



ACL によるネットワーク セキュリティ の設定

この章では、Access Control List (ACL; アクセス制御リスト) を使用して、Catalyst 3550 スイッチにネットワーク セキュリティを設定する方法について説明します。ACL は、コマンドやテーブルではアクセス リストと表します。

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンス、『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Addressing and Service」の章にある「Configuring IP Services」および次のソフトウェア コンフィギュレーション コマンドリファレンスを参照してください。

- 『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』Release 12.2
- 『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2
- 『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』Release 12.2

この章で説明する内容は、次のとおりです。

- [ACL の概要 \(p.29-2\)](#)
- [IP ACL の設定 \(p.29-7\)](#)
- [名前指定の MAC 拡張 ACL の設定 \(p.29-30\)](#)
- [VLAN マップの設定 \(p.29-33\)](#)
- [ルータ ACL と VLAN マップの併用 \(p.29-40\)](#)
- [ACL 情報の表示 \(p.29-44\)](#)



(注)

スイッチで使用できるセキュリティ Access Control Entry (ACE; アクセス制御エントリ) 数が最大になるようにシステム リソースを割り当てるには、**sdm prefer access** 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、Switch Database Management (SDM) 機能をアクセス テンプレートに設定します。SDM テンプレートの詳細については、「[ユーザが選択した機能に対するシステム リソースの最適化](#)」(p.6-28)を参照してください。

設定に合わせたリソース使用方法の判別については、「[ACL リソースの利用率および設定問題の表示](#)」(p.29-46)を参照してください。

ACL の概要

パケット フィルタリングを使用すると、ネットワーク トラフィックを制限したり、特定のユーザやデバイスによるネットワークの使用を制限できます。ACL はルータ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でパケットを許可、または、拒否します。ACL は、パケットに適用される許可および拒否条件を順番に並べたものです。インターフェイスにパケットが着信すると、スイッチはパケットのフィールドを該当する ACL と比較し、ACL で指定されている条件に基づいて、パケットに対して転送が許可されているかどうかを検証します。パケットは、アクセス リスト内の条件に対して 1 つずつテストされます。最初に見つかった一致条件によって、パケットが許可されるか、または拒否されるかが決まります。スイッチは、最初の一致が見つかった時点でテスト環境を終了するので、アクセス リスト内の条件の順序が重要となります。一致する条件がない場合、パケットは拒否されます。制約がない場合、スイッチはパケットを転送し、制約がある場合はパケットを廃棄します。

従来、スイッチはレイヤ 2 でのみ稼働し、VLAN (仮想 LAN) 内でトラフィックをスイッチングしていましたが、一方、ルータは VLAN 間でトラフィックをルーティングしていましたが、Catalyst 3550 スイッチは、レイヤ 3 スイッチングを使用して VLAN 間のパケット ルーティングを高速化します。スイッチでブリッジングされたパケットは、外部ルータに送信されずに内部ルーティングされ、再度ブリッジングされて宛先に送信されます。スイッチはこのプロセス中に、VLAN 内でブリッジングされるパケットを含め、スイッチングされるすべてのパケットのアクセスを制御します。

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、ルータまたはスイッチにアクセス リストを設定します。ACL を設定しないと、スイッチを通過するすべてのパケットが、ネットワーク内のすべての場所に転送されることがあります。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て、Telnet トラフィックの転送を禁止することが可能です。ACL が着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。ただし、レイヤ 2 インターフェイスでは、ACL を適用できるのは着信方向だけです。

ACL には ACE が順番に記述されています。各 ACE は、許可 (*permit*) または拒否 (*deny*)、および ACE と一致するために要求されるパケットの必須条件を指定します。許可または拒否の意味は、ACL の使用状況に応じて変わります。

このスイッチでは次の 2 つの ACL タイプがサポートされます。

- IP ACL は、TCP、UDP、Internet Group Management Protocol (IGMP)、Internet Control Message Protocol (ICMP) などの IP トラフィックをフィルタリングします。
- イーサネット ACL または MAC (メディア アクセス制御) ACL は、非 IP トラフィックをフィルタリングします。

サポートされる ACL

このスイッチは、トラフィックをフィルタリングするため、次に示す 3 種類の ACL をサポートします。

- 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 インターフェイスに適用されます。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。
- 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のアクセスを制御します。このスイッチは、発信方向のポート ACL をサポートしません。1 つのレイヤ 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。
- VLAN ACL または VLAN マップは、すべてのパケット (ブリッジド パケットおよびルーテッド パケット) のアクセスを制御します。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、IP のレイヤ 3 ア

ドレスに基づいてアクセス制御するように設定されています。サポートされていないプロトコルはイーサネット ACE を使用し、MAC アドレスを通じてアクセス制御されます。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経由して、ルーティングされたパケットの場合は、ルーテッドポートを経由して VLAN に入ります。

同じスイッチでルータ ACL と VLAN マップを両方使用できます。ただし、入力ルータ ACL または VLAN マップが設定されているスイッチでポート ACL を使用することはできません。

- スイッチに、IP アクセスリストまたは MAC アクセスリストが適用されているレイヤ 2 インターフェイスがある場合、IP アクセスリストと VLAN マップを作成することは可能ですが、そのスイッチの入力レイヤ 3 インターフェイスに IP アクセスリストを適用したり、そのスイッチのいずれかの VLAN に VLAN マップを適用することはできません。適用しようとすると、エラーメッセージが生成されます。ポート ACL が設定されたスイッチの出力レイヤ 3 インターフェイスに IP アクセスリストを適用することは可能です。
- スイッチに、適用済みの入力レイヤ 3 ACL または VLAN マップがある場合、このスイッチのレイヤ 2 インターフェイスに IP アクセスリストまたは MAC アクセスリストを適用することはできません。適用しようとすると、エラーメッセージが生成されます。スイッチの出力レイヤ 3 インターフェイスに ACL が適用されている場合は、そのスイッチにポート ACL を適用できます。

IEEE 802.1Q トンネリングがインターフェイス上に設定されている場合、このトンネルポートで受信された IEEE 802.1Q カプセル化 IP パケットを MAC ACL でフィルタリングすることは可能ですが、IP ACL ではフィルタリングできません。スイッチは IEEE 802.1Q ヘッダー内のプロトコルを認識できないためです。この制約は、ルータ ACL、ポート ACL、VLAN マップに適用されます。IEEE 802.1Q トンネリングの詳細については、第 14 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

このスイッチは、Quality of Service (QoS; サービス品質) 分類 ACL もサポートしています。詳細については、「QoS ACL に基づく分類」(p.30-7) を参照してください。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスである Switch Virtual Interface (SVI; スイッチ仮想インターフェイス)、物理レイヤ 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。各方向に 1 つずつ IP アクセスリストを適用できます。

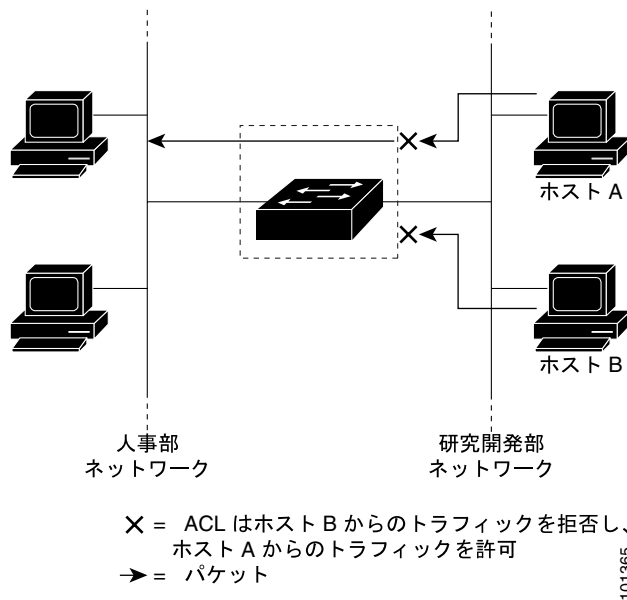
1 つの ACL をある特定インターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回テストされます。

- 標準 IP アクセスリストは、送信元アドレスを使用して一致処理を行います。
- 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。

スイッチは、特定のインターフェイスおよび方向に対して設定された機能に関連付けられている ACL をテストします。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 がテストされます。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 がテストされます。

ACL は、ACL 内のエントリとの一致結果に基づいて、転送を許可または拒否します。たとえば、アクセスリストを使用すると、ネットワークの特定の場所へのアクセスを特定のホストに許可し、別のホストにはアクセスを禁止できます。図 29-1 では、ルータへの入力に適用されている ACL により、ホスト A は人事部ネットワークへのアクセスを許可されますが、ホスト B は拒否されます。

図 29-1 ACL によるネットワーク トラフィックの制御



101365

ポート ACL

スイッチのレイヤ 2 インターフェイスにも ACL を適用できます。ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用できません。ポート ACL をインターフェイスに適用できるのは、着信方向に対してのみです。レイヤ 2 インターフェイスでは、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標準 IP アクセス リスト
- 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 タイプ情報を使用する拡張 IP アクセス リスト
- 送信元 MAC アドレス、宛先 MAC アドレス、およびオプションのプロトコル タイプ情報を使用する MAC 拡張アクセス リスト

ルータ ACL 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 をテストし、パケットが ACL 内のエン트리と一致するかどうかによって、パケットの転送を許可または拒否します。ただし、レイヤ 2 インターフェイスで、ACL を適用できるのは、着信方向に対してのみです。図 29-1 の例では、すべてのワークステーションが同じ VLAN 内にある場合、レイヤ 2 の入力に適用されている ACL によって、ホスト A は人事部ネットワークへのアクセスを許可されますが、ホスト B は同じネットワークへのアクセスを拒否されます。

ポート ACL をトランク ポートに適用すると、そのトランク ポートにあるすべての VLAN で ACL によるトラフィックのフィルタリングが実行されます。音声 VLAN があるポートにポート ACL を適用すると、データ VLAN と音声 VLAN の両方でその ACL によるトラフィックのフィルタリングが実行されます。

ポート ACL を使用すると、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し、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 インターフェイスに IP アクセス リストと MAC アクセス リストを両方適用すると、そのレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックをフィルタリングできます。



(注)

1 つのレイヤ 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 リストと MAC アクセス リストが 1 つずつ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、新しい ACL が前に設定した ACL に置き換わります。

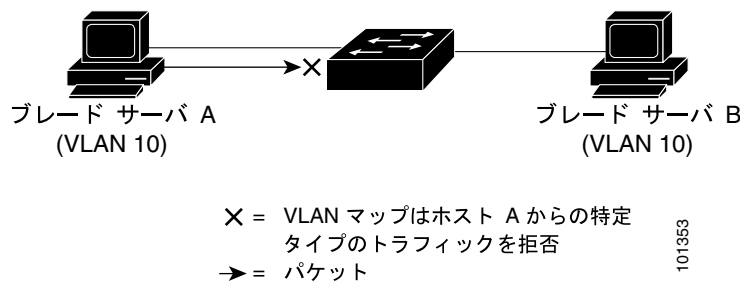
VLAN マップ

VLAN マップを使用すると、すべてのトラフィックのアクセスを制御できます。VLAN の内部や外部へルーティングされる、または VLAN 内でブリッジされるすべてのパケットに対して、スイッチの VLAN マップを適用できます。VLAN マップはパケットを安全にフィルタリングするために必ず使用されます。ルータ ACL と異なり、VLAN マップで方向（着信または発信）は定義されません。

VLAN マップを設定すると、IP トラフィックのレイヤ 3 アドレスを比較できます。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 によってアクセス制御されます（IP トラフィックには、MAC VLAN マップによるアクセス制御が行われません）。VLAN マップはスイッチを通過するパケットにのみ適用できます。ハブのホスト間、またはこのスイッチに接続された別のスイッチのホスト間を通過するトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、パケットの転送はマップに指定されたアクションに基づいて許可または拒否されます。図 29-2 に、VLAN マップを適用して、特定タイプのトラフィックを 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。

図 29-2 VLAN マップによるトラフィックの制御



分割されたトラフィックおよび分割されていないトラフィックの処理

ネットワークを通過する IP パケットは分割できます。IP パケットを分割すると、パケットの先頭を含むフラグメントにのみ、TCP、UDP ポート番号、ICMP タイプおよびコードなどのレイヤ 4 情報が格納されます。その他のすべてのフラグメントには、この情報が格納されません。

一部の ACE ではレイヤ 4 情報が確認されないため、このような ACE はすべてのパケットフラグメントに適用されます。レイヤ 4 情報をテストする ACE を、分割された IP パケットのほとんどのフラグメントに通常の方法で適用することはできません。レイヤ 4 情報が格納されていないフラグメントに対してレイヤ 4 情報がテストされる場合、一致規則は次のように変更されます。

- フラグメントのレイヤ 3 情報（TCP や UDP のようなプロトコル タイプなど）を確認する許可 ACE の場合は、格納されていないレイヤ 4 情報に関係なく、フラグメントが一致するとみなされます。

- レイヤ 4 情報を確認する拒否 ACE の場合は、フラグメントが一致しないとみなされます。ただし、フラグメントにレイヤ 4 情報が格納されている場合は、一致するとみなされます。

次のコマンドで設定し、3 つの分割パケットに適用されるアクセス リスト 102 の例を以下に示します。

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



(注)

この例の最初の 2 つの ACE では、宛先アドレスの後ろに *eq* キーワードが指定されています。これは、TCP 宛先ポートのうち、Simple Mail Transfer Protocol (SMTP) および Telnet それぞれに対応する well-known 番号についてテストすることを示します。

- 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。このパケットが分割パケットの場合、最初のフラグメントにはすべてのレイヤ 4 情報が格納されているため、完全なパケットと同様にみなされ、最初の ACE (許可) に一致します。SMTP ポート情報が入っていない場合、残りのフラグメントも最初の ACE に一致します。最初の ACE はフラグメントに適用されたとき、レイヤ 3 情報のみを確認するためです。この例での情報は、パケットが TCP で、宛先が 10.1.1.1 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。このパケットが分割パケットの場合、最初のフラグメントにはレイヤ 3 情報およびレイヤ 4 情報がすべて格納されているため、2 番目の ACE (拒否) に一致します。このパケットの残りのフラグメントにはレイヤ 4 情報が格納されていないため、2 番目の ACE には一致しません。残りのフラグメントは 3 番目の ACE (許可) に一致します。

最初のフラグメントが拒否されているため、ホスト 10.1.1.2 は完全なパケットを再構築できません。したがって、実際にはパケット B は拒否されます。ただし、ホスト 10.1.1.2 がパケットを再構築しようとするとき、許可されたフラグメントによってネットワーク帯域幅とこのホストのリソースが消費されます。

- 分割パケット 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。このパケットが分割パケットの場合、最初のフラグメントは 4 番目の ACE (拒否) に一致します。その他のすべてのフラグメントも 4 番目の ACE に一致します。これは、すべてのフラグメントについてレイヤ 4 情報が確認されず、レイヤ 3 情報によってすべてのフラグメントがホスト 10.1.1.3 に送信中であることが認識されたため、およびこの宛先ホストがこれ以前の許可 ACE の確認対象から外れていたためです。

IP ACL の設定

レイヤ 2 またはレイヤ 3 スイッチ、あるいは VLAN インターフェイス上に IP ACL を設定する方法は、他のシスコ製ルータ上に ACL を設定する方法と同じです。その手順を簡単に示します。ルータ ACL の設定の詳細については、『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。コマンドの詳細については、次のマニュアルを参照してください。

- 『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』Release 12.2
- 『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2
- 『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』Release 12.2

Catalyst 3550 スイッチでサポートされない IOS 機能については、「サポートされない機能」(p.29-9) を参照してください。



注意

デフォルトでは、パケットがアクセス グループによって拒否されると、ルータは ICMP 到達不能メッセージを送信します。アクセス グループによって拒否されたパケットは、ハードウェア内で廃棄されずにスイッチの CPU にブリッジングされ、そこで ICMP 到達不能メッセージが生成されます。アクセス グループによって拒否されたパケットをハードウェアで廃棄するには、`no ip unreachable` 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、ICMP 到達不能をディセーブルにする必要があります。`ip unreachable` コマンドは、デフォルトでイネーブルに設定されています。

具体的な内容は次のとおりです。

- ルータ ACL のハードウェアおよびソフトウェア処理 (p.29-7)
- 入力ルータ ACL 設定時の注意事項 (p.29-8)
- サポートされない機能 (p.29-9)
- 標準および拡張 IP ACL の作成 (p.29-9)
- インターフェイスまたは端末回線への IP ACL の適用 (p.29-22)
- IP ACL の設定例 (p.29-24)

ルータ ACL のハードウェアおよびソフトウェア処理

ACL は主にハードウェアで処理されますが、一部のトラフィックは CPU に転送してソフトウェア処理する必要があります。ソフトウェアで転送されるトラフィックの転送速度は、ハードウェアで転送されるトラフィックに比べて大幅に低下します。両方のトラフィック フローをロギングして転送する場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。ハードウェアとソフトウェアではパケット処理機能が異なるため、ロギング中であるすべてのフロー（許可フローと拒否フロー）の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

次の場合、パケットは CPU に送信されます。

- `log` キーワードを使用する。
- ICMP 到達不能 (ICMP unreachable) をイネーブルにする。
- ACL 設定を格納するためのハードウェア容量が限界に達する。

ACL によって多数のパケットが CPU に転送されると、スイッチのパフォーマンスが低下することがあります。



(注)

ACL 設定が指定されたインターバル内で安定した状態になると、システムは設定をハードウェアにロードします。ハードウェアのアップデート中は、影響を受けるすべてのインターフェイスで転送がブロックされます。この動作を変更する場合は、`mls aclmerge delay` および `access-list hardware program nonblocking` 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。これらのコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

`show ip access-lists` イネーブル EXEC コマンドを入力したときに表示される一致の個数に、ハードウェアでアクセス制御されるパケットは含まれません。ハードウェアで ACL 処理されるスイッチド パケットおよびルーテッド パケットの基本的な統計情報を取得する場合は、`show access-lists hardware counters` イネーブル EXEC コマンドを使用します。

IP ACL は、次のように処理されます。

- 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、アクセス制御のセキュリティを強化します。
- IP 到達不能がディセーブルの場合、`log` を指定しないと、セキュリティ ACL の拒否 (`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廃棄されます。許可 (`permit`) 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。ポート ACL のロギングはサポートされません。
- 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、ロギングのみが行われます。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。



(注)

レイヤ 2 インターフェイス (ポート ACL) のロギングはサポートされません。

入力ルータ ACL 設定時の注意事項

入力ルータ ACL では、ACL が適用されると Ternary CAM (TCAM) エントリ数を大幅に増加できます。TCAM エントリ数が、割り当てられたリソース数を超える場合、ACL フィルタリングはハードウェアの代わりにソフトウェアで実行されてパフォーマンスの低下を招くことがあります。

次に、過度な TCAM 利用を避ける方法を示します。

- より多くのアクセス リストを許可するよう SDM テンプレートを変更するには、`sdm prefer access` 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。
- 入力ルータ ACL の代わりに出力ルータ ACL を使用します。
- 明示的な許可または拒否を設定することで、入力ルータ ACL の TCAM の利用率を最小限にします。

入力ルータ ACL が適用されると、ACL は、ルーティング プロトコル パケットと比較し、パケットをプロトコル キューへ送信する暗黙的な ACL と自動的に統合されます。この統合により、TCAM エントリが追加されます。エントリ数を最小限にするには、ACL の最初で ACE を許可または拒否するよう設定することによって、RIP、EIGRP、OSPF、BGP、PIM などのルーティング プロトコルを明示的に許可または拒否するようルータ ACL を設定できます。

次に、TCAM の利用率を最小限にするよう入力ルータ ACL を設定する例を示します。

```
Switch(config)# access-list 100 [permit|deny] tcp any any eq bgp
Switch(config)# access-list 100 [permit|deny] eigrp any any
Switch(config)# access-list 100 [permit|deny] pim any any
Switch(config)# access-list 100 [permit|deny] ospf any any
Switch(config)# access-list 100 [permit|deny] udp any any eq rip
Switch(config)# access-list 100 ..... ACL 100's ACE(s)
Switch(config)# exit
```

サポートされない機能

Catalyst 3550 スイッチは、次の Cisco IOS ルータ ACL 関連機能をサポートしません。

- 非 IP プロトコルの ACL (表 29-1 [p.29-10] を参照)
- ブリッジグループ ACL
- IP アカウンティング
- 着信速度および発信速度の制限 (QoS ACL による制限を除く)
- ヘッダー長が 5 未満の IP パケットは、アクセス制御されません (ICMP パラメータ エラーが発生します)
- 再帰 ACL
- ダイナミック ACL (スイッチのクラスタリング機能で 사용되는一部の特殊ダイナミック ACL は除く)
- レイヤ 2 ポート ACL に関して、ロギングと送信 ACL はサポートされません。

標準および拡張 IP ACL の作成

ここでは、ルータ IP ACL 作成手順の概要を示します。ACL は許可および拒否条件を順に並べたものです。パケットは、アクセス リスト内の条件に対して 1 つずつテストされます。最初に見つかった一致条件によって、パケットが許可されるか、または拒否されるかが決まります。最初の一致が見つかりとテストは終了するので、条件の順序が重要となります。一致する条件がない場合、パケットは拒否されます。

IP ACL を使用する手順は、次のとおりです。

-
- ステップ 1** アクセス リスト番号または名前、およびアクセス条件を指定して ACL を作成します。
- ステップ 2** 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。
-

ソフトウェアは次に示す形式の ACL、または IP のアクセス リストをサポートします。

- 標準 IP アクセス リストは、送信元アドレスを使用して一致処理を行います。
- 拡張 IP アクセス リストは、送信元アドレスおよび宛先アドレスを使用して一致処理を行います。より細部にわたる制御を行う場合は、オプションのプロトコルタイプ情報を使用します。

ここでは、アクセス リストの詳細、およびアクセス リストを使用する手順について説明します。

- [アクセス リスト番号 \(p.29-10\)](#)
- [番号指定標準 ACL の作成 \(p.29-11\)](#)
- [番号指定拡張 ACL の作成 \(p.29-13\)](#)
- [名前指定の標準および拡張 IP ACL の作成 \(p.29-17\)](#)
- [ACL での時間範囲の使用法 \(p.29-19\)](#)
- [ACL へのコメントの挿入 \(p.29-21\)](#)

アクセス リスト番号

ACL を表す番号は、作成しているアクセス リストのタイプを示します。表 29-1 に、アクセス リスト番号および対応するアクセス リスト タイプ、スイッチでのアクセス リストに対するサポートの有無を示します。スイッチでは、IP 標準および IP 拡張アクセス リストがサポートされています(番号は 1 ~ 199、1300 ~ 2699)。

表 29-1 アクセス リスト番号

アクセス リスト番号	タイプ	サポートの有無
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 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




(注)

番号指定の標準 ACL および拡張 ACL 以外に、サポートされている番号を使用して名前指定の標準 IP ACL および拡張 IP ACL を作成することもできます。つまり、標準 IP ACL の名前には 1 ~ 99 を、拡張 IP ACL の名前には 100 ~ 199 を使用できます。番号指定の ACL ではなく名前指定の ACL を使用することで、名前指定リストから個別にエントリを削除することが可能となります。

番号指定標準 ACL の作成

番号指定の標準 ACL を作成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>access-list access-list-number {deny permit} source [source-wildcard] [log]</code>	<p>送信元アドレスおよびワイルドカードを使用し、標準 IP アクセス リストを定義します。</p> <p><i>access-list-number</i> は 1 ~ 99 または 1300 ~ 1999 の 10 進数です。</p> <p>条件が一致する場合にアクセスを拒否するか、許可するかを指定するには、deny または permit を入力します。</p> <p><i>source</i> はパケットの送信元であるネットワークまたはホストのアドレスです。次のいずれかで指定します。</p> <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビットの数値 <i>source</i> と <i>source-wildcard</i> の値 0.0.0.0 255.255.255.255 の短縮形であるキーワード any。 <i>source-wildcard</i> は入力必須ではありません。 <i>source</i> と <i>source-wildcard</i> の値 <i>source</i> 0.0.0.0 の短縮形であるキーワード host。 <p>(任意) <i>source-wildcard</i> を指定すると、送信元にワイルドカード ビットが適用されます。</p> <p>(任意) log 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作成され、コンソールに送信されます。</p> <p> (注) レイヤ 2 インターフェイスに適用された ACL で、log キーワードは無視されます。</p>
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 5	<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。

ACL 全体を削除するには、**no access-list access-list-number** 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。番号指定のアクセス リストからは、ACE を個別に削除できません。



(注) ACL を作成するときは、ACL の末尾に暗黙的な拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致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、対応する IP ホスト アドレスの ACL を指定するときにマスクを省略すると、0.0.0.0 がマスクとして使用されます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否してそれ以外のアドレスへのアクセスを許可してその結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    10 deny    171.69.198.102
    20 permit any
```

host 一致条件が指定されたエントリ、および 0.0.0.0 の無視 (*don't care*) マスクが指定されたエントリが、リストの先頭 (ゼロ以外の無視マスクが指定された、すべてのエントリの上) にくるように、標準アクセス リストの順序が書き換えられます。したがって、**show** コマンドの出力およびコンフィギュレーション ファイルで、ACE は必ずしも入力した順番に表示されません。

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、スイッチ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。コンソールにロギングされるメッセージのレベルは、Syslog メッセージを制御するロギング コンソール コマンドで制御されます。



(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ません。

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)

出力 ACL はマルチキャスト パケットをロギングできません。レイヤ 2 インターフェイスに適用された ACL のロギングはサポートされません。

作成した ACL を、回線またはインターフェイスに適用する必要があります (「[インターフェイスまたは端末回線への IP ACL の適用](#)」 [p.29-22] を参照)。

番号指定拡張 ACL の作成

標準 ACL の場合、一致基準には送信元アドレスのみが使用されますが、拡張 ACL の場合は、一致処理に送信元アドレスおよび宛先アドレスを使用したり、オプションのプロトコル タイプ情報を使用したりして、より細部にわたる制御を行うことができます。番号指定の拡張 ACL を作成したあとに ACE を新たに作成するときは、リストの末尾に新しい ACE が配置されることに注意してください。リストを再び並べ替えたり、番号が指定された ACL の特定の位置で ACE を追加または削除することはできません。

一部のプロトコルには、専用のパラメータおよびキーワードを使用することもできます。

拡張 ACL では、次の IP プロトコルがサポートされています (プロトコル キーワードは括弧内の太字で示しています)。

Authentication Header Protocol (**ahp**)、Enhanced Interior Gateway Routing Protocol (**eigrp**)、Encapsulation Security Payload (**esp**)、Generic Routing Encapsulation (**gre**)、ICMP (**icmp**)、IGMP (**igmp**)、Interior Gateway Routing Protocol (**igrp**)、任意の Interior Protocol (**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**)、Payload Compression Protocol (**pcp**)、Protocol Independent Multicast (**pim**)、TCP (**tcp**)、または UDP (**udp**)



(注) ICMP エコー応答はフィルタリングできません。他のすべての ICMP コードまたはタイプはフィルタリング可能です。

各プロトコルに関連するキーワードの詳細については、次のソフトウェア コンフィギュレーション ガイドおよびコマンド リファレンスを参照してください。

- 『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』Release 12.2
- 『Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols』Release 12.2
- 『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』Release 12.2





(注) スイッチで、ダイナミック アクセス リストや再帰アクセス リストはサポートされません。また、最小コストの Type of Service (ToS; サービス タイプ) ビットに基づくフィルタリングもサポートされません。

サポートされているパラメータは、TCP、UDP、ICMP、IGMP、またはその他の IP の、いずれかのカテゴリにグループ分けできます。

拡張 ACL を作成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	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。

コマンド	目的
<p>ステップ 2a <code>access-list access-list-number</code> <code>{deny permit} protocol source</code> <code>source-wildcard destination</code> <code>destination-wildcard [precedence</code> <code>precedence] [tos tos] [fragments]</code> <code>[log] [log-input] [time-range</code> <code>time-range-name] [dscp dscp]</code></p> <p> (注) dscp 値を入力した場合、tos または precedence を入力することはできません。dscp を入力しない場合は、tos と precedence を両方とも入力できます。</p>	<p>拡張 IP アクセス リストおよびアクセス条件を定義します。</p> <p><code>access-list-number</code> は 100 ~ 199 または 2000 ~ 2699 の 10 進数です。</p> <p>条件が一致する場合にパケットを拒否するか許可するかを指定するため、<code>deny</code> または <code>permit</code> を入力します。</p> <p><code>protocol</code> を指定する場合は、IP プロトコルの名前または番号を入力します。<code>ahp</code>、<code>eigrp</code>、<code>esp</code>、<code>gre</code>、<code>icmp</code>、<code>igmp</code>、<code>igrp</code>、<code>ip</code>、<code>ipinip</code>、<code>nos</code>、<code>ospf</code>、<code>pcp</code>、<code>pim</code>、<code>tcp</code>、<code>udp</code>、IP プロトコル番号を表す 0 ~ 255 の整数を使用できます。すべてのインターネット プロトコル (ICMP、TCP、UDP を含む) と一致させる場合は、キーワード <code>ip</code> を使用します。</p> <p> (注) このステップには、ほとんどの IP プロトコルに使用可能なオプションが含まれます。TCP、UDP、ICMP、IGMP の具体的なパラメータについては、ステップ 2b ~ 2e を参照してください。</p> <p><code>source</code> はパケットの送信元であるネットワークまたはホストの番号です。</p> <p><code>source-wildcard</code> を指定すると、送信元にワイルドカード ビットが適用されます。</p> <p><code>destination</code> はパケットの宛先となるネットワークまたはホストの番号です。</p> <p><code>destination-wildcard</code> を指定すると、宛先にワイルドカード ビットが適用されます。</p> <p><code>source</code>、<code>source-wildcard</code>、<code>destination</code>、<code>destination-wildcard</code> は、次の 3 つの方法で指定できます。</p> <ul style="list-style-type: none"> ドット付き 10 進表記による 32 ビットの数値 0.0.0.0 255.255.255.255 を表すキーワード <code>any</code> (任意のホスト) 単一のホスト 0.0.0.0 を表すキーワード <code>host</code> <p>その他のキーワードは任意で、意味は次のとおりです。</p> <ul style="list-style-type: none"> <code>precedence</code> 0 ~ 7 の番号または名前指定された優先順位を使用し、パケットを比較します。使用できる名前および番号は、<code>routine</code> (0)、<code>priority</code> (1)、<code>immediate</code> (2)、<code>flash</code> (3)、<code>flash-override</code> (4)、<code>critical</code> (5)、<code>internet</code> (6)、<code>network</code> (7) です。 <code>fragments</code> 先頭以外のフラグメントを確認します。 <code>tos</code> 0 ~ 15 の番号または名前指定された ToS レベルを使用して比較します。使用できる名前および番号は、<code>normal</code> (0)、<code>max-reliability</code> (2)、<code>max-throughput</code> (4)、<code>min-delay</code> (8) です。 <code>log</code> 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を作成し、コンソールに送信します。<code>log-input</code> 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。レイヤ 2 インターフェイスに適用された ACL (ポート ACL) のロギングはサポートされません。 <code>time-range</code> このキーワードの説明については、「ACL での時間範囲の使用法」(p.29-19) を参照してください。 <code>dscp</code> 0 ~ 63 の番号で指定された DSCP 値を使用してパケットを比較します。疑問符 (?) を使用すると、使用可能な値のリストが表示されます。

	コマンド	目的
または	<pre>access-list access-list-number {deny permit} protocol any any [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</pre>	<p>アクセス リスト コンフィギュレーション モードで、送信元と送信元ワイルドカードの値 0.0.0.0 255.255.255.255 の短縮形を使用するか、または宛先と宛先ワイルドカードの値 0.0.0.0 255.255.255.255 の短縮形を使用し、拡張 IP アクセス リストを定義します。</p> <p>送信元および宛先のアドレスとワイルドカードの代わりに、any キーワードを使用できます。</p>
または	<pre>access-list access-list-number {deny permit} protocol host source host destination [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</pre>	<p>送信元と送信元ワイルドカードの値 source 0.0.0.0 の短縮形を使用するか、または宛先と宛先ワイルドカードの値 destination 0.0.0.0 の短縮形を使用し、拡張 IP アクセス リストを定義します。</p> <p>送信元と宛先のワイルドカードまたはマスクの代わりに、host キーワードを使用できます。</p>
ステップ 2b	<pre>access-list access-list-number {deny permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] [flag]</pre>	<p>(任意) 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>TCP の場合は tcp を入力します。</p> <p>次に示す例外を除き、ステップ 2a で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) operator および port を入力すると、送信元ポート (source source-wildcard のあとに入力した場合) または宛先ポート (destination destination-wildcard のあとに入力した場合) が比較されます。使用可能な演算子は eq (一致)、gt (より大きい)、lt (未満)、neq (不一致)、range (包含範囲) などです。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>port にポート番号を 10 進数 (0 ~ 65535) として入力するか、または TCP ポート名を入力します。TCP ポート名を確認するには、? を使用するが、『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときは、TCP ポートの番号または名前のみを使用します。</p> <p>その他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 確立された接続と比較します。このキーワードは、ack または rst フラグを指定した場合の一致検索機能と同じです。 • flag 指定された TCP ヘッダー ビットを基準にして比較します。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)、urg (緊急) です。
ステップ 2c	<pre>access-list access-list-number {deny permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</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 の場合は、udp を入力します。</p> <p>UDP パラメータは TCP に関して説明されてい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とします。UDP の場合、flag および established パラメータは無効です。</p>

	コマンド	目的
ステップ 2d	<code>access-list access-list-number</code> {deny permit} icmp source source-wildcard destination destination-wildcard [icmp-type / [[icmp-type icmp-code] [icmp-message]] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]	(任意) 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 の場合は、icmp を入力します。 ICMP パラメータはステップ 2a の IP プロトコルで説明されているパラメータと同じですが、ICMP メッセージ タイプとコード 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は次の意味をもちます。 <ul style="list-style-type: none">• icmp-type ICMP メッセージ タイプを使用してフィルタリングします。0 ~ 255 の値を使用できます。• icmp-code ICMP メッセージ タイプを基準にしてフィルタリングされた ICMP パケットを、ICMP メッセージ コードを基準にしてフィルタリングします。0 ~ 255 の値を使用できます。• icmp-message ICMP メッセージ タイプ名または ICMP メッセージのタイプおよびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージ タイプ名および ICMP メッセージのタイプおよびコード名のリストを表示するには、? を使用するか、『Cisco IOS IP Configuration Guide』Release 12.2 の「Configuring IP Services」を参照してください。
ステップ 2e	<code>access-list access-list-number</code> {deny permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]	(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。 IGMP の場合は、igmp を入力します。 IGMP パラメータはステップ 2a の IP プロトコルで説明されているパラメータと同じですが、次に示すパラメータが追加されています。 igmp-type 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。
ステップ 3	<code>show access-lists [number name]</code>	アクセス リストの設定を確認します。
ステップ 4	<code>copy running-config</code> <code>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。

アクセス リスト全体を削除するには、`no access-list access-list-number` 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。番号指定のアクセス リストからは、ACE を個別に削除できません。

次に、ネットワーク 171.69.198.0 内の任意のホストからネットワーク 172.20.52.0 内の任意のホストへの Telnet アクセスを拒否し、それ以外のアドレスへのアクセスを許可する拡張アクセス リストを作成、表示する例を示します (eq キーワードを宛先アドレスのあとに指定すると、Telnet に対応する TCP 宛先ポート番号がテストされます)。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255
eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
 10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
 20 permit tcp any any
```

ACL が作成されたあとに追加された ACE (端末から入力された ACE など) は、リストの末尾に配置されます。番号が指定されたアクセス リストの特定の位置で ACE を追加または削除することはできません。



(注)

ACL を作成するときは、アクセス リストの末尾に暗黙的な拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致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。

作成した ACL を、回線またはインターフェイスに適用する必要があります (「[インターフェイスまたは端末回線への IP ACL の適用](#)」 [p.29-22] を参照)。

ACL での ACE の再シーケンス

Cisco IOS Release 12.2(18)SE 以降では、アクセス リスト内のエントリのシーケンス番号は新しい ACL を作成するときに自動的に生成されます。ip access-list resequence 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 ACL のシーケンス番号を編集して ACE が適用される順番を変更できます。たとえば、新しい ACE を ACL に追加した場合、リストの最後に追加されます。シーケンス番号を変更することで、ACE を ACL の別の位置に移動できます。

ip access-list resequence コマンドの詳細については、次の URL を参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s14/fsaclseq.htm>

名前指定の標準および拡張 IP ACL の作成

IP ACL は、番号でなく英数字 (名前) で指定することもできます。名前指定の ACL を使用すると、番号指定のアクセス リストを使用する場合よりも多くの IP アクセス リストをスイッチに設定できます。アクセス リストを番号でなく名前で指定する場合は、モードおよびコマンド構文が若干異なります。ただし、IP アクセス リストを使用するすべてのコマンドで、名前指定のアクセス リストを使用できるとは限りません。



(注)



標準または拡張 ACL に指定する名前には、サポートされているアクセス リスト番号範囲内の番号を指定することもできます。つまり、標準 IP ACL の名前には 1 ~ 99 を、拡張 IP ACL の名前には 100 ~ 199 を使用できます。番号指定 ACL ではなく名前指定 ACL を使用することで、名前指定リストから個別にエントリを削除することが可能となります。

名前指定の ACL を設定する前に、次に示す注意事項および制限事項を考慮してください。

- 番号指定の ACL を指定できるすべてのコマンドで、名前指定の ACL を指定できるとは限りません。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、VLAN マップには名前を使用できます。
- 標準 ACL および拡張 ACL に、同じ名前を設定することはできません。
- 番号指定の ACL も使用できます (「[標準および拡張 IP ACL の作成](#)」 [p.29-9] を参照)。
- VLAN マップには、標準 ACL および拡張 ACL (名前指定または番号指定) を適用できます。


■ IP ACL の設定


名前を使用して標準 ACL を作成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>ip access-list standard name</code>	名前を使用して標準 IP 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。  (注) 名前には 1 ~ 99 の番号を使用できます。
ステップ 3	<code>deny {source [source-wildcard] host source any} [log]</code> または <code>permit {source [source-wildcard] host source any} [log]</code>	アクセス リスト コンフィギュレーション モードで、1 つまたは複数の条件を拒否または許可に指定し、パケットの転送または廃棄を決定します。 <ul style="list-style-type: none"> • <code>host source</code> 送信元と送信元ワイルドカードの値 <code>source 0.0.0.0</code> • <code>any</code> 送信元と送信元ワイルドカードの値 <code>0.0.0.0 255.255.255.255</code>  (注) レイヤ 2 インターフェイスに適用された ACL (ポート ACL) に関して、 <code>log</code> キーワードはサポートされません。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<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。

名前指定の標準 ACL を削除するには、`no ip access-list standard name` 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。

名前を使用して拡張 ACL を作成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>ip access-list extended name</code>	名前を使用して拡張 IP 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。  (注) 名前には 100 ~ 199 の番号を使用できます。

	コマンド	目的
ステップ 3	<code>{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]</code>	<p>アクセスリスト コンフィギュレーション モードで、許可または拒否の条件を指定します。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> <p>プロトコルおよびその他キーワードの定義については、「番号指定拡張 ACL の作成」(p.29-13) を参照してください。</p> <ul style="list-style-type: none"> • <code>host source</code> 送信元と送信元ワイルドカードの値 <code>source 0.0.0.0</code> • <code>host destination</code> 宛先と宛先ワイルドカードの値 <code>destination 0.0.0.0</code> • <code>any</code> 送信元と送信元ワイルドカードの値、または宛先と宛先ワイルドカードの値である <code>0.0.0.0 255.255.255.255</code> <p> (注) レイヤ 2 インターフェイスに適用された ACL (ポート ACL) に関して、log キーワードはサポートされません。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<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。

名前指定の拡張 ACL を削除するには、`no ip access-list extended name` 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。

標準または拡張 ACL を作成するときは、ACL の末尾に暗黙的な拒否ステートメントがデフォルトで存在し、それ以前のステートメントで一致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、対応する IP ホスト アドレスのアクセス リストを指定するときにマスクを省略すると、0.0.0.0 がマスクとして使用されます。

ACL を作成したあとに追加された ACE は、リストの末尾に配置されます。特定の ACL では選択的に ACL エントリを追加することはできません。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、名前指定の ACL からエントリを削除できます。次に、名前指定のアクセス リスト `border-list` から ACE を個別に削除する例を示します。

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

番号指定の ACL ではなく、名前指定の ACL を使用することで、名前指定の ACL から行を個別に削除することが可能となります。

作成した ACL を、回線またはインターフェイスに適用する必要があります(「[インターフェイスまたは端末回線への IP ACL の適用](#)」[p.29-22] を参照)。

ACL での時間範囲の使用法

曜日および時刻に基づいて拡張 ACL を選択的に適用するには、`time-range` グローバル コンフィギュレーション コマンドを使用します。最初に時間範囲の名前を定義し、時間範囲の時刻、日付、または曜日を設定します。次に、ACL を適用するときに時間範囲名を入力し、アクセス リストに制限を適用します。時間範囲を使用することで、ACL の許可ステートメントまたは拒否ステートメントが有効な時期(指定期間内、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、前述の「[標準および拡張 IP ACL の作成](#)」(p.29-9) および「[名前指定の標準および拡張 IP ACL の作成](#)」(p.29-17) に記載されている、名前指定および番号指定の拡張 ACL に関するタスク表を参照してください。

時間範囲を使用する利点のうち、2つを次に示します。

- 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 アクセスをより正確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。



(注) 時間範囲には、スイッチのシステム クロックが使用されるため、信頼できるクロック ソースが必要です。スイッチ クロックを同期するには、Network Time Protocol (NTP) を使用してください。詳細については、「システム日時の管理」(p.6-2) を参照してください。

ACL の time-range パラメータを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>time-range time-range-name</code>	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。名前の先頭には文字を指定し、途中にスペースまたは引用符を含めないようにします。
ステップ 3	<code>absolute [start time date] [end time date]</code> または <code>periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm</code> または <code>periodic {weekdays weekend daily} hh:mm to hh:mm</code>	時間範囲を適用する関数が機能する時間を指定します。 <ul style="list-style-type: none"> • 時間範囲内では、absolute ステートメントを 1 回に限り使用できます。複数の absolute ステートメントを設定した場合は、最後に設定されたステートメントのみが実行されます。 • 複数の periodic ステートメントを入力できます。たとえば、平日と週末で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 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show time-range</code>	設定した時間範囲を確認します。
ステップ 6	<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。

設定された時間範囲の制限を削除するには、`no time-range time-range-name` 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。

異なる時刻に機能するように設定する複数の項目がある場合は、このステップを繰り返します。

次に、営業時間 (*workhours*) および会社の休業日として 2005 年 1 月 1 日を表す時間範囲を設定し、その設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2005
Switch(config-time-range)# absolute start 00:00 1 Jan 2005 end 23:59 1 Jan 2005
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2005 (inactive)
    absolute start 00:00 01 January 2005 end 23:59 01 January 2005
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

適用される時間範囲に関しては、適用先の拡張 ACL 内に、時間範囲名を指定して記述する必要があります。次に、定義された休日中に任意の送信元から任意の宛先に送信される TCP トラフィックを拒否し、営業時間中にすべての TCP トラフィックを許可する拡張アクセス リスト 188 を作成、確認する例を示します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2005
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
    10 deny tcp any any time-range new_year_day_2005 (inactive)
    20 permit tcp any any time-range workhours (inactive)
```

次に、名前指定の 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。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2005
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# 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_2005 (inactive)
Extended IP access list may_access
    40 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入

remark キーワードを使用すると、エントリに関するコメント (備考) を任意の IP 標準および拡張 ACL に追加できます。コメントを追加すると、ACL の把握および走査がより簡単になります。各コメント行には、最大 100 文字まで入力できます。

コメントは許可ステートメントまたは拒否ステートメントの前後に指定できます。コメントに対応する許可ステートメントまたは拒否ステートメントが明確になるように、コメントの記述位置を統一する必要があります。混乱を避けるため、たとえば、許可ステートメントまたは拒否ステートメントの前に記述されているコメントと、後ろに記述されているコメントが混在しないようにします。

番号指定の IP 標準 ACL または拡張 ACL にコメントを追加する場合は、**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、上記のコマンドの **no** 形式を使用します。

次の例では、Jones が所有するワークステーションのアクセスは許可されますが、Smith が所有するワークステーションのアクセスは禁止されます。

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

名前指定の IP ACL にエントリする場合は、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、上記のコマンドの no 形式を使用します。

次の例では、Jones サブネットでの発信 Telnet の使用が禁止されます。

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

インターフェイスまたは端末回線への IP ACL の適用

作成した IP ACL は、1 つまたは複数のインターフェイスまたは端末回線に適用できます。レイヤ 3 インターフェイスには、発信と着信のいずれかの ACL を適用できますが、レイヤ 2 インターフェイスに適用できるのは着信 ACL だけです。ここでは、端末回線とネットワーク インターフェイスの両方にアクセス リストを適用する方法について説明します。次の注意事項を考慮してください。


- 回線へのアクセスを制御する場合は、番号を使用する必要があります。回線に適用できるのは、番号指定の ACL だけです。
- インターフェイスへのアクセスを制御する場合は、名前または番号を使用できます。
- 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、すべての仮想端末回線に同一の制限を設定します。
- 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 で想定されているパケットのみがフィルタリングされます。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。
- 入力ルータ ACL と VLAN マップが設定されているスイッチで、ポート ACL を使用することはできません。
 - 入力レイヤ 3 ACL または VLAN マップが適用されているスイッチのレイヤ 2 インターフェイスに ACL を適用しようとすると、*conflict* エラー メッセージが生成されます。スイッチに出力レイヤ 3 ACL が適用されている場合は、そのスイッチのレイヤ 2 インターフェイスに ACL を適用できません。
 - レイヤ 2 ACL が適用されているスイッチで入力レイヤ 3 インターフェイスに ACL を適用しようとすると、*conflict* エラー メッセージが生成されます。スイッチにレイヤ 2 ACL が適用されている場合は、そのスイッチの出力レイヤ 3 インターフェイスに ACL を適用できません。
- レイヤ 2 インターフェイスには、入力に対する IP アクセス リストを 1 つ適用できます。レイヤ 3 インターフェイスには、入力と出力に 1 つずつ IP アクセス リストを適用できます。すでに IP ACL が設定されているインターフェイスに IP ACL を適用すると（同じ方向で）、新しい ACL が前に設定した ACL に置き換わります。
- ポート ACL を適用できるのは、物理レイヤ 2 インターフェイスだけです。EtherChannel インターフェイスには、ポート ACL を適用できません。

ACL 内のアドレスと仮想端末回線との間の着信接続および発信接続を制限するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>line [console vty] line-number</code>	<p>設定する特定の回線を指定し、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。</p> <ul style="list-style-type: none"> <code>console</code> 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。 <code>vty</code> 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><code>line-number</code> は、連続した一連の番号の最初の回線番号で、回線タイプを指定するときに設定する必要があります。指定できる範囲は 0 ~ 16 です。</p>
ステップ 3	<code>access-class access-list-number {in out}</code>	特定のアクセス リストの条件を使用し、仮想端末回線 (デバイス側) との間の着信接続または発信接続を制限します。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<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。

端末回線に関するアクセス制限を削除するには、`no access-class access-list-number {in | out}` ライン コンフィギュレーション コマンドを使用します。

レイヤ 2 またはレイヤ 3 インターフェイスへのアクセスを制御するために IP アドレス リストを適用するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>interface interface-id</code>	<p>設定する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。</p> <p>このインターフェイスは、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) です。</p>
ステップ 3	<code>ip access-group {access-list-number name} {in out}</code>	<p>IP アクセス リストを使用し、指定したインターフェイスへのアクセスを制御します。標準または拡張の IP アクセス番号または名前を入力できます。</p> <p> (注) <code>out</code> キーワードは、レイヤ 2 インターフェイスに対して無効です。ポート ACL は、着信方向に関してのみサポートされます。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<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。

指定されたアクセス グループを削除するには、`no ip access-group {access-list-number | name} {in | out}` インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス GigabitEthernet 0/3 にアクセス リスト 2 を適用し、インターフェイスに入るパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet0/3
Router(config-if)# ip access-group 2 in
```



(注) `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。

着信 ACL の場合、スイッチは受信したパケットを ACL と照合します。ACL によってパケットが許可された場合は、パケットの処理が続行されます。拒否された場合、パケットは廃棄されます。

発信 ACL の場合 (レイヤ 3 インターフェイスのみ)、スイッチは制御対象インターフェイスに着信し、ルーティングされたパケットを ACL と照合します。パケットが許可された場合、パケットは送信されます。拒否された場合、パケットは廃棄されます。

ICMP 到達不能メッセージを送信するように設定された入力インターフェイスで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、これらの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て処理を行い、すべてのパケットが許可されてしまいます。ネットワーク セキュリティのため、未定義の ACL を使用する場合は注意してください。

IP ACL の設定例

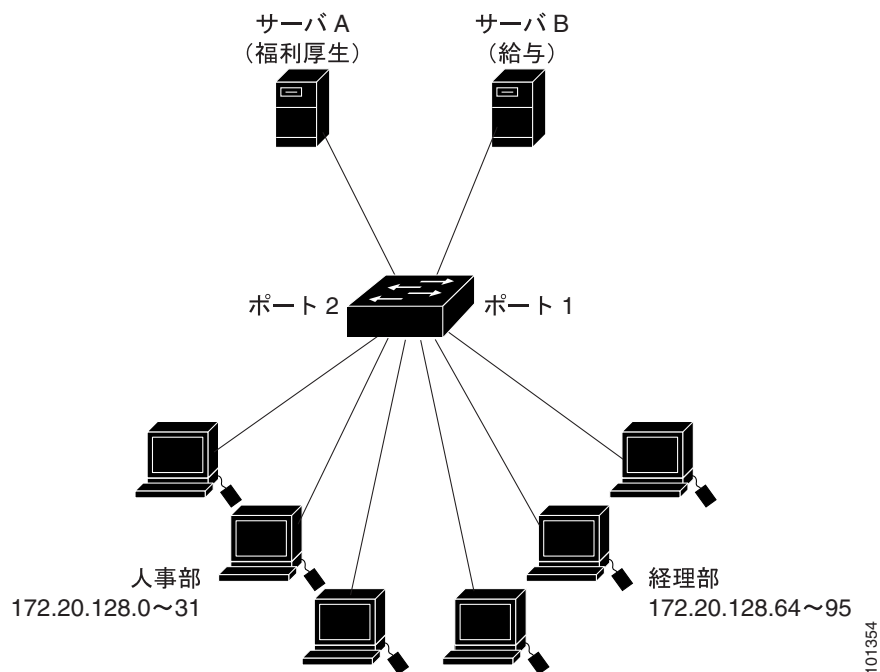
ここでは、IP ACL の設定例を示します。ACL の編集の詳細については、『Cisco IOS Security Configuration Guide』Release 12.2 および『Cisco IOS IP Configuration Guide』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。

図 29-3 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福利厚生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 IP 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 IP 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。

図 29-3 ルータ ACL によるトラフィックの制御



次の例では、標準 ACL を使用してインターフェイスからサーバ 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のみを許可します。この ACL は、指定された送信元アドレスのルーテッドポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
    permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 6 out
```

次の例では、拡張 ACL を使用してサーバ B 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、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のみを許可します。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のみを許可します。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。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
    permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 106 in
```

番号指定 ACL

次の例のネットワーク 36.0.0.0 は、2 番め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 36.0.0.0 アドレスの 3 番めおよび 4 番めのオクテットは、特定のホストを指定します。アクセス リスト 2 が使用されているため、サブネット 48 のアドレスが 1 つ許可され、同じサブネットの他のアドレスはすべて拒否されます。このアクセス リストの最終行は、他のすべてのネットワーク 36.0.0.0 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、インターフェイス GigabitEthernet 0/1 に入るパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

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 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。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。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

拡張 ACL を使用する別の例として、インターネットに接続されたネットワーク上の任意のホストに、インターネットの任意のホストへの TCP 接続を設定する場合を考えます。ただし、IP ホストには、専用メール ホストのメール (SMTP) ポートへの接続を除き、ネットワーク上のホストへの TCP 接続を設定しないものとします。

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。発信パケットのポート番号は予約されています。ルータの背後に置かれた安全なシステムでは、常にポート 25 でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。ACL は発信インターフェイスの入力 ACL および着信インターフェイスの出力 ACL として設定される必要があります。

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、一致とみなされます。インターフェイス GigabitEthernet 0/1 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。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

名前指定 ACL

次のように設定すると、*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 が作成されます。*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。

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

marketing_group ACL は、宛先アドレスと宛先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。また、任意の 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 トラフィックは拒否され、結果を示すログが表示されます。

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

次に示す ACL は、レイヤ 3 ポートとして設定されたポート GigabitEthernet 0/5 に適用されます。*Internet_filter* ACL は着信トラフィックに、*marketing_group* ACL は発信トラフィックに適用されま

```
Switch(config)# interface gigabitethernet0/5
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
...
```

IP ACL に適用される時間範囲

次の例では、月曜日から金曜日の午前 8 時 ~ 午後 6 時の間、IP の HTTP トラフィックが拒否されま

す。UDP トラフィックは、土曜日および日曜日の正午 ~ 午後 8 時の間のみ許可されます。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group strict in
```

コメント付きの IP ACL エントリ

次に示す番号指定 ACL の例では、Jones が所有するワークステーションのアクセスは許可されますが、Smith が所有するワークステーションのアクセスは禁止されます。

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

次に示す番号指定 ACL の例では、Winter および Smith のワークステーションでの Web 閲覧が禁止されます。

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

次に示す名前指定 ACL の例では、Jones のサブネットのアクセスが禁止されます。

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

次に示す名前指定 ACL の例では、Jones のサブネットでの発信 Telnet の使用が禁止されます。

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

ACL のロギング



(注) ポート ACL でのロギングはサポートされません。

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、名前指定の標準アクセス 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。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end

Switch# 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
```

(テキスト出力は省略)

```
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
00:15:33:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 2009 packets
```

次に、名前指定の拡張アクセス 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。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface gigabitethernet0/3
Switch(config-if)# ip access-group ext1 in
```

次に、拡張 IP 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-IPACCESSLOGDP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGDP: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 キーワードを使用して同じ種類のパケットに関するログ メッセージを作成した場合、ログ メッセージには入力インターフェイス情報が追加されません。

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

名前指定の MAC 拡張 ACL の設定

VLAN および物理レイヤ 2 インターフェイスで非 IP トラフィックをフィルタリングする場合は、MAC アドレスおよび名前指定の MAC 拡張 ACL を使用します。手順については、他の名前指定拡張 ACL の場合と同様です。アクセス リストの名前として番号を使用することもできますが、700 ~ 799 の MAC アクセス リスト番号はサポートされません。



(注) 名前指定の MAC 拡張 ACL は、レイヤ 3 インターフェイスに適用できません。

`mac access-list extended` コマンドでサポートされている非 IP プロトコルの詳細については、このリリースのコマンド リファレンスを参照してください。



(注) `appletalk` はコマンドライン ヘルプ スtring 内に表示されますが、`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はサポートされません。また、ゼロ以外の Organizational Unique Identifier (OUI) を含む EtherType の SNAP カプセル化パケットに対しても一致しません。

名前指定の MAC 拡張 ACL を作成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>mac access-list extended name</code>	名前を使用して拡張 MAC アクセス リストを定義します。
ステップ 3	<code>{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]</code>	<p>拡張 MAC アクセスリスト コンフィギュレーション モードでは、あらゆる (<code>any</code>) 送信元 MAC アドレス、マスク付きの送信元 MAC アドレス、または特定の (<code>host</code>) 送信元 MAC アドレス、およびあらゆる (<code>any</code>) 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、<code>permit</code> または <code>deny</code> 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"> <code>type mask</code> 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。EtherType に適用される <i>無視</i> (<i>don't care</i>) ビットの任意のマスクが付加され、一致検査が行われます。 <code>lsap lsap mask</code> 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。無視ビットの任意のマスクが付加されます。 <code>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</code> 非 IP プロトコル。 <code>cos cos</code> プライオリティを設定するために使用される、0 ~ 7 の IEEE 802.1Q サービス コスト番号
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。

	コマンド	目的
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<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。

ACL 全体を削除するには、`no mac access-list extended name` 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。名前指定の MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、DECnet Phase IV という EtherType のトラフィックのみを拒否し、その他のすべてのタイプのトラフィックを許可する、`mac1` という名前のアクセス リストを作成、表示する例を示します。


```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list mac1
    10 deny any any decnet-iv
    20 permit any any
```

レイヤ 2 インターフェイスへの MAC ACL の適用

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 を適用する場合は、次の注意事項を考慮してください。

- 入力レイヤ 3 ACL または VLAN マップが適用されているスイッチのレイヤ 2 インターフェイスに、ACL を適用できません。適用しようとすると、エラー メッセージが生成されます。出力レイヤ 3 ACL が適用されているスイッチのレイヤ 2 インターフェイスには、ACL を適用できます。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アクセス 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 ACL を適用すると、新しい ACL が前に設定した ACL に置き換わります。
- MAC アドレスを許可するために MAC ACL または VLAN フィルタが設定される場合、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) や Cisco Discovery Protocol (CDP) パケットなどのすべての制御トラフィックが拒否されます。

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 MAC アクセスリストを適用するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>interface interface-id</code>	設定する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。 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 3	<code>mac access-group {name} {in}</code>	MAC アクセスリストを使用し、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。  (注) ポート ACL は、着信方向に関してのみサポートされます。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。

■ 名前指定の MAC 拡張 ACL の設定

	コマンド	目的
ステップ 5	<code>show mac access-group [interface interface-id]</code>	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 6	<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。

指定されたアクセス グループを削除するには、`no mac access-group {name} in` インターフェイス コンフィギュレーション コマンドを使用します。

次に、インターフェイス GigabitEthernet 0/3 に MAC アクセス リスト mac1 を適用し、インターフェイスに入るパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet0/3
Router(config-if)# mac access-group mac1 in
```



(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た場合のみ有効となります。

着信 ACL の場合、スイッチは受信したパケットを ACL と照合します。ACL によってパケットが許可された場合は、パケットの処理が続行されます。拒否された場合、パケットは廃棄されます。

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て処理を行い、すべてのパケットが許可されてしまいます。ネットワーク セキュリティのため、未定義の ACL を使用する場合は注意してください。

VLAN マップの設定

ここでは、VLAN マップを設定する方法について説明します。この方法は、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向がありません。VLAN マップを使用して、特定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 マップ内に該当タイプのパケット (IP または MAC) に対する match コマンド文が存在する場合、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が廃棄されます。該当タイプのパケットに対する match コマンド文が存在しない場合、デフォルトではパケットが転送されます。



(注)

ここで使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンスを参照してください。

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、次の手順を実行します。

- ステップ 1** VLAN に適用する標準 IP ACL または拡張 IP ACL、または名前指定の MAC 拡張 ACL を作成します。「[標準および拡張 IP ACL の作成](#)」(p.29-9) および「[名前指定の MAC 拡張 ACL の設定](#)」(p.29-30) を参照してください。
- ステップ 2** VLAN ACL マップ エントリを作成するには、`vlan access-map` グローバル コンフィギュレーション コマンドを入力します。
- ステップ 3** アクセスマップ コンフィギュレーション モードでは、`action` として `forward` (デフォルト) または `drop` を任意で入力できます。また、`match` コマンドを入力し、既知の MAC アドレスのみが格納された IP パケットまたは非 IP パケットを指定したり、1 つまたは複数の ACL (標準または拡張) とパケットを照合したりすることもできます。



(注)

該当タイプのパケット (IP または MAC) に対する match コマンド文が VLAN マップに存在する場合でも、パケットがそのタイプに一致しない場合は、デフォルトでパケットが廃棄されます。該当タイプのパケットに対する match コマンド文が VLAN マップ内になく、それに対するアクションが指定されていない場合、パケットは転送されます。

- ステップ 4** VLAN マップを 1 つまたは複数の VLAN に適用するには、`vlan filter` 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。



(注)

レイヤ 2 インターフェイスに ACL (ポート ACL) が適用されているスイッチの VLAN には、VLAN マップを適用できません。

ここでは、次の内容について説明します。

- [VLAN マップ設定時の注意事項](#) (p.29-34)
- [VLAN マップの作成](#) (p.29-34)

■ VLAN マップの設定

- VLAN への VLAN マップの適用 (p.29-37)
- ネットワークでの VLAN マップの使用法 (p.29-37)

VLAN マップ設定時の注意事項

VLAN マップの設定を行うときは、次の注意事項に従ってください。

- ルーテッド VLAN インターフェイス(入力または出力)でトラフィックを拒否するように設定されたルータ ACL が存在せず、VLAN マップが設定されていない場合は、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比較検査されます。一致した場合は、VLAN マップで指定されたアクションが行われます。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比較検査されます。
- 該当タイプのパケット (IP または MAC) に対する match コマンド文が VLAN マップに 1 つまたは複数存在する場合でも、パケットがそれらの match コマンド文に一致しない場合は、デフォルトでパケットが廃棄されます。該当タイプのパケットに対する match コマンド文が VLAN マップ内に存在しない場合、デフォルトではパケットが転送されます。
- 多数の ACL が設定されている場合は、システムの起動に時間がかかることがあります。
- ルータ ACL および VLAN マップを組み合わせる方法については、「ルータ ACL と VLAN マップを併用する場合の注意事項」(p.29-40) を参照してください。
- 設定例については、「ネットワークでの VLAN マップの使用法」(p.29-37) を参照してください。
- スwitchのレイヤ 2 インターフェイスに IP アクセス リストまたは MAC アクセス リストが適用されている場合、VLAN マップを作成することはできますが、スイッチの VLAN に VLAN マップを適用することはできません。適用しようとすると、エラーメッセージが生成されます。
- 存在しない VLAN マップを VLAN に適用すると、警告メッセージが表示されます。存在しない VLAN マップを VLAN に適用できても、VLAN マップが定義されるまでイネーブルになりません。誤ってパケットを廃棄して設定プロセスの途中で接続をディセーブルにすることを回避するために、VLAN に適用する前に VLAN マップを完全に定義することを推奨します。

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、削除するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>vlan access-map name [number]</code>	VLAN マップを作成し、名前および番号 (任意) を付けます。番号は、マップ内のエントリの順序を表す数字です。 同じ名前の VLAN マップを作成すると、10 ずつ増分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、目的のマップ エントリの番号を入力できます。 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。
ステップ 3	<code>action {drop 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。デフォルトは転送です。

	コマンド	目的
ステップ 4	<code>match {ip mac} address {name / number} [name / number]</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比較します (IP または MAC アドレスを使用)。パケットの比較は、対応するプロトコル タイプのアクセス リストに対してのみ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して比較されます。非 IP パケットは、名前指定の MAC 拡張アクセス リストに対してのみ比較されます。
ステップ 5	<code>end</code>	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 6	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 7	<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。

マップを削除するには、`no vlan access-map name` 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。

マップ内の単一のシーケンス エントリを削除するには、`no vlan access-map name number` 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。

デフォルトのアクションである転送を強制的に行うには、`no action` アクセスマップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の `permit` または `deny` キーワードは使用されません。VLAN マップを使用してパケットを拒否するには、パケットと比較する ACL を作成し、アクションを廃棄に設定します。ACL に `permit` キーワードを指定した場合は一致とみなされます。ACL に `deny` キーワードを指定した場合は一致しないとみなされます。

ACL および VLAN マップの例

次に、特定の目的で ACL および VLAN マップを作成する例を示します。

例 1

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廃棄されます。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` コマンド文が存在するため、デフォルトではどの `match` コマンド文とも一致しないすべての IP パケットが廃棄されます。

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

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 パケットを許可します。`ip2` ACL と一致するすべてのパケットが転送されます。

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

このマップでは、これ以前のどの ACL ととも一致しなかったすべての IP パケット (TCP でも UDP でもないパケット) が廃棄されます。

例 2

次の例の VLAN マップでは、デフォルトで IP パケットが廃棄され、MAC パケットが転送されます。標準の ACL 101 と名前指定の拡張アクセス 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 パケットが廃棄されます。
- 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 パケットが廃棄されます。
- すべての非 IP パケットが転送されます。

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

例 3

次の例の VLAN マップでは、デフォルトで MAC パケットが廃棄され、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` とこのマップを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-ip` 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 パケットが廃棄されます。
- すべての IP パケットが転送されます。

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

例 4

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) が廃棄されます。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 パケットが廃棄されます。
- その他のすべての MAC パケットが廃棄されます。

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

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<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	<code>vlan filter mapname vlan-list list</code>	VLAN マップを 1 つまたは複数の VLAN ID 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 からなるストリング (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 3	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 4	<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。



(注) レイヤ 2 インターフェイスに ACL (ポート ACL) が適用されているスイッチの VLAN には、VLAN マップを適用できません。

VLAN マップを削除するには、`no vlan filter mapname vlan-list list` 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。

次に、VLAN マップ 1 を VLAN 20 ~ 22 に適用する例を示します。

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

ネットワークでの VLAN マップの使用法

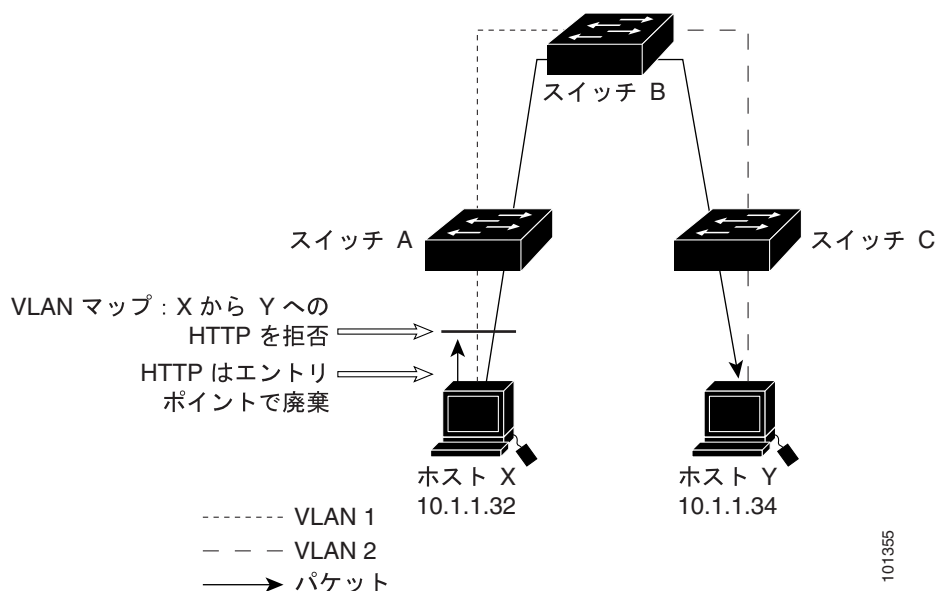
ここでは、VLAN マップの一般的な使用法について説明します。具体的な内容は次のとおりです。

- [配線クローゼットの構成 \(p.29-38\)](#)
- [別の VLAN にあるサーバへのアクセス拒否 \(p.29-39\)](#)

配線クローゼットの構成

配線クローゼット構成におけるスイッチでは、ルーティングがイネーブルでない可能性があります。ただし、この構成でも VLAN マップおよび QoS 分類 ACL はサポートされています。図 29-4 では、ホスト X およびホスト Y は異なる VLAN 内にあり、配線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ています。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたスイッチ 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 でアクセス制御できます。

図 29-4 配線クローゼットの構成



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) への HTTP トラフィックがスイッチ B にブリッジされず、すべてスイッチ A で廃棄されるようにスイッチ A の VLAN マップを設定できます。

まず、HTTP ポートですべての 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。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(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廃棄され、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。

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

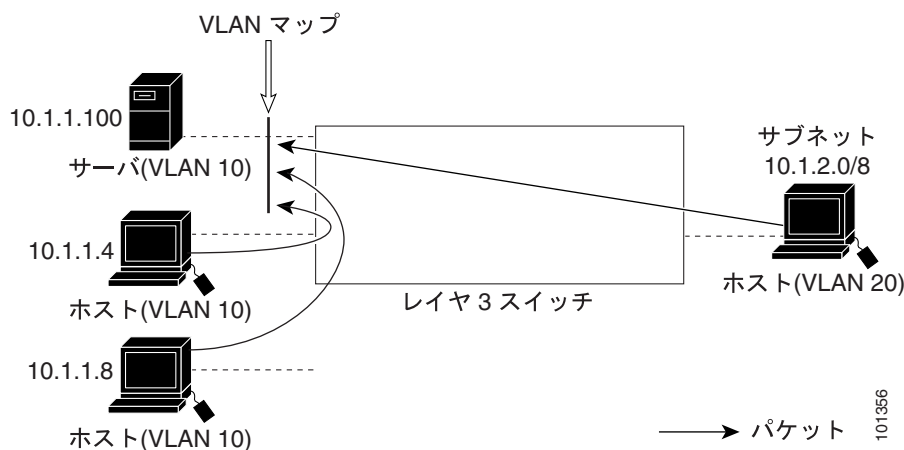
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN にあるサーバへのアクセス拒否

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 に対しては、次のようにアクセスを制限する必要があります（図 29-5 を参照）。

- 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。

図 29-5 別の VLAN にあるサーバへのアクセス拒否



この例では、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 を作成して、別の VLAN 内のサーバへのアクセスを拒否する方法を示しています。最後に、VLAN マップ SERVER1 を VLAN 10 に適用します。

ステップ 1 対応するパケットと比較する IP ACL を定義します。

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

ステップ 2 SERVER1_ACL と一致する IP パケットを廃棄し、一致しない IP パケットを転送するこの ACL を使用して、VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

ステップ 3 VLAN 10 に VLAN マップを適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

ルータ ACL と VLAN マップの併用

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制御を行うには、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で使用します。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制御する VLAN マップを定義できます。



(注) 1つのスイッチで、VLAN マップまたは入力ルータ ACL とポート ACL を組み合わせて使用することはできません。

パケットフローが ACL 内 VLAN マップの deny コマンド文と一致した場合、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。

該当タイプのパケット (IP または MAC) に対する match コマンド文が VLAN マップに存在する場合でも、パケットがそのタイプに一致しない場合は、デフォルトでパケットが廃棄されます。VLAN マップ内に match コマンド文がなく、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。

ここでは、ルータ ACL を VLAN マップと組み合わせて使用する方法について説明します。

- [ルータ ACL と VLAN マップを併用する場合の注意事項 \(p.29-40\)](#)
- [VLAN に適用されるルータ ACL と VLAN マップの例 \(p.29-41\)](#)

ルータ ACL と VLAN マップを併用する場合の注意事項

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場合に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる場合に、これらの注意事項は適用されません。

スイッチ ハードウェアは、方向 (入力および出力) ごとにセキュリティ ACL を 1 回検索します。したがって、ルータ ACL および VLAN マップを同じ VLAN に設定する場合は、これらを統合する必要があります。ルータ ACL と VLAN マップを統合すると、ACE の数が急増することがあります。

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する注意事項に従ってください。

- 可能なかぎり、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のみがもう一方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。可能なかぎり、IP アドレスには無視（*don't care*）ビットを使用してください。

レイヤ 4 情報を含む IP ACE と 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。



(注)

ACL 設定が指定されたインターバル内で安定した状態になると、システムは設定をハードウェアにロードします。ハードウェアのアップデート中は、影響を受けるすべてのインターフェイスで転送がブロックされます。この動作を変更する場合は、`mls aclmerge delay` および `access-list hardware program nonblocking` 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。これらのコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

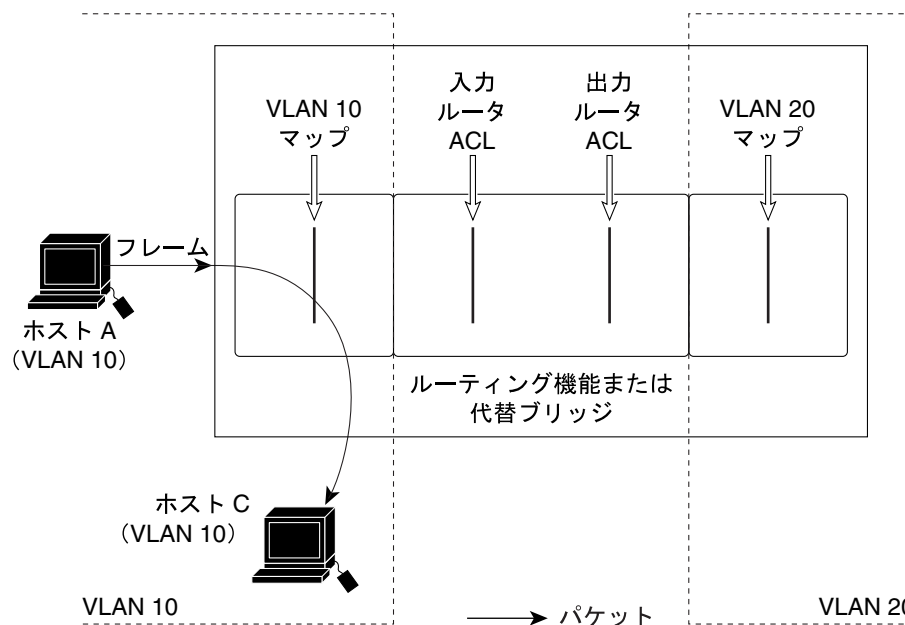
VLAN に適用されるルータ ACL と VLAN マップの例

ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す回線と交差するポイントで、パケットを転送せずに廃棄することもできます。

ACL およびスイッチド パケット

図 29-6 に、VLAN 内でスイッチングされるパケットに ACL を適用する方法を示します。代替ブリッジングによってルーティングまたは転送されず、VLAN 内でスイッチングされるパケットには、入力 VLAN の VLAN マップのみが適用されます。

図 29-6 スイッチド パケットへの ACL の適用

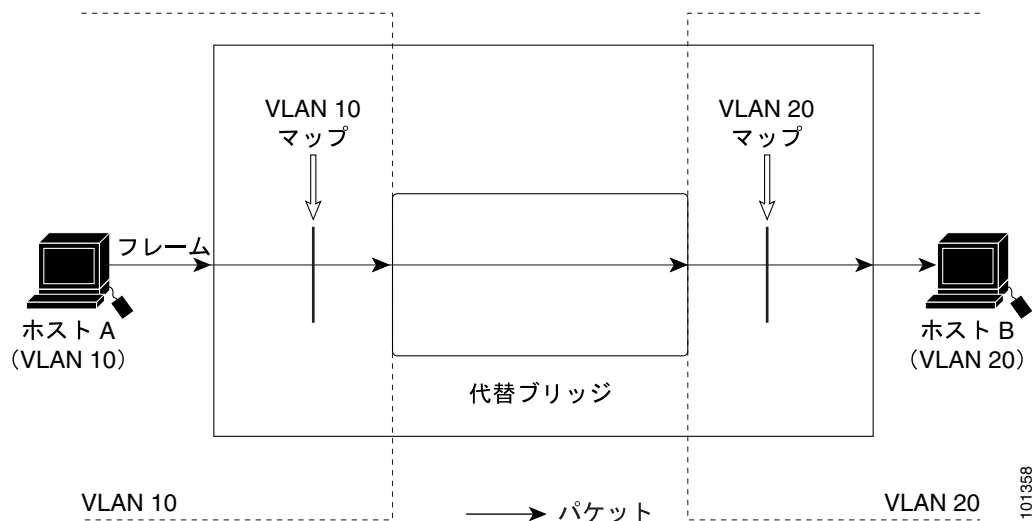


101357

ACL およびブリッジド パケット

図 29-7 に、代替ブリッジド パケットに ACL を適用する方法を示します。ブリッジド パケットの場合は、入力 VLAN にレイヤ 2 ACL のみが適用されます。また、非 IP および非 ARP パケットのみが代替ブリッジド パケットとなります。

図 29-7 ブリッジド パケットへの ACL の適用

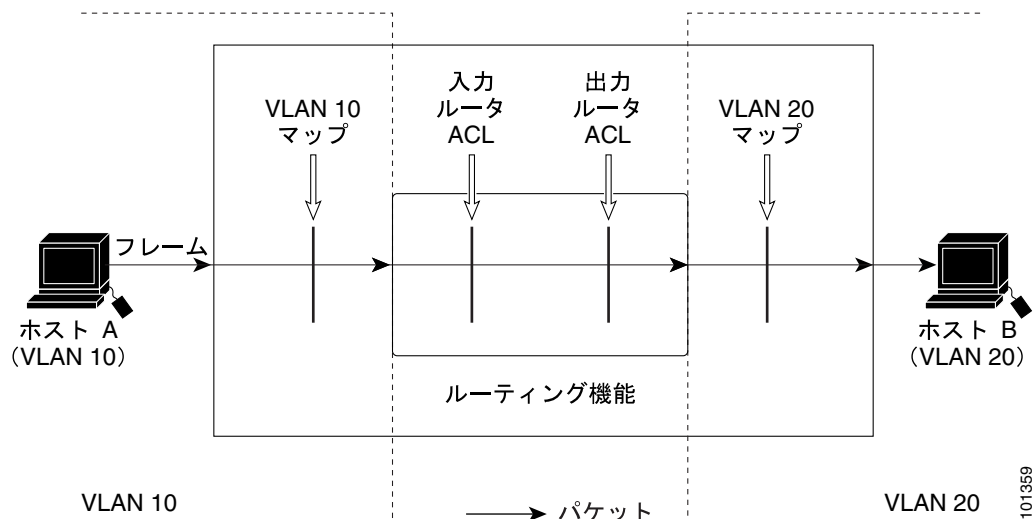


ACL およびルーテッド パケット

図 29-8 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合、ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

図 29-8 ルーテッド パケットへの ACL の適用

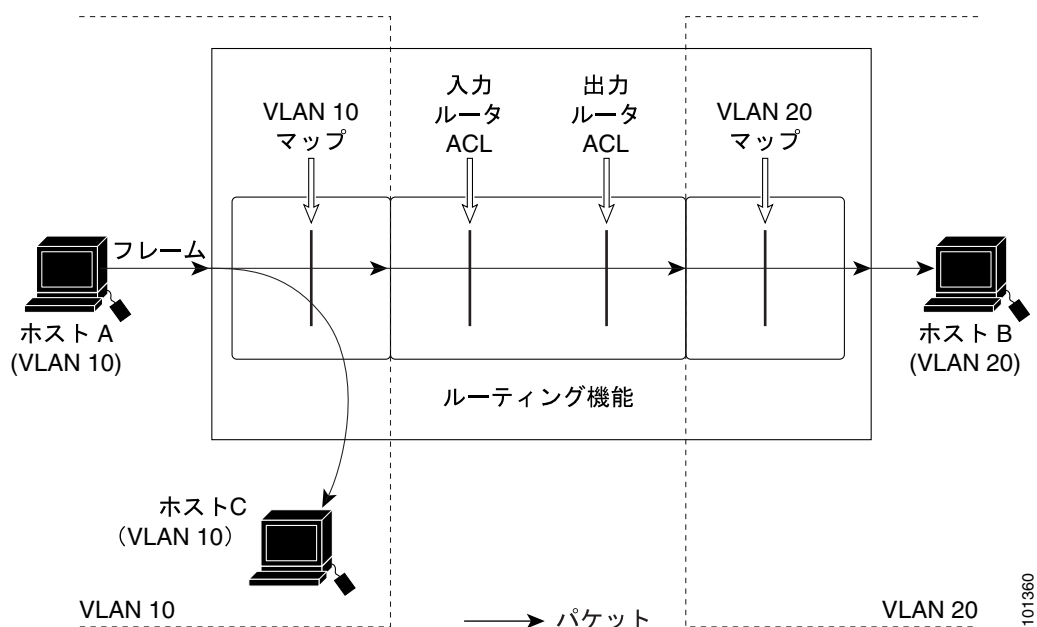


ACL およびマルチキャスト パケット

図 29-9 に、IP マルチキャスト用に複製されたパケットに ACL を適用する方法を示します。ルーティングされるマルチキャスト パケットには、2 つの異なるフィルタが適用されます。1 つは、宛先が入力 VLAN 内の他のポートである場合に使用され、もう 1 つは、宛先がパケットのルーティング先である別の VLAN 内にある場合に使用されます。パケットは複数の出力 VLAN にルーティングされますが、この場合は宛先 VLAN ごとに異なるルータ出力 ACL および VLAN マップが適用されます。

最終的に、パケットは一部の出力 VLAN 内で許可され、それ以外の VLAN で拒否されます。パケットのコピーが、許可された宛先に転送されます。ただし、入力 VLAN マップ (図 29-9 の VLAN 10 マップ) によってパケットが廃棄される場合、パケットのコピーは宛先に送信されません。

図 29-9 マルチキャスト パケットへの ACL の適用



ACL 情報の表示

スイッチに設定されている ACL、およびインターフェイスや VLAN に適用された ACL を表示できます。また、設定の矛盾に関する情報や ACL に関連したリソースの利用についての情報も表示できます。

ここで説明する内容は次のとおりです。

- [ACL の設定の表示 \(p.29-44 \)](#)
- [ACL リソースの利用率および設定問題の表示 \(p.29-46 \)](#)

ACL の設定の表示

既存の ACL を表示できます。 `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。レイヤ 2 インターフェイスに適用された MAC ACL を表示することもできます。この情報を表示するには、イネーブル EXEC コマンドを使用します ([表 29-2](#) を参照)。

表 29-2 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
<code>show access-lists [number / name]</code>	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 (番号指定または名前指定) の内容を表示します。
<code>show ip access-lists [number / name]</code>	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 (番号指定または名前指定) を表示します。
<code>show ip interface interface-id</code>	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 がイネーブルであるインターフェイスに、 <code>ip access-group</code> 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 グループも表示されます。
<code>show running-config [interface interface-id]</code>	スイッチまたは特定のインターフェイスに関する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、インターフェイスに適用されているアクセス グループなど) を表示します。
<code>show mac access-group [interface interface-id]</code>	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。

次に、`show access-lists` イネーブル EXEC コマンドを実行し、すべての標準 ACL および拡張 ACL を表示する例を示します。

```
Switch# show access-lists
Standard IP access list 1
  permit 172.20.10.10
Standard IP access list 10
  permit 12.12.12.12
Standard IP access list 12
  deny 1.3.3.2
Standard IP access list 32
  permit 172.20.20.20
Standard IP access list 34
  permit 10.24.35.56
  permit 23.45.56.34
Extended IP access list 120
  permit eigrp host 12.3.6.5 host 25.36.1.24
Extended MAC access list mac1
```

次に、`show ip access-lists` イネーブル EXEC コマンドの出力例を示します。IP 標準および拡張 ACL のみが表示されます。前述の例で表示された名前指定の MAC 拡張 ACL は、この例で表示されません。

```
Switch# show ip access-lists
Standard IP access list 1
  permit 172.20.10.10
Standard IP access list 10
  permit 12.12.12.12
Standard IP access list 12
  deny 1.3.3.2
Standard IP access list 32
  permit 172.20.20.20
Standard IP access list 34
  permit 10.24.35.56
  permit 23.45.56.34
Extended IP access list 120
  permit eigrp host 12.3.6.5 host 25.36.1.24
```

次に、`show mac access-group` イネーブル EXEC コマンドの出力例を示します。この出力で、MAC アクセスリスト (`mac1-e1`) が適用されているインターフェイスは 1 つしかありません (GigabitEthernet インターフェイス 2)。

```
Switch# show mac access-group
Interface GigabitEthernet0/1:
  Inbound access-list is not set
Interface GigabitEthernet0/2:
  Inbound access-list is mac1_e1
Interface GigabitEthernet0/3:
  Inbound access-list is not set
Interface GigabitEthernet0/4:
  Inbound access-list is not set
Interface GigabitEthernet0/5:
  Inbound access-list is not set
```

(テキスト出力は省略)

VLAN アクセスマップまたは VLAN フィルタに関する情報を表示できます。VLAN マップ情報を表示するには、表 29-3 に記載されたイネーブル EXEC コマンドを使用します。

表 29-3 VLAN マップ情報を表示するコマンド

コマンド	目的
<code>show vlan access-map [mapname]</code>	すべての VLAN アクセスマップまたは指定されたアクセスマップに関する情報を表示します。
<code>show vlan filter [access-map name / vlan vlan-id]</code>	すべての VLAN フィルタに関する情報、または指定された VLAN や VLAN アクセスマップに関する情報を表示します。

次は、`show vlan access-map` イネーブル EXEC コマンドの出力例です。

```
Switch# show vlan access-map
Vlan access-map "map_1" 10
  Match clauses:
    ip address: ip1
  Action:
    drop
Vlan access-map "map_1" 20
  Match clauses:
    mac address: mac1
  Action:
    forward
```

次に、`show vlan filter` イネーブル EXEC コマンドの出力例を示します。

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

ACL リソースの利用率および設定問題の表示

スイッチの機能マネージャは、設定された ACL にリソースを割り当てます。設定に必要なだけの十分なハードウェア リソースがない場合、または設定に問題がある場合は、エラー メッセージが生成されます。コンソールがエラー メッセージ受信用に設定されていない場合は、`show fm` イネーブル EXEC コマンドを使用して機能マネージャのメッセージを表示し、インターフェイスの ACL を処理するリソースについての情報を入手できます。また、`show tcam` イネーブル EXEC コマンドを使用すると、スイッチの TCAM の容量に関するステータス情報を入手できます。

表 29-4 に、ACL 機能マネージャ情報を表示するイネーブル EXEC コマンドを示します。

表 29-4 VLAN マップ情報を表示するコマンド

コマンド	目的
<code>show fm vlan <i>vlan-id</i></code> または <code>show fm interface <i>interface-id</i></code>	インターフェイスまたは VLAN の機能マネージャ情報（ハードウェア ポートラベルまたは VLAN ラベルのインターフェイス番号、機能マネージャに発生した問題など）を表示します。
<code>show fm vlan-label <i>label-id</i></code> または <code>show fm port-label <i>label-id</i></code>	ハードウェアに適合した設定済み ACL の機能など、識別ラベルについての情報を表示します。VLAN ラベルはルータ ACL と VLAN マップに使用され、ポート ラベルはポート ACL に使用されます。VLAN <i>label-id</i> の範囲は 0 ~ 255、ポート <i>label-id</i> の範囲は 0 ~ 127 です。
<code>show tcam {<i>inacl</i> <i>outacl</i>} <i>tcam-id</i> {{<i>port-labels</i> [<i>label-id</i>]} <i>size</i> {{<i>statistics</i> [<i>entries</i> <i>hits</i> <i>labels</i> <i>masks</i>]} {<i>vlan-labels</i> [<i>label-id</i>]}}</code>	TCAM の入力 ACL 領域または出力 ACL 領域についての情報を表示します。TCAM ID の有効範囲は、1 ~ 3 です（スイッチ モデルによって異なります）。このコマンドに関するその他のキーワードは、主にシスコのテクニカル サポート スタッフが使用する情報の表示に使用されます。

これらのコマンドの詳細については、このリリースのコマンド リファレンスを参照してください。

ここでは、次の ACL 問題に関する情報表示方法について説明します。

- [設定の矛盾 \(p.29-47\)](#)
- [ハードウェアでの ACL 設定の適合性 \(p.29-48\)](#)
- [TCAM の利用率 \(p.29-50\)](#)

設定の矛盾

ルータ ACL がすでに設定されているスイッチのインターフェイスにポート ACL を適用するなど、許可されていない ACL 設定を入力しようとすると、エラーメッセージがログに記録されます。

次の例では、ギガビットポート 1 はレイヤ 2 インターフェイスです。アクセスリスト *ip3* を適用しようとすると、すでにスイッチのレイヤ 3 インターフェイスに ACL が適用されていることを示すエラーメッセージが表示されます。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group ip3 in
Switch(config-if)#
1d18h:%FM-3-CONFLICT:Port ACL ip3 conflicts with input router ACLs
```

ACL の設定に矛盾があるかどうかを判断し、そのポートのポートラベル番号を調べるには、インターフェイスに対して **show fm interface** イネーブル EXEC コマンドを実行します。さらに詳細情報を表示するには、次の例のように **show fm port-label** イネーブル EXEC コマンドを入力します。

```
Switch# show fm interface gigabitethernet0/1
Conflicts exist with layer 3 access groups.
Input Port Label:2
Switch# show fm port-label 2
Conflicts exist with layer 3 access groups.
Needed in CAM(s):1
Loaded into CAM(s):1
Sent to CPU by CAM(s):
Interfaces: Gi0/1
IP Access Group:ip3 0 VMRs
DHCP Broadcast Suppression Disabled.
MAC Access Group:(None) 0 VMRs
```

次の例は、レイヤ 2 インターフェイスに ACL がすでに適用されているスイッチで、SVI である VLAN 1 に ACL 121 を適用しようとした結果を示しています。

```
Switch(config)# interface vlan 1
Switch(config-if)# ip access-group 121 in
Switch(config-if)#
1d18h:%FM-3-CONFLICT:Input router ACL 121 conflicts with port ACLs
```

show fm vlan イネーブル EXEC コマンドを入力すると設定の矛盾が表示され、VLAN *label-ids* を判断できます。さらに詳細情報を表示するには、**show fm vlan-label** コマンドを入力します。

```
Switch# show fm vlan 1
Conflicts exist with layer 2 access groups.
Input VLAN Label:1
Output VLAN Label:0 (default)
Priority:normal
Switch# show fm vlan-label 1
Conflicts exist with layer 2 access groups.
Input Features:
  Interfaces or VLANs: V11
  Priority:normal
  Vlan Map:(none)
  Access Group:121, 0 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs:
  Priority:low
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:(none), 0 VMRs
```

ハードウェアでの ACL 設定の適合性

前述のように、Catalyst 3550 スイッチでの ACL 処理は、大部分がハードウェアで処理されます。ただし、ACL 設定を格納するためのハードウェア容量が限界に達した場合は、スイッチのソフトウェアによって、ハードウェア内の設定が単純になるように調整されます。設定が単純になると、設定されたフィルタリング処理の一部が実行されなくなり、一部またはすべてのパケットが CPU に送られて、ソフトウェアによりフィルタリングされます。この方法で、設定されたすべてのフィルタリング処理が実行されますが、ソフトウェアでフィルタリングが行われるとパフォーマンスが大幅に低下します。

たとえば、VLAN インターフェイスに適用される入力ルータ ACL と、同じ VLAN に適用される VLAN マップの組み合わせがハードウェアに適合しない場合は、次のようになります。

- VLAN マップのみがハードウェアに適合する場合、ソフトウェアはハードウェアに対して、ルーティングの必要があるすべてのパケットを CPU に送信し、そこでフィルタリングまたは（パケットがフィルタを通過した場合は）ルーティングが行われるように設定します。入力 VLAN 内でのブリッジングのみが必要なパケットは、すべてハードウェアで処理され、CPU には送信されません。
- VLAN マップがハードウェアに適合しない場合は、VLAN のすべてのパケットをソフトウェアでフィルタリングし、転送する必要があります。

ハードウェアに対する設定の適合性問題はすべてログに記録されます。`show fm` イネーブル EXEC コマンドを使用すると、ハードウェアに適合しないインターフェイスの設定または VLAN の設定があるかどうかを判別できます。

ポート ACL の例

次に、使用可能な TCAM スペースに対してポート アクセス リストが大きすぎる例を示します。

```
Switch(config-if)# interface gigabitethernet0/3
Switch(config-if)# ip access-group 100 in
Switch(config-if)#
00:04:58:%FM-3-UNLOADING:Unloading port label 3 feature from TCAM 1
```

ポート ラベルを確認したり、ラベルがインターフェイスに割り当てられているかどうかを調べる場合は、`show fm interface` コマンドを入力します。

```
Switch# show fm interface gigabitethernet0/3
Input Port Label:3
```

次の例では、`show fm port-label 3` イネーブル EXEC コマンドの出力から、CAM 1 に必要なラベル 3 が CAM 1 にロードされず、代わりに CPU に送信されていることがわかります。

```
Switch# show fm port-label 3
Needed in CAM(s):1
Loaded into CAM(s):
Sent to CPU by CAM(s):1
Interfaces: Gi0/3
IP Access Group:100 3400 VMRs
DHCP Broadcast Suppression Disabled.
MAC Access Group:(None) 2 VMRs
```

スイッチの TCAM の数はスイッチ モデルによって異なります (1 ~ 3)。TCAM を複数個装備しているスイッチで、同じポート ACL が複数のインターフェイスに適用されている場合、必要な TCAM の一部 (全部ではない) に設定が適合しないことがあります。このような場合、ACL が適用されたときに生成されたログメッセージに、その ACL をロードできなかった TCAM が指定されます。

```
Switch(config)# interface gigabitethernet0/10
Switch(config-if)# ip access-group 101 in
Switch(config-if)#
01:46:25:%FM-3-UNLOADING:Unloading port label 4 feature from TCAM 1
```

ラベル 4 に対して `show fm port-label` コマンドを入力すると、各 TCAM に機能がロードされているかどうかわかります。

```
Switch# show fm port-label 4
Needed in CAM(s):1 3
Loaded into CAM(s):3
Sent to CPU by CAM(s):1
Interfaces: Gi0/3, Gi0/10
IP Access Group:101 379 VMRs
DHCP Broadcast Suppression Disabled.
MAC Access Group:(None) 2 VMRs
```

この出力は、CAM 1 と 3 でポート ラベル 4 が必要とされているのに、CAM 1 にポート ラベル 4 が適合していないことを示しています。CAM 1 に他のポート ラベルのエントリがすでに含まれ CAM 3 よりも使用可能な空き容量が少ないためです。また、この出力から、CAM 3 にはポート ラベル 4 がロードされているものの、このラベルのポート ACL のエントリが CAM 1 からアンロードされているため、CAM 1 はこのラベルのパケットを CPU に送信していることがわかります。

VLAN またはルータ ACL の例

次に、VLAN 1 の機能マネージャ情報を表示する例を示します。

```
Switch# show fm vlan 1
Input VLAN Label:1
Output VLAN Label:0 (default)
Priority:normal
```

次に、`show fm vlan-label` イネーブル EXEC コマンドの出力例を示します。入力アクセス グループでマージに失敗したことがわかります。

```
Switch# show fm vlan-label 1
Unloaded due to merge failure or lack of space:
  InputAccessGroup
  Merge Fail:input
Input Features:
  Interfaces or VLANs: V11
  Priority:normal
  Vlan Map:(none)
  Access Group:131, 6788 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs:
  Priority:low
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:(none), 0 VMRs
```

次に、`show fm vlan-label` イネーブル EXEC コマンドの出力例を示します。入力アクセス グループに使用できる十分な空き容量がハードウェアにないことがわかります。

```
Switch# show fm vlan-label 1
Unloaded due to merge failure or lack of space:
  InputAccessGroup
Input Features:
  Interfaces or VLANs: V11
  Priority:normal
  Vlan Map:(none)
  Access Group:bigone, 11 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs:
  Priority:low
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:(none), 0 VMRs
```

次に、`show fm vlan-label` イネーブル EXEC コマンドの例を示します。この出力から、このラベルの入力アクセス グループまたは出力アクセス グループに対して十分な空き容量がないことがわかります(アクセス グループは2つの異なるインターフェイスに設定されています。ラベルは入力および出力に関して個別に割り当てられます)。

```
Switch# show fm label 1
Unloaded due to merge failure or lack of space:
  InputAccessGroup OutputAccessGroup
Input Features:
  Interfaces or VLANs: V11
  Priority:normal
  Vlan Map:(none)
  Access Group:bigone, 11 VMRs
  Multicast Boundary:(none), 0 VMRs
Output Features:
  Interfaces or VLANs: V12
  Priority:normal
  Bridge Group Member:no
  Vlan Map:(none)
  Access Group:bigtwo, 11 VMRs
```



(注)

ACL に割り当てられるハードウェア リソースが最大になるように ACL を設定する場合は、`sdm prefer access` グローバル コンフィギュレーション コマンドを使用し、アクセス テンプレートに SDM 機能を設定します。SDM テンプレートの詳細については、「[ユーザが選択した機能に対するシステム リソースの最適化](#)」(p.6-28) を参照してください。

TCAM の利用率

`show tcam` イネーブル EXEC コマンドを使用すると、ACL を設定する前後に TCAM の空き容量を表示したり、特定のインターフェイスまたは VLAN に割り当てられている TCAM 内の容量を調べることができます。

TCAM 内で ACL が入力されている領域の合計サイズを表示するには、`show tcam size` を使用します。

```
Switch# show tcam inacl 1 size
Ingress ACL TCAM Size:6592 Entries
```

さまざまな TCAM 領域に割り当てる容量を変更する場合は、`sdm prefer` 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。このコマンドを使用して、ACL、ルーティング、またはレイヤ 2 スイッチングに割り当てるリソースを増やすことができます。

入力または出力の TCAM 領域に対して `show tcam statistics` コマンドを入力すると、マスクおよびエントリの割り当て量と使用可能量が表示されるため、その TCAM 領域がどの程度利用されているかがわかります。次に示すのは、このコマンドの出力例です。

```
Switch# show tcam inacl 1 statistics
Ingress ACL TCAM#1:Number of active labels:3
Ingress ACL TCAM#1:Number of masks allocated: 14, available: 810
Ingress ACL TCAM#1:Number of entries allocated: 17, available:6575
```

インターフェイスまたは VLAN への ACL の設定に使用できる TCAM の量を判断するには、まず `show fm interface` コマンドまたは `show fm vlan` コマンドを使用します。これらのコマンドの出力から、そのポートまたは VLAN の ACL 設定に使用されるポート ラベルまたは VLAN ラベルを判別できます。さらに、`show tcam port-label` コマンドまたは `show tcam vlan-label` コマンドを使用すると、そのラベルに割り当てられている TCAM の容量が表示されます。VLAN ラベルはルータ ACL と VLAN マップに、ポート ラベルはポート ACL に使用されます。

```
Switch# show fm vlan 1
Input VLAN Label:1
Output VLAN Label:0 (default)
Priority:normal
Switch# show tcam inacl 1 vlan-labels 1
Label Value :      8193(vlan label 1)
Number of entries :779
Entry List
-----
Mask Index :4
F7 00 00 00 00 00 00 00 80 FF C0 00 C0 FF FF 00 00
Entry Index :32 Timestamp:1
96 00 00 00 00 00 00 00 80 01 40 00 80 00 01 00 00 As Data(hex) :00260086
Mask Index :5
F7 00 00 00 00 00 00 00 80 FF C0 00 C0 00 00 FF FF
Entry Index :33 Timestamp:4
96 00 00 00 00 00 00 00 80 01 40 00 80 00 00 00 B3 As Data(hex) :00260086
Mask Index :6
F5 00 00 00 00 E0 00 00 00 80 FF C0 00 C0 00 00 00 00
Entry Index :48 Timestamp:1
94 00 00 00 00 E0 00 00 00 80 01 40 00 80 00 00 00 00 As Data(hex) :00210086
Mask Index :7
F7 00 00 00 00 00 00 00 80 FF C0 00 C0 00 00 00 00
Entry Index :49 Timestamp:4
96 00 00 00 00 00 00 00 80 01 40 00 80 00 00 00 00 As Data(hex) :00210086
Mask Index :8
F5 00 00 00 00 00 00 00 80 FF C0 00 C0 00 00 00 00
Entry Index :64 Timestamp:1
```

(テキスト出力は省略)



(注)

`show tcam vlan-label` の出力に含まれているエントリ数 (*Number of entries*) フィールドでは、2 つのデフォルト エントリがカウントされていないため、このフィールドの値からは 2 つのエントリが除外されています。デフォルト エントリはポート ラベルに使用されないため、このフィールドの出力は正確な値となります。

