



IPv4 ACL

- [IPv4 アクセスコントロールリストの制約事項 \(1 ページ\)](#)
- [IPv4 アクセスコントロールリストに関する情報 \(3 ページ\)](#)
- [IPv4 アクセスコントロールリストの設定方法 \(15 ページ\)](#)
- [IPv4 ACL のモニタリング \(33 ページ\)](#)
- [IPv4 アクセスコントロールリストの設定例 \(34 ページ\)](#)
- [IPv4 アクセスコントロールリストに関する追加情報 \(47 ページ\)](#)
- [IPv4 アクセスコントロールリストの機能履歴 \(48 ページ\)](#)

IPv4 アクセスコントロールリストの制約事項

一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケットフィルタおよびルートフィルタ用の ACL では、名前を使用できます。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプストリングに表示されますが、**deny** および **permit** MAC アクセスリスト コンフィギュレーションモード コマンドの一致条件としてサポートされていません。
- ACL ワイルドカードは、ダウンストリーム クライアント ポリシーではサポートされていません。
- プロトコルの TCAM をプログラムしないインターフェイスと、アンロードされた ACL にスケール ACL を適用すると、他のプロトコルのトラフィックの既存の通常移動に影響を与える可能性があります。IPv6 および MAC アドレストラフィックにこの制限は適用されます。

IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。
- パケットをフィルタリングするために **preauth_ipv4_acl** ACL が設定されている場合、ACL は認証後に削除されます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。



(注) **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポートチャネルでは使用できません。

IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミックアクセスリスト、再帰アクセスリスト、またはファイアウォールアクセス リストをサポートしていません。

IPv4 アクセスコントロールリストに関する情報

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL は、トラフィックをデバイスの通過時にフィルタリングし、パケットが指定されたインターフェイスを通過することを許可または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、転送するすべてのパケット上で ACL を使用できます。

ネットワークに基本的なセキュリティを導入する場合は、デバイスにアクセスリストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、デバイスインターフェイスで転送またはブロックされるトラフィックの種類を決定できます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ (ACE) の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

ACL でサポートされるタイプ

デバイスは、IP ACL とイーサネット (MAC) ACL をサポートしています。

- IP ACL は、TCP、ユーザ データ グラム プロトコル (UDP)、インターネット グループ 管理 プロトコル (IGMP)、およびインターネット 制御 メッセージ プロトコル (ICMP) などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このデバイスは、Quality of Service (QoS) 分類 ACL もサポートしています。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。IPv4 と MAC どちらのアクセスリストタイプのどの方向に対してでも、レイヤ 2 インターフェイスにポート ACL を適用できます。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（インバウンドまたはアウトバウンド）に適用されます。

ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

ポート ACL

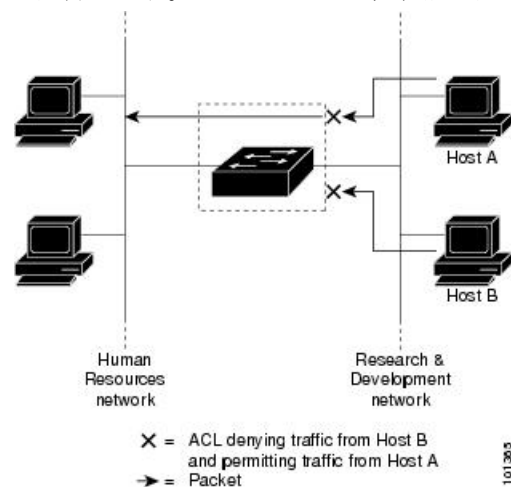
ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は、物理インターフェイスおよび EtherChannel インターフェイス上でサポートされています。ポート ACL は、着信方向のインターフェイスに適用できます。次のアクセス リストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

図 1: ACL によるネットワーク内のトラフィックの制御

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2



インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセスリストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。



- (注) レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス (SVI)、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

VLAN マップ

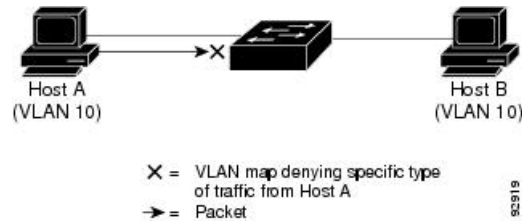
VLAN ACL または VLAN マップは、VLAN 内のネットワークトラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VLAN マップではアクセス制御されません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 2: VLAN マップによるトラフィックの制御

次の図に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用で



きます。

ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ (ACE) には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報 (TCP や UDP などのプロトコル タイプを含む) をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。



(注) L4 Ops をともなう ACE の TCP では、フラグメント化パケットは RFC 1858 ごとにドロップします。

- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

標準 IPv4 ACL および拡張 IPv4 ACL

ACL は、許可条件と拒否条件の順序付けられた集まりです。デバイスは、アクセスリスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、デバイスがパケットを受け入れるか拒否するかが決定されます。デバイスは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、デバイスはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさが高めることもできます。

IPv4 ACL スイッチでサポートされていない機能

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リストタイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 1: アクセス リスト番号

| アクセス リスト番号 | タイプ | サポートあり |
|-------------|--------------------------|--------|
| 1 ～ 99 | IP 標準アクセス リスト | あり |
| 100 ～ 199 | IP 拡張アクセス リスト | あり |
| 200 ～ 299 | プロトコルタイプコードアクセス リスト | なし |
| 300 ～ 399 | DECnet アクセス リスト | なし |
| 400 ～ 499 | XNS 標準アクセス リスト | なし |
| 500 ～ 599 | XNS 拡張アクセス リスト | なし |
| 600 ～ 699 | AppleTalk アクセス リスト | なし |
| 700 ～ 799 | 48 ビット MAC アドレス アクセス リスト | なし |
| 800 ～ 899 | IPX 標準アクセス リスト | なし |
| 900 ～ 999 | IPX 拡張アクセス リスト | なし |
| 1000 ～ 1099 | IPX SAP アクセス リスト | なし |

| アクセス リスト番号 | タイプ | サポートあり |
|-------------|-------------------------------------|--------|
| 1100 ～ 1199 | 拡張 48 ビット MAC サマリー アドレス アクセス リスト | なし |
| 1200 ～ 1299 | IPX サマリー アドレス アクセ ス リスト | なし |
| 1300 ～ 1999 | IP 標準アクセス リスト（拡張 範囲） | あり |
| 2000 ～ 2699 | IP 拡張アクセス リスト（拡張 範囲） | あり |

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホストアドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

デバイスは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセスリストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を VLAN、端末回線、またはインターフェイスに適用できます。

番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコルタイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このデバイスは、ダイナミックまたはリフレクシブアクセスリストをサポートしていません。また、タイプ オブ サービス (ToS) の **minimize-monetary-cost** ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このデバイスは以下の IP プロトコルをサポートします。



(注) ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル (**ahp**)
- カプセル化セキュリティペイロード (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- 総称ルーティング カプセル化 (**gre**)
- インターネット制御メッセージ プロトコル (**icmp**)
- インターネット グループ管理プロトコル (**igmp**)
- すべての内部プロトコル (**ip**)
- IP-in-IP トンネリング (**ipinip**)
- KA9Q NOS 互換 IP over IP トンネリング (**nos**)
- Open Shortest Path First ルーティング (**ospf**)
- ペイロード圧縮プロトコル (**pcp**)
- プロトコル独立マルチキャスト (**pim**)
- 伝送制御プロトコル (**tcp**)
- ユーザ データグラム プロトコル (**udp**)

名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、デバイス上で番号付きアクセスリストの場合より多くの IPv4 アクセスリストを設定できます。アクセスリストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。



(注) 標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。つまり、標準の IP ACL の名前は 1～99 を指定できます。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- VLAN マップには、標準 ACL または拡張 ACL（名前付きまたは番号付き）を使用できません。

ACL ロギング

標準 IP アクセスリストによって許可または拒否されたパケットに関するログメッセージが、デバイスのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。



(注) ACL ロギングは、RACL でのみサポートされます。



(注) ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可 (*permit*) または拒否 (*deny*) ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログメッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログメッセージにはアクセスリスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。



(注) ロギングメッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギングメッセージが複数ある場合、ロギング設備ではロギングメッセージパケットの一部をドロップすることがあります。この動作によって、ロギングパケットが多すぎてデバイスがクラッシュすることを回避します。そのため、課金ツールや、アクセスリストと一致する数の正確な情報源としてロギング設備を使用しないでください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。



- (注) デバイスまたはスタックメンバのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、デバイスに着信した該当 VLAN 内のトラフィックだけです。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードの使用
- ICMP 到達不能メッセージを生成する。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチドパケットおよびルーテッドパケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show platform software fed switch { switch_num | active | standby } acl counters hardware** 特権 EXEC コマンドを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL（入力および出力）の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- *ip unreachable* が無効の場合、**log**を指定しないと、セキュリティ ACL の *deny* ステートメントと一致するフローがハードウェアによってドロップされます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

VLAN マップの設定時の注意事項

VLAN マップは、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケット タイプ（IP または MAC）に対する **match** 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケット タイプに対する **match** コマンドがない場合、デフォルトでは、パケットが転送されます。

次は、VLAN マップ設定の注意事項です。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。デバイスに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行され

ます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。

- 該当パケットタイプ（IP または MAC）に対する **match** 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの **match** 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケットタイプに対する **match** 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセスリストまたは MAC アクセスリストがデバイスにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップよりも優先されます。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットがドロップします。

VLAN マップとルータ ACL

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセスコントロールを行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせ使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケットフローが ACL 内 VLAN マップの **deny** ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケットフローは拒否されます。



- (注) ルータ ACL を VLAN マップと組み合わせ使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケットタイプ（IP または MAC）に対する **match** 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。VLAN マップ内に **match** 句がなく、アクションが指定されていない場合、どの VLAN マップエントリとも一致しないパケットは転送されます。

VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。

- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルトアクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

```
permit... permit... permit... deny ip any any
```

または

```
deny... deny... deny... permit ip any any
```

- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコル ポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

ACL の時間範囲

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。**time-range** キーワードおよび引数については、名前付きおよび番号付き拡張 ACL タスクの表を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、ハードウェアメモリにロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセスリストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。



- (注) 時間範囲は、デバイスのシステムクロックに基づきます。したがって、信頼できるクロックソースが必要です。ネットワーク タイム プロトコル (NTP) を使用してデバイスクロックを同期させることを推奨します。

IPv4 ACL のインターフェイスに関する注意事項

インバウンド ACL の場合、パケットの受信後デバイスはパケットを ACL と照合します。ACL がパケットを許可する場合、デバイスはパケットの処理を継続します。ACL がパケットを拒否する場合、デバイスはパケットを廃棄します。

アウトバウンド ACL の場合、パケットを受信し制御対象インターフェイスにルーティングした後、デバイスはパケットを ACL と照合します。ACL がパケットを許可した場合は、デバイスはパケットを送信します。ACL がパケットを拒否する場合、デバイスはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、デバイスは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワークセキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

IPv4 アクセスコントロールリストの設定方法

IPv4 ACL の設定

このスイッチで IP ACL を使用する手順は次のとおりです。

手順

- ステップ 1** アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。
- ステップ 2** その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | access-list access-list-number {deny permit} source source-wildcard] 例 : Device(config)# access-list 2 deny your_host | 送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 <i>access-list-number</i> には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は deny を指定し、許可する場合は permit を指定します。 <i>source</i> には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビット長の値。 キーワード any は 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形です。<i>source-wildcard</i> を入力する必要はありません。 キーワード host は送信元および <i>source</i> 0.0.0.0 の <i>source-wildcard</i> の省略形です。 |

| | コマンドまたはアクション | 目的 |
|-------|---|---|
| | | <p>(任意) <i>source-wildcard</i> は、ワイルドカードビットを送信元アドレスに適用します。</p> <p>(注) ロギングは、レイヤ3インターフェイスに割り当てられたACLでだけサポートされます。</p> |
| ステップ4 | end 例 : Device(config)# end | グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

番号付き拡張 ACL の作成

番号付き拡張 ACL を作成するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|-------|---|--|
| ステップ1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ3 | access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] 例 : Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log | 拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 <i>access-list-number</i> には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は deny を指定し、許可する場合は permit を指定します。 |

| | コマンドまたはアクション | 目的 |
|--|--------------|---|
| | | <p>source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。</p> <ul style="list-style-type: none"> • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード any。 • 単一のホスト 0.0.0.0 を表すキーワード host。 <p>その他のキーワードはオプションであり、次の意味を持ちます。</p> <ul style="list-style-type: none"> • precedence : パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、routine (0)、priority (1)、immediate (2)、flash (3)、flash-override (4)、critical (5)、internet (6)、network (7) です。 • fragments : 2 つ目以降のフラグメントをチェックする場合に入力します。 • tos : パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、normal (0)、max-reliability (2)、max-throughput (4)、min-delay (8) です。 • time-range : 時間範囲の名前を指定します。 • dscp : パケットを 0 ～ 63 の番号で指定する DSCP 値と一致させる場合に入力します。または、指定できる値のリストを表示するには、疑問符 (?) を使用します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | | (注) dscp 値を入力する場合は、 tos または precedence を入力できません。 dscp を入力せずに tos と precedence の両方の値を入力できます。 |
| ステップ 4 | <p>access-list access-list-number {deny permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] [flag]</p> <p>例 :</p> <pre>Device(config)# access-list 101 permit tcp any any eq 500</pre> | <p>拡張 TCP アクセス リストおよびアクセス条件を定義します。</p> <p>次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。</p> <p>(任意) <i>operator</i> および <i>port</i> を入力すると、送信元ポート (<i>source source-wildcard</i> の後に入力した場合) または宛先ポート (<i>destination destination-wildcard</i> の後に入力した場合) が比較されます。演算子の候補には、eq (次の値に等しい)、gt (次の値より大きい)、lt (次の値より小さい)、neq (次の値に等しくない)、および range (次の範囲) があります。演算子にはポート番号を指定する必要があります (range の場合は 2 つのポート番号をスペースで区切って指定する必要があります)。</p> <p><i>port</i> には、10 進数 (0 ~ 65535) のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。</p> <p>他のオプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • established : 確立された接続と照合する場合に入力します。このキーワードは、ack または rst フラグでの照合と同じ機能を果たします。 • flag : 指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、ack (確認応答)、fin (終了)、psh (プッシュ)、rst |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | | (リセット)、 syn (同期)、または urg (緊急) です。 |
| ステップ 5 | access-list access-list-number {deny permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] 例 : Device(config)# access-list 101 permit udp any any eq 100 | (任意) 拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前を指定する必要があります。また、UDP では、 flag キーワードと established キーワードは無効です。 |
| ステップ 6 | access-list access-list-number {deny permit} icmp source source-wildcard destination destination-wildcard [icmp-type [[icmp-type icmp-code] [icmp-message]]] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] 例 : Device(config)# access-list 101 permit icmp any any 200 | 拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • icmp-type : ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-code : ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message : ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。 |
| ステップ 7 | access-list access-list-number {deny permit} igmp source source-wildcard destination destination-wildcard [igmp-type] | (任意) 拡張 IGMP アクセス リストおよびアクセス条件を定義します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | <p>[precedence <i>precedence</i>] [tos <i>tos</i>]</p> <p>[fragments] [time-range <i>time-range-name</i>]</p> <p>[dscp <i>dscp</i>]</p> <p>例 :</p> <pre>Device(config)# access-list 101 permit igmp any any 14</pre> | <p>IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。</p> <p><i>igmp-type</i> IGMP メッセージタイプと比較するには、0～15の番号またはメッセージ名 (dvmrp、host-query、host-report、pim、または trace) を入力します。</p> |
| ステップ 8 | <p>end</p> <p>例 :</p> <pre>Device(config)# end</pre> | <p>グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p> |

名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | <p>enable</p> <p>例 :</p> <pre>Device> enable</pre> | <p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | <p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre> | <p>グローバル コンフィギュレーション モードを開始します。</p> |
| ステップ 3 | <p>ip access-list standard name</p> <p>例 :</p> <pre>Device(config)# ip access-list standard 20</pre> | <p>名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。</p> <p>名前には、1～99の番号を使用できます。</p> |
| ステップ 4 | <p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> deny { <i>source</i> [<i>source-wildcard</i>] host <i>source</i> any } [log] | <p>アクセス リスト コンフィギュレーション モードで、パケットを転送するかドロップするかを決定する1つ以上の拒否条件または許可条件を指定します。</p> |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | <ul style="list-style-type: none"> • permit {<i>source</i> [<i>source-wildcard</i>] host <i>source</i> any} [log] <p>例 :</p> <pre>Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</pre> <p>または</p> <pre>Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</pre> | <ul style="list-style-type: none"> • host source : 送信元および送信元ワイルドカードの値である <i>source</i> 0.0.0.0。 • any : 送信元および送信元ワイルドカードの値である 0.0.0.0 255.255.255.255 |
| ステップ 5 | <p>end</p> <p>例 :</p> <pre>Device(config-std-nacl)# end</pre> | アクセスリスト コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | <p>enable</p> <p>例 :</p> <pre>Device> enable</pre> | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。 |
| ステップ 2 | <p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre> | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | <p>ip access-list extended name</p> <p>例 :</p> <pre>Device(config)# ip access-list extended 150</pre> | <p>名前を使用して拡張 IPv4 アクセスリストを定義し、アクセスリスト コンフィギュレーションモードを開始します。</p> <p>名前には、100 ～ 199 の番号を使用できます。</p> |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 4 | <p>{deny permit} protocol {source [source-wildcard] host source any} {destination [destination-wildcard] host destination any} [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</p> <p>例 :</p> <pre>Device(config-ext-nacl)# permit 0 any any</pre> | <p>アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。log キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。</p> <ul style="list-style-type: none"> • host source : 送信元および送信元ワイルドカードの値である <i>source</i> 0.0.0.0。 • host destination : 接続先および接続先ワイルドカードの値である <i>destination</i> 0.0.0.0。 • any : source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255 |
| ステップ 5 | <p>end</p> <p>例 :</p> <pre>Device(config-ext-nacl)# end</pre> | <p>アクセスリスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。</p> |

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

次のタスク

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

ACL の時間範囲の設定

ACL の時間範囲パラメータを設定するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例 : <pre>Device> enable</pre> | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : <pre>Device# configure terminal</pre> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | time-range time-range-name 例 : <pre>Device(config)# time-range workhours</pre> | 作成する時間範囲には意味のある名前（ <i>workhours</i> など）を割り当て、時間範囲 コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。 |
| ステップ 4 | 次のいずれかを使用します。 <ul style="list-style-type: none"> absolute [<i>start time date</i>] [<i>end time date</i>] periodic <i>day-of-the-week hh:mm to [day-of-the-week] hh:mm</i> periodic { <i>weekdays</i> <i>weekend</i> <i>daily</i> } <i>hh:mm to hh:mm</i> 例 : <pre>Device(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006</pre> または <pre>Device(config-time-range)# periodic weekdays 8:00 to 12:00</pre> | 適用対象の機能がいつ動作可能になるかを指定します。 <ul style="list-style-type: none"> 時間範囲には、absolute ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。 複数の periodic ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 |
| ステップ 5 | end 例 : <pre>Device(config-time-range)# end</pre> | 時間範囲 コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

次のタスク

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | line [console vty] line-number 例 : Device(config)# line console 0 | 設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 <ul style="list-style-type: none">console : コンソール端末回線を指定します。コンソール ポートは DCE です。vty : リモートコンソールアクセス用の仮想端末を指定します。 <p><i>line-number</i> は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ～ 16 です。</p> |
| ステップ 4 | access-class access-list-number {in out} 例 : Device(config-line)# access-class 10 | (デバイスへの) 特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | in | |
| ステップ 5 | end 例 : Device(config-line)# end | 回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。 |

インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。インターフェイスへのアクセスを制御する管理には、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例 : Device(config)# interface gigabitethernet1/0/1 | 設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ 3 インターフェイス（ルータ ACL）を指定できます。 |
| ステップ 4 | ip access-group {access-list-number name} {in out} 例 : Device(config-if)# ip access-group 2 in | 指定されたインターフェイスへのアクセスを制御します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 5 | end 例 : <pre>Device(config-if) # end</pre> | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

名前付き MAC 拡張 ACL を作成するには、次の手順に従ってください。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例 : <pre>Device> enable</pre> | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : <pre>Device# configure terminal</pre> | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | mac access-list extended name 例 : <pre>Device(config)# mac access-list extended mac1</pre> | 名前を使用して MAC 拡張アクセス リストを定義します。 |
| ステップ 4 | <pre>{deny permit} {any host source MAC address source MAC address mask} {any host destination MAC address destination MAC address mask} [type mask lsap lsap mask aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat larc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp 0-65535] [cos cos]</pre> | 拡張 MAC アクセスリスト コンフィギュレーション モードでは、すべての送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定の host の送信元 MAC アドレスと、 any の宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、 permit または deny を指定します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| | <p>例 :</p> <pre>Device(config-ext-macl)# deny any any decnet-iv</pre> <p>または</p> <pre>Device(config-ext-macl)# permit any any</pre> | <p>(任意) 次のオプションを入力することもできます。</p> <ul style="list-style-type: none"> • <i>type mask</i> : Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる <i>don't care</i> ビットのマスクが EtherType に適用されます。 • <i>lsap lsap mask</i> : IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で <i>don't care</i> ビットのマスクを指定できます。 • <i>aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp</i> : 非 IP プロトコル。 • <i>cos cos</i> : プライオリティを設定する 0 ～ 7 の IEEE 802.1Q CoS 番号。 |
| ステップ 5 | <p>end</p> <p>例 :</p> <pre>Device(config-ext-macl)# end</pre> | <p>拡張 MAC アクセスリストコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p> |

レイヤ2 インターフェイスへの MAC ACL の適用

レイヤ2 インターフェイスへのアクセスを制御するために MAC アクセスリストを適用するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---------------------------------|---|
| ステップ 1 | <p>enable</p> <p>例 :</p> | <p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| | Device> enable | |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例 : Device(config)# interface gigabitethernet1/0/2 | 特定のインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。指定するインターフェイスは物理レイヤ2インターフェイス（ポート ACL）でなければなりません。 |
| ステップ 4 | mac access-group {name} {in out} 例 : Device(config-if)# mac access-group mac1 in | MAC アクセスリストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL はアウトバウンドおよびインバウンド方向でサポートされます。 |
| ステップ 5 | end 例 : Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 6 | show mac access-group [interface interface-id] 例 : Device# show mac access-group interface gigabitethernet1/0/2 | そのインターフェイスまたはすべてのレイヤ2インターフェイスに適用されている MAC アクセスリストを表示します。 |

デバイスは、パケットを受信すると、インバウンド ACL とパケットを照合します。ACL がパケットを許可する場合、デバイスはパケットの処理を継続します。ACL がパケットを拒否する場合、デバイスはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、デバイスは ACL がインターフェイスに適用されていないものとして、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

VLAN マップの設定

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

始める前に

VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例 : <pre>Device> enable</pre> | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : <pre>Device# configure terminal</pre> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | vlan access-map name [number] 例 : <pre>Device(config)# vlan access-map map1 20</pre> | <p>VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。</p> <p>同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。</p> <p>VLAN マップでは、特定の permit または deny キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。</p> <p>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。</p> |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 4 | <p>match {ip mac} address {name number} [name number]</p> <p>例 :</p> <pre>Device(config-access-map)# match ip address ip2</pre> | <p>1つまたは複数の標準または拡張アクセスリストに対してパケットを照合します（IPまたはMACアドレスを使用）。パケットの照合は、対応するプロトコルタイプのアクセスリストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセスリストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセスリストに対してだけ照合されます。</p> <p>(注) パケットタイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップアクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップがなく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。</p> |
| ステップ 5 | <p>IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。</p> <ul style="list-style-type: none"> • action { forward } <pre>Device(config-access-map)# action forward</pre> <ul style="list-style-type: none"> • action { drop } <pre>Device(config-access-map)# action drop</pre> | <p>マップエントリに対するアクションを設定します。</p> |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 6 | exit 例 : Device(config-access-map) # exit | アクセスマップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーションモードに戻ります。 |
| ステップ 7 | vlan filter mapname vlan-list list 例 : Device(config) # vlan filter map1 vlan-list 20-22 | VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12、22、30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。 |
| ステップ 8 | end 例 : Device(config) # end | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、次の手順に従います。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | vlan filter mapname vlan-list list 例 : Device(config) # vlan filter map 1 vlan-list 20-22 | VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12、22、30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 4 | end 例 : Device(config)# end | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに 戻ります。 |

IPv4 ACL のモニタリング

デバイスに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニタできます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセスグループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 2: アクセス リストおよびアクセス グループを表示するコマンド

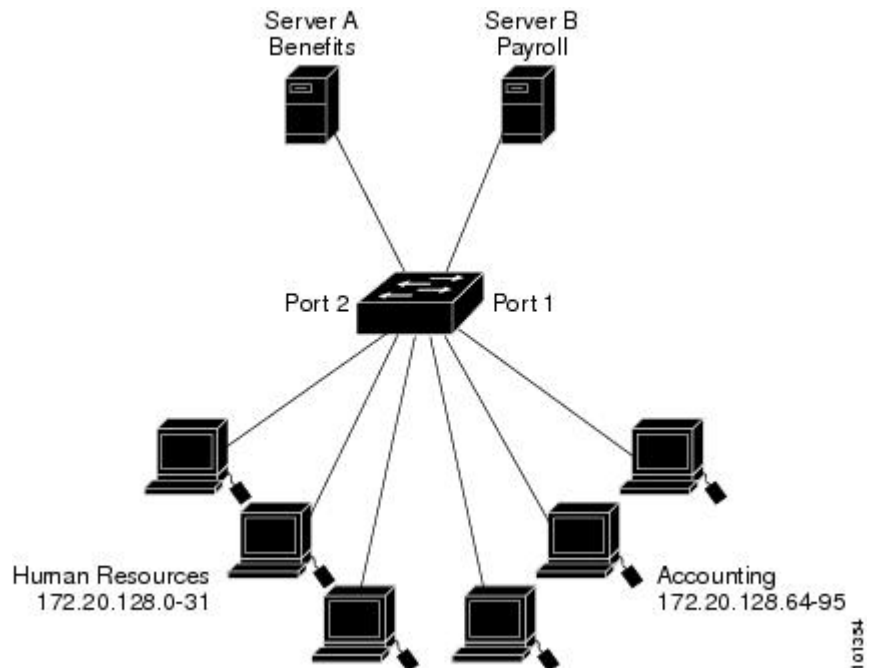
| コマンド | 目的 |
|--|---|
| show access-lists [<i>number</i> <i>name</i>] | 最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセスリスト（番号付きまたは名前付き）の内容を表示します。 |
| show ip access-lists [<i>number</i> <i>name</i>] | 最新の IP アクセスリスト全体、または特定の IP アクセスリスト（番号付きまたは名前付き）を表示します。 |
| show ip interface <i>interface-id</i> | インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、 ip access-group インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセスグループも表示に含まれます。 |
| show running-config [<i>interface interface-id</i>] | デバイスまたは指定されたインターフェイスのコンフィギュレーションファイルの内容（設定されたすべての MAC および IP アクセスリストや、どのアクセスグループがインターフェイスに適用されたかなど）を表示します。 |
| show mac access-group [<i>interface interface-id</i>] | すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。 |

IPv4 アクセスコントロールリストの設定例

小規模ネットワークが構築されたオフィス用の ACL

図 3: ルータ ACL によるトラフィックの制御

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッドポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッドポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユー



ザは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

例：小規模ネットワークが構築されたオフィスの ACL

次に、標準 ACL を使用してポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ~ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッドポート 1 から送信されるトラフィックに適用されます。

```

Device> enable
Device# configure terminal
Device(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Device(config)# exit
Device# show access-lists

Standard IP access list 6
 10 permit 172.20.128.64, wildcard bits 0.0.0.31

Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 6 out
Device(config-if)# end

```

次に、拡張ACLを使用してサーバBからポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバB）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。このACLは、ルーテッドポート1に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張ACLを使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```

Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# exit
Device# show access-lists

Extended IP access list 106
 10 permit ip any 172.20.128.64 0.0.0.31

Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 106 in
Device(config-if)# end

```

例：番号付き ACL

次の例のネットワーク 10.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネットマスクは 255.255.0.0 です。ネットワーク 10.0.0.0 アドレスの 3 番目および 4 番目のオクテットで特定のホストを指定します。アクセスリスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセスリストの最終行は、ネットワーク 10.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```

Device> enable
Device# configure terminal
Device(config)# access-list 2 permit 10.48.0.3
Device(config)# access-list 2 deny 10.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 10.0.0.0 0.255.255.255
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip access-group 2 in
Device(config-if)# end

```

例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 行目で、ホスト 172.16.0.0 の Simple Mail Transfer Protocol (SMTP) ポートへの着信 TCP 接続を許可しています。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Device> enable
Device# configure terminal
Device(config)# access-list 102 permit tcp any 172.16.0.0 0.0.255.255 gt 1023
Device(config)# access-list 102 permit tcp any host 172.16.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# ip access-group 102 in
Device(config-if)# end
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール (SMTP) ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。安全なネットワークシステムでは常にポート 25 でのメール接続が使用されているため、着信サービスは個別に制御されます。

```
Device> enable
Device# configure terminal
Device(config)# access-list 102 permit tcp any 172.16.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 172.16.0.0 0.0.255.255 eq 25
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip access-group 102 in
Device(config-if)# end
```

次の例では、ネットワークはアドレスが 172.16.0.0 のクラス B ネットワークで、メールホストのアドレスは 172.16.1.2 です。established キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。ギガビットイーサネットインターフェイス 1 は、デバイスをインターネットに接続するインターフェイスです。

```
Device> enable
Device# configure terminal
Device(config)# access-list 102 permit tcp any 172.16.0.0 0.0.255.255 established
Device(config)# access-list 102 permit tcp any host 172.16.1.2 eq 25
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip access-group 102 in
Device(config-if)# end
```

例：名前付き ACL

名前付き標準 ACL および名前付き拡張 ACL の作成

次に、Internet_filter という名前の標準 ACL および marketing_group という名前の拡張 ACL を作成する例を示します。Internet_filter ACL は、送信元アドレス 10.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 10.2.3.4
Device(config-ext-nacl)# exit
Device(config-ext-nacl)# end
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 172.16.0.0 0.0.255.255 への任意の TCP/Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 172.16.0.0 ~ 172.16.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended marketing_group
Device(config-ext-nacl)# permit tcp any 172.16.0.0 0.0.255.255 eq telnet
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# permit icmp any any
Device(config-ext-nacl)# deny udp any 172.16.0.0 0.0.255.255 lt 1024
Device(config-ext-nacl)# deny ip any any log
Device(config-ext-nacl)# end
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet3/0/2
Device(config-if)# no switchport
Device(config-if)# ip address 10.0.5.1 255.255.255.0
Device(config-if)# ip access-group Internet_filter out
Device(config-if)# ip access-group marketing_group in
Device(config-if)# end
```

名前付き ACL からの個別 ACE の削除

次に、名前付きアクセスリスト *border-list* から ACE を個別に削除する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
Device(config-ext-nacl)# end
```

例：ACL ロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Device> enable
```

```

Device# configure terminal
Device(config)# ip access-list standard stan1
Device(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Device(config-std-nacl)# permit any log
Device(config-std-nacl)# exit
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group stan1 in
Device(config-if)# end
Device# show logging

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet

```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# ip access-list extended ext1
Device(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Device(config-ext-nacl)# deny udp any any log
Device(config-std-nacl)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip access-group ext1 in
Device(config)# end

```

次に、拡張 ACL のログの例を示します。

```

01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets

```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```

00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
->

```

```
10.1.1.61 (0/0), 1 packet
```

log キーワードを指定した場合、同様のパケットに関するログメッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0),
1 packet
```

例：ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

次のコマンドで構成され、フラグメント化された3つのパケットに適用されるアクセスリスト102を例にとって説明します。

```
Device> enable
Device# configure terminal
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
Device(config)# end
```



(注) 最初の2つのACEには宛先アドレスの後に *eq* キーワードがありますが、これは既知のTCP宛先ポート番号がそれぞれシンプルメール転送プロトコル (SMTP) および Telnet と一致するかどうかをチェックすることを意味します。

- パケットAは、ホスト10.2.2.2のポート65000からホスト10.1.1.1のSMTPポートに送信されるTCPパケットです。このパケットがフラグメント化された場合、レイヤ4情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初のACE (permit) と一致します。残りのフラグメントも最初のACEと一致します。これは、それらのフラグメントにSMTPポート情報が含まれていなくても、最初のACEが適用されたときにレイヤ3情報だけをチェックするからです。この例の情報は、パケットがTCPであることと、宛先が10.1.1.1であることです。
- パケットBは、ホスト10.2.2.2のポート65001からホスト10.1.1.2のTelnetポートに送信されます。このパケットがフラグメント化された場合、レイヤ3情報とレイヤ4情報がすべて揃っているため、最初のフラグメントが2つめのACE (deny) と一致します。残りのフラグメントは、レイヤ4情報が含まれていないため、2つめのACEと一致しません。残りのフラグメントは3つめのACE (permit) と一致します。

最初のフラグメントが拒否されたため、ホスト10.1.1.2は完全なパケットを再構成できず、その結果、パケットBは拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト10.1.1.2がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE (deny) と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

例：ACL での時間範囲を使用

次の例に、*workhours*（営業時間）の時間範囲および会社の休日（2006 年 1 月 1 日）を設定し、設定を確認する例を示します。

```
Device# show time-range

time-range entry: new_year_day_2003 (inactive)
    absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
Device> enable
Device# configure terminal
Device(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Device(config)# access-list 188 permit tcp any any time-range workhours
Device(config)# exit
Device# show access-lists

Extended IP access list 188
 10 deny tcp any any time-range new_year_day_2006 (inactive)
 20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended deny_access
Device(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Device(config-ext-nacl)# exit
Device(config)# ip access-list extended may_access
Device(config-ext-nacl)# permit tcp any any time-range workhours
Device(config-ext-nacl)# end
Device# show ip access-lists

Extended IP access list lpip_default
 10 permit ip any any
Extended IP access list deny_access
 10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
```



```
10 permit tcp any any time-range workhours (inactive)
```

例：IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時～午後 6 時（18 時）の間、IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
Device> enable
Device# configure terminal
Device(config)# time-range no-http
Device(config)# periodic weekdays 8:00 to 18:00
Device(config)# time-range udp-yes
Device(config)# periodic weekend 12:00 to 20:00
Device(config)# ip access-list extended strict
Device(config-ext-nacl)# deny tcp any any eq www time-range no-http
Device(config-ext-nacl)# permit udp any any time-range udp-yes
Device(config-ext-nacl)# exit
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip access-group strict in
Device(config-if)# end
```

例：ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。コメントがどの **permit** ステートメントまたは **deny** ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する **permit** または **deny** ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list access-list number remark remark** グローバルコンフィギュレーションコマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、**user1** のワークステーションにはアクセスを許可し、**user2** のワークステーションにはアクセスを許可しません。

```
Device> enable
Device# configure terminal
Device(config)# access-list 1 remark Permit only user1 workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow user2 through
Device(config)# access-list 1 deny 171.69.3.13
Device(config)# end
```

名前付き IP ACL のエントリには、**remark** アクセスリスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、サブネット subnet1 にはアウトバウンド Telnet の使用が許可されません。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow subnet1 subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
Device(config-ext-nacl)# end
```

例：パケットを拒否する ACL および VLAN マップの作成

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL（TCP パケット）に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1* ACL を作成します。VLAN マップには IP パケットに対する *match* 句が存在するため、デフォルトのアクションでは、どの *match* 句とも一致しない IP パケットがすべてドロップされます。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ip1
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 10
Device(config-access-map)# match ip address ip1
Device(config-access-map)# action drop
Device(config-access-map)# end
```

例：パケットを許可する ACL および VLAN マップの作成

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL ととも一致しないすべての IP パケット（TCP でも UDP でもないパケット）がドロップされます。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ip2
Device(config-ext-nacl)# permit udp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map_1 20
Device(config-access-map)# match ip address ip2
Device(config-access-map)# action forward
Device(config-access-map)# exit
```

例：IP パケットのドロップおよび MAC パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト **igmp-match** および **tcp-match** をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
Device> enable
Device# configure terminal
Device(config)# access-list 101 permit udp any any
Device(config)# ip access-list extended igmp-match
Device(config-ext-nacl)# permit igmp any any
Device(config-ext-nacl)# action forward
Device(config-ext-nacl)# permit tcp any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-ip-default 10
Device(config-access-map)# match ip address 101
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 20
Device(config-access-map)# match ip address igmp-match
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan access-map drop-ip-default 30
Device(config-access-map)# match ip address tcp-match
Device(config-access-map)# action forward
Device(config-access-map)# end
```

例：MAC パケットのドロップおよび IP パケットの転送のデフォルト アクション

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせて使用すると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

例：すべてのパケットをドロップするデフォルトアクション

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended good-hosts
Device(config-ext-macl)# permit host 000.0c00.0111 any
Device(config-ext-macl)# permit host 000.0c00.0211 any
Device(config-ext-nacl)# exit
Device(config)# action forward
Device(config-ext-macl)# mac access-list extended good-protocols
Device(config-ext-macl)# permit any any vines-ip
Device(config-ext-nacl)# exit
Device(config)# vlan access-map drop-mac-default 10
Device(config-access-map)# match mac address good-hosts
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-mac-default 20
Device(config-access-map)# match mac address good-protocols
Device(config-access-map)# action forward
Device(config-access-map)# end
```

例：すべてのパケットをドロップするデフォルトアクション

次の例の VLAN マップでは、デフォルトですべてのパケット（IP および非 IP）がドロップされます。例2および例3のアクセスリスト **tcp-match** および **good-hosts** をこのマップと組み合わせて使用すると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```
Device> enable
Device# configure terminal
Device(config)# vlan access-map drop-all-default 10
Device(config-access-map)# match ip address tcp-match
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan access-map drop-all-default 20
Device(config-access-map)# match mac address good-hosts
Device(config-access-map)# action forward
Device(config-access-map)# end
```

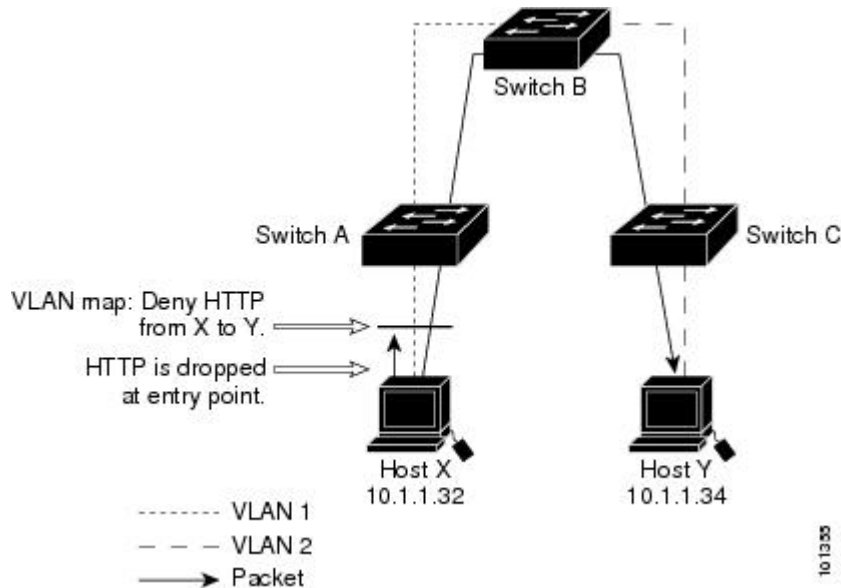
例：ネットワークでの VLAN マップの使用

例：ワイヤリングクローゼットの設定

図 4: ワイヤリングクローゼットの設定

ワイヤリングクローゼット構成では、ルーティングがスイッチ上で有効にされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。

す。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリングクローゼットスイッチ A およびスイッチ C に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングが有効に設定されたレイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリポイントであるスイッチ A でアクセスコントロールできます。



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X (IP アドレス 10.1.1.32) からホスト Y (IP アドレス 10.1.1.34) に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可 (一致) する IP アクセスリスト *http* を定義します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended http
Device(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Device(config-ext-nacl)# end
```

次に、*http* アクセスリストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセスマップ *map2* を作成します。

```
Device> enable
Device# configure terminal
Device(config)# vlan access-map map2 10
Device(config-access-map)# match ip address http
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# ip access-list extended match_all
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# vlan access-map map2 20
Device(config-access-map)# match ip address match_all
Device(config-access-map)# action forward
```

例：別の VLAN にあるサーバへのアクセスの制限

```
Device(config-access-map)# end
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

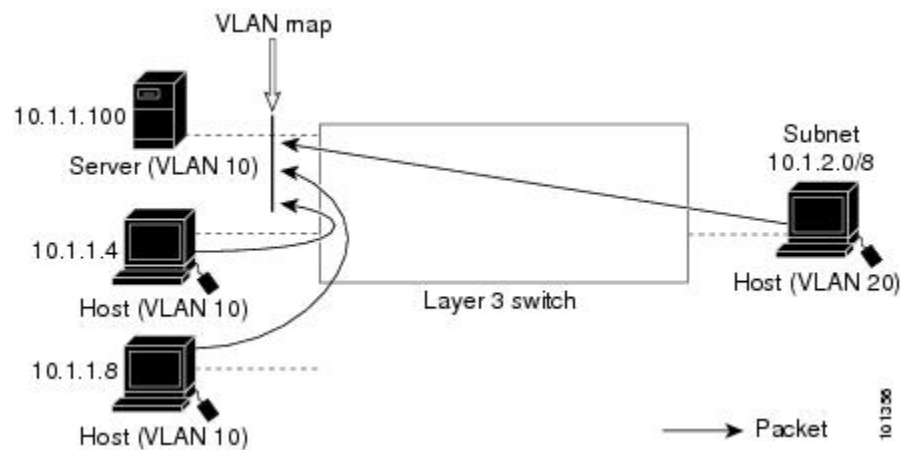
```
Device> enable
Device# configure terminal
Device(config)# vlan filter map2 vlan 1
Device(config)# end
```

例：別の VLAN にあるサーバへのアクセスの制限

図 5: 別の VLAN 上のサーバへのアクセスの制限

別の VLAN にあるサーバへのアクセスを制限できます。たとえば、VLAN 10 内のサーバ 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。



例：別の VLAN にあるサーバへのアクセスの拒否

次に、サブネット 10.1.2.0/8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ *SERVER1-ACL* を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップ *SERVER1* を VLAN 10 に適用します。

正しいパケットと一致する IP ACL を定義します。

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended SERVER1_ACL
Device(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Device(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Device(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Device(config-ext-nacl)# end
```

SERVER1_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
Device> enable
Device# configure terminal
Device(config)# vlan access-map SERVER1_MAP
Device(config-access-map)# match ip address SERVER1_ACL
Device(config-access-map)# action drop
Device(config)# vlan access-map SERVER1_MAP 20
Device(config-access-map)# action forward
Device(config-access-map)# end
```

VLAN 10 に VLAN マップを適用します。

```
Device> enable
Device# configure terminal
Device(config)# vlan filter SERVER1_MAP vlan-list 10
Device(config)# end
```

IPv4 アクセスコントロールリストに関する追加情報

関連資料

| 関連項目 | マニュアル タイトル |
|----------|--------------------------------------|
| IPv6 ACL | 『セキュリティ コンフィギュレーションガイド』の「IPv6 ACL」の章 |

シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| <p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p> | http://www.cisco.com/support |

IPv4 アクセスコントロールリストの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

| リリース | 機能 | 機能情報 |
|-----------------------------|--------------------|---|
| Cisco IOS XE Everest 16.6.1 | IPv4 アクセスコントロールリスト | この章では、ACL を使用して、スイッチのネットワークセキュリティを設定する方法について説明します。パケットフィルタリングは、ネットワークトラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL は、トラフィックをデバイスの通過時にフィルタリングし、パケットが指定されたインターフェイスを通過することを許可または拒否します。 |

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。