D-Link DGS-1520 シリーズ

Gigabit Layer3 Stackable Smart Managed Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意　必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

⚠危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
⚠警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。

記号の意味　⃠ してはいけない**「禁止」**内容です。　❗ 必ず実行していただく**「指示」**の内容です。

⚠危険

⃠ 禁止　分解・改造をしない
火災、やけど、けが、感電などの原因となります。

⃠ 禁止　ぬれた手でさわらない
感電の原因となります。

⃠ 禁止　水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、故障の原因となります。

⃠ 禁止　水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止　各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止　油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止　内部に金属物や燃えやすいものを入れない
火災、感電、故障の原因となります。

⃠ 禁止　砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない
火災、やけど、けが、感電、故障の原因となります。

⃠ 禁止　電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない
火災、やけど、けが、感電、故障の原因となります。

⚠警告

⃠ 禁止　落としたり、重いものを乗せたり、強いショックを与えたり、圧力をかけたりしない
故障の原因となります。

⃠ 禁止　発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因になります。
使用を止めて、ケーブル / コード類を抜いて、煙が出なくなってから販売店に修理をご依頼ください。

⃠ 禁止　表示以外の電圧で使用しない
火災、感電、または故障の原因となります。

⃠ 禁止　たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の原因となります。

❗　設置、移動のときは電源プラグを抜く
火災、感電、または故障の原因となります。

⃠ 禁止　雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電の原因となります。

⃠ 禁止　ケーブル / コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いものの下敷きなどは、ケーブル / コードや端子の破損の原因となり、火災、感電、または故障の原因となります。

❗　本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
火災、感電、または故障の原因となります。

⃠ 禁止　各光源をのぞかない
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや LED をのぞきますと強力な光源により目を損傷するおそれがあります。

⃠ 禁止　各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほこりが内部に入ったりしないようにする
火災、やけど、けが、感電または故障の原因となります。

⃠ 禁止　使用中に布団で覆ったり、包んだりしない
火災、やけどまたは故障の原因となります。

❗　ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。

⃠ 禁止　カメラのレンズに直射日光などを長時間あてない
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の原因となります。

❗　無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。

⃠ 禁止　本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
火災、または故障の原因となります。

❗　耳を本体から離してご使用ください
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。

❗　無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
医療電気機器に悪影響を及ぼすおそれがあります。

❗　高精度な制御や微弱な信号を取り扱う電子機器の近くでは使用しない
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。

❗　ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
破損部や露出部に触れると、やけど、けが、感電の原因となります。

❗　ペットなどが本機に噛みつかないように注意する
火災、やけど、けがなどの原因となります。

⃠ 禁止　コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない
火災、やけど、感電または故障の原因となります。

⃠ 禁止　AC アダプタや電源ケーブルに海外旅行用の変圧器等を使用しない
発火、発熱、感電または故障の原因となります。

⚠警告

- ACアダプタもしくは電源プラグについたほこりは、拭き取る
  ほこりが付着した状態で使用すると、
  火災、やけど、感電または故障の原因となります。
- ACアダプタや電源ケーブルをコンセントに
  さしこむときは、確実に差し込む
  確実に差し込まないと、火災、やけど、
  感電もしくは故障の原因となります。
- 接続端子が曲がるなど変形した場合は、直ちに使用を中止する。
  また、変形をもとに戻しての使用も行わない
  端子のショートにより、火災、やけど、けが、
  感電または故障の原因となります。
- 各種接続端子を機器本体に接続する場合、斜めに差したり、
  差した状態で引っ張ったりしない
  火災、やけど、感電または故障の原因となります。
- 使用しない場合は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  電源プラグを差したまま放置すると、火災、やけど、
  感電または故障の原因となります。
- お手入れの際は、ACアダプタもしくは
  電源ケーブルをコンセントから抜く
  抜かずに行うと、火災、やけど、感電または故障の原因となります。
- 禁止 SDやMicroSDカード、USBメモリの使用中は、
  カードやメモリを取り外したり、本製品の電源を切ったりしない
  データの消失、機器本体の故障の原因となります。
- 禁止 磁気カードや磁気を帯びたものを本製品に近づけない
  磁気カードのデータが消えてしまうおそれもしくは
  機器本体の誤作動の原因となります。
- ディーリンクジャパンが販売している無線機器は
  国内専用のため、海外で使用しない
  海外では国によって電波使用制限があるため、
  本製品を使用した場合、罰せられる場合があります。
  海外から持ち込んだディーリンク製品や並行輸入品を
  日本国内で使用する場合も同様に、罰せられる場合があります。

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 コードを持って抜かない
  コードを無理に曲げたり、引っ張ると、
  コードや機器本体の破損の原因となります。
- 禁止 振動が発生する場所では使用しない
  故障の原因となります。
- 付属品の使用は取扱説明書に従う
  本製品の付属品は、取扱説明書に従い、
  他の製品に使用しないでください。機器の破損の原因となります。
- 禁止 破損したまま使用しない
  火災、やけどまたはけがの原因となります。
- 禁止 ぐらついた台の上や傾いた場所などの
  不安定な場所や高所には置かない
  落下して、けがなどの原因となります。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 コンセントにつないだ状態で、ACアダプタや
  電源コンセントに長時間触れない
  やけど、感電の原因となります。
- 一般の電話機やコードレス電話、テレビ、ラジオなどを
  お使いになっている近くで使用しない
  近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、
  なるべく離れた場所で使用してください。
- 禁止 D-Linkが指定したオプション品がある場合は、
  指定オプションを使用する
  不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

この装置は、クラスA機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI - A

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法でのご使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。
さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注意事項や手順についてもよくお読みください。

- システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも含みます。

警告 前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。

警告 接地用伝導体を壊したり、接地用伝導体を適切に取り付けないで装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告 システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケーブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- ラックにシステム / コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つのみとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と規制に準拠していることを確認してください。

バッテリの取り扱いについて

警告 不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

安全にお使いいただくために

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/product-assurance-provision

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用の前にご確認ください。
製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。
https://www.dlink-jp.com/support

警告 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

目次

安全にお使いいただくために 2
ご使用上の注意 4
静電気障害を防止するために 4
電源の異常 4
ラック搭載型製品に関する一般的な注意事項 5
バッテリの取り扱いについて 5

はじめに 14

本マニュアルの対象者 16
表記規則について 16
製品名 / 品番一覧 16

第 1 章　本製品のご使用にあたって 17

DGS-1520 シリーズについて 17
ポート 17
SFP 18
オプション製品 18
前面パネル 19
Reset/ZTP（リセット / ゼロタッチプロビジョニングボタン） 19
LED 表示 20
背面パネル 22
背面パネル LED 表示 22
側面パネル 24
スマートファンについて 24

第 2 章　スイッチの設置 25

パッケージの内容 25
ネットワーク接続前の準備 25
ゴム足の取り付け (19 インチラックに設置しない場合) 25
19 インチラックへの取り付け 26
光トランシーバの接続 27
電源抜け防止クリップの装着 27
MGMT ポートに DPS-520 を接続する 29
RPS ポートに DPS-700 を接続する 30
電源の投入 31
電源の異常 31

第 3 章　スイッチの接続 32

エンドノードと接続する 32
ハブまたはスイッチと接続する 32
バックボーンまたはサーバと接続する 33

第 4 章　スイッチ管理について 34

Web GUI による管理 34
SNMP による管理 34
CLI による管理 34
端末をコンソールポートに接続する 34
ユーザアカウント / パスワードの設定 35
IP アドレスの割り当て 36
管理ポートへの接続 36

第 5 章　Web ベースのスイッチ管理 37

Web ベースの管理について 37
Web マネージャへのログイン 37
スマートウィザード設定 38
Web GUI について 40
Web GUI の各エリアについて 40
Web マネージャのメニュー構成 41

第 6 章　システム 45

デバイス情報 46
システム情報設定 47
周辺機器設定 48
ポート設定 49
ポート設定 49
ポートステータス 50

GBIC ポート 50
ポートオートネゴシエーション 51
エラー Disable 設定 51
ジャンボフレーム 52
インタフェース説明 53
ループバックテスト 54
PoE（DGS-1520-28MP/52MP） 55
PoE システム 55
PoE ステータス 56
PoE 設定 56
PD Alive 57
PoE 統計 57
PoE 計測 58
PoE LLDP クラシフィケーション 58
システムログ 59
システムログ設定 59
システムログ識別設定 61
システムログサーバ設定 62
システムログ 63
システム攻撃ログ 63
時間と SNTP 64
時刻設定 64
タイムゾーン設定 64
SNTP 設定 66
タイムレンジ 67
リセットボタンの設定 68

第 7 章　管理 69

コマンドロギング 70
ユーザアカウント設定 70
パスワード暗号化 71
パスワードリカバリ 72
ログイン方法 72
SNMP 設定 74
トラップ 74
MIB 74
SNMP グローバル設定 75
SNMP リンクチェンジトラップ設定 76
SNMP ビューテーブル設定 76
SNMP コミュニティテーブル設定 77
SNMP グループテーブル設定 78
SNMP エンジン ID ローカル設定 79
SNMP ユーザテーブル設定 79
SNMP ホストテーブル設定 80
SNMP コンテキストマッピングテーブル設定 81
RMON 設定 82
RMON グローバル設定 82
RMON 統計設定 82
RMON 履歴設定 83
RMON アラーム設定 84
RMON イベント設定 85
Telnet/Web 設定 86
セッションタイムアウト 87
DHCP 設定 88
DHCP サービス 88
DHCP クラス設定 88
DHCP プール設定 89
DHCP サーバ 90
DHCPv6 サーバ設定 96
DHCP リレー 100
DHCPv6 リレー 107
DHCP 自動設定 112
DHCP 自動イメージ設定 113
DNS 114
DNS グローバル設定 114
DNS サーバ設定 114

DNS ホスト設定 115
NTP 116
NTP グローバル設定 116
NTP サーバ設定 117
NTP ピア設定 117
NTP アクセスグループ設定 118
NTP キー設定 119
NTP インタフェース設定 119
NTP アソシエーション 120
NTP ステータス 120
IP 送信元インタフェース 121
ファイルシステム設定 121
スタッキング設定 123
物理スタッキング 128
スタッキング帯域 129
仮想スタック設定（SIM） 130
シングル IP マネジメント（SIM）の概要 130
シングル IP マネジメント（SIM）のルールと動作 130
バージョン 1.61 へのアップグレード 131
シングル IP 設定 132
トポロジ 133
ファームウェアアップグレード 136
設定ファイルバックアップ / リストア 136
ログファイルをアップロード 137
D-Link ディスカバリプロトコル 138
DDP 設定 138
DDP 隣接 138
SMTP 設定 139
NLB FDB 設定 140

第 8 章　L2 機能 141

FDB 142
スタティック FDB 142
MAC アドレステーブル設定 143
MAC アドレステーブル 144
MAC 通知 145
VLAN について 146
IEEE 802.1p プライオリティについて 146
VLAN とは 146
IEEE 802.1Q VLAN 146
VLAN 151
VLAN 設定ウィザード 151
802.1Q VLAN 152
VLAN インタフェース 153
802.1v プロトコル VLAN 158
GVRP 159
Asymmetric VLAN 161
MAC VLAN 162
L2VLAN インタフェース説明 162
サブネット VLAN 163
スーパー VLAN 163
自動サーベイランス VLAN 165
Voice VLAN 167
プライベート VLAN 170
VLAN トンネル 171
Dot1q トンネル 171
VLAN マッピング 172
VLAN マッピングプロファイル 173
STP 178
802.1Q-2005 MSTP 178
802.1D-2004 Rapid STP 178
ポートの状態遷移 179
STP グローバル設定 180
STP ポート設定 181
MST 設定識別子 182

STP インタンス設定 183
MSTP ポート情報 184
ERPS (G.8032) 185
ERPS 185
ERPS プロファイル 188
ループバック検知 189
リンクアグリゲーション 190
ポートトランクグループについて 190
L2 プロトコル トンネル 193
L2 マルチキャストコントロール 194
IGMP スヌーピング 194
MLD スヌーピング 202
マルチキャスト VLAN 210
PIM スヌーピング 213
マルチキャストフィルタリングモード 215
LLDP 216
LLDP グローバル設定 216
LLDP ポート設定 217
LLDP 管理アドレスリスト 218
LLDP 基本 TLVs 設定 218
LLDP Dot1 TLVs 設定 219
LLDP Dot3 TLVs 設定 219
LLDP-MED ポート設定 220
LLDP 統計情報 221
LLDP ローカルポート情報 221
LLDP 隣接ポート情報 223

第 9 章　L3 機能 224

ARP 225
ARP エージングタイム 225
スタティック ARP 設定 226
プロキシ ARP 227
ARP テーブル 227
Gratuitous ARP 228
IPv6 隣接 229
インタフェース 230
IPv4 インタフェース 230
IPv6 インタフェース 232
ループバックインタフェース 234
Null インタフェース 235
UDP Helper 236
IP 転送プロトコル 236
IP ヘルパーアドレス 236
IPv4 スタティック / デフォルトルート 237
IPv4 ルートテーブル 238
IPv6 スタティック / デフォルトルート 239
IPv6 ルートテーブル 240
ルート優先 241
ECMP 設定 241
IPv6 General プレフィックス 242
URPF 設定 243
RIP 244
RIP 設定 244
RIP 配布リスト 245
RIP インタフェース設定 245
RIP データベース 246
RIPng 247
RIPng 設定 247
RIPng インタフェース 248
RIPng データベース 248
OSPF 249
OSPFv2 249
OSPFv3 259
IP マルチキャストルーティングプロトコル 269
IGMP 269
MLD 272
IGMP プロキシ 275

MLD プロキシ 277
DVMRP 279
PIM 281
IPMC 306
IPv6MC 311
IP ルートフィルタ 313
ルートマップ 313
ポリシールート 316
VRRP 317
VRRPv3 設定 319

第 10 章　QoS 321

QoS の長所 321
QoS について 322
基本設定 323
ポートデフォルト CoS 323
ポートスケジューラ方式 323
キュー設定 325
CoS とキューのマッピング 325
ポートレート制限 326
キューレート制限 327
詳細設定 328
DSCP 変換マップ 328
ポートトラストステートと変換バインディング 328
DSCP CoS マッピング 329
CoS カラーマッピング 329
DSCP カラーマッピング 330
クラスマップ 330
集約ポリサー 332
ポリシーマップ 334
ポリシーバインディング 336
QoS PFC 337
ネットワーク QoS クラスマップ 337
ネットワーク QoS ポリシーマップ 338
ネットワーク QoS ポリシーバインディング 339
PFC ポート設定 339
WRED 340
WRED プロファイル 340
WRED キュー 341

第 11 章　ACL 342

ACL コンフィグレーションウィザード 343
ACL コンフィグレーションウィザード 343
パケットタイプ選択（ACL コンフィグレーションウィザード） 344
ルール追加（ACL コンフィグレーションウィザード） 344
ポート設定（ACL コンフィグレーションウィザード） 352
ACL アクセスリスト 353
標準 IP ACL 354
拡張 IP ACL 355
標準 IPv6 ACL 357
拡張 IPv6 ACL 358
拡張 MAC ACL 360
拡張 Expert ACL 361
ACL インタフェースアクセスグループ 364
ACL VLAN アクセスマップ 365
アクセスリスト合致 365
ACL VLAN フィルタ 366
CPU ACL 367

第 12 章　セキュリティ 369

ポートセキュリティ 370
ポートセキュリティグローバル設定 370
ポートセキュリティポート設定 371
ポートセキュリティアドレスエントリ 372
802.1X 373
802.1X グローバル設定 377

802.1X ポート設定 377
認証セッション情報 378
オーセンティケータ統計 378
オーセンティケータセッション統計 379
オーセンティケータ診断 379
AAA 380
AAA グローバル設定 380
アプリケーション認証設定 380
アプリケーションアカウンティング設定 381
認証設定 382
アカウンティング設定 383
RADIUS サーバダイナミックオーサー設定 384
RADIUS 385
RADIUS グローバル設定 385
RADIUS サーバ設定 386
RADIUS グループサーバ設定 386
RADIUS 統計 387
TACACS+ 388
TACACS+ グローバル設定 388
TACACS+ サーバ設定 389
TACACS+ グループサーバ設定 389
TACACS+ 統計 390
IMPB 391
IPv4 391
IPv6 400
DHCP サーバスクリーニング 407
DHCP サーバ スクリーニンググローバル設定 407
DHCP サーバ スクリーニングポート設定 408
ARP スプーフィング防止 409
BPDU アタック防止 410
NetBIOS フィルタリング 411
MAC 認証 412
Web アクセスコントロール 413
Web 認証 415
WAC ポート設定 416
WAC カスタマイズページ 416
ネットワークアクセス認証 417
ゲスト VLAN 417
ネットワークアクセス認証グローバル設定 417
ネットワークアクセス認証ポート設定 419
ネットワークアクセス認証セッション情報 420
セーフガードエンジン 421
セーフガードエンジン設定 422
CPU プロテクトカウンタ 422
CPU プロテクトサブインタフェース 423
CPU プロテクトタイプ 423
トラスト ホスト 424
トラフィック セグメンテーション 424
ストーム制御設定 425
DoS 攻撃防御設定 427
ゾーンディフェンス設定 428
SSH 428
SSH グローバル設定 429
ホスト鍵 429
SSH サーバ 接続 430
SSH ユーザ 設定 430
SSH クライアント 設定 431
SSL 432
SSL グローバル設定 433
暗号化 PKI トラストポイント 434
SSL サービスポリシー 435
SFTP サーバ設定 436
ネットワークプロトコルポートプロテクション設定 436

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守) 437

ケーブル診断 438
DDM 439
DDM 設定（DDM 設定）..... 439
DDM 温度閾値設定 440
DDM 電圧閾値設定 440
DDM バイアス電流閾値設定 441
DDM TX パワー閾値設定 441
DDM RX パワー 閾値設定 442
DDM ステータステーブル 442

第 14 章　モニタリング 443

VLAN カウンタ 444
利用率 445
ポート利用率 445
履歴利用率 446
統計 447
ポート 447
CPU ポート 448
インタフェースカウンタ 449
インタフェース履歴カウンタ 450
カウンタ 451
ミラー設定 452
sFlow 453
sFlow エージェント情報 453
sFlow レシーバ設定 453
sFlow サンプラ設定 454
sFLow ポーラー設定 454
デバイス環境 455

第 15 章　Green（省電力機能） 456

省電力 457
EEE 458

第 16 章　保存メニュー / ツールメニュー 459

保存 460
コンフィグレーションの保存 460
ツール 460
ファームウェアアップグレード＆バックアップ 460
設定リストアおよびバックアップ 464
証明書およびキーリストアおよびバックアップ 468
ログバックアップ 471
Ping 473
トレースルート 474
言語管理 475
リセット 476
システム再起動 476

付録 477

付録 A パスワードリカバリ手順 477
付録 B システムログエントリ 478
付録 C トラップログエントリ 502
付録 D RADIUS 属性割り当て 513
付録 E IETF RADIUS 属性サポート 517
付録 F ERPS 情報 519
付録 G 機能設定例 520
対象機器について 520
Traffic Segmentation（トラフィックセグメンテーション）..... 520
VLAN 521
Link Aggregation（リンクアグリゲーション）..... 522
Access List（アクセスリスト）..... 524
Loopback Detection（LBD）（ループ検知）..... 525

はじめに

DGS-1520 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

- 第 1 章　本製品のご使用にあたって
  - 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。
- 第 2 章　スイッチの設置
  - システムの基本的な設置方法について説明します。また、本スイッチの電源接続の方法についても紹介します。
- 第 3 章　スイッチの接続
  - スイッチをご使用のネットワークに接続する方法を説明します。
- 第 4 章　スイッチ管理について
  - パスワード設定、SNMP 設定、および各種デバイスからの本スイッチへの接続など基本的なスイッチの管理について説明します。
- 第 5 章　Web ベースのスイッチ管理
  - Web ベースの管理機能への接続方法および使用方法について説明します。
- 第 6 章　システム
  - デバイス情報、ポート設定、ユーザアカウント、システムログ設定、時刻設定などの基本機能の設定について説明します。
- 第 7 章　管理
  - シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。
- 第 8 章　L2 機能
  - VLAN、トランキング、スパニングツリー、LLDP などのレイヤ 2 機能について説明します。
- 第 9 章　L3 機能
  - ARP 設定、インタフェース設定、ルート再配布設定、スタティック / ダイナミックルート設定、ルート優先度設定、RIP、OSPF、VRRP、IP マルチキャストルーティングプロトコルなどのレイヤ 3 機能について説明します。
- 第 10 章　QoS
  - QoS 機能について説明します。帯域制御、QoS スケジューリング、802.1p デフォルトプライオリティ、802.1p ユーザプライオリティなどの機能を含みます。
- 第 11 章　ACL
  - ACL アクセスリスト、ACL VLAN アクセスマップ、CPU ACL などの ACL（アクセスコントロールリスト）機能について説明します。
- 第 12 章　セキュリティ
  - 802.1X、トラストホスト、アクセス認証コントロール、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC- ポートバインディング、IP マルチキャスト範囲の制限、Web 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およびセーフガードエンジンなどのセキュリティ機能について説明します。
- 第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)
  - DDM、ケーブル診断機能について説明します。
- 第 14 章　モニタリング
  - CPU 使用率、パケット統計情報、エラー、パケットサイズ、ミラーリング、sFlow などのモニタ機能について説明します。
- 第 15 章　Green（省電力機能）
  - Power Saving（省電力）、EEE（Energy Efficient Ethernet/ 省電力イーサネット）について説明します。
- 第 16 章　保存メニュー / ツールメニュー
  - コンフィグレーションの保存、ファームウェアアップグレード＆バックアップ、コンフィグレーションリストア＆バックアップ、ログファイルのバックアップ、Ping、トレースルート、リセット、システム再起動について説明します。

● 付録

- 付録 A パスワードリカバリ手順
  - パスワードのリセット、リカバリについて説明します。
- 付録 B システムログエントリ
  - スイッチのシステムログに表示される可能性のあるログイベントについて説明します。
- 付録 C トラップログエントリ
  - トラップログエントリついて説明します。
- 付録 D RADIUS 属性割り当て
  - スイッチの RADIUS 属性割り当てについて説明します。
- 付録 E IETF RADIUS 属性サポート
  - 現在スイッチによりサポートされる IETF RADIUS 属性一覧です。
- 付録 F ERPS 情報
  - ERPS 情報についてサポートします。
- 付録 G 機能設定例
  - スイッチの機能設定例です。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に "（13 ページ）をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	`(switch-prompt)#`
courier 太字	コマンド、ユーザによるコマンドライン入力。	**`show network`**
courier 斜体	コマンドパラメータ（可変または固定）。	*value*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*value*>
[ ]	任意の固定パラメータ。	[*value*]
[< >]	任意の可変パラメータ。	[<*value*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*choice1* | *choice2*}
|（垂直線）	相互排他的なパラメータ。	*choice1* | *choice2*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*choice1* | *choice2*}]

製品名 / 品番一覧

製品名	HW バージョン	品番
DGS-1520-28	**A1**	DGS-1520-28/A1
DGS-1520-52	**A1**	DGS-1520-52/A1
DGS-1520-28MP	**A1**	DGS-1520-28MP/A1
DGS-1520-52MP	**A1**	DGS-1520-52MP/A1

第 1 章　本製品のご使用にあたって

- DGS-1520 シリーズについて
- ポート
- SFP
- オプション製品
- 前面パネル
- 背面パネル
- 側面パネル

DGS-1520 シリーズについて

DGS-1520 シリーズは、SMB からエンタープライズ向けの中規模ネットワークにおいて柔軟性、冗長性、セキュリティを実現し、安定したパフォーマンスでネットワーク通信を提供することが可能なギガビットレイヤ 3 スマートマネージドスイッチです。

本シリーズは、DGS-1520-28、DGS-1520-52 に加え、2.5G 対応の給電ポートを搭載した DGS-1520-28MP、DGS-DGS-1520-52MP の 4 製品で構成されています。全ての製品に 10G SFP+ スロットが 2 つ搭載されており、物理スタック /10G アップリンクとして利用が可能です。

本マニュアルでは、DGS-1520 シリーズの設置、管理および設定の方法について記述しています。
本シリーズは機能設定やハードウェア構成は一部機能を除き同じであるため、本マニュアルの情報をすべての種類にほぼ適用できます。
Web による管理画面例には、DGS-1520 シリーズのいずれかの機種のものを記載します。一部機能、ポート数を除き設定内容はほぼ同じです。

ポート

DGS-1520 シリーズは以下の製品で構成されるギガビットレイヤ 3 スタッカブルスマートマネージドスイッチです。

以下のポートを搭載しています。

製品名	DGS-1520-28	DGS-1520-28MP	DGS-1520-52	DGS-1520-52MP
10/100/1000 BASE-T ポート (RJ-45)	24	—	48	—
10/100/1000 BASE-T PoE 給電ポート (RJ-45)	—	20	—	44
100/1000/2.5G BASE-T PoE 給電ポート (RJ-45)	—	4	—	4
1000/10G BASE-T ポート (RJ-45)	2	2	2	2
10G SFP+ スロット	2	2	2	2
コンソールポート (RJ-45)	1	1	1	1
管理ポート (MGMT) (RJ-45)	1	—	1	—

SFP

DGS-1520 シリーズは、前面パネルの SFP+ スロットで以下の光トランシーバを使用できます。

■ SFP+ モジュール

光トランシーバ

種別	製品名
SFP+（10Giga）	DEM-431XT
	DEM-432XT
Copper SFP+（10Giga）	DEM-410T※1※2
WDM 対応 1 芯 SFP（1Giga）	DEM-330T
	DEM-330R
	DEM-331T
	DEM-331R
2 芯 SFP（1Giga）	DEM-310GT
	DEM-311GT
	DEM-312GT2
	DEM-314GT
Copper SFP（1Giga）	DGS-712

※1 DEM-410T を使用する場合、環境温度（室温）が 40℃までの環境での利用のみをサポートします。そのため、この場合のスイッチの動作温度範囲も 0~40℃までとなりますので、十分にご注意ください。

※2 DEM-410T の取り付けは、スイッチ 1 台に対し最大 2 個までとなります。

※ スイッチ /SFP モジュールのハードウェアバージョンの組み合わせによっては、接続できない場合があります。サポートされる SFP モジュールのハードウェア バージョンについては、弊社 Web ページで公開されている「光トランシーバ対応製品一覧」をご確認ください。

オプション製品

DGS-1520 シリーズは、以下のリダンダント電源とダイレクトアタッチケーブルを使用できます。

■ リダンダント電源

種別	製品名
リダンダント電源システム	DPS-520※1
	DPS-700※2※3

※1 DPS-520 は、DGS-1520-28/52 でのみ使用できます。

※2 DPS-700 は、DGS-1520-28MP/52MP でのみ使用できます。

※3 DPS-700 のハードウェアバージョン：A2/B1 のみサポートされます。（B1 はリリース予定）

■ ダイレクトアタッチケーブル

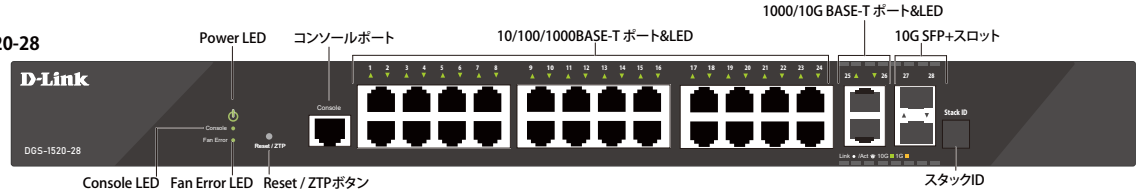
種別	製品名
SFP+ ダイレクトアタッチケーブル	DEM-CB100S
	DEM-CB300S
	DEM-CB700S

前面パネル

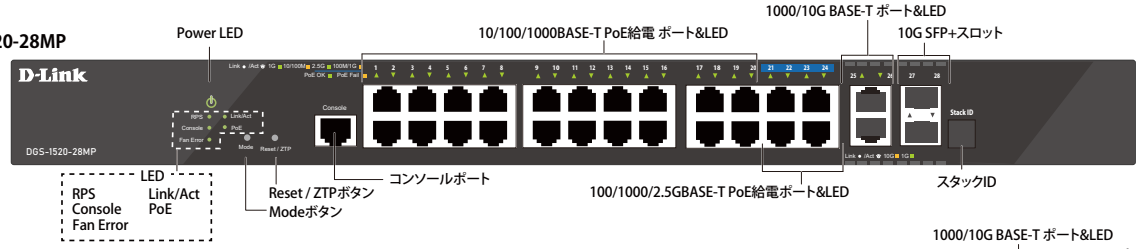
DGS-1520 シリーズの前面パネルについて説明します。

前面

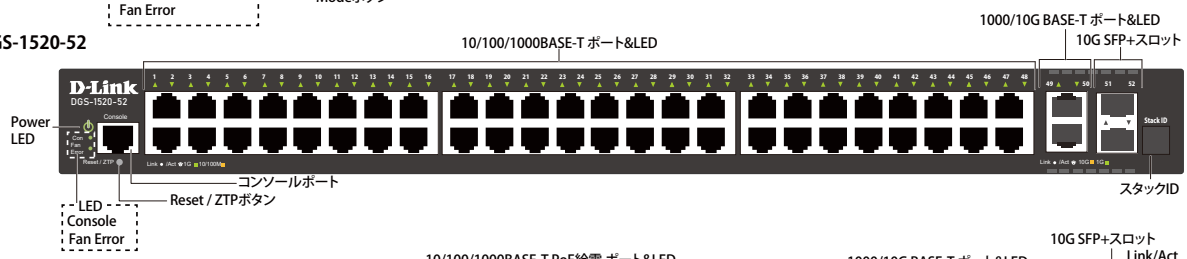
DGS-1520-28



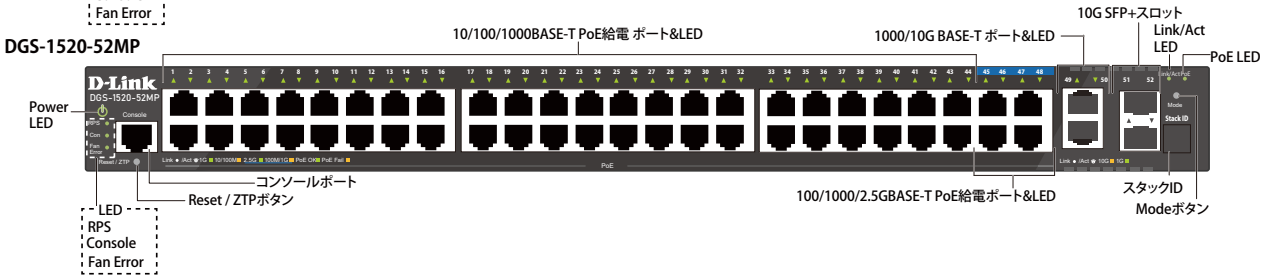
DGS-1520-28MP



DGS-1520-52



DGS-1520-52MP



Reset/ZTP（リセット / ゼロタッチプロビジョニングボタン）

スイッチの前面パネルには Reset/ZTP（リセット / ゼロタッチプロビジョニングボタン）があります。
再起動や設定のリセット、ゼロタッチプロビジョニング（ZTP：Zero Touch Provisioning）を実行できます。

DGS-1520 シリーズをネットワークに追加した際、ZTP ボタンを押すことで IP アドレスを DHCP サーバから自動的に取得し、TFTP サーバからファームウェアとコンフィグを取得することができます。※

※ DHCP サーバおよび TFTP サーバ側での設定を行う必要があります。

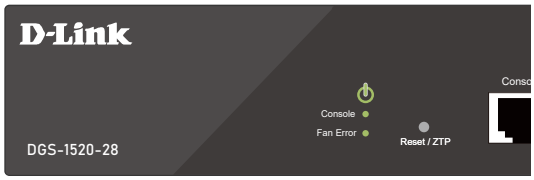


図 3-1　DGS-1520-28 Reset/ZTP ボタン

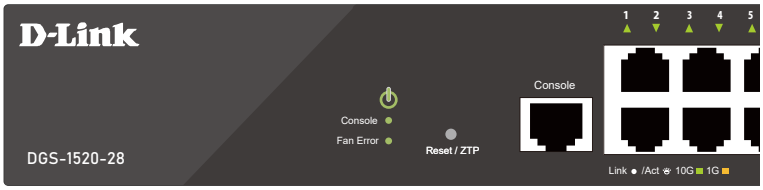
■ 再起動と設定のリセット方法

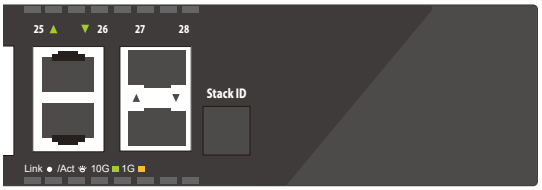
- リセットボタンを 5 秒未満押下する：スイッチは再起動します。保存していない設定は破棄されます。
- リセットボタンを 5 -10 秒押下する：スイッチは ZTP 機能を使用して再起動します。保存していない設定は破棄されます。
- リセットボタンを 10 秒以上押下する：スイッチの設定内容を工場出荷値へリセットします。

LED 表示

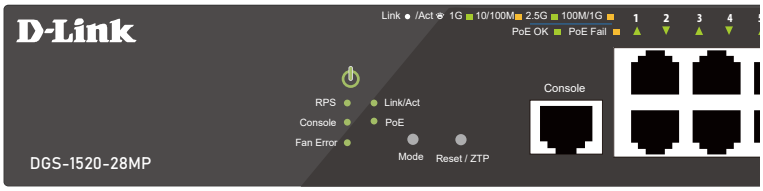
前面パネルの LED 表示について説明します。

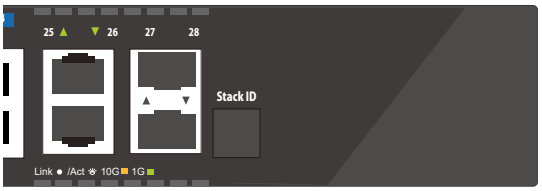
DGS-1520-28



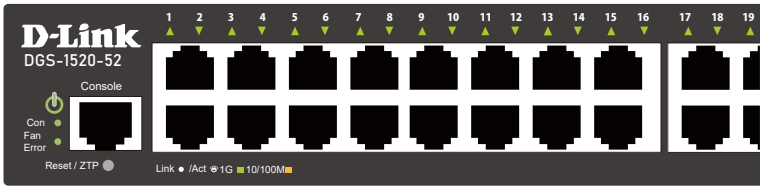


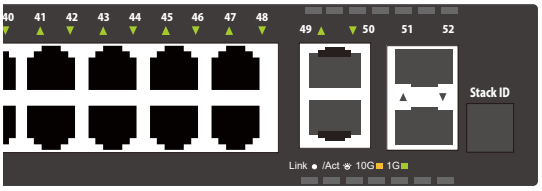
DGS-1520-28MP



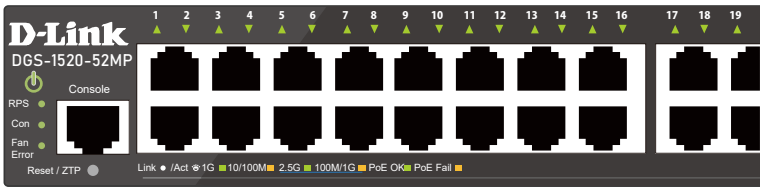


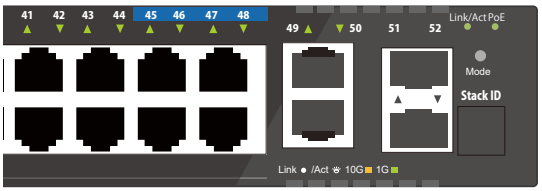
DGS-1520-52





DGS-1520-52MP





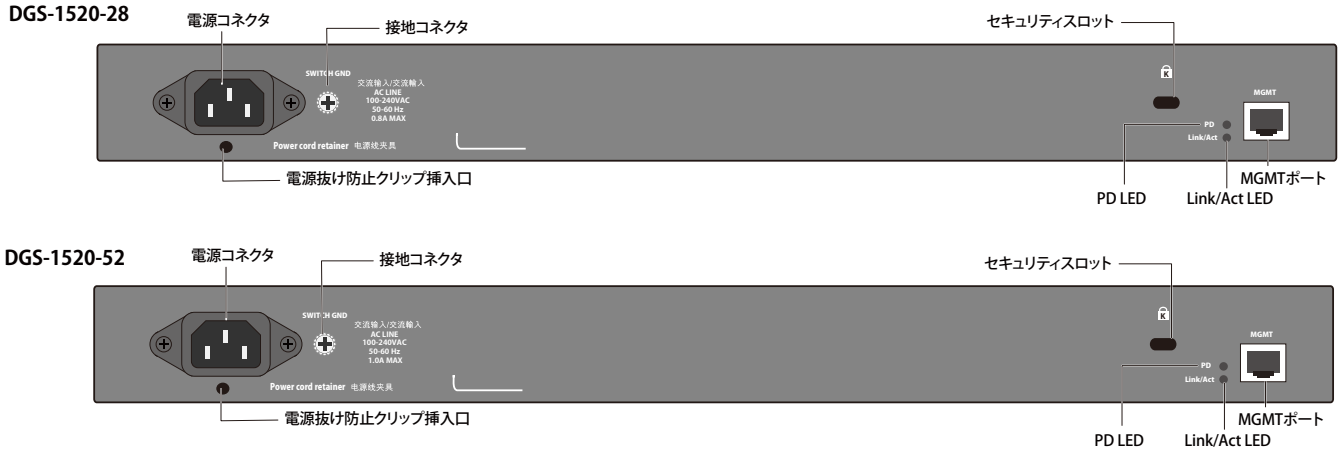
以下の表に LED の状態が意味するスイッチの状態を示します。

LED	色	状態	状態説明
Mode ボタン& LED（DGS-1520-28MP/52MP のみ）（PoE モード、Link/Act モードへの切り替え）			
PoE	緑	点灯	ポート LED は各ポートの PoE の状態について表示します。
Link/Act	緑	点灯	ポート LED は各ポートの Link/Act/Speed の状態について表示します。
システム LED			
Power	緑	点灯	スイッチに電源が供給され正常に動作しています。
	緑	点滅	システムセルフテスト中です。
	ー	消灯	スイッチに電源が供給されていません。
RPS	緑	点灯	リダンダント電源ユニットが動作しています。
	ー	消灯	リダンダント電源ユニットは動作していません。
Console	緑	点灯	RJ-45 コンソールポートのリンクが確立しています。
	ー	消灯	リンクが確立していません。
Fan Err	赤	点灯	ファンに不具合が発生しています。
	緑	点灯	ファンは正常に動作しています。
Link/Act Mode（DGS-1520-28MP/52MP のみ）	緑	点灯	Link/Act/Speed モードで動作しています。
	ー	消灯	PoE モードで動作しています。
PoE Mode（DGS-1520-28MP/52MP のみ）	緑	点灯	PoE モードで動作しています。
	ー	消灯	Link/Act/Speed モードで動作しています。
Stack ID	緑	点灯（1-8）	スイッチスタックにおけるスイッチのボックス番号が表示されます。
		点灯（H）	スイッチがスイッチスタックのプライマリマスタである場合、大文字の「H」の文字が表示されます。
		点灯（h）	スイッチがスイッチスタックのバックアップマスタの場合は、小文字の「h」が表示されます。
		点灯（E）	システムによるセルフテストエラーです。
		点灯（G）	セーフガードエンジンが「exhausted」モードに入っています。
RJ-45 ポート LED			
Link/Act (1G、10/100M)	緑	点灯	1Gbps でリンクが確立しています。
		点滅	1Gbps でデータを送受信しています。
	橙	点灯	10/100Mbps でリンクが確立しています。
		点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
Link/Act (2.5G、100M/1G)（DGS-1520-28MP/52MP のみ）	緑	点灯	2.5Gbps でリンクが確立しています。
		点滅	2.5Gbps でデータを送受信しています。
	橙	点灯	100Mbps または 1Gbps でリンクが確立しています。
		点滅	100Mbps または 1Gbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
Link/Act (10G、1G)	緑	点灯	10Gbps でリンクが確立しています。
		点滅	10Gbps でデータを送受信しています。
	橙	点灯	1Gbps でリンクが確立しています。
		点滅	1Gbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
PoE OK/Fail（DGS-1520-28MP/52MP のみ）	緑	点灯	接続中の PoE 受電機器に給電中です。
	橙	点灯	PoE ポートにエラーが発生しました。
	ー	消灯	給電をしていません。
SFP+ スロット LED			
Link/ACT	緑	点灯	10Gbps でリンクが確立しています。
		点滅	10Gbps でデータを送受信しています。
	橙	点灯	1Gbps でリンクが確立しています。
		点滅	1Gbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

背面パネル

背面パネルの各部名称について説明します。

DGS-1520-28/52 の背面パネル



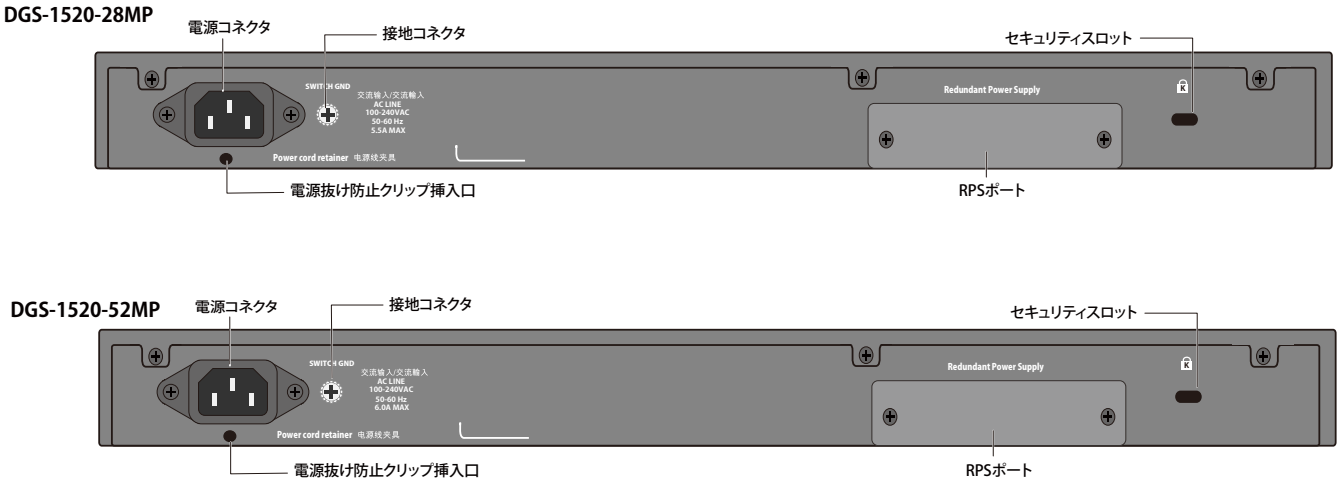
DGS-1520-28/52 の背面パネルには以下が配備されています。

- 電源コネクタ：付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 - 240VAC 内の電圧に調整されます。
- 電源抜け防止クリップ挿入口：電源抜け防止クリップを接続します。
- 接地コネクタ：アース線を接続します。
- 管理（MGMT）ポート：
  10/100/1000 Mbps で動作する、Telnet/Web/SNMP 用の管理ポートです。
  このポートを使用し、ネットワークに接続せずにスイッチを設定できます。
  MGMT ポートは、Power over HDBaseT を使用して 90W DC 電力をスイッチに供給するためにも使用できます。これは、スイッチの主電源または副電源として使用できます。

背面パネル LED 表示

LED	色	状態	状態説明
Link/Act	緑	点灯	MGMT ポートにて 1Gbps でリンクが確立しています。
		点滅	MGMT ポートにて 1Gbps でデータを送受信しています。
	橙	点灯	MGMT ポートにて 10/100Mbps でリンクが確立しています。
		点滅	MGMT ポートにて 10/100Mbps でデータを送受信しています。
	ー	消灯	MGMT ポートにてリンクが確立していません。
PD LED	緑	点灯	MGMT ポートに接続された給電デバイスから DC 電源が供給されています。
	橙	点灯	通常の MGMT 接続を行っています。給電デバイスは MGMT ポートに接続されていません。給電デバイスを接続しても PD LED が橙色に点灯する場合は、給電に失敗しています。
	ー	消灯	MGMT ポートで通常の接続および給電デバイスの接続が行われていません。

DGS-1520-28MP/52MP の背面パネル



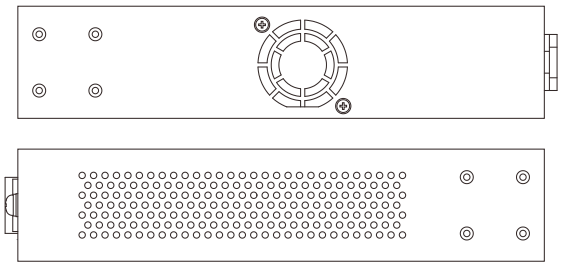
DGS-1520-28MP/52MP の背面パネルには以下が配備されています。

- 電源コネクタ：付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 - 240VAC 内の電圧に調整されます。
- 電源抜け防止クリップ挿入口：電源抜け防止クリップを接続します。
- 接地コネクタ：アース線を接続します。
- RPS ポート：
  オプションのリダンダント電源ユニットを接続します。内蔵電源ユニットに異常が発生した場合に外部リダンダント電源ユニット（オプション）が自動的にスイッチに電源を供給します。

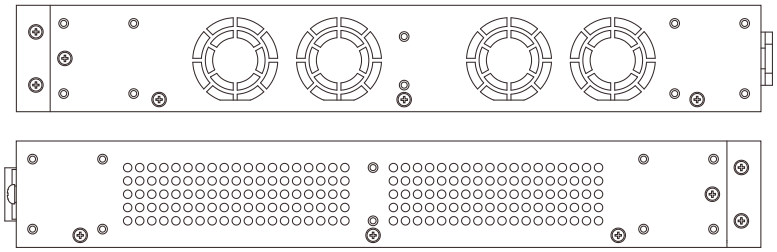
側面パネル

側面パネルには、通気口、ファン、ラック取り付けネジ穴などがあります。
側面パネルにある通気口には、スイッチが持つ熱を放出する役割があります。通気口をふさがないようにご注意ください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

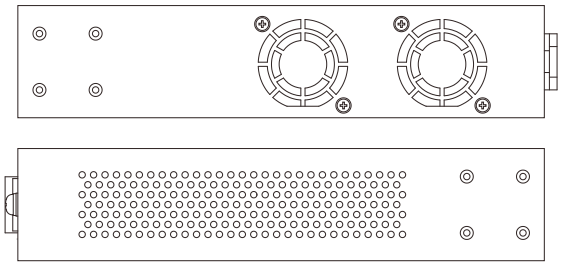
DGS-1520-28



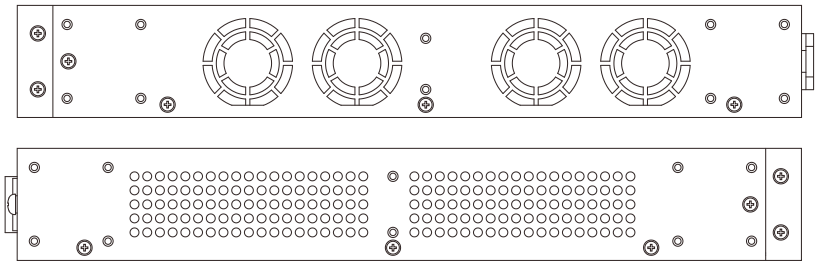
DGS-1520-28MP



DGS-1520-52



DGS-1520-52MP



スマートファンについて

DGS-1520 はハードウェアに内蔵されたセンサによってスイッチ内部の温度を検出し、自動的にファンのスピードを調整する「スマートファン」を搭載しています。スピードには「低スピード回転」「中スピード回転」「高スピード回転」の 3 つの状態があります。
以下が各機種のスマートファンによるスピード調整の基準になります。

- （温度上昇時）内部温度が 33℃より高温になった場合、ファンは「低スピード回転」から「中スピード回転」に移行します。
- （温度上昇時）内部温度が 40℃より高温になった場合、ファンは「中スピード回転」から「高スピード回転」に移行します。
  ※ファンが「低スピード回転」の時は 33℃を上回るまで「低スピード回転」の状態を維持し、「中スピード回転」の時は 40℃を上回るまで「中スピード回転」の状態を維持します。

- （温度下降時）内部温度が 37℃より低温になった場合、ファンは「高スピード回転」から「中スピード回転」に移行します。
- （温度下降時）内部温度が 30℃より低温になった場合、ファンは「中スピード回転」から「低スピード回転」に移行します。
  ※ファンが「高スピード回転」の時は 37℃を下回るまで「高スピード回転」の状態を維持し、「中スピード回転」の時は 30℃を下回るまで「中スピード回転」の状態を維持します。

第 2 章　スイッチの設置

- パッケージの内容
- ネットワーク接続前の準備
- ゴム足の取り付け (19 インチラックに設置しない場合)
- 19 インチラックへの取り付け
- 光トランシーバの接続
- 電源抜け防止クリップの装着
- MGMT ポートに DPS-520 を接続する
- RPS ポートに DPS-700 を接続する
- 電源の投入

パッケージの内容

ご購入いただいたスイッチの梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- 本体　x　1
- 電源ケーブル　x　1
- RJ-45/RS232C コンソールケーブル　x　1
- 19 インチラックマウントキット
- ゴム足　x　4
- 電源抜け防止クリップ　x　1
- マニュアル　x　1
- PL シート　x　1

万一、不足しているもの損傷を受けているものがありましたら、ご購入頂いた販売代理店までご連絡ください。

ネットワーク接続前の準備

スイッチの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

- スイッチは、しっかりとした水平面で耐荷重性のある場所に設置してください。また、スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかり差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と充分な換気ができることを確認してください。換気のためには少なくとも製品の前後 10 cm 以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- スイッチは強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

ゴム足の取り付け (19 インチラックに設置しない場合)

机や棚の上に設置する場合は、まずスイッチに同梱されていたゴム製足をスイッチの裏面の四隅に取り付けます。スイッチの周囲に十分な通気を確保するようにしてください。

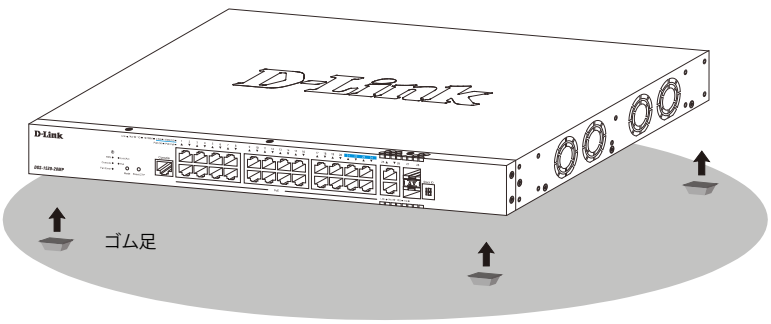


図 2-1　ゴム足の取り付け

19 インチラックへの取り付け

警告 前面、側面にスタビライザを取り付けないで製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム / コンポーネントを取り付けた後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つだけとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

注意 スイッチをラックに固定するネジは付属品には含まれません。別途ご用意ください。

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

1. 電源ケーブルおよびケーブル類が本体、拡張モジュールに接続していないことを確認します。
2. 付属のネジで、スイッチの両側側面にブラケットを取り付けます。

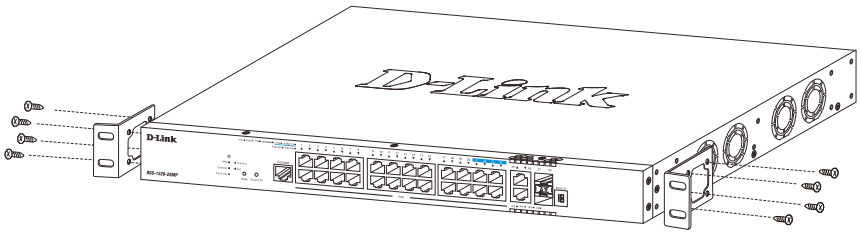


図 2-2　スイッチへのブラケットの取り付け図

3. 完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の 19 インチラックに固定します。

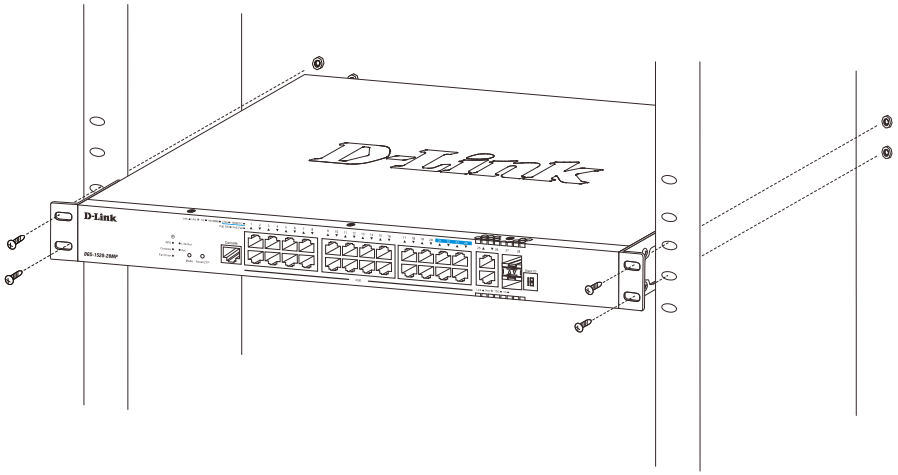


図 2-3　スイッチのラックへの設置図

光トランシーバの接続

スイッチの前面パネルには SFP + スロットがあり、光トランシーバを接続できます。

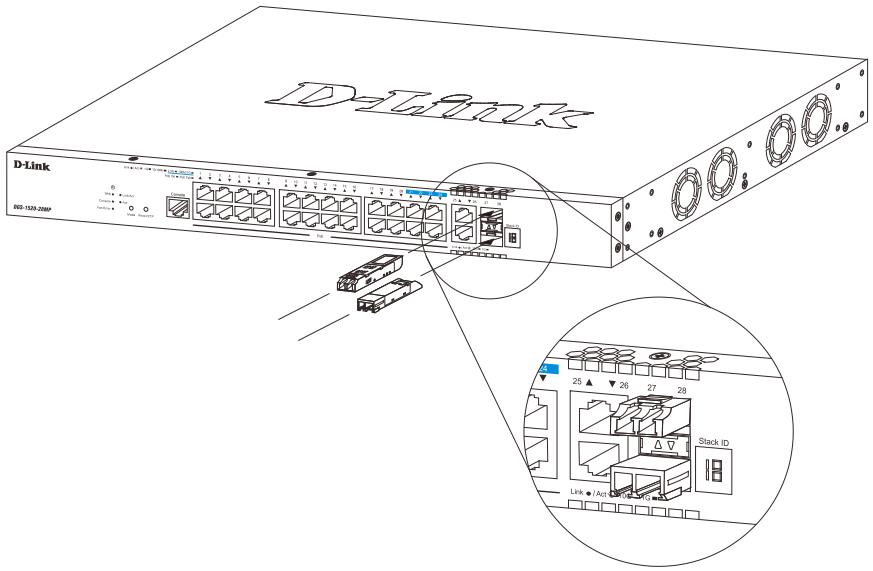


図 2-4　SFP+ スロットに光トランシーバを挿入

電源抜け防止クリップの装着

アクシデントにより AC 電源コードが抜けてしまうことを防止するために、スイッチに電源抜け防止クリップを装着します。
以下の手順に従って電源抜け防止クリップを装着します。

1. スイッチの背面の電源プラグの下にある穴に、付属の電源抜け防止クリップのタイラップ（挿し込み先のあるバンド）を下記の図のように差し込みます。

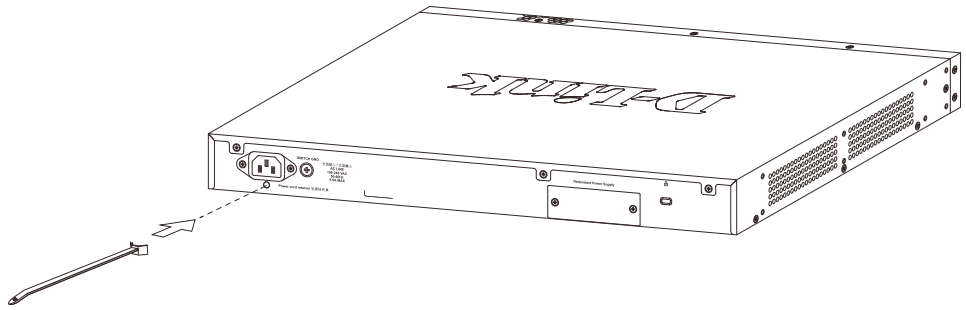


図 2-5　タイラップの挿し込み

2. AC 電源コードをスイッチの電源プラグに挿し込みます。

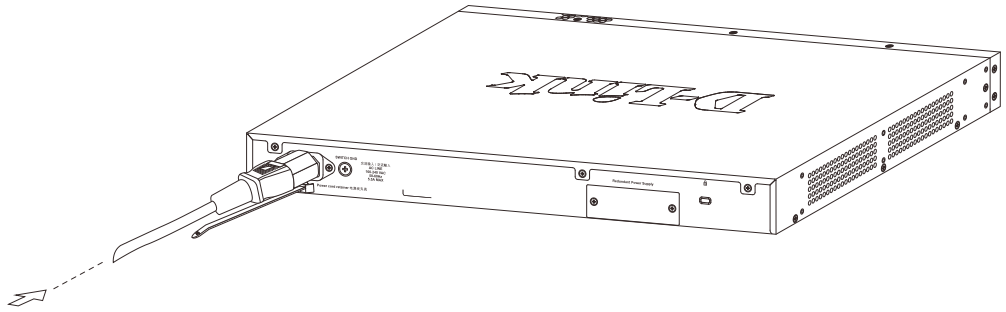


図 2-6　電源コード挿し込み

3. 以下の図のように挿し込んだタイラップにリテイナー（固定具）をスライドさせ装着します。

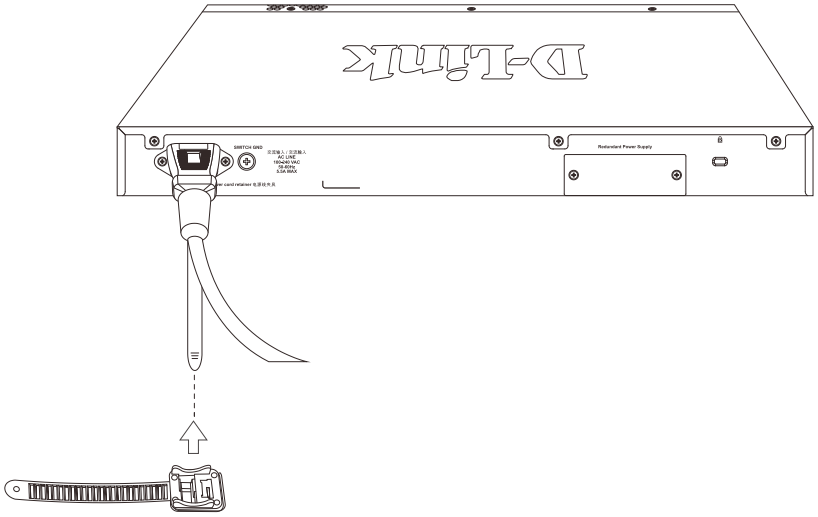


図 2-7　リテイナー（固定具）のスライド

4. 以下の図のようにリテイナーを電源コードに巻き付け、リテイナーのロック部分に挿し込みます。

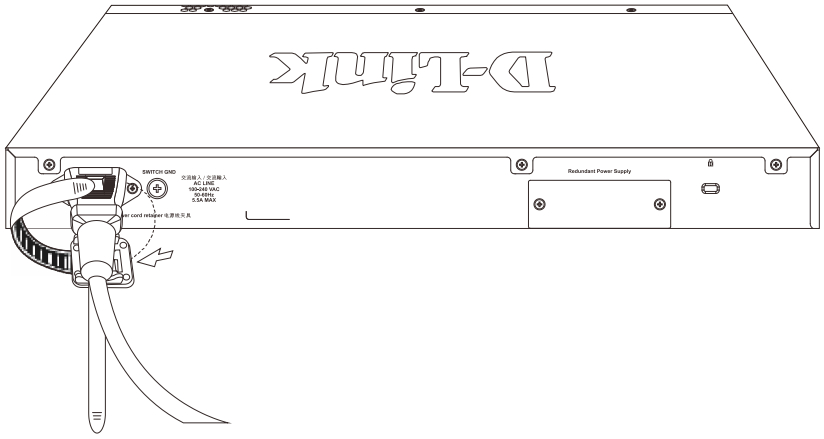


図 2-8　リテイナーの巻き付け、固定

5. リテイナーを電源コードにしっかりと巻き付けた後、電源コードが抜けないか確かめます。

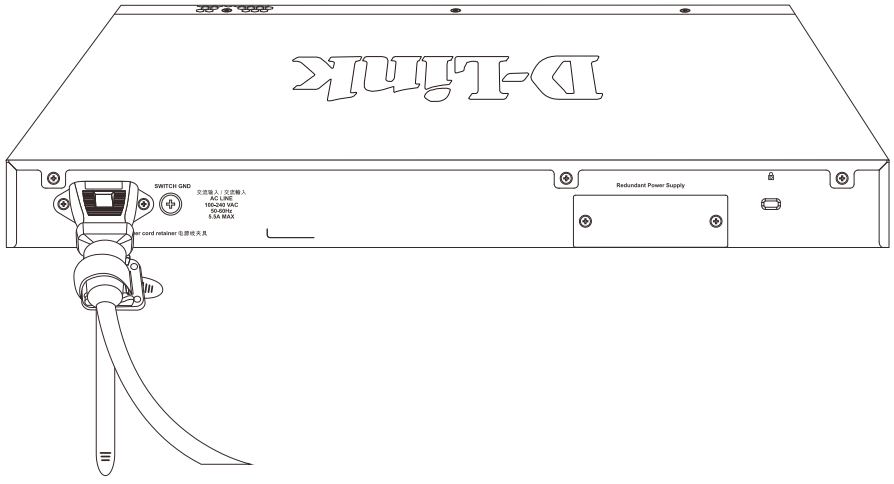


図 2-9　電源抜け防止クリップの固定確認

MGMT ポートに DPS-520 を接続する

DGS-1520-28/52 では、MGMT ポートに DPS-520（RPS/ リダンダントパワーサプライ) を接続し、PoH（Power over HDBaseT）を使用して最大 90W の DC 電力を供給することができます。DPS-520 の MGMT ポートへの接続にはカテゴリ 5e/6a の LAN ケーブルを使用します。

AC 電源を使用している場合は DPS-520 をバックアップ電源として使用できます。AC 電源から電力を供給できなくなった場合に、DPS-520 が DGS-1520-28/52 に電力を供給します。

注意　背面パネルに MGMT ポートがあるのは DGS-1520-28 と DGS-1520-52 のみです。

注意　LAN ケーブルを MGMT ポートに接続する前に、RPS を AC 電源に接続しないでください。内部電源が破損する恐れがあります。

DPS-520 を MGMT ポートに接続する図は以下のとおりです。

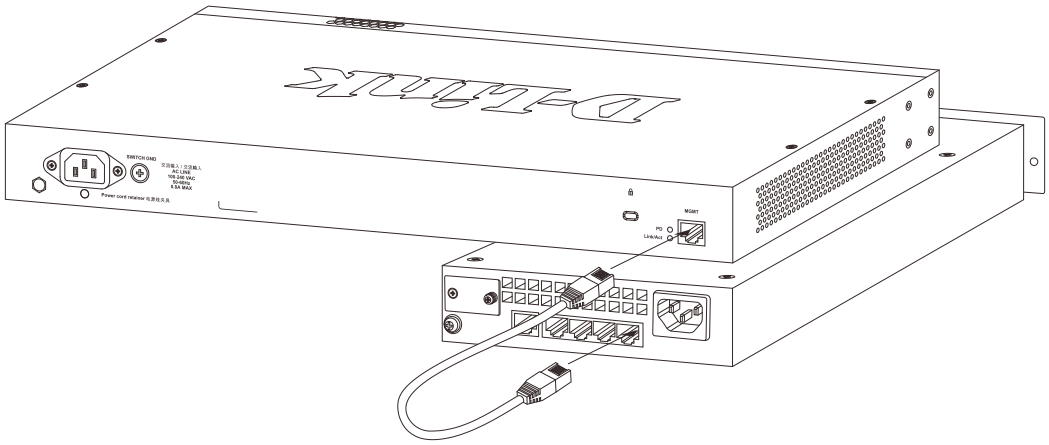


図 2-10　DGS-1520-28/52 と DPS-520 の接続

注意　ケーブルの損傷を防ぐため、DPS-520 を取り付ける場合はスイッチの後ろに 15cm 以上のスペースを確保してください。

RPS ポートに DPS-700 を接続する

DGS-1520-28MP/52MP の背面パネルには DPS-700（RPS/ リダンダントパワーサプライ) を接続できる RPS ポートがあります。RPS は、スイッチの予測できない電源故障によってスイッチを含むネットワークシステム全体がシャットダウンすることなどを回避し、安定した電源供給を提供します。

注意　背面パネルに RPS ポートがあるのは DGS-1520-28MP と DGS-1520-52MP のみです。

注意　DC 電源ケーブルを接続する前に、DPS-700 を AC 電源に接続しないでください。内蔵電源が破損するおそれがあります。

1. DPS-700 はホットスワップに対応していないため、スイッチの AC 電源コネクタから AC 電源ケーブルを取り外します。
2. プラスドライバーを使用し、RPS ポートのカバーを固定しているネジ 2 つを取り外します。

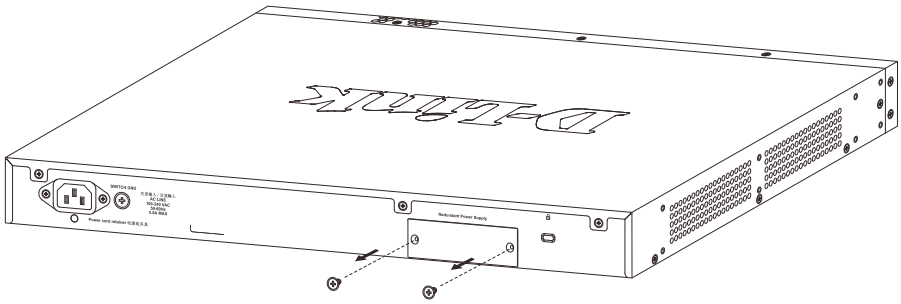


図 2-11　RPS ポートカバーの取り外し

3. 22 ピンの DC 電源ケーブルの一端をスイッチの RPS ポートに挿入し、もう片方を DPS-700 に挿入します。

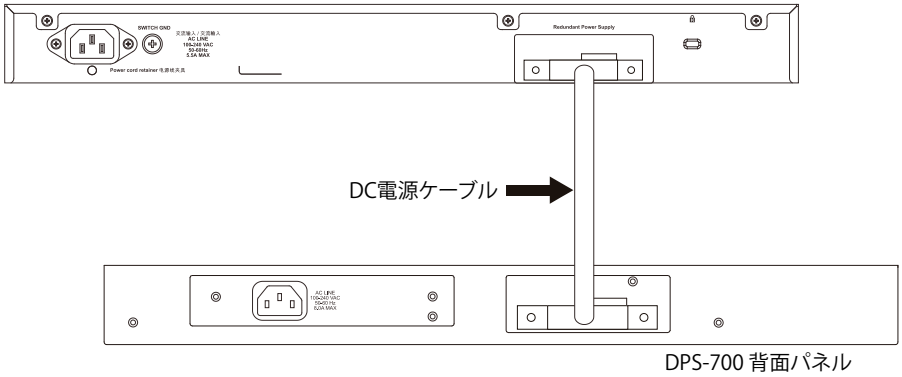


図 2-12　DPS-700 の接続

4. DPS-700 を AC 電源に接続します。接続に成功すると、DPS-700 の前面パネルにある緑色の LED が点灯します。
5. AC 電源ケーブルを DGS-1520-28MP/52MP の電源コネクタに再度接続します。

DGS-1520-28MP/52MP の前面パネルにある RPS LED は、DPS-700 の動作状況を示します。
本手順の実行による設定変更は必要ありません。

注意　ケーブルの損傷を防ぐため、DPS-700 を取り付ける場合はスイッチの後ろに 15cm 以上のスペースを確保してください。

DGS-1520-28MP/52MP に DPS-700 を接続しない場合は、RPS ポートのカバーを取り付けたままにしてください。

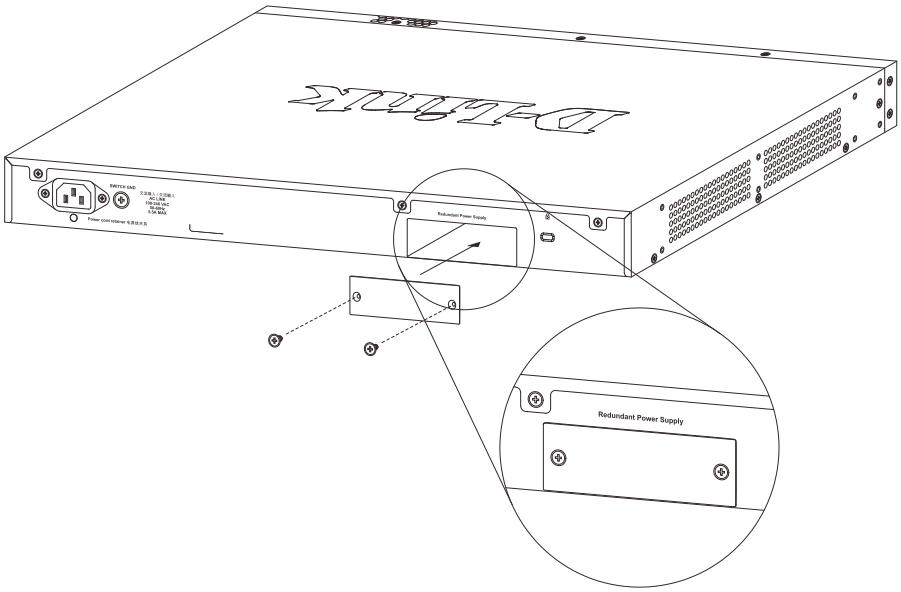


図 2-13　RPS ポートカバーの装着

電源の投入

1. 電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
2. 本スイッチに電源が供給されると、Power LED が点灯します。システムのリセット中、LED は点滅します。

電源の異常

万一停電などの電源異常が発生する / した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

第 3 章　スイッチの接続

- エンドノードと接続する
- ハブまたはスイッチと接続する
- バックボーンまたはサーバと接続する

注意　すべてのポートは Auto MDI/MDI-X 接続をサポートしています。

エンドノードと接続する

UTP ケーブルを使用して DGS-1520 シリーズとエンドノードを接続します。エンドノードとは、RJ45 ネットワークポートを装備した PC やルータの総称です。接続が正常に確立されると、対応するポートライトが点灯・点滅し、そのポートでデータの送受信が行われていることを示します。

下図は、本装置に接続されている一般的なエンドノードを示しています。

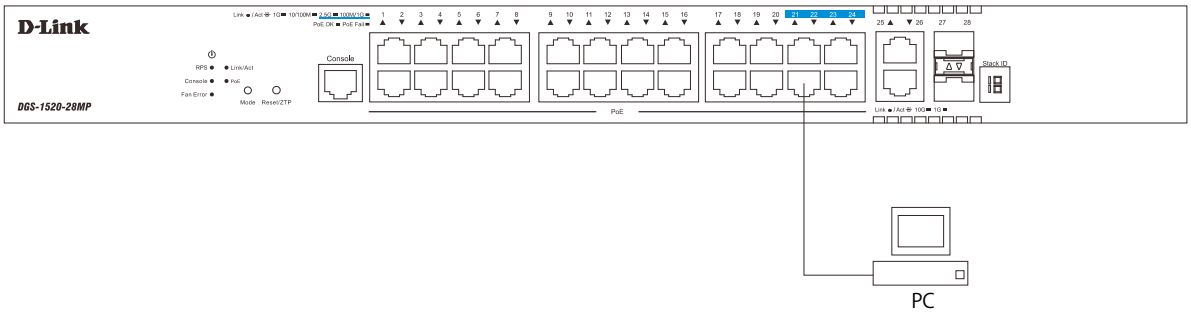


図 3-1　エンドノードと接続した図

エンドノードと正しくリンクが確立すると本スイッチの各ポートの Link/Act LED は緑または橙に点灯します。データの送受信中は点滅します。

ハブまたはスイッチと接続する

DGS-1520 シリーズは、ネットワーク内の他の任意のスイッチやハブに接続するために使用できます。
このネットワークトポロジは、ネットワーク内のすべてのエンドノードに対応するのに十分なポートがスイッチにない場合に使用されます。

使用するケーブルによって以下のように接続します。
- カテゴリ 3/4/5 の UTP/STP ケーブル : 10BASE-T または 100BASE-TX スイッチポートと接続します。
- カテゴリ 5e UTP/STP ケーブル : 1000BASE-T スイッチポートと接続します。
- カテゴリ 5e/6UTP/STP ケーブル : 2.5GBASE-T スイッチポートと接続します。
- カテゴリ 6a の UTP/STP ケーブル : 10GBASE-T スイッチポートと接続します。
- 光ファイバケーブル : SFP+ ポート経由で光ファイバをサポートするスイッチにアップリンクします。

注意　100BASE-TX 以上の速度を使用する場合、接続ケーブルは 8 芯 4 対のツイストペアケーブル（UTP）を使用してください。

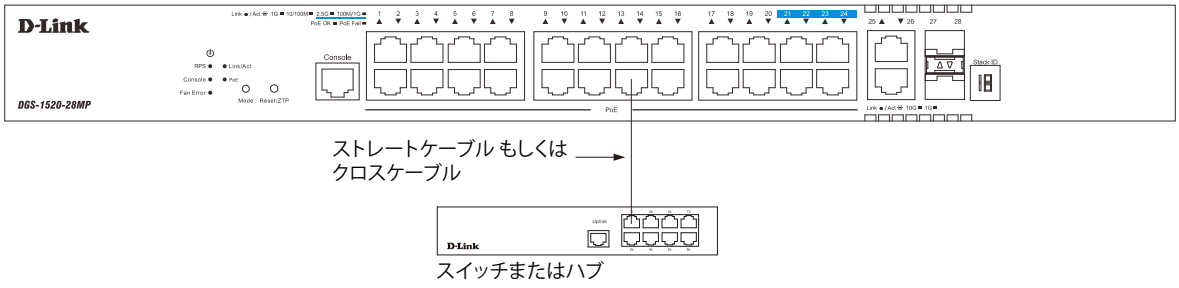


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

DGS-1520 は、ネットワークバックボーン、サーバ、サーバファームへ接続できます。
RJ45 ポートは 10M/100M/1000M/2.5G/10Gbps ※の速度で動作します。SFP+ ポートは、1/10Gbps の速度で動作します。

※ポートにより対応している速度は異なります。

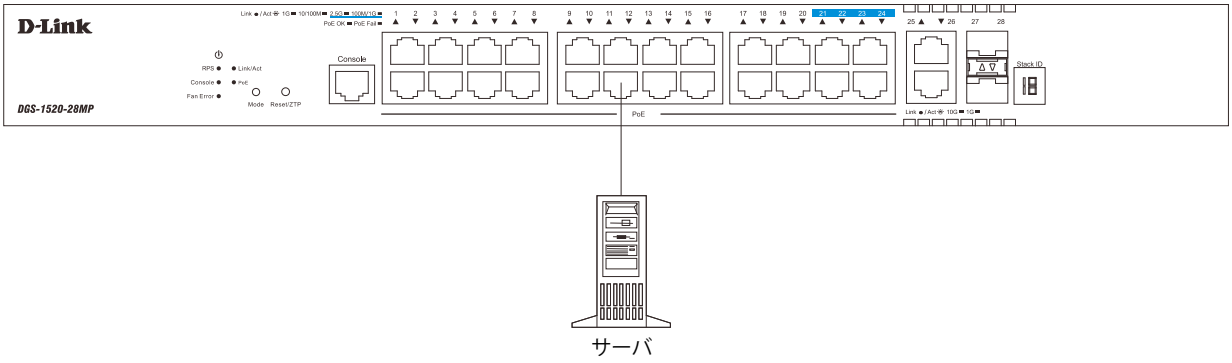


図 3-3　サーバとの接続図

第 4 章　スイッチ管理について

- Web GUI による管理
- SNMP による管理
- CLI による管理

Web GUI による管理

標準的な Web ブラウザを使用して、本製品の設定をグラフィカルに表示し、管理することができます。

Web GUI の詳細については「第 5 章　Web ベースのスイッチ管理」を参照してください。

SNMP による管理

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルです。ネットワークに接続された通信機器の管理や監視を行います。

SNMP の詳細については「SNMP 設定」を参照してください。

CLI による管理

スイッチのモニタリングと設定のために、RJ-45 コンソールポートを搭載しています。コンソールポートを使用するためには、以下をご用意ください。

- ターミナルソフトを操作する、シリアルポート搭載の端末またはコンピュータ
- RJ-45/RS-232C 変換ケーブル

端末をコンソールポートに接続する

ケーブルの接続

1. RJ-45/RS-232C 変換ケーブルの RS-232C コネクタを、シリアルポート搭載の端末またはコンピュータに接続します。
2. RJ-45/RS-232C 変換ケーブルの RJ-45 コネクタを、本製品のコンソールポートに接続します。

ターミナルソフトの設定

1. VT100 のエミュレーションが可能なターミナルソフトを起動します。
2. 適切なシリアルポート（COM 1 など）を選択します。
3. ターミナルソフトの設定をスイッチのシリアルポートの設定に合わせます。
   スイッチのシリアルポートの設定は以下の通りです。
   - スピード：「115200」
   - データ：「8bit」
   - パリティ：「なし（none）」
   - ストップビット：「1bit」

ログインとログアウト

1. 本製品と管理 PC をケーブルで接続後、本製品の電源をいれます。
2. 管理 PC とスイッチが正しく接続されると、画面に「`Press any key to login...`」というメッセージが表示されます。
   キーボード上のいずれかのキーを押します。
3. ユーザ名とパスワードを入力し、「Enter」を押します。
   パスワードとユーザ名の初期値は「admin」です。

注意　パスワードの大文字と小文字は区別されます。

4. コマンドを入力し、必要な設定を行います。

   コマンドの多くは管理者レベルのアクセス権が必要です。
   管理者レベルのアカウント作成については「ユーザアカウント / パスワードの設定」を参照してください。
   CLI の詳細及びコマンドリストについては、CLI マニュアルを参照してください。
5. ログアウトする場合は、logout コマンド使用するか、ターミナルソフトを終了します。

ユーザアカウント / パスワードの設定

管理者レベルのユーザアカウントとパスワードを設定する方法について説明します。

注意 工場出荷時のユーザアカウントおよびパスワードは「admin」、権限レベルは「15」です。
はじめてログインした際は、本スイッチに対する不正アクセスを防ぐために、ユーザ名に対して必ず新しいパスワードを設定してください。
このパスワードは忘れないように記録しておいてください。

```
Switch> enable
Switch# configure terminal
Switch(config)# username Administrator password 12345
Switch(config)# username Administrator privilege 15
Switch(config)# line console
Switch(config-line)# login local
Switch(config-line)#
```

1. 「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
2. 「configure terminal」コマンドを入力し、Global Configuration モードにアクセスします。
3. 「username Administrator password 12345」コマンドを入力し、ユーザ名「Administrator」、パスワード「12345」を指定します。
4. 「username Administrator privilege 15」コマンドを入力し、ユーザアカウントに権限レベル 15 を指定します。
   権限レベルは 1 から 15 まで指定できます。「15」が最大、「1」が最小の権限レベルです。
5. 「line console」コマンドを入力し、LINE Configuration モードにアクセスします。
6. 管理インタフェースにアクセス可能なユーザアカウントが作成されました。コマンドは「login local」です。

注意 パスワードの大文字と小文字は区別されます。
ユーザ名とパスワードは 15 文字以内の半角英数字で指定してください。

注意 CLI の設定コマンドは実行中の設定ファイルの編集でありスイッチが再起動した場合、設定は保存されません。設定内容変更の安全な保存については「copy running-config startup-config」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。詳細は DGS-1520 シリーズの CLI マニュアルを参照してください。

IP アドレスの割り当て

CLI を使用してスイッチの IP アドレスを設定する方法について説明します。

- IP アドレスの初期値：10.90.90.90/8

```
Switch> enable
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy
Switch(config-if)#
```

1. 「enable」コマンドを入力し、Privileged EXEC モードにアクセスします。
2. 「configure terminal」コマンドを入力し、Global Configuration モードになります。
3. 「interface vlan 1」コマンドを入力し、デフォルト VLAN の VLAN Configuration モードに入り「VLAN 1」を指定します。
4. 「ip address xxx.xxx.xxx.xxx yyy.yyy.yyy.yyy」を入力し、IP アドレスを変更します。
   xxx.xxx.xxx.xxx　：　IP アドレス
   yyy.yyy.yyy.yyy　：　IP アドレスに対応するサブネットマスク

管理ポートへの接続

DGS-1520-28/52 の背面パネルには管理ポート (MGMT ポート) があります。
ポートは、標準的なイーサネットケーブルを使用してノート PC に簡単に接続可能な RJ-45 ポートです。管理ポートを使ってスイッチに接続するために、Web ブラウザもしくは Telnet クライアントを使用することができます。

管理ポートを使用するためには、イーサネットケーブルを使用してスイッチ管理に使用するコンピュータのイーサネットインタフェースにポートを接続します。IP アドレスの初期値は 192.168.0.1 で、サブネットマスクは 255.255.255.0 です。スイッチ管理に使用するコンピュータが、192.168.0.x サブネットで重複しない IP アドレスを持っていることを確認してください。

コンソールポート、または Web ベースのスイッチ管理インタフェースを通じて IP 設定または管理ポートのステータスを変更することができます。

管理ポートの設定を変更するためには、以下のコマンドを使用します。

```
Switch#configure terminal
Switch(config)#interface mgmt 0
Switch(config-if)#ip default-gateway 192.168.0.254
Switch(config-if)#
```

IP 設定のステータスを参照するためには、以下のコマンドを使用します。

```
Switch#show ip interface mgmt 0
mgmt_ipif 0 is enabled, Link status is up
IP address is 192.168.0.1/24
Gateway is 0.0.0.0
Switch#
```

注意　管理ポートの MAC アドレスは、「System MAC」を使用するため、「VLAN1」と重複します。

注意　VLAN インタフェースを経由して「Mgmt 0」の IP アドレス宛に通信を行うことはできません。

第 5 章　Web ベースのスイッチ管理

- Web ベースの管理について
- Web マネージャへのログイン
- スマートウィザード設定
- Web GUI について
- Web マネージャのメニュー構成

Web ベースの管理について

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース（HTML) インタフェース経由で管理、設定およびモニタできます。標準的なブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理できます。ブラウザが普遍的なアクセスツールの役割をし、HTTP プロトコルを使用してスイッチと直接通信することが可能です。

Web ベースの管理モジュールとコンソールプログラム（および Telnet）は、異なるインタフェースを経由して同じスイッチ内部のソフトウェアにアクセスし、その設定を行います。つまり、Web ベースでスイッチ管理を実行して行う設定は、コンソール接続によっても行うことができます。

Web マネージャへのログイン

スイッチの管理を行うには、はじめにコンピュータでブラウザを起動し、本スイッチに定義した IP アドレスを入力します。
ブラウザのアドレスバーに以下のように URL を入力します。例 : http://10.90.90.90（10.90.90.90 はスイッチの IP アドレス）。
この接続においてはプロキシ設定を無効とする必要があります。

1. Web ブラウザを開きます。
2. アドレスバーに本スイッチの IP アドレスを入力し、「Enter」キーを押下します。



図 5-1　URL の入力

注意　工場出荷時設定では IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。
端末側の IP インタフェースを本スイッチに合わせるか、本スイッチを端末側の IP インタフェースに合わせてください。

3. 以下のユーザ認証画面が表示されます。



図 5-2　パスワード入力用画面

ユーザ名とパスワードを入力し、「ログイン」をクリックします。

ユーザ名とパスワードの初期値は以下です。
・ユーザ名：admin
・パスワード：admin

「言語」では Web GUI を表示する言語を選択できます。

4. スマートウィザード画面が表示されます。

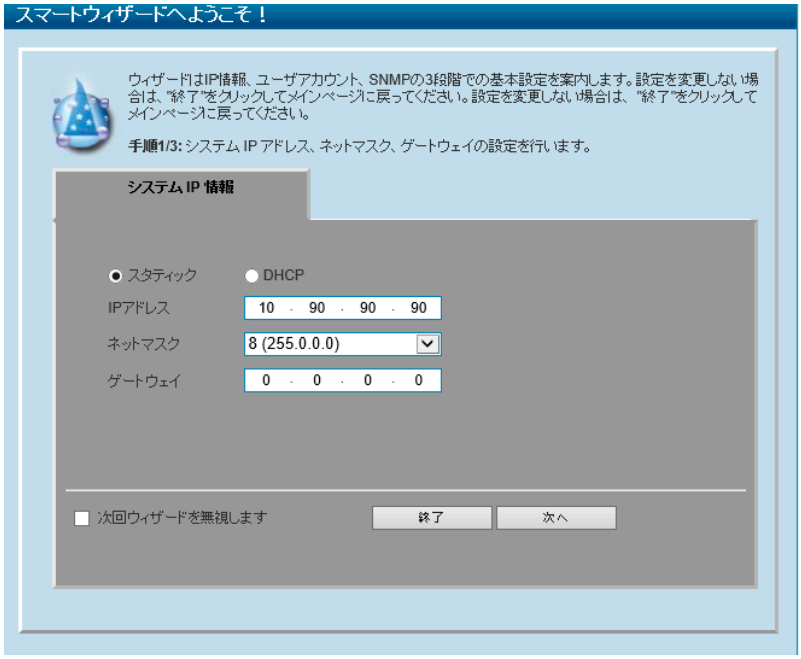


図 5-3　　スマートウィザード画面

ウィザード画面では、Web モードの選択や IP アドレス・パスワード・SNMP の設定を行うことができます。
ウィザードを使用して設定する場合は、「スマートウィザード設定」を参照してください。

スマートウィザード設定

スマートウィザードで Web モードの選択や基本的なシステム設定（IP アドレス、パスワード、SNMP）を行います。

注意　スマートウィザードでは、IPv4 アドレスのみ設定可能です。

注意　Web マネージャメイン画面の「スマートウィザード」から、スマートウィザード画面に移動できます。

注意　「次回ウィザードを無視します」にチェックをいれた場合は、次回のログイン時にスマートウィザード 画面が表示されません。

1. IP アドレスの設定を行います。設定後「次へ」をクリックします。

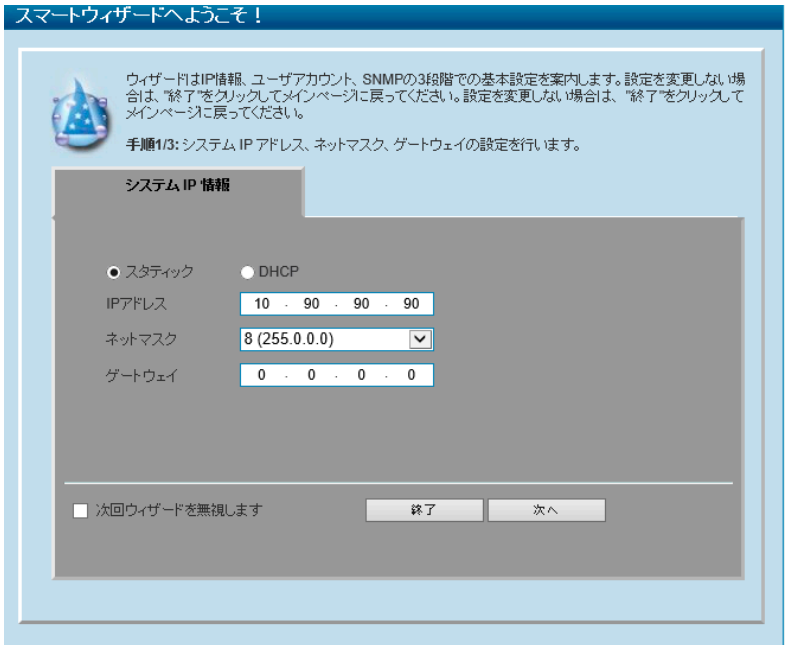


図 5-4　　システム IP 情報画面

- 「スタティック」：固定設定。「IP アドレス」「ネットマスク」「ゲートウェイ」を入力します。
- 「DHCP」：DHCP による自動取得。

注意　スイッチの IP アドレスを変更すると、現在の PC とスイッチの接続が切断します。
Web ブラウザに正しい IP アドレスを入力して、必ずご使用のコンピュータをスイッチと同じサブネットに設定してください。

2. ユーザアカウントの設定を行います。設定後「次へ」をクリックします。

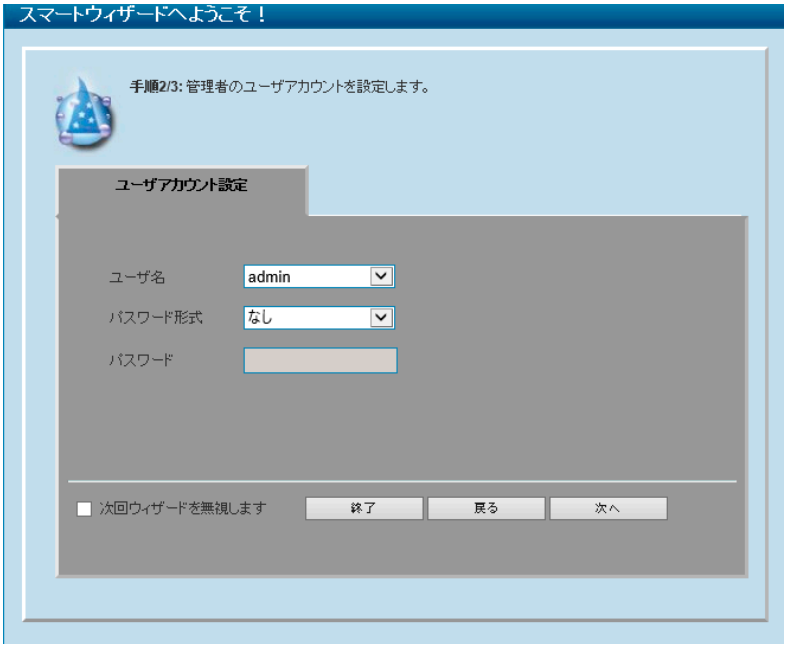


図 5-5　ユーザアカウント設定画面

画面に表示される項目：

項目	説明
ユーザ名	ユーザアカウントに使用するユーザ名を入力します。
パスワード形式	パスワード形式を以下から指定します。 • なし - ユーザアカウントにパスワードを指定しません。 • 平文 - プレーンテキストでパスワードを指定します。「暗号化フォーマット」へ暗号化できないことを意味します。 • 暗号化 -SHA1 - SHA-1 でパスワードを指定します。「SHA-1」方式の暗号化パスワードになります。 • 暗号化 -MD5 - MD5 でパスワードを指定します。「MD5」方式の暗号化パスワードになります。
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。パスワード形式を「なし」にした場合は入力できません。

3. SNMP を有効 / 無効に設定します。



図 5-6　SNMP 画面

4. 「適用して保存」をクリックします。

Web GUI について

本製品の Web GUI について説明します。

Web GUI の各エリアについて

Web GUI のメイン画面は 3 つのエリアで構成されています。Web GUI の「デバイス情報」画面では以下の情報を参照することができます。

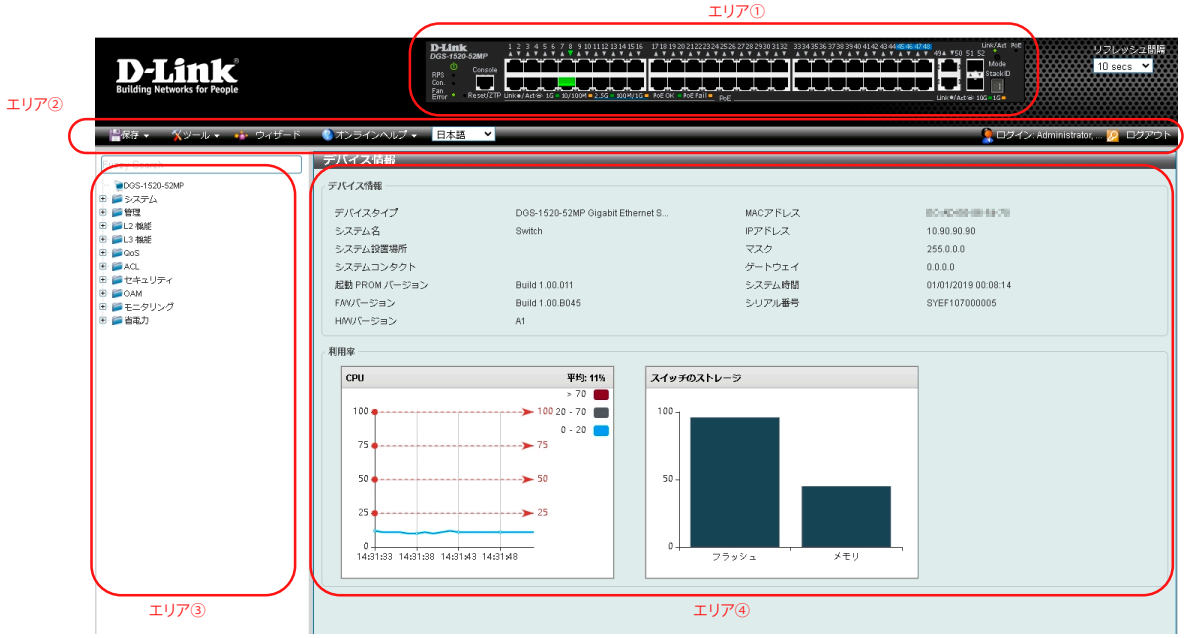


図 5-7　デバイス情報画面

エリア	機能
エリア①	本エリアではスイッチの前面パネルの状態がほぼリアルタイムにグラフィカル表示されます。 スイッチのポート、拡張モジュールが表示されます。ポートモニタなどの管理機能はここからアクセスする事も可能です。「D-Link」ロゴをクリックすると D-Link Web サイト（英語）へ移動します。
エリア②	スイッチの再起動、コンフィグレーションのバックアップとリストア、ファームウェアの更新、設定の初期化などを行う「ツール」メニューと設定の保存を行う「保存」メニューがあります。 ツールバーの右側には、現在接続中のユーザ名とスイッチの IP アドレス、ログアウトボタンが表示されます。
エリア③	WebUI を使用して設定可能な機能のツリービューが表示されます。ツリー項目をクリックして各機能の設定画面に移動します。 製品名をクリックすると、デバイス情報画面が表示されます。 また、メニュー項目をキーワードで検索するための検索フィールドも用意されています。
エリア④	ツリービューで選択した各機能の設定画面が表示されます。

補足　Web UI を表示する最適の解像度は「1280 x 1024」ピクセルです。

警告　スイッチ設定を変更した場合、以下で説明する Web ブラウザの「保存」メニューまたはコマンドラインインタフェース（CLI）の「save」コマンドにて保存する必要があります。

Web マネージャのメニュー構成

Web マネージャで本スイッチに接続し、ログイン画面でユーザ名とパスワードを入力して本スイッチの管理モードにアクセスします。
Web マネージャで設定可能な機能を次に説明します。

メインメニュー	サブメニュー	説明
システム	デバイス情報	スイッチの主な設定情報を表示します。
	システム情報設定	スイッチの基本情報を表示します。
	周辺機器設定	システムの警告温度や環境トラップの設定を行います。
	ポート設定	スイッチポートの詳細設定などを行います。
	インタフェース説明	スイッチの各ポートの概要、管理ステータスなどについて表示します。
	ループバックテスト	物理ポートインタフェースのループバック設定とループバックテストを行います。
	PoE（DGS-1520-28MP/52MP）	DGS-1520-28MP/52MP の PoE 機能について設定を行います。
	システムログ	スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。
	時間と SNTP	スイッチに時刻を設定します。
	タイムレンジ	スイッチのタイムレンジを設定します。
	リセットボタンの設定	リセット /ZTP ボタンの設定を行います。
管理	コマンドロギング	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
	ユーザアカウント設定	スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。
	パスワード暗号化	パスワードを暗号化し設定ファイルに保存します。
	パスワードリカバリ	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
	ログイン方法	各管理インタフェースでのログイン方法について設定します。
	SNMP	SNMP 設定を有効にします。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
	RMON	SNMP 機能に対するリモートモニタリング（RMON）ステータスを有効にします。
	Telnet/Web	スイッチに Telnet/Web 設定を有効にします。
	セッションタイムアウト	各セッション（Web やコンソールなど）のタイムアウトの設定をします。
	DHCP	スイッチの DHCP について設定します。
	DHCP 自動設定	DHCP 自動コンフィグ機能の設定を行います。
	DHCP 自動イメージ設定	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイルを取得する機能です。
	DNS	DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
	NTP	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
	IP 送信元インタフェース	IP ソースインタフェースの設定を行います。
	ファイルシステム	フラッシュファイルシステムにより、ファームウェア、Config 情報、および Syslog 情報はフラッシュ内のファイルに保存されます。
	スタッキング	物理スタッキングの設定を行います。
	仮想スタックキング（SIM）	仮想（SIM）スタッキングの設定を行います。
	D-Link ディスカバリプロトコル	D-Link ディスカバリプロトコル（DDP）の設定を行います。
	SMTP 設定	Simple Mail Transfer Protocol（SMTP）の設定を行います。
	NLB FDB 設定	ネットワークロードバランシング（NLB）の設定を行います。

メインメニュー	サブメニュー	説明
L2 機能	FDB	FDB（Forwarding DataBase）フォワーディングデータベースの設定を行います。
	VLAN	802.1Q スタティック VLAN の設定を行います。
	VLAN Tunnel	802.1Q VLAN トンネルの設定を行います。
	STP	スパニングツリープロトコル（STP）設定を行います。3 つのバージョンの STP（802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。
	ERPS（G.8032）	Ethernet Ring Protection Switching（ERPS）の表示、設定を行います。 ERPS はイーサネットリング保護スイッチングの業界標準（ITU-T G.8032）です。
	ループバック検知	ループバック検知（LBD）機能の設定を行います。
	リンクアグリゲーション	Link Aggregation（リンクアグリゲーション / ポートトランキング機能）の設定を行います。
	L2 プロトコルトンネル	L2 Protocol Tunnel（レイヤ 2 プロトコルトンネル）の設定を行います。
	L2 マルチキャストコントロール	IGMP（Internet Group Management Protocol）スヌーピング機能を始めとした L2 マルチキャストコントロール）の設定を行います。
	LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。
L3 機能	ARP	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
	Gratuitous ARP	Gratuitous ARP の設定を行います。
	IPv6 隣接	IPv6 Neighbor の設定を行います。
	インタフェース	IP インタフェース設定を行います。
	UDP Helper	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを指定します。
	IPv4 スタティック / デフォルトルート	本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。
	IPv4 ルートテーブル	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。
	IPv6 スタティック / デフォルトルート	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。
	IPv6 ルートテーブル	IPv6 ルーティングテーブルを表示します。
	ルート優先	ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。
	ECMP 設定	ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。
	IPv6 General プリフィクス	VLAN インタフェース IPv6 汎用プリフィクスの設定を行います。
	URPF 設定	「Unicast Reverse Path Forwarding」（URPF）の設定と表示を行います。
	RIP	RIP（Routing Information Protocol）は、距離ベクトル型のルーティングプロトコルです。
	RIPng	RIPng（Routing Information Protocol next generation）をサポートしています。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。
	OSPF	OSPF を設定します。
	IP マルチキャストルーティングプロトコル	IP Multicast Routing Protocol（IP マルチキャストルーティングプロトコル）の設定を行います。
	IP ルートフィルタ	IP プレフィックスリスト、ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。
	ポリシールート	ポリシーベースルーティングの設定、表示を行います。
	VRRP 設定	VRRP（Virtual Routing Redundancy Protocol）は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。
	VRRPv3 設定	VRRPv3 設定を行います。
QoS	基本設定	QoS の基本設定を行います。
	詳細設定	QoS の詳細設定を行います。
	QoS PFC	ネットワーク「Quality of Service」（QoS）プライオリティベースフローコントロール（PFC）クラスマップの設定を行います。
	WRED	WRED（Weighted Random Early Detection）の設定を行います。
ACL	ACL コンフィグレーションウィザード	アクセスプロファイルと ACL ルールの新規作成を行います。
	ACL アクセスリスト	ACL アクセスリストの設定を行います。
	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の設定を行います。
	ACL VLAN アクセスマップ	ACL VLAN アクセスマップの設定を行います。
	ACL VLAN フィルタ設定	ACL VLAN フィルタの設定を行います。
	CPU ACL	CPU インタフェースフィルタリング機能の設定を行います。

メインメニュー	サブメニュー	説明
セキュリティ	ポートセキュリティ	ポートセキュリティは、ポートのロックを行う前にスイッチが（ソースMACアドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。
	802.1X	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
	AAA	AAA（Authentication、Authorization、Accounting）の設定を行います。
	RADIUS	RADIUS の設定を行います。
	TACACS+	TACACS+ の設定を行います。
	IMPB	P-MAC- ポートバインディングにより、スイッチにアクセスするユーザ数を制限します。
	DHCP サーバスクリーニング	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
	ARP スプーフィング防止	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった IP アドレスの ARP パケットをバイパスします。
	BPDU アタック防止	スイッチのポートに BPDU 防止機能を設定します。
	NetBIOS フィルタリング設定	NetBIOS フィルタリングの設定を行います。
	MAC 認証	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
	Web アクセスコントロール	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
	ネットワークアクセス認証	ネットワークアクセス認証の設定を行います。
	セーフガードエンジン	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
	トラストホスト	トラストホストの設定を行います。
	トラフィックセグメンテーション	トラフィックセグメンテーション機能はポート間のトラフィックの流れを制限を行います。
	ストーム制御設定	ストームコントロールの設定を行います。
	DoS 攻撃防御設定	各 DoS 攻撃に対して防御設定を行います。
	ゾーンディフェンス設定	ゾーンディフェンス（Zone Defense）機能の設定と表示を行います。
	SSH	SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。
	SSL	Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。
OAM	ケーブル診断機能	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
	DDM	Digital Diagnostic Monitoring（DDM）機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。
モニタリング	VLAN カウンタ	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。
	利用率	スイッチの利用率を表示します。
	統計	スイッチの統計情報を表示します。
	ミラー設定	ミラーリング機能の設定を行います。本スイッチは対象ポートで送受信するフレームをコピーし、フレームの出力先を他のポートに変更する機能（ポートミラーリング）があります。
	sFlow	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
省電力	省電力	スイッチの省電力機能を設定、表示します。
	EEE	「Energy Efficient Ethernet」（EEE/ 省電力イーサネット）は「IEEE 802.3az」によって定義されており、パケットの送受信がリンクに発生していない場合の電力消費を抑える目的で設計されています。

メインメニュー	サブメニュー	説明
ツールバー	保存	コンフィグレーションの保存を行います。
	ツール	ファームウエアアップグレードやバックアップ、コンフィグレーションのリストア、バックアップなどを行います。
	ウィザード	スマートウィザードを開始します。
	オンラインヘルプ	D-Link のサポート Web サイト（英語）/ またはユーザガイド（英語版）を表示します。インターネット接続が必要です。
	ログアウト	Web GUI からログアウトします。

第 6 章　システム

以下は、「システム」サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
デバイス情報	スイッチの主な設定情報を表示します。
システム情報設定	スイッチの基本情報を表示します。
周辺機器設定	システムの警告温度や環境トラップの設定を行います。
ポート設定	スイッチポートの詳細設定などを行います。
インタフェース説明	スイッチの各ポートの概要、管理ステータスなどについて表示します。
ループバックテスト	物理ポートインタフェースのループバック設定とループバックテストを行います。
PoE（DGS-1520-28MP/52MP）	PoE 機能の設定、表示を行います。（DGS-1520-28MP/52MP のみ）
システムログ	システムログ機能のステータスや、ログの保存方法などを設定します。
時間と SNTP	スイッチに時刻を設定します。
タイムレンジ	スイッチのタイムレンジを設定します。アクセスプロファイル機能を実行する期間を決定します。
リセットボタンの設定	リセット /ZTP ボタンの設定を行います。

デバイス情報

本画面は、ログインを行うと自動的に表示される画面です。スイッチの主な設定情報を確認できます。
別の画面から本画面に戻るには、メニューツリーの一番上にある製品名のリンクをクリックします。

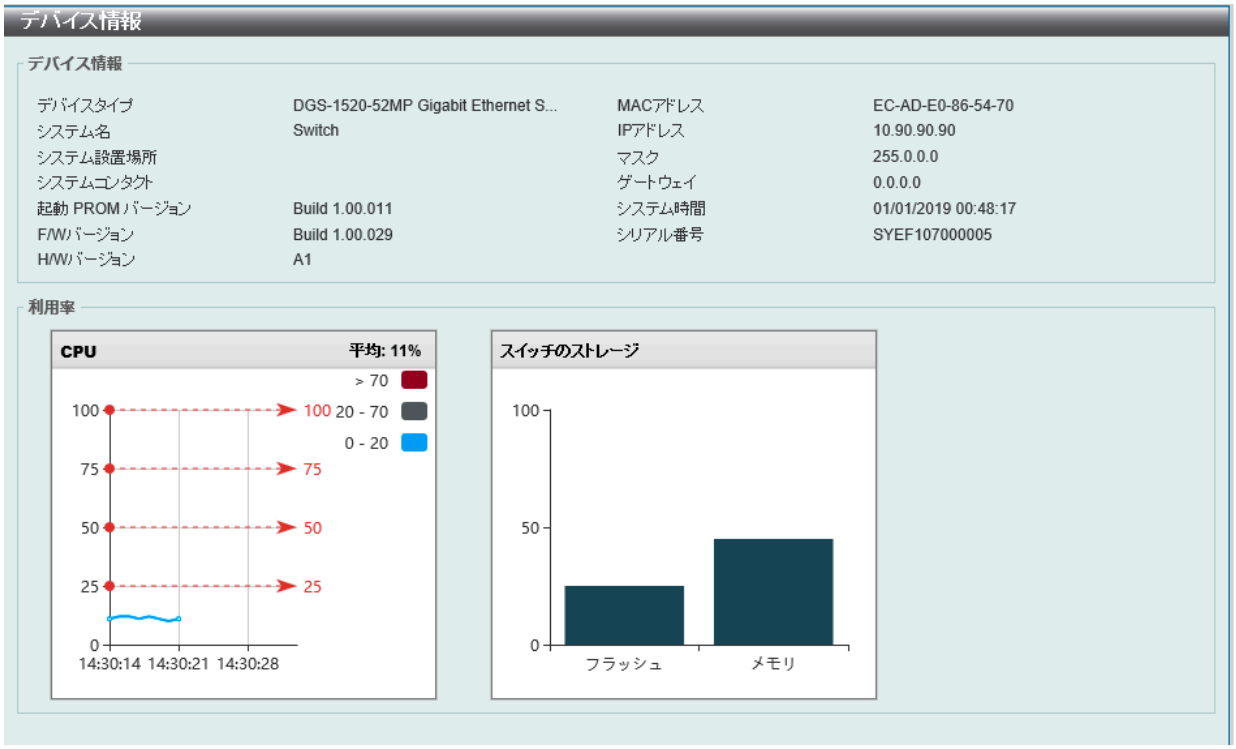


図 6-1　デバイス情報画面

画面に表示される項目：

項目	説明
デバイス情報	
デバイスタイプ	工場にて定義した機種名と型式を表示します。
システム名	ユーザが定義したシステム名を表示します。
システム設置場所	システムが現在動作している場所を表示します。
システムコンタクト	担当者名を表示します。
起動 PROM バージョン	デバイスのブートバージョンを表示します。
F/W バージョン	デバイスのファームウェアバージョンを表示します。
H/W バージョン	デバイスのハードウェアバージョンを表示します。
MAC アドレス	デバイスに割り当てられた MAC アドレスを表示します。
IP アドレス	デバイスに割り当てられた IP アドレスを表示します。
マスク	デバイスに割り当てられたサブネットマスクを表示します。
ゲートウェイ	デバイスに割り当てられたデフォルトゲートウェイを表示します。
システム時間	最後のデバイスリセットからの経過時間を表示します。
シリアル番号	デバイスのシリアル番号を表示します。
利用率	
CPU	CPU の使用率を表示します。
フラッシュ	フラッシュの使用率を表示します。
メモリ	メモリの使用率を表示します。

システム情報設定

システム情報設定画面では、システム情報の設定と管理（MGMT）インタフェースの設定を行います。
「管理インタフェース」セクションは、DGS-1520-28/52 でのみ表示されます。

システム > システム情報設定の順にメニューをクリックして、以下の画面を表示します。

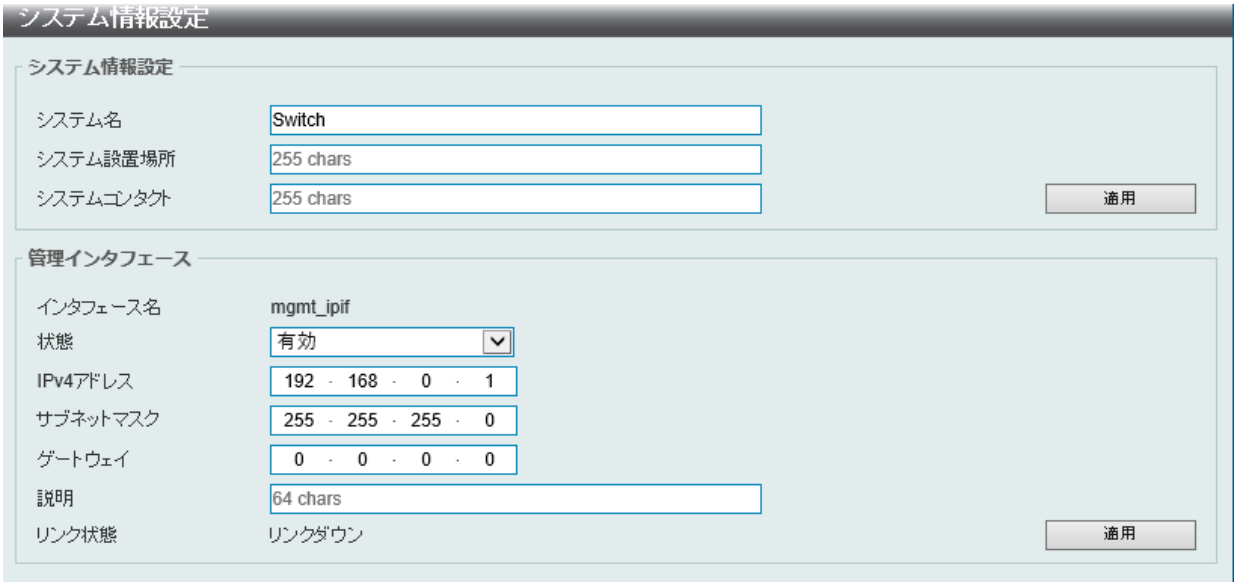


図 6-2　システム情報設定画面

画面に表示される項目：

項目	説明
システム情報設定	
システム名	必要に応じて、スイッチのシステム名を変更します。ネットワーク内での識別名となります。
システム設置場所	必要に応じて、システムが稼働している場所を定義します。
システムコンタクト	必要に応じて、スイッチの管理者情報を入力します。
管理インタフェース	
状態	管理インタフェースの有効 / 無効を指定します。
IPv4 アドレス	管理インタフェースの IPv4 アドレスを指定します。
サブネットマスク	管理インタフェースのサブネットマスクを指定します。
ゲートウェイ	管理インタフェースのゲートウェイ IPv4 アドレスを指定します。
説明	管理インタフェースについての説明を入力します。

「適用」をクリックして、設定内容を適用します。

周辺機器設定

システムの警告温度や環境トラップの設定を行います。

システム > 周辺機器設定の順にクリックし、以下の画面を表示します。

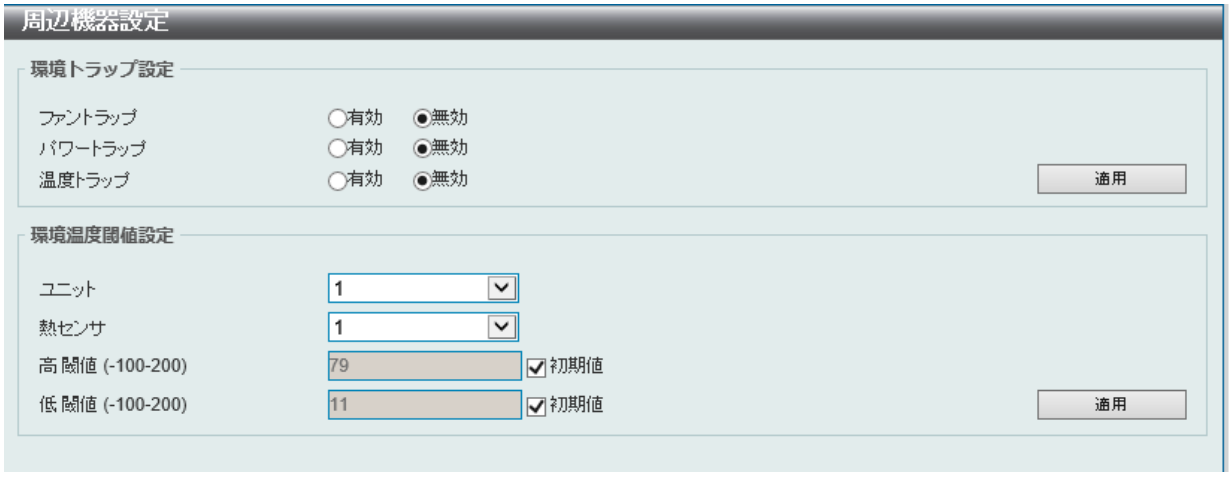


図 6-3　　周辺機器設定画面

画面に表示される項目：

項目	説明
環境トラップ設定	
ファントラップ	ファン警告イベント（ファンエラーまたは回復）のトラップを有効 / 無効に設定します。
パワートラップ	電源警告イベント（電源エラーまたは回復）のトラップを有効 / 無効に設定します。
温度トラップ	温度警告イベント（温度しきい値の超過または回復）のトラップを有効 / 無効に設定します。
環境温度閾値設定	
ユニット	設定するユニットを指定します。
熱センサ	温度センサ ID を選択します。
高 閾値	高温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 「初期値」をチェックすると初期値に戻ります。
低 閾値	低温警告しきい値を指定します。 • 設定可能範囲：「-100℃」-「200℃」 「初期値」をチェックすると初期値に戻ります。

「適用」をクリックして、設定内容を適用します。

ポート設定

各ポートの設定を行います。

ポート設定

ポートの詳細を設定します。

システム > ポート設定 > ポート設定の順にメニューを選択し、以下の画面を表示します。



図 6-4　　ポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	物理ポートのステータスを有効 / 無効に設定します。
MDIX	MDIX の設定を以下から選択します。 • 「自動」- 最適なケーブル接続を自動的に設定します。 • 「ノーマル」- 通常のケーブル接続の場合は、このオプションを選択します。このオプションを選択すると、ポートは MDIX モードになり、ストレートケーブルを使用して PC の NIC に接続するか、クロスケーブルを介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」- ポートは MDI モードとなり、ストレートケーブルで別のスイッチのポート (MDIX モード) に接続することができます。
フロー制御	「オン」（フロー制御あり）または「オフ」（フロー制御なし）を選択します。 Full-Duplex のポートでは 802.3x フローコントロールによる制御を行います。「自動」のポートは自動的にいずれかを使用します。 物理スタックのスイッチはサポートしていません。
デュプレックス	全二重 / 半二重モードの設定を「自動」「ハーフ」「フル」から選択します。 ハードウェアの制限により、速度が 100Mbps で動作している場合、2.5Gbps ポートでは Half-Duplex の動作はサポートされません。 Full-Duplex の動作のみがサポートされます。100Mbps の Half-Duplex の動作の場合は、1Gbps ポートのいずれかに接続します。
速度	ポートの速度を以下から選択します。2500M の項目が表示されるのは DGS-1520-28MP/52MP のみです。 「自動」を選択した場合は、接続相手の状況に合わせて最適な通信を行うよう自動的に判別します。 「10M」「100M」「1000M」「1000M Master」「1000M Slave」「2500M」「2500M Master」「2500M Slave」 「10G」「10G Master」「10G Slave」 マスタ設定 (1000M Master) によりポートはデュプレックス、速度および物理レイヤタイプに関連する情報を通知します。 さらに接続している物理レイヤ間におけるマスタとスレーブを決定します。この関係は物理レイヤ間の連携のタイミングをコントロールするために必要です。タイミングのコントロールには、ローカルソースによってマスタの物理層に設定されます。スレーブ設定 (1000M Slave) はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続に「1000M Master」を設定した場合、他方の接続は「1000M Slave」とする必要があります。その他の設定では両ポートのリンクダウンを引き起こします。
機能アドバタイズ	「速度」を「自動」に設定した場合、指定した項目がオートネゴシエーションの間にアドバタイズされます。
説明	ポートの説明を入力します。（64 文字以内）

「適用」をクリックして、設定内容を適用します。

注意　1Gbps のポートにおいて、4 芯 2 対のツイストペアケーブル（UTP）を使用した場合、オートネゴシエーションの設定ではリンクアップしません。

ポートステータス

ポートの状態、設定について表示します。

システム > ポート設定 > ポートステータスの順にメニューをクリックし、以下の画面を表示します。



図 6-5　ポートステータス画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。

GBIC ポート

スイッチの各物理ポートの GBIC 情報について表示します。

システム > ポート設定 > GBIC ポートの順にメニューをクリックし、以下の画面を表示します。



図 6-6　GBIC ポート画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。

ポートオートネゴシエーション

オートネゴシエーションの詳細情報を表示します。

システム > ポート設定 > ポートオートネゴシエーションの順にメニューをクリックし、以下の画面を表示します。



図 6-7　ポートオートネゴシエーション画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。

エラー Disable 設定

エラー Disable は、ループバック検出などのエラーが発生したポートを Disable（無効）状態にする機能です。
本画面では、エラーの原因や Disable 状態のポートのリカバリ間隔の設定などを行います。

システム > ポート設定 > エラー Disable 設定の順にメニューをクリックし、以下の画面を表示します。



図 6-8　エラー Disable 設定画面

画面には以下の項目があります。

項目	説明
エラー Disable トラップ設定	
アサート	エラー無効状態になったときの通知送信の有効 / 無効を指定します。
クリア	エラー無効状態から回復したときの通知送信の有効 / 無効を指定します。
通知レート	1 分あたりのトラップ数を入力します。指定したしきい値超えたパケットは破棄されます。 • 設定可能範囲：0 - 1000 • 初期値：0 初期値の「0」は、無効状態が変更されるたびに SNMP トラップが生成されることを示します。
エラー Disable リカバリ設定	
エラー Disable 原因	エラー無効の原因を次から選択します。 • 選択肢：「すべて」「ポートセキュリティ」「ストーム制御」「BPDU アタック防止」「ダイナミック ARP インスペクション」「DHCP スヌーピング」「ループバック検知」「L2PT ガード」
状態	指定した原因によるエラー無効ポートの自動リカバリ機能を有効 / 無効にします。
間隔	ポートリカバリを実行する間隔を設定します。 • 設定可能範囲：5 - 86400（秒）

「適用」をクリックして、設定内容を適用します。

ジャンボフレーム

ジャンボフレームは、1,518Byte を超えるフレームサイズを意味します。ジャンボフレームにより、同じデータを少ないフレームで転送することができます。DGS-1520 シリーズでは、最大フレームサイズが 12,288 バイトまでのジャンボフレームをサポートしています。

システム > ポート設定 > ジャンボフレーム の順にクリックし、以下の画面を表示します。



図 6-9　ジャンボフレーム画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
最大受信フレームサイズ	スイッチのジャンボフレーム機能の最大値を指定します。 • 設定可能範囲：64 - 12288（bytes） • 初期値：1536（bytes）

「適用」をクリックして、設定内容を適用します。

インタフェース説明

スイッチの各ポートの概要、管理ステータスなどについて表示します。

システム > インタフェース説明 の順にクリックし、以下の画面を表示します。

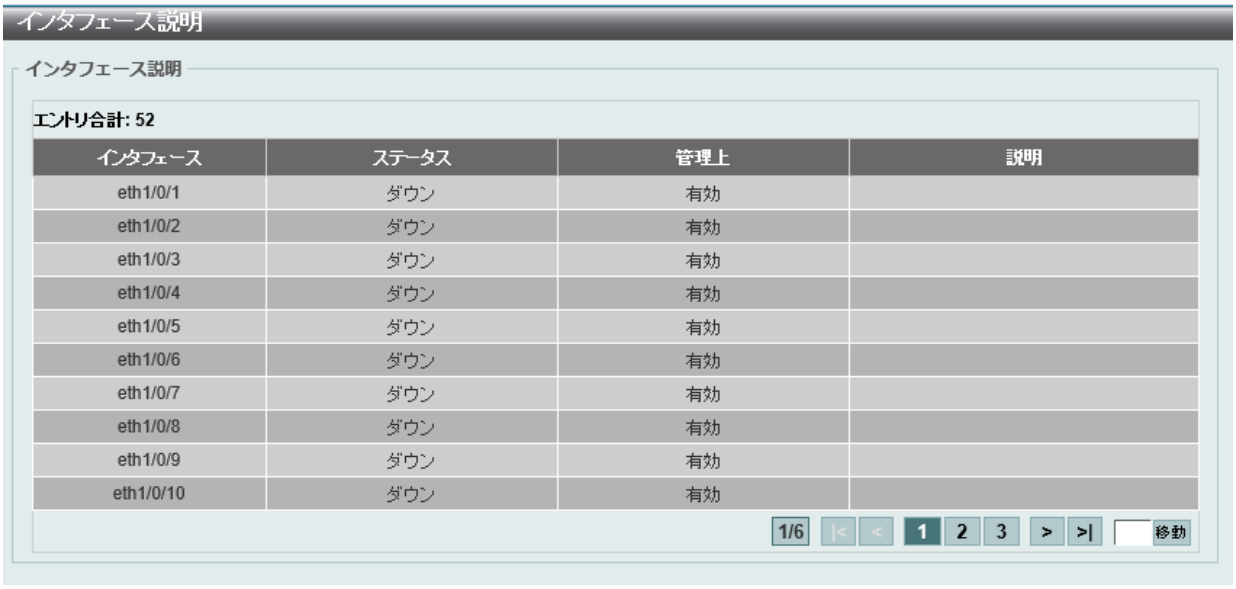


図 6-10　インタフェース説明画面

ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

ループバックテスト

物理ポートインタフェースのループバック設定とループバックテストを行います。

システム > ループバックテストの順にメニューをクリックし、以下の画面を表示します。



図 6-11　ループバックテスト 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ループバックモード	ループバックモードを指定します。 • 「なし」- ループバックモードを有効にしません。 • 「内部 MAC」- MAC レイヤでの内部ループバックモードを指定します。 • 「内部 PHY のデフォルト」- PHY レイヤでの内部ループバックモードを指定します。デフォルトメディアに対してテストを実行します。 • 「内部 PHY カッパー」- PHY レイヤでの内部ループバックモードを指定します。カッパーメディアに対してテストを実行します。 • 「内部 PHY ファイバー」- PHY レイヤでの内部ループバックモードを指定します。ファイバメディアに対してテストを実行します。 • 「外部 MAC」- MAC レイヤでの外部ループバックモードを指定します。 • 「外部 PHY のデフォルト」- PHY レイヤでの外部ループバックモードを指定します。デフォルトメディアに対してテストを実行します。 • 「外部 PHY カッパー」- PHY レイヤでの外部ループバックモードを指定します。カッパーメディアに対してテストを実行します。 • 「外部 PHY ファイバー」- PHY レイヤでの外部ループバックモードを指定します。ファイバメディアに対してテストを実行します。

「適用」をクリックして、設定内容を適用します。

注意　以下の機能を有効にしている場合、内部 PHY（Internal PHY）および内部 MAC（Internal MAC）のループバックモードは機能しません。

- STP
- ループバック検知
- ミラーリング
- ポートチャネル設定

ただし、内部 MAC（Internal MAC）のループバックモードはインタフェースで STP を無効にすることで併用可能です。

注意　内部 PHY（Internal PHY）のループバックモードは、リンクアップしているインタフェースでは使用できません。

PoE（DGS-1520-28MP/52MP）

DGS-1520-28MP/52MP は、IEEE802.3af 規格および IEEE802.3at 規格の PoE 機能をサポートしています。
すべてのポートは、最大 30W の PoE をサポートしています。
ポートは、カテゴリ 5 またはカテゴリ 3 の UTP Ethernet ケーブルを介して、約 48VDC の電源を受電機器（PD/Powered Devices）に供給できます。
本スイッチは PSE pinout Alternative A に準拠しており、電力はピン 1、2、3、および 6 を通じて供給されます。
本スイッチでは以下の PoE 機能を使用できます。

- Auto-discovery 機能は PD（受電機器）に自動的に電力を供給します。
- Auto-disable 機能は、「消費電力がシステム電源のリミットを超えている場合」と「各ポートの消費電力リミットを超えている場合」において動作します。
- Active circuit protection 機能は電力の不足が生じた場合、自動的にポートを無効にする機能です。他のポートは有効性は変わりません。

802.3af/at 準拠の受電機器の最大受信電力一覧：

クラス	受電機器の最大受信電力
0	12.95W
1	3.84W
2	6.49W
3	12.95W
4	25.5W

PSE を使用した最大電力一覧：

クラス	PSE の最大供給電力
0	15.4W
1	4W
2	7W
3	15.4W
ユーザ定義	30W

PoE システム

デバイスの PoE 情報を参照および変更します。
システム > PoE > PoE システム の順にクリックし、以下の画面を表示します。



図 6-12　PoE システム画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
利用量閾値	ログの記録や通常の通知送信を実行するしきい値を指定します。 • 設定可能範囲：1 - 99（%）
ポリシープリエンプト	ポリシープリエンプトを有効 / 無効にします。 ポリシープリエンプトは、電力が不足している状態で新しくデバイスを接続した場合に、優先度の低いデバイスを切断して、新規のデバイスに供給する電力を確保する機能です。
トラップステート	PoE の通知送信を有効 / 無効にします。

「適用」をクリックして、設定内容を適用します。
「詳細を表示」をクリックすると以下の画面が表示されます。

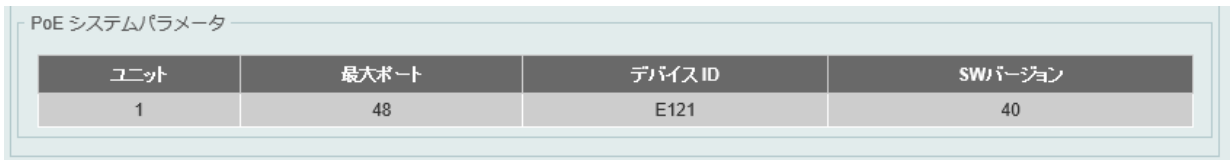


図 6-13　PoE システムパラメータ 画面

PoE ステータス

各ポートの PoE ステータスを表示、設定します。

システム > PoE > PoE ステータスの順にクリックし、以下の画面を表示します。



図 6-14　PoE ステータス 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
説明	PoE インタフェースに接続中の PD の説明を入力します。(32 文字以内)

「記述を削除」をクリックすると入力した概要が削除されます。
「適用」をクリックして、設定内容を適用します。

PoE 設定

PoE 機能の有効化、現在の電力消費の表示、PoE トラップの有効化などシステムの PoE 情報の操作を行います。

注意　IEEE802.3at PD への給電に失敗する場合は、以下を確認、実行してください。
・対象の PD デバイスが IEEE802.3at に準拠しているか確認する
・対象のポートを手動で 30W に設定する

システム > PoE > PoE 設定の順にクリックし、以下の画面を表示します。



図 6-15　PoE 設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
優先度	ポートの優先度を指定します。ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。 • 選択肢：「重大な」「高」「低」
レガシーサポート	レガシー PD へのサポートを有効 / 無効にします。
モード	PoE ポートの電力管理モードを選択します。 • 選択肢：「自動」「Never」。
最大ワット数	「モード」で「自動」を選択した場合に最大電力を入力します。チェックボックスにチェックを入れ、自動検出 PD へ供給する最大電力を指定します。数値を設定しない場合、PD のクラスによって、供給可能な電力が自動的に決定されます。 • 設定可能範囲：1000 - 30000（mW）
タイムレンジ	「モード」で「自動」を選択した場合にタイムレンジを入力します。 タイムレンジは、ポートの PoE 機能を有効にする時間を指定します。

「タイムレンジ削除」をクリックするとタイムレンジが削除されます。
「適用」をクリックして、設定内容を適用します。

PD Alive

PD アライブ機能の設定を行います。PD の状態について「Ping」を使用して確認します。PD が動作していない場合、リセット、通知などを行います。

システム > PoE > PD Alive の順にクリックし、以下の画面を表示します。

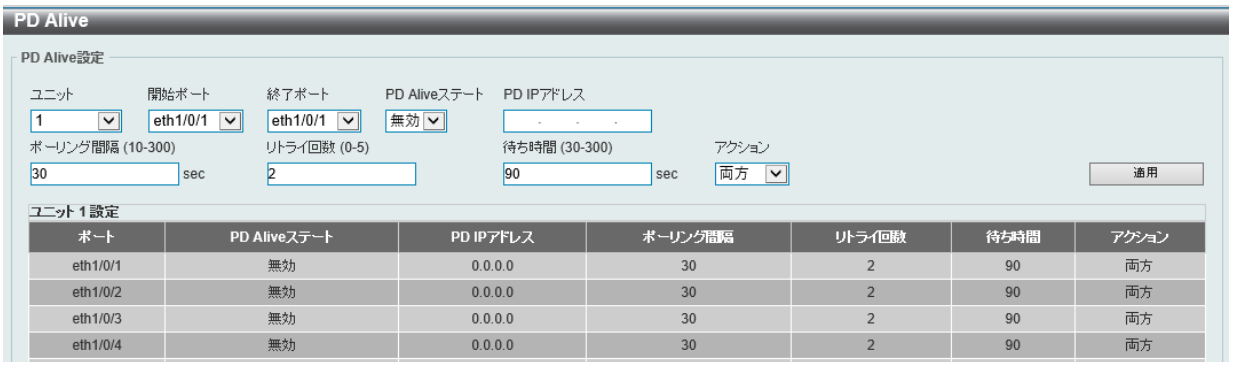


図 6-16　PD Alive 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
PD Alive ステート	PD アライブ機能を有効 / 無効にします。
PD IP アドレス	PD の IPv4 アドレスを指定します。
ポーリング間隔	ポーリング間隔を指定します。ポーリング間隔は、指定の PD の状況を確認するための Ping を送信する間隔です。 • 設定可能範囲：10 - 300（秒）
リトライ回数	リトライ回数を指定します。リトライ回数は、指定の PD から応答がなかった際に Ping を再送信する回数です。 • 設定可能範囲：0 - 5
待ち時間	待機時間（指定の PD が再起動から回復するまでスイッチが待つ時間）を指定します。 • 設定可能範囲：30 - 300（秒）
アクション	実行する動作を指定します。 •「リセット」- PoE ポートをリセットします。 •「通知」- 管理者に通知するログとトラップを送信します。 •「両方」- 管理者に通知するログとトラップを送信し、PoE ポートをリセットします。

「適用」をクリックして、設定内容を適用します。

注意　タイムレンジ を PD アライブ と併用した場合、PD アライブ は機能しません。

PoE 統計

PoE の統計情報を表示します。

システム > PoE > PoE 統計 の順にクリックし、以下の画面を表示します。



図 6-17　PoE 統計 画面

画面に表示される項目：

項目	説明
ユニット	情報を表示するユニットを指定します。

「すべてをクリア」をクリックすると全ポートの PoE 統計情報がクリアされます。
「クリア」をクリックすると対象ポートの PoE 統計情報がクリアされます。

注意　未給電のポートでは、「不正な署名」のカウンタが上昇しますが、異常ではありません。

PoE 計測

PoE の測定情報を表示します。

システム > PoE > PoE 計測の順にクリックし、以下の画面を表示します。



図 6-18　PoE 計測画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。

PoE LLDP クラシフィケーション

PoE の LLDP 分類情報を表示します。

システム > PoE > PoE LLDP クラシフィケーションの順にクリックし、以下の画面を表示します。

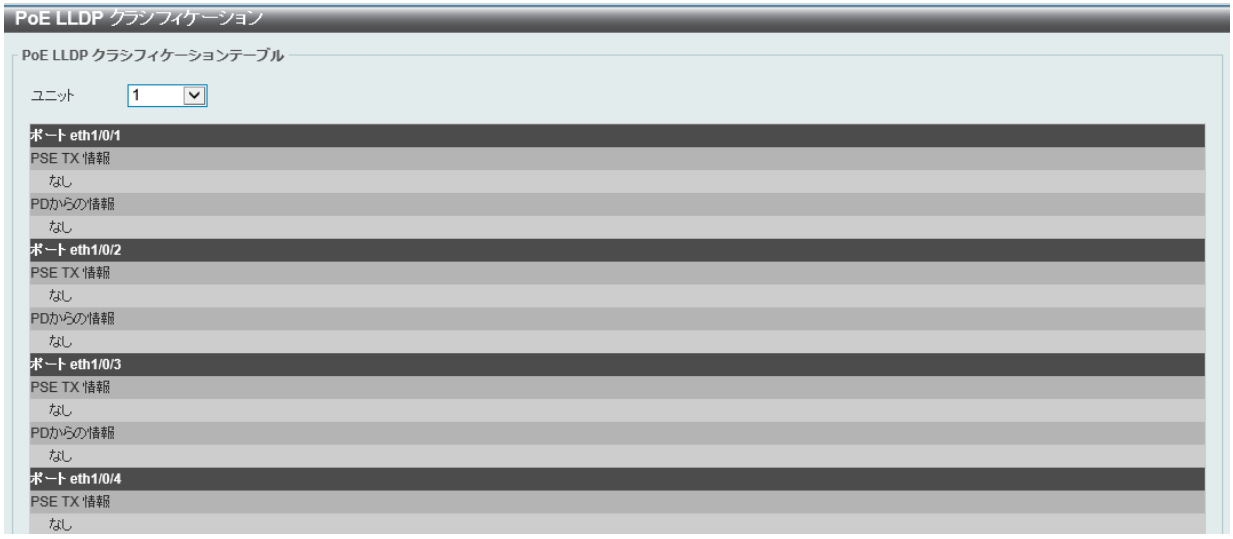


図 6-19　PoE LLDP クラシフィケーション画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。

システムログ

システムログの設定を行います。

システムログ設定

システムログ機能のステータスや、ログの保存方法などを設定します。

システム > システムログ > システムログ設定の順にメニューをクリックし、以下の画面を表示します。



図 6-20　システムログ設定画面

画面に表示される項目：

項目	説明
ログステート	
ログステート	シスログのグローバルステータスを有効 / 無効に指定します。
送信元インタフェース設定	
送信元インタフェースステート	送信元インタフェースのグローバルステータスを有効 / 無効に指定します。
タイプ	インタフェースの種類を選択します。 • 選択肢：「ループバック」「MGMT」「VLAN」
インタフェース ID	インタフェース ID を指定します。管理（MGMT）インタフェースの場合、この値は常に「0」です。 • ループバックインタフェースの設定可能範囲：1-8 • VLAN インタフェースの設定可能範囲：1-4094
バッファログ設定	
バッファログステート	バッファログのグローバルステータスを指定します。 • 選択肢：「有効」「無効」「初期値」 「初期値」を選択するとバッファログのグローバルステータスは初期設定のまま動作します。

項目	説明
セベリティ	ログ出力される情報のレベルを選択します。 • 選択肢： 「0（緊急）」「1（アラート）」「2（クリティカル）」「3（エラー）」「4（警告）」「5（通知）」「6（情報）」「7（デバッギング）」
識別名	識別名を入力します。（15 文字以内）
書き込み遅延	フラッシュにロギングバッファを定期的に書き込む間隔を指定します。 「無限」にチェックを入れると本機能は無効になります。 • 設定可能範囲：0 - 65535（秒） • 初期値：300（秒）
コンソールログ設定	
コンソールログステート	コンソールログのグローバルステータスを有効 / 無効にします。
セベリティ	ログ出力される情報のレベルを選択します。 • 選択肢： 「0（緊急）」「1（アラート）」「2（クリティカル）」「3（エラー）」「4（警告）」「5（通知）」「6（情報）」「7（デバッギング）」
識別名	識別名を入力します。（15 文字以内）
SMTP ログ設定	
SMTP ログステート	SMTP ログのグローバルステータスを有効 / 無効にします。
セベリティ	ログ出力される情報のレベルを選択します。 • 選択肢： 「0（緊急）」「1（アラート）」「2（クリティカル）」「3（エラー）」「4（警告）」「5（通知）」「6（情報）」「7（デバッギング）」
識別名	識別名を入力します。（15 文字以内）
モニタログ設定	
モニタログステート	モニタログのグローバルステータスを有効 / 無効にします。
セベリティ	ログ出力される情報のレベルを選択します。 • 選択肢： 「0（緊急）」「1（アラート）」「2（クリティカル）」「3（エラー）」「4（警告）」「5（通知）」「6（情報）」「7（デバッギング）」
識別名	識別名を入力します。（15 文字以内）

「適用」をクリックして、設定内容を適用します。

システムログ識別設定

システムログ識別名の設定、設定内容の表示を行います。

システム > システムログ > システムログ識別設定の順にクリックし、以下の画面を表示します。

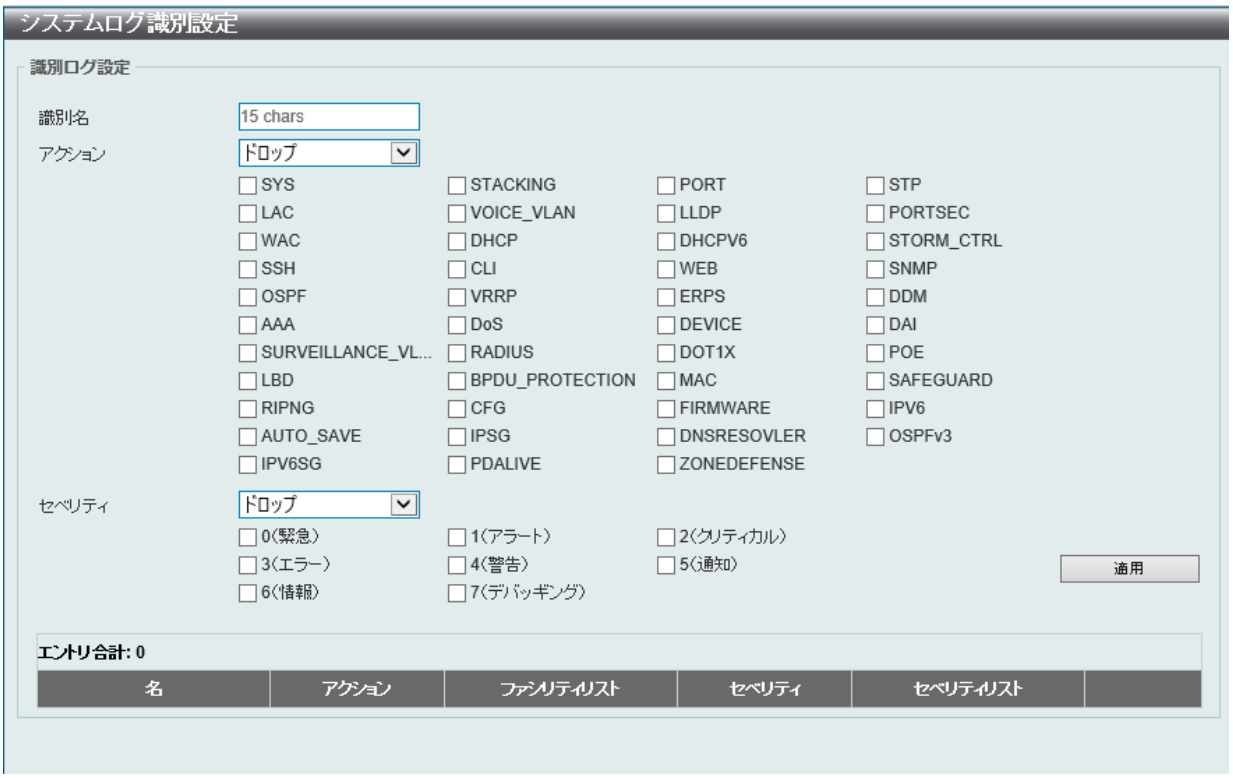


図 6-21　システムログ識別設定画面

画面に表示される項目：

項目	説明
識別名	識別名を入力します。(15 文字以内)
アクション	動作を「ドロップ」「含む」から選択します。 動作に関連づけるファシリティタイプのチェックボックスを選択します。
セベリティ	セベリティ（重要度）の動作を「ドロップ」「含む」から選択します。 ログに記録される情報の種類をチェックボックスで選択します。 • 選択肢:「0（緊急）」「1（アラート）」「2（クリティカル）」「3（エラー）」「4（警告）」「5（通知）」「6（情報）」「7（デバッギング）」

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリが削除されます。

システムログサーバ設定

シスログサーバを設定します。

システム > システムログ > システムログサーバ設定の順にクリックし、以下の画面を表示します。



図 6-22　システムログサーバ設定画面

画面に表示される項目：

項目	説明
ホスト IPv4 アドレス	システムログサーバの IPv4 アドレスを設定します。
ホスト IPv6 アドレス	システムログサーバの IPv6 アドレスを設定します。
UDP ポート	システムログサーバの UDP ポートを設定します。 • 設定可能範囲：514、1024-65535 • 初期値：514
セベリティ	ログ出力される情報のレベルを選択します。 • 選択肢： 「0（緊急）」「1（アラート）」「2（クリティカル）」「3（エラー）」「4（警告）」「5（通知）」「6（情報）」「7（デバッギング）」
Facility	ログ出力されるファシリティの番号を選択します。 • 設定可能範囲 :0 - 23
識別名	識別名を入力します。（15 文字以内）

Facility 値	Facility 名	Facility 概要
0	kern	カーネルメッセージ
1	user	ユーザレベルメッセージ
2	mail	メールシステム
3	daemon	システム daemon
4	auth1	セキュリティ / 権限メッセージ 1
5	syslog	Syslog により内部生成されたメッセージ
6	lpr	ラインプリンタサブシステム
7	news	ネットワークニュースサブシステム
8	uucp	UUCP サブシステム
9	clock1	クロック daemon 1
10	auth2	セキュリティ / 権限メッセージ 2
11	ftp	FTP daemon
12	ntp	NTP サブシステム
13	logaudit	ログ検査
14	logalert	ログ警告
15	clock2	クロック daemon 2
16	local0	ローカル使用 0（local0）
17	local1	ローカル使用 1（local1）
18	local2	ローカル使用 2（local2）
19	local3	ローカル使用 3（local3）
20	local4	ローカル使用 4（local4）
21	local5	ローカル使用 5（local5）
22	local6	ローカル使用 6（local6）
23	local7	ローカル使用 7（local7）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリが削除されます。

システムログ

システムログの閲覧 / 消去を行います。

システム > システムログ > システムログの順にメニューをクリックし、以下の画面を表示します。

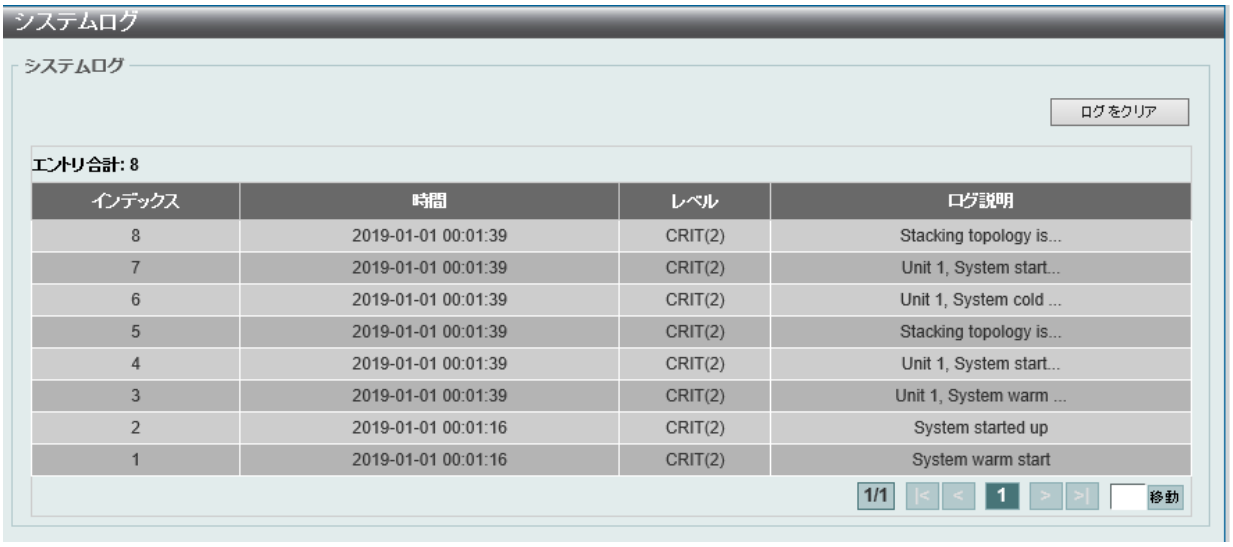


図 6-23　システムログ画面

「移動」をクリックすると、次のページへ移動します。
「ログをクリア」をクリックして、表示画面内のすべてのエントリをクリアします。

システム攻撃ログ

システム攻撃ログの閲覧、消去を行います。

システム > システムログ > システム攻撃ログの順にクリックし、以下の画面を表示します。



図 6-24　システム攻撃ログ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。

「攻撃ログをクリア」をクリックして、表示画面内のすべてのエントリをクリアします。

時間と SNTP

システム > 時間と SNTP
スイッチの時刻設定を行います。手動または SNTP サーバにより時刻を設定することができます。

注意 DGS-1520 シリーズは、リアルタイムクロック（RTC）を持っていないため、手動で設定する場合は、再起動後時刻を再設定する必要があります。

時刻設定

スイッチの時刻を設定します。

システム > 時間と SNTP > 時刻設定の順にクリックし、以下の画面を表示します。

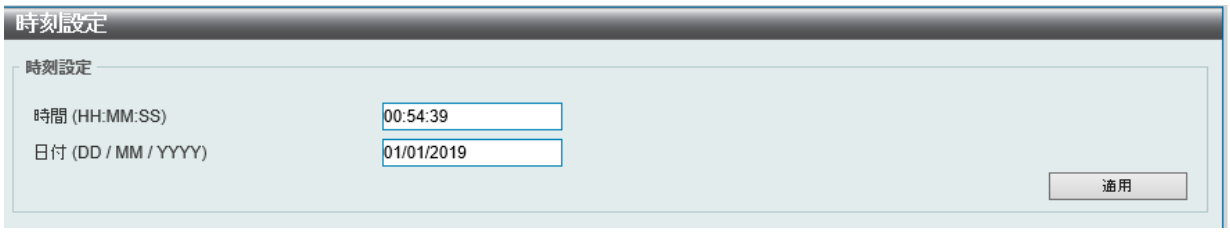


図 6-25　時刻設定画面

画面に表示される項目：

項目	説明
時間（HH:MM:SS）	現在時刻を入力します。フォーマットは「時 : 分 : 秒」です。（例：「18:30:30」）
日付（DD/MM/YYYY）	現在の日付を入力します。フォーマットは「日 / 月 / 年」です。（例：「30/04/2015」

「適用」をクリックして、設定内容を適用します。

タイムゾーン設定

SNTP のタイムゾーンとサマータイム（Daylight Saving Time）の設定を行います。

システム > 時間と SNTP > タイムゾーン設定の順にメニューをクリックし、以下の設定画面を表示します。

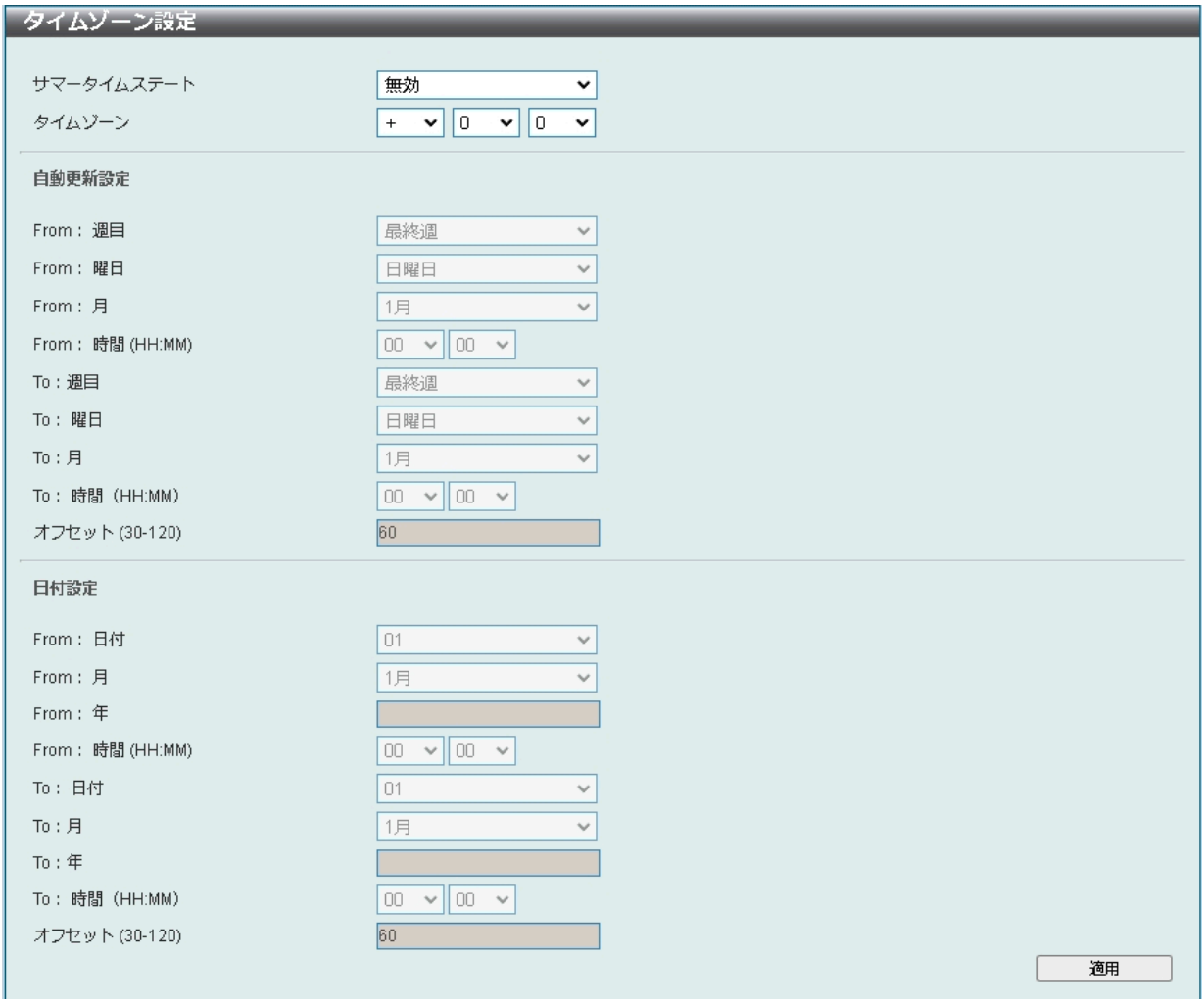


図 6-26　タイムゾーン設定画面

画面に表示される項目：

項目	説明
サマータイムステート	デバイスに設定するサマータイムの種類を選択します。 • 「無効」- サマータイムを無効にします。（初期値） • 「自動更新設定」- サマータイムを周期的に有効にします。このオプションでは、指定月の指定曜日にサマータイムが開始 / 終了します。 • 「日付設定」- サマータイムを日付指定で有効にします。このオプションでは、指定年月日にサマータイムが開始 / 終了します。
タイムゾーン	ローカルタイムゾーンの UTC からのオフセットを指定します。
自動更新設定	
「自動更新設定」モードを使用すると、サマータイムの設定を指定した期間で自動的に調整できるようになります。 例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。	
From: 週目	月の第何週から DST が始まるかを設定します。 • 「最終週」- 月の最後の週に設定します。 • 「第 1 週」- 月の最初の週に設定します。 • 「第 2 週」- 月の 2 番目の週に設定します。 • 「第 3 週」- 月の 3 番目の週に設定します。 • 「第 4 週」- 月の 4 番目の週に設定します。
From: 曜日	サマータイムが開始する曜日を指定します。
From: 月	サマータイムが開始する月を指定します。
From: 時間 (HH:MM)	サマータイムが開始する時間を指定します。
To: 週目	月の第何週でサマータイムが終わるかを設定します。 • 「最終週」- 月の最後の週に設定します。 • 「第 1 週」- 月の最初の週に設定します。 • 「第 2 週」- 月の 2 番目の週に設定します。 • 「第 3 週」- 月の 3 番目の週に設定します。 • 「第 4 週」- 月の 4 番目の週に設定します。
To: 曜日	サマータイムが終了する曜日を指定します。
To: 月	サマータイムが終了する月を指定します。
To: 時間 (HH:MM)	サマータイムが終了する時間を指定します。
オフセット	サマータイムに追加する時間を以下から指定します。 • 選択肢：「30」「60」「90」「120」（分） • 初期値：60（分）
日付設定	
From: 日付	サマータイムが始まる月日を指定します。
From: 月	サマータイムが開始する月を指定します。
From: 年	サマータイムが開始する年を指定します。
From: 時間 (HH:MM)	サマータイムが開始する時間を指定します。
To: 日付	サマータイムが修了する月日を指定します。
To: 月	サマータイムが終了する月を指定します。
To: 年	サマータイムが終了する年を指定します。（毎年）
To: 時間 (HH:MM)	サマータイムが終了する時間を指定します。（毎年）
オフセット	サマータイムに追加する時間を以下から指定します。 • 選択肢：「30」「60」「90」「120」（分） • 初期値：60（分）

「適用」をクリックして、設定内容を適用します。

SNTP 設定

SNTP（Simple Network Time Protocol ）は、インターネット経由でコンピュータのクロックに同期するプロトコルです。標準時と周波数標準サービスへのアクセス、サーバとクライアントの SNTP サブネットの体系付け、および各関連機器のシステムクロックの調整を行う包括的なメカニズムを提供します。

システム > 時間と SNTP > SNTP 設定の順にクリックし、以下の画面を表示します。



図 6-27　SNTP 設定画面

画面に表示される項目：

項目	説明
SNTP グローバル設定	
現在の時間ソース	現在の日付と時刻の提供元を表示します。
SNTP ステート	SNTP を有効 / 無効にします。
ポーリング間隔	同期する間隔を指定します。 • 設定可能範囲：30 - 99999（秒） • 初期値：720（秒）
SNTP サーバ設定	
IPv4 アドレス	SNTP 情報の取得元であるサーバの IPv4 アドレスを設定します。
IPv6 アドレス	SNTP 情報の取得元であるサーバの IPv6 アドレスを設定します。

「適用」をクリックして、設定内容を適用します。
「追加」をクリックして SNTP サーバを追加します。
「削除」をクリックして指定のエントリを削除します。

注意　DGS-1520 シリーズはリアルタイムクロック（RTC）を持っていません。そのため、タイムレンジ等、時刻に依存する機能は SNTP により時刻同期されるまで正常に動作しません。

タイムレンジ

スイッチのタイムレンジを設定します。

注意 DGS-1520 シリーズはリアルタイムクロック（RTC）を持っていないため、タイムレンジの設定は時刻の同期後に行ってください。

システム > タイムレンジ の順にメニューをクリックし、以下の画面を表示します。



図 6-28　タイムレンジ画面

画面に表示される項目：

項目	説明
レンジ名	タイムレンジのプロファイル名を入力します。(32 文字以内)
From 週 / To 週	タイムレンジに使用する「始まり」と「終わり」の曜日を指定します。 「毎日」にチェックを入れると「毎日」がタイムレンジとして指定されます。 「平日終わり」にチェックを入れると「始まり」に指定された日から週の最後（日曜日）までがタイムレンジになります。
From 時間 / To 時間	タイムレンジに使用する「始まり」と「終わり」の時間を指定します。ドロップダウンメニューから時間と分を指定します。

「適用」をクリックして、設定内容を適用します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
関連情報を入力して「検索」をクリックすると指定のエントリを検索できます。

エントリの削除
削除するエントリ横の「削除」をクリックすると該当エントリは削除されます。
削除するエントリ横の「周期を削除」をクリックすると定期エントリは削除されます。

リセットボタンの設定

リセット /ZTP ボタンの動作を設定します。

システム > **リセットボタン設定**の順にメニューをクリックし、以下の画面を表示します。

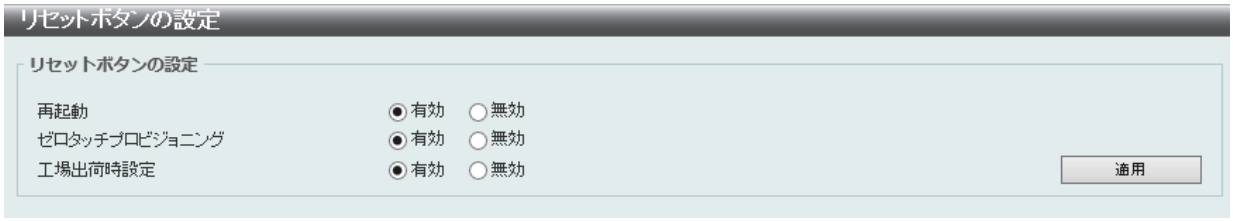


図 6-29　リセットボタンの設定画面

画面に表示される項目：

項目	説明
リセットボタンの設定	
再起動	リセットボタンのリブート機能を有効または無効にします。 有効にした場合、スイッチのリセット /ZTP ボタンを 0 - 5 秒間押すと、スイッチが再起動します。
ゼロタッチプロビジョニング	リセットボタンの ZTP（Zero Touch Provisioning）機能を有効または無効にします。 有効にした場合、スイッチのリセット /ZTP ボタンを 5 - 10 秒間押すと、ZTP が開始されます。
工場出荷時設定	有効にした場合、スイッチのリセット /ZTP ボタンを 10 秒以上押すと、スイッチが工場出荷時の設定にリセットされます。

「適用」をクリックして、設定内容を適用します。

第 7 章　管理

以下は、管理サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
コマンドロギング	コマンドログ設定を有効にします。コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
ユーザアカウント設定	スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。
パスワード暗号化	パスワードを暗号化し設定ファイルに保存します。
パスワードリカバリ	パスワードリカバリを行います。例えば管理者がパスワードを忘れた場合に有効です。
ログイン方法	各管理インタフェースでのログイン方法について設定します。
SNMP 設定	SNMP 設定を有効にします。本スイッチシリーズは、SNMP v1、v2c、および v3 をサポートしています。
RMON 設定	SNMP 機能に対するリモートモニタリング（RMON）ステータスを有効にします。
Telnet/Web 設定	スイッチに Telnet/Web 設定を有効にします。
セッションタイムアウト	各セッション（Web やコンソールなど）のタイムアウトの設定をします。
DHCP 設定	スイッチの DHCP について設定します。
DHCP 自動設定	DHCP 自動コンフィグ機能の設定を行います。
DHCP 自動イメージ設定	DHCP 自動イメージ設定を行います。スタートアップ時に、外部サーバからイメージファイルを取得する機能です。
DNS	DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
NTP	スイッチの時刻を同期するための NTP プロトコルの設定を行います。
IP 送信元インタフェース	IP 送信元インタフェースの設定を行います。
ファイルシステム設定	フラッシュファイルシステムにファームウェア、コンフィグレーションファイルなどの保存を行います。
スタッキング設定	物理スタッキングの設定を行います。
仮想スタック設定（SIM）	仮想（SIM）スタッキングの設定を行います。
D-Link ディスカバリプロトコル	D-Link ディスカバリプロトコル（DDP）の設定を行います。
SMTP 設定	Simple Mail Transfer Protocol（SMTP）の設定を行います。
NLB FDB 設定	ネットワークロードバランシング（NLB）の設定を行います。

コマンドロギング

コマンドログ設定を有効または無効にします。
コマンドログ出力機能は、コマンドラインインタフェースを通じてスイッチへの設定が成功したコマンドをログに出力するために使用されます。
システムログには、コマンド及びコマンドを入力したユーザ情報が含まれます。
スイッチの設定または操作で変更を引き起こさないコマンド（例 : show）はログに出力されません。

管理 > コマンドロギング の順にメニューをクリックし、以下の画面を表示します。



図 7-1　コマンドロギングステート画面

画面に表示される項目：

項目	説明
コマンドロギングステート	コマンドログ機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

ユーザアカウント設定

ユーザアカウントの作成と更新を行います。アクティブなユーザのセッションを確認することもできます。
Web UI で利用可能な設定オプションは、アカウントの権限レベルによって異なります。

管理 > ユーザアカウント設定の順にクリックし、次の画面を表示します。



図 7-2　ユーザアカウント設定 - ユーザ管理設定画面

画面に表示される項目：

項目	説明
ユーザ名	ユーザ名を定義します。（32 文字以内）
特権	アカウントの権限レベルを指定します。 • 設定可能範囲：1-15
パスワード形式	アカウントで使用する暗号化の方法を以下から選択します。 • 選択肢：「なし」「平文」「暗号化 -SHA1」「暗号化 -MD5」
パスワード	アカウントで使用するパスワードを入力します。

「適用」をクリックして、設定内容を適用します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

エントリの削除
削除するエントリ横の「削除」をクリックすると該当エントリは削除されます。

セッションテーブル

「セッションテーブル」タブをクリックするとユーザアカウントの現在の状況が表示されます。

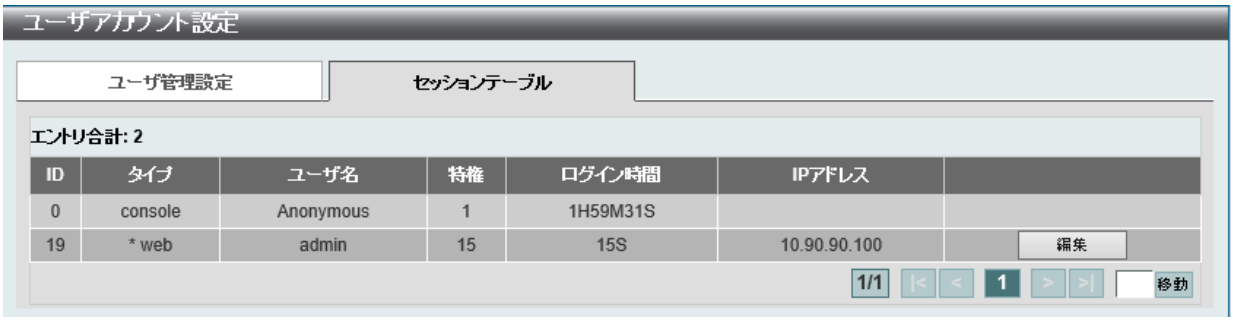


図 7-3　ユーザアカウント設定 - セッションテーブル画面

■ ユーザ権限

「セッションテーブル」タブで「編集」をクリックするとユーザ権限設定が表示されます。

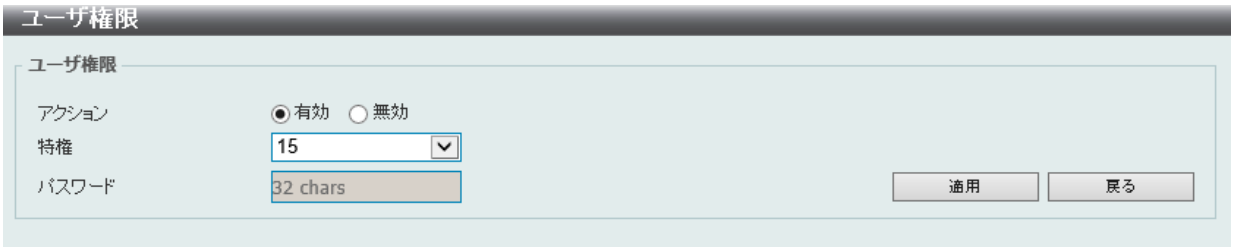


図 7-4　ユーザアカウント設定 - ユーザ権限画面

画面に表示される項目：

項目	説明
アクション	ユーザレベルのセキュリティ設定を有効 / 無効に設定します。
特権	アカウントの権限レベルを指定します。 • 設定可能範囲：1-15
パスワード	パスワードを入力します。(32 文字以内)

「適用」をクリックして、設定内容を適用します。
前の画面に戻るには、「戻る」をクリックします。

パスワード暗号化

パスワードを暗号化して設定ファイルに保存します。

管理 > パスワード暗号化の順にクリックし、次の画面を表示します。



図 7-5　パスワード暗号化画面

画面に表示される項目：

項目	説明
パスワード暗号化ステート	コンフィグファイル保存時のパスワード暗号化を有効 / 無効を設定します。
パスワード形式	パスワード暗号化を有効すると、次のオプションが選択可能です。 • 「暗号化 -SHA1」-「SHA-1」を使用してパスワードを暗号化します。 • 「暗号化 -MD5」-「MD-5」を使用してパスワードを暗号化します。

「適用」をクリックして、設定内容を適用します。

パスワードリカバリ

パスワードリカバリの設定を行います。管理者がパスワードを忘れた場合などにアカウントの更新が必要になります。

管理 > パスワードリカバリの順にクリックし、次の画面を表示します。



図 7-6　パスワードリカバリ画面

画面に表示される項目：

項目	説明
パスワードリカバリ	パスワードリカバリを有効 / 無効に設定します。有効にすると、CLI でのリセットコンフィグレーションモードへのアクセスが可能になります。リセットコンフィグモードでは以下の内容を実行できます。 - ユーザアカウントの更新 - 管理者権限レベルの enable password 機能の更新 - AAA 機能を無効にしてローカル認証を許可 その後、実行中のコンフィグレーションをブートコンフィグとして保存することが可能です。再起動が必要です。

「適用」をクリックして、設定内容を適用します。

ログイン方法

各管理インタフェースでのログイン方法について表示、設定します。

管理 > ログイン方法の順にクリックし、次の画面を表示します。



図 7-7　ログイン方法画面

画面に表示される項目：

項目	説明
パスワードを有効化	
レベル	ユーザの権限レベルを指定します。 • 設定可能範囲：1-15
パスワード形式	暗号化の方法を選択します。 • 選択肢：「平文」「暗号化 -SHA1」「暗号化 -MD5」
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。 • 「平文」選択時：32 文字以内（大文字と小文字を区別、スペースを含める） • 「暗号化 -SHA1」選択時：35 バイト（大文字と小文字を区別） • 「暗号化 -MD5」選択時：31 バイト（大文字と小文字を区別）
ログイン方法	
ログイン方法	「編集」をクリックしてパラメータの設定を行います。指定のアプリケーションへのログイン方法を選択します。 •「ログインなし」- 指定アプリケーションへアクセスするためのログイン認証は不要です。 •「ログイン」- 指定アプリケーションへアクセスするにはパスワードを入力する必要があります。 •「ローカルログイン」- 指定アプリケーションへアクセスするにはユーザ名とパスワードの入力が必要になります。
ログインパスワード	
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。 • 選択肢：「コンソール」「Telnet」「SSH」
パスワード形式	暗号化の方法を選択します。 • 選択肢：「平文」「暗号化 -SHA1」「暗号化 -MD5」
パスワード	選択したアプリケーションで使用するパスワードを入力します。 指定のアプリケーションのログイン方法が「ログイン」に設定されている時のパスワードになります。 •「平文」選択時：32 文字以内（大文字と小文字を区別、スペースを含める） •「暗号化 -SHA1」選択時：35 バイト（大文字と小文字を区別） •「暗号化 -MD5」選択時：31 バイト（大文字と小文字を区別）

「適用」をクリックして、設定内容を適用します。
「編集」をクリックすると、設定内容を編集できます。

エントリの削除
削除するエントリ横の「削除」をクリックすると該当エントリは削除されます。

SNMP 設定

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルです。ネットワークに接続された通信機器の管理や監視を行います。

SNMP によって、ネットワーク管理ステーションはゲートウェイやルータなどのネットワークデバイスの設定状態の確認・変更をすることができます。適切な動作のためにシステム機能を設定、パフォーマンスを監視し、スイッチやスイッチグループおよびネットワークの潜在的な問題を検出します。

SNMP をサポートするデバイスは、SNMP エージェントと呼ばれるソフトウェアを実装しています。
定義された変数（管理対象オブジェクト）が SNMP エージェントに保持され、デバイスの管理に使用されます。これらの管理オブジェクトは MIB（Management Information Base）内に定義され、SNMP エージェントにより管理される情報表示の基準を管理ステーションに伝えます。
SNMP は、MIB の仕様フォーマット、およびネットワーク経由で情報にアクセスするために使用するプロトコルの両方を定義しています。

■ SNMP のバージョンについて

SNMP には、「SNMPv1」「SNMPv2c」「SNMPv3」の 3 つのバージョンがあります。
これらの 3 つのバージョンでは、ネットワーク管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルが異なります。

注意　本製品がサポートしている SNMP のバージョンは SNMPv1、SNMPv2c、SNMPv3 です。

● SNMPv1 と SNMPv2c

SNMPv1 と SNMPv2c では、SNMP のコミュニティ名を使用して認証を行います。
リモートユーザの SNMP アプリケーションとスイッチの SNMP は同じコミュニティ名を使用する必要があります。認証が行われていない SNMP パケットを受信した場合、そのパケットは破棄されます。
SNMPv1 と SNMP v2c を使用する場合、初期値のコミュニティ名は以下のとおりです。

- public：管理ステーションは、MIB オブジェクトの読み取りができます。
- private： 管理ステーションは、MIB オブジェクトの読み取りと書き込みができます。

● SNMPv3

SNMPv3 では、2 つのパートで構成される、より高度な認証を行います。
最初のパートは SNMP マネージャとして動作することのできるユーザとその属性を掲載したリストを保持しています。次のパートではリスト上のユーザの SNMP マネージャとしての権限を記載しています。

ユーザのグループをリストにまとめ、権限を設定できます。また、リスト上の SNMP マネージャのグループに対して、SNMP バージョン情報を登録可能です。「SNMPv1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ」や、「SNMPv3 を使用して高いセキュリティレベルを与え、読み書き可能にするグループ」など、グループごとに異なる設定を登録することができます。

個別のユーザや SNMP マネージャグループに SNMPv3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。
管理機能の可否は各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMPv3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。

トラップ

トラップは、スイッチ上で発生したイベントをネットワーク管理者に警告するためのメッセージです。

イベントには、再起動（誤ってスイッチの電源を切ってしまった）などの重大なものから、ポートの状態変化を知らせる軽微なものまで幅広い種類があります。スイッチはトラップを生成し、事前に設定された IP アドレスに送信します。トラップの例には、認証の失敗、トポロジの変化などがあります。

MIB

MIB（Management Information Base）には、管理情報およびカウンタ情報が格納されています。

本製品は標準 MIB-II モジュールを使用し、MIB オブジェクトの値を SNMP ベースのネットワーク管理ソフトウェアにより取得します。本製品は、標準 MIB-II に加えて、拡張 MIB としてベンダ固有の MIB もサポートしています。MIB OID の指定によってもベンダ固有の MIB を取得することができます。
MIB の値には「読み取り専用」「読み書き可能」があります。

SNMP グローバル設定

SNMP グローバル設定とトラップ設定を行います。

管理 > SNMP > SNMP グローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-8　SNMP グローバル設定画面

画面に表示される項目：

項目	説明
SNMP グローバル設定	
SNMP グローバル状態	SNMP 機能を有効 / 無効に設定します。
SNMP 応答ブロードキャストリクエスト	SNMP GetRequest パケットのブロードキャストに対応するサーバを有効 / 無効に指定します。
SNMP UDP ポート	SNMP UDP ポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：161
トラップ送信元インタフェース	SNMP トラップパケットを送信する送信元アドレスとしての IP アドレスのインタフェースを入力します。
トラップ設定	
トラップグローバルステート	SNMP トラップを有効 / 無効にします。
SNMP 認証トラップ	SNMP 認証失敗の通知を有効 / 無効に設定します。 機器が正しく認証されていない SNMP メッセージを受信すると、authenticationFailuretrap トラップが生成されます。認証方法は使用している SNMP のバージョンによって異なります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。
ポートリンクアップ	ポートリンクアップ通知送信の設定を行います。通信リンクのいずれかが起動すると、linkUp トラップが生成されます。
ポートリンクダウン	ポートリンクダウン通知送信の設定を行います。通信リンクのいずれかがダウンすると、linkDown トラップが生成さ れます。
Coldstart	coldStart 通知の設定を行います。
Warmstart	warmStart 通知の設定を行います。

「適用」をクリックして、設定内容を適用します。

SNMP リンクチェンジトラップ設定

SNMP リンクチェンジトラップを設定します。

管理 > SNMP > SNMP リンクチェンジトラップ設定の順にメニューをクリックし、以下の画面を表示します。



図 7-9　SNMP リンクチェンジトラップ設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を設定します。
トラップ送信	SNMP 通知トラップ送信の有効 / 無効を指定します。
トラップステート	SNMP linkChange トラップを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

SNMP ビューテーブル設定

コミュニティ名に対しビュー（アクセスできる MIB オブジェクトの集合）を割り当て、リモート SNMP マネージャがどの MIB オブジェクトにアクセスするかを定義するために使用します。

管理 > SNMP > SNMP ビューテーブル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-10　SNMP ビューテーブル設定画面

画面に表示される項目：

項目	説明
ビュー名	ビュー名を入力します。（半角英数字 32 文字以内）SNMP ビューを識別する際に使用します。
サブツリー OID	ビューの OID（Object Identifier）サブツリーを入力します。OID は、オブジェクトツリー（MIB ツリー）が SNMP マネージャによってアクセス可能な範囲かどうかを識別します。
ビュータイプ	「サブツリー OID」で指定した OID について、ビューのタイプを指定します。 ・「含める」- SNMP マネージャがアクセス可能なオブジェクトリストに含めます。 ・「除外する」- 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除外します。

「削除」をクリックすると指定のエントリが削除されます。
「追加」をクリックして SNMP ビューを追加します。

SNMP コミュニティテーブル設定

SNMP マネージャとエージェントの関係を定義する SNMP コミュニティ名の登録を行います。
コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。
以下の特性の 1 つ以上をコミュニティ名に関連付けることができます。

- コミュニティ名を使用して、スイッチの SNMP エージェントにアクセスを行う SNMP マネージャの IP アドレスを含むアクセスリスト
- SNMP コミュニティがアクセスできる MIB オブジェクトのサブセットを定義する MIB ビュー
- SNMP コミュニティにアクセス可能な MIB オブジェクトの「読み取り / 書き込み」または「読み取り専用」レベルのアクセス許可

エントリの設定
「SNMP コミュニティテーブル設定」画面でコミュニティエントリを設定します。

管理 > SNMP > SNMP コミュニティテーブル設定の順にクリックし、以下の画面を表示します。



図 7-11　SNMP コミュニティテーブル設定画面

画面に表示される項目：

項目	説明
鍵タイプ	SNMP コミュニティのキーの種類を選択します。 • 選択肢：「平文」「暗号化」
コミュニティ名	SNMP コミュニティメンバを識別するためのコミュニティ名を入力します。（32 文字以内） 本コミュニティ名は、リモートの SNMP マネージャがスイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用されます。
ビュー名	ビュー名を入力します。（32 文字以内） リモート SNMP マネージャがアクセスすることのできる MIB グループの識別に使用します。 「ビュー名」が「SNMP ビューテーブル」で定義されている必要があります。
アクセス権	アクセス権限の種類を設定します。 • 「読み取り専用」- 指定したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取りのみ可能となります。 • 「読み書き」- 指定したコミュニティ名を使用する SNMP コミュニティメンバは、スイッチの MIB の内容の読み取り、および書き込みが可能です。
IP アクセスリスト名	ユーザを制限するために使用するアクセスリストの名前を入力します。 許可されるユーザは、コミュニティ文字列を使用して SNMP にアクセスすることができます。
コンテキスト名	コンテキスト名を入力します。（32 文字以内）

「追加」をクリックして新しいエントリを追加します。
「削除」をクリックして、エントリを削除します。

SNMP グループテーブル設定

SNMP グループを登録します。
本グループは、SNMP ユーザ（「SNMP ユーザテーブル設定」）と SNMP ビューテーブル（「SNMP ビューテーブル設定」）で設定するビューを関連付けます。

管理 > SNMP > SNMP グループテーブル設定の順にメニューをクリックし、以下の画面を表示します。

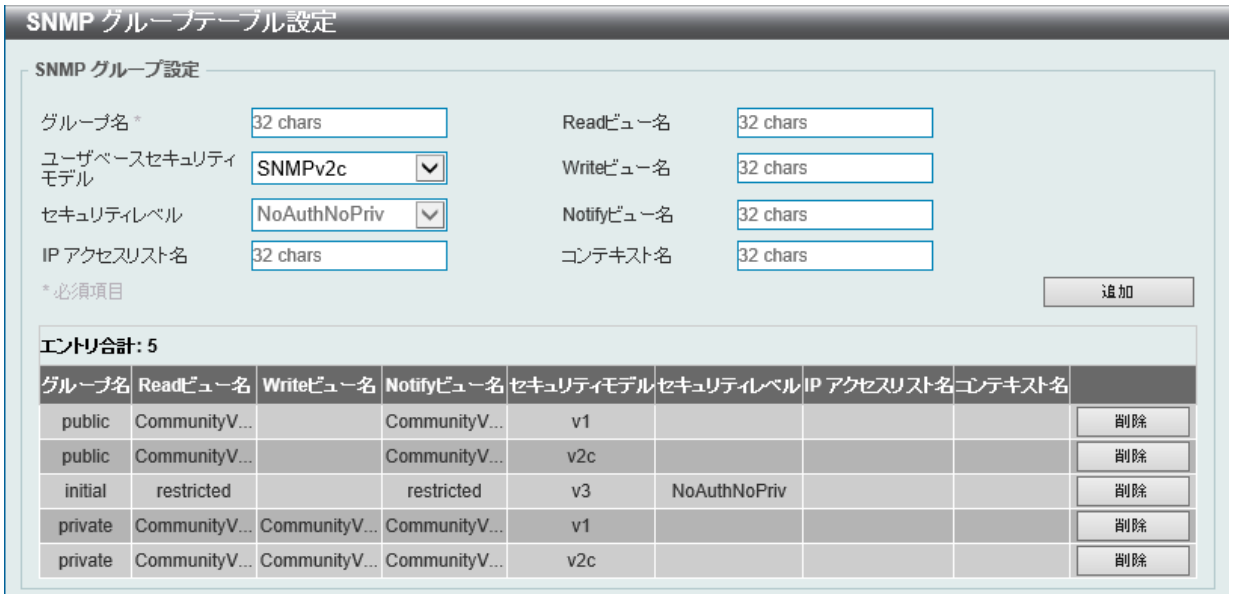


図 7-12　SNMP グループテーブル設定画面

画面に表示される項目：

項目	説明
グループ名	グループ名を指定します。（32 文字以内、スペース使用不可）
ユーザベースセキュリティモデル	セキュリティモデルを選択します。 • 「SNMPv1」- SNMP バージョン 1 を使用します。 • 「SNMPv2c」- SNMP バージョン 2c を使用します。 • 「SNMPv3」- SNMP バージョン 3 を使用します。
セキュリティレベル	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証も暗号化も行われません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証は行われますが暗号化は行われません。 「AuthPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証と暗号化が行われます。
IP アクセスリスト名	アクセスするための IP アクセスコントロールリスト（ACL）の名前を入力します。
Read ビュー名	グループのユーザがアクセス可能な Read ビュー名を入力します。
Write ビュー名	グループのユーザがアクセス可能な Write ビュー名を入力します。
Notify ビュー名	グループのユーザがアクセス可能な Notify ビュー名を入力します。 グループユーザに対しトラップパケット経由でステータスの通知が可能なオブジェクトです。
コンテキスト名	コンテキスト名を入力します。（32 文字以内）

「追加」をクリックして、新しいエントリを追加します。
「削除」をクリックして、エントリを削除します。

SNMP エンジン ID ローカル設定

エンジン ID は、SNMP バージョン 3 で使用される固有の識別名です。

管理 > SNMP > SNMP エンジン ID ローカル設定の順にメニューをクリックし、以下の画面を表示します。

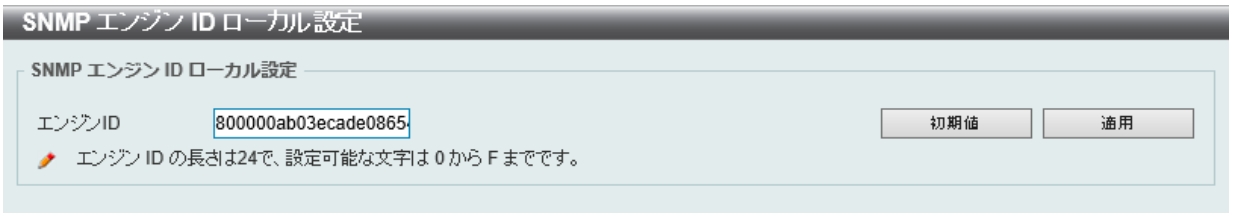


図 7-13　SNMP エンジン ID ローカル設定画面

画面に表示される項目：

項目	説明
エンジン ID	スイッチの SNMP エンジンの識別子を指定します。（24 文字以内）

新しいエンジン ID を入力し、「適用」をクリックします。
「初期値」をクリックするとエンジン ID は初期値に戻ります。

SNMP ユーザテーブル設定

SNMP ユーザの登録、表示を行います。

管理 > SNMP > SNMP ユーザテーブル設定の順にメニューをクリックし、以下の画面を表示します。

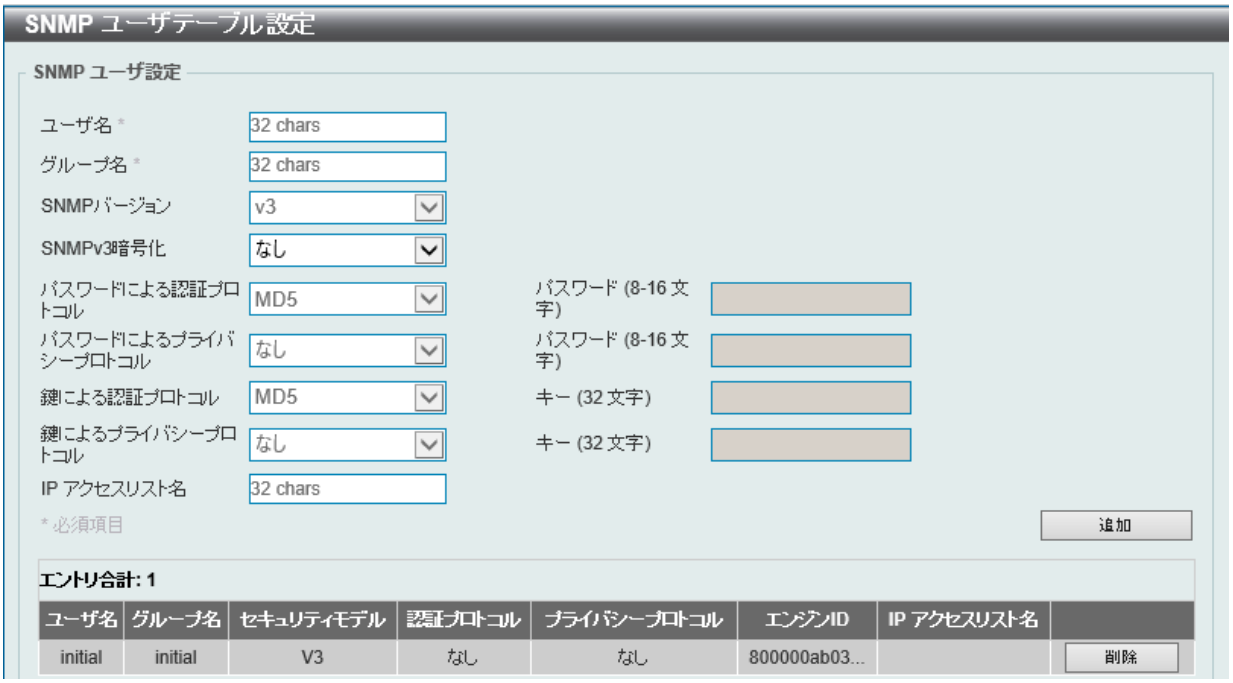


図 7-14　SNMP ユーザテーブル設定画面

画面に表示される項目：

項目	説明
ユーザ名	SNMP ユーザ名を入力します。（32 文字以内）
グループ名	ユーザが属する SNMP グループ名を入力します。（32 文字以内）
SNMP バージョン	SNMPv3 が選択されています。
SNMPv3 暗号化	SNMPv3 暗号化のタイプを選択します。 • 選択肢：「なし」「キー」「パスワード」
パスワードによる認証プロトコル	「SNMPv3 暗号化」で「パスワード」を選択した場合に有効になります。以下から認証プロトコルを選択後、パスワードを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。 • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。

項目	説明
パスワードによるプライバシープロコル	「SNMPv3 暗号化」で「パスワード」を選択した場合に有効になります。以下からプライバシープロトコル選択後、パスワードを入力します。 • 「なし」- 認証プロトコルは使用されません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。 • 「AES」- AES 暗号が使用されます。
鍵による認証プロコル	「SNMPv3 暗号化」で「キー」を選択した場合に有効になります。以下から認証プロトコル選択後、キーを入力します。 • 「MD5」- HMAC-MD5-96 認証レベルが使用されます。 • 「SHA」- HMAC-SHA 認証プロトコルが使用されます。
鍵によるプライバシープロトコル	「SNMPv3 暗号化」で「キー」を選択した場合に有効になります。以下からプライバシープロトコル選択後、キーを入力します。 • 「なし」- 認証プロトコルは使用されていません。 • 「DES56」- CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されます。 • 「AES」- AES 暗号が使用されます。
IP アクセスリスト名	ユーザに関連付ける標準 IP アクセスコントロールリストの名前を入力します。

「追加」をクリックして新しいエントリを追加します。
「削除」をクリックして、エントリを削除します。

SNMP ホストテーブル設定

SNMP トラップの送信先を設定します。

管理 > SNMP > SNMP ホストテーブル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-15　SNMP ホストテーブル設定画面

画面に表示される項目：

項目	説明
ホスト IPv4 アドレス	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
ホスト IPv6 アドレス	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）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	SNMP バージョンを選択します。 • 「SNMPV1」- SNMP バージョン 1 を使用します。 • 「SNMPV2c」- SNMP バージョン 2c を使用します。 • 「SNMPV3」- SNMP バージョン 3 を使用します。
セキュリティレベル	「SNMPv3」を選択した場合、セキュリティレベルを設定します。 • 「NoAuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証も暗号化も行われません。 • 「AuthNoPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証は行われますが暗号化は行われません。 • 「AuthPriv」- スイッチとリモート SNMP マネージャ間のパケットについて、認証 / 暗号化が行われます。
UDP ポート	UDP ポート番号を入力します。ポート番号によっては他のプロトコルと競合する可能性があります。 • 設定可能範囲：1 - 65535 • 初期値：162
コミュニティ列 /SNMPv3 ユーザ名	コミュニティ名または SNMP V3 ユーザ名を入力します。

「追加」をクリックして新しいエントリを追加します。
「削除」をクリックして、エントリを削除します。

SNMP コンテキストマッピングテーブル設定

SNMP コンテキストマッピングテーブルの表示、設定を行います。

管理 > SNMP > SNMP コンテキストマッピングテーブル設定の順にメニューをクリックし、以下の画面を表示します。

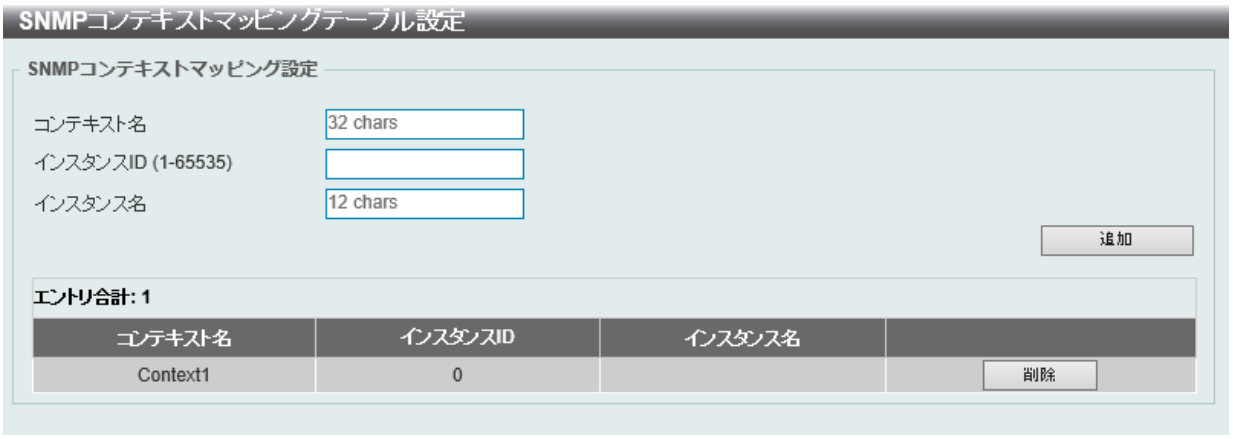


図 7-16　SNMP コンテキストマッピングテーブル設定画面

画面に表示される項目：

項目	説明
コンテキスト名	SNMP View-based Access Control Model（VACM）コンテキスト名を入力します。（32 文字以内） コンテキスト名の先頭はアルファベット、末尾はアルファベットまたは数字で設定することができます。 それ以外はアルファベット、数字、ハイフンが使用可能です。
インスタンス ID	インスタンス ID を入力します。 • 設定可能範囲：1-65535
インスタンス名	インスタンス名を入力します。（12 文字以内）

「追加」をクリックして新しいエントリを追加します。
「削除」をクリックして、エントリを削除します。

RMON 設定

スイッチの SNMP 機能に対する上昇 / 下降しきい値トラップのリモートモニタリング（RMON）ステータスを有効または無効にします。

RMON グローバル設定

管理 > RMON > RMON グローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-17　RMON グローバル設定画面

画面に表示される項目：

項目	説明
RMON 上昇アラームトラップ	「RMON」における上昇しきい値警告トラップを有効にします。
RMON 下降アラームトラップ	「RMON」における下降しきい値警告トラップを有効にします。

「適用」をクリックし、設定を適用します。

RMON 統計設定

RMON 統計情報を表示、設定します。

管理 > RMON > RMON 統計設定の順にメニューをクリックし、以下の画面を表示します。

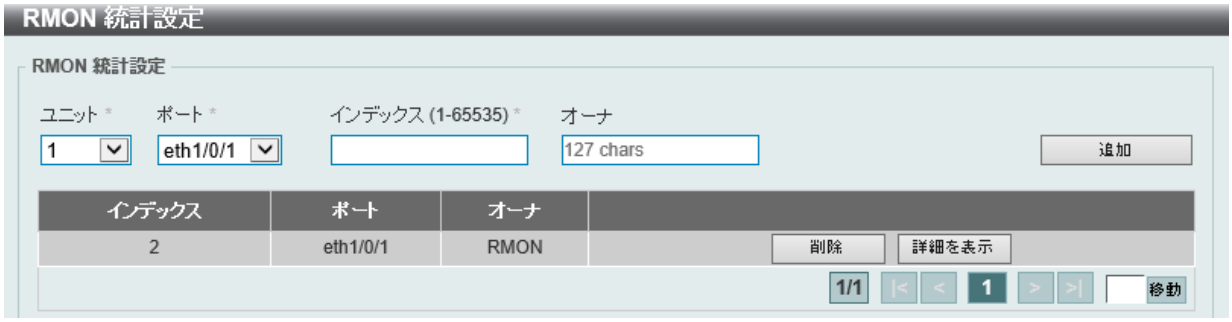


図 7-18　RMON 統計設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
ポート	設定するポートを指定します。
インデックス	RMON テーブルインデックスを入力します。 • 設定可能範囲：1-65535
オーナ	オーナの文字列を入力します。（127 文字以内）

「追加」をクリックしてエントリを追加します。
「削除」をクリックして、エントリを削除します。
「詳細を表示」をクリックして、特定のポートの VLAN の詳細情報を表示します。

設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

指定ポートの統計情報を表示する場合

「詳細を表示」をクリックします。以下の画面が表示されます。



図 7-19　RMON 統計テーブル画面

前の画面に戻るには、「戻る」をクリックします。

RMON 履歴設定

ポートで収集された RMON MIB のヒストリ（履歴）統計を表示、設定します。

管理 > RMON > RMON 履歴設定の順にメニューをクリックし、以下の画面を表示します。



図 7-20　RRMON 履歴設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
ポート	RMON 情報を取得するポートを指定します。
インデックス	ヒストリグループテーブルのインデックス番号を指定します。 • 設定可能範囲：1-65535
バケット番号	統計における RMON 収集ヒストリグループのバケット数を指定します。 • 入力可能範囲：1 - 65535 • 初期値：50
間隔	ポーリング間隔を設定します。 • 入力可能範囲：1-3600（秒） • 初期値：1800（秒）
オーナ	オーナの文字列を入力します。（127 文字以内）

「追加」をクリックしてエントリを追加します。

「削除」をクリックして、エントリを削除します。

設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

指定ポートの履歴情報を表示する場合

「詳細を表示」をクリックします。以下の画面が表示されます。



図 7-21　RMON 統計設定画面

前の画面に戻るには、「戻る」をクリックします。

RMON アラーム設定

インタフェースをモニタするためのアラームエントリを表示、設定します。

管理 > RMON > RMON アラーム設定の順にメニューをクリックし、以下の画面を表示します。



図 7-22　RMON アラーム設定画面

画面に表示される項目：

項目	説明
インデックス	アラームのインデックス番号を指定します。 • 設定可能範囲：1-65535
間隔	変数のサンプリングおよびしきい値に対するチェックの間隔を定義します。 • 設定可能範囲：0 - 2147483648（秒）
変数	サンプリング対象の MIB 変数の値を指定します。
タイプ	モニタリングのタイプを選択します。 • 選択肢：「Delta」「アブソルート」
しきい値の上限	上昇しきい値を設定します。 • 設定可能範囲：0 - 2147483647
しきい値の下限	下降しきい値を設定します。 • 設定可能範囲：0 - 2147483647
上昇イベント番号	上昇しきい値を超えたときに開始するイベントのインデックス番号を指定します。 指定しない場合、しきい値を超えてもアクションは実行されません。 • 設定可能範囲：1 - 65535
下降イベント番号	下降しきい値を超えたときに開始するイベントのインデックス番号を指定します。 指定しない場合、しきい値を超えてもアクションは実行されません。 • 設定可能範囲：1 - 65535
オーナ	オーナの文字列を入力します。（127 文字以内）

「追加」をクリックしてエントリを追加します。
「削除」をクリックして、エントリを削除します。
複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます

RMON イベント設定

RMON イベントの設定を行います。

管理 > RMON > RMON イベント設定の順にメニューをクリックし、以下の画面を表示します。



図 7-23　RMON イベント設定画面

画面に表示される項目：

項目	説明
インデックス	イベントのインデックス番号を指定します。 • 設定可能範囲：1 - 65535
説明	RMON イベントエントリの説明を入力します。（127 文字以内）
タイプ	イベントタイプを指定します。 •「なし」- イベントは発生しません。 •「ログ」- ログを出力します。 •「トラップ」- トラップを送信します。 •「ログとトラップ」- ログを出力し、トラップを送信します。
コミュニティ	コミュニティ文字列を指定します。（127 文字以内）
オーナ	オーナの文字列を入力します。（127 文字以内）

「追加」をクリックしてエントリを追加します。
「削除」をクリックして、エントリを削除します。
「ログを閲覧」をクリックすると、特定のポートの詳細情報が表示されます。
複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

指定エントリのログ情報を表示する場合

「ログを閲覧」をクリックします。以下の画面が表示されます。



図 7-24　イベントログテーブル画面

前の画面に戻るには、「戻る」をクリックします。

Telnet/Web 設定

スイッチの Telnet/Web 設定を行います。

管理 > Telnet/Web の順にメニューをクリックし、以下の画面を表示します。

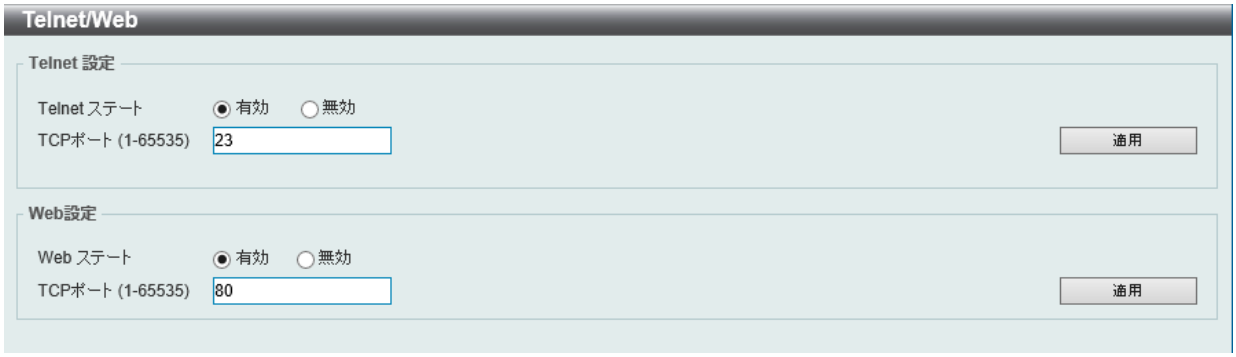


図 7-25　Telnet/Web 画面

画面に表示される項目：

項目	説明
Telnet 設定	
Telnet ステート	Telnet サーバ機能を有効 / 無効に設定します。
TCP ポート	スイッチの Telnet 管理に使用する TCP ポート番号を入力します。 Telnet プロトコルに通常使用される TCP ポートは 23 です。 • 設定可能範囲：1-65535
Web 設定	
Web ステート	Web ベースマネジメントを有効 / 無効に設定します。
TCP ポート	スイッチの Web ベースマネジメントに使用する TCP ポート番号を入力します。 Web プロトコルに通常使用される TCP ポートは 80 です。 • 設定可能範囲：1-65535

「適用」をクリックして、設定内容を適用します。

セッションタイムアウト

各セッション（Web やコンソールなど）のタイムアウトの設定をします。
外向き（outgoing）セッションのタイムアウト値は、他スイッチの Telnet インタフェースに対する CLI 経由の「Console/Telnet/SSH」接続で使用されます。

管理 > セッションタイムアウトの順にメニューをクリックし、以下の画面を表示します。



図 7-26　セッションタイムアウト画面

画面に表示される項目：

項目	説明
Web セッションタイムアウト	Web セッションのタイムアウト時間（秒）を設定します。 「初期値」にチェックを入れると初期値に戻ります。 • 設定可能範囲：60 - 36000（秒） • 初期値：180（秒）
コンソール セッションタイムアウト	コンソールセッションのタイムアウト時間（分）を設定します。 「初期値」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 - 1439（分） • 初期値：3（分）
出力コンソールセッションタイムアウト	出力（Outgoing）コンソールセッションのタイムアウト時間（分）を設定します。 「初期値」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 -1439（分） • 初期値：0（分）
Telnet セッションタイムアウト	Telnet セッションのタイムアウト時間（分）を設定します。 「初期値」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 - 1439（分） • 初期値：3（分）
出力 Telnet セッションタイムアウト	外向き（Outgoing）Telnet セッションのタイムアウト時間（分）を設定します。 「初期値」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 -1439（分） • 初期値：0（分）
SSH セッションタイムアウト	SSH セッションのタイムアウト時間（分）を設定します。 「初期値」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 - 1439（分） • 初期値：3（分）
出力 SSH セッションタイムアウト	外向き（Outgoing）SSH セッションのタイムアウト時間（分）を設定します。 「初期値」にチェックを入れると初期値に戻ります。0 に指定するとタイムアウトしません。 • 設定可能範囲：0 -1439（分） • 初期値：0（分）

「適用」をクリックして、設定内容を適用します。

DHCP 設定

スイッチの DHCP について設定します。

DHCP サービス

スイッチの DHCP サービスについて設定します。

管理 > DHCP > DHCP サービスの順にメニューをクリックし、以下の画面を表示します。



図 7-27　DHCP サービス画面

画面に表示される項目：

項目	説明
DHCP サービスステート	DHCP サービスを有効 / 無効に設定します。
IPv6 DHCP サービスステート	IPv6 DHCP サービスを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

DHCP クラス設定

DHCP クラスと、クラスに対する DHCP オプションのマッチングパターンについて表示、設定します。

管理 > DHCP > DHCP クラス設定の順にメニューをクリックし、以下の画面を表示します。

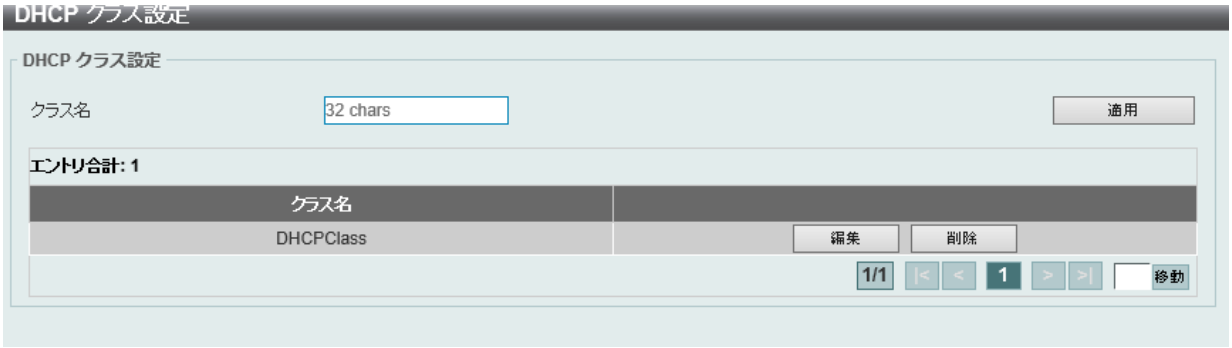


図 7-28　DHCP クラス設定画面

画面に表示される項目：

項目	説明
クラス名	DHCP クラス名を指定します。(32 文字以内)

「適用」をクリックして、設定内容を適用します。
複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。
「削除」をクリックして、エントリを削除します。

指定エントリの編集を行う場合
「編集」をクリックします。以下の画面が表示されます。

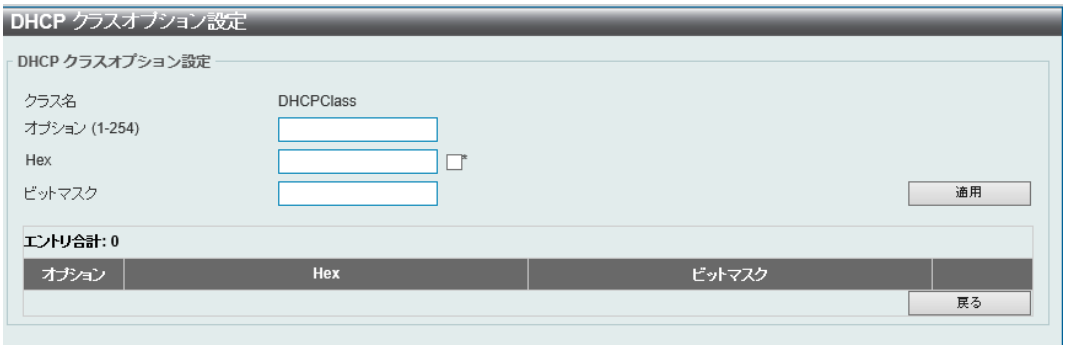


図 7-29　DHCP クラスオプション設定（編集）画面

画面に表示される項目：

項目	説明
オプション	DHCP オプション番号を指定します。 • 設定可能範囲：1-254
Hex	指定した DHCP オプションの 16 進数方式を入力します。「*」にチェックを入れると残りのオプションのビットは照合されません。
ビットマスク	16 進数ビットマスクを入力します。 マスクされたパターンのビットが照合されます。指定しない場合、16 進数のすべてのビットがチェックされます。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、エントリを削除します。
前の画面に戻るには、「戻る」をクリックします。

DHCP プール設定

DHCP プールの設定を行います。

管理 > DHCP > DHCP プール設定の順にメニューをクリックし、以下の画面を表示します。

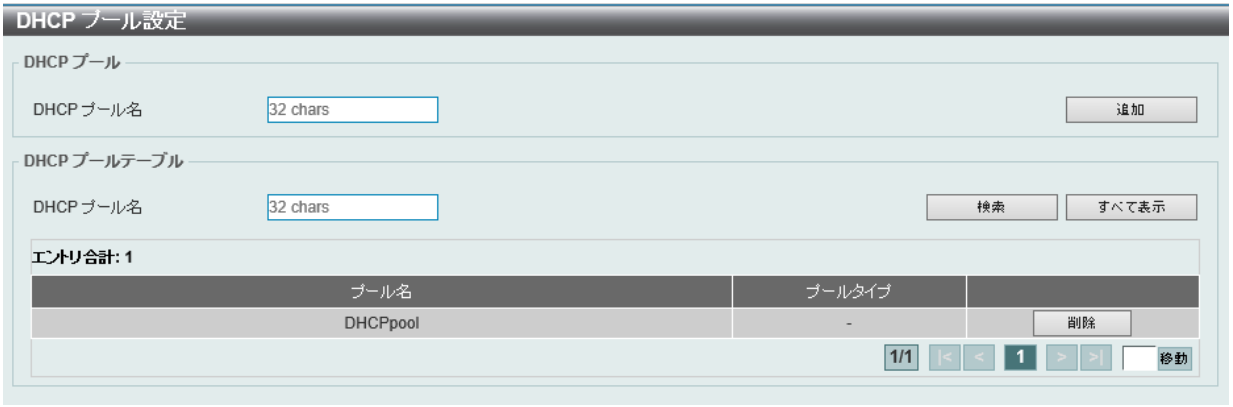


図 7-30　DHCP プール設定画面

画面に表示される項目：

項目	説明
DHCP プール名	DHCP プール名を指定します。（32 文字以内）

「追加」をクリックしてエントリを追加します。
「削除」をクリックして、エントリを削除します。

エントリの検索・表示
「検索」をクリックすると、指定のエントリを検索できます。
「すべて表示」をクリックすると、テーブル上のすべての DHCP プールを表示します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCP サーバ

管理 > DHCP > DHCP サーバ

DHCP（Dynamic Host Configuration Protocol）を使用すると、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および他の IP パラメータについて、これらの情報を要求するデバイスに発行することができます。この処理は、DHCP が有効化されたデバイスが起動またはローカルなネットワークに接続された際に実行されます。ネットワーク情報を受信するデバイスは DHCP クライアントと呼ばれ、DHCP クライアントステータスが有効な場合、IP パラメータが設定される前にネットワークにクエリメッセージを送信します。DHCP サーバがこのリクエストを受信すると、クライアントに対して IP アドレスを割り当てます。その後、DHCP クライアントは割り当てられた IP アドレスをローカル構成として使用します。

自動 IP 設定が適用されるクライアントに対して、ローカル接続ネットワークで利用するための DHCP に関連する多くのパラメータ（割り当て IP アドレスのリース時間、DHCP プールで許可される IP アドレス範囲、除外 IP アドレス）を設定することができます。また、DNS サーバやデフォルトルートの IP アドレスなど重要なデバイスに対して IP アドレスを設定することもできます。

さらに、DHCP プール内の IP アドレスを特定の MAC アドレスに割り当てることで、重要なデバイスの IP アドレスを固定することができます。

注意　DHCP サーバ機能の設定変更を行った際は、設定変更後に必ず DHCP サーバサービスの再起動を行ってください。

DHCP サーバグローバル設定

DHCP サーバグローバルパラメータを設定します。

管理 > DHCP > DHCP サーバ > DHCP サーバグローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-31　DHCP サーバグローバル設定画面

画面に表示される項目：

項目	説明
DHCP 使用クラスステート	
DHCP 使用クラスステート	DHCP Use Class ステータスを有効 / 無効に設定します。 有効にした場合、DHCP サーバはアドレス割り当てに DHCP クラスを使用します。
DHCP サーバ設定	
DHCP Ping パケット	割り当て済みの IP アドレスを含むネットワークにスイッチが送信する ping パケットの数を指定します。 ping リクエストが戻らない場合、その IP アドレスはローカルネットワークに対して固有であると見なされ、要求側クライアントに割り当てられます。0 は ping テストを行わないことを意味します。 • 設定可能範囲：0 - 10（パケット） • 初期値：2（パケット）
DHCP Ping タイムアウト	ping パケットがタイムアウトになるまでの DHCP サーバの待機時間を指定します。 • 設定可能範囲：100-10000（ミリ秒） • 初期値：500（ミリ秒）

「適用」をクリックして、設定内容を適用します。

DHCP サーバプール設定

DHCP サーバプールの設定を行います。

管理 > DHCP > DHCP サーバ > DHCP サーバプール設定の順にメニューをクリックし、以下の画面を表示します。



図 7-32　DHCP サーバプール設定画面

画面に表示される項目：

項目	説明
DHCP プール名	DHCP サーバプール名を入力します。(32 文字以内)

「検索」をクリックすると、指定のエントリを検索できます。
「全て表示」をクリックすると、テーブル上のすべての DHCP プールを表示します。
作成されたプールは、「クラスを編集」「オプションを編集」「設定」をクリックして、設定内容を編集することができます。
「削除」をクリックして、エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

エントリの編集（クラスを編集）
「クラスを編集」をクリックすると、以下の画面が表示されます。



図 7-33　DHCP サーバプールクラス設定画面

画面に表示される項目：

項目	説明
プール名	編集する DHCP プール名が表示されます。
クラス名	DHCP プールに紐づける DHCP クラス名を指定します。
開始アドレス	DHCP クラスに紐づける開始 IPv4 アドレスを指定します。
終了アドレス	DHCP クラスに紐づける終了 IPv4 アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「名前で削除」をクリックすると DHCP クラスを名前で削除します。
「アドレスで削除」をクリックすると DHCP クラスをアドレスで削除します。
前の画面に戻るには、「戻る」をクリックします。

エントリの編集（オプションを編集）

「オプションを編集」をクリックすると、以下の画面が表示されます。

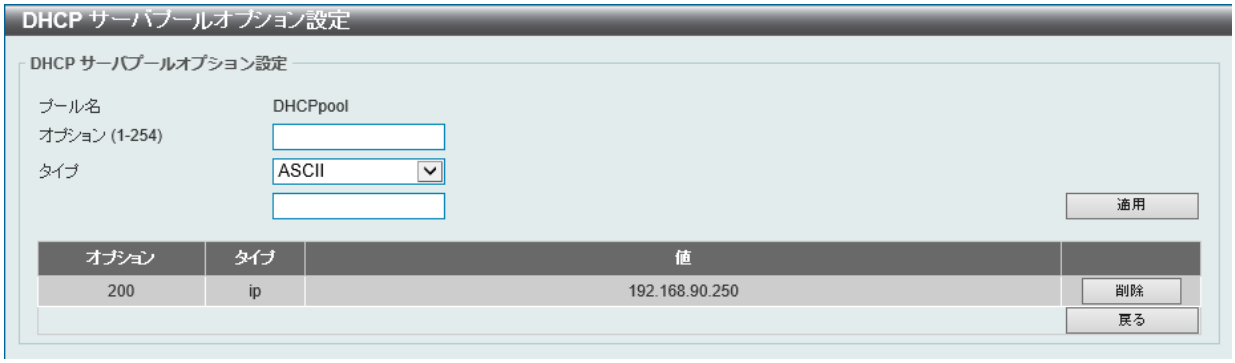


図 7-34　DHCP サーバプールオプション設定画面

画面に表示される項目：

項目	説明
プール名	編集する DHCP プール名が表示されます。
オプション	DHCP オプション番号を指定します。 • 設定可能範囲：1-254
タイプ	DHCP オプションタイプを「ASCII」「Hex」「IP」から選択し、値を入力します。 • 「ASCII」- ASCII 文字列で入力します。（255 文字以内） • 「HEX」- 16 進数文字列で入力します。（254 文字以内） • 「IP」- IPv4 アドレスを入力します。最大 8 個のアドレスを入力できます。 「Hex」を選択した場合に、長さ 0 の hex 文字列を指定する場合は、「なし」オプションにチェックを入れます。

「適用」をクリックして、設定内容を適用します。

「削除」をクリックして、指定のエントリを削除します。

前の画面に戻るには、「戻る」をクリックします。

エントリの編集（設定）

「設定」をクリックすると、以下の画面が表示されます。

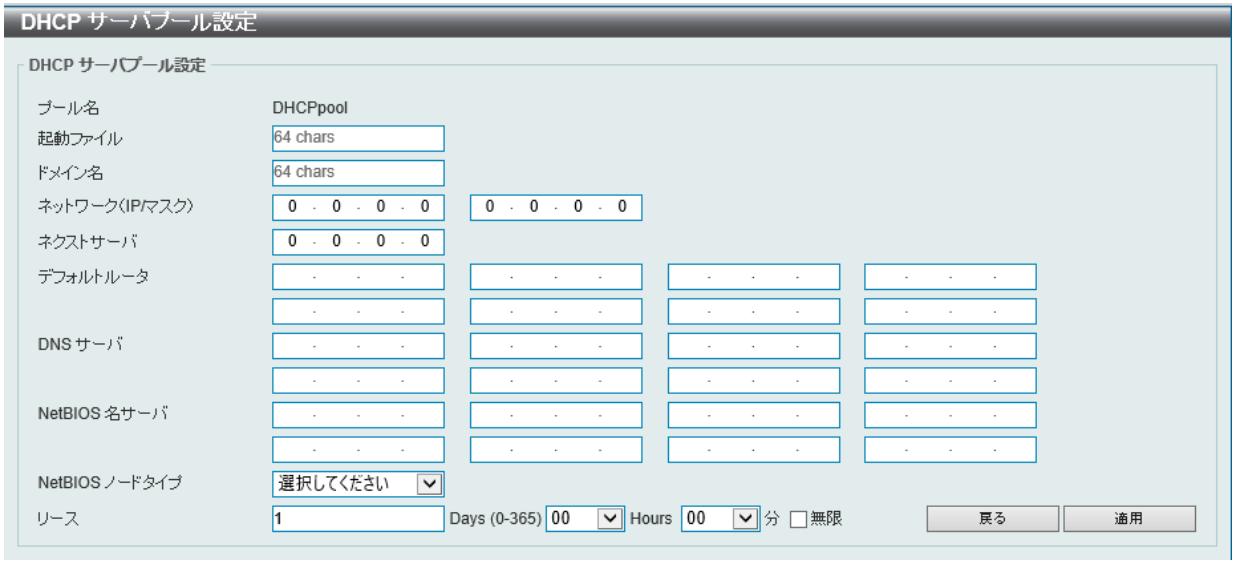


図 7-35　DHCP サーバプール設定画面

画面に表示される項目：

項目	説明
プール名	編集する DHCP プール名が表示されます。
起動ファイル	ブートイメージのファイル名を指定します。（64 文字以内）
ドメイン名	クライアントのドメイン名を入力します。（64 文字以内）
ネットワーク（IP/ マスク）	プールのネットワークアドレスと対応するネットマスクを入力します。
ネクストサーバ	ネクストサーバの IP アドレスを指定します。本サーバに格納されているブートイメージファイルが DHCP クライアントに検索されます。一般的に TFTP サーバが使用されます。ネクストサーバの IP アドレスは 1 つのみ指定できます。

項目	説明
デフォルトルータ	DHCP クライアントのデフォルトルータの IP アドレスを入力します。 ここでは最大 8 つの IP アドレスを指定できます。本ルータの IP アドレスはクライアントのサブネットと同じサブネットである必要があります。ルータは優先度の高い順に並んでいます。デフォルトルータが既に設定済みの場合、後から設定されたデフォルトルータはデフォルトインタフェースリストに追加されます。
DNS サーバ	DHCP クライアントが使用する DNS サーバの IP アドレスを入力します。 ここでは最大 8 つの IP アドレスを指定できます。DNS サーバは優先度の高い順に並んでいます。DNS サーバが既に設定済みの場合、後から設定された DNS サーバは DNS サーバリストに追加されます。
NetBIOS 名サーバ	DHCP クライアントが使用する WINS サーバの IP アドレスを指定します。 ここでは最大 8 つの IP アドレスを指定できます。サーバは優先度の高い順に並んでいます。ネームサーバが既に設定済みの場合、後から設定されたネームサーバはデフォルトインタフェースリストに追加されます。
NetBIOS ノードタイプ	マイクロソフト DHCP クライアントの NetBIOS のノードタイプを設定します。 • 「ブロードキャスト」- システムはブロードキャストを使用します。 • 「ピアツーピア」（p-node）- ネームサーバ（WINS）に対して Peer to Peer による名前クエリのみを使用します。 • 「混在」（h-nod）- まずブロードキャストを使用し、その後ネームサーバへの問い合わせを行います。 • 「Hybrid」- まずネームサーバへの問い合せを行い、その後ブロードキャストを使用します。
リース	アドレスプールから割り当てるアドレスのリース期間を指定します。 • 「Days」- リースする日数（0-365） • 「Hours」- リースする時間（時） • 「分」- リースする時間（分） • 「無限」- リース期間が無制限

「適用」をクリックして、設定内容を適用します。
前の画面に戻るには、「戻る」をクリックします。

DHCP サーバ除外アドレス

DHCP サーバがクライアントに割り当てない IP アドレスを指定します。
DHCP サーバは、DHCP アドレスプール内のアドレスを DHCP クライアントに自動的に割り当てます。 ルータ上のインタフェースの IP アドレスとここで指定された除外アドレスを除くすべてのアドレスが割り当て可能です。 複数の範囲のアドレスを除外できます。

管理 > DHCP > DHCP サーバ > DHCP サーバ除外アドレスの順にメニューをクリックし、以下の画面を表示します。



図 7-36　DHCP サーバ除外アドレス 画面

画面に表示される項目：

項目	説明
開始アドレス	除外する IP アドレス範囲の開始 IP アドレスを指定します。
終了アドレス	除外する IP アドレス範囲の終了 IP アドレスを指定します。

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。

DHCP サーバ手動バインディング

DHCP サーバの手動バインディング設定を行います。手動バインディングエントリを使用すると、IP アドレスをクライアント識別子にバインドできます。また、ホストのハードウェアアドレスにバインドすることも可能です。

管理 > DHCP > DHCP サーバ > DHCP サーバ手動バインディングの順にメニューをクリックし、以下の画面を表示します。

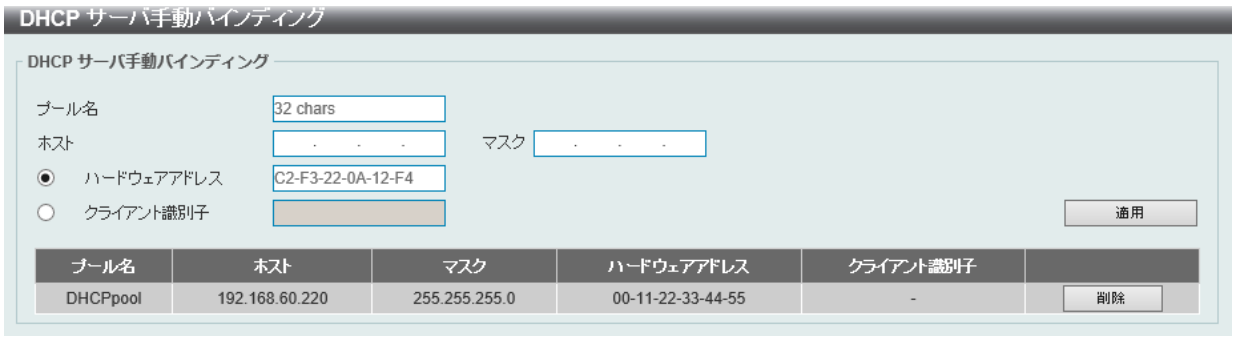


図 7-37　DHCP サーバ手動バインディング画面

画面に表示される項目：

項目	説明
プール名	DHCP サーバプール名を入力します。(32 文字以内)
ホスト	DHCP ホスト IPv4 アドレスを入力します。
マスク	DHCP ホストネットワークのサブネットマスクを入力します。
ハードウェアアドレス	DHCP ホストの MAC アドレスを入力します。
クライアント識別子	DHCP ホスト識別子を 16 進表記で入力します。 クライアント識別子は、メディアタイプと MAC アドレスによってフォーマットされます。

「適用」をクリックして、設定内容を適用します。
前の画面に戻るには、「戻る」をクリックします。
「削除」をクリックして、指定のエントリを削除します。

DHCP サーバダイナミックバインディング

DHCP サーバダイナミックバインディングテーブルの表示と削除を行います。

管理 > DHCP > DHCP サーバ > DHCP サーバダイナミックバインディングの順にメニューをクリックし、以下の画面を表示します。

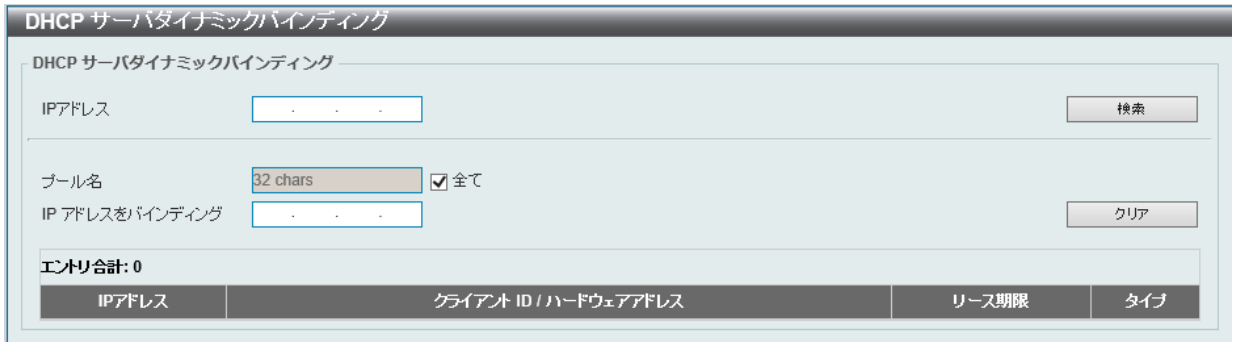


図 7-38　DHCP サーバダイナミックバインディング画面

画面に表示される項目：

項目	説明
IP アドレス	バインディングエントリの IPv4 アドレスを入力します。
プール名	DHCP サーバプール名を入力します。 「全て」オプションにチェックを入れると、全てのプールのバインディングエントリを削除します。
IP アドレスをバインディング	バインディング IP アドレスを入力します。

「クリア」をクリックして、入力した情報に基づくエントリをクリアします。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

DHCP サーバ重複 IP

DHCP サーバデータベースの DHCP 重複エントリを表示、クリアします。

管理 > DHCP > DHCP サーバ > DHCP サーバ重複 IP の順にメニューをクリックし、以下の画面を表示します。



図 7-39　DHCP サーバ重複 IP 画面

画面に表示される項目：

項目	説明
IP アドレス	検出する重複エントリの IPv4 アドレスを入力します。
プール名	DHCP サーバプール名を入力します。 「全て」オプションにチェックを入れると、全てのプールの重複エントリを削除します。

「クリア」をクリックして、本欄に入力したすべてのエントリをクリアします。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

DHCP サーバ統計

DHCP サーバの統計情報を表示します。

管理 > DHCP > DHCP サーバ > DHCP サーバ統計の順にメニューをクリックし、以下の画面を表示します。

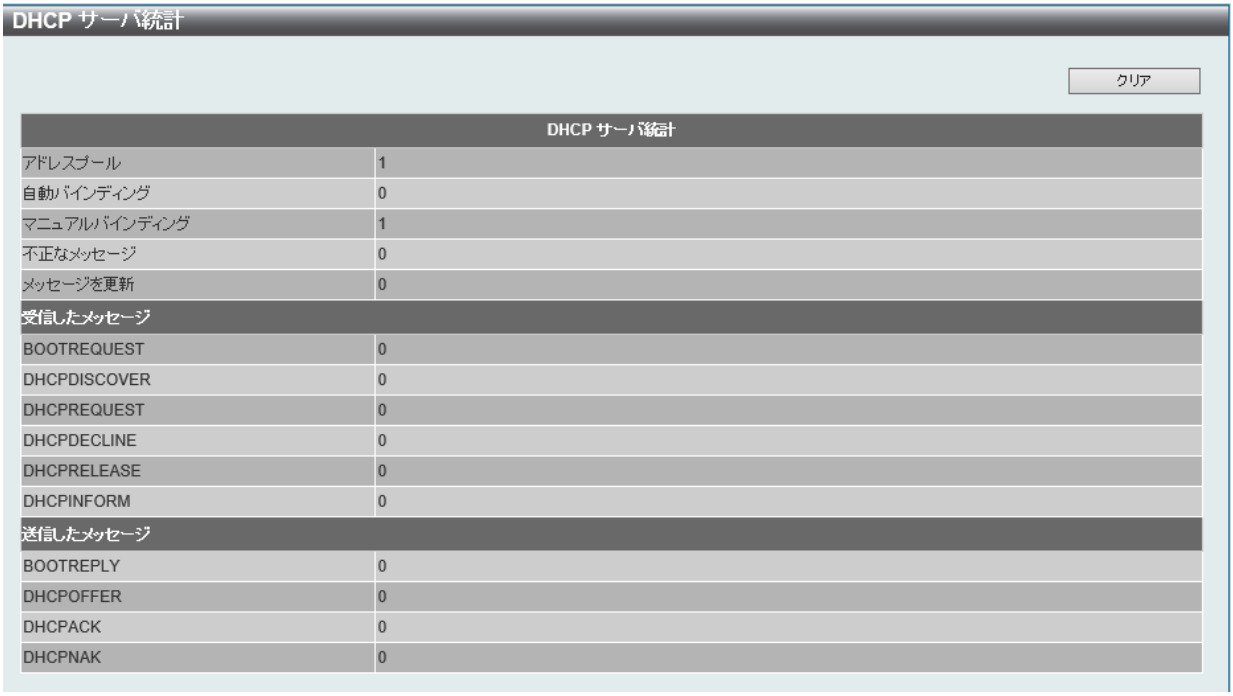


図 7-40　DHCP サーバ統計画面

「クリア」をクリックして、統計情報をクリアします。

DHCPv6 サーバ設定

管理 > DHCP > DHCPv6 サーバ

注意　DHCPv6 サーバは、接続済の IPv6 プリフィクス以外への リースは機能しません。

DHCPv6 サーバプール設定

DHCPv6 プールの作成および設定を行います。

管理 > DHCP > DHCPv6 サーバ > DHCPv6 サーバプール設定の順にメニューをクリックし、以下の画面を表示します。

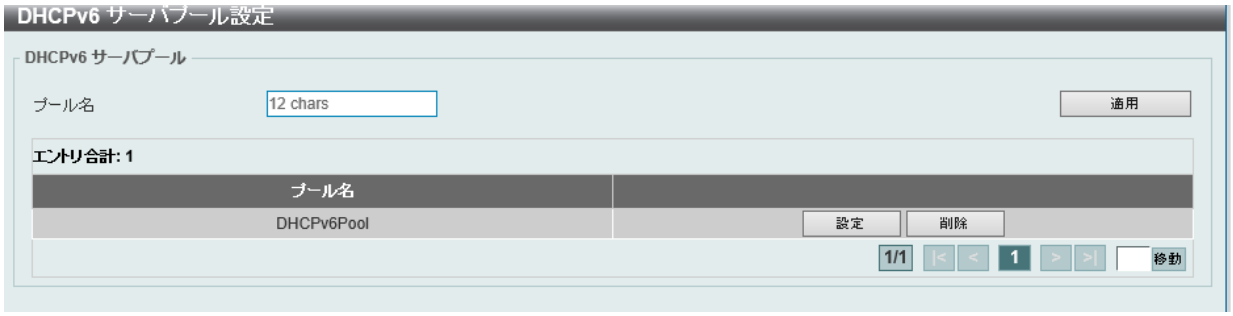


図 7-41　DHCPv6 サーバプール設定画面

画面に表示される項目：

項目	説明
プール名	DHCPv6 サーバプール名を入力します。(12 文字以内)

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。
「設定」をクリックして、該当エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

エントリの編集（設定）
「設定」をクリックすると、以下の画面が表示されます。

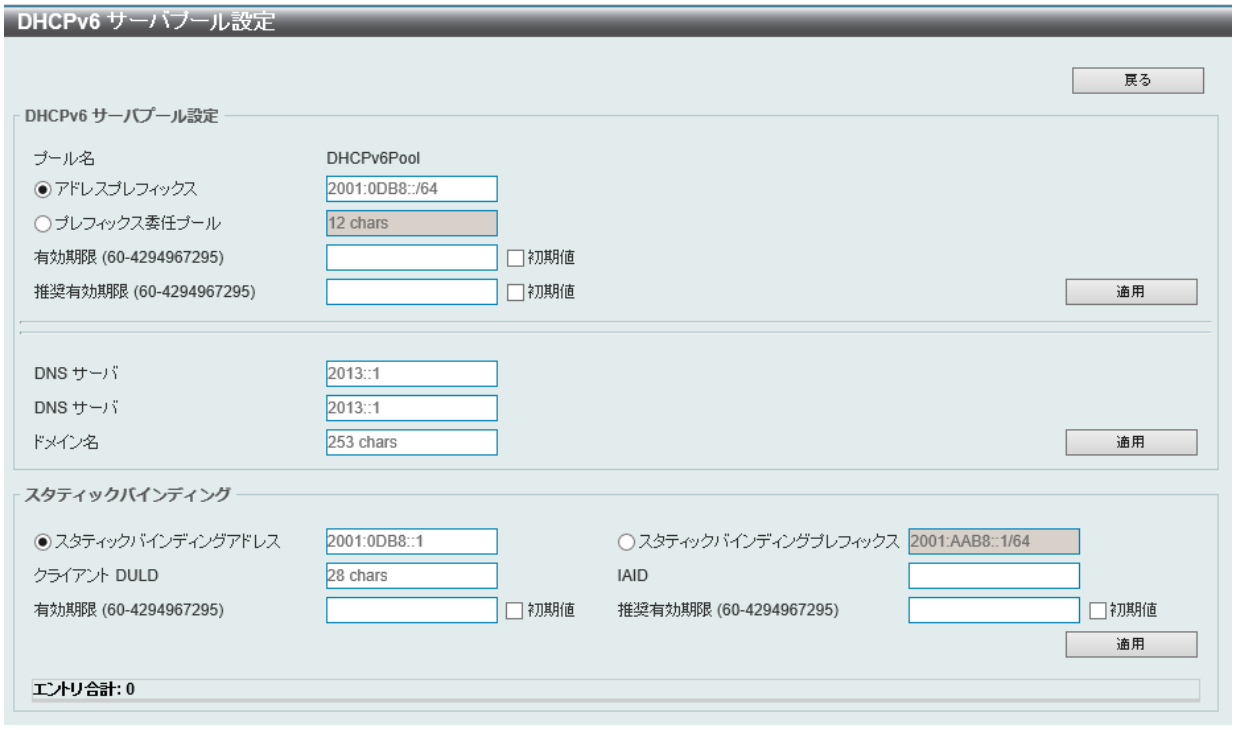


図 7-42　DHCPv6 サーバプール設定画面

画面に表示される項目：

項目	説明
DHCPv6 サーバプール設定	
アドレスプレフィックス	DHCPv6 サーバプール IPv6 ネットワークアドレスとプレフィクス長を入力します。（例： 2015::0/64）
プレフィックス委任プール	DHCPv6 サーバプールプレフィックス委任名を入力します。（12 文字以内）
有効期限	IPv6 アドレスが有効な状態を維持する時間を入力します。「推奨有効期限」よりも大きい値である必要があります。「初期値」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）＝ 30 日
推奨有効期限	preferred-lifetime（推奨有効期限）を入力します。「初期値」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：60-4294967295（秒） • 初期値：604800（秒）＝ 7 日
DNS サーバ	DHCPv6 クライアントに割り当てる DNS サーバの IPv6 アドレスを入力します。
ドメイン名	DHCPv6 クライアントに割り当てるドメイン名を指定します。
スタティックバインディング	
スタティックバインディングアドレス	指定クライアントに割り当てるスタティックバインディング IPv6 アドレスを入力します。
スタティックバインディングプレフィックス	スタティックバインディング IPv6 ネットワークアドレスとプレフィクスを入力します。
クライアント DUID	デバイスの DHCP 固有識別子（DUID）を入力します。（28 文字以内）
IAID	「Identity Association Identifier」（IAID/IA 識別子）を入力します。 これは、クライアントに割り当てられる一時的ではないアドレス（IANA）の集合体を識別します。
有効期限	IPv6 アドレスが有効な状態を維持する時間を入力します。「推奨有効期限」よりも大きい値である必要があります。「初期値」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）＝ 30 日
推奨有効期限	preferred-lifetime（推奨有効期限）を入力します。「初期値」にチェックを入れると、初期値が使用されます。 • 設定可能範囲：60-4294967295（秒） • 初期値：604800（秒）＝ 7 日

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。

DHCPv6 サーバローカルプール設定

DHCPv6 サーバローカルプールの表示および設定を行います。

管理 > DHCP > DHCPv6 サーバ > DHCPv6 サーバローカルプール設定の順にメニューをクリックし、以下の画面を表示します。



図 7-43　DHCPv6 サーバローカルプール設定画面

画面に表示される項目：

項目	説明
プール名	DHCPv6 サーバプール名を入力します。（12 文字以内）
IPv6 アドレス / プレフィックス長	IPv6 プレフィクスアドレスとプレフィクス長を入力します。
割り当てられた長さ	プール内のユーザに委任されるプレフィクス長を入力します。 「割り当てられた長さ」に設定する値はプレフィクス長の値より長い必要があります。

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「ユーザ詳細」をクリックするとユーザについての詳細が表示されます。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCPv6 サーバ除外アドレス

DHCPv6 クライアントへの割り当てから除外する IPv6 アドレスの範囲を設定します。DHCPv6 サーバは全てのアドレス（スイッチ自身の IPv6 アドレスを除く）をクライアントへ割り当てることが可能です。本画面では、割り当て範囲から IPv6 アドレス / アドレス範囲を除外する設定を行うことができます。除外された除外アドレスはアドレス割り当てプールにのみ適用されます。

管理 > DHCP > DHCPv6 サーバ > DHCPv6 サーバ除外アドレスの順にメニューをクリックし、以下の画面を表示します。



図 7-44　DHCPv6 サーバ除外アドレス画面

画面に表示される項目：

項目	説明
最初の IPv6 アドレス	除外する IPv6 アドレス（単体）、または除外 IPv6 アドレス範囲の開始 IPv6 アドレスを指定します。
最後の IPv6 アドレス	除外 IPv6 アドレス範囲の終了 IPv6 アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、エントリを削除します。

DHCPv6 サーババインディング

DHCPv6 バインディング情報を参照、クリアします。

管理 > DHCP > DHCPv6 サーバ > DHCPv6 サーババインディングの順にメニューをクリックし、以下の画面を表示します。



図 7-45　DHCPv6 サーババインディング画面

画面に表示される項目：

項目	説明
IPv6 アドレス	表示、クリアするバインディングエントリの IPv6 アドレスを入力します。 「全て」を選択するとバインディングテーブルの全ての DHCPv6 クライアントプリフィクスバインディングが対象になります。

「検索」をクリックして、入力した情報に基づくエントリを検出します。
「クリア」をクリックして、入力した情報に基づくエントリをクリアします。

DHCPv6 サーバインタフェース設定

DHCPv6 サーバインタフェースの設定を行います。

管理 > DHCP > DHCPv6 サーバ > DHCPv6 サーバインタフェース設定の順にメニューをクリックし、以下の画面を表示します。



図 7-46　DHCPv6 サーバインタフェース設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	VLAN インタフェースを指定します。 • 設定可能範囲：1-4094
プール名	DHCPv6 サーバプール名を入力します。（12 文字以内）
高速コミット	2 メッセージ交換を有効 / 無効に設定します。 • 初期値：「無効」
優先度	優先度を指定します。 「ヒントを許可」を選択するとヒントが表示されます。「初期値」を選択すると初期値を使用します。
インタフェース名	インタフェース名を入力します。

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。
「検索」をクリックして、入力した情報に基づくエントリを検出します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCPv6 サーバ運用情報

DHCPv6 サーバ状態を表示します。

管理 > DHCP > DHCPv6 サーバ > DHCPv6 サーバ運用情報の順にメニューをクリックし、以下の画面を表示します。

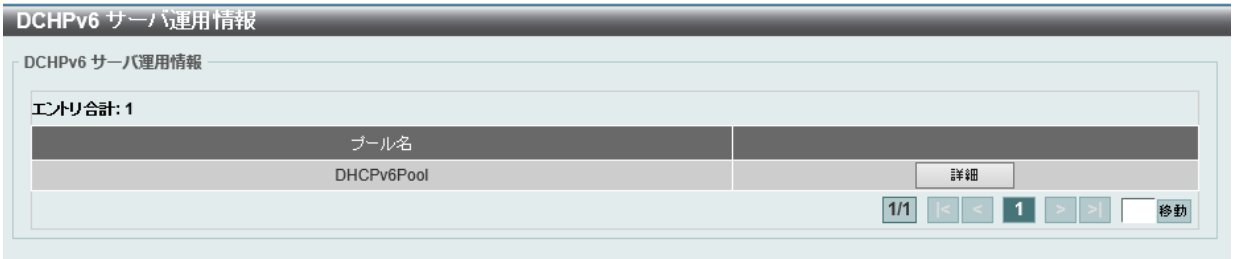


図 7-47　DHCPv6 サーバ運用情報画面

「詳細」をクリックすると詳細情報を表示します。

DHCP リレー

管理 > DHCP > DHCP リレー

DHCP リレーグローバル設定

DHCP リレーグローバル設定の有効化および設定を行います。

管理 > DHCP > DHCP リレー >DHCP リレーグローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-48　DHCP リレーグローバル設定画面

画面に表示される項目：

項目	説明
DHCP リレーグローバル設定	
DHCP スマートリレーステート	DHCP スマートリレーを有効 / 無効に指定します。
DHCP リレーユニキャストステート設定	
DHCP リレーユニキャストステート	DHCP リレーユニキャストのグローバルステータスを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

注意　DHCP リレーが有効の場合、discover パケットが対象 VLAN 内に flooding されません。

DHCP リレープール設定

DHCP リレーエージェントの DHCP リレープールの表示、設定を行います。

管理 > DHCP > DHCP リレー > DHCP リレープール設定の順にメニューをクリックし、以下の画面を表示します。



図 7-49　DHCP リレープール設定画面

画面に表示される項目：

項目	説明
DHCP プール名	プール名を指定します。(32 文字以内)

「検索」をクリックすると、指定したエントリが検索されます。
「すべて表示」をクリックすると、すべてのエントリを表示します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

各プールエントリの編集を行う（編集）

各エントリの「送信元」「送信先」「クラス」下にある「編集」をクリックして、それぞれの内容を編集します。

■ 「送信元」の編集を行う場合

「送信元」下の「編集」をクリックします。以下の画面が表示されます。



図 7-50　DHCP リレープールソース設定画面

画面に表示される項目：

項目	説明
送信元 IP アドレス	クライアントパケットのソースサブネットを入力します。
サブネットマスク	ソースサブネットのネットマスクを入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、エントリを削除します。
前の画面に戻るには、「戻る」ボタンをクリックします。

■ 「送信先」の編集を行う場合

「送信先」下の「編集」をクリックします。以下の画面が表示されます。

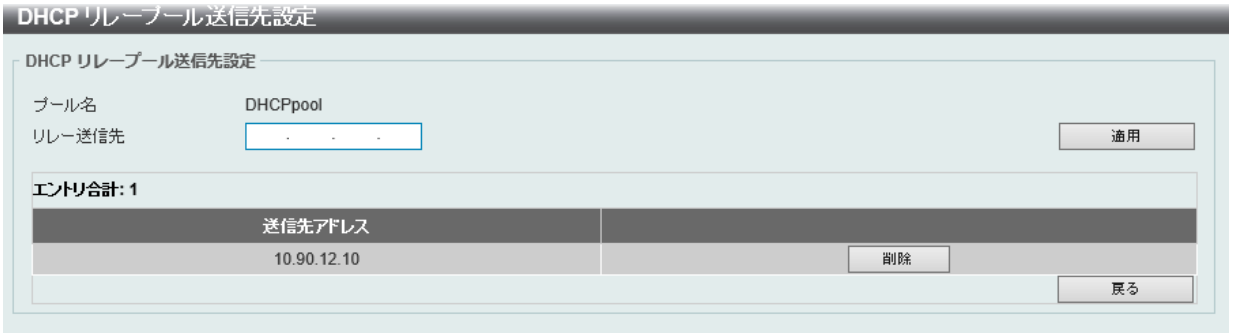


図 7-51　DHCP リレープール送信先設定画面

以下の項目が使用されます。

項目	説明
リレー送信先	リレー宛先 DHCP サーバの IP アドレスを入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、エントリを削除します。
前の画面に戻るには、「戻る」ボタンをクリックします。

■「クラス」の編集を行う場合

「クラス」下の「編集」をクリックします。以下の画面が表示されます。

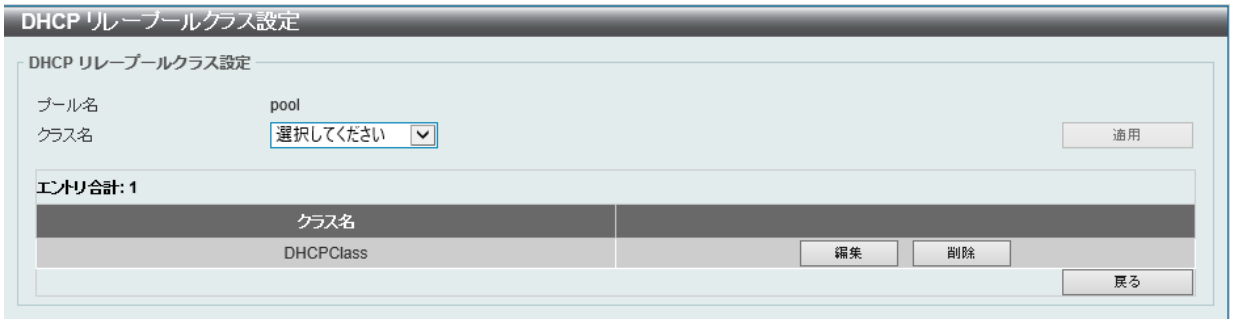


図 7-52　DHCP リレープールクラス設定画面

画面に表示される項目：

項目	説明
クラス名	DHCP クラスの名前を選択します。

「適用」をクリックして、設定内容を適用します。

「削除」をクリックして、エントリを削除します。

前の画面に戻るには、「戻る」をクリックします。

クラス名の横の「編集」をクリックすると以下の画面が表示されます。

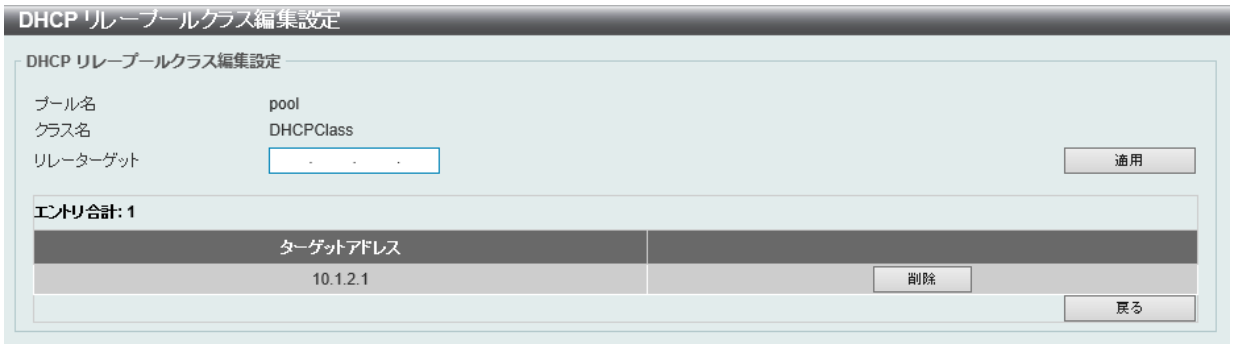


図 7-53　DHCP リレープールクラス編集設定画面

画面に表示される項目：

項目	説明
リレーターゲット	DHCP クラスで設定したオプションの値パターンと一致するパケットをリレーする DHCP リレーターゲットを入力します。

「適用」をクリックして、設定内容を適用します。

「削除」をクリックして、エントリを削除します。

前の画面に戻るには、「戻る」をクリックします。

DHCP リレー情報設定

DHCP リレー情報の設定を行います。

管理 > DHCP > DHCP リレー > DHCP リレー情報設定の順にメニューをクリックし、以下の画面を表示します。



図 7-54　DHCP リレー情報設定画面

画面に表示される項目：

項目	説明
すべてのトラスト情報	すべてのインタフェースで DHCP リレーエージェントによる IP DHCP リレーインフォメーションへの信頼を有効 / 無効に設定します。
情報チェック	DHCP リレーエージェントによる、受信した DHCP リレーパケットに含まれるリレーエージェントインフォメーションの検証と破棄を有効 / 無効に設定します。
ポリシー情報	DHCP リレーエージェントの Option82 再転送ポリシーを選択します。 • 「リプレース」- DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。（初期値） • 「破棄」- DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • 「保持」- DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。
オプション情報	DHCP リクエストパケットがリレーされる間のリレーエージェント情報（Option82）の挿入を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。
「編集」をクリックして対応するインタフェースの編集を行うことができます。
複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCP リレー情報オプションフォーマット設定

DHCP 情報フォーマットの表示、設定を行います。

管理 > DHCP > DHCP リレー > DHCP リレー情報オプションフォーマット設定の順にメニューをクリックし、以下の画面を表示します。



図 7-55　DHCP リレー情報オプションフォーマット設定画面

画面に表示される項目：

項目	説明
DHCP リレー情報オプションフォーマットグローバル	
フォーマットリモート ID 情報	DHCP 情報リモート ID のサブオプションを選択します。 • 「初期値」- リモート ID はシステムの MAC アドレスを使用します。 • 「ユーザ定義」- リモート ID はユーザ定義の文字列を使用します。（32 文字以内） • 「ベンダ 2」- リモート ID はベンダ 2 を使用します。 • 「ベンダ 3」- リモート ID はベンダ 3 を使用します。 • 「エキスパート UDF」- エキスパート UDF リモート ID を使用します。スタンドアロンのユニットフォーマットを選択します。

項目	説明
フォーマットサーキット ID 情報	DHCP 情報サーキット ID のサブオプションを選択します。 • 「初期値」- 初期値のサーキット ID を使用します。 • 「ユーザ定義」- ユーザ定義のサーキット ID を使用します。（32 文字以内） • 「ベンダ 1-6」- サーキット ID はベンダ 1 -6 を使用します。 • 「エキスパート UDF」- エキスパート UDF サーキット ID を使用します。スタンドアロンのユニットフォーマットを選択します。
DHCP リレー情報オプションフォーマットタイプ	
ユニット	本設定を適用するユニットを選択します。
開始ポート / 終了ポート	本設定を適用するポート範囲を指定します。
フォーマット	リレー情報オプションのフォーマットを指定します。 • 選択肢：「ベンダ 3」「エキスパート UDF」
タイプ	リレー情報オプションの種類を選択します。 • 選択肢：「リモート ID」「サーキット D」
値	Option82 情報として、リモート / サーキット ID サブオプションに含まれるベンダ定義の文字列を入力します。（32 文字以内）

「適用」をクリックして、設定内容を適用します。

DHCP リレー情報プロファイル設定

DHCP リレー情報プロファイルの設定、表示を行います。

管理 > DHCP > DHCP リレー > DHCP リレー情報プロファイル設定の順にメニューをクリックし、以下の画面を表示します。

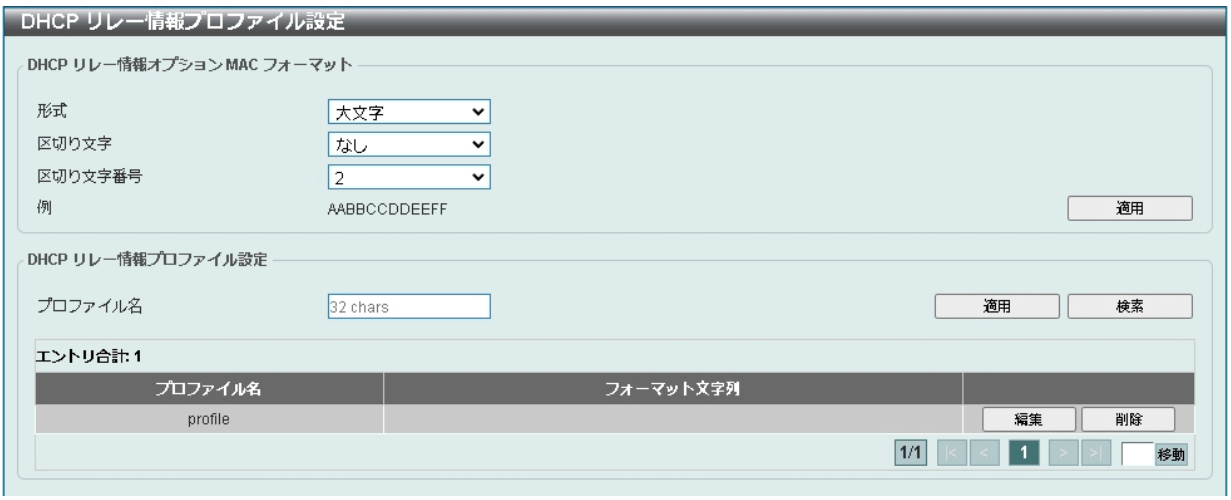


図 7-56　DHCP リレー情報プロファイル設定画面

画面に表示される項目：

項目	説明
DHCP リレー情報オプション MAC フォーマット	
形式	オプション 82 のネットワークアクセス認証に使用する MAC アドレスの形式を選択します。 • 「小文字」- 小文字を使用します。（例：aa-bb-cc-dd-ee-ff） • 「大文字」- 大文字を使用します。（例：AA-BB-CC-DD-EE-FF）
区切り文字	MAC アドレスを入力する際の区切りを選択します。区切り文字を持たない場合には「なし」を選択します。各項目の例は次の通りです。 • 「ハイフン」-「 AA-BB-CC-DD-EE-FF」 • 「コロン」-「 AA:BB:CC:DD:EE:FF」 • 「ドット」-「 AA.BB.CC.DD.EE.FF」 • 「なし」-「 AABBCCDDEEFF」
区切り文字番号	MAC アドレスにおける区切り数を選択します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」
DHCP リレー情報プロファイル設定	
プロファイル名	Option82 のプロファイル名を入力します。プロファイルにより、ユーザ定義の Option82 エントリを作成します。
フォーマット文字列	「Edit」をクリックし、ユーザ定義の Option82 フォーマット文字列を指定します。（251 文字以内）ルールは次の通りです。

項目	説明
	• 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション (" ") で括られた形式（例："Ethernet"）とします。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":":」のように ASCII 文字列と 16 進数の両方を含むことができます。 • 「%」の後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。（オプション）フォーマットキー文字列において文字長オプションの指定文字数（バイト数）を満たすために使用されます。 - 「$」はスペース（0x20）を埋めます。 - 「0」は（0）を埋めます。「0」が初期値です。 • 「1-32」は文字長オプションです。（オプション）キー文字列に変換される文字やバイトの文字数 / バイト数を指定します。変換されたキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。 • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。 - 「devtype」は機器のモデル名です。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」(IF-MIB) から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値です。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は 0 です。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合、この最後の文字（":"）は無視されます。「%」と「:」の間のスペース (0x20) は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットされたキー文字列を任意に組み合わせることができます。「\」はエスケープ文字であり、「\」の後の特殊文字はそのままになります。例えば「\%」は「%」を意味し、フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列に含まれないスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「編集」をクリックして、指定エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCP リレーポート設定

DHCP リレーポートの設定、表示を行います。

管理 > DHCP > DHCP リレー > DHCP リレーポート設定の順にメニューをクリックし、以下の画面を表示します。

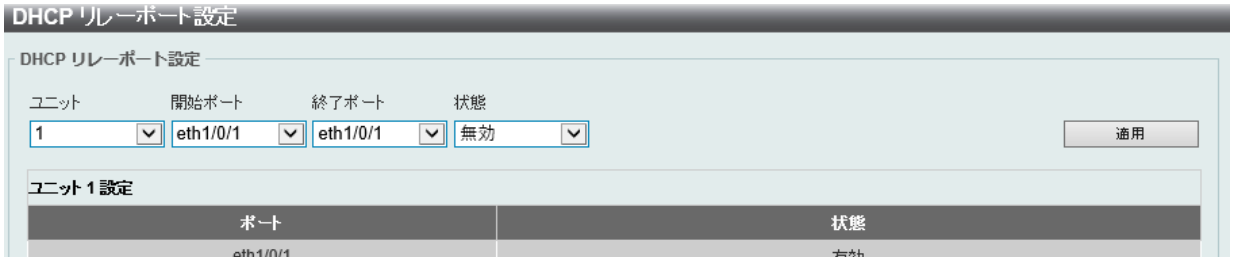


図 7-57　DHCP リレーポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定のポートの DHCP リレーを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

DHCP ローカルリレー VLAN

VLAN、またはグループ VLAN のリレー設定を行います。

管理 > DHCP > DHCP リレー > DHCP ローカルリレー VLAN の順にメニューをクリックし、以下の画面を表示します。



図 7-58　DHCP ローカルリレー VLAN 画面

画面に表示される項目：

項目	説明
DHCP ローカルリレー VID リスト	DHCPv6 ローカルリレー VLAN ID を入力します。一つ以上の VLAN ID が入力可能です。 「すべての VLAN」にチェックを入れると、すべての VLAN が対象になります。
状態	指定した VLAN の DHCP ローカルリレー機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

注意　DHCP リレーポートが無効の場合、ポートは受信 DHCP パケットのリレー / ローカルリレーを行いません。

DHCPv6 リレー

DHCPv6 リレーグローバル設定

スイッチの DHCPv6 リレー機能を設定します。

管理 > DHCP > DHCPv6 リレー > DHCPv6 リレーグローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-59　DHCPv6 リレーグローバル設定画面

画面に表示される項目：

項目	説明
DHCPv6 リレー リモート ID 設定	
IPv6 DHCP リレーリモート ID フォーマット	IPv6 DHCP リレーのリモート ID フォーマットを選択します。 • 選択肢：「初期値」「ユーザ定義の CID」「ユーザ定義」「エキスパート UDF」
スタンドアローンユニットフォーマット	「エキスパート UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
IPv6 DHCP リレーリモート ID UDF	リモート ID のユーザ定義項目（UDF）の入力形式 を選択します。 • 「なし」- リモート ID の UDF を空のままにします。 • 「ASCII」- ASCII 文字列で入力します。（128 文字以内） • 「HEX」- 16 進数文字列で入力します。（256 文字以内）
IPv6 DHCP リレーリモート ID ポリシー	DHCPv6 リレーエージェントの Option37 フォワーディングポリシーを選択します。 • 「破棄」- DHCP クライアントから受信したパケット内に既に Option37 リレー情報があった場合はそのパケットを破棄します。 • 「保持」- DHCP クライアントから受信したパケット内の既存の Option37 リレー情報を保持します。
Pv6 DHCP リレーリモート ID オプション	DHCP IPv6 リクエストパケットのリレーの間のリレーエージェント情報（Option37）の挿入を有効 / 無効に設定します。
DHCPv6 リレーインタフェース ID 設定	
IPv6 DHCP リレーインタフェース ID フォーマット	インタフェース ID のフォーマットを指定します。 • 選択肢：「初期値」「CID」「ベンダ 1」「エキスパート UDF」
スタンドアローンユニットフォーマット	「エキスパート UDF」を選択した場合、スタンドアロンユニットのフォーマットを選択します。 • 選択肢：「0」「1」
Pv6 DHCP リレーインタフェース ID ポリシー	DHCPv6 リレーエージェントの Option18 フォワーディングポリシーを選択します。 • 「破棄」- DHCP クライアントから受信したパケット内に既に Option18 リレー情報があった場合はそのパケットを破棄します。 • 「保持」- DHCP クライアントから受信したパケット内の既存の Option18 リレー情報を保持します。
IPv6 DHCP リレーインタフェース ID オプション	DHCP IPv6 リクエストパケットのリレーの間のリレーエージェント情報（Option18）の挿入を有効 / 無効に設定します。
DHCPv6 リレー情報オプション MAC フォーマット	
ケース	MAC アドレスの形式を選択します。 • 「小文字」- 小文字を使用します。（例：aa-bb-cc-dd-ee-ff） • 「大文字」- 大文字を使用します。（例：AA-BB-CC-DD-EE-FF）

項目	説明
区切り文字	MAC アドレスを入力する際の区切り文字を選択します。 区切り文字をいれない場合は「なし」を選択します。各項目の例は次の通りです。 • 「ハイフン」-「AA-BB-CC-DD-EE-FF」 • 「コロン」-「AA:BB:CC:DD:EE:FF」 • 「ドット」-「AA.BB.CC.DD.EE.FF」 • 「なし」-「AABBCCDDEEFF」
区切り文字番号	MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。各項目の例は次の通りです。 • 「1」-「AABBCC.DDEEFF」 • 「2」-「AABB.CCDD.EEFF」 • 「5」-「AA.BB.CC.DD.EE.FF」

「適用」をクリックして、設定内容を適用します。

DHCPv6 リレーインタフェース設定

DHCPv6 リレーインタフェースの設定を行います。

管理 > DHCP > DHCPv6 リレー > DHCPv6 リレーインタフェース設定の順にメニューをクリックし、以下の画面を表示します。



図 7-60　DHCPv6 リレーインタフェース設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	DHCPv6 リレーの VLAN を指定します。 • 設定可能範囲：1-4094
送信先 IPv6 アドレス	DHCPv6 リレーの宛先アドレスを入力します。
出力インタフェース VLAN	リレー宛先の送信インタフェースを指定します。 • 設定可能範囲：1-4094

「適用」ボタンをクリックし、設定を適用します。
「検索」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックすると指定のエントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCPv6 リレーリモート ID プロファイル設定

DHCPv6 リレーリモート ID プロファイル設定の表示と設定を行います。DHCPv6 リレー Option37 のプロファイルの作成に使用されます。

管理 > DHCP > DHCPv6 リレー > DHCPv6 リレーリモート ID プロファイル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-61　DHCPv6 リレーリモート ID プロファイル設定画面

以下の項目を使用して設定、表示を行います。

項目	説明
プロファイル名	Option37 のプロファイル名を入力します。（32 文字以内）
フォーマット文字列	「編集」をクリックし、ユーザ定義の Option37 フォーマット文字列を指定します。（251 文字以内） ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション（" "）で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列、または 16 進数のどちらも含むことができます。 • 「%」後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「$」はスペースを埋め（0x20）、「0」は（0）を埋めます。「0」が初期値です。（オプション） • 「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。（オプション） • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。: - 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」（IF-MIB）から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例 ,「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例 ,「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合（:）は無視されます。「%」と「:」の間のスペース（0x20）は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープキャラクターになります。「\」以後の特別なキャラクターはキャラクターそのものになります。例えば「\%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列内のスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「編集」をクリックして、指定エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCPv6 リレーインタフェース ID プロファイル設定

DHCPv6 リレーインタフェース ID プロファイル設定の表示と設定を行います。DHCPv6 リレー Option82 のプロファイルを作成に使用されます。

管理 > DHCP > DHCPv6 リレー > DHCPv6 リレーインタフェース ID プロファイル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-62　DHCPv6 リレーインタフェース ID プロファイル設定画面

画面に表示される項目：

項目	説明
プロファイル名	Option82 のプロファイル名を入力します。
フォーマット文字列	「編集」をクリックし、ユーザ定義の Option82 フォーマット文字列を指定します。（251 文字以内） ルールは次の通りです。 • 本パラメータは、16 進数、ASCII 文字列、または 16 進数と ASCII 文字列の組み合わせで指定することができます。ASCII 文字列はダブルコーテーション（" "）で括られた "Ethernet" のような形になります。ダブルコーテーションに括られない文字は 16 進数として認識されます。 • フォーマットされたキー文字列はパケットに格納される前に変換される必要があります。フォーマットされたキー文字列は、「"%" +"$"+"1-32"+"keyword"+":"」のように ASCII 文字列、または 16 進数のどちらも含むことができます。 • 「%」後の文字列はフォーマットされたキー文字列を意味します。 • 「$」または「0」はフィルインディケータです。文字長オプションに対してフォーマットキー文字列の対応方法を設定します。「$」はスペースを埋め（0x20）、「0」は（0）を埋めます。「0」が初期値です。（オプション） • 「1-32」は文字長オプションです。どれくらいの文字やバイトがキー文字列に変換されるのかを指定します。もし変換済みキー文字列の実際の文字長が本オプションに指定された文字長よりも短い場合、フィルインディケータにより埋められます。そうでない場合、文字長オプションとフィルインディケータは無視され、実際の文字長がそのまま採用されます。（オプション） • 「keyword」はシステムの実際の値を基に変換されます。次の「Keyword」がサポートされています。： - 「devtype」は機器のモデル名です。「show version」コマンドのモジュール名項目から生成されます。ASCII 文字列のみ有効です。 - 「sysname」はスイッチのシステム名を意味します。最大文字長は 128 です。ASCII 文字列のみ有効です。 - 「ifdescr」は「ifDescr」（IF-MIB）から生成されます。ASCII 文字列のみ有効です。 - 「portmac」はポートの MAC アドレスを意味します。ASCII 文字列、または 16 進数値で表示されます。ASCII 文字列フォーマットの場合、MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例 ,「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「sysmac」はシステムの MAC アドレスを意味します。ASCII 文字列で表示されます。MAC アドレスのフォーマットは特定のコマンドでカスタムされます。（例 ,「ip dhcp relay information option mac-format case」など）。16 進数フォーマットの場合、MAC アドレスは 16 進数として格納されます。 - 「unit」はユニット ID を意味します。ASCII 文字列、または 16 進数値で表示されます。スタンドアロンのデバイスの場合、ユニット ID は「ip dhcp relay information option format remote-id」、そして「ip dhcp relay information option format circuit-id」コマンドで設定されます。 - 「module」はモジュール ID 番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「port」はローカルポート番号を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「svlan」はアウタ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 - 「cvlan」はインナ VLAN ID を意味します。ASCII 文字列、または 16 進数値で表示されます。 • 「:」はフォーマット文字列の終わりを意味します。フォーマット文字列がコマンドの最後のパラメータの場合（:）は無視されます。「%」と「:」の間のスペース（0x20）は無視され、他のスペースはパケットに格納されます。 • ASCII 文字列は「0-9」「a-z」「A-Z」「!」「@」「#」「$」「%」「^」「&」「*」「(」「)」「_」「+」「|」「-」「=」「\」「[」「]」「{」「}」「;」「:」「'」「"」「/」「?」「.」「,」「<」「>」「`」とスペース、フォーマットキー文字列のいかなる組み合わせも可能です。「\」はエスケープキャラクターになります。「\」以後の特別なキャラクターはキャラクターそのものになります。例えば「\%」は「%」を意味します。フォーマットキー文字列の開始インディケータではありません。フォーマットキー文字列内のスペースもまたパケットに格納されます。 • 16 進数値は「0-9」「A-F」「a-f」とスペースとフォーマットキー文字列からなります。フォーマットキー文字列は 16 進数をサポートするキーワードのみサポートします。フォーマットキー文字列外のスペースは無視されます。

「適用」をクリックして、エントリを追加します。
「削除」をクリックして、エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「編集」をクリックして、指定エントリの編集を行います。
複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

DHCPv6 リレーフォーマットタイプ設定

DHCPv6 リレーフォーマットタイプ設定の表示と設定を行います。
各ポートの「エキスパート UDF」文字列の DHCPv6 Option37 と Option18 を設定します。

管理 > DHCP > DHCPv6 リレー > DHCPv6 リレーフォーマットタイプ設定の順にメニューをクリックし、以下の画面を表示します。



図 7-63　DHCPv6 リレーフォーマットタイプ設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
タイプ	以下からタイプを指定します。 • 「リモート ID」-「エキスパート UDF」フォーマットタイプ文字列を DHCPv6 Option37 で指定します。 • 「インタフェース ID」-「エキスパート UDF」フォーマットタイプ文字列を DHCPv6 Option18 で指定します。
フォーマットタイプエキスパート UDF	指定ポートで使用する「エキスパート UDF」文字列を入力します。

「適用」をクリックして、設定内容を適用します。

DHCPv6 リレーポート設定

DHCPv6 リレーポート設定を行います。

管理 > DHCP > DHCPv6 リレー > DHCPv6 リレーポート設定の順にメニューをクリックし、以下の画面を表示します。



図 7-64　DHCPv6 リレーポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートの DHCPv6 リレーポート機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

DHCPv6 ローカルリレー VLAN

DHCPv6 ローカルリレー VLAN 設定を行います。
DHCPv6 ローカルリレーが有効の場合、クライアントからのリクエストパケットに Option 37 と 18 を追加します。Option 37 のチェックステートが有効の場合、クライアントからのリクエストパケットをチェックし、Option 37DHCPv6 リレー機能が含まれる場合、パケットを破棄します。無効の場合、ローカルリレー機能は、Option 37 の有効 / 無効にかかわらず、常に Option 37 をリクエストパケットに追加します。DHCPv6 ローカルリレー機能はサーバからのパケットを直接クライアントに転送します。

管理 > DHCP > DHCPv6 リレー > DHCPv6 ローカルリレー VLAN の順にメニューをクリックし、以下の画面を表示します。



図 7-65　DHCPv6 ローカルリレー VLAN 画面

画面に表示される項目：

項目	説明
DCHPv6 ローカルリレー VID リスト	DHCPv6 ローカルリレー VLAN ID を入力します。1 つ以上の VLAN ID が入力可能です。 「すべての VLAN」オプションを指定すると、すべての VLAN が対象になります。
状態	指定 VLAN の DHCPv6 ローカルリレー機能を有効 / 無効に指定します。

「適用」をクリックして、設定内容を適用します。

注意　「DHCPv6 リレーポート」が無効の場合、ポートは受信した DHCPv6 パケットをリレー / ローカルにリレーしません。

DHCP 自動設定

DHCP 自動コンフィグ機能の設定を行います。

管理 > DHCP > DHCP 自動設定の順にメニューをクリックし、以下の画面を表示します。

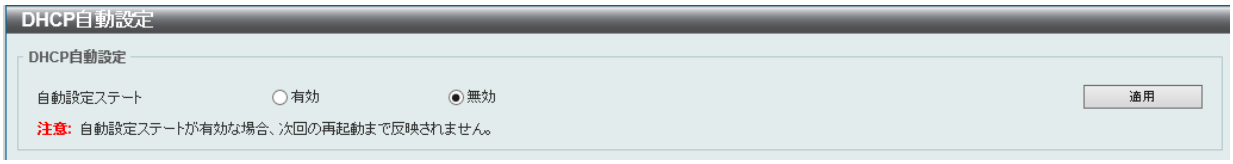


図 7-66　DHCP 自動設定画面

画面に表示される項目：

項目	説明
自動設定ステート	自動設定機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

DHCP 自動イメージ設定

ここでは DHCP 自動イメージ設定を行います。本機能は、スイッチの起動時に外部 TFTP サーバからイメージファイルを取得する機能です。
この TFTP サーバの IP アドレスとファイル名は、DHCP サーバからの「DHCP OFFER」メッセージに含まれています。システムはこのイメージファイルを起動イメージとして使用します。システムが起動し、自動イメージ機能が有効になると、本スイッチは自動的に DHCP クライアントになります。

DHCP クライアントがアクティブになると、DHCP サーバからネットワーク設定を取得します。DHCP サーバからのメッセージには、TFTP サーバの IP アドレスとイメージファイル名が含まれています。スイッチがこの情報を受信した後、指定した TFTP サーバからの TFTP ダウンロード機能を起動します。このタイミングで、ダウンロード設定パラメータがコンソールに表示されます。レイアウトは download firmware コマンドを使用した場合と同じです。ファームウェアのダウンロードが完了すると、スイッチはすぐに再起動します。

自動コンフィグ機能（auto-configuration）と自動イメージ（auto-image）機能の両方が有効な場合、イメージファイルが先にダウンロードされ、次にコンフィグがダウンロードされます。その後、スイッチはコンフィグレーションを保存して再起動します。

スイッチはダウンロードされたファームウェアを常にチェックします。バージョンが現在実行中のファームウェアと同じ場合、本装置は自動イメージ処理を終了します。ただし、自動コンフィギュレーション機能も有効になっている場合は、ダウンロードしたコンフィギュレーションは引き続き実行されます。

本機能は自動コンフィグ機能に似ています。DHCP オプションフィールドは自動イメージ機能だけでなく、自動設定機能でも使用されるため、イメージファイルと設定ファイルの両方を同じ TFTP サーバ配置する必要があります。TFTP サーバの IP アドレスは、引き続き Option66 または Option150 の DHCP siaddr フィールドに配置されます。Option66、Option150、および siaddr フィールドが同時に DHCP 応答メッセージに存在する場合、Option150 が最初に解決されます。システムが TFTP サーバへの接続に失敗した場合、システムは Option66 を解決します。
それでもシステムが TFTP サーバへの接続に失敗した場合は、siaddr フィールドが最後の選択肢になります。

本スイッチは、Option66 を使用して TFTP サーバ名を取得すると、最初に Option6 を解決して DNS サーバの IP アドレスを取得します。
スイッチが DNS サーバへの接続に失敗した場合、または応答メッセージにオプション 6 が存在しない場合、スイッチシステム内に定義されている DNS サーバに接続しようとします。

Option67 は、DHCP ヘッダの「file」フィールドが DHCP オプションに使用されている場合に、ブートファイルを識別するために使用されます。
これは、DHCP 自動コンフィギュレーションモードでのみ使用でき、DHCP 自動イメージモードでは使用できません。詳細については、RFC2132 を参照してください。イメージファイル名を指定する場合は、DHCP Option125（RFC3925）を使用する必要があります。
本スイッチでは enterprise-number1 フィールドを確認する必要があります。値が D-Link ベンダ ID（171）でない場合、プロセスが停止します。オプションが複数のフィールドを含む場合、最初のエントリ enterprise-number1 のみが使用されます。

管理 > DHCP > DHCP 自動イメージ設定の順にメニューをクリックし、以下の画面を表示します。

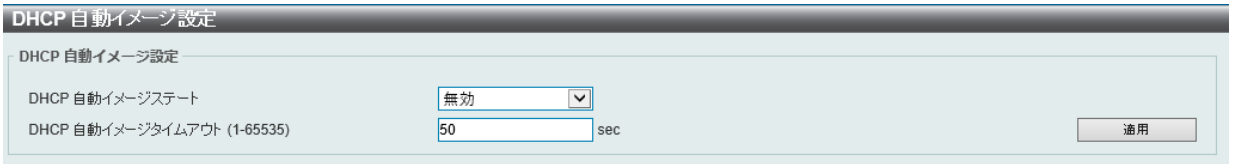


図 7-67　DHCP 自動イメージ設定画面

画面に表示される項目：

項目	説明
DHCP 自動イメージステート	DHCP 自動イメージ機能を有効 / 無効に設定します。
DHCP 自動イメージタイムアウト	DHCP 自動イメージ機能のタイムアウト時間を指定します。 • 設定可能範囲：1- 65535（秒）

「適用」をクリックして、設定内容を適用します。

DNS

DNS（Domain Name System）は、ドメイン名と IP アドレスの関連付けをコンピュータ間の通信で行います。
DNS サーバは「name-to-address」翻訳を実行し、ドメイン名とアドレスの変換を行うためにいくつかのネームサーバと連絡を取る必要があります。
ドメインネームサービスを行うデバイスのアドレスは、DHCP または BOOTP サーバから取得する場合と、初期設定時に手動で OS に設定する場合があります。

DNS グローバル設定

本項目ではグローバルに DNS を設定します。

管理 > DNS > DNS グローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-68　DNS グローバル設定画面

画面に表示される項目：

項目	説明
IP ドメイン Lookup	IP ドメインルックアップを有効 / 無効に設定します。
IP ネームサーバタイムアウト	指定ネームサーバからの回答を待つ待機時間を指定します。 • 設定可能範囲：1 - 60（秒）

「適用」をクリックして、設定内容を適用します。

DNS サーバ設定

スイッチに DNS の IP アドレスを設定します。

管理 > DNS > DNS サーバ設定の順にメニューをクリックし、以下の画面を表示します。

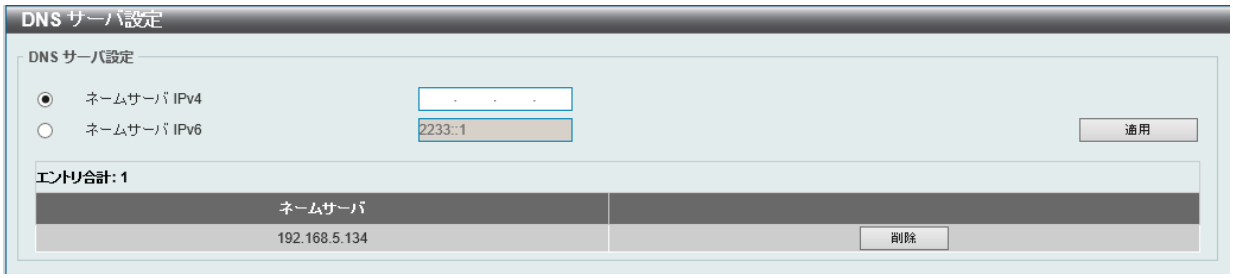


図 7-69　DNS サーバ設定画面

画面に表示される項目：

項目	説明
ネームサーバ IPv4	選択して DNS サーバの IPv4 アドレスを入力します。
ネームサーバ IPv6	選択して DNS サーバの IPv6 アドレスを入力します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックして、指定エントリを削除します。

DNS ホスト設定

ホスト名のスタティックマッピングの設定とホストテーブルの IP アドレスを設定します。

管理 > DNS > DNS ホスト設定の順にメニューをクリックし、以下の画面を表示します。



図 7-70　DNS ホスト設定画面

画面に表示される項目：

項目	説明
ホスト名	ホスト名を入力します。
IP アドレス	ホストの IPv4 アドレスを入力します。
IPv6 アドレス	ホストの IPv6 アドレスを入力します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。
「削除」をクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

NTP

スイッチの時刻を同期するための通信プロトコル（NTP/Network Time Protocol）の設定を行います。

NTP グローバル設定

NTP のグローバル設定を行います。

管理 > NTP > NTP グローバル設定の順にメニューをクリックし、以下の画面を表示します。



図 7-71　NTP グローバル設定画面

画面に表示される項目：

項目	説明
NTP ステート	
NTP ステート	NTP 機能をグローバルに有効 / 無効にします。
NTP 認証ステート	
NTP 認証ステート	NTP の認証を有効 / 無効にします。 この機能を有効にすると、ネットワークノードは、認証キーの 1 つを持っていない限り、スイッチと同期しません。
NTP アップデートカレンダ	
NTP アップデートカレンダ	NTP のアップデートカレンダーを有効 / 無効にします。 この機能は、NTP ソースからハードウェアクロックを定期的に更新するために使用されます。
NTP 設定	
NTP マスタ層	NTP マスタの階層値を指定します。 外部 NTP が使用できない場合に、CPU クロックを NTP マスタクロックとして設定するために使用されます。「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1 - 15
NTP 最大アソシエーション	NTP への接続最大値を指定します。 スイッチ上の NTP ピアとクライアントの最大数を設定するために使用します。 • 設定可能範囲：1 - 64

「適用」をクリックして、設定内容を適用します。

注意　DGS-1520 シリーズはリアルタイムクロック（RTC）を持っていません。そのため、タイムレンジ等、時刻に依存する機能は NTP/SNTP により時刻同期されるまで正常に動作しません。

NTP サーバ設定

NTP サーバの設定を行います。

管理 > NTP > NTP サーバ設定の順にメニューをクリックし、以下の画面を表示します。

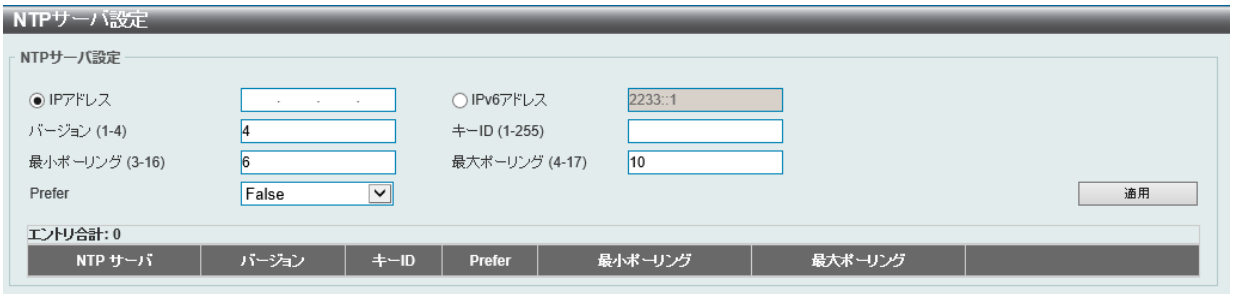


図 7-72　NTP サーバ設定画面

画面に表示される項目：

項目	説明
IP アドレス	NTP サーバの IPv4 アドレスを指定します。
IPv6 アドレス	NTP サーバの IPv6 アドレスを指定します。
バージョン	NTP サーバのバージョンを指定します。 • 設定可能範囲：1 - 4
キー ID	認証鍵 ID を指定します。 • 設定可能範囲：1 - 255
最小ポーリング	NTP メッセージ送信の最小ポーリング間隔を指定します。 この値は、指定された最小ポーリング間隔値の 2 の累乗として計算されます。たとえば、ここで指定された値が 6 の場合、使用される最小ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：3-16
最大ポーリング	NTP メッセージ送信の最大ポーリング間隔を指定します。 この値は、指定された最大ポーリング間隔値の 2 の累乗として計算されます。たとえば、ここで指定された値が 6 の場合、使用される最大ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：4-17
Prefer	このエントリを同期するサーバとして優先するかどうかを選択します。 • 選択肢：「True」「False」

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。
「編集」をクリックして、指定エントリの編集を行います。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

注意　経路に従ってソース IP が決定されるため、構成によりクライアントは同期に失敗する場合があります。

NTP ピア設定

NTP のピア設定を行います。

管理 > NTP > NTP ピア設定の順にメニューをクリックし、以下の画面を表示します。



図 7-73　NTP ピア設定画面

画面に表示される項目：

項目	説明
IP アドレス	NTP ピアの IPv4 アドレスを指定します。
IPv6 アドレス	NTP ピアの IPv6 アドレスを指定します。
バージョン	NTP バージョンを指定します。 • 設定可能範囲：1 - 4
キー ID	認証鍵 ID を指定します。 • 設定可能範囲：1 - 255
最小ポーリング	NTP メッセージ送信の最小ポーリング間隔を指定します。 この値は、指定された最小ポーリング間隔値の 2 の累乗として計算されます。たとえば、ここで指定された値が 6 の場合、使用される最小ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：3-16
最大ポーリング	NTP メッセージ送信の最大ポーリング間隔を指定します。 この値は、指定された最小ポーリング間隔値の 2 の累乗として計算されます。たとえば、ここで指定された値が 6 の場合、使用される最大ポーリング間隔は 64 秒（$2^6 = 64$）です。 • 設定可能範囲：4-17
Prefer	対象のピアを優先するか否かを選択します。 • 選択肢：「True」「False」

「適用」をクリックして、設定内容を適用します。「削除」で指定エントリを削除します。

NTP アクセスグループ設定

NTP アクセスグループの設定を行います。
IPv4 アドレス /IPv6 アドレスとマスクを設定し、アクセスコントロールリストを作成します。

管理 > NTP > NTP アクセスグループ設定の順にメニューをクリックし、以下の画面を表示します。



図 7-74　NTP アクセスグループ設定画面

画面に表示される項目：

項目	説明
初期値	チェックを入れるとデフォルトのエントリが最小の優先値でリストに含まれます。 初期値：IPv4（0.0.0.0/0.0.0.0）、IPv6（::/::）
IP アドレス	ホスト IPv4 アドレスを指定します。
ネットマスク	ホストネットワークの IPv4 ネットワークマスクを指定します。
IPv6 アドレス	ホスト IPv6 アドレスを指定します。
IPv6 マスク	ホストネットワークの IPv6 プレフィックス長を指定します。
無視	NTP コントロールクエリを含むすべてのパケットを拒否します。
保持なし	NTP コントロールクエリを除く、すべてのパケットを拒否します。
信頼なし	暗号認証されていないパケットを拒否します。
バージョン	現在の NTP バージョンと一致しないパケットを拒否します。
ピアなし	認証されない限り、アソシエーションを形成する可能性のあるパケットを拒否するには、「ピアなし」を選択します。設定されたアソシエーションが存在しない場合、パケットには Broadcast、Symmetric Active、Many Cast Server パケットが含まれます。「ピアなし」は、アソシエーションを形成しようとしないパケットには適用されないことに注意してください。
クエリなし	すべての NTP コントロールクエリを拒否します。
編集なし	サーバの状態を変更しようとする NTP コントロールクエリを拒否します。

「適用」をクリックして、設定内容を適用します。
「編集」をクリックして、エントリを編集します。
「削除」をクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

NTP キー設定

NTP キーの設定を行います。

管理 > NTP > NTP キー設定の順にメニューをクリックし、以下の画面を表示します。

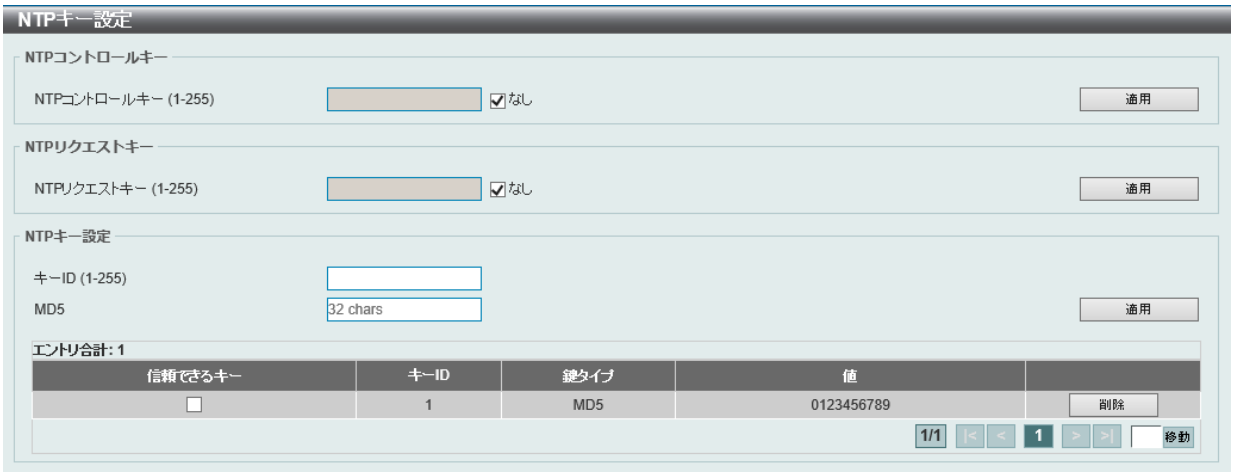


図 7-75　NTP キー設定画面

画面に表示される項目：

項目	説明
NTP コントロールキー	
NTP コントロールキー	NTP コントロールキー（制御鍵）を指定します。「なし」を選択すると NTP コントロールキーを使用しません。 • 設定可能範囲：1-255
NTP リクエストキー	
NTP リクエストキー	NTP リクエストキー（要求鍵）を指定します。 ntpdc ユーティリティプログラムによって使用される NTP モード 7 パケットのキー ID を定義するために使用されます。 「なし」を選択すると NTP リクエストキーを使用しません。 • 設定可能範囲：1-255
NTP キー設定	
キー ID	NTP キー ID を指定します。 • 設定可能範囲：1-255
MD5	MD5 認証キーを指定します。（32 文字以内）
信頼できるキー	ピア NTP システムのキーが認証に合致するための設定を行います。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

NTP インタフェース設定

NTP のインタフェース設定を行います。インタフェースの NTP パケット受信を許可 / 拒否します。

管理 > NTP > NTP インタフェース設定の順にメニューをクリックし、以下の画面を表示します。



図 7-76　NTP インタフェース設定画面

画面に表示される項目：

項目	説明
NTP ステート	「編集」をクリックして、VLAN インタフェース上の NTP 機能を有効 / 無効にします。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

NTP アソシエーション

NTP アソシエーションを表示します。

管理 > NTP > NTP アソシエーションの順にメニューをクリックし、以下の画面を表示します。



図 7-77　NTP アソシエーション画面

指定エントリ横の「詳細を表示」をクリックし、該当 NTP アソシエーションの詳細を表示します。



図 7-78　NTP アソシエーション - 詳細画面

NTP ステータス

NTP ステータスを表示します。

管理 > NTP > NTP ステータスの順にメニューをクリックし、以下の画面を表示します。

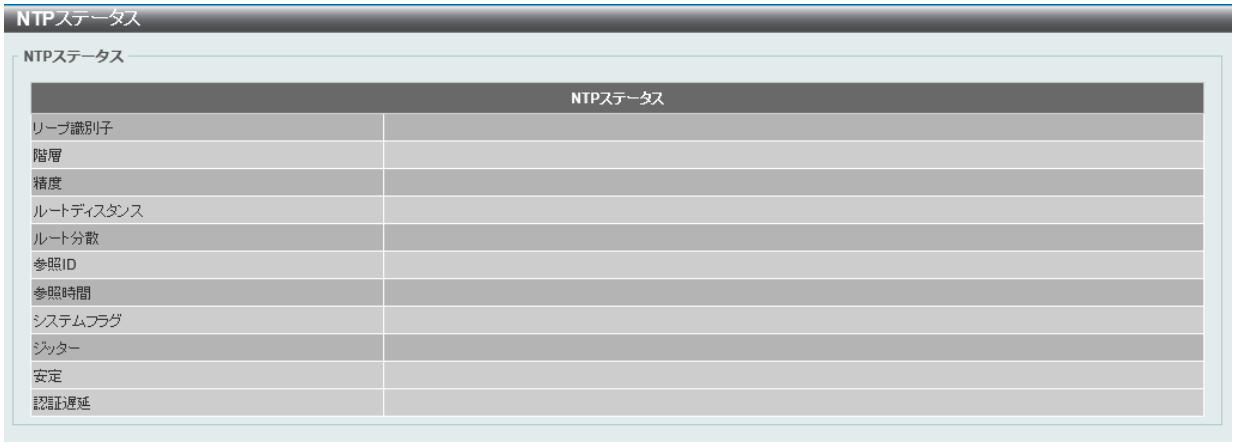


図 7-79　NTP ステータス画面

IP 送信元インタフェース

IP 送信元インタフェースを設定します。

管理 > IP 送信元インタフェースの順にメニューをクリックし、以下の画面を表示します。

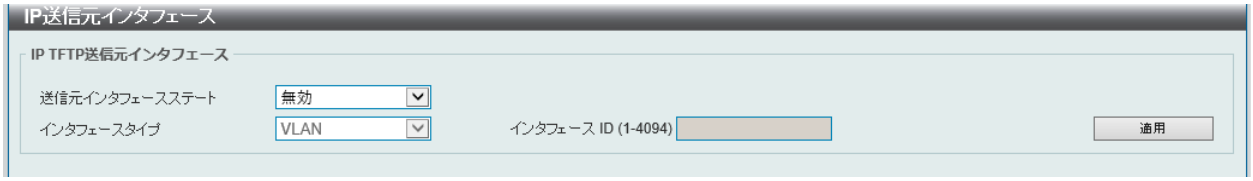


図 7-80　IP 送信元インタフェース画面

画面に表示される項目：

項目	説明
送信元インタフェースステート	IP TFTP 送信元インタフェースを指定します。
インタフェースタイプ	インタフェースの種類を指定します。 • 選択肢：「ループバック」「MGMT」「VLAN」 「MGMT」は DGS-1520-28/52 でのみ表示されます。
インタフェース ID	インタフェース ID を指定します。 • ループバックインタフェースの場合：1 - 8 • 管理インタフェース（MGMT）の場合：常に 0 • VLAN インタフェースの場合：1 - 4094

「適用」をクリックして、設定内容を適用します。

ファイルシステム設定

スイッチのファイルシステムを閲覧、管理および設定します。
フラッシュファイルシステムには、ファームウェアやコンフィグレーション等を保存できます。

管理 > ファイルシステム設定の順にメニューをクリックし、以下の画面を表示します。



図 7-81　ファイルシステム設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
パス	パスの文字列を入力します。

「移動」をクリックすると入力したパスに遷移します。
「コピー」をクリックすると指定のファイルをスイッチへコピーします。
「C:」リンクをクリックすると、「C:」ドライブに遷移します。

「C:」リンクをクリックすると、以下の画面が表示されます。

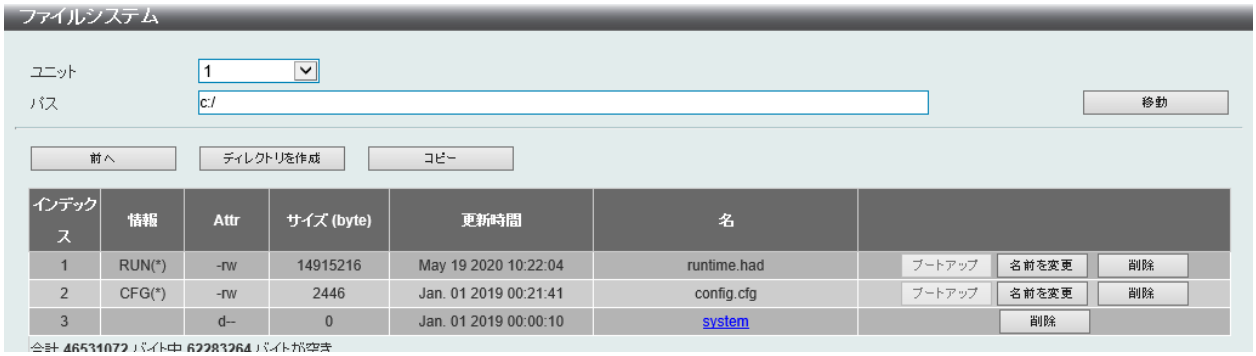


図 7-82　ファイルシステム - 詳細画面

画面に表示される項目：

項目	説明
移動	入力したパスへ移動します。
前へ	前のページに戻ります。
ディレクトリを作成	スイッチのファイルシステムに新しいディレクトリを作成します。
コピー	指定ファイルをスイッチにコピーします。
ブートアップ	起動用のブートアップイメージとコンフィグレーションを指定します。
名前を変更	ファイル名を変更します。
削除	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

「コピー」をクリックすると、以下の画面が表示されます。

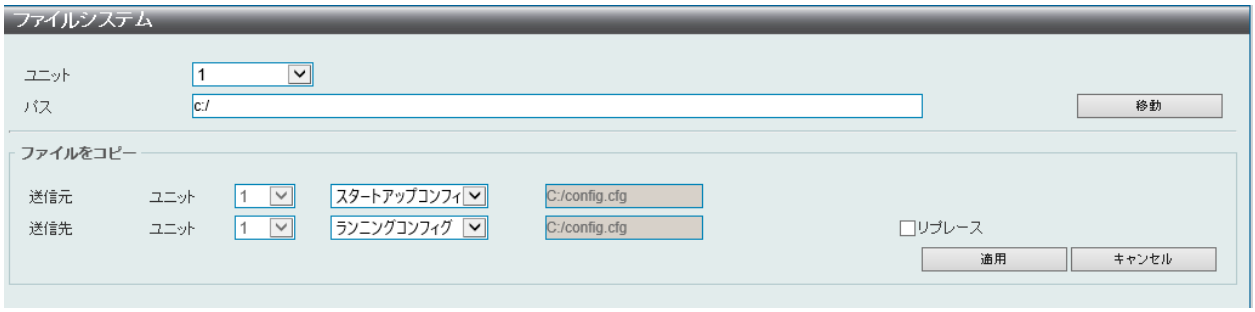


図 7-83　ファイルシステム - コピー画面

このスイッチのファイルシステムにファイルをコピーする場合、送信元と送信先のパスを入力します。

項目	説明
送信元	コピー元ファイルのあるスイッチのユニット ID とコピーされるファイルのタイプを以下から選択します。 ・「スタートアップコンフィグ」 ・「送信元ファイル」 「送信元ファイル」選択を選択した場合は、ファイルパスを入力します。
送信先	宛先スイッチのユニット ID とコピーファイルのタイプを以下から選択します。 ・「スタートアップコンフィグ」 ・「ランニングコンフィグ」 ・「送信先ファイル」 「送信先ファイル」選択を選択した場合は、ファイルパスを入力します。 「リプレース」をチェックすると、現在実行中のコンフィグファイルを指定のコンフィグファイルと差し替えます。

「適用」をクリックして、コピーを開始します。
「キャンセル」をクリックすると処理は破棄されます。

注意　ブートコンフィグファイルが破損しているとスイッチは自動的に初期設定に戻ります。

注意　ブートイメージファイルが破損しているとスイッチは自動的にバックアップイメージファイルを使用します。

スタッキング設定

DGS-1520 シリーズは、最大 8 台のスイッチのスタックをサポートしています。Telnet、Web GUI、コンソールポート、MGMT ポート、または SNMP を介して 1 つの IP アドレスで管理することができます。
スタックにより、ネットワークのアップグレードをリーズナブルでコストパフォーマンスの高い方法で実現します。これによりお使いのネットワークの信頼性、サービス性、そして可用性が向上します。

スタッキングを行うには、**管理 > 物理スタッキング**でスタッキングモードを有効にする必要があります。
2 ポートまたは 4 ポートのスタッキング設定をサポートしています。

スタッキングポートは、SIO1、SIO2 と呼ばれる 2 つの論理スタッキングポートにグループ化されます。（SIO：Stacking Input/Output ）
論理スタッキングポートのグループは、常にグループとしてスタック内の別のスイッチに接続する必要があります。

次の表に、対応する SIO ポートペアを使用したスタック構成を示します。

設定	スイッチ	論理 SIO1	論理 SIO2	帯域幅
2 ポート 10GBASE-T	DGS-1520-28	ポート 25	ポート 26	40 Gbps（全二重）
	DGS-1520-28MP	ポート 25	ポート 26	40 Gbps（全二重）
	DGS-1520-52	ポート 49	ポート 50	40 Gbps（全二重）
	DGS-1520-52MP	ポート 49	ポート 50	40 Gbps（全二重）
2 ポート SFP+	DGS-1520-28	ポート 27	ポート 28	40 Gbps（全二重）
	DGS-1520-28MP	ポート 27	ポート 28	40 Gbps（全二重）
	DGS-1520-52	ポート 51	ポート 52	40 Gbps（全二重）
	DGS-1520-52MP	ポート 51	ポート 52	40 Gbps（全二重）
4 ポート	DGS-1520-28	ポート 25 および 26	ポート 27 および 28	80 Gbps（全二重）
	DGS-1520-28MP	ポート 25 および 26	ポート 27 および 28	80 Gbps（全二重）
	DGS-1520-52	ポート 49 および 50	ポート 51 および 52	80 Gbps（全二重）
	DGS-1520-52MP	ポート 49 および 50	ポート 51 および 52	80 Gbps（全二重）

スイッチでは、以下のスタッキングトポロジがサポートされています。

- Duplex Chain
  Duplex Chain トポロジはチェーン・リンク形式でスイッチをスタックします。この方法を使用すると、一方向のデータ転送だけが可能となります。そして、1 カ所中断が発生すると、データ転送は明らかに影響を受けます。
- Duplex Ring
  Duplex Ring は、データが双方向に転送できるようにリングまたはサークルの形式でスイッチをスタックします。このトポロジは、リングに 1 カ所中断が発生しても、データはスタック内のスイッチ間の代替えパスのスタックケーブル経由で転送されるため高い冗長性を実現できます。

次の図では、2 つの 10GBASE-T ポートを介した 2 ポートスタッキング構成を使用して、偶数（4 台）のスイッチがデュプレックスチェーントポロジでスタックされています。

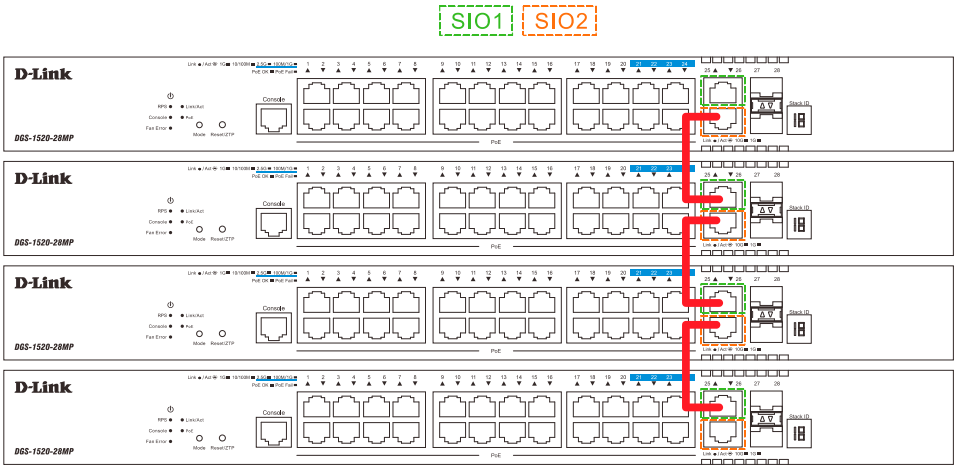


図 7-84　2 ポート・Duplex Chain でスタックされている 4 台のスイッチ

次の図では、2 つの 10GBASE-T ポートを介した 2 ポートスタッキング構成を使用して、偶数（4 台）のスイッチがデュプレックスリングトポロジでスタックされています。

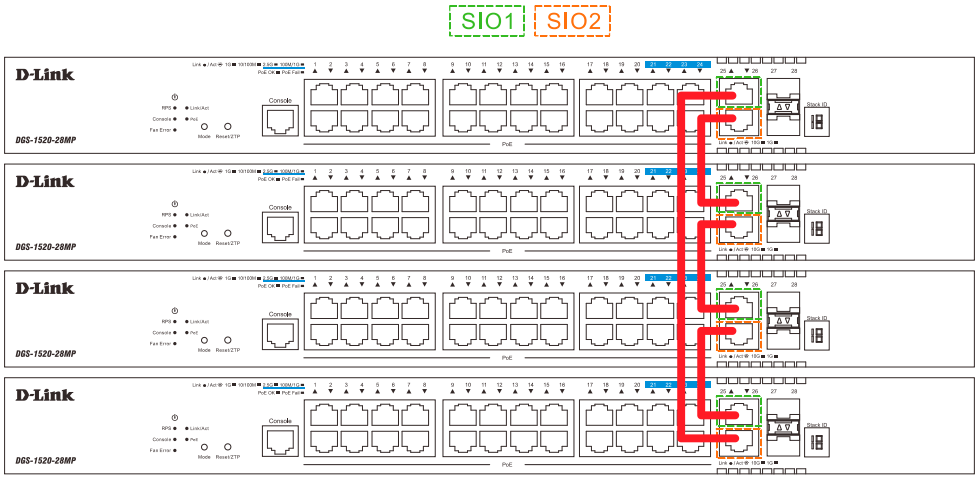


図 7-85　2 ポート・Duplex Ring でスタックされているスイッチ（4 台）

次の図では、4 ポートスタッキング構成を使用して、偶数（4 台）のスイッチがデュプレックスチェーントポロジでスタックされています。

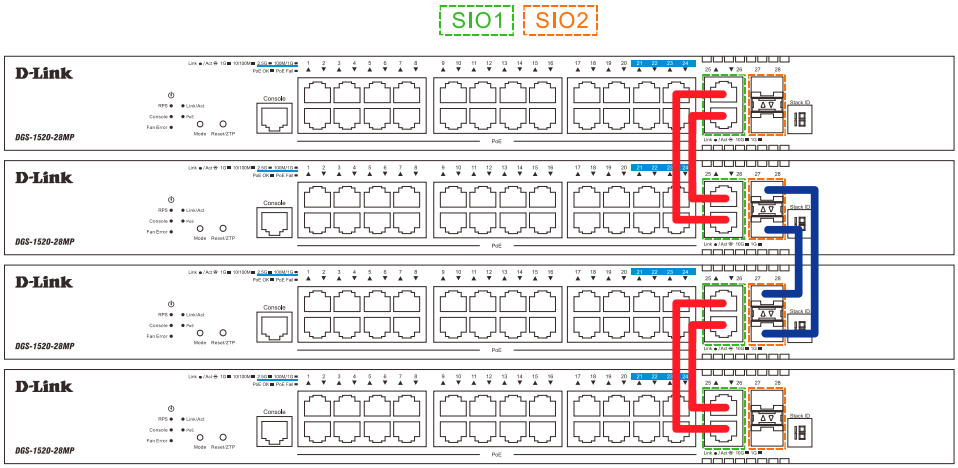


図 7-86　4 ポート・Duplex Chain でスタックされているスイッチ（4 台）

次の図では、4 ポートスタッキング構成を使用して、偶数（4 台）のスイッチがデュプレックスリングトポロジにスタックされています。

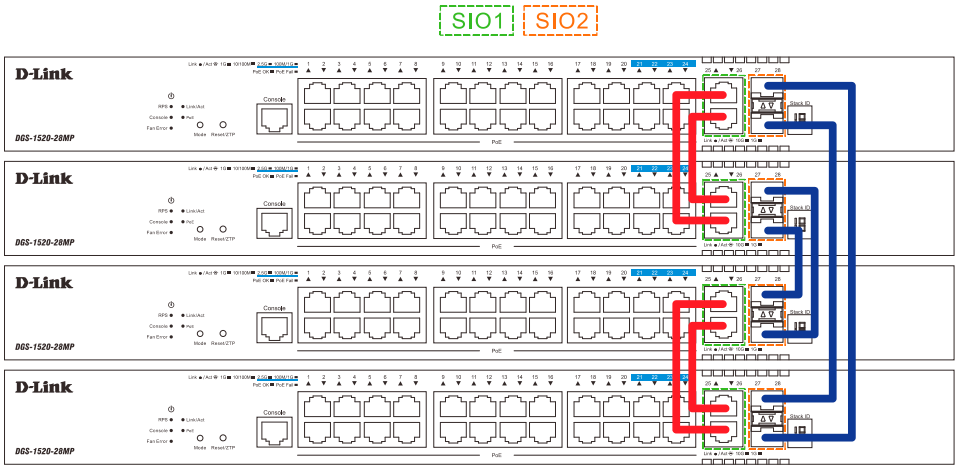


図 7-87　4 ポート・Duplex Chain でスタックされているスイッチ（4 台）

次の図では、4 ポートスタッキング構成を使用して、奇数（3 台）のスイッチがデュプレックスチェーントポロジでスタックされています。

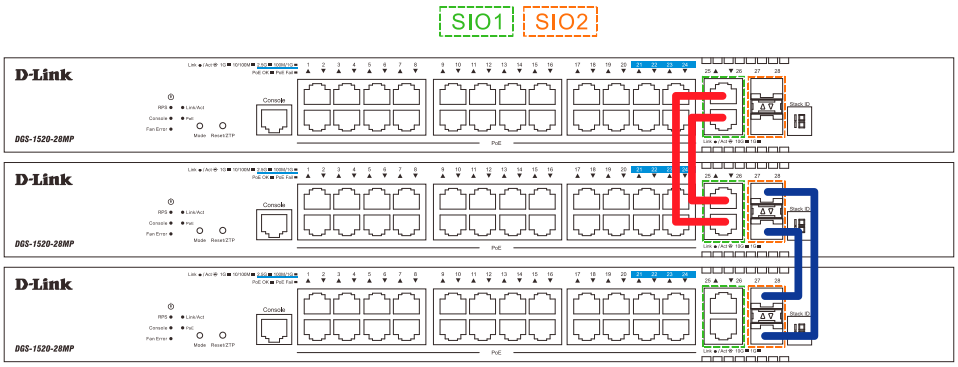


図 7-88　4 ポート・Duplex Chain でスタックされているスイッチ（3 台）

次の図では、4 ポートスタッキング構成を使用して、奇数（3 台）のスイッチがデュプレックスリングトポロジでスタックされています。
このトポロジは、DGS-1520 シリーズではサポートしていません。

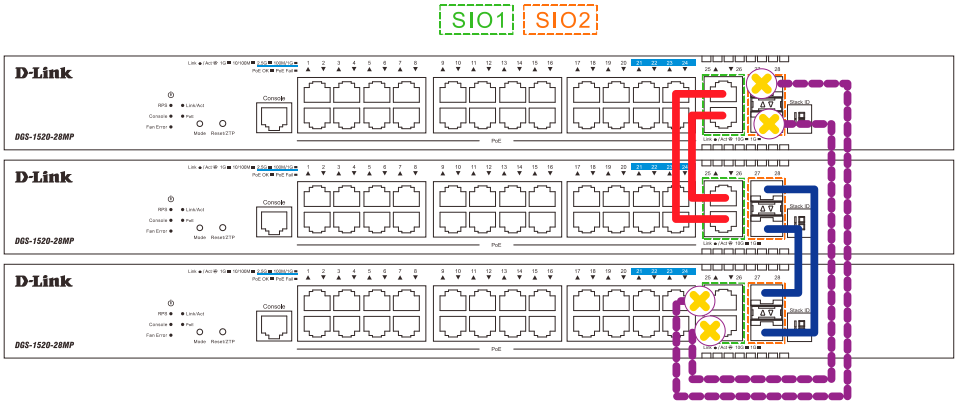


図 7-89　4 ポート・Duplex Chain でスタックされているスイッチ（3 台）

注意 DGS-1520 シリーズは、3、5、7 など奇数のスイッチを 4 ポートのデュプレックスリングトポロジでスタックできません。
スタッキングポートペアは常にスタック内の同じスイッチに接続する必要があり、奇数のスイッチの場合は上図のように「Stacking Input/Output logical port 1」（SIO1）と「SIO2」を正しくペアにできないためです。

注意 スタッキングを有効にしている時、スタッキング帯域として指定している全てのポートは他のデバイスやスイッチなどへのアップリンクとして使用できません。

注意 「Stacking Input/Output logical port 1」（SIO1）と「SIO2」は、それぞれ論理スタッキングポートのペアです。
4 ポートスタッキングを行う場合、1 つの論理スタッキングポートのペア（例：スイッチ A の SIO2 × 2）が、接続先スイッチの同じ SIO（例：スイッチ B の SIO1 × 2）に接続するようにしてください。それぞれ異なるスイッチや異なる SIO ポートに接続された場合、安定したスタッキング接続を保証できません。

スタック内のスイッチ役割

各トポロジにおいて、各スイッチはスイッチスタックにおける役割を果たします。各スイッチには役割を設定でき、スイッチスタック機能により自動的に決定することもできます。スイッチをスタックする場合に、3 つの役割があります。

● プライマリマスタ

プライマリマスタは、スタックのリーダです。スタックの通常操作、モニタ操作、およびトポロジの実行をメンテナンスします。本スイッチは、スイッチスタック内にあるスイッチにスタックユニット番号の割り当て、コンフィグレーションの同期、コマンドの送信を行います。プライマリマスタには、スタックを物理的に構成する前、またはすべての優先度が同じである場合には最も数字の低い MAC アドレスを持つスイッチに決定します。また、スタックが自動的に決定される前に、最も高い優先度（低い番号ほど優先度は高くなります。）を本スイッチに割り当てることで手動で設定することができます。プライマリマスタは、スイッチの前面パネルの一番右にある LED によって Box ID と「H」が表示されます。

● バックアップマスタ

バックアップマスタは、プライマリマスタに対するバックアップであり、プライマリマスタが故障、またはスタックから取り外される場合に、プライマリマスタの機能を引き継ぎます。また、スタック内で隣接するスイッチの状態をモニタし、プライマリマスタによって割り当てられたコマンドを実行して、プライマリマスタの動作状態をモニタします。バックアップマスタは、スタックを物理的に構成する前、またはすべての優先度が同じである場合には 2 番目に数字の低い MAC アドレスに決定します。また、スタックが自動的に決定される前に、2 番目に高い優先度（低い番号ほど優先度は高くなります。）を本スイッチに割り当てることで手動で設定することができます。バックアップマスタは、スイッチの前面パネルの一番右にある LED によって Box ID と「h」が表示されます。

● スレーブ

スレーブスイッチは、残りのスイッチスタックを構成します。プライマリマスタまたはバックアップマスタスイッチではありません。プライマリマスタおよびバックアップマスタが故障、またはスタックから取り外される場合に、それらの機能を引き継ぎます。スレーブスイッチは、マスタに要求された操作を実行して、スタックとスタックトポロジにある近接スイッチの状態をモニタします。さらに、バックアップマスタがプライマリマスタになるとバックアップマスタのコマンドに従います。スレーブスイッチは、バックアップマスタがプライマリマスタに移行する場合、バックアップマスタが故障、またはスイッチから取り外される場合に、セルフチェックを行い、自身がバックアップマスタになるかどうかを決定します。プライマリマスタとバックアップマスタの両方が故障、またはスイッチから取り外される場合、プライマリマスタになるかどうか決定します。これらの役割は、はじめに優先度によって決定され、さらに優先度が同じである場合は、最も低い MAC アドレスによって決定されます。

スイッチが希望したトポロジで構成されると、スタックは機能する状態に到達するまでに 3 つの過程を経由します。

- 初期化状態
  これは、スタックの最初の状態で、ランタイムコードが設定および初期化され、システムは各スイッチが適切に機能していることを検証するために周辺機器の診断を行います。

- マスタ選出状態
  コードがロードされ、初期化されると、スタックはマスタ選出状態になり、使用されるトポロジのタイプを検出し、プライマリマスタ、バックアップマスタの順に選出します。

- 同期状態
  プライマリマスタとバックアップマスタが確立すると、プライマリマスタがスイッチにスタックユニット番号を割り当て、すべてのスイッチに構成を同期させ、プライマリマスタの構成に基づき、残りのスイッチにコマンドを送信します。

これらの手順が終了すると、スイッチスタックは正常な操作モードに入ります。

スタックスイッチのスワップ

スイッチのスタック機能は、動作中のスタック内またはスタック外のスイッチの「ホットスワップ」をサポートしています。いくつかの簡単な条件により、電源オフやスタック内のスイッチ間のデータ転送に大きな影響を与えずに、スタックからのスイッチの取り外しやスタックへの追加を行うことができます。

スイッチが動作中のスタックに「ホットインサート」される場合、設定された優先度や MAC アドレスなど新たに追加されたコンフィグレーションによって、新しいスイッチはプライマリマスタ、バックアップマスタまたはスレーブとなる可能性があります。しかし、共に以前の選出過程を経て、その結果、プライマリマスタとバックアップマスタを持った 2 つのスタックが追加されると、新しいプライマリマスタが、優先度または MAC アドレスに基づいて、既存のプライマリマスタから選出されます。このプライマリマスタは、ホットインサートされた新しいスイッチすべてにプライマリマスタの全役割を引き継ぎます。この過程は、検出処理が完了するまで 1.5 秒ごとにスイッチスタックを通して循環するディスカバリパケットを使用して行われます。

「ホットリムーブ」の動作は、スタックが既に動作している場合にスタックからデバイスを取り外すことを意味します。ホットリムーブは、指定した間にデバイスからハートビートパケットを受信しない場合、またはスタックポートの中の 1 つのリンクがダウンした場合に、スタックによって検出されます。デバイスが一度取り外されると、残りのスイッチは、スタックトポロジデータベースを更新し、変更を反映します。スタックから 3 つの役割（プライマリマスタ、バックアップマスタ、またはスレーブ）のどれか 1 つが取り外される場合には、異なる過程がそれぞれの特定デバイス取り外しに発生します。

スレーブデバイスが取り外される場合、プライマリマスタはユニット leave メッセージの使用を通じ、このデバイスのホットリムーブを他のスイッチに通知します。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。

バックアップマスタがホットリムーブされると、新しくバックアップマスタが前述の選出過程を経由して選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。その後、データベース同期がスタックによって完了した際に、バックアップマスタはプライマリマスタのバックアップを開始します。

プライマリマスタが取り外されると、バックアップマスタはプライマリマスタの役割を引き受けて、新しいバックアップマスタが選出過程を経て選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。新しいプライマリマスタは、スタックとネットワーク内の矛盾を避けるために、前のプライマスタの MAC と IP アドレスを引き継ぎます。

プライマリマスタとバックアップマスタの両方が取り外される場合、選出過程では、直ちに処理を行い、新しいプライマリマスタとバックアップマスタを決定します。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。スタティックなスイッチ構成は、スタックに存在するスイッチに関するデータベースに残りますが、それらの機能には影響されません。

注意 スタックが検出過程にある時、Box ID の矛盾があると、そのデバイスは特別なスタンドアロントポロジモードに入ります。ユーザはデバイス情報の取得、Box ID の設定、保存、および再起動だけ行うことができます。すべてのスタックポートが無効とされ、エラーメッセージがスタック内の各デバイスのローカルコンソールポートに生成されます。ユーザは、Box ID を再設定し、スタックを再起動する必要があります。

物理スタッキング

物理スタッキングの設定を行います。

管理 > スタッキング > 物理スタッキングの順にメニューをクリックし、以下の画面を表示します。



図 7-90　物理スタッキング画面

画面に表示される項目：

項目	説明
物理スタッキング	
スタッキングモード	スタッキングモードを有効 / 無効にします。 • 初期値：無効
スタッキングプリエンプト	Stack Preempt 機能の有効 / 無効を設定します。「無効」に設定した場合、現在のマスタスイッチの優先度が 0 に変更され、新しいデバイスを現在のスタックトポロジに追加した場合でも、マスターとなるスイッチが変更されません。
トラップステート	スタック関連の SNMP トラップの送信を有効 / 無効にします。
スタック ID	
現在のユニット ID	スタックにおけるスイッチの現在のユニット番号を選択します。
新しいボックス ID	「現在のユニット ID」で選択したスタック内のスイッチに新しくボックス番号を指定します。 「自動」はスイッチスタック内のスイッチに自動的にボックス番号を割り当てます。 • 設定可能範囲：1-8
優先度	スイッチの優先度番号を指定します。 低い値ほど高い優先度を示します。スタック内で最も低い優先度番号を持つボックス（スイッチ）が、プライマリマスタです。 プライマリマスタスイッチは、スイッチスタックにおけるアプリケーションを設定するために使用されます。 • 設定可能範囲：1-63

「適用」をクリックして、設定内容を適用します。

スタッキング帯域

本項目ではスタッキング帯域の設定、表示を行います。物理スタッキングは有効化と、2 ポート /4 ポートでのスタッキング設定を行う必要があります。

「2 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 40Gbps が使用可能です。
「4 ポート」スタッキング設定時にはスイッチ間のフルデュプレックススピードで、最大 80Gbps が使用可能です。

次の表に、対応する SIO ポートペアを使用したスタック構成を示します。

設定	スイッチ	論理 SIO1	論理 SIO2	帯域幅
2 ポート 10GBASE-T	DGS-1520-28	ポート 25	ポート 26	40 Gbps（全二重）
	DGS-1520-28MP	ポート 25	ポート 26	40 Gbps（全二重）
	DGS-1520-52	ポート 49	ポート 50	40 Gbps（全二重）
	DGS-1520-52MP	ポート 49	ポート 50	40 Gbps（全二重）
2 ポート SFP+	DGS-1520-28	ポート 27	ポート 28	40 Gbps（全二重）
	DGS-1520-28MP	ポート 27	ポート 28	40 Gbps（全二重）
	DGS-1520-52	ポート 51	ポート 52	40 Gbps（全二重）
	DGS-1520-52MP	ポート 51	ポート 52	40 Gbps（全二重）
4 ポート	DGS-1520-28	ポート 25 および 26	ポート 27 および 28	80 Gbps（全二重）
	DGS-1520-28MP	ポート 25 および 26	ポート 27 および 28	80 Gbps（全二重）
	DGS-1520-52	ポート 49 および 50	ポート 51 および 52	80 Gbps（全二重）
	DGS-1520-52MP	ポート 49 および 50	ポート 51 および 52	80 Gbps（全二重）

注意 「Stacking Input/Output logical port 1」（SIO1）と「SIO2」は、それぞれ論理スタッキングポートのペアです。4 ポートスタッキングを行う場合、1 つの論理スタッキングポートのペア（例：スイッチ A の SIO2 × 2）が、接続先スイッチの同じ SIO（例：スイッチ B の SIO1 × 2）に接続するようにしてください。それぞれ異なるスイッチや異なる SIO ポートに接続された場合、安定したスタッキング接続を保証できません。

注意 スタッキング帯域のボックス ID、プライオリティの設定はスイッチをスタックする前に設定する必要があります。

管理 > スタッキング > スタッキング帯域の順にメニューをクリックし、以下の画面を表示します。



図 7-91　スタッキング帯域画面

画面に表示される項目：

項目	説明
スタッキング帯域	スタッキング帯域を指定します。 • 「2-Port-SFP+」- スタックに 2 つの SFP+ ポートを使用します。 • 「2-Port-10G-Base-T」- スタックに 2 つの RJ45 ポートを使用します。 • 「4-Port-Hybrid」- スタックにすべてのポートを使用します。

「適用」をクリックして、設定内容を適用します。

仮想スタック設定（SIM）

シングル IP マネジメント（SIM）の設定を行います。

シングル IP マネジメント（SIM）の概要

D-Link シングル IP マネジメントとは、スタックポートやモジュールを使用する代わりにイーサネット上でスイッチをスタックする方法です。シングル IP マネジメント機能を利用する利点を以下に示します。

- 帯域幅の需要の増加に対応するためにネットワークを拡張しつつ、小規模なワークグループや配線の管理を簡素化できます。
- ネットワークで必要な IP アドレスの数を減らすことができます。
- スタック接続のための特別なケーブル配線を必要としません。また、他のスタック技術ではトポロジ上の制限となり得る、距離的な問題を取り除きます。

シングル IP マネジメント（SIM）のルールと動作

D-Link シングル IP マネジメント（以下、SIM）機能を搭載するスイッチは、次のルールに従います。

- SIM はスイッチのオプション機能であり、CLI または Web インタフェース経由で簡単に有効 / 無効に設定することができます。また、SIM グループはネットワーク内のスイッチの通常動作に影響を与えることはありません。
- スイッチは 3 つの役割に分類されます。
  - **Commander Switch（CS）-** グループのマスタスイッチ
  - **Member Switch（MS）**- CS によって SIM グループのメンバとして認識されるスイッチ
  - **Candidate Switch（CaS）**- SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチ
- SIM グループの Commander Switch（CS）は 1 台のみです。
- SIM グループには、最大 32 台のスイッチ（番号：1-32）が所属できます。（Commander Switch（番号：0）を除く）
- SIM グループ内のすべてのスイッチは、同じ IP サブネット内にある必要があります。
- 同じ IP サブネット内の SIM グループ数に制限はありませんが、各スイッチは 1 つの SIM グループにしか所属することができません。
- 複数の VLAN が設定されている場合、SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- SIM は SIM をサポートしていないデバイスを経由することができます。そのため CS から 1 ホップ以上離れたスイッチを管理することができます。

SIM グループは、1 つのエンティティとして管理されるスイッチのグループです。SIM スイッチは次の 3 つのいずれかの役割を持ちます。

1. **Commander Switch（CS）-** グループの管理用デバイスとして手動で設定されるスイッチです。CS は以下の特長を持っています。
   - IP アドレスを 1 つ持つ。
   - 他の SIM グループの CS や MS ではない。
   - マネジメント VLAN 経由で MS に接続する。
2. **Member Switch（MS）**- SIM グループに所属し、CS からアクセスが可能なスイッチです。MS は以下の特徴を持っています。
   - 他の SIM グループの CS や MS ではない。
   - CS のマネジメント VLAN 経由で CS に接続する。
3. **Candidate Switch（CaS）**- SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。手動により SIM グループの MS として設定することで、SIM グループに参加させることができます。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っています。
   - 他の SIM グループの CS や MS ではない。
   - CS のマネジメント VLAN 経由で CS に接続する。

これらの役割には、さらに以下のルールが適用されます。

- 各デバイスは、まず CaS の状態から始まります。
- CaS から CS への遷移
  - ユーザは、手動により CaS を CS に設定することができます。
- CS が SIM グループの MS になるには、CS → CaS → MS の順で遷移する必要があります。CS から MS へ直接遷移することはできません。
- CS から CaS への遷移
  - ユーザは、手動により CS を CaS に設定することができます。
- CaS から MS への遷移
  - ユーザは、CS を介して、手動により CaS を MS に設定することができます。
- MS から CaS への遷移
  - ユーザは、CS を介して、手動により MS を CaS に設定することができます。
  - CS から MS への Report パケットがタイムアウトになると、MS から CaS に遷移します。

SIM グループの CS として 1 台のスイッチを設定した後、追加のスイッチをグループの MS として登録することができます。設定後、CS は MS へのアクセス用インバンドエントリポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証によって、SIM グループのすべての MS へのアクセスが制御されます。

SIM 機能を有効にすると、CS 内のアプリケーションはパケットを処理せずにリダイレクト（宛先変更）します。アプリケーションは管理者からのパケットを復号化し、データの一部を変更し、MS へ送信します。パケットが処理された後、CS は MS から Response パケットを受け取り、符号化して管理者に返送します。

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ（read/write 権限、read only 権限を含む）のメンバになります。MS が IP アドレスを持っている場合は、グループ内の他のスイッチ（CS を含む）が所属していない SNMP コミュニティに加入することができます。

バージョン 1.61 へのアップグレード

SIM 管理機能強化の目的で、本スイッチは本リリースにおいて、バージョン 1.61 にアップグレードしています。
本バージョンでは以下の改善点が加わりました。

1. CS は、再起動または Web での異常検出によって、SIM グループから抜けたメンバスイッチを自動的に再検出する機能が搭載しました。この機能は、以前設定された SIM メンバが再起動の後に発行する Discovery パケットと Maintain パケットを使用することにより実現されます。一度 MS の MAC アドレスとパスワードが CS のデータベースに記録され、MS が再起動を行うと、CS はこの MS の情報をデータベースに保存し、MS が再検出された場合、これを SIM ツリーに自動的に戻します。これらのスイッチを再検出するために設定を行う必要はありません。一度保存を行った MS の再検出ができないという場合もあります。例えば、スイッチの電源がオンになっていない場合、他のグループのメンバとなっている場合、または CS スイッチとして設定された場合は再検出処理をすることができません。

2. トポロジマップには、ポートトランクグループのメンバの接続に関する新機能が加わりました。これはポートトランクグループを構成するイーサネット接続の速度と接続数を表示する機能です。

3. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、およびログファイルのアップロードやダウンロードを複数スイッチに対して行う機能が追加されました。
   - ファームウェア : TFTP サーバから複数の MS に対するファームウェアダウンロードがサポートされました。
   - コンフィグレーションファイル : TFTP サーバを使用した複数のコンフィグレーションのダウンロード / アップロード（コンフィグレーションの復元やバックアップ用）が可能になりました。
   - ログ : 複数のログファイルを TFTP サーバにアップロード可能になりました。

4. 詳細に構成を確認しやすいようにトポロジ画面を拡大、縮小することができます。

注意 SIM 状態が有効で、スイッチの役割が Commander の場合、トポロジ、ファームウェアアップグレード、設定ファイルのバックアップ / 復元、およびログファイルのアップロードウィンドウが使用可能になります。

シングル IP 設定

スイッチは工場出荷時設定で Candidate Switch（CaS）として設定され、SIM は無効になっています。

Web インタフェースを使用してスイッチの SIM を有効にするためには**管理 > 仮想スタッキング（SIM）> シングル IP 設定**の順にメニューをクリックし、以下の画面を表示します。

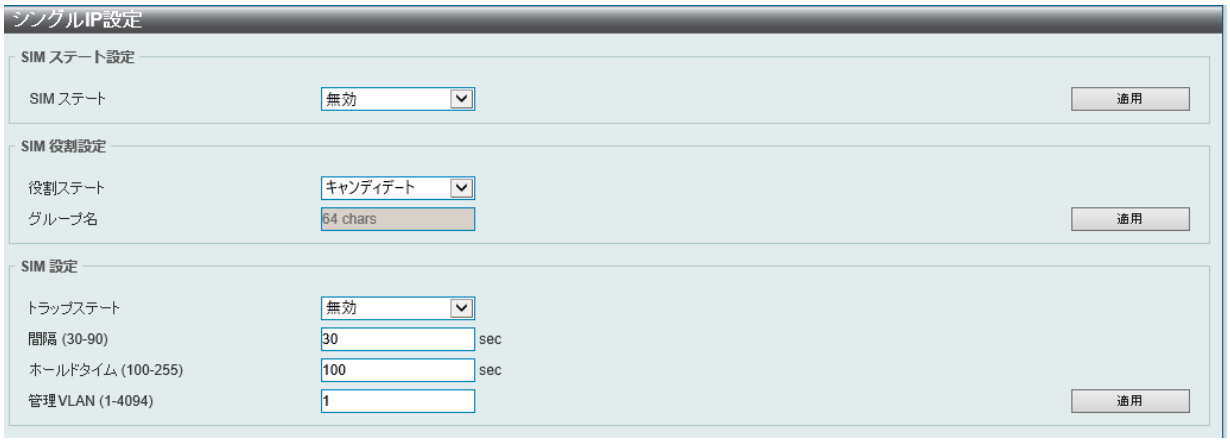


図 7-92　シングル IP 設定画面

画面に表示される項目：

項目	説明
SIM ステート設定	
SIM ステート	SIM 機能を有効 / 無効に設定します。
SIM 役割設定	
役割ステート	スイッチの SIM での役割を選択します。 • 「キャンディデート」- Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。（初期値） • 「コマンダ」- Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。
グループ名	SIM グループ名を入力します。
SIM 設定	
トラップステート	SIM トラップを有効 / 無効にします。
間隔	スイッチが Discovery パケットを送信する間隔を設定します。 • 設定可能範囲：30 - 90（秒） • 初期値：30（秒）
ホールドタイム	他のスイッチが「間隔」ので指定した間隔で送信してきた情報をスイッチが保持する時間を指定します。 • 設定可能範囲：100 - 255（秒） • 初期値：100（秒）
管理 VLAN	シングル IP マネージメントメッセージ VLAN ID を指定します。

「適用」をクリックして、設定内容を適用します。

スイッチを CS（Commander Switch）として登録すると、「仮想スタッキング（SIM）」フォルダには 4 つのリンクが追加され、Web を使用した SIM 設定が続けられるようになります。

CS スイッチで設定可能なメニューリンク：
- 「トポロジ」
- 「ファームウェアアップグレード」
- 「設定ファイルバックアップ / リストア」
- 「ログファイルをアップロード」

トポロジ

SIM グループ内のスイッチの設定および管理を行います。本画面は表示のためには、ご使用のコンピュータに Java スクリプトが必要です。

管理 > 仮想スタッキング（SIM）> トポロジの順にメニューをクリックします。以下の画面が表示されます。



図 7-93　トポロジ画面

メニューバー

トポロジ画面には、デバイスの設定のために以下のようなメニューバーが配置されています。



図 7-94　トポロジメニューバー

メニューバーには以下の 5 つのメニューが存在します。

■「ファイル」メニュー

- トポロジの印刷 – トポロジマップを印刷します。
- 優先度 – ポーリング間隔を設定します。

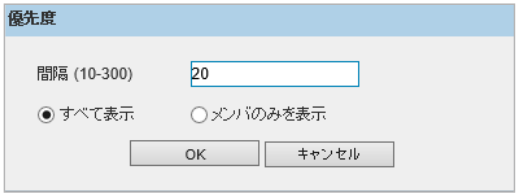


図 7-95　優先度

画面に表示される項目：

項目	説明
間隔	SIM トポロジ表示の更新間隔を指定します。 • 設定可能範囲：10-300
全て表示	トポロジにおいて全ての有効な SIM デバイスを表示します。
メンバのみを表示	トポロジにおいて SIM メンバデバイスのみを表示します。

設定を変更する際は、「OK」をクリックし、設定内容を適用してください。
「キャンセル」をクリックし、変更した設定内容を破棄します。

■「グループ」メニュー

- 「グループに追加」– グループに CaS を追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS を SIM グループに追加するための認証を行います。パスワードを入力して「適用」をクリックするか、「キャンセル」をクリックして画面を閉じます。

- 「グループから削除」– MS をグループから削除します。

■「デバイス」メニュー

- 「設定」– 指定したデバイスの Web マネージャを開きます。

■「閲覧」メニュー

- 更新 – ビューを最新の状態に更新します。
- トポロジ – トポロジビューを表示します。

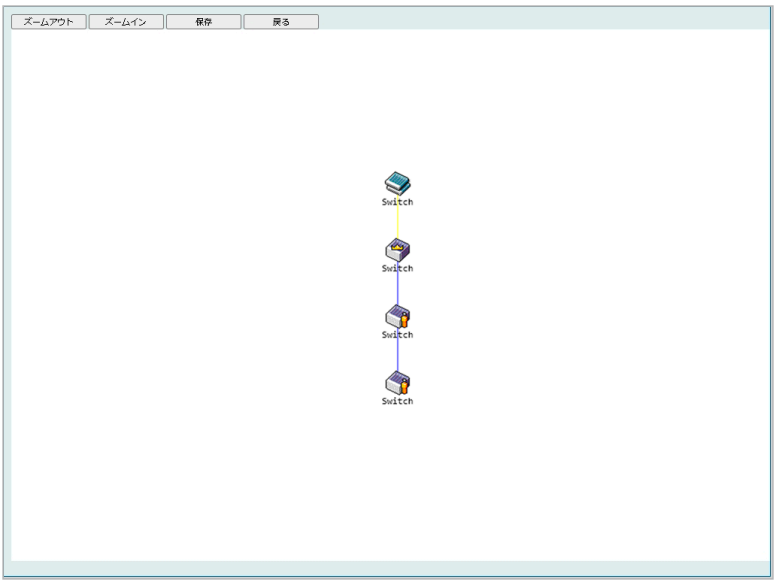


図 7-96　閲覧 - トポロジ画面

「ズームイン」をクリックすると表示アイテムが拡大します。
「ズームアウト」をクリックすると表示アイテムが縮小します。
「保存」をクリックすると表示が保存されます。
「戻る」をクリックすると前画面に戻ります。

本画面は、SIM グループ内のデバイスが他のグループやデバイスとどのように接続しているかを表示します。

本画面で表示されるアイコンは以下の通りです。

アイコン	説明
	グループ
	レイヤ 2 Commander スイッチ
	レイヤ 3 Commander スイッチ
	他のグループの Commander スイッチ
	レイヤ 2 Member スイッチ
	レイヤ 3 Member スイッチ

アイコン	説明
	他のグループの Member スイッチ
	レイヤ 2 Candidate スイッチ
	レイヤ 3 Candidate スイッチ
	不明なデバイス
	SIM 非対応のデバイス

ツールヒント

トポロジビュー画面では、マウスはデバイス情報の確認と設定のために重要な役割を果たします。トポロジ画面の特定のデバイス上にマウスポインタを指定すると、ツリービューと同様にデバイス情報（ツールヒント）を表示します。以下にその例を示します。

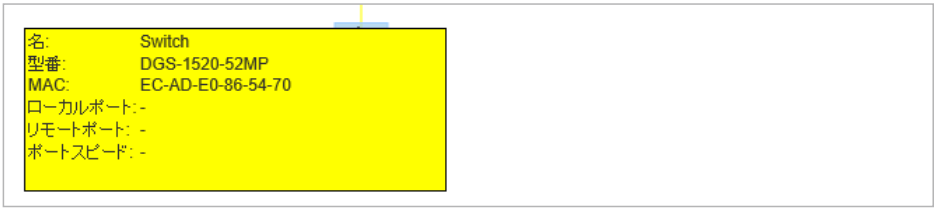


図 7-97　ツールヒントを利用したデバイス情報の表示

2 つのデバイスの間のライン上でマウスポインタを静止させると、以下の図のようにデバイス間の接続速度を表示します。

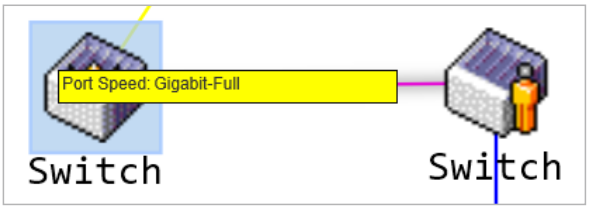


図 7-98　ツールヒントを利用したポート速度の表示

右クリックメニュー

デバイスのアイコン上で右クリックすると、スイッチのプロパティの表示や機能の設定、グループへの追加 / 削除を実行できます。

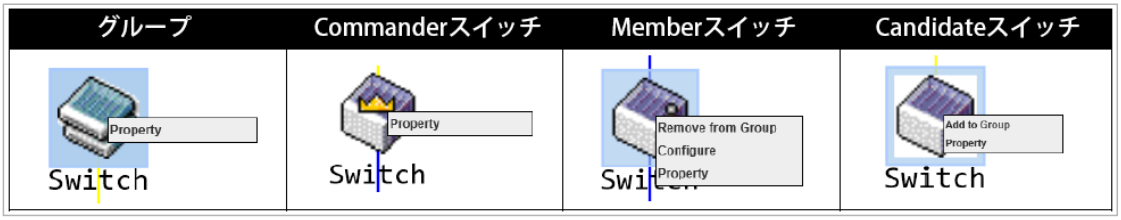


図 7-99　各アイコン上での右クリック

画面に表示される項目：

項目	説明
プロパティ	ポップアップ画面が開き、デバイスの情報を表示します。
設定	Web 管理機能を起動して、スイッチの設定を可能にします。
グループに追加	CaS をグループに追加します。このオプションを選択すると、パスワード入力画面が表示され、CaS スイッチを SIM グループに追加するための認証を行います。
グループから削除	メンバをグループから削除します。

■　プロパティ画面

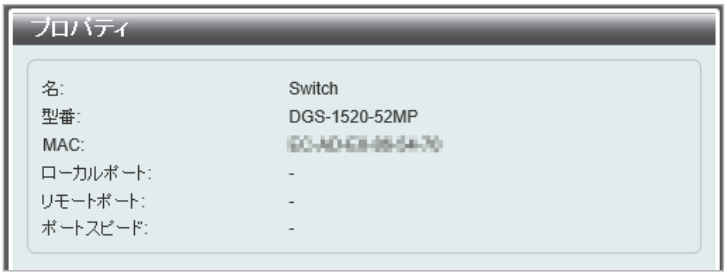


図 7-100　プロパティ画面

画面に表示される項目：

項目	説明
名	SIM グループ内のスイッチのデバイス名を表示します。
型番	スイッチの型番を表示します。
MAC	スイッチの MAC アドレスを表示します。
ローカルポート	MS または CaS が接続している CS の物理ポートの番号を表示します。CS の場合は何も表示されません。
リモートポート	CS が接続している MS または CaS の物理ポートの番号を表示します。CS の場合は何も表示されません。
ポートスピード	CS と MS/CaS 間の接続スピードを表示します。

■ 「ヘルプ」メニュー

• 「概要」– 現在の SIM バージョンなどの SIM 情報を表示します。



図 7-101　概要ダイアログボックス

ファームウェアアップグレード

CS から MS へのファームウェアの更新を行います。

管理 > 仮想スタッキング（SIM）> ファームウェアアップグレードの順にメニューをクリックし、以下の画面を表示します。



図 7-102　ファームウェアアップグレード画面

画面に表示される項目：

項目	説明
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。
パスファイル名	パスとファイル名を入力します。

「ダウンロード」をクリックすると、ファイル転送が開始されます。

設定ファイルバックアップ / リストア

CS から MS に対して TFTP サーバを使用してコンフィグレーションファイルのバックアップまたはリストアを行います。

管理 > 仮想スタッキング（SIM）> 設定ファイルバックアップ / リストアの順にメニューをクリックし、以下の画面を表示します。



図 7-103　設定ファイルバックアップ / リストア画面

画面に表示される項目：

項目	説明
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。
パスファイル名	パスとファイル名を入力します。

「復元」をクリックし、TFTP サーバからメンバスイッチへのコンフィグレーションのリストアを実行します。
「バックアップ」をクリックし、TFTP サーバへバックアップファイルを保存します。

ログファイルをアップロード

以下の画面は、SIM メンバスイッチから指定した PC へログファイルのアップロードを行う際に使用します。

管理 > 仮想スタッキング（SIM）> ログファイルをアップロードの順にメニューをクリックし、以下の画面を表示します。



図 7-104　ログファイルをアップロード画面

画面に表示される項目：

項目	説明
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。
パスファイル名	パスとファイル名を入力します。

「アップロード」をクリックすると、ファイル転送が開始されます。

D-Link ディスカバリプロトコル

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

DDP 設定

D-Link ディスカバリプロトコル（DDP）を有効 / 無効にします。

管理 > D-Link ディスカバリプロトコル > DDP 設定の順にメニューをクリックし、以下の画面を表示します。



図 7-105　DDP 設定画面

画面に表示される項目：

項目	説明
DDP グローバル設定	
D-Link ディスカバリプロトコルステート	DDP をグローバルに有効 / 無効にします。
レポートタイマ	DDP レポートメッセージの送信間隔（秒）を指定します。 「Never」を選択すると、スイッチはレポートメッセージの送信を停止します。 • 選択肢：「30」「60」「90」「120」「Never」（秒）
DDP ポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートの DDP 機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

DDP 隣接

DDP 隣接機器の表示を行います。

管理 > D-Link ディスカバリプロトコル > DDP 隣接の順にメニューをクリックし、以下の画面を表示します。



図 7-106　DDP 設定画面

画面に表示される項目：

項目	説明
ユニット	ユニットを選択します。
ポート	ポートを選択します。

「検索」をクリックすると、指定したポートを介して接続している DDP 隣接機器が表示されます。
「すべて表示」をクリックすると、本スイッチに接続しているすべての DDP 隣接機器が表示されます。
「詳細を表示」をクリックすると、エントリの詳細情報が表示されます。

SMTP 設定

Simple Mail Transfer Protocol（SMTP）の表示、設定を行います。

管理 > SMTP 設定の順にメニューをクリックし、以下の画面を表示します。

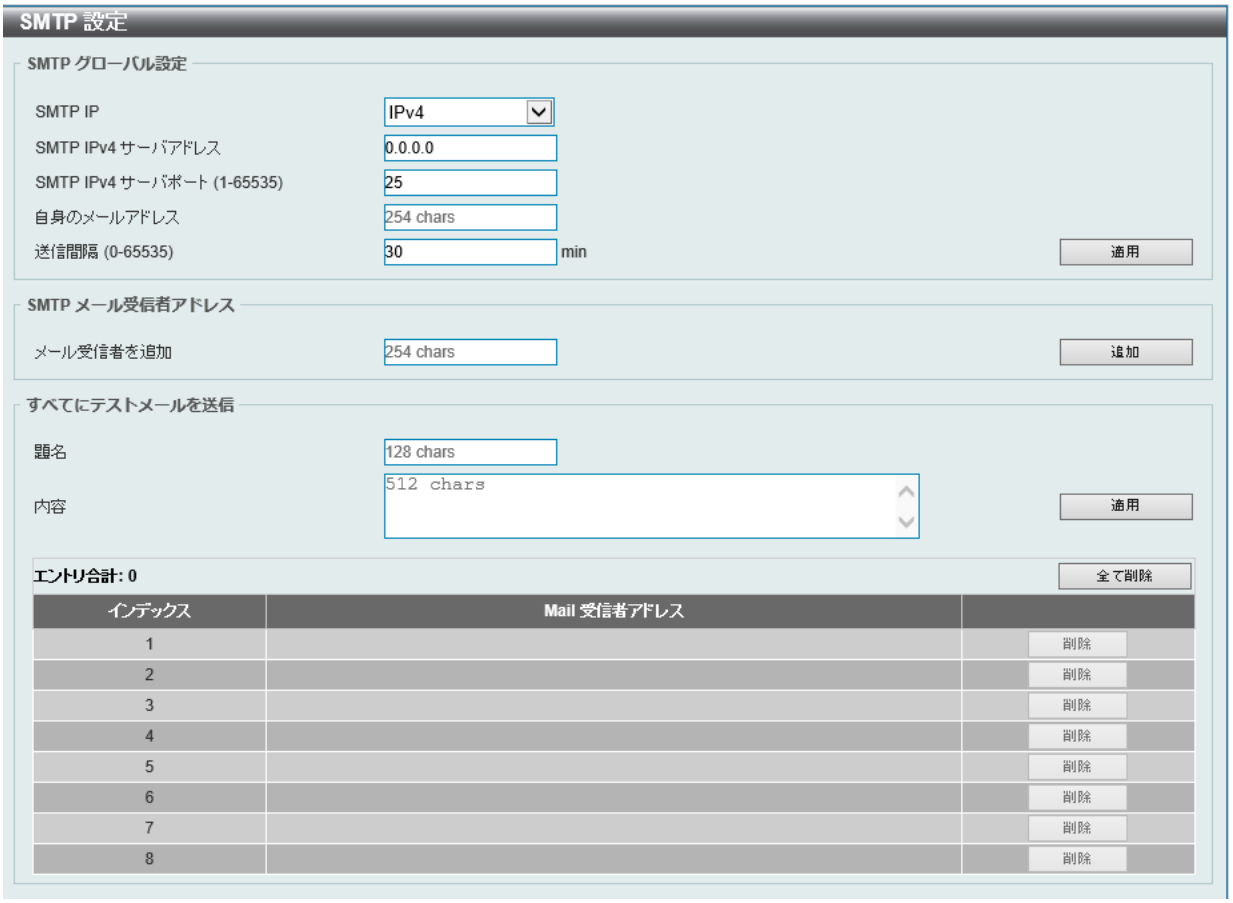


図 7-107　SMTP 設定画面

画面に表示される項目：

項目	説明
SMTP グローバル設定	
SMTP IP	SMTP サーバ IP アドレスタイプを指定します。 • 選択肢：「IPv4」「IPv6」
SMTP IPv4 サーバアドレス	SMTP サーバ IPv4 アドレスを指定します。
SMTP IPv6 サーバアドレス	SMTP サーバ IPv6 アドレスを指定します。
SMTP IPv4 サーバポート	SMTP IPv4 サーバポート番号を指定します。 • 設定可能範囲：1 - 65535 • 初期値：25
SMTP IPv6 サーバポート	SMTP IPv6 サーバポート番号を指定します。 • 設定可能範囲：1 - 65535 • 初期値：25
自身のメールアドレス	スイッチの E メールアドレスを指定します。（254 文字以内）
送信間隔	送信間隔を指定します。 • 設定可能範囲：0 - 65535（分） • 初期値：30（分）
SMTP メール受信者アドレス	
メール受信者を追加	受信者の E メールアドレスを指定します。（254 文字以内）
すべてにテストメールを送信	
題名	E メールの件名を指定します。（128 字以内）
内容	E メールの内容を指定します。（512 字以内）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「全て削除」をクリックして、すべてのエントリを削除します。

NLB FDB 設定

本スイッチはネットワークロードバランシング（NLB）をサポートしています。
本機能は、複数のサーバが同じ IP アドレスと MAC アドレスを共有する Microsoft サーバロードバランシングアプリケーションをサポートするために使用されます。クライアントからの要求はすべてのサーバに転送されますが、そのうちの 1 つによってのみ処理されます。サーバは、2 つの異なるモードで動作可能です。

- ユニキャストモード：クライアントはユニキャスト MAC アドレスをサーバへの宛先 MAC として使用します。
- マルチキャストモード：クライアントはマルチキャスト MAC アドレスをサーバへの宛先 MAC として使用します。

この宛先 MAC アドレスは、共有 MAC アドレスと呼ばれます。ただし、サーバは応答パケットの送信元 MAC アドレスとして（共有 MAC アドレスではなく）自身の MAC アドレスを使用します。つまり、NLB ユニキャストアドレスは通常、パケットの送信元 MAC アドレスではありません。

受信したパケットに、設定されたユニキャスト MAC アドレスと一致する宛先 MAC アドレスが含まれている場合、VLAN メンバシップ設定に関係なく、指定のポートに転送されます。

管理者は、MAC アドレステーブルのスタティックアドレスを NLB アドレスとして設定することはできません。ただし、MAC アドレスが NLB MAC アドレスエントリとして作成されている場合、同じ MAC アドレスをレイヤ 2MAC アドレステーブルで動的に学習できます。この場合、NLB の方が優先順位が高くなり、動的に学習された FDB エントリは有効になりません。

管理 > NLB FDB 設定の順にメニューをクリックし、以下の画面を表示します。



図 7-108　NLB FDB 設定画面

画面に表示される項目：

項目	説明
NLB タイプ	NLB タイプを指定します。 • 選択肢：「ユニキャスト」「マルチキャスト」
VID	「マルチキャスト」を選択した場合、設定する VLAN ID を入力します。
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。 受信したパケットに、指定された MAC アドレスと一致する宛先 MAC アドレスが含まれている場合、指定されたインタフェースに転送されます。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を設定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。
「全て削除」をクリックするとすべてのエントリを削除します。

複数ページ存在する場合、ページ番号を指定して「移動」をクリックすることで、特定のページへ移動することができます。

注意　物理スタックしているスイッチにおいて、L3 の NLB を行っているサーバを筐体またぎの LAG（リンクアグリゲーショングループ）では接続できません。物理スタックとの併用はしないでください。

第 8 章　L2 機能

L2 機能メニューを使用し、本スイッチにレイヤ 2 機能を設定することができます。

以下は L2 機能サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
FDB	FDB（Forwarding DataBase/ フォワーディングデータベース）の設定を行います。
VLAN	802.1Q スタティック VLAN の設定を行います。
VLAN トンネル	802.1Q VLAN トンネルの設定を行います。
STP	スパニングツリープロトコル（STP）設定を行います。3 つのバージョンの STP（802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。
ERPS（G.8032）	「Ethernet Ring Protection Switching」（ERPS）の表示、設定を行います。 ERPS はイーサネットリング保護スイッチングの業界標準（ITU-T G.8032）です。
ループバック検知	ループバック検知（LBD）機能の設定を行います。
リンクアグリゲーション	リンクアグリゲーションの設定を行います。
L2 プロトコル トンネル	L2 プロトコル トンネルの設定を行います。
L2 マルチキャストコントロール	IGMP（Internet Group Management Protocol）スヌーピング機能はじめとした L2 マルチキャストコントロールの設定を行います。
LLDP	Link Layer Discovery Protocol（LLDP）の設定を行います。

FDB

FDB（Forwarding DataBase/ フォワーディングデータベース）の設定を行います。

スタティック FDB

ユニキャストスタティック FDB

スイッチにスタティックなユニキャストフォワーディングを設定します。

L2 機能 > FDB > スタティック FDB > ユニキャストスタティック FDB の順にメニュークリックし、以下の画面を表示します。

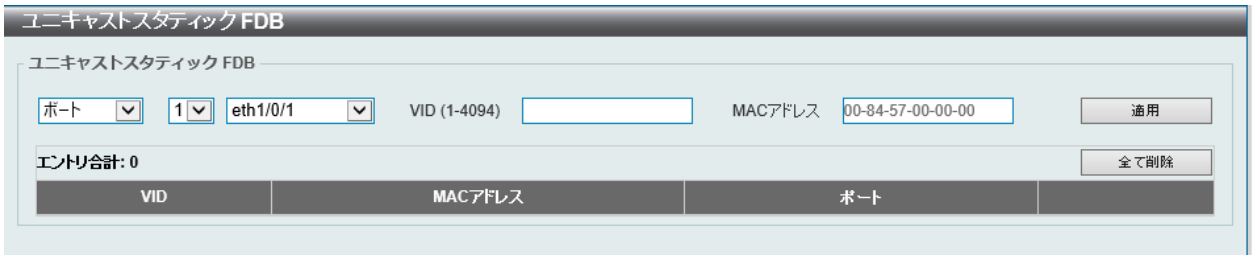


図 8-1　ユニキャストスタティック FDB 画面

画面に表示される項目：

項目	説明
ポート / 破棄	指定 MAC アドレスのあるポート番号を指定します。 また、本オプションはユニキャストのスタティック FDB から MAC アドレスを削除することもできます。 • 「ポート」- 指定 MAC アドレスのあるポート番号を指定します。「ユニット ID: ポート番号」（例 1:5）または「ポート番号」（例 5）という形式とします。ポート番号だけを入力する場合、ユニット番号の初期値は 1 となります。 • 「破棄」- ユニキャストのスタティック FDB から MAC アドレスを破棄します。
ユニット	設定するユニットを指定します。
ポート番号	「ポート」を選択した場合、ポート番号を入力します。
VID	関連するユニキャスト MAC アドレスが存在する VLAN ID を指定します。
MAC アドレス	パケットがスタティックに送信される宛先の MAC アドレスを入力します。ユニキャスト MAC アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。「全て削除」をクリックするとすべてのエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

マルチキャストスタティック FDB

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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 の順にメニュークリックし、以下の画面を表示します。



図 8-2　マルチキャストスタティック FDB 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
VID	指定のマルチキャスト MAC アドレスが所属する VLAN の VLAN ID を入力します。
MAC アドレス	マルチキャストパケットのスタティック送信先 MAC アドレスを入力します。マルチキャスト MAC アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。「全て削除」をクリックするとすべてのエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

MAC アドレステーブル設定

スイッチの MAC アドレステーブルの設定を行います。

L2 機能 > FDB > MAC アドレステーブル設定の順にメニューをクリックし、以下の画面を表示します。

グローバル設定タブ

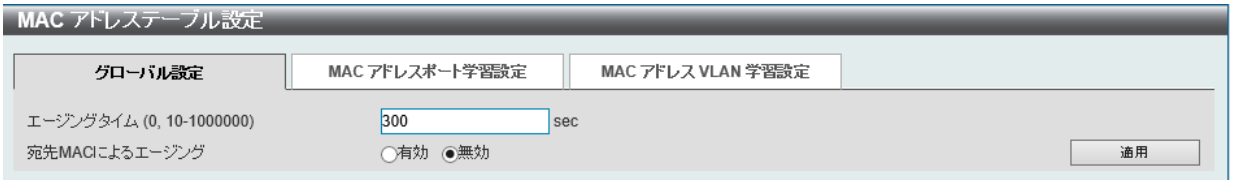


図 8-3　MAC アドレステーブル設定 - グローバル設定タブ画面

画面に表示される項目：

項目	説明
エージングタイム	MAC アドレステーブルのエージングタイムを入力します。 設定した時間中にアクセスのない端末について、学習した MAC アドレスを MAC アドレステーブルから削除します。 • 入力可能範囲：0，10 - 1000000（秒） • 初期値：300（秒） 0 に設定した場合、学習した MAC アドレスは削除されません。
宛先 MAC によるエージング	送信元 MAC アドレスだけでなく、宛先 MAC アドレスによる MAC アドレステーブルの更新を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

MAC アドレスポート学習設定タブ



図 8-4　MAC アドレステーブル設定 - MAC アドレスポート学習設定タブ画面

以下の項目を使用して、設定および表示を行います。

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ステータス	指定したポートの MAC アドレスラーニングを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

MAC アドレス VLAN 学習設定タブ



図 8-5　MAC アドレステーブル設定 - MAC アドレス VLAN 学習設定タブ画面

画面に表示される項目：

項目	説明
VID リスト	本設定を適用する VLAN ID を入力します。 複数の VLAN ID をカンマで区切って入力、または VLAN ID の範囲をハイフンで区切って入力することも可能です。
ステータス	指定した VLAN の MAC アドレスラーニングを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

MAC アドレステーブル

スイッチの MAC アドレスフォワーディングテーブルを参照します。

L2 機能 > FDB > MAC アドレス テーブルの順にメニューをクリックし、以下の画面を表示します。



図 8-6　MAC アドレステーブル画面

画面に表示される項目：

項目	説明
ポート	削除 / 表示するエントリのユニット ID およびポート番号を指定します。
VID	削除 / 表示するエントリの VLAN ID を入力します。
MAC アドレス	削除 / 表示するエントリの MAC アドレスを入力します。

複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

エントリの検索 / 表示

「検索」をクリックして、指定したポート、VLAN または MAC アドレスをキーとして検索します。
「すべて表示」をクリックして、アドレステーブルのすべてのエントリを表示します。

ダイナミックエントリの削除

「Dynamic をクリア（ポート毎 /VLAN 毎 /MAC 毎）」をクリックして、アドレステーブルのダイナミックエントリを削除します。
「すべてをクリア」をクリックして、アドレステーブルのすべてのエントリを表示します。

MAC 通知

スイッチの MAC 通知をグローバルに設定します。また、スイッチの各ポートに MAC 通知を設定します。

L2 機能 > FDB > MAC 通知 の順にメニューをクリックし、以下の画面を表示します。



図 8-7　MAC 通知 画面

画面に表示される項目：

項目	説明
MAC アドレス通知	スイッチ上の MAC 通知のグローバルステータスを有効 / 無効に設定します。
間隔	通知を行う間隔を指定します。 • 設定可能範囲：1-2147483647（秒） • 初期値 : 1（秒）
履歴サイズ	通知用に使用するヒストリログの最大エントリ数を指定します。（最大 500 エントリ） • 設定可能範囲：0-500 • 初期値 : 1
MAC 通知トラップステート	MAC 通知トラップを有効 / 無効に設定します。
トラップタイプ	トラップタイプを選択します。 •「VID なし」- トラップ情報に VLAN ID を含めません。 •「VID 付」- トラップ情報に VLAN ID を含めます。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	MAC 通知設定を有効または無効にするポートの範囲を指定します。
追加されたトラップ	選択したポートの追加トラップを有効 / 無効に設定します。
削除されたトラップ	選択したポートの削除トラップを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

MAC 通知履歴タブ



図 8-8　MAC 通知 - MAC 通知履歴タブ画面

MAC 通知メッセージの履歴が表示されます。

VLAN について

IEEE 802.1p プライオリティについて

IEEE 802.1p 標準規格で定義されるプライオリティタグ機能では、多くの異なる種類のデータが同時に送受信されるようなネットワークにおいてトラフィックを制御することができます。本機能は、混雑したネットワーク上でのタイムクリティカルなデータの伝送時に発生する問題を解決するために開発されました。例えばビデオ会議のような、タイムクリティカルなデータに依存するタイプのアプリケーションの品質は、わずかな伝送遅延にも多大な影響を受けてしまいます。

IEEE 802.1p 標準規格に準拠するネットワークデバイスは、データパケットのプライオリティレベル（優先度）を認識することができます。また、これらのデバイスでは、パケットに対してプライオリティレベルやタグを割り当てたり、パケットからタグを取り外したりすることも可能です。このプライオリティタグ（優先タグ）により、パケットの緊急度および送信キューが決定します。

プライオリティタグは 0 から 7 までの値で設定され、0 が最も低い優先度、7 が最も高い優先度を表します。一般的にプライオリティ値「7」は、伝送遅延に影響を受けやすい音声・映像に関連するデータや、データ転送速度が保証されているような特別なユーザに対して使用されます。

本スイッチでは、プライオリティタグ付きのパケットをどのように扱うかを細かく調整することができます。キューを利用してプライオリティタグ付きのデータを管理することにより、ご使用のネットワークのニーズに合わせてデータの優先度を設定できます。複数の異なるタグ付きパケットを同じキューにグループ化することで効果を発揮するケースもありますが、通常は、優先度の最も高いキュー（キュー 7）をプライオリティレベル 7 のパケットに割り当てることをお勧めします。プライオリティレベルが設定されていないパケットは、キュー 0 に割り当てられ、最も低い送信優先度となります。

本スイッチは、優先制御方式として Strict モードと WRR（重み付けラウンドロビン）モードをサポートしています。WRR モードではキューからパケットが送信される比率が決定します。キュー 0 とキュー 7 の送信比率が 4 : 1 の場合、キュー 0 から 1 つのパケットが送信される毎に、キュー 7 から 4 つのパケットが送信されます。

プライオリティキューはスイッチ上のすべてのポートに対して設定されるため、スイッチに接続されるすべてのデバイスがこの設定による影響を受けることに注意してください。ご利用のネットワーク上のスイッチがプライオリティタグ割り当て機能をサポートしている場合、プライオリティキューイング機能は特に効果を発揮します。

VLAN とは

VLAN（Virtual Local Area Network : 仮想 LAN）とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。VLAN を使用することで、LAN セグメントの集まりを自律的なユーザグループへと結合し、1 つの LAN のように見せることができます。また、ネットワークを異なるブロードキャストドメインに論理的に分割し、パケットが特定 VLAN 内のポート間にのみ送信されるように設定することが可能です。一般的に、VLAN とサブネットは 1 対 1 で対応付けられますが、必ずしもそうである必要はありません。

VLAN では、ネットワーク帯域の消費を抑えることでパフォーマンスを改善し、トラフィックを特定のドメイン内に制限することでセキュリティを強化します。

VLAN は、物理的位置ではなく論理的にエンドノードを束ねた集合体です。頻繁に通信を行うエンドノード同士に対しては、ネットワーク上の物理的位置に関わらず、同じ VLAN を割り当てます。ブロードキャストパケットは送信元と同じ VLAN メンバに対してのみ送信されるため、VLAN は論理的にはブロードキャストドメインと同等と言えます。

本スイッチシリーズにおける VLAN について

エンドノードの識別方法や VLAN メンバシップ割り当て方法に関わらず、VLAN 間にルーティング機能を持つネットワークデバイスが存在しない限り、パケットが VLAN をまたいで送信されることはありません。

本スイッチは、IEEE 802.1Q VLAN とポートベース VLAN をサポートします。タグなし機能では、パケットヘッダから 802.1Q タグを取り外すことにより、タグを認識しないデバイスとの互換性を保ちます。

スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。
「default」VLAN の VID は 1 です。ポートベース VLAN のメンバポートは重複して設定することが可能です。

IEEE 802.1Q VLAN

用語の説明

- タグ付け - パケットのヘッダに 802.1Q VLAN 情報を挿入すること。
- タグなし - パケットのヘッダから 802.1Q VLAN 情報を削除すること。
- イングレスポート（Ingress Port）- スイッチ上のパケットを受信するポート。VLAN の照合が行われます。
- イーグレスポート（Egress Port）- スイッチ上のパケットを送信するポート。タグ付けの決定が行われます。

本スイッチには、IEEE 802.1Q（タグ付き）VLAN が実装されています。802.1Q VLAN で行われるタグ付けによってネットワーク全体で 802.1Q VLAN が有効になります（ネットワーク上のすべてのスイッチが IEEE 802.1Q 準拠である場合）。

VLAN によりネットワークを分割することで、ブロードキャストドメインの範囲を小さくすることができます。パケットは、（IEEE 802.1Q をサポートするスイッチを経由して）受信 VLAN と同じ VLAN メンバのステーションのみに送信されます。このパケットには、送信元の不明なブロードキャスト、マルチキャスト、ユニキャストパケットも含まれます。

このほか、VLAN はネットワークにおけるセキュリティ機能を提供します。IEEE 802.1Q VLAN では、VLAN メンバであるステーションにのみパケットが送信されます。

各ポートに対して、タグ付けまたはタグなしに設定することが可能です。IEEE 802.1Q VLAN のタグなし機能により、パケットヘッダ中の VLAN タグを認識しない旧式のスイッチと連携することができます。タグ付け機能では、802.1Q 準拠の複数のスイッチを 1 つの物理接続により結びつけ、すべてのポート上でスパニングツリーを有効にして正常に動作させることができます。

IEEE 802.1Q 標準では、受信ポートが所属する VLAN へのタグなしパケットの送信を禁じています。

IEEE 802.1Q 標準規格の主な特徴は以下の通りです。
- フィルタリングによりパケットを VLAN に割り当てます。
- 全体で 1 つのスパニングツリーが構成されていると仮定します。
- 1 レベルのタグ付けにより明示的なタグ付けスキームを使用します。
- 802.1Q VLAN のパケット転送
- パケットの転送は以下の 3 種類のルールに基づいて決定されます。
  イングレスルール - VLAN に所属する受信フレームの分類に関するルール。
  ポート間のフォワーディングルール - 転送するかしないかを決定します。
  イーグレスルール - パケットが送信される時にタグ付きかタグなしかを決定します。

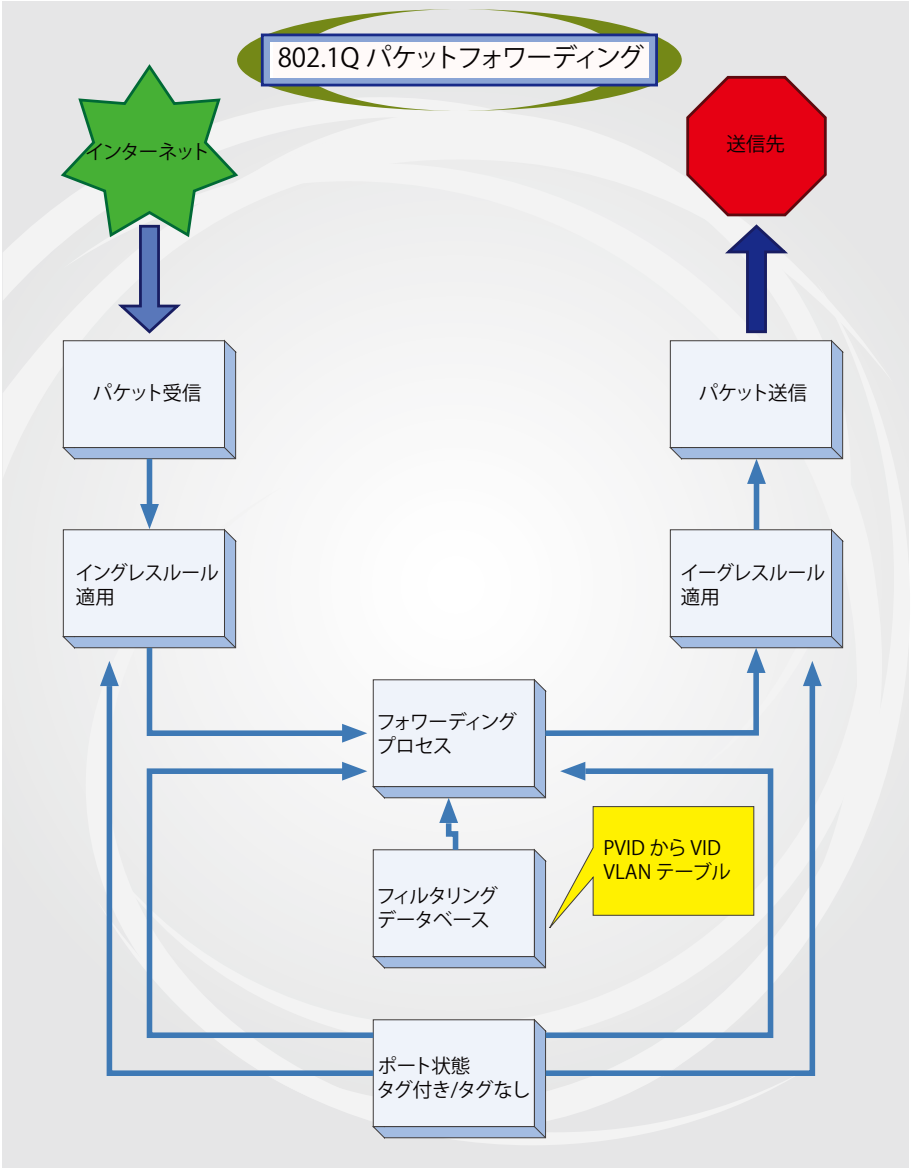


図 8-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表しています。ソース MAC アドレスの後に 4 オクテットのフィールドが挿入されており、EtherType フィールドに設定された 0x8100 という値により、パケットに IEEE 802.1Q/802.1p タグが含まれていることが示されています。タグはその後に続く 2 オクテットに含まれており、ユーザプライオリティの 3 ビット、CFI(Canonical Format Identifier: イーサネットバックボーンを介して転送できるようにトークンリングパケットをカプセル化するために使用される) の 1 ビット、および VID(VLAN ID) の 12 ビットによって構成されています。ユーザプライオリティの 3 ビットは 802.1p によって使用されます。VID は VLAN を識別するためのもので、802.1Q 規格によって使用されます。VID は長さが 12 ビットであるため、4094 個の一意の VLAN を構成することができます。

タグはパケットヘッダに埋め込まれ、パケット全体は 4 オクテット分長くなります。元々のパケットに含まれていた情報はすべて保持されます。

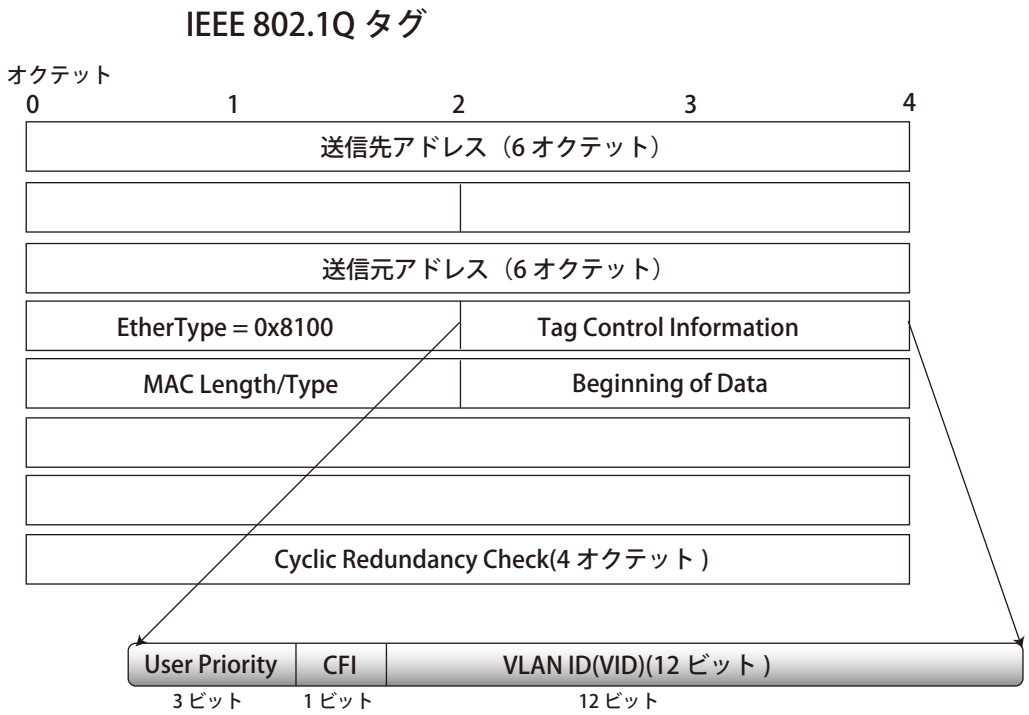


図 8-2　IEEE 802.1Q タグ

EtherType と VLAN ID は、ソース MAC アドレスと元の Length/EtherType または Logical Link Control の間に挿入されます。パケットは元のものよりも少し長くなるため、CRC は再計算されます。

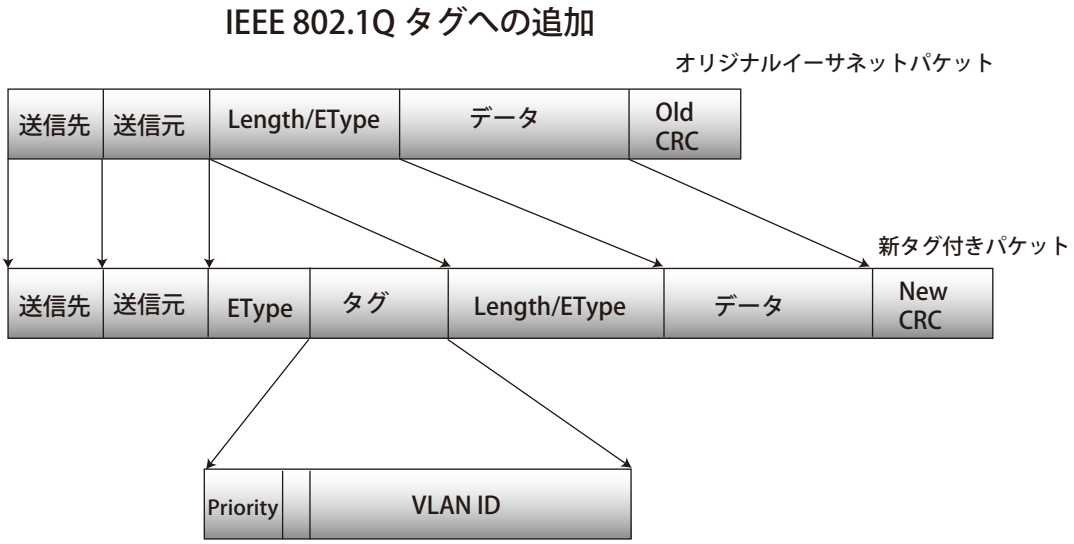


図 8-3　IEEE 802.1Q タグの挿入

ポート VLAN ID

802.1Q VID 情報が含まれるタグ付きパケットは、802.1Q に対応したネットワークデバイスから他のデバイスまで、VLAN 情報を完全に保持したまま転送されます。従って、すべてのネットワークデバイスが 802.1Q に準拠している場合、ネットワーク全体をまるごと 802.1Q VLAN によって結ぶことができます。

しかしながら、すべてのネットワークデバイスが 802.1Q に準拠しているわけではありません。これらの 802.1Q 非準拠のデバイスを tag-unaware（タグ認識不可）、802.1Q 準拠のデバイスを tag-aware（タグ認識可能）と呼ぶことにします。

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これら VLAN のパケット送信は、ポート VLAN ID（PVID）を元に行われます。あるポートでタグなしパケットを受信した場合、パケットにはその受信ポートの PVID が割り当てられ、パケットの宛先アドレスに対応するポート（スイッチのフォワーディングテーブルで検出）へと送信されます。パケットを受信したポートの PVID が送信先ポートの PVID と異なる場合、パケットは破棄されます。

スイッチ内では、PVID が異なるということは VLAN が異なることを意味します（2 つの VLAN は外部ルータを経由しないと通信ができません）。そのため、PVID をベースにした VLAN の識別の場合、スイッチ（またはスイッチスタック）の外部へ VLAN を拡張することができません。

スイッチの各物理ポートには PVID が割り当てられています。802.1Q ポートにも PVID が割り当てられており、スイッチ内で使用されます。スイッチ上で VLAN が定義されていない場合、すべてのポートは PVID 1 のデフォルト VLAN が割り当てられます。タグなしのパケットは、パケットの受信ポートの PVID が割り当てられます。フォワーディングはこの PVID を元に決定されます。タグ付きのパケットにも PVID が割り当てられますが、フォワーディング処理はタグ中に含まれる VID に従います。

tag-aware（タグ認識可能）スイッチは、スイッチ内の PVID とネットワークの VID を対応付けるテーブルを保持している必要があります。スイッチは送信されるパケットの VID と、パケット送信を行うポートの VID を比較します。これらの VID が一致しない場合、パケットは廃棄されます。タグなしパケットには PVID、タグ付きパケットには VID が存在するため、タグを認識するネットワークデバイスも認識しないデバイスも、同じネットワーク内に共存が可能になります。

PVID は 1 ポートあたり 1 つしか持つことはできませんが、VID はスイッチの VLAN テーブルのメモリ上限まで持つことができます。

ネットワーク上にはタグを認識しないデバイスが存在するため、送信するパケットにタグを付けるかどうかの判断を、タグを認識できるデバイスの各ポートで行わなければなりません。送信するポートがタグを認識しないデバイスと接続していれば、タグなしのパケットを送信し、逆にタグを認識するデバイスと接続していれば、タグ付きのパケットを送信します。

タグ付きとタグなし

802.1Q に対応するスイッチのすべてのポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは、送受信するすべてのパケットのヘッダに VID、プライオリティ、その他の VLAN 情報を埋め込みます。パケットが既にタグ付けされている場合、パケットは変更されず VLAN 情報は完全に保たれます。これにより、ネットワーク上の他の 802.1Q 対応デバイスは、タグの VLAN 情報を使用してパケットの転送処理を決定することができます。
タグなしとして設定されているポートは、送受信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがない場合、ポートはパケットを変更しません。従って、タグなしのポートで受信、転送されたすべてのパケットは 802.1Q VLAN 情報を持っていません。PVID はスイッチの内部のみで使用されます。タグの削除は、802.1Q 対応のデバイスから非対応のデバイスにパケットを送信する場合に使用されます。

イングレスフィルタリング

スイッチ上のポートの内、スイッチへのパケットの入り口となり、VLAN を照合するポートをイングレスポートと呼びます。イングレスフィルタリングがポート上で有効に設定されていれば、スイッチはパケットヘッダ内の VLAN 情報を参照し、パケットの送信を行うかどうかを決定します。

パケットに VLAN 情報のタグが付加されている場合、イングレスポートはまず、自分自身がその VLAN のメンバであるかどうかを確認します。メンバでない場合、そのパケットは廃棄されます。イングレスポートが 802.1Q VLAN のメンバであれば、スイッチは送信先ポートが 802.1Q VLAN のメンバであるかどうかを確認します。802.1Q VLAN メンバでない場合は、そのパケットは廃棄されます。送信先ポートが 802.1Q VLAN のメンバであれば、そのパケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

パケットに VLAN 情報のタグが付加されていない場合は、イングレスポートはそのパケットに VID として自分の PVID を付加します。するとスイッチは、送信先ポートはイングレスポートと同じ VLAN のメンバであるか（同じ VID を持っているか）を確認します。同じ VLAN メンバでない場合、パケットは廃棄されます。同じ VLAN メンバである場合、パケットは送信され、送信先ポートはそのパケットを接続するネットワークセグメントに転送します。

本プロセスは、イングレスフィルタリングと呼ばれ、イングレスポートとの VLAN とは異なるパケットを受信時に廃棄することにより、スイッチ内での帯域を有効利用するために使用されます。これにより、送信先ポートに届いてから廃棄されるパケットを事前に処理することができます。

デフォルト VLAN

スイッチには、初期設定で「default」という名前で VID が 1 の VLAN が設定されています。本製品の初期設定ではスイッチ上のすべてのポートが「default」に割り当てられています。新しい VLAN がポートベースモードで設定される時、そのポートは自動的に「default」VLAN から削除されます。

パケットは VLAN 間を通過できません。ある VLAN のメンバが他の VLAN と接続を行うためには、そのリンクは外部ルータを経由する必要があります。

注意 スイッチ上に VLAN が設定されていない場合、各パケットは任意の送信先ポートへと転送されます。宛先アドレスが不明なパケットやブロードキャストパケット、マルチキャストパケットはすべてのポートに送信されます。

VLAN の設定例を以下に示します。

VLAN 名	VID	ポート番号
System (default)	1	5、6、7
Engineering	2	9、10
Sales	5	1、2、3、4

ポートベース VLAN

ポートベース VLAN は、スイッチポート単位で送受信するトラフィックを制限します。そのため、スイッチのポートに 1 台のコンピュータが直接接続されていようと、部門全体が接続されていようと、そのポートに接続されたすべてのデバイスは、そのポートが所属している VLAN のメンバになります。

ポートベース VLAN では、NIC はパケットヘッダ内の 802.1Q タグを識別できる必要はありません。NIC は通常のイーサネットパケットを送受信します。パケットの送信先が同じセグメント上にある場合、通常のイーサネットプロトコルを使用して通信が行われます。パケットの送信先が別のスイッチポートである場合、スイッチによってパケットが破棄されるか転送を行うかは VLAN の照会によって決定されます。

VLAN セグメンテーション

VLAN 2 に所属するポート 1 から送信されるパケットを例に説明します。宛先が別のポートである場合（通常のフォワーディングテーブル検索により判定）、スイッチはそのポート（ポート 10）が VLAN 2 に所属しているか（つまり VLAN 2 パケットを受け取れるか）どうかを確認します。ポート 10 が VLAN 2 のメンバでない場合は、スイッチはそのパケットを廃棄します。メンバである場合、パケットは送信されます。ポート 1 が VLAN2 にのみ送信を行うという点が重要です。このように VLAN の仕組みに基づいて選択的にフォワーディング処理が行われることで、ネットワークの分割を実現します。

VLAN

VLAN 設定ウィザード

ウィザードを使用して VLAN の作成と設定を行います。

L2 機能 > VLAN > VLAN 設定ウィザード の順にメニューをクリックして、以下の画面を表示します。

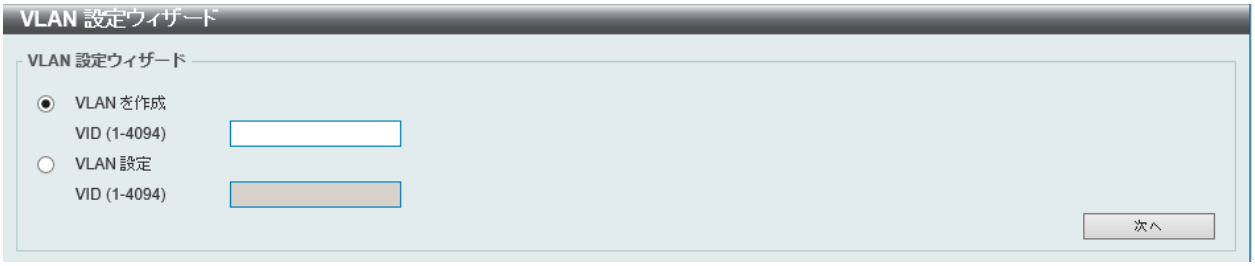


図 8-4　VLAN 設定ウィザード 画面

画面に表示される項目：

項目	内容
VLAN を作成	新しく VLAN を作成する場合に選択します。 • 設定可能範囲：2-4094 VID 1 は初期値 VLAN に設定されているため、本項目では入力できません。
VLAN 設定	作成済みの VLAN を編集する場合に選択します。 • 設定可能範囲：1-4094

「次へ」をクリックし、以下の画面で設定を行います。

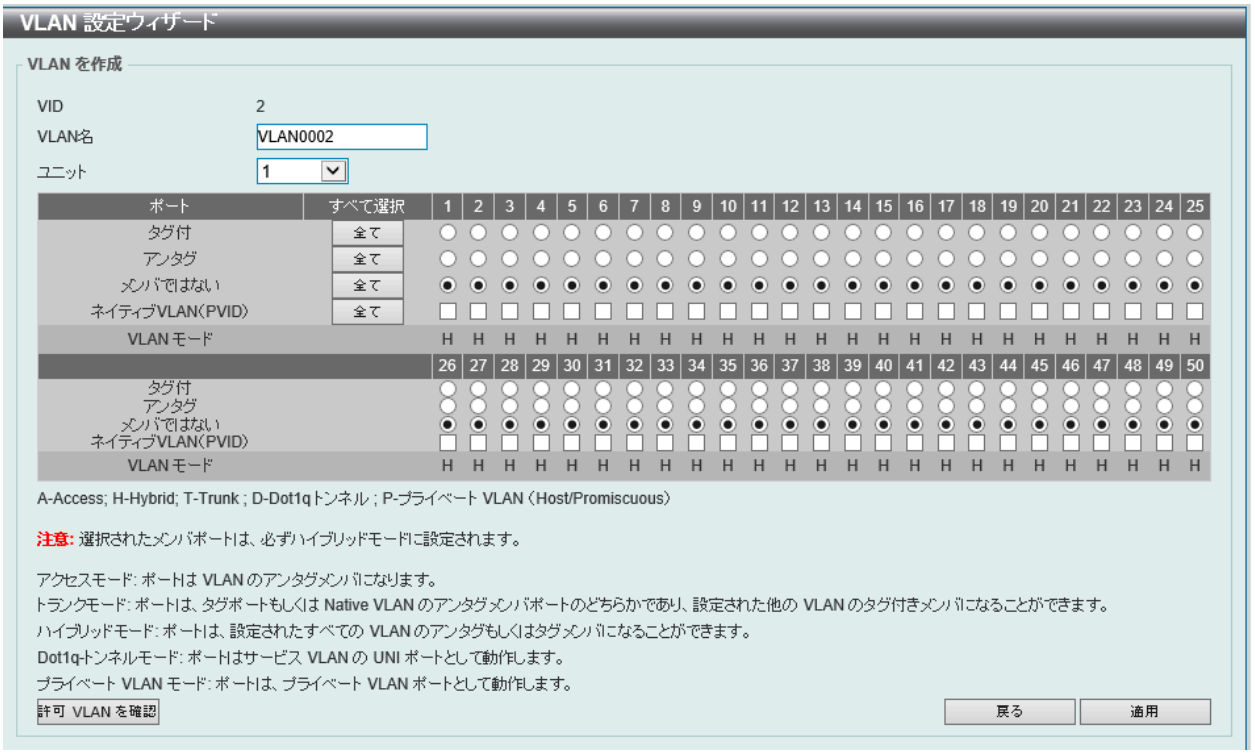


図 8-5　VLAN 設定ウィザード画面

画面に表示される項目：

項目	内容
VID	選択した VID が表示されます。
VLAN 名	VLAN 名を入力します。
ポート	各ポートを以下の通り VLAN のメンバとして定義します。 • 「タグ付」- ポートを 802.1Q タグ付きとして定義します。タグ付きとするポートのボックスをチェックします。 • 「アンタグ」- ポートを 802.1Q タグなしとして定義します。タグなしとするポートのボックスをチェックします。 • 「メンバではない 」- 各ポートが VLAN メンバでないことを定義します。 • 「ネイティブ VLAN（PVID）」- ポートをネイティブ VLAN として定義します。 「全て」をクリックすると、すべてのポートが選択されます。
VLAN モード	各ポートの VLAN モードが表示されます。 アルファベットの表示は以下のモードを表します。 • A：Access モード ポートは VLAN のタグなしメンバになります。 • H：Hybrid モード ポートは設定されているすべての VLAN のタグなしまたはタグ付きメンバにすることができます。 • T：Trunk モード ポートはネイティブ VLAN のタグ付きポートまたはタグなしメンバポートのいずれかであり、設定されている他の VLAN のタグ付きメンバにすることができます。 • D：Dot1q トンネルモード ポートはサービス VLAN の UNI（User Network Interface ）ポートとして動作します。 • P：プライベート VLAN（Host/Promiscuous/Trunk Promiscuous/Trunk セカンダリ）モード ポートはプライベート VLAN ポートとして動作します。
許可 VLAN を確認	許可された VLAN の一覧が別ウィンドウで表示されます。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

802.1Q VLAN

802.1Q VLAN を設定します。

L2 機能 > VLAN > 802.1Q VLAN の順にメニューをクリックして、以下の画面を表示します。



図 8-6　802.1Q VLAN 画面

画面に表示される項目：

項目	内容
802.1Q VLAN	
VID リスト	作成する VLAN ID または VLAN ID の範囲を指定します。
VLAN 検索	
VID	表示する VLAN ID を指定します。
VLAN 名	既存エントリの「編集」をクリックした後、VLAN 名を編集することができます。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

VLAN インタフェース

VLAN インタフェースの設定を行います。

L2 機能 > VLAN > VLAN インタフェース の順にメニューをクリックします。
本画面には、「VLAN インタフェース 設定」タブと「ポートサマリ」タブがあります。

VLAN インタフェース設定タブ

「VLAN インタフェース 設定」タブでは、各ポートの VLAN インタフェース設定の確認、および編集を実行できます。



図 8-7　VLAN インタフェース - VLAN インタフェース設定タブ 画面

エントリの編集
「編集」をクリックして、指定エントリの編集をします。

VLAN 詳細情報の表示
「詳細を表示」をクリックして、指定インタフェースの VLAN について詳細情報について表示します。

■ VLAN 詳細情報の表示

「詳細を表示」をクリックすると、以下の画面で各ポートの VLAN インタフェース設定を確認できます。



図 8-8　VLAN インタフェース情報画面

「戻る」をクリックすると前の画面に戻ります。

■ VLAN インタフェース設定の編集

「編集」をクリックすると、各ポートの VLAN インタフェース設定を編集できます。

画面に表示される項目は、「VLAN モード」で設定した VLAN モードによって異なります。
選択できる VLAN モードは以下です。

「Access」「Hybrid」「Trunk」「Dot 1q トンネル」「Promiscuous」「Host」

● **VLAN モード「Access」を選択した場合：**

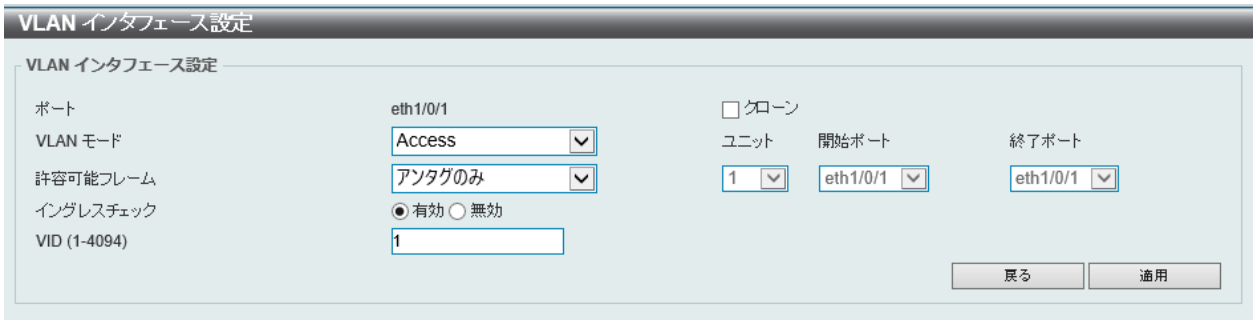


図 8-9　VLAN インタフェース設定 - Access 画面

画面に表示される項目：

項目	内容
ポート	選択したポートが表示されます。
VLAN モード	VLAN モードを「Access」にします。
許容可能フレーム	許可するフレームの種類を選択します。 • 選択肢：「タグのみ」「アンタグのみ」「すべて承認」
イングレスチェック	イングレスチェック機能を有効 / 無効に設定します。
VID	VLAN ID を指定します。 • 設定可能範囲：1 -4094
クローン	クローン機能を有効にして、設定内容を他のポートにコピーします。
ユニット	設定内容をコピーするユニットを指定します。
開始ポート / 終了ポート	設定内容をコピーするポート範囲を指定します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

● **VLAN モード「Hybrid」を選択した場合：**



図 8-10　VLAN インタフェース設定 - Hybrid 画面

画面に表示される項目：

項目	内容
ポート	選択したポートが表示されます。
VLAN モード	VLAN モードを「Hybrid」にします。
許容可能フレーム	許可するフレームの種類を選択します。 • 選択肢：「タグのみ」「アンタグのみ」「すべて承認」
イングレスチェック	イングレスチェック機能を有効 / 無効に設定します。
VLAN 優先	優先 VLAN を以下から選択します。 • 選択肢：「MAC ベース VLAN」「サブネットベース VLAN」
ネイティブ VLAN	ネイティブ VLAN を有効にします。
VID	ネイティブ VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
アクション	実行する動作を選択します。 • 選択肢：「追加」「削除」「タグ付」「アンタグ」
追加モード	追加モードのパラメータとして、タグ付きまたはタグなしを指定します。 • 選択肢：「アンタグ」「タグ付き」
許可された VLAN 範囲	許可される VLAN 範囲を指定します。
クローン	クローン機能を有効にして、設定内容を他のポートにコピーします。
ユニット	設定内容をコピーするユニットを指定します。
開始ポート / 終了ポート	設定内容をコピーするポート範囲を指定します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

● **VLAN モード「Trunk」を選択した場合：**

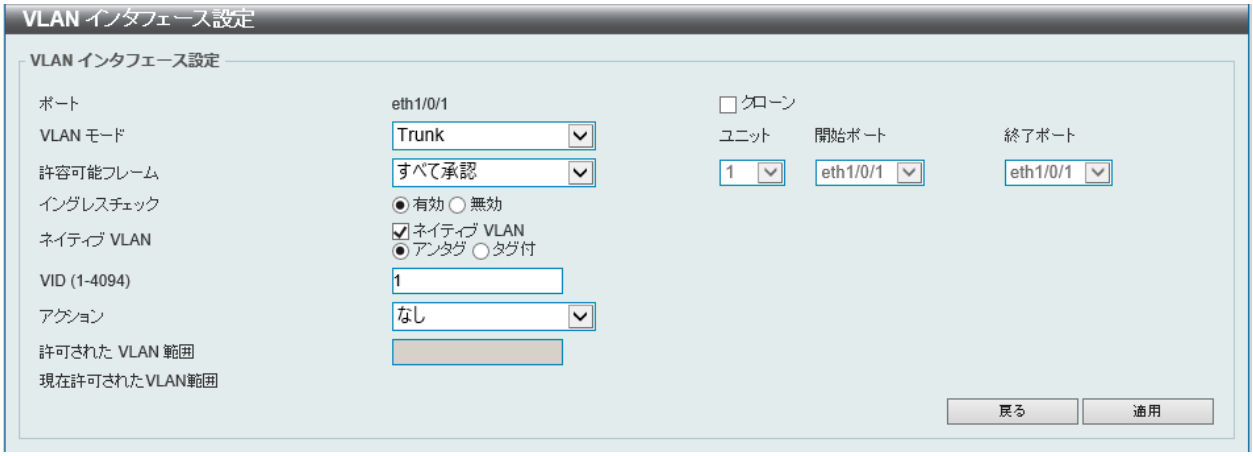


図 8-11　VLAN インタフェース設定 - Trunk 画面

画面に表示される項目：

項目	内容
ポート	選択したポートが表示されます。
VLAN モード	VLAN モードを「Trunk」にします。
許容可能フレーム	許可するフレームの種類を選択します。 • 選択肢：「タグのみ」「アンタグのみ」「すべて承認」
イングレスチェック	イングレスチェック機能を有効 / 無効に指定します。
ネイティブ VLAN	ネイティブ VLAN を有効にします。
VID	ネイティブ VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
アクション	実行する動作を選択します。 • 選択肢：「全て」「追加」「削除」「除く」「リプレース」
許可された VLAN 範囲	許可される VLAN 範囲を指定します。
クローン	クローン機能を有効にして、設定内容を他のポートにコピーします。
ユニット	設定内容をコピーするユニットを指定します。
開始ポート / 終了ポート	設定内容をコピーするポート範囲を指定します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

● **VLAN モード「Dot1q トンネル」を選択した場合：**

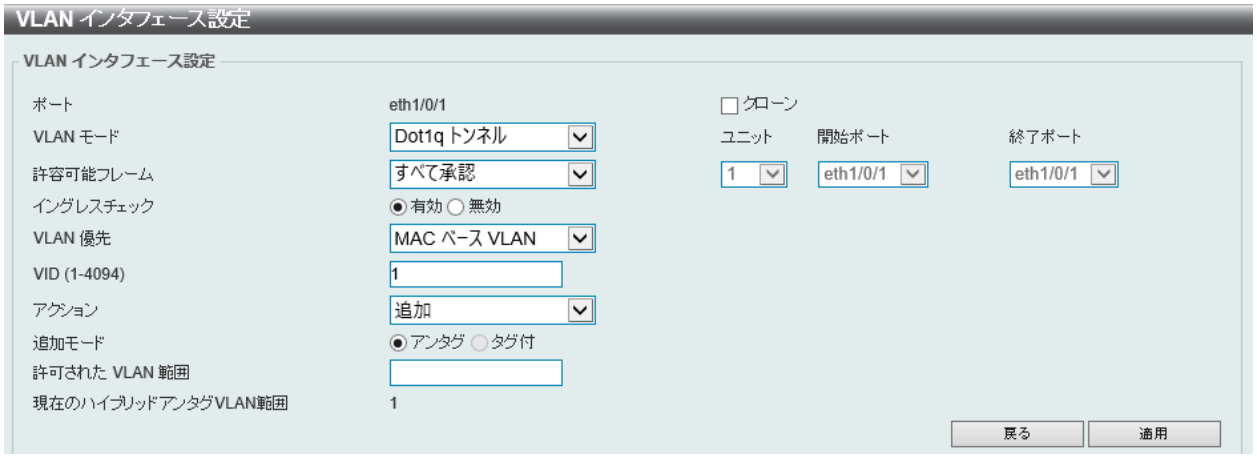


図 8-12　VLAN インタフェース設定 - Dot1q トンネル 画面

画面に表示される項目：

項目	内容
ポート	選択したポートが表示されます。
VLAN モード	VLAN モードを「Dot1q トンネル」にします。
許容可能フレーム	許可するフレームの種類を選択します。 • 選択肢：「タグのみ」「アンタグのみ」「すべて承認」
イングレスチェック	イングレスチェック機能を有効 / 無効に指定します。
VLAN 優先	優先 VLAN を選択します。 • 選択肢：「MAC ベース VLAN」「サブネットベース VLAN」
VID	ネイティブ VLAN を有効にした場合は、設定する VLAN ID を指定します。 • 設定可能範囲：1 -4094
アクション	実行する動作を選択します。 • 選択肢：「追加」「削除」
追加モード	「追加モード」のパラメータに「アンタグ」を追加します。
許可された VLAN 範囲	許可される VLAN 範囲を指定します。
クローン	クローン機能を有効にして、設定内容を他のポートにコピーします。
ユニット	設定内容をコピーするユニットを指定します。
開始ポート / 終了ポート	設定内容をコピーするポート範囲を指定します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

● **VLAN モード「Promiscuous」を選択した場合：**



図 8-13　VLAN インタフェース設定 - Promiscuous 画面

画面に表示される項目：

項目	内容
ポート	選択したポートが表示されます。
VLAN モード	VLAN モードを「Promiscuous」にします。
許容可能フレーム	許可するフレームの種類を選択します。 • 選択肢：「タグのみ」「アンタグのみ」「すべて承認」
イングレスチェック	イングレスチェック機能を有効 / 無効に指定します。
クローン	クローン機能を有効にして、設定内容を他のポートにコピーします。
ユニット	設定内容をコピーするユニットを指定します。
開始ポート / 終了ポート	設定内容をコピーするポート範囲を指定します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

● **VLAN モード「Host」を選択した場合：**

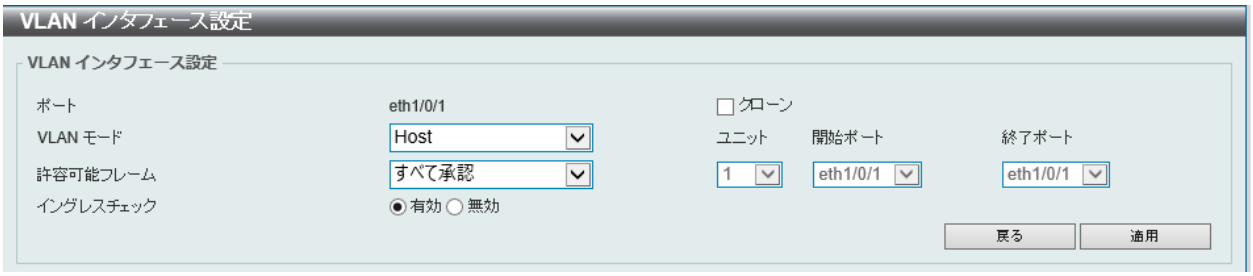


図 8-14　VLAN インタフェース設定 - Host 画面

画面に表示される項目：

項目	内容
ポート	選択したポートが表示されます。
VLAN モード	VLAN モードを「Host」にします。
許容可能フレーム	許可するフレームの種類を選択します。 • 選択肢：「タグのみ」「アンタグのみ」「すべて承認」
イングレスチェック	イングレスチェック機能を有効 / 無効に指定します。
クローン	クローン機能を有効にして、設定内容を他のポートにコピーします。
ユニット	設定内容をコピーするユニットを指定します。
開始ポート / 終了ポート	設定内容をコピーするポート範囲を指定します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックすると前の画面に戻ります。

ポート サマリ タブ

「ポート サマリ」タブでは、各ポートの VLAN インタフェース設定を確認できます。

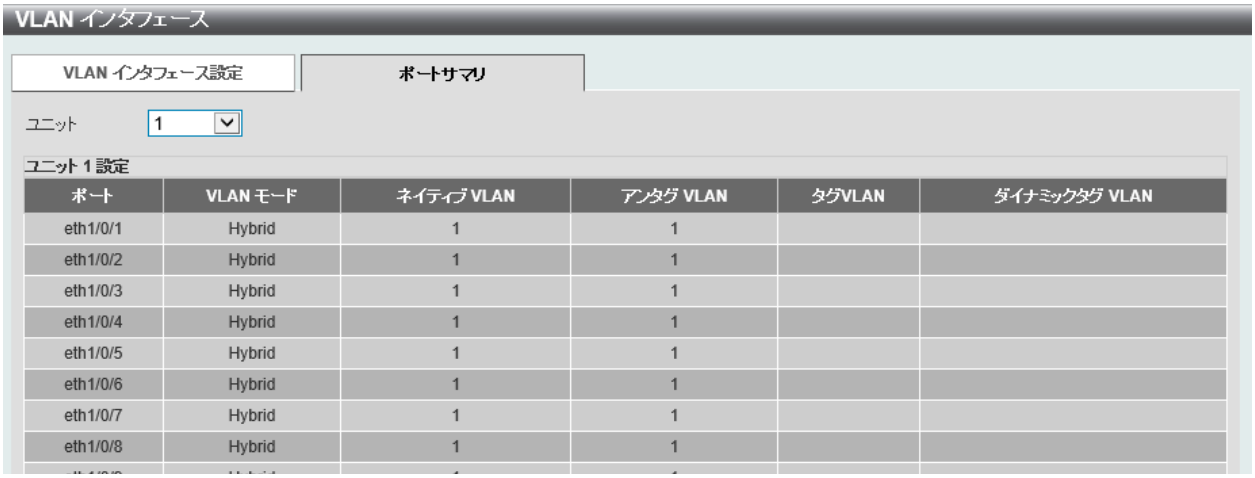


図 8-15　VLAN インタフェース - ポートサマリタブ画面

802.1v プロトコル VLAN

802.1v プロトコル VLAN の設定を行います。

プロトコル VLAN プロファイル

802.1v プロトコル VLAN プロファイルを作成します。
802.1v プロトコル VLAN グループ設定は、各プロトコルに対して複数の VLAN をサポートし、同じ物理ポート上に異なるプロトコルを持つアンタグポートを設定することができます。たとえば、同じ物理ポートで 802.1Q および 802.1v の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 プロファイルの順にメニューをクリックし、以下の画面を表示します。



図 8-16　プロトコル VLAN プロファイル画面

画面に表示される項目：

項目	説明
プロファイル ID	802.1v プロトコル VLAN のプロファイル ID を指定します。 • 設定可能範囲：1-16
フレームタイプ	フレームタイプを選択します。 本機能は、パケットヘッダ内のタイプオクテットを検証し、関連するプロトコルのタイプを検出することにより、パケットをプロトコル定義 VLAN にマッピングします。 • 選択肢：「イーサネット 2」「LLC」「SNAP」
Ether タイプ	グループに対してイーサネットタイプを指定します。 プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は 0x0 から 0xffff です。 オクテット文字列は、フレームタイプに応じて以下のいずれかになります。 • 「イーサネット 2」- 16 ビット (2 オクテット) の 16 進数です。例えば、IPv4 は 0800、IPv6 は 86dd、ARP は 0806 です。 • 「SNAP」- 16 ビット（2 オクテット）の 16 進数です。 • 「LLC」- 2 オクテットの IEEE 802.2 Link Service Access Point（LSAP）ペアです。 最初のオクテットは Destination Service Access Point（ DSAP）用で、2 番目のオクテットは送信元用の値です

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。

プロトコル VLAN プロファイルインタフェース

プロトコル VLAN ポートの設定を行います。
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の順にメニューをクリックし、以下の画面を表示します。

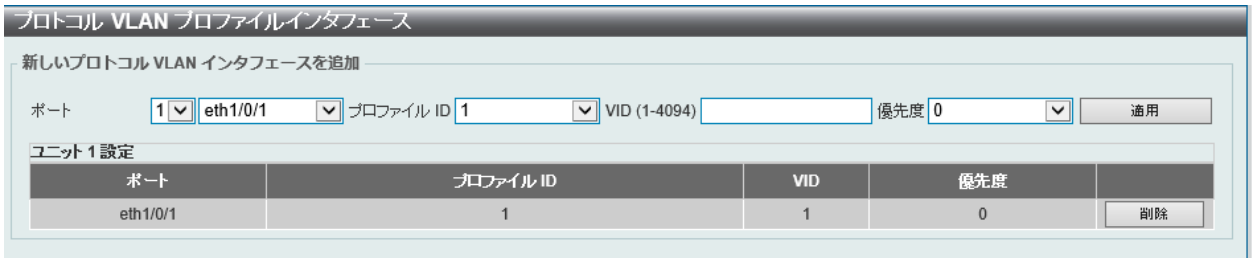


図 8-17　プロトコル VLAN プロファイルインタフェース画面

画面に表示される項目：

項目	説明
ポート	設定するスタッキングユニット ID とポート番号を指定します。
プロファイル ID	定義済みの 802.1v プロトコル VLAN プロファイル ID を選択します。
VID	VLAN ID を入力します。
優先度	優先度（プライオリティ）の値を選択します。 このパラメータは、スイッチに定義済みの 802.1p のデフォルトプライオリティを書き換えるために指定し、パケットが転送される CoS キューを決定するために使用されます。本項目が指定されると、このプライオリティに一致する受信パケットは、指定した CoS キューに転送されます。 • 設定可能範囲：0-7

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。

GVRP

GVRP グローバル

GVRP（GARP VLAN Registration Protocol）の設定を行います。

L2 機能 > VLAN > GVRP > GVRP グローバルの順にクリックし、以下の画面を表示します。

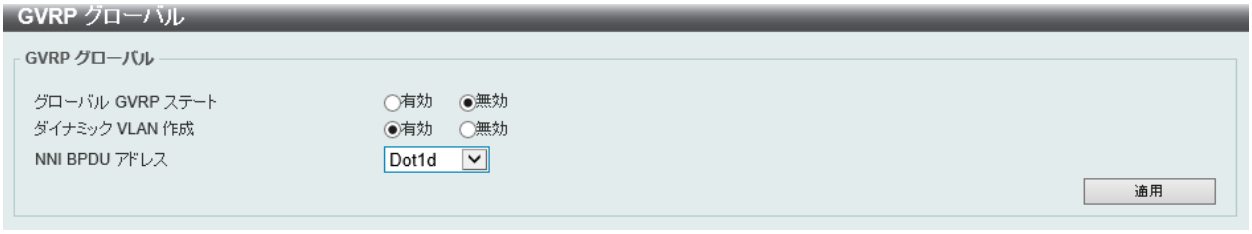


図 8-18　GVRP グローバル画面

画面に表示される項目：

項目	説明
グローバル GVRP ステート	GVRP のグローバルステータスを有効 / 無効に設定します。
ダイナミック VLAN 作成	ダイナミック VLAN クリエーション機能を有効 / 無効に設定します。
NNI BPDU アドレス	NNI BPDU アドレスオプションを選択します。 これにより、カスタマネットワークにおける GVRP の BPDU プロトコルアドレスを決定します。802.1d GVRP アドレスまたは 802.1ad サービスプロバイダ GVRP アドレスを使用することができます。 • 選択肢：「Dot1d」「Dot1ad」

「適用」をクリックして、設定内容を適用します。

GVRP ポート

GVRP ポートパラメータを設定します。

L2 機能 > VLAN > GVRP > GVRP ポート の順にクリックし、以下の画面を表示します。

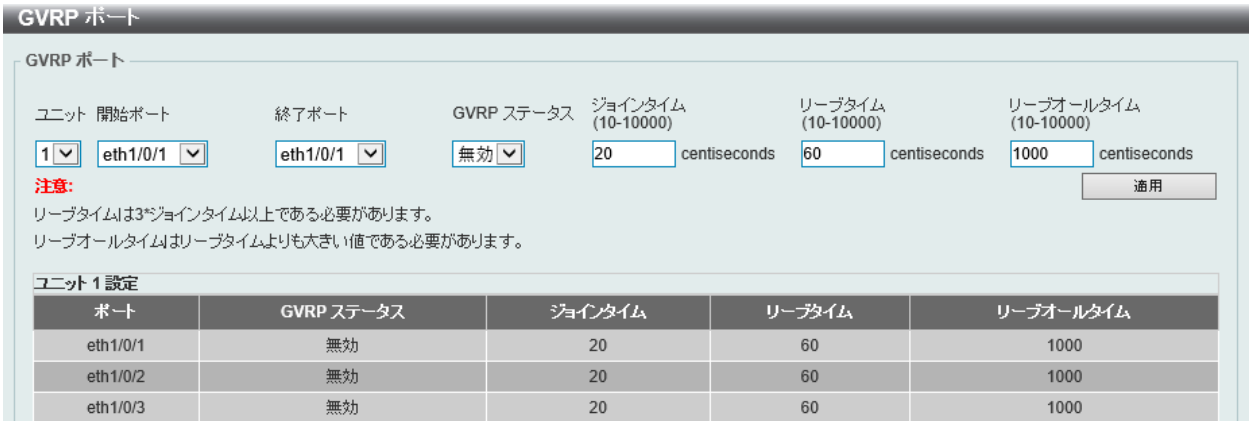


図 8-19　GVRP ポート 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
GVRP ステータス	各ポートの GVRP ステータスを有効 / 無効に設定します。有効にするとポートが自動的に VLAN のメンバになります。 • 初期値：「無効」
ジョインタイム	開始時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 期値：20
リーブタイム	終了時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：60
リーブオールタイム	全終了時間を設定します。 • 設定可能範囲：10-10000（センチ秒） • 初期値：1000

「適用」をクリックし、設定内容を適用します。

GVRP アドバタイズ VLAN

GVRP アドバタイズ VLAN の設定、表示を行います。

L2 機能 > VLAN > GVRP > GVRP アドバタイズ VLAN の順にクリックし、以下の画面を表示します。



図 8-20　GVRP アドバタイズ VLAN 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
アクション	アドバタイズ VLAN に対するアクションを選択します。 「全て」を選択するとすべてのアドバタイズ VLAN が対象となります • 選択肢：「全て」「追加」「削除」「リプレース」
アドバタイズ VID リスト	アドバタイズ VLAN ID を入力します。

「適用」をクリックし、設定内容を適用します。

GVRP 禁止 VLAN 設定

GVRP 禁止 VLAN の設定、表示を行います。

L2 機能 > VLAN > GVRP > GVRP 禁止 VLAN の順にクリックし、以下の画面を表示します。



図 8-21　GVRP 禁止 VLAN 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
アクション	禁止 VLAN に対するアクションを選択します。「全て」を選択するとすべての禁止 VLAN が対象となります。 • 選択肢：「全て」「追加」「削除」「リプレース」
禁止 VID リスト	禁止 VLAN ID を入力します。

「適用」をクリックし、設定内容を適用します。

GVRP 統計テーブル

GVRP の統計情報を表示します。

L2 機能 > VLAN > GVRP > GVRP 統計テーブル の順にクリックし、以下の画面を表示します。

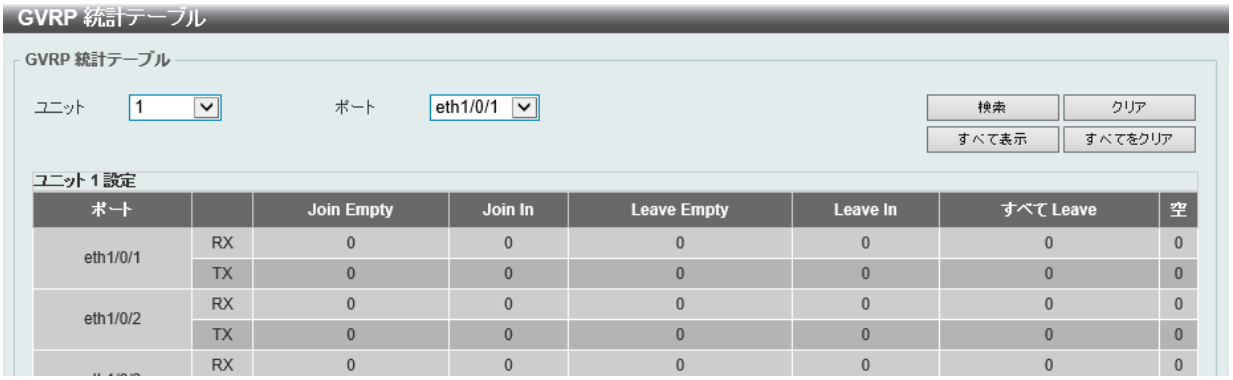


図 8-22　GVRP 統計テーブル画面

画面に表示される項目：

項目	説明
ユニット	統計情報を表示するユニットを指定します。
ポート	統計情報を表示するポートを指定します。

「検索」をクリックして、エントリを検索します。
「すべて表示」をクリックして、すべてのエントリを表示します。

「クリア」をクリックして、表示されたエントリを削除します。
「すべてをクリア」をクリックして、すべての表示エントリを削除します。

Asymmetric VLAN

Asymmetric VLAN（非対称 VLAN）の設定を行います。
非対称 VLAN は、それぞれ異なった VLAN に所属するクライアントから、サーバやファイアウォールなどのリソースを共有させる機能です。

L2 機能 > VLAN > Asymmetric VLAN の順にメニューをクリックし、以下の画面を表示します。

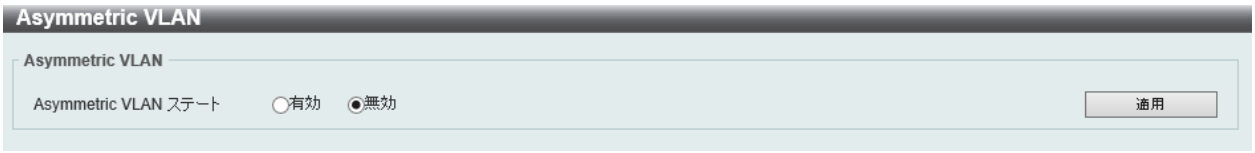


図 8-23　Asymmetric VLAN 画面

画面に表示される項目：

項目	説明
Asymmetric VLAN ステート	Asymmetric VLAN（非対称 VLAN）を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

注意　Asymmetric VLAN は、重複する全 VLAN に学習した MAC Address を乗せる事により異なる Native VLAN 間の Flooding を抑止します。

MAC VLAN

MAC ベース VLAN を設定、表示します。
スタティック MAC ベース VLAN エントリが作成されると、ポートの VLAN は接続するデバイスによって変わります。

L2 機能 > VLAN > MAC VLAN の順にメニューをクリックし、以下の画面を表示します。



図 8-24　MAC VLAN 画面

画面に表示される項目：

項目	説明
MAC アドレス	ユニキャスト MAC アドレスを入力します。
VID	VLAN ID を入力します。
優先度	タグなしパケットに割り当てる優先度を選択します。 • 設定可能範囲：0-7

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

L2VLAN インタフェース説明

L2 VLAN インタフェースの概要について表示、設定を行います。

L2 機能 > VLAN > L2VLAN インタフェース説明をクリックします。次の画面が表示されます。



図 8-25　L2VLAN インタフェース 説明 画面

画面に表示される項目：

項目	説明
L2VLAN インタフェース	L2 VLAN インタフェースの ID を指定します。
説明	L2 VLAN インタフェースの説明を入力します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
「記述を削除」をクリックすると指定の L2 VLAN の概要を削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

サブネット VLAN

サブネット VLAN を設定します。サブネット VLAN エントリは、IP サブネットベースの VLAN 分類ルールです。
タグなしまたはプライオリティタグを持つ IP パケットを受信すると、送信元 IP アドレスがサブネット VLAN エントリに照合されます。送信元 IP がエントリのサブネットに存在する場合、パケットは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 の順にメニューをクリックし、以下の画面を表示します。



図 8-26　サブネット VLAN 画面

画面に表示される項目：

項目	説明
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クス長を入力します。
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クス長を入力します。
VID	サブネット VLAN の VID を入力します。
優先度	優先度を選択します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

スーパー VLAN

スーパー VLAN 設定の表示と設定を行います。
スーパー VLAN は、同じ IP サブネットにある複数のサブ VLAN を集約するために使用されます。サブ VLAN は L2 の独立したブロードキャストドメインです。スーパー VLAN に物理メンバポートを設定することはできません。スーパー VLAN とサブ VLAN を同時に設定することはできません。IP インタフェースがスーパー VLAN に割り当てられると、サブ VLAN 間の通信のためにインタフェースでプロキシ ARP が自動的に有効になります。スーパー VLAN を複数設定することも可能であり、各スーパー VLAN は複数のサブ VLAN で構成されます。

注意　プライベート VLAN とスーパー VLAN は相互排他機能です。プライベート VLAN はスーパー VLAN として設定できません。
L3 ルーティングプロトコル、マルチキャストプロトコル、IPv6 プロトコルは、スーパー VLAN インタフェースで動作できません。

L2 機能 > VLAN > スーパー VLAN の順にメニューをクリックして以下の画面を表示します。



図 8-27　スーパー VLAN 画面

画面に表示される項目：

項目	説明
スーパー VLAN を追加	
スーパー VID リスト	作成するスーパー VLAN の VLAN を入力します。
サブ VLAN を追加	
スーパー VID	サブ VLAN に関連するスーパー VLAN の VLAN ID を入力します。 • 設定可能範囲：1-4094
サブ VID リスト	スーパー VLAN のサブ VLAN を入力します。
Super VLAN を検索	
スーパー VID	表示するスーパー VLAN の VLAN ID を入力します。 • 設定可能範囲：1-4094

「削除」をクリックすると指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「IP 範囲リスト」をクリックするとサブ VLAN に IP 範囲を指定することができます。

■ サブ VLAN の IP 範囲を設定

「IP 範囲リスト」をクリックすると、以下の画面が表示されます。



図 8-28　サブ VLAN - IP 範囲リスト画面

画面に表示される項目：

項目	説明
アクション	サブ VLAN の指定 IP アドレスを「追加」または「削除」します。
開始 IP アドレス	サブ VLAN の IP アドレス範囲の開始 IP アドレスを入力します。
終了 IP アドレス	サブ VLAN の IP アドレス範囲の終了 IP アドレスを入力します。

「適用」をクリックし、設定内容を適用します。
「戻る」をクリックして前のページに戻ります。

自動サーベイランス VLAN

自動サーベイランス VLAN は、IP サーベイランスサービスを強化するための機能です。音声 VLAN と同様、D-Link IP カメラからのビデオトラフィックに対して自動的に VLAN をアサインします。優先度が高いこと、また個別の VLAN を使用することで、サーベイトラフィックの品質とセキュリティを保証します。

自動サーベイランスプロパティ

L2 機能 > VLAN > 自動サーベイランス VLAN > 自動サーベイランスプロパティの順にクリックし、次の画面を表示します。



図 8-29　自動サーベイランスプロパティ 画面

画面に表示される項目：

項目	説明
グローバル設定	
サーベイランス VLAN	サーベイランス VLAN を有効 / 無効に設定します。
サーベイランス VLAN ID	サーベイランス VLAN の VLAN ID を指定します。 VLAN をサーベイランス VLAN に割り当てる前に、通常の VLAN として作成する必要があります。 • 設定可能範囲：2-4094
サーベイランス VLAN CoS	サーベイランス VLAN の優先値を指定します。 サーベイランス VLAN 対応ポートで受信するサーベイランスパケットは、ここで指定された CoS でマークされます。 CoS のリマーキングにより、サーベイランス VLAN トラフィックをデータトラフィックと区別することができます。 • 設定可能範囲：0-7
エージングタイム	エージングタイムを設定します。 本機能は、サーベイランス VLAN ダイナミックメンバポートのエージングタイムを設定するために使用されます。 ポートに接続されている最後のサーベイランスデバイスがトラフィックの送信を停止し、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイランストラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分）
ポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定したポートでサーベイランス VLAN を有効 / 無効に設定します。 サーベイランス VLAN が有効な場合、ポートはアンタグのサーベイランス VLAN メンバとして自動的に学習され、受信したアンタグのサーベイランスパケットはサーベイランス VLAN に転送されます。受信したパケットの送信元 MAC アドレスが OUI（Organizationally Unique Identifier）アドレスに一致している場合、そのパケットはサーベイランスパケットとして認識されます。

「適用」をクリックし、設定内容を適用します。

MAC 設定およびサーベイランスデバイス

サーベイランスデバイスの表示と MAC アドレスの設定を行います。

L2 機能 > VLAN > 自動サーベイランス VLAN > MAC 設定およびサーベイランスデバイス の順にメニューをクリックして以下の画面を表示します。

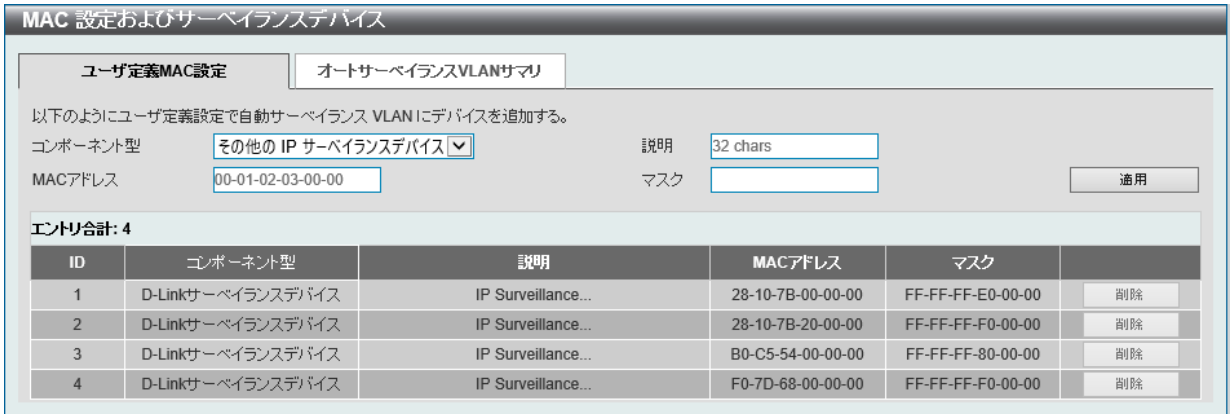


図 8-30　MAC 設定およびサーベイランスデバイス - ユーザ定義 MAC 設定タブ画面

画面に表示される項目：

項目	説明
コンポーネント型	サーベイランス VLAN が自動検出可能なサーベイランスコンポーネントを選択します。 • 選択肢： 「ビデオ管理サーバ」「VMS クライアント / リモートビューワ」「ビデオエンコーダ」「ネットワークストレージ」 「その他の IP サーベイランスデバイス」
説明	ユーザ定義の OUI に関する説明を入力します。（32 文字以内）
MAC アドレス	ユーザ定義の OUI MAC アドレスを入力します。 受信パケットの MAC アドレスが OUI パターンにいずれかと一致すると、そのパケットはサーベイランスパケットとして識別されます。
マスク	ユーザ定義の OUI MAC アドレスマスクを入力します。

「適用」をクリックし、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。

自動サーベイランス VLAN サマリの表示

「オートサーベイランス VLAN サマリ」タブをクリックして、以下の画面を表示します。



図 8-31　MAC 設定およびサーベイランスデバイス - オートサーベイランス VLAN サマリタブ画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。

Voice VLAN

Voice VLAN グローバル

音声 VLAN の設定を行います。音声 VLAN は、VoIP サービスを強化するために、IP 電話からの音声トラフィックに対し VLAN を自動的にアサインする機能です。高い優先度と個別の VLAN を使用することで、VoIP トラフィックの品質とセキュリティを保証します。
本スイッチの音声 VLAN は 1 つのみです。

L2 機能 > VLAN > Voice VLAN > Voice VLAN グローバル の順にメニューをクリックし、以下の画面を表示します。

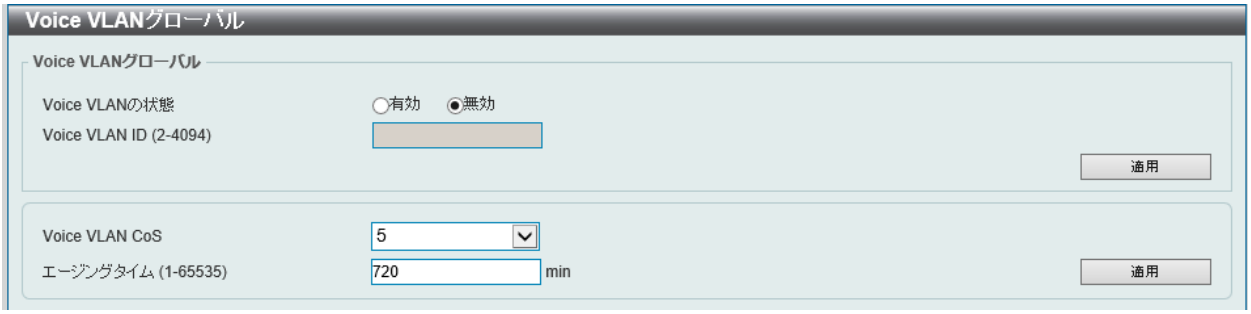


図 8-32　Voice VLAN グローバル画面

画面に表示される項目：

項目	説明
Voice VLAN の状態	音声 VLAN 機能を有効 / 無効に設定します。
Voice VLAN ID	音声 VLAN の VLAN ID を入力します。指定する VLAN は事前に作成しておく必要があります。 • 設定可能範囲：2-4094
Voice VLAN CoS	音声 VLAN の優先度を設定します。 音声 VLAN が有効化されたポートで受信した音声パケットは、この CoS 値でマークされます。これにより、QoS データトラフィックとは区別されます。 • 設定可能範囲：0-7 • 初期値：5
エージングタイム	自動学習された音声デバイスと音声 VLAN 情報のエージングタイム を設定します。 最後の音声デバイスがトラフィックの送信を停止し、音声デバイスの MAC アドレスが FDB テーブルで期限切れになると、音声 VLAN エージングタイマが開始されます。 ポートは音声 VLAN のエージングタイム経過後に音声 VLAN から削除されます。 音声トラフィックがエージングタイム内に再開すると、エージングタイマはキャンセルされます。 • 設定可能範囲：1-65535（分） • 初期値：720（分）

「適用」をクリックし、設定内容を適用します。

Voice VLAN のポート

ポートの音声 VLAN 設定を行います。

L2 機能 > VLAN > Voice VLAN > Voice VLAN のポート の順にメニューをクリックし、以下の画面を表示します。



図 8-33　Voice VLAN のポート画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートの音声 VLAN 機能を有効 / 無効に設定します。 音声 VLAN が有効になると、受信した音声パケットは音声 VLAN として送信されます。受信した音声 VLAN パケットの送信元 MAC アドレスが OUI アドレスに一致すると、音声 VLAN と認識されます。
モード	モードを選択します。 • 「自動アンタグ」- タグなしの音声 VLAN メンバシップが自動的に学習されます。 • 「自動タグ」- タグ付きの音声 VLAN 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。 指定ポートで自動学習が有効化されている場合、音声 VLAN メンバは自動的に学習され、エージアウトします。 「自動タグ」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、ポートは自動的にタグ付きメンバとして音声 VLAN に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは Port VLAN ID（PVID）で転送されます。 「自動アンタグ」モードにおいて、デバイスの OUI により音声デバイスがキャプチャされた場合、タグなしメンバとして音声 VLAN に自動的に参加します。音声デバイスにより送信されたタグ付きパケットの優先度は変更されます。タグなしパケットは音声 VLAN で転送されます。 スイッチが LLDP-MED パケットを受信した場合、VLAN ID、タグ付きフラグ、優先度フラグがチェックされます。スイッチはタグ付きフラグ、優先度フラグに従います。

「適用」をクリックして、変更内容を適用します。

Voice VLAN OUI

ユーザ定義の音声トラフィックの OUI を設定します。
OUI は音声トラフィックを識別するために使用されます。多くの定義済み OUI があり、必要に応じてユーザ定義の OUI を設定できます。
ユーザ定義 OUI は定義済みの OUI と同じとすることはできません。また、定義済み OUI の削除はできません。

L2 機能 > VLAN > Voice VLAN > Voice VLAN OUI の順にメニューをクリックし、以下の画面を表示します。



図 8-34　Voice VLAN OUI 画面

画面に表示される項目：

項目	説明
OUI アドレス	ユーザ定義の OUI MAC アドレスを入力します。
マスク	ユーザ定義の OUI MAC アドレスマスクを入力します。
説明	ユーザ定義の OUI に関する説明を入力します。（32 文字以内）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。

Voice VLAN デバイス

ポートに接続する音声デバイスを表示します。

L2 機能 > VLAN > Voice VLAN > Voice VLAN デバイスの順にメニューをクリックし、以下の画面を表示します。



図 8-35　Voice VLAN デバイス画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。

Voice VLAN LLDP-MED デバイス

スイッチに接続する Voice VLAN LLDP-MED デバイスを表示します。

L2 機能 > VLAN > Voice VLAN > Voice VLAN LLDP-MED デバイスの順にメニューをクリックして以下の画面を表示します。



図 8-36　Voice VLAN LLDP-MED デバイス画面

複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

プライベート VLAN

プライベート VLAN の設定を行います。

L2 機能 > VLAN > プライベート VLAN の順にメニューをクリックし、以下の画面を表示します。

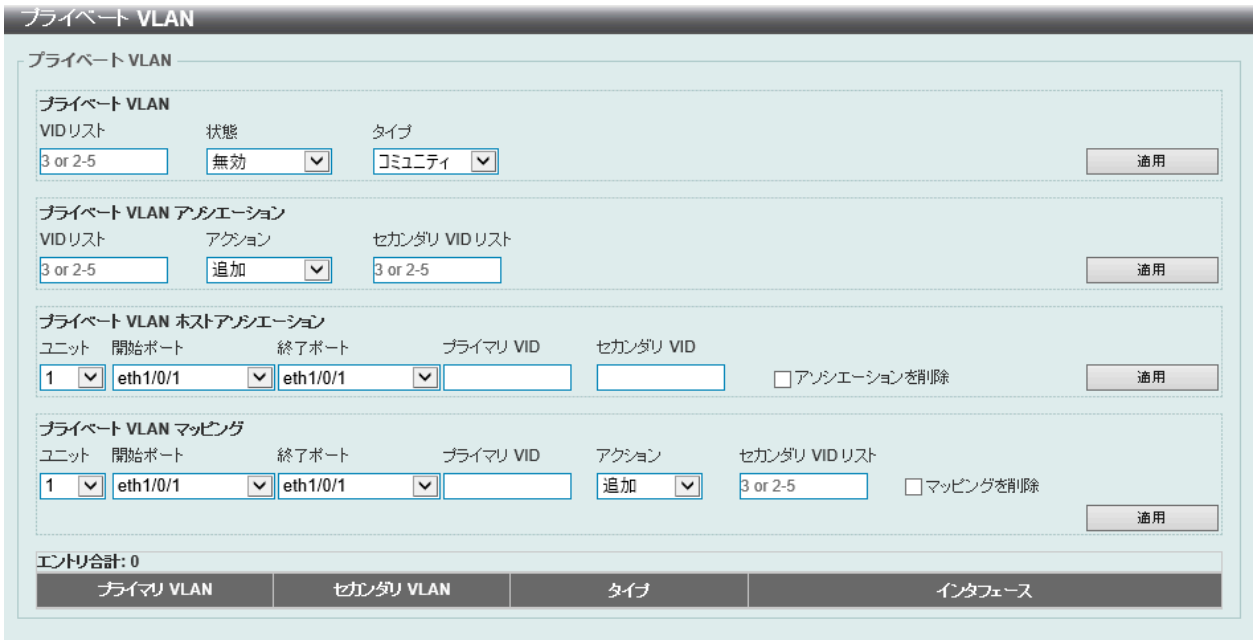


図 8-37　プライベート VLAN 画面

画面に表示される項目：

項目	説明
プライベート VLAN	
VID リスト	プライベート VLAN の VLAN ID を指定します。
状態	プライベート VLAN を有効 / 無効に設定します。
タイプ	プライベート VLAN のタイプを指定します。 • 選択肢：「コミュニティ」「アイソレート」「プライマリ」
プライベート VLAN アソシエーション	
VID リスト	プライベート VLAN の VLAN ID を指定します。
アクション	プライベート VLAN に対して実行するアクションを指定します。 • 選択肢：「追加」「削除」「無効」
セカンダリ VID リスト	セカンダリ VLAN の VLAN ID を入力します。
プライベート VLAN ホストアソシエーション	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
プライマリ VID	プライマリ VLAN の VLAN ID を入力します。
セカンダリ VID	セカンダリ VLAN の VLAN ID を入力します。 「アソシエーションを削除」にチェックを入れると本設定は有効になりません。
プライベート VLAN マッピング	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
プライマリ VID	プライマリ VLAN の VLAN ID を入力します。
アクション	• 「追加」- 入力した情報に基づきエントリを追加します。 • 「削除」- 入力した情報を削除します。
セカンダリ VID	セカンダリ VLAN ID を入力します。 「マッピングを削除」にチェックを入れると本設定は有効になりません。

「適用」をクリックして、設定内容を適用します。

VLAN トンネル

L2 機能 > VLAN Tunnel
VLAN トンネルの設定を行います。

Dot1q トンネル

802.1Q VLAN トンネルの設定、表示を行います。
802.1Q トンネルポートはサービス VLAN において「User Network Interface」（UNI）ポートとして動作します。サービス VLAN のタグ付きメンバであるトランクポートは、サービス VLAN の「Network Node Interface」（NNI）ポートとして動作します。
サービス VLAN タグ付きフレームを送受信するプロバイダーブリッジネットワークに接続されているポートでのみ、802.1Q トンネリングイーサネットタイプを設定します。トンネルイーサネットタイプが設定されると、この値はポートの送信フレームの出力 VLAN タグ「Tag Protocol ID」（TPID）に指定されます。また、指定 TPID は当該ポートの受信フレームのサービス VLAN タグの識別にも使用されます。

L2 機能 > VLAN Tunnel > Dot1q トンネルの順にメニューをクリックし、以下の画面を表示します。



図 8-38　Dot1q トンネル - TPID 設定タブ画面

画面に表示される項目：

項目	説明
内部 TPID	インナー TPID 値を指定します。インナー TPID は、イングレスパケットが「C タグ付き」であるかどうかを判別するために使用されます。このインナー TPID はシステム毎に設定することができます。 • 設定可能範囲：0x1-0xFFFF（16 進数方式）
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
外部 TPID	アウター TPID 値を指定します。 • 設定可能範囲：0x1-0xFFFF（16 進数方式）

「適用」をクリックして、設定内容を適用します。

Dot1q トンネル ポート設定タブをクリックすると以下の画面が表示されます。



図 8-39　Dot1q トンネル - Dot1q トンネル ポート設定タブ 画面

以下の項目を使用して設定します。

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
トラストインナープライオリティ	802.1Q Inner Trust Priority 機能を有効 / 無効に設定します。 802.1Q トンネルポートで Trust Priority オプションが有効な場合、受信パケットの VLAN タグの優先値はサービス VLAN タグにコピーされます。
Miss Drop	Miss Drop 機能を有効 / 無効に設定します。受信ポートで VLAN マッピング Miss Drop オプションが有効な場合、受信パケット VLAN が VLAN マッピングエントリやポートのルールと一致しないと、パケットは破棄されます。
Dot1q タグを挿入	802.1Q トンネルポートで受信したタグなしパケットに挿入される 802.1Q VLAN ID を指定します。 • 設定可能範囲：1-4094
VLAN マッピングプロファイル	VLAN マッピングプロファイル ID を指定します。値の小さい方が優先度が高くなります。 • 設定可能範囲：1-4
アクション	• 「追加」- 入力した情報に基づきエントリを追加します。 • 「削除」- 入力した情報を削除します。

「適用」をクリックして、設定内容を適用します。

VLAN マッピング

本項目では VLAN マッピングの設定、表示を行います。インタフェースにプロファイルが適用されると、スイッチはプロファイルルールに従い受信パケットを照合します。パケットがルールに合致したことを確認すると、ルールに設定されたアクションが実行されます。このアクションには、outer VID の追加や置換、新しい outer タグの優先値設定、またはパケットの新しい inner VID の設定などがあります。
この照合はプロファイル内にあるルールのシーケンス番号に依存しており、最初のエントリが合致すると照合は停止します。シーケンス番号が設定されていない場合、自動的に付与されます。シーケンス番号は、10 から始まり 10 ずつ増加します。1 つのインタフェースに対し、複数の異なるタイプのプロファイルを設定することができます。

L2 機能 > VLAN Tunnel > VLAN マッピングの順にメニューをクリックし、以下の画面を表示します。

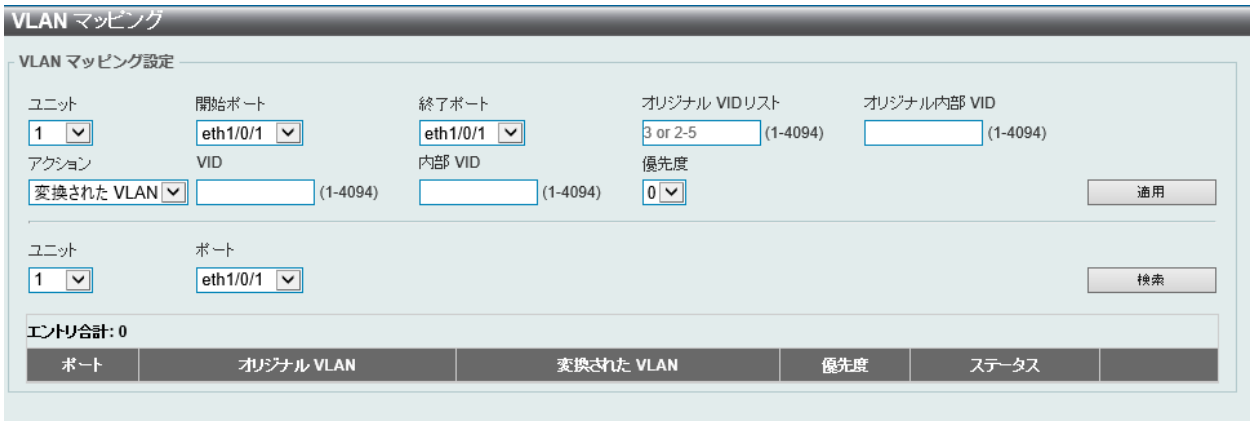


図 8-40　VLAN マッピング 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ポート	検索するポートを指定します。
オリジナル VID リスト	オリジナルの VID リストを指定します。 • 設定可能範囲：1-4094
オリジナル内部 VID	オリジナルのインナー VID を指定します。 • 設定可能範囲：1-4094
アクション	実行する動作を指定します。 • 「変換された VLAN」- VID が一致したパケットの outer VID と交換する VID を指定します。 • 「Dot1q トンネル」- VID が一致したパケットに outer VID を追加します。
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094
内部 VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
優先度	優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7

「適用」をクリックして、設定内容を適用します。

「削除」をクリックすると指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

VLAN マッピングプロファイル

本項目では VLAN マッピングプロファイルの設定、表示を行います。

L2 機能 > VLAN Tunnel > VLAN マッピングプロファイルの順にメニューをクリックし、以下の画面を表示します。



図 8-41　VLAN マッピングプロファイル画面

画面に表示される項目：

項目	説明
プロファイル ID	VLAN マッピングプロファイルの ID を入力します。値の小さい方が優先度が高くなります。 • 設定可能範囲：1-4
タイプ	プロファイルタイプを指定します。 • 「イーサネット」- プロファイルは L2 項目を照合します。 • 「IP」- プロファイルは L3 IP 項目を照合します。 • 「IPv6」- プロファイルは IPv6 宛先 / 送信元アドレス項目を照合します。 • 「イーサネット -IP」- プロファイルは L2/L3 IP 項目を照合します。

「プロファイルを追加」をクリックし、新しい VLAN マッピングプロファイルを追加します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「ルールを追加」をクリックし、新しいルールを追加します。
「削除」をクリックすると指定のエントリを削除します。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

VLAN マッピング ルールを追加（Ethernet）

「VLAN マッピング プロファイル」の「タイプ」で「イーサネット」を選択、「ルールを追加」をクリックし、新しいルールを追加します。

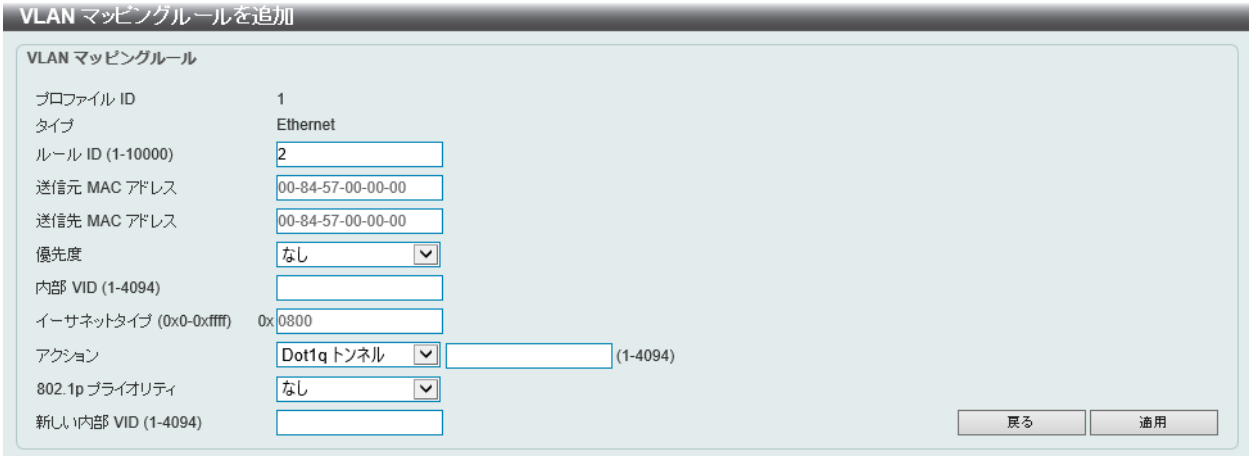


図 8-42　VLAN マッピング ルールを追加（Ethernet）画面

画面に表示される項目：

項目	説明
ルール ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
送信元 MAC アドレス	送信元 MAC アドレスを指定します。
送信先 MAC アドレス	宛先 MAC アドレスを指定します。
優先度	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
内部 VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
イーサネットタイプ	イーサネットタイプを指定します。 • 設定可能範囲：0x0-0xFFFF
アクション	実行する動作を指定します。 • 「変換された VLAN」- 一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q トンネル」- 一致したパケットにアウター VID を追加します。
802.1p プライオリティ	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
新しい内部 VID	「Dot1q トンネル」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

「戻る」をクリックすると前のページに戻ります。
「適用」をクリックして、設定内容を適用します。

VLAN マッピングルールの追加（IP）

「VLAN マッピング プロファイル」の「タイプ」で「IP」を選択、「ルールを追加」をクリックし、新しいルールを追加します。

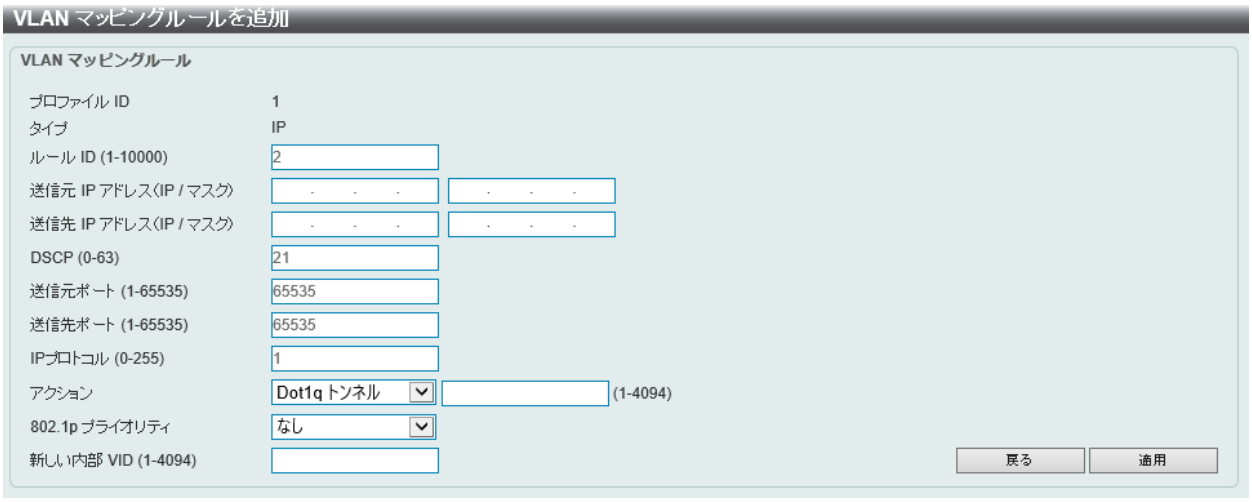


図 8-43　VLAN マッピング ルールを追加（IP）画面

画面に表示される項目：

項目	説明
ルール ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
送信元 IP アドレス（IP/ マスク）	送信元 IP アドレスとサブネットマスクを指定します。
送信先 IP アドレス（IP/ マスク）	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。 • 設定可能範囲：0-63
送信元 / 送信先ポート	送信元 / 宛先 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
IP プロトコル	L3 IP プロトコル値を指定します。 • 設定可能範囲：0-255
アクション	実行する動作を指定します。 •「変換された VLAN」- 一致したパケットのアウター VID と交換する VID を指定します。 •「Dot1q トンネル」- 一致したパケットにアウター VID を追加します。
802.1p プライオリティ	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
新しい内部 VID	「Dot1q トンネル」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

「戻る」をクリックすると前のページに戻ります。
「適用」をクリックして、設定内容を適用します。

VLAN マッピングルールを追加（IPv6）

「VLAN マッピング プロファイル」の「タイプ」で「IPv6」を選択、「ルールを追加」をクリックし、新しいルールを追加します。

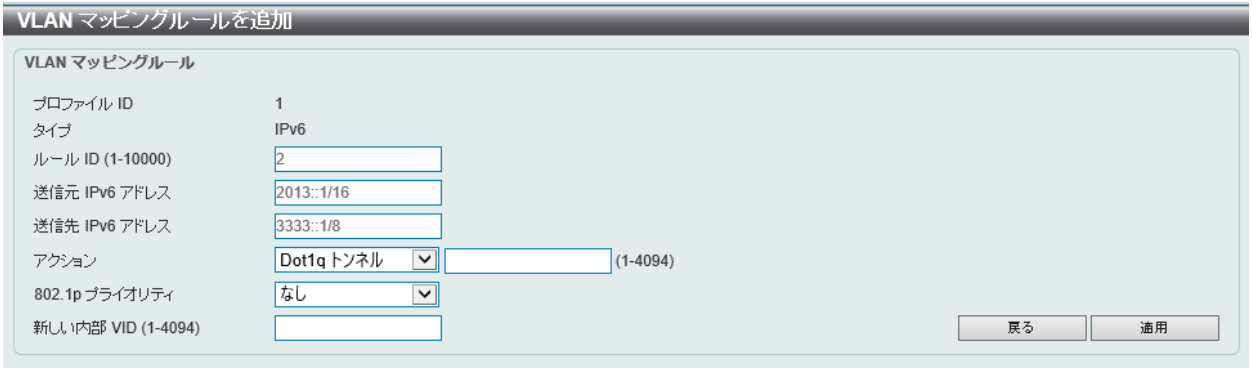


図 8-44　VLAN マッピングルールを追加（IPv6）画面

画面に表示される項目：

項目	説明
ルール ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
送信元 IPv6 アドレス	送信元 IPv6 アドレスとプリフィクス長を指定します。
送信先 IPv6 アドレス	宛先 IPv6 アドレスとプリフィクス長を指定します。
アクション	実行する動作を指定します。 • 「変換された VLAN」- 一致したパケットのアウター VID と交換する VID を指定します。 • 「Dot1q トンネル」- 一致したパケットにアウター VID を追加します。
802.1p プライオリティ	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
新しい内部 VID	「Dot1q トンネル」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

「戻る」をクリックすると前のページに戻ります。
「適用」をクリックして、設定内容を適用します。

VLAN マッピングルールを追加（Ethernet-IP）

「VLAN マッピング プロファイル」の「タイプ」で「イーサネット -IP」を選択、「ルールを追加」をクリックし、新しいルールを追加します。

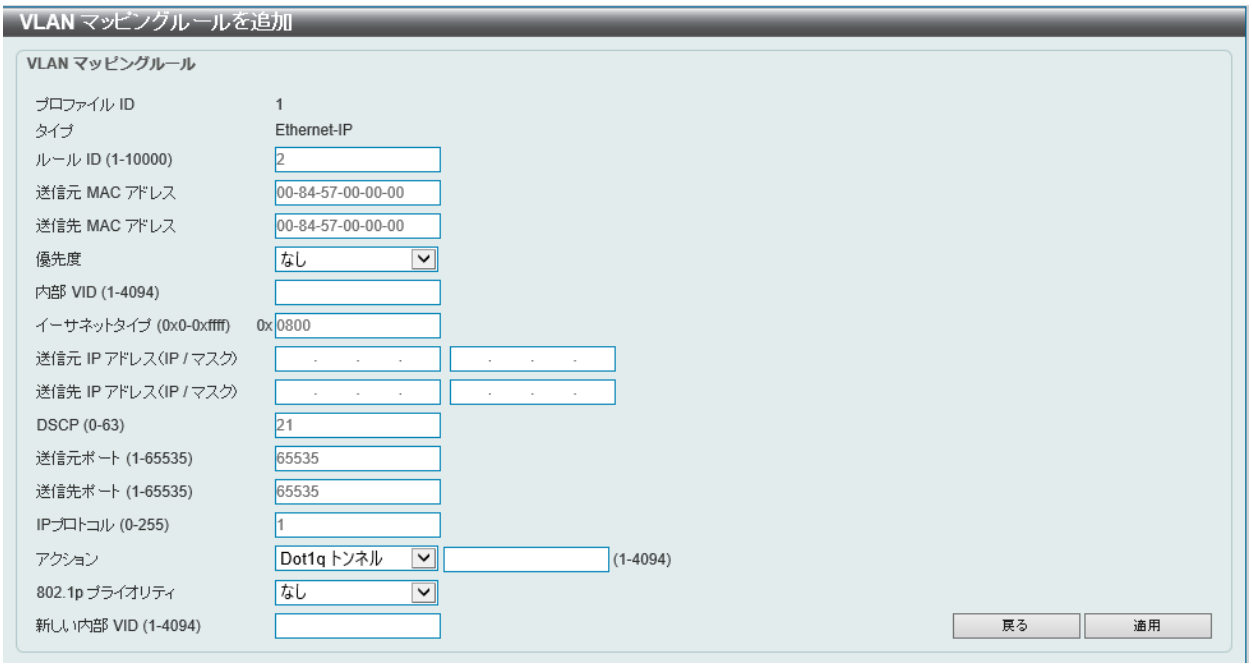


図 8-45　VLAN マッピングルールを追加（Ethernet-IP）画面

画面に表示される項目：

項目	説明
ルール ID	VLAN マッピングルール ID を入力します。 指定されていない場合、ルール ID は 10 から始まり新しいルールごとに 10 ずつ増えていきます。 • 設定可能範囲：1-10000
送信元 MAC アドレス	送信元 MAC アドレスを指定します。
送信先 MAC アドレス	宛先 MAC アドレスを指定します。
優先度	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
内部 VID	インナー VLAN ID を指定します。 • 設定可能範囲：1-4094
イーサネットタイプ	イーサネットタイプを指定します。 • 設定可能範囲：0x0-0xFFFF
送信元 IP アドレス	送信元 IP アドレスとサブネットマスクを指定します。
送信先 IP アドレス	宛先 IP アドレスとサブネットマスクを指定します。
DSCP	DSCP 値を指定します。 • 設定可能範囲：0-63
送信元 / 送信先 ポート	送信元 / 宛先 TCP/UDP ポートを指定します。 • 設定可能範囲：1-65535
IP プロトコル	L3 IP プロトコル値を指定します。 • 設定可能範囲：0-255
アクション	実行する動作を指定します。 •「変換された VLAN」- 一致したパケットのアウター VID と交換する VID を指定します。 •「Dot1q トンネル」- 一致したパケットにアウター VID を追加します。
802.1p プライオリティ	802.1p 優先値を指定します。値の大きい方が優先度が高くなります。 • 設定可能範囲：0-7
新しい内部 VID	「Dot1q トンネル」を選択後、新しいインナー VLAN ID を指定します。 • 設定可能範囲：1-4094

「戻る」をクリックすると前のページに戻ります。
「適用」をクリックして、設定内容を適用します。

STP

L2 機能 > STP

本スイッチは 3 つのバージョンのスパニングツリープロトコル（IEEE 802.1D-1998 STP、IEEE 802.1D-2004 Rapid STP、および IEEE 802.1Q-2005 MSTP）をサポートしています。ネットワーク管理者の間では IEEE 802.1D-1998 STP が最も一般的なプロトコルとして認識されていますが、D-Link のマネジメントスイッチには IEEE 802.1D-2004 RSTP と IEEE 802.1Q-2005 MSTP も導入されています。これらの技術について、以下に概要を紹介します。また、802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても説明します。

802.1Q-2005 MSTP

MSTP（Multiple STP Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク上に複数の経路を提供します。ロードバランシングが可能となるため、 1 つのインスタンスに障害が発生した場合でも、広い範囲に影響を与えないようにすることができます。障害発生時には、障害が発生したインスタンスに代わって新しいトポロジが素早く収束されます。

VLAN が指定されたフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用し、相互接続されたブリッジを介して素早く適切に処理されます。

MSTI ID（MST インスタンス ID）は、これらのインスタンスをクラス分けする ID です。MSTP では、複数のスパニングツリーを CIST（Common and Internal STP）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を判定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、VLAN が割り当てられた各フレームは、定義 VLAN の誤りや対応するスパニングツリーに関係なくシンプルで完全なフレーム処理が保持されたまま、ネットワーク上で管理用に設定されたリージョン内において異なるデータ経路を通ることができます。

ネットワーク上で MSTP を使用しているスイッチは、以下の 3 つの属性を持つ 1 つの MSTP で構成されています。

1. 32 文字までの半角英数字で定義された「設定名」（「MST 設定識別子」画面の「設定名」で設定）。
2. 「設定リビジョン番号」（「MST 設定識別子」画面の「リビジョンレベル」で設定）。
3. 4094 エレメントテーブル（「MST 設定識別子」画面の「VID リスト」で設定）。スイッチがサポートする 4094 件までの VLAN とインスタンスとの関連付けです。

スイッチ上で MSTP 機能を利用するためには、以下の手順を実行してください。

1. スイッチに MSTP 設定を行います。（「STP グローバル設定」画面の「STP 状態」で設定）
2. MSTP インスタンスに適切なスパニングツリープライオリティを設定します。（「MSTP ポート情報」画面の「優先度」で設定）
3. 共有する VLAN を MSTP インスタンス ID に追加します。（「MST 設定識別子」画面の「VID リスト」で設定）

802.1D-2004 Rapid STP

本スイッチは、IEEE 802.1Q-2005 に定義される MSTP（Multiple STP Protocol）、IEEE 802.1D-2004 に定義される RSTP（Rapid STP Protocol）、および 802.1D-1998 で定義される STP（STP Protocol）の 3 つのプロトコルを実装しています。RSTP は IEEE 802.1D-1998 をサポートするレガシー機器との併用が可能ですが、その場合 RSTP を使用する利点は失われます。

RSTP は 802.1D-1998 STP 標準の改良型プロトコルであり、STP を使用する上での制限を克服する目的で開発されました。制限とは、特に今日イーサネットスイッチに取り入れられているレイヤ 3 の諸機能を妨げるものを指しています。RSTP の基本的な機能や用語の多くは STP と同じです。STP 用の設定項目の多くも RSTP で同じように使用されます。本項では、スパニングツリーの新しいコンセプトと、これらのプロトコル間の主な違いについて説明します。

ポートの状態遷移

3 つのプロトコル間の根本的な相違点は、ポートがどのように Forwarding 状態に遷移するかという点と、この状態遷移がトポロジ内でのポートの役割（Forwarding/Not Forwarding）にどのように対応するかという点にあります。802.1D-1998 規格で使用されていた 3 つの状態「無効」「Blocking」「Listening」が、MSTP 及び RSTP では「Discarding」という 1 つの状態に統合されました。いずれの場合も、ポートはパケットの送信を行わない状態です。STP の「無効」「Blocking」「Listening」であっても、RSTP/MSTP の「Discarding」であっても、ネットワークトポロジ内では「非アクティブ状態」であり、機能の差はありません。以下の表では、3 つのプロトコルにおけるポートの状態遷移の違いを示しています。

トポロジの計算については、3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへのパスが 1 つ存在し、すべてのブリッジで BPDU パケットをリッスンします。RSTP/MSTP では、ルートブリッジから BPDU を受信しなくても BPDU パケットが Hello パケット送信毎に送信されます。ブリッジ間の各リンクはリンクの状態を素早く検知することができるため、リンク断絶時の素早い検出とトポロジの調整が可能となります。802.1D-1998 規格では、隣接するブリッジ間においてこのような素早い状態検知が行われません。

ポート状態の比較

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	不可能	不可能
Discarding	Discarding	Blocking	不可能	不可能
Discarding	Discarding	Listening	不可能	不可能
Learning	Learning	Learning	不可能	可能
Forwarding	Forwarding	Forwarding	可能	可能

RSTP では、タイマ設定への依存がなくなり、Forwarding 状態への高速な遷移が可能になりました。RSTP 準拠のブリッジは、他の RSTP に準拠するブリッジリンクのフィードバックを素早く検知します。ポートはトポロジの安定を待たずに Forwarding 状態へ遷移することができます。こうした高速な状態遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge ポートと P2P ポート）が使用されています。

Edge ポート

エッジポートは、ループが発生しないセグメントに直接接続しているポートに対して設定することができます。例えば、1 台のワークステーションに接続しているポートがこれに該当します。エッジポートとして指定されたポートは、Listening 及び Learning の段階を経ずに、直接 Forwarding 状態に遷移します。エッジポートは BPDU パケットを受け取った時点でそのステータスを失い、通常のスパニングツリーポートに変わります。

P2P ポート

P2P ポートにおいても高速な状態遷移が可能です。P2P ポートは他のブリッジとの接続に使用されます。RSTP と MSTP では、手動で設定の変更が行われていない限り、全二重モードで動作しているすべてのポートは P2P ポートと見なされます。

802.1D-1998/802.1D-2004/802.1Q-2005 の互換性

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。ただし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である高速な状態遷移やトポロジ変更の検出を享受することはできません。また、これらのプロトコルでは、セグメント上でレガシー機器の更新により RSTP や MSTP を使用する場合に必要となる変数が用意されており、マイグレーションの際に使用されます。

2 つのレベルで動作するスパニングツリープロトコル

1. スイッチレベルでは、設定はグローバルに実行されます。
2. ポートレベルでは、設定はポートベースのユーザ定義のグループに対して実行されます。

STP グローバル設定

STP をグローバルに設定します。

L2 機能 > STP > STP グローバル設定の順にメニューをクリックし、以下に示す画面を表示します。



図 8-46　STP グローバル設定画面

画面に表示される項目：

項目	説明
STP 状態	
STP 状態	STP のグローバルステータスを有効 / 無効に設定します。
STP トラップ	
STP 新ルートトラップ	新しいルートトラップ送信を有効 / 無効に設定します。
STP トポロジーチェンジトラップ	トポロジ変更トラップ送信を有効 / 無効に設定します。
STP モード	
STP モード	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • 「STP」- スイッチ上で STP がグローバルに使用されます。 • 「RSTP」- スイッチ上で RSTP がグローバルに使用されます。 • 「MSTP」- スイッチ上で MSTP がグローバルに使用されます。
STP 優先度	
優先度	STP 優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0-61440 • 初期値：32768
STP 設定	
ブリッジ最大エージ	ブリッジの最大エージタイマを設定します。 本項目は、古い情報がネットワーク内の冗長パスを無限に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。この値はルートブリッジによりセットされ、ブリッジで相互接続された LAN 内のデバイスと本スイッチの STP 設定値が整合性を持っていることを確認します。 • 設定可能範囲：6-40（秒） • 初期値：20（秒）
ブリッジ Hello 時間	Bridge Hello タイムを入力します。 ルートブリッジは、他のスイッチに自身がルートブリッジであることを示すために BPDU パケットを送信します。本値は、BPDU パケットの送信間隔です。「STP モード」で STP または RSTP が選択された場合にのみ本項目が表示されます。MSTP については、Hello Time はポートごとに設定される必要があります。 • 設定可能範囲：1-2 秒 • 初期値：2（秒）
ブリッジ転送時間	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間、本値で指定した時間 Listening 状態を保ちます。 • 設定可能範囲：4-30（秒） • 初期値：15（秒）

項目	説明
TX ホールド回数	Hello パケットの最大送信回数を指定します。 • 設定可能範囲：1-10 • 初期値：6
最大ホップ	スパニングツリー範囲のデバイス間で、スイッチが送信した BPDU パケットが破棄されるまでのホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。0 に到達すると、BPDU パケットが破棄され、ポートに保持していた情報は解放されます。 • 設定可能範囲：1-40 • 初期値：20
NNI BPDU アドレス	NNI BPDU アドレスを指定します。このパラメータはサービスプロバイダネットワークの STP の BPDU プロトコルアドレスを決定するために使用されます。「802.1d STP アドレス」と「802.1ad サービスプロバイダ STP アドレス」が使用されます。 • 選択肢：「Dot1d」「Dot1ad」

「適用」をクリックし、設定内容を適用します。

STP ポート設定

STP をポートごとに設定します。

L2 機能 > STP > STP ポート設定の順にクリックし、以下の画面を表示します。



図 8-47　STP ポート設定画面

参照　STP グループと VLAN グループを関連付けて定義することをお勧めします。

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
終了ポート	連続するポートグループの最後の番号を設定します。
コスト	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。 • 「0（自動）」- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。（初期値） • 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。 10Mbps のポートコストは 2000000、100Mbps は 200000、1Gbps は 20000、2.5Gbps は 8000、10Gbps は 2000 です。
状態	ポートグループでの STP の有効 / 無効を設定します。初期値：「有効」
ガードルート	ガードルート（Guard Root）を有効 / 無効に設定します。
リンクタイプ	リンクの種類を設定します。全二重ポートは P2P ポートとして判別され、半二重ポートは共有（Shared）ポートとして判別されます。共有（Shared）設定の場合、ポートは即時に Forwarding 状態にはなりません。 • 選択肢：「P2P」「共有」「自動」 • 初期値：「自動」

項目	説明
ポートファスト	ポートファストオプションを指定します。 • 「ネットワーク」- ポートは 3 秒だけ非ポートファスト状態に残ります。BPDU が受信されず、転送状態に移行した場合、ポートファスト状態になります。その後、BPDU を受信すると非ポートファスト状態へ戻ります。（初期値） • 「無効」- ポートは常に非ポートファスト状態です。常に「forward-time delay」の時間待機し、転送状態へ移行します。 • 「エッジ」- ポートは「forward-time delay」の時間を待たずに直接 STP 転送状態に移行します。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。
TCN フィルタ	TCN（Topology Change 通知）フィルタを有効 / 無効に設定します。 本オプションが有効な場合、ポートで受信した TC イベントは無視されます。 • 初期値：「無効」
BPDU 転送	BPDU パケットの転送を有効 / 無効に設定します。有効にすると受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。 • 初期値：「無効」
優先度	優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0-240 • 初期値：128
Hello 時間	ハロータイムの値を指定します。この設定は指定ポートによる各設定メッセージの定期的な送信の間隔となります。 • 設定可能範囲：1-2（秒）
ループガード	指定ポートでのループガードを有効 / 無効に指定します。 本機能は、L2 フォワーディングループ（STP ループ）に対する追加の防御機能です。STP ループは、冗長トポロジ内の STP ブロッキングポートが、誤ってフォワーディングステートへ移行する際に発生します。これは通常、物理冗長トポロジ内のポートの一つ（必ずしも STP ブロッキングポートではない）が、STP BPDU を受信しなくなることにより発生します。このような状況において、BPDU の送受信はポートに割り当てられた役割に依存することになります。つまり、指定ポート（Designated Port）は BPDU を送信し、非指定ポート（Non Designated Port）は BPDU を受信します。 物理冗長ポロジのポートの一つが BPDU を受信しなくなると、STP はトポロジをループ解除状態と認識します。これにより、ブロッキング / バックアップポートであった代替ポートが、指定ポート（Designated Port）となりフォワーディングステートに移行します。この結果ループが発生します。

「適用」をクリックして、設定内容を適用します。

MST 設定識別子

スイッチ上で MST インスタンスの設定を行います。本設定は MSTI（マルチプルスパニングツリーインスタンス）を識別するためのものです。
スイッチは初期状態で 1 つの CIST（Common Internal STP）を持ちます。ユーザはパラメータを変更できますが、MSTI ID の変更や削除は行うことができません。

L2 機能 > STP > MST 設定識別子の順にメニューをクリックし、以下の画面を表示します。



図 8-48　MST 設定識別子画面

画面に表示される項目：

項目	説明
設定名	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
リビジョンレベル	MST リージョンの値を設定します。 「設定名」とともに、スイッチ上の MSTP リージョンを識別するために使用します。 • 設定可能範囲：0-65535 • 初期値：0
プライベート VLAN 同期化	「適用」をクリックし、プライベート VLAN を同期します。
インスタンス ID	スイッチにインスタンス ID を設定します。 • 設定可能範囲：1-64
アクション	MSTI に行う変更を選択します。 •「VID 追加」- VID リスト項目に指定された VID を MSTI ID に追加します。 •「VID を削除」- VID リスト項目に指定された VID を MSTI ID から削除します。
VID リスト	VLAN の VID の範囲を指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。
「編集」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

STP インスタンス設定

STP インスタンスの設定を行います。

L2 機能 > STP > STP インスタンスをクリックし、以下の画面を表示します。



図 8-49　STP インスタンス画面

画面に表示される項目：

項目	説明
編集	「編集」をクリックし、指定エントリの編集を行います。
インスタンスプライオリティ	「編集」をクリック後、指定したインスタンスのためのプライオリティを設定します。 • 設定可能範囲：0-61440

「適用」をクリックして、設定内容を適用します。
「編集」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

MSTP ポート情報

MSTP（Multiple Spanning Tree Protocol）ポート情報を表示、編集します。

各ポートに MSTP の設定を行うには、**L2 機能 > STP > MSTP ポート情報**の順にメニューをクリックし、以下の画面を表示します。



図 8-50　MSTP ポート情報画面

画面に表示される項目：

項目	説明
ユニット	エントリを表示 / 削除するユニットを指定します。
ポート	エントリを表示 / 削除するポートを指定します。
コスト	「編集」をクリックした後、パケットを転送するコストを設定します。 • 設定可能範囲：1-200000000
優先度	「編集」をクリックした後、優先値を指定します。値が小さい方が優先度は高くなります。 • 設定可能範囲：0-240 • 初期値：128

「適用」をクリックし、設定内容を適用します。
「検知したプロトコルをクリア」をクリックし、選択したポートの検出したプロトコル設定をクリアします。
特定ポートの MSTP 設定を参照するには、プルダウンメニューでポート番号を選択し、「検索」をクリックします。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

ERPS（G.8032）

ERPS（Ethernet Ring Protection Switching）はイーサネットリング保護スイッチングの業界標準（ITU-T G.8032）です。これは、イーサネットリングネットワークに対して十分に考慮されたイーサネット操作、管理、およびメンテナンス機能と簡単な APS（Automatic Protection Switching）プロトコルを統合することによって実行されます。ERPS はリングトポロジ内のイーサネットトラフィックに sub-50ms 保護を提供します。これはイーサネットレイヤにループが全く形成されないことを保証します。

リング内の 1 つのリンクが、ループを回避するためにブロックされます（RPL : Ring Protection Link）。障害が発生すると、保護スイッチングは障害のあるリンクをブロックして RPL のブロックを解除します。障害が解決すると、保護スイッチングは再度 RPL をブロックして、障害が解決したリンクのブロックを解除します。

ERPS

本項目では「Ethernet Ring Protection Switching」（ERPS）の表示、設定を行います。STP とループバック検知（LBD）は ERPS の有効化の前にリングポートで無効になる必要があります。ERPS は「R-APS VLAN」リングポート、RPL ポート、RPL オーナが設定されていない状態では、有効にできません。

注意　ERPS バージョンを変更するとプロトコルが再起動します。

L2 機能 > ERPS（G.8032）> ERPS の順にメニューをクリックし、以下の画面を表示します。



図 8-51　ERPS > ERPS ステータスタブ画面

画面に表示される項目：

項目	説明
ERPS バージョン設定	
ERPS バージョン	ERPS バージョンを選択します • 選択肢：「G.8032v1」「G.8032v2」 「G.8032v2」では以下の機能をサポートしています。 • 物理リング内のマルチインスタンス • 「manual」「force」「clear」などの操作コマンド • 物理リングのリング ID を持つ「R-APS PDU 宛先アドレス」の送信 「G.8032v2」を実行している機器に対し「G.8032v1」を設定する前に、「G.8032v1」がサポートしない全ての ERPS 設定を削除する必要があります。そうでない場合バージョンの変更は行えません。ERPS バージョンを変更すると、実行中のプロトコルは再起動します。 「G.8032v2」から「G.8032v1」へ変更する前に、次の設定であることをチェックする必要があります。 • 手動（manual）または強制（force）スイッチコマンドの消去 • 内部接続のメジャーリングインスタンスとサブリングインスタンス機器が違う「R-APS VLAN ID」を保持している • 物理リング内で一つのインスタンスのみをサポート イーサネットリングで「ITU-T G.8032v1」と「ITU-T G.8032v2」のイーサネットリングノードが同時に存在している場合、「G.8032v2」機器に対して次の設定を行う必要があります。 • 全ての物理リング ID は初期値の 1 であること • 内部接続のメジャーリングインスタンスとサブリングインスタンス機器が、それぞれ違う「R-APS VLAN ID」の保持 • 手動（manual）または強制（force）スイッチコマンドの消去 • 物理リング内で一つのインスタンスのみをサポート
イーサネットリング G.8032	
リング名	ERP インスタンス名を入力します。（最大 32 文字）

「適用」をクリックして「ITU-T G.8032 ERP リング」を作成します。
「リングを編集」をクリックして ERP リングを編集します。
「詳細を表示」をクリックして「ITU-T G.8032 ERP リング」の情報について表示します。
「削除」をクリックして指定の「ITU-T G.8032 ERP リング」を削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ リングの編集

「リングを編集」をクリックすると、以下の設定画面が表示されます。



図 8-52　イーサネットリングを編集画面

画面に表示される項目：

項目	説明
インスタンス ID	チェックを入れ「ERP インスタンス」の番号を指定します。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-32
サブリング名	チェックを入れ「サブリング名」を指定します。（32 文字以内） 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。
ポート 0	チェックを入れユニット ID を選択し、初期リングになるユニット ID とポート番号を指定します。 ドロップダウンメニューから「なし」を選択すると、内部接続されたノードがオープンリングのローカルノードエンドポイントとして指定されます。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。
ポート 1	チェックを入れユニット ID を選択し、2 番目のリングになるユニット ID とポート番号を指定します。 ドロップダウンメニューから「なし」を選択すると内部接続されたノードがオープンリングのローカルノードエンドポイントとして指定されます。 「指定にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります
リング ID	チェックを入れリング ID を指定します。 「指定」にチェックを入れパラメータを指定します。「なしにチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-239
リングタイプ	チェックを入れリングタイプを指定します。 • 選択肢：「メジャーリング」「サブリング」

「戻る」をクリックすると設定は破棄され前画面に戻ります。
「適用」をクリックして設定を適用します。

ERPS 概要タブ

「ERPS 概要」タブをクリックすると、以下の画面が表示されます。



図 8-53　ERPS - ERPS 概要タブ画面

「インスタンスを編集」をクリックすると、ERP インスタンスを設定します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ **イーサネットインスタンスを編集**

「インスタンスを編集」をクリックすると、以下の設定画面が表示されます。



図 8-54　イーサネットインスタンスを編集画面

画面に表示される項目：

項目	説明
説明	チェックを入れ「ERP インスタンス」の説明を入力します。（64 文字以内） 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。
R-APS チャネル VLAN	チェックを入れ「ERP インスタンス」の「R-APS チャネル VLAN ID」を指定します。サブインスタンスの「APS チャネル VLAN」はサブリングの仮想チャネルでもあります。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-4094
包括 VLAN リスト	チェックを入れインスタンスに含まれる VLAN リストを指定します。 「-」を使用すると範囲として指定され、「,」を使用すると個別に複数の VLAN を指定します（例：「VLAN1 から 5」は「1-5」、「VLAN1 と 3 と 5」は「1,3,5」）。指定された VLAN は ERP のメカニズムで保護されます。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックを入れ ERP インスタンスの「MEL」を指定します。 同じ ERP インスタンスに所属する全てのリングノードの MEL 値は同じ値である必要があります。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：0-7
プロファイル名	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します。（32 文字以内） 複数の ERP インスタンスが同じ G.8032 プロファイルに含まれることも可能です。同じプロファイルに含まれるインスタンスは同じセットの VLAN や一つのインスタンスに保護される VLAN、他のインスタンスに保護される LAN のサブセットを保護します。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。
RPL ポート	チェックを入れ RPL ポートオプションを選択します。選択されたオプションは RPL ポートとして設定されます。 • 選択肢：「ポート 0」「ポート 1」
RPL 役割	チェックを入れノードの種類を選択します。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。 • 選択肢：「オーナ」「隣接」
アクティベート	チェックを入れ ERP インスタンスをアクティブにするか選択します。「有効」の場合、ERP インスタンスはアクティブになります。 • 選択肢：「有効」「無効」
サブリングインスタンス	チェックを入れ ERP インスタンスの識別子を指定します。物理リングインスタンスのサブリングインスタンスを指定する場合に使用されます。 「指定」にチェックを入れパラメータを指定します。「なし」にチェックを入れるとパラメータの値は初期値になります。 • 設定可能範囲：1-32
強制リングポートブロック	チェックを入れブロックされる ERP インスタンスポートを選択します。リンク不具合などの発生有無にかかわらず、本設定が有効になると即時にインスタンスポートがブロックされます。 • 選択肢：「ポート 0」「ポート 1」
マニュアルリングポートブロック	チェックを入れブロックされる ERP インスタンスポートを選択します。リンク不具合や FS（強制切替）がない場合、MS が設定されたポートがブロックされます。 • 選択肢：「ポート 0」「ポート 1」

「戻る」をクリックすると設定は破棄され前画面に戻ります。

「適用」をクリックして設定を適用します。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。

ERPS プロファイル

ERPS プロファイル設定を行います。

L2 機能 > ERPS (G.8032) > ERPS プロファイルの順にメニューをクリックし、以下の画面を表示します。



図 8-55　ERPS プロファイル画面

画面に表示される項目：

項目	説明
プロファイル名	「G.8032」のプロファイル名を指定します（32 文字以内）。 複数の ERP インスタンスを同じ「G.8032」プロファイルに関連づけることができます。同じプロファイルに含まれる各インスタンスは、同じ VLAN セットを保護します。つまり、この場合 VLAN セットは複数の異なるインスタンスに保護されることになります。

「適用」をクリックして「G.8032」プロファイルと ERP インスタンスを作成します。
「削除」をクリックして指定の「G.8032」プロファイルと ERP インスタンスを削除します。
「編集」をクリックして「G.8032」プロファイルを編集します。

■「G.8032」プロファイルの編集

「編集」をクリックすると、以下の設定画面が表示されます。

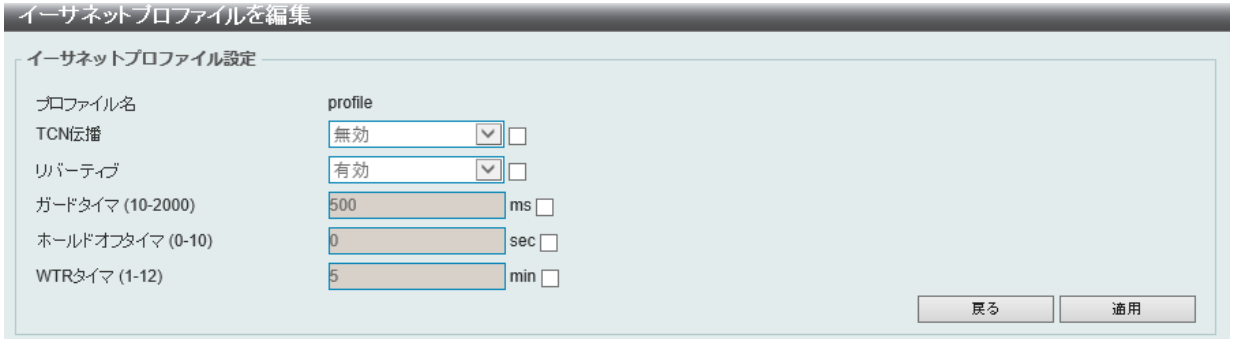


図 8-56　イーサネットプロファイルを編集画面

画面に表示される項目：

項目	説明
TCN 伝播	チェックを入れ「TCN 伝播」（TCN Propagation）の設定を行います。 本機能はサブ ERP インスタンスからメジャーインスタンスへのトポロジ変更の通知の伝播を有効にします。 • 選択肢：「有効」「無効」
リバーティブ	チェックを入れ「リバーティブ」（Revertive）の設定を行います。RPL がブロックされた場合などに、稼働中の送信エンティティに戻すために使用されます。 • 選択肢：「有効」「無効」
ガードタイマ	チェックを入れガードタイマの設定を行います。 • 設定可能範囲：10-2000（ミリ秒） • 初期値：500（ミリ秒）
ホールドオフタイマ	チェックを入れホールドオフタイマの設定を行います。 • 設定可能範囲：0-10（秒） • 初期値：0（秒）
WTR タイマ	チェックを入れ Wait To Restore（WTR）タイマ の設定を行います。 • 設定可能範囲：1-12（分） • 初期値：5（分）

「戻る」をクリックすると設定は破棄され前画面に戻ります。
「適用」をクリックして設定を適用します。

ループバック検知

ループバック検知（LBD）機能は、特定のポートに生成されるループを検出するために使用されます。本機能は、CTP（Configuration Testing Protocol）パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。Loopback Detection Recover Time がタイムアウトになると、ループバック検知ポートは再起動（Normal 状態へ遷移）を行います。ループバック検知機能はポート範囲に実行されます。

L2 機能 > ループバック検知 の順にメニューをクリックし、以下の画面を表示します。



図 8-57　ループバック検知 画面

画面に表示される項目：

項目	説明
ループバック検知グローバル設定	
ループバック検知ステート	ループバック検知機能を有効 / 無効に設定します。 • 初期値：「無効」
モード	ループ検知のモードを選択します。 • 選択肢：「ポートベース」「VLAN ベース」
VLAN ID リストを有効化	「モード」で「VLAN ID」を選択した場合、VLAN ID のリストを入力します。
間隔	ループ検知間隔を設定します。 本設定の間隔で Configuration Test Protocol（CTP）パケットが送信され、ループバックイベントを検知します。 • 設定可能範囲：1-32767（秒） • 初期値：10（秒）
トラップステート	ループバック検出トラップを有効 / 無効に設定します。
動作モード	動作モードを指定します。 • 「シャットダウン」- ループ検出時にポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックします。 • 「なし」- ループ検出時でもポートベースモードのポートをシャットダウン、または VLAN ベースモードの指定 VLAN のトラフィックをブロックしません。
アドレスタイプ	アドレスタイプを指定します。 • 選択肢：「マルチキャスト」「ブロードキャスト」
ループバック検知 ポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	ポートのループバック検知ステータスを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

注意　VLAN ベースを使用する場合、CTP は 100VLAN を検出後、該当の VLAN のみに送出されます。

リンクアグリゲーション

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。
トランクグループは最大 32 個まで作成可能であり、各グループには 1 ～ 8 個までの物理ポートを割り当てることができます。

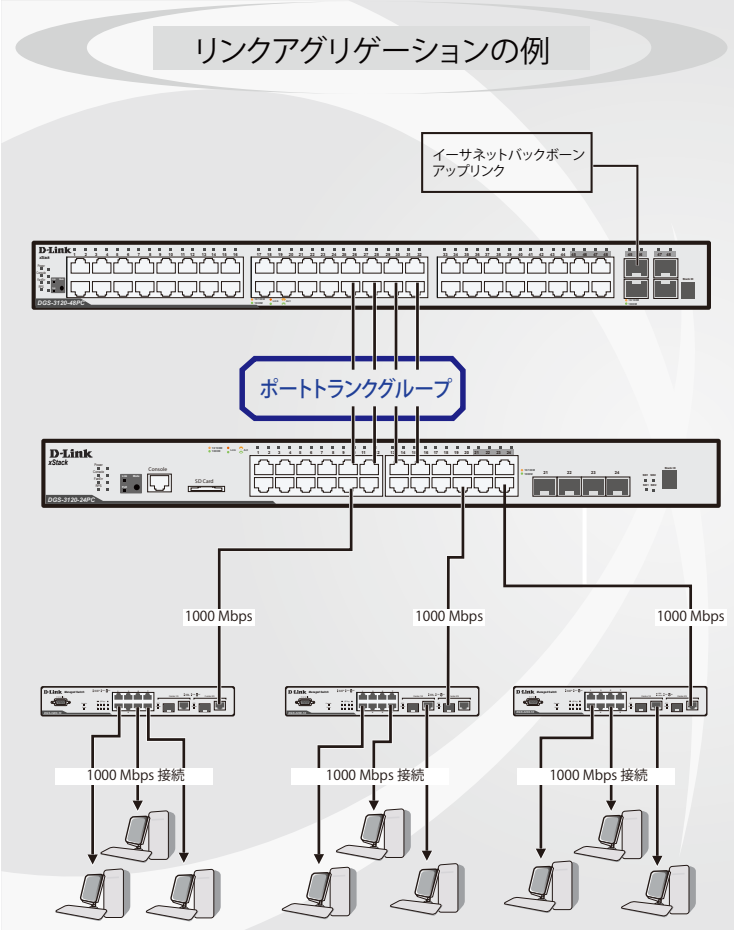


図 8-58　ポートトランクグループの例

トランクグループ内のすべてのポートは 1 つのポートと見なされます。あるホスト（宛先アドレス）へデータ転送が行われる際には、常にトランクグループ内の特定のポートが使用されるため、データは送信された順で宛先ホスト側に到着します。

リンクアグリゲーション機能により複数のポートが 1 つのグループとして束ねられ、1 つのリンクとして動作します。この時、1 つのリンクの帯域は束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバなどの広帯域を必要とするネットワークデバイスをバックボーンネットワークに接続する際に広く利用されています。

本スイッチでは、1 ～ 8 個のリンク（ポート）から構成される最大 32 個のリンクアグリゲーショングループの構築が可能です。各ポートは 1 つのリンクアグリゲーショングループにのみ所属することができます。グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断が発生した場合、ネットワークトラフィックはグループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとして扱います。ポートレベルでは、STP はマスタポートのパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチに冗長化された 2 つのリンクアグリゲーショングループが設定されている場合、STP において片方のグループはブロックされます（冗長リンクを持つポートがブロックされるケースと同様）。

注意　トランクグループ内のいずれかのポートが接続不可になると、そのポートが処理するパケットはリンクアグリゲーション（集約）グループ内の他のポート間でロードシェアされます。

L2 機能 > リンクアグリゲーションの順にクリックし、以下の画面を表示します。



図 8-59　リンクアグリゲーション画面

画面に表示される項目：

項目	説明
システムプライオリティ	システム優先値を指定します。システム優先値はどのポートがポートチャネルに属するか、そしてポートがスタンドアロンモードに入るかを決定します。低い値の方が高い優先値を示します。二つ以上のポートで同じ優先値を与えられた場合、ポート番号で優先値が決まります。 • 設定可能範囲：1-65535 • 初期値：32768
ロードバランスアルゴリズム	ポートトランクグループを構成するポートのロードバランスに使用するアルゴリズムを以下から選択します。 • 選択肢：「送信元 MAC」「送信先 MAC」「送信元 送信先 MAC」「送信元 IP」「送信先 IP」「送信元 送信先 IP」「送信元 L4 ポート」「送信先 L4 ポート」「送信元 送信先 L4 ポート」 • 初期値：「送信元 送信先 MAC」 注意　L4 ポートを含むロードバランスアルゴリズムの設定は、Chipset 制限により、IP も Hash 対象になります。
チャネルグループ情報	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
グループ ID	グループの ID 番号を設定します。 • 設定可能範囲：1-32
モード	動作モードを指定します。チャネルグループは、固定もしくは LACP メンバのどちらかのみで構成されます。チャネルグループが決定すると、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。 • 「スタティック」- チャネルグループタイプは固定です。 • 「有効」- チャネルグループは LACP になります。LACP パケットを送信してネゴシエーションを開始します。 • 「パッシブ」- チャネルグループは LACP になります。LACP パケットへの応答のみ行います。

指定のエントリを削除するためには、削除するグループの「チャネルを削除」をクリックします。
指定のメンバポートを削除するためには、削除するグループの「メンバ ポートを削除」をクリックします。

■ ポートトランキンググループの設定

各項目を入力後、「追加」をクリックし、ポートトランキンググループを設定します。

■ ポートトランキンググループの編集

チャネルについてのより詳細な情報の確認には「詳細を表示」をクリックします。



図 8-60　ポートチャネル画面

画面に表示される項目：

項目	説明
ポートチャネル説明情報	
説明	ポートチャネルの説明を入力します。(64 字以内)
ポートチャネル情報	
LACP タイムアウト	「編集」をクリックし、LACP タイムアウトを設定します。 • 選択肢：「ショート」「ロング」
動作モード	「編集」をクリックし、動作モードを選択します。 • 選択肢：「有効」「パッシブ」
ポートプライオリティ	「編集」をクリックし、ポートプライオリティを設定します。

「記述を削除」でポートチャネルの概要を削除します。

「戻る」をクリックし前の画面に戻ります。

L2 プロトコル トンネル

レイヤ 2 プロトコルトンネルの設定を行います。

L2 機能 > L2 プロトコルトンネルの順にメニューをクリックし、以下の画面を表示します。



図 8-61　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タブ画面

画面に表示される項目：

項目	説明
カプセル化されたパケットの CoS	カプセル化されたパケットの CoS 値を指定します。「初期値」を指定すると初期値を指定します。 • 設定可能範囲：0 - 7
ドロップしきい値	破棄しきい値を指定します。 L2 プロトコルパケットのトンネリングは、パケットのカプセル化、非カプセル化、フォワーディングに CPU 処理容量を消費します。本オプションを使用することにより、システムにより処理される全 L2 プロトコルパケットの数にしきい値を設定し、消費される CPU プロセス帯域を制限します。パケットの最大値がしきい値を超えた場合、超えた分のパケットは破棄されます。「初期値」を指定すると初期値を使用します。 • 設定可能範囲：100 - 20000 • 初期値：0

「適用」をクリックして、設定内容を適用します。

L2 プロトコル トンネル ポート 設定タブをクリックし、次の画面を表示します。



図 8-62　L2 プロトコルトンネル - L2 プロトコルトンネル ポート設定タブ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
アクション	実行する動作を指定します。 • 選択肢：「追加」「削除」
タイプ	ポートタイプを指定します。 • 選択肢：「なし」「シャットダウン」「破棄」
トンネルされるプロトコル	トンネリングされるプロトコルを選択します。 • 選択肢：「STP」「GVRP」「プロトコル MAC」「全て」
プロトコル MAC	トンネルプロトコルにプロトコル MAC を選択した場合、プロトコル MAC オプションを指定します。 選択肢：「01-00-0C-CC-CC-CC」「01-00-0C-CC-CC-CD」
しきい値	「タイプ」で「シャットダウン」「破棄」を指定した場合、しきい値を入力します。 • 設定可能範囲：1-4096

「適用」をクリックして各セクションで行った変更を適用します
「クリア」をクリックすると入力したエントリをクリアします。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。

L2 マルチキャストコントロール

IGMP（Internet Group Management Protocol）スヌーピング 機能を始めとした L2 マルチキャストコントロールの設定を行います。

IGMP スヌーピング

IGMP（Internet Group Management Protocol）Snooping 機能を利用すると、スイッチはネットワークステーションまたはデバイスと IGMP ホスト間で送信される IGMP クエリと IGMP レポートを認識するようになります。また、スイッチを通過する IGMP メッセージの情報に基づいて、指定したデバイスに接続するポートをオープン / クローズできるようになります。

IGMP スヌーピング 設定

IGMP スヌーピング設定をグローバルに有効または無効にします。

IGMP スヌーピング 設定をグローバルに有効または無効にします。
IGMP スヌーピング能を利用するためには、まず本機能をスイッチ全体で有効にする必要があります。
その後、対応する「編集」ボタンをクリックして、各 VLAN に詳細な設定を行います。IGMP スヌーピングを有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートをオープンまたはクローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストが存在しなくなった場合、マルチキャストパケットの送信を停止します。

L2 機能 > L2 マルチキャストコントロール > IGMP スヌーピング > IGMP スヌーピング設定の順にクリックし、以下の画面を表示します。



図 8-63　IGMP スヌーピング設定画面

画面に表示される項目：

項目	説明
グローバル設定	
グローバルステート	IGMP スヌーピングのグローバルステータスを有効 / 無効に設定します。 • 初期値：「無効」
VLAN ステータス設定	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の IGMP スヌーピング を有効 / 無効に設定します。 • 定可能範囲：1-4094
IGMP スヌーピングテーブル	
VID	IGMP スヌーピング テーブルに表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

「検索」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。
「すべて表示」をクリックして IGMP スヌーピングテーブル上のすべてのエントリを表示します。

■ IGMP スヌーピング VLAN の詳細情報表示

関連する VLAN エントリの「詳細を表示」をクリックし、指定 VLAN の詳細情報を表示します。

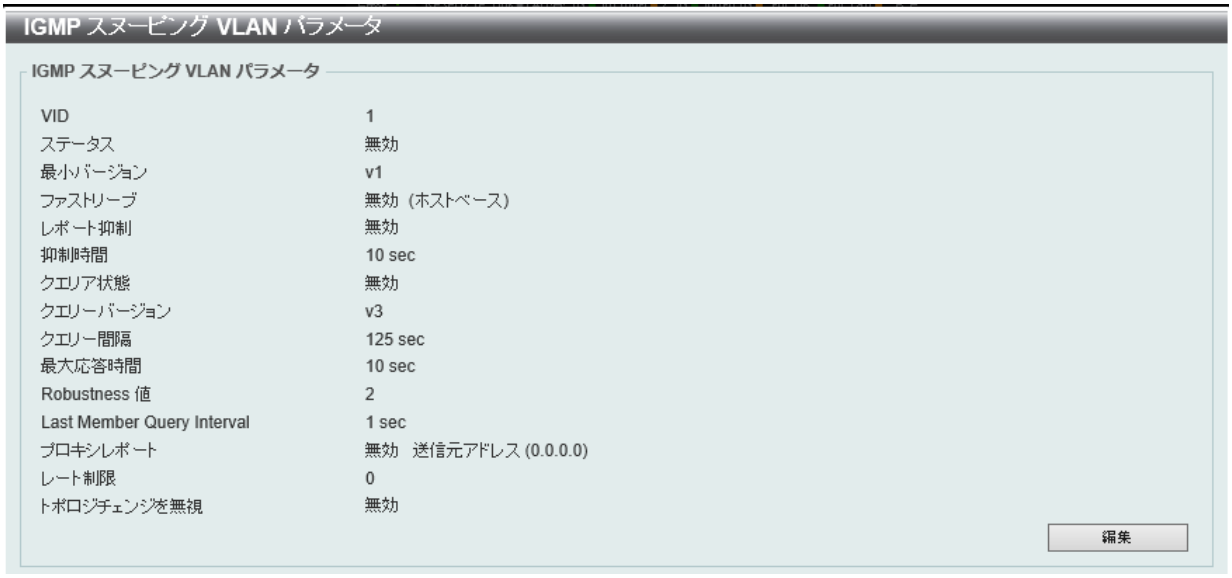


図 8-64　IGMP スヌーピング VLAN パラメータ画面

本画面の「編集」をクリックすると「IGMP スヌーピング VLAN 設定」画面へ移動し、IGMP スヌーピングの VLAN 設定を行うことができます。

■ IGMP スヌーピング機能の詳細設定

「IGMP スヌーピング設定」で関連する VLAN エントリの「編集」をクリックし、以下の画面を表示して各 VLAN に対して詳細な設定を行います。



図 8-65 IGMP スヌーピング VLAN 設定画面

画面に表示される項目：

項目	説明
VID	IGMP スヌーピング設定を変更する VLAN を識別する VLAN ID が表示されます。
ステータス	VLAN の IGMP スヌーピング機能のステータスを表示します。
最小バージョン	VLAN に対して許可される IGMP ホストの最小バージョンを選択します。 • 選択肢：「1」「2」「3」
ファストリーブ	ファストリーブ（Fast Leave）機能を有効 / 無効に設定します。 この機能が有効になると、システムが IGMP done メッセージを受信すると、メンバシップがすぐに削除されます。

項目	説明
レポート抑制	特定の VLAN への IGMP スヌーピングレポートの抑制を有効 / 無効に設定します。 レポートサスペンション機能は「IGMPv1」「IGMPv2」トラフィックでのみ機能します。 有効になるとホストにより送信される重複メッセージを抑制します。同じグループへのレポートもしくはリーブメッセージの抑制は、抑制時間が経過するまで継続されます。同じグループへのレポートもしくはリーブメッセージの場合、1 つのレポートまたはリーブメッセージのみが転送されます。残りのレポートおよびリーブメッセージは抑制されます。
抑制時間	スヌーピングレポートの抑制時間を設定します。 • 設定可能範囲：1-300（秒）
クエリア状態	クエリア機能を有効 / 無効に設定します。
クエリーバージョン	IGMP スヌーピングクエリアで送信されるクエリパケットのバージョンを選択します。 • 選択肢：「1」「2」「3」
クエリー間隔	IGMP スヌーピングクエリアが General クエリを送信する間隔を指定します。 • 設定可能範囲：1-31744（秒）
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る最大応答時間を指定します。 • 設定可能範囲：1-25（秒）
Robustness 値	パケットロスに対するロバストネス変数を指定します。 • 設定可能範囲：1-7
Last Member Query Interval	IGMP スヌーピングクエリアが IGMP Group-Specific クエリまたは Group-Source-Specific (Channel) クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1-25
プロキシレポート	プロキシレポーティング機能を有効 / 無効に設定します。
送信元アドレス	プロキシレポーティングの送信元 IP アドレスを指定します。
レート制限	レートリミットを指定します。「無制限」を指定すると、プロファイルにレート制限が適用されません。 • 設定可能範囲：1-1000
トポロジチェンジを無視	「トポロジチェンジを無視」機能を有効 / 無効に設定します。有効にするとトポロジの変更は無視されます。

「適用」をクリックして、設定内容を適用します。

注意　IGMP スヌーピングについて、ファストリーブ（Fast Leave）は IGMPv2 のみサポートします。

IGMP スヌーピング AAA 設定

IGMP スヌーピング AAA 設定を指定、表示します。

L2 機能 > L2 マルチキャストコントロール > IGMP スヌーピング > IGMP スヌーピング AAA 設定の順にクリックし、以下の画面を表示します。

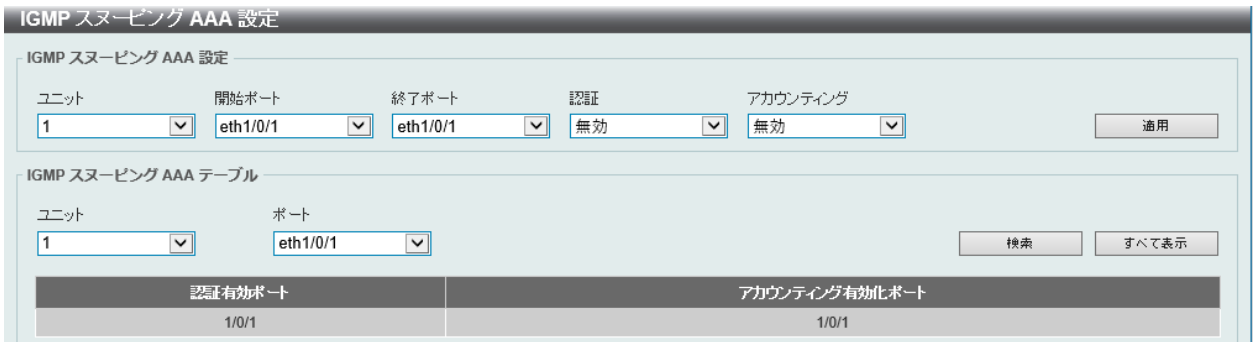


図 8-66　IGMP スヌーピング AAA 設定画面

画面に表示される項目：

項目	説明
IGMP スヌーピング AAA 設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
認証	認証を有効 / 無効に設定します。 本パラメータは、IGMP join メッセージの認証機能を有効または無効にするために使用されます。有効に設定すると、クライアントがグループに参加を希望した場合、システムは最初に認証を実行します。
アカウンティング	アカウンティングを有効 / 無効に設定します。 本パラメータは、リスナーが IGMP グループに参加する際のアカウンティングを有効または無効にするために使用されます。有効に設定すると、クライアントがグループに参加する際に、アカウンティングメッセージが RADIUS に送信されます。
IGMP スヌーピング AAA テーブル	
ユニット	設定するユニットを指定します。

項目	説明
ポート	設定を行うポートを指定します。

「検索」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。
「すべて表示」をクリックして IGMP スヌーピングテーブル上のすべてのエントリを表示します。

IGMP スヌーピンググループ設定

IGMP スヌーピンググループテーブルを表示、設定します。

L2 機能 > L2 マルチキャストコントロール > 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表示します。



図 8-67　IGMP スヌーピンググループ設定画面

画面に表示される項目：

項目	説明
IGMP スヌーピング スタティックグループ設定	
VID	マルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	マルチキャストグループの IP アドレスを入力します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
IGMP スヌーピングスタティックグループテーブル	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	チェックを入れ、検索するマルチキャストグループの IP アドレスを入力します。
IGMP スヌーピンググループテーブル	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	チェックを入れ、検索するマルチキャストグループの IP 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。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、入力した情報に基づいて指定エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。

IGMP スヌーピング フィルタ 設定

IGMP スヌーピングフィルタの設定を行います。

L2 機能 > L2 マルチキャストコントロール > 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表示します。



図 8-68　IGMP スヌーピングフィルタ設定画面

画面に表示される項目：

IGMP スヌーピングレート制限設定

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
制限数	スイッチが特定のインタフェースで処理できる IGMP コントロールパケットのレートを指定します。 「無制限」を指定すると、制限を行いません。 • 設定可能範囲：1-1000（パケット / 秒）

「適用」をクリックして、設定内容を適用します。

IGMP スヌーピング制限設定

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
制限数	生成される IGMP キャッシュエントリ数の上限値を指定します。 • 設定可能範囲：1-512
超えた際のアクション	しきい値を超過した場合の動作について指定します。 制限を超えた場合、新しく学習したグループに対して以下の処理を実行します。 • 「初期値」- デフォルトのアクションを実行します。 • 「破棄」- 新規グループは破棄されます。 • 「リプレース」- 新規グループは古いグループに置き換わります。
ACL 名を除く	標準 IP アクセスリストを指定します。（32 文字以内） アクセスリストに許可されたグループ (*,G) は制限から外れます。グループ (*,G) を許可するにはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「選択してください」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	トランクポートのレイヤ 2VLAN 名を入力します。この VLAN で受信するパケットにフィルタを適用します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。

アクセスグループ設定

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
アクション	• 「追加」- 入力した情報に基づき新しいエントリを追加します。 • 「削除」- 入力した情報に基づき既存エントリを削除します。
ACL 名	標準 IP アクセスリストを指定します（32 文字以内）。グループ (*,G) への参加をユーザに許可する場合に使用します。アクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「選択してください」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	設定する VLAN を指定します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。

IGMP スヌーピングフィルタテーブル

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。
「詳細を表示」指定のエントリの詳細情報を表示します。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「選択してください」をクリックすると次の画面が表示されます。



図 8-69　ACL アクセスリスト画面

ACL を選択し「OK」をクリックします。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「詳細を表示」をクリックすると次の画面が表示されます。

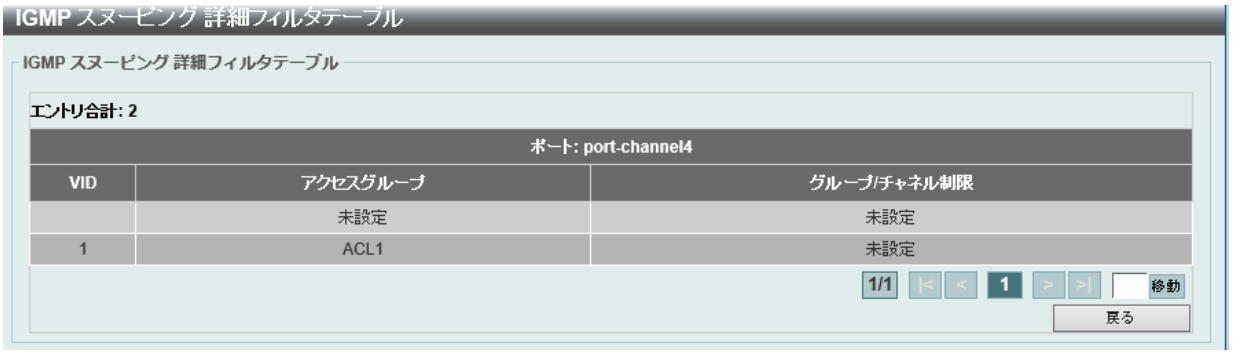


図 8-70　IGMP スヌーピング詳細フィルタテーブル画面

「戻る」をクリックすると前のページに戻ります。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IGMP スヌーピング Mrouter 設定

IGMP スヌーピングマルチキャストルータの設定を行います。

L2 機能 > L2 マルチキャストコントロール > IGMP スヌーピング > IGMP スヌーピング Mrouter 設定をクリックして表示します。



図 8-71　IGMP スヌーピング Mrouter 設定画面

画面に表示される項目：

項目	説明
IGMP スヌーピング Mrouter 設定	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094
設定	ポートの設定を選択します。 •「ポート」- ポートをマルチキャストルータポートに指定します。 •「禁止ポート」- ポートを非マルチキャストポートに指定します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
IGMP スヌーピング Mrouter テーブル	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、入力した情報に基づいて指定エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。

IGMP スヌーピング統計設定

現在の IGMP スヌーピングの統計情報を表示します。

L2 機能 > L2 マルチキャストコントロール > IGMP スヌーピング > IGMP スヌーピング 統計設定の順にメニューをクリックし、以下の画面を表示します。

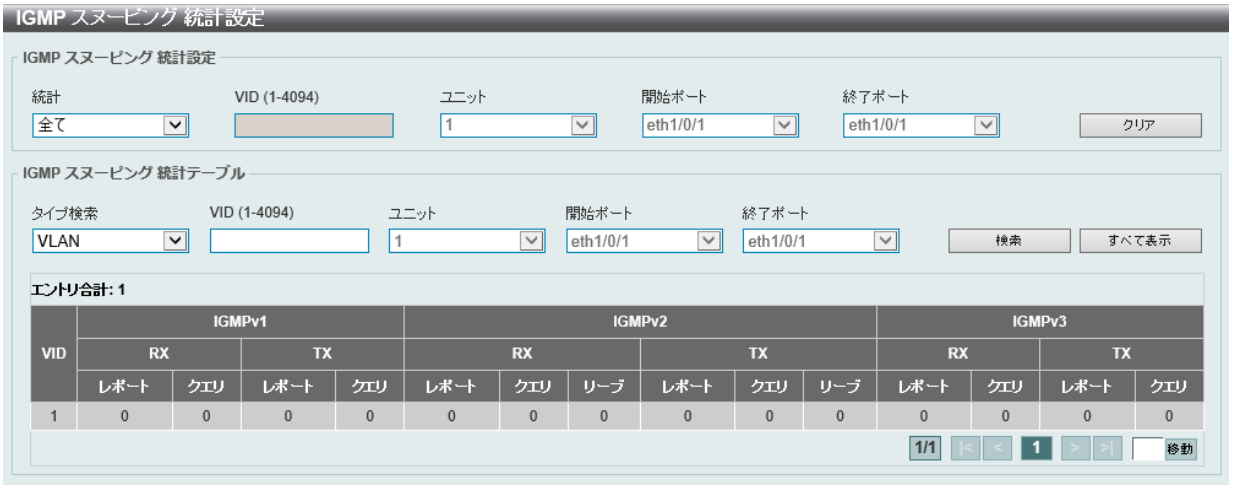


図 8-72　IGMP スヌーピング 統計設定画面

画面に表示される項目：

項目	説明
IGMP スヌーピング統計設定	
統計	インタフェースを選択します。 • 選択肢：「全て」「VLAN」「ポート」
VID	VLAN ID を指定します。「統計」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
ユニット	設定するユニットを指定します。「統計」で「ポート」を選択すると設定可能になります。
開始ポート / 終了ポート	設定するポートの範囲を指定します。「統計」で「ポート」を選択すると設定可能になります。
IGMP スヌーピング 統計テーブル	
タイプ検索	インタフェースを選択します。 • 選択肢：「VLAN」「ポート」
VID	VLAN ID を指定します。「タイプ検索」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
ユニット	設定するユニットを指定します。「タイプ検索」で「ポート」を選択すると設定可能になります。
開始ポート / 終了ポート	設定するポートの範囲を指定します。「タイプ検索」で「ポート」を選択すると設定可能になります。

「クリア」をクリックすると表示された統計情報がクリアされます。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。

MLD スヌーピング

Multicast Listener Discovery（MLD）スヌーピングは、IPv4 の IGMP スヌーピングと同じ機能を持つ、IPv6 用のマルチキャストトラフィック制御機能です。VLAN 上でマルチキャストデータを要求するポートを検出するために使用されます。

MLD スヌーピングでは、所定の VLAN 上のすべてのポートにマルチキャストトラフィックを流すのではなく、要求元ポートとマルチキャストの送信元によって生成される MLD クエリと MLD レポートを使用して、データを受信したいポートに対してのみ、マルチキャストデータを転送します。

MLD スヌーピングは、エンドノードと MLD ルータとの間で交換される MLD 制御パケットのレイヤ 3 部分を調べることでパケットを処理します。スイッチは、ルートがマルチキャストトラフィックをリクエストしていることを検出すると、そのルートに直接接続されているポートを IPv6 マルチキャストテーブルに追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のエントリには、該当ポートや VLAN ID、関連する IPv6 マルチキャストグループアドレスが記録され、このポートはアクティブな Listening ポートと見なされます。アクティブな Listening ポートのみがマルチキャストグループデータを受信します。

MLD コントロールメッセージ

MLD スヌーピングを使用するデバイス間で以下の MLD コントロールメッセージが交換されます。これらのメッセージは、130、131、132 および 143 でラベル付けされた 4 つの ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query – IPv4 の IGMPv2 Host Membership Query（HMQ）に相当するメッセージです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query はリンク上のすべての Listening ポートに対し送信され、Multicast Specific Query は、特定のマルチキャストアドレスに対して送信されます。この 2 種類のメッセージは、IPv6 ヘッダ内のマルチキャスト宛先アドレス及び Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別されます。
2. Multicast Listener Report – IGMPv2 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。
3. Multicast Listener Done – IGMPv2 の Leave Group Message に相当するメッセージです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからのマルチキャストデータの受信を停止すること、つまり、このアドレスからのマルチキャストデータが "done"（完了）となった旨を伝えます。スイッチが本メッセージを受信すると、この Listening ホストには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しなくなります。
4. Multicast Listener Report Version2 – IGMPv3 の Host Membership Report（HMR）に相当するメッセージです。Listening ポートは、Multicast Listener クエリメッセージへの応答として、ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージを送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

MLD スヌーピング設定

MLD スヌーピング設定を有効または無効にします。

L2 機能 > L2 マルチキャストコントロール > MLD スヌーピング > MLD スヌーピング設定の順にクリックし、以下の画面を表示します。



図 8-73　MLD スヌーピング設定画面

画面に表示される項目：

項目	説明
グローバル設定	
グローバルステート	MLD スヌーピングのグローバルステータスを有効 / 無効に設定します。有効 - デバイスで MLD スヌーピングを有効にします。 • 初期値：「無効」
VLAN ステータス 設定	
VID	VLAN を識別する VLAN ID を入力し、指定 VLAN 上の MLD スヌーピング を有効 / 無効に設定します。 • 設定可能範囲：1-4094
MLD スヌーピングテーブル	
VID	MLD スヌーピングテーブル に表示する VLAN の VLAN ID を指定します。 • 検設定可能範囲：1-4094

「検索」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。
「すべて表示」をクリックして MLD スヌーピングテーブル 上のすべてのエントリを表示します。

MLD スヌーピング VLAN の詳細情報表示

関連する VLAN エントリの「詳細を表示」をクリックし、指定 VLAN の詳細情報を表示します。

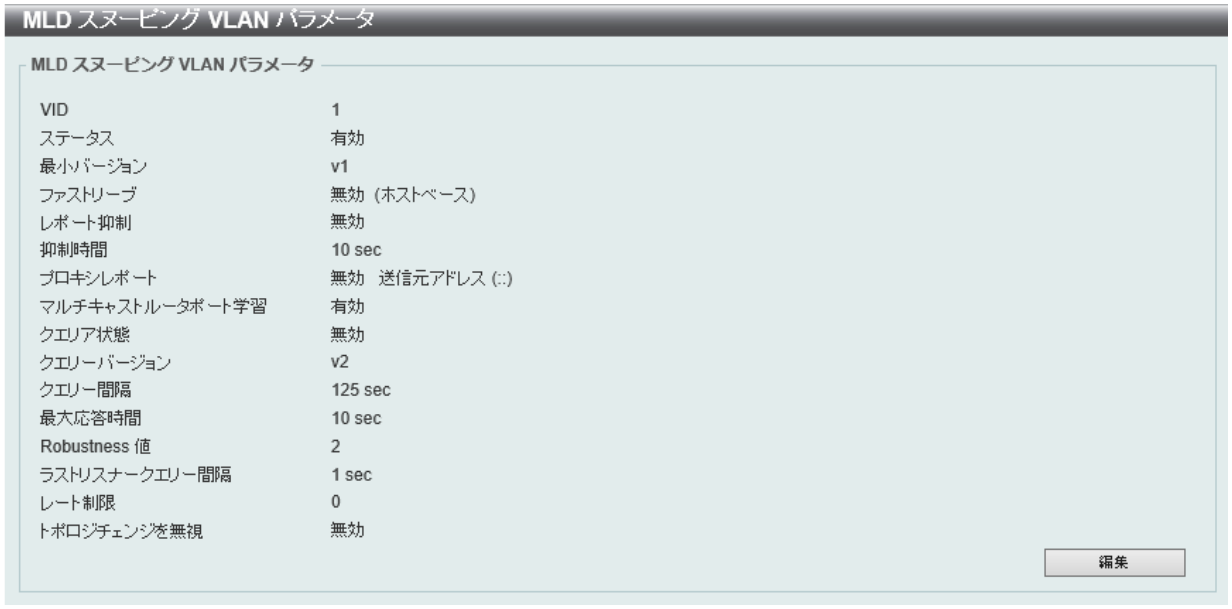


図 8-74　MLD スヌーピング VLAN パラメータ画面

本画面の「編集」をクリックすると「MLD スヌーピング VLAN 設定」画面へ移動し、MLD スヌーピングの VLAN 設定を行うことができます。

MLD スヌーピング機能の詳細設定

「MLD スヌーピング設定」で関連する VLAN エントリの「編集」をクリックし、以下の画面を表示して各 VLAN に対して詳細な設定を行います。



図 8-75 MLD スヌーピング VLAN 設定画面

画面に表示される項目：

項目	説明
VID	MLD スヌーピング設定を変更する VLAN を識別する VLAN ID を表示します。
ステータス	VLAN の MLD スヌーピング機能の有効 / 無効を表示します。
最小バージョン	VLAN に許可された MLD ホストの最小バージョンを選択します。 • 選択肢：「1」「2」
ファストリーブ	ファストリーブ（Fast Leave）機能を有効 / 無効に設定します。 本機能が有効の場合、スイッチが MLD Leave メッセージを受信すると、マルチキャストグループのメンバは直ちにグループから脱退します。
レポート抑制	特定の VLAN への MLD スヌーピングレポートの抑制を有効 / 無効に設定します。 レポートサスペンション機能は「MLDv1」「MLDv2」トラフィックでのみ機能します。 有効になるとホストによるレポートの送信は抑制されます。抑制は抑制時間を過ぎるまで続きます。
抑制時間	スヌーピングレポートの抑制時間を設定します。 • 設定可能範囲：1-300（秒）
プロキシレポート	プロキシレポーティング機能を有効 / 無効に設定します。
送信元アドレス	プロキシレポーティングの送信元 IP アドレスを指定します。
マルチキャストルータポート学習	マルチキャストルータポート学習機能を有効 / 無効に設定します。
クエリア状態	MLD クエリア機能を有効 / 無効に設定します。有効にした場合、MLD クエリパケットの送信が可能になります。
クエリーバージョン	MLD スヌーピングクエリアによって送信される General クエリパケットのバージョンを選択します。 • 選択肢：「1」「2」
クエリー間隔	MLD スヌーピングクエリアが MLD General クエリメッセージを送信する間隔を入力します。 • 設定可能範囲：1-31744（秒）
最大応答時間	MLD スヌーピングクエリでアドバタイズされる最大応答時間を指定します。 • 設定可能範囲：1-25（秒）
Robustness 値	MLD スヌーピングで使用されるロバストネス変数の値を指定します。 ロバストネス変数は、ネットワーク上で予想されるパケットロスに対する耐性を調整します。 • 設定可能範囲：1-7
ラストリスナークエリー間隔	MLD スヌーピングクエリアが MLD Group-Specific クエリまたは Group-Source-Specific (Channel) クエリメッセージを送信する間隔を設定します。 • 設定可能範囲：1-25（秒）
レート制限	レートリミットを指定します。「無制限」を指定すると本プロファイルでは制限がなしになります。 • 設定可能範囲：1-1000
トポロジチェンジを無視	「トポロジチェンジを無視」を有効 / 無効に設定します。有効にするとトポロジの変更は無視されます。

「適用」をクリックして、設定内容を適用します。

MLD スヌーピンググループ設定

「MLD スヌーピンググループテーブルを表示します。
MLD スヌーピング機能では、スイッチを通過する MLD パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

L2 機能 > L2 マルチキャストコントロール > 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表示します。

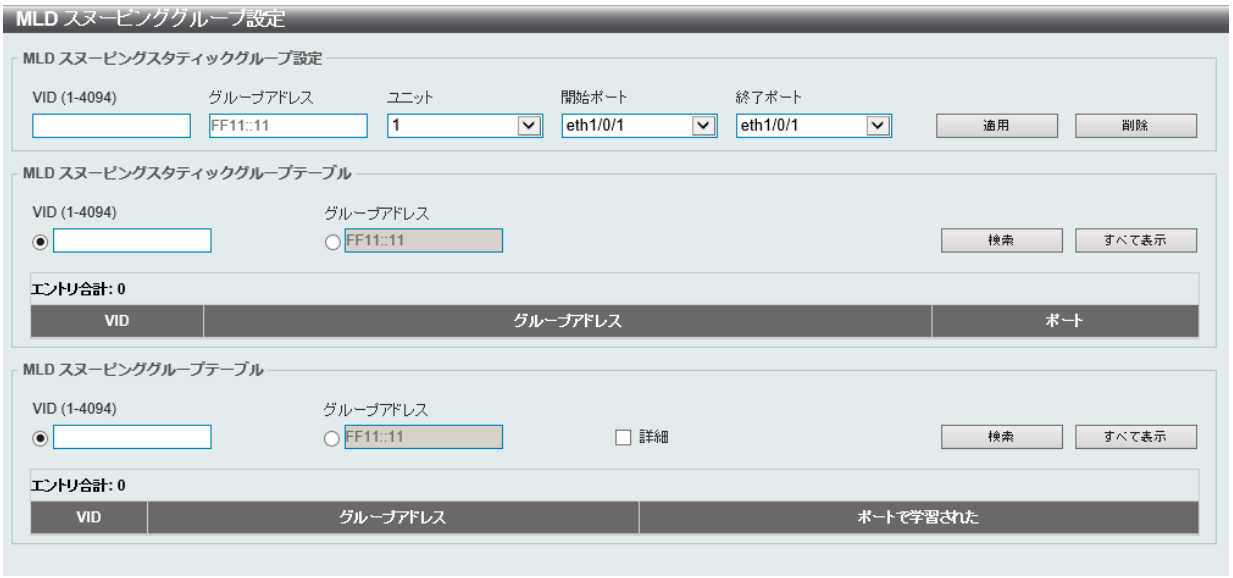


図 8-76　MLD スヌーピンググループ設定画面

画面に表示される項目：

項目	説明
MLD スヌーピングスタティックグループ設定	
VID	登録または削除する IPv6 マルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	登録または削除する IPv6 マルチキャストグループの IPv6 アドレスを入力します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。
MLD スヌーピングスタティックグループテーブル	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。
詳細	MLD グループの詳細について表示します。
MLD スヌーピンググループテーブル	
VID	チェックを入れ、検索するマルチキャストグループの VLAN ID を入力します。 • 設定可能範囲：1-4094
グループアドレス	チェックを入れ、検索するマルチキャストグループの IPv6 アドレスを入力します。
詳細	MLD グループの詳細について表示します。

「適用」をクリックして、設定内容を適用します。

「削除」をクリックして、入力した情報に基づいて指定エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。

MLD スヌーピングフィルタ設定

MLD スヌーピングフィルタの設定を行います。

L2 機能 > L2 マルチキャストコントロール > 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表示します。

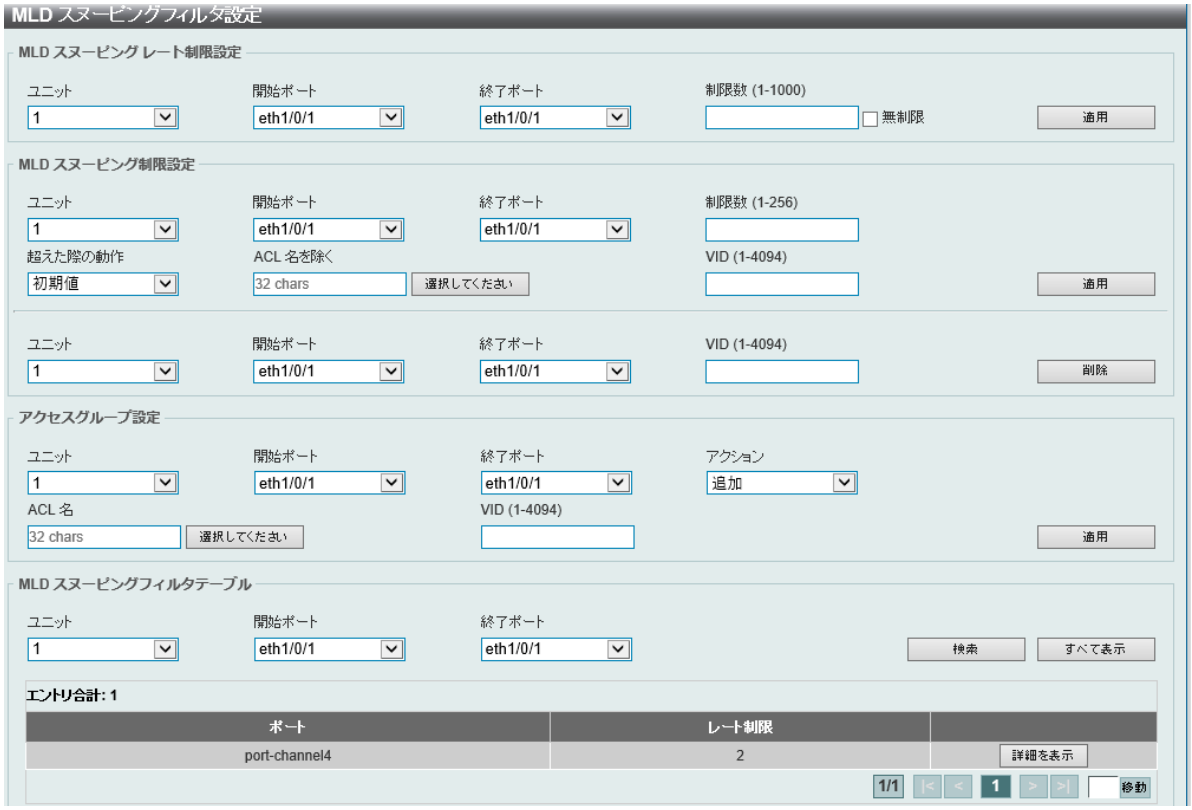


図 8-77　MLD スヌーピングフィルタ設定画面

画面に表示される項目：

項目	説明
MLD スヌーピングレート制限設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
制限数	指定のインタフェースでスイッチがプロセス可能な MLD コントロールパケットのレートを指定します。 「無制限」で制限を設定しません。 • 設定可能範囲：1-1000（パケット / 秒）
MLD スヌーピング制限設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
制限数	生成される MLD キャッシュエントリ数の上限値を指定します。 • 設定可能範囲：1-256
超えた際の動作	制限を超えた場合、新しく学習したグループに対して以下の処理を実行します。 •「初期値」- デフォルトのアクションを実行します。 •「破棄」- 新規グループは破棄されます。 •「リプレース」- 新規グループは古いグループに置き換わります。
ACL 名を除く	標準 IP アクセスリストを指定します。（32 文字以内） アクセスリストに許可されたグループ (*,G) は制限から除外されます。グループ (*,G) を許可するにはアクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「選択してください」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	トランクポートのレイヤ 2 VLAN 名を入力します。この VLAN で受信するパケットにフィルタを適用します。 • 設定可能範囲：1-4094

項目	説明
アクセスグループ設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
アクション	• 「追加」- 入力した情報に基づき新しいエントリを追加します。 • 「削除」- 入力した情報に基づき既存エントリを削除します。
ACL 名	標準 IP アクセスリストを指定します。(32 文字以内) グループ (*,G) への参加をユーザに許可する場合に使用します。アクセスリストエントリの送信元アドレスに「any」、宛先アドレスに「G」を指定します。「選択してください」をクリックして、作成済みのアクセスリストを選択することもできます。
VID	設定する VLAN を指定します。 • 設定可能範囲：1-4094
MLD スヌーピングフィルタテーブル	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「適用」をクリックして、設定内容を適用します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。
「詳細を表示」指定のエントリの詳細情報を表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「選択してください」をクリックすると次の画面が表示されます。



図 8-78　ACL アクセスリスト画面

ACL を選択し「OK」クリックします。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「詳細を表示」クリックすると次の画面が表示されます。



図 8-79　MLD スヌーピング詳細フィルタテーブル画面

「戻る」をクリックすると前のページに戻ります。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

MLD スヌーピング Mrouter 設定

VLAN インタフェースで、マルチキャストルータポートを指定します。

L2 機能 > L2 マルチキャストコントロール > MLD スヌーピング > MLD スヌーピング Mrouter 設定をクリックして表示します。



図 8-80　MLD スヌーピング Mrouter 設定画面

画面に表示される項目：

項目	説明
MLD スヌーピング Mrouter 設定	
VID	VLAN ID を入力します。
設定	ポートの設定を行います。 • 「ポート」- マルチキャストが有効なルータと接続するポート範囲を設定します。 • 「禁止 ポート」- マルチキャストが有効なルータと接続しないポート範囲を設定します。 • 「マルチキャストルータポート学習」- マルチキャストルータポートの自動取得を有効にします。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
MLD スヌーピング Mrouter テーブル	
VID	VLAN ID を入力します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、入力した情報に基づいて指定エントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。

MLD スヌーピング統計設定

現在の MLD スヌーピングの統計情報を表示します。

L2 機能 > L2 マルチキャストコントロール > MLD スヌーピング > MLD スヌーピング統計設定の順にメニューをクリックし、以下の画面を表示します。

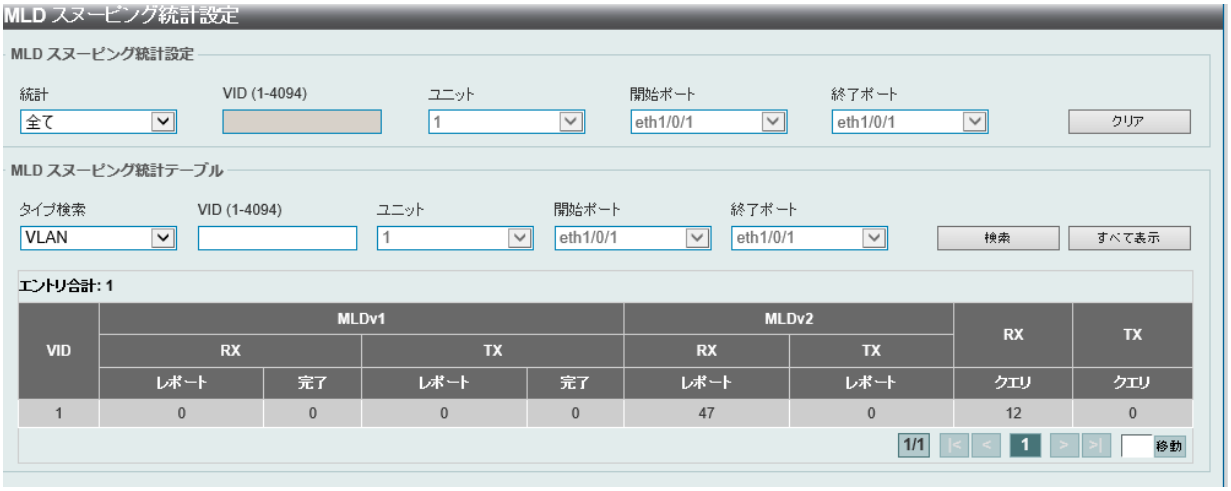


図 8-81　MLD スヌーピング統計設定画面

画面に表示される項目：

項目	説明
MLD スヌーピング統計設定	
統計	インタフェースを選択します。 • 選択肢：「全て」「VLAN」「ポート」
VID	VLAN ID を指定します。「統計」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
ユニット	設定するユニットを指定します。「統計」で「ポート」を選択すると設定可能になります。
開始ポート / 終了ポート	設定するポートの範囲を指定します。「統計」で「ポート」を選択すると設定可能になります。
MLD スヌーピング統計テーブル	
タイプ検索	インタフェースを選択します。 • 選択肢：「VLAN」「ポート」
VID	VVLAN ID を指定します。「タイプ検索」で「VLAN」を選択すると設定可能になります。 • 設定可能範囲：1-4094
ユニット	設定するユニットを指定します。「タイプ検索」で「ポート」を選択すると設定可能になります。
開始ポート / 終了ポート	設定するポートの範囲を指定します。「タイプ検索」で「ポート」を選択すると設定可能になります。

「クリア」をクリックすると表示された統計情報がクリアされます。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

「すべて表示」をクリックして、すべての定義済みエントリを表示します。

マルチキャスト VLAN

L2 機能 > L2 マルチキャストコントロール > マルチキャスト VLAN

マルチキャスト VLAN 設定

マルチキャスト VLAN の設定を行います。

L2 機能 > L2 マルチキャストコントロール > マルチキャスト VLAN > マルチキャスト VLAN 設定をクリックして表示します。

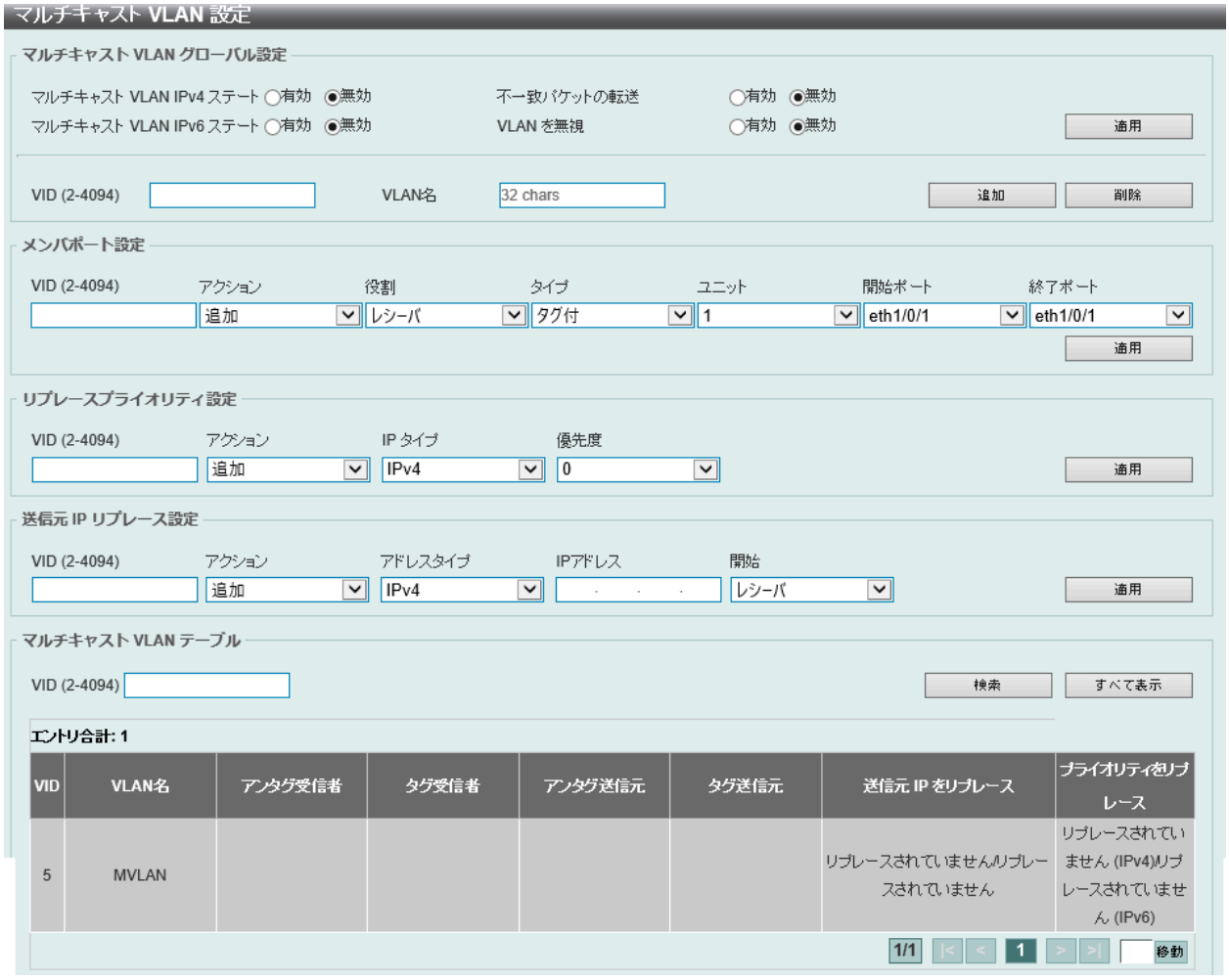


図 8-82　マルチキャスト VLAN 設定画面

画面に表示される項目：

項目	説明
マルチキャスト VLAN グローバル設定	
マルチキャスト VLAN IPv4 ステート	マルチキャスト VLAN の IPv4 IGMP コントロールパケットを有効 / 無効に設定します。
不一致パケットの転送	「不一致パケットの転送」を有効 / 無効に設定します。 受信した IGMP または MLD 制御パケットがタグなしで、どのプロファイルとも一致せず、関連付けられたデフォルト VLAN がマルチキャスト VLAN である場合、またはタグ付けされているが関連付けられたプロファイルと一致しない場合、パケットはこの設定に基づいて転送または破棄されます。 • 初期値：「無効」（不一致パケットは破棄されます。）
マルチキャスト VLAN IPv6 ステート	マルチキャスト VLAN の IPv6 MLD コントロールパケットを有効 / 無効に設定します。
VLAN を無視	タグ付き IGMP/MLD コントロールパケットに対する「VLAN を無視」を有効 / 無効に設定します。 本設定を有効にすると、受信 IGMP/MLD コントロールパケットの VLAN は無視され、プロファイルの照合を行います。
VID	作成 / 削除する VLAN の VID を指定します。 • 設定可能範囲：2-4094
VLAN 名	作成 / 削除する VLAN 名を指定します。
メンバポート設定	
VID	設定する VLAN の VID を指定します。 • 設定可能範囲：2-4094
アクション	実行する動作を指定します。 • 選択肢：「追加」「削除」

項目	説明
役割	メンバポートの役割を指定します。 • 「レシーバ」- マルチキャスト VLAN のマルチキャストデータのみを受信するサブスクライバポートとして設定します。 • 「送信元」- マルチキャスト VLAN のマルチキャストデータのみを送信するアップリンクポートとして設定します。
タイプ	メンバポートの種類を指定します。「タグ付」「アンタグ」から指定可能です。 • 「タグ付き」- ポートがタグ付きメンバに指定されると、当該ポートから送信されるパケットはマルチキャスト VLAN ID でタグ付けされます。 • 「アンタグ」- 当該ポートから送信されるパケットはタグ無しフォームで転送されます。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
リプレースプライオリティ設定	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
アクション	実行する動作を指定します。 • 選択肢：「追加」「削除」
IP タイプ	メンバポートの種類を指定します。 • 「IPv4」- マルチキャスト VLAN に転送される IPv4 マルチキャストパケットの優先値を再マップします。 • 「IPv6」- マルチキャスト VLAN に転送される IPv6 マルチキャストパケットの優先値を再マップします。
優先度	優先値を指定します。 • 設定可能範囲：0-7
送信元 IP リプレース設定	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094
アクション	実行する動作を指定します。 • 選択肢：「追加」「削除」
アドレスタイプ	アドレスの種類を指定します。 • 「IPv4」- ルータに送信される IGMP コントロールパケットの送信元 IPv4 アドレスを指定します。 • 「IPv6」- ルータに送信される MLD コントロールパケットの送信元 IPv6 アドレスを指定します。
IP アドレス	IPv4/IPv6 アドレスを指定します。
開始	送信元を指定します。 • 「レシーバ」- マルチキャスト VLAN Receiver ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。 • 「送信元」- マルチキャスト VLAN Source ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。 • 「両方」- 全てのマルチキャスト VLAN ポートで受信した IGMP/MLD report/leave パケットの送信元 IPv4/IPv6 アドレスを置き換えます。
マルチキャスト VLAN テーブル	
VID	設定するマルチキャスト VLAN の VID を指定します。 • 設定可能範囲：2-4094

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

マルチキャスト VLAN グループ設定

マルチキャスト VLAN グループの設定、表示を行います。

L2 機能 > L2 マルチキャストコントロール > マルチキャスト VLAN > マルチキャスト VLAN グループ設定をクリックして表示します。



図 8-83　マルチキャスト VLAN グループ設定画面

画面に表示される項目：

項目	説明
グループプロファイル設定	
プロファイル名	マルチキャスト VLAN のグループプロファイル名を指定します。(32 文字以内)
アクション	実行する動作を指定します。マルチキャスト VLAN プロファイルには複数の範囲を追加することができます。同じプロファイルに対して指定される IP アドレス範囲は同じアドレスファミリである必要があります。 • 選択肢：「追加」「削除」
アドレスタイプ	アドレスタイプを指定します。 • 「IPv4」- IPv4 マルチキャストアドレスを使用します。 • 「IPv6」- IPv6 マルチキャストアドレスを使用します。
開始 IP アドレス	送信元 IPv4/IPv6 アドレスを指定します。
送信先 IP アドレス	送信先 IPv4/IPv6 アドレスを指定します。
アクセスグループ設定	
VID	VLAN ID を指定します。 • 設定可能範囲：2-4094
プロファイル名	マルチキャスト VLAN のグループプロファイル名を指定します。(32 文字以内)
アクション	実行する動作を指定します。 • 選択肢：「追加」「削除」
グループプロファイルテーブル	
プロファイル名	マルチキャスト VLAN のグループプロファイル名を指定します。(32 文字以内)
アクセスグループテーブル	
VID	VLAN ID を指定します。 • 設定可能範囲：2-4094

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、入力した情報に基づいて指定エントリを削除します。
「全て削除」をクリックするとすべてのエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべての定義済みエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

PIM スヌーピング

L2 機能 > L2 マルチキャストコントロール > PIM スヌーピング

PIM スヌーピンググローバル設定

Protocol Independent Multicast（PIM）をグローバルに設定します。

L2 機能 > L2 マルチキャストコントロール > PIM スヌーピング > PIM スヌーピンググローバル設定をクリックして表示します。



図 8-84　PIM スヌーピンググローバル設定画面

画面に表示される項目：

項目	説明
グローバル設定	
グローバルステート	PIM スヌーピングのグローバルステータスを有効 / 無効に設定します。
VLAN ステータス設定	
VID	PIM スヌーピング機能を使用する VLAN ID を入力します。 また、指定 VLAN 上の PIM スヌーピングを有効 / 無効に設定します。 • 設定可能範囲：1-4094
PIM スヌーピングテーブル	
VID	PIM スヌーピングテーブルで表示する VLAN の VLAN ID を指定します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

PIM スヌーピング隣接テーブル

PIM スヌーピング隣接（ネイバ）テーブルを表示します。

L2 機能 > L2 マルチキャストコントロール > PIM スヌーピング > PIM スヌーピング隣接テーブル をクリックして表示します。



図 8-85　PIM スヌーピング隣接テーブル 画面

画面に表示される項目：

項目	説明
VID	表示する VLAN を識別する VLAN ID を指定します。 • 設定可能範囲：1-4094

「検索」をクリックして指定の VLAN ID を入力して指定のエントリを表示します。

PIM スヌーピングマルチキャストルートテーブル

PIM スヌーピングマルチキャストルートテーブルを表示します。

L2 機能 > L2 マルチキャストコントロール > PIM スヌーピング > PIM スヌーピングマルチキャストルートテーブルをクリックして表示します。



図 8-86　PIM スヌーピングマルチキャストルートテーブル画面

画面に表示される項目：

項目	説明
VID	表示する VLAN を識別する VLAN ID を指定します。 • 設定可能範囲：1-4094
グループアドレス	グループアドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

PIM スヌーピング統計テーブル

現在の PIM スヌーピングの統計情報を表示します。

L2 機能 > L2 マルチキャストコントロール > PIM スヌーピング > PIM スヌーピング統計テーブルの順にメニューをクリックし、以下の画面を表示します。

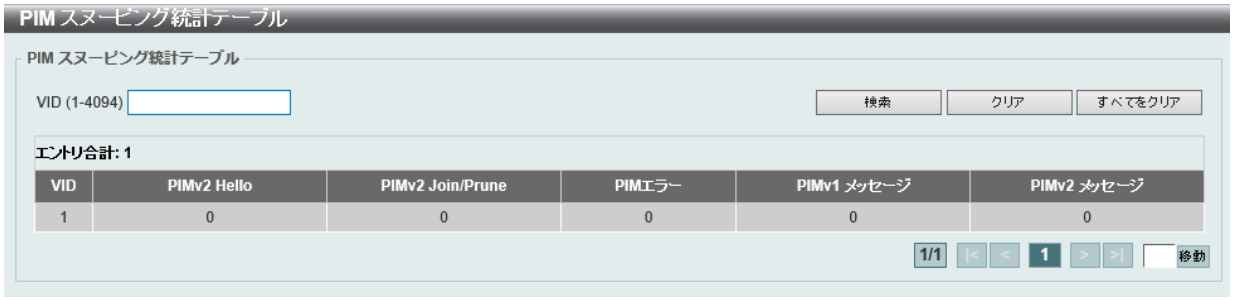


図 8-87　PIM スヌーピング統計テーブル画面

画面に表示される項目：

項目	説明
VID	検索 / 削除するエントリの VLAN を識別する VLAN ID を指定します。 • 設定可能範囲：1-4094

「クリア」をクリックすると表示された統計情報がクリアされます。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

マルチキャストフィルタリングモード

L2 マルチキャストフィルタリング設定を行います。

L2 機能 > L2 マルチキャストコントロール > マルチキャストフィルタリングモードをクリックし、以下の画面を表示します。



図 8-88　マルチキャストフィルタリングモード画面

画面に表示される項目：

項目	説明
VID リスト	設定する VLAN の VLAN ID リストを入力します。
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モードを選択します。 • 「未登録パケットの転送」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づいて転送され、登録されていないマルチキャストパケットは VLAN ドメインに基づきフラッドされます。 • 「すべて転送」- すべてのマルチキャストパケットは VLAN ドメインに基づきフラッドされます。 • 「未登録フィルタ」- 登録されたマルチキャストパケットはフォワーディングテーブルに基づき転送され、登録されていないマルチキャストパケットはフィルタされます。

「適用」をクリックして、設定内容を適用します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

LLDP

L2 機能 > LLDP

LLDP（Link Layer Discovery Protocol）は、IEEE 802 ネットワークに接続しているステーションから同じ IEEE 802 ネットワークに接続している他のステーションに通知を出します。本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース（MIB）に格納されるため、SNMP（Simple Network Management Protocol）などの管理プロトコル使ったネットワーク管理システム（NMS）からその情報にアクセスできるようになります。

LLDP グローバル設定

L2 機能 > LLDP > LLDP グローバル設定の順にメニューをクリックし、以下の画面を表示します。

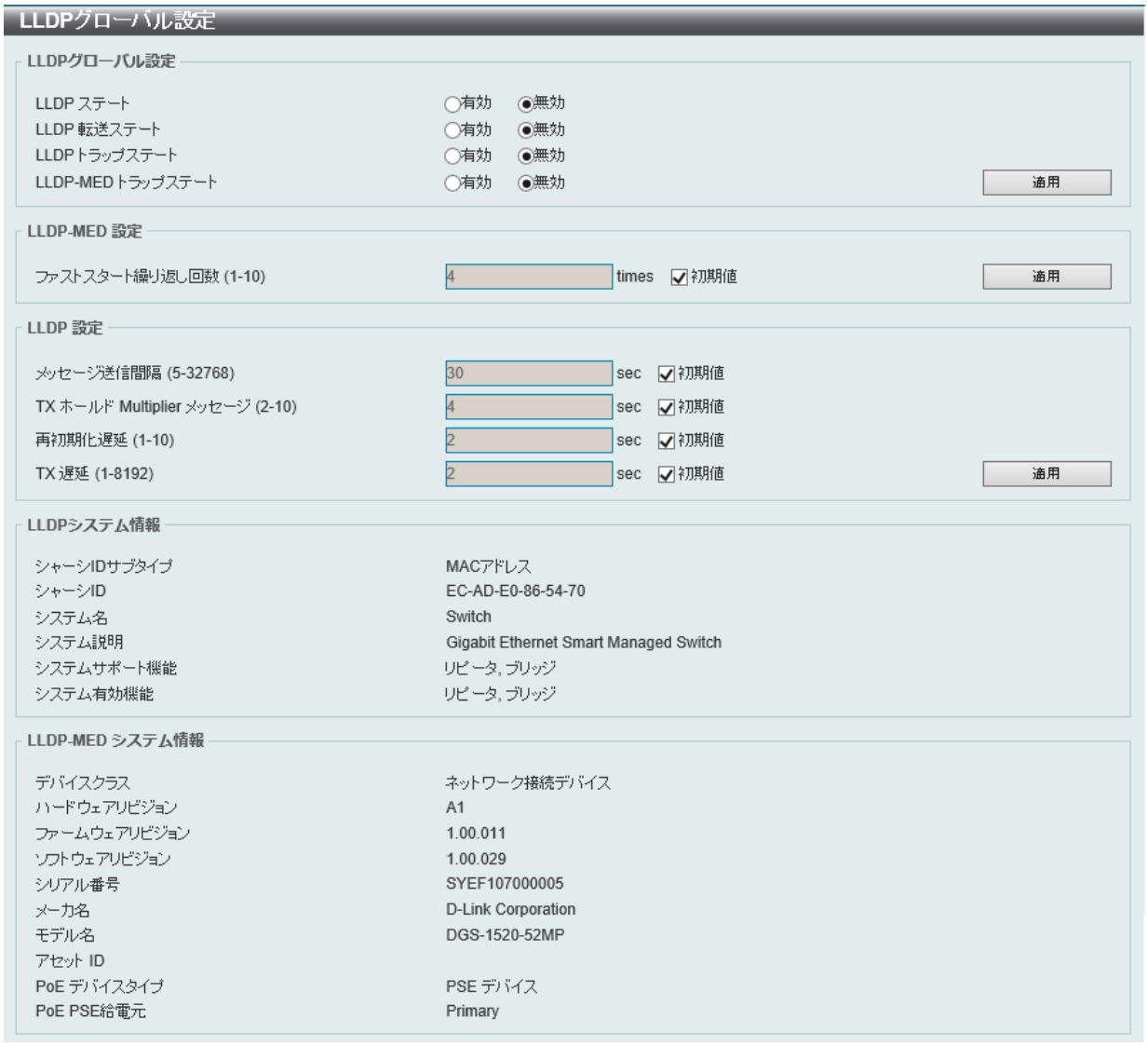


図 8-89　LLDP グローバル設定画面

画面に表示される項目：

項目	説明
LLDP グローバルステート	
LLDP ステート	スイッチにおける LLDP 機能を有効 / 無効に設定します。
LLDP 転送ステート	LLDP 転送ステータスを有効 / 無効に設定します。 「LLDP ステート」が 無効で「LLDP 転送ステート」が有効の場合、受信した LLDPDU（LLDP data unit）パケットは転送されます。
LLDP トラップステート	LLDP Trap を有効 / 無効に指定します。
LLDP-MED トラップステート	LLDP-MED Trap を有効 / 無効に指定します。
LLDP-MED 設定	
ファストスタート繰り返し回数	「LLDP-MED」ファストスタートリピートカウント値を指定します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-10

項目	説明
LLDP 設定	
メッセージ送信間隔	インタフェースが LLDP アドバタイズメントを連続して送信する際の送信間隔を入力します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：5-32768（秒）
TX ホールド Multiplier メッセージ	LLDPDU の TTL（有効期間 /Time to Live）値の計算に使用される、LLDPDU 送信間隔の乗数を入力します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：2-10
再初期化遅延	LLDP ポートが再初期化を行うまでの待機時間を指定します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-10（秒）
TX 遅延	インタフェースで LLDPDU を送信するまでの待機時間を指定します。送信間隔の数値の 1/4 より大きくすることはできません。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-8192（秒）

「適用」をクリックし、設定内容を適用します。

LLDP ポート設定

LLDP ポートの設定を行います。

L2 機能 > LLDP > LLDP ポート 設定の順にメニューをクリックし、以下の画面を表示します。

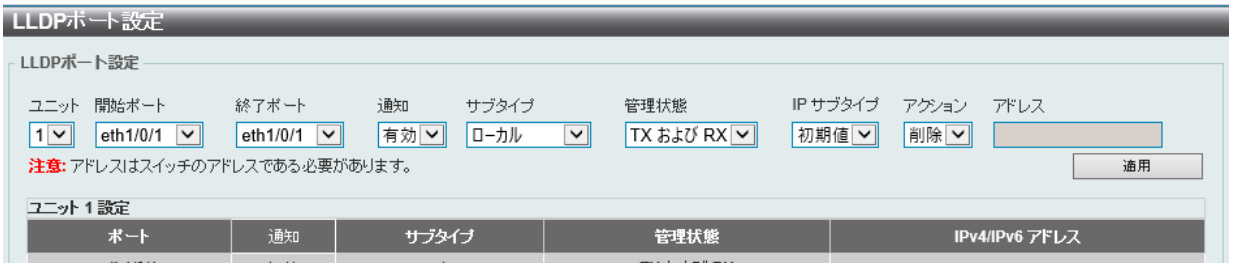


図 8-90　LLDP ポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
通知	LLDP 通知を有効 / 無効に設定します。
サブタイプ	LLDP TLV（s）のサブタイプを選択します。 • 選択肢：「MAC アドレス」「ローカル」
管理状態	ローカル LLDP エージェントを選択し、ポートで LLDP フレームを送受信できるようにします。 • 「TX」- ローカル LLDP エージェントは、LLDP フレームの送信のみ行います。 • 「RX」- ローカル LLDP エージェントは、LLDP フレームの受信のみ行います。 • 「TX および RX」- ローカル LLDP エージェントは LLDP フレームの送受信をします。（初期値） • 「無効」- ローカル LLDP エージェントは LLDP フレームの送受信をしません。
IP サブタイプ	プルダウンメニューを使用して送信する IP アドレスの種類を選択します。
アクション	アクションを選択します。 選択肢：「追加」「削除」
アドレス	通知するエンティティの管理アドレスを入力します。

「適用」をクリックして、設定内容を適用します。

注意　入力の IPv4/IPv6 アドレスは既存の LLDP 管理 IP アドレスである必要があります。

LLDP 管理アドレスリスト

L2 機能 > LLDP > LLDP 管理アドレスリストの順にメニューをクリックし、以下の画面を表示します。

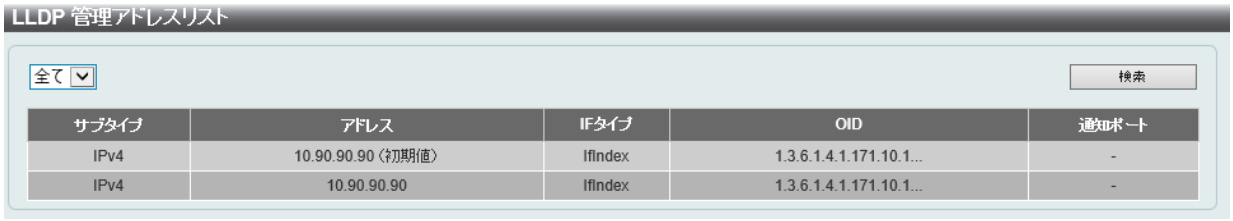


図 8-91　LLDP 管理アドレスリスト画面

画面に表示される項目：

項目	説明
サブタイプ	表示する LLDP 管理アドレスのサブタイプを選択します。 • 選択肢：「全て」「IPv4」「IPv6」

「検索」をクリックし、LLDP 管理情報を検索します。

LLDP 基本 TLVs 設定

LLDP の Type-Length-Value（TLV）設定を行います。TLV により、LLDP パケット内で特定の情報を送信できます。
スイッチのアクティブな LLDP ポートには、通常、その外向き通知に必須データが含まれています。

必須のデータタイプには、以下の 4 タイプの TLV が含まれます。必須のデータタイプを無効にすることはできません。
- end of LLDPDU TLV
- chassis ID TLV
- port ID TLV
- TTL TLV

さらに、オプションで選択可能な 4 つのデータタイプがあります。
- ポート説明（Port Description）
- システム名（System Name）
- システム説明（System Description）
- システム機能（System Capability）

L2 機能 > LLDP > LLDP 基本 TLVs 設定の順にメニューをクリックし、以下の画面を表示します。



図 8-92　LLDP 基本 TLVs 設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ポート説明	ポート説明を有効 / 無効に設定します。
システム名	システム名を有効 / 無効に設定します。
システム説明	システム説明を有効 / 無効に設定します。
システム機能	システム機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

LLDP Dot1 TLVs 設定

VLAN 関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

L2 機能 > LLDP > LLDP Dot1 TLVs 設定の順にメニューをクリックし、以下の画面を表示します。



図 8-93　LLDP Dot1 TLVs 設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ポート VLAN	ポート VLANID TLV の送信を有効 / 無効に設定します。 ポート VLANID TLV は、オプションのフィックス長 TLV です。VLAN ブリッジポートが、「タグなし」または「優先度タグ付き」フレームに関連付けられるポート VLAN ID（PVID）をアドバタイズできるようにします。
プロトコル VLAN	ポートおよびプロトコル VLANID（PPVID）TLV の送信を有効 / 無効に設定します。 PPVID TLV の VLAN ID を入力します。
VLAN 名	VLAN 名 TLV の送信を有効 / 無効に設定します。VLAN 名 TLV に VLAN ID を入力します。
プロトコル識別子	プロトコル ID TLV とプロトコル名の送信を有効 / 無効に設定します。 対象とするプロトコルを選択します。 • 選択肢：「なし」「EAPOL」「LACP」「GVRP」「STP」「全て」

「適用」をクリックして、設定内容を適用します。

LLDP Dot3 TLVs 設定

イーサネット関連の TLV について、外向き LLDP 通知の有効化 / 無効化を設定します。

L2 機能 > LLDP > LLDP Dot3 TLVs 設定の順にメニューをクリックし、以下の画面を表示します。



図 8-94　LLDP Dot3 TLVs 設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
MAC/PHY 設定 / ステータス	送信する MAC/PHY 設定 / ステータス TLV を有効 / 無効にします。 MAC/PHY 設定 / ステータス TLV は、 (1) 送信 IEEE802.3 LAN ノードのデュプレックスおよびビットレート機能 (2) 送信 IEEE802.3 LAN ノードの現在のデュプレックスおよびビットレート設定 を識別するオプションの TLV です。
リンクアグリゲーション	送信するリンクアグリゲーション TLV を有効 / 無効にします。 リンクアグリゲーション TLV は、リンクが集約可能かどうか、リンクが現在集約されているかどうか、およびポートの集約されたポートチャネル ID、が含まれていることを示しています。 ポートが集約されていない場合、ID は 0 です
最大フレームサイズ	送信する最大フレームサイズ TLV を有効 / 無効にします。 最大フレームサイズ TLV は、実装された MAC および PHY の最大フレームサイズを示します。
MDI 経由の電源	「MDI TLV」経由での電力送信を有効 / 無効に設定します。 IEEE802.3 PMD の実装により接続した電力供給のないシステムに対し電力を供給します。「MDI TLV 経由の電源」により IEEE 802.3 LAN ステーションに MDI 電力サポート機能を提供するネットワーク管理を実現します。

「適用」をクリックして、設定内容を適用します。

LLDP-MED ポート設定

LLDP-MED TLV の送信を有効または無効にします。

L2 機能 > LLDP > LLDP-MED ポート設定の順にメニューをクリックし、以下の画面を表示します。



図 8-95　LLDP-MED ポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
通知	LLDP-MED 通知 TLV（LLDP-MED notification TLV）の送信を有効 / 無効に設定します。
機能	LLDP-MED 機能 TLV（LLDP-MED capabilities TLV）の送信を有効 / 無効に設定します。
インベントリ	LLDP-MED インベントリ TLV（LLDP-MED inventory TLV）の送信を有効 / 無効に設定します。
ネットワークポリシ	LLDP-MED ネットワークポリシ TLV（LLDP-MED network policy TLV）の送信を有効 / 無効に設定します。
PSE	「MDI TLV」経由での LLDP-MED 拡張電力送信を有効 / 無効に設定します。 接続しているデバイスが「PSE」または「PD」である必要があります。

「適用」をクリックして変更を適用します。

LLDP 統計情報

スイッチにおける LLDP 統計情報と各ポートの設定を参照できます。

L2 機能 > LLDP > LLDP 統計情報の順にメニューをクリックし、以下の画面を表示します。



図 8-96　LLDP 統計情報画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。
ポート	表示するポートを指定します。

「カウンタをクリア」をクリックして統計情報のカウンタ数をクリアします。
「すべてをクリア」をクリックしてすべてのカウンタ数をクリアします。

LLDP ローカルポート情報

外向き LLDP 通知に入力するために、現在利用可能な LLDP ローカルポートの情報を表示します。
L2 機能 > LLDP > LLDP ローカルポート情報の順にメニューをクリックし、以下の画面を表示します。

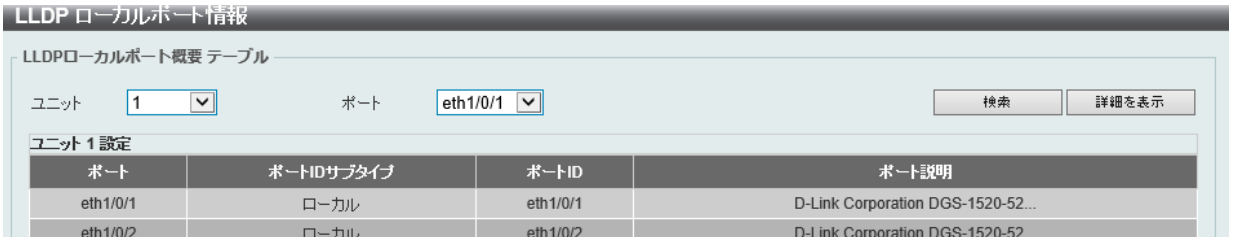


図 8-97　LLDP ローカルポート情報画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。
ポート	表示するポートを指定します。

ポートを選択し、「検索」をクリックします。情報が画面下半分に表示されます。

■ パラメータの詳細の参照

「詳細を表示」リンクをクリックし、以下の画面を表示します。

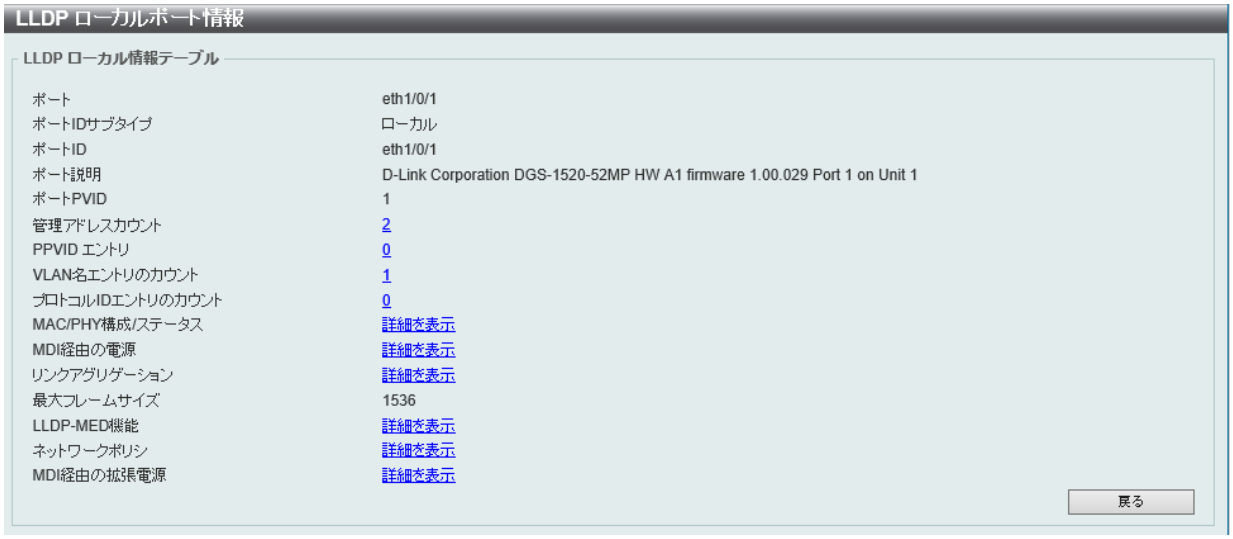


図 8-98　LLDP ローカルポート情報 - 詳細を表示画面

■ 「MAC/PHY 構成 / ステータス」情報の参照

「詳細を表示」リンクをクリックし、以下の画面を表示します。

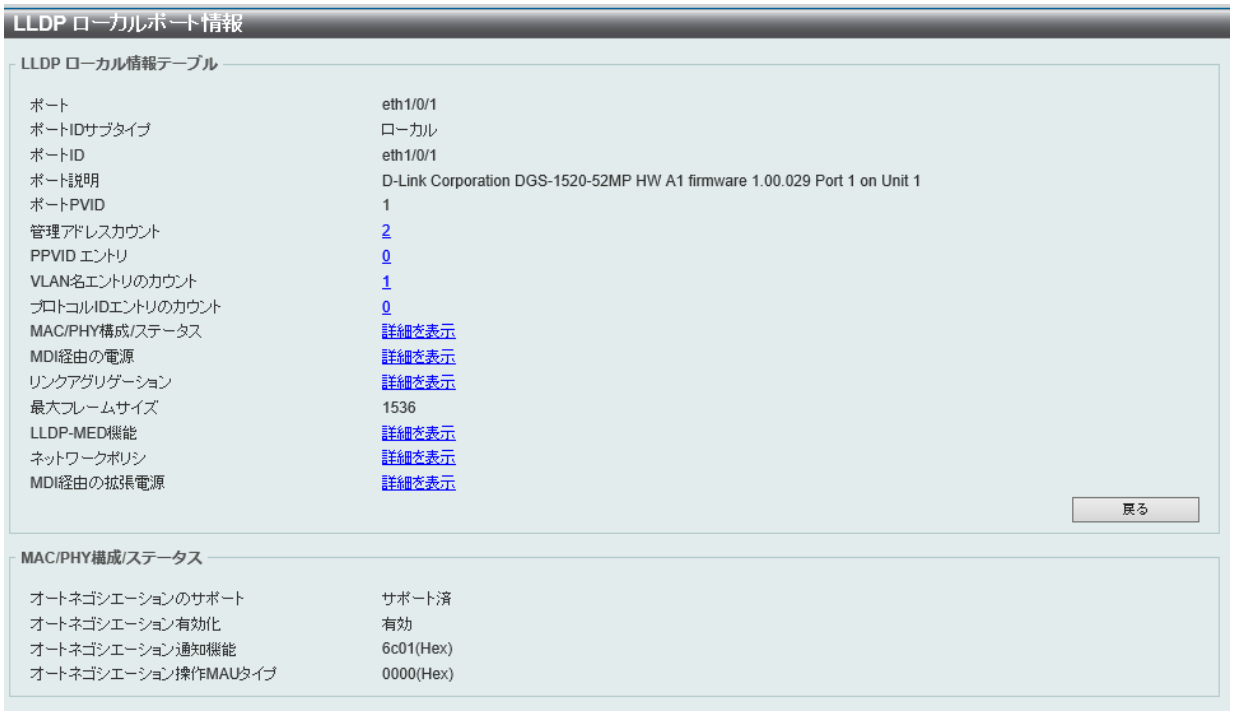


図 8-99　LLDP ローカルポート情報 - MAC/PHY 構成ステータス 画面

LLDP 隣接ポート情報

隣接（ネイバ）から学習したポート情報を表示します。

L2 機能 > LLDP > LLDP 隣接ポート情報の順にメニューをクリックし、以下の画面を表示します。



図 8-100　LLDP 隣接ポート情報画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。
ポート	表示するポートを指定します。

ポートを選択し、「検索」をクリックします。情報が画面下半分に表示されます。
「クリア」をクリックしてポート情報をクリアします。
「すべてをクリア」をクリックして全てのポート情報をクリアします。
「詳細を表示」をクリックして指定ポート詳細情報を表示します。

第 9 章　L3 機能

L3 機能メニューを使用し、本スイッチにレイヤ 3 機能を設定することができます。

以下は L3 機能サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
ARP	ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。
Gratuitous ARP	Gratuitous ARP の設定、編集を行います。
IPv6 隣接	IPv6 隣接（ネイバ）の設定を行います。
インタフェース	IP インタフェース設定を行います。
UDP Helper	IP 転送プロトコルの設定を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。また UDP ブロードキャストパケットを転送するターゲットアドレスを指定します。
IPv4 スタティック / デフォルトルート	本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。
IPv4 ルートテーブル	IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。
IPv6 スタティック / デフォルトルート	IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。
IPv6 ルートテーブル	IPv6 ルーティングテーブルを表示します。
ルート優先	ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。
ECMP 設定	ECMP OSPF 状態と ECMP ルートロードバランシングアルゴリズムを設定します。
IPv6 General プレフィックス	VLAN インタフェース IPv6 汎用プレフィックスの設定を行います。
URPF 設定	「Unicast Reverse Path Forwarding」（URPF）の設定と表示を行います。
RIP	RIP（Routing Information Protocol）は、距離ベクトル型のルーティングプロトコルです。
RIPng	RIPng（Routing Information Protocol next generation）をサポートしています。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。
OSPF	OSPF を設定します。
IP マルチキャストルーティングプロトコル	IP マルチキャストルーティングプロトコルの設定を行います。
IP ルートフィルタ	IP プレフィックスリスト、ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。
ポリシールート	ポリシーベースルーティングの設定、表示を行います。
VRRP	VRRP（Virtual Routing Redundancy Protocol）は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。
VRRPv3 設定	VRRPv3 設定を行います。

ARP

L3 機能 > ARP

ARP（Address Resolution Protocol）の設定を行います。ARP により、IP アドレスから Ethernet の MAC アドレス情報を取得できます。

ARP エージングタイム

ARP エージングタイムの設定を行います。

L3 機能 > ARP > ARP エージングタイムの順にクリックし、以下の画面を表示します。

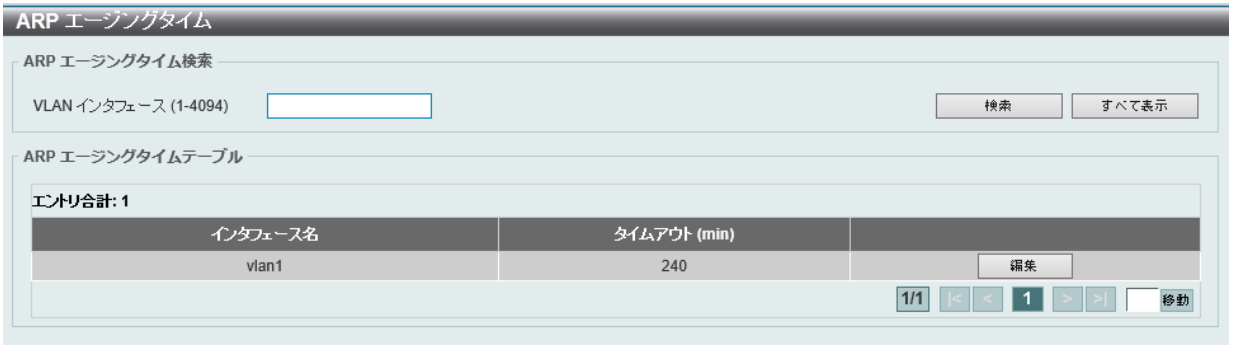


図 9-1　ARP エージングタイム画面

画面に表示される項目：

項目	説明
ARP エージングタイム検索	
VLAN インタフェース	VLAN インタフェース ID を入力します。 • 設定可能範囲：1-4094
ARP エージングタイムテーブル	
タイムアウト	「編集」をクリックし、ARP エイジングタイムアウト値（分）を入力します。 この時間が経過すると、エントリはテーブルから削除されます。

「検索」をクリックして指定のエントリを表示します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

スタティック ARP 設定

スタティック ARP の設定を行います。
スタティック ARP エントリを ARP テーブルに追加、または削除します。

L3 機能 > ARP > スタティック ARP の順にクリックし、以下の画面を表示します。

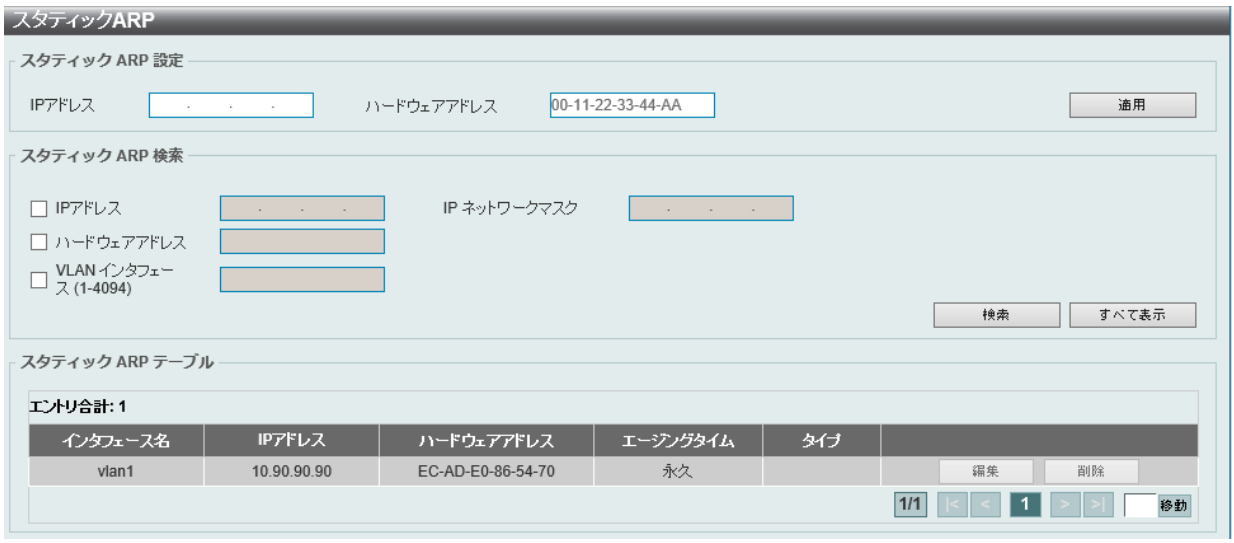


図 9-2　スタティック ARP 画面

画面に表示される項目：

項目	説明
スタティック ARP 設定	
IP アドレス	MAC アドレスに紐づける IP アドレスを設定します。
ハードウェアアドレス	IP アドレスに紐づける MAC アドレスを設定します。
スタティック ARP 検索	
IP アドレス	スタティック ARP エントリの IP アドレスを入力します。
ネットマスク	スタティック ARP エントリのサブネットマスクを選択して入力します。
ハードウェアアドレス	スタティック ARP エントリの MAC アドレスを選択して入力します。
VLAN インタフェース	検索する VLAN インタフェースを入力します。

「適用」をクリックして、設定内容を適用します。

「検索」をクリックして、エントリを検索します。
「削除」をクリックして、指定のエントリを削除します。
「編集」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

プロキシ ARP

プロキシ ARP 設定の設定を行います。
プロキシ ARP は、他のデバイス当ての ARP リクエストに対して、L3 スイッチやルータが代理で ARP 応答を行う機能です。
スタティックルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルーティングできます。
ホスト（通常レイヤ 3 スイッチ）は別の機器宛てのパケットに応答します。

L3 機能 > ARP > プロキシ ARP の順にメニューをクリックし、以下の画面を表示します。



図 9-3　プロキシ ARP 画面

画面に表示される項目：

項目	説明
プロキシ ARP ステート	「編集」をクリックし、プロキシ ARP を有効 / 無効に設定します。
ローカルプロキシ ARP ステート	「編集」をクリックし、ローカルプロキシ ARP を有効 / 無効に設定します。 ローカルプロキシ ARP 機能により、送信元 IP と宛先 IP が同じインタフェースにある場合、スイッチはプロキシ ARP に応答できます。

「適用」をクリックして、設定内容を適用します。

ARP テーブル

ARP テーブルの表示と設定を行います。

L3 機能 > ARP > ARP テーブルの順にメニューをクリックし、以下の画面を表示します。



図 9-4　ARP テーブル画面

画面に表示される項目：

項目	説明
VLAN インタフェース	表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP アドレス	表示する IP アドレスを入力します。
マスク	上記 IP アドレスのマスクを指定します。
ハードウェアアドレス	表示する MAC アドレスを入力します。
タイプ	表示する ARP の種類を指定します。 • 選択肢：「全て」「ダイナミック」
MGMT	MGMT（管理）ポートについての情報を表示します。 本項目は DGS-1520-28/52 でのみ表示されます。

「検索」をクリックして、入力した情報に基づく指定のエントリを検索します。
「クリア」をクリックして、エントリを消去します。
「すべてをクリア」をクリックするとテーブル上のエントリが全て消去されます。

Gratuitous ARP

Gratuitous ARP の設定を行います。
Gratuitous ARP リクエストパケットは、送信元 / 宛先 IP アドレスが送信元デバイスのアドレスに設定され、宛先 MAC アドレスがブロードキャストアドレスとなっている ARP リクエストパケットです。通常、Gratuitous ARP リクエストパケットを使用して、IP アドレスが他のデバイスと競合していないかどうかを検出したり、インタフェースに接続されたホストの ARP キャッシュエントリを事前ロードまたは再構成したりします。

L3 機能 > Gratuitous ARP の順にメニューをクリックし、以下の画面を表示します。

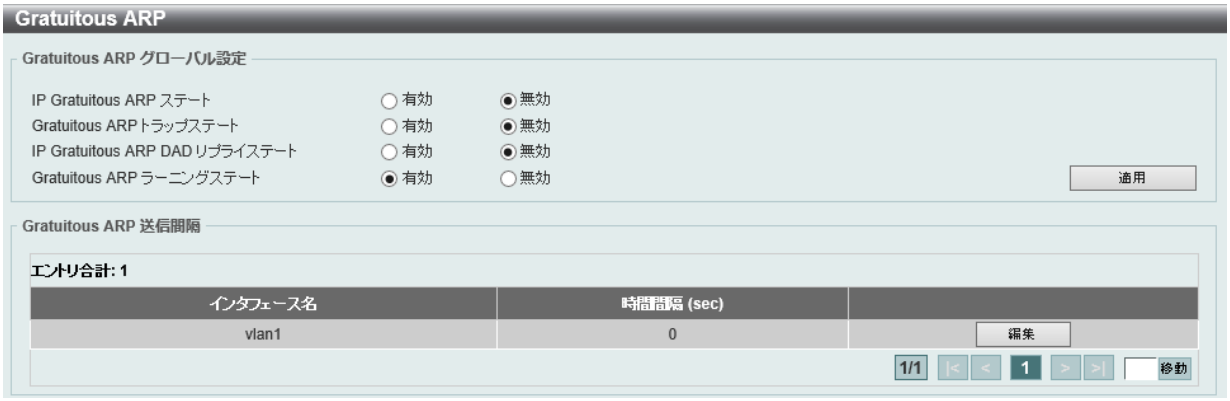


図 9-5　Gratuitous ARP 画面

画面に表示される項目：

項目	説明
Gratuitous ARP グローバル設定	
IP Gratuitous ARP ステート	ARP キャッシュテーブルの Gratuitous ARP パケットの習得を有効 / 無効に設定します。
Gratuitous ARP トラップステート	Gratuitous ARP トラップ を有効 / 無効に設定します。
IP Gratuitous ARP DAD リプライステート	IP Gratuitous ARP Dad-reply を有効 / 無効に設定します。
Gratuitous ARP ラーニングステート	GratuitousARP のラーニングステート（学習状態）を有効 / 無効に設定します。 システムは通常、ARP 応答パケットや、スイッチの IP アドレスに対応する MAC アドレスを問い合せるための通常の ARP リクエストパケットからのみ ARP エントリを学習します。 このオプションを使用すると、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 / 無効に設定できます。Gratuitous ARP パケットは、送信元アドレスと問合せ IP アドレスが同一のパケットです。
Gratuitous ARP 送信間隔	
送信間隔	「編集」をクリックし、定期的に Gratuitous ARP を送信する間隔（秒）を入力します。

「適用」をクリックして、設定内容を適用します。

IPv6 隣接

スイッチの IPv6 隣接（ネイバ）の設定を行います。

L3 機能 > IPv6 隣接の順にメニューをクリックし、以下の画面を表示します。



図 9-6　IPv6 隣接画面

画面に表示される項目：

項目	説明
VLAN インタフェース	IPv6 ネイバの VLAN インタフェースを指定します。 • 設定可能範囲：1-4094
IPv6 アドレス	IPv6 アドレスを入力します。
MAC アドレス	MAC アドレスを指定します。

IPv6 ネイバの新規登録
画面上段の「VLAN インタフェース」、「IPv6 アドレス」および「MAC アドレス」を入力し、「適用」をクリックします。

エントリの検索
画面中央の「VLAN インタフェース」、「IPv6 アドレス」を入力し「検索」をクリックします。

検索結果の消去
検索結果を消去するには「クリア」、表示されているすべてのエントリを消去するには、「すべてをクリア」ボタンをクリックします。

エントリの削除
該当エントリの「削除」をクリックします。

複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、指定のページへ移動します。

インタフェース

スイッチの IP インタフェース設定を行います。

IPv4 インタフェース

スイッチの IPv4 インタフェース設定を行います。

L3 機能 > インタフェース > IPv4 インタフェース の順にメニューをクリックし、以下の画面を表示します。



図 9-7　IPv4 インタフェース画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
VLAN インタフェース	設定、表示するインタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックして、指定エントリを削除します。

IPv4 インタフェース設定タブ

指定エントリの「編集」をクリックして以下の画面を表示します。

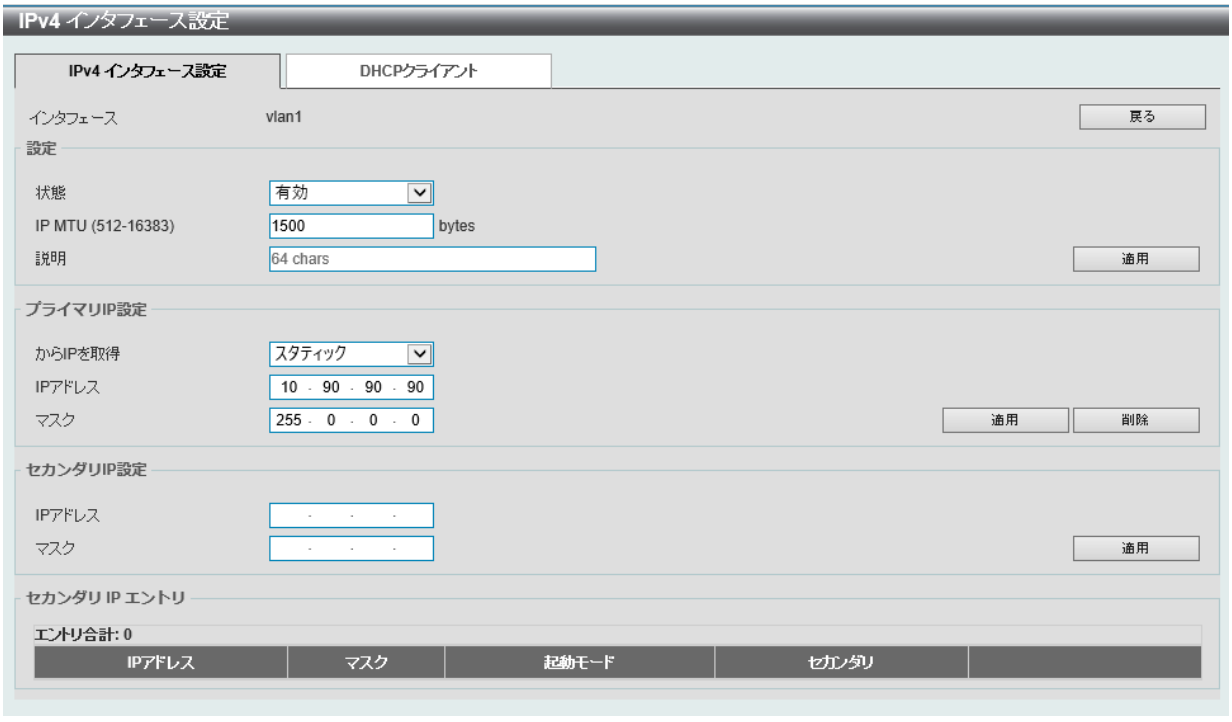


図 9-8　IPv4 インタフェース設定 - IPv4 インタフェース設定タブ画面

画面に表示される項目：

項目	説明
設定	
状態	該当エントリの IPv4 インタフェースをグローバルに有効 / 無効に設定します。
IP MTU	使用する IP レイヤの MTU 値を入力します。 • 設定可能範囲：512 - 16383（bytes） • 初期値：1500（bytes）
説明	エントリの説明を入力します。（64 文字以内）
プライマリ IP 設定 / セカンダリ IP 設定	
から IP を取得	IP アドレスの設定方法を選択します。 • 「スタティック」- インタフェースに設定する IPv4 アドレスを手動で設定します。 • 「DHCP」- ローカルネットワーク上の DHCP サーバから自動的に IPv4 情報を取得します。
IP アドレス	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
マスク	IPv4 インタフェースに割り当てるサブネットマスクを入力します。

「適用」をクリックして、設定内容を適用します。
前のページに戻る場合は「戻る」をクリックします。
「削除」をクリックして、指定エントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

DHCP クライアントタブ

「IPv4 インタフェース 設定」の「DHCP クライアント」タブをクリックして以下の画面を表示します。

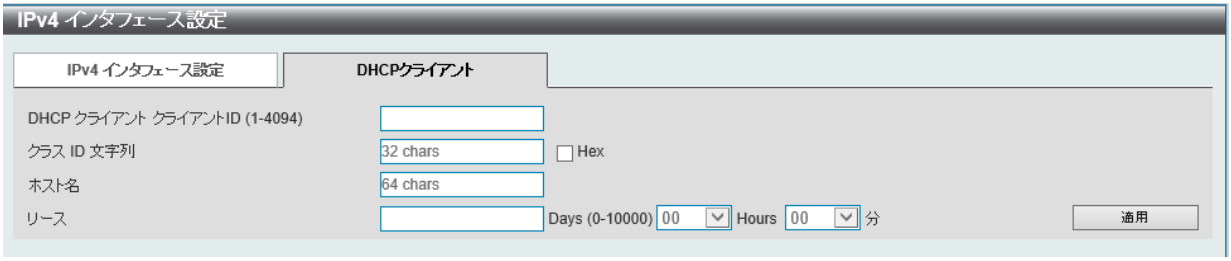


図 9-9　IPv4 インタフェース - DHCP クライアントタブ 画面

画面に表示される項目：

項目	説明
DHCP クライアント クライアント ID	DHCP クライアント ID を入力します。この ID は VLAN インタフェースを指定します。 該当インタフェースの 16 進数 MAC アドレスは、DISCOVER メッセージと一緒に送信されるクライアント ID として使用されます。 • 設定可能範囲：1-4094
クラス ID 文字列	クラス識別名を入力します（32 文字以内）。 「Hex」にチェックを入れると 16 進数方式（64 文字以内）になります。DHCP DISCOVER メッセージに含まれる Option60 の値として使用されます。
ホスト名	ホスト名を入力します。（64 文字以内） DHCP DISCOVER メッセージと一緒に送信されるホスト名オプションの値です。
リース	DHCP サーバから割り振られる IP アドレスのリース時間を指定します。オプションで時間と分を指定することもできます。 • 設定可能範囲：0-10000（日）

「適用」をクリックして、設定内容を適用します。
前のページに戻る場合は「戻る」をクリックします。
「削除」をクリックして、指定エントリを削除します。

IPv6 インタフェース

L3 機能 > インタフェース > IPv6 インタフェース の順にメニューをクリックし、以下の画面を表示します。



図 9-10　IPv6 インタフェース 画面

画面に表示される項目：

項目	説明
IPv6 オプティミスティック DAD	
IPv6 オプティミスティック DAD ステート	IPv6 Optimistic DAD を有効 / 無効に設定します。
IPv6 インタフェース	
VLAN インタフェース	設定、表示する IPv6 インタフェースの VLAN ID を入力します。 • 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPv6 インタフェース設定タブ

指定エントリの「詳細を表示」をクリックして以下の画面を表示します。



図 9-11　IPv6 インタフェース - IPv6 インタフェース 設定タブ画面

画面に表示される項目：

項目	説明
インタフェース	
IPv6 MTU	使用する IPv6 レイヤの MTU 値を入力します。RA メッセージ内でアドバタイズされる MTU の値です。 • 設定可能範囲：1280 - 65534（bytes） • 初期値：1500（ bytes）
IPv6 ステート	該当エントリの IPv6 インタフェースをグローバルに有効 / 無効に設定します。
IPv6 アドレス自動設定	
状態	ステートレス自動設定を使用した IPv6 アドレスの自動設定を有効 / 無効に設定します。 「初期値」に指定すると、このインタフェースでデフォルトルータが選択されている場合、そのデフォルトルータを使用してデフォルトルートがインストールされます。このオプションは 1 つのインタフェースのみで指定可能です。
スタティック IPv6 アドレス設定	
IPv6 アドレス	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。 •「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。 •「リンクローカル」- IPv6 インタフェースにリンクローカルアドレスを使用します。

「適用」をクリックして、設定内容を適用します。

注意　IPv6 インタフェースにおいて、64 ビットより長い プリフィクス長は設定できません。

IPv6 アドレスインタフェースタブ

指定エントリの「詳細を表示」をクリックして、「IPv6 アドレスインタフェース」タブを表示します。



図 9-12　IPv6 インタフェース - IPv6 アドレスインタフェースタブ画面

エントリの削除

対象のエントリの「削除」をクリックします。

隣接検出タブ

指定エントリの「詳細を表示」をクリックして、「隣接検出」タブを表示します。



図 9-13　IPv6 インタフェース - 隣接検出タブ画面

画面に表示される項目：

項目	説明
管理設定フラグ	管理設定フラグをオン / オフにします。 隣接（ネイバ）ホストがフラグがオンになっている RA を受信すると、ホストは IPv6 アドレスを取得するためにステートフル設定プロトコルを使用する必要があります。
他の設定フラグ	その他の設定フラグ をオン / オフにします。 オンにした場合、ルータは接続されたホストにステートフル構成プロトコルを使用して IPv6 アドレス以外の自動構成情報を取得するように指示します。
RA 最小間隔	RA 間隔の最小値を入力します。この値は、最大値の 0.75 倍より小さくする必要があります。 • 設定可能範囲：3 - 1350（秒）
RA 最大間隔	RA 間隔の最大時間値を入力します。 • 設定可能範囲：4 - 1800（秒）
RA 有効期間	RA の有効期間値を入力します。 RA の有効期間値は、ルータをデフォルトルータとする有効期間値を受信ホストに指示します。 • 設定可能範囲：0 - 9000（秒）
RA 抑制	RA 抑制機能を有効 / 無効に設定します。
到達可能時間	到達可能時間を入力します。0 の場合、ルータはインタフェースで 1200 秒を使用し、RA メッセージで 0（指定なし）をアドバタイズします。到達可能時間は、近隣ノードの到達可能性を決定する際に IPv6 ノードによって使用されます。 • 設定可能範囲：0 - 3600000（ミリ秒）
NS 間隔	近隣要請（Neighbor Solicitation）間隔値を入力します。 「0」の場合、ルータはインタフェースで 1 秒を使用し、ルータ広告（RA）メッセージで 0（指定なし）を使用します。 • 設定可能範囲：0 - 3600000（ミリ秒）、1000 の倍数
ホップ制限	ホップ制限値を入力します。 システムによって発信された IPv6 パケットも、この値を初期ホップ制限として使用します。 • 設定可能範囲：0 - 255

「適用」をクリックして、設定内容を適用します。

DHCPv6 クライアントタブ

指定エントリの「詳細を表示」をクリックして、「DHCPv6 クライアント」を表示します。



図 9-14　IPv6 インタフェース > DHCPv6 クライアントタブ画面

画面に表示される項目：

項目	説明
DHCPv6 クライアント	
再スタート	「再スタート」をクリックすると、DHCPv6 クライアントサービスを再始動します。
DHCPv6 クライアント設定	
クライアントステート	DHCPv6 クライアントを有効 / 無効に指定します。 「高速コミット」を選択して、アドレス委任の 2 つの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、2 メッセージのハンドシェイクを要求するための Solicit メッセージに含まれます。
DHCPv6 クライアント PD 設定	
クライアント PD ステート	指定インタフェースに Prefix Delegation（PD）をリクエストする DHCPv6 クライアントプロセスを有効 / 無効に指定します。「高速コミット」を選択して、アドレス委任の 2 つの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、2 メッセージのハンドシェイクを要求するための Solicit メッセージに含まれます。
General プレフィックス名	IPv6 の一般的なプレフィックス名を指定します。（12 文字以内）
IPv6 DHCP クライアント PD ヒント	ヒントとしてメッセージで送信する IPv6 プレフィックスを入力します。

「適用」をクリックして、設定内容を適用します。

ループバックインタフェース

ループバックインタフェースの設定を行います。ループバックインタフェースは論理インタフェースであり、常に UP 状態となります。

L3 機能 > インタフェース > ループバックインタフェース の順にメニューをクリックし、以下の画面を表示します。



図 9-15　ループバックインタフェース 画面

画面に表示される項目：

項目	説明
インタフェースループバック	ループバックするインタフェース ID を入力します。 • 設定可能範囲：1-8

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

ループバックインタフェースの編集

「編集」をクリックして、以下の画面を表示します。

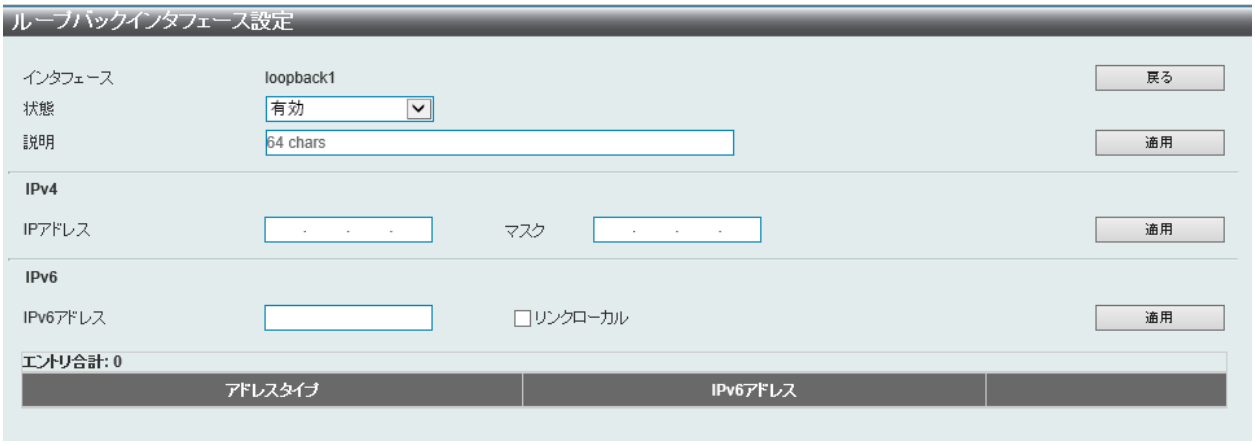


図 9-16　ループバックインタフェース設定（編集）画面

画面に表示される項目：

項目	説明
状態	ループバックインタフェースを有効 / 無効に指定します。
説明	ループバックインタフェースの説明を入力します。（64 文字以内）
IP アドレス	ループバックインタフェースの IPv4 アドレスを入力します。
マスク	ループバックインタフェースに割り当てるサブネットマスクを入力します。
IPv6 アドレス	ループバックインタフェースの IPv6 アドレスを入力します。 注意　64 ビットを超える IPv6 アドレスは入力できません。
リンクローカル	指定した IPv6 アドレスをリンクローカル IPv6 アドレスとして指定します。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックして、前のページに戻ります。
「削除」をクリックし、エントリを削除します。

Null インタフェース

Null インタフェースを設定します。

L3 機能 > インタフェース > Null インタフェース の順にメニューをクリックし、以下の画面を表示します。



図 9-17　Null インタフェース画面

画面に表示される項目：

項目	説明
インタフェース Null	Null インタフェース ID を指定します。「0」のみ指定可能です。
説明	「編集」をクリックし Null インタフェースの説明を入力します。（64 文字以内）

「適用」をクリックして、設定内容を適用します。
「編集」をクリックして、指定エントリの編集を行います。

UDP Helper

L3 機能 > UDP Helper
IP 転送プロトコルの設定を行います。

IP 転送プロトコル

本項目では、IP 転送プロトコルの設定、表示を行います。本機能は指定の UDP サービスタイプのパケットの転送を有効にします。

L3 機能 > UDP Helper > IP 転送プロトコルの順にメニューをクリックし、以下の画面を表示します。

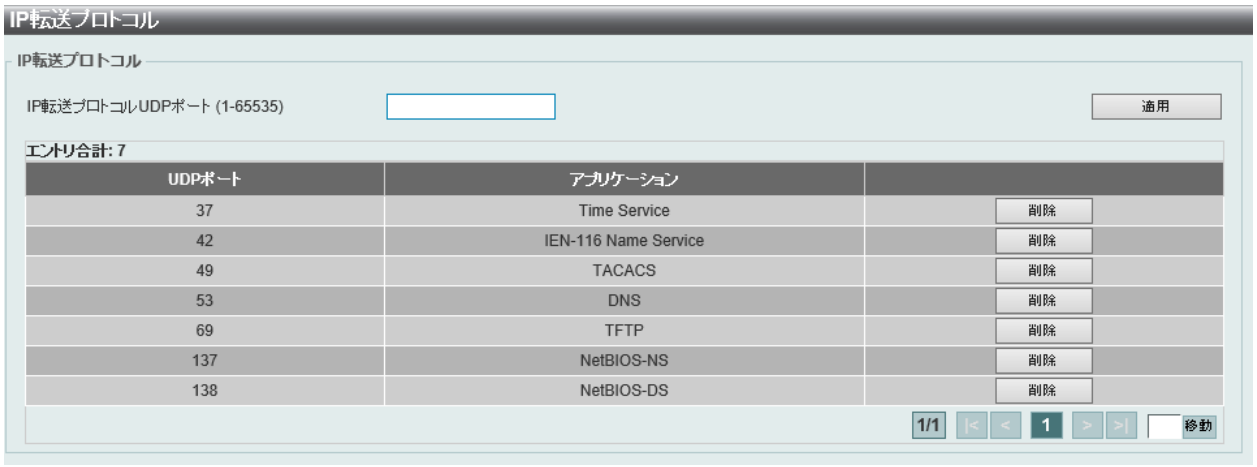


図 9-18　IP 転送プロトコル 画面

画面に表示される項目：

項目	説明
IP 転送プロトコル UDP ポート	転送する UDP サービスの宛先ポートを指定します。 • 設定可能範囲：1-65535

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IP ヘルパーアドレス

本項目では UDP ブロードキャストパケットを転送するターゲットアドレスの追加 / 削除を指定します。
本機能は IP アドレスがアサインされた受信インタフェースのみ有効です。システムは以下の制限をクリアした場合のみパケットを転送します。

- 宛先 MAC アドレスがブロードキャストアドレスである。
- 宛先 IP アドレスがオールワンブロードキャストである。
- パケットが IPv4 UDP パケットである。
- 「IP TTL 値」が「2」以上である。

L3 機能 > UDP Helper > IP ヘルパーアドレスの順にメニューをクリックし、以下の画面を表示します。



図 9-19　IP ヘルパーアドレス 画面

画面に表示される項目：

項目	説明
VLAN インタフェース	VLAN インタフェース ID（1-4094）を指定します。
ヘルパーアドレス	UDP ブロードキャストパケットの転送のためのターゲット IPv4 アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPv4 スタティック / デフォルトルート

IPv4 スタティック / デフォルトルートの設定を行います。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。

IPv4 スタティックルートが設定されると、スイッチによってネクストホップルータに ARP リクエストパケットが送信されます。スイッチに対しネクストホップから ARP の応答が返されると、ルートが有効になります。ただし、ARP エントリが既に存在している場合には、ARP 要求は送信されません。

スイッチはフローティングスタティックルートをサポートしています。ユーザは、異なるネクストホップを持つ代替のスタティックルートを作成することができます。この 2 個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートが失われた場合、バックアップルートがアクティブになり、トラフィックの転送を開始します。本スイッチのフォワーディングテーブル内のエントリは、IP アドレス、サブネットマスクおよびゲートウェイを使用して作成します。

L3 機能 > IPv4 スタティック / デフォルトルート の順にメニューをクリックし、以下の画面を表示します。



図 9-20　IPv4 スタティック / デフォルトルート 画面

画面に表示される項目：

項目	説明
IP アドレス	スタティックルートに割り当てる IPv4 アドレスを入力します。 「デフォルトルート」をチェックすると、IPv4 アドレスとしてデフォルトルートを使用します。
マスク	このルートのサブネットマスクを入力します。
ゲートウェイ	このルートのゲートウェイ IP アドレスを入力します。
Null インタフェース	Null インタフェースを有効 / 無効に設定します。
バックアップステート	バックアップオプションを選択します。 • 「プライマリ」- 宛先へのプライマリルートとしてルートを指定します。 • 「バックアップ」- 宛先へのバックアップルートとしてルートを指定します。 • 「加重」-「0」より大きく、最大パス数より小さい重みの数値を指定します。本数値はルーティングテーブルのルートパスの複製（複数コピー）に使用され、これによりトラフィックルーティングの際にパスが当たる確率が上がります。「加重」選択後に表示される空欄に数値（1-4）を指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定のエントリを削除します。

IPv4 ルートテーブル

IPv4 ルートテーブルの設定と表示を行います。

L3 機能 > IPv4 ルートテーブルの順にメニューをクリックし、以下の画面を表示します。

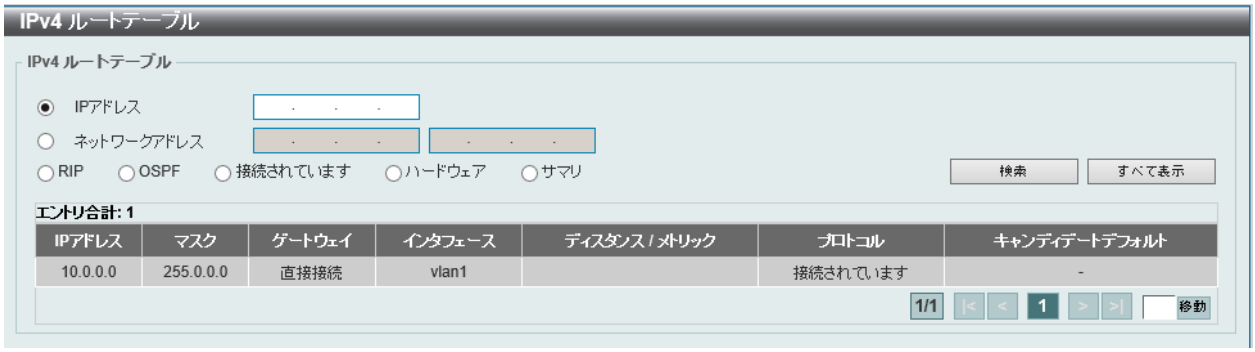


図 9-21　IPv4 ルートテーブル画面

画面には以下の項目が表示されます。

項目	説明
IP アドレス	表示するルートの宛先 IP アドレスを指定します。
ネットワークアドレス	表示するルートの宛先ネットワークアドレスを指定します。 1 つ目の入力欄にネットワークプレフィックス、2 つ目の入力欄にネットワークマスクを入力します。
RIP	RIP ルートのみ表示します。
OSPF	OSPF ルートのみ表示します。
接続されています	接続されたルートのみ表示します。
ハードウェア	ハードウェアチップに記録されたルートのみ表示します。
サマリ	スイッチに設定されているルートソースの概要と数が表示されます。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

IPv6 スタティック / デフォルトルート

IPv6 スタティックルートまたはデフォルトルートを表示および設定します。

L3 機能 > IPv6 スタティック / デフォルトルート の順にメニューをクリックし、以下の画面を表示します。

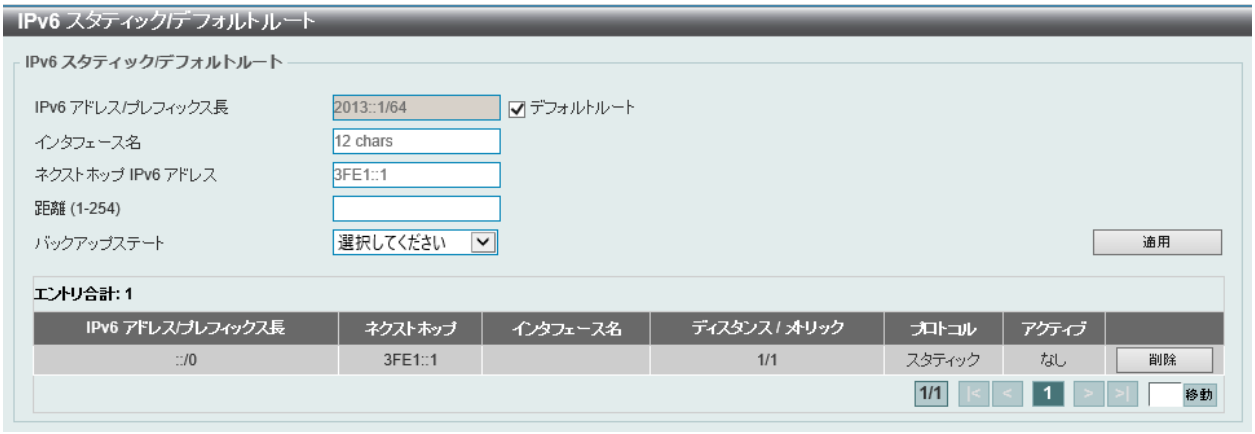


図 9-22　IPv6 スタティック / デフォルトルート 画面

画面に表示される項目：

項目	説明
IPv6 アドレス / プレフィックス長	スタティックルートに割り当てる IPv6 アドレスおよびプレフィックスを入力します。 「デフォルトルート」をチェックすると、このルートをデフォルトルートとして使用します。
インタフェース名	このルートのゲートウェイ IP アドレスを入力します。
ネクストホップ IPv6 アドレス	ネクストホップ IPv6 アドレスを指定します。
距離	スタティックルートの管理ディスタンスを指定します。小さい値の方が、より適切なルートを意味します。 • 設定可能範囲：1-254 • 初期値：1
バックアップステート	バックアップオプションを選択します。 • 「プライマリ」- 宛先へのプライマリルートとしてルートを指定します。 • 「バックアップ」- 宛先へのバックアップルートとしてルートを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定のエントリを削除します。

IPv6 ルートテーブル

現在の IPv6 ルーティングテーブルを表示します。

L3 機能 > IPv6 ルートテーブルの順にメニューをクリックし、以下の画面を表示します。

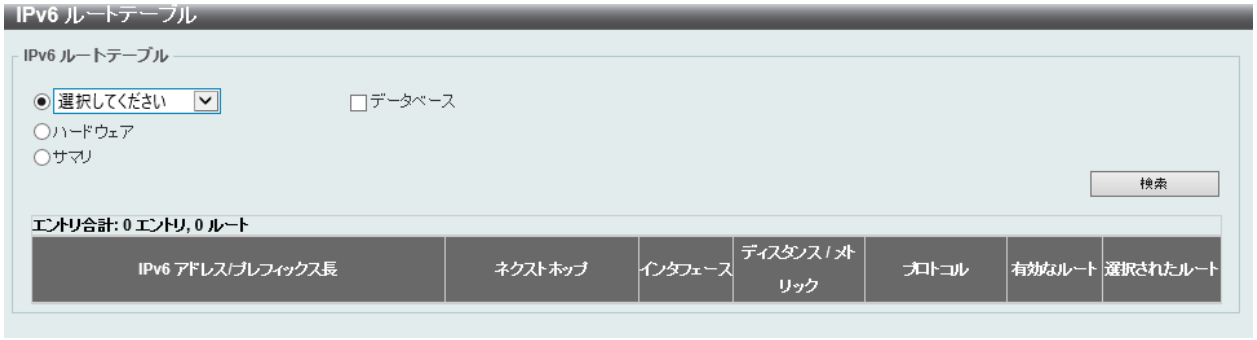


図 9-23　IPv6 ルートテーブル画面

画面には以下の項目が表示されます。

項目	説明
IPv6 アドレス	プルダウンメニューから本項目を選択し、IPv6 アドレスを入力します。
IPv6 アドレス / プレフィックス長	プルダウンメニューから本項目を選択し、ルートの IPv6 アドレスとプレフィックスを指定します。「Longer プレフィックス」を指定するとプレフィックス長と同等、もしくはそれよりも長いプレフィックスの IPv6 ルートを表示します。
インタフェース名	プルダウンメニューから本項目を選択し、表示するインタフェース名を指定します。
接続されています	接続されたルートのみ表示します。
RIPng	RIPng ルートエントリのみ表示します。
OSPFv3	OSPFv3 ルートエントリのみ表示します。
データベース	ベストルートだけでなく、ルーティングデータベース内のすべてのエントリを表示します。
ハードウェア	ハードウェアチップに記録されたルートのみ表示します。
サマリ	スイッチに設定されているルートソースの概要と数が表示します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

ルート優先

ルート優先度を設定します。
ルート信頼度レーティングを示すディスタンスを設定します。ルートのディスタンス値が小さいほど優先度が高くなります。

L3 機能 > ルート優先 の順にメニューをクリックし、以下の画面を表示します。



図 9-24　ルート優先画面

画面に表示される項目：

項目	説明
デフォルトディスタンス	デフォルトルートの管理ディスタンスを指定します。 • 設定可能範囲：1-255 • 初期値：1
ディスタンススタティック	スタティックルートの管理ディスタンスを指定します。 • 設定可能範囲：1-255 • 初期値：60

「適用」をクリックし、設定を適用します。

ECMP 設定

ECMP ルーティング設定を行います。
負荷分散ハッシュアルゴリズムを設定し、同じ宛先への複数のパスのネクストホップエントリを決定するために使用されます。

L3 機能 > ECMP 設定をクリックし、以下の画面を表示します。

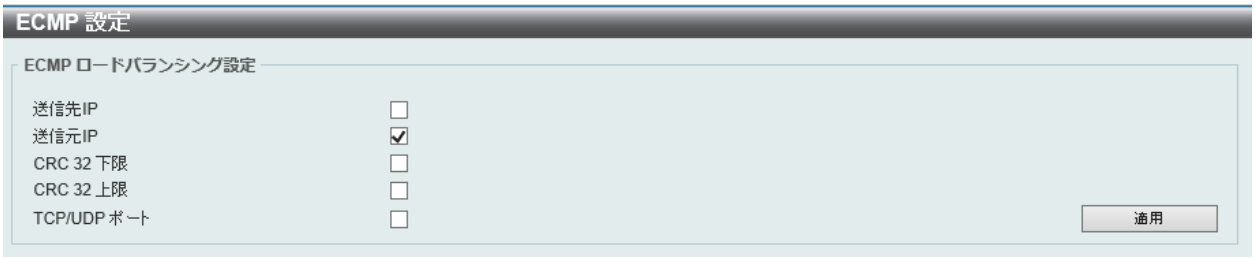


図 9-25　ECMP 設定画面

画面に表示される項目：

項目	説明
ECMP ロードバランシング設定	
送信先 IP	ECMP ハッシュ鍵として宛先 IP を使用します。
送信元 IP	ECMP ハッシュアルゴリズムとして送信元 IP の最下位ビットを使用します。
CRC 32 下限	ECMP ハッシュアルゴリズムとして CRC-32 の下位ビットを使用します。
CRC 32 上限	ECMP ハッシュアルゴリズムとして CRC-32 の上位ビットを使用します。
TCP/UDP ポート	ECMP ハッシュ鍵として TCP または UDP ポート番号を使用します。

「適用」をクリックして、設定内容を適用します。

IPv6 General プレフィックス

本項目では、VLAN インタフェース IPv6 汎用プレフィックスの設定、表示を行います。

L3 機能 > IPv6 General プレフィックスをクリックし、以下の画面を表示します。



図 9-26　IPv6 General プレフィックス画面

画面に表示される項目：

項目	説明
VLAN インタフェース	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
プレフィックス名	IPv6 汎用プレフィックスエントリ名を指定します。（12 文字以内）
IPv6 アドレス	IPv6 アドレスとプレフィックス長を指定します。 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」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

URPF 設定

Unicast Reverse Path Forwarding（URPF）の設定と表示を行います。
ネットワーク上で攻撃を開始する一般的な方法の 1 つとして、IPv4/IPv6 送信元アドレススプーフィングの利用があります。この方法では、ターゲットによって信頼されている / 既知の送信元アドレスを使用してトラフィックがネットワークに送信されます。保護が行われていない場合、組織のネットワークはトラフィックを許可し、様々な種類の攻撃にさらされる可能性があります。ユニキャスト RPF は、ルータを通過する不正な形式または偽造された IPv4/IPv6 送信元アドレスによって引き起こされる問題を軽減するのに役立ちます。

L3 機能 > URPF 設定の順にメニューをクリックして以下の画面を表示します。



図 9-27　URPF 設定画面

画面に表示される項目：

項目	説明
URPF グローバル設定	
URPF ステート	URPF を有効 / 無効に指定します。 **注意** 有効になると、まずハードウェアルーティングテーブルの「Session Initiation Protocol」（SIP）を使った検出、その後「Dynamic Inspection Protocol」（DIP）を使用した検出が必要になります。このプロセスでは、テーブルは半分に分割され、IP ルーティングテーブルは半分に削減されます。本設定はコンフィグを保存し、スイッチを再起動した後に有効になります。
URPF ポートデフォルト設定	
ユニット	設定を行うユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
経由到達可能	デフォルトの到達可能な via 設定（RX）が使用されます。
IP アクセスリスト名	デフォルトの IP アクセスリスト設定を使用します。
IPv6 アクセスリスト名	デフォルトの IPv6 アクセスリスト設定を使用します。
URPF ポート設定	
ユニット	設定を行うユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を設定します。
経由到達可能	「経由到達可能」のオプションを選択します。 • 「Any」- 送信元アドレスがルーティングテーブルに存在しているか確認します。（Loose モード）
IP アクセスリスト名	URPF チェックに使用する IP アクセスリスト名を指定します。（32 文字以内）
IPv6 アクセスリスト名	URPF チェックに使用する IPv6 アクセスリスト名を指定します。（32 文字以内）

「適用」をクリックし、設定を適用します。

RIP

L3 機能 > RIP
RIP（Routing Information Protocol）は、ルーティングプロトコルの 1 つです。通信機器間の最短経路を割り出すために使用します。

RIP 設定

IP インタフェースに RIP 設定を行います。

L3 機能 > RIP > RIP 設定の順にメニューをクリックし、以下の画面を表示します。



図 9-28　RIP 設定画面

画面に表示される項目：

項目	説明
RIP グローバル設定	
RIP ステート	RIP の状態を有効または無効にします。初期値：無効
再配布設定	
再配布	次の手順で指定します。 1. RIP 再配布機能を有効 / 無効に指定します。 2. RIP に再配布されるルーティングプロトコル（ドメイン）を「接続されています」「OSPF」「スタティック」から指定します。「スタティック」は IP スタティックルートを再配布します。「接続されています」はインタフェースの IP アドレス設定の際に自動的に構築するルートを意味します。 3. 再配布ルートのメトリック値（0-16）を指定します。 4. 現在のルートプロトコルに再配布するルートのフィルタリングに使用するためのルートマップ名を指定します。指定しない場合、全てのルートが再配布されます。
RIP 設定	
更新タイマ	RIP アップデートメッセージを送信する間隔を指定します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
無効なタイマ	無効タイマ値を入力します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：180（秒）
フラッシュタイマ	Flush タイマ値を入力します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）
デフォルトメトリック	初期メトリック値を指定します。他のルーティングプロトコルからのルートの再配布に使用されます。 再配布されるルートは他のプロトコルに学習され、RIP との互換性がないメトリックになる場合があります。メトリックの指定により、メトリックを同期します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16

項目	説明
バージョン	すべてのインタフェースで初期バージョンとして使用されるグローバル RIP バージョンを指定します。 「初期値」を指定すると初期値を使用します。初期値では v1/v2 どちらも受信しますが、v1 のみ送信します。 • 選択肢：「v1（RIPv1）」「v2（RIPv2）」
距離	RIRIP の管理ディスタンスを指定します。小さい値ほど適切なルートを意味します。 「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-255 • 初期値：100
グローバルパッシブインタフェース	グローバルパッシブインタフェース機能を有効 / 無効に設定します。 「初期値」を指定すると初期値である「無効」を使用します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

RIP 配布リスト

RIP ディストリビュートリストの設定を行います。

L3 機能 > RIP > RIP 配布リストの順にメニューをクリックし、以下の画面を表示します。

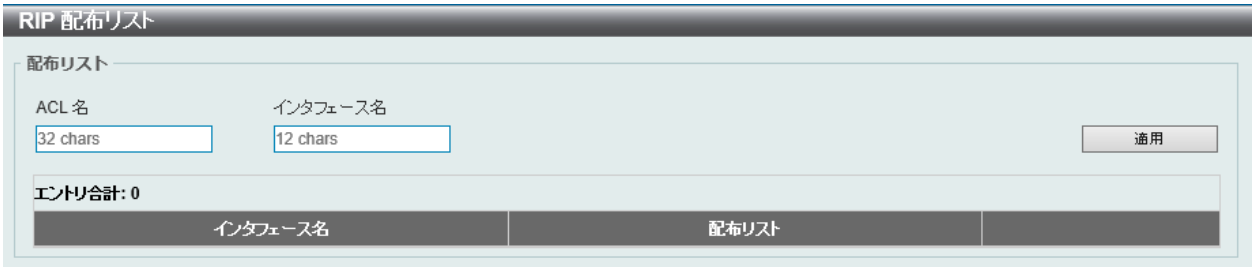


図 9-29　RIP 配布リスト画面

画面に表示される項目：

項目	説明
ACL 名	アクセスリスト名を入力します。（32 文字以内）
インタフェース名	インタフェース名を 12 字以内で入力します。（12 文字以内）

「適用」をクリックし、設定を適用します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

RIP インタフェース設定

RIP インタフェースの設定を行います。

L3 機能 > RIP >RIP インタフェース設定の順にメニューをクリックし、以下の画面を表示します。



図 9-30　RIP インタフェース設定画面

画面に表示される項目：

項目	説明
ネットワーク	RIP に使用される IPv4 ネットワークアドレスアドレスを指定します。 本項目で指定するネットワークのサブネットを持つインタフェースの RIP が有効になります。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。

「編集」をクリックすると以下の画面が表示されます。

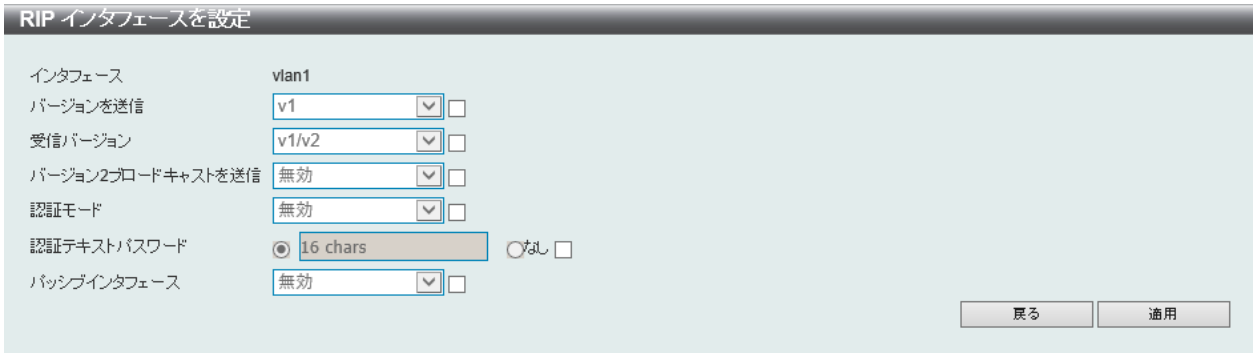


図 9-31　RIP インタフェースを設定画面

画面に表示される項目：

項目	説明
バージョンを送信	送信する RIP パケットのバージョンを選択します。 • 選択肢：「v1」「v2」
受信バージョン	受信する RIP パケットのバージョンを選択します。 • 選択肢：「v1」「v2」「v1/v2」
バージョン2ブロードキャストを送信	RIP バージョン 2 の更新パケットを、マルチキャストパケットではなくブロードキャストパケットとして送信することを有効 / 無効に設定します。
認証モード	認証モードを選択します。 •「無効」- インタフェースで RIP 認証を無効にします。 •「テキスト」- インタフェースで RIP 認証を有効にします。
認証テキストパスワード	認証を有効にした場合、テキストパスワードを入力します。（16 文字以内） 空のパスワードを設定する場合は「なし」を選択します。
パッシブインタフェース	パッシブインタフェース機能を有効 / 無効に設定します。 パッシブインタフェース機能は、インタフェースでのルーティングアップデートの送信を無効にするために使用されます。スイッチは、インタフェースを介してマルチキャスト RIP パケットを送信しませんが、このインタフェースで受信した他のルータからの RIP パケットは引き続き処理されます。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックし、前の画面に戻ります。

RIP データベース

「Routing Information Protocol」（RIP）ルーティングデータベースの設定を行います。サマリアドレスは、子ルートがサマライズ（要約）されている場合、データベース内に表示されます。最後のサマリアドレスの子ルートが無効になると、サマリアドレスはルーティングテーブルから削除されます。

L3 機能 > RIP > RIP データベースの順にメニューをクリックし、以下の画面を表示します。



図 9-32　RIP データベース画面

画面に表示される項目：

項目	説明
ネットワークアドレス	ネットワークのサブネットプレフィックスとプレフィックス長を指定します。

「適用」をクリックして、設定内容を適用します。
「すべて表示」をクリックして、すべてのエントリを表示します。

RIPng

スイッチは、RIPng（Routing Information Protocol next generation）をサポートしています。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用に使用されます。

RIPng 設定

本画面では、RIPng の設定を行います。

L3 機能 > RIPng > RIPng 設定の順にメニューをクリックして以下の画面を表示します。



図 9-33　RIPng 設定画面

画面に表示される項目：

項目	説明
RIPng グローバル設定	
グローバルステート	RIPng の状態を有効または無効にします。初期値は無効です。
RIPng 設定	
デフォルトメトリック	初期メトリック値を指定します。他のルーティングプロトコルからの再配布されたルートの初期メトリック値を指定します。再配布されるルートは他のプロトコルに学習され、RIPng との互換性がないメトリックになる場合があります。メトリックを再指定することにより、メトリックを同期させることができます。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-16 • 初期値：0
距離	RIPng のアドミニストレーティブディスタンスを指定します。これは、ルートの信頼レートを意味します。小さい値ほど優先的なルートを意味します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-254 • 初期値：120
更新タイマ	RIP アップデートメッセージを送信する間隔値を入力します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：5-65535（秒） • 初期値：30（秒）
無効なタイマ	無効（Invalid）タイマの値を入力します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：180（秒）
フラッシュタイマ	フラッシュタイマの値を入力します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：120（秒）
ポイズンリバース	ポイズンリバース（Poison Reverse）を有効 / 無効に設定します。 本機能が有効の場合、インタフェースから学習したルートは到達不能メトリックとともに同じインタフェースに通知されます。

項目	説明
スプリットホライズン	スプリットホライズン（Split Horizon）を有効 / 無効に設定します。 本機能が有効の場合、インタフェースから学習したルートは同じインタフェースに通知されません。
再配布設定	
プロトコル	ルートを再配布するプロトコルを指定します。 「スタティック」は IPv6 スタティックルートを再配布します。 「接続されています」は IPv6 インタフェースの IP アドレス設定の際に自動的に構築するルートを意味します。
メトリック	再配布されるルートのメトリックとして使用される値を指定します。「初期値」は初期メトリック値を使用します。 • 設定可能範囲：0-16

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。

RIPng インタフェース

RIPng インタフェースの設定を行います。

L3 機能 > RIPng > RIPng インタフェースの順にメニューをクリックして以下の画面を表示します。



図 9-34　RIPng インタフェース設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	RIPng 設定の VLAN インタフェースを入力します。 「すべてのインタフェース」を選択すると全インタフェースで適用します。 • 設定可能範囲：1-4094
状態	指定の VLAN インタフェースの IPv6 RIP 機能を有効 / 無効に指定します。
メトリックオフセット	指定インタフェースで受信する IPv6 RIP ルートのメトリック値に本値を追加します。メトリックはホップ数を参照します。初期値では、IPv6 RIP ルートを受信すると、ルーティングテーブルに挿入される前にメトリック値「1」がルートに追加されます。この設定を使用すると、各インタフェースで受信するルートのメトリックおよびルートの優先度を調整することができます。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-16
パッシブインタフェース	パッシブインタフェースを有効 / 無効に設定します。本設定が無効になると、ルータはインタフェースを介して RIPng を送信しません。ただし、インタフェースで受信した他のルータからの RIPng パケットは、引き続き処理されます

「適用」をクリックして、設定内容を適用します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

RIPng データベース

RIPng データベースの設定を行います。

L3 機能 > RIPng > RIPng データベース の順にメニューをクリックして以下の画面を表示します。



図 9-35　RIPng データベース画面

画面に表示される項目：

項目	説明
IPv6 アドレス / プレフィックス長	IPv6 アドレスを入力します。

「検索」をクリックして、入力したエントリを検出します。

OSPF

L3 機能 > OSPF

OSPF の設定を行います。OSPF（Open Shortest Path First）はリンクステート型のルーティングプロトコルです。
ネットワーク内のどのルータとどのルータが隣接しているかという接続情報（リンクステート）を基に経路を選択します。

OSPFv2

L3 機能 > OSPF > OSPFv2

OSPFv2 プロセス設定

OSPFv2 プロセスを設定、表示します。

L3 機能 > OSPF > OSPFv2 > OSPFv2 プロセス設定の順にメニューをクリックし、以下の画面を表示します。



図 9-36　OSPFv2 プロセス設定 画面

「適用」をクリックして、設定内容を適用します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「編集」をクリックすると、以下の画面が表示されます。

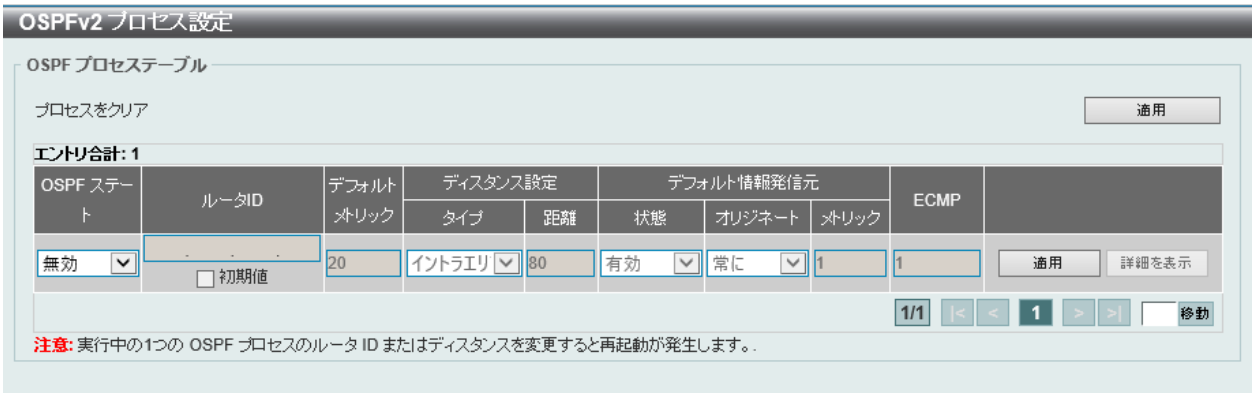


図 9-37　OSPFv2 プロセス設定（編集）画面

画面に表示される項目：

項目	説明
OSPF ステート	OSPFv2 機能を有効 / 無効に設定します。
ルータ ID	IPv4 アドレス形式でルータ ID を指定します。 ルータ ID は、OSPF プロトコルを実行する各ルータにアサインされる 32 ビットの数値です。AS 内のルータを固有に識別します。AS 内で、各ルータは一意のルータ ID を持ちます。「初期値」にチェックを入れると、デフォルトルータ ID を使用します。
デフォルトメトリック	初期メトリック値を指定します。 • 設定可能範囲：1-16777214
タイプ	ディスタンス設定の種類を指定します。 • 「内部 - エリア」- OSPF インターエリアルートのディスタンスを指定します。 • 「イントラエリア」- OSPF イントラエリアルートのディスタンスを指定します。 • 「外部 -1」- タイプ 1 メトリックを使用して、OSPF 外部タイプ 5 およびタイプ 7 ルートの距離を指定します。 • 「外部 -2」- タイプ 2 メトリックを使用して、OSPF 外部タイプ 5 およびタイプ 7 ルートの距離を指定します。

項目	説明
距離	管理ディスタンス値を指定します。 • 設定可能範囲：1-255
状態	初期「オリジネート」情報を有効 / 無効に指定します。 AS に向かう初期外部ルート（タイプ -5 LSA）ネットワーク「0.0.0.0」の生成に使用されます。
オリジネート	「オリジネート」のオプションを指定します。 • 選択肢：「常に」「なし」 「常に」を指定すると、再配布されたルート内にデフォルトルートが存在していても、常にデフォルトルートを生成し続けます。
メトリック	生成されたデフォルトルートにかかるコストを入力します。指定しない場合、初期メトリックは「1」になります。 • 設定可能範囲：1-65535
ECMP	ECMP 値を指定します。 • 設定可能範囲：1-4

「適用」をクリックして、設定内容を適用します。

「詳細を表示」をクリックすると、以下の画面が表示されます。



図 9-38　OSPFv2 プロセス設定（詳細を表示）　画面

画面に表示される項目：

項目	説明
RFC 1583 互換	RFC1583 の実装を有効 / 無効に設定します。
RFC 3509 互換	RFC3509 の実装を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。
「OK」をクリックして、設定内容を適用します。

OSPFv2 配布リスト

OSPFv2 配布リストの設定、表示を行います。

L3 機能 > OSPF > OSPFv2 >OSPFv2 配布リストの順にメニューをクリックし、以下の画面を表示します。



図 9-39　OSPFv2 配布リスト画面

画面に表示される項目：

項目	説明
ACL 名	アクセスリスト名を入力します。(32 文字以内)
インタフェース名	インタフェース名を入力します。(12 文字以内)

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

OSPFv2 パッシブインタフェース設定

OSPFv2 パッシブインタフェースの設定、表示を行います。

L3 機能 > OSPF > OSPFv2 > OSPFv2 パッシブインタフェース設定の順にメニューをクリックし、以下の画面を表示します。

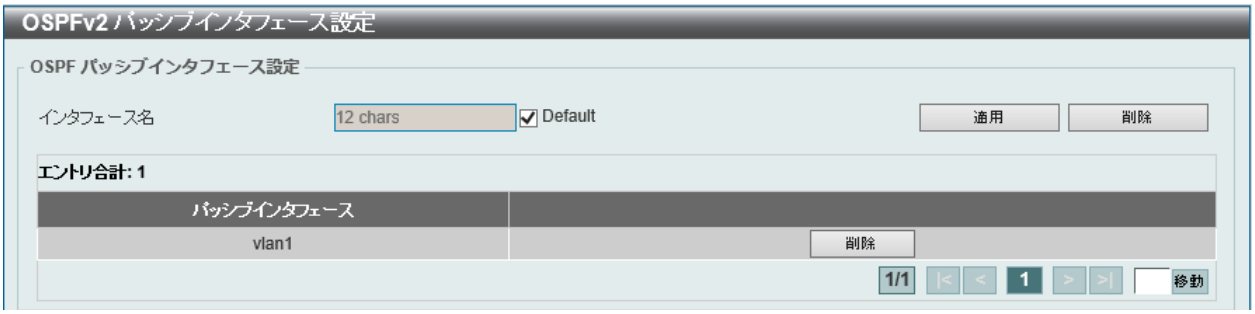


図 9-40　OSPFv2 パッシブインタフェース設定 画面

画面に表示される項目：

項目	説明
インタフェース名	使用するインタフェース名を指定します。(12 文字以内) 「初期値」を選択すると全ての有効なインタフェースを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

OSPFv2 エリア設定

本項目では OSPFv2 エリア設定を行います。

L3 機能 > OSPF > OSPFv2 > OSPFv2 エリア設定の順にメニューをクリックし、以下の画面を表示します。



図 9-41　OSPFv2 エリア設定画面

画面に表示される項目：

項目	説明
OSPF エリア設定	
OSPF エリア ID	OSPFv2 エリア識別子を選択して入力します。 IP アドレス形式（xxx.xxx.xxx.xxx）または 10 進数値形式（0-4294967295）で指定できます。インタフェースで構成されたサブネットがここで指定されたネットワーク範囲内にある場合に、エリアはインタフェース上に作成されます。
範囲	Area Border Router（ABR）の OSPF ルートを集約します。
NSSA	OSPF エリアを Not-So-Stubby Area（NSSA）として割り当てます。
スタブ	Stub エリアとして OSPF エリアを設定します。
エリア 範囲 IP	OSPF エリアに対応するネットワークを識別する IP アドレス範囲を入力します。
エリア 範囲 マスク	OSPF エリアに対応するネットワークを識別するネットマスク範囲を入力します。
広告	広告（Advertisement）を有効または無効にします。 • 「広告」- 指定されたアドレス範囲の「Type-3 summary Link-State Advertisement（LSA）」を通知します。 • 「広告なし」-「Type-3 summary LSA」の通知を抑制します。コンポーネントのルートは存在しています。
デフォルトコスト	「NSSA」または「スタブ」選択時に有効です。 デフォルトのコスト値を入力します。スタブエリアおよび Not-So-Stubby エリアに挿入される Type-3 デフォルトルートに関連するコストです。（設定可能範囲：0-665535） • 「初期値」- デフォルトのコスト値を使用します。 • 「サマリなし」- このエリアに集約ルートを挿入しません。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。

エントリをダブルクリックすると、エントリの詳細情報が表示されます。

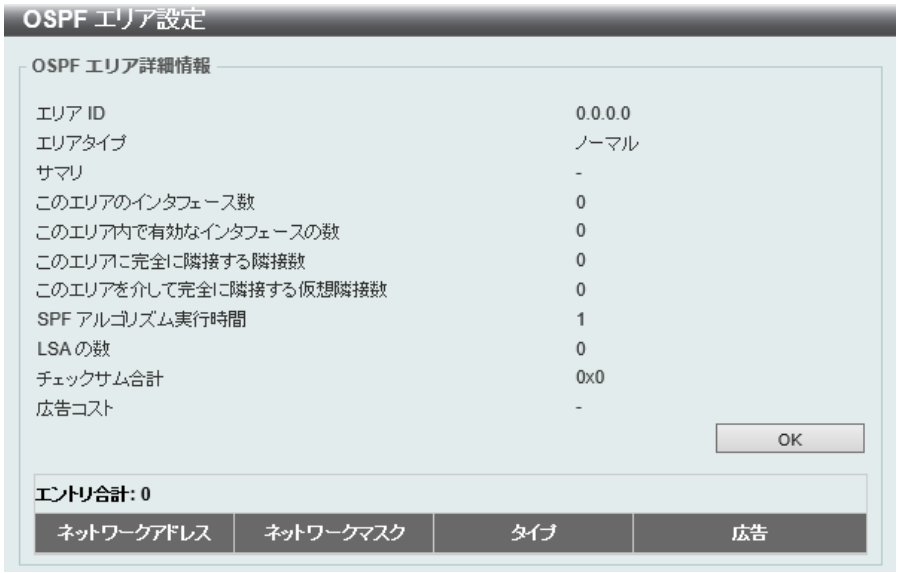


図 9-42　OSPFv2 エリア設定（詳細情報）画面

OSPFv2 インタフェース設定

OSPFv2 インタフェースを設定します。

L3 機能 > OSPF > OSPFv2 > OSPFv2 インタフェース設定の順にメニューをクリックし、以下の画面を表示します。

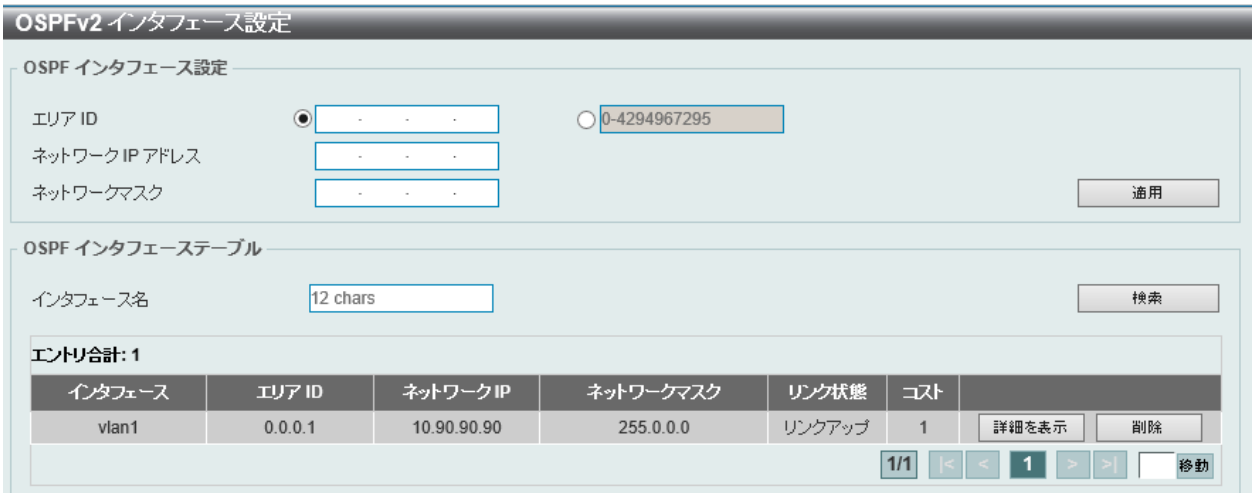


図 9-43　OSPFv2 インタフェース設定画面

画面に表示される項目：

項目	説明
OSPF インタフェース設定	
エリア ID	OSPFv2 ドメイン内の OSPF エリアを識別する 32 ビットの番号（IP アドレスと同じ xxx.xxx.xxx.xxx 形式）または、10 進数（0-4294967295）を指定します。
ネットワーク IP アドレス	IPv4 アドレスを指定します。
ネットワーク マスク	IPv4 サブネットマスクを指定します。
OSPF インタフェーステーブル	
インタフェース名	インタフェース名を指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「検索」をクリックして、入力したインタフェースを検出します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。

編集するポートの「詳細を表示」をクリックし、以下の画面を表示します。

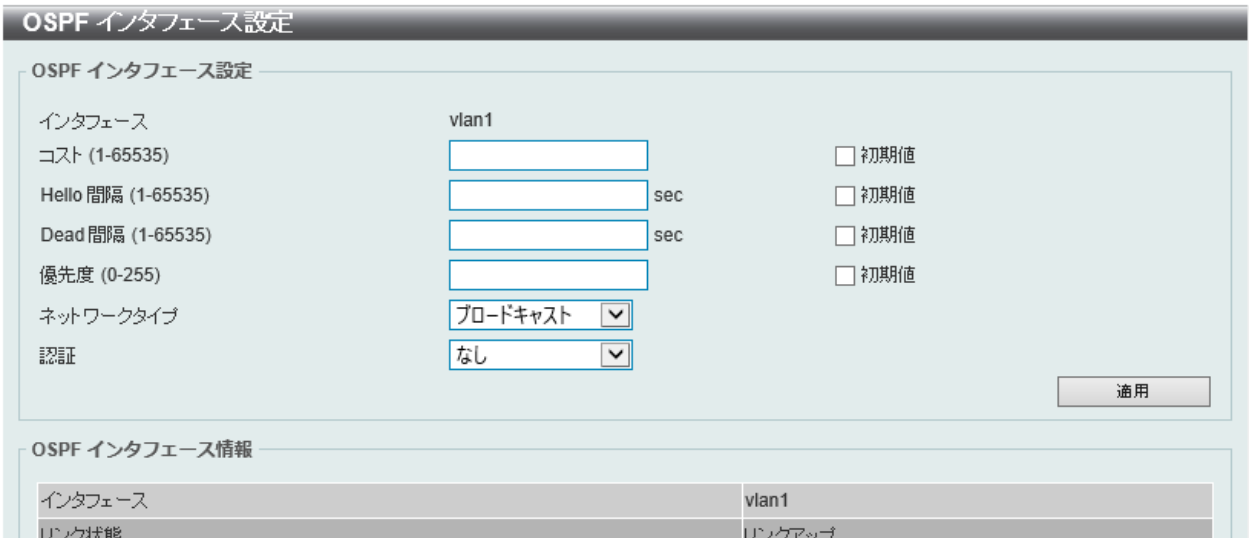


図 9-44　OSPFv2 インタフェース設定（詳細を表示）画面

画面に表示される項目：

項目	説明
コスト	コストの値を指定します。インタフェースのコストはインタフェース上のパケット送信のオーバーヘッドを反映します。 コストはルータリンク通知の中でリンクコストとして通知されます。 「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1
Hello 間隔	Hello 間隔（Hello Interval）の値を指定します。 この値は、Hello パケットでアドバタイズされます。特定のネットワーク上のすべてのすべてのルータで同じ値に設定します。この値を短くするとトポロジの変更をより迅速に検出できますが、ルーティングトラフィックが多く生成されることでルーティングが不安定になる可能性があります。「初期値」をチェックすると初期値を使用します。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead 間隔	隣接ルータが Hello パケットを最後に受信してから、送信側のルータがダウンしたと判断するまでの時間を指定します。この値は、Hello パケットでアドバタイズされます。特定のネットワーク上のすべてのルータで同じである必要があります。この値を小さくすると、トポロジの変更をより迅速に検出できますが、ルーティングが不安定になる可能性があります。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
優先度	代表ルータ選出のプライオリティ（0-255）を指定します。2 台のルータが代表ルータになろうとすると、ルータの優先度が高いルータが代表ルータに選出されます。ルータの優先順位が同じ場合は、ルータ ID の大きいルータが優先されます。 ルータプライオリティ 0 が指定されると、スイッチはそのネットワークの代表ルータとして選出されなくなります。 • 設定可能範囲：0-255
ネットワークタイプ	ネットワークタイプを指定します。 •「ブロードキャスト」- ネットワークタイプをブロードキャストとして指定します。ブロードキャストネットワークでは指定ルータ（DR）とバックアップ指定ルータ（BDR）のみが他の全てのルータのネイバになることが可能です。 •「ポイントツーポイント」- ネットワークタイプを「point-to-point」として指定します。「point-to-point」ネットワークでは、通信可能な 2 台のルータのみがネイバになることが可能です。
認証	認証方法を選択します。 • 選択肢：「なし」「簡易パスワード」「MD5」
パスワード	「認証」で「簡易パスワード」を選択した場合、シンプルテキストのパスワードを入力します。（8 文字以内） パスワードにはスペースを含めることはできません。 このパスワード情報は、ルータがルーティングプロトコルパケットを送信する際の OSPF ヘッダに挿入されます。各インタフェースのそれぞれのネットワークに対し、パスワードを設定します。同じネットワーク上のルータには同じパスワードを設定し、OSPF ルーティングデータが交換できるようにします。同じルーティングドメインのルータには同じパスワードを設定してください。
MD5 キー ID	MD5 暗号キー ID を入力します。 • 設定可能範囲：1-255
MD5	「認証」で「MD5」を選択した場合、MD5 キーを指定します。（16 文字以内）スペースなしの英数字文字列で指定します。 MD5 モードでは OSPF メッセージ送信者は送信メッセージのメッセージダイジェストキーを基にメッセージのダイジェストを解析します。メッセージダイジェストとキー ID はパケット内でエンコードされます。パケットの受信者は、同じキー ID に関連するローカル定義されたメッセージダイジェストキーを基に、メッセージ中のダイジェストを検証します。 ネイバルータ上の同じキー ID は、同じキー文字列で定義されている必要があります。同じインタフェースのネイバルータに対しては同じキーを設定し、お互いに OSPF パケットが交換できるようにします。 通常、同じインタフェースのすべてのネイバルータは同じキーを使用します。MD5 ダイジェストモードでは、現在のメッセージ交換を中断することなく、ユーザは新しいキーにロールオーバーできます。 ルータが古いキーを使用して隣接ルータと OSPF パケットを交換している処理中の場合、ユーザが新しいキーを設定すると、ルータは古いキーと新しいキーの両方に重複したパケットを送信し、ロールオーバープロセスを開始します。 ネットワーク上のすべてのルータが新しいキーを学習するまで、重複したパケットが送信されます。 ロールオーバープロセスが完了した後、ユーザは古いキーを削除して、ルータが古いキーを使用してルータと通信できないようにする必要があります。

「適用」をクリックして、設定内容を適用します。

OSPFv2 再配布設定

本項目では OSPFv2 再配布（redistribution）について、設定、表示します。外部ルートは ASBR により、「Type-5」外部ルートとしてノーマルエリアに、「Type-7」外部ルートとして NSSA スタブエリアに再配布されます。
再配布外部ルートが「Type-1」の場合、メトリックは内部メトリックを意味します。再配布外部ルートが「Type-2」の場合、メトリックは外部メトリックを意味します。内部メトリックは、自身から再配布ルータまでのルートのコストに加え、宛先に到達するためにアドバタイズされたコストを考慮します。初期メトリックとしてメトリック値が設定されていない場合、他のプロトコルから再配布されたルートはメトリック値 20 を取得します。

L3 機能 > OSPF > OSPFv2 > OSPFv2 再配布設定 の順にメニューをクリックし、以下の画面を表示します。



図 9-45　OSPFv2 再配布設定 画面

画面に表示される項目：

項目	説明
プロトコル	再配布される送信元プロトコルを指定します。OSPF のようなルーティングプロトコルの場合、自立したシステムに外部として再配布されます。 • 選択肢：「接続されています」「スタティック」「RIP」
メトリックタイプ	メトリックの種類を指定します。OSPF ルーティングドメインに再配布されるルートの外部リンクタイプを指定します。メトリックタイプが指定されていないと、スイッチは「Type -2」外部ルートを採用します。 • 選択肢：「外部 タイプ -1」「外部 タイプ -2」
メトリック	再配布ルートのメトリックを指定します。 • 設定可能範囲：1-16777214
ルートマップ名	送信元ルーティングプロトコルからインポートされたルートをフィルタするルートマップ名を指定します。 指定されないと全ルートが再配布されます。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックして、指定のエントリを削除します。

OSPFv2 仮想リンク設定

OSPFv2 仮想リンク設定を行います。「non-zero」エリアが物理的にゼロエリアと接続していない場合、仮想リンクを通じてゼロエリアに接続する必要があります。仮想リンクは「point-to-point」リンクです、ルータは OSPF メッセージをユニキャスト IP パケットとしてネイバルータに送信します。

L3 機能 > OSPF > OSPFv2 > OSPFv2 仮想リンク設定の順にメニューをクリックし、以下の画面を表示します。

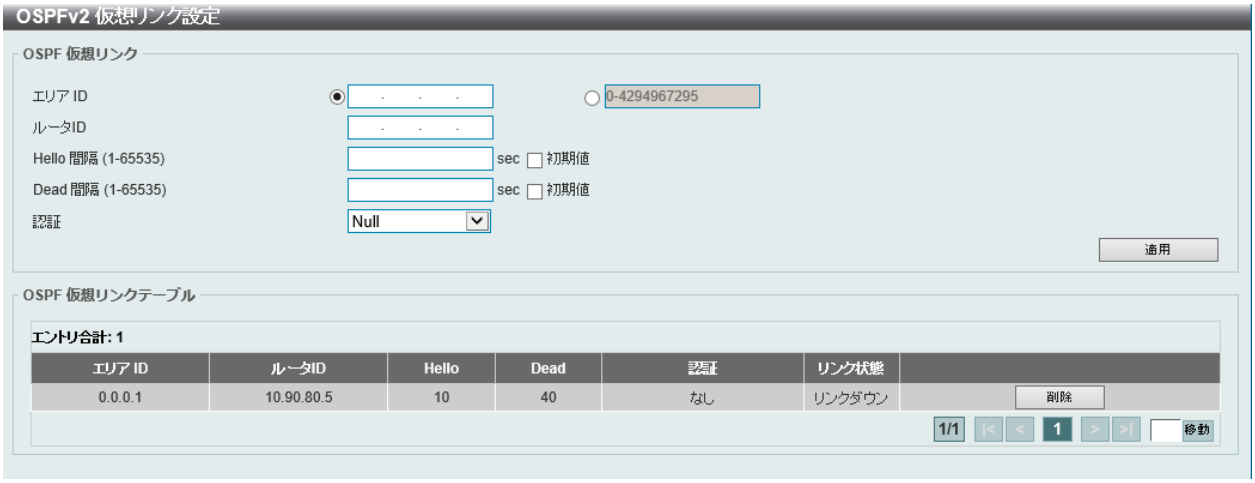


図 9-46　OSPF 仮想リンク設定画面

画面に表示される項目：

項目	説明
OSPF 仮想リンク	
エリア ID	OSPFv2 エリア識別子を選択して入力します。IP アドレス形式（xxx.xxx.xxx.xxx）または 10 進数値形式（0-4294967295）で指定できます。このエリアは、仮想リンクを確立するために使用されます。
ルータ ID	仮想リンクの隣接ルータ ID を入力します。
Hello 間隔	OSPF Hello パケットの送出間隔（秒）を指定します。「初期値」を選択すると初期値を使用します。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead 間隔	Hello パケットの最後の受信から、ネイバがオフラインになったと判断するまでの Dead インターバル を入力します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
認証	使用する認証を選択します。 • 選択肢：「Null」「簡易パスワード」「MD5」
パスワード	「認証」で「簡易パスワード」を選択した場合、シンプルテキストのパスワードを入力します。（8 文字以内）
MD5 キー ID	「認証」で「MD5」を選択した場合、MD5 認証キー ID を入力します。 • 設定可能範囲：1-255
MD5 キー	「認証」で「MD5」を選択した場合、MD5 認証キーを指定します。（16 文字以内）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

エントリをダブルクリックすると次の画面が表示されます。

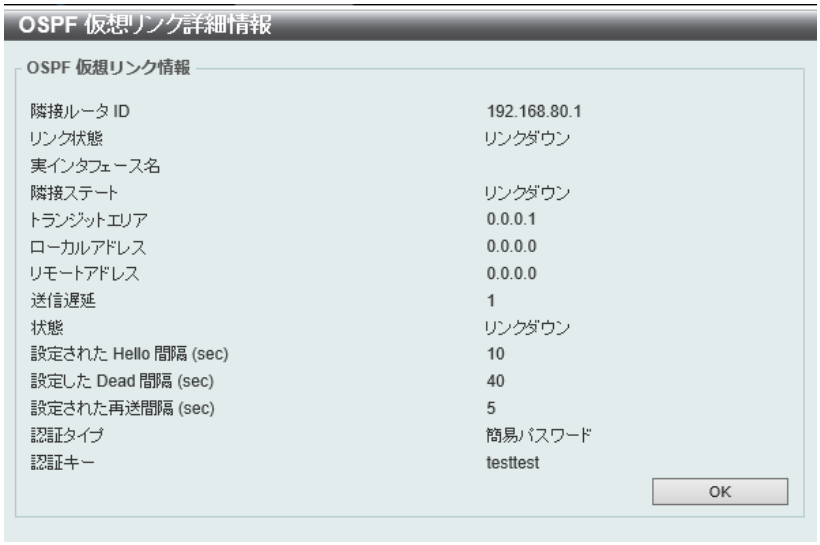


図 9-47　OSPF 仮想リンク詳細情報画面

OSPFv2 LSDB テーブル

OSPFv2 Link State Database（LSDB）を表示します。

L3 機能 > OSPF > OSPFv2 > OSPFv2 LSDB テーブルの順にメニューをクリックし、以下の画面を表示します。



図 9-48　OSPFv2 LSDB テーブル画面

画面に表示される項目：

項目	説明
LS タイプ	表示する LSDB タイプを指定します。 • 選択肢：「全て」「ルータ」「ネットワーク」「サマリ」「ASBR サマリ」「外部」「スタブ」「NSSA 外部」
リンクステート	表示されるリンクステート情報を選択します。 • 「全て」- 全ての OSPFv2 リンクステート情報を表示します。 • 「リンクステート ID」- 指定したリンクステート ID に関する情報を表示します。表示される欄にリンクステート ID を指定します。 • 「自己発信」- ローカルルータによって生成された LSA を表示します。 • 「ADV ルータ」- 通知ルータによって生成された全ての LSA を表示します。通知ルータ ID を空欄に入力します。

「検索」をクリックして、指定したエントリを検索します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
エントリを指定し「OK」をクリック、設定内容を適用します。

■ OSPFv2 LSDB の詳細表示

「詳細を表示」をクリックすると、以下の画面が表示されます。

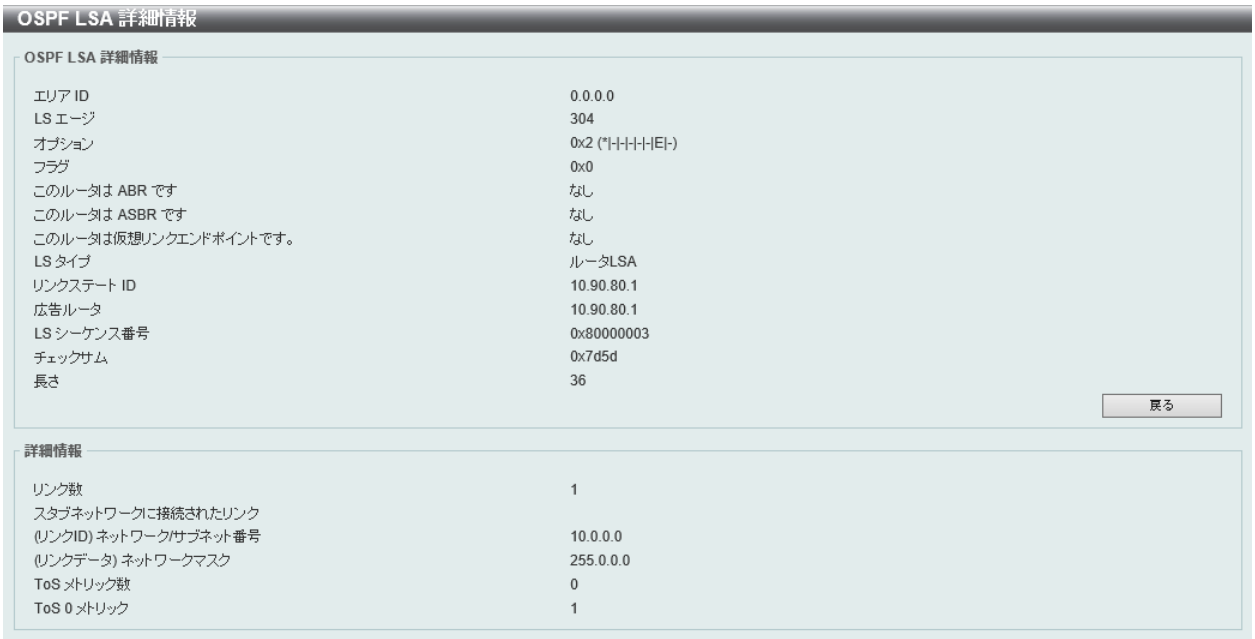


図 9-49　OSPFv2 LSDB テーブル（詳細を表示）画面

「戻る」をクリックして前のページに戻ります。

OSPFv2 隣接テーブル

インタフェースごとの OSPF 隣接（ネイバ）情報を表示します。

L3 機能 > OSPF > OSPFv2 > OSPF 隣接テーブルの順にメニューをクリックし、以下の画面を表示します。

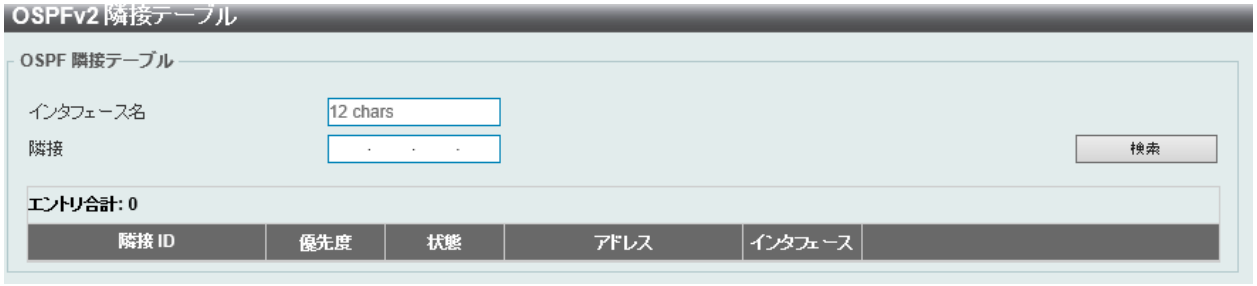


図 9-50　OSPFv2 隣接テーブル画面

画面に表示される項目：

項目	説明
インタフェース名	使用されるインタフェースを指定します。
隣接	ネイバ ID を入力します。

「検索」をクリックして、指定したエントリを検索します。
「詳細を表示」をクリックすると、エントリの詳細情報が表示されます。

OSPFv2 ホストルート設定

OSPFv2 ホストルート設定を行います。ルータは、Stub リンクのルータ LSA として特定のホストルートを通知します。

L3 機能 > OSPF > OSPFv2 > OSPFv2 ホストルート設定 の順にメニューをクリックし、以下の画面を表示します。



図 9-51　OSPFv2 ホストルート設定画面

画面に表示される項目：

項目	説明
OSPFv2 ホストルート設定	
エリア ID	OSPFv2 エリア識別子を選択して入力します。IP アドレス形式（xxx.xxx.xxx.xxx）または 10 進数値形式（0-4294967295）で指定できます。このエリアは、仮想リンクを確立するために使用されます。
ホスト IP	ホストの IP アドレスを指定します。
コスト	スタブエントリのコスト値を指定します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

OSPFv3

OSPFv3 プロセス設定

スイッチに OSPFv3 プロセス設定を行います。

L3 機能 > OSPF > OSPFv3 > OSPFv3 プロセス設定の順にメニューをクリックして以下の画面を表示します。

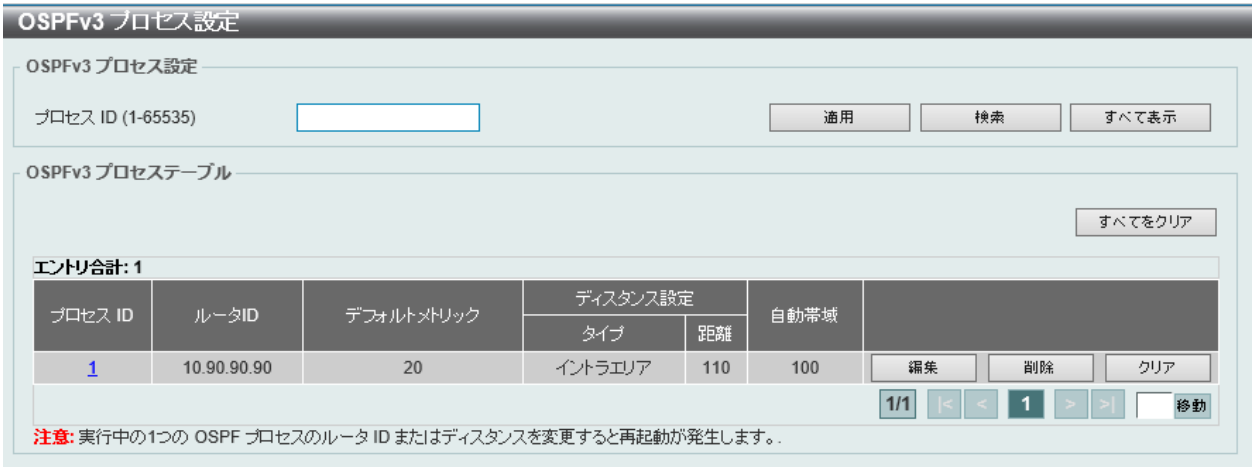


図 9-52　OSPFv3 プロセス設定画面

画面に表示される項目：

項目	説明
プロセス ID	OSPFv3 のプロセス ID（1-65535）を指定します。 • 設定可能範囲：1-65535

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
「編集」をクリックして、指定エントリの編集を行います。
「プロセス ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
「クリア」をクリックすると入力したエントリをクリアします。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「編集」をクリックすると、以下の画面が表示されます。

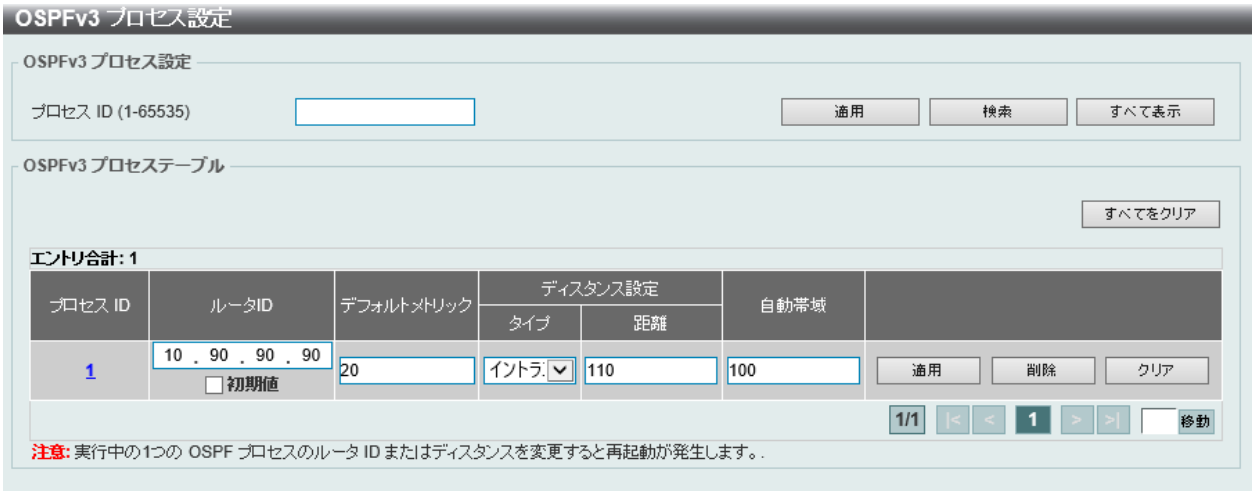


図 9-53　OSPFv3 プロセス設定（編集）画面

画面に表示される項目：

項目	説明
ルータ ID	OSPF プロセスのためのルータ ID を入力します。初期値では、ルータ ID が自動的に選択されます。 「初期値」にチェックを入れると初期値に設定されます。
デフォルトメトリック	OSPF プロセスの初期メトリック値を指定します。この設定は、OSPFv3 再配布機能とともに使用され、現在のルーティングプロトコルを有効化してすべての再配布ルートに同じメトリック値を使用します。整合性のないメトリックを持つルートの再配布を行う場合、初期メトリックが役に立ちます。メトリックの直接変換ができない場合に、初期メトリックにより再配布が実行されます。 • 設定可能範囲：1-16777214 • 初期値：20
タイプ	ディスタンス設定の種類を指定します。 •「内部 - エリア」- OSPF 間エリアルートのディスタンスを指定します。 •「イントラエリア」- OSPF 内エリアルートのディスタンスを指定します。 •「外部」- OSPF 外部ルートのディスタンスを指定します。
距離	OSPF プロセスのディスタンス値を指定します。 • 設定可能範囲：1-254 • 初期値：110（全ての OSPF ルート）
自動帯域	自動帯域幅の値を指定します。インタフェースのメトリックの計算時に IPv6 OSPF が使用する参照値を制御するために使用されます。 • 設定可能範囲：1-4294967

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「プロセス ID」のリンクを指定すると次の画面が表示されます。



図 9-54　OSPFv3 プロセス設定（プロセス ID）画面

「OK」をクリックして画面を終了し前画面に戻ります。

OSPFv3 パッシブインタフェース設定

スイッチに OSPFv3 パッシブインタフェース設定を行います。インタフェースがパッシブ（受動態）の場合、OSPF ルーティングアップデートパケットは指定のインタフェースを通じての送受信がされなくなります。

L3 機能 > OSPF > OSPFv3 > OSPFv3 パッシブインタフェース設定の順にメニューをクリックして以下の画面を表示します。

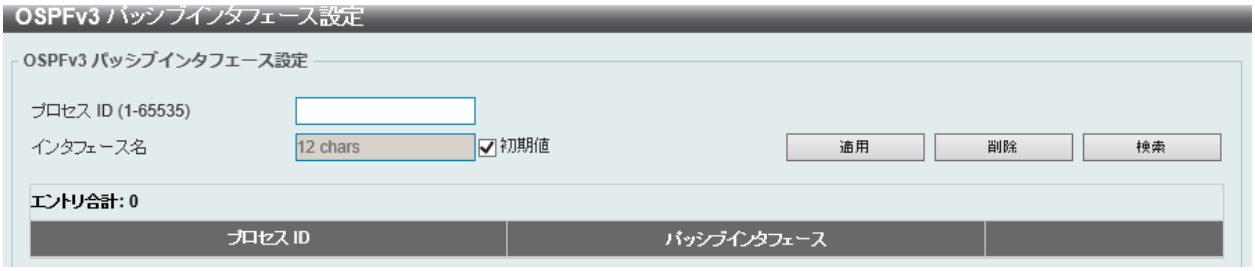


図 9-55　OSPFv3 パッシブインタフェース設定画面

画面に表示される項目：

項目	説明
プロセス ID	OSPFv3 のプロセス ID を指定します。 • 設定可能範囲：1-65535
インタフェース名	パッシブインタフェース名を指定します。（12 文字以内） 「初期値」を選択すると全てのインタフェースをパッシブインタフェースとして指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

OSPFv3 エリア設定

スイッチに OSPFv3 エリア設定を行います。

L3 機能 > OSPF > OSPFv3 > OSPFv3 エリア設定の順にメニューをクリックして以下の画面を表示します。

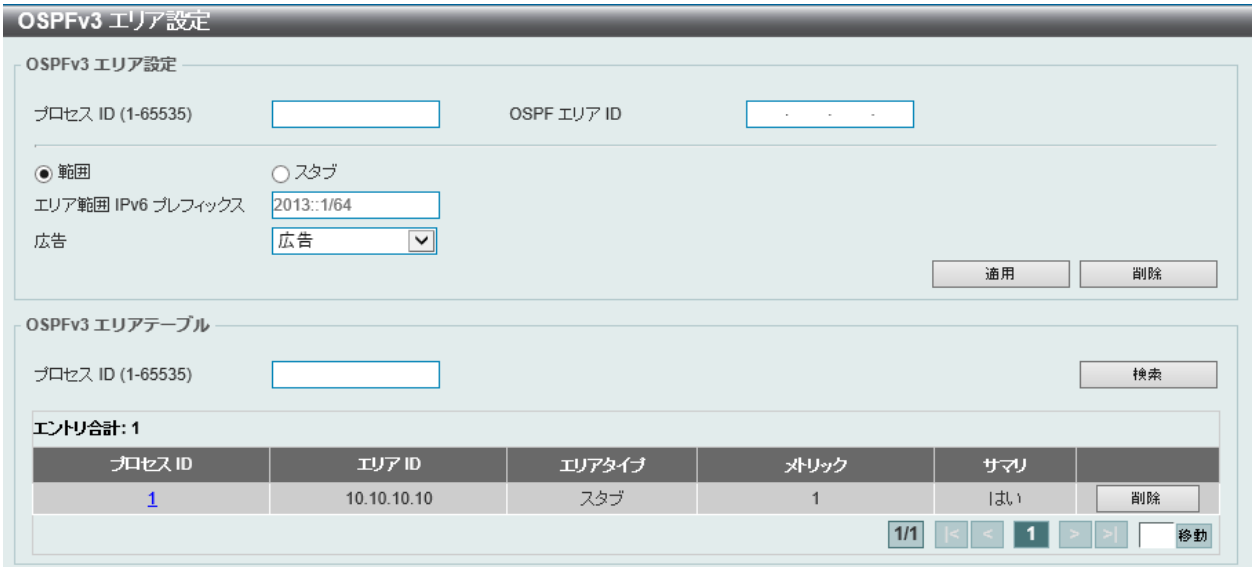


図 9-56　OSPFv3 エリア設定画面

画面に表示される項目：

項目	説明
OSPFv3 エリア設定	
プロセス ID	OSPF のプロセス ID を指定します。 • 設定可能範囲：1-65535
OSPF エリア ID	OSPF エリア ID を入力します。IPv4 アドレス形式で指定します。

項目	説明
範囲	Area Border Router（ABR）で OSPF ルートを集約します。この機能は、ABR でのみ使用されます。エリアのルートが統合・集約され、1 つのサマリールートが ABR によって他のエリアにアドバタイズされます。ルーティング情報はエリア境界で集約されます。エリア外には、アドレス範囲ごとに 1 つのルートがアドバタイズされます。 • 「エリア 範囲 IPv6 プレフィックス」- OSPF エリア範囲 IPv6 プレフィックスとプレフィックス長を入力します。 • 「広告」- 通知オプションを選択します。 - 「広告」- 指定されたアドレス範囲のエリア間プレフィックス LSA をアドバタイズして生成します。 - 「広告なし」- 指定されたアドレス範囲のステータスを「Do-Not-Advertise」に設定します。エリア間プレフィックス LSA は抑制され、設定されたネットワークは他のネットワークから認識されない状態のままです。
スタブ	エリアをスタブエリアとして定義します。 • 「デフォルトコスト」- このエリアのデフォルトメトリック値（1）が使用されます。 • 「初期値」- デフォルトのコスト値を使用します。 • 「サマリなし」- ABR がエリア間プレフィックス LSA をスタブエリアに送信しないように設定します。
OSPFv3 エリアテーブル	
プロセス ID	OSPF のプロセス ID を指定します。 • 設定可能範囲：1-65535

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「プロセス ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「OSPFv3 エリアテーブル」エリアの「プロセス ID」をクリックすると、以下の画面が表示されます。



図 9-57　OSPFv3 エリア設定（詳細）画面

「OK」をクリックして画面を終了し、前画面に戻ります。

OSPFv3 インタフェース設定

OSPFv3 設定または OSPFv3 インタフェース情報を表示します。

L3 機能 > OSPF > OSPFv3 > OSPFv3 インタフェース設定の順にメニューをクリックして以下の画面を表示します。

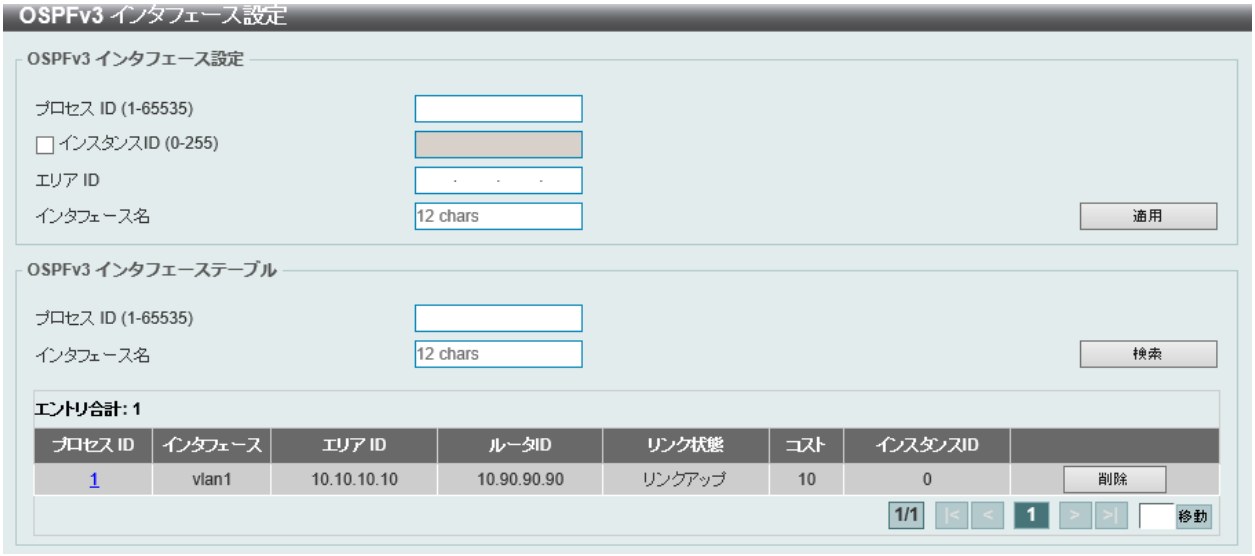


図 9-58　OSPFv3 インタフェース設定画面

画面に表示される項目：

項目	説明
OSPFv3 インタフェース設定	
プロセス ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 • 設定可能範囲：1-65535
インスタンス ID	インスタンス ID を指定します。 • 設定可能範囲：0-255 • 初期値：0
エリア ID	エリアの識別子として IPv4 アドレスを指定します。
インタフェース名	インタフェース名を入力します。（12 文字以内）
OSPFv3 インタフェーステーブル	
プロセス ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 • 設定可能範囲：1-65535
インタフェース名	インタフェース名を入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「プロセス ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「プロセス ID」をクリックすると、以下の画面が表示されます。

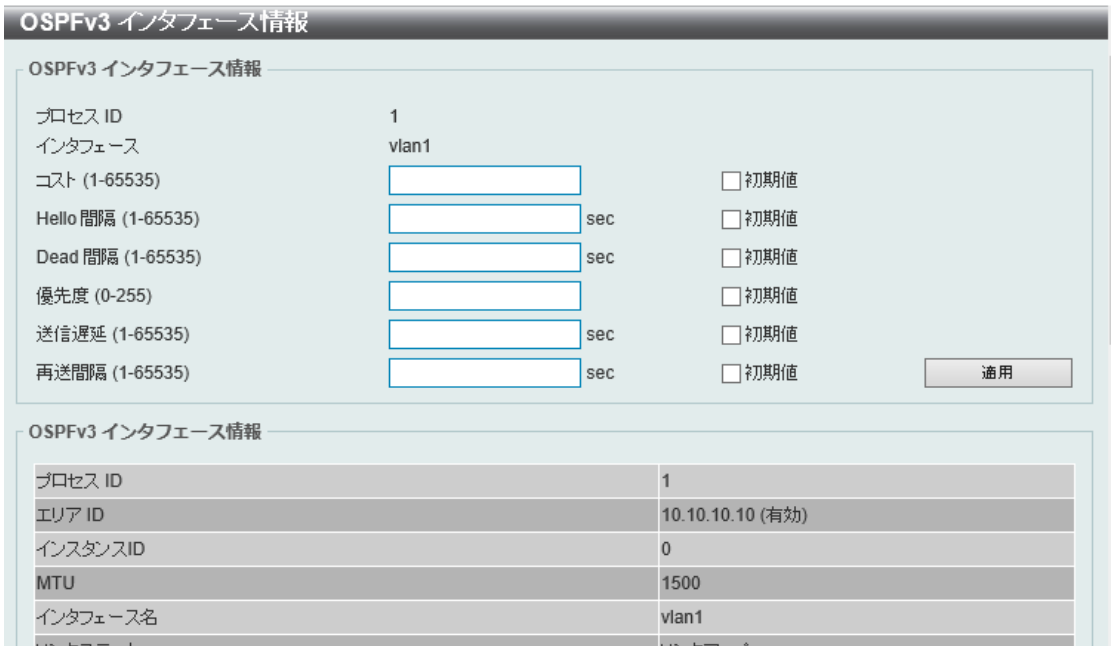


図 9-59　OSPFv3 インタフェース設定（プロセス ID）画面

画面に表示される項目：

項目	説明
コスト	コストの値を指定します。リンク状態メトリックとして表される整数値です。 「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535 • 初期値：1
Hello 間隔	Hello インターバル値を指定します。Hello Interval は Hello パケット内で通知されます。この間隔が短いほど、トポロジ変更の検知が早くなりますが、ルーティングトラフィックが増加します。対象ネットワーク上のすべてのルータとアクセスサーバで同じである必要があります。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead 間隔	Dead インターバル値を指定します。指定時間パケットが受信されない場合、ネイバがオフラインと認識されます。 この値は Hello パケット内で通知されます。対象ネットワーク上のすべてのルータとアクセスサーバで同じである必要があります。 「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
優先度	ルータのプライオリティを指定します。OSPF ルータは、ネットワークの代表ルータ（Designated Router/DR）を選出するために使用されます。2 台のルータがルータになろうとしている場合、高いプライオリティのルータが選出されます。同じプライオリティ値を持つ場合は、ルータ ID の高い方が優先されます。「0」の場合は代表ルータまたはバックアップ代表ルータ（BDR）として選出されません。（ポイントツーポイントではなく）マルチアクセスネットワークのみにルータプライオリティを設定します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：0-255 • 初期値：1
送信遅延	「Transmit Delay（送信遅延）の値を入力します。Link State Updates（LSU）は、その送信前に seconds 引数で指定された分を増加させます。設定する値は、インタフェースの伝送・伝播遅延を考慮する必要があります。リンク上での送信の前に遅延時間が追加されない場合、LSA の伝播時間は考慮されません。この設定は、低速のリンクでは重要になります。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：1（秒）
再送間隔	Retransmit Interval（再送信間隔）の値を指定します。ネイバに LSA を送信した後、ルータは Ack 応答を受信するまで LSA を保持します。指定時間（「Retransmit Interval」）ルータが応答を受信しなかった場合、LSA を再送信します。不要な再送信を減らすために、再送信間隔は控えめに指定することを推奨します。この間隔は、2 つのルータ間で予想される往復の遅れよりも大きい値である必要があります。「初期値」を指定すると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）

「適用」をクリックして、設定内容を適用します。

OSPFv3 再配布設定

OSPFv3 リディストリビュート（再配布）について設定、表示を行います。

L3 機能 > OSPF > OSPFv3 > OSPFv3 再配布設定の順にメニューをクリックし、以下の画面を表示します。



図 9-60　OSPFv3 再配布設定画面

画面に表示される項目：

項目	説明
プロセス ID	IPv6 OSPF ルーティングのプロセス ID を指定します。ローカルに割り当てられる値であり、ルータの IPv6 OSPF ルーティングプロセス毎に一意である必要があります。 • 設定可能範囲：1-65535
プロトコル	再配布される送信元プロトコルを指定します。 • 選択肢：「接続されています」「スタティック」「RIPng」
メトリックタイプ	IPv6 OSPF ルーティングドメインにアドバタイズされるデフォルトルートに関連付けられている外部リンクタイプを選択します。メトリックタイプを指定しない場合、スイッチは「外部 タイプ -2」ルートを採用します。これは IPv6 OSPF のみに適用されます。 • 選択肢：「外部 タイプ -1」「外部 タイプ -2」
メトリック	メトリック値を指定します。この設定は、他のプロセスを IPv6 OSPF プロセスに再配布する際に使用されます。 • 設定可能範囲：0-16777214 • 初期値：20

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックして、指定のエントリを削除します。

OSPFv3 仮想リンク設定

OSPFv3 仮想リンク設定を行います。

L3 機能 > OSPF > OSPFv3 > OSPFv3 仮想リンク設定の順にメニューをクリックして以下の画面を表示します。

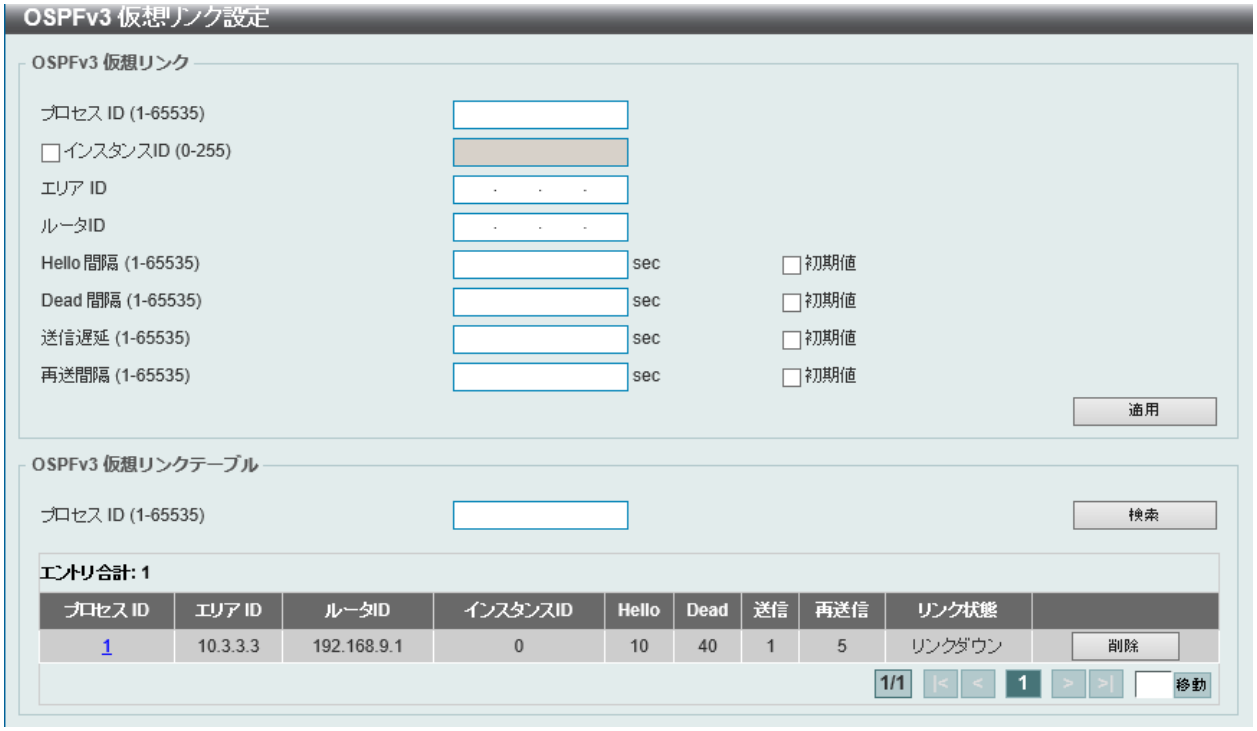


図 9-61　OSPFv3 仮想リンク設定画面

画面に表示される項目：

項目	説明
プロセス ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 ローカルに割り当てられる値であり、ルータの IPv6OSPF ルーティングプロセス毎に一意である必要があります。 • 設定可能範囲：1-65535
インスタンス ID	インスタンス ID を入力します。 • 設定可能範囲：0-255
エリア ID	OSPF エリア ID を IPv4 アドレス形式で入力します。
ルータ ID	仮想リンクネイバのルータ ID を入力します。
Hello 間隔	ルータがインタフェース上で送信する Hello パケットの送信間隔を指定します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
Dead 間隔	Dead インターバル値を指定します。指定時間パケットが受信されない場合、ネイバがオフラインと認識されます。 「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：40（秒）
送信遅延	ルータがパケットを送信するまでに待機する時間を指定します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：1（秒）
再送間隔	ルータがパケットを再送信するまでに待機する時間を指定します。「初期値」にチェックを入れると初期値に設定されます。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）
OSPFv3 仮想リンクテーブル	
プロセス ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 • 設定可能範囲：1-65535

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「プロセス ID」のリンクをクリックすると指定の OSPFv3 プロセスのへのアクセス、設定を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「プロセス ID」をクリックすると、以下の画面が表示されます。

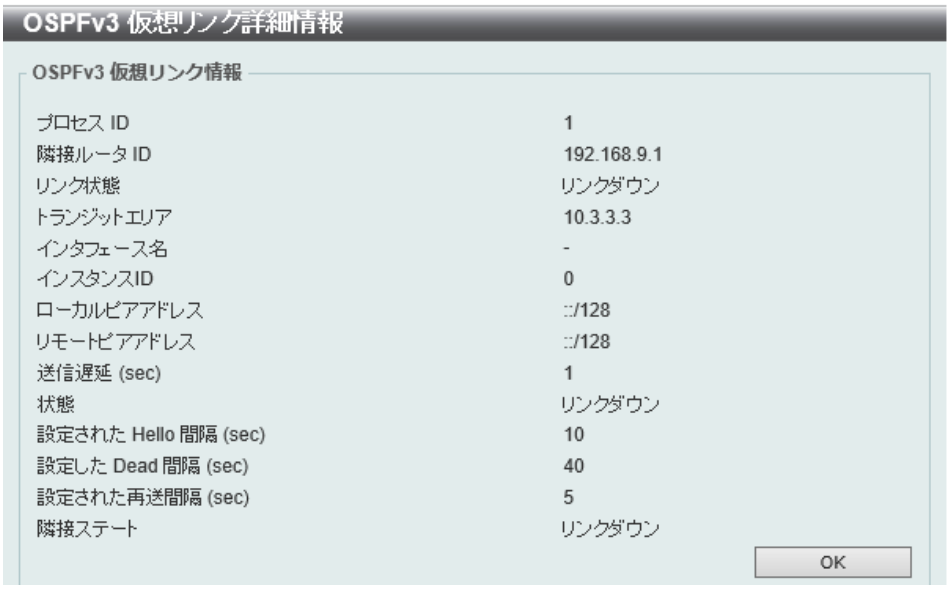


図 9-62　OSPFv3 仮想リンク詳細情報画面

OSPFv3 LSDB テーブル

OSPFv3 リンクステート データベース（LSDB）を表示します。

L3 機能 > OSPF > OSPFv3 > OSPFv3 LSDB テーブルの順にメニューをクリックして以下の画面を表示します。

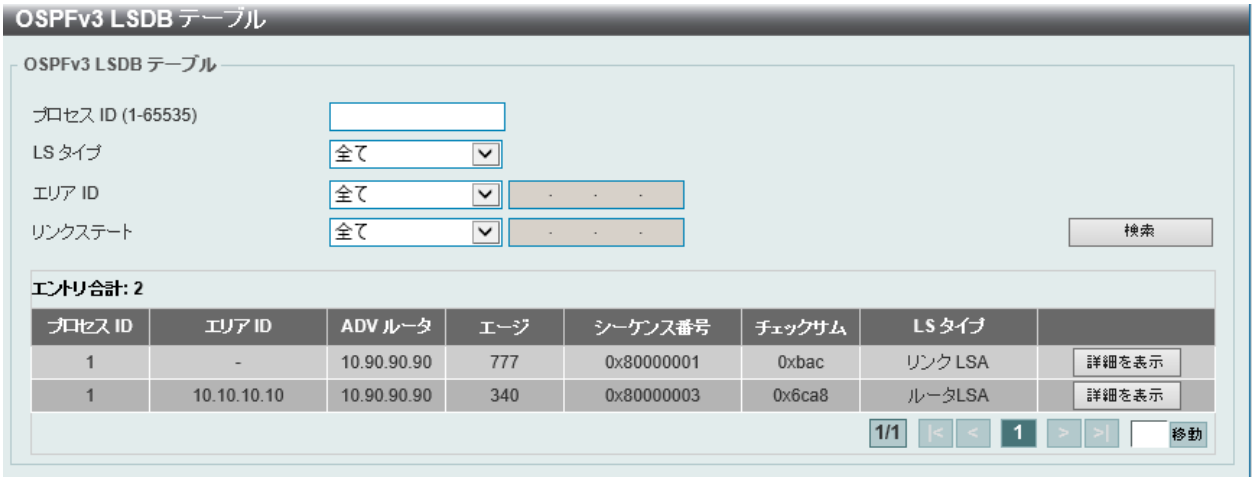


図 9-63　OSPFv3 LSDB テーブル画面

画面に表示される項目：

項目	説明
プロセス ID	IPv6 OSPF ルーティングのプロセス ID を指定します。 ローカルに割り当てられる値であり、ルータの IPv6OSPF ルーティングプロセス毎に一意である必要があります。 • 設定可能範囲：1-65535
LS タイプ	表示する LSDB タイプを以下から指定します。 •「全て」- すべての種類の LSDB 情報を表示します。 •「ルータ LSA」- ルータ LSA の情報のみ表示します。 •「ネットワーク LSA」- ネットワーク LSA の情報のみ表示します。 •「プレフィックス」- エリア内プレフィックス LSA の情報のみ表示します。 •「リンク LSA」- リンク LSA の情報のみ表示します。 •「内部 - エリア プレフィックス LSA」- エリア間プレフィックス LSA に基づいた LSA の情報のみ表示します。 •「内部 - エリアルータ LSA」- エリア間ルータ LSA に基づいた LSA の情報のみ表示します。 •「AS- 外部 -LSA」- 外部 LSA の情報のみ表示します。
エリア ID	エリア ID オプションを指定します。指定されたエリアのすべての LSA を表示するには、「エリア ID」を指定し、OSPF エリア ID を空欄に入力します。IPv4 アドレスの形式で指定します。 • 選択肢：「全て」「エリア ID」

項目	説明
リンクステート	表示するリンクステート情報を選択します。 • 「全て」- 全てのリンクステート情報を表示します。 • 「自己発信」-（ローカルルータによって生成された）自己発信 LSA を表示します。 • 「ADV ルータ」- 通知ルータによって生成されたの全ての LSA を表示します。通知ルータ ID を空欄に入力します。

「検索」をクリックして、指定したエントリを検索します。

■ エントリの詳細表示

「詳細を表示」をクリックすると、以下の画面が表示されます。

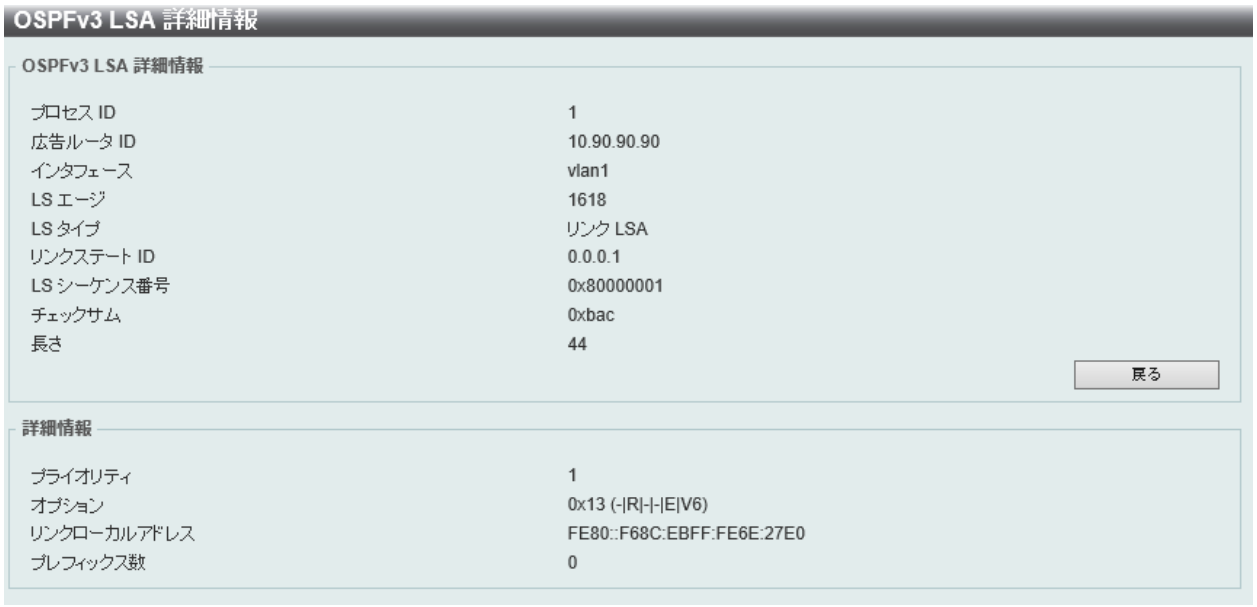


図 9-64　OOSPFv3 LSA 詳細情報 画面

「戻る」をクリックして前のページに戻ります。

OSPFv3 隣接テーブル

OSPFv3 隣接（ネイバ）情報を表示します。

L3 機能 > OSPF > OSPFv3 > OSPFv3 隣接テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-65　OSPFv3 隣接テーブル画面

画面に表示される項目：

項目	説明
プロセス ID	OSPFv3 プロセス ID を指定します。 • 設定可能範囲：1-65535
VLAN インタフェース	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
隣接	OSPF ネイバ ID を入力します。IPv4 アドレスで指定します。

「検索」をクリックして、指定したエントリを検索します。

「詳細を表示」をクリックして、エントリの詳細を表示します。

OSPFv3 境界ルータテーブル

OSPFv3 境界ルータについての情報を表示します。

L3 機能 > OSPF > OSPFv3 > OSPFv3 ボーダールータテーブルの順にメニューをクリックして以下の画面を表示します。



図 9-66　OSPFv3 境界ルータテーブル画面

画面に表示される項目：

項目	説明
プロセス ID	検索する OSPFv3 プロセス ID を指定します。 • 設定可能範囲：1-65535

「検索」をクリックして、指定したエントリを検索します。

IP マルチキャストルーティングプロトコル

L3 機能 > IP マルチキャストルーティングプロトコル

IP マルチキャストルーティングプロトコル（IP マルチキャストルーティングプロトコル）の設定を行います。

IGMP

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP

IGMP インタフェース設定

IGMP（Internet グループ Management Protocol）は、IP インタフェースごとを基本にスイッチに設定されます。
スイッチに設定した各 IP インタフェースは、以下の「IGMP インタフェース設定」画面に表示されます。

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP > IGMP インタフェース設定の順にメニューをクリックして、以下の画面を表示します。



図 9-67　IGMP インタフェース設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ エントリの編集

「編集」をクリックして、以下の画面を表示します。

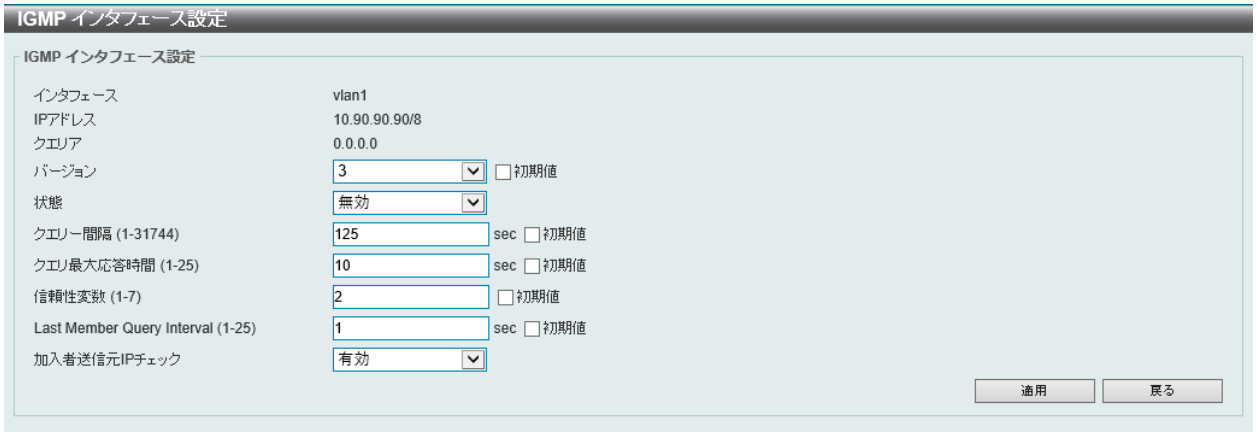


図 9-68　IGMP インタフェース設定（編集）画面

画面に表示される項目：

項目	説明
バージョン	IGMP のバージョン番号を 1-3 から選択します。「初期値」を指定すると初期値を使用します。 • 選択肢：「1」「2」「3」 • 初期値：「3」
状態	インタフェースの IGMP ステータスを有効 / 無効に設定します。
クエリー 間隔	IGMP クエリを送信する間隔 を指定します。IGMP クエリアは、指定された間隔で IGMP クエリメッセージを送信し、マルチキャストグループへ参加しようとしているレシーバを検出します。この問い合わせに対し、ホストは参加するマルチキャストグループを示す IGMP レポートメッセージで応答します。「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1 - 31744（秒） • 初期値：125（秒）
クエリ最大応答時間	グループメンバが IGMP クエリメッセージに対して応答可能な時間を指定します。この時間を超えると、ルータによりメンバシップが削除されます。「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒） • 初期値：10（秒）
信頼性変数	ロバストネス変数の値を指定します。この値は、インタフェース上で予想されるパケット損失を許容するための調整に使用されます。「初期値」を指定すると初期値を使用します。 • 指定可能範囲：1 - 7 • 初期値：2
Last Member Query Interval	Last Member Query Interval 値を入力します。 ルータは、グループまたはチャネルを離れるための Leave メッセージをレシーバから受信すると、Group Specific Query または Group-Source Specific Query メッセージをレシーバインタフェースに送信します。IGMP Last Member Query Interval は、クエリメッセージでアドバタイズされ、レシーバに送信されます。 本設定は、特定のグループまたはチャネルのレシーバからのレポートがない場合に、ルータが次の Group Specific Query または Group-Source Specific Query クエリメッセージを送信する期間を指定します。ルータは、最後のメンバクエリカウントを再試行します。再試行回数後にレポートメッセージが受信されない場合、インタフェースは特定のグループまたはチャネルからメンバシップを削除します。 「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1 - 25（秒）
加入者送信元 IP チェック	サブスクライバ（加入者）送信元アドレスチェック機能を有効 / 無効に設定します。 デフォルトでは、インタフェースで受信された IGMP レポートまたは Leave メッセージは、その送信元 IP がインタフェースと同じネットワーク内にあるかどうかチェックされます。同じネットワークに存在しない場合、メッセージ情報は IGMP プロトコルによって学習されません。

「適用」をクリックして、設定を適用します。

「戻る」をクリックして前のページに戻ります。

IGMP スタティックグループ設定

IGMP スタティックグループを設定します。
接続されたホストが IGMP プロトコルをサポートしていない場合、IGMP スタティックグループを作成します。設定が完了すると、グループメンバエントリが IGMP キャッシュに追加されます。

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP > IGMP スタティックグループ設定 の順にクリックして以下の画面を表示します。



図 9-69　IGMP スタティックグループ設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
グループ	マルチキャストグループ IP アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。

IGMP ダイナミックグループテーブル

IGMP ダイナミックグループ情報の表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP > IGMP ダイナミックグループテーブルの順にクリックして以下の画面を表示します。



図 9-70　IGMP ダイナミックグループテーブル画面

画面に表示される項目：

項目	説明
VLAN インタフェース	本設定に使用する VLAN インタフェースを指定します。 • 設定可能範囲：1-4094
グループ	IP マルチキャストグループアドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「クリア」をクリックすると入力したエントリをクリアします。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。

MLD

MLD（マルチキャスト Listener Discovery）はルータとホスト間で使用される IPv6 マルチキャストグループ管理プロトコルです。
IPv4 マルチキャストの IGMP と同様の機能を持っています。

MLD インタフェース設定

MLD インタフェースの設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > MLD > MLD インタフェース設定の順にメニューをクリックして以下の画面を表示します。



図 9-71　MLD インタフェース設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	本設定に使用する VLAN インタフェースを指定します。 • 設定可能範囲：1-4094

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ エントリの編集

「編集」をクリックして、以下の画面を表示します。

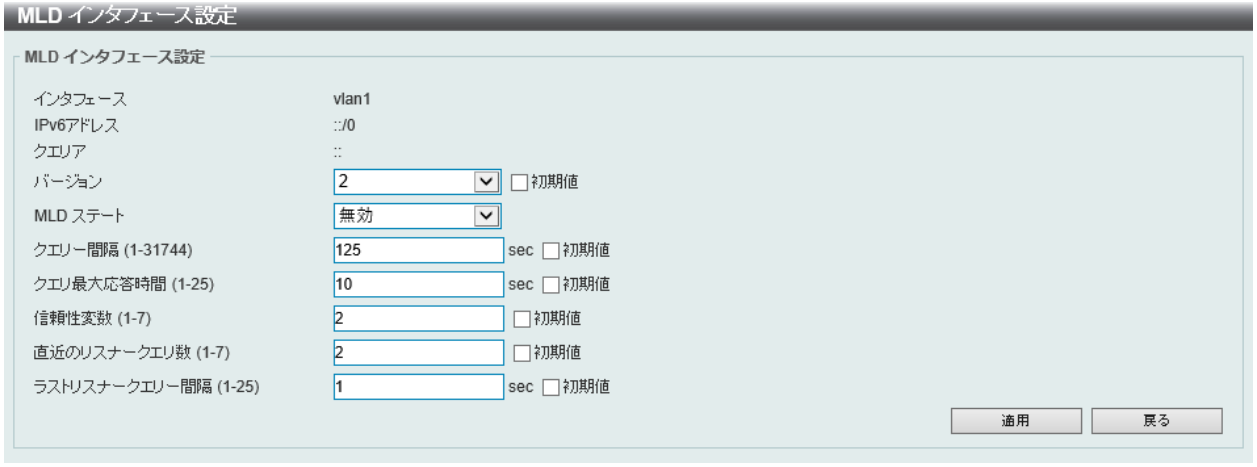


図 9-72　MLD インタフェース（編集）設定 画面

画面に表示される項目：

項目	説明
バージョン	インタフェースで使用する MLD バージョンを選択します。「初期値」を指定すると初期値を使用します。 • 選択肢：「1」「2」 • 初期値：「2」
MLD ステート	インタフェースの MLD 機能を有効 / 無効に設定します。
クエリー間隔	代表ルータが MLD General クエリメッセージを送信する間隔を指定します。General クエリを受信すると、MLD リスナはレポートパケットに応答して、指定されたマルチキャストグループへの参加を要求します。 「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1-31744（秒） • 初期値：125（秒）
クエリ最大応答時間	クエリメッセージに対する最大応答時間を指定します。MLD クエリ内でアドバタイズされます。 「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒） • 初期値：10（秒）
信頼性変数	ロバストネス変数の値を指定します。この値は、インタフェース上で予想されるパケット損失を許容するための調整に使用されます。 「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1-7 • 初期値：2
直近のリスナークエリ数	「group-specific」または「group-source specific」クエリが指定回数送信されると、ルータはグループ内にローカルメンバがいないと判断します。ルータがタイムアウトまでにホストからレポートを受信しない場合、ルータはインタフェースのマルチキャストグループトラフィックの送信を中止します。 「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1-7 • 初期値：2
ラストリスナークエリー間隔	Group Specific Query またはGroup-Source Specific Query メッセージのクエリ間隔を指定します。MLD クエリアは、グループまたはチャネルを離れるための Leave メッセージをレシーバから受信すると、Group Specific Query またはGroup-Source Specific Query メッセージをレシーバインタフェースに送信します。MLD クエリアがインタフェース上でパケットを受信すると、Leave タイマが開始されます。タイマが期限切れになるまでにインタエースでレポートパケットを受信しない場合、インタフェースのメンバシップは、離脱しているグループまたはチャネルから削除されます。「初期値」を指定すると初期値を使用します。 • 設定可能範囲：1-25（秒） • 初期値：1（秒）

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックして前のページに戻ります。

MLD スタティックグループ設定

MLD スタティックグループ設定を行います。
付属のホストが MLD プロトコルをサポートしていない場合に MLD スタティックグループを作成します。設定すると、グループメンバエントリが MLD キャッシュに追加されます。

L3 機能 > IP マルチキャストルーティングプロトコル > MLD > MLD スタティックグループ設定の順にクリックし、以下の画面を表示します。



図 9-73　MLD スタティックグループ設定画面

画面に表示される項目：

項目	説明
VLAN インタフェース	本設定に使用する VLAN インタフェースを指定します。 • 設定可能範囲：1-4094
グループ	IPv6 マルチキャストグループアドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

MLD グループテーブル

スイッチにおける MLD スタティックグループを表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > MLD > MLD グループテーブルの順にメニューをクリックして以下の画面を表示します。



図 9-74　MLD グループテーブル画面

画面に表示される項目：

項目	説明
VLAN インタフェース	本設定に使用する VLAN インタフェースを指定します。 • 設定可能範囲：1-4094
グループ	IPv6 グループアドレスを入力します。

「検索」をクリックして、入力したインタフェースを検出します。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IGMP プロキシ

IGMP プロキシ設定の表示と設定を行います。
IGMP プロキシは、単純なツリートポロジでのみ機能します。ツリートポロジにプロキシデバイス以外のマルチキャストルータがないことを確認します。IGMP レポートパケットをダウンストリームインタフェースから受信すると、IGMP プロキシはメンバシップデータベースを更新します。このパケットは、ダウンストリームインタフェースのすべてのサブスクリプションの統合により生成されます。データベースが変更されると、プロキシデバイスは Unsolicited レポートを送信するか、アップストリームインタフェースから離脱します。また、クエリを受信したときは、アップストリームインタフェースからメンバシップレポートを送信することもできます。

IGMP プロキシ設定

IGMP プロキシを設定します。

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP プロキシ > IGMP プロキシ設定の順にメニューをクリックし、以下の画面を表示します。



図 9-75　IGMP プロキシ設定画面

画面に表示される項目：

項目	説明
IGMP プロキシグローバル設定	
グローバルステート	IGMP プロキシのグローバルステータスを有効 / 無効に設定します。
IGMP プロキシアップストリーム設定	
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
アップストリーム	アップストリーム IGMP プロキシとしてのインタフェースを有効 / 無効に指定します。
IGMP プロキシダウンストリーム設定	
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
ダウンストリーム	ダウンストリーム IGMP プロキシとしてのインタフェースを有効 / 無効に指定します。
IGMP プロキシ指定フォワーディング設定	
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
指定フォワーディング	非クエリア IGMP プロキシダウンストリームインタフェースでの指定転送を有効 / 無効に設定します。複数の IGMP ベースのフォワーダによるダウンストリームリンクとみなされるリンクのローカルループと冗長トラフィックを回避するために、IGMP クエリアの選出を使用して、IGMP プロキシは LAN 上で単一のフォワーダを選択します。非クエリアデバイスをフォワーダにするには、このオプションを使用します。この機能は、インタフェースがダウンストリームインタフェースとして設定されていないか、アップストリームインタフェースとして設定されている場合は有効になりません。

「適用」をクリックして各セクションで行った変更を適用します。

IGMP プロキシグループテーブル

IGMP プロキシグループ設定を検索、表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP プロキシ > IGMP プロキシグループテーブルの順にクリックし、以下の画面を表示します。

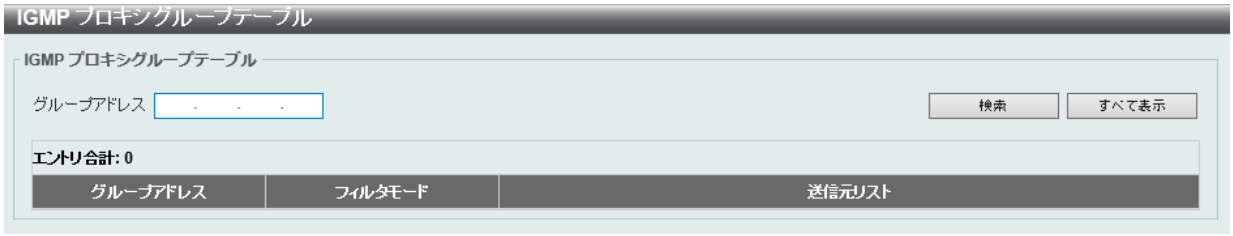


図 9-76　IGMP プロキシグループテーブル画面

画面に表示される項目：

項目	説明
グループ アドレス	IPv4 グループマルチキャストアドレスを入力します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IGMP プロキシフォワーディングテーブル

IGMP プロキシのフォワーディング情報を検索、表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > IGMP プロキシ > IGMP プロキシフォワーディングテーブルの順にクリックし、以下の画面を表示します。



図 9-77　IGMP プロキシフォワーディングテーブル画面

画面に表示される項目：

項目	説明
グループ アドレス	IPv4 グループマルチキャストアドレスを入力します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

MLD プロキシ

MLD プロキシはアップストリームインタフェースでホストの役割を果たします。MLD Report パケットはルータポートに送信されます。MLD プロキシはダウンストリームインタフェースでルータの役割を果たします。これによりコアネットワークに送信される MLD コントロールパケット数を削減します。

MLD プロキシ設定

MLD プロキシ設定の表示と設定を行います。
MLD プロキシは、単純なツリートポロジでのみ機能します。ツリートポロジにプロキシデバイス以外のマルチキャストルータがないことを確認します。MLD レポートパケットをダウンストリームインタフェースから受信すると、MLD プロキシはメンバシップデータベースを更新します。このパケットは、ダウンストリームインタフェースのすべてのサブスクリプションの統合により生成されます。データベースが変更されると、プロキシデバイスは Unsolicited レポートを送信するか、アップストリームインタフェースから離脱します。また、クエリを受信したときは、アップストリームインタフェースからメンバシップレポートを送信することもできます。

L3 機能 > IP マルチキャストルーティングプロトコル > MLD プロキシ > MLD プロキシ設定の順にメニューをクリックし、以下の画面を表示します。

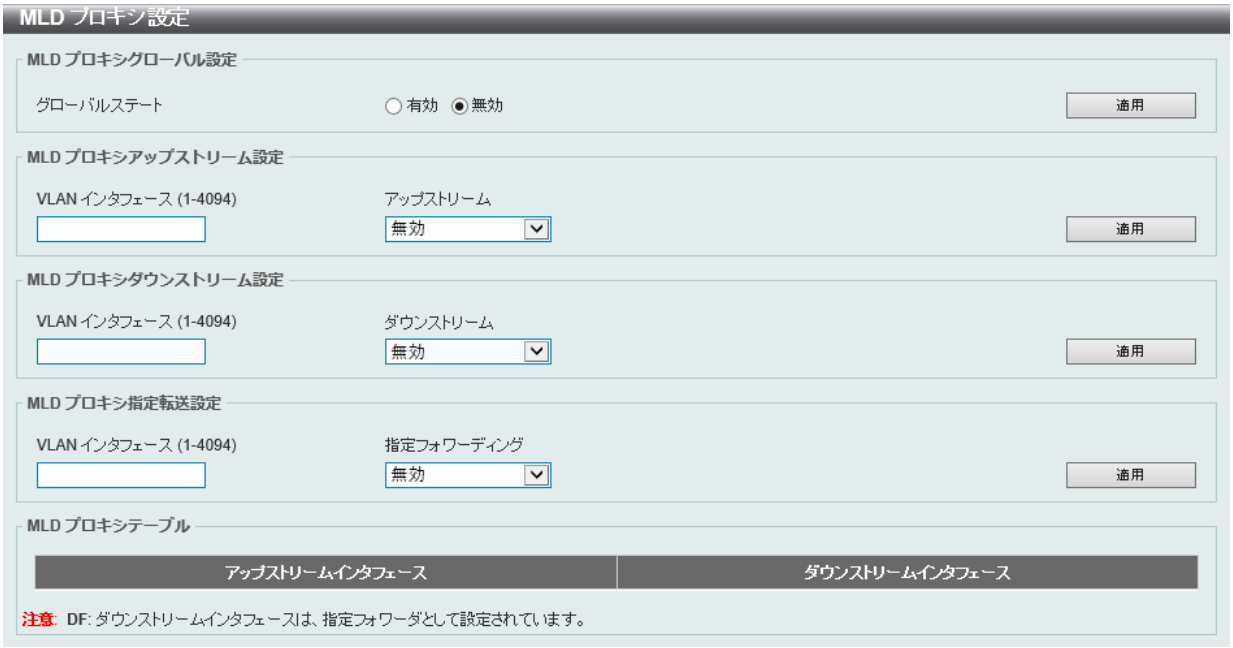


図 9-78　MLD プロキシ設定画面

画面に表示される項目：

項目	説明
MLD プロキシグローバル設定	
グローバルステート	MLD プロキシのグローバルステータスを有効 / 無効に設定します。
MLD プロキシアップストリーム設定	
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
アップストリーム	アップストリーム MLD プロキシとしてインタフェースを有効 / 無効に設定します。 本機能は、インタフェースに IPv6 アドレスが設定されている場合にのみ有効になります。MLD プロキシデバイスに存在できるアップストリームインタフェースは 1 つだけです。
MLD プロキシダウンストリーム設定	
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
ダウンストリーム	ダウンストリーム MLD プロキシとしてのインタフェースを有効 / 無効に指定します。
MLD プロキシ 指定転送設定	
VLAN インタフェース	本設定に適用する VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
指定フォワーディング	非クエリア MLD プロキシダウンストリームインタフェースでの指定転送を有効 / 無効に設定します。 複数の MLD ベースのフォワーダによるダウンストリームリンクと見なされるリンクのローカルループと冗長トラフィックを回避するために、MLD プロキシは MLD クエリア選択を使用して LAN 上の単一のフォワーダを選択します。このオプションにより、非クエリアデバイスをフォワーダにすることができます。この機能は、インタフェースがダウンストリームインタフェースとして設定されていない場合、またはアップストリームインタフェースとして設定されている場合は有効になりません。

「適用」をクリックして各セクションで行った変更を適用します。

MLD プロキシグループテーブル

MLD プロキシグループテーブルを参照します。

L3 機能 > IP マルチキャストルーティングプロトコル > MLD プロキシ > MLD プロキシ グループテーブルの順にメニューをクリックし、以下の画面を表示します。



図 9-79　MLD プロキシグループテーブル画面

画面に表示される項目：

項目	説明
グループ アドレス	IPv6 グループマルチキャストアドレスを入力します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

MLD プロキシ 転送テーブル

MLD プロキシ転送情報を表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > MLD プロキシ > MLD プロキシ転送テーブルの順にメニューをクリックし、以下の画面を表示します。



図 9-80　MLD プロキシ 転送テーブル画面

画面に表示される項目：

項目	説明
グループ アドレス	IPv6 グループマルチキャストアドレスを入力します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

DVMRP

L3 機能 > IP マルチキャストルーティングプロトコル > DVMRP

DVMRP インタフェース設定

DVMRP（Distance Vector Multicast Routing Protocol）インタフェース設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > DVMRP > DVMRP インタフェース設定の順にメニューをクリックして以下の画面を表示します。



図 9-81　DVMRP インタフェース設定画面

画面に表示される項目：

項目	説明
インタフェース名	DVMRP のインタフェース名を入力します。

「検索」をクリックして、入力したインタフェースを検出します。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ エントリの編集

編集するエントリの「編集」をクリックして以下の画面を表示します。



図 9-82　DVMRP インタフェース設定（編集）画面

画面に表示される項目：

項目	説明
隣接タイムアウト	ネイバの有効期間を指定します。指定時間までに、ルータがネイバからのプルーブメッセージを受信しない場合、ネイバはダウンしていると判断されます。 • 設定可能範囲：1-65535（秒） • 初期値：35（秒）
Probe 時間	DVMRP プルーブ間隔の値を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：10（秒）
メトリック	メトリック値を指定します。報告された各送信元ネットワークに対し、報告されたルートにルートメトリックが関連付けられます。メトリックは、レポートを発信するルータとソースネットワーク間のインタフェースメトリックの合計です。DVMRP の場合、「32」の値は到達不能であることを意味します。DVMRP ネットワーク全体の幅を制限し、プロトコルの収束時間に上限を設けるために必要です。 • 設定可能範囲：1-32
状態	指定インタフェースでの DVMRP 機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

DVMRP ルーティングテーブル

スイッチにおける DVMRP ルーティングテーブルを表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > DVMRP > DVMRP ルーティングテーブルの順にメニューをクリックして以下の画面を表示します。



図 9-83　DVMRP ルーティングテーブル画面

画面に表示される項目：

項目	説明
送信元ネットワーク	送信先の IPv4 ネットワークアドレスとネットマスクを入力します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。

DVMRP 隣接テーブル

スイッチにおける DVMRP 隣接（ネイバ）テーブルを表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > DVMRP > DVMRP 隣接テーブルの順にメニューをクリックして以下の画面を表示します。

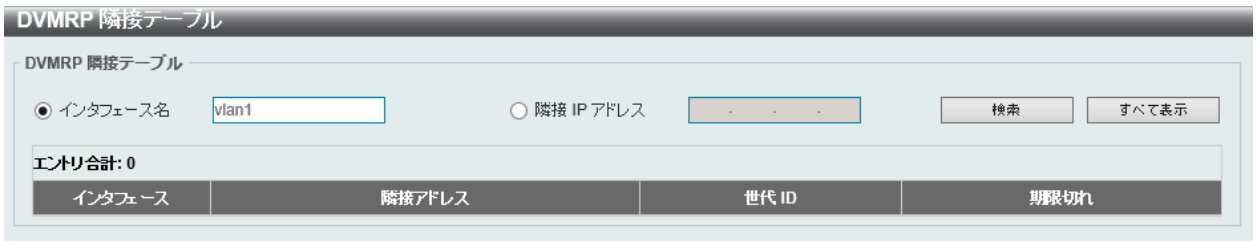


図 9-84　DVMRP 隣接テーブル画面

画面に表示される項目：

項目	説明
インタフェース名	インタフェース名を入力します。
隣接 IP アドレス	ネイバの IP アドレスを入力します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。

PIM

L3 機能 > IP マルチキャストルーティングプロトコル > PIM

PIM（Protocol Independent Multicast）は、LAN、WAN 、またはインターネット上にデータの 1 対多および多対多の配布を提供する IP（Internet Protocol）ネットワーク用のマルチキャストルーティングプロトコルのファミリです。
PIM は、自身のトポロジ検出メカニズムを含まないため、プロトコルに依存しませんが、RIP または OSPF など他の従来型ルーティングプロトコルが提供するルーティング情報を使用します。本スイッチは Dense Mode（PIM-DM）、Sparse Mode（PIM-SM）、PIM Source Specific multicast（PIM-SSM）、および Sparse-Dense Mode（PIM-DM-SM）の 4 つの PIM タイプをサポートしています。

● PIM-SM（Protocol Independent Multicast-Sparse Mode）

Sparse Mode（PIM-SM）は、基本的なユニキャストルーティング情報または個別のマルチキャストが可能なルーティング情報をベースに使用できるマルチキャストルーティングプロトコルです。これは、グループごとの RP（Rendezvous Point）をルートとする単方向の共有ツリーを構築し、オプションで送信元ごとに最短パスツリーを作成します。

PIM-SM は、ネットワークをマルチキャストパケットでフラッドさせる多くのマルチキャストルーティングプロトコルと異なり、Rendezvous Point（RP）を使用して、明示的にマルチキャストグループに属するルータに対してトラフィックを転送します。この RP は PIM-SM が有効であるルータからすべてのリクエストを取得し、その情報を分析してから、送信元から受信したマルチキャスト情報を、ネットワーク内の要求ルータに対して返します。この方法により、RP をルートとして配送ツリーが作成されます。この配送ツリーには、PIM-SM が有効であるすべてのルータが含まれ、これらのルータから収集された情報は RP によって保持されます。
マルチアクセスネットワーク内に複数のルータが存在する場合、代表ルータ（DR）が選出されます。DR の主な機能は、RP に Join/Prune メッセージを送信することです。LAN 上で最も高いプライオリティを持つルータが DR として選出されます。最も高いプライオリティを持つルータが複数存在する場合、より高い IP アドレスを持つルータが選出されます。
PIM-SM 設定で作成される 3 番目のルータタイプは、Boot Strap Router（BSR）です。BSR の目的は、RP 情報を収集し、LAN 上の PIM-SM が有効であるルータにリレーすることです。RP はスタティックに設定することができますが、BSR メカニズムによって RP を決定することもできます。ネットワーク上には複数の Candidate BSR（C-BSR）を設定できますが、RP 情報を処理するために選出され BSR は 1 つのみです。BSR となる C-BSR が指定されていない場合、すべての C-BSR は、PIM-SM が有効であるネットワークに Boot Strap Messages（BSM）を発信し、より高いプライオリティを持つ C-BSR が BSR として選出されます。選出された BSR は、PIM-SM ネットワークで Candidate RP から送信される RP データを収集し、コンパイルしてから、定期的なブートストラップメッセージ（BSM）を使用して LAN 上に送信します。すべての PIM-SM ルータは Boot Strap メカニズムから RP 情報を取得し、データベースに保存します。

● マルチキャストグループの検出と参加

PIM-SM ルータは Hello パケットにより検出されますが、これらのルータは、DR と RP 間で交換される Join/Prune メッセージを介してのみ、マルチキャストグループへ参加または「Pruned（削除）」されます。Join/Prune メッセージは、どのインタフェースでマルチキャストデータを受信するか / しないかを効果的に記述している、ルータ間で中継されるパケットです。ネットワーク上でこれらのメッセージが送信される頻度を設定することが可能です。また、Hello パケットが最初に受信されたルータに対してのみ有効です。Hello パケットは、ルータが存在すること、RP の配信ツリーの一部になる準備ができていることを単純に記載したものです。ルータが IGMP グループのメンバを受け入れ、PIM-SM が有効である場合、関連ルータは明示的な Join/Prune メッセージを RP に送信します。RP は送信元から関連ルータにマルチキャストデータをルーティングし、グループの単一方向の配布ツリーを生成します。その後、マルチキャストパケットがこれらのツリー上の全ノードに送信されます。RP の配布ツリーのメンバであるルータで Prune メッセージを受信すると、ルータは配布ツリーからインタフェースを破棄します。

● 配信ツリー

PIM-SM プロトコルには、Rendezvous-Point Tree（RPT）および最短経路ツリー（Shortest Path Tree：SPT）の 2 種類の配布ツリーがあります。
RP は、マルチキャストデータを受信することが可能なすべての外向きインタフェースに対し、送信元から受信した特定のマルチキャストデータを送信しますが、ルータが送信元の位置を決定すると、送信元と宛先間のホップ（RP など）を削除して、SPT が生成することができます。これは、マルチキャストデータ転送速度のしきい値により設定することができます。しきい値を越えると、データの経路は SPT に切り換わります。これにより、以前使用されていたホップを削除して、マルチキャストパケットが送信元から最終到達先に送信される時間を短縮することで、より近いリンクを送信元と宛先の間で作成することが可能となります。

● Register と Register-stop メッセージ

マルチキャストソースは、意図する受信グループに常に参加するとは限りません。最初のホップルータ（DR）は、グループのメンバでなくても、または明示された送信元を持たなくてもマルチキャストデータを送信することができます。これは、この情報を RP 配信ツリーに中継する方法についての情報を持っていないと言うことを意味しています。この問題は、Register と Register-Stop メッセージにより緩和されます。DR が受信した最初のマルチキャストパケットはカプセル化され、RP に送信されます。RP はこのカプセル化を解いて RP 配信ツリーにパケットを送信します。
ルートが確立すると、ルータをソースに直接接続するための SPT が作成されるか、マルチキャストトラフィックは DR から RP に送信されます。後者の場合、カプセル化されているパケットとカプセル化されていないパケットで、同じパケットが 2 回送信される可能性があります。RP がこの不備を検出すると、Register-stop メッセージを DR に返して、カプセル化されたパケットの送信を中止するように要求します。

● Assert メッセージ

PIM-SM 対応ネットワークにおいて、送信元から受信先へのパラレルパスが作成されることがあります。
これは、複数の受信先が 2 回同じマルチキャストパケットを受信することを意味します。この状況を改善するために、受信デバイスから両方のマルチキャストソースに対して Assert メッセージが送信され、どのルータが受信者に必要なマルチキャストデータを送信するかを決定します。最短メトリック（ホップカウント）を持つ送信元がプライマリマルチキャストソースとして選出されます。このメトリック値は Assert メッセージ内に含まれています。

● PIM-SSM

SSM（Source Specific Multicast）機能は、IP マルチキャストの拡張機能です。
データトラフィックは、レシーバが明示的に参加しているマルチキャスト送信元のみからレシーバに送信されます。SSM 範囲のマルチキャストグループでは、送信元を指定したマルチキャスト配信ツリー（共有ツリーなし）のみ作成可能です。
IANA（Internet Assigned Numbers Authority）は SSM アプリケーションとプロトコル用に 232.0.0.0 ～ 232.255.255.255 のアドレス範囲を予約しています。スイッチは IP マルチキャストアドレス範囲 224.0.0.0 ～ 239.255.255.255 の任意のサブセットに SSM を設定できます。

● PIM-DM

PIM-DM（Protocol Independent Multicast-Dense Mode）プロトコルは、オーバヘッド削減の目的ではなく、マルチキャストパケットの配送を保証するために最適化されているため、低遅延で高帯域のネットワークに適したプロトコルです。
PIM-DM マルチキャストルーティングプロトコルは、下流のルータがマルチキャストメッセージの受信を希望していると仮定し、下流のルータから Prune メッセージ（削除メッセージ）を受けて、マルチキャスト配信ツリーから、マルチキャストグループメンバの存在しない枝葉を Pruned します（削除します）。
PIM-DM には明示的な “Join" メッセージは存在しません。その代わりに、すべてのインタフェースマルチキャストメッセージの定期的なフラッディングに依存し、その後、タイマの期限切れ（Join/Prune インターバル）を待つか、または下流のルータがブランチにマルチキャストメンバが存在しない旨を示す明示的な “Prune" メッセージを送信します。PIM-DM はその後マルチキャスト配信ツリーからこれらのブランチを削除（Prune）します。マルチキャスト配信ツリーから刈り込まれたブランチ（枝）も、マルチキャスト配信グループへの参加を（将来的に）希望する可能性があります。そのため、プロトコルは定期的にデータベースから “Prune（削除）" 情報を削除し、そのブランチ上のすべてのインタフェース宛てにマルチキャストメッセージのフラッディングを行います。この、“Prune" 情報の削除を行う間隔が Join/Prune インターバルです。

● PIM-SM-DM

PIM-SM では、RP は送信側の最初のホップのキーポイントとなります。
送信者が情報を送信するときに最初のホップに RP 情報がない場合、パケットを破棄し、何も実行しません。Sparse-Dense モードはこのようなケースで有用です。Sparse-Dense モードでは、パケットがすべての外向きのインタフェースでフラッドし、RP が検出されない場合に pruning/joining（Prune/Graft）を使用して外向きのインタフェースを制御することが可能です。つまり、PIM Sparse-Dense モードは、Sparse モードまたは Dense モードのいずれかで動作します。これは、マルチキャストグループがどのモードで動作するかによって異なります。インタフェースがマルチキャストトラフィックを受信する場合、グループに既知の RP があれば、インタフェースの現在の操作モードは Sparse モードになり、そうでない場合、インタフェースの現在の操作モードは Dense モードになります。

IPv4 PIM

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM

■ PIM インタフェース

PIM インタフェースの設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM インタフェース の順にメニューをクリックして以下の画面を表示します。



図 9-85　PIM インタフェース画面

画面に表示される項目：

項目	説明
インタフェース名	インタフェース名を指定します。
モード	検出する PIM プロトコルのタイプを選択します。 • 選択肢：「Dense モード」「Sparse モード」「Spare-Dense モード」

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

エントリの編集

「編集」をクリックして、以下の画面を表示します。



図 9-86　PIM インタフェース詳細画面

画面に表示される項目：

項目	説明
PIM ステート	インタフェースの PIM ステータスを有効 / 無効に設定します。
モード	使用する PIM プロトコルのタイプを選択します。初期値：「Dense モード」 • 「Dense モード」- PIM-DM は、送信元が送信を開始すると、すべてのダウンストリームルータはマルチキャストデータストリームの受信を希望していると想定します。最初に、マルチキャストデータストリームはすべての下流ルータと、グループ・メンバを持つインタフェースにフラッディングされます。ダウンストリームルータやグループメンバがない場合、ルータはマルチキャストデータが必要とされていないことを示すプルーンメッセージを送信します。 • 「Sparse モード」- Sparse Mode のインタフェースでマルチキャストトラフィックを受信すると、最初のホップルータは登録メッセージをカプセル化し、RP へ送信します。ルータがファーストホップでない場合、トラフィックはマルチキャストルートエントリに基づいて転送されます。Sparse モードインタフェースは、ダウンストリームルータから Join メッセージを受信した場合、または Sparse モードのインタフェース上のグループメンバの場合にのみ、Multicast Route メンバのインタフェースとして設定されます。PIM ジョインプロセスにより共有ツリーまたはソースツリーが作成されます。 • 「Sparse-Dense モード」- インタフェースが PIM Sparse-Dense モードとして設定されると、インタフェースにより受信したマルチキャストグループは「sparse」/「dense」モードどちらでも動作が可能になります。インタフェースがマルチキャストトラフィックを受信すると、グループの RP を学習済みの場合、グループは Sparse モードで動作します。そうでない場合、マルチキャストグループは Dense モードで動作します。
PIM パッシブ	PIM パッシブ機能を有効 / 無効に設定します。 パッシブモードが有効の場合、インタフェースは PIM メッセージの送受信を行いません。ルータはネットワークで唯一の PIM ルータとして動作します。この機能は、LAN に PIM ルータが 1 つしかない場合のみ使用してください。
クエリー間隔	Hello メッセージを送信する間隔を入力します。 PIMv2 ルータは、PIM ハローメッセージを介して PIM ネイバを学習します。IP マルチキャスト用に設定されたルータは、PIM ルータを検出するために PIM ハローメッセージを送信します。SM の場合、Hello メッセージを使用して、各 LAN セグメントの指定ルータとして機能するルータも決定されます。設定されたクエリ間隔は、ホールド時間の値としても使用されます。間隔を短く設定すると、応答しないネイバをより迅速に検出できるため、より効率的にフェイルオーバとリカバリを実行できます。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18724（秒） • 初期値：30（秒）
DR プライオリティ	Sparse モードまたは Sparse-Dense モードを選択した場合に、このパラメータを設定できます。 指定ルータ（DR）の優先値を入力します。値が大きいほど、優先順位が高くなります。 Dense モード（DM）では、DR 優先オプションは Hello メッセージで伝送されません。プライオリティ値が最も高いルータが DR になります。複数のルータが同じプライオリティステータスの場合、IP アドレスが最も高いルータが DR になります。Hello メッセージ内の DR プライオリティをサポートしていないルータが LAN 上にある場合、LAN 上のすべてのルータは DR プライオリティを無視し、IP アドレスのみを使用して DR を選択します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-4294967295 • 初期値：1
Join Prune 間隔	Sparse モードまたは Sparse-Dense モードを選択した場合に、このパラメータを設定できます。 Join/Prune メッセージの送信間隔を入力します。Join/Prune インターバルを設定するときは、設定された帯域幅や、接続されたネットワークやリンクで想定されるマルチキャストルートの平均エントリ数などの要素を考慮してください。Sparse モード（SM）の場合、ルータはこの指定間隔に基づいて定期的に Join メッセージを送信します。Join/Prune メッセージの hold-time は「Join Prune 間隔」の 3.5 倍です。受信ルータはこのホールド時間に基づいてタイマーを開始し、このインタフェースで Join メッセージが受信されなかった場合はインタフェースを削除します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18000（秒） • 初期値：60（秒）
BSR ドメイン境界	Bootstrap Router（BSR）ドメイン境界機能を有効 / 無効に設定します。 この機能は、インタフェースで PIM が有効な場合にのみ有効になります。2 つのドメイン間での BSR メッセージの交換を回避するには、別のドメインと境界を結ぶインタフェースでこの機能を使用します。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックして前のページに戻ります。

■ PIM BSR 候補

PIM BSR 候補設定の表示と設定を行います。
この機能は、インタフェースに IP アドレスが設定され、PIM Sparse モードになっている場合にのみ有効になります。

この機能により、ルータは Bootstrap メッセージを送信して、指定されたインタフェースの IP アドレスを CBSR アドレスとしてアナウンスします。ハッシュマスクは、ドメイン内のすべてのルータによって使用され、「グループ範囲 -RP」マッピングの一致するセットからランデブーポイント（RP）にグループをマッピングします（このセットは、すべて同じ最長のマスク長 / 最高のプライオリティを持ちます）。このアルゴリズムは、グループアドレスとマップからの候補 RP のアドレスを入力として取得し、使用する RP アドレスを出力として 1 つ指定します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM BSR 候補の順にメニューをクリックして以下の画面を表示します。

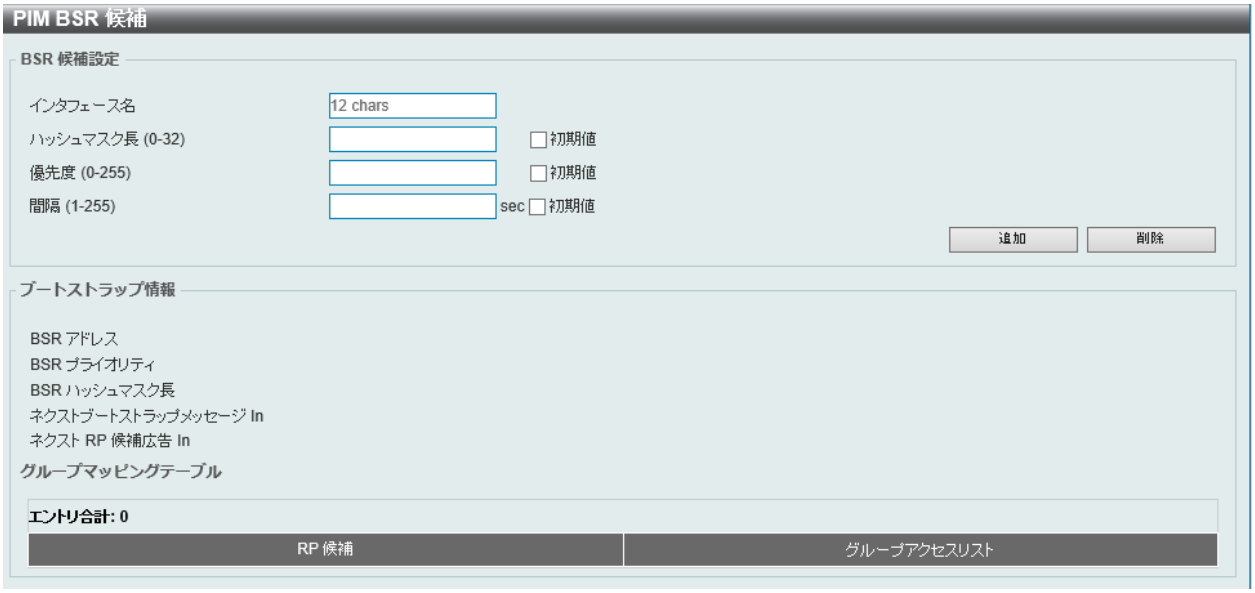


図 9-87　PIM BSR 候補画面

画面に表示される項目：

項目	説明
インタフェース名	インタフェース名を入力します。
ハッシュマスク長	RP 選出で使用するハッシュマスク長を入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-32 • 初期値：30
優先度	「Candidate Bootstrap Router」(CBSR) の優先値を入力します。優先値が最も高い候補が優先されます。優先値が同じ場合は、IP アドレスが最も高いルータが優先されます。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：64
間隔	Bootstrap メッセージの送信間隔を入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255（秒） • 初期値：60（秒）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。

■ PIM RP アドレス

スタティックマルチキャストグループから RP へのマッピングを表示、設定します。
マルチキャストドメインでは、静的マルチキャストグループから RP へのマッピングを BSR と一緒に使用できます。ドメイン内のすべてのルータは、一貫したマルチキャストグループ - RP マッピングを持つ必要があります。レジスタメッセージを開始するファーストホップルータは、マッピングエントリを使用して、特定のグループ宛ての PIM レジスタメッセージを送信するための RP を決定します。Join メッセージを開始するラストホップルータは、マッピングエントリを使用して、特定のグループの Join および Prune メッセージを送信するための RP を決定します。ルータは、Join メッセージを受信すると、メッセージ転送のためにマッピングエントリをチェックします。RP がレジスタメッセージを受信すると、ルータがマルチキャストグループの正しい RP でない場合、レジスタ停止メッセージが送信されます。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM RP アドレスの順にメニューをクリックして以下の画面を表示します。

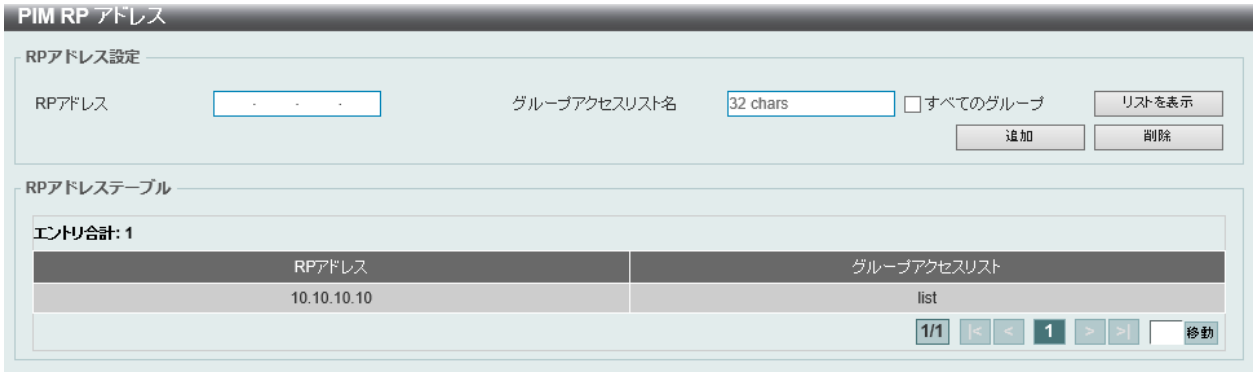


図 9-88　PIM RP アドレス画面

画面に表示される項目：

項目	説明
RP アドレス	RP IPv4 アドレスを入力します。
グループ アクセスリスト名	使用する標準アクセスリストを指定します。 「リストを表示」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。 「すべてのグループ」を指定すると「RP」を全マルチキャストグループにマッピングします。

「適用」をクリックして、設定内容を適用します。

エントリの登録

「追加」をクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「削除」をクリックして、指定エントリを削除します。
「リストを表示」をクリックすると、以下の画面が表示されます。

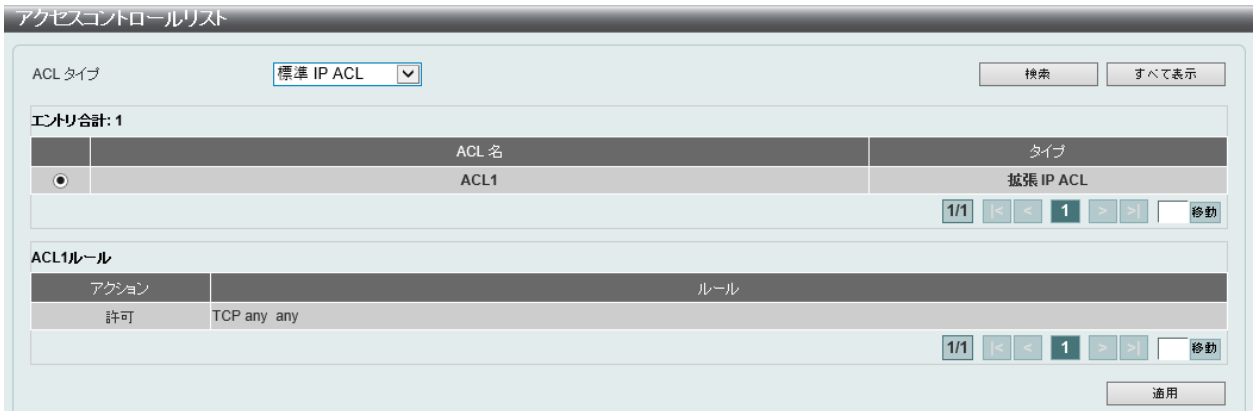


図 9-89　アクセスコントロールリスト 画面

以下の項目を使用します。

項目	説明
ACL タイプ	表示する ACL の種類を指定します。 • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「適用」をクリックして、設定内容を適用します。

■ PIM RP 候補

本画面では PIM RP 候補の設定、表示を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM RP 候補の順にメニューをクリックして以下の画面を表示します。



図 9-90　PIM RP 候補画面

画面に表示される項目：

項目	説明
RP 候補 グローバル設定	
優先度	Candidate RP のプライオリティ値（優先度）を指定します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：192
間隔	Candidate RP のアドバタイズメント間隔をここに入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-16383（秒） • 初期値：60（秒）
ワイルドカードプレフィックスカウント	C-RP メッセージのマルチキャストグループアドレスワイルドカード（224.0.0.0/4）プレフィックスカウント値を入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-1 • 初期値：0
RP 候補設定	
インタフェース名	インタフェース名を入力します。
グループ アクセスリスト名	使用する標準アクセスリストを指定します。 「リストを表示」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。 「すべてのグループ」を指定すると「RP」を全マルチキャストグループにマッピングします。

「適用」をクリックして、設定内容を適用します。
「追加」をクリックして、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」をクリックして、指定エントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「リストを表示」をクリックすると、以下の画面が表示されます。



図 9-91　アクセスコントロールリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	表示する ACL の種類を指定します。 • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「適用」をクリックして、設定内容を適用します。

■ PIM RP テーブル

本画面では PIM RP 情報の検索、表示を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM RP テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-92　PIM RP テーブル画面

以下の項目を使用します。

項目	説明
RP ハッシュ	IPv4 マルチキャストグループアドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

■ PIM レジスタ設定

本画面では PIM レジスタの設定、表示を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM レジスタ設定の順にメニューをクリックして以下の画面を表示します。

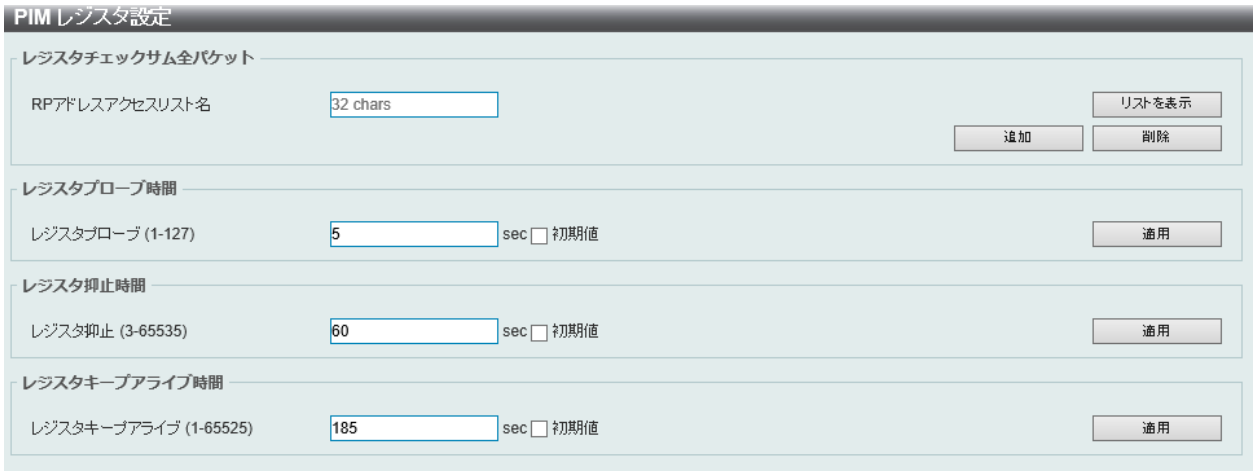


図 9-93　PIM レジスタ設定画面

画面に表示される項目：

項目	説明
レジスタチェックサム全パケット	
RP アドレス アクセスリスト名	使用する標準アクセスリストを指定します。「リストを表示」をクリックすると、定義済みの ACL リストを検出、選択することができます。
レジスタプローブ時間	
レジスタプローブ	レジスタプローブ（Register Probe）時間を入力します。 設定した時間が経過すると、レジスタストップタイマ（RST）が期限切れになり、DR が RP に Null-Register を送信して、RP により Register-Stop メッセージが再送信されます。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-127（秒） • 初期値：5（秒）
レジスタ抑止時間	
レジスタ抑止	レジスタ抑止（Register Suppression）のタイムアウト値を入力します。DR は、Register-Stop メッセージを受信すると、サプレッションタイマを開始します。抑制期間中、DR は RP への Register メッセージの送信を停止します。ファーストホップルータでこの機能を使用してください。レジスタストップタイマの設定で負の値が発生しないようにするには、「レジスタプローブ」時間の値が「レジスタ抑止」時間の半分未満である必要があります。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-65535（秒） • 初期値：60（秒）
レジスタキープアライブ時間	
レジスタキープアライブ	レジスタキープアライブ（Register Keepalive）の時間を入力します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65525（秒） • 初期値：185（秒）

「適用」をクリックして、設定内容を適用します。

「追加」をクリックして、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」をクリックして、指定エントリを削除します。

「リストを表示」をクリックすると、以下の画面が表示されます。



図 9-94　アクセスコントロールリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	表示する ACL の種類を指定します • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「適用」をクリックして、設定内容を適用します。

■ PIM SPT しきい値設定

PIM SPT しきい値を設定します。ルータのラストホップでこの機能を使用します。
PIM-SM モードでは、最初、送信元からのマルチキャストトラフィックは RPT 共有ツリーに沿って受信側に送信されます。最初のパケットがラストホップルータに到着した後、トラフィックの各グループは次の 2 つのモードのいずれかで動作します。「無限」モードでは、トラフィックは引き続き共有ツリーに従います。「0」モードでは、ソースツリーが確立され、トラフィックはソースツリーへの切り替え（スイッチオーバ）が行われます。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM SPT しきい値設定の順にメニューをクリックして以下の画面を表示します。

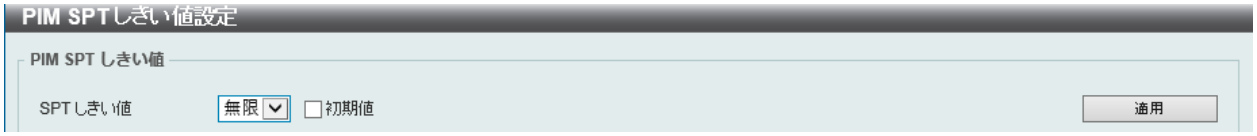


図 9-95　PIM SPT しきい値設定画面

画面に表示される項目：

項目	説明
SPT しきい値	SPT しきい値を指定します。「初期値」にチェックを入れると、初期値を使用します。 • 「無限」- 常に共有ツリーに従います。（初期値） • 「0」- 最初のパケットの到着時にソースツリーを確立します。

「適用」をクリックして、設定内容を適用します。

■ PIM SSM 設定

本画面では PIM SSM の設定、表示を行います。最後のホップルータでのみ使用可能です。SSM が有効な場合、最後のホップルータは、添付のホストから SSM 範囲内で破棄される（S,G）リクエストを含む IGMPv3 を受信するチャンネル（S,G）のソースベースツリーの構築を開始します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM SSM 設定の順にメニューをクリックして以下の画面を表示します。



図 9-96　PIM SSM 設定画面

画面に表示される項目：

項目	説明
マルチキャストグループアドレス名	ユーザ指定の SSM グループアドレスを定義する標準 IP アクセスリストを指定します。 グループアドレスは、ルールエントリの宛先 IP アドレス項目で定義されます。 「リストを表示」から既存のアクセスリストを指定することも可能です。 「デフォルト SSM グループ（232.0.0.0/8）」オプションを指定すると、初期値の SSM グループアドレス（232/8）を指定します。

「追加」をクリックして、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」をクリックして、指定エントリを削除します。

「リストを表示」をクリックすると、以下の画面が表示されます。



図 9-97　アクセスコントロールリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	表示する ACL の種類を指定します。 • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ PIM 隣接テーブル

本画面では PIM 隣接（ネイバ）情報の検索、表示を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv4 PIM > PIM 隣接テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-98　PIM 隣接テーブル画面

以下の項目を使用します。

項目	説明
インタフェース名	PIM-SM ネイバ情報を表示する VLAN インタフェースを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IPv6 PIM

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM
IPv6 用 PIM Sparse モード（PIM-SMv6）および IPv6 用 PIM Dense モード（PIM-DMv6）に関する設定を行います。

■ IPv6 PIM インタフェース

PIM IPv6 インタフェースの設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM インタフェース の順にメニューをクリックして以下の画面を表示します。



図 9-99　IPv6 PIM インタフェース画面

画面に表示される項目：

項目	説明
インタフェース名	VLAN インタフェース名を指定します。
モード	フィルタ検索における IPv6 PIM エントリの操作モードを指定します。 • 選択肢：「Sparse モード」「Dense モード」

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

エントリの編集

「編集」をクリックして、以下の画面を表示します。

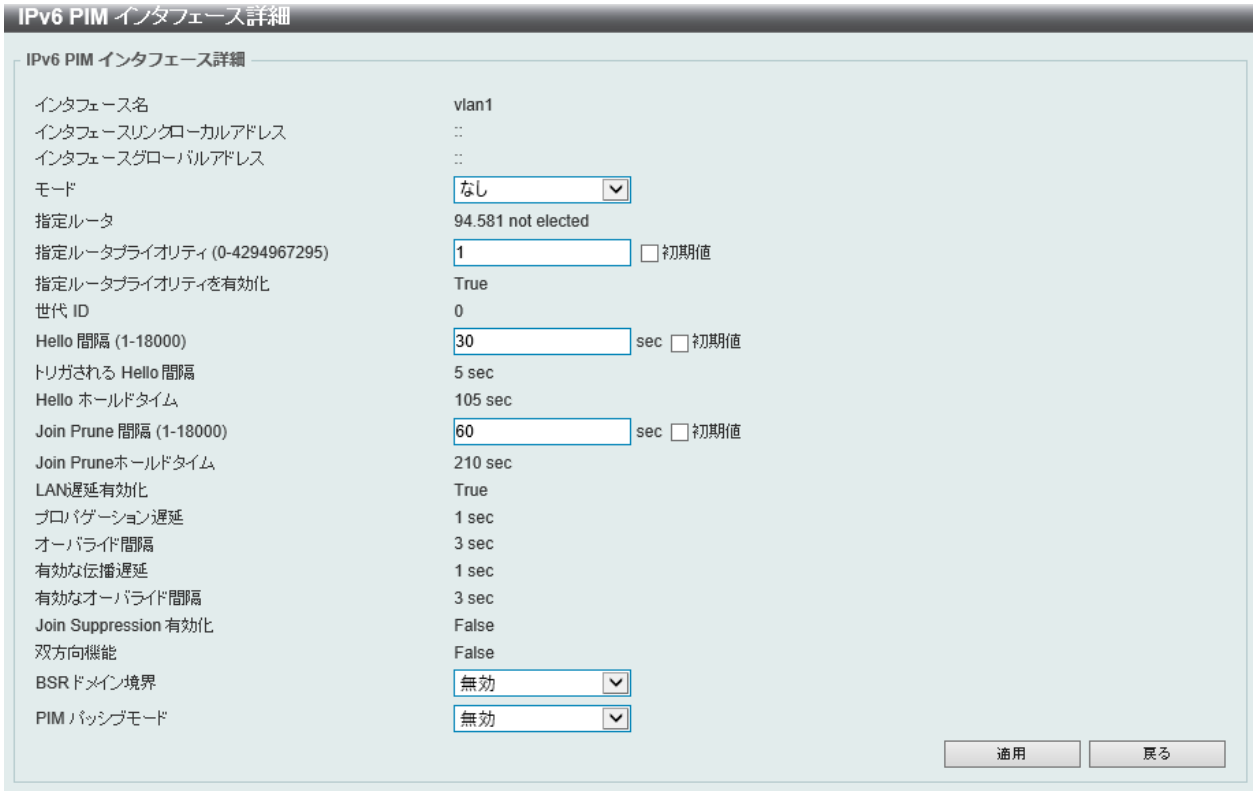


図 9-100　IPv6 PIM インタフェース詳細 画面

画面に表示される項目：

項目	説明
モード	使用する IPv6 PIM プロトコルのタイプを選択します。 「なし」オプションが選択されている場合、IPv6 の PIM はこのインタフェースで無効になります。 • 選択肢：「なし」「Sparse モード」「Dense モード」
指定ルータプライオリティ	指定ルータプライオリティ（Designated Router Priority）値を入力します。値が大きいほど優先順位が高くなります。この機能は、VLAN インタフェースで PIM-SM モードが有効な場合にのみ有効になります。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-4294967295 • 初期値：1 DR が選出の候補である場合、以下の条件が適用されます。 • インタフェースに設定されている最も高いプライオリティ値を持つルータが DR として選択されます。複数のルータが同じ最高値のプライオリティを持つ場合、インタフェースに設定されている最も高い IPv6 アドレスを持つルータが DR として選出されます。 • ルータが Hello メッセージで優先値をアドバタイズしない場合、このルータは最も高いプライオリティを持つと見なされ、DR として選択されます。複数のルータが Hello メッセージに DR プライオリティオプションを含まない場合、最も高い IPv6 アドレスを持つルータが DR として選択されます。
Hello 間隔	Hello メッセージの送信間隔を入力します。PIM ルータは、Hello メッセージを介して PIM ネイバを学習します。 IP マルチキャスト用に設定されたルータは、PIM ルータを検出するために PIM Hello メッセージを送信します。 SM の場合、Hello メッセージは、各 LAN セグメントの指定ルータとして選択されるルータを決定するためにも使用されます。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18000（秒） • 初期値：30（秒）

項目	説明
Join Prune 間隔	Join/Prune メッセージの送信間隔を入力します。 Join/Prune インターバルを設定するときは、設定された帯域幅や、接続されたネットワークやリンクで想定されるマルチキャストルートの平均エントリ数などの要素を考慮してください。（例えば低速リンクや、多数のエントリを持つネットワークの中心に存在するルータでは、この期間は長くなります。） Sparse モード（SM）の場合、ルータはこの指定間隔に基づいて定期的に Join メッセージを送信します。Join/Prune メッセージの hold-time は「Join Prune Interval 」の 3.5 倍です。受信ルータはこのホールド時間に基づいてタイマを開始し、このインタフェースで Join メッセージが受信されなかった場合はインタフェースを削除します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-18000（秒） • 初期値：60（秒）
BSR ドメイン境界	Bootstrap Router（BSR）ドメイン境界機能を有効 / 無効に設定します。 インタフェースが境界として設定されている場合、Bootstrap ルータ（BSR）メッセージが境界を介して送受信されないようにします。
PIM パッシブモード	インタフェースの PIM パッシブ機能を有効 / 無効に設定します。 この機能は、インタフェースで IPv6 PIM が有効な場合にのみ有効になります。パッシブモードが有効の場合、インタフェースは PIM の送受信を行いません。ルータはネットワークで唯一の PIM ルータとして動作します。本機能は LAN 上に PIM ルータが一つしかない場合にのみ使用してください。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックして前のページに戻ります。

■ IPv6 PIM BSR 候補設定

IPv6 PIM BSR Candidate（候補）を設定します。この機能は、PIM-SM 動作にのみ影響します。
これにより、ルータは、指定されたインタフェースのアドレスを BSR アドレスとして、すべての PIM ネイバに Bootstrap メッセージを送信します。
PIM-SM ドメインには、RP 情報の収集とアドバタイズを実行する一意の BSR（Bootstrap ルータ）が含まれている必要があります。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM BSR 候補設定 の順にメニューをクリックして以下の画面を表示します。

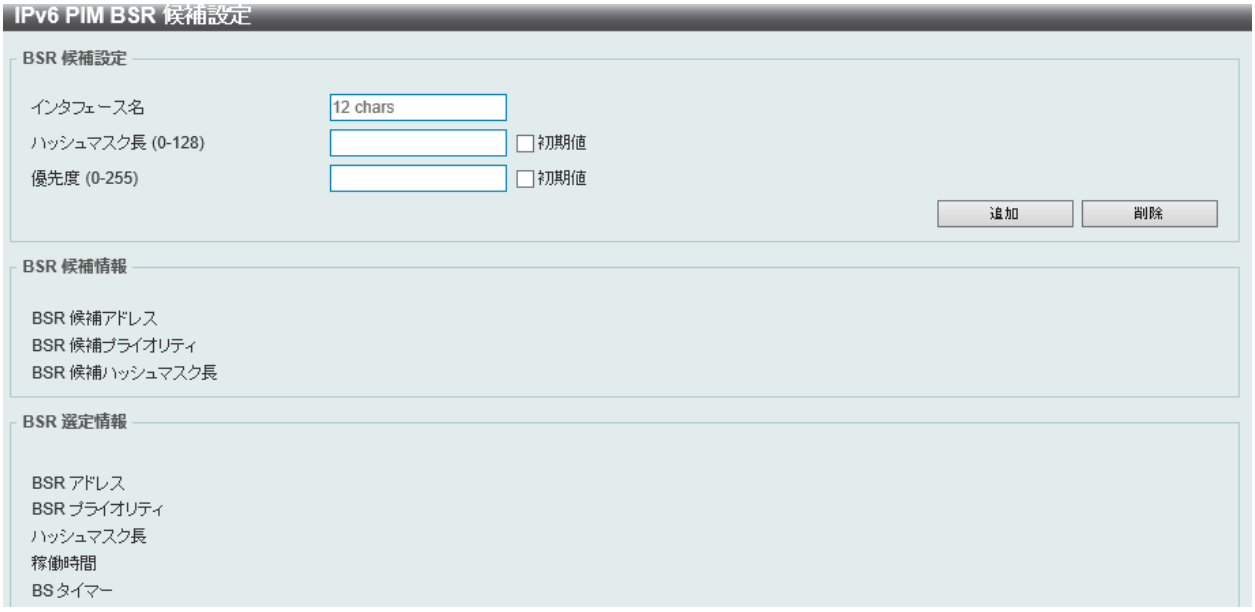


図 9-101　IPv6 PIM BSR 候補設定 画面

画面に表示される項目：

項目	説明
インタフェース名	VLAN インタフェース名を入力します。
ハッシュマスク長	RP 選出で使用するハッシュマスク長を入力します。ハッシュ関数を実行する前にグループアドレスと論理積をとるマスク（最大 128 ビット）です。同じシードハッシュを持つすべてのグループは、同じ RP に対応します。したがって、1 つの RP を複数のグループに派生させることができます。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-128 • 初期値：126
優先度	BSR Candidate の優先値をここに入力します。優先値の高い BSR が優先されます。優先値が同じ場合、IPv6 アドレスが大きい方のルータが BSR になります。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：64

「追加」をクリックし、入力した情報に基づくエントリを追加します。
「削除」をクリックして、指定のエントリを削除します。

■ IPv6 PIM BSR テーブル

「IPv6 PIM BSR」情報を表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM BSR テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-102　IPv6 PIM BSR テーブル画面

■ PIM for IPv6 RP アドレス

IPv6 PIM RP アドレスの設定、表示を行います。この機能は、PIM-SM 動作にのみ影響します。この機能を使用して、Sparse モードで動作するマルチキャストグループの RP アドレスを静的に定義します。

複数のグループに 1 つの RP を使用します。アクセスリストで指定された条件により、RP を使用できるグループが決まります。複数の RP が定義可能で、各 RP は 1 つのアクセスリストを保持します。古い設定は新しい設定により上書きされます。

ドメイン内のすべてのルータは、一貫したマルチキャストグループ - RP マッピングを持つ必要があります。レジスタメッセージを開始するファーストホップルータは、マッピングエントリを使用して、特定のグループ宛ての PIM レジスタメッセージを送信するための RP を決定します。Join メッセージを開始するラストホップルータは、マッピングエントリを使用して、特定のグループの Join および Prune メッセージを送信するための RP を決定します。ルータは、Join メッセージを受信すると、メッセージ転送のためにマッピングエントリをチェックします。RP がレジスタメッセージを受信すると、ルータがマルチキャストグループの正しい RP でない場合、レジスタ停止メッセージが送信されます。

PIM ドメインが組み込み RP を使用している場合、組み込み RP 範囲の RP として静的に設定する必要があるのは RP のみです。他のルータは、IPv6 グループアドレスから RP アドレスを検出します。これらのルータが組み込み RP ではなくスタティック RP を選択する場合は、スタティック RP のアクセスリストで特定の組み込み RP グループ範囲を設定する必要があります。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM RP アドレスの順にメニューをクリックして以下の画面を表示します。



図 9-103　IPv6 PIM RP アドレス画面

画面に表示される項目：

項目	説明
RP アドレス	RP IPv6 アドレスを入力します。
グループ アクセスリスト名	使用する標準 IPv6 アクセスリストを指定します。 「リストを表示」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。 「すべてのグループ」を指定すると「RP」を全マルチキャストグループにマッピングします。
オーバライド	自動的に学習した RP をスタティック RP が上書きします。

「追加」をクリックし、入力した情報に基づくエントリを追加します。
「削除」をクリックして、指定エントリを削除します。

「リストを表示」をクリックすると、以下の画面が表示されます。



図 9-104　アクセスコントロールリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	表示する ACL の種類を指定します。 • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM RP 候補

IPv6 PIM RP（Rendezvous Point）Candidate に関連する項目を設定します。インタフェース毎に 1 つのアクセスリストのみ指定可能です。古い設定は新しい設定に上書きされます。異なるインタフェースに対してそれぞれ設定することが可能です。
この設定により、ルータは自身を Candidate RP として通知する PIMv2 メッセージを BSR に送信します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM RP 候補 の順にメニューをクリックして以下の画面を表示します。



図 9-105　IPv6 PIM RP 候補 画面

画面に表示される項目：

項目	説明
インタフェース名	Candidate RP として機能するインタフェースを入力します。 このインタフェースの IPv6 アドレスが、Candidate RP（C-RP）としてアドバタイズされます。
グループ アクセスリスト名	使用する標準アクセスリストを指定します。 「リストを表示」をクリックするとスイッチに既存作成されている ACL リストを検出、選択することができます。 「すべてのグループ」を指定すると「RP」を全マルチキャストグループにマッピングします。
優先度	RP 優先度の値を入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：192
間隔	RP Candidate の通知間隔を入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-16383（秒） • 初期値：60（秒）

「追加」をクリックして、入力した情報に基づいて新しいエントリを追加します。

「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

エントリの削除
削除するエントリの「削除」をクリックします。

「リストを表示」をクリックすると、以下の画面が表示されます。

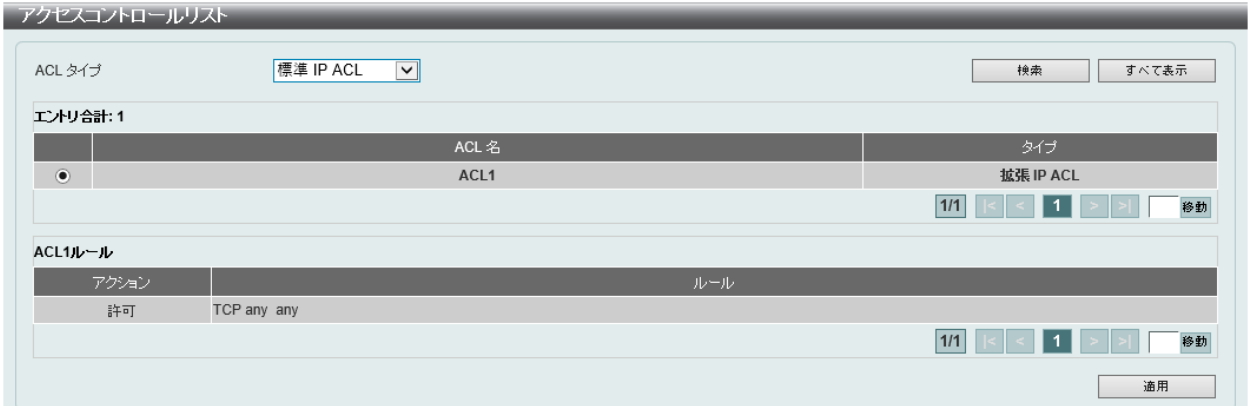


図 9-106　アクセスコントロールリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	表示する ACL の種類を指定します。 • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「適用」をクリックして、設定内容を適用します。

「編集」をクリックすると以下の画面が表示され、「RP 候補テーブル」欄の編集が可能となります。



図 9-107　PIM for IPv6 RP 候補（編集）画面

画面に表示される項目：

項目	説明
優先度	RP 優先値を指定します。 • 設定可能範囲：0-255
間隔	RP 候補（RP Candidate）の通知間隔値を指定します。 • 設定可能範囲：1-16383（秒）

「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM Enbedded RP 設定

本項目では、IPv6 PIM Embedded の設定と表示を行います。
「Embedded RP」は IPv6 マルチキャストグループアドレスにエンコードされた RP のアドレスを定義するアドレス割当ポリシーです。これにより、スケーラブルなドメイン間マルチキャストの容易な展開が可能になり、ドメイン内マルチキャスト設定も簡素化されます。IPv6RP 情報が埋め込まれたマルチキャストグループアドレスは、ff70::/12 で始まり、フラグ値 7 は埋め込み RP を意味します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM Enbedded RP 設定の順にメニューをクリックして以下の画面を表示します。

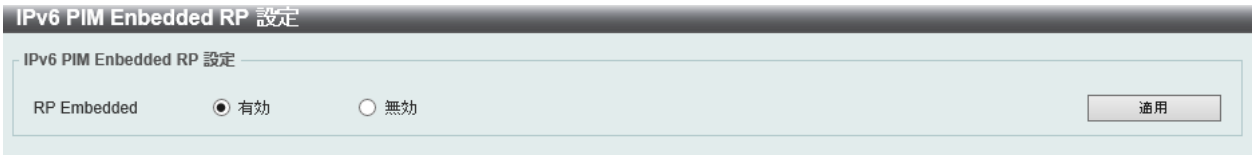


図 9-108　IPv6 PIM Enbedded RP 設定画面

画面に表示される項目：

項目	説明
RP Embedded	RP 埋め込み機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM RP テーブル

本項目では、IPv6 PIM RP 情報を表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM RP テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-109　IPv6 PIM RP テーブル画面

画面に表示される項目：

項目	説明
グループ アドレス / プレフィックス長	マルチキャストグループ IPv6 アドレスとプレフィクス長を指定します。
情報送信元	表示する情報送信元を指定します。 • 「ブートストラップ」- BSR を通じて学習した範囲を表示します。 • 「Embedded RP」- 埋め込み RP を通じて学習したグループ範囲を表示します。 • 「スタティック」- 手動設定で指定した範囲を表示します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

■ IPv6 PIM レジスタ設定

本画面では IPv6 PIM レジスタの設定、表示を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM レジスタ設定の順にメニューをクリックして以下の画面を表示します。



図 9-110　IPv6 PIM レジスタ設定画面

画面に表示される項目：

項目	説明
	レジスタチェックサム全パケット
レジスタチェックサム全パケット	全パケットのレジスタチェックサムを有効 / 無効に設定します。 本設定を有効にした場合、ルータはデータ部分を含めた全 PIM メッセージのレジスタメッセージのチェックサムを計算します。デフォルトでは、レジスタチェックサム方法は、レジスタメッセージのデータ部分を除いて、PIM RFC に準拠しています。
	レジスタプローブ 時間
レジスタプローブ	レジスタプローブ（Register Probe）時間を入力します。 レジスタプローブ時間は、DR が RP に Null-Register を送信して Register-Stop メッセージを再送信する場合に、Register-Stop Timer（RST）が期限切れになるまでの時間です。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-127（秒） • 初期値：5（秒）
	レジスタ抑止時間
レジスタ抑止	レジスタ抑止（Register Suppression）のタイムアウト値を入力します。 DR は、Register-Stop メッセージを受信すると、サプレッションタイマを開始します。抑制期間中、DR は RP への Register-encapsulated データの送信を停止します。指定ルータでこの機能を使用してください。レジスタストップタイマの設定で負の値が発生しないようにするには、「レジスタプローブ」時間の値が「レジスタ抑止」時間の半分未満である必要があります。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-65535（秒） • 初期値：60（秒）

「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM SPT しきい値設定

本画面では PIM for IPv6 SPT しきい値を表示、設定します

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM SPT しきい値設定 の順にメニューをクリックして以下の画面を表示します。

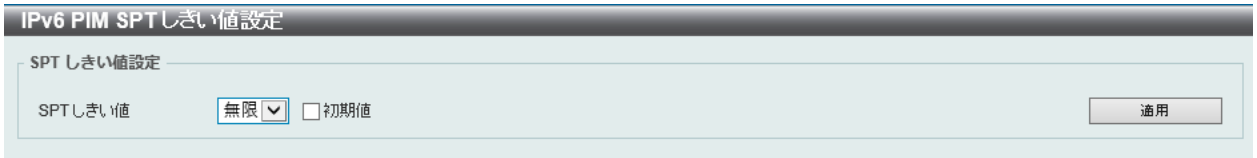


図 9-111　IPv6 PIM SPT しきい値設定 画面

画面に表示される項目：

項目	説明
SPT しきい値	SPT しきい値を指定します。「初期値」にチェックを入れると、初期値を使用します。 • 「0」- 最初のパケットの到着時にソースツリーを確立します。 • 「無限」- 常に共有ツリーに従います。（初期値）

「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM SSM 設定

本画面では IPv6 PIM SSM の設定、表示を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM SSM 設定の順にメニューをクリックして以下の画面を表示します。



図 9-112　IPv6 PIM SSM 設定画面

画面に表示される項目：

項目	説明
マルチキャストグループアドレス名	ユーザ指定の SSM グループアドレスを定義するアクセスリストを指定します。 「リストを表示」から既存のアクセスリストを指定することも可能です。 「デフォルト SSM グループ」オプションを指定すると、初期値の SSM グループアドレス（FF3x::/32）を使用します。

「追加」をクリックして、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」をクリックして、指定エントリを削除します。

「リストを表示」をクリックすると、以下の画面が表示されます。



図 9-113　アクセスコントロールリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	表示する ACL の種類を指定します。 • 選択肢：「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ACL リスト	使用するアクセスリストを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM（S,G）キープアライブ時間

本項目では「IPv6 PIM（S,G）」キープアライブ時間の設定、表示を行います。
明示的な（S, G）ローカルメンバシップや（S, G）ジョインメッセージの受信がない間、PIM ルータが（S, G）ステートを維持するキープアライブタイマを指定します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM（S,G）キープアライブ時間の順にメニューをクリックして以下の画面を表示します。



図 9-114　IPv6 PIM（S,G）キープアライブ時間画面

画面に表示される項目：

項目	説明
(S,G) キープアライブ時間	(S,G) キープアライブ時間を入力します。これは、明示的な（S,G）ローカルメンバーシップまたはそれを維持するために受信する（S,G）Join メッセージがない場合に、PIM ルータが（S,G）状態を維持する時間です。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：120-65535（秒） • 初期値：210（秒）

「適用」をクリックして、設定内容を適用します。

■ IPv6 PIM マルチキャストルートテーブル

IPv6 マルチキャストルーティングテーブルの全エントリを表示します。
スイッチスターグループ（*,G）エントリからソースグループ（S,G）エントリを作成することにより、マルチキャストルーティングテーブルを設定します。スター（*）は全ソースアドレスを意味し、"S" は単一ソースアドレス、"G" は宛先マルチキャストグループアドレスを意味します。
(S,G) エントリの作成には、ソフトウェアは「Reverse Path Forwarding」(RPF) を通じてユニキャストルーティングテーブル内で見つかった宛先グループへの最適パスを使用します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > IPv6 PIM > IPv6 PIM マルチキャストルートテーブルの順にメニューをクリックして以下の画面を表示します。



図 9-115　IPv6 PIM マルチキャストルートテーブル画面

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
「詳細を表示」をクリックするとエントリの詳細情報が表示されます。

■ IPv6 PIM 隣接テーブル

現在の IPv6 PIM 隣接（ネイバ）ルータテーブルを表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > PIM for IPv6 > IPv6 PIM 隣接テーブル の順にメニューをクリックして以下の画面を表示します。



図 9-116　IPv6 PIM 隣接テーブル 画面

画面に表示される項目：

項目	説明
インタフェース名	VLAN インタフェース名を指定します。
モード	フィルタ検索における IPv6 PIM エントリの操作モードを選択します。 • 選択肢：「Sparse モード」「Dense モード」

「検索」をクリックして、入力したインタフェースを検出します。
「すべて表示」をクリックして、本スイッチに定義済みの全インタフェースを表示します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。

MSDP

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > MSDP

■ MSDP グローバル設定

Multicast Source Discovery Protocol（MSDP）の表示、グローバル設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > MSDP > MSDP グローバル設定 の順にメニューをクリックして以下の画面を表示します。



図 9-117　MSDP グローバル設定画面

画面に表示される項目：

項目	説明
グローバルステート	MSDP のグローバルステータスを有効 / 無効に設定します。
接続リトライ間隔	接続再試行間隔を入力します。これは、ピア・セッションのリセットから再確立の試行までの間に、MSDP ピアが待機する時間を設定するために使用されます。時間間隔を大きくすると、ピア・セッションの再確立を試行するまでの時間が遅延します。最適な結果を得るには、1-60 秒の範囲で値を設定します。 「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
SA キャッシュ期限切れ時間	Source-Active（SA）キャッシュエントリの有効期限を入力します。SA の発信元の間隔は 60 秒であり、変更できません。SA キャッシュの有効期限により、ネットワーク上で予期されるパケット損失の暗黙的なチューニングが可能になります。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：65-65535（秒）
SA 発信元フィルタ	「設定済」を指定し、SA オリジナルフィルタの文字列を指定します。文字列は 32 字以内で指定します。RP によって MSDP の実行が設定されていて、該当の RP をレジスタする全ローカルソースへの SA メッセージを作成します。リストのフィルタ設定により、RP は、通常 IP アクセスリストでマッチする指定グループに送信する、ローカルソースへの SA メッセージを開始します。 「設定済」オプションを選択してフィルタ文字列を指定しない場合、全ローカルソースのオリジナル SA メッセージからの RP を防ぐことができます。

「適用」をクリックして、設定内容を適用します。

■ MSDP ピア設定

Multicast Source Discovery Protocol（MSDP）の表示、ピア設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > MSDP > MSDP ピア設定の順にメニューをクリックして以下の画面を表示します。



図 9-118　MSDP ピア設定画面

画面に表示される項目：

項目	説明
IP MSDP ピア	MSDP ピア IP アドレスを指定します。
接続インタフェース	接続インタフェースを指定します（12 文字以内）。 TCP 接続のソース IP アドレスとして使用するローカルインタフェースを指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「クリア」をクリックすると入力したエントリをクリアします。
「すべてをクリア」をクリックすると入力したエントリを全てクリアします。
「統計をクリア」をクリックすると入力したエントリの統計情報をクリアします。
「すべての統計をクリア」をクリックすると入力したエントリの統計情報を全てクリアします。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。
「編集」をクリックして、指定エントリの編集を行います。

設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「編集」をクリックすると、以下の画面が表示されます。

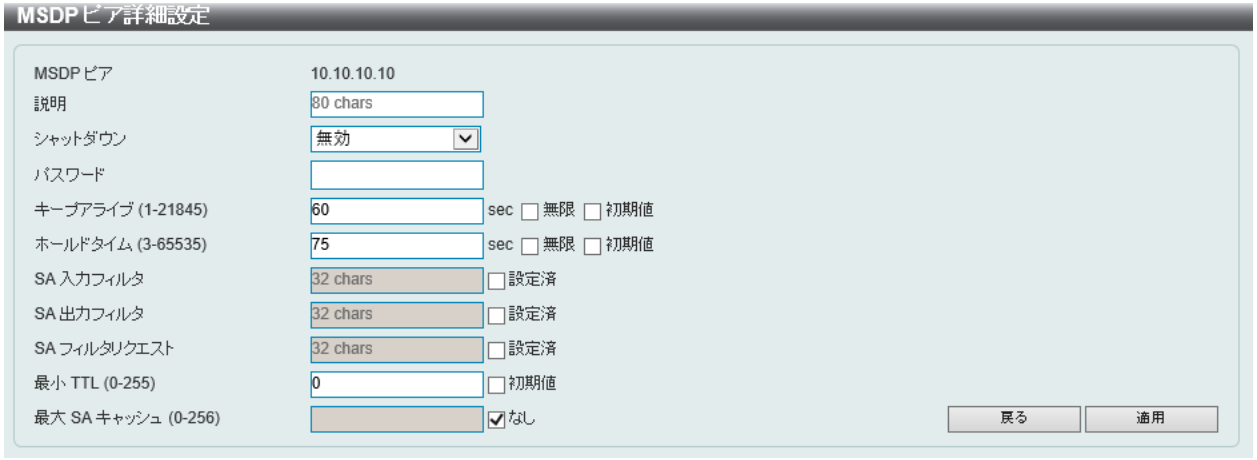


図 9-119　MSDP ピア 詳細設定画面

画面に表示される項目：

項目	説明
説明	MSDP ピアの説明を指定します。（80 文字以内）
シャットダウン	シャットダウン機能を有効 / 無効に設定します。 シャットダウン状態は、既存の MSDP ピアで設定する必要があります。MSDP ピアがシャットダウン状態の場合、2 つのピア間の TCP 接続は確立されません。MSDP ピアがシャットダウン状態でなくなる場合、2 つのピア間の TCP 接続は再確立を試みます。
パスワード	2 つのピア間の TCP 接続用の MD5 パスワードを入力します。 MD5 認証は、両方の MSDP ピアで同じパスワードを使用する必要があります。パスワードが異なる場合、ピア間の接続を確立できません。
キープアライブ	キープアライブの時間を入力します。 キープアライブ間隔は、MSDP TCP 接続のリモート側で設定されたホールド時間より短くする必要があります。そうでない場合、MSDP Keep-Alive メッセージを受信する前に、MSDP TCP 接続のリモート側が切断される可能性があります。「無限」オプションを指定すると、キープアライブメッセージを送信しないように MSDP ピアを設定します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-21845（秒） • 初期値：60（秒）
ホールドタイム	ホールドタイムの値を入力します。 Hold Time インターバルは、MSDP TCP 接続のリモート側で設定されたキープ・アライブ・タイムよりも大きくなければなりません。そうでない場合、MSDP Keep-Alive メッセージを受信する前に MSDP TCP 接続が切断される可能性があります。2 つのピア間の接続が切断されないように指定するには、「Infinity」オプションを選択します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：3-65535（秒）
SA 入力フィルタ	「設定済」オプションを選択し、SA filter-in 文字列を入力します（32 文字以内）。 ルータは、指定されたピアから送信されたすべての SA メッセージを受信します。この文字列を指定しないと、ルータは指定されたピアから送信されたすべての SA メッセージを無視します。この文字列を設定することで、ルータは、標準 IP アクセスリストで定義されている（S,G）ペアに一致する指定されたピアからの受信 SA メッセージのみを受信します。
SA 出力フィルタ	「設定済」オプションを選択し、SA filter-Out 文字列を入力します（32 文字以内）。 ルータは、すべての SA メッセージを MSDP ピアに転送します。この文字列を指定しないと、ルータは指定されたピアへの SA メッセージの転送を停止します。この文字列を指定することで、ルータは、標準 IP アクセスリストで定義されている（S,G）ペアに一致する SA メッセージのみを、指定されたピアに転送します。
SA フィルタリクエスト	「設定済」オプションを選択し、SA filter-Request 文字列を入力します（32 文字以内）。 ルータは、指定されたピアからのすべての SA 要求メッセージを処理します。この文字列を指定しないと、ルータは指定されたピアからの Source-Active 要求メッセージの処理を停止します。この文字列を指定することで、ルータは、指定されたピアからの標準 IP アクセスリストで定義されているグループを要求する SA 要求メッセージのみを処理します。
最小 TTL	最小 TTL 値を入力します。 SA メッセージが MSDP ピアから送信されるときに、SA メッセージ内のマルチキャストデータパケットの Time-To-Live（TTL）値が減少する際、減少した TTL 値が SA メッセージが送信された MSDP ピアの最小 TTL 値より小さいと、SA は送信されません。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：0-255 • 初期値：0
最大 SA キャッシュ	SA キャッシュの最大値を入力します。 SA キャッシュエントリの最大値が 0 に設定されている場合、本スイッチはピアから SA キャッシュエントリを学習できません。SA キャッシュエントリの最大値が既存の SA キャッシュエントリより小さい場合、SA キャッシュエントリの数が最大値に等しくなるまで、古い既存の SA キャッシュエントリは削除されます。 「なし」オプションを指定すると、Source-Active キャッシュエントリの数を制限しません。 • 設定可能範囲：0-256

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックすると前のページに戻ります。

「詳細を表示」をクリックすると、以下の画面が表示されます。

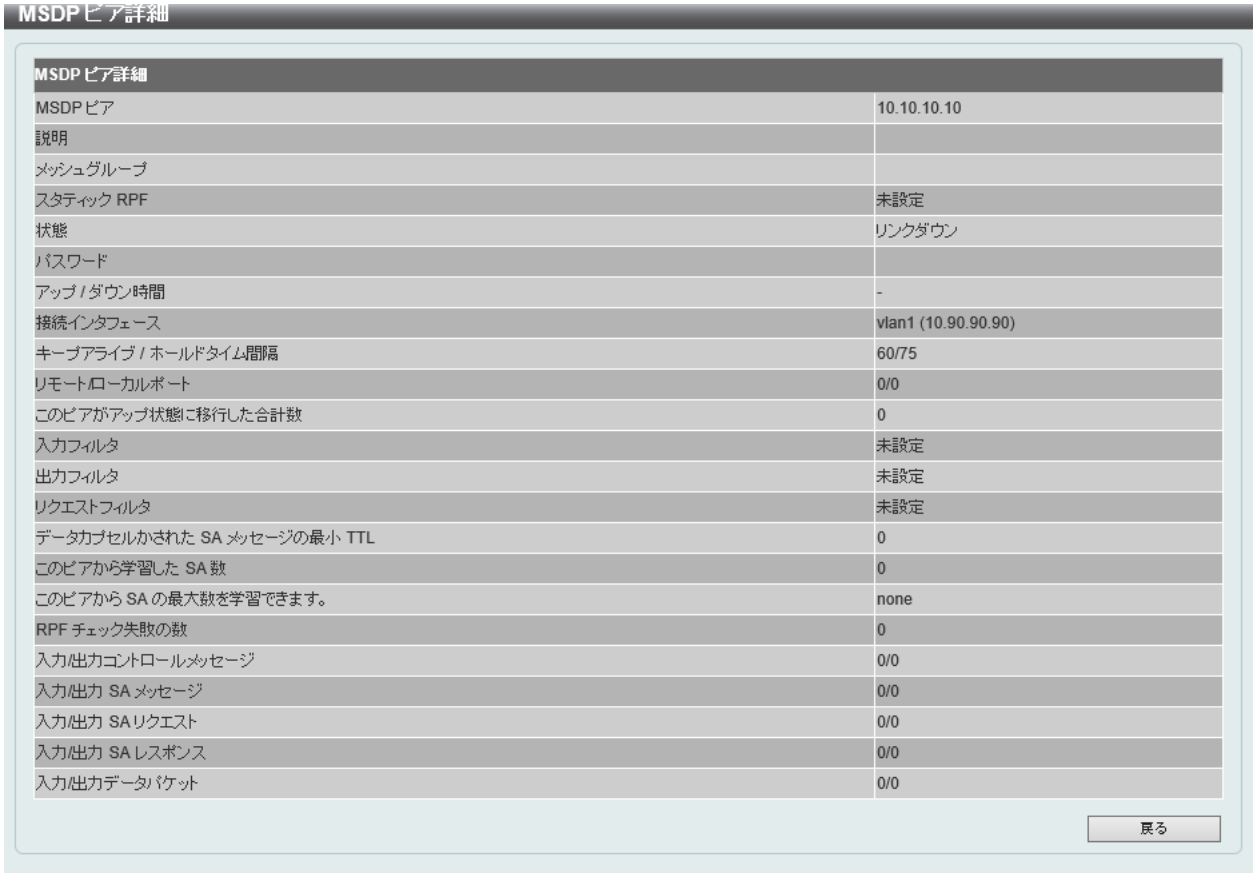


図 9-120　MSDP ピア詳細 画面

「戻る」をクリックすると前のページに戻ります。

■ MSDP SA キャッシュ

Multicast Source Discovery Protocol（MSDP）SA のキャッシュ設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > MSDP > MSDP SA キャッシュの順にメニューをクリックして以下の画面を表示します。

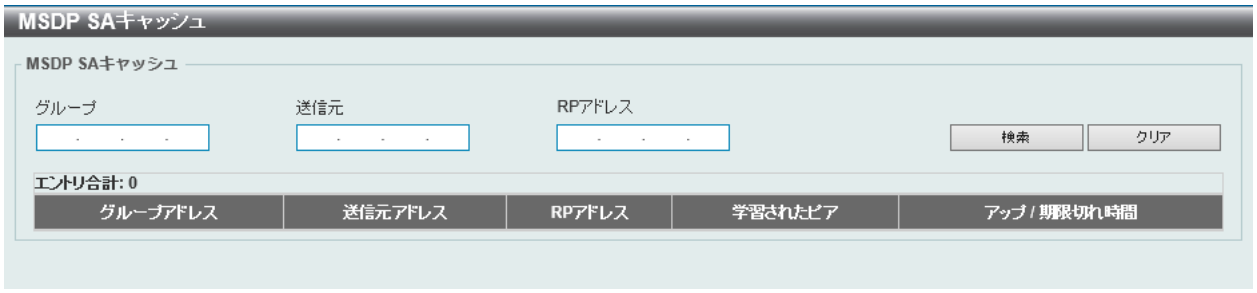


図 9-121　MSDP SA キャッシュ画面

画面に表示される項目：

項目	説明
グループ	グループアドレスを指定します。
送信元	ソースアドレスを指定します。
RP アドレス	RP アドレスを指定します。

「クリア」をクリックすると入力したエントリをクリアします。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

■ MSDP スタティック RPF 設定

MSDP スタティック RPF 設定を行います。
スタティック RPF ピアを設定する前に、MSDP ピアを追加する必要があります。RP プリフィクスリストが設定されると、ピアはプリフィクスリスト内の RP に対してのみスタティック RPF ピアになります。RP プレフィックスリストなしで複数のスタティック RPF ピアを指定した場合、アドレスが最も小さい接続ピアのみがアクティブなスタティック RPF ピアになります。MSDP ピアがスタティック RPF ピアとして複数設定されていると、最新の設定が有効になります。MSDP ピアが一つだけの場合、この MSDP ピアはスタティック RPF ピアとなります。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > MSDP > MSDP スタティック RPF 設定 の順にメニューをクリックして以下の画面を表示します。



図 9-122　MSDP スタティック RPF 設定画面

以下の項目を使用します。

項目	説明
ピアアドレス	MSDP ピアアドレスを指定します。
RP リスト	RP プレフィックスリストを定義する標準 IP リストを指定します。（32 文字以内）
RP アドレス	RP アドレスを指定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

■ MSDP メッシュグループ設定

本項目では、MSDP メッシュグループの設定を行います。
MSDP ピアをメッシュグループに追加する前に、MSDP ピアを追加する必要があります。MSDP ピアが複数のメッシュグループに追加されている場合、最新の設定内容が有効になります。

L3 機能 > IP マルチキャストルーティングプロトコル > PIM > MSDP > MSDP メッシュグループ設定 の順にメニューをクリックして以下の画面を表示します。



図 9-123　MSDP メッシュグループ設定画面

以下の項目を使用します。

項目	説明
ピアアドレス	MSDP ピアアドレスを指定します。
メッシュ名	メッシュグループ名を指定します。（64 文字以内）

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックして、指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPMC

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC

IP マルチキャストグローバル設定

IP マルチキャストグローバル設定（IP マルチキャストグローバル設定）の表示、グローバル設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC > IP マルチキャストグローバル設定の順にメニューをクリックして以下の画面を表示します。



図 9-124　IP マルチキャストグローバル設定画面

画面に表示される項目：

項目	説明
IP マルチキャストルーティンググローバルステート	
グローバルステート	IP マルチキャストルーティングを有効 / 無効に指定します。 IP マルチキャストルーティングが無効の場合、マルチキャストルーティングプロトコルが有効でも、システムはルーティングマルチキャストパケットを停止します。
IP マルチキャストテーブルルックアップモード	
テーブルルックアップモード	IP マルチキャストフォワーディングルックアップモードを指定します。 • 「IP」- IP アドレスに基づいてマルチキャストフォワーディングルックアップを行います。 • 「MAC」- MAC アドレスに基づいてマルチキャストフォワーディングルックアップを行います。
IP マルチキャスト境界	
VID	VLAN ID を指定します。 • 設定可能範囲：1-4094
ACL 名	指定する IP アクセスリスト名を指定します。（32 文字以内） 「選択してください」をクリックし、既存のアクセスリストを選択することも可能です。
フィルタモード	フィルタモードを指定します。 • 「両方」- 入力 / 出力トラフィックの両方をフィルタします。 • 「Out」- インタフェースに到着する PIM ジョインメッセージ、または IGMP ジョインメッセージをフィルタします。このフィルタリングにより、インタフェースが拒否エントリ (*,G) (S,G) の外向きインタフェースになることを防止します。 • 「In」- インタフェースに到着するマルチキャストユーザトラフィックを指定のアクセスリストに基づきフィルタします。これにより、特定のグループトラフィックまたは特定の送信元からの特定のグループのマルチキャストトラフィックがフィルタリングされます。
アクション	実行するアクションを指定します。 • 「追加」「削除」
IP マルチキャストインタフェーステーブル	
インタフェース名	表示するインタフェース名を指定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「選択してください」をクリックすると、次の画面を表示します。



図 9-125　ACL アクセスリスト画面

設定するエントリを選択し「OK」をクリックします。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IP マルチキャストルート設定

IP マルチキャストルート設定の表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC > IP マルチキャストルート設定の順にメニューをクリックして以下の画面を表示します。

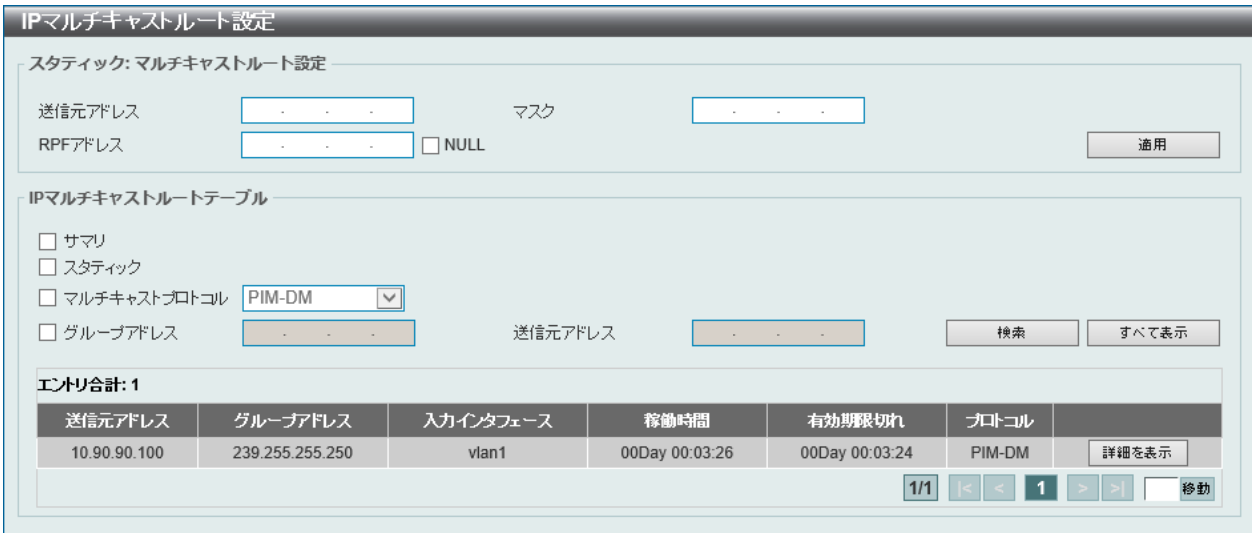


図 9-126　IP マルチキャストルート設定画面

画面に表示される項目：

項目	説明
スタティック マルチキャストルート設定	
送信元アドレス	マルチキャストソースとなるネットワークアドレスを指定します。
マスク	マルチキャストソースとなるサブネットマスクを指定します。
RPF アドレス	RPF ネイバ IP アドレスを入力します。 「NULL」オプションを選択すると、ソースネットワークから送信されたマルチキャストトラフィックの RPF チェックは必ず失敗します。
IP マルチキャストルートテーブル	
サマリ	IP マルチキャストルーティングテーブルのサマリについて表示します。
スタティック	マルチキャストスタティックルートを表示します。
マルチキャストプロトコル	表示するマルチキャストプロトコルを選択します。 • 「PIM-DM」- PIM-DM ルートのみを表示します。 • 「PIM-SM」- PIM-SM ルートのみを表示します。 • 「DVMRP」- DVMRP ルートのみを表示します。
グループ アドレス	マルチキャストグループ IP アドレスを指定します。
送信元アドレス	送信元 IP アドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IP マルチキャスト RPF テーブル

ユニキャストホストアドレスの RPF（Reverse Path Forwarding）情報を表示します。

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC > IP マルチキャスト RPF テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-127　IP マルチキャスト RPF テーブル画面

画面に表示される項目：

項目	説明
IP アドレス	ユニキャスト IPv4 アドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

IP マルチキャストルーティングフォワーディングキャッシュテーブル

IP マルチキャストフォワーディングキャッシュの表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC > IP マルチキャストルーティングフォーワーディングキャッシュテーブル の順にメニューをクリックして以下の画面を表示します。

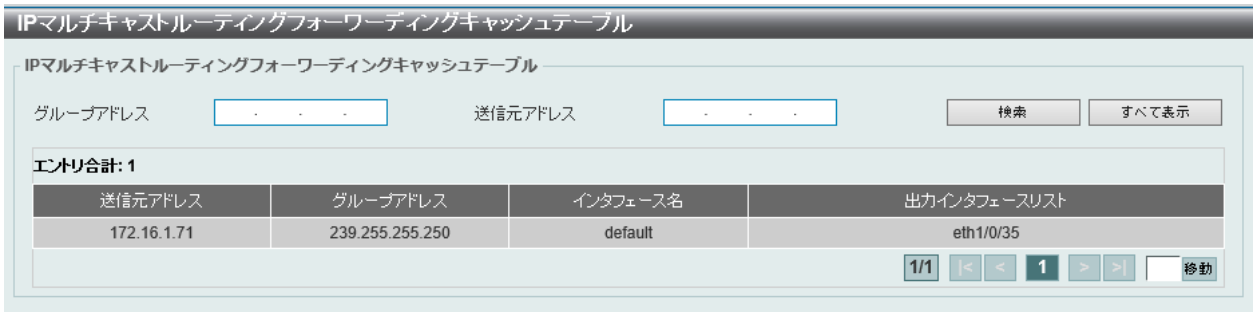


図 9-128　IP マルチキャストルーティングフォーワーディングキャッシュテーブル 画面

画面に表示される項目：

項目	説明
グループ アドレス	マルチキャストグループ IP アドレスを指定します。
送信元アドレス	送信元 IP アドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IP マルチキャストプロトコル統計

IP マルチキャストプロトコル統計の表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC > IP マルチキャストプロトコル統計の順にメニューをクリックして以下の画面を表示します。

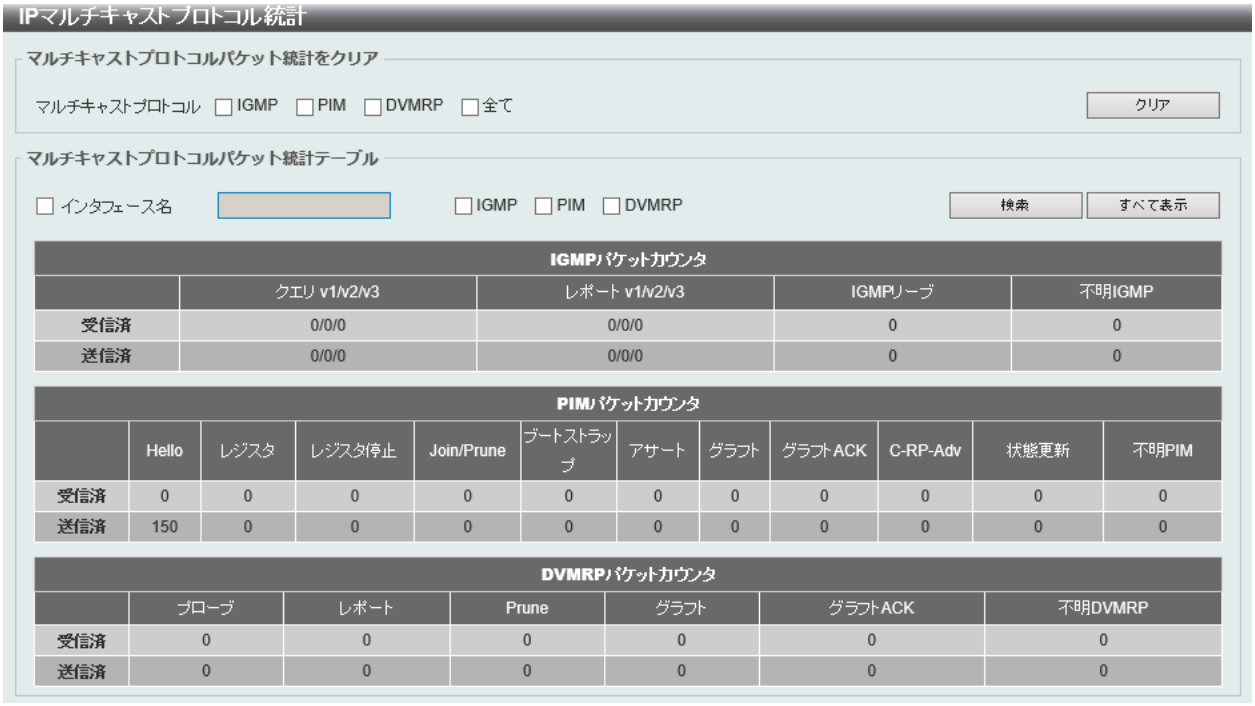


図 9-129　IP マルチキャストプロトコル統計画面

画面に表示される項目：

項目	説明
マルチキャストプロトコル パケット統計をクリア	
マルチキャストプロトコル	クリアするマルチキャストプロトコルを選択します。 • 選択肢：「IGMP」「PIM」「DVMRP」「全て」
マルチキャストプロトコル パケット統計テーブル	
インタフェース名	本設定に使用するインタフェース名を指定します。
マルチキャストプロトコル	表示するマルチキャストプロトコルを選択します。 • 選択肢：「IGMP」「PIM」「DVMRP」

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

パケット CPU フィルタリングの制御

IPMC 制御パケット CPU フィルタリング設定の表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPMC > パケット CPU フィルタリングの制御 の順にメニューをクリックして以下の画面を表示します。



図 9-130　パケット CPU フィルタリングの制御画面

画面に表示される項目：

項目	説明
パケット CPU フィルタリング設定の制御	
ユニット	設定を行うユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を設定します。
パケットタイプ	パケットの種類を指定します。 • 「DVMRP」- CPU に対して送信された「DVMRP L3 コントロールパケット」を破棄します。 • 「PIM」- CPU に対して送信された「PIM L3 コントロールパケット」を破棄します。 • 「IGMP クエリ」- CPU に対して送信された「IGMP クエリ L3 コントロールパケット」を破棄します。 • 「OSPF」- CPU に対して送信された「OSPF L3 コントロールパケット」を破棄します。 • 「RIP」- CPU に対して送信された「RIP L3 コントロールパケット」を破棄します。 • 「VRRP」- CPU に対して送信された「VRRP L3 コントロールパケット」を破棄します。
アクション	実行するアクションを指定します。 • 「追加」「削除」
パケット CPU フィルタリングテーブルの制御	
ユニット	表示するユニットを指定します。
開始ポート / 終了ポート	表示するポートの範囲を指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IPv6MC

L3 機能 > IP マルチキャストルーティングプロトコル > IPv6MC

IPv6 マルチキャストグローバル設定

IPv6 マルチキャストグローバル設定の表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPv6MC > IPv6 マルチキャストグローバル設定の順にメニューをクリックして以下の画面を表示します。



図 9-131　IPv6 マルチキャストグローバル設定画面

画面に表示される項目：

項目	説明
IPv6 マルチキャストルーティング	
IPv6 マルチキャストルーティンググローバルステート	IPv6 マルチキャストルーティング機能のグローバルステータスを有効 / 無効に設定します。IPv6 マルチキャストルーティングが無効の場合、マルチキャストルーティンプロトコルが有効でも、システムはルーティングマルチキャストパケットのルーティングを停止します。
IPv6 マルチキャスト インタフェーステーブル	
インタフェース名	本設定に適用する VLAN インタフェース ID を指定します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPv6 マルチキャストルーティングテーブル

IPv6 マルチキャストルートテーブルの表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPv6MC > IPv6 マルチキャストルーティングテーブルの順にメニューをクリックして以下の画面を表示します。



図 9-132　IPv6 マルチキャストルートテーブル画面

画面に表示される項目：

項目	説明
グループ IPv6 アドレス	マルチキャストグループ IPv6 アドレスを指定します。
送信元 IPv6 アドレス	マルチキャストソース IPv6 アドレスを指定します。 • 「Dense」- PIM-DM ルートのみ表示します。 • 「Sparse」- PIM-SM ルートのみ表示します。 • 「サマリ」- IPv6 マルチキャストルーティングテーブルにおける 1 行の要約されたサマリを表示します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IPv6 マルチキャストフォワーディングキャッシュテーブル

IPv6 マルチキャストフォワーディングキャッシュテーブルの表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPv6MC > IPv6 マルチキャストフォワーディングキャッシュテーブルの順にメニューをクリックして以下の画面を表示します。



図 9-133　IPv6 マルチキャストフォワーディングキャッシュテーブル画面

画面に表示される項目：

項目	説明
グループ IPv6 アドレス	マルチキャストグループ IPv6 アドレスを指定します。
送信元 IPv6 アドレス	送信元 IPv6 アドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「すべて表示」をクリックして、すべてのエントリを表示します。

IPv6 RPF テーブル

ユニキャストホストアドレスの RPF（Reverse Path Forwarding）情報の表示、設定を行います。

L3 機能 > IP マルチキャストルーティングプロトコル > IPv6MC > IPv6 RPF テーブルの順にメニューをクリックして以下の画面を表示します。



図 9-134　IPv6 RPF テーブル画面

画面に表示される項目：

項目	説明
IPv6 送信元アドレス	ユニキャストホスト IPv6 アドレスを指定します。

「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。

IP ルートフィルタ

IP プレフィックスリスト、ルートマップの作成を行います。

ルートマップ

ルートマップの作成、またはルートマップへのシーケンスの追加、およびシーケンスの削除を行います。

L3 機能 > IP ルートフィルタ > ルートマップの順にメニューをクリックして以下の画面を表示します。



図 9-135　ルートマップ画面

以下の項目を使用して設定を行います。

項目	説明
ルートマップ名	ルートマップ名を入力します。(16 文字以内)
方向	ルールを選択します。 • 「許可」- ルールエントリに一致するルートは許可されます。 • 「拒否」- ルールエントリに一致するルートは拒否されます。
シーケンス ID	ルールのシーケンス番号を指定します。 • 設定可能範囲：1-65535

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「削除」をクリックして、指定エントリを削除します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「条件に合致」の編集

「条件に合致」下の「編集」をクリックすると、以下の画面が表示されます。

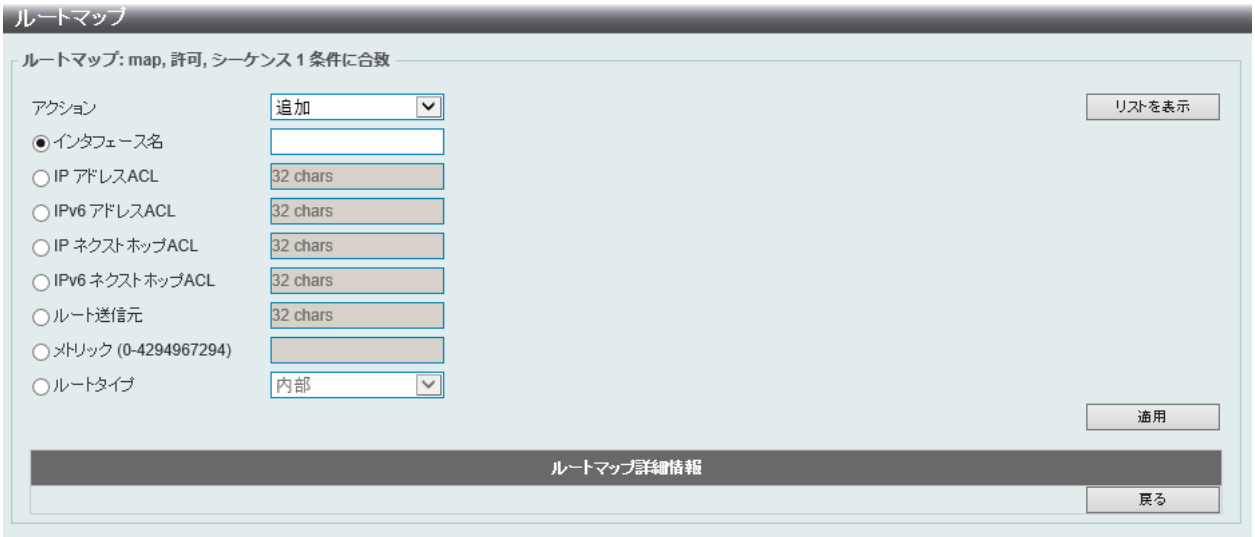


図 9-136　ルートマップ - 条件に合致画面

画面に表示される項目：

項目	説明
アクション	アクションを選択します。 • 「追加」- 入力した情報に基づいてエントリを追加します。 • 「削除」- 入力した情報に基づいてエントリを削除します。
インタフェース名	インタフェース名を指定します。ルートの外向きインタフェースを照合するための条件を定義します。
IP アドレス ACL	標準 / 拡張 IP アクセスリストを指定します。（32 文字以内） 標準 / 拡張 IP アクセスリストに基づいてルートを照合します。
IPv6 アドレス ACL	標準 / 拡張 IPv6 アクセスリストを指定します。（32 文字以内） 標準 / 拡張 IPv6 アクセスリストに基づいてルートを照合します。
IP ネクストホップ ACL	標準 IP アクセスリストを指定します。（32 文字以内） 標準 IP アクセスリストに基づいてルートのネクストホップを照合します。
IPv6 ネクストホップ ACL	標準 IPv6 アクセスリストを指定します。（32 文字以内） 標準 IPv6 アクセスリストに基づいてルートのネクストホップを照合します。
ルート送信元	標準 / 拡張 IP/IPv6 アクセスリストを指定します。（32 文字以内） 標準 / 拡張 IP4/IPv6 アクセスリストに基づいてルート送信元を照合します
メトリック	ルートのメトリック値を指定します。ルートのメトリックの照合に使用されます。 • 設定可能範囲：0-4294967294
ルートタイプ	ルートタイプを指定します。 • 「内部」- OSPF のエリア内ルートとエリア間ルートを指定します。 • 「外部」- 自律システムの OSPF 外部ルートを指定します。タイプ 1 およびタイプ 2 オプションが指定されていない場合、タイプ 1 およびタイプ 2 外部ルートは含まれます。 • 「外部 タイプ 1」- OSPF の タイプ 1 外部ルートを指定します。 • 「外部 タイプ 2」- OSPF のタイプ 2 外部ルートを指定します。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックして前のページに戻ります。

「条件を設定」の編集

「条件を設定」の下の「編集」をクリックすると、以下の画面が表示されます。

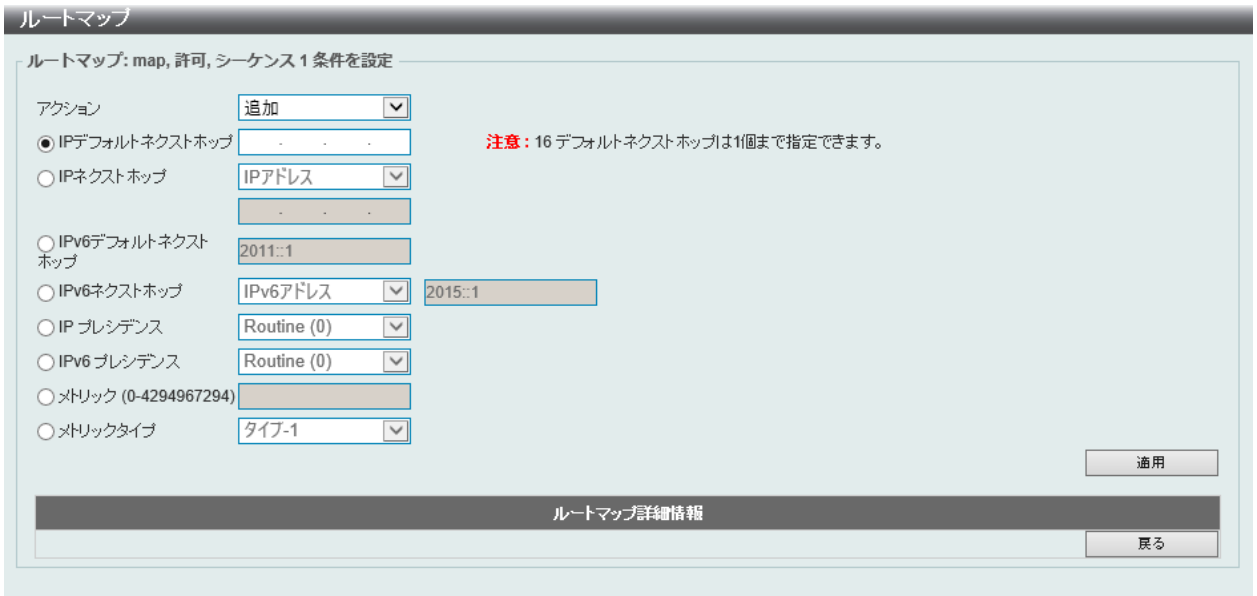


図 9-137　ルートマップ設定 - 条件を設定画面

画面に表示される項目：

項目	説明
アクション	アクションを選択します。 • 「追加」- 入力した情報に基づいてエントリを追加します。 • 「削除」- 入力した情報に基づいてエントリを削除します。
IP デフォルトネクストホップ	パケットのルーティングに使用されるデフォルトのネクストホップ IP アドレスを入力します。 この機能は、複数のデフォルトのネクストホップルータを指定するために使用できます。デフォルトのネクストホップがすでに設定されている場合は、後で設定されたデフォルトのネクストホップがデフォルトのネクストホップリストに追加されます。指定された最初のデフォルトのネクストホップルータがダウンしている場合、次のデフォルトネクストホップルータがパケットのルーティングを試行します。最大 16 個のデフォルトのネクストホップ IP アドレスを入力できます
IP ネクストホップ	IP ネクストホップの種類を選択します。この機能は、ルートマップシーケンスの一致条件に合致したパケットをルーティングするように、ネクストホップルータを設定します。 • 「IP アドレス」- パケットをルーティングするネクストホップの IP アドレスを指定します。入力欄にネクストホップ IP アドレスを入力します。最大 16 個のネクストホップ IP アドレスを入力できます。 • 「帰納的」- ネクストホップルータとして帰納的な IP アドレスを指定します。入力欄に帰納的ネクストホップ IP アドレスを入力します。
IPv6 デフォルトネクストホップ	パケットのルーティングに使用されるデフォルトのネクストホップ IPv6 アドレスを入力します。 この機能は、複数のデフォルトのネクストホップルータを指定するために使用できます。デフォルトのネクストホップがすでに設定されている場合は、後で設定されたデフォルトのネクストホップがデフォルトのネクストホップリストに追加されます。指定された最初のデフォルトのネクストホップルータがダウンしている場合、次のデフォルトネクストホップルータがパケットのルーティングを試行します。最大 16 個のデフォルトのネクストホップ IPv6 アドレスを入力できます。
IPv6 ネクストホップ	IPv6 ネクストホップの種類を選択します。この機能は、ルートマップシーケンスの一致条件に合致したパケットをルーティングするように、ネクストホップルータを設定します。 • 「IP アドレス」- パケットをルーティングするネクストホップの IPv6 アドレスを指定します。入力欄にネクストホップ IPv6 アドレスを入力します。 • 「帰納的」- ネクストホップルータとして帰納的な IPv6 アドレスを指定します。入力欄に帰納的ネクストホップ IP アドレスを入力します。
IP プレシデンス	IP 優先オプションを指定します。IP ヘッダに含まれる優先値となります。このオプションは、ポリシールーティングが IPv4 パケットに関連する場合にのみ有効になります。 • 選択肢：「Routine（0）」「Priority（1）」「Immediate（2）」「Flash（3）」「Flash Override（4）」「重大な（5）」「インターネット（6）」「ネットワーク（7）」
IPv6 プレシデンス	IPv6 優先オプションを以下から指定します。IPv6 ヘッダに含まれる優先値となります。このオプションは、ポリシールーティングが IPv6 パケットに関連する場合にのみ有効になります。 • 選択肢：「Routine（0）」「Priority（1）」「Immediate（2）」「Flash（3）」「Flash Override（4）」「重大な（5）」「インターネット（6）」「ネットワーク（7）」
メトリック	メトリック値を入力します。 • 設定可能範囲：0 - 4294967294
メトリックタイプ	メトリックタイプを指定します。 • 「タイプ -1」- OSPF 外部タイプ 1 メトリックを使用します。 • 「タイプ -2」- OSPF 外部タイプ 2 メトリックを使用します。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックして前のページに戻ります。

ポリシールート

ポリシーベースルーティングの設定、表示を行います。

L3 機能 > ポリシールートの順にメニューをクリックし、以下の画面を表示します。



図 9-138　ポリシールート画面

画面に表示される項目：

項目	説明
タイプ	ポリシールートタイプを指定します。 • 選択肢：「IP ポリシ」「IPv6 ポリシー」

「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

エントリの編集

ポリシールートの編集をするためには、「編集」をクリックして以下の画面を表示します。

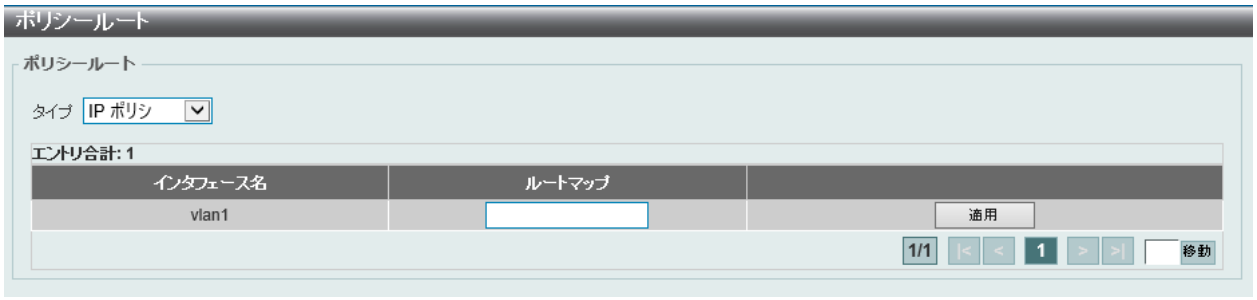


図 9-139　ポリシールート（編集）画面

画面に表示される項目：

項目	説明
ルートマップ	ポリシールートエントリで使用されるルートマップ名を入力します。

「適用」をクリックして、設定内容を適用します。

VRRP

Virtual Router Redundancy Protocol（VRRP）の設定を行います。
同じ VRRP グループ内のすべてのルータに、同じ仮想ルータ ID と IP アドレスを設定する必要があります。

仮想ルータグループは、仮想ルータ ID で表されます。 仮想ルータの IP アドレスは、ホストに設定されているデフォルトルータです。 仮想ルータの IP アドレスは、ルーターに設定されている実際のアドレス、または未使用の IP アドレスにすることができます。 仮想ルータアドレスが実際の IP アドレスである場合、この IP アドレスを持つルータが IP アドレスの所有者になります。

同じ仮想ルータをサポートするルータのグループ内で、マスタが選出されます。その他のルータはバックアップルータになります。
マスタは、仮想ルータに送信されるパケットの転送を行います。

L3 機能 > VRRP 設定の順にメニューをクリックし、以下の画面を表示します。



図 9-140　VRRP 設定画面

画面に表示される項目：

項目	説明
VRRP 設定	
SNMP サーバトラップ VRRP 新マスタ	新しい VRRP マスタの SNMP サーバトラップ機能を有効 / 無効に設定します。 本設定を有効にした場合、デバイスがマスタ状態に遷移したときに、トラップが送信されます。
SNMP サーバトラップ VRRP 認証失敗	認証失敗時の SNMP サーバトラップ機能を有効 / 無効に設定します。 本設定を有効にした場合、受信したパケットの認証キーまたは認証タイプがこのルータのものと不一致であったときに、トラップが送信されます。
非オーナー Ping 応答	「非オーナ Ping 応答」（Non-owner-ping Response）機能を有効 / 無効に設定します。 この仮想ルータに関連付けられているものの非オーナである IP アドレスの ICMP エコー要求に対し、マスタ状態の仮想ルータが応答できるように設定します。
仮想ルータ設定	
VLAN インタフェース	VLAN インタフェース ID を指定します。 • 設定可能範囲：1-4094
VRID	作成する仮想ルータの ID を入力します。この ID は、VRRP グループ内の仮想ルータを識別するために使用されます。 • 設定可能範囲：1-255
仮想 IP アドレス	作成する仮想ルータグループの IPv4 アドレスを指定します。
VRRP 認証	インタフェースで VRRP 認証のプレーンテキスト認証パスワードを有効にします。 パスワードの文字列の長さは最大 8 文字です。認証はこのインタフェース上のすべての仮想ルータに適用されます。 同じ VRRP グループ内のデバイスには、同じ認証パスワードが設定されている必要があります。
インタフェース名	表示するインタフェース名を指定します。（12 文字以内）
VRID	表示する仮想ルータの ID を入力します。 • 設定可能範囲：1-255

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「編集」をクリックすると、以下の画面が表示されます。

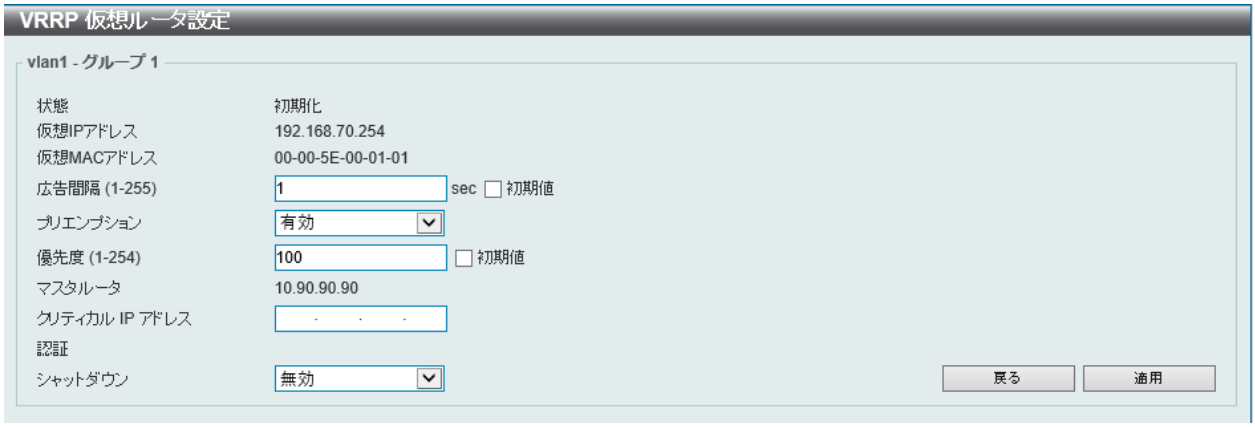


図 9-141　VRRP 仮想ルータ設定（編集）画面

画面に表示される項目：

項目	説明
広告間隔	マスタルータによる VRRP アドバタイズメントの送信間隔を指定します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255（秒） • 初期値：1（秒）
プリエンプション	「プリエンプション」（優先置き換え）機能を有効 / 無効に指定します。 この機能は、現在のマスタよりも優先順位が高いルータが、マスタロールを引き継ぐことを許可するかどうかを指定します。
優先度	プライオリティ値を入力します。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-254
クリティカル IP アドレス	クリティカル IPv4 アドレスを入力します。 仮想ルータに設定されているクリティカル IP アドレスが到達不能な場合、仮想ルータはアクティブ化されません。 VRRP グループ毎に、1 つのクリティカル IP のみを追跡できます。
シャットダウン	シャットダウン機能を有効 / 無効に設定します。インタフェース上の仮想ルータを無効にするために使用されます。 他の非オーナルータをシャットダウンする前に IP アドレスのオーナルータをシャットダウンするミスを回避します。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックすると前のページに戻ります。

VRRPv3 設定

VRRPv3 設定を行います。
L3 機能 > VRRPv3 設定の順にメニューをクリックし、以下の画面を表示します。



図 9-142　VRRPv3 設定画面

画面に表示される項目：

項目	説明
VLAN	VLAN インタフェースの ID を入力します。 • 設定可能範囲：1-4094
VRID	作成する仮想ルータの ID を入力します。 • 設定可能範囲：1-255
アドレスファミリ	アドレスファミリーを指定します。 •「全て」- すべての仮想ルータを指定します。 •「IPv4」- IPv4 仮想ルータを指定します。 •「IPv6」- IPv6 仮想ルータを指定します。
インタフェース名	インタフェース名を指定します。（12 文字以内）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定のエントリを削除します。
「検索」をクリックして、入力した情報に基づく特定のエントリを検出します。
「編集」をクリックして、指定エントリの編集を行います。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPv4「アドレスファミリ」エントリの「編集」をクリックすると、以下の画面が表示されます。



図 9-143　VRRPv3 仮想ルータ設定（編集 /IPv4 アドレスファミリ）画面

IPv6「アドレスファミリ」エントリの「編集」をクリックすると、以下の画面が表示されます。

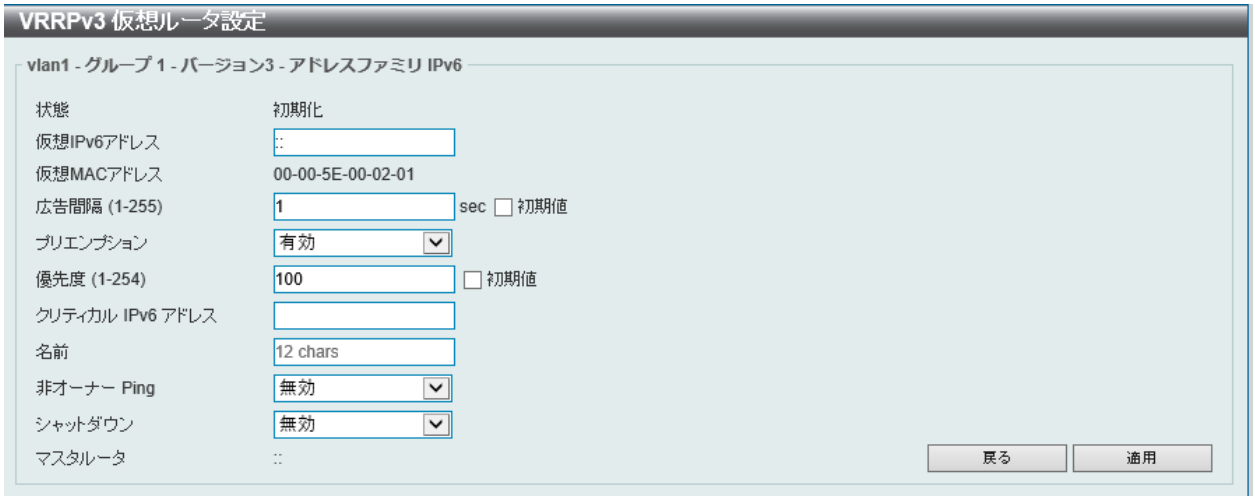


図 9-144　VRRPv3 仮想ルータ設定（編集 /IPv6 アドレスファミリ）画面

画面に表示される項目：

項目	説明
仮想 IP アドレス / 仮想 IPv6 アドレス	仮想 IPv4/IPv6 アドレスを入力します。 同じ VRRP グループ内のすべてのルータに、同じ仮想ルータ ID と仮想アドレスを設定する必要があります。仮想ルータの IPv4/IPv6 アドレスは、ルータに設定されている実際のアドレスでも、未使用のアドレスでもかまいません。仮想アドレスがインタフェースの実際のアドレスと同じ場合、この仮想ルータは IPv4/IPv6 アドレスのオーナとなります。
広告間隔	マスタルータによる VRRP アドバタイズメントの送信間隔を指定します。VRRP グループ内のすべての仮想ルータは、同じタイマ値を使用する必要があります。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-255（秒）
プリエンプション	「プリエンプション」（優先置き換え）機能を有効 / 無効に設定します。 この機能は、現在のマスタよりも優先順位が高いルータが、マスタロールを引き継ぐことを許可するかどうかを指定します。
優先度	仮想ルータの優先値を指定します。 VRRP グループのマスタは、この優先値に基づいて選択されます。優先値が最も高い仮想ルータがマスタになり、他の仮想ルータは VRRP グループのバックアップとして機能します。同じ優先値を持つルータが複数存在する場合、IPv4 アドレスの値の大きい方がマスタになります。VRRP グループの IPv4 アドレスオーナであるルータは、常に VRRP グループのマスタであり、最も高いプライオリティ「255」を持ちます。「初期値」にチェックを入れると、初期値を使用します。 • 設定可能範囲：1-254
クリティカル IPv6 アドレス	クリティカル IPv6 アドレスを入力します。 仮想ルータに設定されているクリティカル IPv6 アドレスが到達不能な場合、仮想ルータはアクティブ化されません。VRRP グループ毎に、1 つのクリティカル IPv6 アドレスのみを追跡できます。
名前	IPv6 アドレスファミリの名前を入力します。（12 文字以内） IPv6「アドレスファミリ」エントリの画面にのみ表示されます。
非オーナー Ping	「非オーナ Ping」（Non-owner ping）機能を有効 / 無効に指定します。 マスタ状態の非 IPv4/IPv6 アドレスオーナ仮想ルータが IPv4/IPv6 アドレスの ICMP エコー要求に応答できるようにするために使用します。
シャットダウン	シャットダウン機能を有効 / 無効に設定します。 インタフェース上の仮想ルータを無効にするために使用されます。 他の非オーナルータをシャットダウンする前に IPv4/IPv6 アドレスのオーナルータをシャットダウンするミスを回避します。

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックすると前のページに戻ります。

第 10 章　QoS

本スイッチは、802.1p プライオリティキューイングの QoS（Quality of Service）機能をサポートしています。
次のセクションでは、QoS（Quality of Service）の実装と、802.1p プライオリティキューイングを使用する利点について説明します。

以下は QoS サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
基本設定	QoS の基本設定を行います。
詳細設定	QoS の詳細設定を行います。
QoS PFC	ネットワーク「Quality of Service」（QoS）プライオリティベースフローコントロール（PFC）クラスマップの設定を行います。
WRED	WRED（Weighted Random Early Detection）の設定を行います。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術であり、VoIP（Voice-over Internet Protocol）、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、ビデオ会議など、広帯域を必要としたり高い優先順位を持つ重要なサービスのために、帯域を確保することができます。ネットワーク帯域を拡張するだけでなく、重要度の低いトラフィックに対して制限を行うことで、ネットワークが必要以上の帯域を使用しないようにします。スイッチの各物理ポートには個別のハードウェアキューがあり、様々なアプリケーションからのパケットがマッピングされ、優先順位が付けられます。
以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示します。

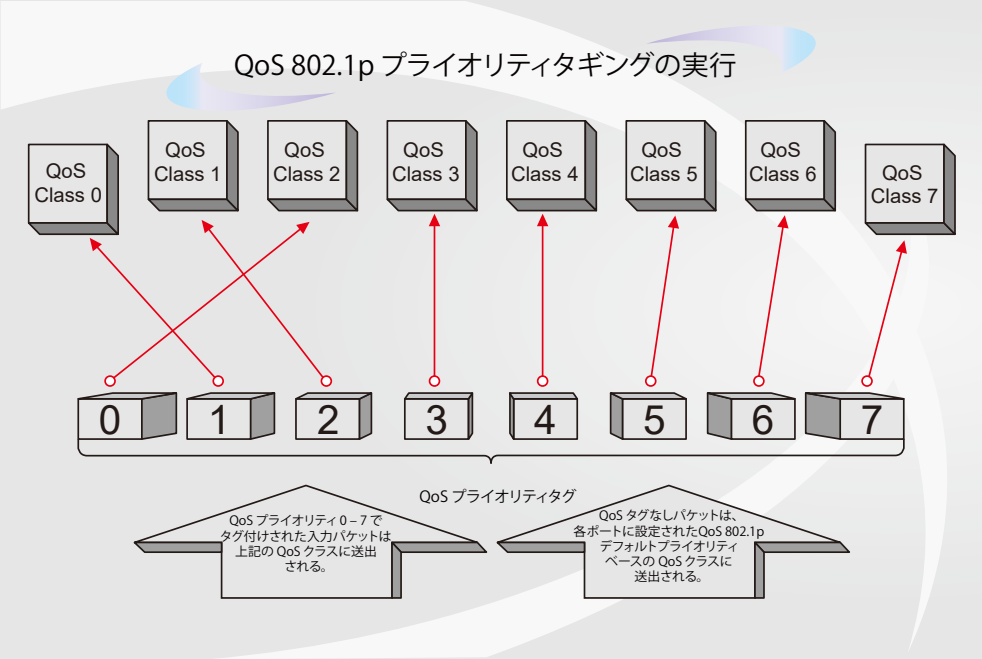


図 10-1　スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス 7 はスイッチにおける 7 つのプライオリティクラスの中で、最も高い優先度を持っています。QoS を実行するためには、パケットのヘッダを調べて適切な識別タグがあるかどうかを確認するようにスイッチに指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した 2 台のコンピュータ間でビデオ会議を行うとします。管理者は Access プロファイルコマンドを使用して、送信するビデオパケットにプライオリティタグを追加することができます。そして、受信側ではそのタグを検査するように設定し、受信したタグ付きパケットをスイッチのクラスキューに関連付けるようにします。また、管理者はこのキューに優先順位を与え、他のパケットよりも先に送信されるように設定を行います。この結果、このサービス用のパケットはできる限り早く送信されます。キューが優先されることにより、パケットは中断せずに送信されるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチは、802.1p プライオリティキューをサポートしており、8 個のプライオリティキューがあります。プライオリティキューには、最高レベルの 7 番キュー（クラス 7）から最低レベルの 0 番キュー（クラス 0）までがあります。IEEE 802.1p（p0 から p7）に規定される 8 つのプライオリティタグは、以下のようにスイッチのプライオリティキューにマッピングされます。

- プライオリティ 0 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 2 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 3 は、スイッチの Q3 キューに割り当てられます。
- プライオリティ 4 は、スイッチの Q4 キューに割り当てられます。
- プライオリティ 5 は、スイッチの Q5 キューに割り当てられます。
- プライオリティ 6 は、スイッチの Q6 キューに割り当てられます。
- プライオリティ 7 は、スイッチの Q7 キューに割り当てられます。

Strict（絶対優先）のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。Strict 方式のキューが複数ある場合、プライオリティタグに従って順番に送信されます。優先度の高いキューが空になると、次の優先度を持つパケットが送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。8 つの CoS（Class of Service）キュー、A ～ H に 8 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。
A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1

重み付けラウンドロビンキューイングにおいて各 CoS キューが同じ重み付けを持つ場合、ラウンドロビンキューイングのように、各 CoS キューのパケットは同じ割合で送信されます。また、ある CoS キューの重み付けとして 0 を設定すると、そのキューから送信するパケットがなくなるまでパケットを処理します。0 以外の値を持つ他のキューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。



本スイッチは、スイッチ上の各ポートに 8 つのプライオリティキューを持っています。これらのクラスの 1 つはスイッチにおける内部利用のために予約されており、設定することができません。次のセクションで参照されるサービスクラスは、管理者によって設定・管理可能な 7 つのクラスのみを示しています。

基本設定

QoS の基本設定（基本設定）を行います。

ポートデフォルト CoS

各ポートにデフォルト CoS の設定を行います。

QoS > 基本設定 > ポートデフォルト CoS の順にメニューをクリックし、以下の画面を表示します。

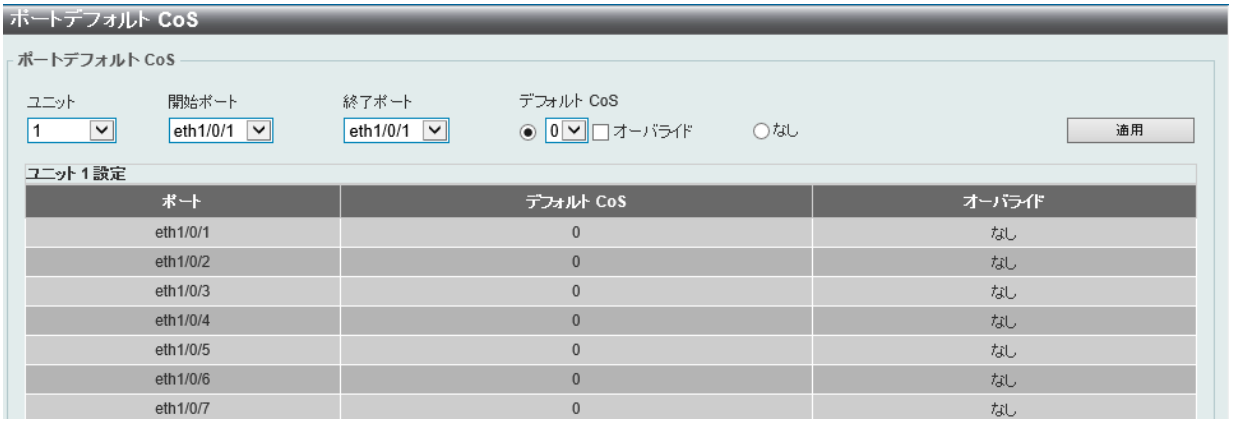


図 10-1　ポートデフォルト CoS 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
デフォルト CoS	ポートのデフォルト CoS を指定します。 「オーバライド」にチェックを入れると、パケットの CoS を上書きします。デフォルト CoS は、ポートで受信した全てのパケット（タグ付き / タグなしの両方）に適用されます。 「なし」を選択すると、タグ付きパケットの場合はパケットの CoS を使用し、タグなしパケットの場合はポートデフォルト CoS となります。 • 設定可能範囲：0-7

「適用」をクリックして、設定内容を適用します。

ポートスケジューラ方式

ポートスケジューラ方式を設定します。

QoS > 基本設定 > ポートスケジューラ方式の順にクリックし、以下の画面を表示します。



図 10-2　ポートスケジューラ方式画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
スケジューラ方式	指定ポートに対するスケジューリングの方法を以下から設定します。 • **「SP」（Strict Priority）**： すべてのキューは Strict Priority（絶対優先）スケジューリングを使用します。最も高い CoS 優先度のキューから絶対優先で送信されます。 • **「RR」（Round-Robin）**： すべてのキューは Round-Robin スケジューリングを使用します。キューを順番に見ながら、均等な比率でパケットが処理されます。 • **「WRR」（Weighted Round-Robin）**： Round-Robin 方式でパケットをキューに送出します。最初に、各キューは可変の重みをセットします。CoS キューからパケットが送信される度に、重み（Weight）の値から「1」が差し引かれ、次の CoS 優先度キューが処理されます。重みが「0」になると、重みが補充されるまでそのキューの処理は停止します。すべての CoS キューの重みが「0」に到達すると、キューの重みが補充されます。（初期値） • **「WDRR」（Weighted Deficit Round Robin）**： Round-Robin 方式で送信キューに蓄積された未処理のクレジットを処理します。最初に、各キューはクレジットカウンタを可変の数値にセットします。CoS キューからパケットが送信される度に、クレジットカウンタからパケットサイズが差し引かれ、次の CoS 優先度キューが処理されます。クレジットカウンタが「0」になると、クレジットが補充されるまでそのキューの処理は停止します。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、クレジットカウンタが補充されます。クレジットカウンタが 0 またはマイナスになり、最後のパケット送信が完了するまで処理が行われます。その後、クレジットは補充されます。クレジットが補充されると、各 CoS キューのクレジットカウンタにクレジットのクオンタムが補充されます。各キューのクオンタムはユーザ定義により異なる場合があります。 特定の CoS キューを SP モードに設定する場合、それより優先度の高い CoS キューについても SP モードである必要があります。

「適用」をクリックして、設定内容を適用します。

キュー設定

キューを設定、表示します。

QoS > 基本設定 > キュー設定の順にクリックし、以下の画面を表示します。

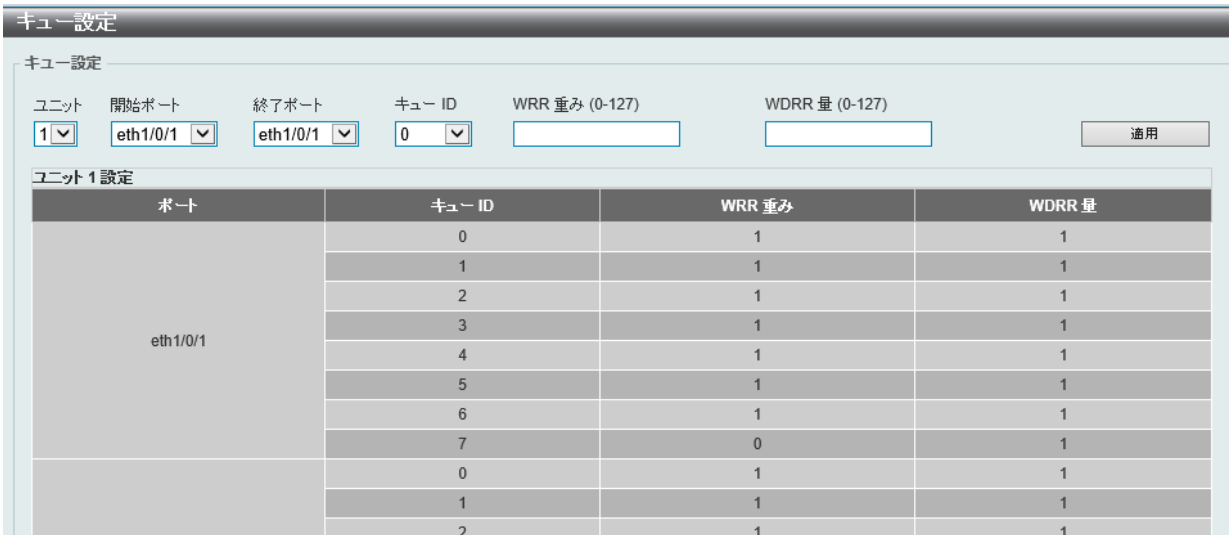


図 10-3　キュー設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
キュー ID	キュー ID を指定します。 • 設定可能範囲：0-7
WRR 重み	WRR の値を入力します。「Expedited Forwarding」(EF) の動作要件を満たすには、最も優先度の高いキューが常に「Per-hop Behavior」(PHB) により選択され、キューのスケジュールモードが Strict プライオリティである必要があります。そのため、「Differentiate Service」がサポートされている場合、最後のキューの重みは 0 に設定する必要があります。 • 設定可能範囲：0-127
WDRR 量	WDRR 量 (WDRR Quantum) の値を入力します。 • 設定可能範囲：0-127

「適用」をクリックして、設定内容を適用します。

CoS とキューのマッピング

CoS とキューのマッピングの表示、設定を行います。

QoS > 基本設定 > CoS とキューのマッピングの順にクリックし、以下の画面を表示します。

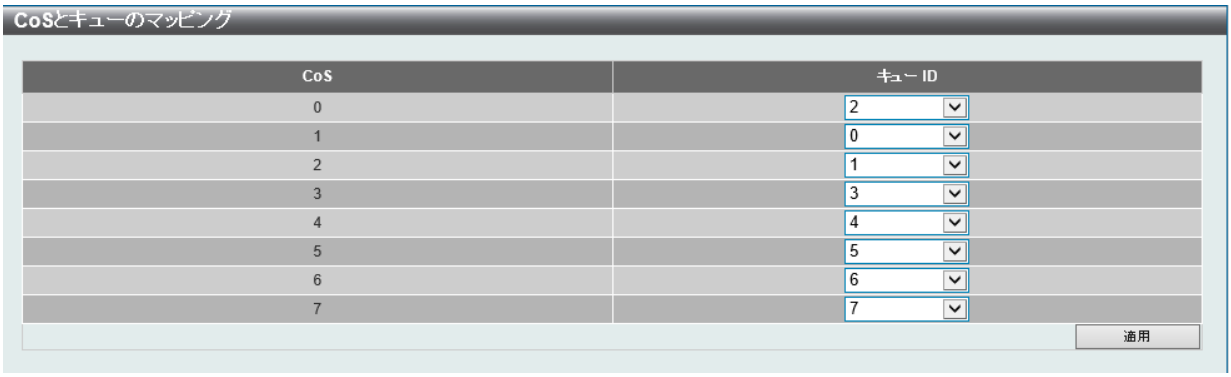


図 10-4　CoS とキューのマッピング画面

画面に表示される項目：

項目	説明
キュー ID	各 CoS 値にマッピングされるキュー ID を指定します。 • 選択肢：0-7

「適用」をクリックして、設定内容を適用します。

ポートレート制限

ポートレート制限の設定を行います。

QoS > 基本設定 > ポートレート制限の順にメニューをクリックし、以下の画面を表示します。

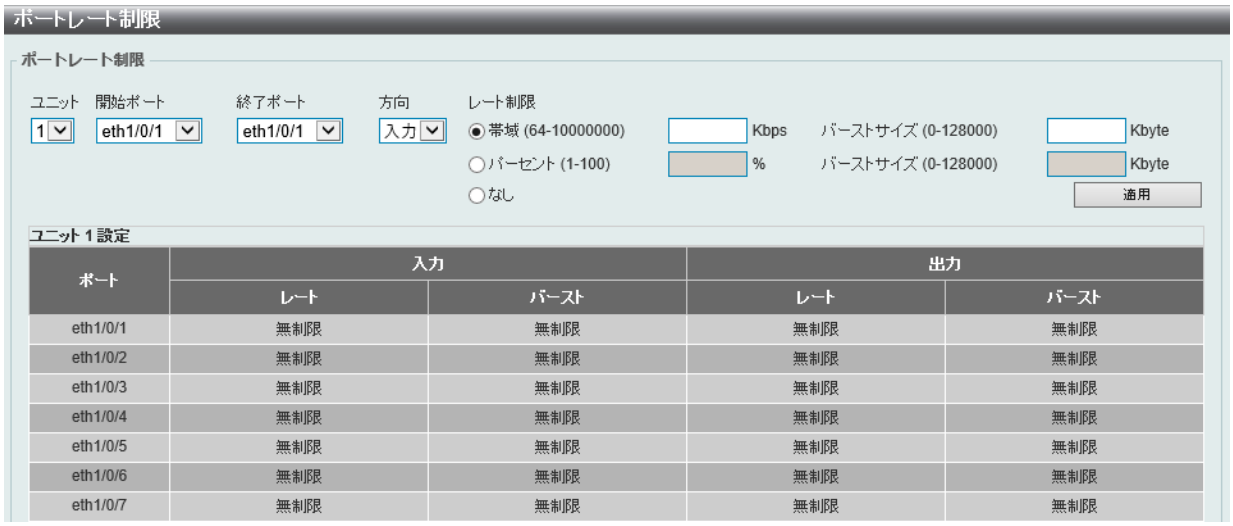


図 10-5　ポートレート制限画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
方向	レート制限の対象を以下から選択します。 • 入力 - 入力（Ingress）パケットのレート制限が設定されます。 • 出力 - 出力（Egress）パケットのレート制限が設定されます。
レート制限	レート制限の値を指定します。 指定された制限は、指定インタフェースの最大速度を超えることはできません。受信帯域幅制限の場合、受信トラフィックが制限を超えたときに、受信側は PAUSE フレームまたはフロー制御フレームを送信します。 • 「帯域」- 受信 / 送信の帯域値を入力欄に入力します。 - 設定可能範囲：64 - 10000000（Kbps） - 「バーストサイズ」：0 -128000（Kbyte） • 「パーセント」- 受信 / 送信の帯域幅パーセンテージを入力欄に入力します。 - 設定可能範囲：1 - 100（%） - 「バーストサイズ」：0 -128000（Kbyte） • 「なし」- 指定ポートのレート制限を削除します。

「適用」をクリックして、設定内容を適用します。

注意　バーストサイズに 0 を指定した場合、レート制限は機能しません。

キューレート制限

キューレートの制限設定をします。

QoS > 基本設定 > キューレート制限の順にメニューをクリックし、以下の画面を表示します。

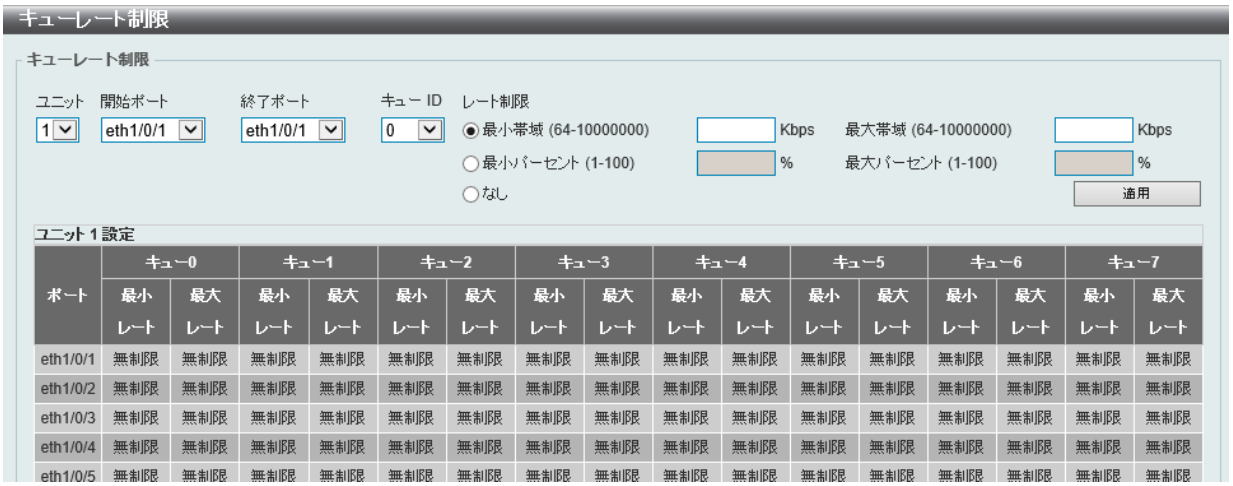


図 10-6　キューレート制限画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
キュー ID	キュー ID を指定します。 • 選択肢：0-7
レート制限	キューレート制限の設定を行います。 •「最小帯域 / 最大帯域」- 最小 / 最大のレート制限帯域値を入力します。 - 設定可能範囲：64-10000000（ Kbps） •「最小パーセント / 最大パーセント」- 最小 / 最大のレート制限パーセンテージを入力します。 - 設定可能範囲：1-100（%） •「なし」- 指定ポートのレート制限を「なし」に設定します。 最小帯域の値により、キューから送信されるパケットが保証されます。また、帯域幅に余裕がある場合でも、キューからの送信パケットは最大帯域幅を超えることはありません。 各キューの最小帯域幅が保証されるようにするために、最小帯域幅の合計はインタフェース帯域幅の 75% 未満である必要があります。最も優先度の高い Strict プライオリティキューに対しては、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が一杯である場合にはこのキューのトラフィックが最初に処理されるためです。 1 つの CoS における最小保証帯域は、物理ポートにまたがって使用することはできないため、本設定は物理ポートにのみ設定可能であり、ポートチャネルに対しては設定できません。

「適用」をクリックして、設定内容を適用します。

詳細設定

QoS の詳細設定を行います。

DSCP 変換マップ

本項目では「Differentiated Services Code Point」(DSCP) 変更マップ設定を行います。
インタフェースでパケットを受信すると、QoS 関連の処理の前に、DSCP 変更マップに基づき受信 DSCP が他の DSCP に変更されます。DSCP 変更機能は、異なる DSCP 割り当てを持つドメインを統合する場合に役に立ちます。DSCP-CoS マップと DSCP-color マップはパケット本来の DSCP に基づいて動作します。後続のすべての動作は変更 DSCP に基づいています。

QoS > 詳細設定 > DSCP 変換マップの順にクリックし、以下の画面を表示します。

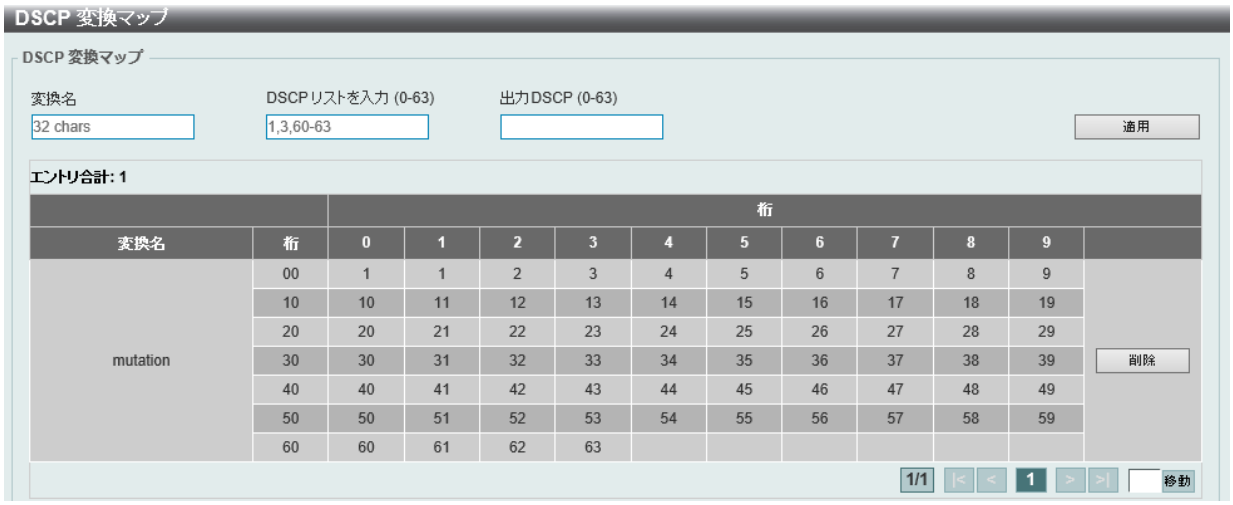


図 10-7　DSCP 変換マップ画面

画面に表示される項目：

項目	説明
変換名	DSCP 変更マップ名を指定します。(32 文字以内)
DSCP リストを入力	インプット DSCP リストの値を入力します。 • 設定可能範囲：0-63
出力 DSCP	アウトプット DSCP リストの値を入力します。 • 設定可能範囲：0-63

「適用」をクリックして、各項目の変更を適用します。
「削除」をクリックすると指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

ポートトラストステートと変換バインディング

本スイッチにおけるポートトラスト設定と表示を行います。

QoS > 詳細設定 > ポートトラストステートと変換バインディングの順にメニューをクリックし、以下の画面を表示します。



図 10-8　ポートトラストステートと変換バインディング画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
トラストステート	ポートトラストの設定をします。 • 選択肢：「CoS」「DSCP」
DSCP 変換マップ	DSCP 変換マップ名を入力します。(32 文字以内) 「なし」を選択すると指定ポートに DSCP 変換マップを割り当てません。

「適用」をクリックして、設定内容を適用します。

DSCP CoS マッピング

本スイッチにおける DSCP CoS マップの設定と表示を行います。

QoS > 詳細設定 > DSCP CoS マッピングの順にメニューをクリックし、以下の画面を表示します。

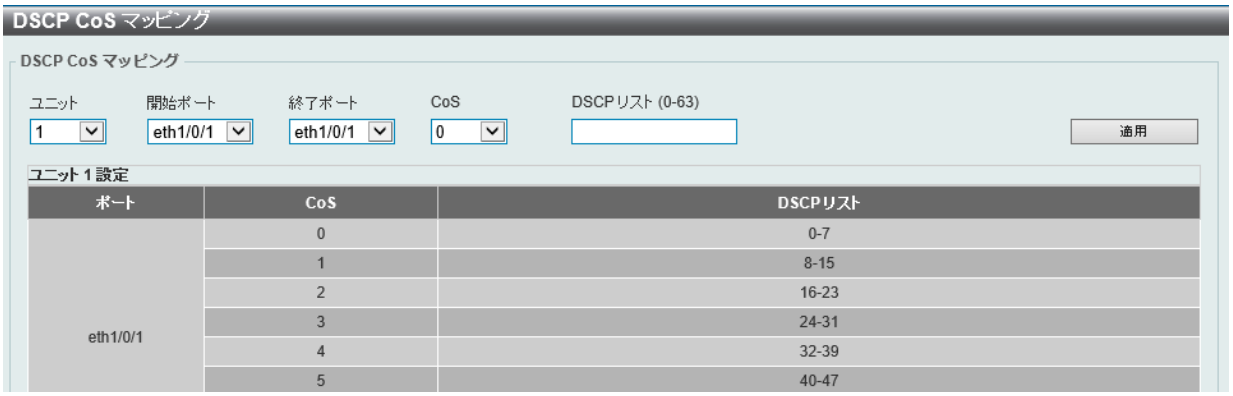


図 10-9　DSCP CoS マッピング画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
CoS	DSCP リストにマッピングする CoS 値を指定します。 • 設定可能範囲：0-7
DSCP リスト	CoS 値をマッピングする DSCP リストの値を入力します。 • 設定可能範囲：0-63

「適用」をクリックして、設定内容を適用します。

CoS カラーマッピング

本スイッチにおける CoS カラーマップの設定と表示を行います。

QoS > 詳細設定 > CoS カラーマッピングの順にメニューをクリックし、以下の画面を表示します。

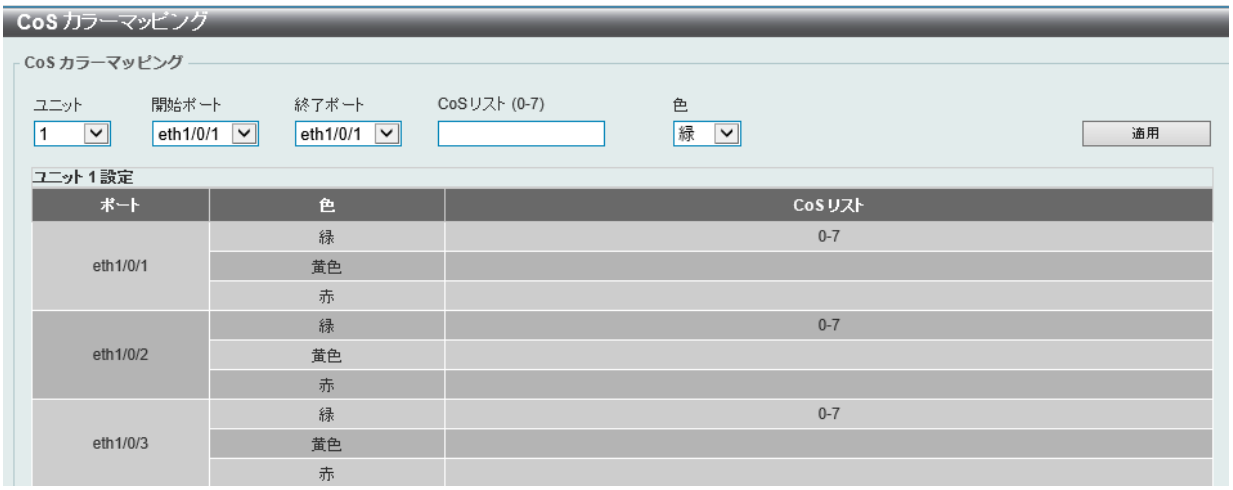


図 10-10　CoS カラーマッピング画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
CoS リスト	カラーマップされる CoS の値を指定します。 • 設定可能範囲：0-7
色	CoS 値にマッピングされるカラーを指定します。 • 選択肢：「緑」「黄色」「赤」

「適用」をクリックして、設定内容を適用します。

DSCP カラーマッピング

本スイッチにおける DSCP カラーマッピングの設定と表示を行います。

QoS > 詳細設定 > DSCP カラーマッピングの順にメニューをクリックし、以下の画面を表示します。

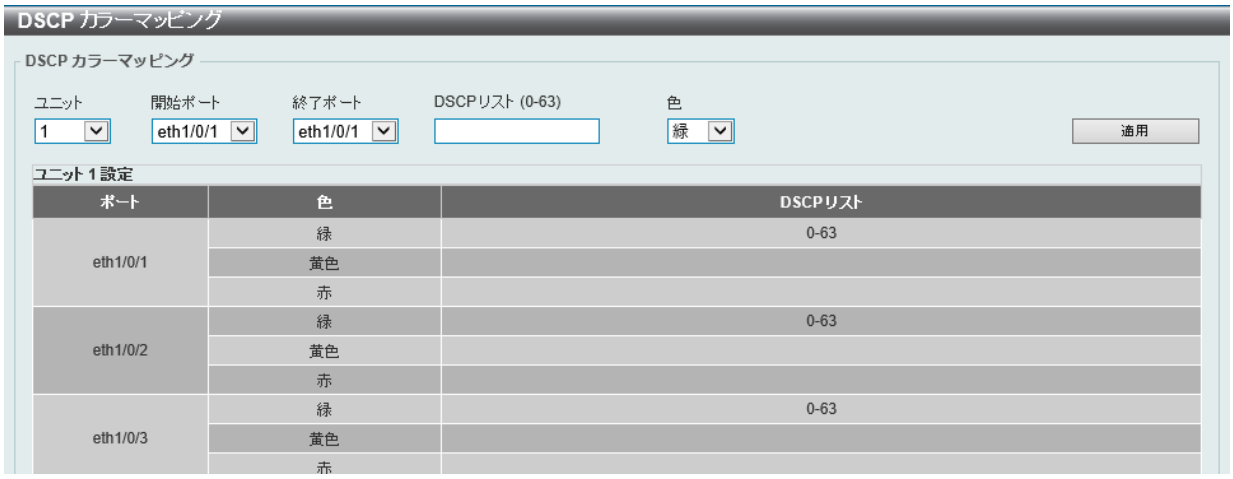


図 10-11　DSCP カラーマッピング画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
DSCP リスト	カラーマッピングされる DSCP リストを指定します。 • 設定可能範囲：0-63
色	DSCP 値にマッピングされるカラーを指定します。 • 選択肢：「緑」「黄色」「赤」

「適用」をクリックして、設定内容を適用します。

クラスマップ

本スイッチにおけるクラスマップの設定と表示を行います。

QoS > 詳細設定 > クラスマップの順にメニューをクリックし、以下の画面を表示します。

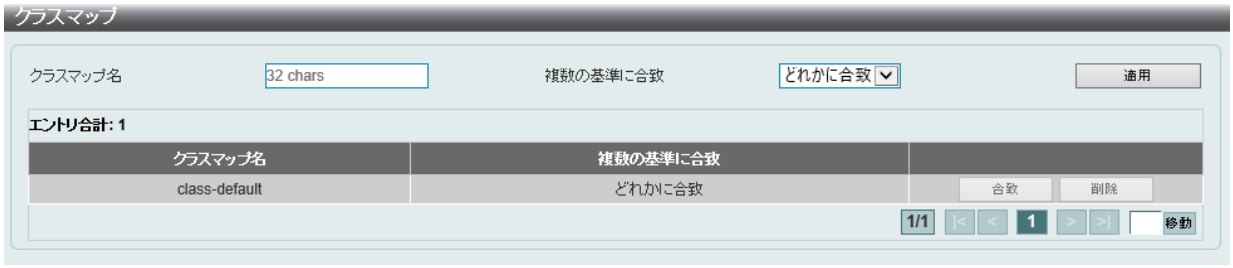


図 10-12　クラスマップ画面

画面に表示される項目：

項目	説明
クラスマップ名	クラスマップ名を指定します。（32 文字以内）
複数の基準に合致	一致条件の種類を指定します。 • 選択肢：「すべて合致」「どれかに合致」

「適用」をクリックして、設定内容を適用します。
「合致」をクリックして、指定のエントリを設定します。
「削除」をクリックして、指定のエントリを削除します。

「合致」ボタンをクリックすると下記の画面が表示されます。

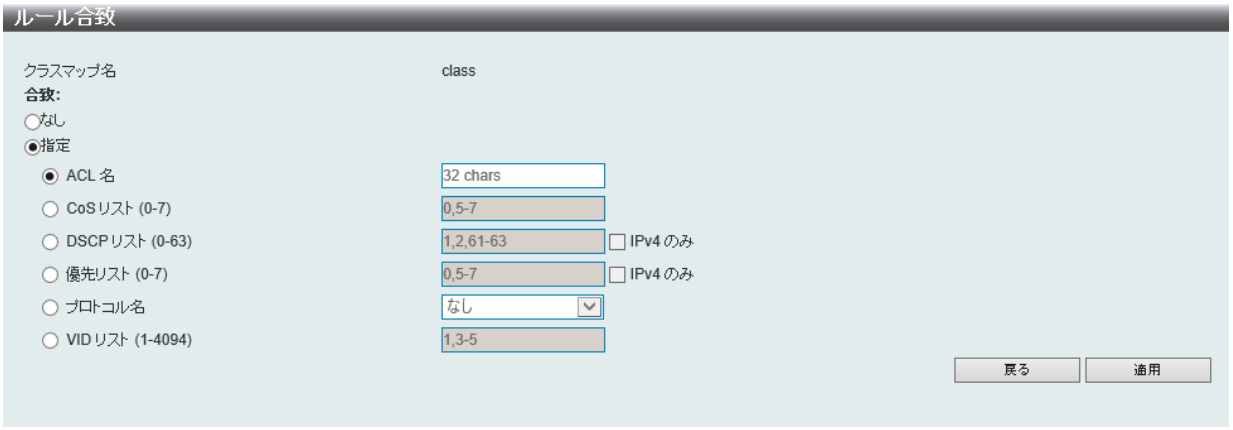


図 10-13　ルール合致画面

画面に表示される項目：

項目	説明
なし	このクラスマップでは照合を行いません。
指定	このクラスマップでは下記のいずれかのオプションで照合を行います。 • 「ACL 名」- クラスマップで照合するアクセスリスト名を指定します。（32 文字以内） • 「CoS リスト」- クラスマップで照合する CoS リスト値を指定します。 - 設定可能範囲：0-7 • 「DSCP リスト」- クラスマップで照合する DSCP リスト値を指定します。「IPv4 のみ」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。 - 設定可能範囲：0-63 • 「優先リスト」- クラスマップで照合する優先（Precedence）リスト値を指定します。「IPv4 のみ」にチェックを入れると、IPv4 パケットのみ照合します。チェックを入れない場合、IPv4/v6 両方のパケットを照合します。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが優先（Precedence）になります。 - 設定可能範囲：0-7 • 「プロトコル名」- クラスマップで照合するプロトコル名を指定します。 - 選択肢:「なし」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」「SSH」「Telnet」「TFTP」 • 「VID リスト」- クラスマップで照合する VLAN リスト値を指定します。 - 設定可能範囲：1-4094

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックすると前のページに戻ります。

集約ポリサー

本スイッチにおける集約ポリサー（Aggregate ポリサー）の設定と表示を行います。

QoS > 詳細設定 > 集約ポリサー の順にメニューをクリックし、以下の画面を表示します。



図 10-14　集約ポリサー 画面

画面に表示される項目：

項目	説明
集約ポリサー名	集約ポリサー名を入力します。
平均レート	平均レート値を入力します。 • 設定可能範囲：0-10000000（ kbps）
通常のバーストサイズ	ノーマルバーストサイズを入力します。 • 設定可能範囲：0-16384（ Kbytes）
最大バーストサイズ	最大バーストサイズを入力します。 • 設定可能範囲：0-16384（ Kbytes）
適合アクション	緑色パケットに対するアクションを指定します。 •「破棄」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 •「Set-DSCP-1P」- IP DSCP 値と 1P 送信値を入力します。 •「送信」- パケットはそのまま送信されます。（初期値）
超えた際の動作	レート制限を超えたパケットに行う操作を指定します。 •「破棄」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（ DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 •「Set-DSCP-1P」- IP DSCP 値と 1P 送信値を入力します。 •「送信」- パケットはそのまま送信されます。
違反動作	シングルレートポリシングにおけるノーマルおよび最大バーストサイズを超えたパケットに対するアクションを指定します。「CIR」や「PIR」を順守しないパケットの動作を指定します。 •「なし」- 違反動作を行いません。 •「破棄」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（ DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 •「Set-DSCP-1P」- IP DSCP 値と 1P 送信値を入力します。 •「送信」- パケットはそのまま送信されます。 シングルレートのポリサーの場合、初期値ではシングルレート 2 色ポリサーが作成されます。 2 レートポリサーの場合、初期値では「破棄」オプションが適用され、パケットは破棄されます。
カラーアウェア	カラーアウェア（Color Aware）を有効 / 無効に指定します。 •「有効」- ポリサーはカラーアウェア（Color-Aware）モードで動作します。 •「無効」- ポリサーはカラーブラインド（Color-Blind）モードで動作します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックすると指定のエントリを削除します。

「レート設定」タブをクリックすると次のページが表示されます。

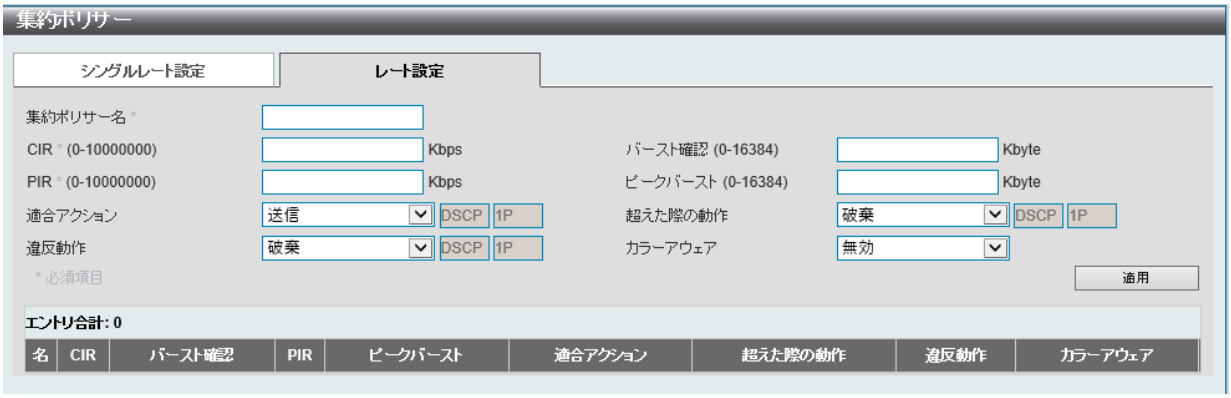


図 10-15　集約ポリサー - レート設定タブ画面

画面に表示される項目：

項目	説明
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。 • 設定可能範囲：0-10000000（kbps） この保証パケットレートは、２レートメータリングにおける最初のトークンバケットになります。
バースト確認	バーストサイズを入力します。 • 設定可能範囲：0-16384（Kbytes） 「バースト確認」は、最初のトークンバケットのバーストサイズ（kbps）になります。
PIR	PIR（Peak Information Rate）値を入力します。 • 設定可能範囲：0-10000000（kbps） PIR は、２レートメータリングにおける二つ目のトークンバケットになります。
ピークバースト	ピークバースト値を入力します。 • 設定可能範囲：0-16384（Kbytes） ピークバーストサイズは、二つ目のトークンバケットのバーストサイズになります。
適合アクション	緑色パケットに対するアクションを指定します。 •「破棄」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 •「Set-DSCP-1P」- IP DSCP 値と 1P 送信値を入力します。 •「送信」- パケットはそのまま送信されます。(初期値)
超えた際の動作	レート制限を超えたパケットに行う操作を指定します。 •「破棄」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 •「Set-DSCP-1P」- IP DSCP 値と 1P 送信値を入力します。 •「送信」- パケットはそのまま送信されます。 ２レートポリサーの場合、初期値では「破棄」オプションが適用され、パケットは破棄されます。
違反動作	シングルレートポリシングにおけるノーマルおよび最大バーストサイズを超えたパケットに対するアクションを指定します。 「CIR」や「PIR」を順守しないパケットの動作を指定します。 •「破棄」- パケットを破棄します。 •「Set-DSCP-Transmit」- IP differentiated services code points（ DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 •「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 •「Set-DSCP-1P」- IP DSCP 値と 1P 送信値を入力します。 •「送信」- パケットはそのまま送信されます。 シングルレートのポリサーの場合、初期値ではシングルレート２色ポリサーが作成されます。 ２レートポリサーの場合、初期値では「破棄」オプションが適用され、パケットは破棄されます。
カラーアウェア	カラーアウェア（Color Aware）を有効 / 無効に指定します。 •「有効」- ポリサーはカラーアウェア（Color-Aware）モードで動作します。 •「無効」- ポリサーはカラーブラインド（Color-Blind）モードで動作します。

「適用」をクリックして、設定内容を適用します。

ポリシーマップ

本スイッチにおけるポリシーマップの設定と表示を行います。

QoS > 詳細設定 > ポリシーマップの順にメニューをクリックし、以下の画面を表示します。



図 10-16　ポリシーマップ画面

画面に表示される項目：

項目	説明
ポリシーマップを作成 / 削除	
ポリシーマップ名	ポリシーマップ名を指定します。(32 文字以内)
トラフィックポリシー	
ポリシーマップ名	ポリシーマップ名を指定します。(32 文字以内)
クラスマップ名	クラスマップ名を指定します。(32 文字以内)

「適用」をクリックして、設定内容を適用します。

「ポリサー」をクリックして、指定のポリシーマップのポリサーアクション設定をします。

「削除」をクリックして、指定のエントリを削除します。

「アクション設定」をクリックして、指定のポリシーマップの設定をします。以下の画面が表示されます。

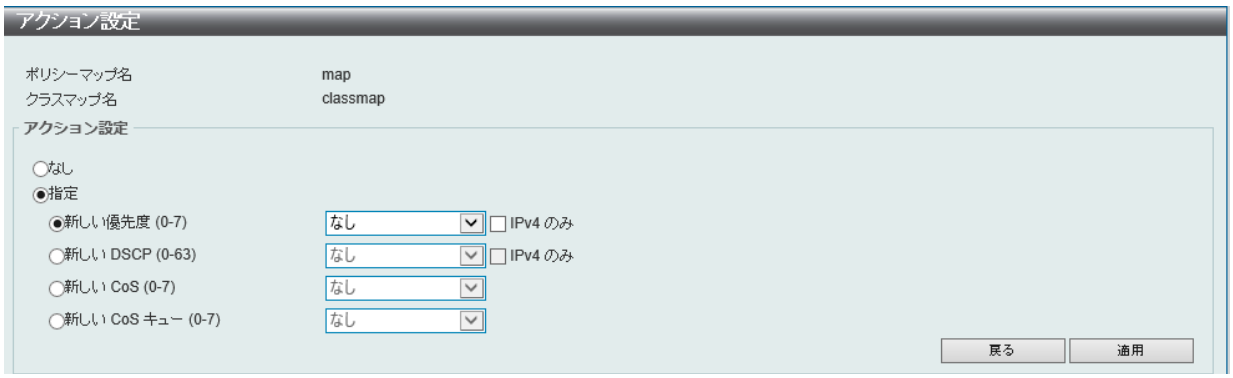


図 10-17　アクション設定画面

画面に表示される項目：

項目	説明
なし	アクションを実行しません。
指定	設定に基づきアクションを実行します。
新しい優先度	新しい優先度 (Precedence) 値を選択します。 「IPv4 のみ」にチェックを入れると、IPv4 の優先度のみマークされます。チェックを入れない場合、IPv4/v6 両方の優先度がマークされます。IPv6 パケットの場合、IPv6 ヘッダに含まれるトラフィッククラスの上位 3 ビットが優先度になります。優先度 の設定は CoS キュー選択には影響しません。 • 設定可能範囲：0-7
新しい DSCP	パケットの新しい DSCP 値を指定します。 「IPv4 のみ」にチェックを入れると、IPv4 DSCP のみマークされます。チェックが入っていない場合、IPv4 と IPv6 の両方の DSCP がマークされます。CoS キュー選択には影響ありません。 • 設定可能範囲：0-63

項目	説明
新しい CoS	パケットの新しい CoS 値を指定します。入力インタフェースにポリシーマップが適用されている場合、CoS 値の設定は CoS キュー選択に影響します。 • 設定可能範囲：0-7
新しい CoS キュー	パケットの新しい CoS キュー値を指定します。元の CoS キュー選択は上書きされます。インタフェースの出力フローにポリシーマップが適用されている場合、CoS 値の設定は影響しません。 • 設定可能範囲：0-7

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックすると前のページに戻ります。

「ポリサー」をクリックすると以下の画面が表示されます。



図 10-18　ポリサー 画面

画面に表示される項目：

項目	説明
なし	このエントリにポリサー設定を指定しない場合に選択します。
指定	このエントリにポリサー設定を指定する場合に選択します。 • 選択肢：「ポリシング」「ポリシング cir」「集約ポリサー」
CIR	CIR 値を入力します。「ポリシング cir」を選択した場合に表示されます。
バースト確認	バーストサイズを入力します。「ポリシング cir」を選択した場合に表示されます。
PIR	PIR 値を入力します。「ポリシング cir」を選択した場合に表示されます。
ピークバースト	ピークバーストサイズを入力します。「ポリシング cir」を選択した場合に表示されます。
平均レート	平均レート値を入力します。「ポリシング」を選択した場合に表示されます。 • 設定可能範囲：0-10000000（Kbps）
通常のバーストサイズ	ノーマルバーストサイズを入力します。「ポリシング」を選択した場合に表示されます。 • 設定可能範囲：0-16384（Kbyte）
最大バーストサイズ	最大バーストサイズを入力します。「ポリシング」を選択した場合に表示されます。 • 設定可能範囲：0-16384（Kbyte）
適合アクション	適合パケットに対するアクションを指定します。「ポリシング」または「ポリシング cir」を選択した場合に表示されます。 • 「破棄」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 • 「Set-DSCP-1P」- DSCP 値および 802.1p 値を入力し、新しい DSCP 値および 802.1p 値でパケットを送信します。 • 「送信」- パケットはそのまま送信されます。
超えた際の動作	超過パケットに対するアクションを指定します。「ポリシング」または「ポリシング cir」を選択した場合に表示されます。 • 「破棄」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 • 「Set-DSCP-1P」- DSCP 値および 802.1p 値を入力し、新しい DSCP 値および 802.1p 値でパケットを送信します。 • 「送信」- パケットはそのまま送信されます。

項目	説明
違反動作	違反パケットに対するアクションを指定します。「ポリシング」または「ポリシング cir」を選択した場合に表示されます。 • 「なし」- 違反動作を行いません。 • 「破棄」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- 1P 送信値を入力し、新しい 802.1p の値でパケットを送信します。 • 「Set-DSCP-1P」- DSCP 値および 802.1p 値を入力し、新しい DSCP 値および 802.1p 値でパケットを送信します。 • 「送信」- パケットはそのまま送信されます。
カラーアウェア	カラーアウェア（Color Aware）を有効 / 無効に指定します。「ポリシング」または「ポリシング cir」を選択した場合に表示されます。 • 「有効」- ポリサーはカラーアウェア（Color-Aware）モードで動作します。 • 「無効」- ポリサーはカラーブラインド（Color-Blind）モードで動作します。

「適用」をクリックして、設定内容を適用します。

ポリシーバインディング

ポリシーバインディング設定を行います。

QoS > 詳細設定 > ポリシーバインディングの順にメニューをクリックし、以下の画面を表示します。



図 10-19　ポリシーバインディング画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
方向	トラフィックの方向を指定します。 • 選択肢：「入力」（イングレストラフィック）、「出力」（イーグレストラフィック）
ポリシーマップ名	ポリシーマップ名を指定します。（32 文字以内） 「なし」を選択すると本エントリにポリシーマップは関連付けられません。

「適用」をクリックして、設定内容を適用します。

QoS PFC

ネットワーク「Quality of Service」（QoS）プライオリティベースフローコントロール（PFC）クラスマップの設定を行います。

ネットワーク QoS クラスマップ

本項目ではネットワーク「Quality of Service」（QoS）プライオリティベースフローコントロール（PFC）クラスマップの設定、表示を行います。
ポリシーバインディング設定を行います。

QoS > QoS PFC > ネットワーク QoS クラスマップの順にメニューをクリックし、以下の画面を表示します。



図 10-20　ネットワーク QoS クラスマップ画面

画面に表示される項目：

項目	説明
ネットワーク QoS クラスマップ 名	トラフィックポリシーに適用するネットワーク QoS クラスマップ名を指定します。（32 文字以内）

設定を変更する際は、必ず「適用」をクリックして、設定内容を適用してください
「削除」をクリックすると指定のエントリを削除します。
「合致」をクリックすると指定のエントリのマッチルール設定を設定します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「合致」をクリックすると、以下の画面が表示されます。

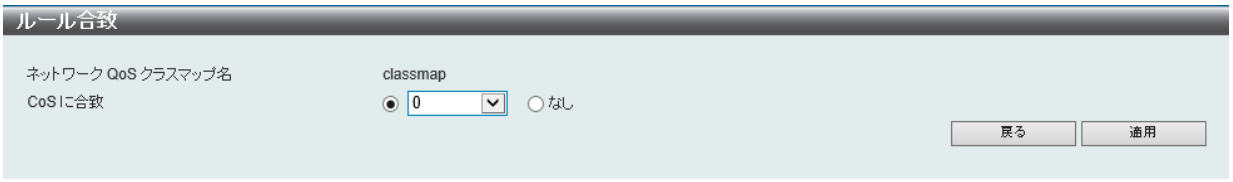


図 10-21　ルール合致画面

画面に表示される項目：

項目	説明
CoS に合致	照合する IEEE 802.1Q Class of Service (CoS) 値を指定します。 パケットを受信すると、このパケットにインターナル CoS が付与されます。このインターナル CoS を使用して、CoS- キューマッピングに基づいた送信キューが選択されます。CoS キューの値が大きいほど、優先度が高くなります。 「なし」を選択すると、CoS 値による照合を無効にします。 • 選択肢：0-7

「戻る」をクリックすると前のページに戻ります。
設定を変更する際は、必ず「適用」をクリックして、設定内容を適用してください。

ネットワーク QoS ポリシーマップ

本項目ではネットワーク「Quality of Service」（QoS）ポリシーマップの設定、表示を行います。

QoS > QoS PFC > ネットワーク QoS ポリシーマップの順にメニューをクリックし、以下の画面を表示します。

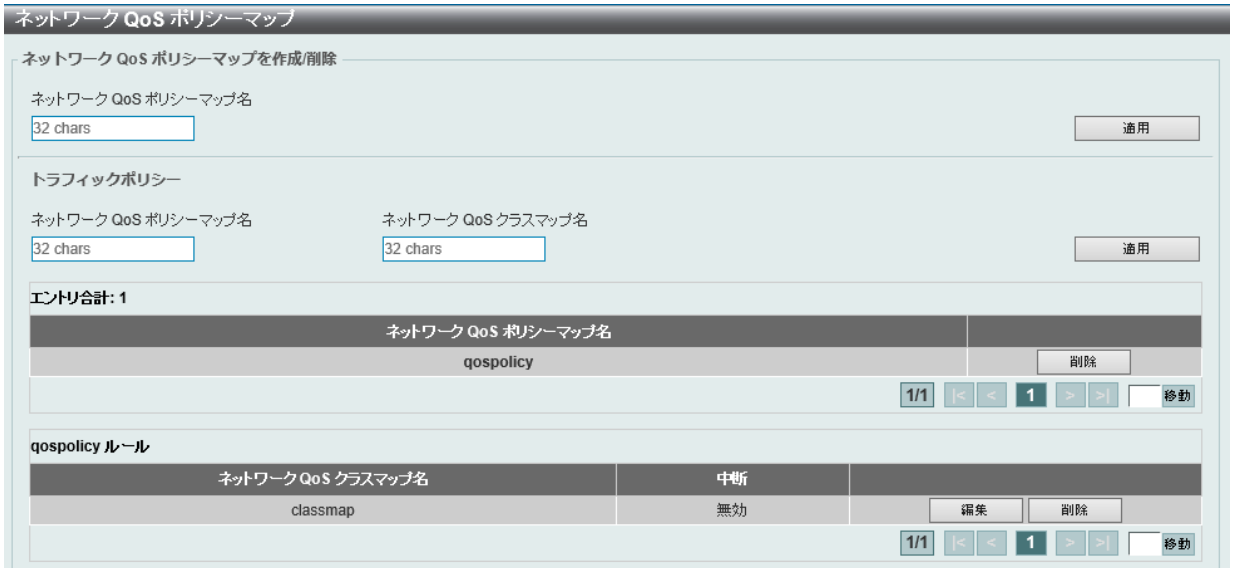


図 10-22　ネットワーク QoS ポリシーマップ画面

画面に表示される項目：

項目	説明
ネットワーク QoS ポリシーマップを作成 / 削除	
ネットワーク QoS ポリシーマップ名	ネットワーク QoS ポリシーマップ名を指定します。（32 文字以内）
トラフィックポリシー	
ネットワーク QoS ポリシーマップ名	ネットワーク QoS ポリシーマップ名を指定します。（32 文字以内）
ネットワーク QoS クラスマップ名	ネットワーク QoS クラスマップ名を指定します。（32 文字以内）

設定を変更する際は、必ず「適用」をクリックして、設定内容を適用してください
「削除」をクリックすると指定のエントリを削除します。
設定エントリページが複数ある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

「編集」をクリックし、以下の画面で指定エントリの編集を行います。



図 10-23　ネットワーク QoS ポリシーマップ（編集）画面

画面に表示される項目：

項目	説明
中断	「中断」機能を有効 / 無効に指定します。タイプネットワーク QoS ポリシーマップ内参照クラスの PFC を有効にします。

「適用」をクリックして、設定内容を適用します。

ネットワーク QoS ポリシーバインディング

本項目ではネットワーク「Quality of Service」（QoS）ポリシーバインディングの設定、表示を行います。

QoS > QoS PFC > ネットワーク QoS ポリシーバインディングの順にメニューをクリックし、以下の画面を表示します。



図 10-24　ネットワーク QoS ポリシーバインディング画面

画面に表示される項目：

項目	説明
ユニット	設定を行うユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
方向	「入力」を指定します。インタフェース上のイングレスフローに対してポリシーマップを適用します。
ネットワーク QoS ポリシーマップ名	ネットワーク QoS ポリシーマップ名を指定します。（32 字以内） 「なし」を選択すると、ネットワーク QoS ポリシーマップへの関連付けを行いません。

「適用」をクリックして、設定内容を適用します。

PFC ポート設定

本項目では Priority-based Flow Control（PFC）の設定、表示を行います。

注意　Priority-based Flow Control（PFC）は 10G ポートでのみ有効です。

QoS > QoS PFC > PFC ポート設定の順にメニューをクリックし、以下の画面を表示します。



図 10-25　PFC ポート設定画面

画面に表示される項目：

項目	説明
PFC カウンタをクリア	
ユニット	設定を行うユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
フレームタイプ	クリアするフレームタイプを指定します。 • 「RX」- 受信した PFC フレームのカウンタをクリアします。 • 「TX」- 送信された PFC フレームのカウンタをクリアします。 • 「両方」- 送受信された PFC フレームのカウンタをクリアします。

「適用」をクリックして、設定内容を適用します。
「クリア」をクリックすると入力したエントリをクリアします。

WRED

重み付けランダム早期検出（WRED）は、QoS キューの全体的なスループットを向上させる QoS 機能の 1 つです。
この方式では、スイッチに設定された QoS の出力キューに基づいて、パケットと QoS キューを分析し、QoS キューに入るパケットにオーバーフローが発生しているかどうかを判断し、ランダムにパケットを破棄してキューへのパケットフローを最小化します。

WRED は、QoS キュー内の輻輳を回避する 2 つの方法を採用しています。

- 各 QoS キューには、パケットを受け入れる最小レベルと最大レベルが設定されます。キューの最大しきい値に達すると、スイッチはすべての入力パケットの破棄を開始します。これにより、QoS に割り当てられた帯域幅を最小化します。最小しきい値を下回ると、スイッチはすべての入力パケットを受け入れます。
- 入力パケットが最大キューと最小キューの範囲内にある場合、スイッチはスロープ確率関数を使用し、キューが最大しきい値に達した際の破棄確率を決める最大破棄レートに基づき、ランダムなパケット破棄方法を決定します。キューが最大しきい値に近い場合、スイッチはランダムパケットの廃棄を増やしてキューへのフローを均等にし、優先度の高いキューへのオーバーフローを回避します。

WRED プロファイル

WRED プロファイル設定を行います。

QoS > WRED > WRED プロファイル の順にメニューをクリックし、以下の画面を表示します。



図 10-26　WRED プロファイル画面

画面に表示される項目：

項目	説明
プロファイル	WRED プロファイル ID を入力します。 • 設定可能範囲：1-32
パケットタイプ	パケットタイプを TCP に指定します。
パケット色	パケットカラーを選択します。 •「緑」- 緑のパケットの WRED 破棄パラメータを設定します。 •「黄色」- 黄色のパケットの WRED 破棄パラメータを設定します。 •「赤」- 赤のパケットの WRED 破棄パラメータを設定します。
最小しきい値	WRED 破棄を開始する最小しきい値を入力します。 • 設定可能範囲：0-100
最大しきい値	最大しきい値を入力します。このしきい値を超えると、WRED により、キュー宛てのすべてのパケットが破棄されます。 • 設定可能範囲：0-100
最大ドロップレート	破棄レートの最大値を入力します。 平均キューサイズが最大しきい値に達したときのドロップレートを指定します。この値が「0」の場合、パケットは破棄されないか、ECN に対して再マーキングされません。 • 設定可能範囲：0-14

「適用」をクリックして、設定内容を適用します。
「検索」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「設定をリセット」をクリックして指定エントリの再設定を行います。

WRED キュー

WRED のキュー設定を行います。
WRED は、輻輳を示す特定のしきい値を超える平均キューサイズに基づいてパケットを破棄します。
「Explicit Congestion Notification」(ECN) は平均キューサイズが特定のしきい値を超えたときに、ECN がパケットをドロップするのではなくマークする WRED の拡張機能です。WRED ECN 機能の設定時に、ルータとエンドホストはこのマーキングをネットワークが輻輳していることを示す信号として使用し、パケットの送信を遅らせます。

QoS > WRED > WRED キューの順にメニューをクリックし、以下の画面を表示します。



図 10-27　WRED キュー画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
CoS	CoS 値を指定します。 • 設定可能範囲：0-7
WRED ステート	指定ポートの WRED 機能を有効 / 無効に設定します。
プロファイル	WERD プロファイル ID を指定します。 • 設定可能範囲：1-32
加重	平均キューサイズ計算に使用される WRED 重み係数を指定します。 • 設定可能範囲：0-15

「適用」をクリックして、設定内容を適用します。

第 11 章　ACL

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールの設定を行うことができます。

以下は、ACL サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
ACL コンフィグレーションウィザード	ACL 設定ウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。
ACL アクセスリスト	ACL アクセスリストの設定を行います。
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の設定を行います。
ACL VLAN アクセスマップ	ACL VLAN アクセスマップの設定を行います。
ACL VLAN フィルタ	ACL VLAN フィルタの設定を行います。
CPU ACL	CPU インタフェースフィルタリング機能の設定を行います。

ACL コンフィグレーションウィザード

ウィザードを使用してアクセスプロファイルとルールを作成・更新します。

ACL コンフィグレーションウィザード

ACL コンフィグレーションウィザードは、アクセスプロファイルと ACL ルールの新規作成を行います。

ACL > ACL コンフィグレーションウィザードの順にメニューをクリックし、以下の画面を表示します。

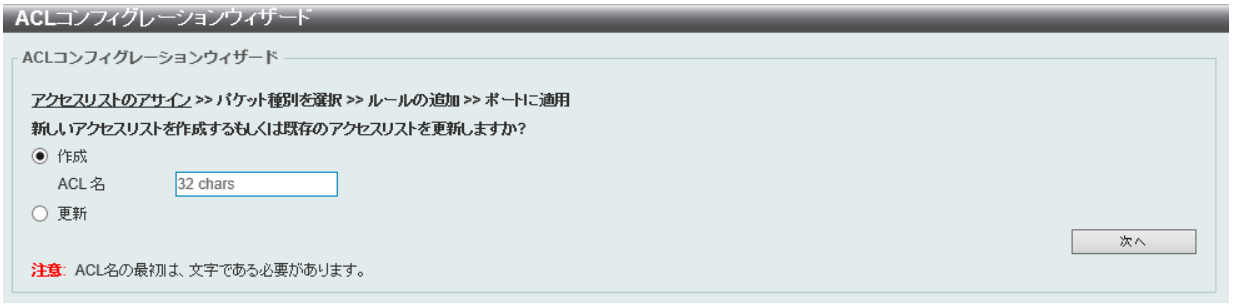


図 11-1　ACL コンフィグレーションウィザード（作成）画面

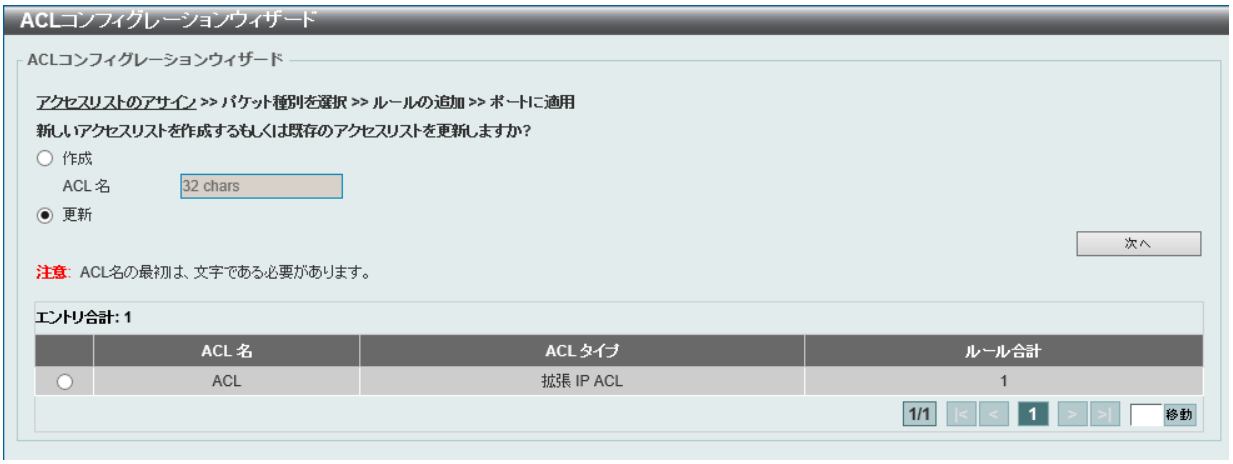


図 11-2　ACL コンフィグレーションウィザード（更新）画面

画面に表示される項目：

項目	説明
作成	新しいアクセスルールを作成する場合は、「作成」を選択します。
ACL 名	作成する ACL 名を指定します。(32 文字以内)
更新	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「次へ」をクリックし、パケットタイプの選択を行います。

パケットタイプ選択（ACL コンフィグレーションウィザード）

「ACL コンフィグレーションウィザード」にて設定する ACL エントリを指定した後、パケットタイプを指定します。

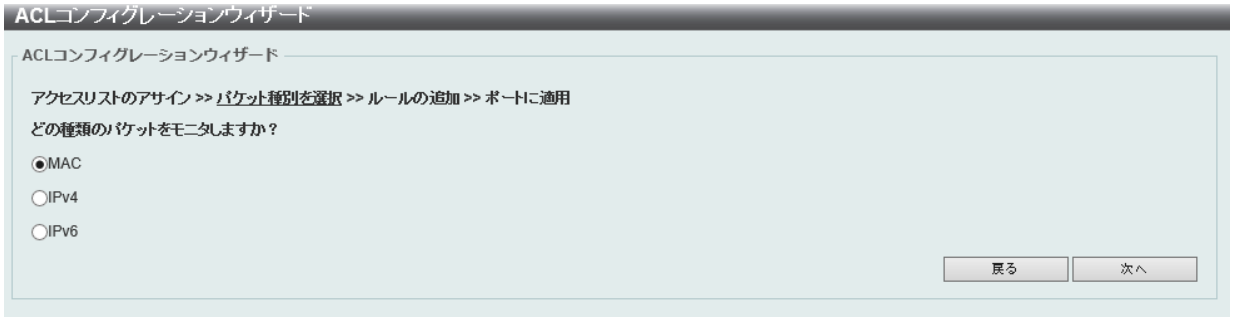


図 11-3　ACL コンフィグレーションウィザード（パケットタイプ選択）画面

画面に表示される項目：

項目	説明
MAC	MAC ACL を作成 / 更新する場合に選択します。
IPv4	IPv4 ACL を作成 / 更新する場合に選択します。
IPv6	IPv6 ACL を作成 / 更新する場合に選択します。

「次へ」をクリックします。選択したパケットの種類により次に表示される画面が異なります。
プロファイルの種類に合わせた設定方法に従い設定を行います。

ルール追加（ACL コンフィグレーションウィザード）

「ACL コンフィグレーションウィザード」にて ACL のパケットタイプを指定した後、各パケットの ACL エントリにおける ACL ルールの追加設定を行います。

MAC ACL ルールの設定

MAC ACL ルールを設定します。「MAC」を選択し「次へ」をクリックし、以下の画面の設定を行います。

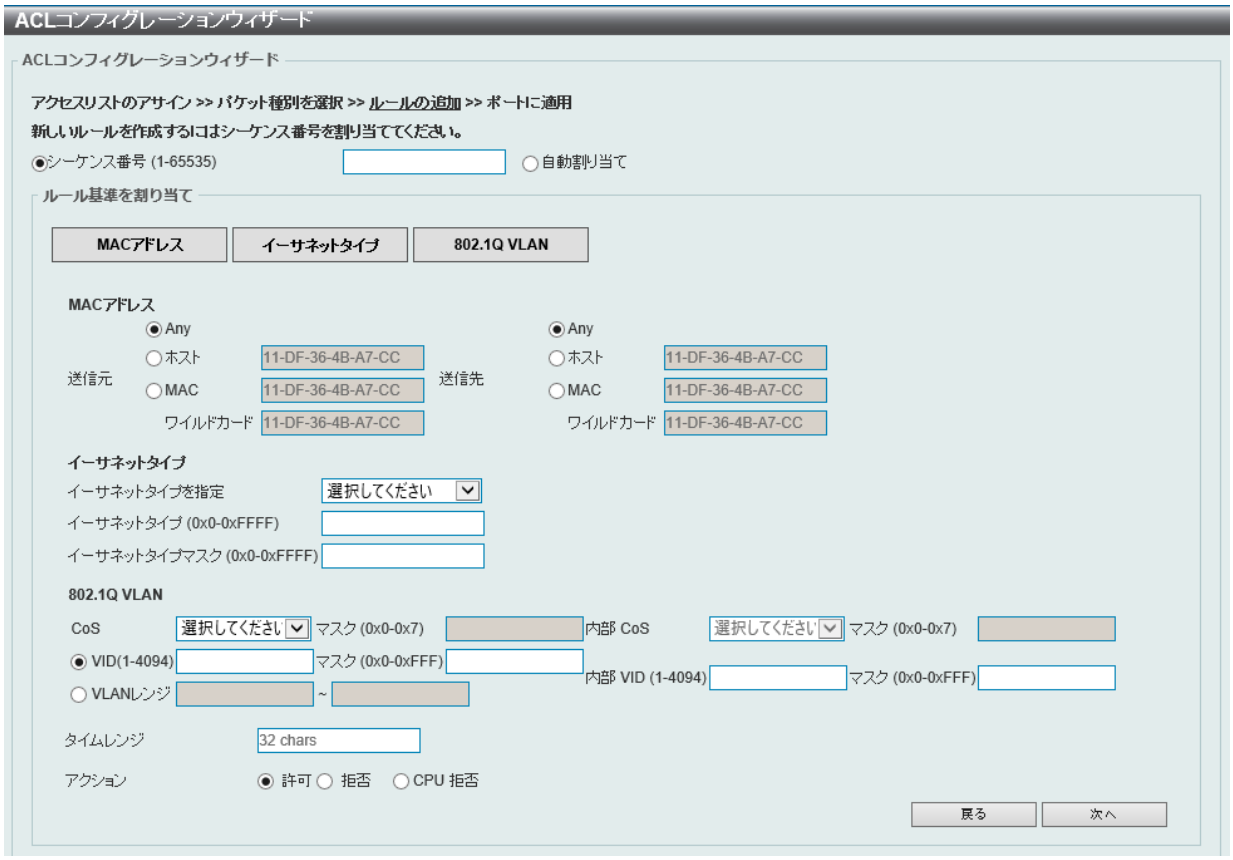


図 11-4　ACL コンフィグレーションウィザード -MAC 画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。 「自動割り当て」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
ルール基準を割り当て	
送信元	送信元の MAC アドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「ホスト」- 送信元ホストの MAC アドレスを入力します。 •「MAC」-「ワイルドカード」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力できます。
送信先	宛先の MAC アドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「ホスト」- 宛先ホストの MAC アドレスを入力します。 •「MAC」-「ワイルドカード」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力できます。
イーサネットタイプを指定	イーサネットタイプを選択します。 • 選択肢：「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
イーサネットタイプ	イーサネットタイプの 16 進数値を指定します。 「イーサネットタイプを指定」で指定したイーサネットタイプに基づき適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
イーサネットタイプ マスク	イーサネットタイプマスクの 16 進数値を指定します。 「イーサネットタイプを指定」で指定したイーサネットタイプに基づき適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「マスク」：CoS マスクを入力します。（0x0-0x7）
内部 CoS	CoS 値を指定後、内部（Inner）CoS の値を入力します。 • 設定可能範囲：0-7 •「マスク」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 •「マスク」：VLAN ID マスクを入力します。（0x0-0xFFF）
内部 VID	ACL ルールに紐づける内部（Inner）VLAN ID を入力します。 • 設定可能範囲：1-4094 •「マスク」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN レンジ	ACL ルールに紐づける VLAN 範囲を指定します。VLAN 範囲の開始 / 終了 VLAN を入力します。 • 設定可能範囲：1-4094
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」

「次へ」をクリックします。
「戻る」をクリックすると前のページに戻ります。

IPv4 ACL ルールの設定

IPv4 ACL ルールを設定します。「IPv4」を選択し「次へ」をクリックし、以下の画面の設定を行います。

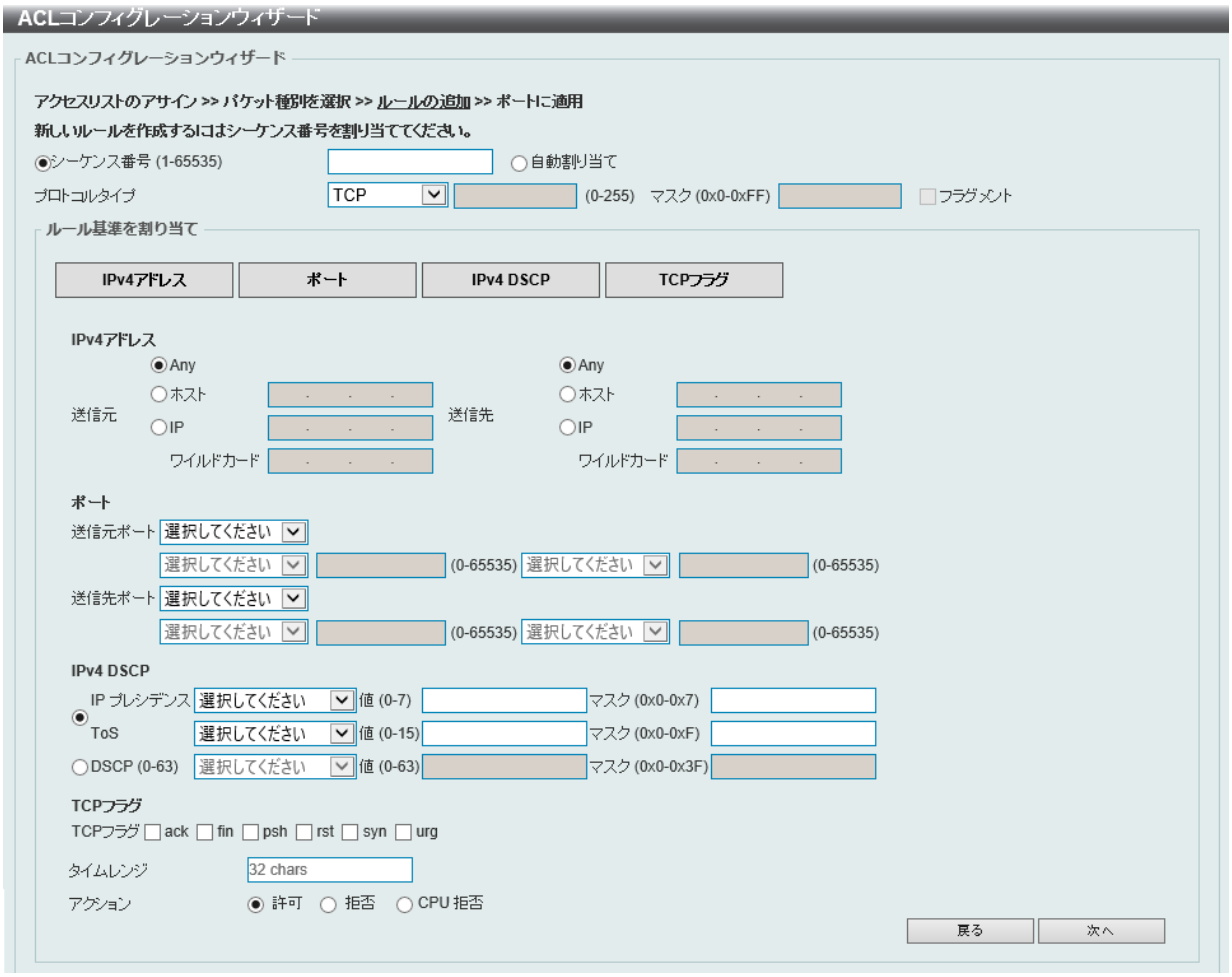


図 11-5　ACL コンフィグレーションウィザード - IPv4 画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。 「自動割り当て」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
プロトコルタイプ	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「プロトコル ID」「なし」 - 「値」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「マスク」-「プロトコル ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「フラグメント」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（IPv4 ACL ルール）

項目	説明
送信元	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
送信先	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
IP プレシデンス	IP 優先値を指定します。 • 選択肢： 「ルーティン」「プライオリティ」「即時」「フラッシュ」「フラッシュ - オーバライド」「クリティカル」「インターネット」「ネットワーク」 - 「値」：IP 優先値を入力します。（0-7） - 「マスク」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「ノーマル」「min mmonetary cost」「max reliability」「最大スループット」「最小遅延」 - 「値」：ToS 値を入力します。（0-15） - 「マスク」：ToS マスクを入力します。（0x0-0x7）
DSCP	使用する DSCP 値を選択します。 • 選択肢：「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5(40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「値」：DSCP 値を入力します。（0-63） - 「マスク」：DSCP マスクを入力します。（0x0-0x3F）
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」

「TCP」「UDP」選択時に表示される項目（IPv4 ACL ルール）

項目	説明
送信元ポート	送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
送信先ポート	宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（IPv4 ACL ルール）

項目	説明
TCP フラグ	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（IPv4 ACL ルール）

項目	説明
ICMP メッセージタイプを指定	使用する ICMP メッセージの種類を指定します。
ICMP メッセージタイプ	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
メッセージコード	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

「次へ」をクリックします。

IPv6 ACL ルールの設定

IPv6 ACL ルールを設定します。「IPv6」を選択し「次へ」をクリックし、以下の画面の設定を行います。

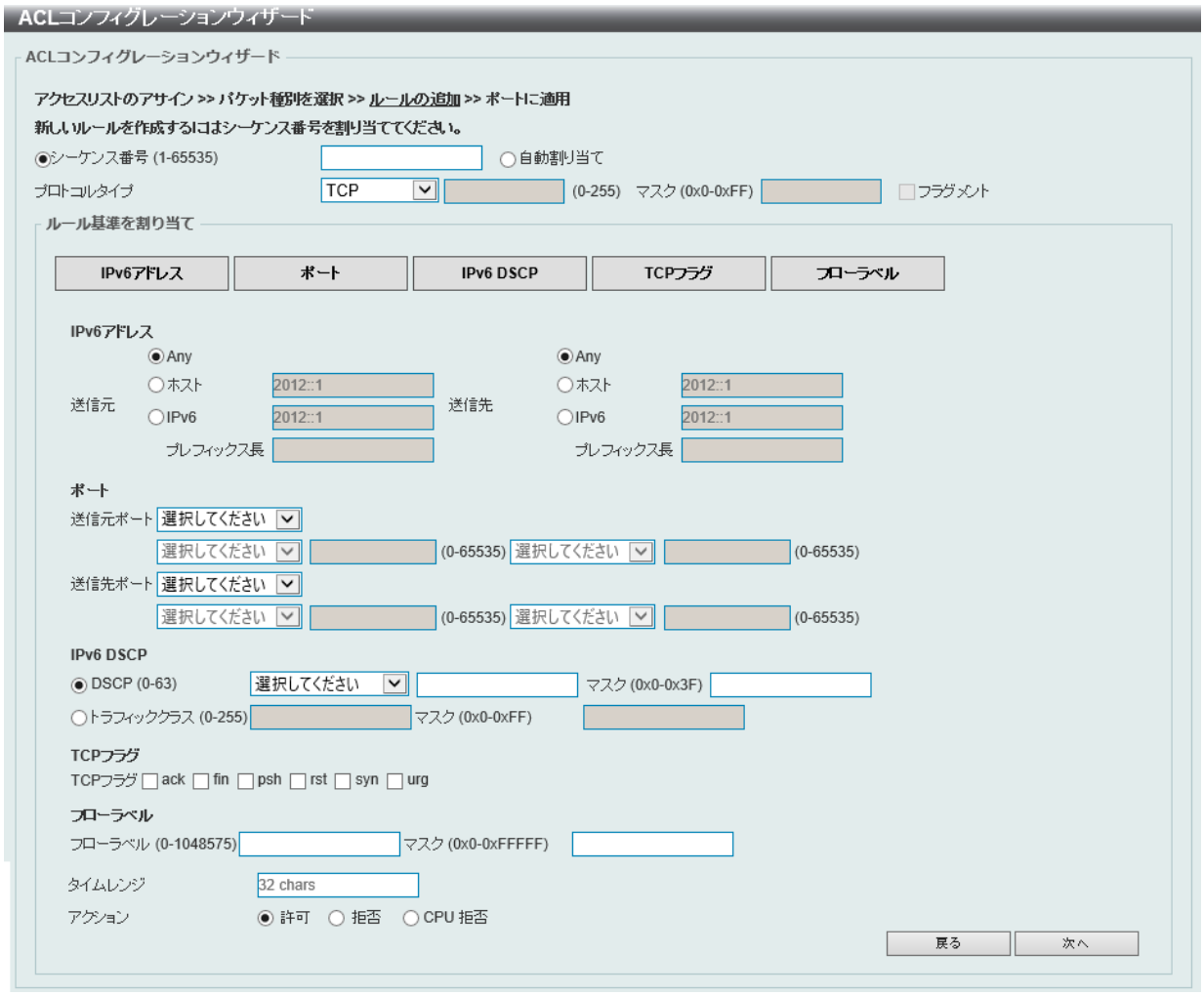


図 11-6　ACL コンフィグレーションウィザード -IPv6 画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。 「自動割り当て」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
プロトコルタイプ	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「ESP」「PCP」「プロトコル ID」「SCTP」「なし」 - 「値」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 -「マスク」-「プロトコル ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 -「フラグメント」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（IPv6 ACL ルール）

項目	説明
送信元	送信元のアドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「ホスト」- 送信元ホストの IPv6 アドレスを入力します。 •「IPv6」-「プレフィックス長」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
送信先	宛先のアドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「ホスト」- 宛先ホストの IPv6 アドレスを入力します。 •「IPv6」-「プレフィックス長」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
DSCP	使用する DSCP 値を選択します。 • 選択肢:「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5(40)」「cs6 (48)」「cs7 (56)」「ef (46)」 -「値」：DSCP 値を入力します。（0-63） -「マスク」：DSCP マスクを入力します。（0x0-0x3F）
フローラベル	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 •「マスク」：フローラベルマスクを入力します。（0x0-0xFFFFF）
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」

「TCP」「UDP」選択時に表示される項目（IPv6 ACL ルール）

項目	説明
送信元ポート	送信元ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
送信先ポート	宛先ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（IPv6 ACL ルール）

項目	説明
TCP フラグ	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（IPv6 ACL ルール）

項目	説明
ICMP メッセージタイプを指定	使用する ICMP メッセージの種類を指定します。
ICMP メッセージタイプ	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
メッセージコード	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

拡張 Expert ACL の設定

拡張 Expert ACL ルールを設定します。既存の拡張 Expert ACL を選択して「次へ」をクリックし、表示された以下の画面の設定を行います。

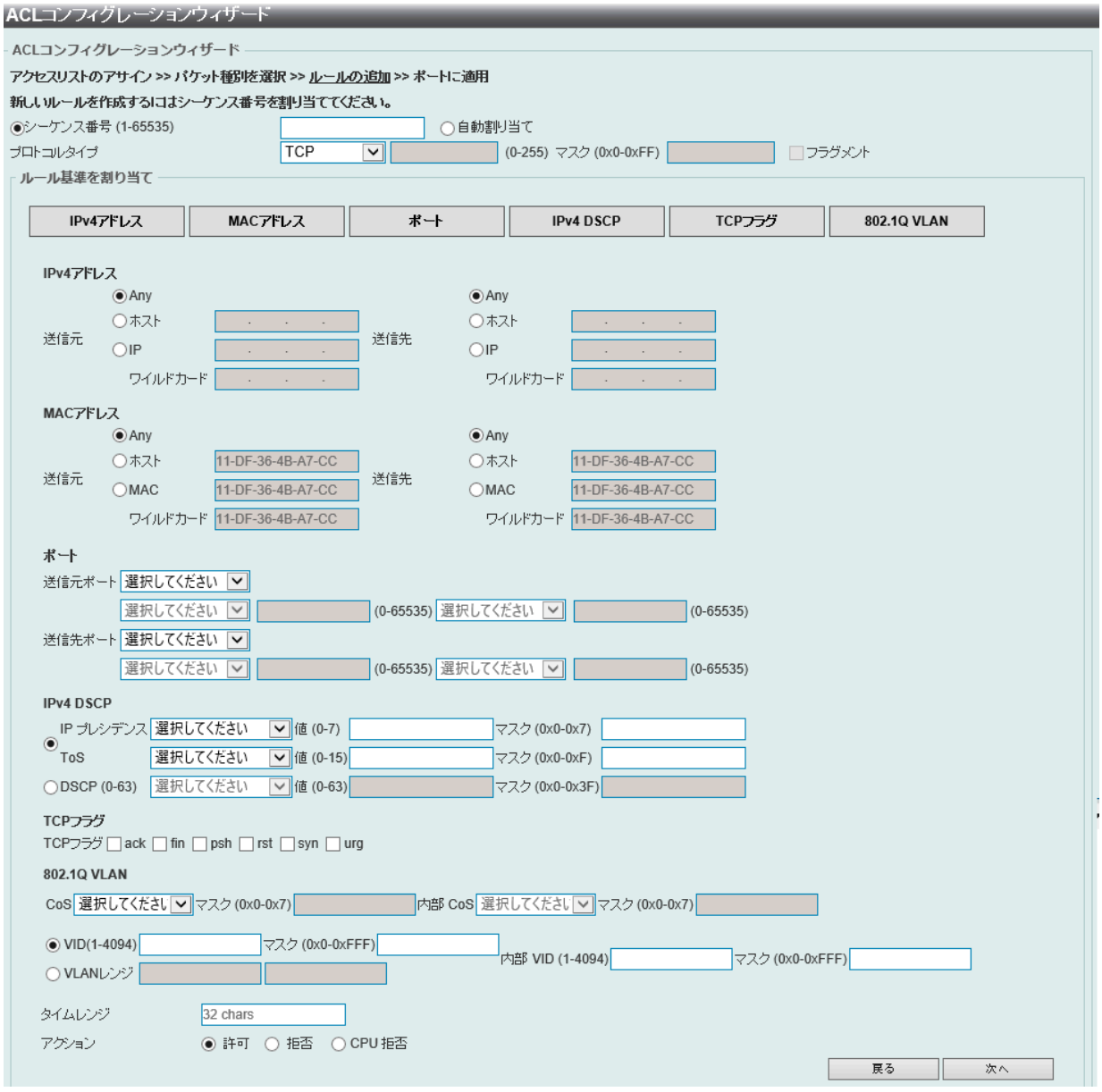


図 11-7　ACL コンフィグレーションウィザード - 拡張 Expert 画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。 「自動割り当て」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535

項目	説明
プロトコルタイプ	プロトコルの種類を選択します。 • 選択肢:「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「プロトコル ID」「なし」 - 「値」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 -「マスク」-「プロトコル ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 -「フラグメント」- パケットフラグメントフィルタを含める場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
IPv4 アドレス	
送信元	送信元のアドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「ホスト」- 送信元ホストの IP アドレスを入力します。 •「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
送信先	宛先のアドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「ホスト」- 宛先ホストの IP アドレスを入力します。 •「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
MAC アドレス	
送信元	送信元の MAC アドレスを指定します。 •「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 •「ホスト」- 送信元ホストの MAC アドレスを入力します。 •「MAC」-「ワイルドカード」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力できます。
送信先	宛先の MAC アドレスを指定します。 •「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 •「ホスト」- 宛先ホストの MAC アドレスを入力します。 •「MAC」-「ワイルドカード」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力できます。
IPv4 DSCP	
IP プレシデンス	IP 優先値を指定します。 • 選択肢：「ルーティン」「プライオリティ」「即時」「フラッシュ」「フラッシュ - オーバライド」「クリティカル」「インターネット」「ネットワーク」 -「値」：IP 優先値を入力します。（0-7） -「マスク」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「ノーマル」「min mmonetary cost」「max reliability」「最大スループット」「最小遅延」 -「値」：ToS 値を入力します。（0-15） -「マスク」：ToS マスクを入力します。（0x0-0x7）
DSCP	使用する DSCP 値を選択します。 • 選択肢:「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5(40)」「cs6 (48)」「cs7 (56)」「ef (46)」 -「値」：DSCP 値を入力します。（0-63） -「マスク」：DSCP マスクを入力します。（0x0-0x3F）
802.1Q VLAN	
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「マスク」：CoS マスクを入力します。（0x0-0x7）
内部 CoS	CoS 値を指定後、内部（Inner）CoS の値を入力します。 • 設定可能範囲：0-7 •「マスク」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 •「マスク」：VLAN ID マスクを入力します。（0x0-0xFFF）
内部 VID	ACL ルールに紐づける内部（Inner）VLAN ID を入力します。 • 設定可能範囲：1-4094 •「マスク」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）

項目	説明
VLAN レンジ	ACL ルールに紐づける VLAN 範囲を指定します。VLAN 範囲の開始 / 終了 VLAN を入力します。 • 設定可能範囲：1-4094
アクション設定	
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」

「TCP」「UDP」選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
送信元ポート	送信元ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
送信先ポート	宛先ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
TCP フラグ	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
ICMP メッセージタイプを指定	使用する ICMP メッセージの種類を指定します。
ICMP メッセージタイプ	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
メッセージコード	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

ポート設定（ACL コンフィグレーションウィザード）

「ACL コンフィグレーションウィザード」にて適用するポートの設定を行います。

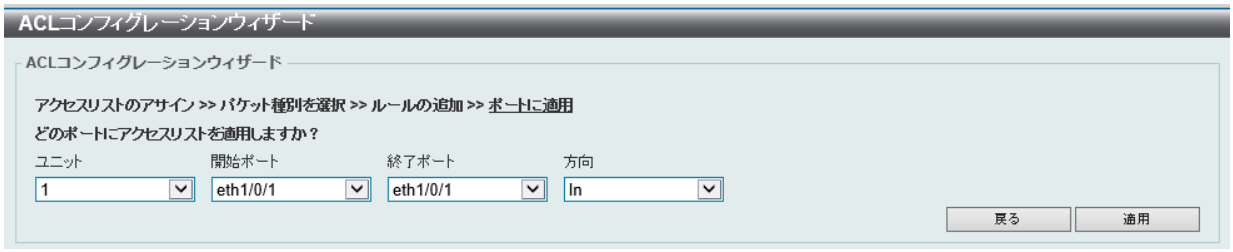


図 11-8　ACL コンフィグレーションウィザード（ポート設定）画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定の対象となるポート範囲を指定します。
方向	方向を指定します。選択肢：「In」「Out」

「適用」をクリックして、設定内容を適用します。
「戻る」をクリックすると前のページに戻ります。

ACL アクセスリスト

アクセスコントロールリスト、ACL ルールの設定、表示を行います。

ACL > ACL アクセスリストの順にメニューをクリックし、以下の画面を表示します。



図 11-9　ACL アクセスリスト画面

画面に表示される項目：

項目	説明
ACL タイプ	ACL プロファイルの種類を選択します。 • 選択肢：「全て」「IP ACL」「IPv6 ACL」「MAC ACL」「エキスパート ACL」
ID	ACL ID を入力します。 • 設定可能範囲：1-14999
ACL 名	ACL 名を入力します。（32 文字以内）

「検索」をクリック し、入力した情報を基にエントリを検索します。
「ACL 追加」をクリック し、新しい ACL プロファイルを作成します。
「編集」をクリックして、指定エントリの編集を行います。「削除」をクリックすると指定のエントリを削除します。

ACL ルールの作成・カウンタの削除

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「ルールの追加」をクリック します。
「すべてのカウンタをクリア」をクリック し、表示されたすべてのカウンタ情報を消去します。
「カウンタをクリア」をクリック し、表示された指定ルールのカウンタ情報を消去します。

■ ACL プロファイルの編集

「編集」をクリックすると、以下の画面が表示されます。

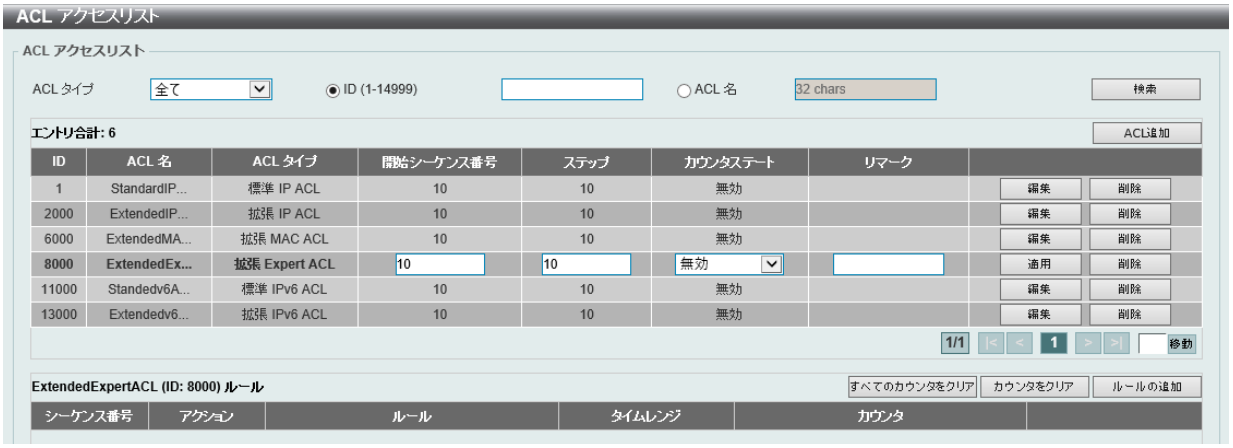


図 11-10　ACL アクセスリスト（編集）画面

画面に表示される項目：

項目	説明
開始シーケンス番号	シーケンス番号の開始番号を指定します。
ステップ	シーケンス番号の増加番号を指定します。
カウンタステート	カウンタ機能の有効 / 無効を指定します。
リマーク	指定プロファイルと関連するリマークを入力します。

「適用」をクリック して、設定を適用します。
「削除」をクリック して、指定エントリを削除します。

■ ACL プロファイルの作成

「ACL 追加」をクリック すると、以下の画面が表示されます。

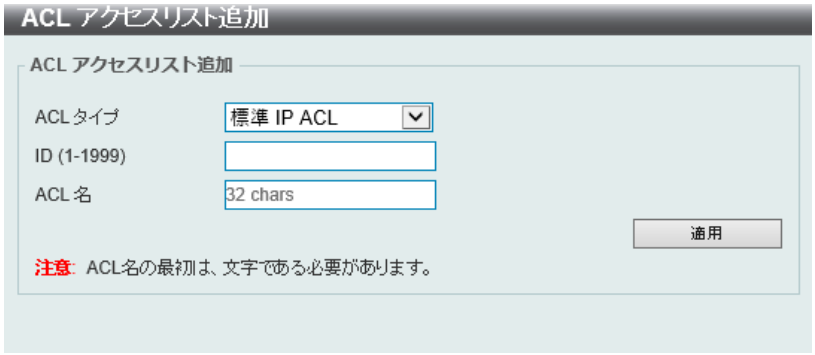


図 11-11　ACL アクセスリスト追加（標準 IP ACL）画面

画面に表示される項目：

項目	説明
ACL タイプ	ACL プロファイルの種類を以下から選択します。 • 「標準 IP ACL」「拡張 IP ACL」「標準 IPv6 ACL」「拡張 IPv6 ACL」「拡張 MAC ACL」「拡張 Expert ACL」
ID	ACL ID を入力します。 • 設定可能範囲： （標準 IP ACL）1-1999 （拡張 IP ACL）2000-3999 （標準 IPv6ACL）11000-12999 （拡張 IPv6 ACL）13000-14999 （拡張 MAC ACL）6000-7999 （拡張 Expert ACL）8000-9999
ACL 名	ACL 名を入力します。（32 文字以内）

「適用」をクリック して、設定を適用します。

標準 IP ACL

ACL ルール追加（標準 IP ACL）

「ACL アクセスリスト」画面で「標準 IP ACL」エントリを選択し、「ルールの追加」をクリックすると、以下の画面が表示されます。

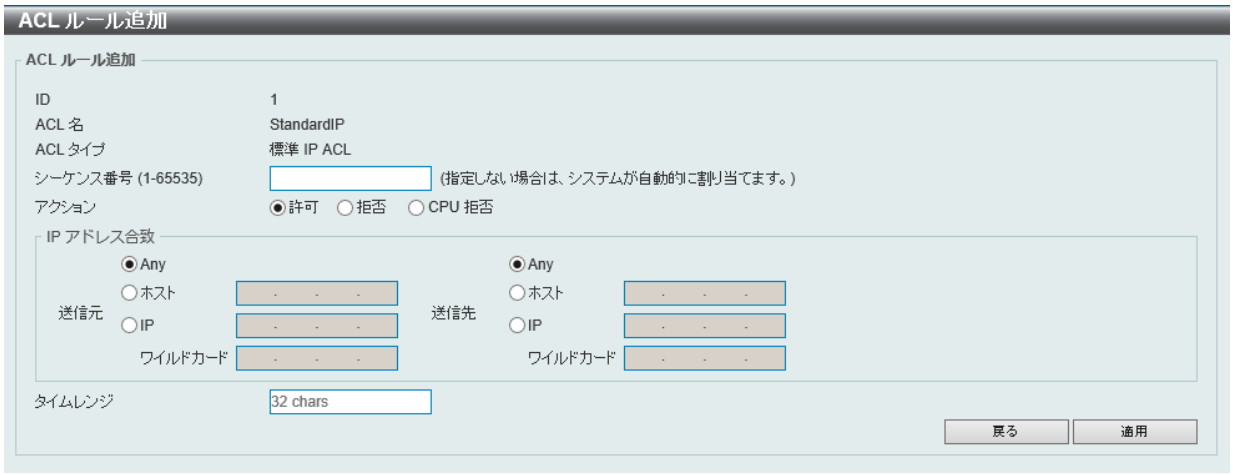


図 11-12　ACL ルール追加（標準 IP ACL）画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」

項目	説明
送信元	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
送信先	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「戻る」をクリック して、変更を破棄し前の画面に戻ります。
「適用」をクリック して、設定を適用します。

拡張 IP ACL

ACL ルール追加（拡張 IP ACL）

「ACL アクセスリスト」画面で「拡張 IP ACL」エントリを選択し、「ルールの追加」をクリックすると、以下の画面が表示されます。



図 11-13　ACL ルール追加（拡張 IP ACL）画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。 「自動割り当て」を指定すると、このルールに対し、シーケンス番号を自動でアサインします。 • 設定可能範囲：1-65535
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」
プロトコルタイプ	プロトコルの種類を選択します。 • 「TCP」「UDP」「ICMP」「EIGRP 」「ESP 」「 GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP 」「プロトコル ID」「なし」 - 「値」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「マスク」-「プロトコル ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（拡張 IP ACL）

項目	説明
送信元	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
送信先	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
IP プレシデンス	IP 優先値を指定します。 • 選択肢:「ルーティン」「プライオリティ」「即時」「フラッシュ」「フラッシュ - オーバライド」「クリティカル」「インターネット」「ネットワーク」 - 「値」: IP 優先値を入力します。(0-7) - 「マスク」: IP 優先値マスクを入力します。(0x0-0x7)
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢 :「ノーマル」「min mmonetary cost」「max reliability」「最大スループット」「最小遅延」 - 「値」: ToS 値を入力します。(0-15) - 「マスク」: ToS マスクを入力します。(0x0-0x7)
DSCP	使用する DSCP 値を選択します。 • 選択肢:「default (0)」「af11 (10)」「af12 (12)」「af13 (14)」「af21 (18)」「af22 (20)」「af23 (22)」「af31 (26)」「af32 (28)」「af33 (30)」「af41 (34)」「af42 (36)」「af43 (38)」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5(40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「値」: DSCP 値を入力します。(0-63) - 「マスク」: DSCP マスクを入力します。(0x0-0x3F)
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。(32 文字以内)

「TCP」「UDP」選択時に表示される項目（拡張 IP ACL）

項目	説明
送信元ポート	送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
送信先ポート	宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（拡張 IP ACL）

項目	説明
TCP フラグ	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢 :「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（拡張 IP ACL）

項目	説明
ICMP メッセージタイプを指定	使用する ICMP メッセージの種類を指定します。
ICMP メッセージタイプ	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
メッセージコード	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

「戻る」をクリック して、変更を破棄し前の画面に戻ります。
「適用」をクリック して、設定を適用します。

標準 IPv6 ACL

ACL ルール追加（標準 IPv6 ACL）

「ACL アクセスリスト」画面で「標準 IPv6 ACL」エントリを選択し、「ルールの追加」をクリックすると、以下の画面が表示されます。

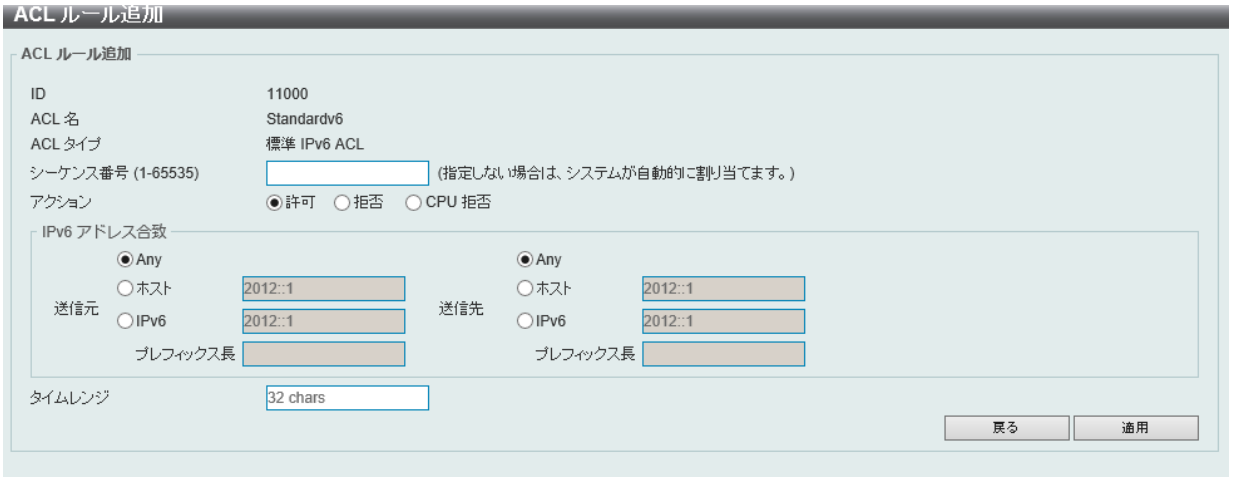


図 11-14　ACL ルール追加（標準 IPv6 ACL）画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」
送信元	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「プレフィックス長」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
送信先	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「プレフィックス長」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「戻る」をクリック して、変更を破棄し前の画面に戻ります。
「適用」をクリック して、設定を適用します。

拡張 IPv6 ACL

ACL ルール追加（拡張 IPv6 ACL）

「ACL アクセスリスト」画面で「拡張 IPv6 ACL」エントリを選択し、「ルールの追加」をクリックすると、以下の画面が表示されます。

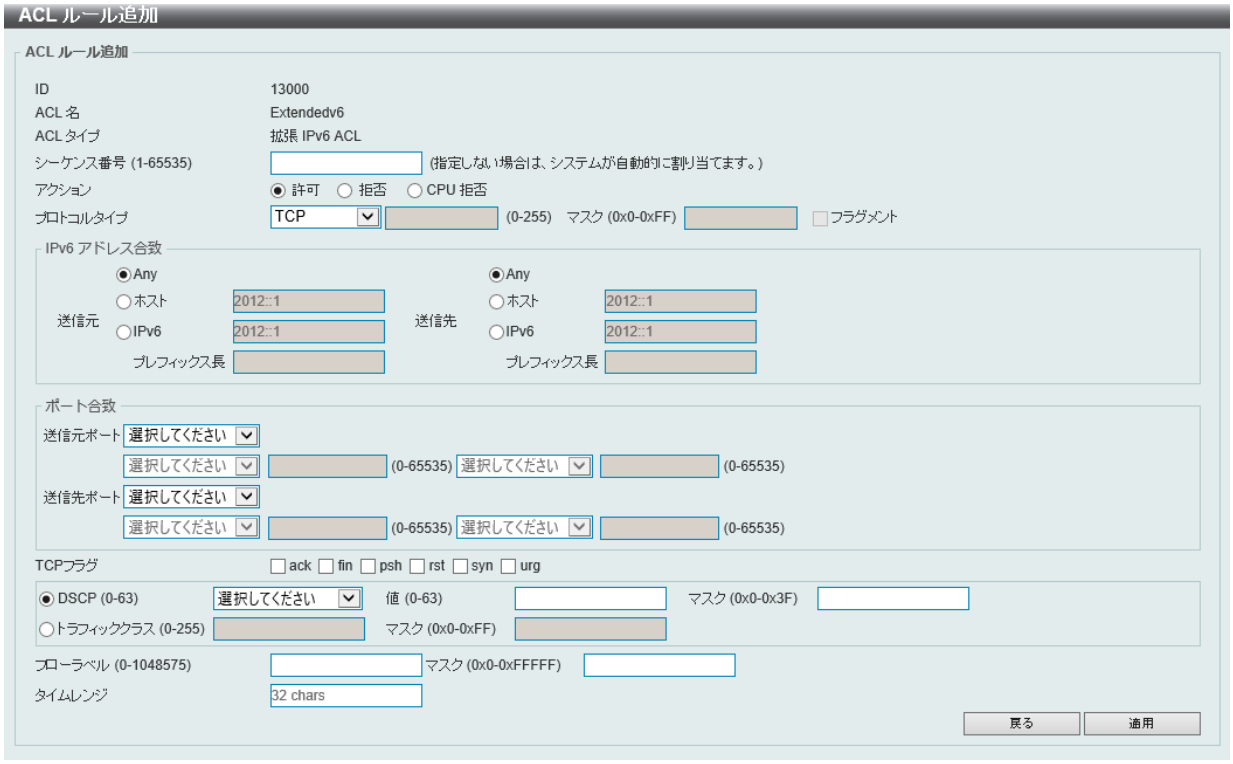


図 11-15　ACL ルール追加（拡張 IPv6 ACL）画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」
プロトコルタイプ	プロトコルの種類を以下から選択します。 • 選択肢：「TCP」「UDP」「ICMP」「ESP」「PCP」「プロトコル ID」「SCTP」「なし」 - 「値」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「マスク」-「プロトコル ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「フラグメント」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコルタイプに表示される項目（拡張 IPv6 ACL）

項目	説明
送信元	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの IPv6 アドレスを入力します。 • 「IPv6」-「プレフィックス長」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
送信先	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの IPv6 アドレスを入力します。 • 「IPv6」-「プレフィックス長」が選択可能になります。送信元 IPv6 アドレスとプレフィックス長を入力します。
DSCP	使用する DSCP 値を選択します。 • 選択肢:「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5(40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「値」：DSCP 値を入力します。（0-63） - 「マスク」：DSCP マスクを入力します。（0x0-0x3F）

項目	説明
トラフィッククラス	トラフィッククラス値を入力します。 • 設定可能範囲：0-255 •「マスク」：トラフィッククラスのマスク値を入力します。（0x0-0xFF）
フローラベル	フローラベルの値を入力します。 • 設定可能範囲：0-1048575 •「マスク」：フローラベルマスクを入力します。（0x0-0xFFFFF）
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「TCP」「UDP」選択時に表示される項目（拡張 IPv6 ACL）

項目	説明
送信元ポート	送信元ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
送信先ポート	宛先ポートの値を指定します。 •「=」- 指定のポート番号が使用されます。 •「>」- 指定ポートよりも大きいポートが使用されます。 •「<」- 指定ポートより小さいポートが使用されます。 •「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 •「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 •「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（拡張 IPv6 ACL）

項目	説明
TCP フラグ	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（拡張 IPv6 ACL）

項目	説明
ICMP メッセージタイプを指定	使用する ICMP メッセージの種類を指定します。
ICMP メッセージタイプ	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
メッセージコード	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

「戻る」をクリック して、変更を破棄し前の画面に戻ります。
「適用」をクリック して、設定を適用します。

拡張 MAC ACL

ACL ルール追加（拡張 MAC ACL）

「ACL アクセスリスト」画面で「拡張 MAC ACL」エントリを選択し、「ルールの追加」をクリックすると、以下の画面が表示されます。



図 11-16　ACL ルール追加（拡張 MAC）画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」
送信元	送信元の MAC アドレスを以下から指定します。 • Any - どの送信元トラフィックでも本ルールに従って評価されます。 • ホスト - ホストの MAC アドレスを入力します。 • MAC -「ワイルドカード」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力できます。
送信先	宛先の MAC アドレスを以下から指定します。 • Any - どの宛先トラフィックでも本ルールに従って評価されます。 • ホスト - 宛先ホストの MAC アドレスを入力します。 • MAC -「ワイルドカード」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力できます。
イーサネットタイプを指定	イーサネットタイプを選択します。 • 選択肢:「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」
イーサネットタイプ	イーサネットタイプの 16 進数値を指定します。 「イーサネットタイプを指定」で指定したイーサネットタイプに基づき適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
イーサネットタイプ マスク	イーサネットタイプマスクの 16 進数値を指定します。 「イーサネットタイプを指定」で指定したイーサネットタイプに基づき適切な値が入力されます。 • 設定可能範囲：0x0-0xFFFF
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 •「マスク」：CoS マスクを入力します。（0x0-0x7）
内部 CoS	CoS 値を指定後、内部（Inner）CoS の値を入力します。 • 設定可能範囲：0-7 •「マスク」：Inner CoS マスクを入力します。（0x0-0x7）
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 •「マスク」：VLAN ID マスクを入力します。（0x0-0xFFF）

項目	説明
内部 VID	ACL ルールに紐づける内部（Inner）VLAN ID を入力します。 • 設定可能範囲：1-4094 •「マスク」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN レンジ	ACL ルールに紐づける VLAN 範囲を指定します。VLAN 範囲の開始 / 終了 VLAN を入力します。 • 設定可能範囲：1-4094
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「戻る」をクリック して、変更を破棄し前の画面に戻ります。
「適用」をクリック して、設定を適用します。

拡張 Expert ACL

ACL ルール追加（拡張 Expert ACL）

「ACL アクセスリスト」画面で「拡張 Expert ACL」エントリを選択し、「ルールの追加」をクリックすると、以下の画面が表示されます。

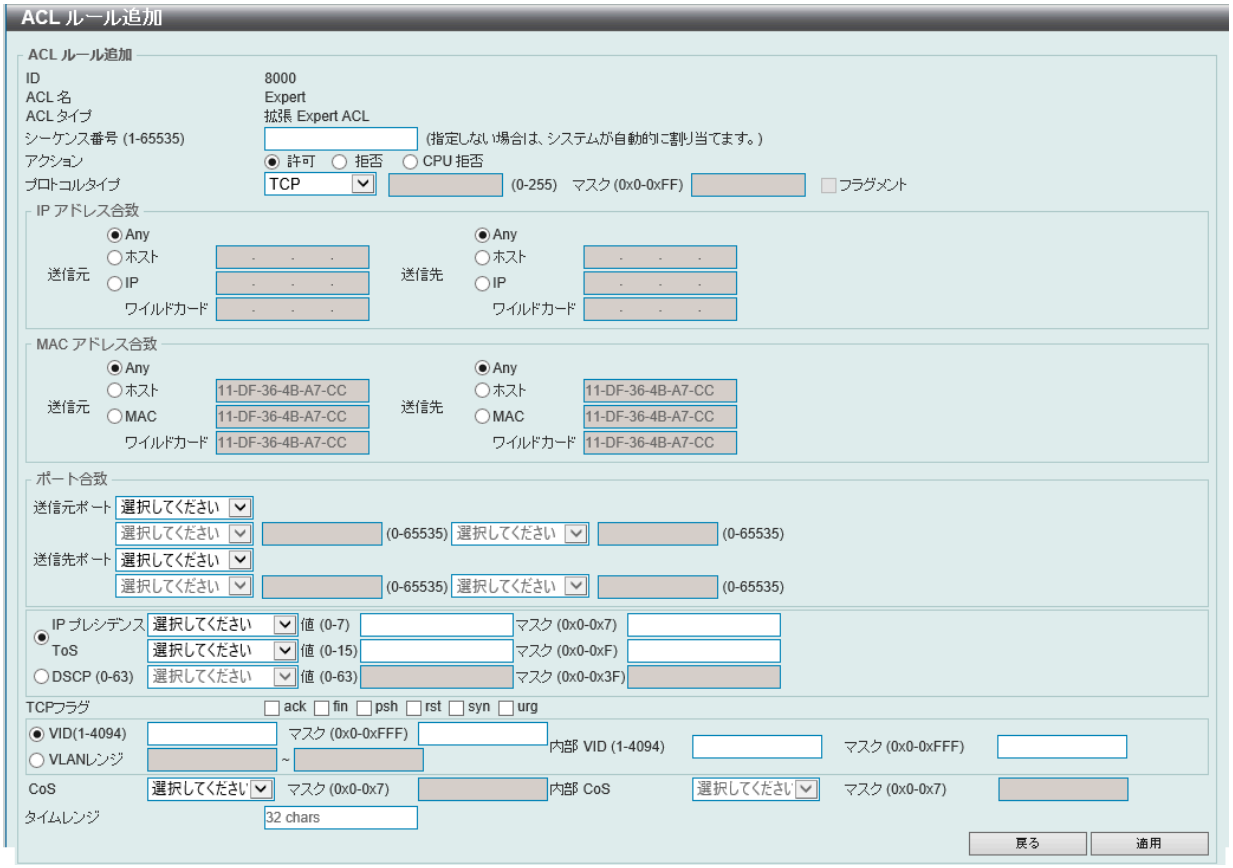


図 11-17　ACL ルール追加（拡張 Expert ACL）画面

画面に表示される項目：

項目	説明
シーケンス番号	シーケンス番号を指定します。値を指定しない場合、自動的に番号が割り振られます。 • 設定可能範囲：1-65535
アクション	本ルールで実行するアクションを選択します。 • 選択肢：「許可」「拒否」「CPU 拒否」
プロトコルタイプ	プロトコルの種類を選択します。 • 選択肢：「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「プロトコル ID」「なし」 - 「値」- 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。 - 「マスク」-「プロトコル ID」選択後、プロトコルマスク（0x0-0xFF）を入力します。 - 「フラグメント」- パケットフラグメントフィルタを含む場合に指定します。

選択したプロトコルにより表示される項目が異なります。以下の表示項目を参照してください。

すべてのプロトコル選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
IP アドレス合致	
送信元	送信元のアドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して送信元 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
送信先	宛先のアドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの IP アドレスを入力します。 • 「IP」-「ワイルドカード」オプションが選択可能になります。ワイルドカードを使用して宛先 IP アドレスグループを入力します。ビットは 1 の値が無視され、0 が認識されます。
MAC アドレス合致	
送信元	送信元の MAC アドレスを指定します。 • 「Any」- 全ての送信元トラフィックは本ルールに従って評価されます。 • 「ホスト」- 送信元ホストの MAC アドレスを入力します。 • 「MAC」-「ワイルドカード」オプションが選択可能になり、送信元 MAC アドレスとワイルドカードを入力できます。
送信先	宛先の MAC アドレスを指定します。 • 「Any」- 全ての宛先トラフィックは本ルールに従って評価されます。 • 「ホスト」- 宛先ホストの MAC アドレスを入力します。 • 「MAC」-「ワイルドカード」オプションが選択可能になり、宛先 MAC アドレスとワイルドカードを入力できます。
IPv4 DSCP	
IP プレシデンス	IP 優先値を指定します。 • 選択肢：「ルーティン」「プライオリティ」「即時」「フラッシュ」「フラッシュ - オーバライド」「クリティカル」「インターネット」「ネットワーク」 - 「値」：IP 優先値を入力します。（0-7） - 「マスク」：IP 優先値マスクを入力します。（0x0-0x7）
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。 • 選択肢：「ノーマル」「min mmonetary cost」「max reliability」「最大スループット」「最小遅延」 - 「値」：ToS 値を入力します。（0-15） - 「マスク」：ToS マスクを入力します。（0x0-0x7）
DSCP	使用する DSCP 値を選択します。 • 選択肢:「default（0）」「af11（10）」「af12（12）」「af13（14）」「af21（18）」「af22（20）」「af23（22）」「af31（26）」「af32（28）」「af33（30）」「af41（34）」「af42（36）」「af43（38）」「cs1 (8)」「cs2 (16)」「cs3 (24)」「cs4 (32)」「cs5(40)」「cs6 (48)」「cs7 (56)」「ef (46)」 - 「値」：DSCP 値を入力します。（0-63） - 「マスク」：DSCP マスクを入力します。（0x0-0x3F）
802.1Q VLAN	
VID	ACL ルールに紐づける VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「マスク」：VLAN ID マスクを入力します。（0x0-0xFFF）
内部 VID	ACL ルールに紐づける内部（Inner）VLAN ID を入力します。 • 設定可能範囲：1-4094 • 「マスク」：Inner VLAN ID マスクを入力します。（0x0-0xFFF）
VLAN レンジ	ACL ルールに紐づける VLAN 範囲を指定します。VLAN 範囲の開始 / 終了 VLAN を入力します。 • 設定可能範囲：1-4094
CoS	CoS の値を入力します。 • 設定可能範囲：0-7 • 「マスク」：CoS マスクを入力します。（0x0-0x7）
内部 CoS	CoS 値を指定後、内部（Inner）CoS の値を入力します。 • 設定可能範囲：0-7 • 「マスク」：Inner CoS マスクを入力します。（0x0-0x7）
スケジュール設定	
タイムレンジ	ACL ルールに適用するタイムレンジ名を指定します。（32 文字以内）

「TCP」「UDP」選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
送信元ポート	送信元ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。
送信先ポート	宛先ポートの値を指定します。 • 「=」- 指定のポート番号が使用されます。 • 「>」- 指定ポートよりも大きいポートが使用されます。 • 「<」- 指定ポートより小さいポートが使用されます。 • 「≠」- 指定ポートは除外され、それ以外のポートが使用されます。 • 「範囲」- 指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。 • 「マスク」- 指定ポートとマスクが使用されます。0x0 から 0xFFFF の範囲でポートマスクを指定します。

「TCP」選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
TCP フラグ	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。 • 選択肢：「ack」「fin」「psh」「rst」「syn」「urg」

「ICMP」選択時に表示される項目（拡張 Expert ACL ルール）

項目	説明
ICMP メッセージタイプを指定	使用する ICMP メッセージの種類を指定します。
ICMP メッセージタイプ	ICMP メッセージの種類を指定しない場合、手動で ICMP メッセージ種類の数値を指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255
メッセージコード	ICMP メッセージの種類を指定しない場合、手動でメッセージコードを指定します。 ICMP メッセージの種類が指定されている場合、自動で数値が入力されます。 • 設定可能範囲：0-255

「戻る」をクリック して、変更を破棄し前の画面に戻ります。
「適用」をクリック して、設定を適用します。

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の設定、表示を行います。

ACL > ACL インタフェースアクセスグループの順にメニューをクリックし、以下の画面を表示します。



図 11-18　ACL インタフェースアクセスグループ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
方向	方向を指定します。 • 選択肢：「In」「Out」
アクション	ACL インタフェースアクセスグループを追加 / 削除します。 • 選択肢：「追加」「削除」
タイプ	ACL の種類を選択します。 • 「IP ACL」「IPv6 ACL」「MAC ACL」「エキスパート ACL」
ACL 名	アクセスコントロールリスト名を入力します。 「選択してください」をクリックし、既存の ACL プロファイルを指定することも可能です。

「適用」をクリック して、設定を適用します。

「選択してください」をクリック すると次の画面が表示されます。



図 11-19　ACL アクセスリスト画面

設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
設定するエントリを選択し「OK」をクリックします。

ACL VLAN アクセスマップ

ACL VLAN アクセスマップの設定、表示を行います。

ACL > ACL VLAN アクセスマップの順にメニューをクリックし、以下の画面を表示します。



図 11-20　ACL VLAN アクセスマップ画面

画面に表示される項目：

項目	説明
アクセスマップ名	アクセスマップ名を入力します。(32 文字以内)
サブマップ番号	サイトマップ番号を入力します。 • 設定可能範囲：1-65535
アクション	実行するアクションを選択します。 • 選択肢：「転送」「破棄」「リダイレクト」 「リダイレクト」を選択した場合、ドロップダウンリストからリダイレクトされるインタフェースを選択できます。
カウンタステート	カウンタの有効 / 無効を指定します。

「適用」をクリック して、設定を適用します。
「すべてのカウンタをクリア」をクリック し、表示されたすべてのカウンタ情報を消去します。
「カウンタをクリア」をクリック し、表示された指定ルールのカウンタ情報を消去します。
「検索」をクリック し、入力した情報を基に特定のエントリを指定します。
「バインディング」をクリック し、新しく合致したアクセスリストを指定します。
「削除」をクリック し、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「移動」をクリック して、特定のページへ移動します。

アクセスリスト合致

「バインディング」をクリック すると以下の画面が表示されます。



図 11-21　アクセスリスト合致画面

画面に表示される項目：

項目	説明
IP アクセスリスト合致	照合する IP アクセスリストを指定します。 「選択してください」をクリックし、既存の ACL プロファイルを指定します。
IPv6 アクセスリスト合致	照合する IPv6 アクセスリストを指定します。 「選択してください」をクリックし、既存の ACL プロファイルを指定します。
MAC アクセスリスト合致	照合する MAC アクセスリストを指定します。 「選択してください」をクリックし、既存の ACL プロファイルを指定します。

「適用」をクリック して、設定を適用します。
「削除」をクリック し、指定エントリを削除します。

ACL 選択画面
「選択してください」をクリック すると次の画面が表示されます。

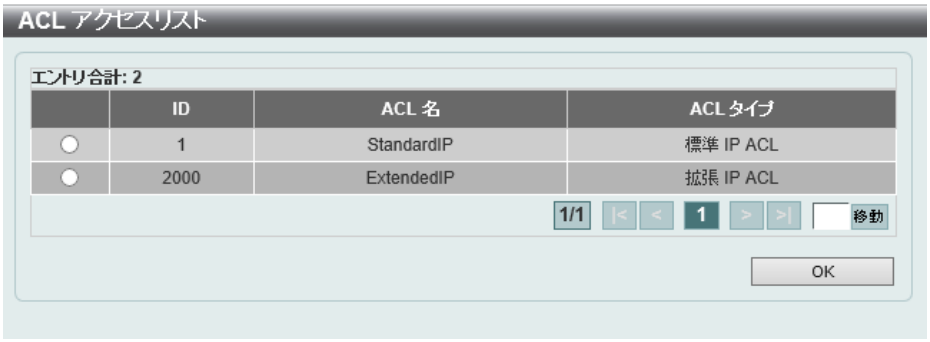


図 11-22　ACL アクセスリスト 画面

設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
設定するエントリを選択し「OK」をクリックします。

ACL VLAN フィルタ

ACL VLAN フィルタの設定、表示を行います。

ACL > ACL VLAN フィルタの順にメニューをクリックし、以下の画面を表示します。



図 11-23　ACL VLAN フィルタ画面

画面に表示される項目：

項目	説明
アクセスマップ 名	アクセスマップ名を入力します。(32 文字以内)
アクション	ACL VLAN フィルタの追加 / 削除をします。 • 選択肢：「追加」「削除」
VID リスト	使用する VLAN ID リストを入力します。 「すべての VLAN」オプションにチェックを入れると、すべての VLAN に本設定を適用します。

「適用」をクリック して、設定を適用します。
「削除」をクリック し、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリック して、特定のページへ移動します。

CPU ACL

CPU ACL 機能の設定を行います。

ACL > CPU ACL の順にメニューをクリックし、以下の画面を表示します。



図 11-24　CPU ACL 画面

画面に表示される項目：

項目	説明
フィルタマップ名	CPU ACL フィルタマップ名を指定します。(32 文字以内)

「適用」をクリックし、設定内容を適用します。
「バインディング」をクリック し、新しく合致したアクセスリストを指定します。
「削除」をクリック し、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリック して、特定のページへ移動します。

「バインディング」をクリック すると以下の画面が表示されます。



図 11-25　アクセスリスト合致画面

画面に表示される項目：

項目	説明
IP アクセスリストに合致	
シーケンス番号	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL 名	マッチする「標準」または「拡張」IP アクセスリスト名を指定します。（32 文字以内） 「選択してください」をクリックし、既存の ACL から選択することも可能です。
IPv6 アクセスリストに合致	
シーケンス番号	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL 名	マッチする「標準」または「拡張」IPv6 アクセスリスト名を指定します。（32 文字以内） 「選択してください」をクリックし、既存の ACL から選択することも可能です。
MAC アクセスリストに合致	
シーケンス番号	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL 名	マッチする「拡張」MAC アクセスリスト名を指定します。（32 文字以内） 「選択してください」をクリックし、既存の ACL から選択することも可能です。
エキスパートアクセスリストに合致	
シーケンス番号	シーケンス番号を指定します。値が小さいほどアクセスリストの優先度が高くなります。 • 設定可能範囲：1-65535
ACL 名	マッチする「拡張」エキスパートアクセスリスト名を指定します。（32 文字以内） 「選択してください」をクリックし、既存の ACL から選択することも可能です。
Ingress インタフェースに合致	
ユニット	設定を行うユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「適用」をクリック して、設定を適用します。
「削除」をクリック し、指定エントリを削除します。

ACL 選択画面

「選択してください」をクリック すると次の画面が表示されます。

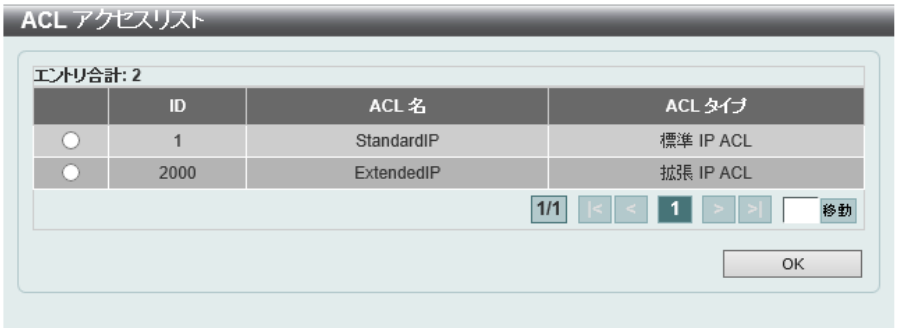


図 11-26　ACL アクセスリスト 画面

設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。
設定するエントリを選択し「OK」をクリックします。

第 12 章　セキュリティ

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

以下はセキュリティサブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
ポートセキュリティ	ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。
802.1X	IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。
AAA	AAA（Authentication、Authorization、Accounting）の設定を行います。
RADIUS	RADIUS の設定を行います。
TACACS+	TACACS+ の設定を行います。
IMPB	IP-MAC バインディングにより、スイッチにアクセスするユーザ数を制限します。
DHCP サーバスクリーニング	DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。
ARP スプーフィング防止	ARP スプーフィング防止機能は、設定したゲートウェイ IP アドレスとマッチしなかった IP アドレスの ARP パケットをバイパスします。
BPDU アタック防止	スイッチのポートに BPDU 防止機能を設定します。
NetBIOS フィルタリング	NetBIOS フィルタリングの設定を行います。
MAC 認証	MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
Web アクセスコントロール	Web ベース認証はスイッチを経由でインターネットにアクセスする場合、ユーザを認証する機能です。
ネットワークアクセス認証	ネットワークアクセス認証（ネットワークアクセス認証）の設定を行います。
セーフガードエンジン	セーフガードエンジンは、攻撃中にスイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。
トラスト ホスト	トラストホストの設定を行います。
トラフィック セグメンテーション	トラフィックセグメンテーション機能はポート間のトラフィックの流れを制限を行います。
ストーム制御設定	ストームコントロールの設定を行います。
DoS 攻撃防御設定	各 DoS 攻撃に対して防御設定を行います。
ゾーンディフェンス設定	ゾーンディフェンス（Zone Defense）機能の設定と表示を行います。
SSH	SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。
SSL	Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。
SFTP サーバ設定	Secure File Transfer プロトコル (SFTP) サーバの設定、表示を行います。
ネットワークプロトコルポートプロテクション設定	ネットワークプロトコルポートプロテクションの設定、表示を行います。

ポートセキュリティ

ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

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は、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

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の順にメニューをクリックし、以下の画面を表示します。



図 12-1　ポートセキュリティグローバル設定画面

画面に表示される項目：

項目	説明
トラップステート	ポートセキュリティのトラップを有効 / 無効に設定します。
トラップレート	1 秒あたりのトラップ数を指定します。 初期値の 31 では、すべてのセキュリティ違反に対して SNMP トラップが生成されます。 • 設定可能範囲：0-1000 • 初期値：31
システム最大アドレス	許可される最大 MAC アドレス数を入力します。初期値では制限なしになります。 「無制限」オプションにチェックを入れると、セキュアな MAC アドレスの最大数が適用されます。 • 設定可能範囲：1-3328

「適用」をクリックして、設定内容を適用します。

ポートセキュリティポート設定

ポートセキュリティのポート設定と設定内容の表示を行います。

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の順にメニューをクリックし、以下の画面を表示します。



図 12-2　ポートセキュリティポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートのポートセキュリティ機能を有効 / 無効に設定します。
最大	指定ポートで許可されるセキュアな MAC アドレスの最大数を指定します。 • 設定可能範囲：0-3328 • 初期値：32
違反動作	違反に対して実行するアクションを指定します。 •「プロテクト」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反としてはカウントされません。 •「制限」- ポートセキュリティのプロセスで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントして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ある場合にポートをシャットダウンし、システムログに記録します。
セキュリティモード	セキュリティモードを選択します。 •「パーマネント」- すべての学習した MAC アドレスは、手動でエントリを削除しない限り削除されません。 •「タイムアウト時に削除」- エントリが期限切れになったとき、またはユーザがこれらのエントリを手動で削除したときに、学習したすべての MAC アドレスが削除されます。
エージングタイム	指定ポートで自動学習された安全なアドレスに使用するエージングタイムを入力します。 • 設定可能範囲：0-1440（分）
エージングタイプ	エージングの種類を以下から指定します。 •「アブソルート」- ポート上のすべてのアドレスは指定された時間を過ぎるとアドレスリストから削除されます。（初期値） •「インアクティビティ」- ポート上のアドレスは、指定の期間そのアドレスからのトラフィックがない場合にエージアウトします。

「適用」をクリックして、設定内容を適用します。

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の設定、表示を行います。

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の順にメニューをクリックし、以下の画面を表示します。



図 12-3　ポートセキュリティアドレスエントリ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
MAC アドレス	MAC アドレスを入力します。 「パーマネント」を選択すると、ユーザが手動でこれらのエントリを削除しない限り、学習したすべての MAC アドレスが削除されないように指定することができます。
VID	VLAN ID を指定します。 • 設定可能範囲：1- 4094

「追加」をクリックして、入力した情報に基づく新しいエントリを追加します。
「削除」をクリックし、入力した情報に基づく新しいエントリを削除します。
「ポート毎にクリア」をクリックし、選択したポートに基づく情報を消去します。
「MAC 毎にクリア」をクリックし、選択した MAC アドレスに基づく情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

802.1X

802.1X（ポートベースおよびホストベースのアクセスコントロール）

IEEE 802.1X は、ユーザ認証を行うセキュリティの規格です。

クライアント / サーバベースのアクセスコントロールモデルを使用し、特定のローカルエリアネットワーク上の有線 / 無線デバイスへのアクセスを許可および認証するために使用します。この認証方法は、ネットワークへアクセスするユーザの認証に RADIUS サーバを使用し、EAPOL（Extensible Authentication Protocol over LAN）と呼ばれるパケットをクライアント / サーバ間でリレーして実現します。

以下の図は、基本的な EAPOL パケットの構成です。

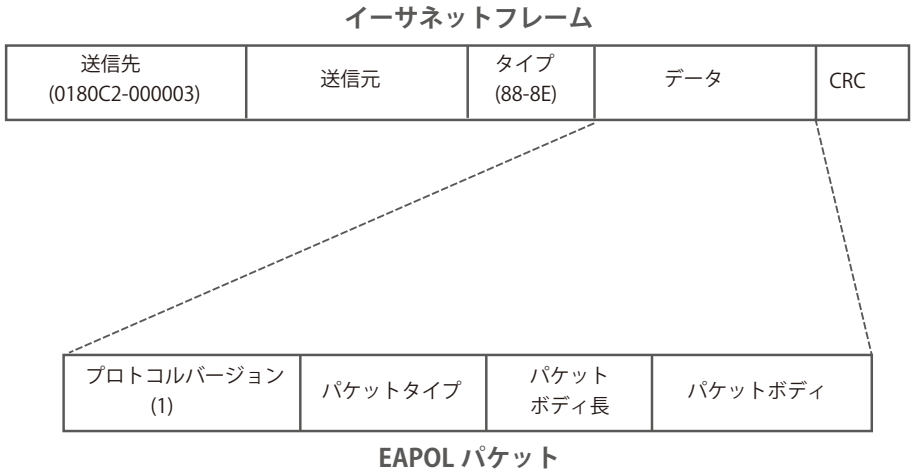


図 12-4　EAPOL パケット

IEEE 802.1X を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。
EAPOL パケットは、承認完了前でも指定ポート経由で送受信できる唯一のトラフィックです。

802.1X アクセスコントロールには認証サーバ、オーセンティケータ、クライアントの 3 つの役割があります。
それぞれがアクセスコントロールセキュリティの作成、状態の維持、動作のために重要です。

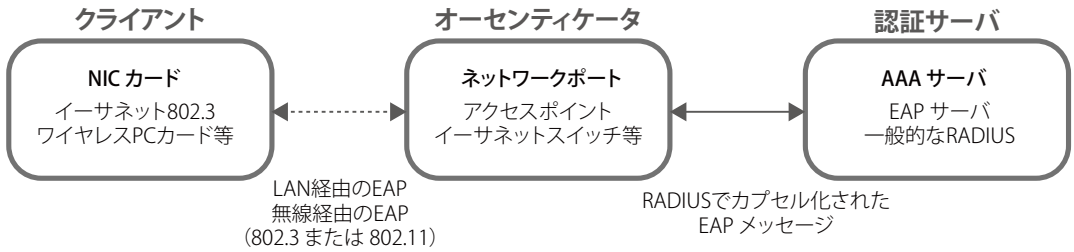


図 12-5　802.1X の 3 つの役割

以降の項目では、認証サーバ、オーセンティケータ、クライアントのそれぞれの役割について説明します。

認証サーバ

認証サーバは、クライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。

認証サーバ上で RADIUS サーバプログラムが実行され、認証サーバのデータがオーセンティケータ（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを使用する前に、認証サーバ（RADIUS）によって認証される必要があります。

認証サーバの役割は、ネットワークにアクセスするクライアントの身元を証明することです。認証サーバ（RADIUS）とクライアントの間で EAPOL パケットによるセキュアな情報交換を行い、クライアントが「LAN やスイッチのサービスに対するアクセス許可があるか」をスイッチに通知します。

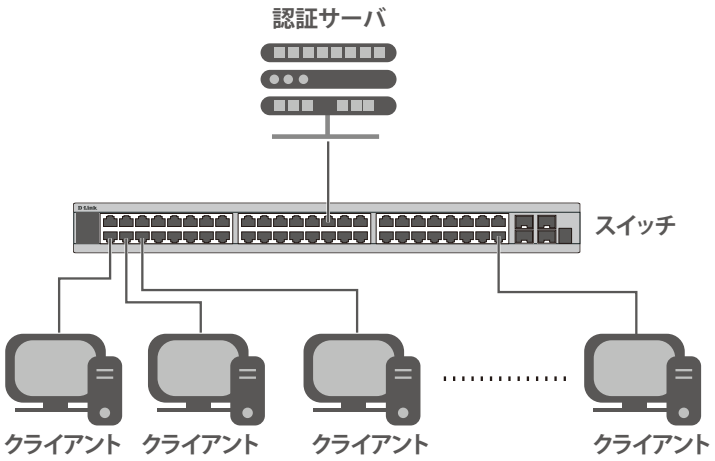


図 12-6　認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を仲介します。

802.1X を使用する場合、オーセンティケータには 2 つの役割があります。

- 1 つ目の役割：
  クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。
  EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。
- 2 つ目の役割：
  クライアントから収集した情報を認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして設定するには、以下の手順を実行します。

1. スイッチの 802.1X 機能を有効にします。（**セキュリティ > 802.1X > 802.1X グローバル設定**）
2. 対象ポートに 802.1X の設定を行います。（**セキュリティ > 802.1X > 802.1X ポート設定**）
3. スイッチに RADIUS サーバの設定を行います。（**セキュリティ > RADIUS > RADIUS サーバ設定**）

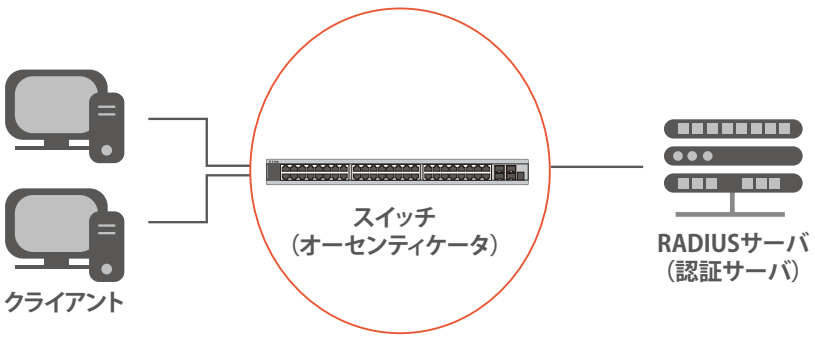


図 12-7　オーセンティケータ

クライアント

クライアントとは、LAN やスイッチが提供するサービスへアクセスしようとする端末です。

クライアントとなる端末では、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。一部の Windows OS のように、OS 内に既にそのソフトウェアが組み込まれている場合がありますが、それ以外の OS をお使いの場合は、802.1X クライアントソフトウェアを別途用意する必要があります。

クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、スイッチからの要求に応答します。

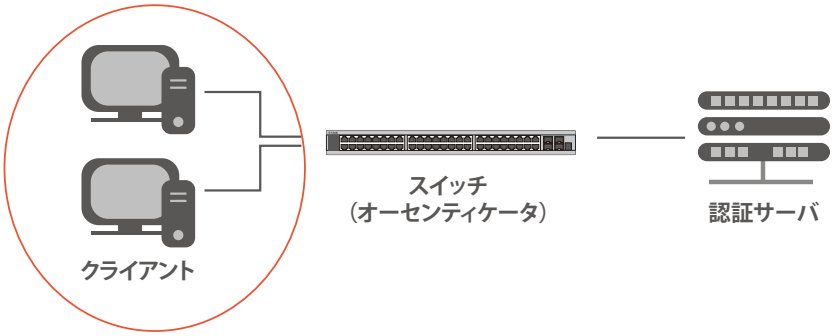


図 12-8　クライアント

認証プロセスについて

前述の「認証サーバ」「オーセンティケータ」「クライアント」により、802.1X プロトコルはネットワークへアクセスするユーザの認証を安定的かつ安全に行います。

認証完了前には EAPOL トラフィックのみが特定のポートの通過を許可されます。このポートは、有効なユーザ名とパスワード（802.1X の設定によっては MAC アドレスも）を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。

本製品の 802.1X では、以下の 2 種類のアクセスコントロールが選択できます。

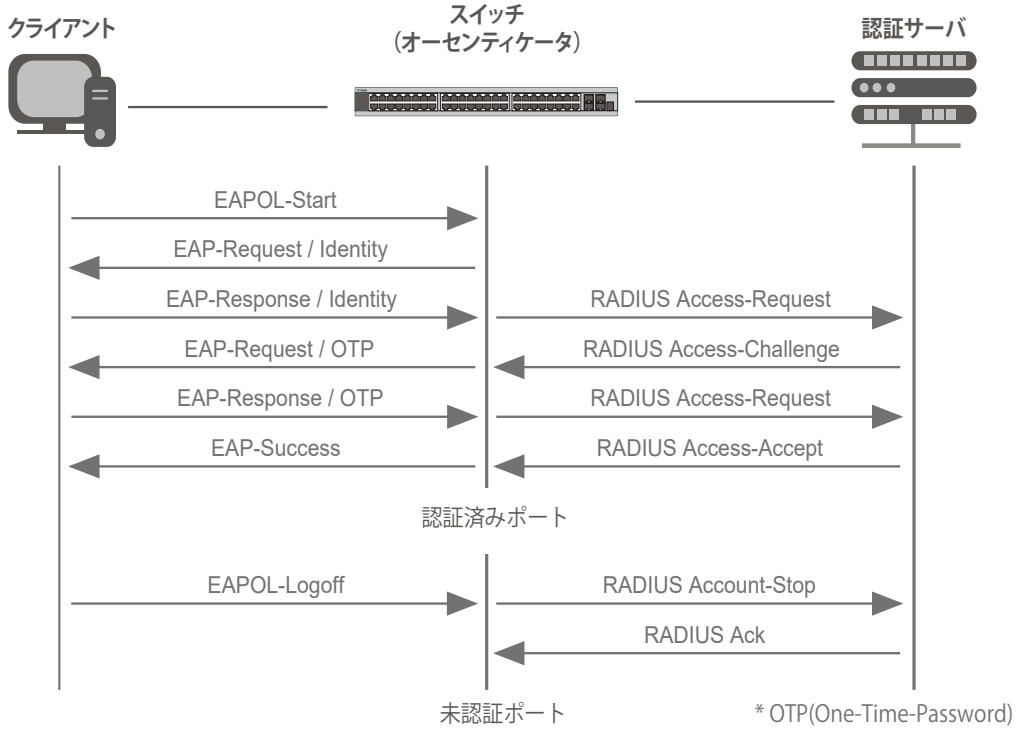


図 12-9　802.1X 認証プロセス

本製品の 802.1X 機能では、以下の 2 つのタイプのアクセスコントロールから選択することができます。

1. **ポートベースのアクセスコントロール**
   本方式では、リモート RADIUS サーバが、ポートごとに 1 人のユーザのみを認証することで、同じポート上の残りのユーザがネットワークにアクセスできるようにします。
2. **ホストベースのアクセスコントロール**
   本方式では、スイッチはデバイスあたり最大 3328 件までの MAC アドレスを自動的に学習してリストに追加します。
   スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に MAC アドレスごと（ユーザごと）の認証を行います。

802.X ポートベース / ホストベースのネットワークアクセスコントロールについて

802.1X は、元々は LAN 上で Point to Point プロトコルの特長を活用するために開発されました。

単一の LAN セグメントが 2 台より多くのデバイスを持たない場合、デバイスのどちらかがブリッジポートとなります。
ブリッジポートは、「リンクのリモートエンドにアクティブなデバイスが接続された」「アクティブなデバイスが非アクティブ状態になった」などのイベントを検知します。これらのイベントをポートの認証状態の制御に利用し、ポートの許可がされていない接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

■ ポートベースネットワークアクセスコントロール

接続デバイスが認証に成功すると、ポートは「Authorized」（認証済み）の状態になります。ポートが未認証になるようなイベントが発生するまで、ポート上のすべてのトラフィックはアクセスコントロール制限の対象になりません。

そのため、ポートが複数のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対してアクセスを許可することになります。このような場合、ポートベースネットワークアクセスコントロールは脆弱であるといえます。

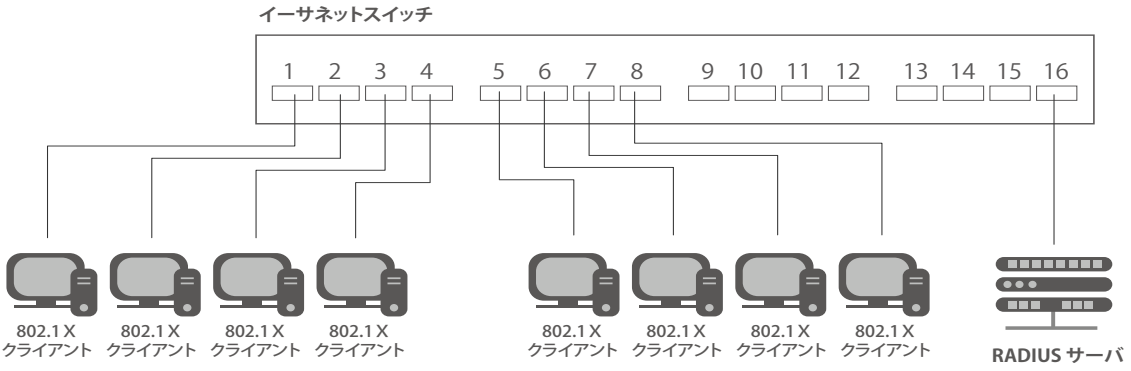


図 12-10　ポートベースアクセスコントロールのネットワーク構成例

■ ホストベースネットワークアクセスコントロール

共有 LAN セグメント内で 802.1X を活用するには、LAN へのアクセスを希望する各デバイスに論理ポートを定義する必要があります。

スイッチは、共有 LAN セグメントに接続する 1 つの物理ポートを異なる論理ポートの集まりであると認識し、それら論理ポートを EAPOL パケット交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための論理ポートを確立します。

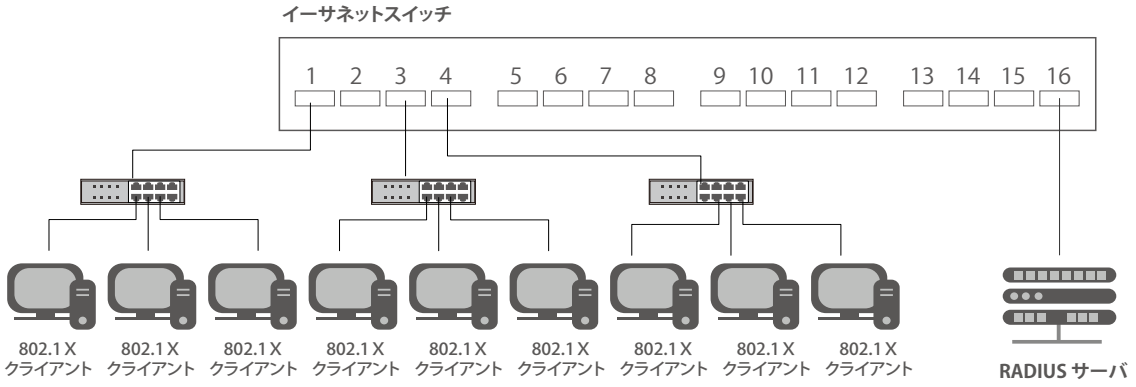


図 12-11　ホストベースアクセスコントロールのネットワーク構成例

802.1X グローバル設定

本画面では 802.1X グローバル設定を行います。

セキュリティ > 802.1X > 802.1X グローバル設定の順にメニューをクリックし、以下の画面を表示します。

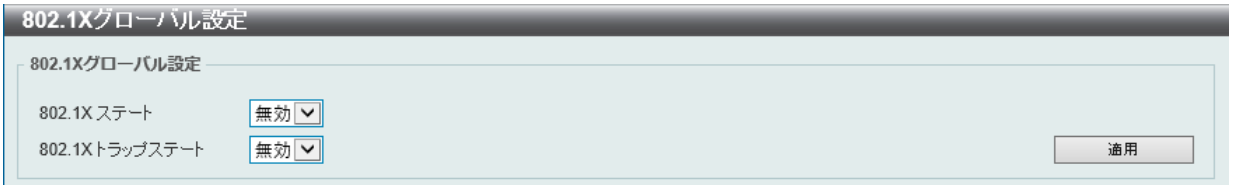


図 12-12　802.1X グローバル設定画面

画面に表示される項目：

項目	説明
802.1X ステート	802.1X 認証を有効 / 無効に設定します。
802.1X トラップステート	802.1X トラップを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

802.1X ポート設定

802.1X 認証ポートを設定します。

セキュリティ > 802.1X > 802.1X ポート設定の順にメニューをクリックし、以下の画面を表示します。

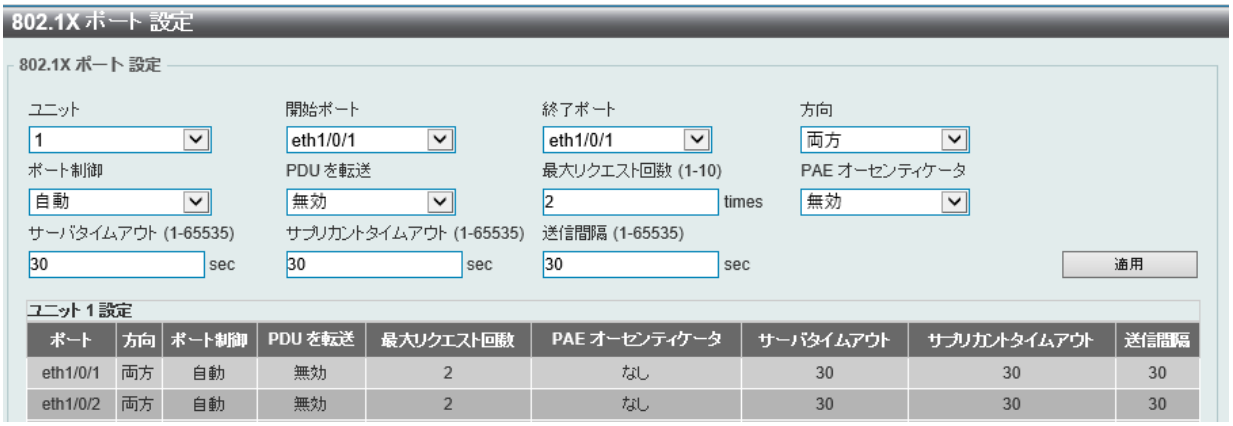


図 12-13　802.1X ポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを表示します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
方向	制御するトラフィックの方向を指定します。 • 「In」- 指定したポートへの入力トラフィックのみ制御対象となります。 • 「両方」- ポートが受信送信する両方向のトラフィッがク制御対象となります。
ポート抑制	ポートの認証状態を指定します。 • 「強制許可」- 両方向の通信でポートは制御されません。 • 「強制未認証」- 制御対象の方向のポートへのアクセスはブロックされます。 • 「自動」- 制御対象の方向のポートへのアクセスには、認証が必要になります。
PDU を転送	PDU 転送機能を有効 / 無効に設定します。
最大リクエスト回数	バックエンドの認証ステートマシンがクライアントに対して Extensible Authentication Protocol（EAP）リクエストフレームを再送する最大回数を指定します。本指定回数後、認証プロセスが再開されます。 • 設定可能範囲：1-10 • 初期値：2
PAE オーセンティケータ	PAE オーセンティケータを有効 / 無効に指定します。 本設定により、特定ポートを IEEE 802.1X Port Access Entity（PAE）オーセンティケータとして指定します。
サーバタイムアウト	サーバのタイムアウト時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
サプリカントタイムアウト	サプリカント（クライアント）のタイムアウト状態となる時間を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）
送信間隔	送信間隔を指定します。 • 設定可能範囲：1-65535（秒） • 初期値：30（秒）

「適用」をクリックして、設定内容を適用します。

注意　定期的に EAP Request/Identity を送信する機能はありません。

認証セッション情報

認証セッションの情報を表示します。

セキュリティ > 802.1X > 認証セッション情報の順にメニューをクリックし、以下の画面を表示します。

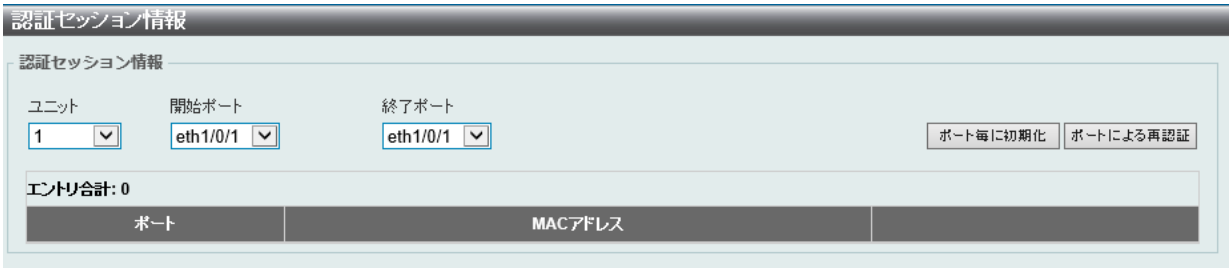


図 12-14　認証セッション情報画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを表示します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「ポート毎に初期化」をクリックして、入力した情報に基づくセッション情報を起動します。
「ポートによる再認証」をクリックして、入力した情報に基づく再認証を行います。
「MAC 毎に初期化」をクリックして、MAC アドレスに基づくセッション情報を起動します。
「MAC による再認証」をクリックして、MAC アドレスに基づく再認証を行います。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

オーセンティケータ統計

オーセンティケータの統計情報を表示します。

セキュリティ > 802.1X > オーセンティケータ統計の順にメニューをクリックし、以下の画面を表示します。



図 12-15　オーセンティケータ統計画面

画面に表示される項目：

項目	説明
ユニット	統計情報を表示 / クリアするユニットを選択します。
ポート	統計情報を表示 / クリアするポート範囲を指定します。

「検索」をクリックし、入力した情報に基づくエントリを検出します。
「カウンタをクリア」をクリックし、選択に基づく情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

オーセンティケータセッション統計

オーセンティケータセッションの統計情報を表示します。

セキュリティ > 802.1X > オーセンティケータセッション統計の順にメニューをクリックし、以下の画面を表示します。

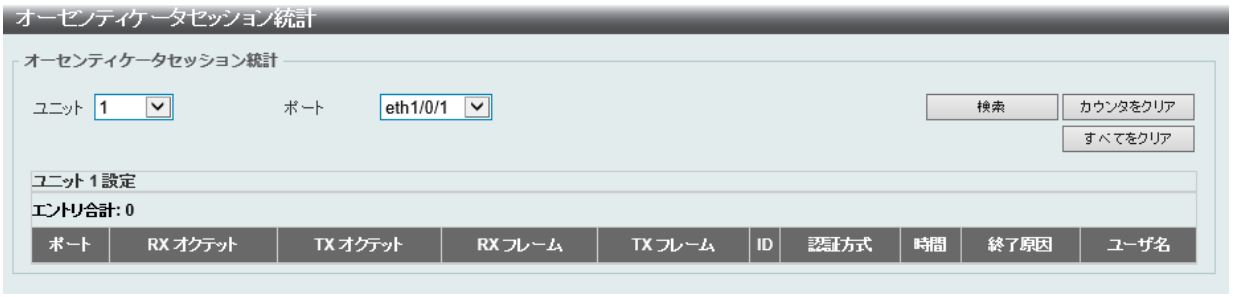


図 12-16　オーセンティケータセッション統計画面

画面に表示される項目：

項目	説明
ユニット	統計情報を表示 / クリアするユニットを指定します。
ポート	統計情報を表示 / クリアするポートの範囲を指定します。

「検索」をクリックし、入力した情報に基づくエントリを検出します。
「カウンタをクリア」をクリックし、選択に基づく情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。

オーセンティケータ診断

オーセンティケータ診断情報を表示します。

セキュリティ > 802.1X > オーセンティケータ診断の順にメニューをクリックし、以下の画面を表示します。



図 12-17　オーセンティケータ診断画面

画面に表示される項目：

項目	説明
ユニット	診断情報を表示 / クリアするユニットを指定します。
ポート	診断情報を表示 / クリアするポートの範囲を指定します。

「検索」をクリックし、入力した情報に基づくエントリを検出します。
「カウンタをクリア」をクリックし、選択に基づく情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

AAA

セキュリティ > AAA
本項目では AAA（Authentication、Authorization、Accounting）の有効 / 無効を行います。

AAA グローバル設定

本項目では AAA をグローバルに有効 / 無効に設定します。

セキュリティ > AAA > AAA グローバル設定の順にメニューをクリックし、以下の画面を表示します。

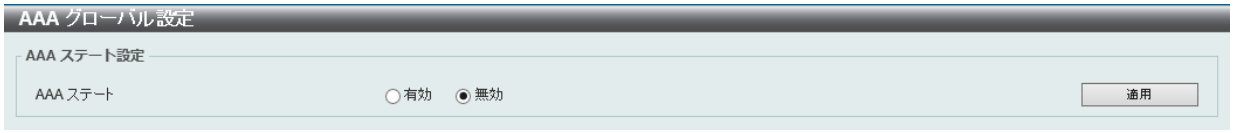


図 12-18　AAA グローバル設定画面

画面に表示される項目：

項目	説明
AAA ステート	AAA のグローバルステータスを有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

アプリケーション認証設定

ログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、HTTP）を設定します。

セキュリティ > AAA > アプリケーション認証設定の順にメニューをクリックし、以下の画面を表示します。

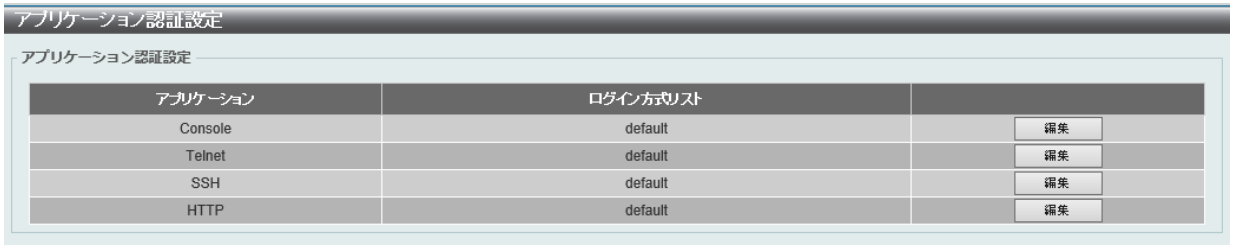


図 12-19　アプリケーション認証設定画面

指定エントリの「編集」をクリックし編集を行います。

「編集」をクリックすると、以下の画面が表示されます。



図 12-20　アプリケーション認証設定（編集）画面

画面に表示される項目：

項目	説明
ログイン方式リスト	指定エントリの「編集」をクリックし編集を行います。使用するログイン方法リスト名を入力します。

「適用」をクリックして、設定内容を適用します。

アプリケーションアカウンティング設定

アプリケーションアカウントを設定します。

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の順にメニューをクリックし、以下の画面を表示します。



図 12-21　アプリケーションアカウンティング設定画面

「編集」をクリックし、以下の画面で指定エントリの設定を行います。



図 12-22　アプリケーションアカウンティング設定（編集）画面

画面に表示される項目：

項目	説明
Exec 方式リスト	使用する EXEC メソッドリスト名を入力します。
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。 • 選択肢：「コンソール」「Telnet」「SSH」
レベル	権限レベルを指定します。 • 設定可能範囲：1-15
コマンド方法リスト	使用するコマンド方法リスト名を入力します。

「削除」をクリックして指定エントリを削除します。
「適用」をクリックして、設定内容を適用します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

認証設定

AAA ネットワークと EXEC 認証設定を行います。

セキュリティ > AAA > 認証設定の順にメニューをクリックし、以下の画面を表示します。



図 12-23　認証設定 - AAA 認証ネットワークタブ画面

AAA 認証ネットワークタブ

「AAA 認証ネットワーク」タブ内の設定を行います。

「AAA 認証 802.1X」「AAA 認証 MAC 認証」「AAA 認証 Web 認証」「AAA 認証 IGMP- 認証デフォルトグループ RADIUS」それぞれの項目において設定を行います。

項目	説明
ステータス	各項目の認証設定の有効 / 無効を設定します。
方式 1 - 4	本設定項目のメソッドリストを選択します。「AAA 認証 IGMP- 認証デフォルトグループ RADIUS」欄には表示されません。 • 「なし」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- 認証にローカルデータベースを使用します。 • 「グループ」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバ設定で定義されたサーバを使用します。

「適用」をクリックして、設定内容を適用します。

AAA 認証 Exec タブ

「AAA 認証 Exec」タブ内の設定を行います。

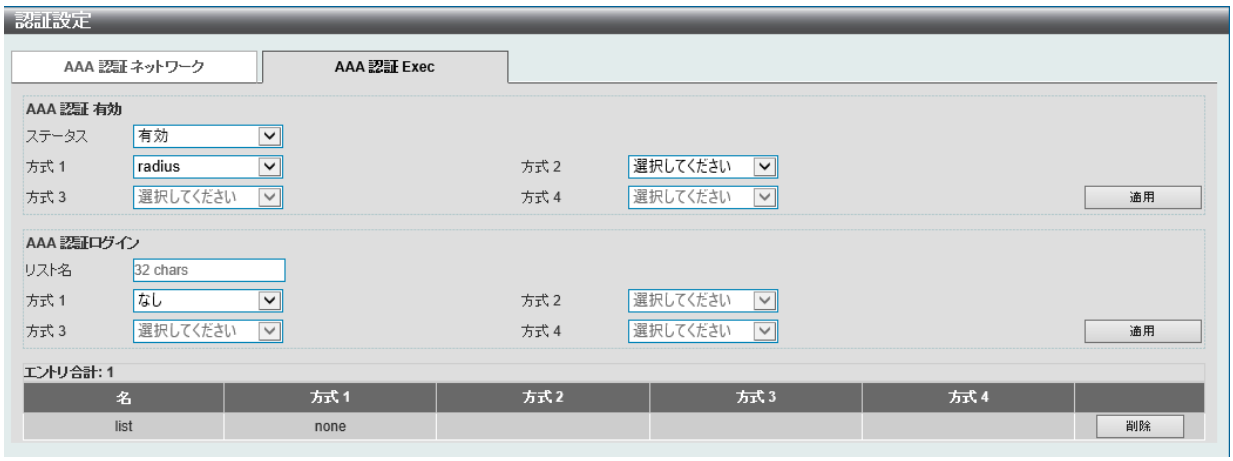


図 12-24　認証設定 - AAA 認証 Exec タブ画面

画面に表示される項目：

項目	説明
AAA 認証 有効	
ステータス	AAA 認証ステータスの有効 / 無効を設定します。
方式 1 - 4	本設定項目のメソッドリストを選択します。 • 「なし」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「有効」- ローカル Enable パスワードを認証に使用します。 • 「グループ」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。 • 「tacacs+」- TACACS+ サーバ設定で定義されたサーバを使用します。
AAA 認証 ログイン	
リスト名	AAA 認証ログインオプションで使用するメソッドリスト名を入力します。
方式 1 - 4	使用するメソッドリストを選択します。 • 「なし」- 通常、このメソッドは最後のメソッドとして指定します。1 つ前のメソッド認証により拒否されない場合、ユーザは認証をパスします。 • 「local」- ローカルデータベースを認証に使用します。 • 「グループ」- AAA グループサーバで定義されているサーバグループを指定します。表示される入力フィールドに AAA グループサーバ名を入力します。（32 文字以内） • 「radius」- RADIUS サーバホストコマンドで定義されたサーバを使用します。 • 「tacacs+」- TACACS+ サーバ設定で定義されたサーバを使用します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。

アカウンティング設定

アカウンティングの設定を行います。
セキュリティ > AAA > アカウンティング設定の順にメニューをクリックし、以下の画面を表示します。



図 12-25　アカウンティング設定画面

「AAA アカウンティング ネットワーク」「AAA アカウンティングシステム」「AAA アカウンティング Exec」「AAA アカウンティングコマンド」それぞれのタブにおいて設定を行います。

項目	説明
「AAA アカウンティングネットワーク」タブ	
初期値	メソッドリストの有効 / 無効を指定します。
方式 1 - 4	使用するメソッドリストを選択します。「なし」オプションは「方式 1」のみで設定可能です。 • 選択肢：「なし」「グループ」「RADIUS」「TACACS+」
「AAA アカウンティングシステム」タブ	
初期値	メソッドリストの有効 / 無効を指定します。
方式 1 - 4	使用するメソッドリストを選択します。「なし」オプションは「方式 1」のみで設定可能です。 • 選択肢：「なし」「グループ」「RADIUS」「TACACS+」
「AAA アカウンティング Exec」タブ	
リスト名	AAA アカウンティング EXEC オプションで使用するメソッドリストを入力します。
方式 1 - 4	使用するメソッドリストを選択します。「なし」オプションは「方式 1」のみで設定可能です。 • 選択肢：「なし」「グループ」「RADIUS」「TACACS+」
「AAA アカウンティングコマンド」タブ	
レベル	権限レベルを指定します。 • 設定可能範囲：1-15
リスト名	AAA アカウンティングコマンドオプションで使用するメソッドリストを入力します。
方式 1 - 4	使用するメソッドリストを選択します。「なし」オプションは「方式 1」のみで設定可能です。 • 選択肢：「なし」「グループ」「TACACS+」

「削除」をクリックして指定エントリを削除します。
「適用」をクリックして、設定内容を適用します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

RADIUS サーバダイナミックオーサー設定

RADIUS サーバのダイナミック認証設定を行います。

セキュリティ > AAA > RADIUS サーバダイナミックオーサー設定 の順にメニューをクリックし、以下の画面を表示します。



図 12-26　RADIUS サーバダイナミックオーサー設定 画面

画面に表示される項目：

項目	説明
RADIUS サーバ ダイナミックオーサーグローバル設定	
ダイナミック Author	ダイナミック認証機能を有効 / 無効に設定します。 ダイナミック認証により、外部ポリシーサーバは、デバイスに更新を動的に送信できます。
ポート	更新パケットのデータ送信に使用されるポート番号を入力します。 • 設定可能範囲：1-65535
RADIUS サーバダイナミックオーサー設定	
クライアント IP アドレス	RADIUS クライアントの IP アドレスを入力します。
クライアントホスト名	RADIUS クライアントのホスト名を入力します。
サーバキータイプ	RADIUS サーバのキータイプを以下から選択します。 •「平文 」- プレーンテキストの RADIUS サーバキータイプを使用します。 •「暗号化」- 暗号化された RADIUS サーバキータイプを使用します。
サーバキー	サーバキータイプに「平文」を選択した場合は、RADIUS サーバ接続のキーをプレーンテキスト形式で入力します（254 文字以内）。 サーバキータイプに「暗号化」を選択した場合は、RADIUS サーバ接続の鍵を暗号化された形式で入力します（344 文字以内）。

「適用」をクリックして、設定内容を適用します。

RADIUS

RADIUS サーバの設定を行います。

RADIUS グローバル設定

RADIUS サーバのグローバルステータスを設定します。

セキュリティ > RADIUS > RADIUS グローバル設定の順にメニューをクリックし、以下の画面を表示します。

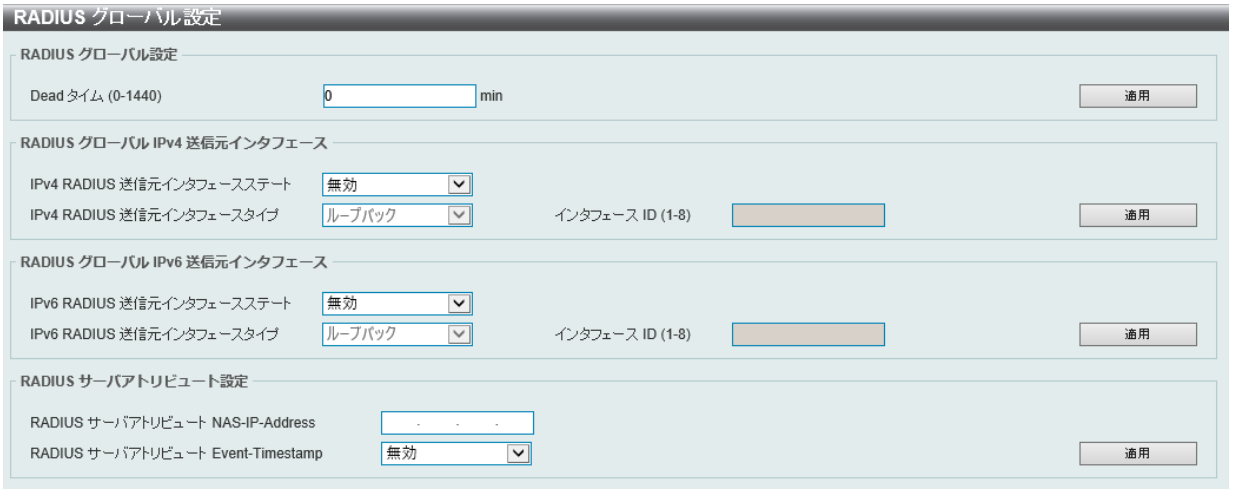


図 12-27　RADIUS グローバル設定 画面

画面に表示される項目：

項目	説明
RADIUS グローバル設定	
Dead タイム	デッドタイムの設定を行います。 0 に設定されている場合、応答しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストのエントリはスキップされ、認証プロセス時間が改善されます。システムが認証サーバへ認証を行う際、一度に一台のサーバへの認証が試みられます。 接続を試みたサーバが応答しない場合、システムは次のサーバに対して接続を試行します。応答しないサーバが検出されると、当該サーバはダウン状態として認識され、「デッドタイム」タイマが開始されます。それ以降のリクエスト認証はデッドタイム時間が経過するまでスキップされます。 • 設定可能範囲：0-1440（分） • 初期値：0（分）
RADIUS グローバル IPv4 送信元インタフェース設定	
IPv4 RADIUS 送信元インタフェースステート	IPv4 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 RADIUS 送信元インタフェースタイプ	IPv4 RADIUS 送信元インタフェースの種類を選択します。 •「ループバック」- IPv4 RADIUS 送信元インタフェースの種類をループバックに指定します。 •「VLAN」- IPv4 RADIUS 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv4 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）
RADIUS グローバル IPv6 送信元インタフェース設定	
IPv6 RADIUS 送信元インタフェースステート	IPv6 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 RADIUS 送信元インタフェースタイプ	IPv6 RADIUS 送信元インタフェースの種類を選択します。 •「ループバック」- IPv4 RADIUS 送信元インタフェースの種類をループバックに指定します。 •「VLAN」- IPv4 RADIUS 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv6 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）
RADIUS サーバアトリビュート設定	
RADIUS サーバアトリビュート NAS-IP-Address	RADIUS パケットに含まれる RADIUS サーバ属性 4 を指定します。
RADIUS サーバアトリビュート Event-Timestamp	RADIUS サーバ属性のイベントタイムスタンプ機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

RADIUS サーバ設定

RADIUS サーバ設定を行います。

セキュリティ > RADIUS > RADIUS サーバ設定をクリックし、以下の画面を表示します。



図 12-28　RADIUS サーバ設定画面

画面に表示される項目：

項目	説明
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	認証ポート番号を入力します。認証を使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1812
アカウンティング ポート	アカウンティングポート番号を入力します。アカウンティングを使用しない場合は「0」を指定します。 • 設定可能範囲：0-65535 • 初期値：1813
再送信	再送回数を設定します。無効にする場合は「0」を指定します。 • 設定可能範囲：0-20（回） • 初期値：2（回）
タイムアウト	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
鍵タイプ	使用する鍵の種類を選択します。 • 選択肢：「平文」「暗号化」
キー	RADIUS サーバとの通信で使用する鍵を指定します。（平文：254 文字以内、暗号化：344 文字以内）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。

RADIUS グループサーバ設定

RADIUS グループサーバの表示、設定を行います。

セキュリティ > RADIUS > RADIUS グループ サーバ設定をクリックし、以下の画面を表示します。



図 12-29　RADIUS グループサーバ設定画面

画面に表示される項目：

項目	説明
グループ サーバ名	RADIUS グループサーバ名を入力します。（32 文字以内）
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。

「追加」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「詳細を表示」をクリックして、指定エントリの詳細について表示します。

「詳細を表示」をクリックすると、以下の画面が表示されます。

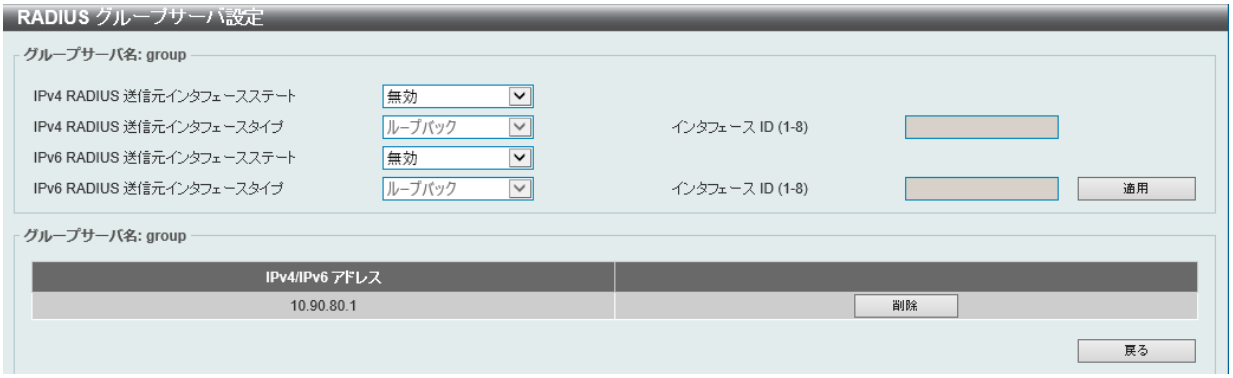


図 12-30　RADIUS グループ サーバ設定（詳細）画面

画面に表示される項目：

項目	説明
IPv4 RADIUS 送信元インタフェースステート	IPv4 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 RADIUS 送信元インタフェースタイプ	IPv4 RADIUS 送信元インタフェースの種類を選択します。 • 「ループバック」- IPv4 RADIUS 送信元インタフェースの種類をループバックに指定します。 • 「VLAN」- IPv4 RADIUS 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv4 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック選択時）、1-4094（VLAN 選択時）
IPv6 RADIUS 送信元インタフェースステート	IPv6 RADIUS 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 RADIUS 送信元インタフェースタイプ	IPv6 RADIUS 送信元インタフェースの種類を選択します。 • 「ループバック」- IPv6 RADIUS 送信元インタフェースの種類をループバックに指定します。 • 「VLAN」- IPv6 RADIUS 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv6 RADIUS 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「戻る」をクリックして以前の画面に戻ります。

RADIUS 統計

RADIUS 統計情報の表示、設定を行います。

セキュリティ > RADIUS > RADIUS 統計をクリックし、以下の画面を表示します。



図 12-31　RADIUS 統計 画面

画面に表示される項目：

項目	説明
グループ サーバ名	表示する RADIUS グループサーバ名を選択します。

複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。
「クリア」をクリックし、選択に基づいて表示した情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。

TACACS+

TACACS+ サーバの設定を行います。

TACACS+ グローバル設定

TACACS+ サーバをグローバルに有効 / 無効に指定します。

セキュリティ > TACACS+ > TACACS+ グローバル設定をクリックし、以下の画面を表示します。



図 12-32　TACACS+ グローバル設定 画面

画面に表示される項目：

項目	説明
TACACS+ グローバル IPv4 送信元インタフェース	
IPv4 TACACS+ ソースインタフェースステート	IPv4 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 TACACS+ ソースインタフェースタイプ	IPv4 TACACS+ 送信元インタフェースの種類を選択します。 • 「ループバック」- IPv4 TACACS+ 送信元インタフェースの種類をループバックに指定します。 • 「VLAN」- IPv4 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv4TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）
TACACS+ グローバル IPv6 送信元インタフェース	
IPv6 TACACS+ ソースインタフェースステート	IPv6 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 TACACS+ ソースインタフェースタイプ	IPv6 TACACS+ 送信元インタフェースの種類を選択します。 • 「ループバック」- IPv6 TACACS+ 送信元インタフェースの種類をループバックに指定します。 • 「VLAN」- IPv6 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv6 TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）

「適用」をクリックして、設定内容を適用します。

TACACS+ サーバ設定

TACACS+ サーバの表示、設定を行います。

セキュリティ > TACACS+ > TACACS+ サーバ設定をクリックし、以下の画面を表示します。



図 12-33　TACACS+ サーバ設定画面

画面に表示される項目：

項目	説明
IP アドレス	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 アドレス	TACACS+ サーバの IPv6 アドレスを入力します。
ポート	TACACS+ サーバのポートを入力します。 • 設定可能範囲：1-65535 • 初期値：49
タイムアウト	タイムアウト時間を設定します。 • 設定可能範囲：1-255（秒） • 初期値：5（秒）
鍵タイプ	使用する鍵の種類を選択します。 •「平文」「暗号化」
キー	TACACS+ サーバとの通信で使用する鍵を指定します。（平文：254 文字以内、暗号化：344 文字以内）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。

TACACS+ グループサーバ設定

TACACS+ グループサーバの表示、設定を行います。

セキュリティ > TACACS+ > TACACS+ グループ サーバ設定をクリックし、以下の画面を表示します。



図 12-34　TACACS+ グループサーバ設定画面

画面に表示される項目：

項目	説明
グループ サーバ名	TTACACS+ グループサーバ名を入力します。（32 文字以内）
IPv4 アドレス	TACACS+ グループサーバの IPv4 アドレスを入力します。
IPv6 アドレス	TACACS+ グループサーバの IPv6 アドレスを入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。

「詳細を表示」をクリックすると TACACS+ グループサーバの詳細情報について表示されます。



図 12-35　TACACS+ グループ サーバ設定（詳細）画面

画面に表示される項目：

項目	説明
IPv4 TACACS+ ソースインタフェースステート	IPv4 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv4 TACACS+ ソースインタフェースタイプ	IPv4 TACACS+ 送信元インタフェースの種類を選択します。 •「ループバック」- IPv4 TACACS+ 送信元インタフェースの種類をループバックに指定します。 •「VLAN」- IPv4 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv4TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）
IPv6 TACACS+ ソースインタフェースステート	IPv6 TACACS+ 送信元インタフェースのステータスを有効 / 無効に設定します。
IPv6 TACACS+ ソースインタフェースタイプ	IPv6 TACACS+ 送信元インタフェースの種類を選択します。 •「ループバック」- IPv6 TACACS+ 送信元インタフェースの種類をループバックに指定します。 •「VLAN」- IPv6 TACACS+ 送信元インタフェースの種類を VLAN に指定します。
インタフェース ID	IPv6 TACACS+ 送信元インタフェース ID を選択します。 • 設定可能範囲：1-8（ループバック 選択時）、1-4094（VLAN 選択時）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「戻る」をクリックして以前の画面に戻ります。

TACACS+ 統計

TACACS+ 統計情報を表示します。

セキュリティ > TACACS+ > TACACS+ 統計をクリックし、以下の画面を表示します。



図 12-36　TACACS+ 統計 画面

画面に表示される項目：

項目	説明
グループ サーバ名	統計情報を削除する TACACS+ グループサーバ名を選択します。

「クリア」をクリックし、選択に基づいて表示した情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。

IMPB

IMPB（IP-MAC-Port Binding) の設定を行います。

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結びつけることにより、レイヤ間のデータ転送が可能になります。

IP-MAC バインディングの主な目的は、スイッチにアクセスするユーザを制限することです。IP アドレスと MAC アドレスのペアについて、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチがスヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IPv4

DHCPv4 スヌーピング

■ DHCP スヌーピンググローバル設定

DHCP スヌーピングについてグローバルに表示、設定します。

セキュリティ > IMPB > IPv4 > DHCPv4 スヌーピング > DHCP スヌーピンググローバル設定の順にクリックして、以下の画面を表示します。

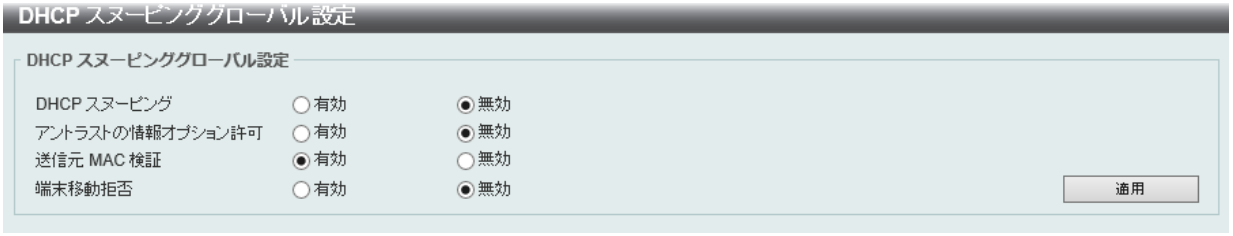


図 12-37　DHCP スヌーピンググローバル設定画面

画面に表示される項目：

項目	説明
DHCP スヌーピング	DHCP スヌーピングのグローバルステータスを有効 / 無効に設定します。
アントラストの情報オプション許可	信頼されていないインタフェースにおけるリレーオプション 82 付き DHCP パケットの許可のグローバルステータスを有効 / 無効に設定します。
送信元 MAC 検証	クライアントのハードウェアアドレスと DHCP パケットの送信元 MAC アドレスが一致しているかどうかの検証を有効 / 無効に設定します。
端末移動拒否	DHCP スヌーピングの端末移動拒否（Station Move Deny）を有効 / 無効に設定します。 端末移動（Station Move）が有効の場合、指定ポート上で同じ VLAN ID と MAC アドレスを持つダイナミック DHCP バインディングエントリは、新しい DHCP プロセスが同じ VLAN ID と MAC アドレスに属していることを検出した場合、他のポートへ移動することが可能です。

「適用」をクリックして、設定内容を適用します。

■ DHCP スヌーピングポート設定

DHCP スヌーピングポートの表示、設定を行います。

セキュリティ > IMPB > IPv4 > DHCPv4 スヌーピング > DHCP スヌーピングポート設定の順にクリックして、以下の画面を表示します。

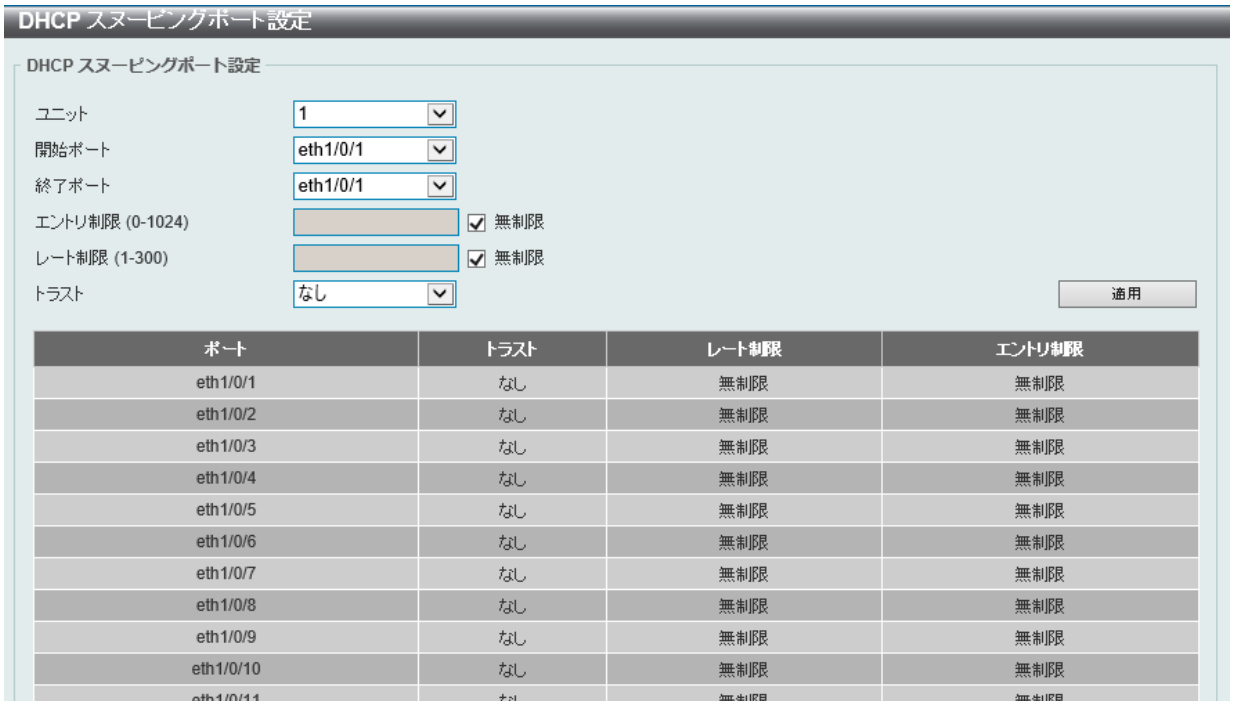


図 12-38　DHCP スヌーピングポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
エントリ制限	エントリ制限の値を入力します。「無制限」をチェックをすると、本機能は無効になります。 • 設定可能範囲：0 -1024
レート制限	レート制限の値を入力します。「無制限」をチェックをすると、本機能は無効になります。 • 設定可能範囲：1 -300
トラスト	トラスト（信頼済み）オプションを選択します。 DHCP サーバや他のスイッチなどに接続しているポートは信頼済みインタフェースとして設定される必要があります。 DHCP クライアントに接続しているポートは信頼されていないポートとして設定します。 DHCP スヌーピングは DHCP サーバと信頼されていないインタフェースの間でファイアウォールとして動作します。 • 選択肢：「なし」「はい」

「適用」をクリックして、設定内容を適用します。

■ DHCP スヌーピング VLAN 設定

DHCP スヌーピング VLAN の設定、表示を行います。

セキュリティ > IMPB > IPv4 > DHCPv4 スヌーピング > DHCP スヌーピング VLAN 設定の順にクリックして、以下の画面を表示します。



図 12-39　DHCP スヌーピング VLAN 設定画面

画面に表示される項目：

項目	説明
VID リスト	設定する VLAN ID リストを入力します。
状態	DHCP スヌーピング VLAN を有効 / 無効に指定します。

「適用」をクリックして、設定内容を適用します。

■ 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の表示、設定を行います。

セキュリティ > IMPB > IPv4 > DHCPv4 スヌーピング > DHCP スヌーピングデータベースの順にクリックして、以下の画面を表示します。

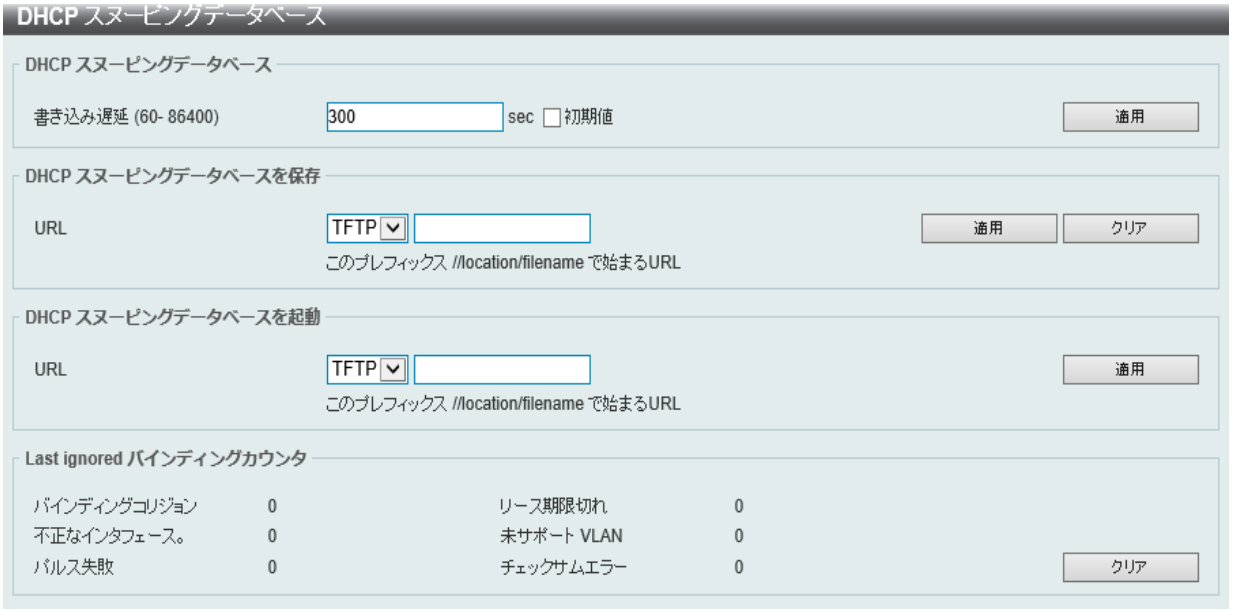


図 12-40　DHCP スヌーピングデータベース画面

画面に表示される項目：

項目	説明
DHCP スヌーピングデータベース	
書き込み遅延	書き込み遅延時間の値を入力します。 • 設定可能範囲：60-86400（秒） • 初期値：300（秒）
DHCP スヌーピングデータベースを保存	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの保存先 URL を入力します。 • 選択肢：「TFTP」
DHCP スヌーピングデータベースを起動	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースの読み込み元 URL を入力します。 • 選択肢：「TFTP」

「適用」をクリックし、設定内容を適用してください。
「クリア」をクリックするとカウンタ情報が消去されます。

■ DHCP スヌーピングバインディングエントリ

DHCP スヌーピングバインディングエントリの表示、設定を行います。

セキュリティ > IMPB > 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の順にクリックして画面を表示します。



図 12-41　DHCP スヌーピングバインディングエントリ画面

本画面には以下の項目があります。

項目	説明
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	DHCP スヌーピングバインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IP アドレス	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
ユニット	設定するユニットを指定します。
ポート	設定するポートを指定します。
期限	有効期限を入力します。 • 設定可能範囲：60-4294967295（秒）

「追加」をクリックして入力した情報を基に新しいエントリを追加します。
「削除」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

ダイナミック ARP インスペクション

■ ARP アクセスリスト

ARP アクセスリストの設定、表示を行います。

セキュリティ > IMPB > IPv4 > ダイナミック ARP インスペクション > ARP アクセスリストの順にクリックして、以下の画面を表示します。

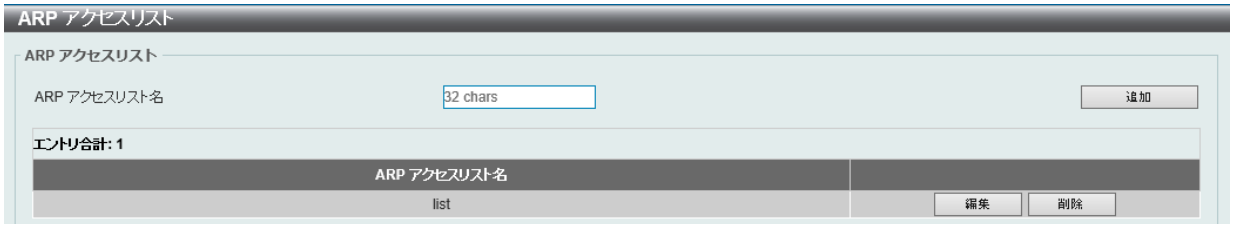


図 12-42　ARP アクセスリスト画面

画面に表示される項目：

項目	説明
ARP アクセスリスト名	ARP アクセスリスト名を入力します。（32 文字以内）

「追加」をクリックして入力した情報を基に新しいエントリを追加します。
「削除」をクリックして指定エントリを削除します。

エントリの編集

「編集」をクリックして指定のエントリを編集します。以下の画面が表示されます。



図 12-43　ARP アクセスリスト（編集）画面

画面に表示される項目：

項目	説明
アクション	実行するアクションを指定します。 • 選択肢：「許可」「拒否」
IP	送信元 IP アドレスの種類を指定します。 • 選択肢：「Any」「ホスト」「マスクを持った IP」
送信元 IP	送信元 IP アドレスを「ホスト」「マスクを持った IP」から選択した後、使用する送信元 IP アドレスを入力します。
送信元 IP マスク	「マスクを持った IP」を選択した場合、使用する送信者の IP マスクを入力します。
MAC	送信者の MAC アドレスの種類を指定します。 • 選択肢：「Any」「ホスト」「マスクを持った MAC」
送信元 MAC	送信者の MAC アドレスを「ホスト」「マスクを持った MAC」から選択した後、使用する送信者の MAC アドレスを入力します。
送信元 MAC マスク	「マスクを持った MAC」を選択した場合、使用する送信者の MAC マスクを入力します。

「戻る」をクリックして前のページに戻ります。
「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。

■ ARP インスペクション設定

ARP インスペクションの設定、表示を行います。

セキュリティ > IMPB > IPv4 > ダイナミック ARP インスペクション > ARP インスペクション設定の順にクリックして、以下の画面を表示します。



図 12-44　ARP インスペクション設定画面

画面に表示される項目：

項目	説明
ARP インスペクション検証	
送信元 MAC	送信元 MAC オプションについて有効 / 無効に設定します。 有効にすると、ARP リクエストおよび応答パケットをチェックし、ARP ペイロードに含まれる送信元 MAC アドレスに対してイーサネットヘッダ内の送信元 MAC アドレスの整合性を検証します。
送信先 MAC	宛先 MAC オプションについて有効 / 無効に設定します。 有効にすると、ARP リクエストおよび応答パケットをチェックし、ARP ペイロードに含まれる宛先 MAC アドレスに対してイーサネットヘッダ内の宛先 MAC アドレスの整合性を検証します。
IP	IP オプションについて有効 / 無効に設定します。 有効にすると、不正な IP アドレスや予期せぬ IP アドレスがないか ARP の body をチェックします。また、ARP ペイロードにおける IP アドレスの妥当性もチェックします。ARP リクエストとレスポンスの両方の送信元 IP、および ARP レスポンスのターゲット IP が検証されます。IP アドレス「0.0.0.0」「255.255.255.255」宛のパケットとすべての IP マルチキャストは破棄されます。送信元 IP アドレスはすべての ARP リクエストとレスポンスにおいてチェックされ、宛先 IP アドレスは ARP レスポンス内のみでチェックされます。
ARP インスペクション VLAN ロギング	
VID リスト	ARP インスペクション VLAN ID リストを入力します。
状態	ARP インスペクション VLAN ロギング機能を有効 / 無効に設定します。
ACL ロギング	「編集」をクリックして、ACL ロギングアクションを選択します。 • 選択肢：「拒否」「許可」「全て」「なし」
DHCP ロギング	「編集」をクリックして、DHCP ロギングアクションを選択します。 • 選択肢：「拒否」「許可」「全て」「なし」
ARP インスペクションフィルタ	
ARP アクセスリスト名	ARP アクセスリスト名を入力します。（32 文字以内）
VID リスト	使用する VLAN ID リストを指定します。
スタティック ACL	スタティック ACL を使用するか否かを選択します。 • 選択肢：「はい」「なし」

「適用」をクリックして、設定内容を適用します。
「追加」をクリックして入力した情報を基に新しいエントリを追加します。
「削除」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

■ ARP インスペクションポート設定

ポートでの ARP インスペクションの設定、表示を行います。

セキュリティ > IMPB > IPv4 > ダイナミック ARP インスペクション > ARP インスペクションポート設定の順にクリックして、以下の画面を表示します。

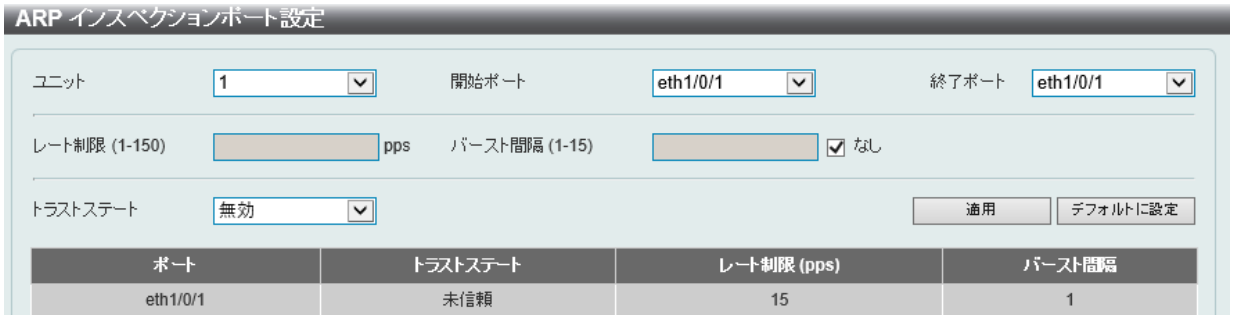


図 12-45　ARP インスペクションポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
レート制限	レート制限の値を入力します。 • 設定可能範囲：1- 150（パケット / 秒）
バースト間隔	バースト間隔の値を入力します。「なし」をチェックをするとオプションは無効になります。 • 設定可能範囲：1-15
トラストステート	トラストステータスを有効 / 無効に設定します。

「適用」をクリックし、設定内容を適用してください。「デフォルトに設定」をクリックすると、設定内容は初期値になります。

■ ARP インスペクション統計

ARP インスペクションの統計情報の表示、消去を行います。

セキュリティ > IMPB > IPv4 > ダイナミック ARP インスペクション > ARP インスペクション統計の順にクリックして、以下の画面を表示します。



図 12-46　ARP インスペクション統計画面

画面に表示される項目：

項目	説明
VID リスト	設定する VLAN ID リストを入力します。

「VLAN 毎にクリア」をクリックし、入力した VLAN ID についての情報を消去します。
「すべてをクリア」をクリックし、テーブルのすべての情報を消去します。

■ ARP インスペクションログ

ARP インスペクションログ情報の表示、消去、設定を行います。

セキュリティ > IMPB > IPv4 > ダイナミック ARP インスペクション > ARP インスペクションログの順にクリックして、以下の画面を表示します。



図 12-47　ARP インスペクションログ画面

画面に表示される項目：

項目	説明
ログバッファ	使用するログバッファの値を入力します。「初期値」をチェックすると初期値を使用します。 • 設定可能範囲：1-1024 • 初期値：32

「適用」をクリックし、設定内容を適用します。「ログをクリア」をクリックし、ログを消去します。

IP ソースガード

■ IP ソースガードポート設定

IP ソースガード（IPSG）の表示、設定を行います。

セキュリティ > IMPB > IPv4 > IP ソースガード > IP ソースガードポート設定の順にクリックして、以下の画面を表示します。

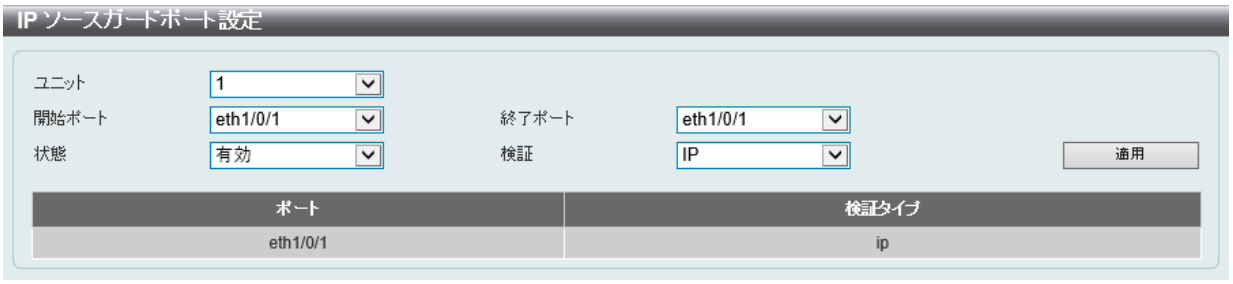


図 12-48　IP ソースガードポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートの IP ソースガードを有効 / 無効に設定します。
検証	検証方法について選択します。 • 「IP」- 受信パケットの IP アドレスがチェックされます。 • 「IP-MAC」- 受信パケットの IP アドレスと MAC アドレスがチェックされます。

「適用」をクリックし、設定内容を適用してください。

■ IP ソースガードバインディング

IP ソースガードバインディングの表示、設定を行います。

セキュリティ > IMPB > IPv4 > IP ソースガード > IP ソースガードバインディングの順にクリックして、以下の画面を表示します。

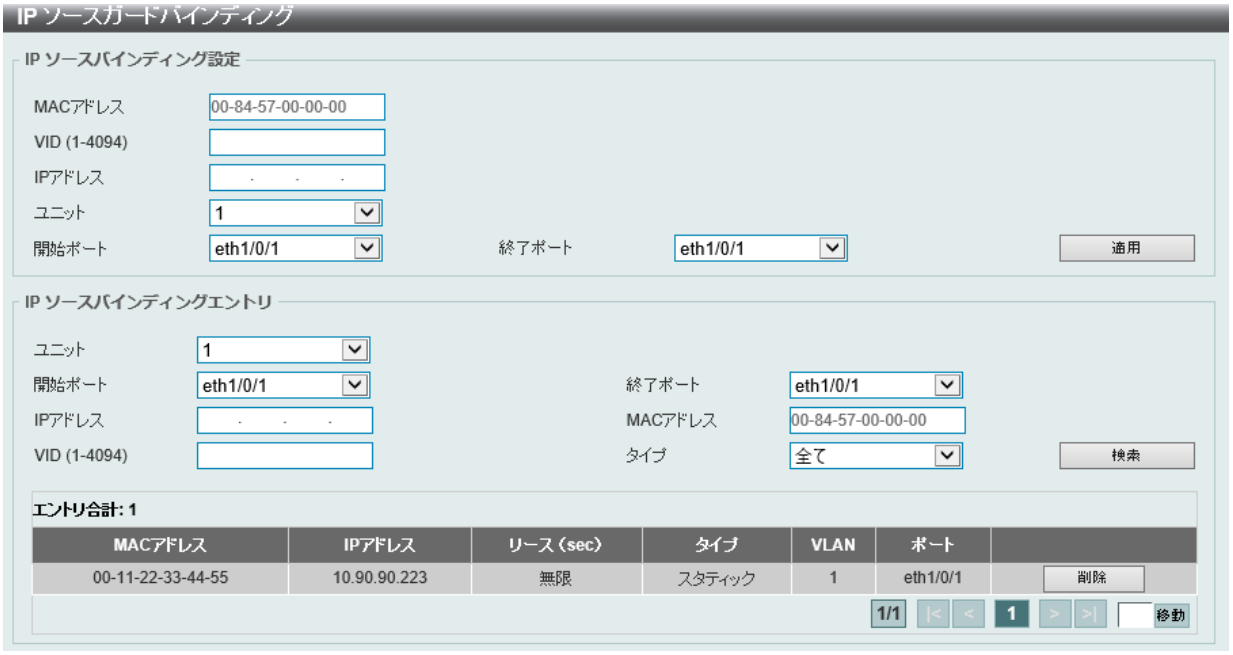


図 12-49　IP ソースガードバインディング画面

画面に表示される項目：

項目	説明
IP ソースバインディング設定	
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	バインディングエントリの VLAN ID を入力します。
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。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
IP 送信元バインディングエントリ	
ユニット	バインディングエントリを検索するユニットを指定します。
開始ポート / 終了ポート	バインディングエントリを検索するポートの範囲を指定します。
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	バインディングエントリの VLAN ID を入力します。
タイプ	バインディングエントリの種類を選択します。 • 「全て」- すべての DHCP バインディングエントリが表示されます。 • 「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が表示されます。 • 「スタティック」- 手動で設定した IP ソースガードバインディングエントリが表示されます。

「適用」をクリックし、設定内容を適用してください。
「削除」をクリックして指定エントリを削除します。
「検索」をクリックして入力した情報を基に指定のエントリを表示します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

■ IP ソースガード HW エントリ

IP ソースガードハードウェアエントリの表示を行います。

セキュリティ > IMPB > IPv4 > IP ソースガード > IP ソースガード HW エントリの順にクリックして、以下の画面を表示します。



図 12-50　IP ソースガード HW エントリ画面

画面に表示される項目：

項目	説明
ユニット	検索対象のユニットを指定します。
開始ポート / 終了ポート	検索対象のポート範囲を指定します。

複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。
「検索」をクリックして入力した情報を基に指定のエントリを表示します。

詳細設定

■ IP-MAC-Port バインディング 設定

IP-MAC ポートバインディングの設定、表示を行います。

セキュリティ > IMPB > IPv4 > 詳細設定 > IP-MAC-Port バインディング 設定の順にクリックして、以下の画面を表示します。



図 12-51　IP-MAC-Port バインディング 設定画面

画面に表示される項目：

項目	説明
IP-MAC- ポートバインディングトラップ設定	
トラップステート	IP-MAC ポートバインディングのトラップ設定を有効 / 無効に指定します。
IP-MAC-Port バインディングポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	ポートの範囲を指定します。
モード	アクセスコントロールのモードを選択します。 • 「無効」- 指定ポートで IP-MAC-Port バインディング機能が無効になります。 • 「Strict」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過した後のみ、ポートへアクセスできます。バインディングチェックを通過するには、送信元 IP アドレス / 送信元 MAC アドレス /VLAN ID/ 受信ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピングによって学習されたダイナミックバインディングエントリのいずれかのエントリに一致する必要があります。 • 「ルーズ」- ホストが ARP/IP パケット送信後、それらのパケットがバインディングチェックを通過しなかった場合にポートへのアクセスが拒否されます。バインディングチェックを通過するには、送信元 IP アドレス / 送信元 MAC アドレス /VLAN ID/ 受信ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピングによって学習されたダイナミックバインディングエントリのいずれかのエントリに一致する必要があります。

「適用」をクリックして、設定内容を適用します。

■ IP-MAC-Port バインディングブロックエントリ

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

セキュリティ > IMPB > IPv4 > 詳細設定 > IP-MAC-Port バインディングブロックエントリの順にクリックして、以下の画面を表示します。

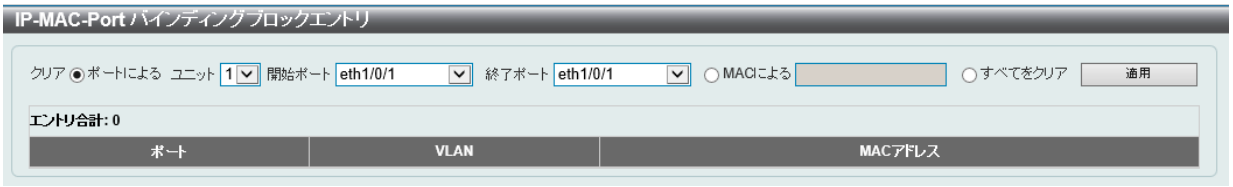


図 12-52　IP-MAC-Port バインディングブロックエントリ画面

画面に表示される項目：

項目	説明
ポートによる	選択ポートに基づいたエントリテーブルをクリアします。
ユニット	エントリを削除するユニットを指定します。
開始ポート / 終了ポート	エントリを削除するポートの範囲を指定します。
MAC による	指定した MAC アドレスに基づきエントリを消去します。項目欄に MAC アドレスを入力します。
すべてをクリア	すべてのエントリを消去します。

「適用」をクリックして、設定内容を適用します。

IPv6

IPv6 スヌーピング

IPv6 スヌーピングについて表示、設定します。

セキュリティ > IMPB > IPv6 > IPv6 スヌーピングの順にクリックして、以下の画面を表示します。

■ **IPv6 スヌーピング ポリシー設定タブ**



図 12-53　IPv6 スヌーピング - IPv6 スヌーピング ポリシー設定タブ画面

画面に表示される項目：

項目	説明
端末移動設定	
端末移動	ステーション移行について設定します。 • 選択肢：「許可」「拒否」
IPv6 スヌーピング ポリシー設定	
ポリシー名	IPv6 スヌーピングポリシー名を入力します。（32 文字以内）
アドレス数制限	アドレスカウント制限の値を指定します。「無制限」を指定するとアドレスカウント制限は無効になります。 • 設定可能範囲：0-511
プロトコル	本ポリシーに対応するプロトコルを選択します。 • 選択肢：「DHCP」「NDP」「DHCP-PD」「DHCP-PD-EXT」 DHCPv6 スヌーピング： アドレス割り当ての際に DHCPv6 クライアントとサーバ間の DHCPv6 パケットをスヌーピングします。DHCPv6 クライアントが有効な IPv6 アドレスを取得すると、DHCPv6 スヌーピングによってバインディングデータベースが作成されます。 ND スヌーピング： ステートレス自動設定による IPv6 アドレスと手動設定による IPv6 アドレスのための機能です。IPv6 アドレスを割り当てる前に、ホストは「Duplicate Address Detection」（DAD：重複アドレス検出）を実行する必要があります。ND スヌーピングは DAD メッセージ（DAD NS と DAD NA）を受信しバインディングデータベースを構築します。NDP パケット (NS と NA) は、ホストが到達可能かを判断しバインディングを削除するかどうかを決定するためにも使用されます。 DHCP-PD スヌーピング： プレフィックス委任（PD）の DHCPv6 スヌーピングを実行して、委任ルータ（IPv6 プレフィックスが割り当てられている）と対応する要求ルータ間のバインディングをセットアップします。そのバインディングは、パケットの送信元プレフィックスを検証するために使用することができます。
データ収集	データ収集（Data-Glean）機能を有効 / 無効に設定します。 ある状況下（DAD-NS パケットの喪失やスイッチの再起動）においては、有効な IPv6 アドレスがバインディングテーブルで検出できず、デバイスとの間のトラフィックが IPv6 ソースガードによって拒否されます。 データ収集機能により、IPv6 Duplicate Address Detection (DAD) を使用して、失われた IPv6 アドレスを回復する手段を提供します。
VID リスト	使用する VLAN ID リストを入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「編集」をクリックして指定エントリを編集します。

■ IPv6 スヌーピング DHCP エントリ設定タブ

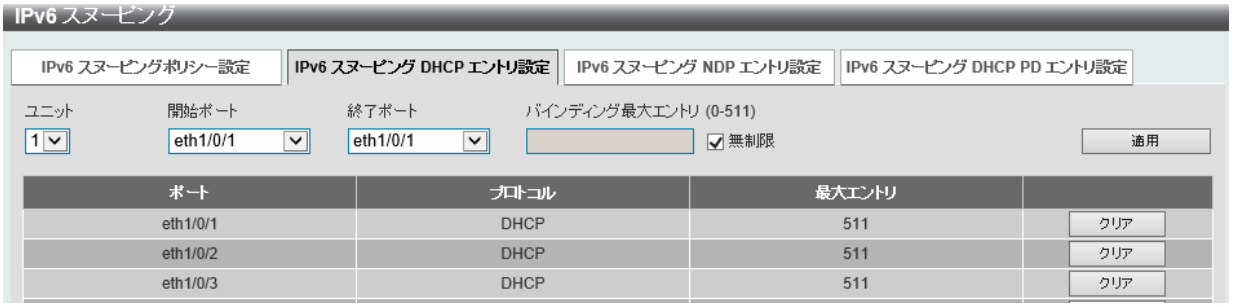


図 12-54　IPv6 スヌーピング - IPv6 スヌーピング DHCP エントリ設定タブ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
バインディング最大エントリ	許可される IPv6 スヌーピングバインディングエントリの最大数を入力します。 • 設定可能範囲：0 - 511

「適用」をクリックして、設定内容を適用します。
「クリア」をクリックすると、ポートの DHCP スヌーピングエントリがクリアされます。

■ IPv6 スヌーピング NDP エントリ設定タブ

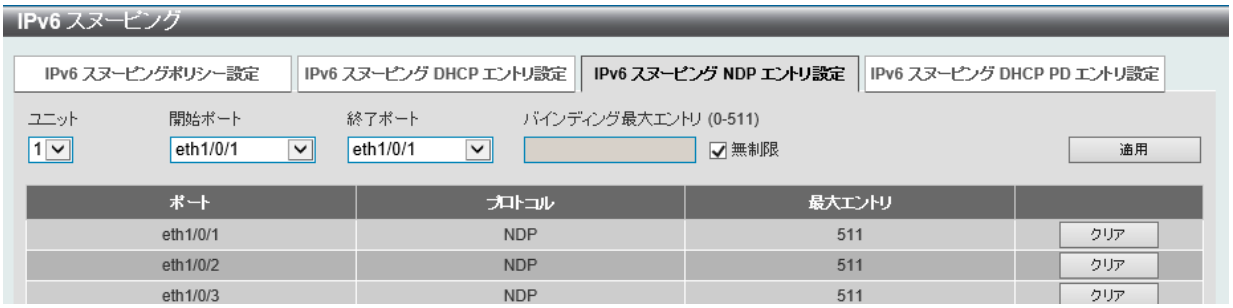


図 12-55　IPv6 スヌーピング - IPv6 スヌーピング NDP エントリ設定タブ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
バインディング最大エントリ	許可される IPv6 スヌーピングバインディングエントリの最大数を入力します。 • 設定可能範囲：0 - 511

「適用」をクリックして、設定内容を適用します。
「クリア」をクリックすると、そのポートの ND スヌーピングエントリがクリアされます。

■ IPv6 スヌーピング DHCP PD エントリ設定タブ



図 12-56　IPv6 スヌーピング - IPv6 スヌーピング DHCP PD エントリ設定タブ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
バインディング最大エントリ	許可される IPv6 スヌーピングバインディングエントリの最大数を入力します。 • 設定可能範囲：0 - 511

「適用」をクリックして、設定内容を適用します。
「クリア」をクリックすると、ポートの DHCP PD スヌーピングエントリがクリアされます。

IPv6 ND インスペクション

IPv6 ND インスペクションについて表示、設定します。

セキュリティ > IMPB > IPv6 > IPv6 ND インスペクションの順にクリックして、以下の画面を表示します。



図 12-57　IPv6 ND インスペクション画面

画面に表示される項目：

項目	説明
ポリシー名	ポリシー名を入力します。（32 文字以内）
デバイスロール	デバイスの役割を選択します。 • 「ホスト」- NS、NA メッセージのインスペクションは動作します。（初期値） • 「ルータ」- NS/NA に対するインスペクションは実行されません。 NS/NA インスペクションが実行されると、DHCP もしくは ND プロトコルから学習したダイナミックバインディングテーブルに対してメッセージの検証が行われます。
モード	モードを以下から選択します。 • 「詳細」- ND インスペクションは、ターゲットアドレスが DANA/NA パケットのソースアドレスと同一であるかどうかをチェックします。 • 「Fuzzy」- ND インスペクションは、ターゲットアドレスとソースアドレスの両方がバインディングテーブルに存在するかどうかをチェックします。
送信元 MAC 検証	送信元 MAC アドレスオプションの検証を有効 / 無効に設定します。 リンクレイヤアドレスを含む ND メッセージを受信した時に、リンクレイヤアドレスに対して送信元 MAC アドレスがチェックされます。リンクレイヤアドレスと MAC アドレスが異なる場合、パケットは破棄されます。
ターゲットポート	チェックを入れターゲットポートを指定します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「編集」をクリックして指定エントリを編集します。

IPv6 RA ガード

IPv6 RA ガードについて表示、設定します。

セキュリティ > IMPB > IPv6 > IPv6 RA ガードの順にクリックして、以下の画面を表示します。



図 12-58　IPv6 RA ガード画面

画面に表示される項目：

項目	説明
ポリシー名	ポリシー名を入力します。(32 文字以内)
デバイスロール	デバイスの役割を選択します。 • 「ホスト」- RA パケットはすべてブロックされます。(初期値) • 「ルータ」- RA パケットは、ポートに設定された ACL に従い転送されます。
IPv6 アクセスリスト合致	照合を行う IPv6 アクセスリストを入力します。 「選択してください」をクリックすると、既存の ACL を選択することができます。
ターゲットポート	チェックを入れターゲットポートを指定します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「編集」をクリックして指定エントリを編集します。

「選択してください」をクリックすると次の画面が表示されます。



図 12-59　ACL アクセスリスト画面

設定するエントリを選択し「OK」をクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPv6 DHCP ガード

IPv6 DHCP ガードについて表示、設定します。

セキュリティ > IMPB > IPv6 > IPv6 DHCP ガードの順にクリックして、以下の画面を表示します。

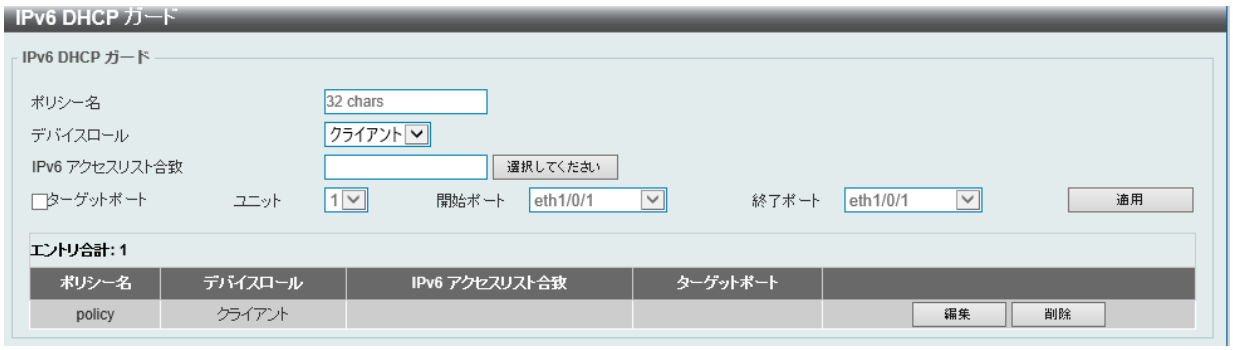


図 12-60　IPv6 DHCP ガード画面

画面に表示される項目：

項目	説明
ポリシー名	ポリシー名を入力します。（32 文字以内）
デバイスロール	デバイスの役割を選択します。 • 「クライアント」- DHCPv6 サーバからの DHCPv6 パケットはすべてブロックされます。（初期値） • 「サーバ」- DHCPv6 サーバパケットはポートに設定された ACL に従い転送されます。
IPv6 アクセスリスト合致	照合する IPv6 アクセスリストを入力します。 「選択してください」をクリックすると、既存のエントリから選択することができます。
ターゲットポート	チェックを入れターゲットポートを指定します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定エントリを削除します。
「編集」をクリックして指定エントリを編集します。

「選択してください」をクリックすると次の画面が表示されます。



図 12-61　ACL アクセスリスト画面

設定するエントリを選択し「OK」をクリックします。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

IPv6 ソースガード

■ IPv6 ソースガード 設定

IPv6 ソースガードの表示、設定を行います。

セキュリティ > IMPB > IPv6 > IPv6 ソースガード > IPv6 ソースガード 設定の順にクリックして、以下の画面を表示します。



図 12-62　IPv6 ソースガード 設定画面

画面に表示される項目：

項目	説明
IPv6 ソースガードポリシー設定	
ポリシー名	ポリシー名を入力します。(32 文字以内)
グローバル自動設定アドレス	自動設定グローバルアドレスからのデータトラフィックの許可 / 拒否を選択します。 リンク上のすべてのグローバルアドレスが DHCP によって割り当てられていて、ホスト自身による設定アドレスからのトラフィック送信をブロックしたい場合に役に立ちます。 • 選択肢：「許可」「拒否」
アドレスを検証	アドレス検証機能を有効 / 無効に指定します。IPv6 ソースガードでアドレス検証機能を実行します。
プレフィックスを検証	プリフィクス検証機能を有効 / 無効に指定します。IPv6 ソースガードで IPv6 プリフィクスガード機能を実行します。
リンクローカル トラフィック	リンクローカルアドレスによって送信されたデータトラフィックの許可 / 拒否を選択します。
IPv6 ソースガード接続ポリシー設定	
ポリシー名	ポリシー名を入力します。(32 文字以内)
ターゲットポート	ターゲットポートを指定します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。

「適用」をクリックし、設定内容を適用してください。
「編集」をクリックして、指定エントリの編集を行います。
「削除」をクリックすると指定のエントリを削除します。

■ IPv6 隣接バインディング

IPv6 隣接（ネイバ）バインディングの表示、設定を行います。

セキュリティ > IMPB > IPv6 > IPv6 ソースガード > IPv6 隣接バインディングの順にクリックして、以下の画面を表示します。

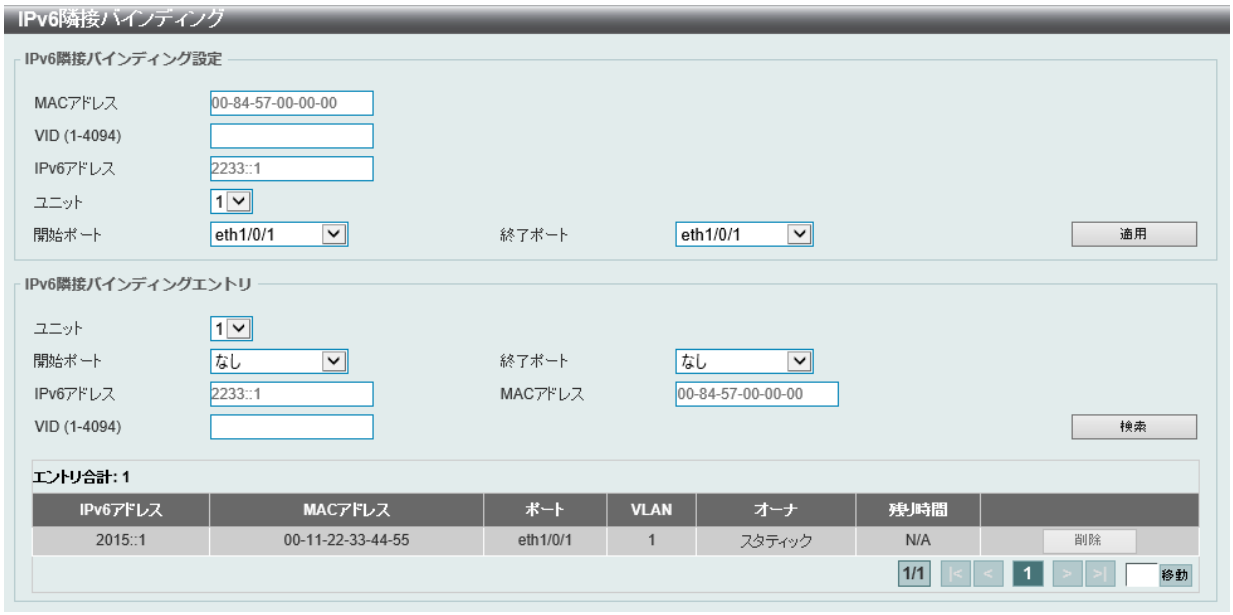


図 12-63　IPv6 隣接バインディング画面

画面に表示される項目：

項目	説明
IPv6 隣接バインディング 設定	
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	バインディングエントリの VLAN ID を入力します。 • 設定可能範囲：1-4094
IPv6 アドレス	バインディングエントリの IPv6 アドレスを入力します。
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
IPv6 隣接バインディングエントリ	
ユニット	バインディングエントリを表示するユニットを指定します。
開始ポート / 終了ポート	バインディングエントリを表示するポートを指定します。
IPv6 アドレス	検索する IPv6 アドレスを入力します。
MAC アドレス	検索する MAC アドレスを入力します。
VID	検索する VLAN ID を入力します。

「適用」をクリックし、設定内容を適用してください。
「削除」をクリックして指定エントリを削除します。
「検索」をクリックして入力した情報を基に指定のエントリを表示します。
設定エントリページが複数ページある場合、ページ番号を指定して「移動」をクリックすると当該のページへ移動します。

DHCP サーバスクリーニング

DHCP サーバパケットの制限や、DHCP クライアントが指定の DHCP サーバパケットを受信するように設定します。
複数の DHCP サーバがネットワーク上に存在し、それぞれ異なる個別のクライアントグループに DHCP サービスを提供する場合に役立ちます。

ポートで DHCP サーバスクリーニング機能が有効になっている場合、このポートで受信したすべての DHCP サーバパケットは、ソフトウェアベースのチェックのために CPU にリダイレクトされます。 正当な DHCP サーバパケットは転送され、不正な DHCP サーバパケットは破棄されます。
DHCP サーバスクリーニング機能を有効にすると、すべての DHCP サーバパケットが特定のポートでフィルタリングされます。

DHCP サーバ スクリーニンググローバル設定

DHCP サーバスクリーニンググローバル設定の表示、設定をします。

セキュリティ > DHCP サーバスクリーニング > DHCP サーバ スクリーニンググローバル設定の順にメニューをクリックして画面を表示します。

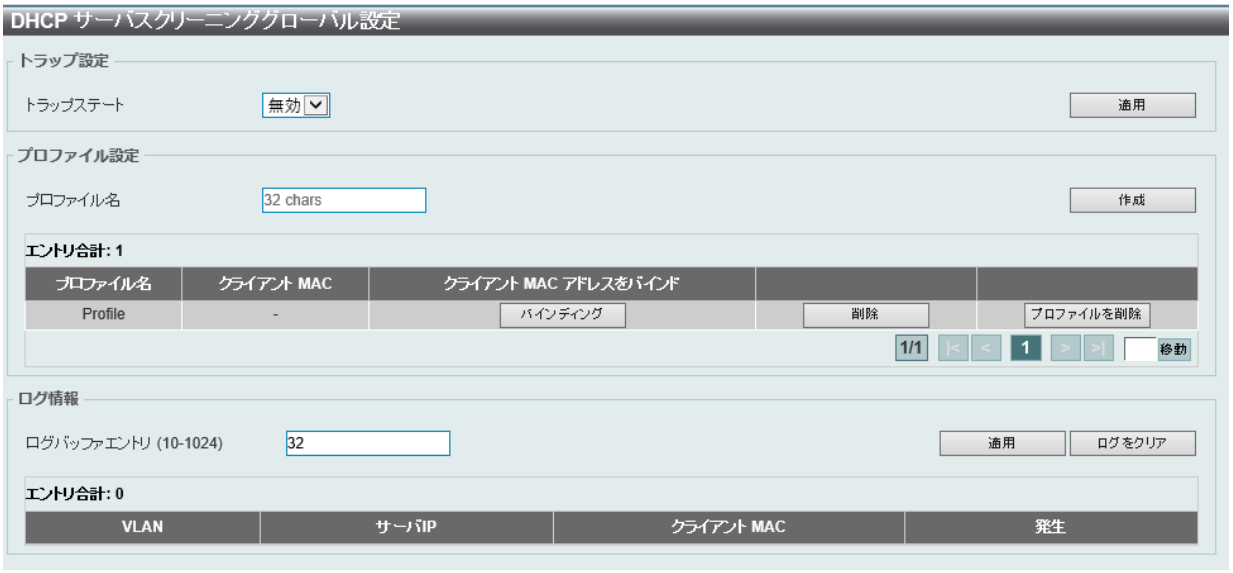


図 12-64　DHCP サーバ スクリーニンググローバル設定画面

画面に表示される項目：

トラップ設定

項目	説明
トラップステート	DHCP サーバスクリーニングトラップ機能を有効 / 無効に設定します。

「適用」をクリックし、設定内容を適用してください。

プロファイル設定

項目	説明
プロファイル名	DHCP サーバスクリーニングのプロファイル名を入力します。（32 文字以内）

「作成」をクリックし、設定内容にて作成します。
「削除」をクリックして指定エントリを削除します。
「プロファイルを削除」をクリックして指定プロファイルを削除します。

ログ情報

項目	説明
ログ情報	
ログバッファエントリ	ログバッファエントリ数を入力します。 • 設定可能範囲：10-1024 • 初期値：32

「適用」をクリックして、設定内容を適用します。
「ログをクリア」をクリックしてログを消去します。

「バインディング」をクリックすると以下の画面が表示されます。



図 12-65　クライアイント MAC アドレスをバインド画面

画面に表示される項目：

項目	説明
クライアント MAC	使用する MAC アドレスを指定します。

「適用」をクリックして、設定内容を適用します。

DHCP サーバ スクリーニングポート設定

DHCP サーバスクリーニングポートの表示、設定を行います。

セキュリティ > DHCP サーバスクリーニング > DHCP サーバ スクリーニングポート設定の順にメニューをクリックし、画面を表示します。



図 12-66　DHCP サーバ スクリーニングポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートでの DHCP サーバスクリーニング機能を有効 / 無効に設定します。
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	ポートに設定する DHCP サーバスクリーニングプロファイル名を入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、入力した情報に基づいて指定エントリを削除します。

ARP スプーフィング防止

ARP のスプーフィングを防止する設定を行うことができます。
エントリが作成されると、送信元 IP アドレスがエントリのゲートウェイ IP アドレスと一致するが、送信元 MAC アドレスフィールドがエントリのゲートウェイ MAC アドレスと一致しない ARP パケットは、システムにより破棄されます。

ARP スプーフィング防止機能は、送信元 IP アドレスが設定済みのゲートウェイ IP アドレスと一致しない ARP パケットをバイパスします。
ARP アドレスが設定されたゲートウェイの IP アドレス、MAC アドレスおよびポートリストと一致する場合、受信ポートが ARP で信頼されているかどうかに関係なく、動的 ARP インスペクション（DAI) チェックをバイパスします。

セキュリティ > ARP スプーフィング防止の順にメニューをクリックし、以下の画面を表示します。



図 12-67　ARP スプーフィング防止画面

画面に表示される項目：

項目	説明
ARP スプーフィング防止ログステート	
ARP スプーフィング防止ログステート	ARP スプーフィング防止ログのステータスを有効 / 無効に指定します。
ARP スプーフィング防止	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ゲートウェイ IP	ゲートウェイの IP アドレスを入力します。
ゲートウェイ MAC	ゲートウェイの MAC アドレスを入力します。

「適用」をクリックし、変更を有効にします。
「削除」をクリックして、指定エントリを削除します。

BPDU アタック防止

スイッチのポートに BPDU 防止機能を設定します。
通常、BPDU 防止機能には 2 つの状態があります。1 つは正常な状態で、もう 1 つはアタック状態です。

アタック状態には、3 つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信するとアタック状態に入ります。そして、設定に基づいてアクションを実行します。

BPDU 防止は、STP 機能における BPDU Forward 設定よりも高い優先度を持っています。つまり、ポートで BPDU Forward 設定が有効になっていても、BPDU 防止が有効である場合には、ポートは STP BPDU を転送しません。

また、BPDU 防止は BPDU トンネルポート設定よりも高い優先度を持っています。つまり、ポートが STP において BPDU トンネルポートとして設定されている場合、通常 STP BPDU を転送しますが、ポートで BPDU 防止が有効である場合には STP BPDU を転送しません。

セキュリティ > BPDU アタック防止の順にメニューをクリックし、以下の画面を表示します。



図 12-68　BPDU アタック防止画面

画面に表示される項目：

項目	説明
BPDU アタック防止グローバル設定	
BPDU アタック防止ステート	BPDU アタック防止機能を有効または無効にします。 • 初期値：無効
BPDU アタック防止トラップステート	トラップの状態を有効 / 無効に設定します。
BPDU アタック防止ポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	指定ポートに対して BPDU アタック防止を有効または無効にします。
モード	BPDU 防止モードを指定します。 •「破棄」- ポートがアタック状態に入ると、受信したすべての BPDU パケットを破棄します。 •「ブロック」- ポートがアタック状態に入るとすべてのパケット（BPDU と正常なパケットを含む）を破棄します。 •「シャットダウン」- ポートがアタック状態に入るとポートをシャットダウンします。

「適用」をクリックし、変更を有効にします。

NetBIOS フィルタリング

本項目では NetBIOS フィルタリングの設定、表示を行います。

セキュリティ > NetBIOS フィルタリングの順にメニューをクリックし、以下の画面を表示します。



図 12-69　NetBIOS フィルタリング画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
NetBIOS フィルタリングステート	指定ポートでの NetBIOS フィルタリングを有効 / 無効に指定します。 これにより物理ポートでの NetBIOS パケットが許可 / 拒否されます。
Extensive NetBIOS フィルタリングステート	指定ポートでの Extensive NetBIOS フィルタリングを有効 / 無効に指定します。 これにより物理ポートでの 802.3 フレーム上の NetBIOS パケットが許可 / 拒否されます。

「適用」をクリックし、変更を有効にします。

MAC 認証

MAC 認証機能は、MAC アドレスを使用してネットワークの認証を行う機能です。
本スイッチでは、ローカル認証方式、RADIUS サーバ認証方式の両方をサポートしています。
ローカルデータベースに基づいて認証を実行、または RADIUS クライアントとしてリモート RADIUS サーバとの間で RADIUS プロトコルを介して認証プロセスを実行します。

セキュリティ > MAC 認証の順にメニューをクリックし、以下の画面を表示します。



図 12-70　MAC 認証画面

画面に表示される項目：

項目	説明
MAC 認証グローバル設定	
MAC 認証ステート	MAC 認証のグローバルステータスを有効 / 無効に設定します。
MAC 認証トラップステート	MAC 認証のトラップのステータスを有効 / 無効に設定します。
MAC 認証ユーザ名 およびパスワード 設定	
ユーザ名	MAC 認証のユーザ名を入力します。（16 文字以内） 「初期値」にチェックを入れると、クライアントの MAC アドレスがユーザ名として指定されます。
パスワード	MAC 認証のパスワードを入力します。 「暗号化」にチェックを入れると、パスワードを暗号化します。 「初期値」にチェックを入れると、クライアントの MAC アドレスをパスワードとして指定します。
MAC 認証ポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	ポートの範囲を指定します。
状態	MAC 認証のポート指定を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

注意　MAC 認証において、Guest VLAN を有効にした際、端末のポート間の移動を許可する場合、インタフェースのイングレスチェック機能を無効にする必要があります。
ただし、IP Broadcast 以外（非 IP 環境）のパケット契機による、認証済みの MAC アドレスはポート間の移動不可となります。

。

Web アクセスコントロール

Web-based Access Control（WAC）は、ユーザがスイッチを経由してインターネットにアクセスを試みる際に、ユーザを認証する機能です。認証処理にはHTTP/HTTPS プロトコルが使用されます。ユーザがWeb ブラウザ経由でWebページ (例 : http://www.dlink.com) を閲覧しようとすると、スイッチは認証段階に進みます。スイッチにより HTTP/HTTPS パケットが検出され、ポートが未認証である場合、ユーザは認証ページにリダイレクトされます。認証処理が完了するまで、ユーザはインターネットにアクセスすることはできません。

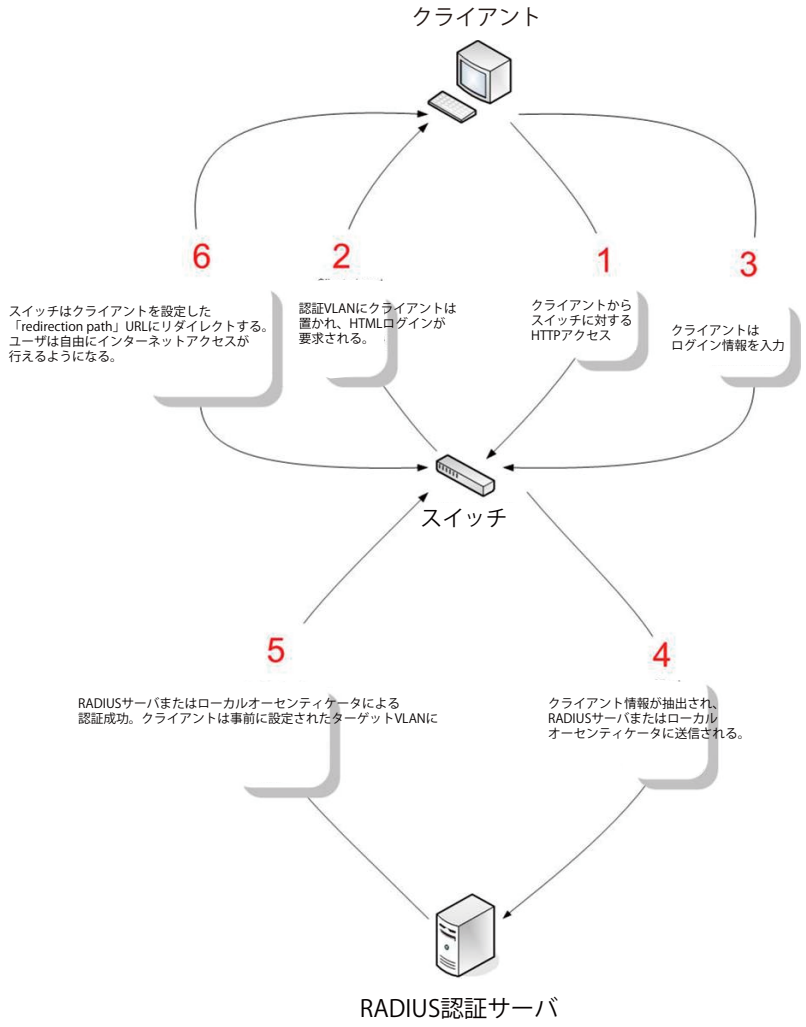
スイッチは、認証サーバとしてローカルデータベースに基づく認証を行うか、RADIUS クライアントとしてリモート RADIUS サーバ経由による RADIUS プロトコルを利用した認証処理を実行します。クライアントユーザが Web へのアクセスを試みると、WAC の認証処理が開始されます。D-Link の WAC の実行には、WAC 機能が排他的に使用している仮想 IP が使用されます。この IP アドレスは、スイッチの他のモジュールには認識されません。スイッチの他の機能への影響を避けるため、WAC は仮想 IP アドレスのみを使用してホストとの通信を行います。従って、すべての認証要求は、スイッチの物理インタフェースの IP アドレスではなく仮想 IP アドレスに送信される必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、この仮想 IP は、スイッチの物理的な IPIF（IP インタフェース）アドレスに変換されて通信が可能になります。ホスト PC や他のサーバの IP 構成は WAC の仮想 IP に依存しません。また、仮想 IP は、ICMP パケットや ARP リクエストに応答しません。つまり、仮想 IP は、スイッチの IPIF（IP インタフェース）と同じサブネット、またはホスト PC のサブネットと同じサブネットに設定することはできません。

認証された / 認証中のホストからの仮想 IP へのすべてのパケットは、スイッチの CPU で処理されます。そのため、仮想 IP が他のサーバや PC の IP アドレスと同じ場合、WAC が有効なポートに接続するホストは、その IP アドレスを実際に使用しているサーバや PC とは通信ができません。ホストがそれらのサーバや PC にアクセスする必要がある場合、仮想 IP をサーバや PC のアドレスと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、認証が適切に実行されるように、PC のユーザはプロキシの例外設定に仮想 IP を追加する必要があります。

スイッチの WAC 機能では、HTTP または HTTPS プロトコルに対し、ユーザ定義の TCP ポート番号を設定することができます。HTTP または HTTPS 用の TCP ポートは、認証処理において CPU で処理される HTTP /HTTPS パケットを識別したり、ログインページにアクセスしたりするために使用されます。ポート番号を指定しない場合、HTTP のポート番号の初期値は 80、HTTPS のポート番号の初期値は 443 となります。

次の図は、Web ベースのアクセスコントロールを実現させるために、認証に関わる各ノードで行われる基本の 6 つのステップを例示しています。



条件および制限

1. クライアントが IP アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サーバまたは DHCP リレー機能を持つ必要があります。
2. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。
   ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要な項目を入力して RADIUS サーバの設定を行ってください。

Web 認証

スイッチの Web 認証設定を行います。

セキュリティ > Web アクセスコントロール > Web 認証をクリックして、以下の画面から設定します。



図 12-71　Web 認証画面

画面に表示される項目：

項目	説明
Web 認証ステート	Web 認証機能のグローバルステータスを有効 / 無効に設定します。
トラップステート	Web 認証のトラップの状態を有効 / 無効に設定します。
仮想 IPv4	仮想 IP アドレスを入力します。 このアドレスは WAC にだけ使用され、スイッチの他のモジュールには知られません。 すべての Web 認証のプロセスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しません。そのため仮想 IP はスイッチやホスト PC のインタフェースと同じサブネットに設定することはできません。でなければ Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定された後、有効になります。仮想 IP アドレス取得のために DNS サーバにストアされた FQDN URL をユーザは取得します。取得した IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定されない場合、IPv4 は Web 認証を開始することができません。
仮想 IPv6	仮想 IPv6 アドレスを入力します。 仮想 IPv6 アドレスが設定されていない場合、IPv6 接続で Web 認証を開始することができません。
仮想 URL	仮想 URL を指定します。（128 文字以内）
リダイレクトパス	リダイレクトパスを入力します。（128 文字以内）

「適用」をクリックし、設定を有効にします。

注意　仮想 IP が設定されていないと WAC が正しく機能しないため、WAC 仮想 IP アドレスは、WAC を有効にする前に設定する必要があります。

注意　WAC 未認証時、DNS Over TCP はブロックします。

WAC ポート設定

WAC ポートの設定を行います。

セキュリティ > Web アクセスコントロール > WAC ポート設定の順にメニューをクリックし、以下の設定用画面を表示します。



図 12-72　WAC ポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	WAC 機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

WAC カスタマイズページ

認証ページの項目をカスタマイズします。

セキュリティ > Web アクセスコントロール > WAC カスタマイズページの順にメニューをクリックし、以下の画面を表示します。

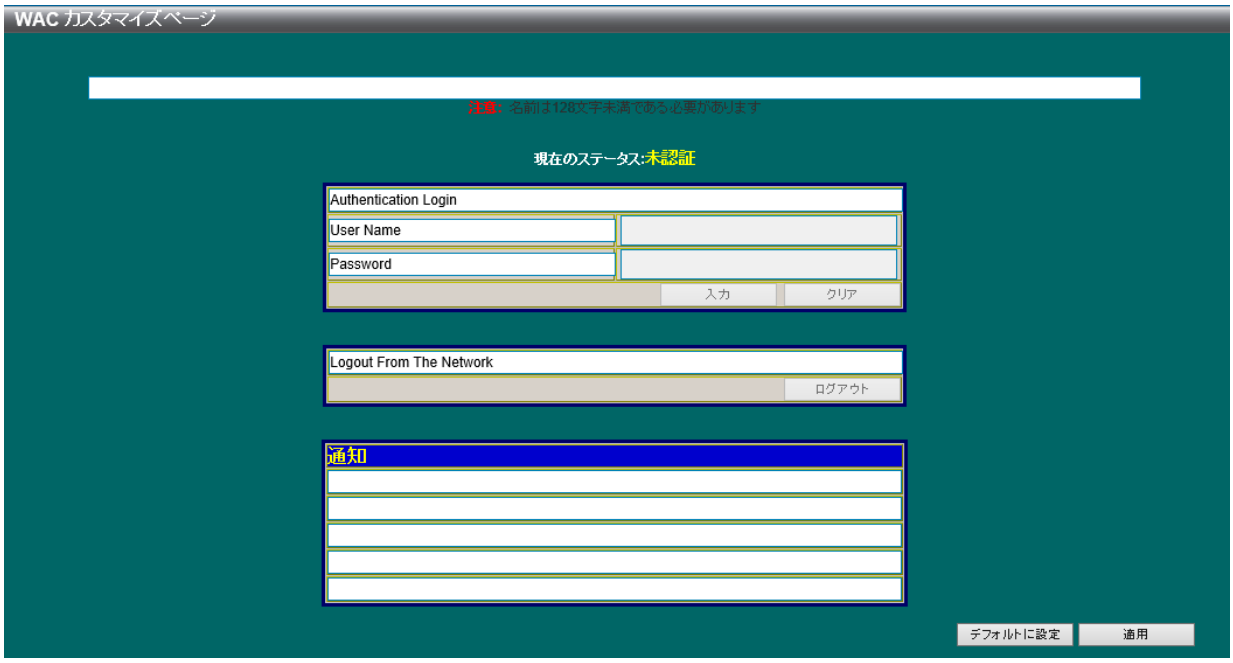


図 12-73　WAC カスタマイズページ画面

画面に表示される項目：

項目	説明
ページタイトル	ページのタイトルとなるメッセージを入力します。（128 文字以内）
ログインウィンドウタイトル	ログイン画面のタイトルを入力します。（64 文字以内）
ユーザ名 タイトル	ユーザ名項目のタイトルを入力します。（32 文字以内）
パスワードタイトル	パスワード項目のタイトルを入力します。（32 文字以内）
ログアウトウィンドウタイトル	ログアウト画面のタイトルを入力します。（64 文字以内）
通知	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

WAC ページの設定を行うには、この画面の WAC 認証情報をすべて入力し、「適用」をクリックして設定内容を適用します。
「デフォルトに設定」をクリックして、全項目を初期設定に復元します。

ネットワークアクセス認証

ネットワークアクセス認証の設定を行います。

ゲスト VLAN

ネットワークアクセス認証のゲスト VLAN の表示、設定を行います。

セキュリティ > ネットワークアクセス認証 > ゲスト VLAN の順にメニューをクリックし、以下の画面を表示します。

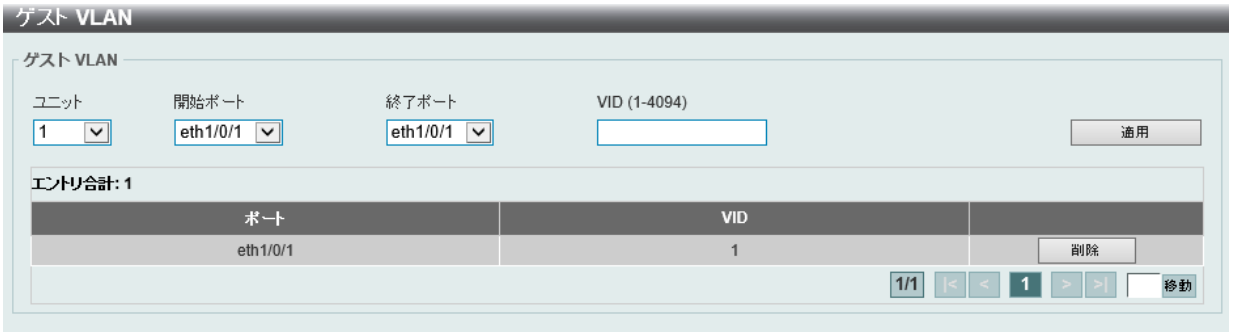


図 12-74　ゲスト VLAN 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
VID	設定する VLAN ID を入力します。 • 設定可能範囲：1-4094

「適用」をクリックし、設定を有効にします。
「削除」をクリックして、指定エントリを削除します。

ネットワークアクセス認証グローバル設定

ネットワークアクセス認証の設定を行います。

セキュリティ > ネットワークアクセス認証 > ネットワークアクセス認証グローバル設定 の順にメニューをクリックし、以下の画面を表示します。



図 12-75　ネットワークアクセス認証グローバル設定画面

画面に表示される項目：

項目	説明
ネットワークアクセス認証 MAC フォーマット設定	
ケース	ネットワークアクセス認証に使用する MAC アドレスの形式を選択します。 • 選択肢：「大文字」「小文字」
区切り文字	MAC アドレスを入力する際の区切りを選択します。区切り文字を使用しない場合は「なし」を選択します。 • 選択肢：「ハイフン」「ドット」「コロン」「なし」
区切り文字 番号	MAC アドレスにおける区切り数を選択します。 • 選択肢：「1」「2」「5」
General 設定	
最大ユーザ	最大ユーザ数を指定します。 • 設定可能範囲：1-1024 • 初期値：1024
MAC 移動を拒否	MAC 移動拒否機能の拒否を有効 / 無効に設定します。 本機能は、認証ホストが異なるポート間でローミングを実行できるようにするかを制御する機能です。 マルチ認証モードに設定されたポートで認証されたホストが別のポートに移動できるようにするかどうかのみを制御します。 ホストによる認証ポート間の移動には二つの状況が考えられます。次のルールに基づき、再認証を行うか、再認証を行うことなく新しいポートに直接移動する必要がある場合があります。 - 新しいポートの認証設定が元のポートと同じ場合、再認証は必要ありません。ホストは新しいポートに同じ許可属性を引き継ぎます。認証されたホストは、ポート 1 からポート 2 へのローミングを実行でき、再認証なしで許可属性を継承します。 - 新しいポートの認証設定が元のポートと異なる場合は、再認証が必要です。ポート 1 の認証済みホストは、ポート 2 に移動して再認証を行うことが可能です。新しいポートで認証方式が有効になっていない場合は、ステーションは新しいポートに直接移動します。元のポートとのセッションは削除されます。ポート 1 の認証済みホストは、ポート 2 に移動できます。 「MAC 移動を拒否」が有効の場合、「マルチ認証」「マルチホスト」いずれのモードにおいても破棄となります。 「MAC 移動を拒否」が無効の場合、それぞれのモードで動作が異なります。「マルチ認証」モードの場合は再認証なしのローミング、「マルチホスト」モードの場合は再認証有りの移動になります。 MAC 移動が無効になっていて、認証されたホストが別のポートに移動した場合、違反エラーとして認識されます。
許可ステート	認証時の許可について有効 / 無効に指定します。 本オプションについては権限設定の受容の有効 / 無効に使用されます。 認証に対して許可ステートが有効になっている場合、RADIUS サーバにより付与される権限属性（VLAN、802.1p default priority、bandwidth、ACL など）が許容されます。「Bandwidth」「ACL」はポートベースでアサインされます。マルチ認証モードの場合「VLAN」と「802.1p」は各ホストベースでアサインされます。それ以外の場合、「Bandwidth」と「ACL」はポートごとに割り当てられます。
ユーザ情報	
ユーザ名	ユーザ名を入力します。（32 文字以内）
VID	VLAN ID を入力します。
パスワード形式	パスワードの種類を選択します。 • 選択肢：「平文」「暗号化」
パスワード	パスワードを入力します。

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。

注意 Guest VLAN を有効にした際、端末のポート間の移動を許可するには、インタフェースのイングレスチェック機能を無効にする必要があります。（※「MAC 移動を拒否」が無効の場合でも、インタフェースのイングレスチェック機能を無効にする必要があります。）
ただし、IP Broadcast 以外（非 IP 環境）のパケット契機による、認証済みの MAC アドレスはポート間の移動不可となります。

ネットワークアクセス認証ポート設定

ネットワークアクセス認証のポート設定を行います。

セキュリティ > ネットワークアクセス認証 > ネットワークアクセス認証ポート設定の順にメニューをクリックし、以下の画面を表示します。

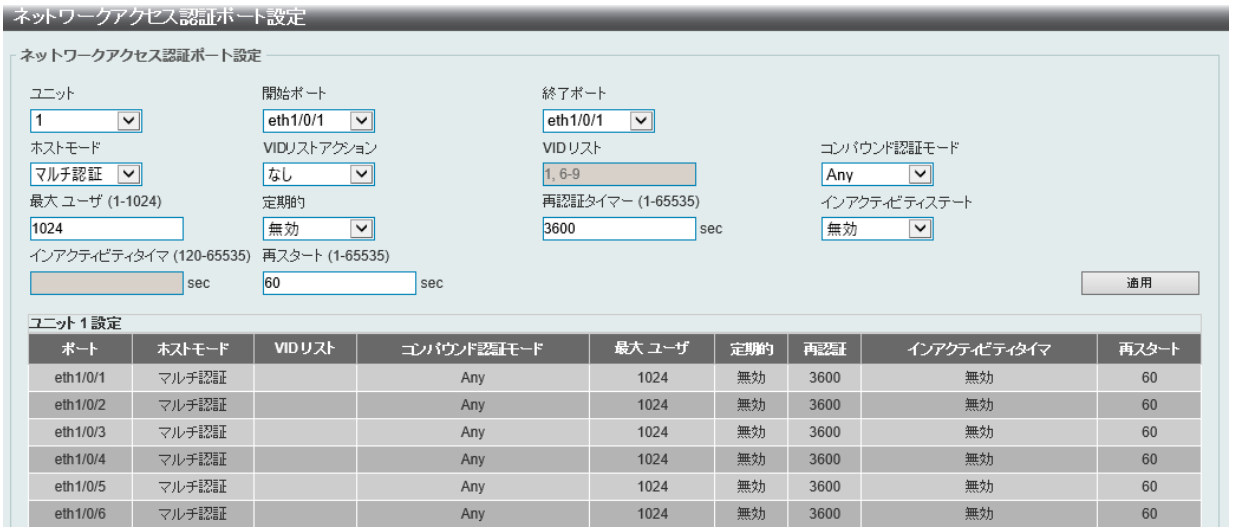


図 12-76　ネットワークアクセス認証ポート設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
ホスト モード	選択ポートに適用するホストモードを選択します。 • 「マルチホスト」- ポートがマルチホストモードで動作していて、1 つのホストがすでに認証されている場合、他のすべてのホストについてもポートへのアクセスが許可されます。802.1X 認証に従い、再認証失敗や認証ユーザのログオフなどが発生した場合、ポートはしばらくの間ブロックされます。一定の時間が過ぎると、EAPOL パケットの処理を元に戻します。 • 「マルチ認証」- ポートがマルチ認証モードで動作している場合、ポートにアクセスするには、各ホストは個別に認証する必要があります。ホストはその MAC アドレスで表されます。 許可されたホストのみがアクセスを許可されます。
VID リストアクション	VLAN リストに対するアクションを設定します。 • 選択肢：「なし」「追加」「削除」
VID リスト	ホストモードでマルチ認証オプションを選択すると、パラメータが有効になります。使用する VLAN ID を入力します。これは複数の認証要件があるスイッチ上で、複数の VLAN がある場合に有効です。クライアントが認証された後、クライアントは他の VLAN から受信しても再認証は必要とされません。このオプションは、トランクポートが VLAN ごとの認証制御を行う場合に便利です。ポートの認証モードがマルチホストに変更された場合、ポート上の以前の認証 VLAN はクリアされます。
コンパウンド認証モード	コンパウンド認証モードのオプションを選択します。 • 「Any」- あらゆる認証方式（802.1X、MAC-based Access Control、WAC）でのアクセスを指定します。 • 「MAC-WAC」-MAC ベースの認証を最初に検証します。クライアントがパスをすると、WAC が次に検証され、最終的には両方の認証をパスする必要があります。
最大ユーザ	最大ユーザ数を指定します。 • 設定可能範囲：1-1024
定期的	選択ポートの定期的な再認証を有効 / 無効に設定します。
再認証タイマー	再認証タイマを指定します。 • 設定可能範囲：1-65535（秒） • 初期値：3600（秒）
インアクティビティステート	非アクティブ状態を有効 / 無効に指定します。
インアクティビティ タイマ	非アクティブ状態を有効にした場合、非アクティブ時間の値を入力します。このパラメータは WAC の認証プロトコルにのみ影響します。 • 設定可能範囲：120-65535（秒）
再スタート	リスタート時間を入力します。 • 設定可能範囲：1-65535（秒）

「適用」をクリックし、設定を有効にします。

ネットワークアクセス認証セッション情報

ネットワークアクセス認証セッションの情報表示、クリアを行います。

セキュリティ > ネットワークアクセス認証 > ネットワークアクセス認証セッション情報の順にメニューをクリックし、以下の画面を表示します。

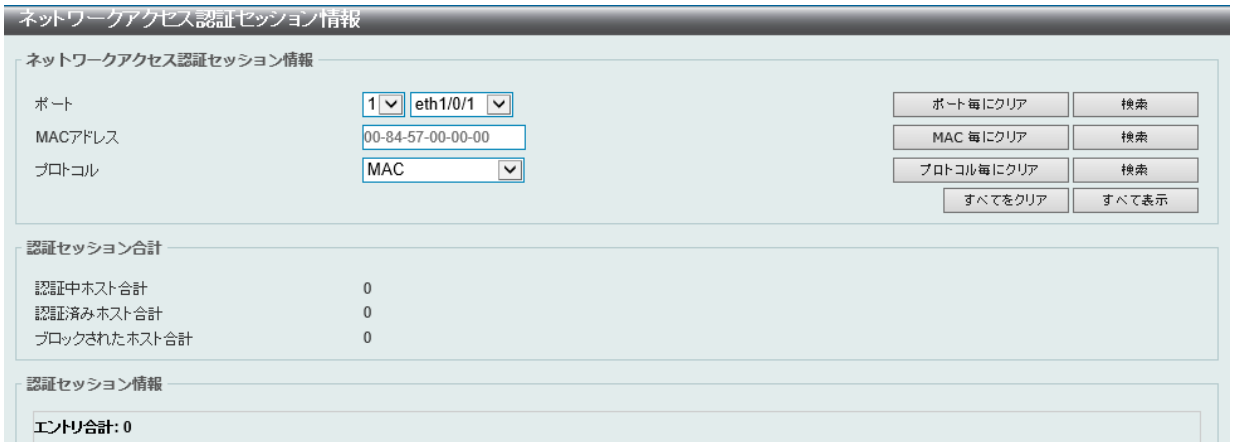


図 12-77　ネットワークアクセス認証セッション情報画面

画面に表示される項目：

項目	説明
ポート	表示 / クリアするポートとユニットを指定します。
MAC アドレス	表示 / クリアする MAC アドレスを指定します。
プロトコル	プロトコルオプションを選択します。 • 選択肢：「MAC」「WAC」「DOT1X」

情報の消去

「ポート毎にクリア」をクリックし、選択したポートに基づく情報を消去します。
「MAC 毎にクリア」をクリックし、選択した MAC アドレスに基づく情報を消去します。
「プロトコル毎にクリア」をクリックし、選択したプロトコルに基づく情報を消去します。
「すべてをクリア」をクリックし、テーブル上のすべての情報を消去します。

エントリの検出 / 表示

「検索」をクリックし、入力した情報を基に指定のエントリを検出します。
「すべて表示」をクリックし、すべてのエントリを表示します。

セーフガードエンジン

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング（ARP ストーム）などを利用して、周期的に攻撃してくることがあります。これらの攻撃により、スイッチの CPU 負荷は対応可能なキャパシティを超えて増大してしまう可能性があります。このような問題を軽減するために、本スイッチにはセーフガードエンジン機能が実装されています。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化してスイッチ全体の操作性を保ち、限られたリソース内で重要なパケットの送受信を可能にします。

CPU 負荷が上昇しきい値を超えると、セーフガードエンジン機能が作動し、スイッチは「Exhausted」モードに入ります。Exhausted モードでは、スイッチは ARP と IP パケットで使用可能な帯域を制限します。CPU 負荷がしきい値を下回った場合、セーフガードエンジンは動作を停止し、スイッチは Exhausted モードを脱却して通常モードへ移行します。

CPU 宛に送信されるパケットは 3 つのグループに分類されます。サブインタフェースとしても知られるこれらのグループは、CPU が特定の種類のトラフィックを識別するために使用する論理的なインタフェースです。この 3 つのグループは「プロトコル」「管理」「ルート」に分類されています。通常、スイッチの CPU が受信パケットを処理する際、「プロトコル」グループが最も高い優先度のパケットを受信し、（スイッチの CPU は基本的にルーティングパケットの処理を行うため）「ルート」グループは最も優先度の低いパケットを受信します。「プロトコル」グループで処理されるパケットは、ルータによって識別されたプロトコルコントロールパケットです。「管理」グループ内では、パケットは Telnet や SSH などの相互通信プロトコルによって、ルータやシステムネットワーク管理インタフェースへ送信されます。「ルート」グループで処理されるパケットは、一般にルータ CPU によって処理される通過ルーティングパケットとして認識されます。

以下の表ではプロトコルと対応するサブインタフェースを表示します。

プロトコル名	サブインタフェース（グループ）	概要
802.1X	Protocol	Port-based Network Access Control（ポートベースアクセスコントロール）
ARP	Protocol	Address resolution Protocol (ARP)
BGP	Protocol	Border Gateway Protocol
DHCP	Protocol	Dynamic Host Configuration Protocol（DHCP）
DNS	Protocol	Domain Name System（DNS）
DVMRP	Protocol	Distance Vector Multicast Routing Protocol
GVRP	Protocol	GARP VLAN Registration Protocol（GVRP）
ICMPv4	Protocol	Internet Control Message Protocol（ICMP）
ICMPv6-Neighbor	Protocol	IPv6 Internet Control Message Protocol Neighbor Discovery Protocol (NS/NA/RS/RA)（ICMPv6-Neighbor）
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)（ICMPv6-Other）
IGMP	Protocol	Internet Group Management Protocol（IGMP）
LACP	Protocol	Link Aggregation Control Protocol（LACP）
NTP	Protocol	Network Time Protocol
OSPF	Protocol	Open Shortest Path First
PIM	Protocol	Protocol Independent Multicast
PPPoE	Protocol	Point-to-point Protocol over Ethernet
RIP	Protocol	Routing Information Protocol
SNMP	Manage	Simple Network Management Protocol（SNMP）
SSH	Manage	Secure Shell（SSH）
STP	Protocol	Spanning Tree Protocol（STP）
Telnet	Manage	Telnet
TFTP	Manage	Trivial File Transfer Protocol（TFTP）
VRRP	Protocol	Virtual Router Redundancy Protocol
Web	Manage	Hypertext Transfer プ Protocol (HTTP) Hypertext Transfer Protocol Secure (HTTPS)

カスタマイズされたレートリミット（パケット / 毎秒）、をセーフガードエンジンのサブインタフェースに対してまとめてアサイン、または管理インタフェースで指定した個々のプロトコルに対してアサインすることが可能です。個々のプロトコルのレートリミットをカスタマイズする場合に注意しなければいけないのは、本機能を使用して不適切なレートリミットを設定すると、スイッチのパケットプロセスに異常をきたす場合があります。

注意 エンジンガードが有効になっている場合、CPU 使用率とトラフィック制限を制御するために、スイッチは FFP（高速フィルタプロセッサ）メータリングテーブルを使用して、さまざまなトラフィックフロー（ARP、IP）に帯域幅を割り当てます。これはネットワークを介してトラフィックをルーティングするスピードが制限される場合があります。

セーフガードエンジン設定

スイッチにセーフガードエンジンの設定を行います。

セキュリティ > セーフガードエンジン > セーフガードエンジン 設定の順にメニューをクリックし、以下の画面を表示します。

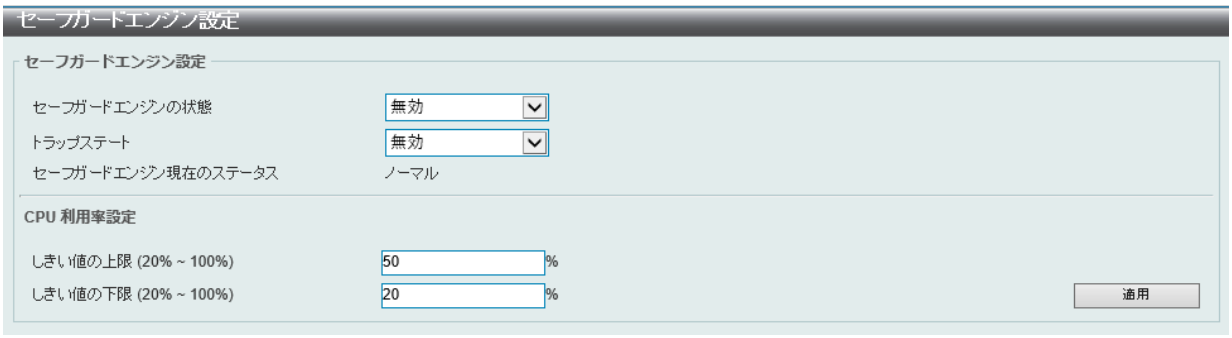


図 12-78　セーフガードエンジン 設定画面

画面に表示される項目：

項目	説明
セーフガードエンジン 設定	
セーフガードエンジンの状態	セーフガードエンジン機能を有効 / 無効に設定します。
トラップステート	セーフガードエンジントラップを有効 / 無効に設定します。
セーフガードエンジン現在のステータス	現在のセーフガードエンジンの状態を表示します。
CPU 利用率設定	
しきい値の上限	CPU 使用率の上限しきい値を設定します。 CPU 使用率がこのしきい値に到達すると、設定値に基づいて Exhausted モードに入ります。 • 設定可能範囲：20-100（%）
しきい値の下限	CPU 使用率の下限しきい値を設定します。 CPU 使用率がこのしきい値を下回ると、セーフガードエンジン状態から Normal モードに戻ります。 • 設定可能範囲：20-100（%）

「適用」をクリックして、設定内容を適用します。

CPU プロテクトカウンタ

CPU プロテクションのカウンタ情報を表示、消去します。

セキュリティ > セーフガードエンジン > CPU プロテクトカウンタの順にメニューをクリックし、以下の画面を表示します。

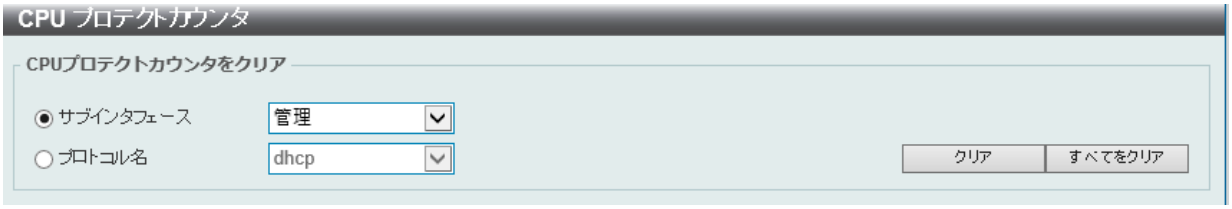


図 12-79　CPU プロテクトカウンタ画面

画面に表示される項目：

項目	説明
サブインタフェース	サブインタフェースのオプションを選択します。指定したサブインタフェースの CPU プロテクトカウンタをクリアします。 • 選択肢：「管理」「プロトコル」「ルート」「全て」
プロトコル名	プロトコル名のオプションを選択します。

「クリア」をクリックし、設定に基づいた情報を消去します。
「すべてをクリア」をクリックし、すべての情報を消去します。

CPU プロテクトサブインタフェース

CPU プロテクションのサブインタフェースを設定、表示します。

セキュリティ > セーフガードエンジン > CPU プロテクトサブインタフェースの順にメニューをクリックし、以下の画面を表示します。



図 12-80　CPU プロテクトサブインタフェース画面

画面に表示される項目：

項目	説明
CPU プロテクトサブインタフェース	
サブインタフェース	サブインタフェースのオプションを選択します。 • 選択肢：「管理」「プロトコル」「ルート」
レート制限	レートリミットの値を入力します。「無制限」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
サブインタフェース情報	
サブインタフェース	サブインタフェースのオプションを選択します。 • 設定可能範囲：「管理」「プロトコル」「ルート」

「適用」をクリックして、設定内容を適用します。
「検索」をクリックし、入力した情報を基に指定エントリを検出します。

CPU プロテクトタイプ

CPU プロテクションの種類の設定、表示します。

セキュリティ > セーフガードエンジン > CPU プロテクトタイプの順にメニューをクリックし、以下の画面を表示します。



図 12-81　CPU プロテクトタイプ画面

画面に表示される項目：

項目	説明
CPU プロテクトタイプ	
プロトコル名	プロトコル名のオプションを選択します。
レート制限	レートリミットの値を入力します。「無制限」を指定するとレートリミットを無効にします。 • 設定可能範囲：0-1024（パケット / 秒）
プロテクトタイプ情報	
タイプ	プロトコルタイプを選択します。プロトコルタイプの選択後、レートリミットの値が表示されます。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックし、入力した情報を基に指定エントリを検出します。

トラスト ホスト

トラストホストの設定、表示を行います。

セキュリティ > トラスト ホストの順にメニューをクリックし、以下の画面を表示します。



図 12-82　トラスト ホスト画面

画面に表示される項目：

項目	説明
ACL 名	使用する ACL 名を入力します。(32 文字以内)
タイプ	トラストホストの種類を指定します。 • 選択肢：「Telnet」「SSH」「Ping」「HTTP」「HTTPS」

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして指定のエントリを削除します。

トラフィック セグメンテーション

トラフィックセグメンテーションを設定します。
トラフィックセグメンテーション転送ドメインが指定されると、ポートで受信するパケットは、レイヤ 2 パケット転送においてドメイン内のインタフェースに制限されます。 ポートの転送ドメインが空の場合、ポートで受信したパケットのレイヤ 2 転送は制限されません。

トラフィックセグメンテーションのメンバリストは、同じ転送ドメインのポートとポートチャネルなど、異なるインタフェースタイプで構成できます。
指定されたインタフェースにポートチャネルが含まれている場合、このポートチャネルのすべてのメンバポートが転送ドメインに含まれます。

インタフェースに転送ドメイン設定されていない場合、ポートが受信したパケットのレイヤ 2 転送は制限されません。

セキュリティ > トラフィック セグメンテーション 設定の順にメニューをクリックし、以下の画面を表示します。



図 12-83　トラフィック セグメンテーション画面

画面に表示される項目：

項目	説明
ユニット	設定する受信スイッチユニットを指定します。
開始ポート / 終了ポート	設定する受信ポートの範囲を指定します。
転送ユニット	設定する転送スイッチユニットを指定します。
From 転送ポート / To 転送ポート	設定する転送ポートの範囲を指定します。

「追加」をクリックすると、入力した情報を基に新しいエントリを追加します。
「削除」をクリックすると、入力した情報を基にエントリを削除します。

ストーム制御設定

ストーム制御の設定、表示を行います。**セキュリティ > ストーム制御設定**の順にクリックします。



図 12-84　ストーム制御設定画面

画面に表示される項目：

項目	説明
ストームコントロールトラップ設定	
トラップステート	ストームコントロールトラップのオプションを指定します。 ・「なし」- トラップは送信されません。 ・「ストーム発生」- ストームの発生を検出した時点でトラップが通知されます。 ・「ストームクリア」- ストームが解消された時点でトラップが通知されます。 ・「両方」- ストームの発生を検出、またはストームが解消された時点でトラップが通知されます。
ストームコントロールポーリング設定	
ポーリング間隔	ポーリング間隔の値を指定します。 ・ 設定可能範囲：5-600（秒） ・ 初期値：5（秒
シャットダウン再試行	シャットダウンの再試行回数を入力します。「無限」にチェックを入れると本機能は無効になります。 ・ 設定可能範囲：0-360（回） ・ 初期値：3（回）
ストームコントロールポート設定	
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
タイプ	コントロールするストームの種類を選択します。 ・ 選択肢：「ブロードキャスト」「マルチキャスト」「ユニキャスト」 シャットダウンモードで選択すると、ユニキャストは「既知」「未知」両方を参照します。「既知」および「未知」のユニキャストパケットが指定されたしきい値に達すると、ポートはシャットダウンされます。それ以外の場合、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指定します。 ・「なし」- ストームパケットをフィルタしません。 ・「シャットダウン」- 指定したしきい値に達するとポートはシャットダウンされます。 ・「破棄」- 指定したしきい値に達するとパケットは破棄されます。
レベルタイプ	レベルタイプを指定します。 ・ 選択肢；「PPS」「Kbps」「レベル」
PPS 上昇	秒あたりのパケット量について上限しきい値を指定します。 ・ 設定可能範囲：0-2147483647（パケット / 秒）
PPS 低下	1 秒あたりのパケット量について下限しきい値を指定します。 ・ 設定可能範囲：0-2147483647（パケット / 秒） ・ 初期値：PPS 上昇 値の 80%

「適用」をクリックして、設定内容を適用します。

「レベルタイプ」で「Kbps」を選択すると、以下の画面が表示されます。



図 12-85　ストームコントロール (Kbps) 画面

画面に表示される項目：

項目	説明
KBPS 上昇	上限 KBPS の値を指定します。ポートで受信するトラフィックの上限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：0-2147483647（Kbps）
KBPS 低下	下限 KBPS の値を指定します。ポートで受信するトラフィックの下限しきい値をキロビット / 秒で指定します。 • 設定可能範囲：0-2147483647（Kbps） • 初期値：KBPS 上昇値の 80%

「適用」をクリックして、設定内容を適用します。

「レベルタイプ」で「レベル」を選択すると、以下の画面が表示されます。



図 12-86　ストームコントロール（レベル）画面

画面に表示される項目：

項目	説明
レベル 上昇	上限レベルについて入力します。 本オプションはポートで受信するトラフィックの総帯域の上限しきい値をパーセンテージとして指定します。 • 設定可能範囲：0-100（%）
レベル 低下	下限レベルについて入力します。 本オプションはポートで受信するトラフィックの総帯域の下限しきい値をパーセンテージとして指定します。 • 設定可能範囲：0-100（%） • 初期値：レベル 上昇値の 80%

「適用」をクリックして、設定内容を適用します。

注意　Multicast を指定した場合、予約 MAC Address（VRRP、OSPF、IGMP、MLD など）に対する制限は適用されません。

DoS 攻撃防御設定

各 DoS 攻撃に対して防御設定を行います。スイッチで検出可能な主な DoS タイプは以下のとおりです。

- Land Attack
  このタイプの攻撃には、送信元と宛先のアドレスがターゲットデバイスのアドレスに設定されている IP パケットが含まれます。ターゲットデバイスが連続的に応答する場合があります。
- Blat Attack
  このタイプの攻撃は、TCP/UDP ソースポートがターゲットデバイスの宛先ポートと等しいパケットを送信します。ターゲットデバイスがそれ自体に応答する可能性があります。
- TCP Null
  このタイプの攻撃には、シーケンス番号 0 とフラグなしを含む特定のパケットを使用したポートスキャンが含まれます。
- TCP Xmas
  このタイプの攻撃には、シーケンス番号 0 と緊急（URG）、プッシュ（PSH）、および FIN フラグを含む特定のパケットを使用したポートスキャンが含まれます。
- TCP SYN-FIN
  このタイプの攻撃には、SYN フラグと FIN フラグを含む特定のパケットを使用したポートスキャンが含まれます。
- TCP SYN SrcPort Less1024
  このタイプの攻撃には、ソースポート 0 ～ 1023、および SYN フラグを含む特定のパケットを使用したポートスキャンが含まれます。
- Ping of Death Attack
  Ping of Death Attack は、コンピュータに対する攻撃の一種で、不正な形式またはその他の悪意のある Ping をコンピュータに送信します。Ping のサイズは通常 64 バイトです（多くのコンピュータでは、最大 IP パケットサイズ（65535 バイト）より大きい Ping を処理できません）。このサイズの Ping を送信すると、ターゲット・コンピュータがクラッシュする可能性があります。従来、このバグは比較的簡単に悪用できました。一般に、65536 バイトの Ping パケットを送信することは、ネットワーキングプロトコルに従って不正ですが、このようなサイズのパケットは、フラグメント化される場合、送信される可能性があります。ターゲットコンピュータがパケットを再構成するとき、バッファオーバーフローが発生する可能性があり、システムクラッシュを引き起こす場合があります。
- TCP Tiny Fragment Attack
  Tiny TCP Fragment 攻撃者は、IP フラグメンテーションを使用して極端に小さいフラグメントを作成し、TCP ヘッダ情報を個別のパケットフラグメントに強制的に渡してルーターのチェック機能を通過させ、攻撃を実行します。
- すべてのタイプ : 上記のすべてのタイプ。

セキュリティ > DoS 攻撃防御設定の順にメニューをクリックし、以下の画面を表示します。

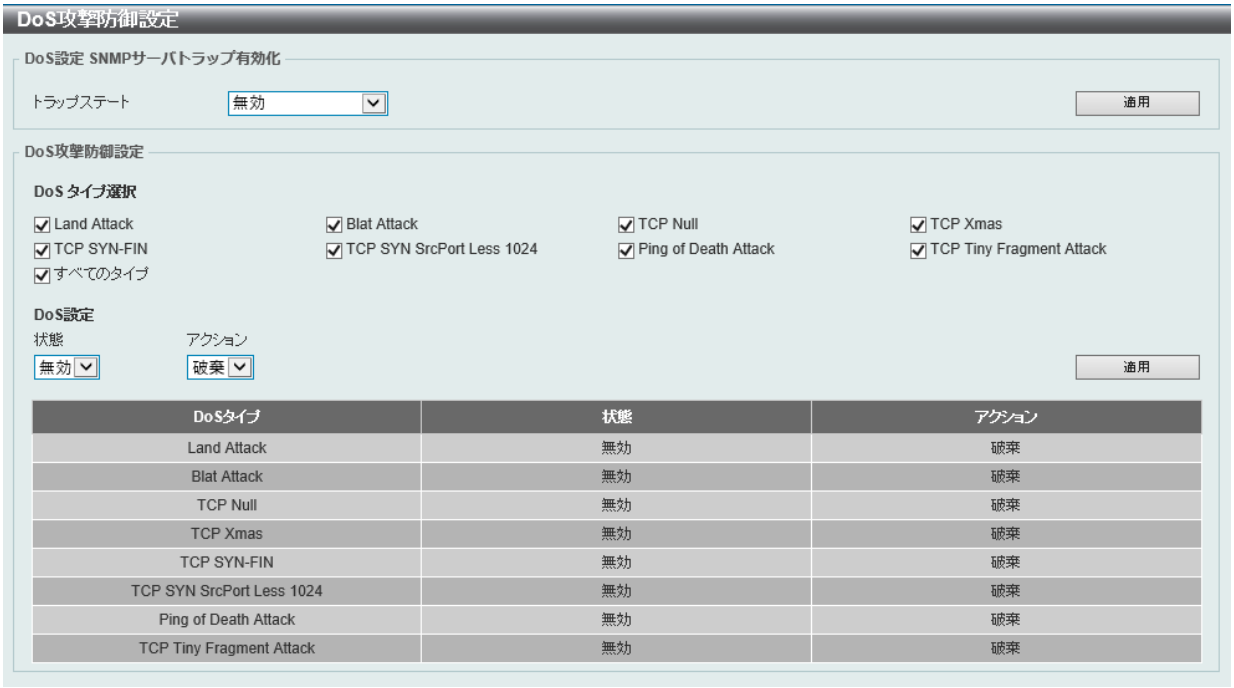


図 12-87　DoS 攻撃防御設定画面

画面に表示される項目：

項目	説明
DoS 設定 SNMP サーバトラップ有効化	
トラップステート	DoS 攻撃防止のトラップ状態を有効 / 無効に設定します。
DoS 攻撃防御設定	
DoS タイプ選択	適切な DoS 攻撃防御のタイプを選択します。
状態	DoS 攻撃防止の状態を有効 / 無効に指定します。
アクション	DoS 攻撃を検出したときに実行されるアクションを指定します。 • 「破棄」- 一致する DoS 攻撃パケットをすべて破棄します。

「適用」をクリックして、設定内容を適用します。

注意　本機能のご利用の際は、お客様がネットワーク上で利用するサービスに影響がないかを確認のうえ、十分に注意してご利用ください

ゾーンディフェンス設定

ゾーンディフェンス（Zone Defense）機能の設定を行います。
ゾーンディフェンスが有効な場合、ACL リソースがゾーンディフェンスのために使用されます。スイッチにゾーンディフェンス用の十分な ACL リソースがない場合は、本機能を有効にできません。

ゾーンディフェンスはネットワークトラフィックの異常がファイアウォールに設定したしきい値に到達すると実行されます。
この場合、ファイアウォールは即座にスイッチにコンタクトし、コマンドを実行します。その結果、疑いのあるホストからのあらゆるトラフィックをブロックします。

セキュリティ > ゾーンディフェンス設定の順にメニューをクリックし、以下の画面を表示します。

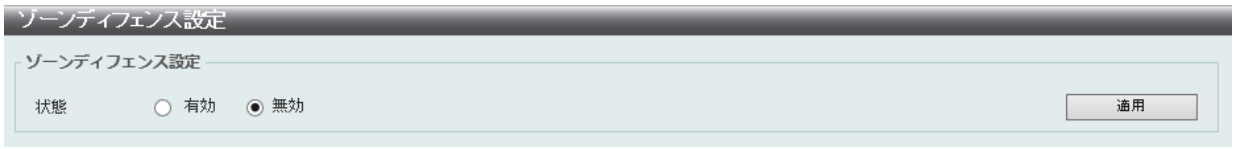


図 12-88　ゾーンディフェンス設定画面

画面に表示される項目：

項目	説明
状態	ゾーンディフェンス機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

SSH

SSH（Secure Shell）は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC（SSH クライアント）とスイッチ（SSH サーバ）間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. 「ユーザ アカウント 設定」で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH ユーザ 設定」画面を使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「ホストベース」、「パスワード」、「公開鍵」の 3 つがあります。
3. 「ホスト鍵」画面を使用して、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
4. 最後に「SSH グローバル設定」画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

SSH グローバル設定

SSH グローバル設定および設定内容の確認に使用します。

セキュリティ > SSH > SSH グローバル設定の順にメニューをクリックします。

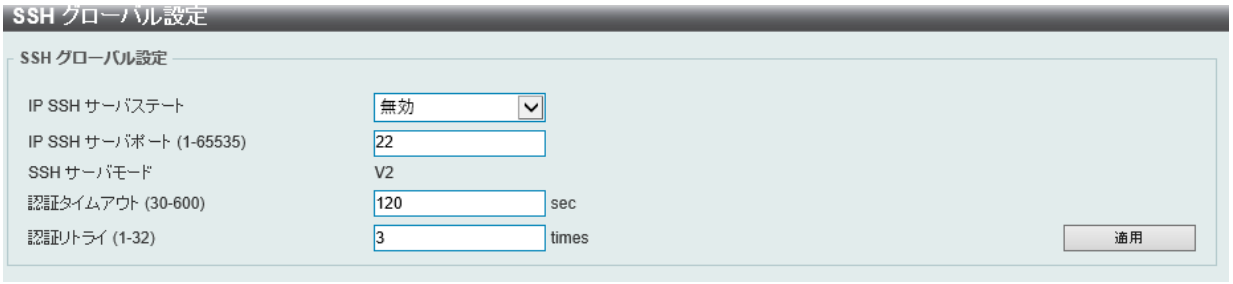


図 12-89　SSH グローバル設定画面

画面に表示される項目：

項目	説明
IP SSH サーバステート	SSH 機能のグローバルステータスを有効 / 無効に設定します。 • 初期値：「無効」
IP SSH サーバポート	SSH サーバポート番号を設定します。 • 設定可能範囲：1-65535 • 初期値：22
認証タイムアウト	認証のタイムアウト時間を指定します。 • 設定可能範囲：30-600（秒） • 初期値：120（秒）
認証リトライ	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。 指定した回数を超えると接続が切断され、ユーザは再度スイッチに接続する必要があります。 • 設定可能範囲：1-32 • 初期値：3

「適用」をクリックして、設定内容を適用します。

ホスト鍵

SSH ホスト鍵の設定および設定内容の確認に使用します。

セキュリティ > SSH > ホスト鍵の順にメニューをクリックし、以下の画面を表示します。

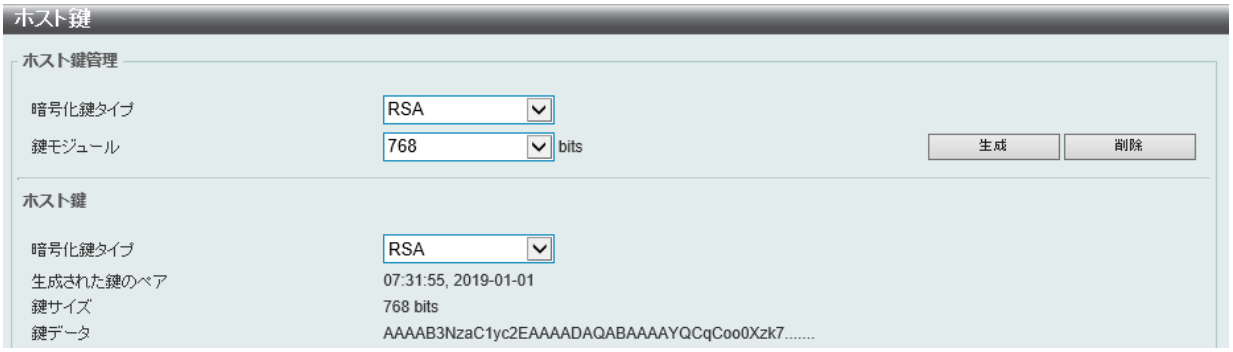


図 12-90　ホスト鍵画面

画面に表示される項目：

項目	説明
ホスト 管理	
暗号化鍵タイプ	暗号鍵の種類を選択します。 • 選択肢：「RSA」（Rivest Shamir Adleman）、「DSA」（Digital Signature Algorithm）
鍵モジュール	鍵係数の値を入力します。 • 選択肢：「360」「512」「768」「1024」「2048」（ビット）
ホスト鍵	
暗号化鍵タイプ	暗号鍵の種類を選択します。 • 選択肢：「RSA」（Rivest Shamir Adleman）、「DSA」（Digital Signature Algorithm）

「生成」をクリックし、指定したホスト鍵を有効にします。
「削除」をクリックし、指定したホスト鍵を削除します。

「生成」をクリックすると次の画面が表示されます。

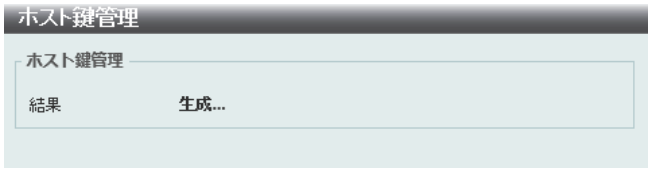


図 12-91　ホスト鍵（生成）画面

鍵の生成が完了すると次の画面が表示されます。

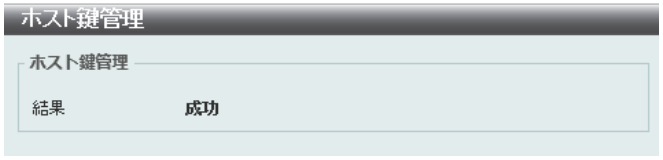


図 12-92　ホスト鍵（生成成功）画面

SSH サーバ接続

SSH サーバ接続テーブルの内容を確認します。

セキュリティ > SSH > SSH サーバ接続の順にメニューをクリックし、以下の画面を表示します。



図 12-93　SSH サーバ接続画面

表示されるエントリの内容を確認します。

SSH ユーザ設定

SSH ユーザの設定を行います。

セキュリティ > SSH > SSH ユーザ設定の順にメニューをクリックし、以下の画面を表示します。



図 12-94　SSH ユーザ設定画面

画面に表示される項目：

項目	説明
ユーザ名	SSH ユーザを識別するユーザ名を指定します。（32 文字以内）
認証方式	スイッチにアクセスを試みるユーザの認証モードを指定します。 • 選択肢：「パスワード」「公開鍵」「ホストベース」
鍵ファイル	「公開鍵」または「ホストベース」を選択した場合、公開鍵（Public Key）を入力します。
ホスト名	「ホストベース」を選択した場合、ホスト名を入力します。（255 文字以内）
IPv4 アドレス	「ホストベース」を選択した場合、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、IPv6 アドレスを入力します。

「適用」をクリックして、設定内容を適用します。
複数ページが存在する場合は、ページ番号を入力後、「移動」をクリックして、特定のページへ移動します。

SSH クライアント 設定

SSH クライアントの設定を行います。

セキュリティ > SSH > SSH クライアント 設定の順にメニューをクリックし、以下の画面を表示します。

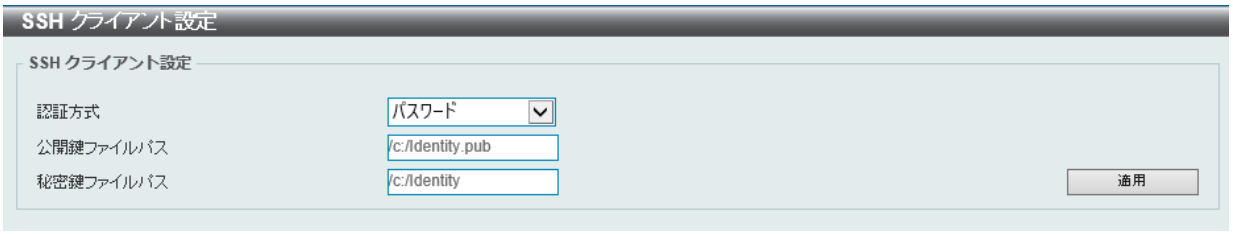


図 12-95　SSH クライアント 設定画面

画面に表示される項目：

項目	説明
認証方式	認証方法を選択します。 • 「パスワード」- ユーザアカウントに対してパスワード認証を行います。（初期値） • 「公開鍵」- ユーザアカウントに対して公開鍵（パブリックキー）認証を行います。このユーザの公開鍵として使用するローカルファイルの URL を入力します。
公開鍵ファイルパス	公開鍵（パブリックキー）として使用するローカルファイルのパスとファイル名を入力します。
秘密鍵ファイルパス	秘密鍵（プライベートキー）として使用するローカルファイルのパスとファイル名を入力します。

「適用」をクリックして、設定内容を適用します。

SSL

Secure Sockets Layer（SSL）とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、暗号スイートを使用して実現されます。暗号スイートは、認証セッションに使用される厳密な暗号化パラメータ、特定の暗号化アルゴリズム、およびキー長を決定するセキュリティ文字列であり、次の 3 つの段階で構成されます。

1. 鍵交換（Key Exchange）
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DSA、ここでは DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。これはクライアントとホスト間の最初の認証プロセスであり、「鍵交換」を行って一致した場合、認証が受諾され、以下のレベルで暗号化のネゴシエーションが行われます。
2. 暗号化（Encryption）
   暗号スイートの次の部分は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号（40 ビット鍵での RC4 と、128 ビット鍵での RC4）に対応しています。これらの鍵はメッセージの暗号化に使用され、最適に利用するためにはクライアントとホスト間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、1 つ前の暗号化テキストのブロックを使用して、現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義される 3 DES EDE 暗号化コードと高度な暗号化規格（AES）をサポートし、暗号化されたテキストを生成します。
3. ハッシュアルゴリズム（Hash Algorithm）
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージと共に暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA（Secure Hash Algorithm）、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 11 個の選択肢として独自に組み合わされ、サーバとクライアント間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。また、本スイッチは、TLSv1.0/1.1/1.2 をサポートしています。それ以外のバージョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

SSL 機能が有効化されると、通常の HTTP 接続はできなくなります。SSL 機能を使用した Web ベースの管理を行うには、SSL 暗号化がサポートされた Web ブラウザにおいて、https:// で始まる URL を使用する必要があります（例 : https://10.90.90.90）。これらの条件を満たさない場合、エラーが発生し、Web ベースの管理機能への接続認証が行われません。

SSL 機能で使用する証明書ファイルは TFTP サーバからスイッチへダウンロードすることができます。
証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者や認証のための鍵、デジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバ側とクライアント側で整合性のある証明書ファイルを保持している必要があります。スイッチには初期状態で証明書がインストールされていますが、ユーザ環境に応じて追加のダウンロードが必要な場合があります。

SSL グローバル設定

SSL グローバル設定を行います。

セキュリティ > SSL > SSL グローバル設定の順にメニューをクリックし、以下の画面を表示します。

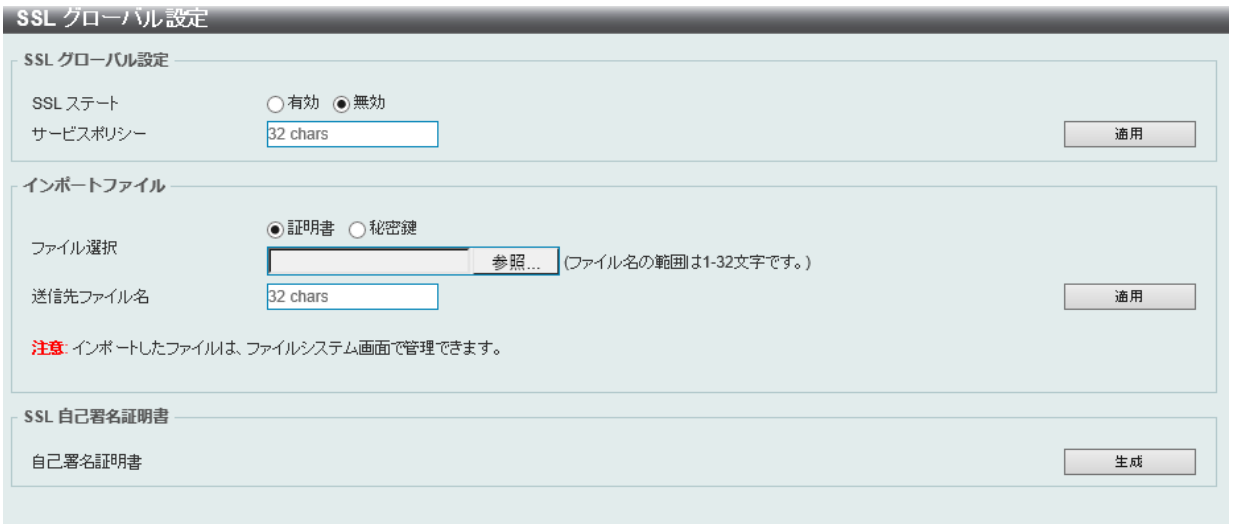


図 12-96　SSL グローバル設定画面

画面に表示される項目：

項目	説明
SSL グローバル設定	
SSL ステート	SSL のグローバルステータスを有効 / 無効に設定します。
サービスポリシー	SSL ポリシー名を入力します。（32 文字以内）
インポートファイル	
ファイル選択	ロードされるファイル種類を指定します。 ファイル種類を選択した後、「参照」をクリックして、適切なファイルを選択しローカルコンピュータからロードします。 • 選択肢：「証明書」「秘密鍵」
送信先ファイル名	宛先ファイル名を指定します。（32 文字以内）
SSL 自己署名証明書	
自己署名証明書	「生成」をクリックすると、組み込みの自己署名証明書があるかどうかに関係なく、新しい自己署名証明書が生成されます。生成された証明書は、ユーザが所有する証明書には影響しません。
送信先ファイル名	宛先ファイル名を指定します。（32 文字以内）

「適用」をクリックして、設定内容を適用します。

注意　SSL 自己署名証明書は、キー長が 2048 ビットの自己署名 RSA 証明書のみをサポートします。

暗号化 PKI トラストポイント

暗号 PKI トラストポイントの表示、設定を行います。

セキュリティ > SSL > 暗号化 PKI トラストポイントの順にメニューをクリックし、以下の画面を表示します。

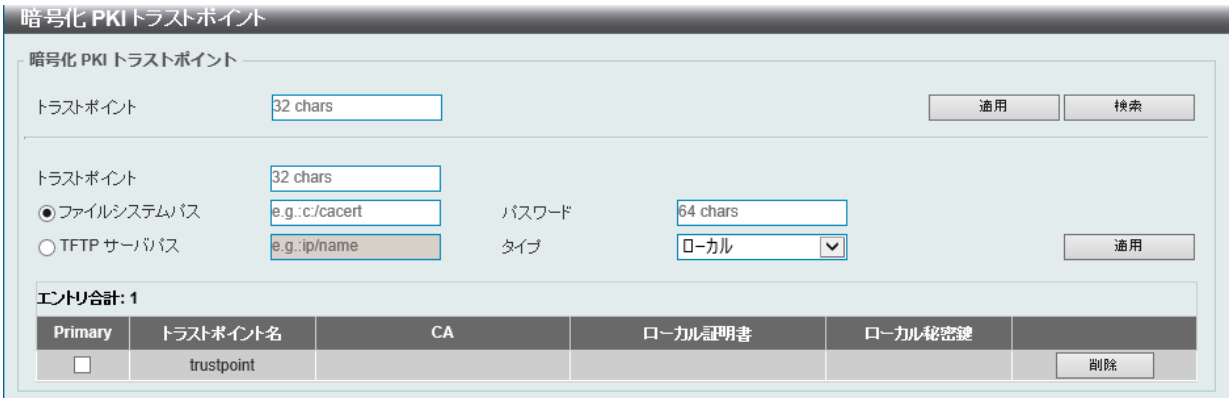


図 12-97　暗号化 PKI トラストポイント画面

画面に表示される項目：

項目	説明
トラストポイント	インポートした証明書と鍵ペアに対応するトラストポイント名を入力します。(32 文字以内)
ファイルシステムパス	証明書と鍵ペアのファイルシステムパスを入力します。
パスワード	インポートしたプライベート鍵の暗号を解除する暗号パスフレーズを入力します。(64 文字以内) パスフレーズが指定されないと「NULL」文字列が使用されます。
TFTP サーバパス	TFTP サーバのパスを指定します。
タイプ	インポートされる証明書の種類を選択します。 • 「両方」-「CA 証明書」「ローカル証明書と鍵ペア」をインポートします。 • 「CA」-「CA 証明書」のみインポートします。 • 「ローカル」-「ローカル証明書と鍵ペア」のみインポートします。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づいて指定エントリを検出します。
「削除」をクリックして、指定エントリを削除します。

SSL サービスポリシー

SSL サービスポリシーの表示、設定を行います。

セキュリティ > SSL > SSL サービスポリシーの順にメニューをクリックし、以下の画面を表示します。

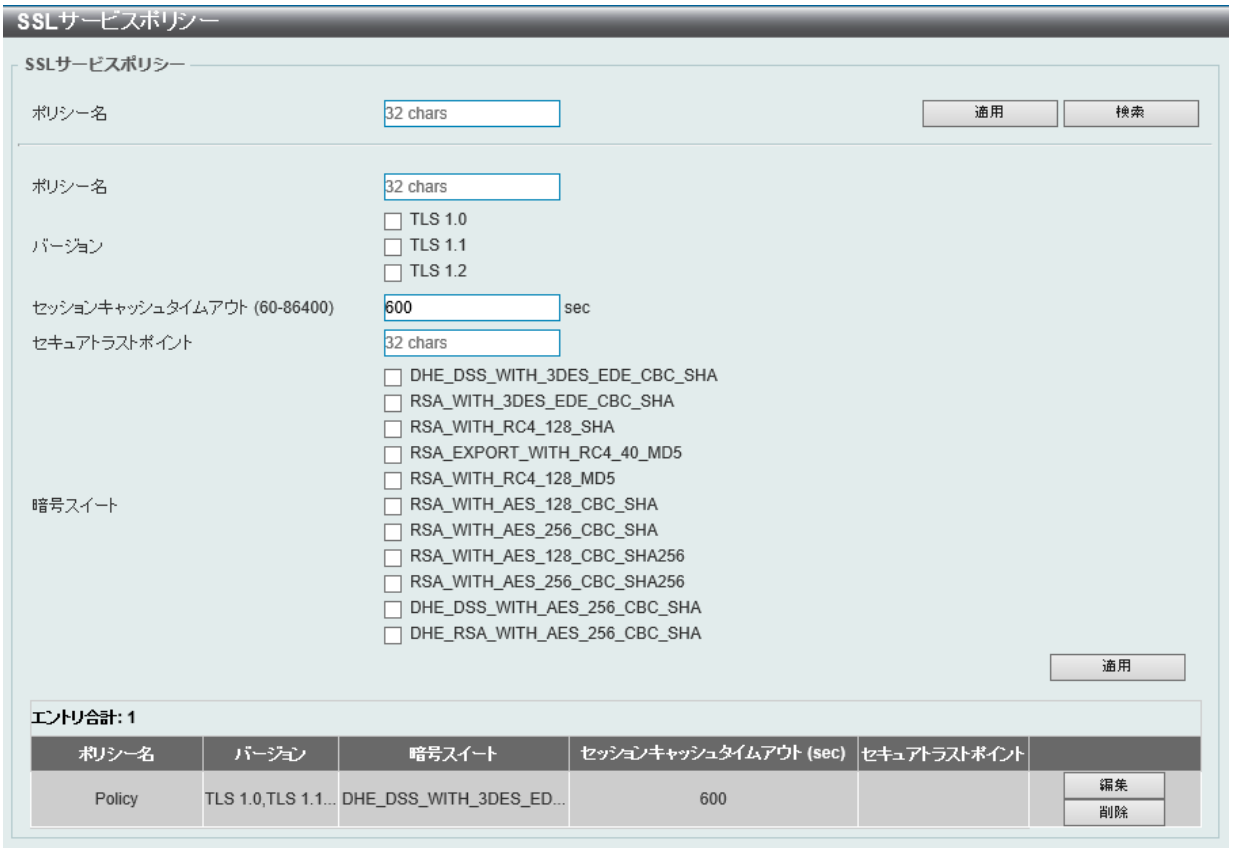


図 12-98　　SSL サービスポリシー画面

画面に表示される項目：

項目	説明
ポリシー名	SSL サービスポリシー名を入力します。（32 文字以内）
バージョン	「Transport Layer Security」(TLS) のバージョンを指定します。 • 選択肢：「TLS 1.0」「TLS 1.1」「TLS 1.2」
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タイムアウトの時間を指定します。 • 設定可能範囲：60-86400（秒） • 初期値：600（秒）
セキュアトラストポイント	セキュアなトラストポイントの名前を入力します。（32 文字以内）
暗号スイート	本プロファイルの暗号スイートを選択します。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報に基づいて指定エントリを検出します。
「編集」をクリックして、指定エントリを編集します。
「削除」をクリックして、指定エントリを削除します。

SFTP サーバ設定

本項目では「Secure File Transfer Protocol」(SFTP) サーバの設定、表示を行います。
SFTP は信頼できるデータストリームにおけるリモートでセキュアなファイルトランスファープロトコルです。
SFTP はそれ自身で認証や、セキュリティを提供しないため、SFTP サーバを SSH サーバのサブシステムとして構築させる必要があります。

セキュリティ > SFTP サーバ設定の順にメニューをクリックし、以下の画面を表示します。

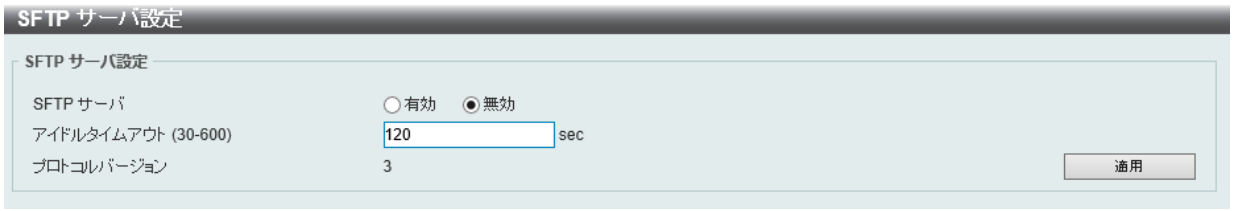


図 12-99　SFTP サーバ設定画面

画面に表示される項目：

項目	説明
SFTP サーバ	SFTP サーバを有効 / 無効に設定します。
アイドルタイムアウト	アイドルタイムアウトの時間を設定します。 指定したセッションアイドルタイマー後、SFTP サーバが動作を検出しない場合、SFTP セッションは終了します。 • 設定可能範囲：30-600（秒） • 初期値：120（秒）

「適用」をクリックして、設定内容を適用します。

ネットワークプロトコルポートプロテクション設定

本項目ではネットワークプロトコルポートプロテクションの設定、表示を行います。

セキュリティ > ネットワークプロトコルポートプロテクション設定 の順にメニューをクリックし、以下の画面を表示します。



図 12-100 ネットワークプロトコルポートプロテクション設定 画面

画面に表示される項目：

項目	説明
TCP ポートプロテクションステート	TCP ポートネットワークプロトコルプロテクション機能を有効 / 無効に設定します。
UDP ポートプロテクションステート	UDP ポートネットワークプロトコルプロテクション機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。

第 13 章　OAM (Operations, Administration, Maintenance：運用・管理・保守)

以下は OAM サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
ケーブル診断	スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。
DDM	Digital Diagnostic Monitoring（DDM）機能を実行します。スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定 (温度しきい値設定、電圧しきい値設定など) を行うことができます。

ケーブル診断

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は UTP ケーブルを簡易的に確認するために設計されています。ケーブルの品質やエラーの種類を診断します。

注意　ケーブル診断機能は簡易機能であり、参考としてご利用ください。正確な検査やテストのためには専用のテスタを使用して行ってください。

OAM > ケーブル診断の順にメニューをクリックし、以下の画面を表示します。



図 13-1　ケーブル診断画面

特定のポートに対するケーブル診断を表示するには、プルダウンメニューを使用して設定するユニットとポートを選択し、「テスト」ボタンをクリックします。情報が画面に表示されます。

「クリア」ボタンをクリックし、指定ポートの情報を消去します。
「すべてをクリア」ボタンをクリックし、テーブル上のすべての情報を消去します。

注意　ケーブル診断を実行すると、対象のポートにおいてリンクダウンを伴います。

■ ケーブル診断機能の制限

- GE ポートのみサポート
- 最大対応ケーブル長 120 メートル
- ケーブル長の誤差± 5 メートル
- より正確な結果を得るには、RJ-45 コネクタで TIA/EIA-568B ピンアサインを使用

■ 障害メッセージ

- Open - UTP ケーブルが断線しているか、接続が外れています。
- Short - UTP ケーブルでショートが発生しています。
- Crosstalk - UTP ケーブルと他のケーブルとのクロストークが発生しています。
- Unknown - ケーブルスのテータスを取得できません。再試行してください。
- NA - ケーブルが見つかりませんでした。ケーブルが診断仕様外であるか、品質が悪い可能性があります。

DDM

本フォルダにはスイッチに Digital Diagnostic Monitoring（DDM）機能を実行する画面があります。これらの画面により、スイッチに挿入した SFP/SFP+ モジュールの DDM 状態の参照、各種設定を行うことができます。

DDM 設定（DDM 設定）

超過しているアラームしきい値または警告しきい値を超過するイベントが発生した場合に、指定ポートに行う動作を設定します。

OAM > DDM > DDM 設定の順にメニューをクリックし、以下の画面を表示します。



図 13-2　DDM 設定画面

画面に表示される項目：

項目	説明
DDM グローバル設定	
トランシーバモニタリング アラームトラップ	アラームしきい値を超過した際にトラップを送信するか否かを指定します。
トランシーバモニタリング 警告トラップ	警告しきい値を超過した際にトラップを送信するか否かを指定します。
DDM シャットダウン設定	
ユニット	設定するユニットを選択します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
状態	DDM の状態を有効 / 無効に設定します。
シャットダウン	動作パラメータが「アラーム」または「警告」しきい値を超過した際に、ポートをシャットダウンするかどうかを指定します。 • 「アラーム」- アラームしきい値を超過した場合にポートをシャットダウンします。 • 「警告」- 警告 しきい値を超過した場合にポートをシャットダウンします。 • 「なし」- しきい値の超過に関わらずシャットダウンは実行されません。（初期値）

「適用」をクリックして、設定内容を適用します。

DDM 温度閾値設定

スイッチの特定ポートに DDM 温度しきい値設定を行います。

OAM > DDM > DDM 温度閾値設定の順にメニューをクリックし、以下の画面を表示します。



図 13-3　DDM 温度閾値設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニット番号を指定します。
ポート	設定するポートを指定します。
アクション	実行するアクションを指定します。 • 選択肢：「追加」「削除」
タイプ	温度しきい値の種類について指定します。 • 「低 アラーム」「低 警告」「高 アラーム」「高 警告」
値	温度しきい値を指定します。 • 「-128」-「127.996」（℃）

「適用」をクリックして、設定内容を適用します。

DDM 電圧閾値設定

スイッチの特定ポートに電圧しきい値を設定します。

OAM > DDM > DDM 電圧閾値設定 の順にメニューをクリックし、以下の画面を表示します。



図 13-4　DDM 電圧閾値設定 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニット番号を指定します。
ポート	設定するポートを指定します。
アクション	実行するアクションを指定します。 • 選択肢：「追加」「削除」
タイプ	電圧しきい値の種類について指定します。 • 「低 アラーム」「低 警告」「高 アラーム」「高 警告」
値	電圧しきい値を指定します。 • 設定可能範囲：0 - 6.55（V）

「適用」をクリックして、設定内容を適用します。

DDM バイアス電流閾値設定

スイッチの特定ポートにバイアス電流しきい値を設定します。

OAM > DDM > DDM バイアス電流閾値設定の順にメニューをクリックし、以下の画面を表示します。



図 13-5　DDM バイアス電流閾値設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニット番号を指定します。
ポート	設定するポートを指定します。
アクション	実行するアクションを指定します。 • 選択肢：「追加」「削除」
タイプ	バイアス電流しきい値の種類について指定します。 • 「低 アラーム」「低 警告」「高 アラーム」「高 警告」
値	バイアス電流しきい値を指定します。 • 設定可能範囲：0-131（mA）

「適用」をクリックして、設定内容を適用します。

DDM TX パワー閾値設定

スイッチの特定ポートに送信電力しきい値を設定します。

OAM > DDM > DDM TX パワー閾値設定 の順にメニューをクリックし、以下の画面を表示します。



図 13-6　DDM TX パワー閾値設定 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニット番号を指定します。
ポート	設定するポートを指定します。
アクション	実行するアクションを指定します。 • 選択肢：「追加」「削除」
タイプ	送信電力しきい値の種類について指定します。 • 選択肢：「低 アラーム」「低 警告」「高 アラーム」「高 警告」
パワーユニット	送信電力単位について指定します。 • 選択肢：「mW」「dBm」
値	送信電力しきい値の値について指定します。 • 設定可能範囲： 「0」-「6.5535」（mW） 「-40」-「8.1647」（dBm）

「適用」をクリックして、設定内容を適用します。

DDM RX パワー 閾値設定

スイッチの特定ポートに受信電力しきい値を設定します。

OAM > DDM > DDM RX パワー 閾値設定の順にメニューをクリックし、以下の画面を表示します。



図 13-7　DDM RX パワー 閾値設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニット番号を指定します。
ポート	設定するポートを指定します。
アクション	実行するアクションを指定します。 • 選択肢：「追加」「削除」
タイプ	受信電力しきい値の種類について指定します。 • 「低 アラーム」「低 警告」「高 アラーム」「高 警告」
パワーユニット	受信電力の単位を指定します。 • 選択肢：「mW」「dBm」
値	受信電力しきい値を指定します。 • 選択肢： 「0」-「6.5535」（mW） 「-40」-「8.1647」（dBm）

「適用」をクリックして、設定内容を適用します。

DDM ステータステーブル

指定ポートで現在操作中の DDM パラメータと SFP モジュールの値を表示します。

OAM > DDM > DDM ステータステーブルの順にメニューをクリックし、以下の画面を表示します。



図 13-8　DDM ステータステーブル画面

画面に表示される項目：

項目	説明
ポート	ポート番号を表示します。
温度	ポートの現在の温度を表示します。
電圧	ポートの現在の電圧を表示します。
バイアス電流	ポートの現在のバイアス電流を表示します。
TX 出力	ポートの現在の送信電力を表示します。
RX パワー	ポートの現在の受信電力を表示します。

第 14 章　モニタリング

モニタリングメニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

以下はモニタリングサブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
VLAN カウンタ	VLAN カウンタの設定を行います。L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。
利用率	スイッチの利用率（利用分析）を表示します。
統計	スイッチの統計（統計情報）を表示します。
ミラー設定	ミラーリング機能の設定を行います。本スイッチは対象ポートで送受信するフレームをコピーし、フレームの出力先を他のポートに変更する機能（ポートミラーリング）があります。
sFlow	sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。
デバイス環境	デバイス環境（機器環境確認）ではスイッチの内部の温度状態を表示します。

VLAN カウンタ

本画面では、VLAN カウンタの設定、表示を行います。
指定の L2 VLAN インタフェースにおけるトラフィック統計のコントロールエントリを指定します。

モニタリング > VLAN カウンタの順にメニューをクリックし、以下の画面を表示します。



図 14-1　VLAN カウンタ画面

画面に表示される項目：

項目	説明
VALN カウンタ設定	
VLAN インタフェース	VLAN インタフェース を指定します。 • 設定可能範囲：1-4094
ユニット	設定するユニットを選択します。
開始ポート / 終了ポート	設定するポートのを範囲を指定します。「全て」を指定すると全ポートを指定します。
フレームタイプ	フレームタイプを指定します。 • 「ブロードキャスト」- ブロードキャストフレームのみをカウントします。 • 「マルチキャスト」- マルチキャストフレームのみをカウントします。 • 「ユニキャスト」- ユニキャストフレームのみをカウントします。 • 「Any」- フレームタイプに関係なく全てのフレームをカウントします。 • 「全て」- 上記全てのフレームをカウントします。
トラフィックの方向	トラフィックの向きを指定します。 • 「RX」- イングレストラフィックを指定します。 • 「TX」- イーグレストラフィックを指定します。 • 「両方」- 両方のトラフィックをカウントします。
VLAN カウンタテーブル	
VLAN インタフェース	VLAN インタフェース を指定します。「全て」を指定するとすべての VLAN を指定します。 • 設定可能範囲：1-4094
トラフィックの方向	トラフィックの向きを指定します。 • 「RX」- イングレストラフィックを指定します。 • 「TX」- イーグレストラフィックを指定します。 • 「両方」- 両方のトラフィックをカウントします。

「適用」をクリックして、設定内容を適用します。
「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「削除」をクリックして、指定したエントリを削除します。

利用率

CPU 使用率、ポートの帯域使用率などを表示します。

ポート利用率

本画面では、ポートの帯域使用率を表示します。

モニタリング > 利用率 > ポート利用率の順にメニューをクリックし、以下の画面を表示します。

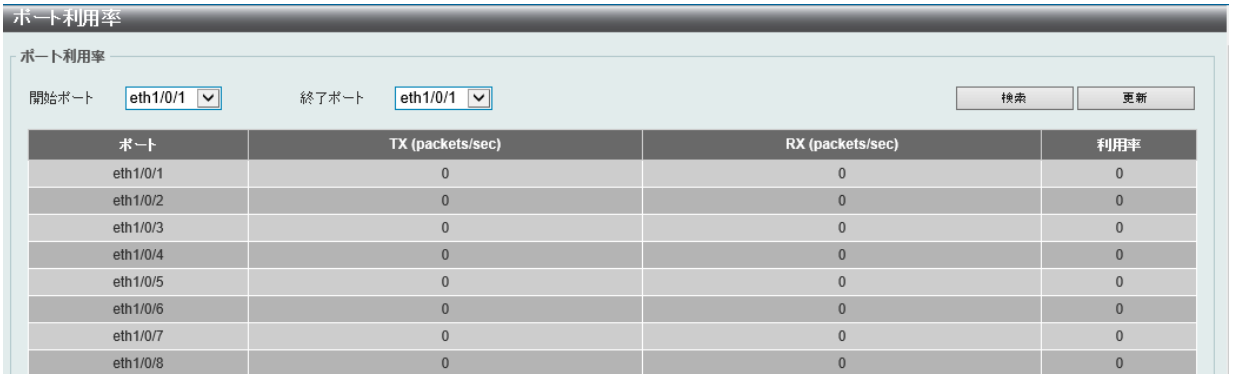


図 14-2　ポート利用率画面

画面に表示される項目：

項目	説明
ユニット	ポート使用率を表示するユニットを指定します。
開始ポート / 終了ポート	ポート使用率を表示するポート範囲を指定します。

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「更新」をクリックして、テーブルを更新します。

履歴利用率

本項目ではメモリ、CPU およびポートの使用履歴について表示します。

モニタリング > 利用率 > 履歴利用率の順にメニューをクリックし、以下の画面を表示します。



図 14-3　履歴利用率（メモリ）画面



図 14-4　履歴利用率（CPU）画面



図 14-5　履歴利用率（ポート）画面

画面に表示される項目：

項目	説明
タイプ	表示する使用履歴の種類を指定します。 • 「メモリ」- メモリの使用履歴を表示します。 • 「CPU」- CPU の使用履歴を表示します。 • 「ポート」- ポートの使用履歴を表示します。
ユニット	使用履歴を表示するユニットを指定します。
開始ポート / 終了ポート	使用履歴を表示するポート範囲を指定します。
時間ベース	表示する統計情報の期間を指定します。 • 「15 Minutes」- 15 分間の使用情報を表示します。 • 「1 Day」- 1 日の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1Day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。 • 選択肢： 「全て」「1」「2」「3」「4」「5」（15 Minutes 選択時） 「全て」「1」「2」（1 Day 選択時）

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。

統計

スイッチの統計情報を表示します。

ポート

ポートのパケット情報を表示します。

モニタリング > 統計 > ポートの順にメニューをクリックし、以下の画面を表示します。

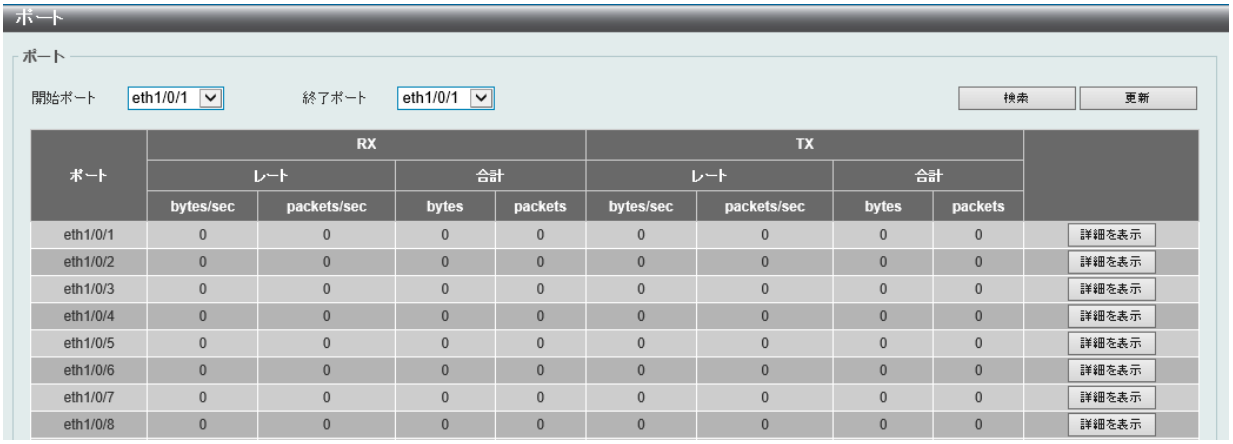


図 14-6　ポート画面

画面に表示される項目：

項目	説明
ユニット	表示するユニットを選択します。
開始ポート / 終了ポート	表示するポートの範囲を指定します。

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「更新」をクリックして、テーブルを更新します。
「詳細を表示」をクリックして、指定ポートの詳細情報について表示します。

「詳細を表示」をクリックすると以下の画面が表示されます。

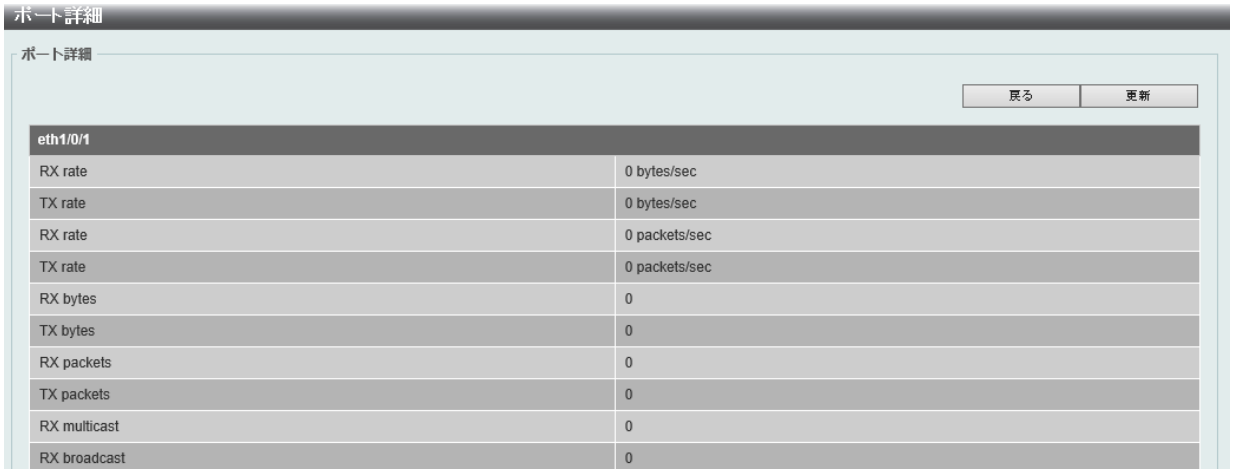


図 14-7　ポート詳細画面

「更新」をクリックして、テーブルを更新します。
「戻る」をクリックして、前の画面に戻ります。

CPU ポート

CPU の統計情報について表示します。

モニタリング > 統計 > CPU Port の順にメニューをクリックし、以下の画面を表示します。

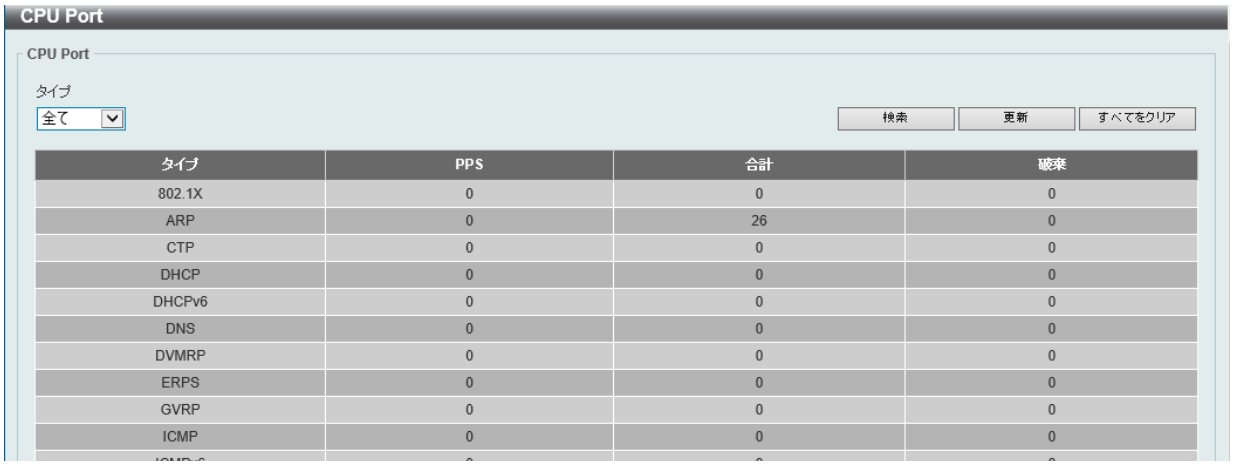


図 14-8　CPU Port 画面

画面に表示される項目：

項目	説明
タイプ	表示する情報のタイプを指定します。 • 選択肢：「全て」「L2」「L3」「プロトコル」

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「更新」をクリックして、テーブルを更新します。
「すべてをクリア」をクリックして、テーブル上のすべての情報を消去します。

インタフェースカウンタ

インタフェースカウンタ情報について表示します。

モニタリング > 統計 > インタフェースカウンタの順にメニューをクリックし、以下の画面を表示します。

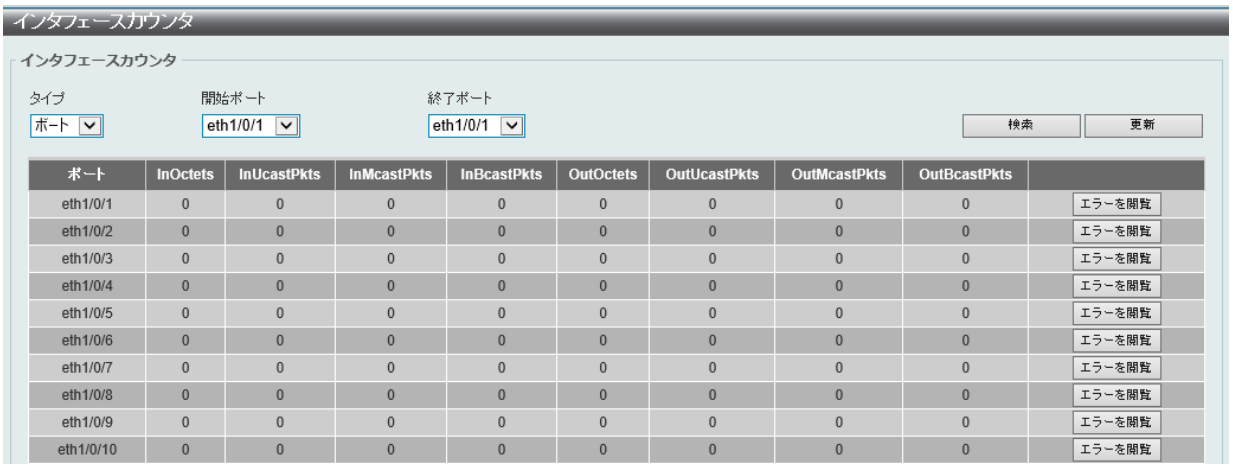


図 14-9　インタフェースカウンタ画面

画面に表示される項目：

項目	説明
タイプ	表示する情報のタイプを指定します。 • 選択肢：「ポート」「VLAN」
ユニット	表示するユニットを選択します。
開始ポート / 終了ポート	表示するポートの範囲を指定します。

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「更新」をクリックして、テーブルを更新します。
「エラーを閲覧」をクリックすると、指定ポートのエラー情報について表示します。

「エラーを閲覧」をクリックすると、次の画面が表示されます。

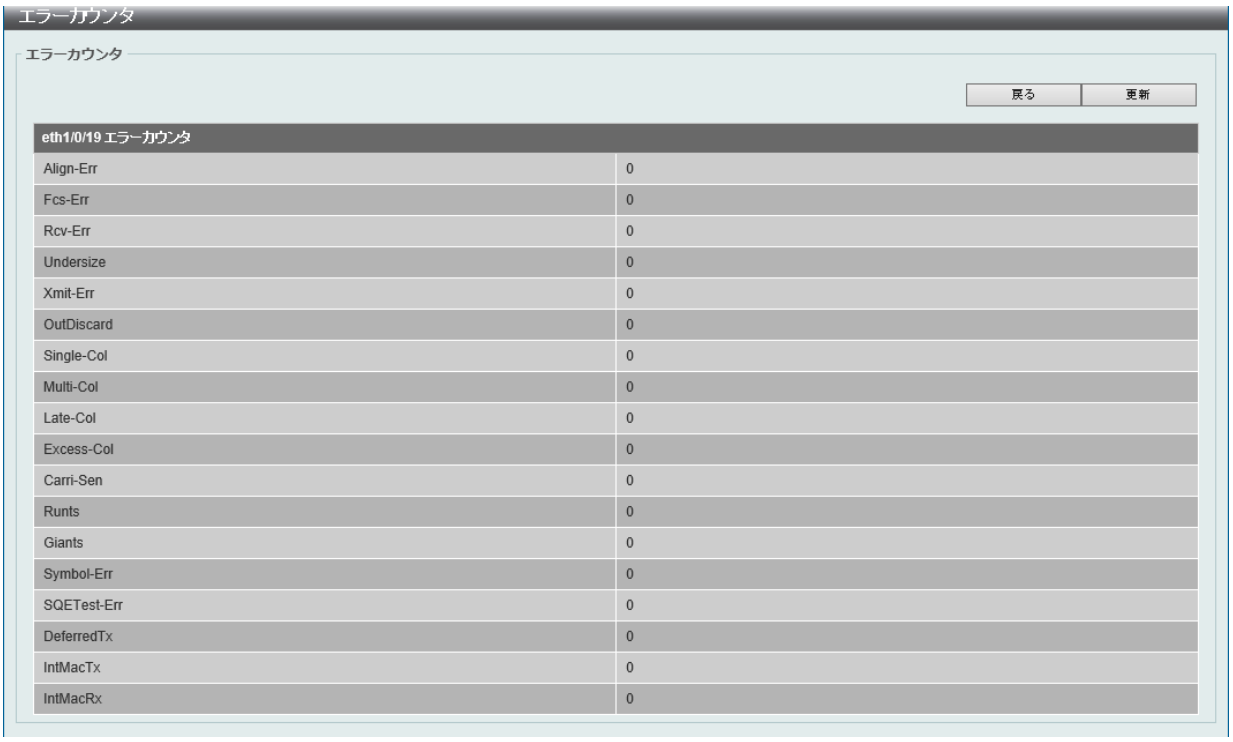


図 14-10　エラーカウンタ画面

「戻る」をクリックすると前のページに戻ります。
「更新」をクリックして、テーブルを更新します。

「タイプ」で「VLAN」を選択すると、次の画面が表示されます。

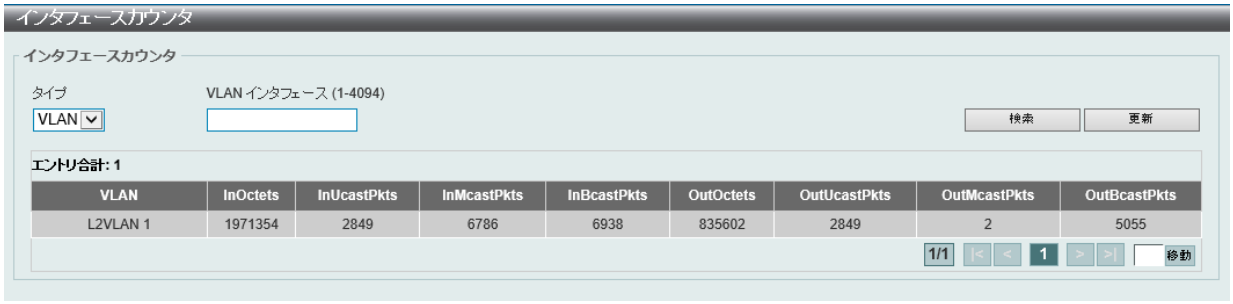


図 14-11　インタフェースカウンタ（VLAN）画面

画面に表示される項目：

項目	説明
タイプ	表示する情報のタイプを指定します。 • 選択肢：「ポート」「VLAN」
VLAN インタフェース	表示する VLAN ID を指定します。

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「更新」をクリックして、テーブルを更新します。

インタフェース履歴カウンタ

本項目ではインタフェースにおけるカウンタの履歴を表示します。

モニタリング > 統計 > インターフェイス履歴カウンタの順にメニューをクリックし、以下の画面を表示します。



図 14-12　インターフェイス履歴カウンタ画面

画面に表示される項目：

項目	説明
タイプ	表示する情報のタイプ指定します。 • 選択肢：「ポート」
ユニット	表示するユニットを選択します。
ポート	表示するポートを指定します。
時間ベース	表示する統計情報の期間を指定します。 • 「15 Minutes」- 15 分間の使用情報を表示します。 • 「1 Day」- 1 日の使用情報を表示します。 「15 Minutes」を選択すると「Slot1」は 15 分前から現在までの情報を表示し、「Slot2」は 30 分前から 15 分前までの情報を表示します。「1Day」を選択すると「Slot1」は 24 時間前から現在までの情報を表示し、「Slot2」は 48 時間前から 24 時間前までの情報を表示します。
Slot Index	スロットのインデックスを指定します。 • 選択肢： 「1」「2」「3」「4」「5」（15 Minutes 選択時） 「1」「2」（1 Day 選択時）

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。

カウンタ

すべてのポートのカウンタ情報を表示、消去します。

モニタリング > 統計 > カウンタの順にメニューをクリックし、以下の画面を表示します。

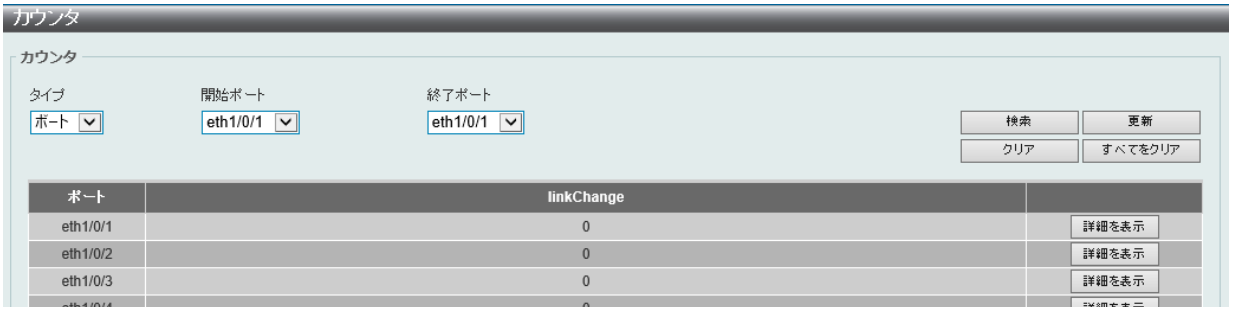


図 14-13　カウンタ（ポート選択時）画面

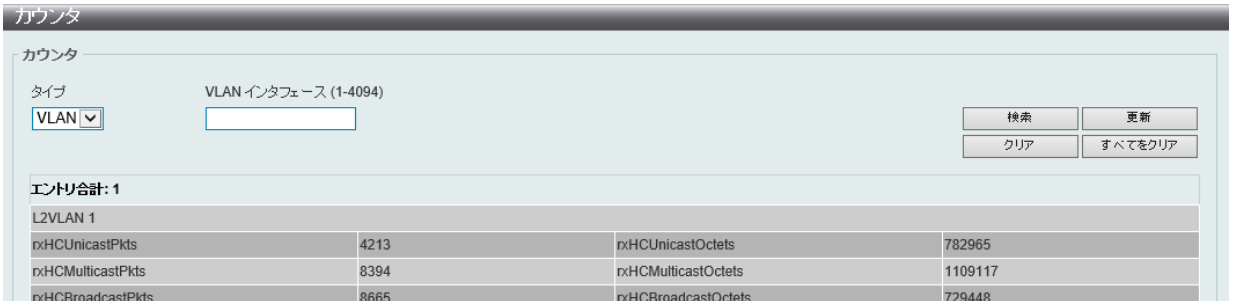


図 14-14　カウンタ（VLAN 選択時）画面

画面に表示される項目：

項目	説明
タイプ	表示するタイプを指定します。 • 「ポート」- ポート毎のカウンタを表示します。 • 「VLAN」- VLAN 毎のカウンタを表示します。
ユニット	「ポート」を選択した場合、表示するユニットを指定します。
開始ポート / 終了ポート	「ポート」を選択した場合、表示するポートの範囲を指定します。
VLAN インタフェース	「VLAN」を選択した場合、表示する VLAN インタフェース を指定します。 • 設定可能範囲：1-4094

「検索」をクリックして、入力した情報を基に指定のエントリを検出します。
「更新」をクリックして、テーブルを更新します。
「クリア」をクリックして、指定ポートの情報を消去します。
「すべてをクリア」をクリックして、テーブル上のすべての情報を消去します。

詳細情報の表示（ポート毎のカウンタ画面）

「詳細を表示」をクリックすると以下の画面が表示されます。

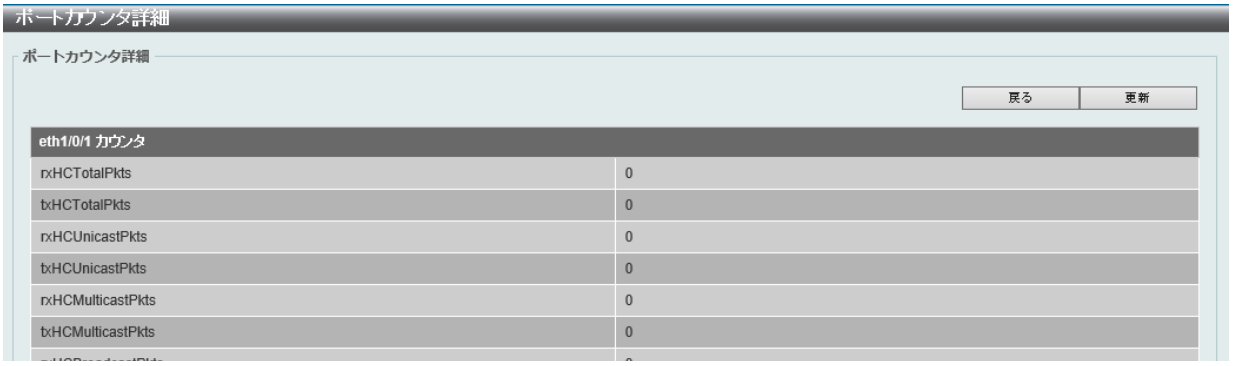


図 14-15　ポートカウンタ詳細画面

「更新」をクリックして、テーブルを更新します。
「戻る」をクリックして、前の画面に戻ります。

ミラー設定

ミラーリング機能についての設定、表示を行います。本スイッチは対象ポートで送受信するフレームをコピーして、そのコピーしたフレームの出力先を他のポートに変更する機能（ポートミラーリング）を持っています。ミラーリングポートに監視機器（スニファや RMON probe など）を接続し、最初のポートを通したパケットの詳細を確認することができます。トラブルシューティングやネットワーク監視の目的において適しています。

モニタリング > ミラー設定をクリックします。

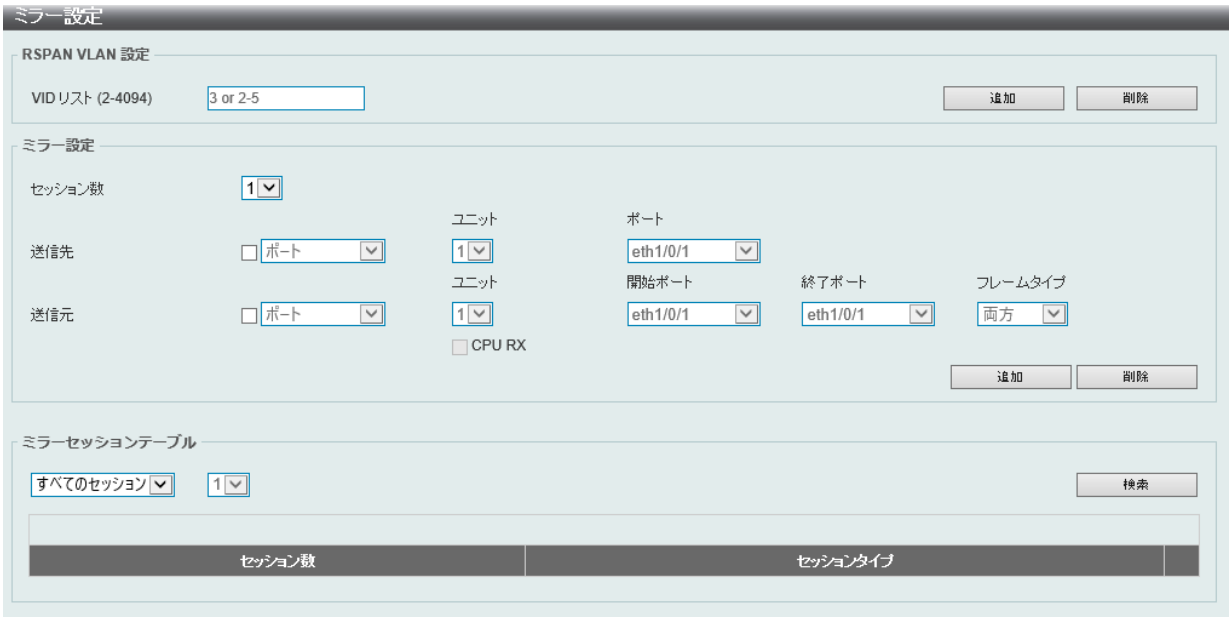


図 14-16　ミラー設定画面

画面に表示される項目：

項目	説明
RSPAN VLAN 設定	
VID リスト	VLAN ID のリストを指定します。
ミラー設定	
セッション数	このエントリのセッション番号を指定します。 • 設定可能範囲：1-4
送信先	チェックボックスにチェックを入れ、ポートミラーエントリの宛先タイプを設定します。 •「ポート」-「ポート」を選択した後に、宛先ユニットやポート番号を指定します。 •「リモート VLAN」-「リモート VLAN」を選択した後に、宛先ユニットやポート番号を指定し、「VID」（2-4094）も指定します。
送信元	チェックボックスにチェックを入れポートミラーエントリの送信元について設定します。 •「ポート」-「ポート」を選択した後に、「ユニット ID」「開始 ポート」「終了ポート」の番号を指定します。 最後に「フレームタイプ」オプションを指定します。 「フレームタイプ」で指定可能なオプションは「両方」「RX」「TX」「TX 転送」です。 「両方」を選択すると送受信どちらのトラフィックもミラーされます。 「RX」の場合、受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。 「CPU RX」オプションにチェックを入れると、CPU RX トラフィックを監視します。 •「ACL」- ACL 名を入力します。 •「VLAN」-「VLAN」を選択した後に、「VID リスト」を指定し、フレームタイプを選択します。 •「リモート VLAN」-「リモート VLAN」を選択した後に「VID」（2-4094）を指定します。
ミラーセッションテーブル	
ミラーセッションタイプ	表示する情報のミラーセッションタイプを選択します。 • 選択肢：「すべてのセッション」「セッション数」「リモートセッション」「ローカルセッション」 「セッション数」を選択した後、ドロップダウンメニューからセッション番号（1-4）を選択します。

「追加」をクリックして、入力した情報に基づいた新規のミラーエントリを追加します。
「削除」をクリックして、入力した情報に基づいた既存のミラーエントリを削除します。
「検索」をクリックして、入力した情報に基づいたエントリを検出します。
「詳細を表示」リンクをクリックし、ミラーセッションの詳細情報を表示します。

注意　各セッションの 送信先（Destination）のポートは別々のポートに設定することはできません。（Destination のポートは 1 ポートのみ対応）

sFlow

sFlow は、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。

sFlow エージェント情報

sFlow エージェント情報を表示します。

モニタリング > sFlow > sFlow エージェント情報 の順にメニューをクリックし、以下の画面を表示します。

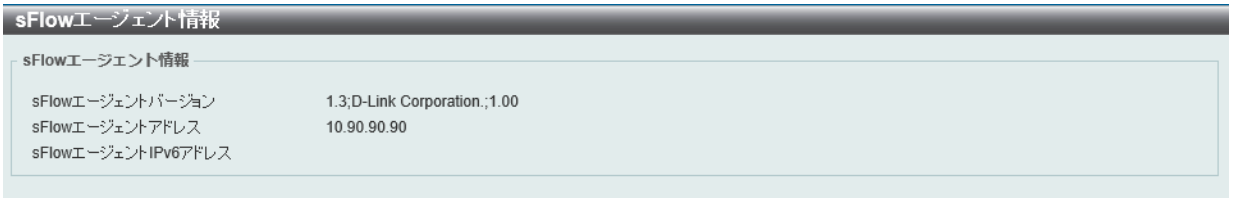


図 14-17　sFlow エージェント情報 画面

sFlow レシーバ設定

sFlow エージェントのレシーバ設定と設定表示を行います。レシーバは sFlow エージェントから消去や追加することはできません。

モニタリング > sFlow > sFlow レシーバ設定の順にメニューをクリックし、以下の画面を表示します。



図 14-18　sFlow レシーバ設定画面

画面に表示される項目：

項目	説明
レシーバインデックス	追加する sFlow レシーバの識別子を指定します。 • 設定可能範囲：1-4
オーナ名	sFlow レシーバのオーナ名を指定します。（32 文字以内）
期限切れ	エントリの有効期限を指定します。期限になるとエントリのパラメータはリセットされます。 「無限」を設定するとエントリはタイムアウトしません。 • 設定可能範囲：1-2000000（秒）
最大データグラムサイズ	sFlow データ 1 つあたりの最大データバイト数を指定します。 • 設定可能範囲：700-1400（Bytes） • 初期値：1400（Bytes）
コレクタアドレス	リモート sFlow コレクタの IPv4/IPv6 アドレスを指定します。
UDP ポート	リモート sFlow コレクタの UDP ポート番号を指定します。 • 設定可能範囲：1-65535 • 初期値：6343

「適用」をクリックして、設定を有効にします。
「リセット」をクリックして、指定エントリの設定を初期値に戻します。

sFlow サンプラ設定

ネットワークからサンプルパケットを取得するための設定をします。これには、サンプリングのレートや抽出されるパケットヘッダの量も含まれます。

モニタリング > sFlow > sFlow サンプラ設定の順にメニューをクリックし、以下の画面を表示します。

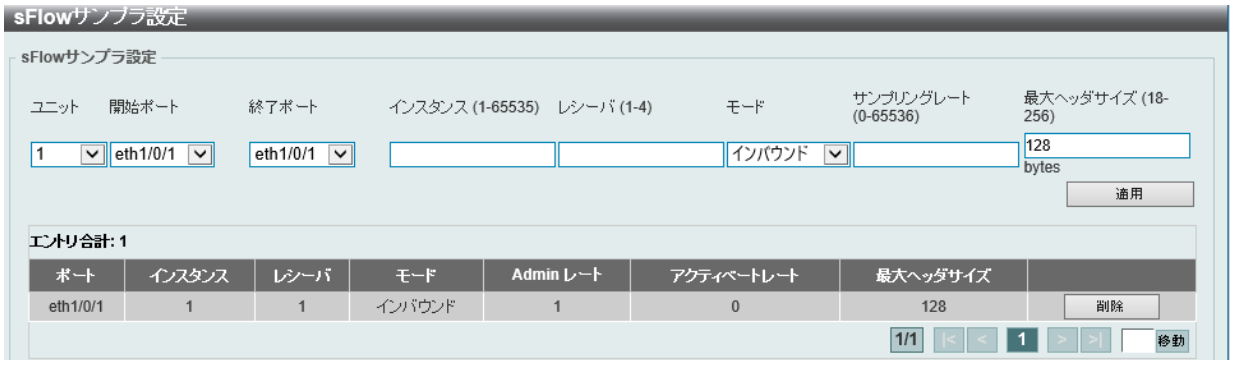


図 14-19　sFlow サンプラ設定画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
インスタンス	インタフェースに複数のサンプラを設定する場合、インスタンスのインデックス番号を指定します。 • 設定可能範囲：1-65535
レシーバ	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。 • 設定可能範囲：1-4
モード	モードを指定します。 •「インバウンド」- 受信パケットをサンプリングします。（初期値） •「アウトバウンド」- 送信パケットをサンプリングします。
サンプリングレート	パケットサンプリングのレートを設定します。 • 設定可能範囲：0-65536 • 初期値：0（サンプリング無効）
最大ヘッダサイズ	サンプリングパケットからコピーすることができる最大バイト数を設定します。 • 設定可能範囲：18-256（Bytes） • 初期値：128（Bytes）

「適用」をクリックして、設定を有効にします。
「削除」をクリックして、指定エントリを削除します。

sFLow ポーラー設定

スイッチのポーラーの設定を行います。

モニタリング > sFlow > sFLow ポーラー設定 の順にメニューをクリックし、以下の画面を表示します。

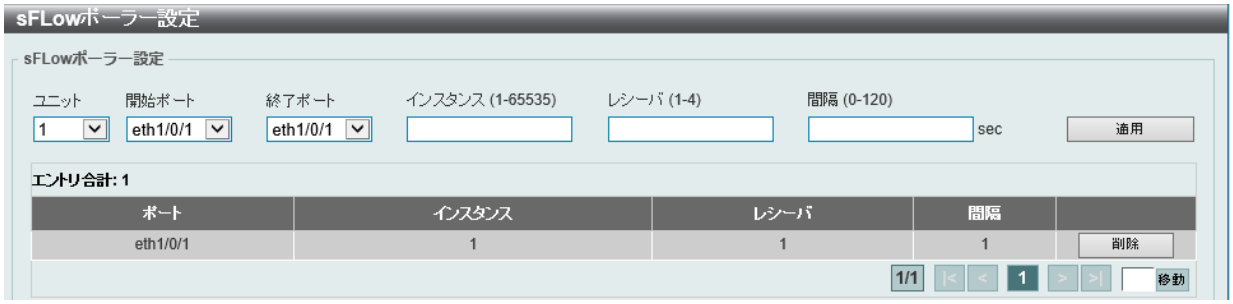


図 14-20　sFLow ポーラー設定 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
インスタンス	インタフェースに複数のサンプラを設定する場合、インスタンスのインデックス番号を指定します。 • 設定可能範囲：1-65535
レシーバ	レシーバの識別番号を指定します。 • 設定可能範囲：1-4

項目	説明
間隔	ポーリングサンプリングの間隔を設定します。「0」を入力すると機能は無効になります。 • 設定可能範囲：0-120（秒） • 初期値：0（秒）

「適用」をクリックして、設定内容を適用します。
「削除」をクリックして、指定エントリを削除します。

デバイス環境

本画面ではスイッチの内部温度状態を表示します。

モニタリング > デバイス環境をクリックして次の画面を表示します。

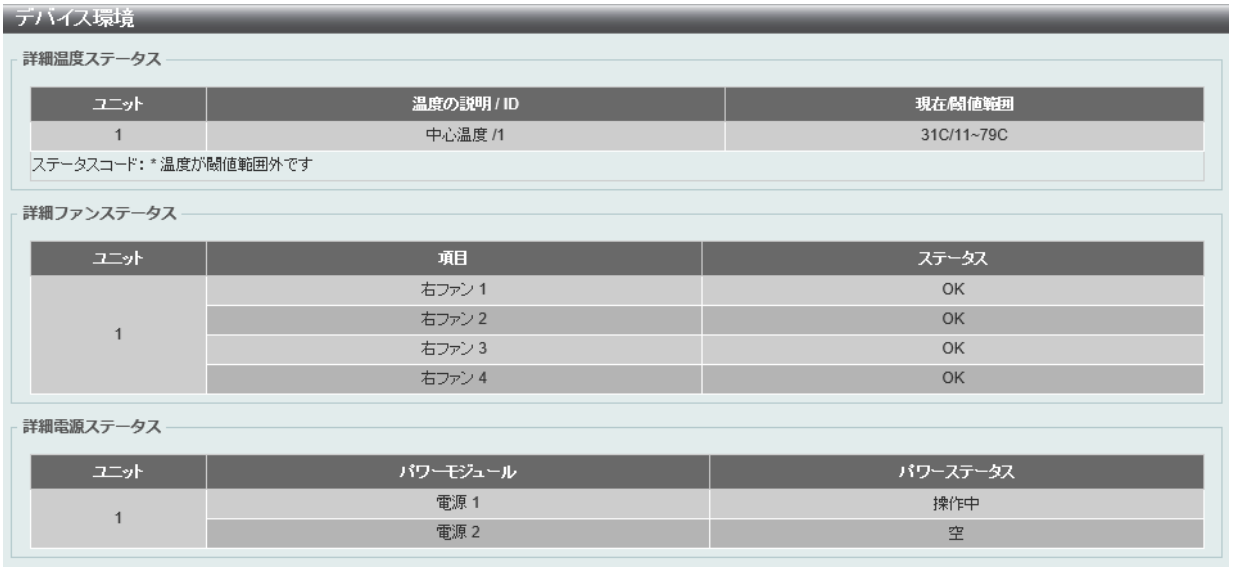


図 14-21　デバイス環境画面

第 15 章　Green（省電力機能）

以下は Green サブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
省電力	スイッチの省電力機能を設定、表示します。
EEE	「Energy Efficient Ethernet」(EEE/ 省電力イーサネット) は「IEEE 802.3az」によって定義されており、パケットの送受信がリンクに発生していない場合の電力消費を抑える目的で設計されています。

省電力

スイッチの省電力機能を設定、表示します。

省電力 > 省電力メニューをクリックし、以下の画面を表示します。

省エネグローバル設定タブ

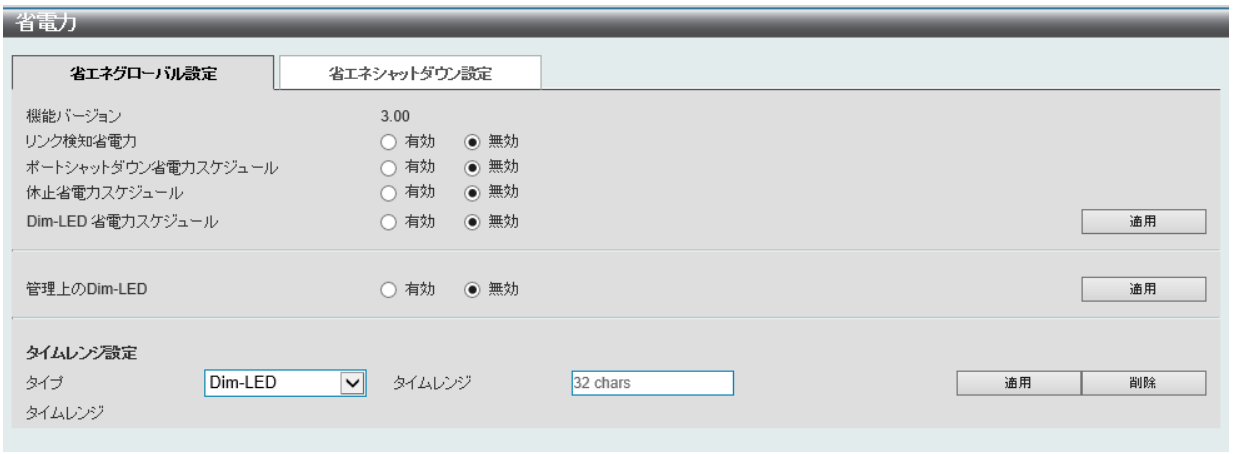


図 15-1　省電力 - 省エネグローバル設定タブ画面

画面に表示される項目：

項目	説明
リンク検知省電力	「リンク検出」を有効 / 無効に指定します。 本設定を有効にすると、リンクダウンしているポートへの電力供給が停止し、スイッチの消費電力を抑えます。 リンクアップしているポートへの影響はありません。
ポートシャットダウン省電力スケジュール	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
休止省電力スケジュール	スケジュールによる休止状態の省電力機能を有効 / 無効に指定します。 この機能は、物理スタッキングが有効になっている場合は使用できません。
Dim-LED 省電力スケジュール	スケジュールによる減光 LED の有効 / 無効を指定します。
管理上の Dim-LED	ポート LED 機能の有効 / 無効を指定します。
タイムレンジ設定	
タイプ	省電力モードの種類を指定します。 • 選択肢：「Dim-LED」「休止」
タイムレンジ	上記省電力機能に対応するスケジュールを指定します。

「適用」をクリックして、設定内容を適用してください。画面は自動的に更新されます。
「削除」をクリックして、指定のエントリを削除します。

注意　「休止」機能を有効にする場合、物理スタック機能は無効である必要があります。

省エネシャットダウンタブ



図 15-2　省電力 - 省エネシャットダウン設定タブ画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポートの範囲を指定します。
タイムレンジ	ポートに対応するスケジュール名を指定します。

「適用」をクリックして、設定内容を適用します。画面は自動的に更新されます。
「削除」をクリックして指定のエントリを削除します。

EEE

「Energy Efficient Ethernet」(EEE/ 省電力イーサネット) は「IEEE 802.3az」によって定義されています。
リンク上でパケットの送受信が発生していない場合、電力消費を抑えることができます。

省電力 > EEE メニューをクリックし、以下の画面を表示します。



図 15-3　EEE 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
開始ポート / 終了ポート	設定するポート範囲を指定します。
状態	本機能を有効 / 無効に設定します。

「適用」をクリックして、設定内容を適用します。画面は自動的に更新されます。

注意　本機能を使用するには、接続する対向の機器も EEE に対応している必要があります。

第 16 章　保存メニュー / ツールメニュー

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

以下はサブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
保存	
コンフィグレーションの保存	コンフィグレーションをスイッチに保存します。
ツール	
ファームウェアアップグレード&バックアップ	様々なプロトコルを使用してファームウェアアップグレード / バックアップを実行します。
設定リストアおよびバックアップ	様々なプロトコルを使用してコンフィグレーションリストア / バックアップを実行します。
証明書およびキーリストアおよびバックアップ	様々なプロトコルを使用して証明書と鍵のリストア / バックアップを実行します。
ログバックアップ	様々なプロトコルを使用してログファイルのバックアップを実行します。
Ping	「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。
トレースルート	パケットの経路をスイッチに到着する前に遡ってトレースすることができます。
言語管理	Web GUI の表示言語を管理します。
リセット	スイッチの設定内容を工場出荷時状態に戻します。
システム再起動	スイッチの再起動を行います。

保存

現在のコンフィグレーションを保存します。

コンフィグレーションの保存

保存 > コンフィグレーションの保存をクリックし、以下の画面を表示します。

「コンフィグレーションの保存」では現在のコンフィグレーションをスイッチに保存します。
スイッチのファイルシステムにおけるパス名を「ファイルパス」に入力して「適用」をクリックします。

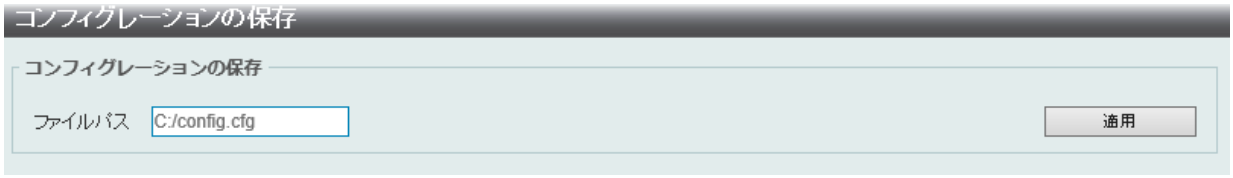


図 16-1　コンフィグレーションの保存画面

ツール

ファームウェアアップグレード＆バックアップ、コンフィグレーションリストア＆バックアップ、ログファイルのバックアップ、Ping、トレースルート、リセット、システム再起動を行います。

ファームウェアアップグレード＆バックアップ

HTTP からファームウェアアップグレード

HTTP を使用してローカル PC からファームウェアアップグレードを実行します。

ツール > ファームウェアアップグレード＆バックアップ > HTTP からファームウェアアップグレードをクリックし、設定画面を表示します。



図 16-2　HTTP からファームウェアアップグレード 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
送信元ファイル	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。 「参照」をクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
送信先ファイル	ファームウェアが保存されるファイルパスとファイル名を入力します。 例：DGS-1520_Run_1_00_B031.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「更新」をクリックしてアップグレードを開始します。

TFTP からファームウェアアップグレード

TFTP を使用してファームウェアアップグレードを実行します。

ツール > ファームウェアアップグレード＆バックアップ > TFTP からファームウェアアップグレードをクリックし、設定画面を表示します。



図 16-3　TFTP からファームウェアアップグレード 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」-TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」-TFTP サーバの IPv6 アドレスを入力します。
送信元ファイル	TFTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内） 例：DGS-1520_Run_1_00_B031.had
送信先ファイル	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内） 例：DGS-1520_Run_1_00_B031.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「更新」をクリックしてアップグレードを開始します。

SFTP からファームウェアアップグレード

SFTP を使用してファームウェアアップグレードを実行します。

ツール > ファームウェアアップグレード＆バックアップ > SFTP からファームウェアアップグレードをクリックし、設定画面を表示します。

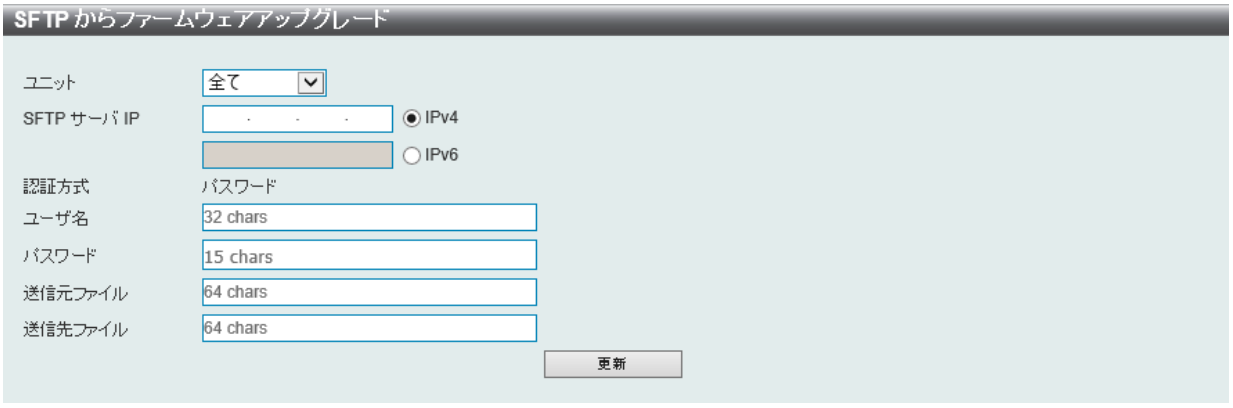


図 16-4　SFTP からファームウェアアップグレード 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
SFTP サーバ IP	SFTP サーバの IP アドレスを入力します。
認証方式	認証方法が表示されます。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信元ファイル	SFTP サーバ上にあるファームウェアのパスとファイル名を入力します。（64 文字以内） 例：DGS-1520_Run_1_00_B031.had
送信先ファイル	ファームウェアが保存されるスイッチの場所を指定します。（64 文字以内） 例：DGS-1520_Run_1_00_B031.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「更新」をクリックしてアップグレードを開始します。

HTTP でファームウェアをバックアップ

HTTP を使用してローカル PC へファームウェアバックアップをバックアップします。

ツール > ファームウェアアップグレード＆バックアップ > HTTP でファームウェアをバックアップをクリックし、設定画面を表示します。

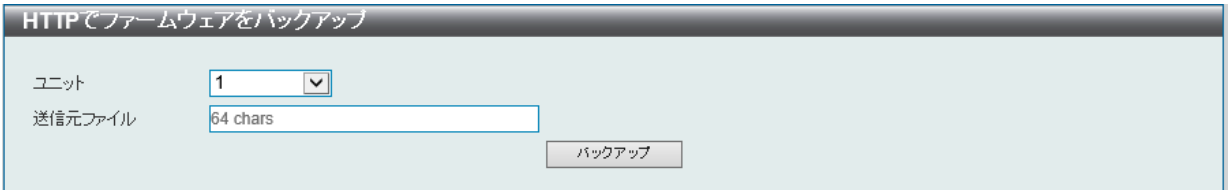


図 16-5　HTTP でファームウェアをバックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
送信元ファイル	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。(64 文字以内) 例：DGS-1520_Run_1_00_B031.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。

「バックアップ」をクリックしてバックアップを開始します。

TFTP でファームウェアをバックアップ

TFTP サーバにファームウェアバックアップを行います。

ツール > ファームウェアアップグレード＆バックアップ > TFTP でファームウェアをバックアップをクリックし、設定画面を表示します。

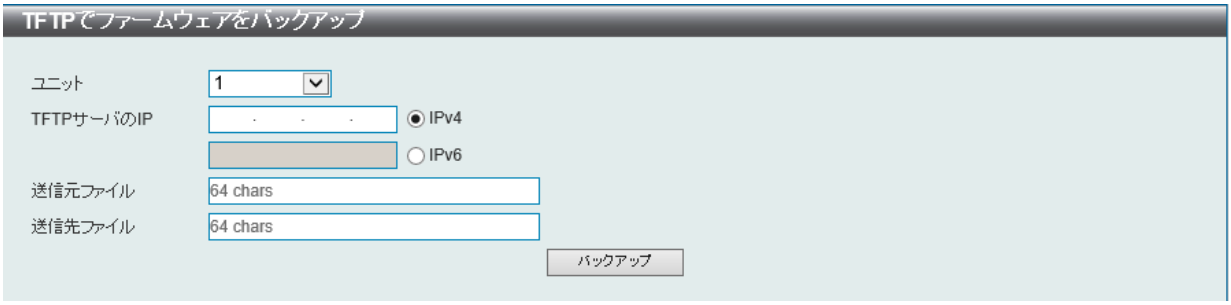


図 16-6　TFTP でファームウェアをバックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」-TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」-TFTP サーバの IPv6 アドレスを入力します。
送信元ファイル	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。(64 文字以内) 例：DGS-1520_Run_1_00_B031.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。
送信先ファイル	ファームウェアファイルがバックアップされる TFTP サーバの場所（パス / ファイル名）を指定します。(64 文字以内) 例：DGS-1520_Run_1_00_B031.had

「バックアップ」をクリックしてバックアップを開始します。

SFTP にファームウェアバックアップ

SFTP サーバにファームウェアバックアップを行います。

ツール > ファームウェアアップグレード＆バックアップ > SFTP にファームウェアバックアップをクリックし、設定画面を表示します。

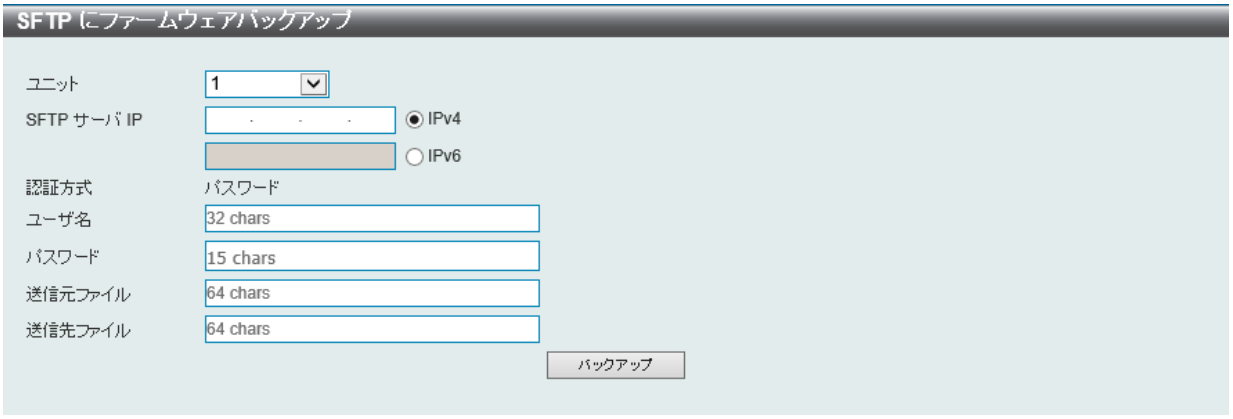


図 16-7　SFTP にファームウェアバックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
SFTP サーバ IP	SFTP サーバの IP アドレスを入力します。
認証方式	認証方法が表示されます。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信元ファイル	スイッチ上でファームウェアが保存されているファイルパスとファイル名を入力します。（64 文字以内） 例：DGS-1520_Run_1_00_B031.had スイッチのルートディレクトリに保存する場合はフォルダパス（c:/）を省略できます。
送信先ファイル	ファームウェアファイルがバックアップされる SFTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内） 例：DGS-1520_Run_1_00_B031.had

「バックアップ」をクリックしてバックアップを開始します。

設定リストアおよびバックアップ

HTTP から設定をリストア

HTTP を使用してローカル PC からコンフィグレーションをリストアします。

ツール > 設定リストアおよびバックアップ > HTTP から設定をリストアをクリックし、設定画面を表示します。

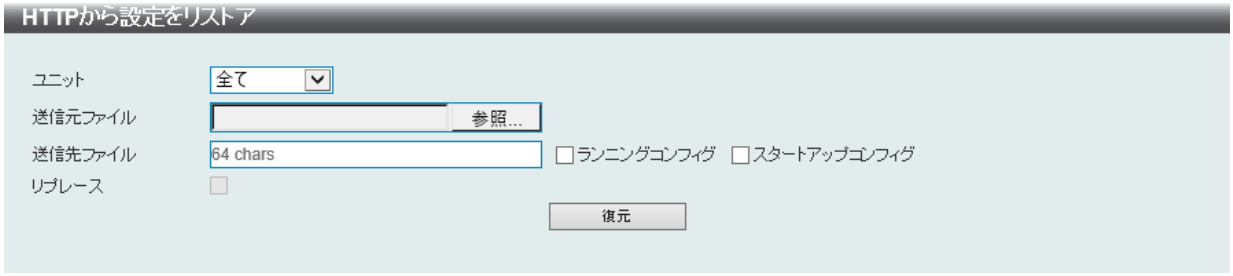


図 16-8　HTTP から設定をリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
送信元ファイル	ローカル PC 上のコンフィグレーションパスとファイル名を入力します。(64 文字以内) 「参照」をクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。
送信先ファイル	コンフィグレーションファイルが保存されるスイッチの場所を指定します。(64 文字以内) 「ランニングコンフィグ」オプションを選択すると、リストアと同時にランニングコンフィグレーションファイルがリストア＆上書きされます。 「スタートアップコンフィグ」スタートアップコンフィグレーションファイルがリストア＆上書きされます。
リプレース	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「復元」をクリックしてコンフィグレーションのリストアを開始します。

TFTP から設定をリストア

TFTP サーバからコンフィグレーションをリストアします。

ツール > 設定リストアおよびバックアップ > TFTP から設定をリストアをクリックし、設定画面を表示します。

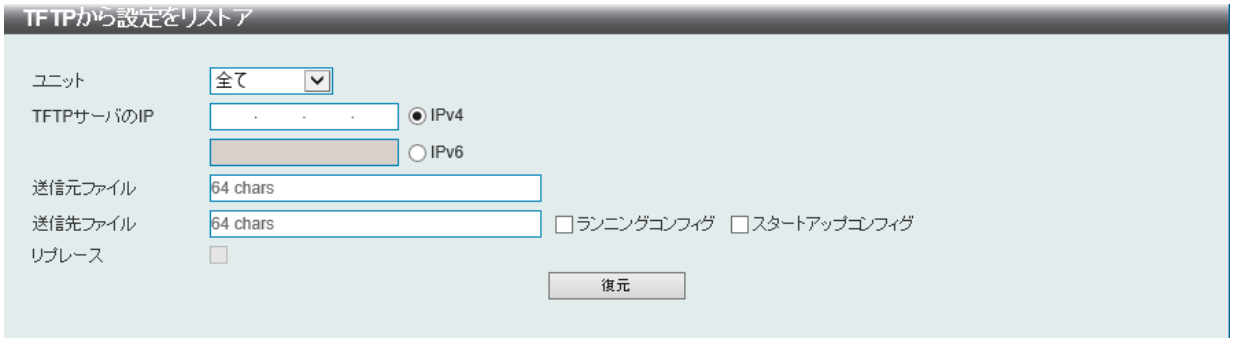


図 16-9　TFTP から設定をリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
送信元ファイル	TFTP サーバに保存されているコンフィグレーションのパスとファイル名を入力します。(64 文字以内)
送信先ファイル	コンフィグレーションファイルが保存されるスイッチの場所を指定します。(64 文字以内) 「ランニングコンフィグ」オプションを選択するとリストアと同時にランニングコンフィグレーションファイルがリストア＆上書きされます。 「スタートアップコンフィグ」オプションを選択するとスタートアップコンフィグレーションファイルがリストア＆上書きされます。
リプレース	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「復元」をクリックしてコンフィグレーションのリストアを開始します。

SFTP からのコンフィグリストア

SFTP サーバからコンフィグレーションをリストアします。

ツール > 設定リストアおよびバックアップ > SFTP からのコンフィグリストアをクリックし、設定画面を表示します。

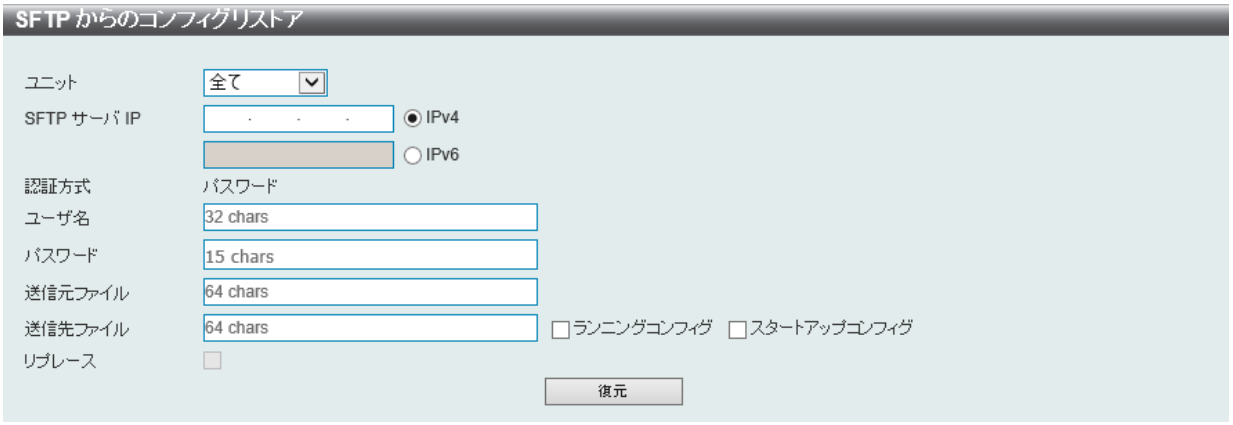


図 16-10　SFTP からのコンフィグリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
SFTP サーバ IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信元ファイル	SFTP サーバにあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。（64 文字以内）
送信先ファイル	コンフィグレーションファイルが保存されるスイッチの場所を指定します。（64 文字以内） 「ランニングコンフィグ」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「スタートアップコンフィグ」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
リプレース	スイッチ上のコンフィグレーションを削除し、新しいコンフィグレーションに置き換えます。

「復元」をクリックしてコンフィグレーションのリストアを開始します。

HTTP で設定バックアップ

HTTP を使用してローカル PC にコンフィグレーションバックアップを行います。

ツール > 設定リストアおよびバックアップ > HTTP で設定バックアップをクリックし、設定画面を表示します。

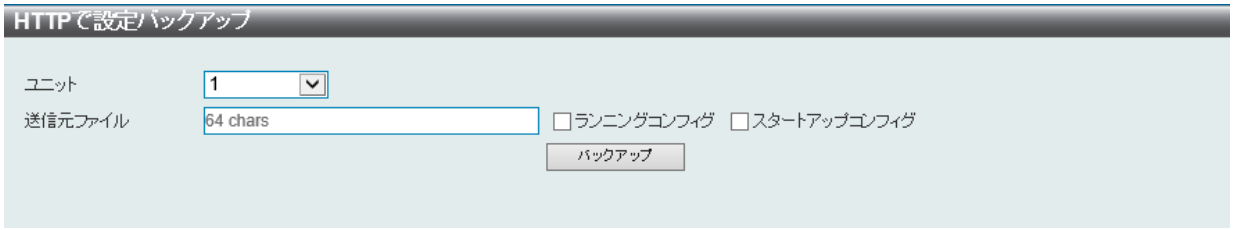


図 16-11　HTTP で設定バックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
送信元ファイル	コンフィグレーションファイルが保存されているスイッチの場所を指定します。(64 文字以内) 「ランニングコンフィグ」オプションを選択するとランニングコンフィグレーションファイルのバックアップを行います。 「スタートアップコンフィグ」オプションを選択するとスタートアップコンフィグレーションファイルのバックアップを行います。

「バックアップ」をクリックしてバックアップを開始します。

TFTP で設定バックアップ

TFTP サーバにコンフィグレーションバックアップを行います。

ツール > 設定リストアおよびバックアップ > TFTP で設定バックアップをクリックし、設定画面を表示します。

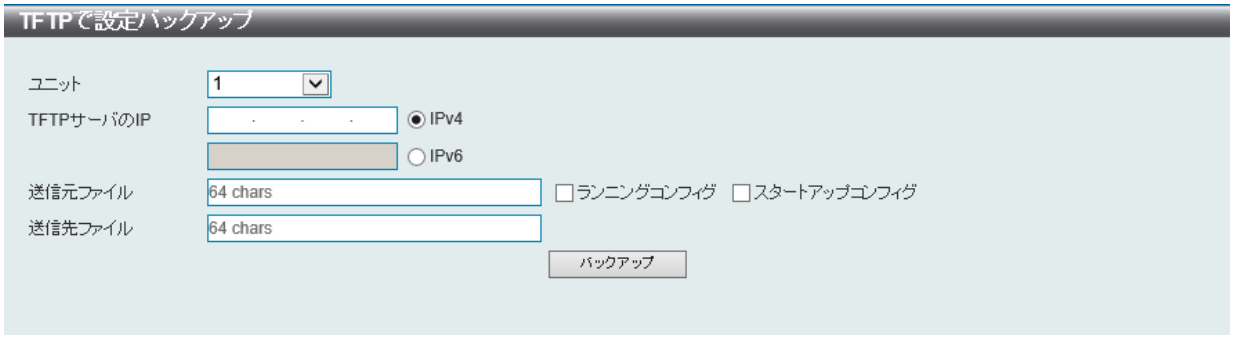


図 16-12　TFTP で設定バックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
送信元ファイル	コンフィグレーションファイルが保存されているスイッチの場所を指定します。(64 文字以内) 「ランニングコンフィグ」オプションを選択するとランニングコンフィグレーションファイルのバックアップを行います。 「スタートアップコンフィグ」オプションを選択するとスタートアップコンフィグレーションファイルのバックアップを行います。
送信先ファイル	コンフィグレーションファイルが保存される TFTP サーバの場所を指定します。(64 文字以内)

「バックアップ」をクリックしてバックアップを開始します。

SFTP へのコンフィグバックアップ

SFTP サーバにコンフィグレーションバックアップを行います。

ツール > 設定リストアおよびバックアップ > SFTP へのコンフィグバックアップをクリックし、設定画面を表示します。

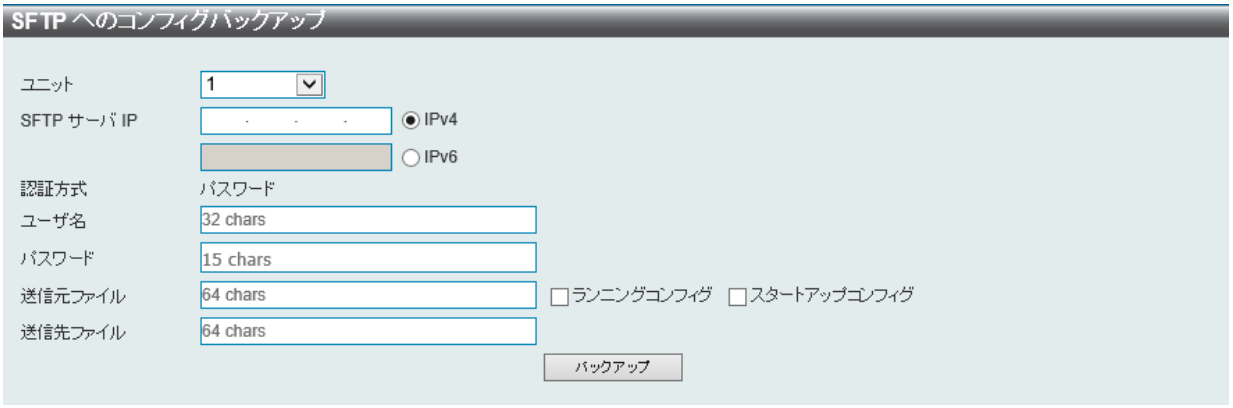


図 16-13　SFTP へのコンフィグバックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
SFTP サーバの IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信元ファイル	コンフィグレーションファイルが保存されているスイッチの場所を指定します。（64 文字以内） 「ランニングコンフィグ」オプションを選択するとランニングコンフィグレーションファイルのバックアップを行います。 「スタートアップコンフィグ」オプションを選択するとスタートアップコンフィグレーションファイルのバックアップを行います。
送信先ファイル	コンフィグレーションファイル保存される SFTP サーバの場所を指定します。（64 文字以内）

「バックアップ」をクリックしてバックアップを開始します。

証明書およびキーリストアおよびバックアップ

HTTP での証明書およびキーリストア

HTTP を使用してローカル PC から証明書 / 鍵リストアを実行します。

ツール > 証明書およびキーリストアおよびバックアップ > HTTP での証明書およびキーリストアをクリックし、設定画面を表示します。



図 16-14　HTTP での証明書およびキーリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
送信元ファイル	ローカル PC にある証明書 / 鍵のパスと証明書 / 鍵ファイル名を入力します。 「参照」をクリックしてローカル PC 上の証明書 / 鍵ファイルの場所を指定できます。
送信先ファイル	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「復元」をクリックしてリストアを開始します。

TFTP での証明書およびキーリストア

TFTP サーバを使用して証明書 / 鍵リストアを実行します。

ツール > 証明書およびキーリストアおよびバックアップ > TFTP での証明書およびキーリストアをクリックし、設定画面を表示します。



図 16-15　TFTP での証明書およびキーリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
送信元ファイル	TFTP サーバ上に保存されている証明書 / 鍵のパスとファイル名を入力します。（64 文字以内）
送信先ファイル	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「復元」をクリックしてリストアを開始します。

SFTP での証明書およびキーリストア

SFTP サーバを使用して証明書 / 鍵リストアを実行します。

ツール > 証明書およびキーリストアおよびバックアップ > SFTP での証明書およびキーリストアをクリックし、設定画面を表示します。

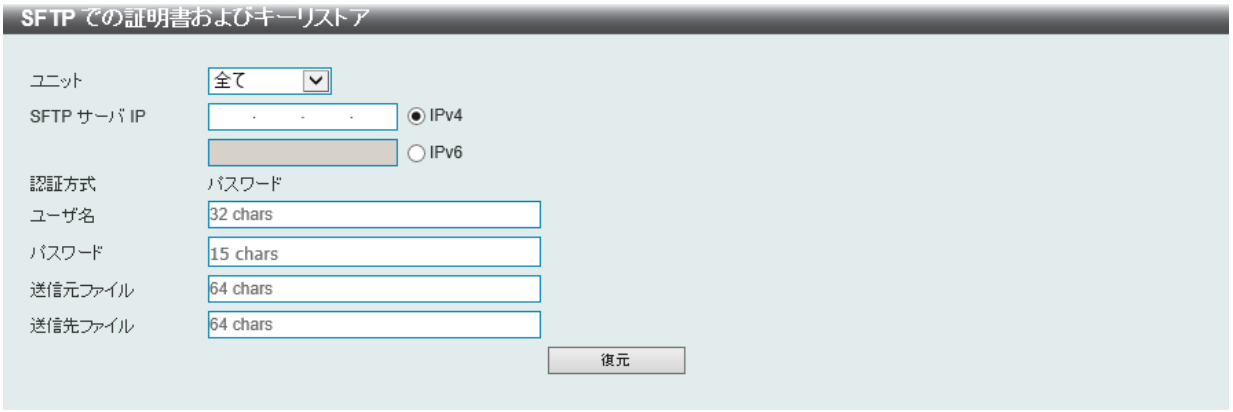


図 16-16　SFTP での証明書およびキーリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
SFTP サーバ IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信元ファイル	SFTP サーバ上に保存されている証明書 / 鍵のパスとファイル名を入力します。（64 文字以内）
送信先ファイル	証明書 / 鍵が保存されるスイッチの場所を指定します。（64 文字以内）

「復元」をクリックしてリストアを開始します。

HTTP で公開鍵をバックアップ

HTTP を使用してローカル PC へ証明書 / 鍵をバックアップします。

ツール > 証明書およびキーリストアおよびバックアップ > HTTP で公開鍵をバックアップをクリックし、設定画面を表示します。

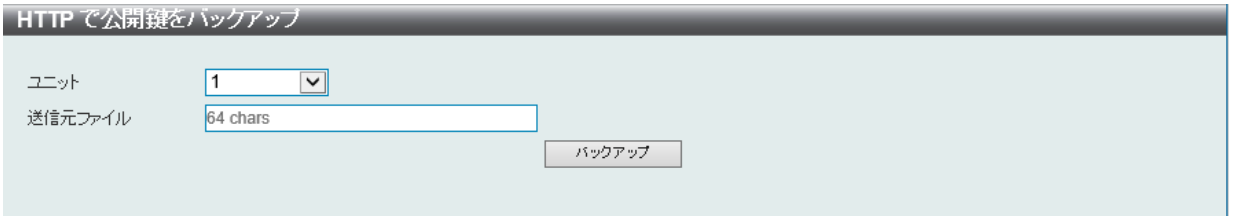


図 16-17　HTTP で公開鍵をバックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
送信元ファイル	スイッチに保存されている公開鍵ファイルのパスとファイル名を入力します。（64 文字以内）

「バックアップ」をクリックしてバックアップを開始します。

TFTP で公開鍵をバックアップ

TFTP サーバに証明書 / 鍵バックアップのバックアップを行います。

ツール > 証明書およびキーリストアおよびバックアップ > TFTP で公開鍵をバックアップをクリックし、設定画面を表示します。

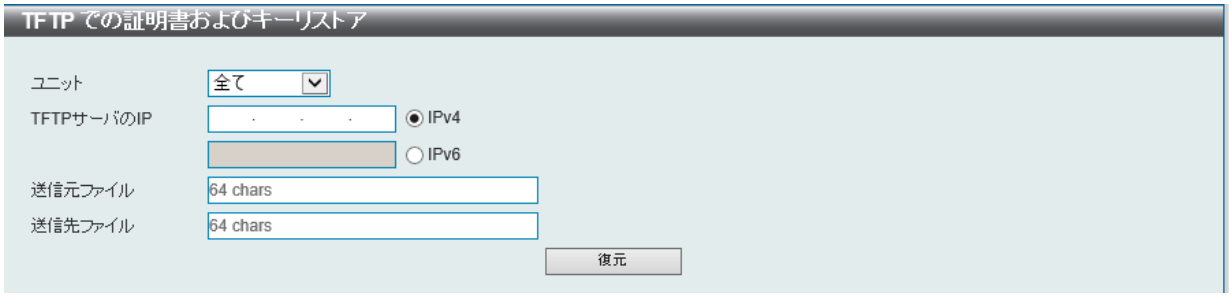


図 16-18　TFTP での証明書およびキーリストア 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
送信元ファイル	スイッチに保存されている公開鍵ファイルのパスとファイル名を入力します。（64 文字以内）
送信先ファイル	公開鍵ファイルがバックアップされる TFTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「バックアップ」をクリックしてバックアップを開始します。

SFTP で公開鍵をバックアップ

SFTP サーバに証明書 / 鍵のバックアップを行います。

ツール > 証明書およびキーリストアおよびバックアップ > SFTP で公開鍵をバックアップをクリックし、設定画面を表示します。

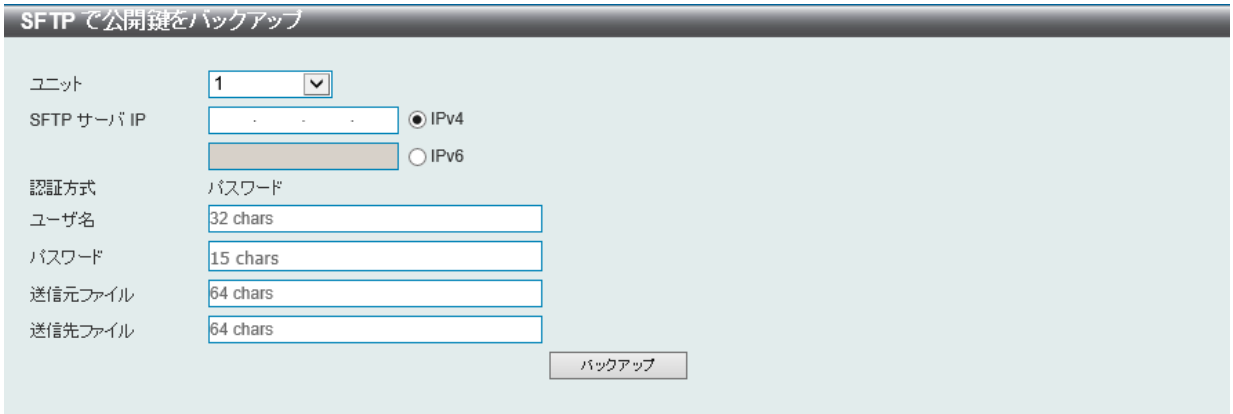


図 16-19　SFTP で公開鍵をバックアップ 画面

画面に表示される項目：

項目	説明
ユニット	設定するユニットを指定します。
SFTP サーバの IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
認証方式	認証方法が表示されます。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信元ファイル	スイッチに保存されている公開鍵ファイルのパスとファイル名を入力します。（64 文字以内）
送信先ファイル	公開鍵ファイルがバックアップされる SFTP サーバの場所（パス / ファイル名）を指定します。（64 文字以内）

「バックアップ」をクリックしてバックアップを開始します。

ログバックアップ

HTTP でログをバックアップ

HTTP を使用してローカル PC へシステムログのバックアップを行います。

ツール > ログバックアップ > HTTP でログをバックアップをクリックし、設定画面を表示します。



図 16-20　HTTP でログをバックアップ 画面

画面に表示される項目：

項目	説明
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の種類を選択します。 • 「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」- 攻撃関連のログをバックアップします。

「バックアップ」をクリックしてバックアップを開始します。

TFTP でログをバックアップ

TFTP サーバへのシステムログのバックアップを行います。

ツール > ログバックアップ > TFTP でログをバックアップをクリックし、設定画面を表示します。

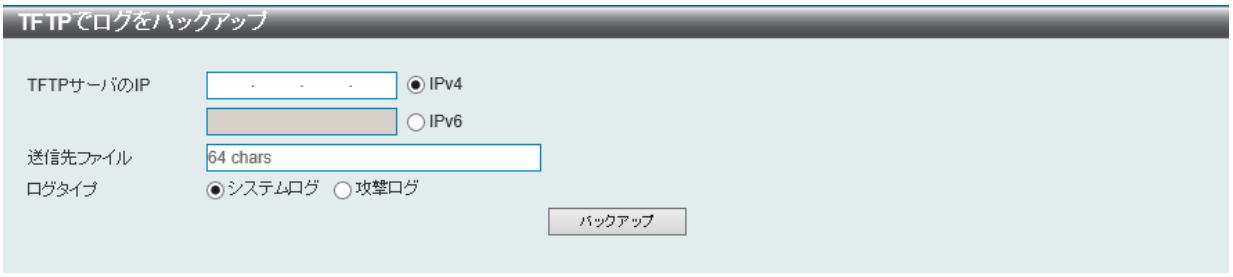


図 16-21　TFTP でログをバックアップ画面

画面に表示される項目：

項目	説明
TFTP サーバの IP	TFTP サーバの IP アドレスを入力します。 • 「IPv4」- TFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- TFTP サーバの IPv6 アドレスを入力します。
送信先ファイル	ログファイルが保存される TFTP サーバの場所を指定します。（64 文字以内）
ログタイプ	バックアップするログの種類を選択します。 • 「システムログ」- システムログエントリをバックアップします。 • 「攻撃ログ」- 攻撃関連のログをバックアップします。

「バックアップ」をクリックしてバックアップを開始します。

SFTP にログをバックアップ

SFTP サーバへのシステムログのバックアップを行います。

ツール > ログバックアップ > SFTP にログをバックアップをクリックし、設定画面を表示します。

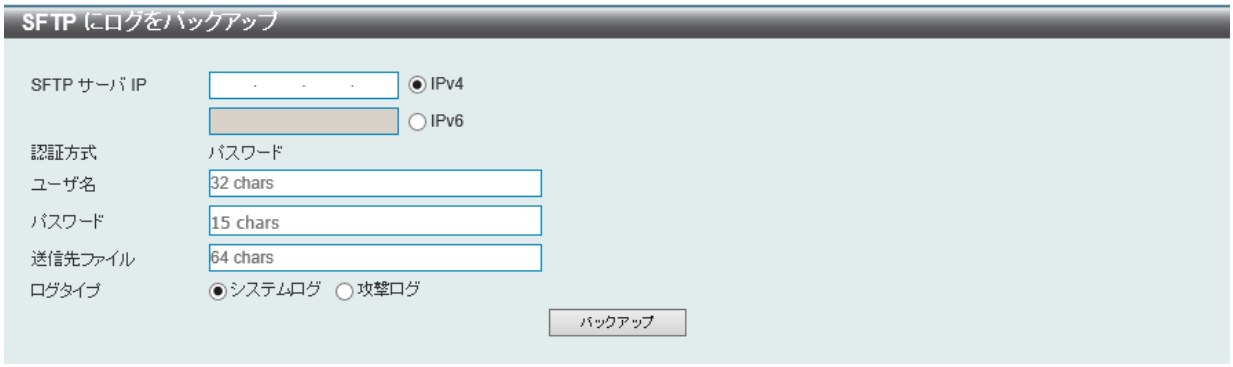


図 16-22　SFTP にログをバックアップ画面

画面に表示される項目：

項目	説明
SFTP サーバ IP	SFTP サーバの IP アドレスを入力します。 • 「IPv4」- SFTP サーバの IPv4 アドレスを入力します。 • 「IPv6」- SFTP サーバの IPv6 アドレスを入力します。
ユーザ名	SFTP 接続のユーザ名を指定します。（32 文字以内）
パスワード	SFTP 接続のパスワードを指定します。（15 字以内）
送信先ファイル	ログファイルが保存される SFTP サーバの場所を指定します。（64 文字以内）
ログタイプ	バックアップするログの種類を選択します。 • 「システムログ」- システムログエントリをバックアップします。 • 「攻撃ログ」- 攻撃関連のログをバックアップします。

「バックアップ」をクリックしてバックアップを開始します。

Ping

「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。宛先の機器はスイッチから送信された "echoes" に応答します。これはネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

ツール > Ping をクリックし、設定画面を表示します。

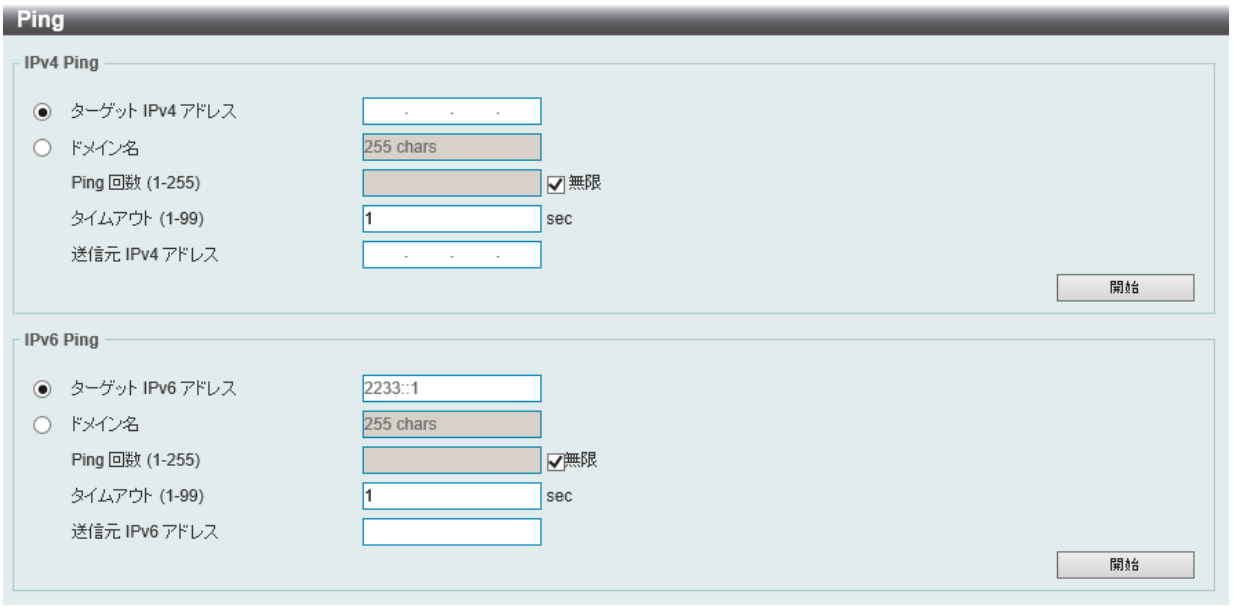


図 16-23　Ping 画面

画面に表示される項目：

項目	説明
IPv4 Ping	
ターゲット IPv4 アドレス	Ping の送信先となる IPv4 アドレスを入力します。
ドメイン名	検出するシステムのドメイン名を入力します。
Ping 回数	Ping の試行回数を入力します。 「無限」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
タイムアウト	Ping メッセージが到達するまでのタイムアウトの時間を指定します。 指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
送信元 IPv4 アドレス	送信元 IPv4 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。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送信元IP アドレスまたはプライマリ IP アドレスとして使用されます。
IPv6 Ping	
ターゲット IPv6 アドレス	Ping の送信先となる IPv6 アドレスを入力します。
ドメイン名	検出するシステムのドメイン名を入力します。
Ping 回数	Ping の試行回数を入力します。 「無限」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。 • 設定可能範囲：1-255
タイムアウト	Ping メッセージが到達するまでのタイムアウトの時間を指定します。 指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。 • 設定可能範囲：1-99（秒）
送信元 IPv6 アドレス	送信元 IPv6 アドレスを入力します。 スイッチが複数の IP アドレスを保持している場合、そのうちのいずれかを入力することが可能です。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送信元IP アドレスまたはプライマリ IP アドレスとして使用されます。

「開始」をクリックして、各個別セクションでの Ping テストを実行します。

「開始」をクリックすると以下の画面が表示されます。

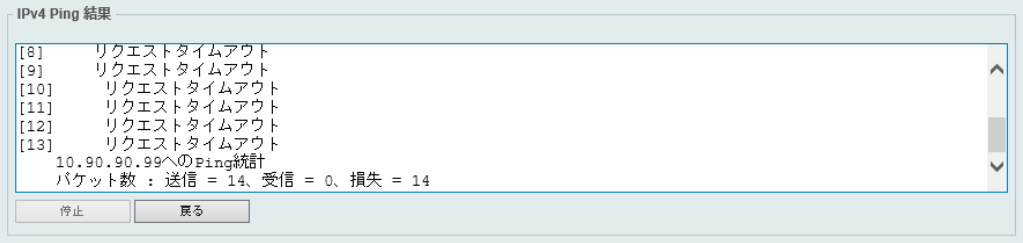


図 16-24　IPv4 Ping 結果 画面

「停止」をクリックして、Ping テストを停止します。
「戻る」をクリックして、前の画面に戻ります。

トレースルート

ネットワークとホスト間のルートをトレースします。

ツール > トレースルートの順にメニューをクリックし、以下の画面を表示します。

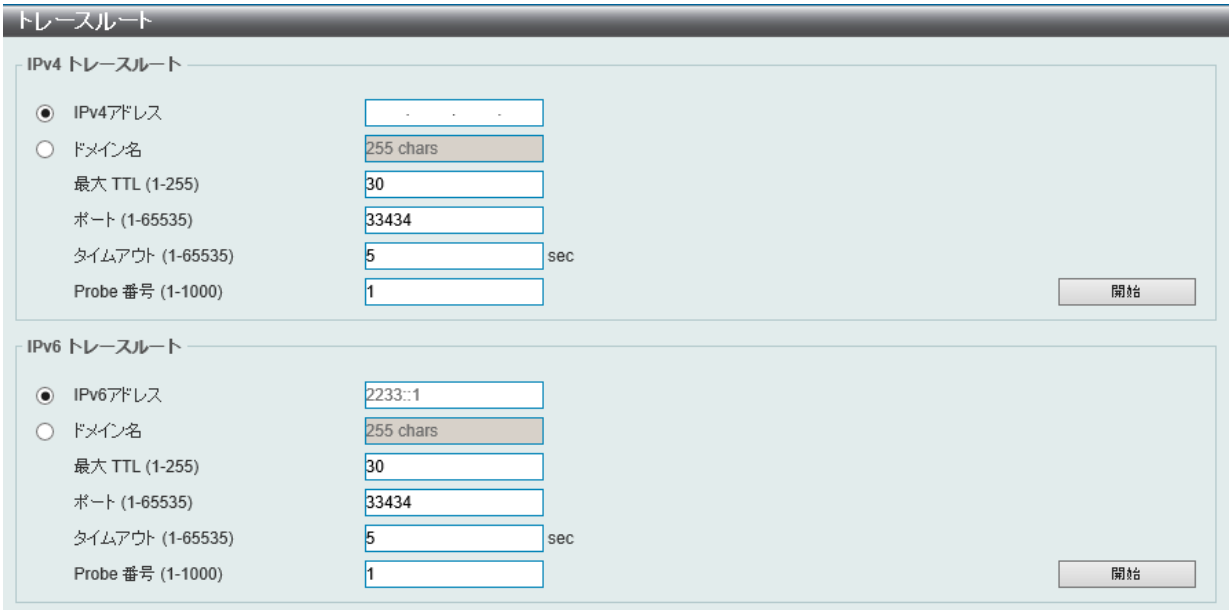


図 16-25　トレースルート画面

画面に表示される項目：

項目	説明
IPv4 トレースルート	
IPv4 アドレス	宛先 IPv4 アドレスを入力します。
ドメイン名	宛先のドメイン名を入力します。
最大 TTL	トレースルートリクエストの Time-To-Live (TTL) 値を入力します。 トレースルートパケットが通過できるルータの最大数となります。2 台のデバイス間でネットワークパスを検出する際に、このトレースルートオプションを使用します。 • 設定可能範囲：1-255
ポート	ポート番号を指定します。 • 設定可能範囲：1-65535
タイムアウト	リモートデバイスからのレスポンスを待機する時間を指定します。この時間を過ぎるとタイムアウトになります。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）
Probe 番号	プローブ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1
IPv6 トレースルート	
IPv4 アドレス	宛先 IPv6 アドレスを入力します。
ドメイン名	宛先のドメイン名を入力します。

項目	説明
最大 TTL	トレースルートリクエストの Time-To-Live (TTL) 値を入力します。 トレースルートパケットが通過できるルータの最大数となります。2 台のデバイス間でネットワークパスを検出する際に、このトレースルートオプションを使用します。 • 設定可能範囲：1-255
ポート	ポート番号を指定します。 • 設定可能範囲：1-65535
タイムアウト	リモートデバイスからのレスポンスを待機する時間を指定します。この時間を過ぎるとタイムアウトになります。 • 設定可能範囲：1-65535（秒） • 初期値：5（秒）
Probe 番号	プローブ数を指定します。 • 設定可能範囲：1-1000 • 初期値：1

「開始」をクリックし、トレースルートプログラムを開始します。

以下の結果画面が表示されます。

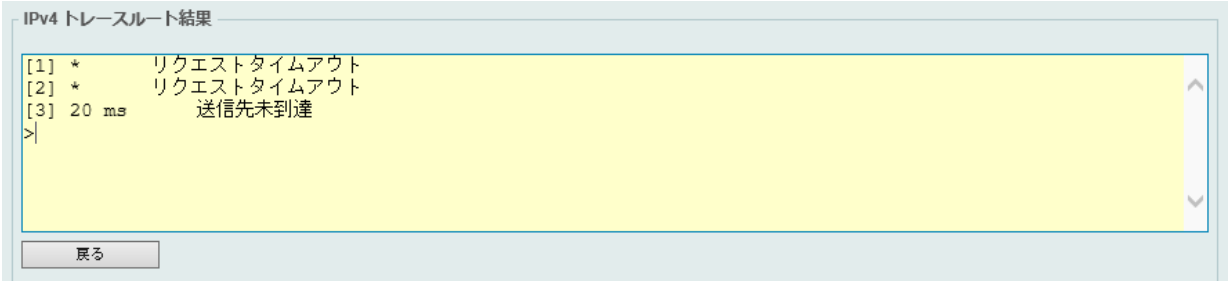


図 16-26　トレースルート結果画面

「戻る」をクリックして、前の画面に戻ります。

言語管理

言語ファイルのインストールを行います。

ツール > 言語管理をクリックし、次の設定画面を表示します。



図 16-27　言語管理画面

画面に表示される項目：

項目	説明
言語ファイル	「参照」をクリックして、ローカル PC の言語ファイルを選択します。

「適用」をクリックし、言語ファイルをインストールします。

リセット

スイッチの設定内容を工場出荷時状態に戻します。

ツール > リセットをクリックし、次の設定画面を表示します。

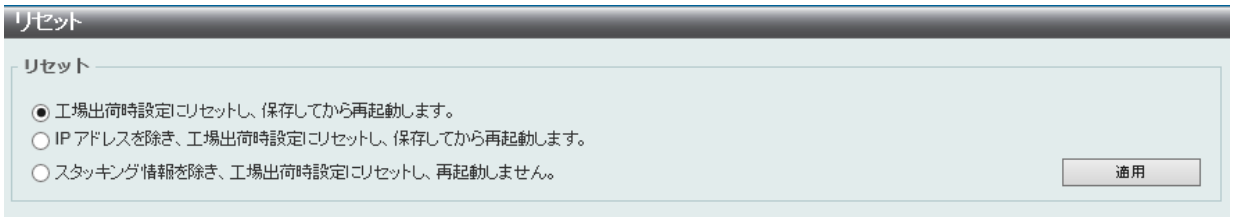


図 16-28　リセット画面

画面に表示される項目：

項目	説明
工場出荷時設定にリセットし、保存してから再起動します。	スイッチを工場出荷時設定にリセットして、保存、再起動を実行します。 (IP アドレス、スタック情報を含む)
IP アドレスを除き、工場出荷時設定にリセットし、保存してから再起動します。	スイッチを工場出荷時の設定に戻し、保存、再起動を実行します。 (IP アドレスは除く)
スタッキング情報を除き、工場出荷時設定にリセットし、再起動しません 。	スイッチを工場出荷時設定にリセットしますが、再起動は行いません。 (スタック情報は除く)

「適用」をクリックして、リセットを開始します。

システム再起動

スイッチの再起動を行います。

ツール > システム再起動をクリックし、以下の設定画面を表示します。

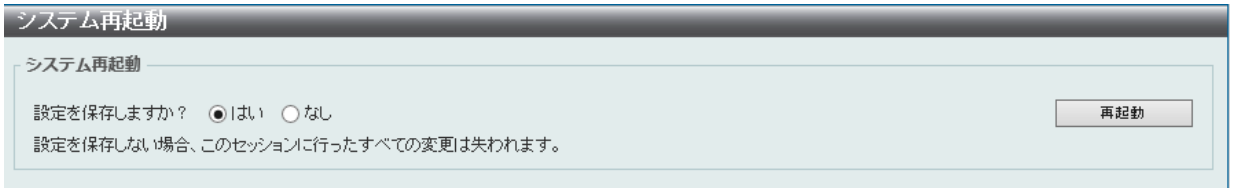


図 16-29　システム再起動画面

画面に表示される項目：

項目	説明
設定を保存しますか？	再起動オプションを指定します。 • 「はい」- スイッチは再起動する前に現在の設定を保存します。 • 「なし」- スイッチは再起動する前に現在の設定を保存しません。 すべての設定情報は破棄され、最後に保存した時の設定が使用されます。

「再起動」をクリックして再起動を開始します。

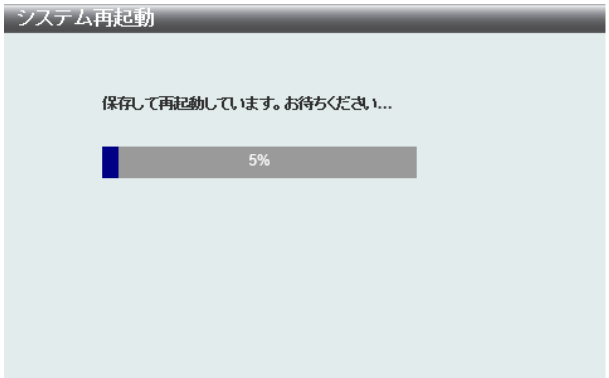


図 16-30　システム再起動画面

付録

付録 A パスワードリカバリ手順

弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。
権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用することです。ネットワーク管理者は、パスワードが忘れられたり、壊れた場合に、これらのパスワードをリセットする必要があります。このパスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下にパスワードを容易に回復するパスワードリカバリ機能の使用方法を説明します。

以下の手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することができます。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。
2. 電源をオンにします。「Password Recovery Mode」に入るためには、「UART init」が 100% までロードされた後 2 秒以内に、ホットキー「 ^ 」を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```
Boot Procedure                                          V1.00.007
--------------------------------------------------------------------------------

Power On Self Test ..................................... 100 %

MAC Address    : 80-26-89-15-28-00
H/W Version    : A1

Please Wait, Loading 2.00.008 Runtime Image ............... 100 %
UART init ................................................. 100 %
```

```
Password Recovery Mode
Switch(reset-config)#
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
no enable password	全アカウントレベルのパスワードを削除します。
no login password	ローカルログイン方法をクリアします。
no username	全ローカルユーザアカウントを削除します。
password-recovery	パスワードリカバリ手順を開始します。
reload	スイッチを再起動します。
reload clear running-config	起動中の設定を工場出荷値に戻し、保存、スイッチを再起動します。
show running-config	起動中の設定を表示します。
show username	ローカルユーザアカウント情報を表示します。

付録 B システムログエントリ

スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）、Notification（通知）

ログの内容	緊急度	イベントの説明
802.1X		
802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • reason：認証失敗の理由 • username：認証されているユーザ名 • interface-id：スイッチインタフェース番号 • mac-address：認証されたデバイスの MAC アドレス	Critical	802.1X 認証に失敗しました。
802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) **パラメータ説明：** • username：認証されたユーザ名 • interface-id：インタフェース名 • mac-address：認証されたデバイスの MAC アドレス	Informational	802.1X 認証に成功しました。
AAA		
AAA is <status> **パラメータ説明：** • status：AAA が有効または無効	Informational	AAA グローバルステートが有効または無効です。
Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Informational	ログインに成功しました。
Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 例：Console、Telnet、SSH、Web、Web(SSL) • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	ログインに失敗しました。

ログの内容	緊急度	イベントの説明
Login failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 例：Console、Telnet、SSH、Web、Web(SSL) • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	AAA サーバのタイムアウトまたは正しくない設定のためログインに失敗しました。
Successful enable privilege through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Informational	特権の有効化に成功しました。
Enable privilege failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) **パラメータ説明：** • exec-type：EXEC タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • aaa-method：認証方式。 （例：none、local、server） • server-ip：認証方式がリモートサーバの場合の AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	特権の有効化に失敗しました。
Enable privilege failed through <exec-type> [from <client-ip>] due to AAA server <server-ip> timeout (Username: <username>) **パラメータ説明：** • exec-type:：EXEC タイプ。 （例：Console、Telnet、SSH、Web、Web(SSL)） • client-ip：IP プロトコルを通し有効なクライアントの IP アドレス • server-ip：AAA サーバ IP アドレス • username：認証されるユーザ名	Warning	リモートサーバが有効なパスワード認証リクエストに応答しません。
RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • vid：RADIUS サーバから認証された VLAN ID 割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な VLAN ID 属性を割り当てました。
RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface -id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • direction:：帯域幅制御の方向。 （例：イングレスまたはイーグレス） • threshold: サーバから認証された帯域幅のしきい値割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な帯域幅属性を割り当てました。

ログの内容	緊急度	イベントの説明
RADIUS server <server-ip> assigned 802.1p default priortiy: <priority> to port < interface -id> (Username: <username>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • priority：RADIUS サーバから認証された優先度割り当て • interface–id：認証されたクライアントのポート番号 • username：認証されるユーザ名	Informational	RADIUS が有効な優先度属性を割り当てました。
RADIUS server <server-ip> assigns <username> ACL failure at port < interface -id> (<acl-script>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • username：認証されるユーザ名 • interface–id：認証されたクライアントのポート番号 • acl-script：RADIUS サーバから認証された ACL スクリプト	Warning	RADIUS が ACL スクリプトを割り当てましたが、不十分なリソースのためシステムへの適用に失敗しました。
RADIUS server <server-ip> assigns <username> ACL success at port < interface -id> (<acl-script>) **パラメータ説明：** • server-ip：RADIUS サーバの IP アドレス • username：認証されるユーザ名 • interface–id：認証されたクライアントのポート番号 • acl-script：RADIUS サーバから認証された ACL スクリプト	Informational	RADIUS が割り当てた ACL スクリプトがシステムに適用されました。
ARP		
Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>). **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • unitID：ユニット番号 • portNum：ポート番号 • ipif_name：IP インタフェース名	Warning	Gratuitous ARP は重複した IP を検出しました。
ARP Spoofing Prevention		
Gateway <ipaddr> is under attack by <macaddr> from <intf-name> **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • intf_name：インタフェース名	Warning	偽の ARP パケットが ARP スプーフィング防止で検出されました。
Auto image		
The downloaded firmware was successfully executed by DHCP Auto image update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：IP アドレス	Informational	DHCP 自動イメージによるファームウェアダウンロードは成功しました。
The downloaded firmware was not successfully executed by DHCP Autoimage update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：IP アドレス	Informational	DHCP 自動イメージによるファームウェアダウンロードは失敗しました。
Auto Save		
CONFIG-6-DDPSAVECONFIG: [Unit <unitID>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) **パラメータ説明：** • unitID：ボックス ID • username：ユーザ名 • ipaddr：IP アドレス	Informational	DDP の設定情報が自動で保存されました。

ログの内容	緊急度	イベントの説明
Auto Surveillance VLAN		
New surveillance device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface–id：インタフェース名（ID） • mac-address：MAC アドレス	Informational	インタフェースで新しい監視デバイスが検出されました。
<interface-id> add into surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名（ID） • vid：VLAN ID	Informational	サーベイランス VLAN が有効のインタフェースが自動的にサーベイランス VLAN に追加されました。
<interface-id> remove from surveillance VLAN <vid> **パラメータ説明：** • interface–id：インタフェース名（ID） • vid：VLAN ID	Informational	インタフェースがサーベイランス VLAN から離脱しました。同時に一定の期間内に当該のインタフェースに監視デバイスが検出されず、ログメッセージが送信されました。
BPDU Protection		
<interface-id> enter STP BPDU under protection state (mode: <mode>) **パラメータ説明：** • interface–id：STP BPDU アタックが検出されたインタフェース • mode：インタフェースの BPDU プロテクションモード。モードは、ドロップ、ブロック、またはシャットダウンにすることができます。	Informational	BPDU アタックが発生しました。
<interface-id> recover from BPDU under protection state **パラメータ説明：** • interface–id：STP BPDU アタックが検出されたインタフェース	Informational	STP BPDU 攻撃から回復しました。
Configuration/Firmware		
[Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Informational	ファームウェアのアップグレードに成功しました。
[Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Warning	ファームウェアのアップグレードに失敗しました。

ログの内容	緊急度	イベントの説明
[Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Informational	ファームウェアのアップロードに成功しました。
[Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Warning	ファームウェアのアップロードに失敗しました。
[Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Informational	コンフィグレーションのダウンロードに成功しました。
[Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • Username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Warning	コンフィグレーションのダウンロードに失敗しました。
[Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Informational	コンフィグレーションのアップロードに成功しました。

ログの内容	緊急度	イベントの説明
[Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Warning	コンフィグレーションのアップロードに失敗しました。
[Unit <unitID>,]Configuration saved to flash by console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名	Informational	コンソールによりコンフィグレーションが Flash に保存されました。
[Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • unitID：ユニット ID • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス	Informational	リモートによりコンフィグレーションが Flash に保存されました。
[Unit <unitID>,] Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Informational	ログメッセージのアップロードに成功しました。
[Unit <unitID>,] Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス	Warning	ログメッセージのアップロードに失敗しました。
[Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) **パラメータ説明：** • unitID：ユニット ID • session：ユーザのセッション • username：現在のログインユーザ名 • ipaddr：クライアントの IP アドレス • macaddr：クライアントの MAC アドレス • serverIP：サーバの IP アドレス • pathFile：サーバのパスとファイル名	Warning	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。
DAD		
Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Solicitation Messages **パラメータ説明：** • ipv6address：NS メッセージの IPv6 アドレス • interface-id：ポートインタフェース ID	Warning	DAD の間に DUT が「Neighbor Solicitation」(NS) メッセージを重複アドレスとともに受信しました。

ログの内容	緊急度	イベントの説明
Duplicate address <ipv6address > on <interface-id> via receiving Neighbor Advertisement Messages **パラメータ説明：** • ipv6address：NA メッセージの IPv6 アドレス • interface-id：ポートインタフェース ID	Warning	DAD の間に DUT が「Neighbor Advertisement」(NA) メッセージを重複アドレスとともに受信しました。
Dynamic ARP Inspection（DAI）		
Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>). **パラメータ説明：** • type：ARP パケットの種類。ARP パケットが、「request」か「ARP response」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 ID	Warning	DAI が無効な ARP パケットを検出しました。
Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) **パラメータ説明：** • type：ARP パケットの種類。ARP パケットが、「request」か「ARP response」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 ID	Informational	DAI が有効な ARP パケットを検出しました。
DDM		
Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のうちのどれか 1 つ。 - temperature - supply voltage - bias current - TX power - RX power - high-low：高もしくは低しきい値	Warning	SFP パラメータのどれかが警告しきい値を超えました。
Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のうちのどれか 1 つ。 - temperature - supply voltage - bias current - TX power - RX power - high-low：高もしくは低しきい値	Critical	SFP パラメータのどれかがアラームしきい値を超えました。

ログの内容	緊急度	イベントの説明
Optical transceiver <interface-id> <component> back to normal **パラメータ説明：** • interface-id：ポートインタフェース ID • component：DDM のしきい値タイプ。しきい値タイプは以下のうちのどれか 1 つ。 - temperature - supply voltage - bias current - TX power - RX power - high-low：高もしくは低しきい値	Warning	SFP パラメータのどれかが警告しきい値から回復しました。
DHCPv6 Client		
DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 クライアントインタフェース管理者ステートが変更されました。
DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name> **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された Ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	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。
The IPv6 address < ipv6address > on interface <ipif-name> starts renewing **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された Ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得した IPv6 アドレスが更新を開始します。
The IPv6 address < ipv6address > on interface <ipif-name> renews success **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された Ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスの更新に成功しました。
The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された Ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスのリバインドを開始します。
Log Message: The IPv6 address < ipv6address > on interface <ipif-name> rebinds success **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された Ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバから取得された IPv6 アドレスがリバインドに成功しました。
The IPv6 address < ipv6address > on interface <ipif-name> was deleted **パラメータ説明：** • ipv6address：DHCPv6 サーバから取得された Ipv6 アドレス • ipif-name：DHCPv6 クライアントインタフェース名	Informational	DHCPv6 サーバからの IPv6 アドレスが削除されました。
DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> **パラメータ説明：** • intf-name：DHCPv6 クライアント PD インタフェース名	Informational	DHCPv6 クライアント PD インタフェースの管理者ステートが変更されました。
DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> **パラメータ説明：** • ipv6networkaddr : デリゲイション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 インタフェース名	Informational	DHCPv6 クライアント PD が、デリゲイションルータから IPv6 プレフィックスを取得しました。

ログの内容	緊急度	イベントの説明
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing **パラメータ説明：** • ipv6networkaddr : デリゲイション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 インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスは更新を開始します。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success **パラメータ説明：** • ipv6networkaddr : デリゲイション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 インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスは更新に成功しました。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding **パラメータ説明：** • ipv6networkaddr : デリゲイション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 インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスはリバインディングを開始します。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success **パラメータ説明：** • ipv6networkaddr : デリゲイション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 インタフェース名	Informational	デリゲイションルータから取得した IPv6 プレフィックスはリバインドに成功しました。
The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted **パラメータ説明：** • ipv6networkaddr : デリゲイション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 インタフェース名	Informational	デリゲイションルータからの IPv6 プレフィックスは削除されました。
DHCPv6 Relay		
DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] **パラメータ説明：** • <ipif-name>：DHCPv6 リレーエージェントインタフェース名	Informational	特定のインタフェースの管理者ステートの DHCPv6 リレーが変更されました。
DHCPv6 Server		
The address of the DHCPv6 Server pool <pool-name> is used up. **パラメータ説明：** • <pool-name>：DHCPv6 サーバプール名	Informational	DHCPv6 サーバプールのアドレスが枯渇しました。
The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.	Informational	割り当てられた IPv6 アドレス数が 4096 に達しました。
DNS Resolver		
[DNS_RESOLVER(1):]Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> **パラメータ説明：** • domainame：ドメイン名文字列 • ipaddr：IP アドレス	Informational	重複するドメイン名キャッシュが追加され、ダイナミックドメイン名キャッシュが削除されました。
DoS Prevention		
<dos-type> is dropped from (IP: <ip-address> Port <interface-id>). **パラメータ説明：** • dos-type：DoS 攻撃タイプ • ip-address:：IP アドレス • interface-id:：インタフェース名	Notification	DoS 攻撃を検出しました。
ErrDisable		
Port <interface-id> enters error disable state due to <reason-id> **パラメータ説明：** • interface-id:：インタフェース名 • reason-id：Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning	ポートが error-disabled モードになりました。

ログの内容	緊急度	イベントの説明
Port <interface-id> leaves the error disable state which is previously caused by <reason-id> **パラメータ説明：** • interface-id:：インタフェース名 • reason-id：Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning	ポートが error-disabled モードではなくなりました。
Port <interface-id> VLAN <vid> enters error disable state due to <reason-id> **パラメータ説明：** • interface-id：インタフェース名 • reason-id：Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. • vid：VLAN ID	Warning	ポートが error-disabled モードになりました。
Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> **パラメータ説明：** • interface-id：インタフェース名 • reason-id：Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. • vid：VLAN ID	Warning	ポートが error-disabled モードではなくなりました。
Interface		
Port <port-type>< interface-id> link down **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース名	Informational	ポートがリンクダウンしました。
Port <port-type>< interface-id> link up, <link-speed> **パラメータ説明：** • port-type：ポートタイプ • interface-id：インタフェース名 • link-speed：ポートのリンクスピード	Informational	ポートがリンクアップしました。
IP Source Guard（IPSG）		
Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) **パラメータ説明：** • ipaddr：IP アドレス • macaddr：MAC アドレス • vlanid：VLAN ID • interface-id：インタフェース ID	Warning	DHCP スヌーピングエントリを ISPG テーブルにセットするに当たり、ハードウェアルールのリソースがない場合、シスログが記録されます。
IPv6 Snooping		
Failed to glean (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Port <interface-id>) **パラメータ説明：** • ipaddr：IPv6 アドレス • macaddr：MAC アドレス • vlanid：VLAN ID • interface-id：インタフェース ID	Notification	IPv6 Data Glean に失敗しました。

ログの内容	緊急度	イベントの説明
Glean to recover (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Port <interface-id>) **パラメータ説明：** • ipaddr：IPv6 アドレス • macaddr：MAC アドレス • vlanid：VLAN ID • interface-id：インタフェース ID	Informational	IPv6 Data Glean に成功しました。
IPv6 Source Guard		
Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) **パラメータ説明：** • ipaddr：IPv6 アドレス • macaddr：MAC アドレス • vlanid：VLAN ID • interface-id：インタフェース ID	Warning	DHCP スヌーピングエントリを IPv6SG テーブルにセットするに当たり、ハードウェアルールのリソースがない場合、シスログが記録されます。
LACP		
Link Aggregation Group <group_id> link up. **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクアップします。
Link Aggregation Group <group_id> link down. **パラメータ説明：** • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	リンクアグリゲーショングループがリンクダウンします。
<ifname> attach to Link Aggregation Group <group_id>. **パラメータ説明：** • ifname：アグリゲーショングループにアタッチするポートのインタフェース名 • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにアタッチします。
<ifname> detach from Link Aggregation Group <group_id>. **パラメータ説明：** • ifname：アグリゲーショングループにアタッチするポートのインタフェース名 • group-id：リンクアップアグリゲーショングループのグループ ID	Informational	メンバポートがリンクアグリゲーショングループにデタッチします。
LBD（ループバック検知）		
<interface-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検出されたインタフェース	Critical	ポートベースモードでループバックが検出されました。
<interface-id> VLAN <vlan-id> LBD loop occurred **パラメータ説明：** • interface-id：ループが検出されたインタフェース • vlan-id：ループが検出された VLAN ID	Critical	VLAN ベースモードでループバックが検出されました。
<interface-id> LBD loop recovered **パラメータ説明：** • interface-id：ループが検出されたインタフェース	Critical	ポートベースモードでループバックから回復しました。
<interface-id> VLAN <vlan-id> LBD loop recovered **パラメータ説明：** • interface-id：ループが検出されたインタフェース • vlan-id：ループが検出された VLAN ID	Critical	VLAN ベースモードでループバックからポートが回復しました。
Loop VLAN numbers overflow	Critical	ループバックが発生した VLAN の数が指定の数に達しました。

ログの内容	緊急度	イベントの説明
LLDP-MED		
LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 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 値のリスト： 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	Notification	LLDP-MED トポロジの変更が検出されました。
Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 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 値のリスト： 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	Notification	LLDP-MED デバイスタイプの重複が検出されました。

ログの内容	緊急度	イベントの説明
Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) **パラメータ説明：** • portNum：ポート番号 • chassisType：シャーシ ID サブタイプ 値のリスト： 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 値のリスト： 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	Notification	LLDP-MED TLV の非互換性が検出されました。
Login/Logout		
[Unit <unitID>,]Successful login through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：ユーザ名	Informational	コンソール経由のログインに成功しました。
[Unit <unitID>,] Login failed through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：ユーザ名	Warning	コンソール経由のログインに失敗しました。
[Unit <unitID>,] Console session timed out (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：ユーザ名	Informational	コンソールのセッションはタイムアウトしました。
[Unit <unitID>,] Logout through Console (Username: <username>) **パラメータ説明：** • unitID：ユニット ID • username：ユーザ名	Informational	コンソール経由でログアウトしました。
Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由のログインに成功しました。
Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Warning	Telnet 経由のログインに失敗しました。

ログの内容	緊急度	イベントの説明
Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet のセッションはタイムアウトしました。
Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	Telnet 経由でログアウトしました。
Successful login through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	SSH 経由のログインに成功しました。
Login failed through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Critical	SSH 経由のログインに失敗しました。
SSH session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	SSH のセッションはタイムアウトしました。
Logout through SSH (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • username：現在のログインユーザ • ipaddr：クライアントの IP アドレス	Informational	SSH 経由でログアウトしました。
MAC（MAC 認証）		
MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id> **パラメータ説明：** • mac-address：ホストの MAC アドレス • interface-id：ホストが認証されたインタフェース • vlan-id：ホストが存在する VLAN ID	Informational	ホストは MAC 認証をパスしました。
MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>). **パラメータ説明：** • mac-address：ホストの MAC アドレス • interface-id：ホストが認証されたインタフェース • vlan-id：ホストが存在する VLAN ID	Informational	ホストはエージアウトしました。
MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>). **パラメータ説明：** • mac-address：ホストの MAC アドレス • interface-id：ホストが認証されたインタフェース • vlan-id：ホストが存在する VLAN ID	Critical	ホストは認証に失敗しました。
MAC-based Access Control enters stop learning state..	Warning	デバイス全体で認証されたユーザ数がユーザの最大制限数に達しました。
MAC-based Access Control recovers from stop learning state	Warning	デバイス全体で認証されたユーザ数が時間間隔内のの最大ユーザ制限数未満になりました。

ログの内容	緊急度	イベントの説明
<interface-id> enters MAC-based Access Control stop learning state **パラメータ説明：** • interface-id：ホストが認証されたインタフェース	Warning	インタフェースの認証されたユーザ数が最大ユーザ制限数に達しました。
<interface-id> recovers from MAC-based Access Control stop learning state **パラメータ説明：** • interface-id：ホストが認証されたインタフェース	Warning	インタフェースの認証されたユーザ数が時間間隔内の最大ユーザ制限数未満になりました。
MSTP Debug		
Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化
Topology changed [([Instance:<Instance-id>] ,port:< portNum> ,MAC: <macaddr>)] **パラメータ説明：** • Instance-id：インスタンス ID • portNum：ポート番号 • macaddr：MAC アドレス	Notification	トポロジに変更がありました。
[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <Instance-id>]MAC: <macaddr> Priority :<value>) **パラメータ説明：** • Instance-id：インスタンス ID • macaddr：MAC アドレス • value：優先値	Informational	新しいルートブリッジが選定されました。
New root port selected (Instance:<Instance-id>, <interface_id>) **パラメータ説明：** • Instance-id：インスタンス ID • interface_id：ポート番号	Notification	新しいルートポートが選定されました。
Spanning Tree port status change (Instance :<Instance-id>, <interface_id>) <old_status> -> <new_status> **パラメータ説明：** • Instance-id：インスタンス ID • interface_id：ポート番号 • old_status：旧ステータス • new_status：新ステータス	Notification	スパニングツリーポートのステートが変更されました。
Spanning Tree port role change (Instance :<Instance-id>, <interface_id>) <old_role> -> <new_role> **パラメータ説明：** • Instance-id：インスタンス ID • interface_id：ポート番号 • old_role：旧ロール • new_role：新ロール	Informational	スパニングツリーポートのロールが変更されました。
Spanning Tree instance created (Instance :< Instance-id >) **パラメータ説明：** • Instance-id：インスタンス ID	Informational	スパニングツリーインスタンスが作成されました。
Spanning Tree instance deleted (Instance :< Instance-id >) **パラメータ説明：** • Instance-id：インスタンス ID	Informational	スパニングツリーインスタンスが削除されました。
Spanning Tree version change (new version :< new_version>) **パラメータ説明：** • new_version：新しいスパニングツリーのバージョン	Informational	スパニングツリーのバージョンが変更されました。

ログの内容	緊急度	イベントの説明
Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>). **パラメータ説明：** • name：指定された MST リージョンの名前 • revision_level：リビジョンレベル	Informational	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更されました。
Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • Instance-id：インスタンス ID • startvlanid：追加する VLAN 範囲の開始 VID • endvlanid：追加する VLAN 範囲の終了 VID	Informational	VLAN が MST インスタンスにマッピングされました。
Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]) **パラメータ説明：** • Instance-id：インスタンス ID • startvlanid：削除する VLAN 範囲の開始 VID • endvlanid：削除する VLAN 範囲の終了 VID	Informational	MST インスタンスから VLAN を削除しました。
Spanning Tree port role change (Instance : <InstanceID>, <Interface_id>) to alternate port due to the guard root. **パラメータ説明：** • Instance-id：インスタンス ID • Interface_id：ポート番号	Informational	ガードルートのためにスパニングツリーポートロールが交代します。
Spanning Tree loop guard blocking(Instance : <InstanceID>, <Interface_id>) **パラメータ説明：** • Instance-id：インスタンス ID • Interface_id：ポート番号	Informational	スパニングツリーループガードがブロックしています。
OSPFv2		
OSPF interface <intf-name> changed state to [Up | Down] **パラメータ説明：** • intf-name：OSPF インタフェース	Informational	OSPF インタフェースのリンクステートが変更されました。
OSPF protocol on interface <intf-name> changed state to [Enabled | Disabled] **パラメータ説明：** • intf-name：OSPF インタフェース	Informational	OSPF インタフェースの管理者ステートが変更されました。
OSPF interface <intf-name> changed from area <area-id> to area <area-id> **パラメータ説明：** • intf-name：OSPF インタフェース • area-id：OSPF エリア ID	Informational	OSPF インタフェースがエリア変更されました。
OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full **パラメータ説明：** • intf-name：OSPF インタフェース • nbr-id：ネイバルータ ID	Notification	OSPF ネイバステートが「Loading」から「Full」に変更されました。
OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down **パラメータ説明：** • intf-name：OSPF インタフェース • nbr-id：ネイバルータ ID	Notification	OSPF ネイバステートが「Full」から「Down」に変更されました。
OSPF nbr <nbr-id> on interface <intf-name> dead timer expired **パラメータ説明：** • intf-name：OSPF インタフェース • nbr-id：ネイバルータ ID	Notification	OSPF ネイバステートデッドタイマ期限が切れました。

ログの内容	緊急度	イベントの説明
OSPF nbr <nbr-id> on virtual link changed state from Loading to Full **パラメータ説明：** • nbr-id：ネイバルータ ID	Notification	OSPF 仮想ネイバステートが「Loading」から「Full」に変わりました。
OSPF nbr <nbr-id> on virtual link changed state from Full to Down **パラメータ説明：** • nbr-id：ネイバルータ ID	Notification	OSPF 仮想ネイバステートが「Full」から「Down」に変わりました。
OSPF router ID changed to <router-id> **パラメータ説明：** • router-id：OSPF ルータ ID	Informational	OSPF ルータ ID が変更されました。
Peripheral (周辺機器)		
Unit <unit-id>, <fan-descr> back to normal **パラメータ説明：** • unit-id：ユニット ID • fan-descr：ファン概要	Critical	ファンが回復しました。
Unit <unit-id> <fan-descr> failed **パラメータ説明：** • unit-id：ユニット ID • fan-descr：ファン概要	Critical	ファンの故障
Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> **パラメータ説明：** • unit-id：ユニット ID • thermal-sensor-descr：センサ ID • degree：温度	Critical	温度センサがアラーム状態に入りました。
Unit <unit-id> <thermal-sensor-descr> temperature back to normal **パラメータ説明：** • unit-id：ユニット ID • thermal-sensor-descr：センサ ID	Critical	温度が通常に戻りました。
Unit <unit-id> <power-descr> failed **パラメータ説明：** • unit-id：ユニット ID • power-descr：電源 ID	Critical	電源故障
Unit <unit-id> <power-descr> back to normal **パラメータ説明：** • unit-id：ユニット ID • power-descr：電源 ID	Critical	電源回復
Unit <unit-id> factory reset button pressed **パラメータ説明：** • unit-id：ユニット ID	Critical	リセットボタンが押されました。
PoE		
Unit <unit-id> usage threshold <percentage> is exceeded **パラメータ説明：** • unit-id：ユニット ID • percentage：使用率しきい値	Warning	総電力の使用率がしきい値を超えました。
Unit <unit-id> usage threshold <percentage> is recovered **パラメータ説明：** • unit-id：ユニット ID • percentage：使用率しきい値	Warning	総電力の使用率がしきい値を下回りました。

ログの内容	緊急度	イベントの説明
PD alive check failed. (Port: <portNum>, PD: <ipaddr>) **パラメータ説明：** • portNum：ポート番号 • ipaddr：IP アドレス	Warning	PD が Ping リクエストに回答しません。
Port Security		
MAC address <macaddr> causes port security violation on <interface-id> **パラメータ説明：** • macaddr：違反 MAC アドレス • interface-id：インタフェース名	Warning	ポート上のアドレスが超過
Limit on system entry number has been exceeded	Warning	システム上のアドレスが超過
Safeguard		
Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode **パラメータ説明：** • unit-id：ユニット ID	Warning	CPU 使用率がしきい値を超え、スイッチは「exhausted」モードに移行、Syslog に記録されます。
Unit <unit-id>, Safeguard Engine enters NORMAL mode **パラメータ説明：** • unit-id：ユニット ID	Informational	CPU 使用率がしきい値を下回り、スイッチはノーマルモードに移行、Syslog に記録されます。
SNMP		
SNMP request received from <ipaddr> with invalid community string **パラメータ説明：** • ipaddr：IP アドレス	Informational	SNMP リクエストは無効なコミュニティストリングを受信しました。
SSH		
SSH server is enabled	Informational	SSH サーバは有効
SSH server is disabled	Informational	SSH サーバは無効
Stacking		
Unit: <unitID>, MAC: <macaddr> Hot insertion. **パラメータ説明：** • unitID：ユニット ID • macaddr：MAC アドレス ID	Informational	デバイスが挿入されました。
Unit: <unitID>, MAC: <macaddr> Hot removal. **パラメータ説明：** • unitID：ユニット ID • macaddr：MAC アドレス ID	Informational	デバイスが削除されました。
Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>) **パラメータ説明：** • Stack_TP_TYPE：スタッキングトポロジタイプ 1. Ring 2. Chain • unitID：ボックス ID • macaddr：MAC アドレス	Critical	スタッキングトポロジ変更
Backup master changed to master. Master (Unit: <unitID>) **パラメータ説明：** • unitID：ボックス ID	Informational	バックアップマスタがマスタに変更
Slave changed to master. Master (Unit: <unitID>) **パラメータ説明：** • unitID：ボックス ID	Informational	スレーブがマスタに変更

ログの内容	緊急度	イベントの説明
Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>) **パラメータ説明：** • unitID：ボックス ID • macaddr：MAC アドレス	Critical	ボックス ID が重複
Stacking port <port> link up **パラメータ説明：** • port：スタックポート番号	Critical	スタックポートがリンクアップ
Stacking port <port> link down **パラメータ説明：** • port：スタックポート番号	Critical	スタックポートがリンクダウン
SIO interface Unit <unitID> <SIOn> link up **パラメータ説明：** • unitID：SIO インタフェースがリンクアップしているボックス ID • SIOn：SIO インタフェース番号。サポートされている SIO インタフェース番号は「SIO1」か「SIO2」です。	Critical	SIO インタフェースがリンクアップ
SIO interface Unit <unitID> <SIOn> link down **パラメータ説明：** • unitID：SIO インタフェースがリンクアップしているボックス ID • SIOn：SIO インタフェース番号。サポートされている SIO インタフェース番号は「SIO1」か「SIO2」です。	Critical	SIO インタフェースがリンクダウン
Storm Control		
<Broadcast | Multicast | Unicast> storm is occurring on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Warning	ストーム発生
<Broadcast | Multicast | Unicast> storm is cleared on <interface-id> **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Informational	ストームが解消されました。

ログの内容	緊急度	イベントの説明
<interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm **パラメータ説明：** • Broadcast：ブロードキャストパケット (DA = FF:FF:FF:FF:FF:FF）によるストーム • Multicast：未知の L2 マルチキャスト、既知の L2 マルチキャスト、未知の IP マルチキャストと既知の IP マルチキャストを含むマルチキャストパケットによるストーム • Unicast：既知と未知のユニキャストパケットを含むユニキャストパケットによるストーム • interface-id：ストーム発生のインタフェース ID	Warning	パケットストームによりポートシャットダウン
System		
[Unit <unitID>,]System warm start **パラメータ説明：** • unitID：ユニット ID	Critical	システムがウォームスタートしました。
[Unit <unitID>,]System cold start **パラメータ説明：** • unitID：ユニット ID	Critical	システムがコールドスタートしました。
[Unit <unitID>,]System started up. **パラメータ説明：** • unitID：ユニット ID	Critical	システムが起動しました。
Telnet		
Successful login through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバーにログインするユーザ名	Informational	Telnet 経由のログインに成功しました。
Login failed through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバーにログインするユーザ名	Warning	Telnet 経由のログインに失敗しました。
Logout through Telnet (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバーにログインするユーザ名	Informational	Telnet からログアウトしました。
Telnet session timed out (Username: <username>, IP: <ipaddr>) **パラメータ説明：** • ipaddr：Telnet クライアントの IP アドレス • username：Telnet サーバーにログインするユーザ名	Informational	Telnet セッションのタイムアウト
Voice VLAN		
New voice device detected (<interface-id>, MAC: <mac-address>) **パラメータ説明：** • interface-id：インタフェース ID • mac-address：MAC アドレス	Informational	インタフェースで音声機器が検出されました。
<interface-id> add into voice VLAN <vid> **パラメータ説明：** • vid：VLAN ID • interface-id：インタフェース ID	Informational	自動音声 VLAN モードのインタフェースが音声 VLAN に追加されました。

ログの内容	緊急度	イベントの説明
<interface-id> remove from voice VLAN <vid> **パラメータ説明：** • vid：VLAN ID • interface-id：インタフェース ID	Informational	インタフェースが音声 VLAN から離脱し、一定期間内に音声機器がインタフェースに検出されませんでした。ログメッセージが送信されます。
VRRP Debug（VRRP デバッグ）		
VR <vr-id> at interface <intf-name> switch to Master **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Informational	ある仮想ルータがマスタに移行しました。
VR <vr-id> at interface <intf-name> switch to Backup **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Informational	ある仮想ルータがバックアップに移行しました。
VR <vr-id> at interface <intf-name> switch to Init **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Informational	ある仮想ルータが「Init」に移行しました。
Authentication type mismatch on VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	認証タイプが受信した VRRP アドバタイズメッセージと合致しません。
Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名 • auth-type：VRRP インタフェース認証タイプ	Warning	受信した VRRP アドバタイズメッセージのチェックに失敗しました。
Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	受信した VRRP アドバタイズメッセージのチェックにエラーが発生しました。
Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	受信した VRRP アドバタイズメッセージと仮想ルータ ID が合致しません。
Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> **パラメータ説明：** • vr-id：VRRP 仮想ルータ ID • intf-name：仮想ルータがベースにしているインタフェース名	Warning	受信した VRRP アドバタイズメッセージとアドバタイズメント間隔が合致しません。
Added a virtual MAC <vrrp-mac-addr> into L2 table **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notification	仮想 MAC アドレスがスイッチの L2 テーブルに追加されました。
Deleted a virtual MAC <vrrp-mac-addr> from L2 table **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notification	仮想 MAC アドレスがスイッチの L2 テーブルから削除されました。

ログの内容	緊急度	イベントの説明
Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notification	仮想 MAC アドレスがスイッチの L3 テーブルに追加されました。
Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Notification	仮想 MAC アドレスがスイッチの L3 テーブルから削除されました。
Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップ L2 テーブルへの仮想 MAC の追加に失敗しました。
Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップ L2 テーブルの仮想 MAC の削除に失敗しました。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。L3 テーブルは満杯です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • mac-port：VRRP 仮想 MAC のポート番号	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したポートが無効です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • mac-intf：VRRP 仮想 MAC アドレスを基にしたインタフェース	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したインタフェースが無効です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • mac-box：VRRP 仮想 MAC アドレスを基にしたインタフェース	Error	スイッチ L3 テーブルへの仮想 MAC の追加に失敗しました。MAC を学習したボックスが無効です。
Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップの L3 テーブルへの仮想 MAC の追加に失敗しました。

ログの内容	緊急度	イベントの説明
Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> **パラメータ説明：** • vrrp-ip-addr：VRRP IP アドレス • vrrp-mac-addr：VRRP 仮想 MAC アドレス • vrrp-errcode：VRRP プロトコル動作のエラーコード	Error	スイッチチップの L3 テーブルへの仮想 MAC の削除に失敗しました。
Web		
Successful login through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログインに成功しました。
Login failed through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Warning	Web 経由でのログインに失敗しました。
Web session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web セッションがタイムアウトしました。
Logout through Web (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログアウトしました。
Successful login through Web (SSL) (Username: <username>, IP:<ipaddr>) **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログイン成功（SSL）
Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Warning	Web 経由でのログイン失敗（SSL）
Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web セッションがタイムアウトしました。（SSL）
Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). **パラメータ説明：** • username：ユーザ名 • ipaddr：IP アドレス	Informational	Web 経由でのログアウト成功（SSL）
Web Authentication		
Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) **パラメータ説明：** • string：ユーザ名 • ipaddr：IP アドレス • ipv6address：IPv6 アドレス • mac-address：MAC アドレス • interface-id：ポート番号 • vlan-id：VLAN ID	Informational	クライアントホストが認証に成功しました。

ログの内容	緊急度	イベントの説明
Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) **パラメータ説明：** • string：ユーザ名 • ipaddr：IP アドレス • ipv6address：IPv6 アドレス • mac-address：MAC アドレス • interface-id：ポート番号 • vlan-id：VLAN ID	Warning	クライアントホストが認証に失敗しました。
Web-Authentication enters stop learning state	Warning	デバイス全体において認証ユーザ数が最大値に達した時、本ログが生成されます。
Web-Authentication recovered from stop learning state	Warning	タイムインターバルのデバイス全体において認証ユーザ数が最大値を割り込んだ時、本ログが生成されます。
ZTP		
The downloaded firmware was successfully executed by ZTP update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：IP アドレス	Informational	ZTP ファームウェアアップデートに成功しました。
The downloaded firmware was not successfully executed by ZTP update (TFTP Server IP: <ipaddr>) **パラメータ説明：** • ipaddr：IP アドレス	Informational	ZTP ファームウェアアップデートに失敗しました。

付録 C トラップログエントリ

スイッチにおいて現れる可能性のあるトラップログエントリとそれらの意味を以下に示します。

カテゴリ	トラップ名	説明	OID
802.1X	dDot1xExtLoggedSuccess	ホストがログインに成功したときに送信されます。（802.1X 認証にパス） 関連オブジェクト： (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
	dDot1xExtLoggedFail	ホストが 802.1X 認証に失敗したときに送信されます。（ログインに失敗） 関連オブジェクト： (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.14.30.0.2
Authentication Fail（認証失敗）	authenticationFailure	authenticationFailure トラップは、SNMPv2 エンティティが、エージェントロールで動作し、正しく認証されないプロトコルメッセージを受信したことを表します。SNMPv2 のすべての実装は、このトラップを生成することができる必要がある一方、snmpEnableAuthenTraps オブジェクトは、このトラップが生成されるか否かを示します。	1.3.6.1.6.3.1.1.5.5
BPDU Protection	dBpduProtectionAttackOccur	インタフェースで BPDU アタックが発生したときに送信されます。 関連オブジェクト： (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.171.14.47.0.1
	dBpduProtectionAttackRecover	インタフェースで BPDU アタックが回復したときに送信されます。 関連オブジェクト： (1) ifIndex	1.3.6.1.4.1.171.14.47.0.2
DDM	dDdmAlarmTrap	異常なアラームが発生、または正常な状態に回復した際に通知されます。現在の値 > low warning または現在の値 < high warning にときにのみリカバトラップを送信します。 関連オブジェクト： (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.1
	dDdmWarningTrap	異常な警告が発生、または正常な状態に回復した際に通知されます。 関連オブジェクト： (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.2

カテゴリ	トラップ名	説明	OID
DHCP サーバスクリーン防止	dDhcpFilterAttackDetected	DHCP サーバスクリーンが有効なとき、スイッチが偽造 DHCP サーバパケットを受信すると、攻撃パケットを受信したイベントをトラップ送信します。 関連オブジェクト : (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1
DoS 防止	dDosPreveAttackDetectedPacket	DoS アタックを検出したとき送信されます。 関連オブジェクト : (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.59.0.2
ErrDisable	dErrDisNotifyPortDisabledAssert	ポートが error-disabled モードになったときに送信されます。 関連オブジェクト : (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
	dErrDisNotifyPortDisabledClear	インターバル後にポートループがリスタートした時に送信されます。 関連オブジェクト : (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2
Gratuitous ARP 機能	agentGratuitousARPTrap	IP アドレスが重複していた場合に送信されます。 関連オブジェクト : (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.14.75.0.1
IP-MAC-Port Binding（IMPB）	dImpbViolationTrap	アドレス違反通知は IP-MAC ポートバインディングアドレス違反が検出された際に生成されます。 関連オブジェクト : (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.171.14.22.0.1

カテゴリ	トラップ名	説明	OID
LACP	linkUp	「linkUp」トラップはエージェント役の SNMP エンティティによって、コミュニケーションリンクの一つが「notPresent」ステート以外の他のステートからダウンステートに移行しようとしている「ifOperStatus」オブジェクトの検出を意味します。他のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
	linkDown	「linkDown」トラップはエージェント役の SNMP エンティティによって、コミュニケーションリンクの一つがダウンステートに残り、「notPresent」ステート以外の他のステートに移行する「ifOperStatus」オブジェクトの検出を意味します。他のステートは「ifOperStatus」に含まれる値によって識別されます。 関連オブジェクト : (1) ifIndex, (2) if AdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3
LBD	swPortLoopOccurred	インタフェースにループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.1
	swPortLoopRestart	間隔時間後、インタフェースのループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.2
	swVlanLoopOccurred	インタフェースに VID ループが発生したときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.3
	swVlanLoopRestart	間隔時間後、VID のインタフェースループが再スタートしたときに送信されます。 関連オブジェクト : (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4
LLDP-MED	lldpRemTablesChange	「lldpRemTablesChange」通知は「lldpStatsRemTableLastChangeTime」変更時に送信されます。 関連オブジェクト : (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
	lldpXMedTopologyChangeDetected	ローカルポートに新しいリモートデバイスがアタッチされた、またはリモートデバイスがポートから切断 / 移動した場合のトポロジの変更を感知するローカルデバイスによって送信されます。 関連オブジェクト : (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

カテゴリ	トラップ名	説明	OID
MAC-based アクセス コントロール	dMacAuthLoggedSuccess	MAC ベースのアクセスコントロールホストがログインに成功したときに送信されます。 関連オブジェクト： (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.1
	dMacAuthLoggedFail	MAC ベースのアクセスコントロールホストがログインに失敗したときに送信されます。 関連オブジェクト： (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.2
	dMacAuthLoggedAgesOut	MAC ベースのアクセスコントロールホストがエージングアウトしたときに送信されます。 関連オブジェクト： (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.3
MAC Notification	dL2FdbMacNotification	本トラップはアドレステーブルの MAC アドレスに変更が生じたことを意味します。 関連オブジェクト： (1) dL2FdbMac ChangeNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
	dL2FdbMacNotificationWithVID	本トラップはアドレステーブルの MAC アドレス（VLAN ID）に変更が生じたことを意味します。 関連オブジェクト： (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2
MSTP	newRoot	newRoot トラップは、送信側の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。トラップは、新しいルートとして選出された後にすぐにブリッジによって送信され、その選出に続いてすぐに Topology Change Timer のアクションの起動などを行います。 本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.1
	topologyChange	topologyChange トラップは、構成するいずれかのポートが Learning 状態から Forwarding 状態に、Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。 本トラップの実行はオプションです	1.3.6.1.2.1.17.0.2

カテゴリ	トラップ名	説明	OID
Peripheral （周辺機器）	dEntityExtFanStatusChg	ファン状態の変更通知 （ファンの不具合 (dEntityExtEnvFanStatus is 'fault') または回復 (dEntityExtEnvFanStatus is 'ok')） 関連オブジェクト : (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.2.1.171.14.5.0.1
	dEntityExtThermalStatusChg	温度状態の変更通知 （温度警告 (dEntityExtEnvTempStatus is 'abnormal') または回復 (dEntityExtEnvTempStatus is 'ok')） 関連オブジェクト : (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.2.1.171.14.5.0.2
	dEntityExtPowerStatusChg	電力状態の変更通知（電源モジュールの不具合、または不具合からの回復） 関連オブジェクト : (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.2.1.171.14.5.0.3
	dEntityExtFactoryResetButton	リセットボタンが押下されました。 関連オブジェクト : (1) dEntityExtEnvPowerUnitId	1.3.6.1.2.1.171.14.5.0.5

カテゴリ	トラップ名	説明	OID
PIM6-SM	pimNeighborLoss	「pimNeighborLoss」通知はネイバとの近隣性の消失時を意味します。本通知はネイバタイマが期限切れになり、同じ IP バージョン、より低い IP アドレスの同じインタフェースにネイバがいない場合に起動します。本通知はカウンタ「pimNeighborLossCount」が増加し、「pimNieghborLossNotificationsPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト： (1) pimNeighborUpTime	1.3.6.1.2.1.157.0.1
	pimInvalidRegister	「pimInvalidRegister」通知はデバイスによって不正な PIM Register メッセージが受信された場合に起動します。 本通知はカウンタ「pimInvalidRegisterMsgsRcvd」が増加し、「pimInvalidRegisterNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト： (1) pimGroupMappingPimMode (2) pimInvalidRegisterAddressType (3) pimInvalidRegisterOrigin (4) pimInvalidRegisterGroup (5) pimInvalidRegisterRp	1.3.6.1.2.1.157.0.2
	pimInvalidJoinPrune	「pimInvalidJoinPrune」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimInvalidJoinPruneMsgsRcvd」が増加し、「pimInvalidJoinPruneNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト： (1) pimGroupMappingPimMode (2) pimInvalidJoinPruneAddressType (3) pimInvalidJoinPruneOrigin (4) pimInvalidJoinPruneGroup (5) pimInvalidJoinPruneRp (6) pimNeighborUpTime	1.3.6.1.2.1.157.0.3
	pimRPMappingChage	「pimRPMappingChange」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimRPMappingChangeCount」が増加し、「pimRPMappingChangeNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト： (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4
	pimInterfaceElection	「pimInterfaceElection」通知はデバイスによって不正な PIM Join/Prune メッセージが受信された場合に起動します。 本通知はカウンタ「pimInterfaceElectionWinCount」が増加し、「pimInterfaceElectionNotificationPeriod」によってレートリミットが指定されている場合も起動します。 関連オブジェクト： (1) pimInterfaceAddressType (2) pimInterfaceAddress	1.3.6.1.2.1.157.0.5

カテゴリ	トラップ名	説明	OID
PoE	pethMainPowerUsageOnNotification	使用率が PSE しきい値に到達した事を示唆しています。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
	pethMainPowerUsageOffNotification	使用率が PSE しきい値を下回った事を示唆しています。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
	dPoeIfPowerDeniedNotification	PSE 状況ダイアグラムが POWER_DENIED になった事を示唆する通知です。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1
	dPoeIfPowerOverLoadNotification	PSE 状況ダイアグラムが ERROR_DELAY_OVER になった事を示唆するトラップです。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171.14.24.0.2
	dPoeIfPowerShortCircuitNotification	PSE 状況ダイアグラムが ERROR_DELAY_SHORT になった事を示唆するトラップです。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。 関連オブジェクト : (1) pethPsePortShortCounter	1.3.6.1.4.1.171.14.24.0.3
	dPoeIfPdAliveFailOccurNotification	PD が動作を中止、回答不能になった事を示唆するトラップです。同じオブジェクトインスタンスによって通知が放出されるまで最低 500 ミリ秒が経過する必要があります。	1.3.6.1.4.1.171.14.24.0.4
Port	linkUp	ポートがリンクアップしたときに生成されます。 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.11.5.4
	linkDown	ポートがリンクダウンしたときに生成されます。 関連オブジェクト : (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.11.5.3
Port Security	dPortSecMacAddrViolation	ポートセキュリティトラップが有効な場合、事前定義されたポートセキュリティ設定に違反する新しい MAC アドレスが送出するトリガトラップメッセージです。 関連オブジェクト : (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.171.14.8.0.1

カテゴリ	トラップ名	説明	OID
RMON	risingAlarm	SNMP トラップは、アラームエントリが上昇しきい値超える時に生成され、SNMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
	fallingAlarm	SNMP トラップは、アラームエントリが下降しきい値を下回るときに生成され、NSMP トラップの送信に設定されたイベントを生成します。 関連オブジェクト : (1)alarmIndex (2) alarmVariable (3)alarmSampleType (4)alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2
Safeguard	dSafeguardChgToExhausted	システムが操作モードをノーマルから exhausted に変更したことを示します。 関連オブジェクト : (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
	dSafeguardChgToNormal	システムが操作モードを exhausted からノーマルに変更したことを示します。 関連オブジェクト : (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2

カテゴリ	トラップ名	説明	OID
SIM	swSingleIPMSColdStart	コマンダースイッチはメンバが cold start 通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.11
	swSingleIPMSWarmStart	コマンダースイッチはメンバが warm start 通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.12
	swSingleIPMSLinkDown	コマンダースイッチはメンバがリンクダウン通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171.12.8.6.0.13
	swSingleIPMSLinkUp	コマンダースイッチはメンバがリンクアップ通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
	swSingleIPMSAuthFail	コマンダースイッチはメンバが認証失敗の通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
	swSingleIPMSnewRoot	コマンダースイッチはメンバが新しいルートの通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
	swSingleIPMSTopologyChange	コマンダースイッチはメンバがトポロジ変更の通知を生成するときにこの通知を送信します。 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17

カテゴリ	トラップ名	説明	OID
Stacking	dStackInsertNotification	ユニットホットインサート（活線挿入）の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.1
	dStackRemoveNotification	ユニットホットリムーブ（活線抜出）の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.2
	dStackFailureNotification	ユニットスタック失敗の通知です。 関連オブジェクト： (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.3
	dStackTPChangeNotification	スタックトポロジ変更の通知です。 関連オブジェクト： (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.4
	dStackRoleChangeNotification	スタックユニットロール変更の通知です。 関連オブジェクト： (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.5
Start	coldStart	coldStart トラップは、SNMPv2 エンティティが、エージェントロールで動作し、自身を再起動し、設定が変更されたかもしれないことを表します。	1.3.6.1.6.3.1.1.5.1
	warmStart	warmStart トラップは、SNMPv2 エンティティが、エージェントロールで動作し、設定が変更されないような再起動を表します。	1.3.6.1.6.3.1.1.5.2
Storm Control	dStormCtrlOccurred	「dStormCtrlNotifyEnable」が "stormOccurred" または "both" で、ストームが検出されたときに送信されます。 関連オブジェクト： (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
	dStormCtrlStormCleared	「dStormCtrlNotifyEnable」が "stormCleared" または "both" で、ストームがクリアされたときに送信されます。 関連オブジェクト： (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2
System File	dsfUploadImage	イメージファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.1
	dsfDownloadImage	イメージファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.2
	dsfUploadCfg	コンフィグレーションファイルのアップロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.3
	dsfDownloadCfg	コンフィグレーションファイルのダウンロードに成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.4
	dsfSaveCfg	コンフィグレーションファイルの保存に成功したときに送信されます。	1.3.6.1.4.1.171.14.14.0.5

カテゴリ	トラップ名	説明	OID
VRRP	vrrpTrapNewMaster	送信エージェントが「Master」に変換された場合、送信されます。 関連オブジェクト : (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.680.1
	vrrpTrapAuthFailure	ルータからの受信したパケットの認証鍵、または認証タイプがルータの認証鍵、または認証タイプと一致しない事を意味します。本トラップの適用はオプションです。 関連オブジェクト : (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.680.2
Web Authentication	swWACLoggedSuccess	クライアントが Web 認証をパスしてログインに成功したときに送信されます。 関連オブジェクト : (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.171.14.154.0.1
	swWACLoggedFail	クライアントが Web 認証に失敗してログインに失敗したときに送信されます。 関連オブジェクト : (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.171.14.154.0.2
ZTP	swResetButtonPressedTrap	リセット /ZTP ボタンの押下によって ZTP 機能が動作しました。	1.3.6.1.4.1.171.12.120.2.0.1

付録 D RADIUS 属性割り当て

本スイッチの RADIUS 属性割り当てが次のモジュールに使用されます。
「コンソール」「Telnet」「SSH」「Web」「802.1X」「MAC ベースアクセスコントロール」「WAC」

RADIUS 属性タイプ：
- 特権レベル
- イングレス / イーグレス帯域幅
- 802.1p 初期値優先度
- VLAN
- ACL

RADIUS サーバで特権レベルを割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。以下は帯域幅のパラメータを表しています。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	1	必須
Attribute-Specific Field	スイッチを操作するユーザの特権レベルの割り当てに使用します。	範囲（1-15）	必須

ユーザが RADIUS サーバの特権レベル属性（例えば、レベル 15）を設定し、コンソール、Telnet、SSH、Web 認証が成功した場合、デバイスは、このアクセスユーザに特権レベル（RADIUS サーバによる）を割り当てます。しかしながら、ユーザが特権レベル属性を設定せず、認証に成功した場合、デバイスはアクセスユーザにいかなる特権レベルも割り当てません。特権レベルは、最小サポート値よりも小さく、最大サポート値よりも大きい場合、特権レベルは無視されます。

RADIUS サーバにより Ingress/Egress 帯域を割り当てるには、正しいパラメータが RADIUS サーバに設定されている必要があります。以下に、帯域のパラメータを示します。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	2（イングレス帯域幅） 3（イーグレス帯域幅）	必須
Attribute-Specific Field	ポートの帯域幅の割り当に使用します。	ユニット (Kbits)	必須

ユーザが RADIUS サーバの帯域属性（例えば、イングレス帯域 1000Kbps）を設定し、802.1X、MAC ベースアクセスコントロール、WAC 認証に成功した場合、デバイスはポートへ帯域（RADIUS サーバによる）を割り当てます。しかしながら、ユーザが帯域属性を設定せず、認証に成功した場合、デバイスは、ポートにいかなる帯域も割り当てません。帯域属性が RADIUS サーバ上で "0" の値で設定されている場合、実効的な帯域は、"no_limited" に設定され、帯域が "0" より小さいもしくは最大サポート値よりも大きい場合、帯域は無視されます。

RADIUS サーバにより 802.1p デフォルトプライオリティを割り当てるには、正しいパラメータが RADIUS サーバに設定されている必要があります。以下に、802.1p デフォルトプライオリティのパラメータを示します。

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	4	必須
Attribute-Specific Field	802.1p 初期値優先度の割り当に使用します。	0-7	必須

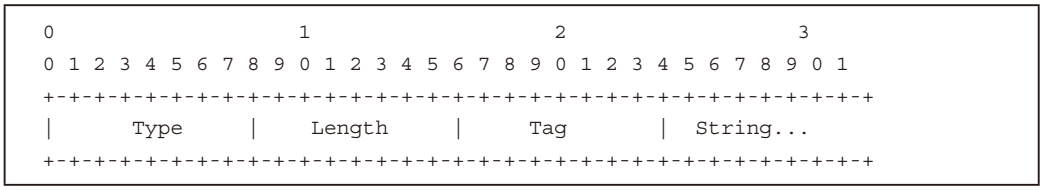
ユーザは、RADIUS サーバの 802.1p 優先度属性（例えば、優先度 7）を設定し、802.1X、MAC ベースアクセスコントロール、WAC 認証に成功した場合、デバイスはポートに 802.1p デフォルト優先度（RADIUS サーバによる）を割り当てます。しかしながら、ユーザが優先度属性を設定せず、認証が成功した場合、デバイスは、このポートにプライオリティを割り当てません。RADIUS サーバで設定された優先度属性が、範囲外の値（> 7）である場合、デバイスに設定しません。

RADIUS サーバにより VLAN を割り当てるには、正しいパラメータが RADIUS サーバに設定されている必要があります。VLAN 割り当てを使うため、RFC3580 は RADIUS パケット内の以下のトンネル属性を定義しています。

VLAN のパラメータ

RADIUS トンネル属性	説明	値	使用法
Tunnel-Type	この属性は、使用される（トンネルイニシエータの場合）トンネリングプロトコルもしくは、使用中の（トンネルターミネータの場合）トンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	使用されるトランスポートミディアムタイプ	6（802）	必須
Tunnel-Private-Group-ID	特定のトンネルセッションのグループ ID	String 値（VID）	必須

トンネルプライベートグループ ID 属性形式の概要



タグフィールドの定義（異なる RFC 2868 の）

タグフィールド値	文字列のフィールド形式
0x01	VLAN 名（ASCII）
0x02	VLAN ID（ASCII）
他 (0x00, 0x03 ~ 0x1F, >0x1F)	スイッチが VLAN の設定文字列を受信するとき、まずはじめに VLAN ID と考えます。つまり、スイッチはすべての存在している VLAN ID を確認し、一致するものがあるかどうかを確認します。一致するものを検出できた場合はその VLAN に移動し、検出できなかった場合は VLAN 設定文字列を VLAN 名だと考え、一致する VLAN 名を検出できたことを確認します。

注意 0x1F より大きなタグフィールドは次に続くフィールドの初めのオクテットとして判断されます。

ユーザが設定された RADIUS サーバの VLAN 属性（VID3 など）を持ち、802.1X、MAC ベースアクセスコントロール、または WAC 認証に成功した場合、ポートは VLAN3 が割り当てられます。しかしながら、ユーザが VLAN 属性を設定していない場合、ポートはゲスト VLAN メンバではないときは、現在の認証 VLAN にとどまり、ポートがゲスト VLAN メンバであるときは、元々の VLAN に割り当てられます。

RADIUS サーバで ACL を割り当てるには、適切なパラメータが RADIUS サーバで設定されている必要があります。
以下は ACL のパラメータを表します。

■ VSA14 ACL Script

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダ定義	171 (DLINK)	必須
Vendor-Type	属性定義	14 (ACL スクリプト)	必須
Attribute-Specific Field	ACL スクリプトの割り当てに使用します。形式は Access Control List (ACL) コマンドに基づきます。	ACL スクリプト 例： ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;	必須

ユーザは RADIUS サーバの ACL 属性を設定（ACL スクリプト：ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit; など）し、802.1X、MAC ベースアクセスコントロール、または WAC に成功した場合、デバイスは RADIUS サーバーによる ACL スクリプトを割り当てます。アクセスコンフィグモードに移行したり、出たりすることは対である必要があります。そうでなければ、ACP スクリプトは拒否されます。

■ NAS-Filter-Rule (92)

NAS-Filter-Rule パラメータ

ベンダ指定属性	説明	値	使用法
NAS-Filter-Rule	この属性は、ユーザに適用されるフィルタ規則を示します。	文字列（個々のフィルタルールを連結し、NULL（0x00）オクテットで区切る）	必須

フィルタルールフォーマット
permit コマンドを使用して、許可エントリを追加します。
deny コマンドを使用して、拒否エントリを追加します。

```
{permit | deny} in tcp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [TCP-PORT-RANGE]
{permit | deny} in udp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [UDP-PORT-RANGE]
{permit | deny} in icmp from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR} [ICMP-TYPE]
{permit | deny} in ip from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR}
{permit | deny} in IP-PROT-VALUE from any to {any | DST-IP-ADDR | DST-IP-NET-ADDR | DST-IPV6-ADDR | DST-IPV6-NET-ADDR}
```

パラメータ

パラメータ	説明
in	Ingress トラフィックを指定します。
any	送信元 IP アドレスまたは宛先 IP アドレスを指定します。
DST-IP-ADDR	宛先ホストの IP アドレスを指定します。
DST-IP-NET-ADDR	1.2.3.4/24 の形式のマスク幅で宛先 IP アドレスのグループを指定します。
DST-IPV6-ADDR	宛先ホストの IPv6 アドレスを指定します。
DST-IPV6-NET-ADDR	2000 :: 1/64 の形式の宛先 IPv6 ネットワークのグループを指定します。
tcp, udp, icmp	L4 プロトコルを指定します。
ip	合致するいずれかのプロトコルを指定します。
IP-PROT-VALUE	IP プロトコル値を指定します。有効な値は 0 ～ 255 です。
TCP-PORT-RANGE	TCP ポートまたはポート範囲に一致するように指定します。22-23、80 のように指定します。
UDP-PORT-RANGE	UDP ポートまたはポート範囲に一致するように指定します。56、67-68 のように指定します。
ICMP-TYPE	ICMP メッセージタイプを指定します。メッセージタイプの有効な番号は 0 ～ 255 です。

ユーザは RADIUS サーバの ACL 属性を設定（ACL スクリプト：ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit

host 00-00-00-01-90-10 any; exit; など）し、802.1X、MAC ベースアクセスコントロール、または WAC に成功した場合、デバイスは RADIUS サーバーによる ACL スクリプトを割り当てます。アクセスコンフィグモードに移行したり、出たりすることは対である必要があります。そうでなければ、ACP スクリプトは拒否されます。

例：

この例は、RADIUS サーバでホストの Telnet サービスを拒否する方法を示しています。

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

この例は、RADIUS サーバ上の IP アドレスのグループにアクセスするようにホストを制限する方法を示しています。

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

ベンダ指定属性パラメータ

ベンダ指定属性	説明	値	使用法
Vendor-ID	ベンダを定義します。	171 (DLINK)	必須
Vendor-Type	属性を定義します。	14 (ACL script)	必須
Attribute-Specific Field	IPv6 フィルタルール。 IPv6 アドレス関連の入力を受け入れるために使用されます。	この属性は、NAS-Filter-Rule の次の IP モードのいずれかを示します。 1=IPv4 および IPv6 トラフィックを転送 2=IPv4 トラフィックのみ転送（IPv6 トラフィックは破棄） この属性が RADIUS サーバによって割り当てられていない場合、IPv4 のみのトラフィックを転送すると、IPv6 パケットはすべてドロップされます。	必須

付録 E IETF RADIUS 属性サポート

リモート認証ダイヤルインユーザサービス（RADIUS）属性は、特定の認証、承認、情報、リクエストとリプライに対する設定詳細を実行します。本付録は現在スイッチによりサポートされる RADIUS 属性一覧です。

RADIUS 属性は、IETF 規格やベンダ特定属性（VSA) によりサポートされます。VSA は、ベンダが、追加で自身の RADIUS 属性を作成することを許可します。D-Link VSA についてのより詳しい情報は、「付録 D RADIUS 属性割り当て」を参照してください。IETF 規格 RADIUS 属性は、RFC2865 リモート認証ダイヤルインユーザサービス（RADIUS)、RFC2866 RADIUS アカウンティング、トンネルプロトコルサポートに対する RFC2868 RADIUS 属性、RFC2869 RADIUS 拡張で定義されています。以下のリストは、D-Link スイッチでサポートされた IETF RADIUS 属性です。

RADIUS 認証属性

ナンバー	IETF 属性
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address

RADIUS アカウンティング属性

ナンバー	IETF 属性
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

付録 F ERPS 情報

イーサネットリングプロテクション（ERPS）のポート毎における「ハードウェア / ソフトウェアベース」情報を表示します。
「ハードウェアベース ERPS」(external PHY) のみ 50ms のリカバリタイムでの「fast link drop interrupt」（ファストリンクドロップ防止）機能をサポートしています。

ERPS「ハードウェア / ソフトウェアベース」情報

機種	ERPS タイプ
DGS-1520-28	ハードウェアベース ERPS：ポート 1 ～ 8、27 ～ 28 ソフトウェアベース ERPS：ポート 9 ～ 26
DGS-1520-28MP	ハードウェアベース ERPS：ポート 1 ～ 4、27 ～ 28 ソフトウェアベース ERPS：ポート 5 ～ 26
DGS-1520-52	ハードウェアベース ERPS：ポート 1 ～ 8、25 ～ 32、51 ～ 52 ソフトウェアベース ERPS：ポート 9 ～ 24、33 ～ 50
DGS-1520-52MP	ハードウェアベース ERPS：ポート 1 ～ 8、25 ～ 28、51 ～ 52 ソフトウェアベース ERPS：ポート 9 ～ 24、29 ～ 50

付録 G 機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

- Traffic Segmentation（トラフィックセグメンテーション）
- VLAN
- Link Aggregation（リンクアグリゲーション）
- Access List（アクセスリスト）
- Loopback Detection（LBD）（ループ検知）

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DGS-1520

Traffic Segmentation（トラフィックセグメンテーション）

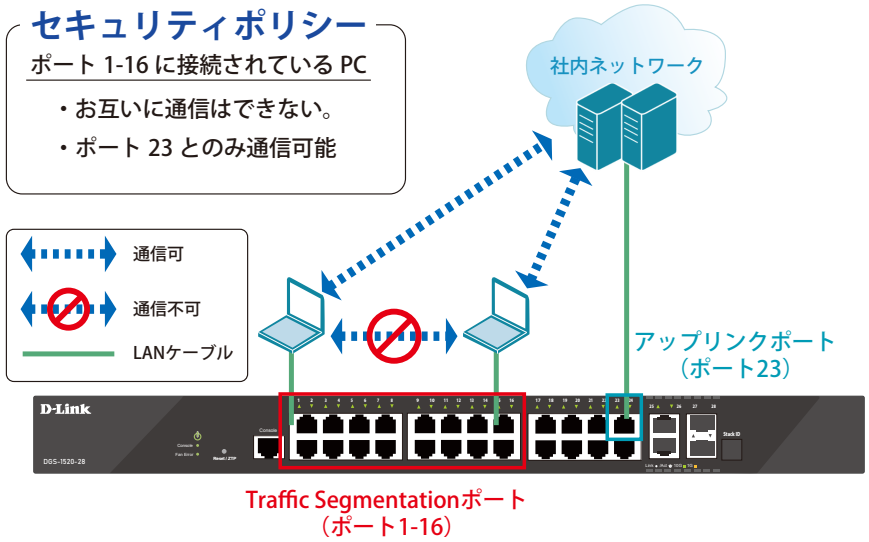


図 17-1　Traffic Segmentation（DGS-1520-28）

概要

ポート 1 ～ 16 に対し、トラフィックセグメンテーションを設定します。1 ～ 16 のポート間ではお互いに通信ができないようにし、ポート 1 ～ 16 は、アップリンクポートとして使用するポート 23 とのみ通信ができるようにします。

設定手順

1. ポート（1-16）のセキュリティ設定をします。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#traffic-segmentation forward interface ethernet 1/0/23
Switch(config-if-range)#end
```

2. 情報確認

```
Switch#show traffic-segmentation forward
```

注意　本機能を利用する場合、送信先 MAC アドレスが不明な Unknown ユニキャストについて、スイッチの全ポートにフラッドされます。

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

VLAN

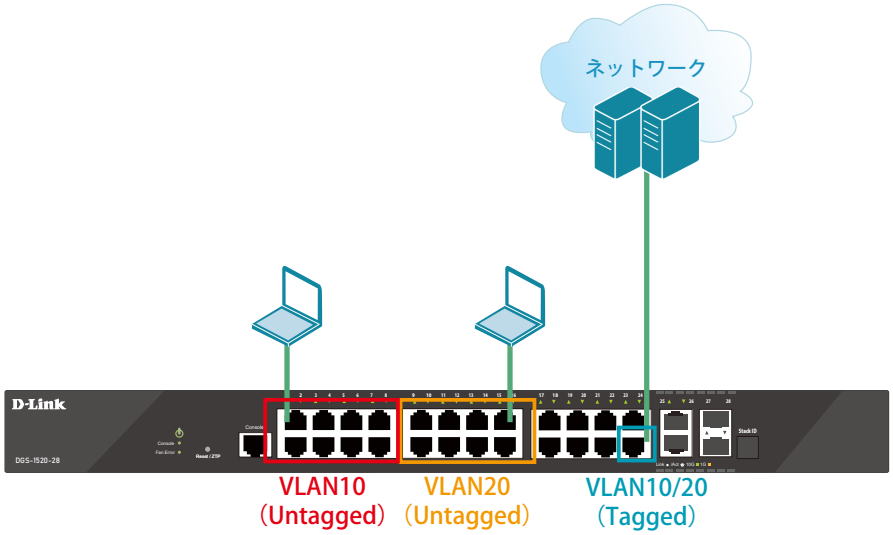


図 17-2　VLAN（DGS-1520-28）

概要

VLAN を設定します。ポート 1 ～ 8 に VLAN10 を「Untagged」で割り当て、ポート 9 ～ 16 に VLAN20 を「Untagged」で割り当て、ポート 24 において、VLAN10 と VLAN20 を「Tagged」で割り当てます。

設定手順

1. VLAN10、VLAN20 を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#exit
```

2. ポート 1-8 に VLAN10、ポート 9-16 に VLAN20 を 割り当てます。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit

Switch#configure terminal
Switch(config)#interface range ethernet 1/0/9-16
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#end
```

3. 上位のネットワークへ接続されているポート 24 に VLAN10、20 の通信を転送することができるように、VLAN を設定します。

■設定方法①（hybrid mode を設定する場合）

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 10,20
Switch(config-if)#end
```

■設定方法②（hybrid mode を使用せず、trunk にて同様の設定を行う場合）

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 10,20
Switch(config-if)#end
```

4. 設定を保存します。

```
Switch#copy running-config startup-config
```

5. 情報確認

```
Switch#show vlan
```

（作成した VLAN と各ポートに割り当てられている VLAN が表示されます。）

```
Switch#show vlan int ethernet 1/0/xx
```

（ポートに紐づいている VLAN 情報が表示されます。）

Link Aggregation（リンクアグリゲーション）

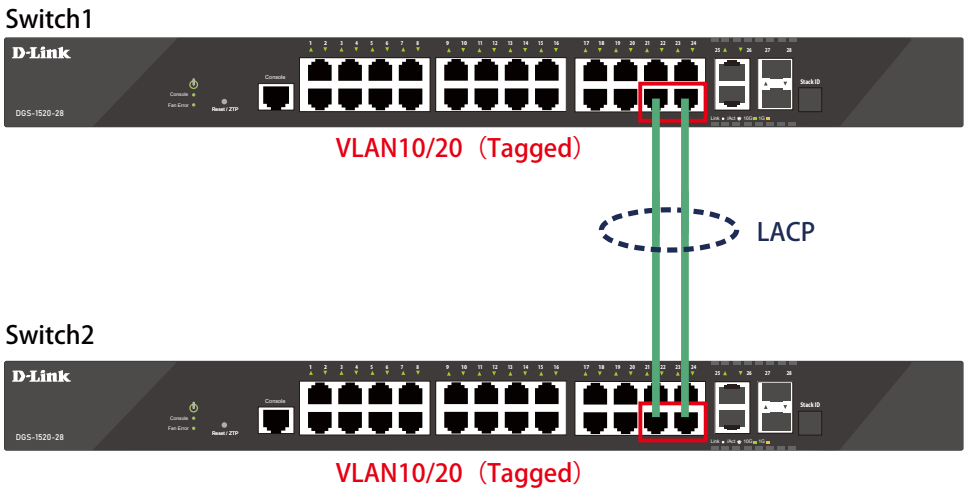


図 17-3　Link Aggregation（DGS-1520-28）

概要

VLAN10 と 20 の Tagged VLAN を設定したポートにリンクアグリゲーションを設定します。ポート 22 と 24 に VLAN10 と VLAN20 を「Tagged」で割り当て、ポート 22 と 24 をグループ 1 として LACP によるリンクアグリゲーションに設定します。

設定手順（Switch1、Switch2 共通）

1. VLAN10、VLAN20 を作成します。

```
Switch#configure terminal
Switch(config)#vlan 10,20
Switch(config-vlan)#exit
```

2. Link Aggregation（LACP）のグループを作成します。

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/22
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
Switch(config)#interface ethernet 1/0/24
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
```

3. Link Aggregation のポートを設定します。

```
Switch(config)#interface port-channel 1
```

4. 作成した port-channel に VLAN を設定します。
LAG ポートに設定する VLAN は、各物理インタフェース上では設定せず、Port-channel インタフェース上で VLAN の設定を行います。

```
Switch(config)#interface port-channel 1
Switch(config if)#switchport mode trunk
Switch(config if)#switchport trunk native vlan 1
Switch(config if)#switchport trunk allowed vlan 1,10,20
Switch(config if)#exit
Switch(config)#exit
```

5. 設定を保存します。

```
Switch#copy running-config startup-config
```

6. 情報確認

- Port-channel に設定されている VLAN 情報を表示します。

```
Switch#show vlan interface port-channel 1
```

- グループ番号とグループで使用されている Protocol を表示します。

```
Switch#show channel-group
```

- 各グループに所属している Port 番号と、リンクアグリゲーションの状態を表示します。

```
Switch#show channel-group channel 1 detail
```

Access List（アクセスリスト）

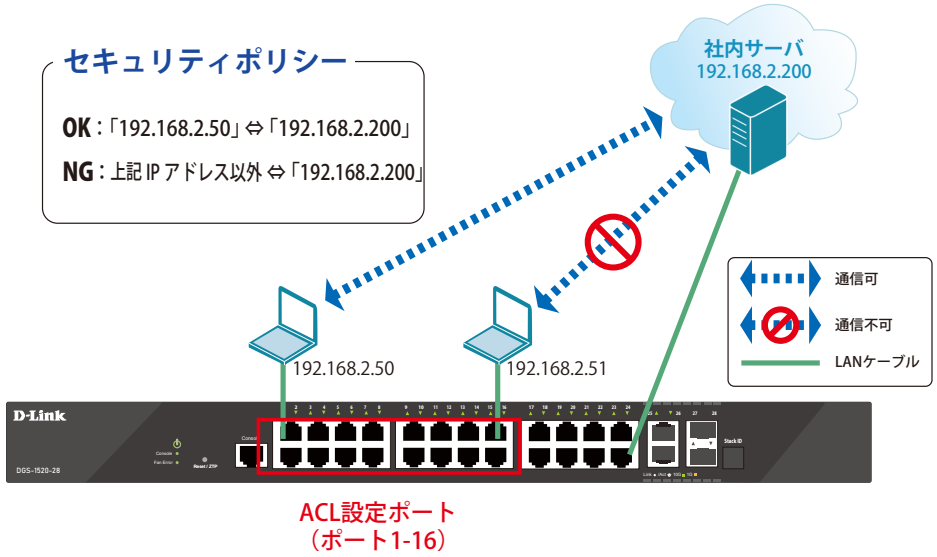


図 17-4　Access List（DGS-1520-28）

概要

ポート 1~16 に対し、アクセスリストを設定します。ポート 1~16 に接続される端末の IP の中から、「192.168.2.50」の端末から社内サーバ（192.168.2.200）へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

設定手順

1. アクセスリストに名前（extended ACL）を付けて定義します。
「192.168.2.50 ⇔ 192.168.2.200」間の通信を許可するルールを追加します。
「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
Switch#configure terminal
Switch(config)#ip access-list extended ACL
Switch(config-ip-ext-acl)#permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#deny any 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#end
```

2. アクセスリストのルールを、適用対象ポート 1 ～ 16 へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

Loopback Detection（LBD）（ループ検知）

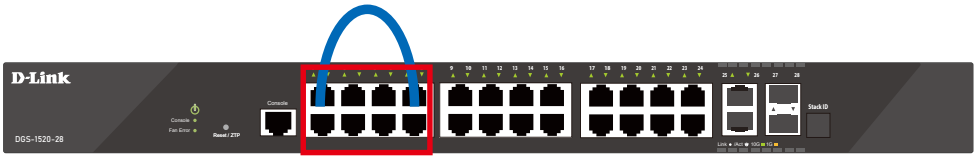


図 17-5　Loopback Detection（DGS-1520-28）

概要

ポート 1~8 に対しループバック検知を設定します。ポート 1~8 でループを検知した際、ポートをシャットダウンするように設定します。

設定手順

1. ポートベースでループ検知機能を動作させ、ループ検知後はポートをシャットダウンする設定をします。

```
Switch#enable
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
```

2. ループ発生を確認する間隔を 20 秒に設定します。

```
Switch(config)#loopback-detection interval 20
```

3. （必要に応じて）ループ発生後のループ解消確認間隔を 20 秒に設定し、ループ解消確認後、自動で Port 開放するように設定します。

```
Switch(config)#errdisable recovery cause loopback-detect interval 20
```

注意　この設定をしない場合、永続的にポートが「shutdown」状態となります。ポートを開放する場合、該当のポートに対し、インタフェースモードにて「no shutdown」コマンドを投入する必要があります。

4. ポート 1-8 でループバック検知機能を有効にします。

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#spanning-tree state disable
Switch(config-if-range)#loopback-detection
Switch(config-if-range)#end
```

注意　「spanning-tree」が「enable」になっている場合、ループ検知機能を設定できないため、設定するインタフェースの「spanning-tree」の設定をまず「disable」にします。

注意　「spanning-tree」はデフォルトでグローバルでは「disable」に設定されていますが、各インタフェース「enable」となっています。各インタフェースにて「disable」設定が必要となります。

5. show コマンドで「Spanning Tree」が無効になっているかを確認します。

```
Switch#show spanning-tree configuration interface ethernet 1/0/1-8
```

6. 「Spanning Tree」がポート単位で「disable」に設定されている場合、ステータスが Disabled と表示されます。

```
Spanning tree state : Disabled
```

7. 設定を保存します。

```
Switch#copy running-config startup-config
```

8. 情報確認

```
Switch#show loopback-detection
```

（ループ検知の有効 / 無効、設定しているモード、対象の VLAN、各ポートのループ状態等を表示します。）

```
Switch#show errdisable recovery
```

（ループ解消後の自動ポート解放設定 有効 / 無効、確認間隔を表示します。）