** オプションを選択した後、IPv6 アドレスを表示された入力フィールドに入力します。

[検索] ボタンをクリックして、指定した検索条件に基づいてテーブル内のエントリを検索し、表示します。

4.8.4 LLDP 基本 TLV 設定

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

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

図 4-64 LLDP 基本 TLV 設定

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

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
ポート説明	ポート説明 TLV の送信を有効または無効にします。
システム名	システム名 TLV の送信を有効または無効にします。
システム説明	システム説明 TLV の送信を有効または無効にします。
システム能力	システム能力 TLV の送信を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

4.8.5 LLDP Dot1 TLV 設定

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

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

図 4-65 LLDP Dot1 TLV 設定

[LLDP Dot1 TLV 設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
ポート VLAN	ポート VLAN ID TLV の送信を有効または無効にします。
プロトコル VLAN	PPVID（ポートとプロトコル VLAN ID）TLV の送信を有効または無効にします。プロトコル VLAN の ID を表示された入力フィールドに入力します。
VLAN 名	VLAN 名 TLV の送信を有効または無効にします。VLAN の ID を表示された入力フィールドに入力します。
プロトコルアイデンティティ	プロトコルアイデンティティ TLV の送信を有効または無効にします。プロトコル名として選択する値は **[なし]**、**[EAPOL]**、**[LACP]**、**[GVRP]**、**[STP]**、および **[全]** です。

[適用] ボタンをクリックして、変更を反映します。

4.8.6 LLDP Dot3 TLV 設定

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

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

図 4-66 LLDP Dot3 TLV 設定

[LLDP Dot3 TLV 設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
MAC/PHY コンフィグ / 状態	MAC/PHY コンフィグ / 状態 TLV の送信を有効または無効にします。
リンクアグリゲーション	リンクアグリゲーション TLV の送信を有効または無効にします。
最大フレームサイズ	最大フレームサイズ TLV の送信を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

4.8.7 LLDP-MED ポート設定

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

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

図 4-67 LLDP-MED ポート設定

[LLDP-MED ポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
通知	LLDP-MED 通知 TLV の送信を有効または無効にします。
能力	LLDP-MED 能力 TLV の送信を有効または無効にします。
資産	LLDP-MED 資産管理 TLV の送信を有効または無効にします。
ネットワークポリシー	LLDP-MED ネットワークポリシー TLV の送信を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

4.8.8 LLDP 統計情報

このウィンドウを用いて、LLDP 統計を表示およびクリアします。

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

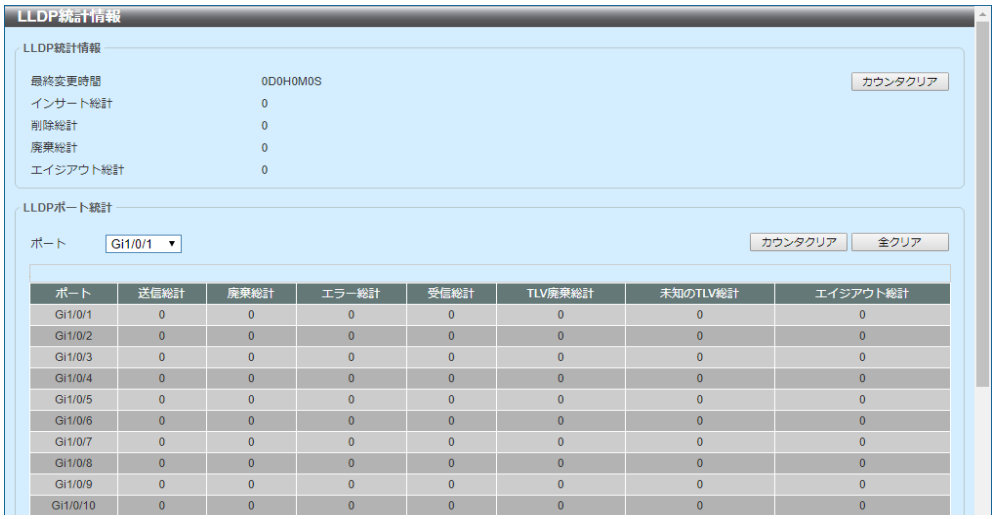


図 4-68 LLDP 統計情報

[LLDP ポート統計] 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
ポート	使用するポートを選択します。

[クリア] ボタンをクリックして、カウンタ情報をクリアします。
[全クリア] ボタンをクリックして、すべてのポートのカウンタ情報をクリアします。

4.8.9 LLDP ローカルポート情報

このウィンドウを用いて、ローカル LLDP ポート情報を表示します。

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

図 4-69 LLDP ローカルポート情報

[LLDP ローカルポート要約テーブル] 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
ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定したポートに関連付けられている LLDP ローカルポート情報を検索します。
[詳細参照] ボタンをクリックして、指定したポートに関連付けられている LLDP ローカルポート詳細情報を表示します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

図 4-70 LLDP ローカルポート情報（詳細参照）

個々のリンクをクリックして、指定した機能に関連する詳細情報をテーブルに表示します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

4.8.10 LLDP ネイバーポート情報

このウィンドウを用いて、ネイバーの LLDP ポート情報を表示します。

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

図 4-71 LLDP ネイバーポート情報

[LLDP ネイバーポート要約テーブル] 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
ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定したポートに関連付けられている LLDP ネイバーポート情報を検索します。
[クリア] ボタンをクリックして、指定したポートに関連付けられている LLDP ネイバーポート情報をクリアします。
[全クリア] ボタンをクリックして、すべての LLDP ネイバーポート情報をクリアします。

4.9 RRP (Ring Redundant Protocol)

このウィンドウを用いて、RRP 設定を行い、設定値を表示します。

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

図 4-72 RRP

[RRP グローバル状態] 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
RRP 状態	RRP 機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[RRP ドメイン状態] 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
ドメイン名	RRP ドメイン名を入力します。指定可能な文字列は 25 文字までです。このドメインは物理リングを表します。

[作成] ボタンをクリックして、新しい RRP ドメインを作成します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。
[削除] ボタンをクリックして、エントリを削除します。

[**詳細参照**] ボタンをクリックして、以下のウィンドウを表示します。

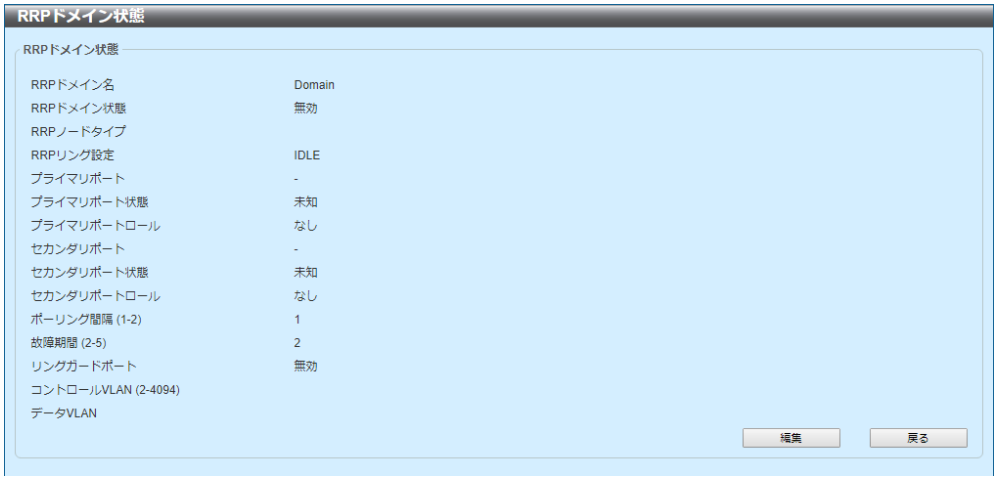


図 4-73 RRP（詳細参照）

[**編集**] ボタンをクリックして、設定を編集します。
[**戻る**] ボタンをクリックして、前のウィンドウに戻ります。

[**編集**] ボタンをクリックして、以下のウィンドウを表示します。

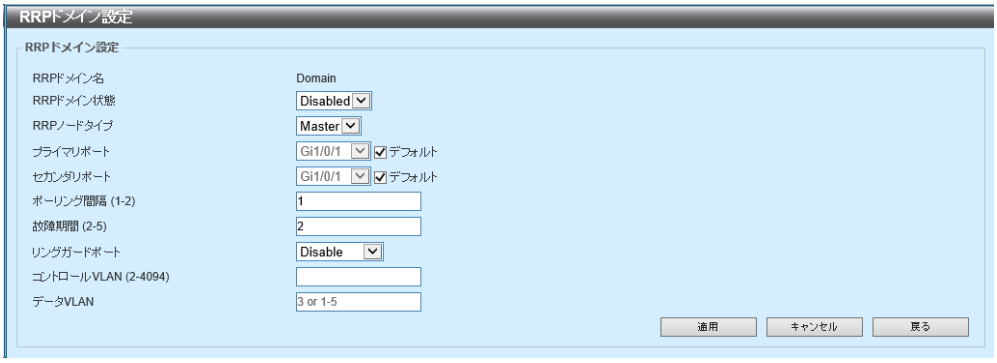


図 4-74 RRP（編集）

[**RRP ドメイン設定**] 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
RRP ドメイン状態	RRP ドメインの有効または無効を選択します。

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

[適用] ボタンをクリックして、変更を反映します。
[キャンセル] ボタンをクリックして、変更を破棄します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

5 L3 機能

5.1 ARP (Address Resolution Protocol)

5.1.1 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 5-75 ARP エージング時間

[ARP エージング時間検索] 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
インタフェース VLAN	VLAN ID を入力します。範囲は 1 ～ 4094 です。
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。範囲は、0 ～ 65535 分です。

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

5.1.2 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 5-76 スタティック ARP

[スタティック ARP 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
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] ボタンをクリックして、新しいスタティック ARP エントリを追加します。

[スタティック ARP 検索] 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
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。範囲は 1 ～ 4094 です。

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

5.1.3 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。

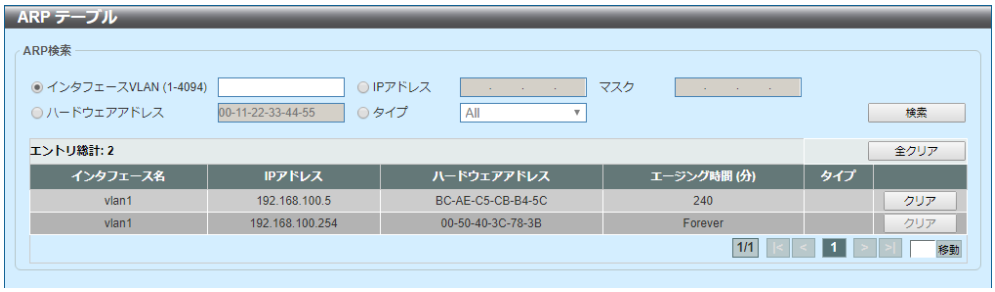


図 5-77 ARP テーブル

[ARP 検索] 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。この範囲は 1 ～ 4094 です。
IP アドレス	表示する IP アドレスを選択および入力します。
マスク	IP アドレスのサブネットマスクを選択および入力します。
ハードウェアアドレス	表示する MAC アドレスを選択および入力します。
タイプ	タイプのオプションを選択します。選択する値は **[全]** および **[ダイナミック]** です。

[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[全クリア] ボタンをクリックして、すべてのエントリをテーブルからクリアします。
[クリア] ボタンをクリックして、指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

5.2 Gratuitous ARP

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

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

図 5-78 Gratuitous ARP

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

[適用] ボタンをクリックして、変更を反映します。

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

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

5.3 IPv6 ネイバー

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

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

図 5-79 IPv6 ネイバー

[IPv6 ネイバー設定] 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
インタフェース VLAN	VLAN インタフェース ID を入力します。
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] ボタンをクリックして、新しいエントリを追加します。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[クリア] ボタンをクリックして、指定した条件に基づき情報をクリアします。
[全クリア] ボタンをクリックして、すべてのダイナミックエントリをクリアします。
[削除] ボタンをクリックして、指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

5.4 インタフェース

5.4.1 IPv4 インタフェース

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

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

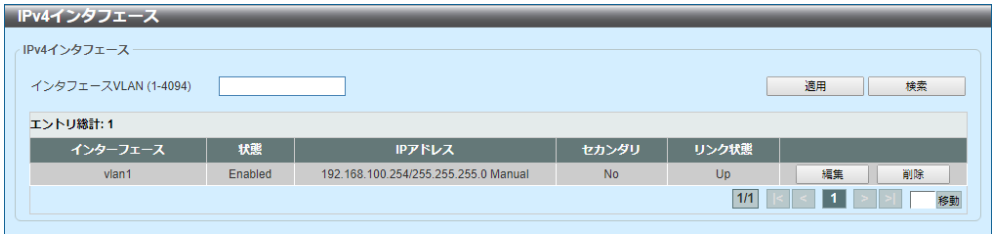


図 5-80 IPv4 インタフェース

[IPv4 インタフェース] 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
インタフェース **VLAN**	インタフェース VLAN ID を入力します。範囲は 1 ～ 4094 です。

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

[編集] ボタンをクリックして、以下のウィンドウを表示します。

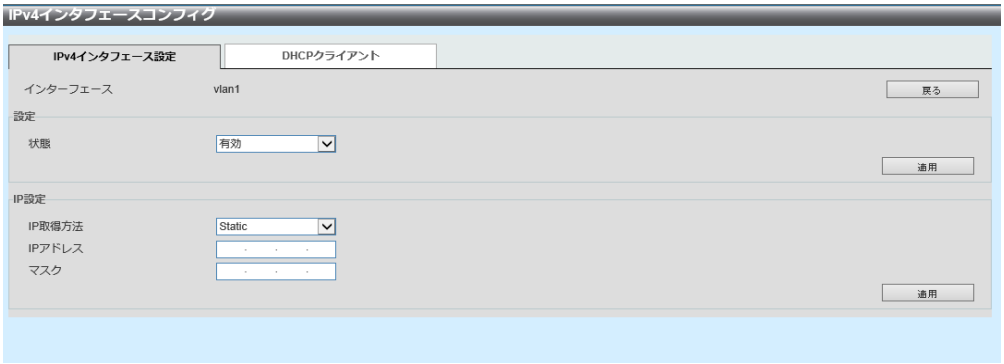


図 5-81 IPv4 インタフェース（編集、IPv4 インタフェース設定）

[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	IPv4 インタフェースのグローバル状態を有効または無効にします。

[戻る] ボタンをクリックして、前のウィンドウに戻ります。
[適用] ボタンをクリックして、変更を反映します。

[IP 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
IP 取得方法	IP アドレスの取得方法を選択します。選択する値は以下のとおりです。 • **[スタティック]** - このインタフェースの IPv4 アドレス設定を表示された入力フィールドに手動で入力します。 • **[DHCP]** - このインタフェースが、ローカルネットワークにある DHCP サーバから自動的に IPv4 設定を取得します。
IP アドレス	このインタフェースの IPv4 アドレスを入力します。
マスク	このインタフェースの IPv4 サブネットマスクを入力します。
セカンダリ	このオプションをオンにした場合、IPv4 アドレスとマスクをセカンダリインタフェース設定として使用します。

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

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

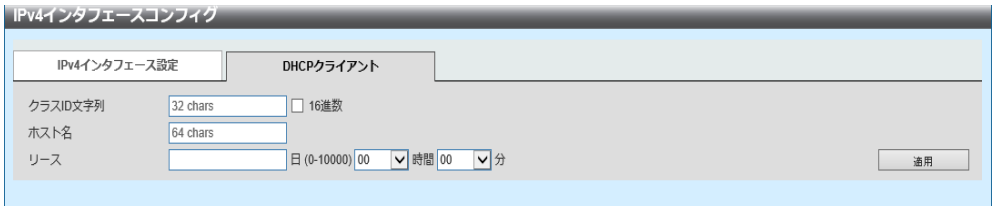


図 5-82 IPv4 インタフェース（編集、DHCP クライアント）

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

[適用] ボタンをクリックして、変更を反映します。

5.4.2 IPv6 インタフェース

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

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

図 5-83 IPv6 インタフェース

[IPv6 インタフェース] 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。

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

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

図 5-84 IPv6 インタフェース（詳細参照、IPv6 インタフェース設定）

[IPv6 インタフェース設定] 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
IPv6 状態	IPv6 インタフェースのグローバル状態を有効または無効にします。

[戻る] ボタンをクリックして、前のウィンドウに戻ります。
[適用] ボタンをクリックして、変更を反映します。

[スタティック IPv6 アドレス設定] 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
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]**（Extended Unique Identifier 64-bit）オプションを選択した場合、EUI-64 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]** オプションを選択した場合、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] ボタンをクリックして、変更を反映します。

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

図 5-85 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] ボタンをクリックして、指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

[ネイバー探索] タブをクリックして、以下のウィンドウを表示します。

図 5-86 IPv6 インタフェース（詳細参照、ネイバー探索）

[ND 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
NS 間隔	NS（Neighbor Solicitation）間隔の値を入力します。範囲は 0 ～ 3600000 ミリ秒（1000 の倍数）です。指定した時間が 0 の場合、ルータは 1 秒を使用します。

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

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

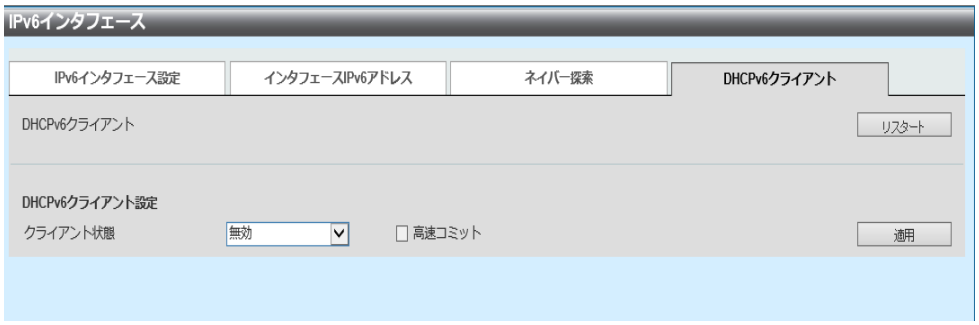


図 5-87 IPv6 インタフェース（詳細参照、DHCPv6 クライアント）

[リスタート] ボタンをクリックして、DHCPv6 クライアント機能を再開します。

[DHCPv6 クライアント設定] 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
クライアント状態	DHCPv6 クライアントサービスを有効または無効にします。**[高速コミット]** オプションを選択した場合、アドレス委任の 2 メッセージ交換を続行します。高速コミットオプションは Solicit メッセージに含まれ、2 メッセージハンドシェイクを要求します。

5.5 IPv4 デフォルトルート

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

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

図 5-88 IPv4 デフォルトルート

[IPv4 デフォルトルート] 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
ゲートウェイ	このルートのゲートウェイアドレスを入力します。

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

5.6 IPv4 ルートテーブル

このウィンドウを用いて、IPv4 ルートテーブルおよび情報を表示します。

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

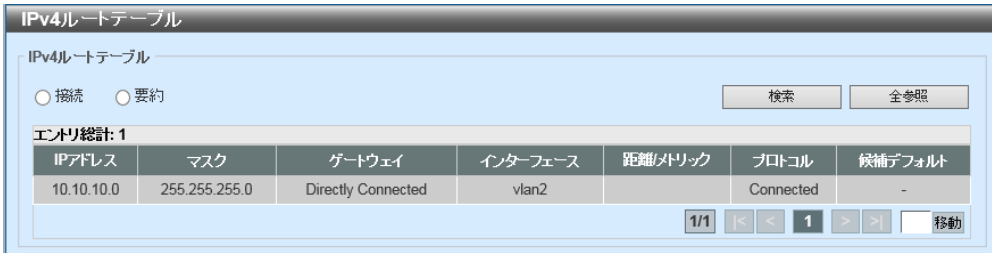


図 5-89 IPv4 ルートテーブル

[IPv4 ルートテーブル] 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
IP アドレス	単一の IPv4 アドレスを選択および入力します。
ネットワークアドレス	IPv4 ネットワークアドレスを選択および入力します。1 つ目（左側）の入力フィールドにネットワークプレフィックスを入力し、2 つ目（右側）の入力フィールドにネットワークマスクを入力します。

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

5.7 IPv6 デフォルトルート

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

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

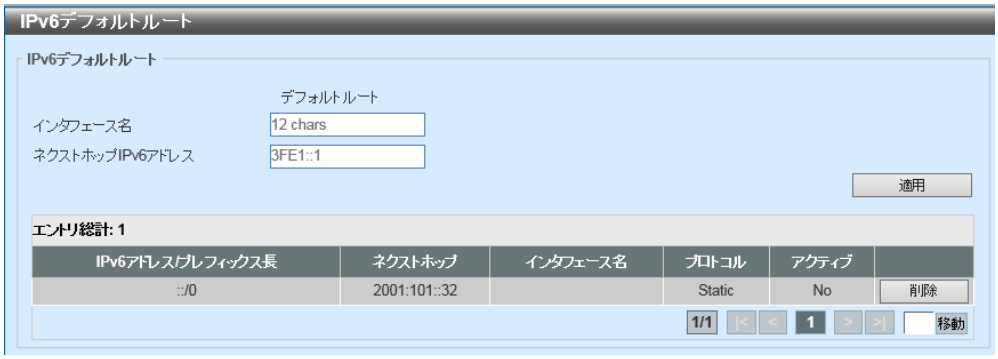


図 5-90 IPv6 デフォルトルート

[IPv6 デフォルトルート] 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
IPv6 アドレス / プレフィックス長	このルートの IPv6 アドレスとプレフィックス長を入力します。**[デフォルトルート]** オプションをオンにした場合、このルートをデフォルトルートで使用します。
インタフェース名	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。
距離	スタティックルートの管理上の距離を入力します。範囲は 1 ～ 254 です。値が小さいほど良いルートになります。指定しない場合、スタティックルートの管理上の距離はデフォルトで 1 になります。

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

5.8 IPv6 ルートテーブル

このウィンドウを用いて、IPv6 ルートテーブルおよび情報を表示します。

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

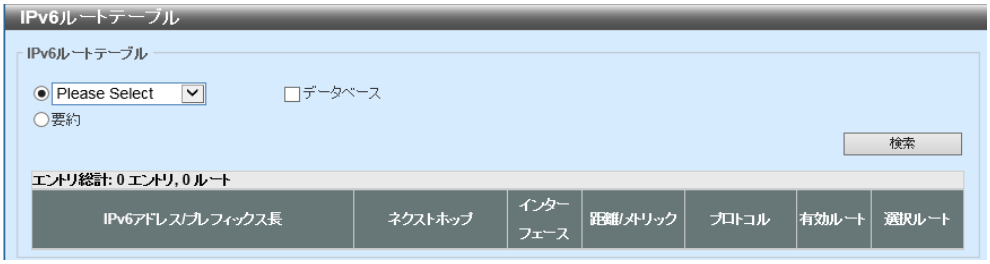


図 5-91 IPv6 ルートテーブル

[IPv6 ルートテーブル] 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
IPv6 アドレス	表示する IPv6 アドレスを選択および入力します。
IPv6 アドレス / プレフィックス長	表示する IPv6 アドレスとプレフィックス長を選択および入力します。**[Longer Prefixes]** オプションを選択した場合、ルート、およびより具体的なすべてのルートを表示します。
インタフェース名	表示するインタフェースの名前を選択および入力します。

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

[要約] オプションをクリックして、以下のウィンドウを表示します。

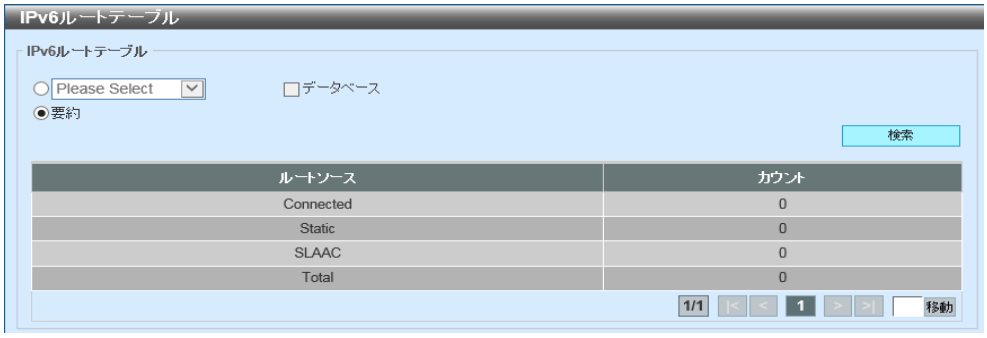


図 5-92 IPv6 ルートテーブル（要約）

5.9 IPv6 ジェネラルプレフィックス

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

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

図 5-93 IPv6 ジェネラルプレフィックス

[IPv6 ジェネラルプレフィックス] 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
インタフェース VLAN	使用する VLAN インタフェース ID を入力します。範囲は 1 ～ 4094 です。
プレフィックス名	IPv6 ジェネラルプレフィックスエントリ名を入力します。名前は 12 文字までです。
IPv6 アドレス	IPv6 アドレスとプレフィックス長を入力します。IPv6 アドレスのプレフィックス長は、VLAN インタフェースのローカルサブネットでもあります。

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

6 QoS（Quality of Service）

6.1 基本設定

6.1.1 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。

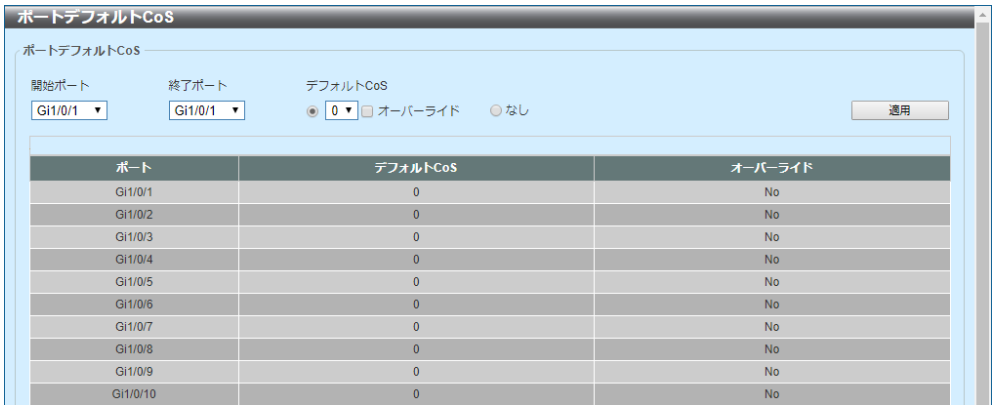


図 6-1 ポートデフォルト CoS

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

パラメータ	概要
開始ポート - 終了ポート	使用する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 オプションを選択します。選択する値の範囲は 0 ～ 7 です。 • **[オーバーライド]** オプションを選択した場合、パケットの CoS が無視されます。デフォルト CoS が、ポートで受信されるすべての着信パケット（タグ / アンタグ）に適用されます。 • **[なし]** オプションを選択した場合、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] ボタンをクリックして、変更内容を確認します。

6.1.2 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 6-2 ポートスケジューラ方式

[ポートスケジューラ方式] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

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

[**適用**] ボタンをクリックして、変更内容を確認します。

6.1.3 キュー設定

このウィンドウを用いて、QoS キューの設定を行い、設定値を表示します。

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

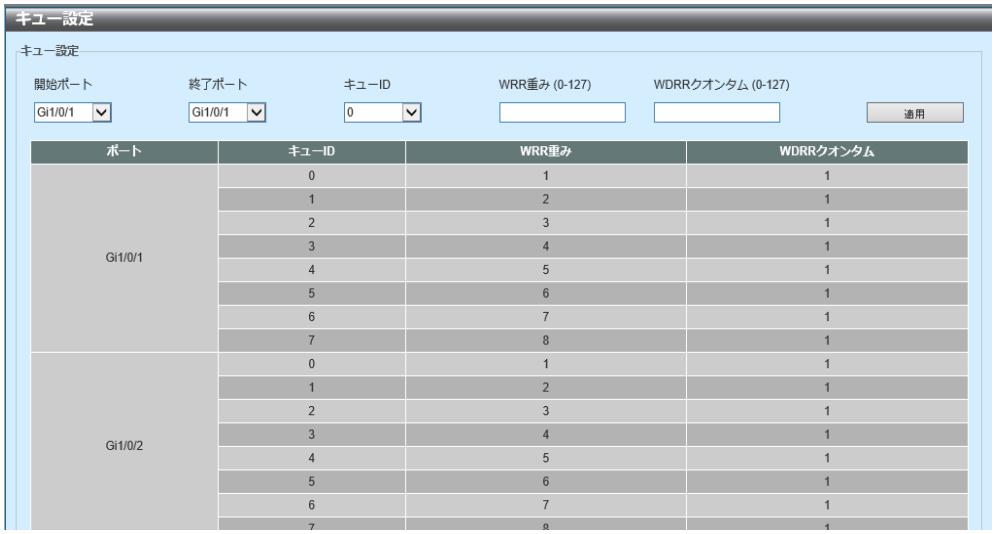


図 6-3 キュー設定

[キュー設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
キュー ID	キュー ID 値を入力します。範囲は 0 ～ 7 です。
WRR 重み	WRR 重み値を入力します。範囲は 0 ～ 127 です。EF（Expedited Forwarding）の動作要件を満たすために、PHB（Per-hop Behavior）EF によって最も高いキューを常に選択します。また、このキューのスケジュールモードを絶対優先スケジューリングに指定する必要があります。Differentiate Service がサポートされている限り、最後のキューの重み付けは 0 でなければなりません。
WDRR クオンタム	WDRR クオンタム値を入力します。範囲は 0 ～ 127 です。

[適用] ボタンをクリックして、変更内容を確認します。

6.1.4 CoS 送信キューマッピング

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

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

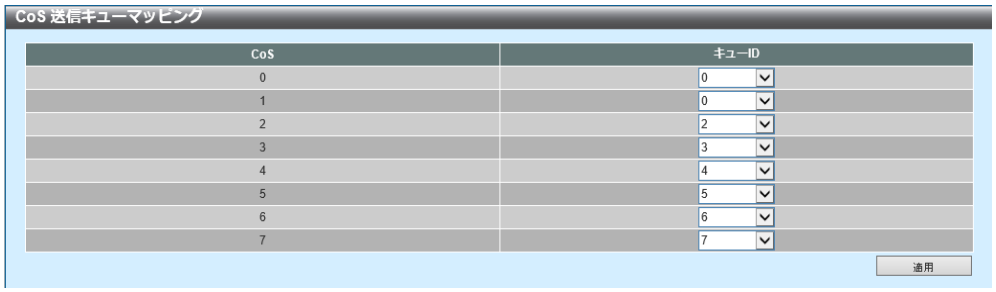


図 6-4 CoS 送信キューマッピング

以下のパラメータを設定できます。

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 を選択します。 選択する値の範囲は 0 ～ 7 です。

[適用] ボタンをクリックして、変更内容を確認します。

6.1.5 ポート帯域制限

このウィンドウを用いて、ポート帯域制限の設定を行い、設定値を表示します。

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

図 6-5 ポート帯域制限

[ポート帯域制限] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
方向	方向オプションを選択します。選択する値は以下のとおりです。 • **入力** - 入口パケットの帯域制限を設定します。 • **出力** - 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]** を選択した場合、使用する入力 / 出力帯域幅を表示された入力フィールドに入力します。範囲は、8 ～ 40000000Kbps です。**バーストサイズ**値を表示された入力フィールドに入力します。範囲は、0 ～ 128000 キロバイトです。 • **[パーセント]** を選択した場合、使用する入力 / 出力帯域幅を表示された入力フィールドにパーセンテージで入力します。範囲は、1 ～ 100 パーセントです。**バーストサイズ**値を表示された入力フィールドに入力します。範囲は、0 ～ 128000 キロバイトです。 • **[なし]** を選択した場合、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] ボタンをクリックして、変更内容を確認します。

6.1.6 キュー帯域制限

このウィンドウを用いて、キュー帯域制限の設定を行い、設定値を表示します。

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

図 6-6 キュー帯域制限

[キュー帯域制限] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
キュー ID	設定するキュー ID を選択します。選択する値の範囲は 0 ～ 7 です。
帯域制限	キューの帯域制限設定を選択および入力します。 • [最小帯域] オプションを選択した場合、帯域制限の最小帯域を表示された入力フィールドに入力します。範囲は、8 ～ 40000000Kbps です。帯域制限の最大帯域（[最大帯域]）を表示された入力フィールドに入力します。範囲は、8 ～ 40000000Kbps です。 最小の帯域幅を設定すると、キューから送信されるパケットが保証されます。最大の帯域幅を設定すると、帯域幅が利用可能な場合でも、キューから送信されるパケットが最大の帯域幅を超えることはありません。 最小帯域幅を設定する場合、設定する最小帯域幅のアグリゲートはインタフェース帯域幅の 75% 未満でなければなりません。これにより、設定する最小帯域幅を保証します。絶対優先キューに最低保証帯域幅を設定する必要はありません。これは、すべてのキューの最小帯域幅を満たす場合に、このキューのトラフィックにまずサービスが提供されるからです。 このコマンドのコンフィグレーションは物理ポートにのみアタッチされ、ポートチャネルにはアタッチされません。これは、1 つの CoS の最低保証帯域幅であり、物理ポート全体では使用できません。 • [最小パーセント] オプションを選択した場合、最小帯域のパーセント値を表示された入力フィールドに入力します。範囲は、1 ～ 100% です。最大パーセント値（[最大パーセント]）を表示された入力フィールドに入力します。範囲は、1 ～ 100% です。 • [なし] を選択した場合、指定したポートに帯域制限は割り当てられません。

[適用] ボタンをクリックして、変更内容を確認します。

6.2 高度な設定

6.2.1 DSCP 変換マップ

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

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

図 6-7 DSCP 変換マップ

[DSCP 変換マップ] 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
ミューテーション名	DSCP 変換マップ名を入力します。名前は 32 文字までです。
入力 DSCP リスト	入力 DSCP リスト値を入力します。範囲は 0 ～ 63 です。
出力 DSCP リスト	出力 DSCP 値を入力します。範囲は 0 ～ 63 です。

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

6.2.2 ポート信頼状態および Mutation バインディング

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

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

図 6-8 ポート信頼状態および Mutation バインディング

[ポート信頼状態] および **[Mutation バインディング]** セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
信頼状態	ポート信頼状態を選択します。選択する値は **[CoS]** および **[DSCP]** です。
DSCP 変換マップ	使用する DSCP 変換マップ名を選択および入力します。名前は 32 文字までです。**[なし]** オプションを選択した場合、DSCP 変換マップをポートに割り当てません。

[適用] ボタンをクリックして、変更内容を確認します。

6.2.3 DSCP CoS マッピング

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

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

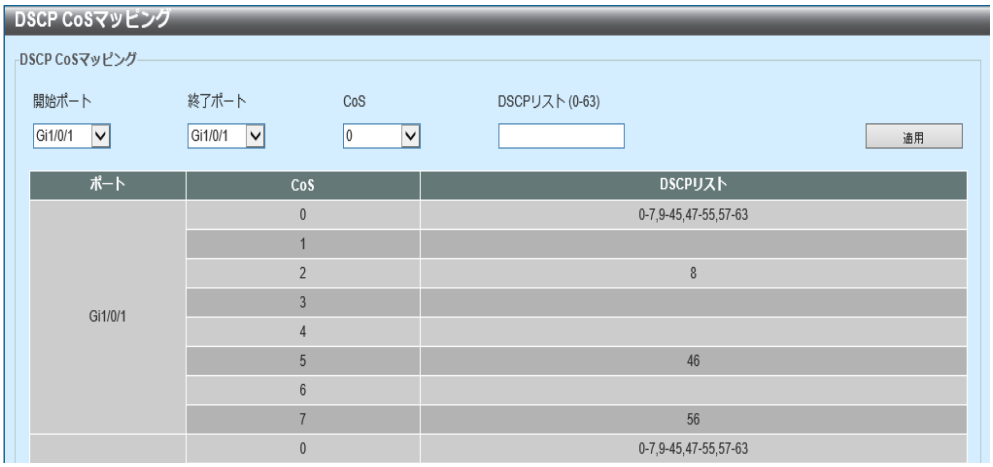


図 6-9 DSCP CoS マッピング

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

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
CoS	DSCP リストにマッピングする CoS 値を選択します。選択する値の範囲は 0 ～ 7 です。
DSCP リスト	CoS 値にマッピングする DSCP リスト値を入力します。範囲は 0 ～ 63 です。

[適用] ボタンをクリックして、変更内容を確認します。

6.2.4 CoS カラーマッピング

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

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

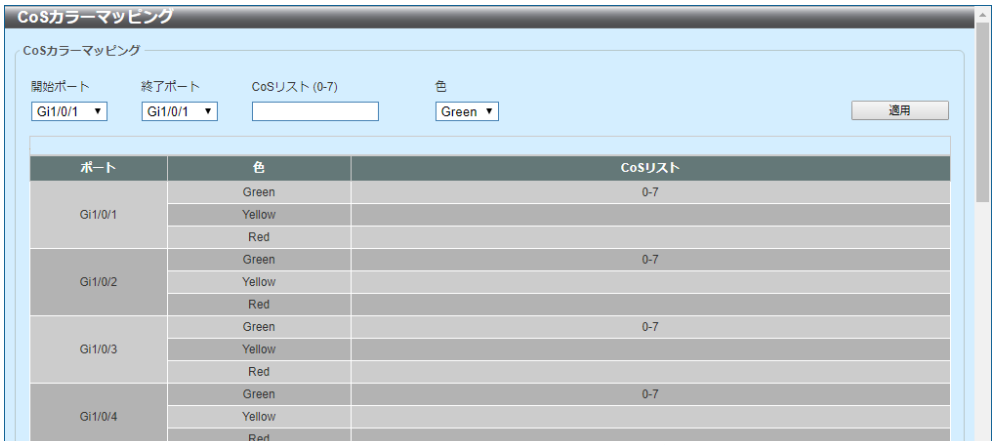


図 6-10 CoS カラーマッピング

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

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
CoS リスト	色にマッピングする CoS 値を入力します。範囲は 0 ～ 7 です。
色	CoS 値にマッピングする色オプションを選択します。選択する値は **[緑]**、**[黄色]**、および **[赤色]** です。

[適用] ボタンをクリックして、変更内容を確認します。

6.2.5 DSCP カラーマッピング

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

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

図 6-11 DSCP カラーマッピング

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

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
DSCP リスト	色にマッピングする DSCP リスト値を入力します。範囲は 0 ～ 63 です。
色	DSCP 値にマッピングする色オプションを選択します。選択する値は **[緑]**、**[黄色]**、および **[赤色]** です。

[適用] ボタンをクリックして、変更内容を確認します。

6.2.6 クラスマップ

このウィンドウを用いて、クラスマップの設定を行い、設定値を表示します。

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

図 6-12 クラスマップ

以下のパラメータを設定できます。

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。名前は 32 文字までです。
複数適合基準	複数適合基準オプションを選択します。選択する値は **[マッチ All]** および **[マッチ Any]** です。

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

[適合] ボタンをクリックして、以下のウィンドウを表示します。

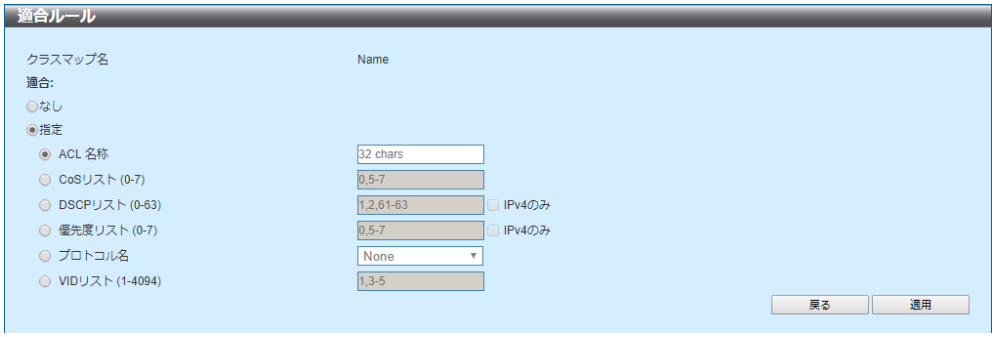


図 6-13 クラスマップ（適合）

以下のパラメータを設定できます。

パラメータ	概要
なし	このオプションを選択した場合、このクラスマップには何も適合させません。
指定	このオプションを選択した場合、以下のいずれかをこのクラスマップと適合させます。
ACL 名称	このクラスマップと適合するアクセスリスト名を選択および入力します。名前は 32 文字までです。
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。範囲は 0 ～ 7 です。
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。範囲は 0 ～ 63 です。**[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。範囲は 0 ～ 7 です。**[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を選択します。選択する値は **[ARP]**、**[BGP]**、**[DHCP]**、**[DNS]**、**[EGP]**、**[FTP]**、**[IPv4]**、**[IPv6]**、**[NetBIOS]**、**[NFS]**、**[NTP]**、**[OSPF]**、**[PPPOE]**、**[RIP]**、**[RTSP]**、**[SSH]**、**[Telnet]**、および **[TFTP]** です。
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。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、変更内容を確認します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

6.2.7 集約ポリサー

このウィンドウを用いて、集約ポリサーの設定を行い、設定値を表示します。

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

図 6-14 集約ポリサー（シングルレート設定）

[シングルレート設定] 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
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。範囲は、0 ～ 10000000Kbps です。
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。範囲は、0 ～ 16384Kbyte です。
最大バーストサイズ	最大バーストサイズ値を入力します。範囲は、0 ～ 16384Kbyte です。
Confirm Action	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。確認アクションを指定しない場合のデフォルトのアクションは **[送信]** です。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

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

[適用] ボタンをクリックして、新しいエントリを追加します。

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

[2 レート設定] タブをクリックして、以下のウィンドウを表示します。

図 6-15 集約ポリサー（2 レート設定）

[2 レート設定] 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
集約ポリサー名	集約ポリサー名を入力します。
CIR	CIR（Committed Information Rate）値を入力します。範囲は、0 ～ 10000000Kbps です。認定パケットレートは、ツーレートメータリングの最初のトークンバケットです。
バースト確認	バースト確認値を入力します。範囲は、0 ～ 16384Kbyte です。バースト確認値は、最初のトークンバケットのバーストサイズ（キロバイト）を指定します。
PIR	PIR（Peak Information Rate）値を入力します。範囲は、0 ～ 10000000Kbps です。ピーク情報レートは、ツーレートメータリングの 2 番目のトークンバケットです。
ピークバースト	ピークバースト値を入力します。範囲は、0 ～ 16384Kbyte です。ピークバースト値は、2 番目のトークンバケットのバーストサイズ（キロバイト）です。

パラメータ	概要
Confirm Action	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。確認アクションを指定しない場合のデフォルトのアクションは **[送信]** です。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
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。ツーレートポリサーでは、超過時アクションを指定しない場合のデフォルトのアクションは **[廃棄]** です。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

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

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

6.2.8 ポリシーマップ

このウィンドウを用いて、ポリシーマップの設定を行い、設定値を表示します。

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

図 6-16 ポリシーマップ

[ポリシーマップ作成 / 削除] 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。名前は 32 文字までです。

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

[トラフィックポリシー] 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
ポリシーマップ名	ポリシーマップ名を入力します。名前は 32 文字までです。
クラスマップ名	クラスマップ名を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しいエントリを追加します。
[アクション設定] ボタンをクリックして、指定したエントリのアクションを設定します。
[ポリサー] ボタンをクリックして、指定したエントリの Police Action を設定します。
[削除] ボタンをクリックして、指定したエントリを削除します。

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

[アクション設定] ボタンをクリックして、以下のウィンドウを表示します。

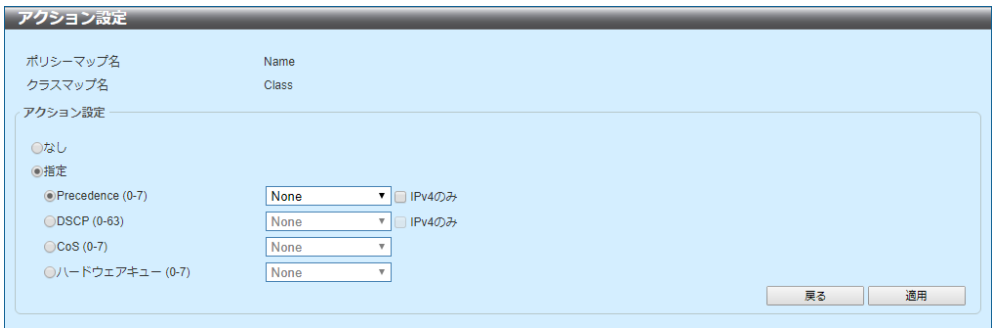


図 6-17 ポリシーマップ（アクション設定）

[アクション設定] 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
なし	このオプションを選択した場合、何もアクションを実行しません。
指定	このオプションを選択した場合、コンフィグレーションに基づいてアクションを実行します。
新優先度	パケットの新優先度値を選択します。範囲は 0 ～ 7 です。**[IPv4 のみ]** オプションを選択した場合、IPv4 の優先度のみマークされます。選択しない場合、IPv4 と IPv6 の両方の優先度がマークされます。IPv6 パケットの場合、IPv6 ヘッダのトラフィッククラスの最上位 3 ビットが優先度になります。
新 DSCP	パケットの新 DSCP 値を選択します。範囲は 0 ～ 63 です。**[IPv4 のみ]** オプションを選択した場合、IPv4 の DSCP のみマークされます。選択しない場合、IPv4 と IPv6 の両方の DSCP がマークされます。
新 CoS	パケットの新 CoS 値を選択します。範囲は 0 ～ 7 です。
新 CoS キュー	パケットの新 CoS キュー値を選択します。これによって元の CoS キューの選択が上書きされます。ポリシーマップがインタフェースの出口フローに適用されている場合、CoS キューの設定は有効になりません。

[適用] ボタンをクリックして、変更内容を確認します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

[ポリサー] ボタンをクリックし、Police Action として **[Police]** を指定して、以下のウィンドウを表示します。

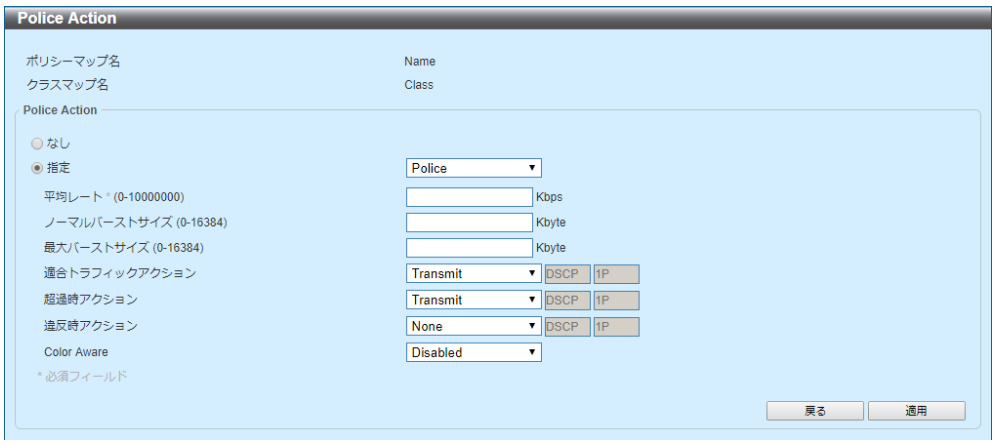


図 6-18 ポリシーマップ（ポリサー、Police）

[Police Action] 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
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	このオプションを選択した場合、このエントリに以下のポリサー設定が適用されます。
平均レート	平均レート値を入力します。範囲は、0 ～ 10000000Kbps です。
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。範囲は、0 ～ 16384Kbps です。
最大バーストサイズ	最大バーストサイズ値を入力します。範囲は、0 ～ 16384Kbps です。
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。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

パラメータ	概要
超過時アクション	実行する超過時アクションを選択します。このアクションは、帯域制限を超過する黄色のパケットに対して実行します。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
違反時アクション	実行する違反時アクションを選択します。このアクションは、赤色のパケットに対して実行します。選択する値は以下のとおりです。 • **なし** - 何も違反時アクションを実行しません。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
Color Aware	Color Aware 機能を有効または無効にします。 • **有効**な場合、ポリサーは Color Aware モードで動作します。 • **無効**な場合、ポリサーは Color Blind モードで動作します。

[適用] ボタンをクリックして、変更内容を確認します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

[ポリサー] ボタンをクリックし、Police Action として **[Police CIR]** を指定して、以下のウィンドウを表示します。

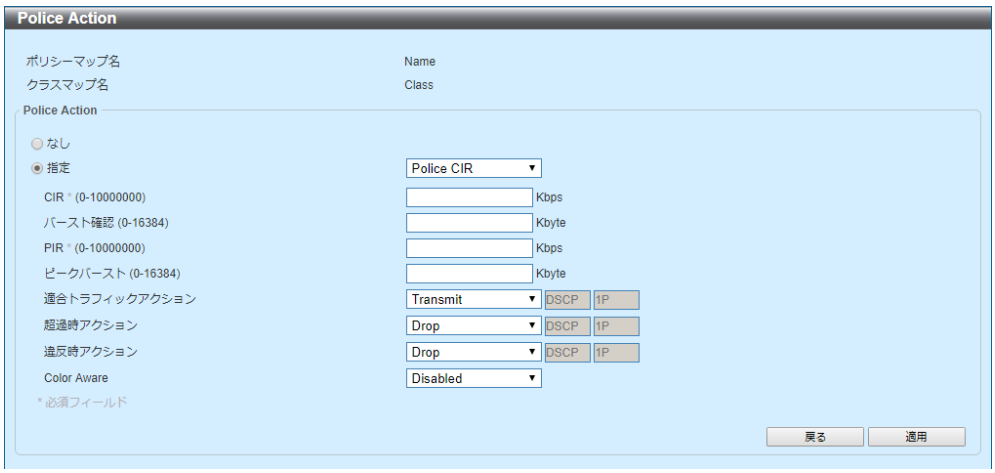


図 6-19 ポリシーマップ（ポリサー、Police CIR）

[Police Action] 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
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	このオプションを選択した場合、このエントリに以下のポリサー設定が適用されます。
CIR	CIR（Committed Information Rate）値を入力します。これは、ツーレートメータリングの最初のトークンバケットです。範囲は、0 ～ 10000000Kbps です。
バースト確認	バースト確認値を入力します。これは、最初のトークンバケットのサイズです。範囲は、0 ～ 16384 キロバイトです。
PIR	PIR（Peak Information Rate）値を入力します。これは、ツーレートメータリングの 2 番目のトークンバケットです。範囲は 0 ～ 10000000 です。
ピークバースト	ピークバースト値を入力します。これは、2 番目のトークンバケットのサイズです。範囲は、0 ～ 16384 キロバイトです。

パラメータ	概要
適合トラフィック アクション	実行する適合トラフィックアクションを選択します。このアクションは、緑色のパケットに対して実行します。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
超過時アクション	実行する超過時アクションを選択します。このアクションは、帯域制限を超過する黄色のパケットに対して実行します。選択する値は以下のとおりです。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。
違反時アクション	実行する違反時アクションを選択します。このアクションは、赤色のパケットに対して実行します。選択する値は以下のとおりです。 • **なし** - 何も違反時アクションを実行しません。 • **廃棄** - パケットを廃棄します。 • **Set-DSCP-Transmit** - パケットに新しい DSCP 値を設定して送信します。DSCP 値を表示された入力フィールドに入力します。 • **Set-1P-Transmit** - パケットに新しい IEEE 802.1p 値を設定して送信します。IEEE 802.1p 値を表示された入力フィールドに入力します。 • **送信** - パケットを変更しないで送信します。 • **DSCP-1P 設定** - パケットに新しい DSCP 値と IEEE 802.1p 値を設定して送信します。DSCP 値と IEEE 802.1p 値を表示された入力フィールドに入力します。

パラメータ	概要
Color Aware	Color Aware 機能を有効または無効にします。 • **有効**な場合、ポリサーは Color Aware モードで動作します。 • **無効**な場合、ポリサーは Color Blind モードで動作します。

[適用] ボタンをクリックして、変更内容を確認します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

[ポリサー] ボタンをクリックし、Police Action として **[Police Aggregate]** を指定して、以下のウィンドウを表示します。

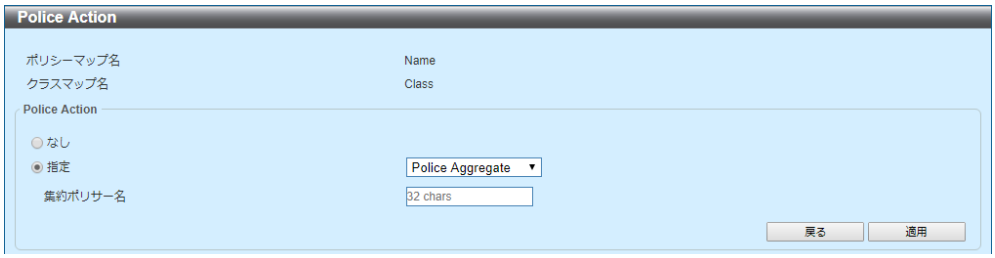


図 6-20 ポリシーマップ（ポリサー、Police Aggregate）

[Police Action] 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
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	このオプションを選択した場合、このエントリに以下のポリサー設定が適用されます。
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。名前は 32 文字までです。

[適用] ボタンをクリックして、変更内容を確認します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

6.2.9 ポリシーバインディング

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

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

図 6-21 ポリシーバインディング

[ポリシーバインドの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
方向	方向オプションを選択します。選択する値は **[入力]** および **[出力]** です。**[入力]** は入口トラフィック、**[出力]** は出口トラフィックをそれぞれ指定します。
ポリシーマップ名	ポリシーマップ名を入力します。名前は 32 文字までです。 • **[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] ボタンをクリックして、変更内容を確認します。

7 ACL（Access Control List）

7.1 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。

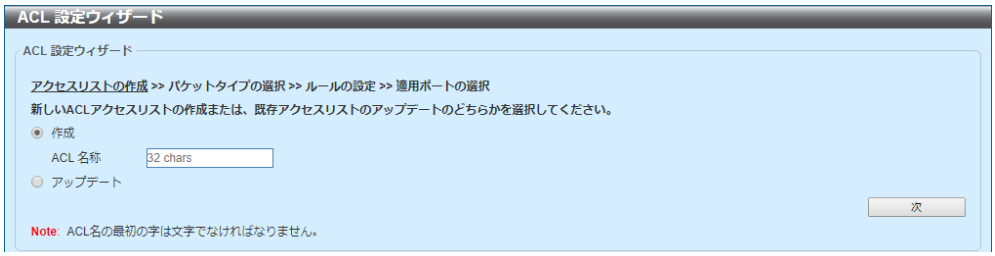


図 7-1 ACL 設定ウィザード（作成）

[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 7-2 ACL 設定ウィザード（アップデート）

以下のパラメータを設定できます。

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。名前は 32 文字までです。
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。

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

[作成] で ACL の作成を選択して **[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。

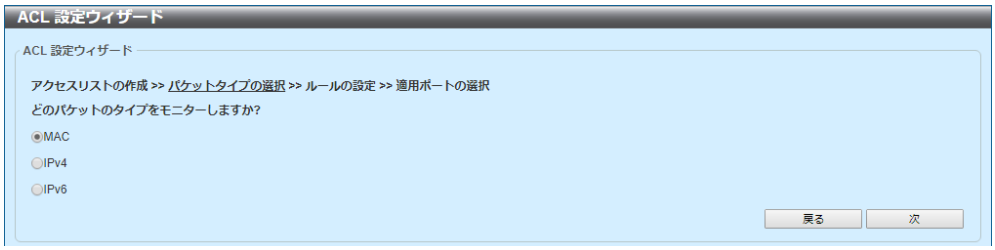


図 7-3 ACL 設定ウィザード（ACL タイプの選択）

以下のパラメータを設定できます。

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] ボタンをクリックして、ウィザードの次のステップに進みます。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

7.1.1 MAC ACL

[MAC ACL] の **[作成 / アップデート]** を選択すると、以下のウィンドウが表示されます。

図 7-4 ACL 設定ウィザード（MAC ACL の設定）

以下のパラメータを設定できます。

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。**[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。
ソース	ソース MAC 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 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。
ディスティネーション	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。選択する値は以下のとおりです。 • **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。

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]**、および **[arp]** です。
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。範囲は 0x600 ～ 0xFFFF です。**[指定イーサタイプ]** ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
イーサネットタイプマスク	イーサネットタイプマスクを 16 進数値で入力します。範囲は 0x0 ～ 0xFFFF です。**[指定イーサタイプ]** ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
CoS	使用する CoS 値を選択します。範囲は 0 ～ 7 です。 • **マスク** - CoS マスク値を入力します。範囲は 0x0 ～ 0x7 です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 • **マスク** - VLAN ID マスク値を入力します。範囲は 0x0 ～ 0xFFF です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。
アクション	このルールで実行するアクションを選択します。選択する値は、**[許可]**、**[拒否]**、および **[CPU 拒否]** です。

[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。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

（前のステップで）**[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。

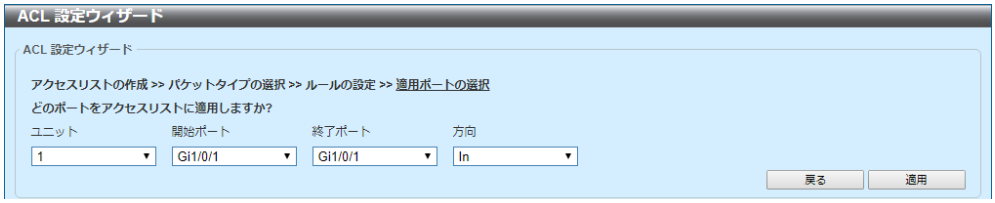


図 7-5 ACL 設定ウィザード（ポートと方向の選択）

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	使用するポートを選択します。
方向	方向を選択します。選択する値は **[In]** および **[Out]** です。

[適用] ボタンをクリックして変更内容を確認し、**[ACL 設定ウィザード]** ウィンドウに戻ります。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

7.1.2 IPv4

標準 IP ACL のアップデートを選択すると、以下のウィンドウが表示されます。

図 7-6 ACL 設定ウィザード（標準 IP ACL の設定）

拡張 IP ACL のアップデートまたは **IPv4 ACL** の作成を選択すると、以下のウィンドウが表示されます。

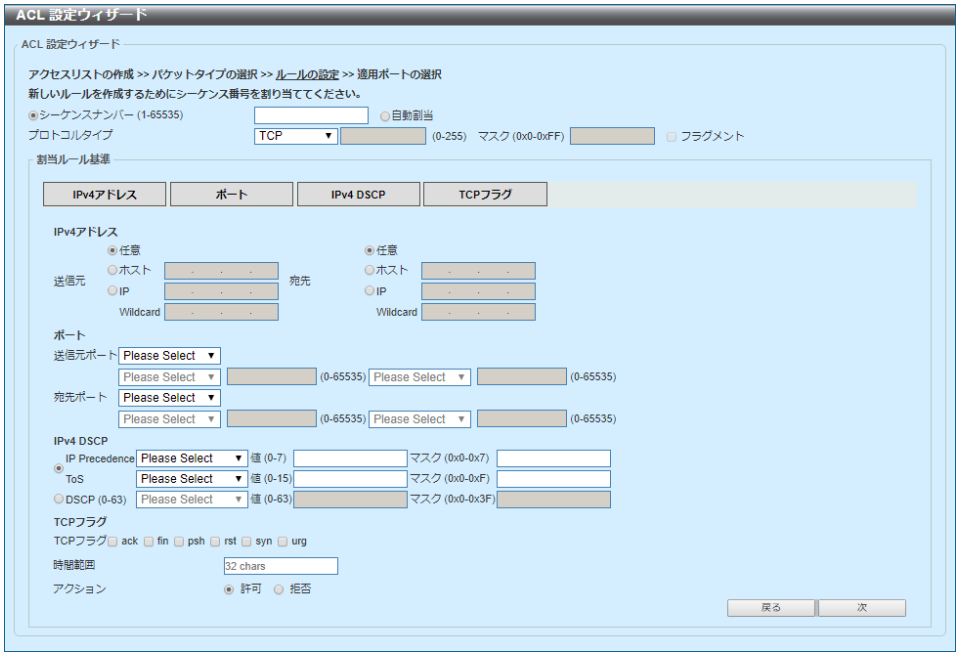


図 7-7 ACL 設定ウィザード（拡張 IP ACL の設定）

以下のパラメータを設定できます。

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。**[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）、**[プロトコル ID]**、および **[なし]** 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** - **[プロトコル ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
ソース	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト 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。
ディスティネーション	ディスティネーション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
ソースポート	ソースポート値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。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。
ディスティネーションポート	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。選択する値は以下のとおりです。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。
指定 ICMP メッセージタイプ	使用する ICMP メッセージタイプを選択します。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。
ICMP メッセージタイプ	**[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。

パラメータ	概要
メッセージコード	**[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。
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）、および **[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）、および **[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）、および **[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	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]**、および **[urg]** です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** を選択した場合のみ利用可能です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。

[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。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

（前のステップで）[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 7-8 ACL 設定ウィザード（IPv4、ステップ 3）

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	使用するポートを選択します。
方向	方向を選択します。選択する値は **[In]** および **[Out]** です。

[適用] ボタンをクリックして変更内容を確認し、**[ACL 設定ウィザード]** ウィンドウに戻ります。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

7.1.3 IPv6

標準 IPv6 ACL のアップデートを選択すると、以下のウィンドウが表示されます。

図 7-9 ACL 設定ウィザード（標準 IPv6 ACL の設定）

拡張 IPv6 ACL のアップデートまたは **IPv6 ACL** の作成を選択すると、以下のウィンドウが表示されます。

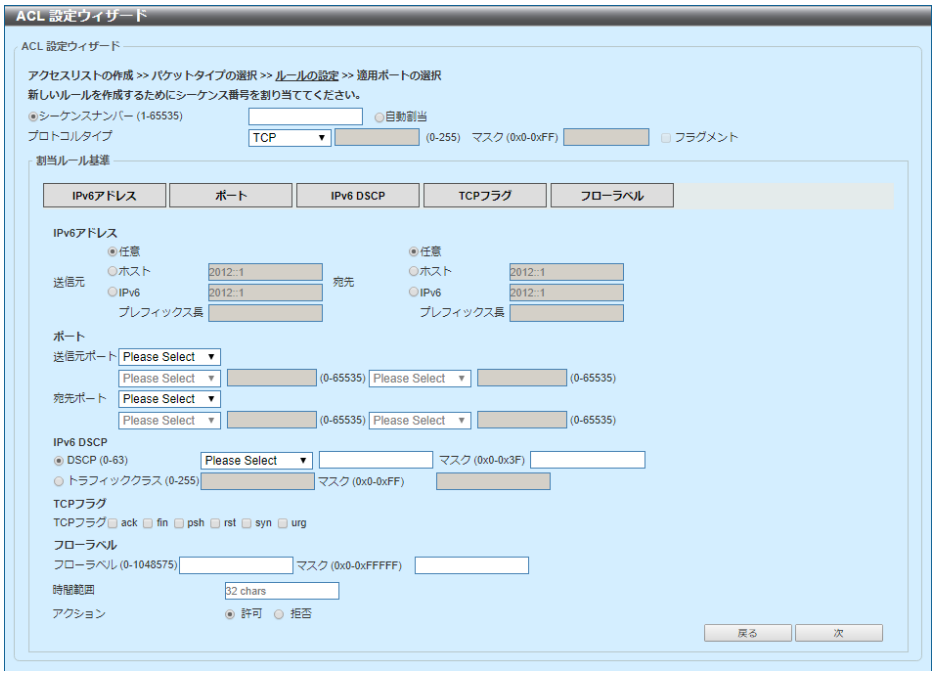


図 7-10 ACL 設定ウィザード（拡張 IPv6 ACL の設定）

以下のパラメータを設定できます。

パラメータ	概要
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。**[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を選択します。選択する値は、**[TCP]**、**[UDP]**、**[ICMP]**、**[プロトコル ID]**、**[ESP]**（50）、**[PCP]**（108）、**[SCTP]**（132）、および **[なし]** 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** - **[プロトコル ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。
ソース	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ソース IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
ディスティネーション	ディスティネーション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** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ディスティネーション IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。

パラメータ	概要
ソースポート	ソースポート値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。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。
ディスティネーションポート	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。選択する値は以下のとおりです。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。
指定 ICMP メッセージタイプ	使用する ICMP メッセージタイプを選択します。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。
ICMP メッセージタイプ	**[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。

パラメータ	概要
メッセージコード	**[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。
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）、および **[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。
TCP フラグ	この ACL で評価する TCP フラグを選択します。選択する値は、**[ack]**、**[fin]**、**[psh]**、**[rst]**、**[syn]**、および **[urg]** です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** を選択した場合のみ利用可能です。
フローラベル	フローラベル値を入力します。範囲は 0 ～ 1048575 です。 • **マスク** - フローラベルマスクを入力します。範囲は 0x0 ～ 0xFFFFF です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。

[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。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

（前のステップで）**[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。

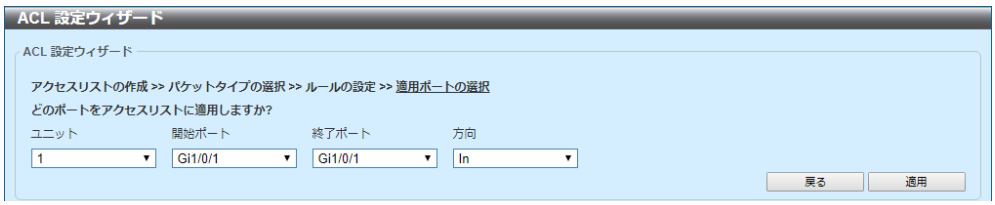


図 7-11 ACL 設定ウィザード（IPv6、ステップ 3）

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	使用するポートを選択します。
方向	方向を選択します。選択する値は **[In]** および **[Out]** です。

[適用] ボタンをクリックして変更内容を確認し、**[ACL 設定ウィザード]** ウィンドウに戻ります。
[戻る] ボタンをクリックして、ウィザードの前のステップに戻ります。

7.2 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 7-12 ACL アクセスリスト

[ACL アクセスリスト] 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
ACL タイプ	検索する ACL タイプを選択します。選択する値は、**[全]**、**[IP ACL]**、**[IPv6 ACL]**、**[MAC ACL]**、および **[Expert ACL]** です。
ID	アクセスリスト ID を選択および入力します。範囲は 1 ～ 14999 です。
ACL 名称	アクセスリスト名を選択および入力します。名前は 32 文字までです。

[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[ACL 追加] ボタンをクリックして、新しい ACL プロファイルエントリを追加します。
[編集] ボタンをクリックして、指定したエントリの設定を編集します。
[削除] ボタンをクリックして、指定したエントリを削除します。
[カウンタ全クリア] ボタンをクリックして、すべてのカウンタ情報をクリアします。
[カウンタクリア] ボタンをクリックして、選択した ACL プロファイルに関連するカウンタ情報をクリアします。

[ルール追加] ボタンをクリックして、選択した ACL プロファイルに新しい ACL ルールエントリを追加します。
複数のページが存在する場合は、ページ番号を入力し、[Go] ボタンをクリックして特定のページに移動します。

[編集] ボタンをクリックして、以下のウィンドウを表示します。

図 7-13 ACL アクセスリスト（編集）

[ACL アクセスリスト] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始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。ステップの範囲は 1 ～ 32 です。これは、シーケンスナンバーのステップ数を指定します。デフォルト値は 10 です。たとえば、増分（ステップ）値が 5、開始シーケンスナンバーが 20 である場合、それ以降のシーケンスナンバーは、25、30、35、40 のようになります。
カウンタ状態	カウンタ状態オプションを有効または無効にします。
注釈	この ACL に関連付けるオプションの注釈を入力します。

[適用] ボタンをクリックして、変更内容を確認します。

7.2.1 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 7-14 ACL アクセスリスト（ACL 追加、標準 IP ACL）

[ACL アクセスリスト追加] 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
ACL タイプ	作成する ACL タイプを選択します。選択する値は、**[標準 IP ACL]**、**[拡張 IP ACL]**、**[標準 IPv6 ACL]**、**[拡張 IPv6 ACL]**、**[拡張 MAC ACL]**、および **[Extended Expert ACL]** です。 このセクションでは、標準 IP ACL の設定方法について説明します。
ID	標準 IP ACL の ID を入力します。範囲は 1 ～ 1999 です。
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL プロファイルを追加します。

標準 IP ACL プロファイルを選択して **[ルール追加]** 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 7-15 ACL アクセスリスト（ルール追加、標準 IP ACL）

[ACL ルール追加] 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
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。このナンバーは、指定しない場合、自動生成されます。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
ソース	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト 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。
ディスティネーション	ディスティネーション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** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IP アドレスを使用および入力します。 • **IP** - **[Wildcard]** のビットマップを使用して、ディスティネーション IP アドレスのグループを使用および入力します。ビット値 1 に対応するビットは無視されます。ビット値 0 に対応するビットはチェックされます。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL ルールを追加します。
[戻る] ボタンをクリックして、**[ACL アクセスリスト]** ウィンドウに戻ります。

7.2.2 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 7-16 ACL アクセスリスト（ACL 追加、拡張 IP ACL）

[ACL アクセスリスト追加] 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
ACL タイプ	作成する ACL タイプを選択します。選択する値は、**[標準 IP ACL]**、**[拡張 IP ACL]**、**[標準 IPv6 ACL]**、**[拡張 IPv6 ACL]**、**[拡張 MAC ACL]**、および **[Extended Expert ACL]** です。 このセクションでは、拡張 IP ACL の設定方法について説明します。
ID	拡張 IP ACL の ID を入力します。範囲は 2000 ～ 3999 です。
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL プロファイルを追加します。

拡張 IP ACL プロファイルを選択して **[ルール追加]** 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。

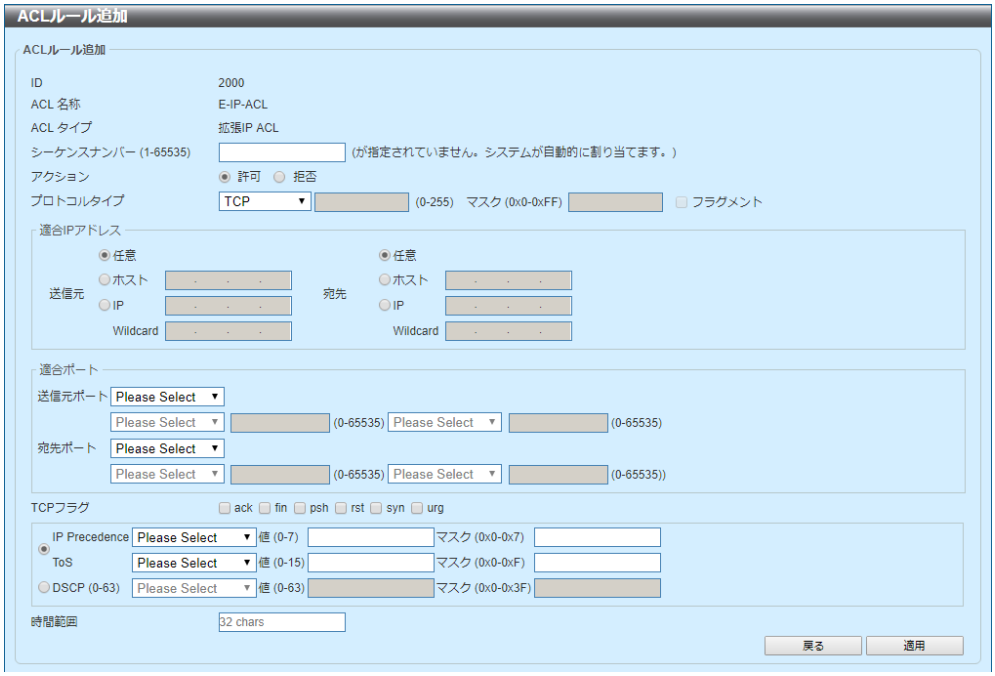


図 7-17 ACL アクセスリスト（ルール追加、拡張 IP ACL）

[ACL ルール追加] 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
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。このナンバーは、指定しない場合、自動生成されます。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
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）、**[プロトコル ID]**、および **[なし]** 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** - **[プロトコル ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。

パラメータ	概要
ソース	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト 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。
ディスティネーション	ディスティネーション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。
ソースポート	ソースポート値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。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。

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

パラメータ	概要
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）、および **[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）、および **[ef]**（46）です。 • **値** - DSCP 値を手動でも入力できます。範囲は 0 ～ 63 です。 • **マスク** - DSCP マスク値を入力します。範囲は 0x0 ～ 0x3F です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL ルールを追加します。
[戻る] ボタンをクリックして、[ACL アクセスリスト] ウィンドウに戻ります。

7.2.3 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 7-18 ACL アクセスリスト（ACL 追加、標準 IPv6 ACL）

[ACL アクセスリスト追加] 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
ACL タイプ	作成する ACL タイプを選択します。選択する値は、**[標準 IP ACL]**、**[拡張 IP ACL]**、**[標準 IPv6 ACL]**、**[拡張 IPv6 ACL]**、**[拡張 MAC ACL]**、および **[Extended Expert ACL]** です。 このセクションでは、標準 IPv6 ACL の設定方法について説明します。
ID	標準 IPv6 ACL の ID を入力します。範囲は 11000 ～ 12999 です。
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL プロファイルを追加します。

標準 IPv6 ACL プロファイルを選択して **[ルール追加]** 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 7-19 ACL アクセスリスト（ルール追加、標準 IPv6 ACL）

[ACL ルール追加] 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
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。このナンバーは、指定しない場合、自動生成されます。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
ソース	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ソース IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
ディスティネーション	ディスティネーション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** - 任意のディスティネーショントラフィックをこのルールの条件に従って評価します。 • **ホスト** - ディスティネーションホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ディスティネーション IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL ルールを追加します。
[戻る] ボタンをクリックして、**[ACL アクセスリスト]** ウィンドウに戻ります。

7.2.4 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。

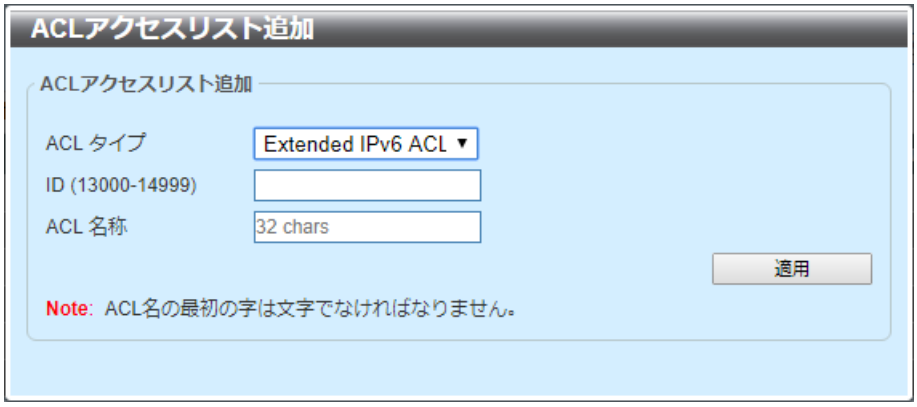


図 7-20 ACL アクセスリスト（ACL 追加、拡張 IPv6 ACL）

[ACL アクセスリスト追加] 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
ACL タイプ	作成する ACL タイプを選択します。選択する値は、**[標準 IP ACL]**、**[拡張 IP ACL]**、**[標準 IPv6 ACL]**、**[拡張 IPv6 ACL]**、**[拡張 MAC ACL]**、および **[Extended Expert ACL]** です。 このセクションでは、**拡張 IPv6 ACL** の設定方法について説明します。
ID	拡張 IPv6 ACL の ID を入力します。範囲は 13000 ～ 14999 です。
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL プロファイルを追加します。

拡張 IPv6 ACL プロファイルを選択して **[ルール追加]** 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 7-21 ACL アクセスリスト（ルール追加、拡張 IPv6 ACL）

[ACL ルール追加] 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
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。このナンバーは、指定しない場合、自動生成されます。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
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]**、**[プロトコル ID]**、**[ESP]**（50）、**[PCP]**（108）、**[SCTP]**（132）、および **[なし]** 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** - **[プロトコル ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。

パラメータ	概要
ソース	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト IPv6 アドレスを使用および入力します。 • **IPv6** - ソース IPv6 アドレスおよび**プレフィックス長**値を表示された入力フィールドに入力します。
ディスティネーション	ディスティネーション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。
ソースポート	ソースポート値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。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。

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

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

[適用] ボタンをクリックして、新しい ACL ルールを追加します。
[戻る] ボタンをクリックして、**[ACL アクセスリスト]** ウィンドウに戻ります。

7.2.5 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 7-22 ACL アクセスリスト（ACL 追加、拡張 MAC ACL）

[ACL アクセスリスト追加] 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
ACL タイプ	作成する ACL タイプを選択します。選択する値は、**[標準 IP ACL]**、**[拡張 IP ACL]**、**[標準 IPv6 ACL]**、**[拡張 IPv6 ACL]**、**[拡張 MAC ACL]**、および **[Extended Expert ACL]** です。 このセクションでは、**拡張 MAC ACL** の設定方法について説明します。
ID	拡張 MAC ACL の ID を入力します。範囲は 6 ～ 7999 です。
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL プロファイルを追加します。

拡張 MAC ACL プロファイルを選択して **[ルール追加]** 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 7-23 ACL アクセスリスト（ルール追加、拡張 MAC ACL）

[ACL ルール追加] 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
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。指定しない場合、このナンバーは自動生成されます。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
ソース	ソース MAC 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 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。
ディスティネーション	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。選択する値は以下のとおりです。 • **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]**、および **[arp]** です。

パラメータ	概要
イーサネットタイプ	イーサネットタイプを 16 進数値で入力します。範囲は 0x600 ～ 0xFFFF です。[指定イーサタイプ] ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
イーサネットタイプマスク	イーサネットタイプマスクを 16 進数値で入力します。範囲は 0x0 ～ 0xFFFF です。[指定イーサタイプ] ドロップダウンリストで任意のイーサネットタイププロファイルを選択した場合、適切な 16 進数値が自動的に表示されます。
CoS	使用する CoS 値を選択します。範囲は 0 ～ 7 です。 • **マスク** - CoS マスク値を入力します。範囲は 0x0 ～ 0x7 です。
VID	使用する VLAN ID を入力します。範囲は 1 ～ 4094 です。 • **マスク** - VLAN ID マスク値を入力します。範囲は 0x0 ～ 0xFFF です。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL ルールを追加します。
[戻る] ボタンをクリックして、**[ACL アクセスリスト]** ウィンドウに戻ります。

7.2.6 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 7-24 ACL アクセスリスト（ACL 追加、Extended Expert ACL）

[ACL アクセスリスト追加] 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
ACL タイプ	作成する ACL タイプを選択します。選択する値は、**[標準 IP ACL]**、**[拡張 IP ACL]**、**[標準 IPv6 ACL]**、**[拡張 IPv6 ACL]**、**[拡張 MAC ACL]**、および **[Extended Expert ACL]** です。 このセクションでは、**Extended Expert ACL** の設定方法について説明します。
ID	Extended Expert ACL の ID を入力します。範囲は 8000 ～ 9999 です。
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL プロファイルを追加します。

Extended Expert ACL プロファイルを選択して **[ルール追加]** 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。

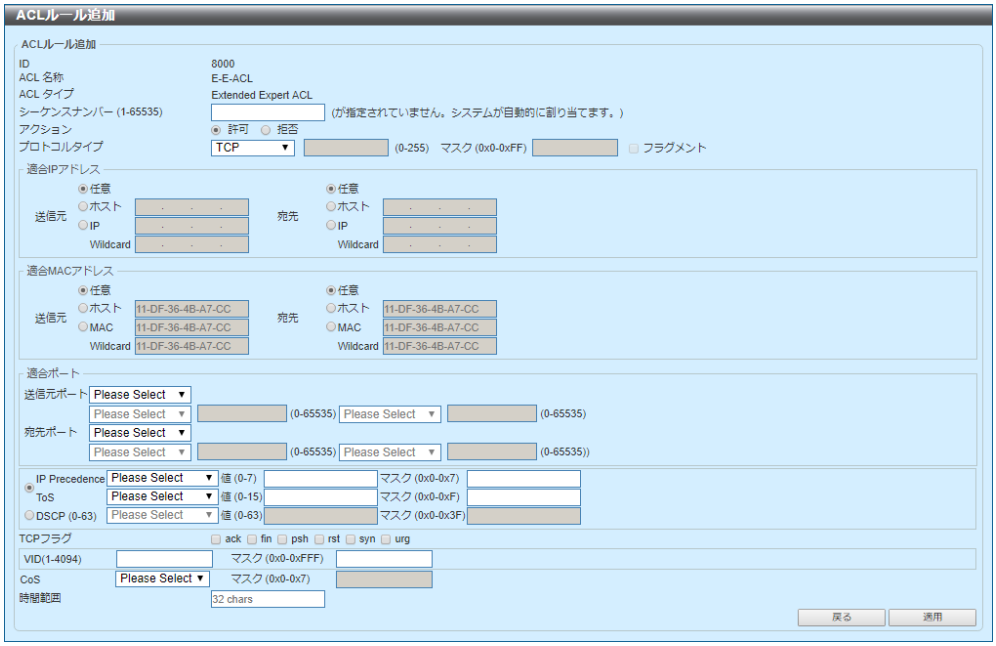


図 7-25 ACL アクセスリスト（ルール追加、Extended Expert ACL）

[ACL ルール追加] 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
シーケンスナンバー	ACL ルールナンバーを入力します。範囲は 1 ～ 65535 です。指定しない場合、このナンバーは自動生成されます。
アクション	このルールで実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
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）、**[プロトコル ID]**、および **[なし]** 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** - **[プロトコル ID]** オプションを選択した後、手動でプロトコルマスク値を入力します。範囲は 0x0 ～ 0xFF です。 • **フラグメント** - このオプションを選択した場合、パケットフラグメントフィルタリングが含まれます。

パラメータ	概要
ソース（**IP** アドレス）	ソース情報を選択および入力します。選択する値は以下のとおりです。 • **任意** - 任意のソーストラフィックをこのルールの条件に従って評価します。 • **ホスト** - ソースホスト 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。
ディスティネーション（**IP** アドレス）	ディスティネーション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。
ソース（**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。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 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。
ディスティネーション（**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。選択する値は以下のとおりです。 • **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。

パラメータ	概要
ソースポート	ソースポート値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。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。
ディスティネーションポート	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。選択する値は以下のとおりです。 • **=** - ACL は指定したポート番号のみ使用します。 • **>** - ACL は指定したポート番号より大きいすべてのポートを使用します。 • **<** - ACL は指定したポート番号より小さいすべてのポートを使用します。 • **≠** - ACL は指定したポート番号を除くすべてのポートを使用します。 • **範囲** - ACL は範囲内の指定されたポートを使用します。 • **マスク** - ACL は指定されたマスクの範囲内のポートを使用します。ポートマスク値を表示された入力フィールドに入力します。範囲は 0x0 ～ 0xFFFF です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** または **[UDP]** を選択した場合のみ利用可能です。
指定 ICMP メッセージタイプ	使用する ICMP メッセージタイプを選択します。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。
ICMP メッセージタイプ	**[指定 ICMP メッセージタイプ]** を選択しない場合、使用する ICMP メッセージタイプの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。

パラメータ	概要
メッセージコード	**[指定 ICMP メッセージタイプ]** を選択しない場合、使用するメッセージコードの数値を入力します。範囲は 0 ～ 255 です。**[ICMP メッセージタイプ]** を選択した場合、メッセージタイプの数値が自動入力されます。 このパラメータは、**[プロトコルタイプ]** で **[ICMP]** を選択した場合のみ利用可能です。
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）、および **[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）、および **[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）、および **[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	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]**、および **[urg]** です。 このパラメータは、**[プロトコルタイプ]** で **[TCP]** を選択した場合のみ利用可能です。
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。
時間範囲	この ACL ルールで使用する時間範囲プロファイルの名前を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、新しい ACL ルールを追加します。
[戻る] ボタンをクリックして、**[ACL アクセスリスト]** ウィンドウに戻ります。

7.3 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 7-26 ACL インタフェースアクセスグループ

[ACL インタフェースアクセスグループ] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
方向	方向を選択します。選択する値は **[In]** および **[Out]** です。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
タイプ	ACL タイプを選択します。選択する値は、**[IP ACL]**、**[IPv6 ACL]**、**[MAC ACL]**、および **[Expert ACL]** です。
ACL 名称	ACL 名称をここに入力します。名前は 32 文字までです。**[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。

[適用] ボタンをクリックして、変更内容を確認します。
[選択してください。] ボタンをクリックして、このウィンドウで使用できる設定済みのアクセスコントロールリストを表示します。

[選択してください。] ボタンをクリックして、以下のウィンドウを表示します。

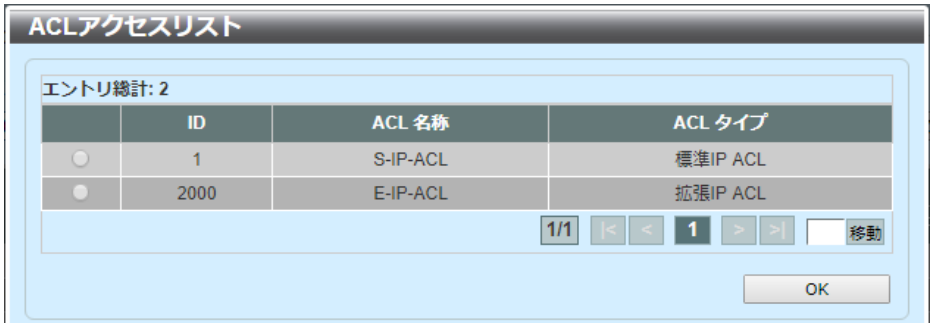


図 7-27 ACL インタフェースアクセスグループ（選択してください。）

[OK] ボタンをクリックして、選択したアクセスコントロールリストを使用します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

7.4 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 7-28 ACL VLAN アクセスマップ

[ACL VLAN アクセスマップ] 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
アクセスマップ名	アクセスマップ名を入力します。名前は 32 文字までです。
サブマップナンバー	サブマップナンバーを入力します。範囲は 1 ～ 65535 です。
アクション	実行するアクションを選択します。選択する値は **[Forward]**、**[Drop]**、および **[Redirect]** です。**[Redirect]** オプションを選択した場合、ドロップダウンリストでリダイレクト先インタフェースを選択します。
カウンタ状態	カウンタ状態を有効または無効にします。

[適用] ボタンをクリックして、新しいエントリを追加します。
[カウンタ全クリア] ボタンをクリックして、すべてのカウンタ情報をクリアします。
[カウンタクリア] ボタンをクリックして、指定したアクセスマップに関連するカウンタ情報をクリアします。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[バインディング] ボタンをクリックして、指定したエントリのバインディングを設定します。
[削除] ボタンをクリックして、指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

[バインディング] ボタンをクリックして、以下のウィンドウを表示します。

図 7-29 ACL VLAN アクセスマップ（バインディング）

[適合アクセスリスト] 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
適合 IP アクセスリスト	適合する IP アクセスリストが表示されます。
適合 IPv6 アクセスリスト	適合する IPv6 アクセスリストが表示されます。
適合 MAC アクセスリスト	適合する MAC アクセスリストが表示されます。

[選択してください。] ボタンをクリックして、このウィンドウで使用できる設定済みのアクセスコントロールリストを表示します。
[適用] ボタンをクリックして、変更内容を確認します。
[削除] ボタンをクリックして、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。] ボタンをクリックして、以下のウィンドウを表示します。

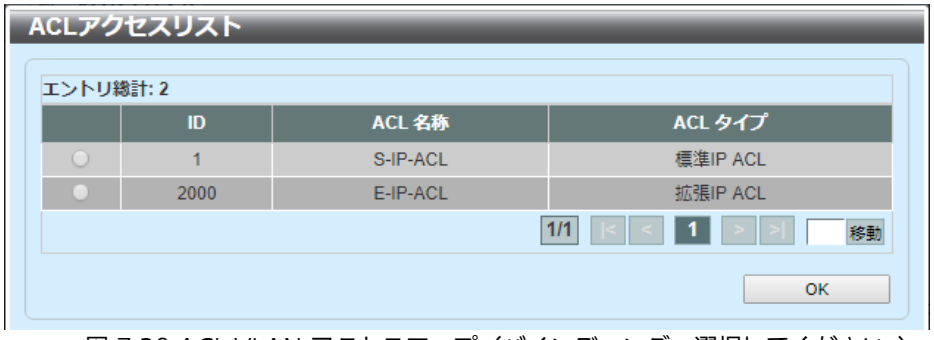


図 7-30 ACL VLAN アクセスマップ（バインディング、選択してください。）

[OK] ボタンをクリックして、選択したアクセスコントロールリストを使用します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

7.5 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 7-31 ACL VLAN フィルタ

[ACL VLAN フィルタ] 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
アクセスマップ名	アクセスマップ名を入力します。名前は 32 文字までです。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
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。範囲は 1 ～ 4094 です。**[全 VLAN]** オプションを選択した場合、このスイッチで設定されているすべての VLAN にこのコンフィグレーションを適用します。

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

8 セキュリティ

8.1 ポートセキュリティ

8.1.1 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 8-1 ポートセキュリティグローバル設定

[ポートセキュリティシステム設定] 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
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。指定しない場合のデフォルト値は **[制限なし]** です。有効な範囲は 1 ～ 3328 です。**[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] ボタンをクリックして、変更内容を確認します。

[ポートセキュリティ VLAN 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
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。範囲は 1 ～ 4094 です。
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。範囲は 1 ～ 3328 です。**[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] ボタンをクリックして、指定した情報に基づいて新しいエントリを追加します。

[検索 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。範囲は 1 ～ 4094 です。

[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。

8.1.2 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 8-2 ポートセキュリティポート設定

[ポートセキュリティポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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を有効または無効にします。
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。範囲は 0 ～ 3328 です。デフォルトでは、この値は 32 です。
違反時アクション	実行する違反時アクションを選択します。選択する値は以下のとおりです。 • **プロテクト** - 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。 • **制限** - 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。 • **シャットダウン** - 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。選択する値は以下のとおりです。 • **不変** - 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。 • **タイムアウト削除** - 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値を入力します。範囲は、0 ～ 1440 分です。
エージングタイプ	エージングタイプを選択します。選択する値は以下のとおりです。 • **アブソリュート** - このポートのセキュアアドレスはすべて、指定した時間が過ぎるとただちにエージアウトし、セキュアアドレスリストから削除されます。これがデフォルトのタイプです。 • **非アクティブ** - このポートのセキュアアドレスがエージアウトするのは、指定した期間にセキュアなソースアドレスからのデータトラフィックがない場合のみです。

[適用] ボタンをクリックして、変更内容を確認します。

8.1.3 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 8-3 ポートセキュリティアドレスエントリ

[ポートセキュリティアドレスエントリ] 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
ポート	使用する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。範囲は 1 ～ 4094 です。

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

8.2 802.1X

8.2.1 802.1X 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 8-4 802.1X グローバル設定

[802.1X グローバル設定] 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
システム認証制御	システム認証制御を有効または無効にします。この機能は、未認証ホストによるネットワークへのアクセスを制限します。
NAS ID	NAS（Network Access Server）の ID を入力します。
EAP リクエスト間隔	EAP（Extensible Authentication Protocol）リクエスト間隔を入力します。範囲は、1 ～ 3600 秒です。

[適用] ボタンをクリックして、変更内容を確認します。

[802.1X 認証ポート設定] 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
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を選択します。選択する値は **[ポートベース]** および **[MAC ベース]** です。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更内容を確認します。

8.2.2 802.1X 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 8-5 802.1X 強制認証 MAC 設定

[強制認証 MAC 設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。範囲は 0 ～ 48 です。
認証状態	認証状態を選択します。選択する値は以下のとおりです。 • **認証済み** - 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。 • **未認証** - 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] ボタンをクリックして、新しいエントリを追加します。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[削除] ボタンをクリックして、指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

8.2.3 802.1X 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。

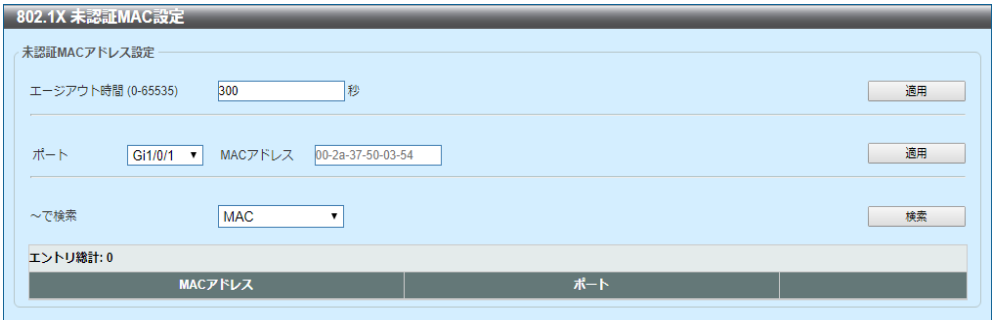


図 8-6 802.1X 未認証 MAC 設定

[未認証 MAC アドレス設定] 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
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。範囲は、0 ～ 65535 秒です。
開始ポート - 終了ポート	使用する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。
MAC で検索	このオプションを選択した場合、未認証の設定済みダイナミックホストを検索し、MAC アドレス順に表示します。
ポートで検索	このオプションを選択した場合、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および表示します。 • **開始ポート - 終了ポート** - 使用するポートを選択します。

[適用] ボタンをクリックして、変更内容を確認します。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。

8.2.4 802.1X 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 8-7 802.1X ポート設定（ポートベースアクセスコントロール）

[ポートベースアクセスコントロール] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。選択する値は以下のとおりです。 • **自動** - ポートの IEEE 802.1X 認証を有効にします。 • **強制認証** - 強制的にポートを認証状態にします。 • **強制未認証** - 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。選択する値は以下のとおりです。 • **両方** - 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。

パラメータ	概要
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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。
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。範囲は 1 ～ 10 です。
ポート毎再認証	指定したポートの定期的な再認証を有効または無効にします。
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使用を有効または無効にします。

[適用] ボタンをクリックして、変更内容を確認します。
[参照] ボタンをクリックして、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] ボタンをクリックして、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] ボタンをクリックして、指定したポートへの接続をすべて再認証します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

[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 8-8 802.1X ポート設定（MAC ベースアクセスコントロール）

[MAC ベースアクセスコントロール] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。範囲は 1 ～ 512 です。
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。選択する値は以下のとおりです。 • **両方** - 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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。
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。範囲は、1 ～ 65535 秒です。

パラメータ	概要
再認証期間	再認証期間を入力します。これは、再認証試行間隔の秒数です。範囲は、1 ～ 65535 秒です。
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。範囲は 1 ～ 10 です。
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使用を有効または無効にします。
ポート毎再認証	指定したポートの定期的な再認証を有効または無効にします。
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。範囲は、0 ～ 65535 秒です。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。

[適用] ボタンをクリックして、変更内容を確認します。
[参照] ボタンをクリックして、指定されたポートに関連付けられている MAC ベースアクセスコントロール設定を表示します。
[初期化] ボタンをクリックして、指定されたポートの MAC 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] ボタンをクリックして、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] ボタンをクリックして、このエントリに関する詳細情報を表示します。

[**詳細参照**] ボタンをクリックして、以下のウィンドウを表示します。

図 8-9 802.1X 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**] ボタンをクリックして、再認証機能を有効または無効にします。
[**初期化**] ボタンをクリックして、指定されたポートの MAC 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**] ボタンをクリックして、指定したサプリカント MAC アドレス接続を再認証します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。
[**戻る**] ボタンをクリックして、前のウィンドウに戻ります。

8.2.5 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。

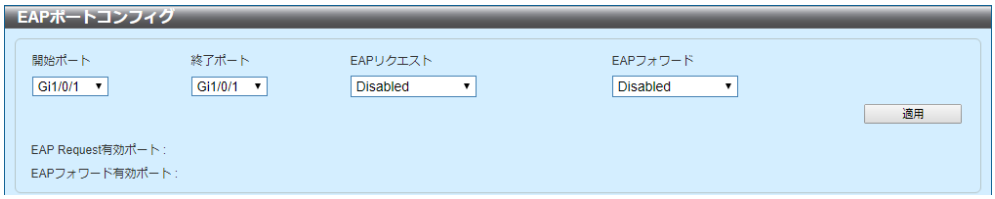


図 8-10 EAP ポートコンフィグ

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	使用するポートを選択します。
EAP リクエスト	指定したポートの EAP リクエスト機能を有効または無効にします。
EAP フォワード	指定したポートの EAP フォワード機能を有効または無効にします。これは、IEEE 802.1X PDU（Protocol Data Unit）のフォワーディングを有効 / 無効にするために使用します。

[適用] ボタンをクリックして、変更内容を確認します。

8.2.6 802.1X 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 8-11 802.1X 認証統計情報

[統計] 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
ポート	使用するポートを選択します。
以来	時間範囲を選択します。選択する値は以下のとおりです。 • **リセット以来** - 最後のスイッチリセット以来の統計を表示します。 • **アップ以来** - 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] ボタンをクリックして、指定した検索条件に基づいて情報を表示します。
[全リセット] ボタンをクリックして、すべての統計情報をリセットします。

8.2.7 802.1X サプリカントグローバル設定

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

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

図 8-12 802.1X サプリカントグローバル設定

[802.1X サプリカントグローバル設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ユーザ名	サプリカントのユーザ名を設定します。
パスワード	サプリカントのパスワードを設定します。
暗号化パスワード	暗号化されたパスワードを設定する際に利用します。
認証方式	認証方式を選択します。選択する値は以下のとおりです。 • md5- 認証方式を md5 に設定します。 • peap-mschapv2 - 認証方式を peap-mschapv2 に設定します。

[適用] ボタンをクリックして、変更を反映します。

8.2.8 802.1X サプリカントポート設定

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

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

図 8-13 802.1X サプリカントポート設定

[802.1X サプリカントポート設定] 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
ポート	設定するポートを選択します。
保存期間	サプリカントが認証を失敗した際に、次の認証まで待つ時間を設定します。 範囲は 0 ～ 65535 です。デフォルトは 60 秒です。
認証期間	オーセンティケーターからのリクエストを待つ時間を設定します。範囲は 1 ～ 65535 です。デフォルトは 30 秒です。
開始期間	認証を開始する際の EAPOL の送信間隔を設定します。 範囲は 1 ～ 65535 です。デフォルトは 30 秒です。
最大開始	EAPOL-Start パケットを送信する最大数を設定します。 範囲は 1 ～ 65535 です。デフォルトは、3 回 です。
状態	ポートのサプリカント機能の有効、無効を設定します。 • **Disabled** - 最後のスイッチリセット以来の統計を表示します。(初期値) • **Enabled** - 最後のスイッチブートアップ以来の統計を表示します。

[適用] ボタンをクリックして、変更を反映します。

8.2.9 802.1X サプリカント統計情報

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

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

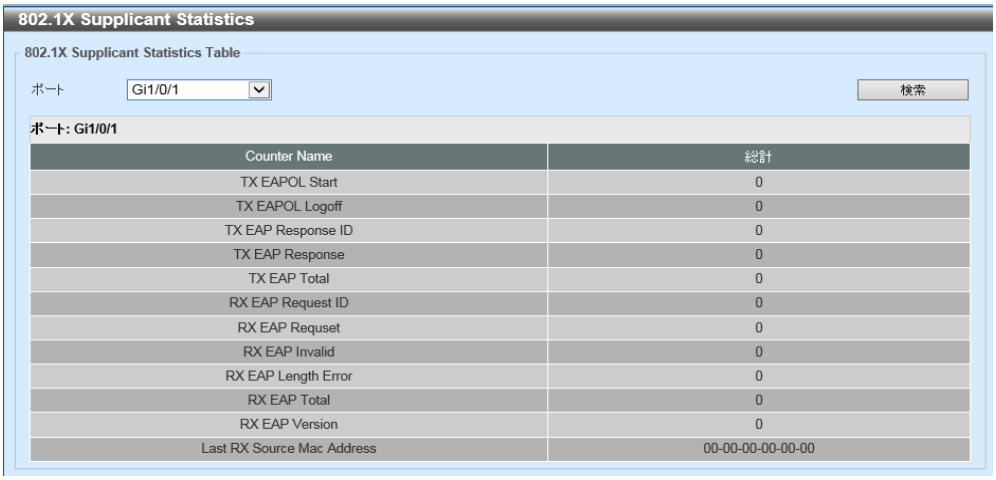


図 8-14 802.1X サプリカント統計情報

[802.1X Supplicant Statistics] 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
ポート	表示するポートを選択します。

[検索] ボタンをクリックして、指定したポート情報を表示します。

8.3 AAA（Authentication, Authorization, and Accounting）

8.3.1 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。

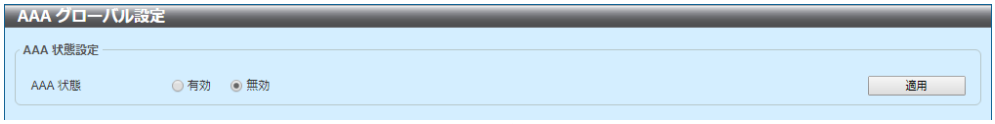


図 8-15 AAA グローバル設定

[AAA 状態設定] 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
AAA 状態	AAA 機能をグローバルに有効または無効にします。

[適用] ボタンをクリックして、変更内容を確認します。

8.3.2 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 8-16 AAA 認証設定

[AAA Web 認証設定] 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
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。選択する値は以下のとおりです。 • **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。 • **ローカル** - スイッチ上のローカルデータベースをプライマリデータベースとして使用します。
セカンダリデータベース	Web 認証に使用するセカンダリデータベースを選択します。選択する値は以下のとおりです。 • **なし** - 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。 • **ローカル** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。
認証失敗時動作	Web 認証が失敗した場合に実行するアクションを選択します。選択する値は以下のとおりです。 • **停止** - 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。 • **セカンダリ 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。範囲は、1 ～ 65535 秒です。

[適用] ボタンをクリックして、変更内容を確認します。

[AAA MAC 認証設定] 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
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。選択する値は以下のとおりです。 • **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。 • **ローカル** - スイッチ上のローカルデータベースをプライマリデータベースとして使用します。
セカンダリデータベース	MAC 認証に使用するセカンダリデータベースを選択します。選択する値は以下のとおりです。 • **なし** - 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。 • **ローカル** - スイッチ上のローカルデータベースをセカンダリデータベースとして使用します。
認証失敗時動作	MAC 認証が失敗した場合に実行するアクションを選択します。選択する値は以下のとおりです。 • **停止** - 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。 • **セカンダリ 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。範囲は、1 ～ 65535 秒です。

[適用] ボタンをクリックして、変更内容を確認します。

[AAA 802.1X 認証設定] 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
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。選択する値は以下のとおりです。 • **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。 • **ローカル** - スイッチ上のローカルデータベースをプライマリデータベースとして使用します。
セカンダリデータベース	IEEE 802.1X 認証に使用するセカンダリデータベースを選択します。選択する値は以下のとおりです。 • **なし** - セカンダリデータベースを使用しません。 • **ローカル** - 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] ボタンをクリックして、変更内容を確認します。

8.3.3 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 8-17 AAA 認証ユーザ設定

[AAA 認証ユーザ設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ユーザ名	ローカル認証アカウントのユーザ名を入力します。名前は 32 文字までです。
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。範囲は 1 ～ 4094 です。
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。選択する値は以下のとおりです。 • **両方** - ローカル認証アカウントを IEEE 802.1X 認証と Web 認証の両方で使用します。 • **Web** - ローカル認証アカウントを Web 認証のみで使用します。 • **Dot1X** - ローカル認証アカウントを IEEE 802.1X 認証のみで使用します。
2 ステップ認証	2 ステップ認証を有効または無効にします。

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

8.3.4 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。

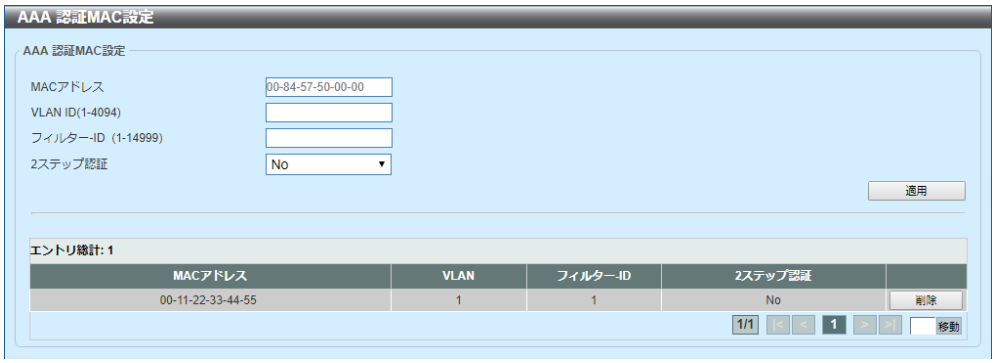


図 8-18 AAA 認証 MAC 設定

[AAA 認証 MAC 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
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。範囲は 1 ～ 4094 です。
2 ステップ認証	2 ステップ認証を有効または無効にします。選択する値は以下のとおりです。 • **No** - ローカル認証アカウントの 2 ステップ認証を無効にします。 • **Web** - 2 ステップ認証を有効にして、2 番目の認証方式として Web 認証を使用します。 • **802.1X** - 2 ステップ認証を有効にして、2 番目の認証方式として IEEE 802.1X 認証を使用します。 • **任意** - 2 ステップ認証を有効にして、2 番目の認証方式として IEEE 802.1X 認証と Web 認証を使用します。

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

8.3.5 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。

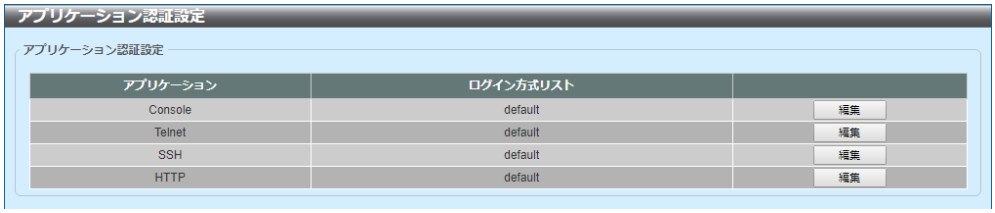


図 8-19 アプリケーション認証設定

[編集] ボタンをクリックして、以下のウィンドウを表示します。

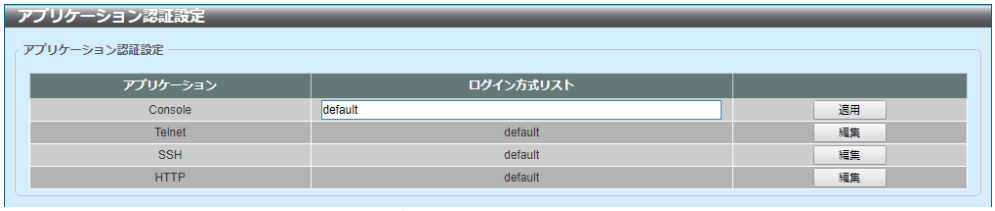


図 8-20 アプリケーション認証設定（編集）

[アプリケーション認証設定] 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
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] ボタンをクリックして、指定したエントリの設定を編集します。
[適用] ボタンをクリックして、変更内容を確認します。

8.3.6 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。

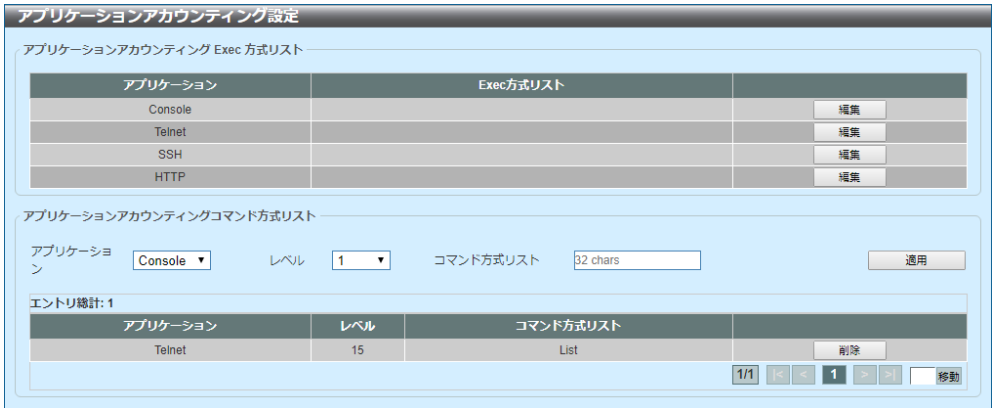


図 8-21 アプリケーションアカウンティング設定

[編集] ボタンをクリックして、以下のウィンドウを表示します。

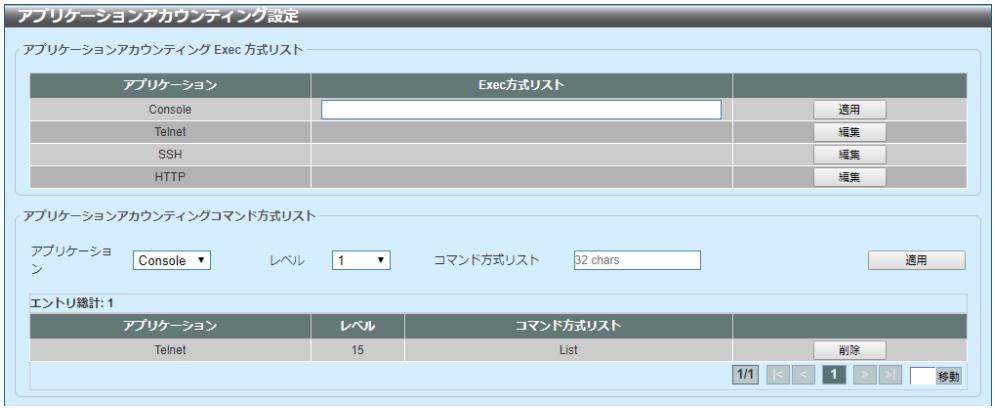


図 8-22 アプリケーションアカウンティング設定（編集）

[アプリケーションアカウンティング Exec 方式リスト] 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
Exec 方式リスト	Exec 方式リストの名前を入力します。

[適用] ボタンをクリックして、変更内容を確認します。

[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] セクションでは、以下のパラメータを設定できます。

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を選択します。選択する値は **[コンソール]**、**[Telnet]**、および **[SSH]** です。
レベル	使用する特権レベルを選択します。選択する値の範囲はレベル 1 ～ 15 です。
コマンド方式リスト	使用するコマンド方式リストの名前を入力します。

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

8.3.7 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 8-23 認証 EXEC の設定

[AAA 認証有効] 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	AAA 認証有効状態を有効または無効にします。
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。選択する値は以下のとおりです。 • **なし** - 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。 • **有効** - 認証にローカルイネーブルパスワードを使用します。 • **グループ** - 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。この文字列は 32 文字までです。 • **RADIUS** - radius server host コマンドによって定義されているサーバを使用します。 • **TACACS+** - tacacs+ server host コマンドによって定義されているサーバを使用します。

[適用] ボタンをクリックして、変更内容を確認します。

[AAA 認証ログイン] 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
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。
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。選択する値は以下のとおりです。 • なし - 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。 • ローカル - 認証にローカルデータベースを使用します。 • グループ - 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。この文字列は 32 文字までです。 • RADIUS - radius server host コマンドによって定義されているサーバを使用します。 • TACACS+ - tacacs+ server host コマンドによって定義されているサーバを使用します。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したエントリを削除します。

8.3.8 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 8-24 アカウンティング設定（AAA アカウンティングネットワーク）

[AAA アカウンティングネットワーク] 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
デフォルト	デフォルト方式リストの使用を有効または無効にします。
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。選択する値は、**[なし]**、**[グループ]**、**[RADIUS]**、および **[TACACS+]** です。**[なし]** オプションは、方式 1 にのみ利用可能です。

[適用] ボタンをクリックして、変更内容を確認します。

[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 8-25 アカウンティング設定（AAA アカウンティングシステム）

[AAA アカウンティングシステム] 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
デフォルト	デフォルト方式リストの使用を有効または無効にします。
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。選択する値は、**[なし]**、**[グループ]**、**[RADIUS]**、および **[TACACS+]** です。**[なし]** オプションは、方式 1 にのみ利用可能です。

[適用] ボタンをクリックして、変更内容を確認します。

[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 8-26 アカウンティング設定（AAA アカウンティング動作契機）

[AAA アカウンティング動作契機] 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
リスト名	[AAA アカウンティング動作契機] オプションで使用する方式リスト名を入力します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リストを選択します。選択する値は、[なし]、[グループ]、[RADIUS]、および [TACACS+] です。[なし] オプションは、方式 1 にのみ利用可能です。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定した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 8-27 アカウンティング設定（AAA アカウンティングコマンド）

[AAA アカウンティングコマンド] 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
レベル	使用する特権レベルを選択します。選択する値の範囲はレベル 1 ～ 15 です。
リスト名	**[AAA アカウンティングコマンド]** オプションで使用する方式リスト名を入力します。
方式 1 ～方式 4	このコンフィグレーションに使用する方式リストを選択します。選択する値は、**[なし]**、**[グループ]**、および **[TACACS+]** です。**[なし]** オプションは、方式 1 にのみ利用可能です。

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

8.4 認証

8.4.1 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。

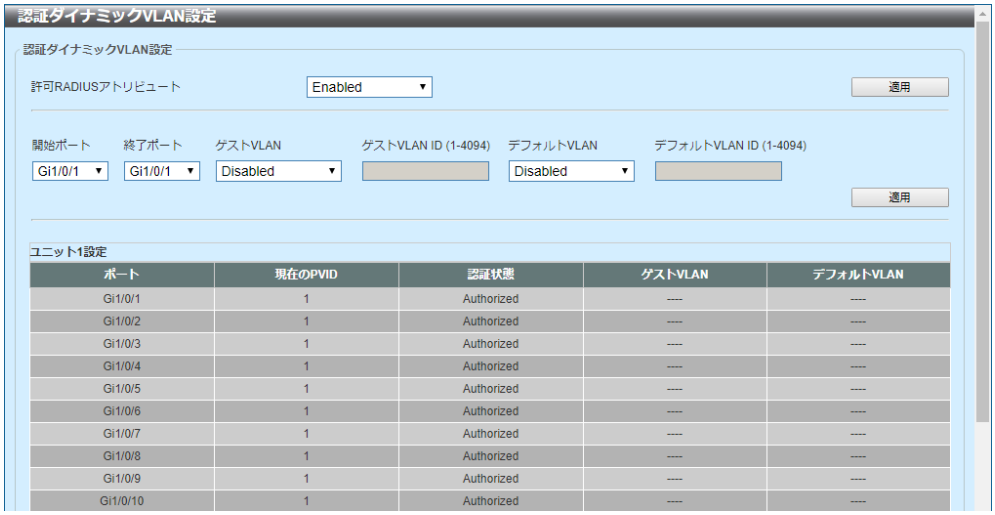


図 8-28 認証ダイナミック VLAN 設定

[認証ダイナミック VLAN 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
許可 RADIUS アトリビュート	RADIUS アトリビュートの受け入れを有効または無効にします。
開始ポート - 終了ポート	使用するポートを選択します。
ゲスト VLAN	ゲスト VLAN を有効または無効にします。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。範囲は 1 ～ 4094 です。
デフォルト VLAN	デフォルト VLAN を有効または無効にします。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。範囲は 1 ～ 4094 です。

[適用] ボタンをクリックして、変更内容を確認します。

8.4.2 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 8-29 認証状態テーブル

[認証状態テーブル] 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
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。範囲は、0 ～ 65535 分です。
Sort By - MAC	このオプションを選択した場合、認証セッションを MAC アドレス順に表示します。
Sort By - ポート	このオプションを選択した場合、指定したポートの認証セッションを表示します。 • **開始ポート - 終了ポート** - 使用するポートを選択します。

[適用] ボタンをクリックして、変更内容を確認します。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。

8.4.3 2 ステップ認証の設定

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

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

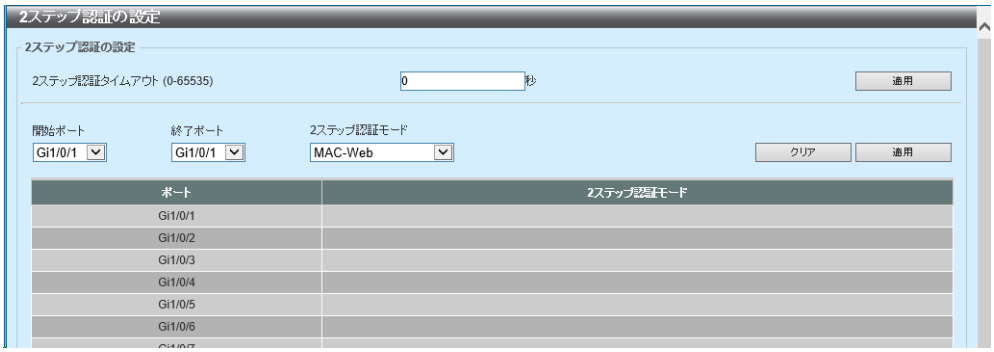


図 8-30 2 ステップ認証の設定

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

パラメータ	概要
2 ステップ認証タイムアウト	タイムアウト値を入力します。この時間が経過すると、認証の第 2 段階を試行します。範囲は、0 ～ 65535 分です。
開始ポート - 終了ポート	使用するポートを選択します。
2 ステップ認証モード	2 ステップ認証モードを選択します。選択する値は以下のとおりです。 • **MAC-Web** - 2 ステップ認証方式の最初のステップで MAC 認証と Web 認証の両方を使用します。 • **MAC-Dot1X** - 2 ステップ認証方式の最初のステップで MAC 認証と IEEE 802.1X 認証の両方を使用します。 • **Dot1X-Web** - 2 ステップ認証方式の最初のステップで IEEE 802.1X 認証と Web 認証の両方を使用します。

[適用] ボタンをクリックして、変更内容を確認します。
[クリア] ボタンをクリックして、指定した条件に基づいて情報をクリアします。

8.5 RADIUS（Remote Authentication Dial-In User Service）

8.5.1 RADIUS グローバル設定

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

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

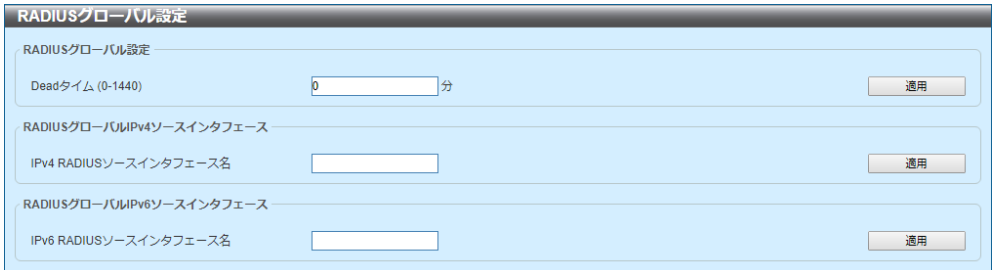


図 8-31 RADIUS グローバル設定

[RADIUS グローバル設定] 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
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。範囲は、1 ～ 1440 分です。デフォルトでは、この値は 0 分です。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。

[適用] ボタンをクリックして、変更を反映します。

[RADIUS グローバル IPv4 ソースインタフェース] 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
IPv4 RADIUS ソースインタフェース名	IPv4 RADIUS ソースインタフェースの名前を入力します。

[適用] ボタンをクリックして、変更を反映します。

[RADIUS グローバル IPv6 ソースインタフェース] 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
IPv6 RADIUS ソースインタフェース名	IPv6 RADIUS ソースインタフェースの名前を入力します。

[適用] ボタンをクリックして、変更を反映します。

8.5.2 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 8-32 RADIUS サーバ設定

[RADIUS サーバ設定] 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
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。範囲は 0 ～ 65535 です。デフォルトでは、この値は 1812 です。認証を使用しない場合は、値 0 を使用します。
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。範囲は 0 ～ 65535 です。デフォルトでは、この値は 1813 です。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。
再送信	再送信回数の値を入力します。範囲は 0 ～ 20 です。デフォルトでは、この値は 3 です。このオプションを無効にするには、値 0 を入力します。
タイムアウト	使用するタイムアウト値を入力します。範囲は、1 ～ 255 秒です。デフォルトでは、この値は 5 秒です。
キータイプ	使用するキータイプを選択します。選択する値は **[プレーンテキスト]** および **[暗号化]** です。
キー	RADIUS サーバとの通信に使用するキーを入力します。このキーは 32 文字までです。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したエントリを削除します。

8.5.3 RADIUS グループサーバ設定

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

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

図 8-33 RADIUS グループサーバ設定

[RADIUS グループサーバ設定] 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] ボタンをクリックして、新しいエントリを追加します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。
[削除] ボタンをクリックして、指定したエントリを削除します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

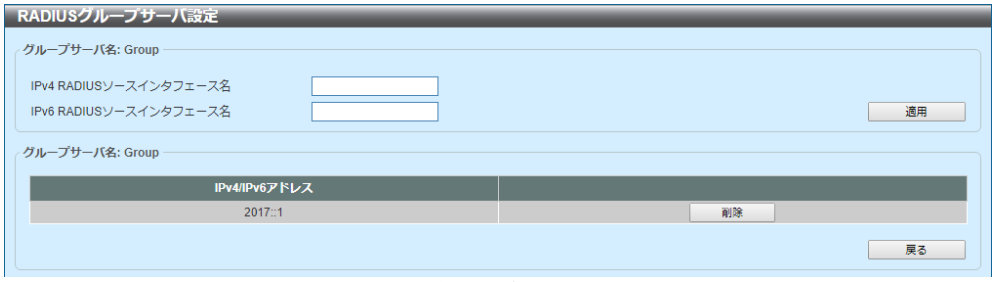


図 8-34 RADIUS グループサーバ設定（詳細参照）

以下のパラメータを設定できます。

パラメータ	概要
IPv4 RADIUS ソースインタフェース名	IPv4 RADIUS ソースインタフェースの名前を入力します。
IPv6 RADIUS ソースインタフェース名	IPv6 RADIUS ソースインタフェースの名前を入力します。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したエントリを削除します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

8.5.4 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 8-35 RADIUS 統計

[RADIUS 統計] 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。

1 番目の **[クリア]** ボタンをクリックして、指定した条件に基づいて統計情報をクリアします。
[全クリア] ボタンをクリックして、すべての統計情報をクリアします。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。
2 番目の **[クリア]** ボタンをクリックして、テーブルの統計情報をクリアします。

8.6 TACACS+（Terminal Access Controller Access-Control System Plus）

8.6.1 TACACS+ グローバル設定

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

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

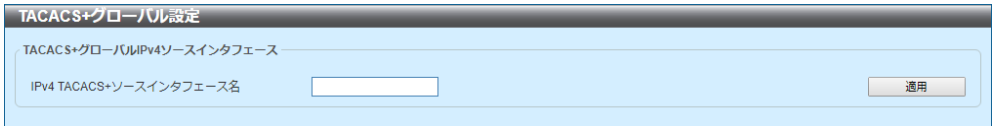


図 8-36 TACACS+ グローバル設定

[TACACS+ グローバル IPv4 ソースインタフェース] 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
IPv4 TACACS+ ソースインタフェース名	IPv4 TACACS+ ソースインタフェースの名前を入力します。

[適用] ボタンをクリックして、変更を反映します。

8.6.2 TACACS+ サーバ設定

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

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

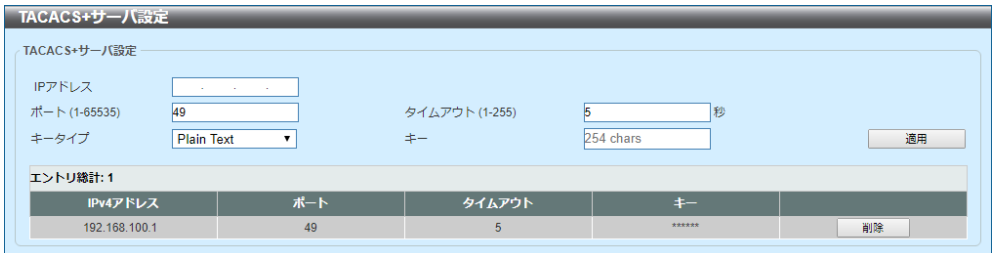


図 8-37 TACACS+ サーバ設定

[TACACS+ サーバ設定] 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
IP アドレス	TACACS+ サーバの IPv4 アドレスを入力します。
ポート	使用するポート番号をここに入力します。範囲は 1 ～ 65535 です。デフォルトでは、この値は 49 です。
タイムアウト	タイムアウト値を入力します。範囲は、1 ～ 255 秒です。デフォルトでは、この値は 5 秒です。
キータイプ	使用するキータイプを選択します。選択する値は **[プレーンテキスト]** および **[暗号化]** です。
キー	TACACS+ サーバとの通信に使用するキーを入力します。このキーは 254 文字までです。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したエントリを削除します。

8.6.3 TACACS+ グループサーバ設定

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

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

図 8-38 TACACS+ グループサーバ設定

[TACACS+ グループサーバ設定] 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
グループサーバ名	TACACS+ グループサーバ名を入力します。名前は 32 文字までです。
IPv4 IP アドレス	TACACS+ グループサーバの IPv4 アドレスを入力します。

[追加] ボタンをクリックして、新しいエントリを追加します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。
[削除] ボタンをクリックして、指定したエントリを削除します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

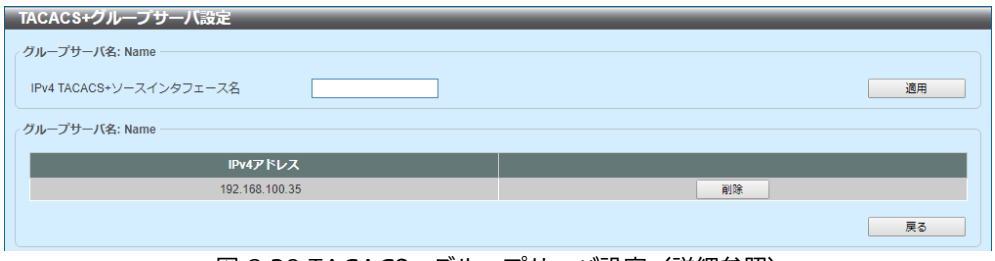


図 8-39 TACACS+ グループサーバ設定（詳細参照）

[TACACS+ グループサーバ設定] 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
IPv4 TACACS+ ソースインタフェース名	IPv4 TACACS+ ソースインタフェースの名前を入力します。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したエントリを削除します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。

8.6.4 TACACS+ 統計

このウィンドウを用いて、TACACS+ 統計情報を表示およびクリアします。

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

図 8-40 TACACS+ 統計

[TACACS+ 統計] 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
グループサーバ名	このリストから TACACS+ グループサーバ名を選択します。

1 番目の **[クリア]** ボタンをクリックして、指定した条件に基づいて統計情報をクリアします。
[全クリア] ボタンをクリックして、すべての統計情報をクリアします。
2 番目の **[クリア]** ボタンをクリックして、指定したエントリの統計情報をクリアします。

8.7 SAVI（Source Address Validation Improvements）

8.7.1 IPv4

8.7.1.1 DHCPv4 スヌーピング

8.7.1.1.1 DHCP スヌーピンググローバル設定

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

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピンググローバル設定] をクリックして、以下のウィンドウを表示します。

図 8-41 DHCP スヌーピンググローバル設定

[DHCP スヌーピンググローバル設定] 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
DHCP スヌーピング	DHCP スヌーピングをグローバルに有効または無効にします。
非信頼許可オプション情報	非信頼インタフェースでリレー Option 82 が設定されている DHCP パケットを許可するオプションをグローバルに有効または無効にします。
ソース MAC 確認	DHCP パケットのソース MAC アドレスがクライアントのハードウェアアドレスと適合することの検証を有効または無効にします。
ステーションムーブ廃棄	DHCP スヌーピングステーションムーブ状態を有効または無効にします。DHCP スヌーピングステーションムーブが有効な場合、特定のポートで同じ VLAN ID と MAC アドレスを持つダイナミック DHCP スヌーピングバインディングエントリは、同じ VLAN ID と MAC アドレスを使用する新しい DHCP プロセスを検出した場合に別のポートに移動できます。

[適用] ボタンをクリックして、変更を反映します。

8.7.1.1.2 DHCP スヌーピングポート設定

このウィンドウを用いて、指定したポートの DHCP スヌーピングの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピングポート設定] をクリックして、以下のウィンドウを表示します。

図 8-42 DHCP スヌーピングポート設定

[DHCP スヌーピングポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。範囲は 0 ～ 508 です。 **[制限なし]** オプションをオンにした場合、機能を無効にします。
帯域制限	帯域制限値を入力します。範囲は 1 ～ 300 です。 **[制限なし]** オプションをオンにした場合、機能を無効にします。
Trusted	Trusted オプションを選択します。選択する値は **[No]** および **[Yes]** です。DHCP サーバまたは他のスイッチに接続しているポートは、Trusted インタフェースとして設定する必要があります。DHCP クライアントに接続しているポートは、非信頼インタフェースとして設定する必要があります。DHCP スヌーピングは、非信頼インタフェースと DHCP サーバの間でファイアウォールとして動作します。

[適用] ボタンをクリックして、変更を反映します。

8.7.1.1.3 DHCP スヌーピング VLAN 設定

このウィンドウを用いて、指定した VLAN の DHCP スヌーピングの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピング VLAN 設定] をクリックして、以下のウィンドウを表示します。

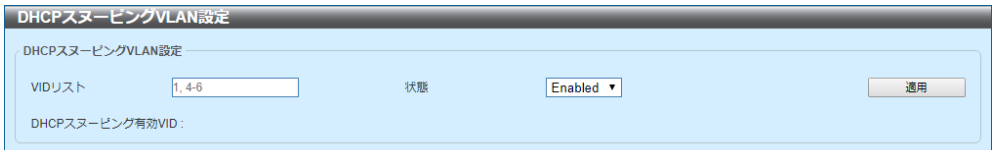


図 8-43 DHCP スヌーピング VLAN 設定

[DHCP スヌーピング VLAN 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
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。範囲は 1 ～ 4094 です。
状態	DHCP スヌーピング VLAN 設定を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

8.7.1.1.4 DHCP スヌーピングデータベース

このウィンドウを用いて、DHCP スヌーピングデータベースの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピングデータベース] をクリックして、以下のウィンドウを表示します。

図 8-44 DHCP スヌーピングデータベース

[DHCP スヌーピングデータベース] 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
書込み遅延	書込み遅延時間を入力します。範囲は、60 ～ 86400 秒です。デフォルトでは、この値は 300 秒です。

[リセット] ボタンをクリックして、DHCP スヌーピングデータベースをリセットします。
[適用] ボタンをクリックして、変更を反映します。

[DHCP スヌーピングデータベースの保存] 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
URL	ドロップダウンリストから場所を選択して、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。選択する場所は **[TFTP]**、**[FTP]**、および **[ローカル]** です。

[リセット] ボタンをクリックして、保存されている DHCP スヌーピングデータベースをリセットします。
[適用] ボタンをクリックして、DHCP スヌーピングデータベースを保存します。
[DHCP スヌーピングデータベースの読み込み] 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
URL	ドロップダウンリストから場所を選択して、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。選択する場所は **[TFTP]**、**[FTP]**、および **[ローカル]** です。

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

8.7.1.1.5 DHCP スヌーピングバインディングエントリ

このウィンドウを用いて、DHCP スヌーピングバインディングエントリの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [DHCPv4 スヌーピング] > [DHCP スヌーピングバインディングエントリ] をクリックして、以下のウィンドウを表示します。

図 8-45 DHCP スヌーピングバインディングエントリ

[DHCP スヌーピングマニュアルバインディング] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
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。範囲は 1 ～ 4094 です。
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	使用するポートを選択します。
Expiry	使用する有効期限値を入力します。範囲は、60 ～ 4294967295 秒です。

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

8.7.1.2 ダイナミック ARP 検査

8.7.1.2.1 ARP アクセスリスト

このウィンドウを用いて、ダイナミック ARP 検査に使用する ARP アクセスリストの設定を行い、設定値を表示します。

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

図 8-46 ARP アクセスリスト

[ARP アクセスリスト] 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
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。名前は 32 文字までです。

[追加] ボタンをクリックして、新しいエントリを追加します。
[編集] ボタンをクリックして、指定したエントリの設定を編集します。
[削除] ボタンをクリックして、指定したエントリを削除します。

[編集] ボタンをクリックして、以下のウィンドウを表示します。

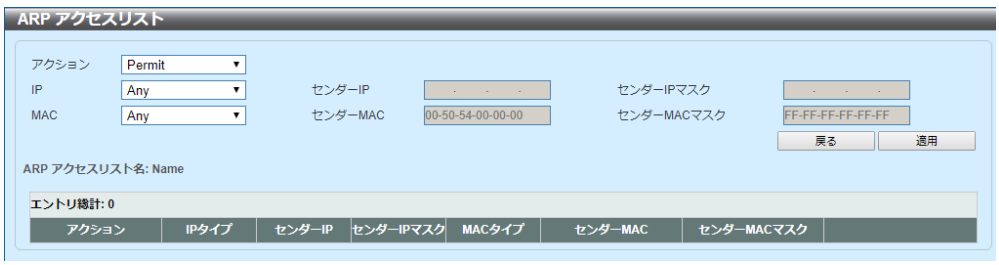


図 8-47 ARP アクセスリスト（編集）

以下のパラメータを設定できます。

パラメータ	概要
アクション	実行するアクションを選択します。選択する値は **[許可]** および **[拒否]** です。
IP	使用するセンダー IP アドレスのタイプを選択します。選択する値は、**[任意]**、**[ホスト]**、および **[IP とマスク]** です。
センダー IP	**[IP]** のタイプとして **[ホスト]** または **[IP とマスク]** のオプションを選択した場合、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]** のタイプとして **[IP とマスク]** オプションを選択した場合、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 アドレスのタイプを選択します。選択する値は、**[任意]**、**[ホスト]**、および **[MAC とマスク]** です。
センダー MAC	**[MAC]** のタイプとして **[ホスト]** または **[MAC とマスク]** のオプションを選択した場合、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]** のタイプとして **[MAC とマスク]** オプションを選択した場合、使用するセンダー MAC マスクを入力します。

[適用] ボタンをクリックして、新しいエントリを追加します。
[戻る] ボタンをクリックして、前のウィンドウに戻ります。
[削除] ボタンをクリックして、指定したエントリを削除します。

8.7.1.2.2 ARP 検査設定

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

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

図 8-48 ARP 検査設定

[ARP 検査項目] 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
ソース MAC	ソース MAC オプションを有効または無効にします。ARP リクエスト / 応答パケットをチェックして、イーサネットヘッダのソース MAC アドレスが ARP ペイロードのセンダー MAC アドレスと一致していることをチェックします。
ディスティネーション MAC	ディスティネーション MAC オプションを有効または無効にします。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。

パラメータ	概要
IP	IP オプションを有効または無効にします。ARP ボディで無効な IP アドレスや予期しない IP アドレスをチェックします。また、ARP ペイロードの IP アドレスの有効性をチェックします。ARP リクエスト / 応答の両方のセンダー IP と ARP 応答のターゲット IP を検証します。IP アドレス 0.0.0.0 と 255.255.255.255、およびすべての IP マルチキャストアドレスをディスティネーションとするパケットは、廃棄されます。センダー IP アドレスは、すべての ARP リクエスト / 応答でチェックされます。ターゲット IP アドレスは、ARP 応答でのみチェックされます。

[適用] ボタンをクリックして、変更を反映します。

[ARP 検査 VLAN ログ収集] 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 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。範囲は 1 ～ 4094 です。
状態	指定した VLAN の ARP 検査 VLAN ログ収集を有効または無効にします。

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

[ARP 検査フィルタ] 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
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。名前は 32 文字までです。
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。範囲は 1 ～ 4094 です。
スタティック ACL	スタティック ACL を使用するかどうかを **[はい]** または **[No]** で選択します。

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

8.7.1.2.3 ARP 検査ポート設定

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

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

図 8-49 ARP 検査ポート設定

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	使用するポートを選択します。
帯域制限	帯域制限値を入力します。範囲は、1 秒あたり 1 ～ 150 パケットです。
バースト間隔	バースト間隔値を入力します。範囲は 1 ～ 15 です。**[なし]** オプションをオンにした場合、オプションを無効にします。
信頼状態	信頼状態を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。
[デフォルト設定] ボタンをクリックして、信頼状態をデフォルト設定に設定します。

8.7.1.2.4 ARP 検査統計情報

このウィンドウを用いて、ダイナミック ARP 検査統計情報を表示およびクリアします。

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

図 8-50 ARP 検査統計情報

以下のパラメータを設定できます。

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。範囲は 1 ～ 4094 です。

[VLAN 単位クリア] ボタンをクリックして、指定した VLAN に関する統計情報をクリアします。
[全クリア] ボタンをクリックして、すべての統計情報をクリアします。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

8.7.1.2.5 ARP 検査ログ

このウィンドウを用いて、ダイナミック ARP 検査ログ情報を表示およびクリアします。また、このウィンドウでログバッファ値も設定できます。

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

図 8-51 ARP 検査ログ

[ARP 検査ログ] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ログバッファ	ログバッファのサイズを入力します。範囲は 1 ～ 1024 です。デフォルトでは、この値は 32 です。**[デフォルト]** オプションを選択した場合、デフォルト値を使用します。

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

8.7.1.3 IP ソースガード

8.7.1.3.1 IP ソースガードポート設定

このウィンドウを用いて、指定したポートの IP ソースガードの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [IP ソースガード] > [IP ソースガードポート設定] をクリックして、以下のウィンドウを表示します。

図 8-52 IP ソースガードポート設定

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	使用するポートを選択します。
状態	指定したポートの IP ソースガード状態を有効または無効にします。
検証	使用する検証方法を選択します。選択する値は以下のとおりです。 • **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] ボタンをクリックして、新しいエントリを追加します。

8.7.1.3.2 IP ソースガードバインディング

このウィンドウを用いて、IP ソースガードバインディングの設定を行い、設定値を表示します。

[セキュリティ] > [SAVI] > [IPv4] > [IP ソースガード] > [IP ソースガードバインディング] をクリックして、以下のウィンドウを表示します。

図 8-53 IP ソースガードバインディング

[IP ソースバインディング設定] 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
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。範囲は 1 ～ 4094 です。
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。
開始ポート - 終了ポート	使用するポートを選択します。

[適用] ボタンをクリックして、変更を反映します。

[IP ソースバインディングエントリ] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。範囲は 1 ～ 4094 です。
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。選択する値は以下のとおりです。 • **全** - すべての DHCP バインディングエントリを表示します。 • **DHCP スヌーピング** - 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。 • **スタティック** - 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] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[削除] ボタンをクリックして、指定したエントリを削除します。
複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。

8.7.1.3.3 IP ソースガード HW エントリ

このウィンドウを用いて、指定したポートの IP ソースガードハードウェアエントリを表示します。

[セキュリティ] > [SAVI] > [IPv4] > [IP ソースガード] > [IP ソースガード HW エントリ] をクリックして、以下のウィンドウを表示します。

図 8-54 IP ソースガード HW エントリ

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	使用するポートを選択します。

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

8.8 DHCP サーバプロテクト

8.8.1 DHCP サーバプロテクトグローバル設定

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

[セキュリティ] > [DHCP サーバプロテクト] > [DHCP サーバプロテクトグローバル設定] をクリックして、以下のウィンドウを表示します。

図 8-55 DHCP サーバプロテクトグローバル設定

[プロファイル設定] 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
プロファイル名	DHCP サーバプロテクトプロファイル名を入力します。名前は 32 文字までです。
クライアント MAC	使用する MAC アドレスを入力します。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したプロファイルから MAC アドレスを削除します。
[プロファイル削除] ボタンをクリックして、プロファイルを削除します。

[ログ情報] 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
ログバッファエントリ	ログに記録するエントリ数を入力します。範囲は 10 ～ 1024 です。デフォルトでは、この値は 32 です。

8.8.2 DHCP サーバプロテクトポート設定

このウィンドウを用いて、指定したポートの DHCP サーバプロテクトの設定を行い、設定値を表示します。

[セキュリティ] > [DHCP サーバプロテクト] > [DHCP サーバプロテクトポート設定] をクリックして、以下のウィンドウを表示します。

図 8-56 DHCP サーバプロテクトポート設定

[DHCP サーバプロテクトポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの DHCP サーバプロテクト機能を有効または無効にします。
サーバ IP	DHCP サーバの IP アドレスを入力します。
プロファイル名	指定したポートで使用する DHCP サーバプロテクトプロファイルを入力します。

[適用] ボタンをクリックして、変更を反映します。
[削除] ボタンをクリックして、指定したポートからサーバ IP アドレスとプロファイル名を削除します。

8.9 BPDU ガード

このウィンドウを用いて、指定したポートの BPDU ガード機能の状態および BPDU ガードの設定を行い、設定値を表示します。

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

図 8-57 BPDU ガード

[BPDU ガード設定] 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
BPDU ガード状態	BPDU ガード機能をグローバルに有効または無効にします。
BPDU ガードトラップ状態	BPDU ガードトラップ状態を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[BPDU ガードポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの BPDU ガードを有効または無効にします。
モード	指定したポートに適用する BPDU ガードモードを選択します。 選択する値は以下のとおりです。 • **廃棄** - ポートでアタックを検出した場合に、受信したすべての BPDU パケットを廃棄します。 • **ブロック** - ポートでアタックを検出した場合に、（BPDU および正常なパケットを含む）すべてのパケットを廃棄します。 • **シャットダウン** - ポートでアタックを検出した場合に、ポートをシャットダウンします。

[適用] ボタンをクリックして、変更を反映します。

8.10 NetBIOS フィルタリング

このウィンドウを用いて、指定したポートの NetBIOS フィルタリングの設定を行い、設定値を表示します。

[セキュリティ] > [NetBIOS フィルタリング] をクリックして、以下のウィンドウを表示します。

図 8-58 NetBIOS フィルタリング

[NetBIOS フィルタリング] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
NetBIOS フィルタリング状態	指定したポートの NetBIOS フィルタリング状態を有効または無効にします。これを用いて、物理ポートで NetBIOS パケットを許可または拒否します。
広域 NetBIOS フィルタリング状態	指定したポートの広域 NetBIOS フィルタリング状態を有効または無効にします。これを用いて、物理ポートで 802.3 フレームを介した NetBIOS パケットを許可または拒否します。

[適用] ボタンをクリックして、変更を反映します。

8.11 MAC 認証

このウィンドウを用いて、MAC 認証の設定を行い、設定値を表示します。

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

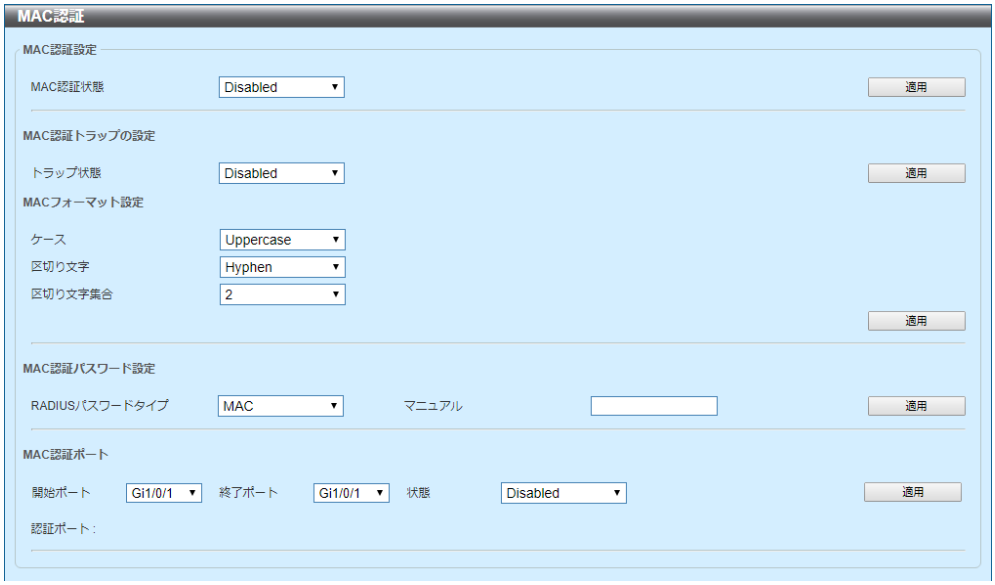


図 8-59 MAC 認証

[MAC 認証設定] 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
MAC 認証状態	MAC 認証機能をグローバルに有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[MAC フォーマット設定] 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
ケース	MAC アドレスで使用する文字の形式を選択します。選択する値は以下のとおりです。 • **大文字** - 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。 • **小文字** - 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。

パラメータ	概要
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。選択する値は以下のとおりです。 • **ハイフン** - 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。 • **コロン** - 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。 • **なし** - 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。選択する値は以下のとおりです。 • **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] ボタンをクリックして、変更を反映します。

[MAC 認証パスワード設定] 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
RADIUS パスワードタイプ	RADIUS パスワードタイプを選択します。選択する値は以下のとおりです。 • **MAC アドレス** - RADIUS パスワードとして MAC アドレスを使用します。 • **マニュアル** - 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] ボタンをクリックして、変更を反映します。

[MAC 認証ポート] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの MAC 認証を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

8.12 Web 認証

8.12.1 Web 認証設定

このウィンドウを用いて、Web 認証の設定を行い、設定値を表示します。

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

図 8-60 Web 認証設定

[グローバル設定] 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
認証状態	Web 認証機能をグローバルに有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[認証ポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの Web 認証機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[**認証設定**] 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
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。範囲は 1 ～ 65535 です。デフォルトでは、この値は 80 です。HTTP は、Hypertext Transfer Protocol の略です。
リダイレクト URL	リダイレクト URL を入力します。これは 64 文字までです。

[**適用**] ボタンをクリックして、変更を反映します。

8.12.2 Web ページコンテンツの設定

このウィンドウを用いて、Web ページコンテンツの設定を行い、設定値を表示します。

[セキュリティ] > [Web 認証] > [Web ページコンテンツの設定] をクリックして、以下のウィンドウを表示します。

図 8-61 Web ページコンテンツの設定

[Web ページコンテンツの設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ロゴデータファイル選択	**[参照]** 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。 これは 64 文字までです。日本語入力が可能です。
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。 これは 32 文字までです。日本語入力が可能です。
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。 これは 32 文字までです。日本語入力が可能です。
メッセージ	カスタムのメッセージを入力します。 これは 256 文字までです。 日本語入力および以下の HTML タグが使用可能です。 以下の <a> <b> <i> <u> <right> <left> <font> <h1> ～ <h5> <p>

パラメータ	概要
説明	カスタムの説明メッセージを入力します。これは 256 文字までです。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] ボタンをクリックして、新しいロゴをアップロードします。
[適用] ボタンをクリックして、変更を反映します。

8.13 信頼されたホスト

このウィンドウを用いて、信頼されたホストのの設定を行い、設定値を表示します。

[セキュリティ] > [信頼されたホスト] をクリックして、以下のウィンドウを表示します。

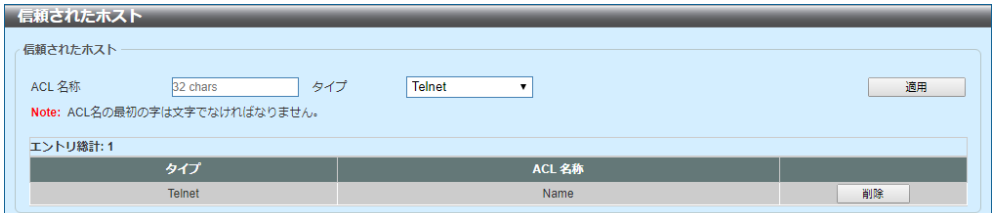


図 8-62 信頼されたホスト

[信頼されたホスト] 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
ACL 名称	ACL の名前を入力します。名前は 32 文字までです。
タイプ	信頼されたホストのタイプを選択します。選択する値は、**[Telnet]**、**[SSH]**、**[Ping]**、**[HTTP]**、および **[HTTPS]**（Hyper Text Transfer Protocol Secure）です。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定したエントリを削除します。

8.14 トラフィックセグメンテーション設定

このウィンドウを用いて、指定したポートのトラフィックセグメンテーションの設定を行い、設定値を表示します。

[セキュリティ] > [トラフィックセグメンテーション設定] をクリックして、以下のウィンドウを表示します。

図 8-63 トラフィックセグメンテーション設定

[トラフィックセグメンテーション設定] 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
開始ポート - 終了ポート	パケットを受信するポートを選択します。
開始フォワードポート - 終了フォワードポート	パケットを転送するポートを選択します。

[追加] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

8.15 ストームコントロール

このウィンドウを用いて、ストームコントロールの設定を行い、設定値を表示します。

[セキュリティ] > [ストームコントロール] をクリックして、以下のウィンドウを表示します。

図 8-64 ストームコントロール（レベルタイプ、PPS)

[ストームコントロールポーリング設定] 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
ポーリング間隔	使用するポーリング間隔値を入力します。範囲は、5 ～ 600 秒です。デフォルトでは、この値は 5 秒です。
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。範囲は 0 ～ 360 です。デフォルトでは、この値は 3 です。**[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] ボタンをクリックして、変更を反映します。

[ストームコントロールポート設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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を選択します。選択する値は **[ブロードキャスト]**、**[マルチキャスト]**、および **[ユニキャスト]** です。**[アクション]** として **[シャットダウン]** 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。選択する値は以下のとおりです。 • **なし** - ストームパケットをフィルタリングしません。 • **シャットダウン** - 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。 • **廃棄** - 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を選択します。選択する値は、**[PPS]** (Packets Per Second)、**[Kbps]**、および **[レベル]** です。
PPS Rise	PPS Rise 値を入力します。このオプションは、1 秒あたりのパケットカウントの上限レートを指定します。範囲は、1 秒あたり 1 ～ 255000 パケットです。[PPS Low] の値を指定しない場合、指定した上昇 PPS の 80% の値がデフォルト値になります。
PPS Low	PPS Low 値を入力します。このオプションは、1 秒あたりのパケットカウントの下限レートを指定します。範囲は、1 秒あたり 1 ～ 255000 パケットです。[PPS Low] の値を指定しない場合、指定した上昇 PPS の 80% の値がデフォルト値になります。

[適用] ボタンをクリックして、変更を反映します。

[レベルタイプ] で **[Kbps]** を選択した場合、以下のウィンドウが表示されます。

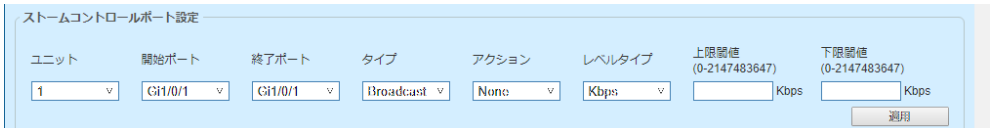


図 8-65 ストームコントロール（レベルタイプ、Kbps)

以下の追加パラメータを設定できます。

パラメータ	概要
KBPS Rise	Kbps Rise 値を入力します。このオプションは、ポートでトラフィックを受信するレート（1 秒あたりのキロビット数）で上昇閾値を指定します。範囲は、1 ～ 2147483647Kbps です。
KBPS Low	Kbps Low 値を入力します。このオプションは、ポートでトラフィックを受信するレート（1 秒あたりのキロビット数）で下限閾値を指定します。範囲は、1 ～ 2147483647Kbps です。[Kbps Low] の値を指定しない場合、指定した上昇 Kbps の 80% の値がデフォルト値になります。

[適用] ボタンをクリックして、変更を反映します。

[レベルタイプ] で [レベル] を選択した場合、以下のウィンドウが表示されます。

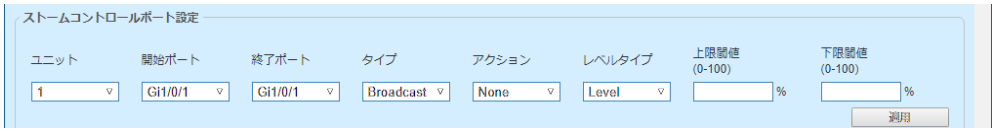


図 8-66 ストームコントロール（レベルタイプ、レベル)

以下の追加パラメータを設定できます。

パラメータ	概要
レベル Rise	レベル Rise 値を入力します。このオプションは、トラフィックを受信するポートあたりの総帯域幅に対するパーセンテージで上昇閾値を指定します。範囲は、1 ～ 100% です。
レベル Low	レベル Low 値を入力します。このオプションは、トラフィックを受信するポートあたりの総帯域幅に対するパーセンテージで下限閾値を指定します。範囲は、1 ～ 100% です。[レベル Low] の値を指定しない場合、指定した上昇レベルの 80% の値がデフォルト値になります。

[適用] ボタンをクリックして、変更を反映します。

8.16 SSH（Secure Shell）

8.16.1 SSH グローバル設定

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

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

図 8-67 SSH グローバル設定

[SSH グローバル設定] 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
IP SSH サーバ状態	SSH サーバをグローバルに有効または無効にします。
IP SSH サービスポート	使用する SSH サービスポート番号を入力します。範囲は 1 ～ 65535 です。デフォルトでは、このナンバーは 22 です。
認証タイムアウト	認証タイムアウト値を入力します。範囲は、30 ～ 600 秒です。デフォルトでは、この値は 120 秒です。
認証リトライ数	認証リトライ回数の値を入力します。範囲は 1 ～ 32 です。デフォルトでは、この値は 3 です。

[適用] ボタンをクリックして、変更を反映します。

8.16.2 ホストキー

このウィンドウを用いて、SSH ホストキーの設定を行い、設定値を表示します。

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

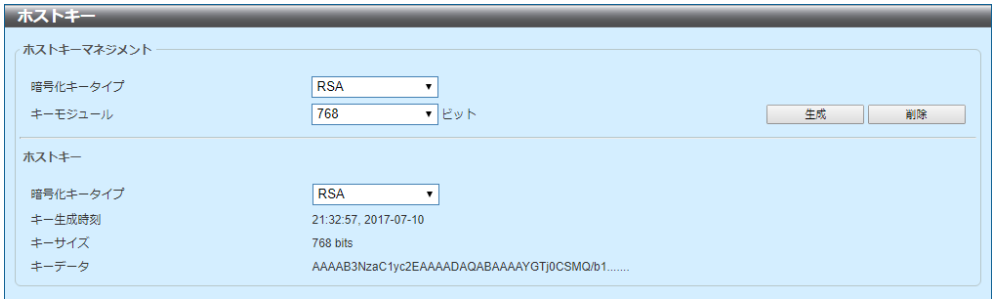


図 8-68 ホストキー

[ホストキーマネジメント] 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
暗号化キータイプ	使用する暗号化キータイプを選択します。選択する値は、**[RSA]**（Rivest Shamir Adleman）キータイプと **[DSA]**（Digital Signature Algorithm）キータイプです。
キーモジュール	キーモジュール値を選択します。選択する値は、**[360]**、**[512]**、**[768]**、**[1024]**、および **[2048]** ビットです。

[生成] ボタンをクリックして、選択内容に基づいてホストキーを生成します。
[削除] ボタンをクリックして、選択内容に基づいてホストキーを削除します。

[ホストキー] 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
暗号化キータイプ	使用する暗号化キータイプを選択します。選択する値は **[RSA]** および **[DSA]** です。

8.16.3 SSH サーバコネクション

このウィンドウを用いて、SSH サーバコネクションテーブルと情報を表示します。

[セキュリティ] > [SSH] > [SSH サーバコネクション] をクリックして、以下のウィンドウを表示します。

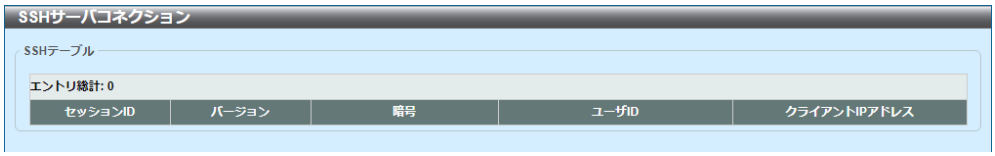


図 8-69 SSH サーバコネクション

8.16.4 SSH ユーザ設定

このウィンドウを用いて、SSH ユーザの設定を行い、設定値を表示します。

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

図 8-70 SSH ユーザ設定

[SSH ユーザ設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ユーザ名	SSH ユーザアカウントのユーザ名を入力します。これは 32 文字までです。
認証方式	SSH 認証方式を選択します。選択する値は **[パスワード]**、**[公開鍵]**、および **[ホストベース]** です。
キーファイル	**[公開鍵]** または **[ホストベース]** を選択した場合に公開鍵を入力します。これは 779 文字までです。
ホスト名	**[ホストベース]** を選択した場合にホスト名を入力します。これは 255 文字までです。
IPv4 アドレス	**[ホストベース]** を選択した場合に 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	**[ホストベース]** を選択した場合に SSH ユーザアカウントの IPv6 アドレスを入力します。

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

8.17 SSL（Secure Sockets Layer）

8.17.1 SSL グローバル設定

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

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

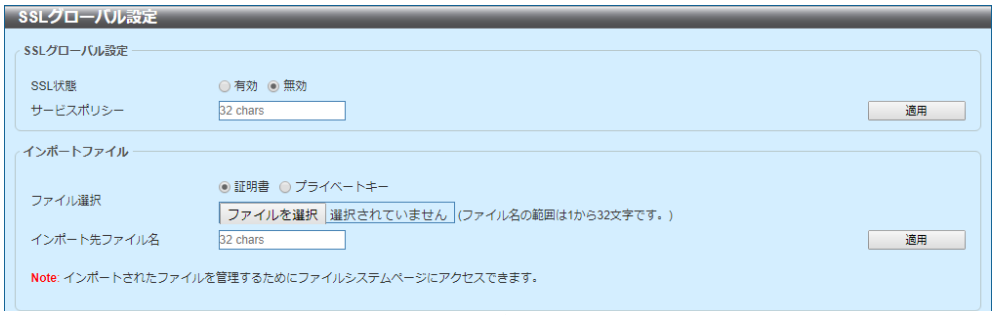


図 8-71 SSL グローバル設定

[SSL グローバル設定] 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
SSL 状態	SSL 機能をグローバルに有効または無効にします。
サービスポリシー	サービスポリシー名を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、変更を反映します。

[インポートファイル] 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
ファイル選択	アップロードするファイルタイプを選択します。選択する値は **[証明書]** および **[プライベートキー]** です。ファイルタイプを選択した後、**[参照]** 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。
ディスティネーションファイル名	使用するディスティネーションファイル名を入力します。名前は 32 文字までです。

[適用] ボタンをクリックして、SSL ファイルをインポートします。

8.17.2 暗号化 PKI トラストポイント

このウィンドウを用いて、SSL 暗号化 PKI（Public Key Infrastructure）トラストポイントの設定を行い、設定値を表示します。

[セキュリティ] > [SSL] > [暗号化 PKI トラストポイント] をクリックして、以下のウィンドウを表示します。

図 8-72 暗号化 PKI トラストポイント

[暗号化 PKI トラストポイント] 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
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。名前は 32 文字までです。
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は、64 文字までの文字列です。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。
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。選択する値は以下のとおりです。 • **両方** - 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。 • **ローカル** - ローカル証明書とキーペアのみをインポートします。

[適用] ボタンをクリックして、新しいエントリを追加します。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[削除] ボタンをクリックして、指定したエントリを削除します。

8.17.3 SSL サービスポリシー

このウィンドウを用いて、SSL サービスポリシーの設定を行い、設定値を表示します。

[セキュリティ] > [SSL] > [SSL サービスポリシー] をクリックして、以下のウィンドウを表示します。

図 8-73 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。名前は 32 文字までです。
バージョン	TLS（Transport Layer Security）のバージョンを選択します。選択する値は、**[TLS 1.0]**、**[TLS 1.1]**、および **[TLS 1.2]** です。
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を入力します。範囲は、60 ～ 86400 秒です。デフォルトでは、この値は 600 秒です。
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。名前は 32 文字までです。
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] ボタンをクリックして、新しいエントリを追加します。
[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。

[**編集**] ボタンをクリックして、指定したエントリの設定を編集します。
[**削除**] ボタンをクリックして、指定したエントリを削除します。

9 OAM（Operations, Administration & Management）

9.1 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。

[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 9-1 ケーブル診断

[ケーブル診断] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

[テスト] ボタンをクリックして、指定したポートでケーブル診断テストを開始します。
[全クリア] ボタンをクリックして、すべてのケーブル診断結果をクリアします。
[クリア] ボタンをクリックして、指定したポートのケーブル診断結果をクリアします。

9.2 DDM（Digital Diagnostic Monitoring）

9.2.1 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 9-2 DDM 設定

[DDM グローバル設定] 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
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の送信を有効または無効にします。
トランシーバモニタリングトラップワーニング	トランシーバモニタリングワーニングトラップの送信を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

[DDM シャットダウン設定] 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
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの DDM 機能を有効または無効にします。
シャットダウン	シャットダウン動作を選択します。選択する値は以下のとおりです。 • **アラーム** - 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。 • **ワーニング** - 設定されているワーニング閾値範囲を超えた場合にポートをシャットダウンします。 • **なし** - 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] ボタンをクリックして、変更を反映します。

9.2.2 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 9-3 DDM 温度閾値設定

[DDM 温度閾値設定] 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
ポート	使用するポートを選択します。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
タイプ	温度閾値のタイプを選択します。選択する値は、**[アラーム下限]**、**[ワーニング下限]**、**[アラーム上限]**、および **[ワーニング上限]** です。
値	閾値を入力します。範囲は、-128 ～ 127.996 ℃です。

[適用] ボタンをクリックして、変更を反映します。

9.2.3 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 9-4 DDM 電圧閾値設定

[DDM 電圧閾値設定] 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
ポート	使用するポートを選択します。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
タイプ	電圧閾値のタイプを選択します。選択する値は、**[アラーム下限]**、**[ワーニング下限]**、**[アラーム上限]**、および **[ワーニング上限]** です。
値	閾値を入力します。範囲は、0 ～ 6.55 ボルトです。

[適用] ボタンをクリックして、変更を反映します。

9.2.4 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。

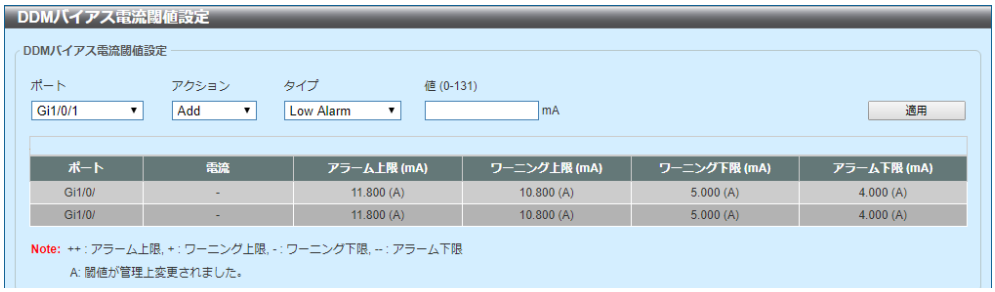


図 9-5 DDM バイアス電流閾値設定

[DDM バイアス電流閾値設定] 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
ポート	使用するポートを選択します。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
タイプ	バイアス電流閾値のタイプを選択します。選択する値は、**[アラーム下限]**、**[ワーニング下限]**、**[アラーム上限]**、および **[ワーニング上限]** です。
値	閾値を入力します。範囲は、0 ～ 131mA です。

[適用] ボタンをクリックして、変更を反映します。

9.2.5 DDM 送信光パワー閾値設定

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

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

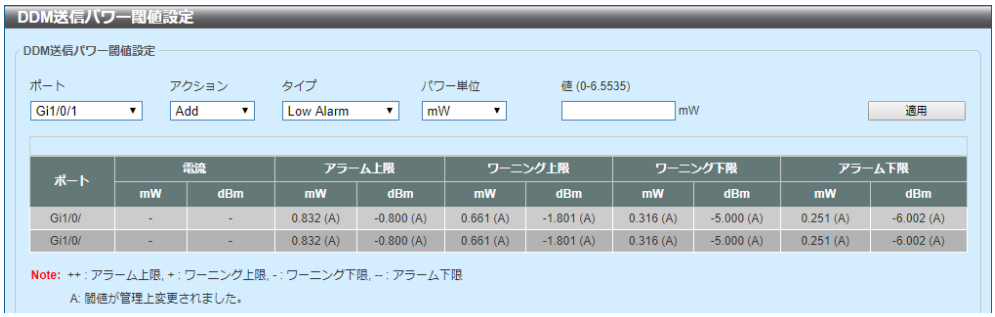


図 9-6 DDM 送信光パワー閾値設定

[DDM 送信光パワー閾値設定] 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
ポート	使用するポートを選択します。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
タイプ	送信パワー閾値のタイプを選択します。選択する値は、**[アラーム下限]**、**[ワーニング下限]**、**[アラーム上限]**、および **[ワーニング上限]** です。
電力単位	電力単位を選択します。選択する値は **[mW]** および **[dBm]** です。
値	閾値を入力します。 • 閾値を **mW** 単位で指定する場合、範囲は 0 ～ 6.5535mW です。 • 閾値を **dBm** 単位で指定する場合、範囲は -40 ～ 8.1647dBm です。

[適用] ボタンをクリックして、変更を反映します。

9.2.6 DDM 受信光パワー閾値設定

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

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

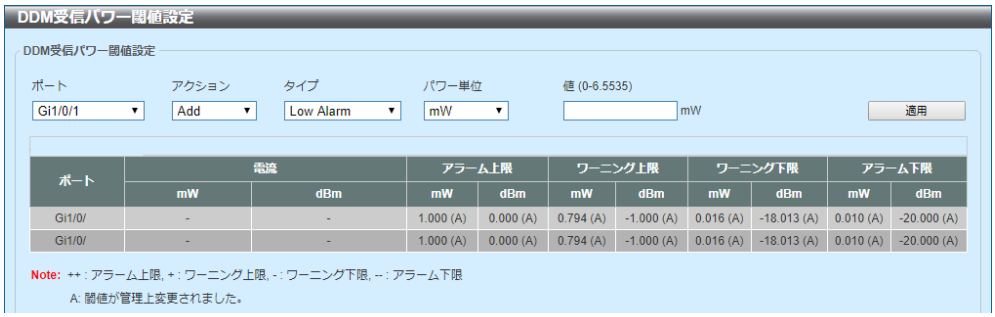


図 9-7 DDM 受信光パワー閾値設定

[DDM 受信光パワー閾値設定] 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
ポート	使用するポートを選択します。
アクション	実行するアクションを選択します。選択する値は **[追加]** および **[削除]** です。
タイプ	受信パワー閾値のタイプを選択します。選択する値は、**[アラーム下限]**、**[ワーニング下限]**、**[アラーム上限]**、および **[ワーニング上限]** です。
電力単位	電力単位を選択します。選択する値は **[mW]** および **[dBm]** です。
値	閾値を入力します。 • 閾値を **mW** 単位で指定する場合、範囲は 0 ～ 6.5535mW です。 • 閾値を **dBm** 単位で指定する場合、範囲は -40 ～ 8.1647dBm です。

[適用] ボタンをクリックして、変更を反映します。

9.2.7 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 9-8 DDM 状態テーブル

9.3 Ethernet OAM

9.3.1 Ethernet OAM 設定

このウィンドウを用いて、イーサネット OAM 設定を表示します。

[OAM]>[イーサネット **OAM**] > をクリックして、以下のウィンドウを表示します。

図 9-9 イーサネット OAM

パラメータ	概要
開始ポート 終了ポート	インターネット OAM 設定の開始 / 終了ポートを表示します。
(インターネット OAM 設定) 状態	インターネット OAM 設定の有効 / 無効を表示します。
モード	インターネット OAM モード Active/Passive を表示します。デフォルトは Active です。
PDU 数 (確認)	1 秒毎に送信される OAM PDUs の最大数を表示します。 (範囲：1 ～ 10) デフォルトは 1 です。
送信間隔	OAM PDUs を送信する送信間隔を秒単位で表示します。(範囲：1 ～ 10 秒) デフォルトは 1 秒です。
リンクタイム アウト	OAM クライアントのタイムアウト値を表示します。(範囲：2 ～ 30 秒) デフォルトは 5 秒です。
しきい値 (高) アクション	上限閾値を超えた時にポートのアクションを表示します。

パラメータ	概要
深刻な障害 アクション	Dying-Gasp 受信時にインターフェースをシャットダウン有無を表示します。
開始ポート 終了ポート	リモートループバックの開始 / 終了ポートを表示します。
(リモートループバック) 状態	リモートループバックの開始 (Support)/ 終了 (No Support) を表示します。
タイムアウト	リモートループバックのタイムアウトを指定します。 (範囲：1 ～ 10 秒）デフォルトは 10 秒です。
開始ポート 終了ポート	リンクモニターの開始ポート / 終了ポートを表示します。
(リンクモニタ) 状態	リンクモニターの開始 (Support)/ 終了 (No Support) を表示します。
フレームエラー しきい値 (高)	エラーフレームの上限閾値を指定します。(範囲：1 ～ 65535)　デフォルトは none です
フレームエラー しきい値 (低)	エラーフレームの下限閾値を表示します。 (範囲：0 ～ 65535)　デフォルトは 10 です。
フレームエラー ウインドウ	エラーフレームをカウントする期間のウィンドウサイズを表示します。 (範囲：10 ～ 600 ミリ秒) 設定値はミリ秒数を 100 倍で表したものになります。デフォルトは 100 ミリ秒です。

[適用] ボタンをクリックして、変更を反映します。

パラメータ	概要
受信フレーム CRC エラーしきい値 (高)	CRC エラーのあるエラーフレームの閾値の上限閾値を表示します。(範囲は 1 ～ 65535）デフォルトは none です。
受信フレーム CRC エラーしきい値 (低)	CRC エラーのあるエラーフレームの閾値の下限閾値を表示します。(範囲：0 ～ 65535）デフォルトは 1 です。
受信フレーム CRC エラーしきい値ウィンドウ	ポーリング期間のウィンドウサイズを表示します。(範囲：10 ～ 1800)　デフォルトは 100 です。

[適用] ボタンをクリックして、変更を反映します。

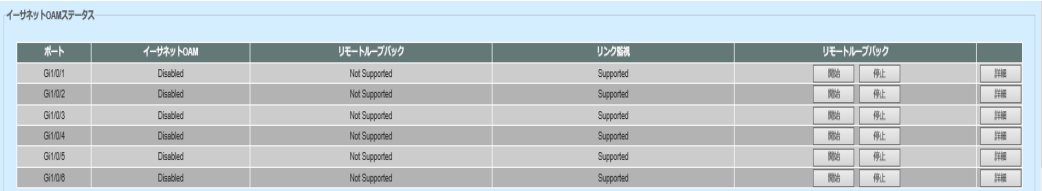


図 9-10 イーサネット OAM ステータス

[**開始**] ボタンをクリックして、リモートループバックを開始します。
[**停止**] ボタンをクリックして、リモートループバックを開始します。
[**詳細**] ボタンをクリックして、Ethernet QAM の設定情報を表示します。

9.3.2 検出情報

このウィンドウを用いて、イーサネット OAM の検出情報を表示します。

[OAM]>[**Ethernet OAM**] > [**検出情報**] をクリックして 、以下のウィンドウを表示します。

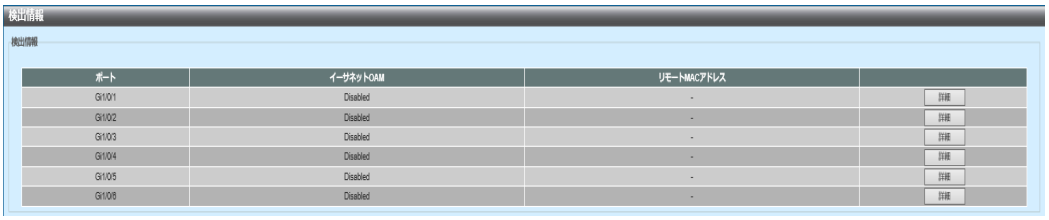


図 9-11 検出情報

パラメータ	概要
ポート	インターネット OAM 設定のポートを表示します。
イーサーネット OAM	インターネット OAM 設定の有効 / 無効を表示します。
リモート MAC アドレス	インターネット OAM 設定のリモート MAC アドレスを表示します。

[詳細] ボタンをクリックして 、当該ポートの検出情報を表示します。

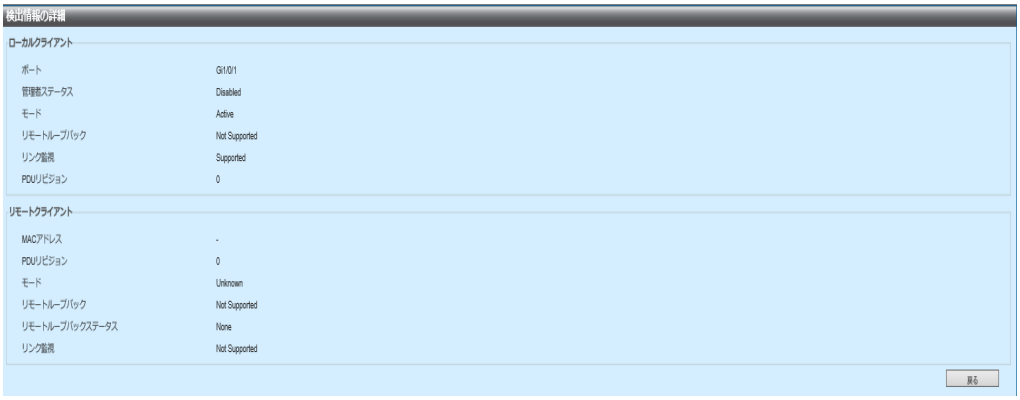


図 9-12 検出情報の詳細

パラメータ	概要
ポート	インターネット OAM 設定のポートを表示します。
管理者ステータス	インターネットOAM設定の有効/無効を表示します。
モード	インターネット OAM モード Active/Passive を表示します。デフォルトは Active です。
リモートループバック	リモートループバックの開始 (Support)/ 終了 (No Support) を表示します。
リモートループバックステータス	リモートループバック状態を表示します。
リンク監視	開始 (Support)/ 終了 (No Support) を表示します。
PDU リビジョン	PDU Revision
MAC アドレス	リモートクライアントの MAC アドレスを表示します。

9.3.3 Ethernet OAM 統計

このウィンドウを用いて、イーサネット OAM の統計を表示します。

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

図 9-13 統計情報

パラメータ	概要
ポート	インターネット OAM 設定のポートを表示します。
OAMPDUTX	OAM PDU の送信数を表示します。
OAMPDURX	OAM PDU の受信数を表示します。
ローカル障害	ローカルクライアントの障害発生数を表示します。
リモート障害	リモートクライアントの障害発生数を表示します。
ローカルイベント	ローカルクライアントのイベント発生数を表示します。
リモートイベント	リモートクライアントのイベント発生数を表示します。

[全クリア] ボタンをクリックして、各ポートの統計をクリアします。
[詳細] ボタンをクリックして、該当ポートの統計情報を表示します。
[クリア] ボタンをクリックして、該当ポートの統計情報を表示します。

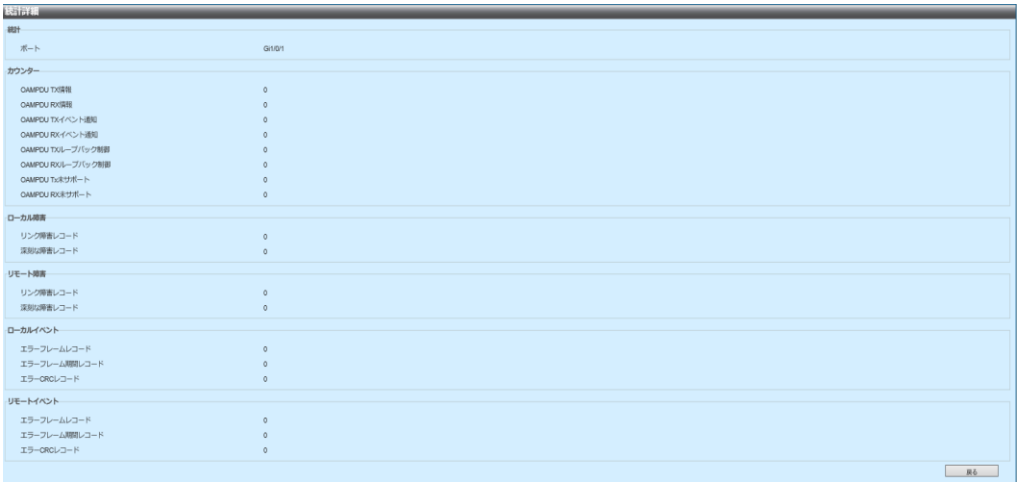


図 9-14 統計情報詳細

パラメータ	概要
ポート	統計情報のポートを表示します。
OAM　PDUTX 情報	Information OAM PDU 送信数を表示します。
OAM　PDURX 情報	Information OAM PDU 受信数を表示します。
OAM　PDUTX イベント通知	Event Notification PDU 送信数を表示します。
OAM　PDURX イベント通知	Event Notification PDU 受信数を表示します。
OAM　PDU TX ループバック制御	Loop back PDU 送信数を表示します。
OAM　PDU RX ループバック制御	Loop back PDU 受信数を表示します。
OAM　PDU TX 未サポート	未サポート PDU の送信数を表示します。
OAM　PDU RX 未サポート	未サポート PDU の受信数を表示します。
リンク障害 レコード	リンク障害発生数を表示します。
深刻な障害 レコード	Dying Gasp 発生数を表示します。
エラーフレームレコード	Error Frame 数を表示します。
エラーフレーム期間レコード	Error Frame 計測間隔を表示します。
フレーム期間レコード	CRC Error フレーム数を表示します。

[戻る] ボタンをクリックして、統計詳細を閉じます。

9.4 CFM (Connectivity Fault Management)

9.4.1 CFM ステータス

このウィンドウを用いて、CFM 機能のグローバル設定を表示します。

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

図 9-15 CFM ステータス設定

パラメータ	概要
CFM ステータス	CFM が有効か無効かを表示します。
メンテナンスドメイン名	ドメイン (maintenance domain) 名を 43 字以内で指定します。
レベル	MD レベルを指定します。 (範囲 : 0 ～ 7)
MA 数	MA (maintenance association) 数を表示します。

[適用]/[作成] ボタンをクリックして、変更を反映します。

9.4.2 CFM メンテナンス中間ポイント

このウィンドウを用いて、CFM maintenance intermediate point (MIP) の定義を表示します。

[CFM] > [CFM メンテナンス中間ポイント] をクリックして、以下のウィンドウを表示します。

図 9-16 CFM メンテナンス中間ポイント

パラメータ	概要
ポート	ポートを表示します。
レベル	MD ドメインレベルを指定します。 (範囲 : 0 ～ 7)
MA サービス名	MA (maintenance association) 名を表示します。(13 文字以内)
VLAN	VLAN ID を表示します。 (範囲 : 1 ～ 4094)

[適用] ボタンをクリックして、変更を反映します。

[DDM シャットダウン設定] 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
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの DDM 機能を有効または無効にします。
シャットダウン	シャットダウン動作を選択します。選択する値は以下のとおりです。 • **アラーム** - 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。 • **ワーニング** - 設定されているワーニング閾値範囲を超えた場合にポートをシャットダウンします。 • **なし** - 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] ボタンをクリックして、変更を反映します。

9.4.3 CFM メンテナンスエンドポイント

このウィンドウを用いて、CFM maintenance end point (MEP) の設定を表示します。

[CFM] > [CFM メンテナンスエンドポイント] をクリックして、以下のウィンドウを表示します。

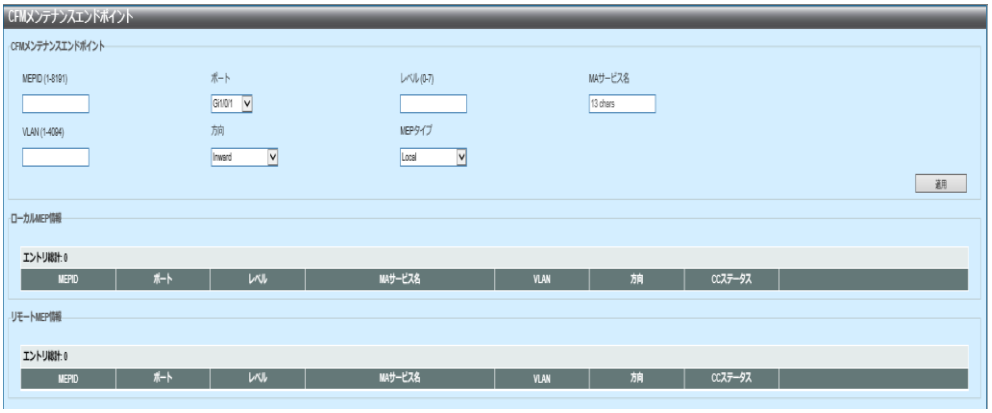


図 9-17 CFM メンテナンスエンドポイント

パラメータ	概要
MEPID	MEP (maintenance end point) ID を表示します。 (範囲 : 1 ～ 8191)
ポート	ポートを表示します。
レベル	MEP レベルを表示します。 (範囲 : 0 ～ 7)
MA サービス	サービス名を表示します。
VLAN	VLAN を表示します。
方向	MEP の入力方向を表示します。 (inward ,outward)
MEP タイプ	MEP type(リモート MEP/Local MEP) を表示します。
CC ステータス	CC (Continuity Check) ステータスを表示します。

[適用] ボタンをクリックして、変更を反映します。

9.4.4 CFM メンテナンスアソシエーション

このウィンドウを用いて、CFM maintenance associate (MA) の定義を表示します。

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

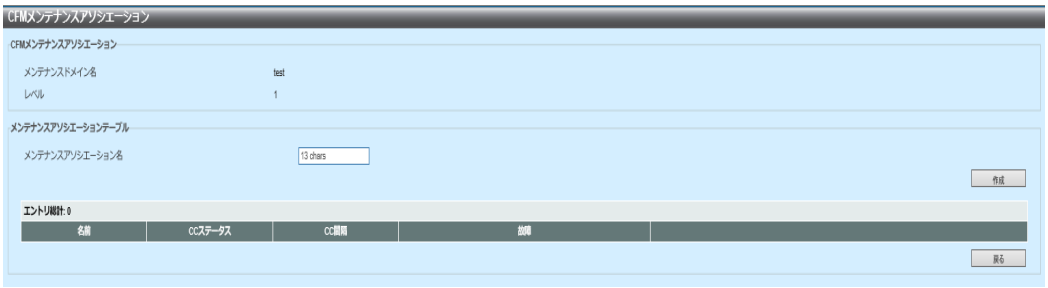


図 9-18 CFM メンテナンスアソシエーション設定

パラメータ	概要
メンテナンス ドメイン名	メンテナンスドメイン名を表示します。
レベル	メンテナンスレベルを表示します。
メンテナンス アソシエーション名	メンテナンスアソシエーション (maintenance associate）名を表示します。(12 文字以内)
CC 間隔	CC (Continuity Check) 間隔を表示します。
故障	故障状態を表示します。

[作成] ボタンをクリックして、変更を反映します。

9.4.5 CFM ループバック

このウィンドウを用いて、CFM ループバックの定義を表示します。

[CFM] > [CFM ループバック] をクリックして、以下のウィンドウを表示します。

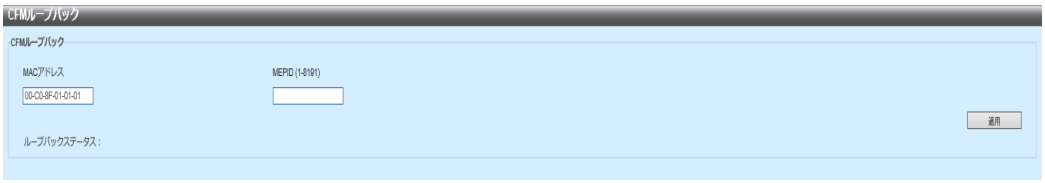


図 9-19 CFM ループバック設定

パラメータ	概要
MAC アドレス	MAC アドレスを表示します。
MEPDID	MEPID を表示します。 (範囲 : 1 ～ 8191)

[適用] ボタンをクリックして、変更を反映します。

9.4.6 CFM リンクトレース

このウィンドウを用いて、CFM リンクトレースの定義を表示します。

[CFM] > [CFM リンクトレース] をクリックして、以下のウィンドウを表示します。

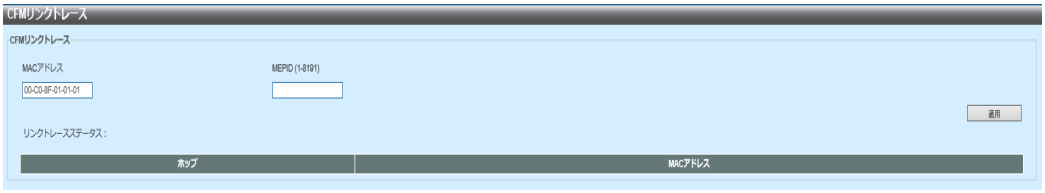


図 9-20 CFM リンクトレース設定

パラメータ	概要
MAC アドレス	MAC アドレスを表示します。
MEPDID	MEPID を表示します。 (範囲 : 1 ～ 8191)
ホップ	ホップする IP アドレスを表示します。

[適用] ボタンをクリックして、変更を反映します。

10 モニタリング

10.1 使用率

10.1.1 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。

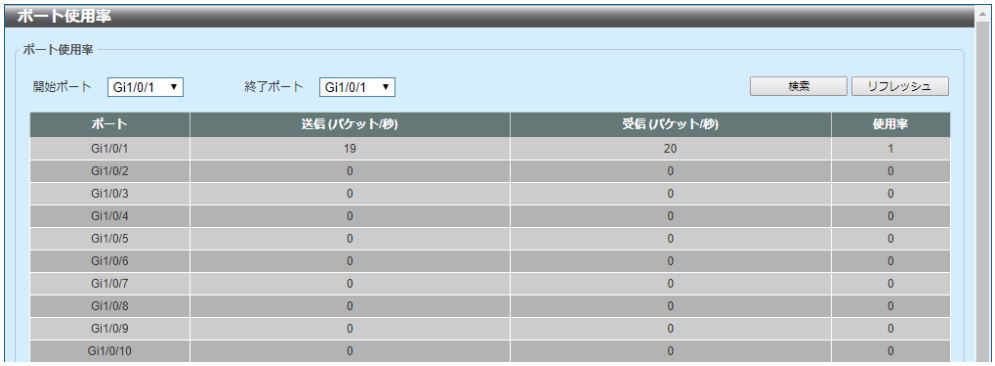


図 10-1 ポート使用率

[ポート使用率] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定したポートに関するポート使用率情報を表示します。
[リフレッシュ] ボタンをクリックして、テーブルに表示されている情報をリフレッシュします。

10.2 統計

10.2.1 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 10-2 ポート

[ポート] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定したポートに関するポート統計情報を表示します。
[リフレッシュ] ボタンをクリックして、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] ボタンをクリックして、このエントリに関する詳細情報を表示します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

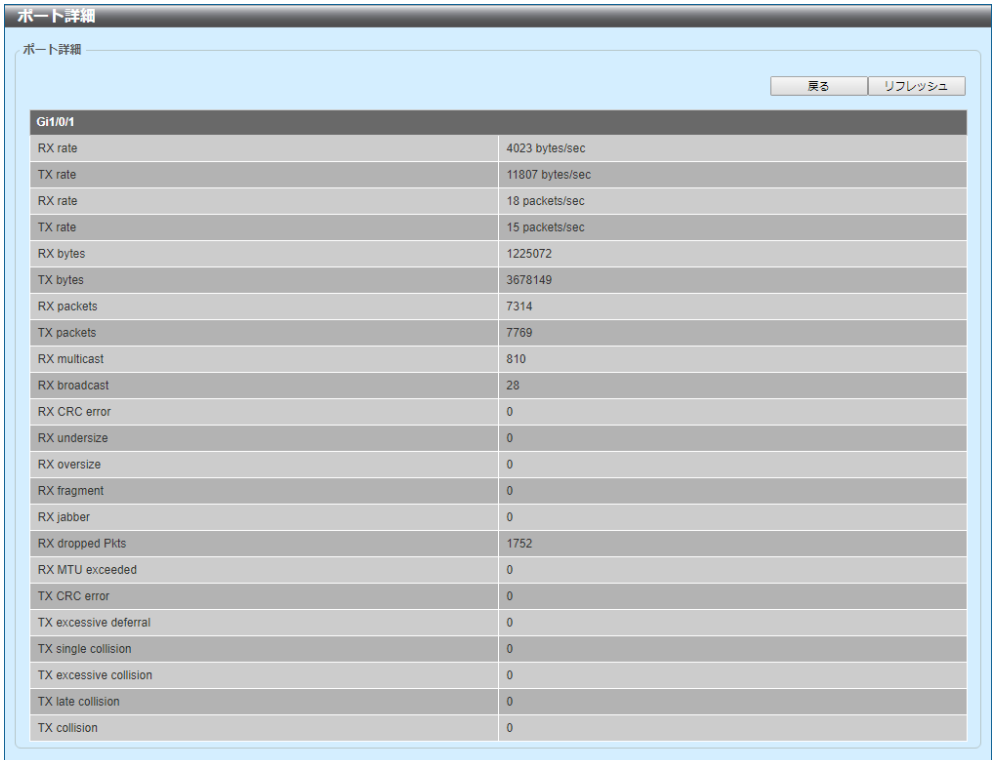


図 10-3 ポート（詳細参照）

[戻る] ボタンをクリックして、前のウィンドウに戻ります。
[リフレッシュ] ボタンをクリックして、テーブルに表示されている情報をリフレッシュします。

10.2.2 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 10-4 インタフェースカウンタ

[インタフェースカウンタ] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定したポートに関するインタフェースカウンタを表示します。
[リフレッシュ] ボタンをクリックして、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] ボタンをクリックして、このエントリに関する詳細エラー情報を表示します。

[エラー参照] ボタンをクリックして、以下のウィンドウを表示します。

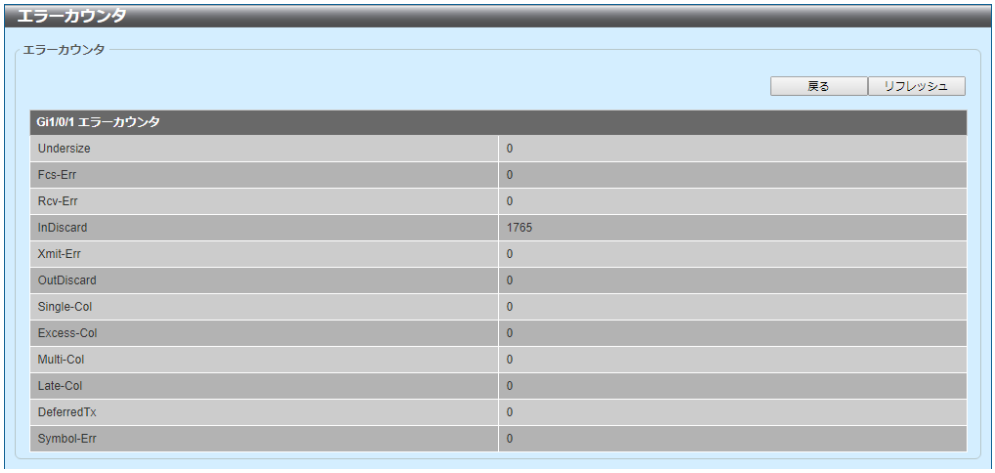


図 10-5 インタフェースカウンタ（エラー参照）

[戻る] ボタンをクリックして、前のウィンドウに戻ります。
[リフレッシュ] ボタンをクリックして、テーブルに表示されている情報をリフレッシュします。

10.2.3 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。

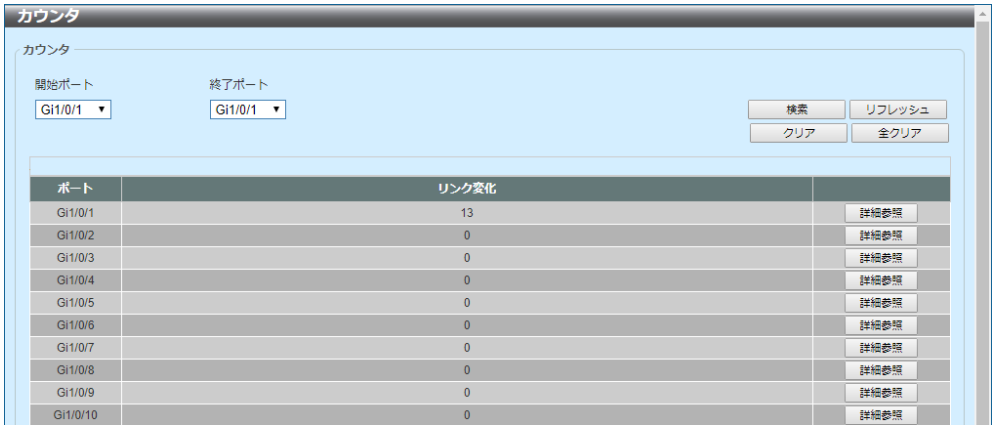


図 10-6 カウンタ

[カウンタ] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。

[検索] ボタンをクリックして、指定したポートに関するリンクチェンジカウンタ情報を表示します。
[リフレッシュ] ボタンをクリックして、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] ボタンをクリックして、指定したポートに関するリンクチェンジカウンタ情報をクリアします。
[全クリア] ボタンをクリックして、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] ボタンをクリックして、このエントリに関する詳細情報を表示します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

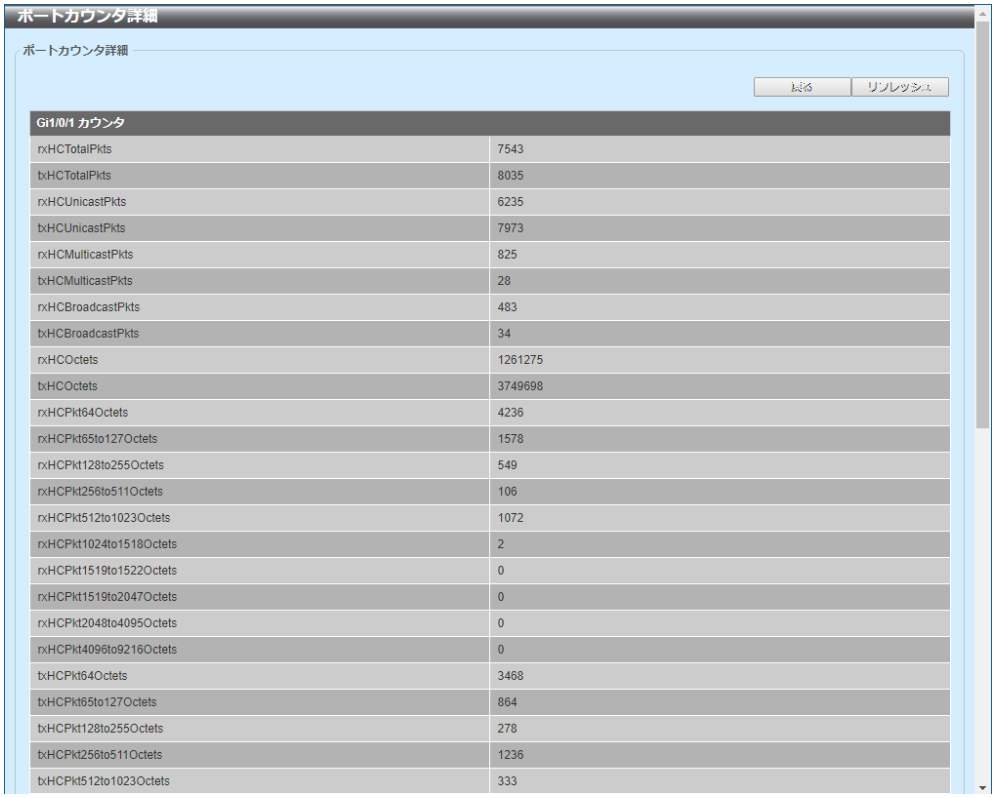


図 10-7 カウンタ（詳細参照）

[戻る] ボタンをクリックして、前のウィンドウに戻ります。
[リフレッシュ] ボタンをクリックして、テーブルに表示されている情報をリフレッシュします。

10.3 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 10-8 ミラー設定

[RSPAN VLAN 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
VID リスト	使用する RSPAN VLAN ID を入力します。カンマ区切りで連続する VLAN ID を入力するか、またはハイフン区切りで VLAN ID の範囲を入力することができます。範囲は 2 ～ 4094 です。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[ミラー設定] 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
セッションナンバー	このエントリのミラーセッションナンバーを選択します。このナンバーの範囲は 1 ～ 4 です。
ディスティネーション	この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。 ディスティネーションの [ポート] または [リモート VLAN] を選択します。 • **ポート** - ディスティネーションポート番号を選択します。 • **リモート VLAN** - ディスティネーションポート番号を選択します。**VID** を表示された入力フィールドに入力します。VID の範囲は 2 ～ 4094 です。
ソース	このポートミラーエントリのソース設定を選択および設定します。 ソースの [ポート]、[ACL]、または [リモート VLAN] を選択します。 • **ポート** -[開始ポート] と [終了ポート] でポート番号の範囲を選択します。[フレームタイプ] を選択します。フレームタイプで選択する値は以下のとおりです。 o**両方** - 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。 o**受信** - 受信方向のみのトラフィックがミラーリングされます。 o**送信** - 送信方向のみのトラフィックがミラーリングされます。 o**CPU RX** - CPU RX トラフィックをモニタリングします。 • **ACL** - **ACL 名称**を表示された入力フィールドに入力します。これは 32 文字までです。 • **リモート VLAN** - リモート VID を表示された入力フィールドに入力します。範囲は 2 ～ 4094 です。

[適用] ボタンをクリックして、新しいエントリを追加します。
[削除] ボタンをクリックして、指定した情報に基づいてエントリを削除します。

[ミラーセッションテーブル] 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
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を選択します。選択する値は、[全セッション]、[セッションナンバー]、[リモートセッション]、および [ローカルセッション] です。[セッションナンバー] オプションを選択した場合、ドロップダウンメニューからセッションナンバーを選択します。範囲は 1 ～ 4 です。

[検索] ボタンをクリックして、指定した検索条件に基づいてエントリを検索し、表示します。
[詳細参照] ボタンをクリックして、このエントリに関する詳細情報を表示します。

[詳細参照] ボタンをクリックして、以下のウィンドウを表示します。

図 10-9 ミラー設定（詳細参照）

[戻る] ボタンをクリックして、前のウィンドウに戻ります。

10.4 デバイス

このウィンドウを用いて、スイッチの現在の温度測定値、ファン状態、および電源モジュール状態を表示します。

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

図 10-10 デバイス

11 ECO モード

11.1 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 11-1 省電力

[省電力設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用する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。選択する値は以下のとおりです。 • **無効** - 省電力機能を無効にします。 • **フル** - 省電力機能の能力を最大限に使用します。 • **ハーフ** - 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] ボタンをクリックして、変更を反映します。

11.2 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。

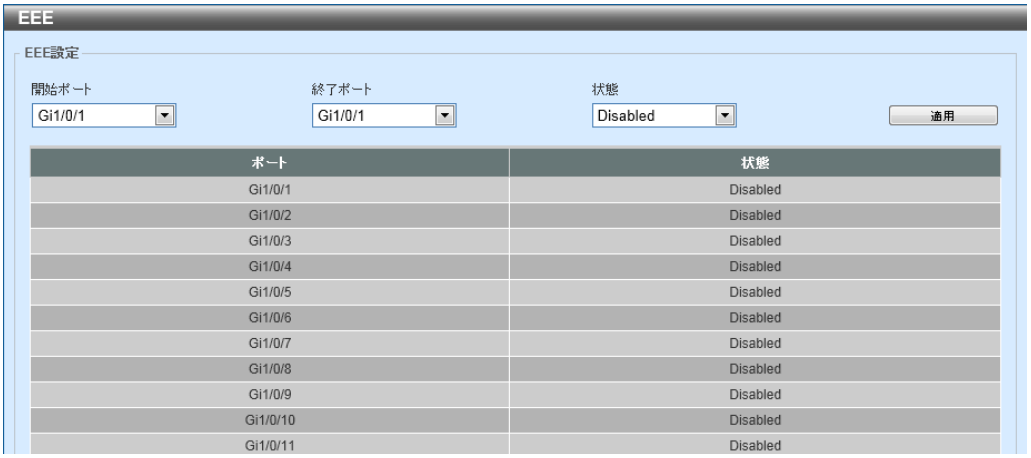


図 11-2 EEE

[EEE 設定] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
開始ポート - 終了ポート	使用するポートを選択します。
状態	指定したポートの EEE 機能を有効または無効にします。

[適用] ボタンをクリックして、変更を反映します。

11.3 LED ベースモード状態

このウィンドウを用いて、LED ベースモード設定を表示します。

[OAM] > [Echo モード] > [LED ベースモード状態] をクリックして、以下のウィンドウを表示します。

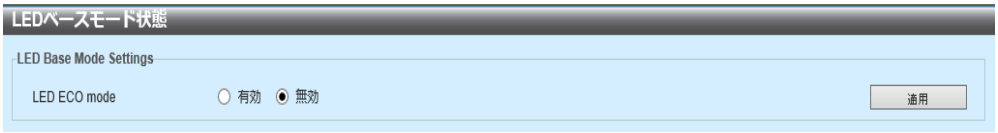


図 11-3 LED ベースモード状態設定

[適用] ボタンをクリックして、変更を反映します。

12 PPS（Power to Progress SDN)

12.1 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。

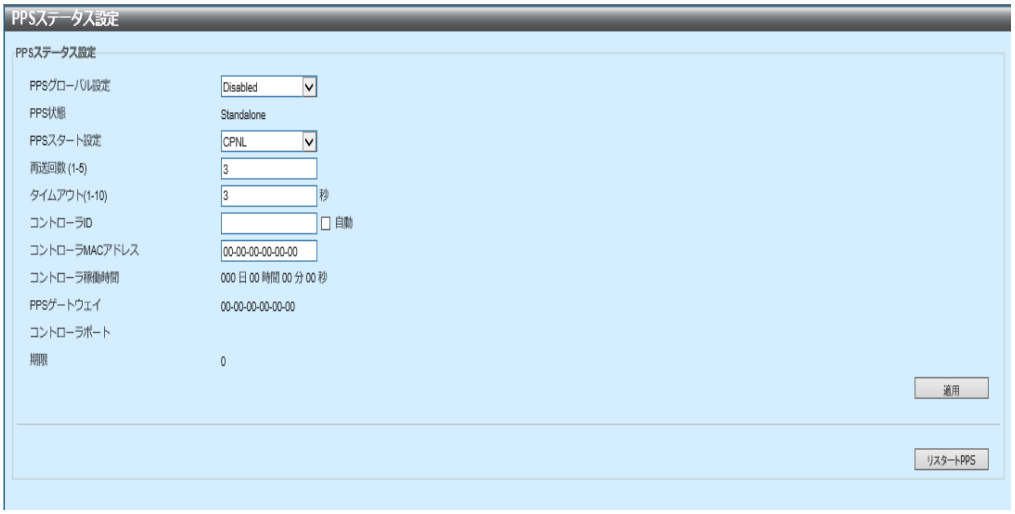


図 12-1 PPS ステータス設定

パラメータ	概要
PPS グローバル設定	PPS 機能を有効または無効に表示します。
PPS 状態	現在の PPS の動作状態を表示します。
PPS スタート設定	PPS スタート状態を表示します。 Standaloneー PPS コントローラに管理されていない状態になります。CPNLー Controller Port Neighbor Lost 状態になり、コントローラを認識しているが、通信不可な状態になります。 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	生存確認を行うパケットの再送回数を表示します (範囲：１～５)

パラメータ	概要
タイムアウト	生存確認のパケットに対する応答のタイムアウト値を表示します。 (範囲：１～１０)
コントローラ ID	PPS コントローラの ID を表示します。
コントローラ MAC アドレス	PPS コントローラの MAC アドレスを表示します。
コントローラ 稼働時間	PPS コントローラの起動からの稼働時間を表示します。
PPS ゲートウェイ	PPS ゲートウェイの MAC アドレスを表示します。
コントローラポート期限	PPS コントローラに対する応答待ち時間を秒単位で指定します。 (範囲：1 ～ 10 秒)

[適用] ボタンをクリックして、変更を反映します。
[リスタート] ボタンをクリックして、PPS をリスタートします。

12.2 PPS 通知設定

このウィンドウを用いて、PPS の通知設定を表示します。

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

図 12-2 PPS 通知設定

パラメータ	概要
システムログ 通知設定	PPS システムログ通知の有効 / 無効を表示します。
カウンターインターバル	PPS パケット統計情報通知間隔を表示します。 (範囲：1 ～ 120 秒)
開始ポート 終了ポート	PPS 通知設定機能に使用するポートを表示します。
カウンタ通知ポート設定	カウンタ通知ポート機能の有効 / 無効を表示します。 設定すると対象のカウンタ通知ポートが表示されます。

[適用] ボタンをクリックして、変更を反映します。

12.3 PPS ポート設定

このウィンドウを用いて、PPS のポート設定を表示します。

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

図 12-3 PPS ポート設定

パラメータ	概要
開始ポート 終了ポート	PPS ポートの開始ポート /PPS ポート検索の終了ポートを表示します。
PPS プライオリティ (管理者プライオリティ)	PPS ポート検索の PPS プライオリティを表示します。 (範囲：０～２５５)
ポート	スイッチのポート番号を表示します。
トランク	トランキングの設定状態をグループ番号を表示します。
リンク	各ポートのリンク状態を Up/Down を表示します。
状態	各ポートの通信状態を表示します。
オペレーション プライオリティ設定	各ポートごとに設定された PPS の通信経路の自動判別のための優先度を表示します。

[適用] ボタンをクリックして、変更を反映します。

12.4 PPS コネクション設定

このウィンドウを用いて、PPS コネクションのエントリーを表示します。

[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。

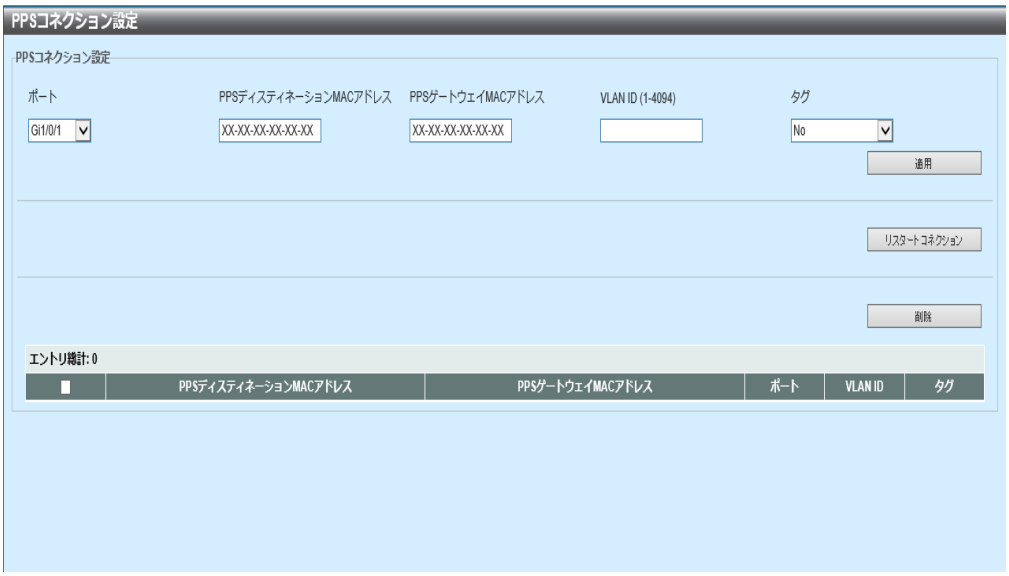


図 12-4 PPS コネクション設定

パラメータ	概要
ポート	PPS コネクションに追加するポートを表示します。
PPS ディスティネーション MAC アドレス	PPS コネクションに追加する 宛先 MAC アドレスを表示します。
PPS ゲートウェイ MAC アドレス	PPS コネクションに追加するゲートウェイ MAC アドレスを表示します。
VLAN-ID	PPS コネクションに追加する VLAN ID を表示します。
タグ	PPS コネクションに追加するタグを表示します。 このタグフィールドは、ゲートウェイへの PPS パケットの送信に使用されます。No 場合、デフォルトではタグなしが使用されます。

[適用] ボタンをクリックして、PPS エントリーに追加します。
[リスタート] ボタンをクリックして、PPS をリスタートします。
[削除] ボタンをクリックして、チェックした PPS エントリーを削除します。

12.5 PPS ネイバー設定

このウィンドウを用いて、PPS Neighbor のエントリを表示します。

[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。

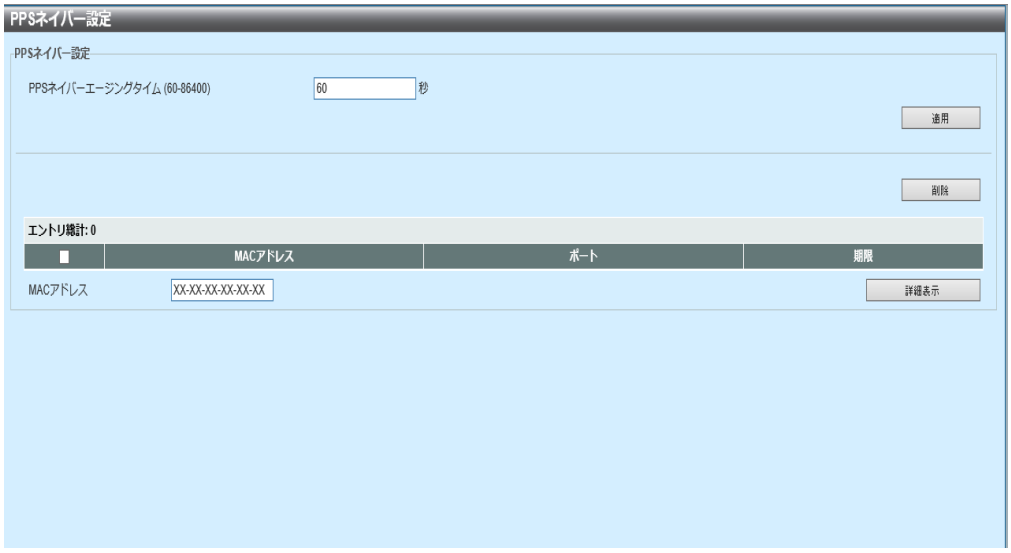


図 12-5 PPS ネイバー設定

パラメータ	概要
PPS ネイバーエージングタイム (期限)	PPS Neighbor のエントリ保有時間を秒単位で表示します。
MAC アドレス	PPS Neighbor のエントリの MAC アドレスを表示します。
ポート	PPS Neighbor のエントリの ポートを表示します。

[適用] ボタンをクリックして、変更を反映します。
[削除] ボタンをクリックして、チェックした PPS エントリーを削除します。
[詳細表示] ボタンをクリックして、PPS エントリー情報詳細を表示します。

13 sFlow

13.1 sFlow

13.1.1 sFlow 設定

このウィンドウを用いて、sFlow コレクタの定義を表示します。

[sFlow] をクリックして、以下のウィンドウを表示します。

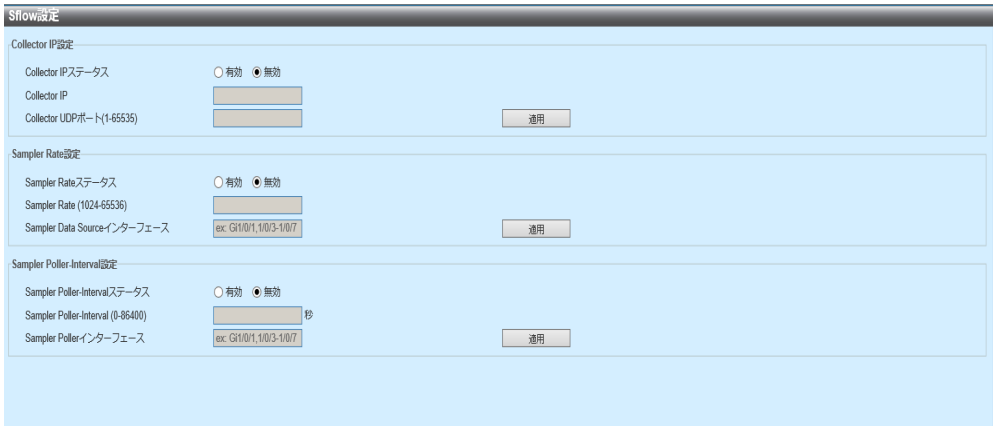


図 13-6 sFlow 設定

パラメータ	概要
Collector IP ステータス	sFlow コレクタとして使用するホストの IPv4 アドレスが有効か無効かを表示します。
Collector IP	sFlow コレクタとして使用するホストの IPv4 アドレスを表示します。
Collector UDP ポート	sFlow メッセージのポート番号を表示します。 指定しない場合、ポート番号は 6343 にデフォルト設定されます。 (範囲 :1 ～ 65535)
Sampler Rate ステータス	Sampler Rate 設定が有効か無効かを表示します。
Sampler Rate	sFlow Sampler Rate 何フレームごとにサンプリングするかを表示します。 sFlow Sampler Rate は 1/rate で計算されます。 (範囲 : 1024 ～ 65536)

パラメータ	概要
Sampler Data Source インターフェース	有効にする sFlow Sampler Data Source ポートが表示します。有効なインターフェースは物理インターフェースです。
Sampler -Poller interval ステータス	Sampler-Poller interval 設定が有効か無効かを表示します。
Sampler -Poller interval	Sampler-Poller interval(秒）を表示します。 （範囲：0 ～ 86400） 0 に設定されている場合は sFlow カウンターサンプルは送信されません。
Sampler -Poller インターフェース	sFlow カウンターサンプリングを有効にするインターフェースを指定します。有効なインターフェースは物理インターフェースです。

[適用] ボタンをクリックして、変更を反映します。

14 ツールバー

14.1 保存

14.1.1 コンフィグ保存

このウィンドウを用いて、実行中のコンフィグレーションをスタートアップコンフィグレーションとして保存します。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。

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

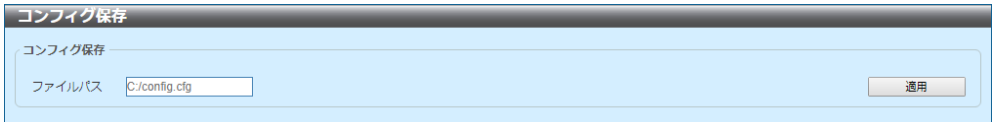


図 14-1 コンフィグ保存

[コンフィグ保存] 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
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] ボタンをクリックして、コンフィグレーションを保存します。

14.2 ツール

14.2.1 ファームウェアアップグレード & バックアップ

14.2.1.1 HTTP サーバからファームウェアアップグレード

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

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [HTTP サーバからファームウェアアップグレード]** をクリックして、以下のウィンドウを表示します。

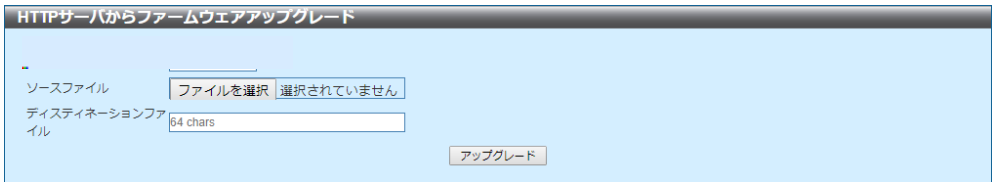


図 14-2 HTTP サーバからファームウェアアップグレード

以下のパラメータを設定できます。

パラメータ	概要
ソースファイル	**[参照]** 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。このフィールドは 64 文字までです。

[アップグレード] ボタンをクリックして、アップグレードを開始します。

14.2.1.2 TFTP サーバからファームウェアアップグレード

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

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [TFTP サーバからファームウェアアップグレード]** をクリックして、以下のウィンドウを表示します。

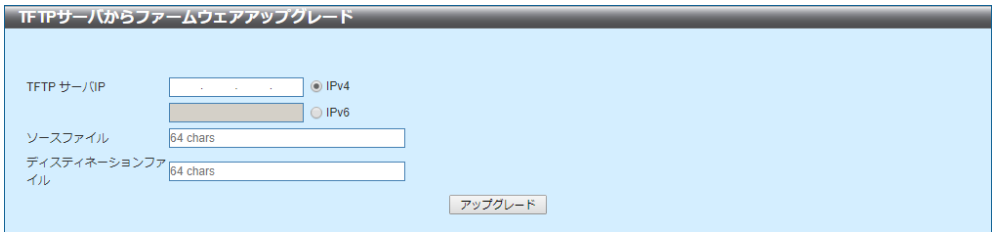


図 14-3 TFTP サーバからファームウェアアップグレード

以下のパラメータを設定できます。

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。このフィールドは 64 文字までです。
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。このフィールドは 64 文字までです。

[アップグレード] ボタンをクリックして、アップグレードを開始します。

14.2.1.3 FTP サーバからファームウェアアップグレード

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

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [FTP サーバからファームウェアアップグレード]** をクリックして、以下のウィンドウを表示します。

図 14-4 FTP サーバからファームウェアアップグレード

以下のパラメータを設定できます。

パラメータ	概要
FTP サーバ IP	FTP サーバの IP アドレスを入力します。
TCP ポート (1-65535)	FTP 接続の TCP ポートを入力します。
ユーザ名	FTP 接続のユーザ名を入力します。名前は 32 文字までです。
パスワード	FTP 接続のパスワードを入力します。名前は 15 文字までです。
ソースファイル	FTP サーバにあるファームウェアファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
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。このフィールドは 64 文字までです。

[アップグレード] ボタンをクリックして、アップグレードを開始します。

14.2.1.4 RCP サーバからファームウェアアップグレード

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

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [RCP サーバからファームウェアアップグレード]** をクリックして、以下のウィンドウを表示します。

図 14-5 RCP サーバからファームウェアアップグレード

以下のパラメータを設定できます。

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。名前は 32 文字までです。
ソースファイル	RCP サーバにあるファームウェアファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
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。このフィールドは 64 文字までです。

[アップグレード] ボタンをクリックして、アップグレードを開始します。

14.2.1.5 HTTP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを HTTP を使用してローカル PC に保存します。

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [HTTP サーバへファームウェアバックアップ]** をクリックして、以下のウィンドウを表示します。

図 14-6 HTTP サーバへファームウェアバックアップ

以下のパラメータを設定できます。

パラメータ	概要
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.1.6 TFTP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを TFTP サーバに保存します。

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [TFTP サーバへファームウェアバックアップ]** をクリックして、以下のウィンドウを表示します。

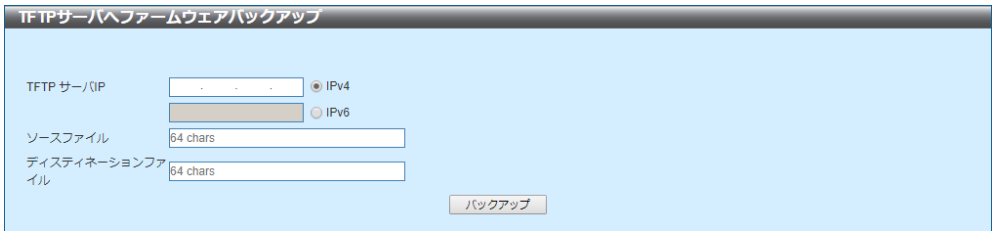


図 14-7 TFTP サーバへファームウェアバックアップ

以下のパラメータを設定できます。

パラメータ	概要
TFTP サーバ IP	TFTP サーバの IP アドレスを入力します。 • **IPv4** - TFTP サーバの IPv4 アドレスを選択および入力します。 • **IPv6** - TFTP サーバの IPv6 アドレスを選択および入力します。
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
ディスティネーションファイル	TFTP サーバにバックアップするファームウェアファイルのディスティネーションファイル名とパスを入力します。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.1.7 FTP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを RCP サーバに保存します。

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [FTP サーバへファームウェアバックアップ]** をクリックして、以下のウィンドウを表示します。

図 14-8 FTP サーバへファームウェアバックアップ

以下のパラメータを設定できます。

パラメータ	概要
FTP サーバ IP	FTP サーバの IP アドレスを入力します。
TCP ポート (1-65535)	FTP 接続の TCP ポートを入力します。
ユーザ名	FTP 接続のユーザ名を入力します。名前は 32 文字までです。
パスワード	FTP 接続のパスワードを入力します。名前は 15 文字までです。
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
ディスティネーションファイル	FTP サーバにバックアップするファームウェアファイルのディスティネーションファイル名とパスを入力します。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.1.8 RCP サーバへファームウェアバックアップ

このウィンドウを用いて、スイッチのファームウェアのバックアップコピーを RCP サーバに保存します。

ツールバーで **[ツール] > [ファームウェアアップグレード & バックアップ] > [RCP サーバへファームウェアバックアップ]** をクリックして、以下のウィンドウを表示します。

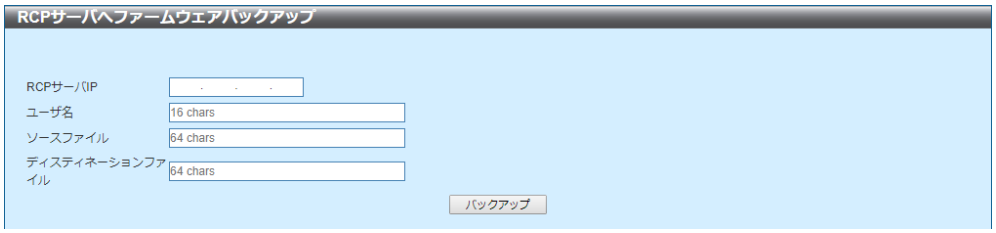


図 14-9 RCP サーバへファームウェアバックアップ

以下のパラメータを設定できます。

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。名前は 32 文字までです。
ソースファイル	スイッチにあるファームウェアファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
ディスティネーションファイル	RCP サーバにバックアップするファームウェアファイルのディスティネーションファイル名とパスを入力します。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.2 コンフィグレーション復旧&バックアップ

14.2.2.1 HTTP サーバからコンフィグレーション復旧

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

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

図 14-10 HTTP サーバからコンフィグレーション復旧

以下のパラメータを設定できます。

パラメータ	概要
ソースファイル	**[参照]** 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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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] ボタンをクリックして、リストアを開始します。

14.2.2.2 TFTP サーバからコンフィグレーション復旧

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

ツールバーで **[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 14-11 TFTP サーバからコンフィグレーション復旧

以下のパラメータを設定できます。

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。このフィールドは 64 文字までです。
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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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] ボタンをクリックして、リストアを開始します。

14.2.2.3 FTP サーバからコンフィグレーション復旧

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

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

図 14-12 FTP サーバからコンフィグレーション復旧

以下のパラメータを設定できます。

パラメータ	概要
FTP サーバ IP	FTP サーバの IP アドレスを入力します。
TCP ポート (1-65535)	FTP 接続の TCP ポートを入力します。
ユーザ名	FTP 接続のユーザ名を入力します。名前は 32 文字までです。
パスワード	FTP 接続のパスワードを入力します。名前は 15 文字までです。
ソースファイル	FTP サーバにあるコンフィグレーションファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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] ボタンをクリックして、リストアを開始します。

14.2.2.4 RCP サーバからコンフィグレーション復旧

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

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

図 14-13 RCP サーバからコンフィグレーション復旧

以下のパラメータを設定できます。

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。名前は 32 文字までです。
ソースファイル	RCP サーバにあるコンフィグレーションファイルのソースファイル名とパスを入力します。このフィールドは 64 文字までです。
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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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] ボタンをクリックして、リストアを開始します。

14.2.2.5 HTTP サーバへコンフィグレーションをバックアップ

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

ツールバーで **[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。

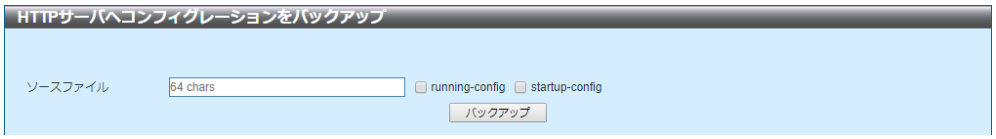


図 14-14 HTTP サーバへコンフィグレーションをバックアップ

以下のパラメータを設定できます。

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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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]** オプションを選択した場合、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] ボタンをクリックして、バックアップを開始します。

14.2.2.6 TFTP サーバへコンフィグレーションをバックアップ

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

ツールバーで **[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。

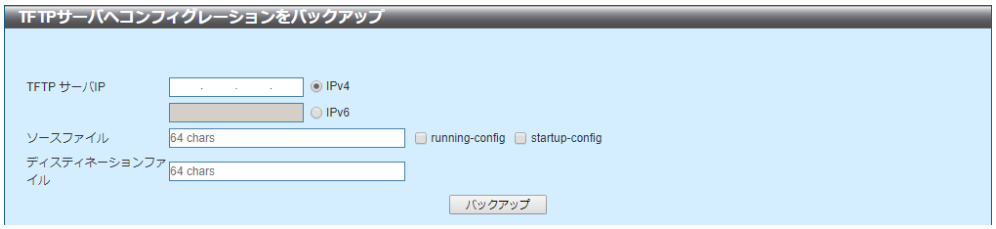


図 14-15 TFTP サーバへコンフィグレーションをバックアップ

以下のパラメータを設定できます。

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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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]** オプションを選択した場合、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。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.2.7 FTP サーバへコンフィグレーションをバックアップ

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

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

図 14-16 FTP サーバへコンフィグレーションをバックアップ

以下のパラメータを設定できます。

パラメータ	概要
FTP サーバ IP	FTP サーバの IP アドレスを入力します。
TCP ポート (1-65535)	FTP 接続の TCP ポートを入力します。
ユーザ名	FTP 接続のユーザ名を入力します。名前は 32 文字までです。
パスワード	FTP 接続のパスワードを入力します。名前は 15 文字までです。
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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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]** オプションを選択した場合、スイッチからスタートアップコンフィグレーションファイルをバックアップします。
ディスティネーションファイル	コンフィグレーションファイルを保存する RCP サーバ上のディスティネーションパスと場所を入力します。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.2.8 RCP サーバへコンフィグレーションをバックアップ

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

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

図 14-17 RCP サーバへコンフィグレーションをバックアップ

以下のパラメータを設定できます。

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。名前は 32 文字までです。
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。このフィールドは 64 文字までです。 • **[running-config]** オプションを選択した場合、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]** オプションを選択した場合、スイッチからスタートアップコンフィグレーションファイルをバックアップします。
ディスティネーションファイル	コンフィグレーションファイルを保存する RCP サーバ上のディスティネーションパスと場所を入力します。このフィールドは 64 文字までです。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.3 ログバックアップ

14.2.3.1 ログを HTTP サーバへバックアップ

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

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

図 14-18 ログを HTTP サーバへバックアップ

以下のパラメータを設定できます。

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] ボタンをクリックして、バックアップを開始します。

14.2.3.2 ログを TFTP サーバへバックアップ

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

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

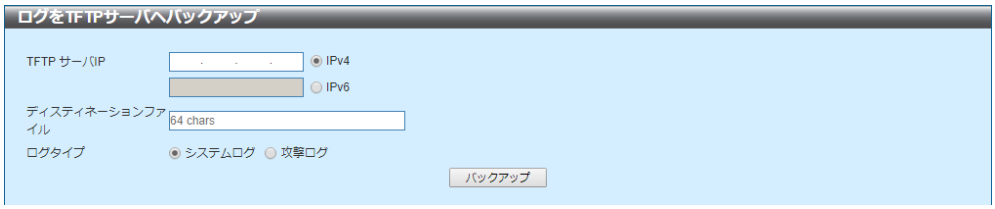


図 14-19 ログを TFTP サーバへバックアップ

以下のパラメータを設定できます。

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。このフィールドは 64 文字までです。
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] ボタンをクリックして、バックアップを開始します。

14.2.3.3 ログを RCP サーバへバックアップ

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

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

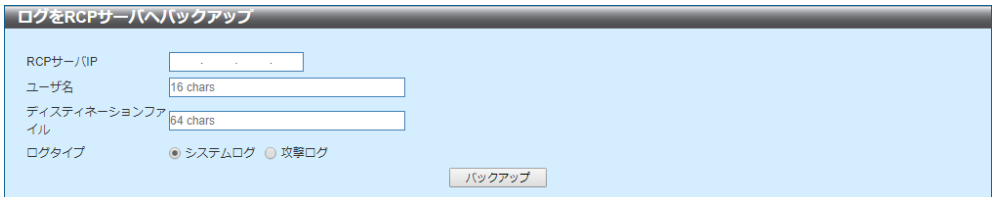


図 14-20 ログを RCP サーバへバックアップ

以下のパラメータを設定できます。

パラメータ	概要
RCP サーバ IP	RCP サーバの IP アドレスを入力します。
ユーザ名	RCP 接続のユーザ名を入力します。名前は 32 文字までです。
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 RCP サーバ上のディスティネーションパスと場所を入力します。このフィールドは 64 文字までです。
ログタイプ	RCP サーバにバックアップするログタイプを選択します。 • **システムログ** - システムログをバックアップします。 • **攻撃ログ** - 攻撃ログをバックアップします。

[バックアップ] ボタンをクリックして、バックアップを開始します。

14.2.4 Ping

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

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

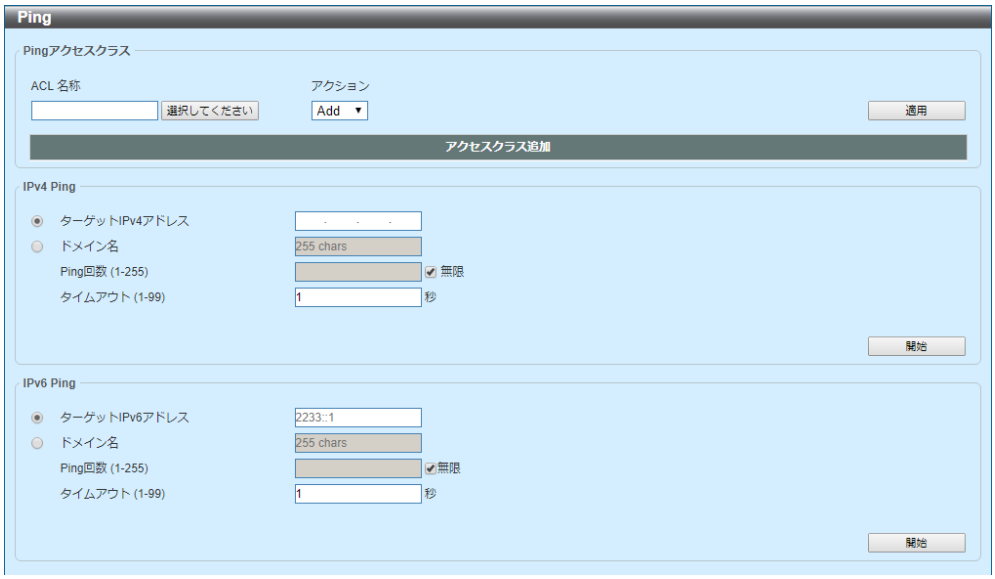


図 14-21 Ping

[Ping アクセスクラス] 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
ACL 名称	使用する ACL の名前を入力します。名前は 32 文字までです。**[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を選択します。選択する値は **[追加]** および **[クリア]** です。

[適用] ボタンをクリックして、選択したアクセスコントロールリストを使用します。

[IPv4 Ping] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ターゲット IPv4 アドレス	ディスティネーション IPv4 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。これは 255 文字までです。
Ping 回数	このウィンドウで設定した IPv4 アドレスに Ping を試行する回数を入力します。範囲は 1 ～ 255 です。 **[無限]** チェックボックスをオンにした場合、プログラムを停止するまで、指定した IPv4 アドレスに ICMP Echo パケットを送信し続けます。
タイムアウト	Ping メッセージのタイムアウト時間を入力します。パケットがここで指定した時間内に IPv4 アドレスを検出できない場合、Ping パケットは廃棄されます。範囲は、1 ～ 99 秒です。
ソース IPv4 アドレス	ソース IPv4 アドレスを入力します。スイッチに複数の IPv4 アドレスが割り当てられている場合は、そのうちの 1 つを入力できます。入力した IPv4 アドレスは、リモートホストに送信されるパケットのソース IPv4 アドレスとして使用されます。

[開始] ボタンをクリックして、IPv4 Ping を開始します。

[IPv6 Ping] セクションでは、以下のパラメータを設定できます。

パラメータ	概要
ターゲット IPv6 アドレス	ディスティネーション IPv6 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。これは 255 文字までです。
Ping 回数	このウィンドウで設定した IPv6 アドレスに Ping を試行する回数を入力します。範囲は 1 ～ 255 です。 **[無限]** チェックボックスをオンにした場合、プログラムを停止するまで、指定した IPv6 アドレスに ICMP Echo パケットを送信し続けます。
タイムアウト	Ping メッセージのタイムアウト時間を入力します。パケットがここで指定した時間内に IPv6 アドレスを検出できない場合、Ping パケットは廃棄されます。範囲は、1 ～ 99 秒です。
ソース IPv6 アドレス	ソース IPv6 アドレスを入力します。スイッチに複数の IPv6 アドレスが割り当てられている場合は、そのうちの 1 つを入力できます。入力した IPv6 アドレスは、リモートホストに送信されるパケットのソース IPv6 アドレスとして使用されます。

[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。

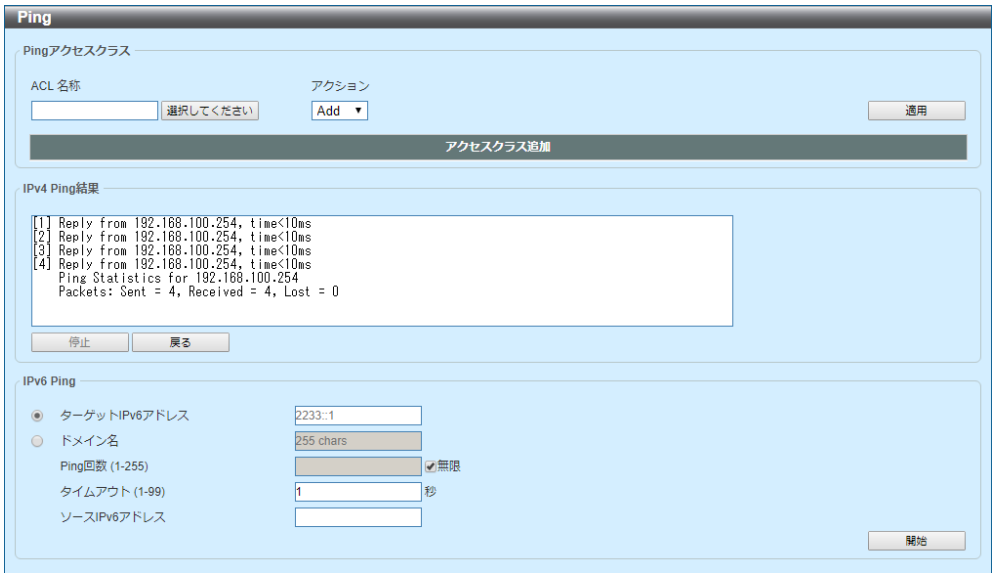


図 14-22 Ping（結果）

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

[選択してください。] ボタンをクリックして、以下のウィンドウを表示します。

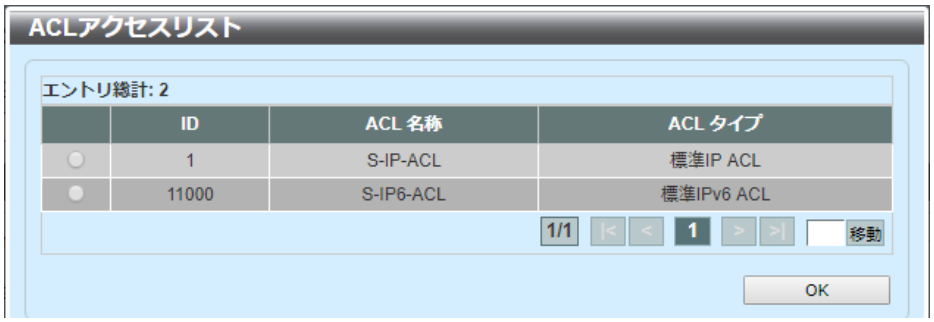


図 14-23 Ping（選択してください。）

複数のページが存在する場合は、ページ番号を入力し、**[Go]** ボタンをクリックして特定のページに移動します。
[OK] ボタンをクリックして、選択したアクセスコントロールリストを使用します。

14.2.5 トレースルート

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

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

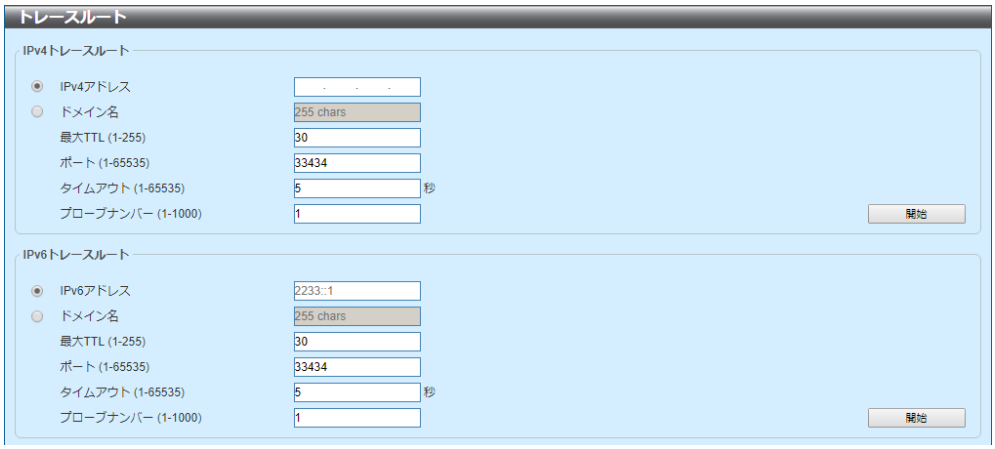


図 14-24 トレースルート

[IPv4 トレースルート] 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
IPv4 アドレス	ディスティネーション IPv4 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。これは 255 文字までです。
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。範囲は、1 ～ 255 ホップです。
ポート	ポート番号を入力します。範囲は 1 ～ 65535 です。
タイムアウト	リモート装置からの応答を待つ際のタイムアウト期間を入力します。範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
プローブナンバー	プローブタイムの数を入力します。範囲は 1 ～ 1000 です。デフォルト値は 1 です。

[開始] ボタンをクリックして、IPv4 トレースルートを開始します。

[IPv6 トレースルート] 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
IPv6 アドレス	ディスティネーション IPv6 アドレスを選択および入力します。
ドメイン名	ディスティネーションドメイン名を選択および入力します。これは 255 文字までです。
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。範囲は、1 ～ 255 ホップです。
ポート	ポート番号を入力します。範囲は 1 ～ 65535 です。
タイムアウト	リモート装置からの応答を待つ際のタイムアウト期間を入力します。範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
プローブナンバー	プローブタイムの数を入力します。範囲は 1 ～ 1000 です。デフォルト値は 1 です。

[開始] ボタンをクリックして、IPv6 トレースルートを開始します。

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

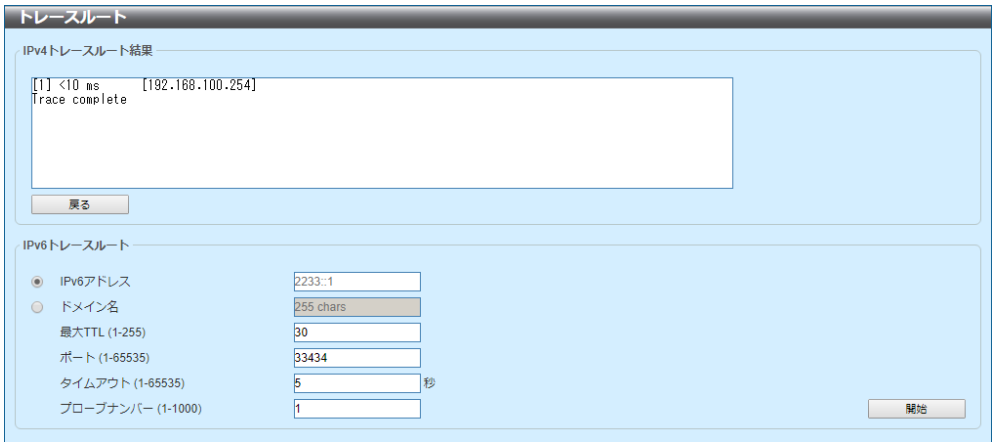


図 14-25 トレースルート（結果）

[戻る] ボタンをクリックして、前の **[トレースルート]** ウィンドウに戻ります。

14.2.6 リセット

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

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

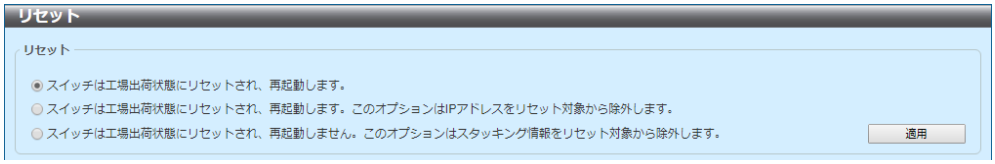


図 14-26 リセット

以下のパラメータを設定できます。

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

[適用] ボタンをクリックして、工場出荷状態へのリセットを開始します。

14.2.7　システム再起動

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

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

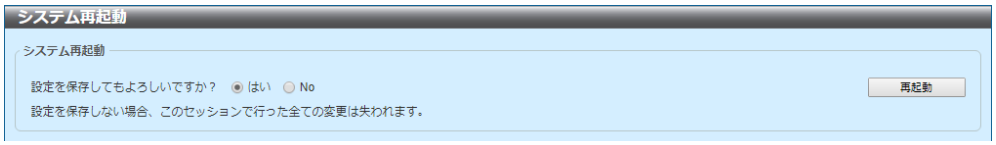


図 14-27 システム再起動

[はい] オプションを選択した場合、再起動するまでに変更された新しいコンフィグレーションが保存されます。
[No] オプションを選択した場合、再起動するまでに変更された新しいコンフィグレーションは廃棄されます。
[再起動] ボタンをクリックして、再起動を開始します。

14.3 言語

Web UI の言語を選択します。デフォルトでは、英語と日本語を選択できます。

以下に示すように、言語を選択します。

図 14-28 言語

14.4 ログアウト

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

図 14-29 ログアウト

15 付録 - システムログ一覧

15.1 802.1X

ID	ログの概要	重大度
1.	イベントの概要：802.1X 認証に成功しました。 ログメッセージ：[802.1X](<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	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

15.2 AAA

ID	ログの概要	重大度
1.	イベントの概要：ログインに成功しました。 ログメッセージ：Successful login through <Console | Telnet | SSH>(Username: <username>, IP: <ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	情報
2.	イベントの概要：ログインに失敗しました。 ログメッセージ：Login failed through <Console | Telnet | SSH> (Username: <username>, IP: <ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	ワーニング
3.	イベントの概要：ログアウトしました。 ログメッセージ：Logout through <Console | Telnet | SSH> (Username: <username>, IP: <ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	情報
4.	イベントの概要：セッションがタイムアウトしました。 ログメッセージ：<Console | Telnet > session timed out (Username: <username>, IP: <ipaddr | ipv6address>) パラメータ概要： ipaddr：IP アドレス。 username：ユーザ名。 ipv6address：IPv6 アドレス。	情報
5.	イベントの概要：SSH サーバが有効になりました。 ログメッセージ：SSH server is enabled	情報
6.	イベントの概要：SSH サーバが無効になりました。 ログメッセージ：SSH server is disabled	情報
7.	イベントの概要：認証ポリシーが有効になりました。 ログメッセージ：Authentication Policy is enabled (Module: AAA)	情報
8.	イベントの概要：認証ポリシーが無効になりました。 ログメッセージ：Authentication Policy is disabled (Module: AAA)	情報
9.	イベントの概要：AAA サーバタイムアウトまたは不適切なコンフィグレーションのためにログインに失敗しました。 ログメッセージ:Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) パラメータ概要： ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング

ID	ログの概要	重大度
10.	イベントの概要：AAA のローカル認証で、認証なしで、またはサーバ認証で、管理者権限の移行が成功しました。 ログメッセージ：Successful Enable Admin through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>) パラメータ概要： local：AAA ローカル認証により管理者権限を移行します。 none：AAA 認証なしで管理者権限を移行します。 server：AAA サーバ認証により管理者権限を移行します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	情報
11.	イベントの概要：AAA サーバタイムアウトまたは不適切なコンフィグレーションのために管理者権限の移行に失敗しました。 ログメッセージ：Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> due to AAA server <ipaddr | ipv6address> timeout or improper configuration (Username: <username>) パラメータ概要： ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング
12.	イベントの概要：AAA ローカル認証または AAA サーバ認証による管理者権限の移行に失敗しました。 ログメッセージ：Enable Admin failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA < local | server <ipaddr | ipv6address>> (Username: <username>) パラメータ概要： local：AAA ローカル認証により管理者権限を移行します。 server：AAA サーバ認証により管理者権限を移行します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング
13.	イベントの概要：AAA のローカル認証で、認証なしで、またはサーバ認証で、ログインに成功しました。 ログメッセージ：Successful login through <Console | Telnet | SSH> from < ipaddr | ipv6address > authenticated by AAA <local | none | server <ipaddr | ipv6address>> (Username: <username>) パラメータ概要： local：AAA ローカル認証を指定します。 none：認証なしを指定します。 server：AAA サーバ認証を指定します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	情報

ID	ログの概要	重大度
14.	イベントの概要：AAA ローカル認証または AAA サーバ認証によるログインに失敗しました。 ログメッセージ:Login failed through <Console | Telnet | SSH> from <ipaddr | ipv6address> authenticated by AAA <local | server <ipaddr | ipv6address>> (Username: <username>) パラメータ概要： local：AAA ローカル認証を指定します。 server：AAA サーバ認証を指定します。 ipaddr：IP アドレス。 ipv6address：IPv6 アドレス。 username：ユーザ名。	ワーニング

15.3 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

15.4 認証（2 ステップ）

ID	ログの概要	重大度
1.	イベントの概要：2 ステップ認証に成功しました。 ログメッセージ：[<step-mode>] (<method>) Authorized user <username> (<macaddr>) on Port <portNum> to VLAN <vid> パラメータ概要： step-mode：2 ステップ認証モードを示します。 method：ローカルまたは RADIUS を示します。 username：認証するユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。 vid：許可する VLAN ID。	情報
2.	イベントの概要：MAC-WEB 認証に失敗しました。 ログメッセージ：[MAC-WEB] (<method>) Rejected at MAC auth <macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
3.	イベントの概要：MAC-WEB 認証に失敗しました。 ログメッセージ：[MAC-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
4.	イベントの概要：MAC-802.1X 認証に失敗しました。 ログメッセージ：[MAC-802.1X] (<method>) Rejected at MAC auth <macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
5.	イベントの概要：MAC-802.1X 認証に失敗しました。 ログメッセージ：[MAC-802.1X] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意
6.	イベントの概要：802.1X-WEB 認証に失敗しました。 ログメッセージ：[802.1X-WEB] (<method>) Rejected at 802.1X auth user <username> (<macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

ID	ログの概要	重大度
7.	イベントの概要：802.1X-WEB 認証に失敗しました。 ログメッセージ：[802.1X-WEB] (<method>) Rejected at WEB auth user <username> (<macaddr>) on Port <portNum> パラメータ概要： method：ローカルまたは RADIUS を示します。 username：拒否されたユーザ。 macaddr：認証する装置の MAC アドレス。 portNum：スイッチのポート番号。	注意

15.5 BPDU ガード

ID	ログの概要	重大度
1.	イベントの概要：BPDU アタックが発生しました。 ログメッセージ：Port<portNum> enter BPDU under attacking state (mode: drop / block / shutdown) パラメータ概要： portNum：ポート番号。 mode：BPDU の現在の状態。	情報
2.	イベントの概要：BPDU アタックから自動回復しました。 ログメッセージ：Port <portNum> recover from BPDU under attacking state automatically パラメータ概要： portNum：ポート番号。	情報
3.	イベントの概要：BPDU アタックからマニュアル回復しました。 ログメッセージ：Port<portNum> recover from BPDU under attacking state manually パラメータ概要： portNum：ポート番号。	情報

15.6 コマンド

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

15.7 コンフィグレーション / ファームウェア

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

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

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

15.8 DAD

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

15.9 DDM

ID	ログの概要	重大度
1.	イベント概要：ワーニング閾値を超えた SFP パラメータがあります。 ログメッセージ：Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded パラメータ概要： interface-id：ポートインタフェース ID。 component：DDM 閾値タイプ。以下のいずれかの可能性があります。 温度 供給電圧 バイアス電流 送信パワー 受信パワー high-low：上限閾値または下限閾値。	ワーニング
2.	イベント概要：アラーム閾値を超えた SFP パラメータがあります。 ログメッセージ：Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded パラメータ概要： interface-id：ポートインタフェース ID。 component：DDM 閾値タイプ。以下のいずれかの可能性があります。 温度 供給電圧 バイアス電流 送信パワー 受信パワー high-low：上限閾値または下限閾値。	クリティカル
3.	イベント概要：ワーニング閾値から回復した SFP パラメータがあります。 ログメッセージ：Optical transceiver <interface-id> <component> back to normal パラメータ概要： interface-id：ポートインタフェース ID。 component：DDM 閾値タイプ。以下のいずれかの可能性があります。 温度 供給電圧 バイアス電流 送信パワー 受信パワー	ワーニング

15.10 デバッグエラー

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

15.11 DHCPv6 クライアント

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

ID	ログの概要	重大度
8.	イベントの概要：DHCPv6 クライアント PD インタフェースの管理者の状態が変化しました。 ログメッセージ：DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> パラメータ概要： intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
9.	イベントの概要：DHCPv6 クライアント PD が委任ルータから IPv6 プレフィックスを取得しました。 ログメッセージ：DHCPv6 client PD obtains an ipv6 prefix <ipv6networkaddr> on interface <intf-name> パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
10.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの更新を開始しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing パラメータ概要： ipv6networkaddr：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
11.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの更新に成功しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success パラメータ概要： ipv6anetworkaddr：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
12.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの再バインディングを開始しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding パラメータ概要： ipv6address：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
13.	イベントの概要：委任ルータから取得した IPv6 プレフィックスの再バインディングに成功しました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success パラメータ概要： ipv6address：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報
14.	イベントの概要：委任ルータから取得した IPv6 プレフィックスが削除されました。 ログメッセージ：The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted パラメータ概要： ipv6address：委任ルータから取得した IPv6 プレフィックス。 intf-name：DHCPv6 クライアント PD インタフェースの名前。	情報

15.12 ダイナミック ARP

ID	ログの概要	重大度
1.	イベントの概要：このログは、DAI が無効な ARP パケットを検出した場合に生成されます。 ログメッセージ：Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) パラメータ概要： type：ARP パケットのタイプ。ARP パケットが ARP リクエストまたは ARP 応答のどちらであるかを示します。 ip-address：IP アドレス。 mac-address：MAC アドレス。 vlan-id：VLAN ID。 interface-id：インタフェースナンバー。	ワーニング
2.	イベントの概要：このログは、DAI が有効な ARP パケットを検出した場合に生成されます。 ログメッセージ：Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) パラメータ概要： type：ARP パケットのタイプ。ARP パケットが ARP リクエストまたは ARP 応答のどちらであるかを示します。 ip-address：IP アドレス。 mac-address：MAC アドレス。 vlan-id：VLAN ID。 interface-id：インタフェースナンバー。	情報

15.13 インタフェース

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

15.14 PoE

ID	ログの概要	重大度
1.	イベントの概要：ポートの給電が ON になりました。 ログメッセージ：Port-<port> Power OFF notification パラメータ概要： port：論理ポート番号を表します。	情報
2.	イベントの概要：ポートの給電が OFF になりました。 ログメッセージ：Port-<port> Power On notification パラメータ概要： port：論理ポート番号を表します。	情報
3.	イベントの概要：PoE の給電電力が閾値を超えました。 ログメッセージ：Usage power is above the threshold	情報
4.	イベントの概要：PoE の給電電力が閾値を超えた後に閾値未満へ下がりました。 ログメッセージ：Usage power is below the threshold	情報
5.	イベントの概要：PoE IC の初期化が失敗しました。 ログメッセージ：PoE IC Reinit Fail	情報
6.	イベントの概要：PoE IC がリセットしました。 ログメッセージ：PoE IC Reset	情報

15.15 PoE スケジューラ

ID	ログの概要	重大度
1.	イベントの概要：PoE スケジューラにより PoE 給電を ON にしました。 ログメッセージ：(PoE) PoE port is changed to ON by PoE Scheduler. パラメータ概要： port：論理ポート番号を表します。	ワーニング
2.	イベントの概要：PoE スケジューラにより PoE 給電を OFF にしました。 ログメッセージ：(PoE) PoE port is changed to OFF by PoE Scheduler. パラメータ概要： port：論理ポート番号を表します。	ワーニング
3.	イベントの概要：PoE スケジューラにより PoE 給電を OFF/ON しました。 ログメッセージ：(PoE) PoE port is reset by PoE Scheduler.	ワーニング

15.16 PoE オートリブート

ID	ログの概要	重大度
1.	イベントの概要：PoE 給電の OFF/ON を実行しました。 ログメッセージ：Execute PoE OFF/ON Port-<port> パラメータ概要： port：論理ポート番号を表します。	情報
2.	イベントの概要：Ping 監視により PoE 端末の異常を検知しました。 ログメッセージ：Detect equipment failure by ICMP <IP> パラメータ概要： IP：IP アドレスを表します。	情報
3.	イベントの概要：LLDP 監視により PoE 端末の異常を検知しました。 ログメッセージ：Detect equipment failure by LLDP Port-<port> パラメータ概要： port：論理ポート番号を表します。	情報
4.	イベントの概要：トラフィック監視により PoE 端末の異常を検知しました。 ログメッセージ：Detect equipment failure by Traffic Port-<port> パラメータ概要： port：論理ポート番号を表します。	情報

15.17 IP ソースガードの検証

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

15.18 LACP

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

15.19 LLDP-MED

ID	ログの概要	重大度
1.	イベントの概要：LLDP-MED トポロジの変化を検出しました。 ログメッセージ：LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) パラメータ概要： portNum：ポート番号。 chassisType：シャーシ ID サブタイプ。 値リスト： 1. chassisComponent（1） 2. interfaceAlias（2） 3. portComponent（3） 4. macAddress（4） 5. networkAddress（5） 6. interfaceName（6） 7. local（7） chassisID：シャーシ ID。 portType：ポート ID サブタイプ。 値リスト： 1. interfaceAlias（1） 2. portComponent（2） 3. macAddress（3） 4. networkAddress（4） 5. interfaceName（5） 6. agentCircuitId（6） 7. local（7） portID：ポート ID。 deviceClass：LLDP-MED デバイスタイプ。	注意

ID	ログの概要	重大度
2.	イベントの概要：競合する LLDP-MED デバイスタイプを検出しました。 ログメッセージ：Conflict LLDP-MED device type detected (on port <portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) パラメータ概要： portNum：ポート番号。 chassisType：シャーシ ID サブタイプ。 値リスト： 1. chassisComponent（1） 2. interfaceAlias（2） 3. portComponent（3） 4. macAddress（4） 5. networkAddress（5） 6. interfaceName（6） 7. local（7） chassisID：シャーシ ID。 portType：ポート ID サブタイプ。 値リスト： 1. interfaceAlias（1） 2. portComponent（2） 3. macAddress（3） 4. networkAddress（4） 5. interfaceName（5） 6. agentCircuitId（6） 7. local（7） portID：ポート ID。 deviceClass：LLDP-MED デバイスタイプ。	注意

ID	ログの概要	重大度
3.	イベントの概要：互換性のない LLDP-MED TLV セットを検出しました。 ログメッセージ：Incompatible LLDP-MED TLV set detected (on port <portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) パラメータ概要： portNum：ポート番号。 chassisType：シャーシ ID サブタイプ。 値リスト： 1. chassisComponent（1） 2. interfaceAlias（2） 3. portComponent（3） 4. macAddress（4） 5. networkAddress（5） 6. interfaceName（6） 7. local（7） chassisID：シャーシ ID。 portType：ポート ID サブタイプ。 値リスト： 1. interfaceAlias（1） 2. portComponent（2） 3. macAddress（3） 4. networkAddress（4） 5. interfaceName（5） 6. agentCircuitId（6） 7. local（7） portID：ポート ID。 deviceClass：LLDP-MED デバイスタイプ。	注意

15.20 ループ検知

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

15.21 MAC ベースアクセスコントロール

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

15.22 MSTP デバッグ拡張機能

ID	ログの概要	重大度
1.	イベントの概要：トポロジが変化しました。 ログメッセージ：Topology changed (Instance : <Instance-id>,<interface-id>, MAC:<macaddr>) パラメータ概要： Instance-id：インスタンス ID。 interface-id：ポート ID。 macaddr：MAC アドレス。	注意
2.	イベントの概要：スパニングツリーの新しいルートブリッジです。 ログメッセージ：[CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :< priority>) パラメータ概要： Instance-id：インスタンス ID。 macaddr：MAC アドレス。 priority：優先度値。	注意
3.	イベントの概要：スパニングツリープロトコルが有効になりました。 ログメッセージ：Spanning Tree Protocol is enabled	情報
4.	イベントの概要：スパニングツリープロトコルが無効になりました。 ログメッセージ：Spanning Tree Protocol is disabled	情報
5.	イベントの概要：新しいルートポートです。 ログメッセージ：New root port selected (Instance:<instance-id>, <interface-id >) パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。	注意
6.	イベントの概要：スパニングツリーポート状態が変化しました。 ログメッセージ：Spanning Tree port status change (Instance :< instance-id>, <interface-id>) <old-status> -> <new-status> パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。 old_status：変化前のステータス。 new_status：変化後のステータス。	注意
7.	イベントの概要：スパニングツリーポートロールが変化しました。 ログメッセージ：Spanning Tree port role change (Instance :< instance-id>, <interface-id>) <old-role> -> <new-role> パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。 old_role：変化前のロール。 new_status：変化後のロール。	情報
8.	イベントの概要：スパニングツリーインスタンスが作成されました。 ログメッセージ：Spanning Tree instance created. (Instance :< instance-id>) パラメータ概要： instance-id：インスタンス ID。	情報

ID	ログの概要	重大度
9.	イベントの概要：スパニングツリーインスタンスが削除されました。 ログメッセージ：Spanning Tree instance deleted. (Instance :< instance-id >) パラメータ概要： instance-id：インスタンス ID。	情報
10.	イベントの概要：スパニングツリーバージョンが変化しました。 ログメッセージ：Spanning Tree version change (new version :< new-version>) パラメータ概要： new_version：変化後の STP バージョン。	情報
11.	イベントの概要：スパニングツリー MST コンフィグレーション ID 名とリビジョンレベルが変化しました。 ログメッセージ：Spanning Tree MST configuration ID name and revision level change (name :< name>, revision level <revision-level>) パラメータ概要： name：変化後の名前。 revision_level：変化後のリビジョンレベル。	情報
12.	イベントの概要：スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが削除されました。 ログメッセージ：Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > delete vlan <startvlanid> [- <endvlanid>]) パラメータ概要： instance-id：インスタンス ID。 startvlanid-endvlanid：VLAN リスト。	情報
13.	イベントの概要：スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが追加されました。 ログメッセージ：Spanning Tree MST configuration ID VLAN mapping table change (instance: < instance-id > add vlan <startvlanid> [- <endvlanid>]) パラメータ概要： instance-id：インスタンス ID。 startvlanid-endvlanid：VLAN リスト。	情報
14.	イベントの概要：ガードルート機能によりスパニングツリーロールが変化しました。 ログメッセージ：Spanning Tree port role change (Instance : < instance-id >, <interface-id>) to alternate port due to the guard root パラメータ概要： instance-id：インスタンス ID。 interface-id：ポート ID。	情報

15.23 ポートセキュリティ

ID	ログの概要	重大度
1.	イベントの概要：ポートでアドレスがフルです。 ログメッセージ：MAC address <mac-address> causes port security violation on <interface-id> パラメータ概要： macaddr：違反 MAC アドレス。 interface-id：違反が発生しているインタフェース。	ワーニング
2.	イベントの概要：システムでアドレスがフルです。 ログメッセージ：Limit on system entry number has been exceeded	ワーニング

15.24 RADIUS

ID	ログの概要	重大度
1.	イベントの概要：このログは、RADIUS が有効な VLAN ID 属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 vid：RADIUS サーバが許可して割り当てた VLAN ID。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報
2.	イベントの概要：このログは、RADIUS が有効な帯域幅属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface-id> (Username: <username>) パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 direction：帯域制御の方向（入口または出口など）を示します。 threshold：RADIUS サーバが許可して割り当てた帯域幅閾値。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報
3.	イベントの概要：このログは、RADIUS が有効な優先度属性を割り当てた場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port < interface-id> (Username: <username>) パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 priority：RADIUS サーバが許可して割り当てた優先度。 interface-id：認証されたクライアントのポート番号。 username：認証するユーザ名を示します。	情報
4.	イベントの概要：このログは、RADIUS が ACL スクリプトを割り当てたが、リソース不足のためにシステムに適用できなかった場合に生成されます。 ログメッセージ：RADIUS server <server-ip> assigns <username> ACL failure at port < interface-id> (<acl-script>) パラメータ概要： server-ip：RADIUS サーバ IP アドレスを示します。 username：認証するユーザ名を示します。 interface-id：認証されたクライアントのポート番号。 acl-script：RADIUS サーバが許可して割り当てた ACL スクリプト。	ワーニング
5.	イベントの概要：このログは、アクセスリストナンバーの割り当てに失敗した場合に生成されます。 ログメッセージ：Local assigns [USERNAME] filter-id ID failure at port INTERFACE-ID パラメータ概要： username：認証するユーザ名を示します。 filter-id：アクセスリストナンバーを示します。 interface-id：認証されたクライアントのポート番号。	ワーニング

15.25 RRP

ID	ログの概要	重大度
1.	イベントの概要：マスターノードの状態が "Failed" から "Complete" に変化しました。 ログメッセージ：Ring topology was recovered to complete	注意
2.	イベントの概要：マスターノードの状態が "Complete" から "Failed" に変化しました。 ログメッセージ：Ring topology was failed	ワーニング
3.	イベントの概要：マスターノードまたはトランジットノードが、RRP パケットまたはステートマシンに基づいて、そのフォワーディングデータベースをフラッシュしました。 ログメッセージ：FDB was flushed	情報
4.	イベントの概要：トランジットノードの RRP 状態が "Link-Up" に変化しました。 ログメッセージ：RRP ring status was changed to Link-Up	ワーニング
5.	イベントの概要：トランジットノードの RRP 状態が "Link-Down" に変化しました。 ログメッセージ：RRP ring status was changed to Link-Down	注意
6.	イベントの概要：トランジットノードの RRP 状態が "Pre-Forwarding" に変化しました。 ログメッセージ：RRP ring status was changed to Pre-Forwarding	情報
7.	イベントの概要：特定のドメインとポートでリングガード機能が有効になりました。 ログメッセージ：Ring Guard was activated on “<domain-name>” domain at port <port> パラメータ概要： <domain name>：ターゲットドメイン名。 <port num>：リングガード機能が有効になったターゲットポート番号。	情報

15.26 SNMP

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

15.27 システム

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

15.28 Telnet

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

15.29 温度

ID	ログの概要	重大度
1.	イベントの概要：温度センサがアラーム状態に移行しました。 ログメッセージ：Unit <unitID> Sensor:<sensorID> detects abnormal temperature <temperature> パラメータ概要： unitID：ユニット ID。 sensorID：センサ ID。 temperature：センサの現在の温度。	クリティカル
2.	イベントの概要：通常の温度に回復しました。 ログメッセージ：Unit <unitID> Sensor:<sensorID> temperature back to normal パラメータ概要： unitID：ユニット ID。 sensorID：センサ ID。 temperature：温度。	クリティカル

15.30 トラフィック制御

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

15.31 音声 VLAN

ID	ログの概要	重大度
1.	イベントの概要：インタフェースで新しい音声装置を検出しました。 ログメッセージ：New voice device detected (<interface-id>, MAC: < mac-address >) パラメータ概要： interface-id：インタフェース名。 mac-address：音声装置の MAC アドレス。	情報
2.	イベントの概要：自動音声 VLAN モードのインタフェースが音声 VLAN に参加しました。 ログメッセージ：< interface-id > add into voice VLAN <vid > パラメータ概要： interface-id：インタフェース名。 vid：VLAN ID。	情報
3.	イベントの概要：このログメッセージは、インタフェースが音声 VLAN を脱退し、さらにそのインタフェースのエージング期間内に音声装置を検出しなかった場合に、送信されます。 ログメッセージ：< interface-id > remove from voice VLAN <vid > パラメータ概要： interface-id：インタフェース名。 vid：LAN ID。	情報

15.32 WAC

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

15.33 Web

ID	ログの概要	重大度
1.	イベントの概要：Web からのログインに成功しました。 ログメッセージ："Successful login through Web (Username: <username>, IP: <ipaddr>)" パラメータ概要： username：ユーザ名。 ipaddr：Web からスイッチにアクセスしたユーザの IP アドレス。	情報
2.	イベントの概要：Web からのログインに失敗しました。 ログメッセージ：Login failed through Web (Username: <username>, IP: <ipaddr>)" パラメータ概要： username：ユーザ名。 ipaddr：Web からスイッチにアクセスしたユーザの IP アドレス。	ワーニング
3.	イベントの概要：HTTPS からのログインに成功しました。 ログメッセージ：Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>) パラメータ概要： username：ユーザ名。 ipaddr：セキュア Web からスイッチにアクセスしたユーザの IP アドレス。	情報
4.	イベント概要：セキュア Web からのログインに失敗しました。 ログメッセージ：Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) パラメータ概要： username：ユーザ名。 ipaddr：セキュア Web からスイッチにアクセスしたユーザの IP アドレス。	ワーニング
5.	イベントの概要：ログのアップロードに成功しました。 ログメッセージ：Log message uploaded by WEB successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) パラメータ概要： username：ユーザ名。 ipaddr：スイッチにアクセスしたユーザの IP アドレス。 macaddr：クライアントの MAC アドレス。 server IP：TFTP サーバ IP アドレス。 filename：ログファイル名。	情報
6.	イベントの概要：ログのアップロードに失敗しました。 ログメッセージ：Log message uploaded by WEB unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>, Server IP: <ipaddr>, File Name: <filename>) パラメータ概要： username：ユーザ名。 ipaddr：スイッチにアクセスしたユーザのアクセス元の IP アドレス。 macaddr：クライアントの MAC アドレス。 server IP：TFTP サーバ IP アドレス。 filename：ログファイル名。	情報

16 付録 - システムトラップ一覧

16.1 BPDU ガード

ID	トラップ名	トラップの概要	OID
1.	mnoBpduProtectionUnderAttackingTrap	BPDU アタックが発生し、廃棄 / ブロック / シャットダウンモードに移行します。 バインディングオブジェクト： mnoBpduProtectionPortIndex ポートインタフェース。 （2）mnoBpduProtectionPortMode 廃棄 / ブロック / シャットダウンモード。	1.3.6.1.4.1.396.5.5.3.4.0.1
2.	mnoBpduProtectionRecoveryTrap	BPDU アタックから自動回復しました。 バインディングオブジェクト： mnoBpduProtectionPortIndex ポートインタフェース。 mnoBpduProtectionRecoveryMethod 自動 / マニュアル回復。	1.3.6.1.4.1.396.5.5.3.4.0.2

16.2 DDM

ID	トラップ名	トラップの概要	OID
1.	mnoDdmAlarmTrap	トラップアクションのコンフィグレーションに応じて、パラメータ値がアラーム閾値を超えたとき、または通常状態に回復したとき、このトラップが送信されます。 バインディングオブジェクト： mnoDdmPort ポート番号 mnoDdmThresholdType DDM 閾値タイプ temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType 超えた閾値がアラーム上限閾値またはアラーム下限閾値のどちらであるか (4) mnoDdmThresholdExceedOrRecover GBIC が DDM 閾値を超えているか、または通常状態に回復しているか	1.3.6.1.4.1.396.5.5.1.4.0.1
2.	mnoDdmWarningTrap	トラップアクションのコンフィグレーションに応じて、パラメータ値がワーニング閾値を超えたとき、または通常状態に回復したとき、このトラップが送信されます。 バインディングオブジェクト： mnoDdmPort ポート番号 mnoDdmThresholdType DDM 閾値タイプ temperature/voltage/bias/txpower/rxpower mnoDdmThresholdExceedType 超えた閾値がワーニング上限閾値またはワーニング下限閾値のどちらであるか (4) mnoDdmThresholdExceedOrRecover GBIC が DDM 閾値を超えているか、または通常状態に回復しているか	1.3.6.1.4.1.396.5.5.1.4.0.2

16.3 DHCP サーバプロテクト

ID	トラップ名	トラップの概要	OID
1.	mnoFilterDetectedTrap	不正な DHCP サーバが検出されたときに、このトラップが送信されます。検出した不正な DHCP サーバの IP アドレスは、ログ停止未認証期間中に 1 回のみトラッププレシーバに送信されます。 バインディングオブジェクト： mnoFilterDetectedIP 不正な DHCP サーバの IP アドレス。 mnoFilterDetectedport ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.7.0.1

16.4 Gratuitous ARP

ID	トラップ名	トラップの概要	OID
1.	mnoAgentGratuitousARPTrap	IP アドレスが競合したときに、このトラップが送信されます。 バインディングオブジェクト： agentGratuitousARPIpAddr Gratuitous ARP で受信した競合 IP アドレス。 agentGratuitousARPMacAddr Gratuitous ARP パケットのセンダー MAC アドレス。 agentGratuitousARPPortNumber Gratuitous ARP パケットを受信したスイッチのポート番号。 agentGratuitousARPInterfaceName Gratuitous ARP を受信したスイッチの IP インタフェース名。	1.3.6.1.4.1.396.5.5.3.6.0.1

16.5 LLDP-MED

ID	トラップ名	トラップの概要	OID
1.	lldpRemTablesChange	lldpStatsRemTableLastChangeTime の値が変化したときに、lldpRemTablesChange 通知が送信されます。 バインディングオブジェクト： (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
2.	lldpXMedTopologyChangeDetected	トポロジの変化を検出したローカル装置によって生成され、新しいリモート装置がローカルポートに接続されたこと、リモート装置が切断されたこと、またはリモート装置がポート間で移動されたことを示す通知。 バインディングオブジェクト： (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

16.6 ループ検知

ID	トラップ名	トラップの概要	OID
1.	mnoLoopDetectNotification	ネットワークループが発生したことを示します。	1.3.6.1.4.1.396.5.5.2.1
2.	mnoLoopRecoveryNotification	ネットワークループが消滅したことを示します。	1.3.6.1.4.1.396.5.5.2.2

16.7 MAC ベースアクセスコントロール

ID	トラップ名	トラップの概要	OID
1.	mnoMacBasedAccessControlLoggedSuccess	MAC ベースアクセスコントロールホストへのログインに成功すると、このトラップが送信されます。 バインディングオブジェクト： mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 mnoMacBasedAuthInfoPortIndex ポートインタフェース。 mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.1
2.	mnoMacBasedAccessControlLoggedFail	MAC ベースアクセスコントロールホストへのログインに失敗すると、このトラップが送信されます。 バインディングオブジェクト： mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 mnoMacBasedAuthInfoPortIndex ポートインタフェース。 mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.2
3.	mnoMacBasedAccessControlAgesOut	MAC ベースアクセスコントロールホストがエージアウトすると、このトラップが送信されます。 バインディングオブジェクト： mnoMacBasedAuthInfoMacIndex ホスト MAC アドレス。 （2）mnoMacBasedAuthInfoMacIndex ポートインタフェース。 （3）mnoMacBasedAuthVID VLAN ID。	1.3.6.1.4.1.396.5.5.3.2.0.3

16.8 MAC 通知

ID	トラップ名	トラップの概要	OID
1.	mnoL2macNotification	このトラップは、アドレステーブルの MAC アドレスに変化があることを示します。 バインディングオブジェクト： mnoL2macNotifyInfo 装置の MAC アドレスの変更情報。詳細情報には、以下が含まれます。 操作コード + MAC アドレス + ボックス ID + インタフェース ID + ゼロ。 操作コード：1、2 1 は新しい MAC アドレスを学習したことを意味します。 2 は古い MAC アドレスを削除したことを意味します。 ボックス ID：スイッチのボックス ID インタフェース ID：ボックスで学習または削除したインタフェース ID。 ゼロ：各メッセージの区切りに使用します（操作コード + MAC アドレス + ボックス ID + ポート番号)。	1.3.6.1.4.1.396 .5.5.3.1.0.1

16.9 MSTP

ID	トラップ名	トラップの概要	OID
1.	newRoot	トラップは、送信エージェントがスパニングツリーの新しいルートになったことを示します。このトラップは、新しいルートとして選定された直後（トポロジ変化タイマーの期限切れ直後、選定の直後など）にブリッジにより送信されます。このトラップの実装はオプションです。	1,3,6,1,2,1,17.0.1
2.	topologyChange	トラップは、設定されているポートのいずれかが学習状態からフォワーディング状態に移行したとき、またはフォワーディング状態からブロッキング状態に移行したとき、ブリッジにより送信されます。そのような移行の際に newRoot トラップが送信された場合、それと同じ移行に関してこのトラップが送信されることはありません。このトラップの実装はオプションです。	1,3,6,1,2,1,17.0.2

16.10 ポートセキュリティ

ID	トラップ名	トラップの概要	OID
1.	mnoL2PortSecurityViolationTrap	ポートセキュリティトラップが有効な場合、事前定義されているポートセキュリティコンフィグレーションに違反する新しい MAC アドレスは、トラップメッセージ送信をトリガーします。 バインディングオブジェクト： mnoPortSecPortIndex ポートインタフェース。 mnoL2PortSecurityViolationMac ホスト MAC アドレス。	1.3.6.1.4.1.396.5.5.3.3.0.1

16.11 ポート

ID	トラップ名	トラップの概要	OID
1.	linkUp	この通知は、ポートがリンクアップしたときに生成されます。 バインディングオブジェクト： (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2.	linkDown	この通知は、ポートがリンクダウンしたときに生成されます。 バインディングオブジェクト： (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

16.12 RMON

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

16.13 SNMP 認証

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

16.14 システム

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

16.15 温度

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

16.16 トラフィック制御

ID	トラップ名	トラップの概要	OID
1.	mnoPktStormOccurred	パケットストームメカニズムによりパケットストープが検出され、アクションとしてシャットダウンを実行する場合。 バインディングオブジェクト： mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.1
2.	mnoPktStormCleared	パケットストームが解消された場合。 バインディングオブジェクト： mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.2
3.	mnoPktStormDisablePort	パケットストームメカニズムによりポートが無効になった場合。 バインディングオブジェクト： mnoPktStormCtrlPortIndex ポートインタフェース。	1.3.6.1.4.1.396.5.5.3.5.0.3

パナソニックEWネットワークス株式会社

〒105-0021　東京都港区東新橋 2 丁目 12 番 7 号　住友東新橋ビル 2 号館 4 階
TEL 03-6402-5301 / FAX 03-6402-5304
URL: https://panasonic.co.jp/ew/pewnw/

P0221-5043