アクセス コントロール

アクセス コントロール リスト（ACL）機能は、セキュリティ メカニズムの一部です。ACL の定義は、特定のサービス品質（QoS）が与えられたトラフィック フローを定義するメカニズムの 1 つとして機能します。詳細については、「Quality of Service」を参照してください。ACL は、入力トラフィックのパターン（フィルタとアクション）を定義するネットワーク マネージャを有効にします。アクティブな ACL があるポートまたは LAG 上のデバイスに着信するパケットは、エントリが許可または拒否されます。ACL には、Mac ACL、IPv4 ACL、および IPv6 ACL の 3 タイプがあります。すべての ACL タイプは、ユーザー設定によってデバイス設定に追加できます。IPv4 ACL タイプは、802.1x 認証および許可プロセスの一部として、たとえば ISE サービスを介して適用することもできます。

（注） ダウンロード可能な ACL のルールは、Catalyst 9200/9300 ACL シンタックスを使用して ISE で定義されます。デバイスはこのシンタックスを Catalyst 1300 シンタックスに変換し、ルールをデバイスに適用します。

（注） Catalyst 1200/1300 バージョン 4.1.6 では、次のネットワーク機能に基づくゲストアクセス制御 ISE ネットワーク アプリケーションのサポートが追加されています。

- ダイナミック ACL：ユーザーごとに ACL を自動的に適用
- URL リダイレクト：事前定義された Web ベースの認証サーバーにユーザーブラウザをリダイレクト

ゲストアクセス制御をサポートするために、Catalyst 1200/1300 バージョン 4.1.4 では次の機能が追加されました。

- RADIUS 標準の Filter-id（タイプ 11）属性に基づくダイナミック ACL
- Cisco VSA 属性 ACS に基づくダイナミック ACL：Cisco Secure-Defined-ACL（別名：ダウンロード可能な ACL）
- Cisco VSA 属性 URL-redirect-ACL および URL-redirect に基づく URL リダイレクション
- IPDT
- 中間アカウンティング更新

この章は、次の項で構成されています。

MACベースACL

MAC ベースの ACL は、レイヤ 2 のフィールドに基づくトラフィックのフィルタリングに使用されます。MAC ベースの ACL は、一致するすべてのフレームをチェックします。MAC ベース ACL を定義するには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [MAC-Based ACL] をクリックします。

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 [Add] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい 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 [Apply] をクリックします。MAC ベースの ACL は実行コンフィギュレーション ファイルに保存されます。設定を永続的に保存するには、[Save] アイコンをクリックします。

MAC ベースの ACE

（注） 各 MAC ベースのルールは、1 つの TCAM ルールを消費します。TCAM 割り当てはペアで実行されます。たとえば、最初の ACE には 2 つの TCAM ルールが割り当てられ、2 番目の TCAM ルールの方は次の ACE に割り当てられます。

アクセス コントロール エントリ（ACE）を ACL に追加するには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [MAC-Based ACE] をクリックします。

ステップ 2 ACL を選択し、[Go] をクリックします。ACL における ACE の一覧が表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

オプション	説明
ACL Name	ACE が追加されている ACL の名前が表示されます。
Priority	ACE の優先順位を入力します。優先度の高い ACE は最初に処理されます。1 が最も高い優先順位です。
Action	一致時に実行されるアクションを選択します。次のオプションがあります。 • [許可]：ACE 条件に一致するパケットを転送します。 • 拒否（Deny）：ACE 条件に一致するパケットをドロップします。 • [シャットダウン]：ACE 条件に一致するパケットをドロップし、パケットを受信したポートを無効にします。
Logging	ACL ルールと一致する ACL フローのロギングを有効にする場合に選択します。
Time Range	ACL の使用時間を指定した時間範囲に制限する場合に選択します。

オプション	説明
Time Range Name	[Time Range] を選択した場合、使用する時間範囲を選択します。時間範囲は [System Time Configuration]システム時刻セクションで定義します。
Destination MAC Address	すべての宛先アドレスを許可する場合は [Any] を選択します。宛先アドレスまたは宛先アドレスの範囲を入力する場合は [User defined] を選択します。
Destination MAC Address Value	宛先 MAC アドレスが一致する MAC アドレスとマスクを入力します（該当する場合）。
Destination MAC Wildcard Mask	MAC アドレスの範囲を定義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の他の用途とは異なります。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値を照合することを意味します。 （注） 0000 0000 0000 0000 0000 0000 1111 1111 というマスクを例に説明します。この場合、0 になっているビットは照合され、1 になっているビットは照合されません。2 進数値は 16 進数（16 進数 1 桁につき 4 ビット）に変換する必要があります。この例では、1111 1111 = FF であるので、マスクは 00:00:00:00:00:FF と記述されます。
Source MAC Address	すべての送信元アドレスを許可する場合は [Any] を選択します。送信元アドレスまたは送信元アドレスの範囲を入力する場合は [User defined] を選択します。
Source MAC Address Value	送信元 MAC アドレスが一致する MAC アドレスとマスク（該当する場合）を入力します。

ステップ 5 [Apply] をクリックします。MAC ベースの ACE は実行コンフィギュレーション ファイルに保存されます。

IPv4 ベース ACL

ACL は、フローごとの QoS 処理のためのフロー定義の構成要素として使用できます。IPv4 パケットを確認するには、IPv4 ベースの ACL を使用します。IPv4 ベース ACL を定義するには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [IPv4-Based ACL] をクリックします。

このページには、現在定義されている IP v 4 ベースの ACL がすべて含まれています。

ステップ 2 [Add] をクリックします。

ステップ 3 [ACL名] フィールドに、新しい ACL の名前を入力します。名前は大文字と小文字が区別されます。

ステップ 4 IPv4 ベースの ACL を実行コンフィギュレーション ファイルに保存するには、[Apply] をクリックします。IPv4 ベースの ACL テーブルに、次のタイプの IPv4 ACL が表示されます。

1. ユーザーによって追加された ACL：[Originator] 列の [Static] 値で示されます。これらの ACL は、ユーザーによって作成および制御されます。
2. 動的に追加された ACL：802.1x 認証プロセスの一部として認証サーバー（ISE など）によってデバイスに追加された ACL。ユーザーは、このタイプの ACL を変更することはできません。

IPv4ベースACE

（注） 各 IP v 4 ベースのルールは、1 つの TCAM ルールを消費します。TCAM の割り当ては、最初の ACE では一対で実行されます。2 つの TCAM ルールが割り当てられ、2 番目の TCAM ルールが次の ACE に割り当てられます。以降も同様です。

ルール（ACE）を IPv4 ベース ACL に追加するには、次の手順を実行します。

（注） ルールは、ユーザーが作成した ACL に対してのみ追加、削除、および編集できます。動的に作成された ACL の場合、[Add] ボタンと [Edit] ボタンはグレー表示されます。

手順

ステップ 1 [Access Control] > [IPv4-Based ACE] をクリックします。

ステップ 2 ACL を選択し、[Go] をクリックします。選択した ACL に現在定義されている IP ACE がすべて表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

ACL Name	ACE が追加されている ACL の名前が表示されます。
Priority	プライオリティを入力します。優先度の高い ACE は最初に処理されます。 （注） 1 が最も高い優先順位です。

Action	ACEに一致するパケットに割り当てられるアクションを、次のオプションから選択します。 • [許可]：ACE 条件に一致するパケットを転送します。 • 拒否（Deny）：ACE 条件に一致するパケットをドロップします。 • [Shutdown]：ACE 基準に一致するパケットをドロップし、パケットの宛先ポートを無効にします。ポートはエラー回復設定ページで再アクティブ化されます。
Logging	ACL ルールと一致する ACL フローのロギングを有効にする場合に選択します。
Time Range	ACL の使用時間を指定した時間範囲に制限する場合に選択します。
Time Range Name	[Time Range] が選択されている場合は、[Edit] ボタンをクリックすると、時間範囲のページにリダイレクトされるので、使用する時間範囲名を選択します。システム時刻セクションでは、時間範囲について説明します。

Protocol	特定のプロトコルまたはプロトコル ID に基づく ACE を作成する場合に選択します。[Any (IPv4)] を選択して、すべての IP プロトコルを受け入れます。それ以外の場合は、次のいずれかのプロトコルを選択します。 • [ICMP]：インターネット制御メッセージ プロトコル • [IGMP]：インターネット グループ管理プロトコル • [IP-in-IP]：IP-in-IP カプセル化 • [TCP]：トランスミッション コントロール プロトコル • [EGP]：外部ゲートウェイ プロトコル • [IGP]：内部ゲートウェイ プロトコル • [UDP]：ユーザ データグラム プロトコル • [HMP]：ホストマッピングプロトコル • [RDP]：信頼性の高いデータグラムプロトコル • [IDPR]：ドメイン間ポリシー ルーティング プロトコル • [IPV6]：IPv6 over IPv4 トンネリング • [IPV6:ROUT]：ゲートウェイ経由で IPv6 over IPv4 ルートに属するパケットを照合 • [IPV6:FRAG]：IPv6 over IPv4 フラグメント ヘッダーに属するパケットを照合 • [IDRP]：ドメイン間ルーティング プロトコル • [RSVP]：ReSerVation プロトコル • [AH]：認証ヘッダー • [IPV6:ICMP]：インターネット制御メッセージ プロトコル • [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 固有のプロトコル • 一致させるプロトコル ID（Protocol ID to Match）：名前を選択せずにプロトコル ID を入力します。

Source IP Address	すべての送信元アドレスを許可する場合は [Any] を選択します。送信元アドレスまたは送信元アドレスの範囲を入力する場合は [User defined] を選択します。
Source IP Address Value	送信元 MAC アドレスが一致する IP アドレスとマスク（該当する場合）を入力します。
Source IP Wildcard Mask	IP アドレスの範囲を定義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の他の用途とは異なります。ここでビットを 1 と設定すると、その値を気にしないことを意味し、0 はその値をマスクすることを意味します。 （注） 0000 0000 0000 0000 0000 0000 1111 1111 のマスクを指定する場合は、1 を 10 進数の整数に変換し、4 つのゼロごとに 0 を記述する必要があります。この例では 1111 1111 = 255 であるので、マスクは 0.0.0.255 と記述されます。
Destination IP Address	すべての宛先アドレスを許可する場合は [Any] を選択します。宛先アドレスまたは宛先アドレスの範囲を入力する場合は [User defined] を選択します。
Destination IP Address Value	宛先 MAC アドレスが一致する IP アドレスとマスクを入力します（該当する場合）。
Destination IP Wildcard Mask	宛先 IP ワイルドカードマスクを入力します。
Source Port	次のいずれかを選択します。 • [Any]：すべての送信元ポートに対して照合を実行します。 • リストから 1 つ（Single from list）：パケットを一致させる TCP/UDP 送信元ポートを 1 つ選択します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。 • 番号で 1 つ（Single by number）：パケットを一致させる TCP/UDP 送信元ポートを 1 つ入力します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。 • [Range]：0 ー 65535 の範囲を入力します。
Destination Port	使用可能ないずれかの値を選択します。これらは、前述の送信元ポート（Source Port）フィールドと同じです。 （注） 送信元または宛先ポートを入力する前に、ACL の IPv4 プロトコルを指定する必要があります。

TCP Flags	パケットのフィルタ処理に使用する TCP フラグを 1 つ以上選択します。フィルタリングされたパケットは転送またはドロップされます。TCP フラグによるパケットのフィルタリングはパケットの制御を増やし、ネットワーク セキュリティを向上させます。各フラグのタイプに対して、次のオプションのいずれかを選択します。 • 設定（Set）：フラグが SET の場合に一致します。 • [Unset]：フラグが Not SET の場合に照合します。 • 無視（Don’t care）：TCP フラグを無視します。
Type of Service	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。 • [DSCP to match]：照合する Differentiated Service Code Point（DSCP）。 • [照合する IP 優先度]：IP 優先度とは、適切な QoS を確実に提供するためにネットワークが使用する TOS（タイプ オブ サービス）のモデルです。このモデルでは、RFC 791 および RFC 1349 で説明されているように、IP ヘッダーのサービスタイプバイトの 3 つの上位ビットを使用します。
ICMP	ACL が ICMP に基づいている場合は、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。メッセージタイプの名前を選択するか、メッセージ タイプの番号を入力します。すべてのメッセージ タイプを受け入れる場合は、[Any] を選択します。 • 任意（Any）：すべてのメッセージ タイプは受け入れられます。 • リストから選択（Select from list）：ドロップダウン リストからメッセージ タイプを名前で選択します。 • [ICMP Type to Match]：フィルタリングに使用するメッセージタイプの数。
ICMP Code	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フィールドが設定されている場合があります。このコードでフィルタリングするかどうかを設定するには、次のオプションのいずれかを選択します。 • [Any]：すべてのコードを受け入れます。 • ユーザ定義（User Defined）：フィルタリング用に ICMP コードを入力します。

IGMP	ACL が IGMP に基づいている場合は、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。メッセージタイプの名前を選択するか、メッセージ タイプの番号を入力します。 • 任意（Any）：すべてのメッセージ タイプは受け入れられます。 • リストから選択（Select from list）：メッセージ タイプを名前で選択します。 • [IGMP Type to Match]：フィルタリングに使用するメッセージタイプの数。

ステップ 5 [Apply] をクリックします。IPv4 ベースの ACE は実行コンフィギュレーション ファイルに保存されます。

IPv6ベースACL

IPv6 ベース ACL は、IPv6 ベースのトラフィックをチェックします。ACL は、フローごとの QoS 処理のためのフロー定義の構成要素としても使用されます。IPv6 ベース ACL を定義するには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [IPv6-Based ACL] をクリックします。
ステップ 2 [Add] をクリックします。
ステップ 3 [ACL Name] フィールドに、新しい ACL の名前を入力します。名前は大文字と小文字が区別されます。
ステップ 4 [Apply] をクリックします。IPv6 ベースの ACL は実行コンフィギュレーション ファイルに保存されます。

IPv6ベースACE

（注） 各 IP v 6 ベースのルールは、2 つの TCAM ルールを消費します。

IPv6 ベース ACE を定義するには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [IPv6-Based ACE] をクリックします。

このウィンドウには、指定された ACL（ルールのグループ）の ACE（ルール）が含まれます。

ステップ 2 ACL を選択し、[Go] をクリックします。選択した ACL に現在定義されている IP ACE がすべて表示されます。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

ACL Name	ACE が追加されている ACL の名前が表示されます。
Priority	プライオリティを入力します。優先度の高い ACE は最初に処理されます。
Action	ACE に一致するパケットに割り当てられるアクションを、次のオプションから選択します。 • [許可]：ACE 条件に一致するパケットを転送します。 • 拒否（Deny）：ACE 条件に一致するパケットをドロップします。 • シャットダウン（Shutdown）：ACE 条件に一致するパケットをドロップし、パケットが向けられたポートを無効にします。ポートはエラー回復設定ページで再アクティブ化されます。
Logging	ACL ルールと一致する ACL フローのロギングを有効にする場合に選択します。
Time Range	ACL の使用時間を指定した時間範囲に制限する場合に選択します。
Time Range Name	[Time Range] が選択されている場合は、[Edit] ボタンをクリックすると、時間範囲のページにリダイレクトされるので、使用する時間範囲名を選択します。システム時刻セクションでは、時間範囲について説明します。
Protocol	次のオプションから特定のプロトコルに基づいて ACE を作成する場合に選択します。 • [Any (IPv6)]：すべての送信元 IPv6 アドレスが ACE に適用されます • [Select from list]：次のいずれかのオプションから選択します。 • [TCP]： 伝送制御プロトコルにより、2 つのホストが通信してデータストリームを交換できるため、TCP はパケット配信を保証し、パケットが送信された順序で送受信されることが保証されます。 • [UDP]：ユーザー データグラム プロトコルはパケットを送信しますが、パケットの配信は保証しません。 • [ICMP]：パケットを Internet Control Message Protocol（ICMP）と照合します。 • [Protocol ID to match]：照合するプロトコルの ID を入力します。

Source IP Address	すべての送信元アドレスを許可する場合は [Any] を選択します。送信元アドレスまたは送信元アドレスの範囲を入力する場合は [User defined] を選択します。
Source IP Address Value	送信元 MAC アドレスが一致する IP アドレスとマスク（該当する場合）を入力します。
送信元IPプレフィクス長	送信元 IP アドレスのプレフィックス長を入力します。
Destination IP Address	すべての宛先アドレスを許可する場合は [Any] を選択します。宛先アドレスまたは宛先アドレスの範囲を入力する場合は [User defined] を選択します。
Destination IP Address Value	宛先 IP アドレスが一致する IP アドレスとマスクを入力します（該当する場合）。
宛先IPプレフィクス値	IP アドレスのプレフィックス長を入力します。
Source Port	次のいずれかを選択します。 • [Any]：すべての送信元ポートに対して照合を実行します。 • [リストから選択]：パケットを照合する TCP/UDP 送信元ポートを 1 つ選択します。このフィールドは、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。 • [番号]：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、800/6-TCP または 800/17-UDP が [IP Protocol] ドロップダウン メニューから選択されている場合にのみ有効です。
Destination Port	使用可能ないずれかの値を選択します。これらは、前述の送信元ポート（Source Port）フィールドと同じです。 （注） 送信元または宛先ポートを入力する前に、ACL の IPv6 プロトコルを指定する必要があります。
フロー ラベル	[IPv6 Flow label] フィールドに基づいて IPv6 トラフィックを分類します。これは IPv6 パケット ヘッダーに含まれる 20 ビットのフィールドです。送信元ステーションでは IPv6 フロー ラベルを使用して、同じフローに属する複数のパケットにラベルを付けることができます。すべてのフロー ラベルを受け入れ可能な場合は [任意] を選択します。または [ユーザー定義] を選択して、ACL で受け入れる特定のフロー ラベルを入力します。

TCP Flags	パケットのフィルタ処理に使用する TCP フラグを 1 つ以上選択します。フィルタリングされたパケットは転送またはドロップされます。TCP フラグによるパケットのフィルタリングはパケットの制御を増やし、ネットワーク セキュリティを向上させます。各フラグのタイプに対して、次のオプションのいずれかを選択します。 • 設定（Set）：フラグが SET の場合に一致します。 • [Unset]：フラグが Not SET の場合に照合します。 • 無視（Don't care）：TCP フラグを無視します。
Type of Service	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。 • [DSCP to match]：照合する Differentiated Service Code Point（DSCP）。 • [照合する IP 優先度]：IP 優先度とは、適切な QoS を確実に提供するためにネットワークが使用する TOS（タイプ オブ サービス）のモデルです。このモデルでは、RFC 791 および RFC 1349 で説明されているように、IP ヘッダーのサービス タイプ バイトの 3 つの最上位ビットを使用します。
ICMP	ACL が ICMP に基づいている場合は、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。メッセージタイプの名前を選択するか、メッセージ タイプの番号を入力します。すべてのメッセージ タイプを受け入れる場合は、[Any] を選択します。 • 任意（Any）：すべてのメッセージ タイプは受け入れられます。 • リストから選択（Select from list）：ドロップダウン リストからメッセージ タイプを名前で選択します。 • [ICMP Type to Match]：フィルタリングに使用するメッセージタイプの数。
ICMP Code	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フィールドが設定されている場合があります。このコードでフィルタリングするかどうかを設定するには、次のオプションのいずれかを選択します。 • [Any]：すべてのコードを受け入れます。 • ユーザ定義（User Defined）：フィルタリング用に ICMP コードを入力します。

ステップ 5 [Apply] をクリックします。

ACLバインディング(VLAN)

ACL をインターフェイスにバインドすると、その ACE ルールが、このインターフェイスに届いたパケットに適用されます。ACL 内のどの ACE にも一致しないパケットは、不一致のパケットをドロップするアクションを行うデフォルトのルールに一致します。各インターフェイスは 1 つの ACL にのみバインドできますが、ポリシー マップにグループ化し、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。ACL がインターフェイスにバインドされた後は、その ACL がバインドされている、または使用中のすべてのポートから削除されるまで、編集、変更、削除することはできません。

（注） インターフェイス（ポート、LAG または VLAN）をポリシーまたは ACL にバインドすることはできますが、ポリシーと ACL の両方にバインドすることはできません。同一のクラスマップでは、宛先 IPv6 アドレスがフィルタリング条件として設定されている IPv6 ACE と同時に MAC ACL を使用することはできません。

ACL を VLAN にバインドするには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [VLAN] をクリックします。

ステップ 2 VLAN を編集するには、VLAN を選択し、[Edit] をクリックします。

必要な VLAN が表示されない場合、[Add] をクリックして、新しい VLAN を追加します。その後、次の手順に進みます。

ステップ 3 次のいずれかを選択します。

MACベースACL	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	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	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。
Default Action	次のオプションのいずれかを選択します。 • [Deny Any]：ACL に一致しないパケットは拒否（ドロップ）されます。 • [Permit Any]：ACL に一致しないパケットは許可（転送）されます。 （注） [Default Action] は、IP ソースガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

ステップ 4 既存の VLAN をコピーするには、[Copy]（コピーアイコン）をクリックします。バインディングテーブルから VLAN を削除する場合は、[Delete] をクリックします。

ステップ 5 [Apply] をクリックします。ACL のバインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

ACLバインディング(ポート)

アクセスコントロールリスト（ACL）は、ポートに送信されるパケットのストリームをフィルタ処理するポートに適用される権限のリストです。ポートにバインドできるのはポリシーまたはACLのいずれかです。両方をバインドすることはできません。デフォルトアクションでは、ACL内のルールを満たさないすべてのパケットが破棄されます（すべて拒否）。ACLのデフォルトアクションをオーバーライドし、対象のポートに [Permit Any] を設定することで該当のパケットを転送できます。

ACL をポートまたは LAG にバインドするには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [ACL Binding（Port] をクリックします。

ステップ 2 インターフェイス タイプ [Ports/LAGs] （ポートまたは LAG）を選択します。

ステップ 3 [Go]をクリックします。選択されているインターフェイスのタイプごとに、そのタイプのすべてのインターフェイスが、現在の ACL のリストとともに表示されます（[Input ACL] および [Output ACL]）。

インターフェイス	ACL が定義されているインターフェイスの識別子。
MAC ACL	インターフェイスにバインドされているMACタイプの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タイプの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タイプのACL（存在する場合）。
Default Action	ACL のルールのアクション（[いずれも拒否（deny any）] または [いずれも許可（permit any）]）。

ステップ 4 インターフェイスを編集する場合は、インターフェイスを選択して [Edit] をクリックします。

ステップ 5 入力 ACL と出力 ACL に関する以下の内容を入力します。

MACベースACL	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	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	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。

Default Action	次のオプションのいずれかを選択します。 • [Deny Any]：ACL に一致しないパケットは拒否（ドロップ）されます。 • [Permit Any]：ACL に一致しないパケットは許可（転送）されます。 （注） [Default Action] は、IP ソースガードがそのインターフェイス上でアクティブでない場合にのみ定義できます。

ステップ 6 [Apply] をクリックします。ACL のバインディングが変更され、実行コンフィギュレーション ファイルが更新されます。

インターフェイス ACL ごとの IPv4

ポートに適用された ACL および ACE の詳細を表示するには、次の手順を実行します。

手順

ステップ 1 [Access Control] > [IPv4 per Interface ACL] の順にクリックし、必要なインターフェイスを選択します。

ステップ 2 [Filter] セクションで、ドロップダウンメニューから [Interface] を選択し、[Go] をクリックします。選択したインターフェイスに応じて ACL が表示されます。

ステップ 3 ACL は、選択したインターフェイスに応じて、[IPv4 per Interface ACL] テーブルに表示されます。デフォルト値は、最初のポートに基づいて入力されます。[Protocol]、[Source Port]、[Destination Port]、または [ICMP Type] の値が特定のプロトコル、アプリケーション、または ICMP にマッピングされている場合、列に表示される値はマッピングされた値であり、受信した数値ではありません。

ステップ 4 [Authenticated Sessions Table] ボタンをクリックして、[Security] > [802.1x Authentication] > [Authenticated Sessions] の順に選択します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。