



IPv4 ACL

- [ACL によるネットワーク セキュリティに関する情報 \(1 ページ\)](#)
- [IPv4 アクセスコントロールリストの制約事項 \(2 ページ\)](#)
- [ACL を使用したネットワーク セキュリティについて理解する \(3 ページ\)](#)
- [サポートされる ACL \(4 ページ\)](#)
- [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 \(8 ページ\)](#)
- [ACL とスイッチ スタック \(9 ページ\)](#)
- [標準 IPv4 ACL および拡張 IPv4 ACL \(10 ページ\)](#)
- [ハードウェアおよびソフトウェアによる IP ACL の処理 \(14 ページ\)](#)
- [VLAN マップの設定時の注意事項 \(15 ページ\)](#)
- [VLAN マップとルータ ACL \(16 ページ\)](#)
- [ACL の時間範囲 \(17 ページ\)](#)
- [IPv4 ACL のインターフェイスに関する注意事項 \(18 ページ\)](#)
- [ACL によるネットワーク セキュリティに関する情報 \(18 ページ\)](#)
- [ACL の設定方法 \(18 ページ\)](#)
- [IPv4 ACL のモニタリング \(41 ページ\)](#)
- [ACL の設定例 \(42 ページ\)](#)
- [IPv4 ACL の設定例 \(43 ページ\)](#)
- [ACL および VLAN マップの設定例 \(50 ページ\)](#)
- [ネットワークでの VLAN マップの使用方法の設定例 \(52 ページ\)](#)
- [ACL の設定例 \(55 ページ\)](#)
- [IPv4 アクセスコントロールリストの機能履歴 \(55 ページ\)](#)

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト (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。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

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 packets 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tring 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せん。
- ルータ ACL は、CPU 生成トラフィックを含むすべてのタイプのトラフィックに適用されます。
- 存続可能時間 (TTL) 分類は、ACL ではサポートされていません。

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。

ACL を使用したネットワーク セキュリティについて理解する

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 はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスを通過するパケット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、転送されるすべてのパケットに ACL を使用します。

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、ルータまたはレイヤ3スイッチ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、ルータ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したりできます。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

スイッチは、IP ACL とイーサネット (MAC) ACL をサポートします。

- 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。

このスイッチは、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 を適応できます。
- 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 (着信または発信) に適用されます。
- VLAN ACL または VLAN マップはレイヤ2 VLAN にのみ適用され、ブリッジされたトラフィックにのみ影響します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4 のレイヤ3 アドレスに基づいてアクセスコントロールするように設定されています。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセスコントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット (ルーテッドパケットまたはブリッジドパケット) が VLAN マップと照合されます。パ

ケットは、スイッチポートを介して、または、ルーティングされたパケットの場合、ルーテッドポートを介して、VLAN に入ることができます。

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

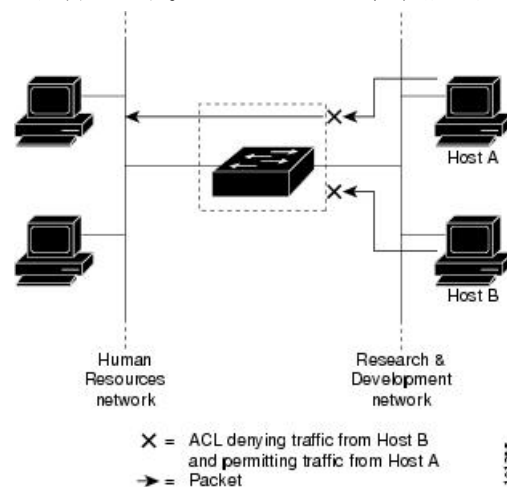
ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は、物理インターフェイスおよび EtherChannel インターフェイス上でサポートされていますが、EtherChannel メンバーインターフェイスではサポートされていません。ポート ACL は、インバウンド方向とアウトバウンド方向のインターフェイスに適用できます。次のアクセスリストがサポートされています。

- 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

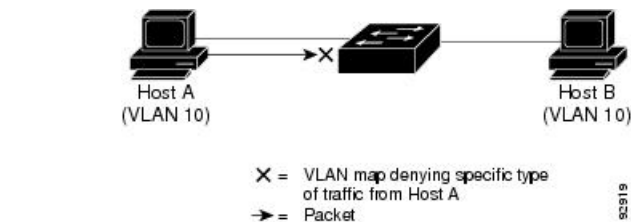
VLAN ACL または VLAN マップは、VLAN 内のネットワークトラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリング および特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向 (入力または出力) で定義されることはありません。

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。

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の例

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。


```
デバイス(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
デバイス(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
デバイス(config)# access-list 102 permit tcp any host 10.1.1.2
デバイス(config)# access-list 102 deny tcp any any
```



(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permitACE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。

ACLとスイッチスタック

スイッチスタックのACLサポートは、スタンドアロンスイッチと同じです。ACLの構成情報は、スタック内のすべてのスイッチに送信されます。アクティブスイッチを含むスタック内のすべてのスイッチでは、情報が処理され、ハードウェアがプログラムされます。

アクティブスイッチおよび ACL の機能

アクティブスイッチにより、次の ACL 機能が実行されます。

- ACL 構成情報が処理され、情報がすべてのスタックメンバに送信されます。
- ACL 情報は、スタックに加入しているすべてのスイッチに配信されます。
- (たとえば、十分なハードウェアリソースがないなど) 何らかの理由で、ソフトウェアによってパケットが送信される必要がある場合、ACL をパケットに適用後にのみ、アクティブスイッチによってパケットが転送されます。
- そのハードウェアは、処理する ACL 情報でプログラムされます。

スタックメンバおよび ACL の機能

スタックメンバにより、次の ACL 機能が実行されます。

- スタックメンバでは、アクティブスイッチから ACL 情報を受信し、ハードウェアがプログラムされます。
- スタンバイスイッチとして設定されたスタックメンバがアクティブスイッチが失敗したイベント内のアクティブスイッチ機能を実行します。

アクティブスイッチの障害および ACL

アクティブとスタンバイの両方のスイッチに ACL 情報があります。アクティブスイッチに障害が発生すると、スタンバイが役割を引き継ぎます。新しいアクティブスイッチにより、すべてのスタックメンバに ACL 情報が配信されます。

標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、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、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、スイッチ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

このスイッチで IPv4 ACL を設定する手順は、他の Cisco スイッチやルータで IPv4 ACL を設定する手順と同じです。

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 または
- 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
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

アクセス リスト番号	タイプ	サポートあり
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。

スイッチは、**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、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が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。

このスイッチは、ダイナミックまたは再帰アクセス 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、このスイッチはこれらの 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、ルータ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。標準 IP ACL の名前は 1 ~ 99 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。

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。

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、Unicast Reverse Path Forwarding (uRPF) で使用される ACL ではサポートされません。ルータ ACL 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、ロギングメッセージ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) スイッチまたはスタックメンバー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、スイッチに着信した該当 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트리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。スイッチ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 リストがスイッチにあって、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 マップに優先します。
- 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て使用します。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て使用し、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のあるためです。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、スイッチ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) を使用してスイッチ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

ip access-group インターフェイス コンフィギュレーション コマンドをレイヤ3 インターフェイス (SVI、レイヤ3 EtherChannel、またはルーテッドポート) に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ3 アクセスグループは、CPU のレイヤ3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

インバウンド ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチ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、スイッチ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あと、スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチ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、スイッチは 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。

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト (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。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

ACL 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。

手順の概要

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。

- 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。

手順の詳細

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。

手順の概要

- enable**
- configure terminal**
- access-list** *access-list-number* {deny | permit} *source source-wildcard*]
- end**
- show running-config**
- copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> 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： デバイス# 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 <i>access-list-number</i> {deny permit} <i>source source-wildcard</i>] 例： デバイス(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。

	コマンドまたはアクション	目的
		<p>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。</p> <p><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。</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。 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。 <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) ログイングは、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： デバイス(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： デバイス# show running-config	入力を確認します。
ステップ 6	copy running-config startup-config 例： デバイス# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **configure terminal**
2. **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*]
3. **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*]
4. **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*]
5. **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*]
6. **access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*]
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： デバイス# 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 2	access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>] 例： デバイス(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。 <i>protocol</i> には、インターネットプロトコルの名前または番号を入力します。 ahp 、 eigrp 、 esp 、 gre 、 icmp 、 igmp 、 igrp 、 ip 、 ipinip 、 nos 、 ospf 、 pcp 、 pim 、 tcp 、 udp 、または IP プロトコル番号を表す 0 ～ 255 の整数を使用できます。一致条件としてインターネットプロトコル (ICMP、TCP、UDP など) を指定するには、キーワード ip を使用します。

	コマンドまたはアクション	目的
		<p>(注) この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。</p> <p><i>source</i> には、パラメータの送信元であるネットワークまたはホストの番号を指定します。</p> <p><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><i>destination</i> には、パラメータの宛先であるネットワークまたはホストの番号を指定します。</p> <p><i>destination-wildcard</i> は、ワイルドカードビットを宛先アドレスに適用します。</p> <p><i>source</i>、<i>source-wildcard</i>、<i>destination</i>、および <i>destination-wildcard</i> 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。

	コマンドまたはアクション	目的
		<p>• 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。</p> <p>(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。</p>
<p>ステップ 3</p>	<p>access-list <i>access-list-number</i> {deny permit} tcp <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [established] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp] [<i>flag</i>]</p> <p>例 :</p> <pre>デバイス(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 (リセット)、syn (同期)、または urg (緊急) です。

	コマンドまたはアクション	目的
ステップ 4	<p>access-list <i>access-list-number</i> {deny permit} udp <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit udp any any eq 100</pre>	<p>(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。</p> <p>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、[<i>operator [port]</i>] 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。</p>
ステップ 5	<p>access-list <i>access-list-number</i> {deny permit} icmp <i>source source-wildcard destination destination-wildcard</i> [<i>icmp-type</i> [[<i>icmp-type icmp-code</i>] [<i>icmp-message</i>]]] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit icmp any any 200</pre>	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • <i>icmp-type</i> : 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。 • <i>icmp-code</i> : 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。 • <i>icmp-message</i> : 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 6	<p>access-list <i>access-list-number</i> {deny permit} igmp <i>source source-wildcard destination destination-wildcard</i> [<i>igmp-type</i>] [precedence precedence] [tos tos] [fragments] [time-range time-range-name] [dscp dscp]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit igmp any any 14</pre>	<p>(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。</p> <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>

	コマンドまたはアクション	目的
ステップ 7	end 例 : デバイス (config) # end	特権 EXEC モードに戻ります。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list standard name**
4. 次のいずれかを使用します。
 - **deny {source [source-wildcard] | host source | any} [log]**
 - **permit {source [source-wildcard] | host source | any} [log]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : デバイス > 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 : デバイス # 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	ip access-list standard name 例 : デバイス (config) # ip access-list standard 20	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。 名前には、1 ~ 99 の番号を使用できます。

	コマンドまたはアクション	目的
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 {source [source-wildcard] host source any} [log] • permit {source [source-wildcard] host source any} [log] <p>例 :</p> <pre>デバイス(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>デバイス(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</pre>	<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のかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。</p> <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 source 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>デバイス(config-std-nacl)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>デバイス# show running-config</pre>	入力を確認します。
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended name**

4. `{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]`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> 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： デバイス# 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	ip access-list extended name 例： デバイス(config)# ip access-list extended 150	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。 名前には、100 ~ 199 の番号を使用できます。
ステップ 4	{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] 例： デバイス(config-ext-nacl)# permit 0 any any	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。 <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 0.0.0.0</i>。 • 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 0.0.0.0</i>。 • any : <i>source</i> および <i>source wildcard</i> の値または <i>destination</i> および <i>destination wildcard</i> の値である <i>0.0.0.0 255.255.255.255</i>
ステップ 5	end 例： デバイス(config-ext-nacl)# end	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	show running-config 例： デバイス# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： デバイス# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **time-range** *time-range-name*
4. 次のいずれかを使用します。
 - **absolute** [*start time date*] [*end time date*]
 - **periodic** *day-of-the-week hh:mm to [day-of-the-week] hh:mm*
 - **periodic** { **weekdays** | **weekend** | **daily** } *hh:mm to hh:mm*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : デバイス (config) # 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 : デバイス # 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	time-range time-range-name 例 : デバイス (config) # time-range workhours	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 : デバイス (config-time-range) # absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006 または デバイス (config-time-range) # periodic weekdays 8:00 to 12:00	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。 設定例を参照してください。
ステップ 5	end 例 : デバイス (config) # end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 :	入力を確認します。

	コマンドまたはアクション	目的
	デバイス# <code>show running-config</code>	
ステップ 7	copy running-config startup-config 例 : デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **line [console | vty] line-number**
4. **access-class access-list-number {in | out}**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : デバイス (config)# <code>enable</code>	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 :	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。

	コマンドまたはアクション	目的
	デバイス# <code>configure terminal</code>	
ステップ 3	line [console vty] line-number 例： デバイス(config)# <code>line console 0</code>	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。 line-number 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。
ステップ 4	access-class access-list-number {in out} 例： デバイス(config-line)# <code>access-class 10 in</code>	(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。
ステップ 5	end 例： デバイス(config-line)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 7	copy running-config startup-config 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **ip access-group {access-list-number | name} {in | out}**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： デバイス# 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 2	interface interface-id 例： デバイス(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 3	ip access-group {access-list-number name} {in out} 例： デバイス(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。
ステップ 4	end 例： デバイス(config-if)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： デバイス# show running-config	アクセス リストの設定を表示します。
ステップ 6	copy running-config startup-config 例： デバイス# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **mac access-list extended name**
4. **{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 | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp | 0-65535] [cos cos]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> 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： デバイス# 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	mac access-list extended name 例： デバイス(config)# mac access-list extended macl	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	{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 lavc-sca	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

	コマンドまたはアクション	目的
	<p> mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp 0-65535] [cos <i>cos</i>]</p> <p>例 :</p> <pre>デバイス(config-ext-macl)# deny any any decnet-iv</pre> <p>または</p> <pre>デバイス(config-ext-macl)# permit any any</pre>	<p>宛先 MAC アドレスに、permit または deny を指定します。</p> <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"> • type mask : 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。 • lsap lsap mask : 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。 • 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 : 非 IP プロトコル。 • cos <i>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>デバイス(config-ext-macl)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p>show running-config</p> <p>例 :</p> <pre>デバイス# show running-config</pre>	<p>入力を確認します。</p>
ステップ 7	<p>copy running-config startup-config</p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	<p>(任意) コンフィギュレーションファイルに設定を保存します。</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。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **mac access-group {*name*} {*in*}**
5. **end**
6. **show mac access-group [interface *interface-id*]**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> 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： デバイス# 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 <i>interface-id</i> 例： デバイス(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 {<i>name</i>} {<i>in</i>} 例： デバイス(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 は着信方向サポートされます。
ステップ 5	end 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス (config-if) # end	
ステップ 6	show mac access-group [interface interface-id] 例 : デバイス # 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。
ステップ 7	show running-config 例 : デバイス # show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : デバイス # copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

スイッチは、パケットを受信すると、着信 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、スイッチ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、スイッチ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、スイッチは 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。

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。

手順の概要

1. **vlan access-map name [number]**
2. **match {ip | mac} address {name | number} [name | number]**

3. 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。

- **action { forward }**

```
デバイス(config-access-map)# action forward
```

- **action { drop }**

```
デバイス(config-access-map)# action drop
```

4. `vlan filter mapname vlan-list list`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p>vlan access-map name [number]</p> <p>例 :</p> <pre>デバイス(config)# vlan access-map map_1 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 <code>permit</code> または <code>deny</code> 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 <code>permit</code> は、一致するという意味です。ACL 内の <code>deny</code> 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>
ステップ 2	<p>match {ip mac} address {name number} [name number]</p> <p>例 :</p> <pre>デバイス(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>

	コマンドまたはアクション	目的
		(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 マップになく、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。
ステップ 3	<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>デバイス(config-access-map) # action forward</pre> <ul style="list-style-type: none"> • action { drop } <pre>デバイス(config-access-map) # action drop</pre>	マップエントリに対するアクションを設定します。
ステップ 4	<p>vlan filter mapname vlan-list list</p> <p>例 :</p> <pre>デバイス(config) # vlan filter map 1 vlan-list 20-22</pre>	<p>VLAN マップを 1 つまたは複数の VLAN に適用します。</p> <p>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。</p>

VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップエントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **vlan access-map name [number]**
3. **match {ip | mac} address {name | number} [name | number]**
4. **action {drop | forward}**
5. **end**

6. `show running-config`
7. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例 : デバイス# <code>configure terminal</code>	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 2	vlan access-map name [number] 例 : デバイス (config)# <code>vlan access-map map_1 20</code>	<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 <code>permit</code> または <code>deny</code> 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 <code>permit</code> は、一致するという意味です。ACL 内の <code>deny</code> 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>
ステップ 3	match {ip mac} address {name number} [name number] 例 : デバイス (config-access-map)# <code>match ip address ip2</code>	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。
ステップ 4	action {drop forward} 例 : デバイス (config-access-map)# <code>action forward</code>	(任意) マップエントリに対するアクションを設定します。デフォルトは転送 (forward) です。
ステップ 5	end 例 :	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
	デバイス (config-access-map) # end	
ステップ 6	show running-config 例： デバイス # show running-config	アクセス リストの設定を表示します。
ステップ 7	copy running-config startup-config 例： デバイス # copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan filter mapname vlan-list list**
4. **end**

手順の詳細

	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

スイッチに設定されている 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 をモニターできます。

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または特定のアクセスリスト（番号付きまたは名前付き）を表示します。
show ip 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。ネットワークになっているインターフェイスに、 ip access-group コマンドを使用してアクセスグループが適用された場合は、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>]	スイッチ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 アドレス、どのアクセスグループがインターフェイスに適用されているか）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。

ACL の設定例

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。

```
デバイス# 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。

```
デバイス(config)# access-list 188 deny tcp any any time-range new_year_day_2006
デバイス(config)# access-list 188 permit tcp any any time-range workhours
デバイス(config)# end
デバイス# 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。

```
デバイス(config)# ip access-list extended deny_access
デバイス(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
デバイス(config-ext-nacl)# exit
デバイス(config)# ip access-list extended may_access
デバイス(config-ext-nacl)# permit tcp any any time-range workhours
デバイス(config-ext-nacl)# end
デバイス# 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：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 にエントリーに関するコメント（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、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88
デバイス(config)# access-list 1 remark Do not allow Smith through
デバイス(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリーには、**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、Jones のサブネットには発信 Telnet の使用が許可されません。

```
デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
デバイス(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

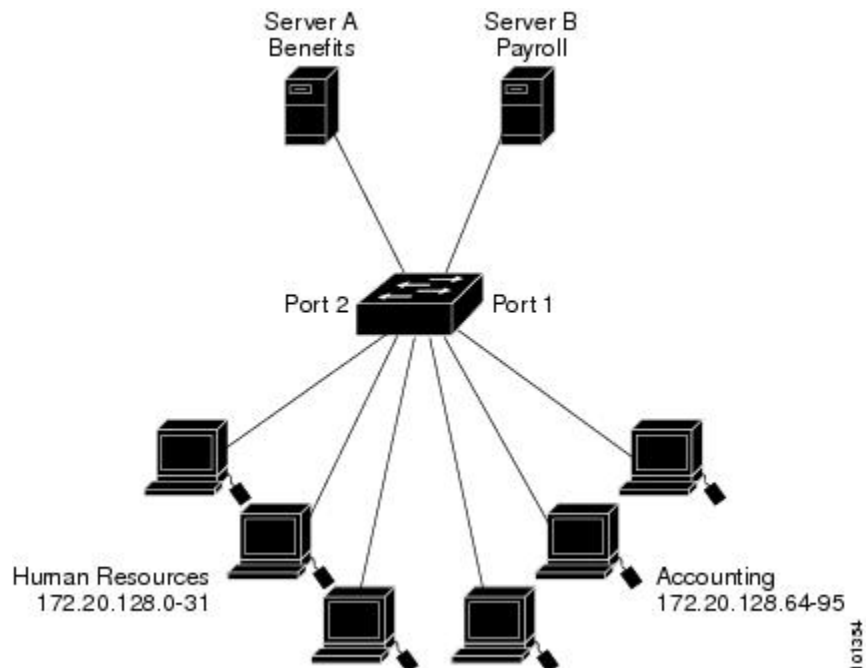
IPv4 ACL の設定例

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ー 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ー 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。サーバー A にはすべてのユーザーがアクセスできますが、サーバー B にアク

セスできるユーザー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 からサーバー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、サーバーからポート 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ー 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。

```

デバイス(config)# access-list 6 permit 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# show access-lists
Standard IP access list 6
 10 permit 172.20.128.64, wildcard bits 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 6 out

```

次に、拡張 ACL を使用してサーバー 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（この場合はサーバー 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。

```
デバイス(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# show access-lists
Extended IP access list 106
  10 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 106 in
```

例：番号付き ACL

次の例のネットワーク 36.0.0.0 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。ネットワークアドレス 36.0.0.0 の 3 番めおよび 4 番目のオクテットは、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 36.0.0.0 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。

```
デバイス(config)# access-list 2 permit 36.48.0.3
デバイス(config)# access-list 2 deny 36.48.0.0 0.0.255.255
デバイス(config)# access-list 2 permit 36.0.0.0 0.255.255.255
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group 2 in
```

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 番目の行は、ホスト 128.88.1.2 のシンプルメール転送プロトコル (SMTP) ポートへの着信 TCP 接続を許可します。3 番目の行は、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。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# access-list 102 permit icmp any any
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group 102 in
```

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、着信サービスとを個別に制御できます。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 102 in
```

次の例では、ネットワークはアドレスが128.88.0.0のクラスBネットワークで、メールホストのアドレスは128.88.1.2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。スタックメンバー1のギガビットイーサネットインターフェイス1は、ルータをインターネットに接続するインターフェイスです。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 102 in
```

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 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
デバイス(config)# ip access-list standard Internet_filter
デバイス(config-ext-nacl)# permit 1.2.3.4
デバイス(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 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 171.69.0.0 ~ 179.69.255.255 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。

```
デバイス(config)# ip access-list extended marketing_group
デバイス(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
デバイス(config-ext-nacl)# deny tcp any any
デバイス(config-ext-nacl)# permit icmp any any
デバイス(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
```

```
デバイス(config-ext-nacl)# deny ip any any log
デバイス(config-ext-nacl)# exit
```

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。

```
デバイス(config)# interface gigabitethernet3/0/2
デバイス(config-if)# no switchport
デバイス(config-if)# ip address 2.0.5.1 255.255.255.0
デバイス(config-if)# ip access-group Internet_filter out
デバイス(config-if)# ip access-group marketing_group in
```

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。

```
デバイス(config)# ip access-list extended border-list
デバイス(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

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。

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

例：コメント付き IP ACL エントリの設定

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88
```

例 : ACL ロギング

```

デバイス(config)# access-list 1 remark Do not allow Smith workstation through
デバイス(config)# access-list 1 deny 171.69.3.13

```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```

デバイス(config)# access-list 100 remark Do not allow Winter to browse the web
デバイス(config)# access-list 100 deny host 171.69.3.85 any eq www
デバイス(config)# access-list 100 remark Do not allow Smith to browse the web
デバイス(config)# access-list 100 deny host 171.69.3.13 any eq www

```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```

デバイス(config)# ip access-list standard prevention
デバイス(config-std-nacl)# remark Do not allow Jones subnet through
デバイス(config-std-nacl)# deny 171.69.0.0 0.0.255.255

```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```

デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
デバイス(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet

```

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。

```

デバイス(config)# ip access-list standard stan1
デバイス(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
デバイス(config-std-nacl)# permit any log
デバイス(config-std-nacl)# exit
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group stan1 in
デバイス(config-if)# end
デバイス# 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。

```
デバイス(config)# ip access-list extended ext1
デバイス(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
デバイス(config-ext-nacl)# deny udp any any log
デバイス(config-std-nacl)# exit
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# ip access-group ext1 in
```

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
```

ACL および VLAN マップの設定例

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。

```
デバイス(config)# ip access-list extended ip1
デバイス(config-ext-nacl)# permit tcp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map_1 10
デバイス(config-access-map)# match ip address ip1
デバイス(config-access-map)# action drop
```

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。

```
デバイス(config)# ip access-list extended ip2
デバイス(config-ext-nacl)# permit udp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map_1 20
デバイス(config-access-map)# match ip address ip2
デバイス(config-access-map)# action forward
```

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。

```

デバイス(config)# access-list 101 permit udp any any
デバイス(config)# ip access-list extended igmp-match
デバイス(config-ext-nacl)# permit igmp any any

デバイス(config)# action forward
デバイス(config-ext-nacl)# permit tcp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map drop-ip-default 10
デバイス(config-access-map)# match ip address 101
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-ip-default 20
デバイス(config-access-map)# match ip address igmp-match
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-ip-default 30
デバイス(config-access-map)# match ip address tcp-match
デバイス(config-access-map)# action forward

```

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

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。

```

デバイス(config)# vlan access-map drop-all-default 10
デバイス(config-access-map)# match ip address tcp-match
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-all-default 20
デバイス(config-access-map)# match mac address good-hosts
デバイス(config-access-map)# action forward

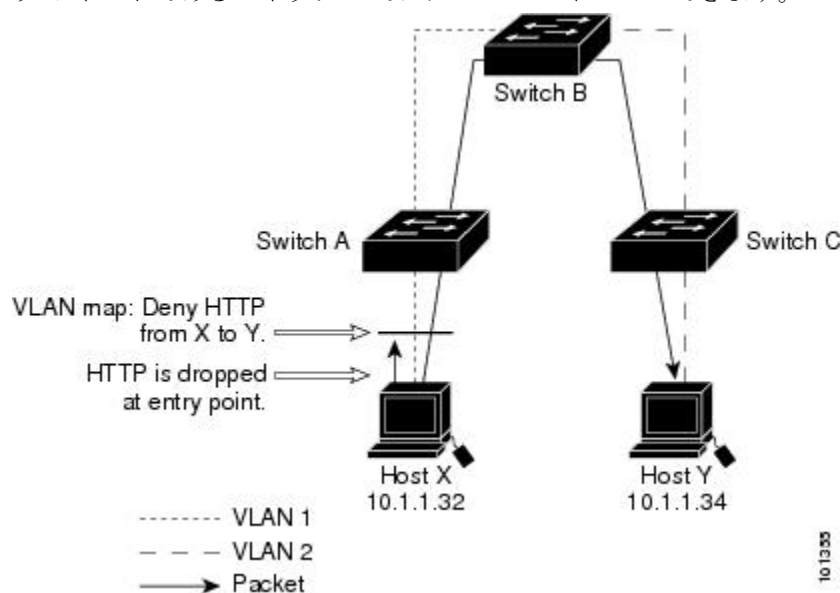
```

ネットワークでの VLAN マップの使用方法の設定例

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。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。

```
デバイス(config)# ip access-list extended http
デバイス(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
デバイス(config-ext-nacl)# exit
```

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。

```
デバイス(config)# vlan access-map map2 10
デバイス(config-access-map)# match ip address http
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(config)# ip access-list extended match_all
デバイス(config-ext-nacl)# permit ip any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map2 20
デバイス(config-access-map)# match ip address match_all
デバイス(config-access-map)# action forward
```

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

```
デバイス(config)# vlan filter map2 vlan 1
```

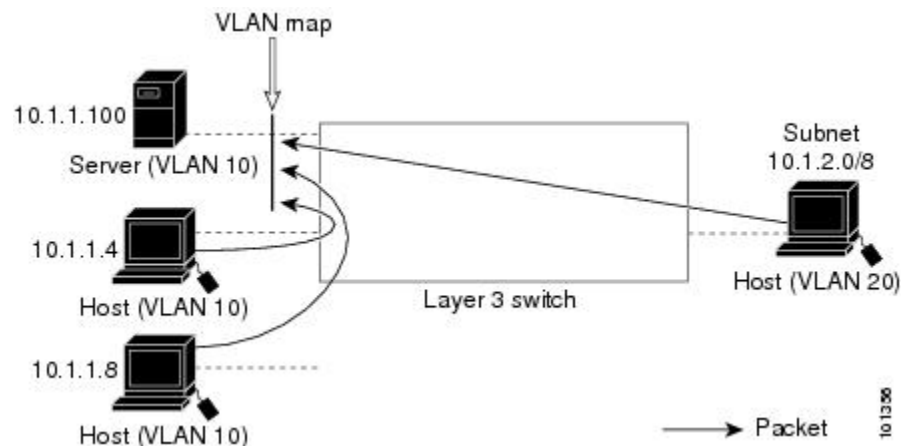
例：別の VLAN にあるサーバーへのアクセスの制限

図 5: 別の VLAN 上のサーバーへのアクセスの制限

別の VLAN にあるサーバーへのアクセスを制限できます。たとえば、VLAN 10 内のサーバー 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 にあるサーバーへのアクセスの拒否



例：別の VLAN にあるサーバー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 内のサーバー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。

```

デバイス(config)# ip access-list extended SERVER1_ACL
デバイス(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
デバイス(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
デバイス(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
デバイス(config-ext-nacl)# exit

```

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。

```

デバイス(config)# vlan access-map SERVER1_MAP
デバイス(config-access-map)# match ip address SERVER1_ACL
デバイス(config-access-map)# action drop
デバイス(config)# vlan access-map SERVER1_MAP 20
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit

```

VLAN 10 に VLAN マップを適用します。

```

デバイス(config)# vlan filter SERVER1_MAP vlan-list 10

```

ACL の設定例

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 16.5.1a	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。

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。