18

アクセス コントロール

Access Control List（ACL; アクセス コントロール リスト）はセキュリティ機構の 1 つです。ACL 定義は、トラフィック フローに対して一定の Quality of Service（QoS; サービス品質）を確保するしくみの 1 つです。詳細については、「QoS の設定」の「QoS の設定：全般」を参照してください。

ネットワーク管理者は ACL を使用することにより、入トラフィックに対するフィルタおよび処理を定義できます。ACL がバインドされているポートまたは LAG に届いたパケットは、許可または拒否されます。

ここで説明する内容は次のとおりです。

- 「アクセス コントロール リスト」
- 「MAC ベース ACL の定義」
- 「IPv4 ベース ACL」
- 「IPv6 ベース ACL」
- 「ACL バインディングの定義」

アクセス コントロール リスト

Access Control List（ACL; アクセス コントロール リスト）は、分類用フィルタと処理のペアの順序付きリストです。それぞれの分類ルールとそれに伴う処理を Access Control Element（ACE; アクセス コントロール要素）と呼びます。

各 ACE は、トラフィック グループを区別するフィルタ、および、そのフィルタに関連付けられた処理で構成されています。1 つの ACL には 1 つ以上の ACE が含まれています。ACE は、入力フレームの内容と照合されます。フレームの内容がフィルタ条件に合致した場合、そのフレームには DENY 処理または PERMIT 処理が適用されます。

このスイッチで定義できる ACL および ACE の数はそれぞれ最大 512 個です。

パケットが ACE フィルタ条件に合致した場合、その ACE 処理が適用され、その ACL の処理が中止されます。パケットが ACE フィルタ条件に合致しなかった場合は、次の ACE と照合されます。ACL 内のどの ACE とも合致しなかった場合、他にも ACL がある場合は、その ACL が同様に処理されます。

（注） すべての ACL 内のどの ACE とも合致しなかった場合、そのパケットは破棄されます。これはデフォルトの処理です。このようにデフォルトでは破棄されるので、管理トラフィックを含む必要なトラフィックを許可する ACE を ACL に明示的に追加する必要があります。管理トラフィックとは、スイッチ自体に送信されるトラフィック（例：Telnet、HTTP、SNMP）のことです。たとえば、ACL の条件に一致しないすべてのパケットを廃棄しない場合は、すべてのトラフィックを許可する最低プライオリティの ACE を ACL に明示的に追加する必要があります。

ACL がバインドされているポートで IGMP/MLD スヌーピングが有効になっている場合は、IGMP/MLD パケットをスイッチに転送する ACE フィルタをその ACL に追加してください。追加しない場合、そのポートで IGMP/MLD スヌーピングが失敗します。

最初に合致した ACE の処理が実行されるため、ACL 内における ACE の順序は重要です。先頭の ACE から順に処理されます。

ACL の用途としては、セキュリティの強化（例：特定のトラフィック フローを許可または拒否）、トラフィックの分類、トラフィックのプライオリティ付けなどがあります。分類とプライオリティ付けは、QoS 拡張モードで利用できます。

（注） 各ポートには ACL または拡張 QoS ポリシーを設定できますが、両方を同時に設定することはできません。

1 つのポートにバインドできる ACL は、原則として 1 つのみです。ただし例外として、1 つのポートに IPv4 ベース ACL と IPv6 ベース ACL の両方をバインドすることができます。1 つのポートに複数の ACL をバインドするには、1 つ以上のクラス マップから成るポリシーを使用する必要があります。詳細については、「QoS 拡張モード」の「ポリシーの設定」を参照してください。定義できる ACL のタイプは次のとおりです。フレーム ヘッダーのどの部分を検査するかによって、定義する ACL が決まります。

- MAC ベース ACL：レイヤ 2 フィールドのみを検査します。「MAC ベース ACL の定義」を参照してください。
- IP ベース ACL：IP フレームのレイヤ 3 を検査します。「IPv4 ベース ACL」を参照してください。
- IPv6 ベース ACL：IPv4 フレームのレイヤ 3 を検査します。「IPv6 ベース ACL の定義」を参照してください。

フレームが ACL 内のフィルタと合致した場合、そのフレームは、その ACL の名前のフローとして定義されます。拡張 QoS の場合、これらのフレームをこのフロー名で呼ぶことができます。また、これらのフレームに QoS を適用できます。詳細については、「QoS 拡張モード」を参照してください。

ACL を作成する手順

ACL を作成してインターフェイスにバインドするには

1. 次のタイプの ACL を 1 つ以上作成します。
   a. MAC ベース ACL。[MAC ベース ACL] ページおよび [MAC ベース ACE] ページを使用して作成します。
   b. IP ベース AC。[IPv4 ベース ACL] ページおよび [IPv4 ベース ACE] ページを使用して作成します。
   c. IPv6 ベース ACL。[IPv6 ベース ACL] ページおよび [IPv6 ベース ACE] ページを使用して作成します。
2. [ACL バインディング] ページを使用して ACL をインターフェイスにバインドします。

ACL を修正する手順

ACL は、使用中は修正できません。ACL を修正するためにインターフェイスからアンバインドする手順を次に示します。

1. ACL が QoS 拡張モード クラス マップに属していないが、インターフェイスにバインドされている場合、[ACL バインディング] ページを使用してインターフェイスからアンバインドします。
2. ACL がクラス マップに属しており、そのクラス マップがインターフェイスにバインドされていない場合、その ACL を修正できます。
3. ACL がクラス マップに属しており、そのクラス マップがポリシーに属しており、そのポリシーがインターフェイスにバインドされている場合、次に示すアンバインド手順を実行する必要があります。
   - 「ポリシーのバインディング」の手順に従って、クラス マップが属しているポリシーをインターフェイスからアンバインドします。
   - 「ポリシーの設定」（編集）の手順に従って、ACL が属しているクラス マップをポリシーから削除します。
   - 「クラス マップの定義」の手順に従って、ACL が属しているクラス マップをポリシーから削除します。

これで ACL を修正できる状態になりました。

MAC ベース ACL の定義

MAC ベース ACL は、レイヤ 2 フィールドの内容に基づいてトラフィックをフィルタリングする際に使用します。MAC ベース ACL ではすべてのフレームが検査されます。

MAC ベース ACL は [MAC ベース ACL] ページで定義します。ルールは、[MAC ベース ACE] ページで定義します。

MAC ベース ACL を定義するには

ステップ 1 [アクセスコントロール] > [MAC ベース ACL] をクリックします。[MAC ベース ACL] ページが開きます。

このページには、現在定義されているすべての MAC ベース ACL のリストが表示されます。

ステップ 2 [追加] をクリックします。[MAC ベース ACL の追加] ページが開きます。

ステップ 3 [ACL 名] フィールドに、新規に作成する ACL の名前を入力します。ACL 名では大文字と小文字が区別されます。

ステップ 4 [適用] をクリックします。MAC ベース ACL が定義され、実行コンフィギュレーション ファイルが更新されます。

MAC ベース ACL へのルールの追加

ACL にルール（ACE）を追加するには

ステップ 1 [アクセスコントロール] > [MAC ベース ACE] をクリックします。[MAC ベース ACE] ページが開きます。

ステップ 2 ACL を選択し、[実行] をクリックします。その ACL 内の ACE のリストが表示されます。

ステップ 3 [追加] をクリックします。[MAC ベース ACE の追加] ページが開きます。

ステップ 4 パラメータを指定します。

- [ACL 名] : ACE が追加される ACL の名前が表示されます。
- [プライオリティ] : ACE のプライオリティを入力します。プライオリティの高い ACE ほど先に処理されます。プライオリティは 1 が最高です。

- [アクション]：合致したときに実行する処理を選択します。次のオプションがあります。
  - [許可]：ACE 基準に合致したパケットを転送します。
  - [拒否]：ACE 基準に合致したパケットを廃棄します。
  - [シャットダウン]：ACE 基準に合致したパケットを廃棄し、そのパケットが届いたポートを無効にします。無効にしたポートを再度アクティブ化するには、[ポート設定] ページを使用します。
- [宛先 MAC アドレス]：すべての宛先アドレスをそのまま受け入れる場合は、[任意] を選択します。宛先アドレスまたは宛先アドレス範囲を入力する場合は、[ユーザ定義] を選択します。
- [宛先 MAC アドレス値]:宛先 MAC アドレスに対応する MAC アドレスとそのマスク（必要な場合）を入力します。
- [宛先 MAC ワイルドカードマスク]:MAC アドレス範囲を指定するためのマスクを入力します。このマスクは、サブネット マスクなどとは異なります。ビットを 1 に設定した場合、その値をマスクしないことを意味します。ビットを 0 に設定した場合、その値をマスクすることを意味します。
- [送信元 MAC アドレス]:すべての送信元アドレスをそのまま受け入れる場合は [任意] を選択します。送信元アドレスまたは送信元アドレス範囲を入力する場合は、[ユーザ定義] を選択します。
- [送信元 MAC アドレス値]:送信元 MAC アドレスに対応する MAC アドレスとそのマスク（必要な場合）を入力します。
- [送信元 MAC ワイルドカードマスク]:MAC アドレス範囲を指定するためのマスクを入力します。
- [VLAN ID]：照合する VLAN タグの VLAN ID セクションを入力します。
- [802.1p]：802.1p を使用する場合は [含める] を選択します。
- [802.1p 値]：VPT タグに追加する 802.1p 値を入力します。
- [802.1p マスク]：VPT タグに適用するワイルドカード マスクを入力します。
- [イーサタイプ]：照合するフレームの EtherType を入力します。

ステップ 5 [適用] をクリックします。MAC ベース ACE が定義され、実行コンフィギュレーション ファイルが更新されます。

IPv4 ベース ACL

IPv4 ベース ACL は、IPv4 パケットを検査する際に使用します。ARP などその他の種類のフレームは検査されません。

照合できるフィールドは次のとおりです。

- IP プロトコル（既知のプロトコルの場合は名前で照合、未知のプロトコルの場合は値で直接照合）
- TCP/UDP トラフィックの送信元ポート/宛先ポート
- TCP フレームの各フラグの値
- ICMP のメッセージ タイプとコード、および、IGMP のメッセージ タイプ
- 送信元 IP アドレスおよび宛先 IP アドレス（ワイルドカードを含む）
- DSCP 値および IP Precedence 値

（注） ACL は、フロー単位で QoS 処理を行う際の、フロー定義の構成要素としても使用されます。詳細については、「QoS 拡張モード」を参照してください。

ACL を定義するには、[IPv4 ベース ACL] ページを使用します。ルールは、[IPv4 ベース ACE] ページで定義します。

IPv6 ACL を定義するには、[IPv6 ベース ACL] ページを使用します。

IPv4 ベース ACL の定義

IPv4 ベース ACL を定義するには

ステップ 1 [アクセスコントロール] > [IPv4 ベース ACL] をクリックします。[IPv4 ベース ACL] ページが開きます。

このページには、現在定義されているすべての IPv4 ベース ACL が表示されます。

ステップ 2 [追加] をクリックします。[IPv4 ベース ACL の追加] ページが開きます。

ステップ 3 [ACL 名] フィールドに、新規に作成する ACL の名前を入力します。ACL 名では大文字と小文字が区別されます。

ステップ 4 [適用] をクリックします。IPv4 ベース ACL が定義され、実行コンフィギュレーション ファイルが更新されます。

IPv4 ベース ACL へのルールの追加

IPv4 ベース ACL にルール（ACE）を追加するには

ステップ 1 [アクセスコントロール] > [IPv4 ベース ACE] をクリックします。[IPv4 ベース ACE] ページが開きます。

ステップ 2 ACL を選択し、[実行] をクリックします。選択した ACL に対して現在定義されている IP ACE が表示されます。

ステップ 3 [追加] をクリックします。[IPv4 ベース ACE の追加] ページが開きます。

ステップ 4 パラメータを指定します。

- [ACL 名] : ACL の名前が表示されます。
- [プライオリティ] : プライオリティを入力します。プライオリティの高い ACE ほど先に処理されます。
- [アクション] : ACE に合致したパケットに対する処理を選択します。選択項目は次のとおりです。
  - [許可] : ACE 基準に合致したパケットを転送します。
  - [拒否] : ACE 基準に合致したパケットを廃棄します。
  - [シャットダウン] : ACE 基準に合致したパケットを廃棄し、そのパケットが届いたポートを無効にします。無効にしたポートを再度アクティブ化するには、[ポート管理] ページを使用します。
- [プロトコル] : 特定のプロトコルまたはプロトコル ID に基づく ACE を作成する場合、そのプロトコルを選択します。すべての IP プロトコルを受け入れるには、[任意 (IPv4)] を選択します。特定のプロトコルのみを受け入れるには、ドロップダウン リストでそのプロトコルを選択します。選択できるプロトコルは 1 つのみです。
  - [ICMP] : Internet Control Message Protocol
  - [IGMP] : Internet Group Management Protocol
  - [IP-in-IP] : IP in IP カプセル化
  - [TCP] : Transmission Control Protocol
  - [EGP] : Exterior Gateway Protocol
  - [IGP] : Interior Gateway Protocol
  - [UDP] : User Datagram Protocol
  - [HMP] : Host Mapping Protocol

- [RDP]：Reliable Datagram Protocol
- [IDPR]：Inter-Domain Policy Routing Protocol
- [IPV6]：IPv6 over IPv4 トンネリング
- [IPV6:ROUT]：ゲートウェイ経由で IPv6 over IPv4 ルートを流れるパケット
- [IPV6:FRAG]：IPv6 over IPv4 フラグメント ヘッダーがあるパケット
- [IDRP]：Inter-Domain Routing Protocol
- [RSVP]：ReSerVation Protocol
- [AH]：Authentication Header
- [IPV6:ICMP]：Internet Control Message Protocol
- [EIGRP]：Enhanced Interior Gateway Routing Protocol
- [OSPF]：Open Shortest Path First
- [IPIP]：IP in IP
- [PIM]：Protocol Independent Multicast
- [L2TP]：Layer 2 Tunneling Protocol
- [ISIS]：IGP-specific Protocol

- [照合するプロトコル ID]：名前を選択するのではなくプロトコル ID を入力します。
- [送信元 IP アドレス]:すべての送信元アドレスをそのまま受け入れる場合は [任意] を選択します。送信元アドレスまたは送信元アドレス範囲を入力する場合は、[ユーザ定義] を選択します。
- [送信元 IP アドレス値]：送信元 IP アドレスに対応する IP アドレスを入力します。
- [送信元 IP ワイルドカードマスク]:IP アドレス範囲を指定するためのマスクを入力します。このマスクは、サブネット マスクなどとは異なります。ビットを 1 に設定した場合、その値をマスクしないことを意味します。ビットを 0 に設定した場合、その値をマスクすることを意味します。
- [宛先 IP アドレス]:すべての宛先アドレスをそのまま受け入れる場合は [任意] を選択します。宛先アドレスまたは宛先アドレス範囲を入力する場合は、[ユーザ定義] を選択します。
- [宛先 IP アドレス値]：宛先 IP アドレスに対応する IP アドレスを入力します。
- [宛先 IP ワイルドカードマスク]:IP アドレス範囲を指定するためのマスクを入力します。

- [送信元ポート] : 次のいずれかを選択します。
  - [任意] : すべての送信元ポートを受け入れます。
  - [シングル] : パケットを照合する TCP/UDP 送信元ポートを 1 つ入力します。このフィールドは、[リストから選択] ドロップダウン リストで [TCP] または [UDP] が選択されている場合にのみアクティブになります。
  - [範囲] : パケットを照合する TCP/UDP 送信元ポート範囲を選択します。送信元ポートと宛先ポート合わせて 8 種類のポート範囲を設定できます。また、TCP プロトコルと UDP プロトコルそれぞれに対して 8 種類のポート範囲を設定できます。
- [宛先ポート] : いずれかを選択します。選択項目は前述の [送信元ポート] フィールドと同じです。

  （注）IP プロトコルを指定してからでないと、送信元ポートおよび宛先ポートを指定できません。
- [TCP フラグ] : パケットをフィルタリングする際に使用する TCP フラグを 1 つ以上選択します。フィルタ処理されたパケットは、転送または破棄されます。TCP フラグを使用してパケットをフィルタリングすると、パケットをきめ細かく制御できるので、ネットワーク セキュリティが向上します。
- [タイプオブサービス] : IP パケットのサービス タイプ。
  - [任意] : 任意のサービス タイプ。
  - [照合する DSCP] : Differentiated Serves Code Point（DSCP）を照合します。
  - [照合する IP precedence] : ネットワークが適切な QoS を実現するために使用する Type of Service（ToS; タイプ オブ サービス）のモデル。このモデルは、RFC 791 および RFC 1349 で説明されている、IP ヘッダー内のサービス タイプ バイトで最も重要度の高い 3 ビットを使用します。
- [ICMP] : ACL の IP プロトコルが ICMP である場合、フィルタリングに使用する ICMP メッセージ タイプを選択します。メッセージ タイプ名を選択するか、または、メッセージ タイプ番号を入力します。
  - [任意] : すべてのメッセージ タイプを受け入れます。
  - [リストから選択] : メッセージ タイプ名を選択します。
  - [照合する ICMP タイプ] : フィルタリングに使用するメッセージ タイプ番号を入力します。

- [ICMP コード] : ICMP メッセージには、そのメッセージの処理方法を示すコードが設定されている場合があります。このコードに基づいてフィルタリングするかどうかを設定するため、次のいずれかを選択します。
  - [任意] : すべてのコードを受け入れます。
  - [ユーザ定義] : フィルタリングに使用する ICMP コードを入力します。
- [IGMP] : ACL の IP プロトコルが IGMP である場合、フィルタリングに使用する IGMP メッセージ タイプを選択します。メッセージ タイプ名を選択するか、または、メッセージ タイプ番号を入力します。
  - [任意] : すべてのメッセージ タイプを受け入れます。
  - [リストから選択] : メッセージ タイプ名を選択します。
  - [照合する IGMP タイプ] : フィルタリングに使用するメッセージ タイプ番号を入力します。

ステップ 5 [適用] をクリックします。IPv4 ベース ACE が定義され、実行コンフィギュレーション ファイルが更新されます。

IPv6 ベース ACL

[IPv6 ベース ACL] ページでは、純粋な IPv6 トラフィックを検査するための IPv6 ベース ACL を表示および作成できます。IPv6 ベース ACL では、IPv6 over IPv4 パケットおよび ARP パケットは検査されません。

（注） ACL は、フロー単位で QoS 処理を行う際の、フロー定義の構成要素としても使用されます。詳細については、「QoS 拡張モード」を参照してください。

IPv6 ベース ACL の定義

IPv6 ベース ACL の定義

IPv6 ベース ACL を定義するには

ステップ 1 [アクセスコントロール] > [IPv6 ベース ACL] をクリックします。[IPv6 ベース ACL] ページが開きます。

このページには、定義済みの ACL とその内容のリストが表示されます。

ステップ 2 [追加] をクリックします。[IPv6 ベース ACL の追加] ページが開きます。

ステップ 3 [ACL 名] フィールドに、新規に作成する ACL の名前を入力します。ACL 名では大文字と小文字が区別されます。

ステップ 4 [適用] をクリックします。IPv6 ベース ACL が定義され、実行コンフィギュレーション ファイルが更新されます。

IPv6 ベース ACL へのルール（ACE）の追加

ステップ 1 [アクセスコントロール] > [IPv6 ベース ACE] をクリックします。[IPv6 ベース ACE] ページが開きます。

このページには、選択した ACL（ルールの集まり）内の ACE（ルール）が一覧表示されます。

ステップ 2 ACL を選択し、[実行] をクリックします。選択した ACL に対して現在定義されている IP ACE が表示されます。

ステップ 3 [追加] をクリックします。[IPv6 ベース ACE の追加] ページが開きます。

ステップ 4 パラメータを指定します。

- [ACL 名] : ACE が追加される ACL の名前が表示されます。
- [プライオリティ] : プライオリティを入力します。プライオリティの高い ACE ほど先に処理されます。
- [アクション] : ACE に合致したパケットに対する処理を選択します。選択項目は次のとおりです。
  - [許可] : ACE 基準に合致したパケットを転送します。
  - [拒否] : ACE 基準に合致したパケットを廃棄します。
  - [シャットダウン] : ACE 基準に合致したパケットを廃棄し、そのパケットが届いたポートを無効にします。無効にしたポートを再度アクティブ化するには、[ポート管理] ページを使用します。
- [プロトコル] : 特定のプロトコルに基づく ACE を作成する場合、そのプロトコルを選択します。すべての IP プロトコルを受け入れるには、[任意 (IPv6)] を選択します。特定のプロトコルのみを受け入れるには、そのプロトコルを選択します。選択できるプロトコルは 1 つのみです。
  - [TCP] : Transmission Control Protocol。2 台のホスト間で通信とデータ ストリーム交換を行うことができます。TCP では、パケットが送信先に届くこと、および、送信した順に伝送および受信されることが保証されます。

- [UDP] : User Datagram Protocol。パケットが送信されますが、送信先に届くかどうかは保証されません。
- [ICMP] : パケットが Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）と照合されます。

- [照合するプロトコル ID] : 照合するプロトコルの ID を入力します。
- [送信元 IP アドレス]:すべての送信元アドレスをそのまま受け入れる場合は [任意] を選択します。送信元アドレスまたは送信元アドレス範囲を入力する場合は、[ユーザ定義] を選択します。
- [送信元 IP アドレス値] : 送信元 IP アドレスに対応する IP アドレスを入力します。また、関連がある場合はそのマスクも入力します。
- [送信元 IP プレフィクス長] : 送信元 IP アドレス プレフィクス長を入力します。
- [宛先 IP アドレス]:すべての宛先アドレスをそのまま受け入れる場合は [任意] を選択します。送信元アドレスまたは送信元アドレス範囲を入力する場合は、[ユーザ定義] を選択します。
- [宛先 IP アドレス値] : 宛先 IP アドレスに対応する IP アドレスとそのマスク（必要な場合）を入力します。
- [宛先 IP プレフィクス値] : 宛先 IP アドレス プレフィクス長を入力します。
- [送信元ポート] : 次のいずれかを選択します。
  - [任意] : すべての送信元ポートを受け入れます。
  - [シングル] : パケットを照合する TCP/UDP 送信元ポートを 1 つ入力します。このフィールドは、[リストから選択] ドロップダウン リストで [TCP] または [UDP] が選択されている場合にのみアクティブになります。
  - [範囲] : パケットを照合する TCP/UDP 送信元ポート範囲を選択します。
- [宛先ポート] : いずれか 1 つ選択します。選択項目は、前述の [送信元ポート] フィールドと同じです。

  （注）IPv6 プロトコルを指定してからでないと、送信元ポートおよび宛先ポートを指定できません。
- [TCP フラグ] : パケットをフィルタリングする際に使用する TCP フラグを 1 つ以上選択します。フィルタ処理されたパケットは、転送または破棄されます。TCP フラグを使用してパケットをフィルタリングすると、パケットをきめ細かく制御できるので、ネットワーク セキュリティが向上します。
  - [設定] : フラグ値が設定されている場合に照合します。
  - [設定解除] : フラグ値が設定されていない場合に照合します。
  - [設定しない] : TCP フラグの値を無視します。

- [タイプオブサービス]：IP パケットのサービス タイプ。
- [ICMP]：ACL の IP プロトコルが ICMP である場合、フィルタリングに使用する ICMP メッセージ タイプを選択します。メッセージ タイプ名を選択するか、または、メッセージ タイプ番号を入力します。すべてのメッセージ タイプを受け入れる場合は、[任意] を選択します。
  - [任意]：すべてのメッセージ タイプを受け入れます。
  - [リストから選択]：メッセージ タイプ名を選択します。
  - [照合する ICMP タイプ]：フィルタリングに使用するメッセージ タイプ番号を入力します。
- [ICMP コード]：ICMP メッセージには、そのメッセージの処理方法を示すコードが設定されている場合があります。このコードに基づいてフィルタリングするかどうかを設定するため、次のいずれかを選択します。
  - [任意]：すべてのコードを受け入れます。
  - [ユーザ定義]：フィルタリングに使用する ICMP コードを入力します。

ステップ 5 [適用] をクリックします。

ACL バインディングの定義

ACL をインターフェイスにバインドすると、そのインターフェイスに届いたパケットにその ACL 内の ACE が適用されます。ACL 内のどの ACE 条件にも合致しなかったパケットに対しては、デフォルトのルールが適用されます。デフォルトのルールでは、どの ACE とも合致しなかったパケットは破棄されます。

1 つのインターフェイスにバインドできる ACL は 1 つのみですが、インターフェイスをポリシー マップにまとめ、そのポリシー マップをインターフェイスにバインドすることで、複数のインターフェイスを同じ ACL にバインドできます。

いったんインターフェイスにバインドした ACL は、アンバインドしない限り、修正も削除もできません。

ACL をインターフェイスにバインドするには

ステップ 1 [アクセスコントロール] > [ACL バインディング] をクリックします。[ACL バインディング] ページが開きます。

ステップ 2 インターフェイス タイプとして [ポート] または [LAG] を選択します。

ステップ 3 [実行] をクリックします。ポートまたは LAG のリストが表示されます。選択したインターフェイスのタイプに応じて、そのタイプのインターフェイス、および、各インターフェイスに現在バインドされている ACL のリストが表示されます。

- [インターフェイス] : インターフェイス ID。
- [MAC ACL] : インターフェイスにバインドされている MAC ベース ACL（存在する場合）。
- [IPv4 ACL] : インターフェイスにバインドされている IPv4 ベース ACL（存在する場合）。
- [IPv6 ACL] : インターフェイスにバインドされている IPv6 ベース ACL（存在する場合）。

（注）インターフェイスから ACL をアンバインドするには、そのインターフェイスをクリックし、[クリア] をクリックします。

ステップ 4 インターフェイスを選択し、[編集] をクリックします。[ACL バインディングの編集] ページが開きます。

ステップ 5 ACL をバインドするインターフェイスを選択します。

ステップ 6 次のいずれかを選択します。

- [MAC ベース ACL の選択]:インターフェイスにバインドする MAC ベース ACL を選択します。
- [IPv4 ベース ACL の選択] : インターフェイスにバインドする IPv4 ベース ACL を選択します。
- [IPv6 ベース ACL の選択] : インターフェイスにバインドする IPv6 ベース ACL を選択します。

ステップ 7 [適用] をクリックします。ACL バインディングが修正され、実行コンフィギュレーションファイルが更新されます。

（注）ACL をまったく選択しなかった場合、そのインターフェイスにバインドされていた ACL がアンバインドされます。