CHAPTER 32

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 コントロール リスト）を使用して、Catalyst 3750 Metro 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 リストとも呼びます。

（注） 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 リファレンスと『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章の「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 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

この章で説明する内容は、次のとおりです。

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することができます。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または VLAN 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るとテストを終了するので、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。スイッチは、VLAN 内でブリッジングされるパケットを含めて、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できます。

ネットワークに基本的なセキュリティを導入する場合は、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することができます。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 を着信トラフィック、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。

ACL には Access Control Entry（ACE; アクセス コントロール エントリ）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 と一致するためにパケットが満たす必要がある条件を指定します。*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。

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

- IP ACL は、TCP、UDP、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）、Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）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 は、非 IPv4 トラフィックをフィルタリングします。

このスイッチは、QoS（Quality of Service）分類 ACL もサポートしています。詳細については、「QoS ACL に基づく入力分類」（p.33-11）を参照してください。

ここでは、次の内容について説明します。

サポートされる ACL

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 がサポートされています。

- ルータ ACL は、VLAN 間でルーティングされたトラフィックをアクセス制御し、レイヤ 3 インターフェイスに適用されます。
- 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制御します。発信方向のポート ACL はサポートされません。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）をアクセス制御します。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することができます。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。

同じスイッチ上でルータ ACL、入力ポート ACL、および VLAN マップを併用できます。ただし、ポート ACL はルータ ACL または VLAN マップよりも優先されます。

- 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。
- Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）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。その他のポートに着信したルーテッド IP パケットは、ルータ 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。発信されるルーテッド IP パケットは、ルータ 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 によってのみフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、VLAN マップおよびルータ ACL の両方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 マップによってのみフィルタリングされます。
- 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 によってのみフィルタリングされます。発信されるルーテッド IP パケットは、VLAN マップとルータ ACL の両方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 マップによってのみフィルタリングされます。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスである SVI、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 を適用することができます。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 つ適用することができます。

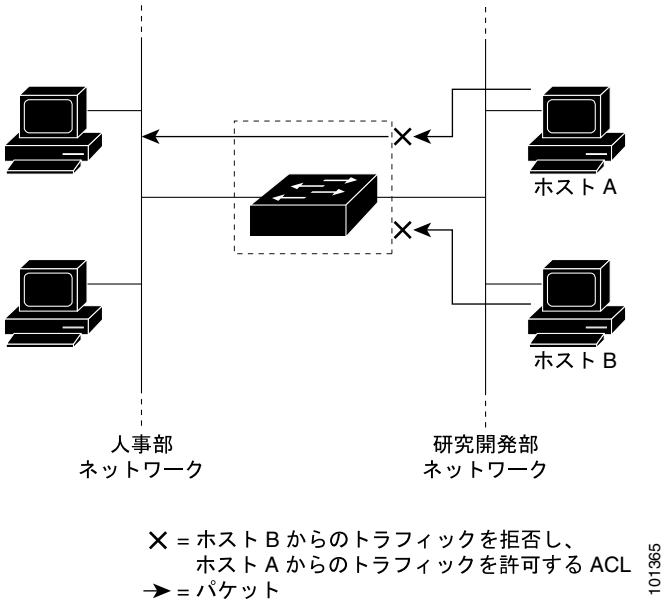
1 つの ACL を特定のインターフェイスの複数の機能に使用することができます。また、1 つの機能に複数の ACL を使用することもできます。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回、照合されます。

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

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 を照合します。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 がパケット転送を許可するか拒否するかは、ACL 内のエントリとパケットの一致結果に応じて決まります。ACL を使用して、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制御が可能です。図 32-1 では、スイッチ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が許可されますが、ホスト B は拒否されます。

図 32-1　ACL によるネットワーク トラフィックの制御



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 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、着信トラフィックに対してのみです。

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た ACL をテストし、パケットと ACL 内のエントリの一致結果に応じて、パケットの転送を許可または拒否します。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 32-1 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 IPv4 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 IPv4 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 リストまたは MAC アクセス リストが 1 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、前に設定した ACL が新しい ACL に置き換わります。

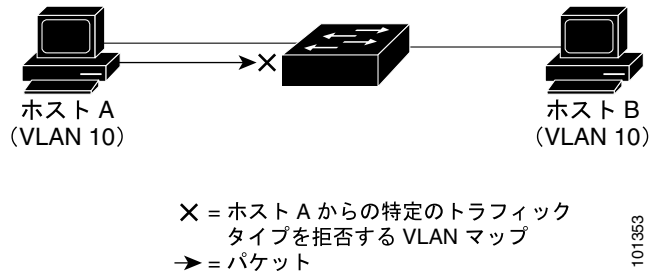
VLAN マップ

VLAN ACL または VLAN マップは、*すべて*のトラフィックをアクセス制御することができます。VLAN との間でルーティングされる、または VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用することができます。VLAN マップは、セキュリティ パケット フィルタリングに使用されます。VLAN マップは方向（着信または発信）ごとに定義されません。

VLAN マップを設定すると、IP トラフィックのレイヤ 3 アドレスと照合することができます。すべての非 IPv4 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、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 32-2 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。1 つの VLAN に適用できる VLAN マップは、1 つだけです。

図 32-2　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、この情報は格納されません。

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。通常の方法では、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適用できません。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され、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）　この例の最初および 2 番めの ACE では、宛先アドレスのあとに *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; シンプル メール転送プロトコル）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 ポート情報が含まれていなくても、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 番めの 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 番めの ACE には一致しません。残りのフラグメントは 3 番めの 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 番めの 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 番めの 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

スイッチに IP ACL を設定する手順は、シスコ製スイッチおよびルータに IP ACL を設定する場合と同じです。その手順を簡単に説明します。ACL の設定に関する詳細は、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章の「Configuring IP Services」を参照してください。コマンドに関する詳細は、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

スイッチは、次の IOS ルータ ACL 関連機能をサポートしません。

- 非 IPv4 プロトコルの ACL（表 32-1 [p.32-8] を参照）またはブリッジグループ 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）
- 再帰 ACL またはダイナミック ACL（スイッチ クラスタリング機能で使用される一部の特殊なダイナミック ACL を除く）
- ポート ACL および VLAN マップに関する ACL ロギング

スイッチ上で 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。

ここでは次の内容について説明します。

標準および拡張 IP ACL の作成

ここでは、IP ACL について説明します。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、ACL 内の条件に対して 1 つずつ照合されます。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ると条件のテストを終了するので、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。

ソフトウェアは次に示す ACL タイプ、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照合処理を行います。
- 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照合処理を行います。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 リストの概要および作成方法について説明します。

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 32-1 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 32-1　アクセス リスト番号

アクセス リスト番号	Type	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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log**]	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。 *access-list-number* は 1 ～ 99 または 1300 ～ 1999 の 10 進数です。 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ため、**deny** または **permit** を入力します。 *source* 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。 • ドット付き 10 進表記による 32 ビットの数値 • *送信元*と*送信元ワイルドカード*の値 0.0.0.0 255.255.255.255 の短縮形であるキーワード **any**。送信元ワイルドカードを入力する必要はありません。 • 送信元と送信元ワイルドカードの値 *source* 0.0.0.0 の短縮形である **host** （任意）*source-wildcard* によって、ワイルドカード ビットが送信元に適用されます。 （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コンソールに送信されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 5	**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。

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、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）に来るように、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。コンソールに表示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。

作成した番号指定の標準 IP ACL は、端末回線（「端末回線への IP ACL の適用」[p.32-20] を参照）、インターフェイス（「インターフェイスへの IP ACL の適用」[p.32-20] を参照）、または VLAN（「VLAN マップの設定」[p.32-31] を参照）に適用できます。

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、照合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、番号指定の 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。

次の IP プロトコルがサポートされます（プロトコル キーワードはカッコ内の太字）。

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。

各プロトコルの特定のキーワードについての詳細は、次のソフトウェアの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） 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; タイプ オブ サービス）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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2a	**access-list** *access-list-number* {**deny** | **permit**} *protocol* *source source-wildcard* *destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log**] [**log-input**] [**time-range** *time-range-name*] [**dscp** *dscp*] **（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** を両方とも入力することができます。	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。 *access-list-number* は 100 ～ 199 または 2000 ～ 2699 の 10 進数です。 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、**deny** または **permit** を入力します。 *protocol* には、IP プロトコルの名前または番号（**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。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 **ip** を使用します。 **（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。 *source* 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。 *source-wildcard* 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。 *destination* 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。 *destination-wildcard* 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。

	コマンド	説明
		送信元、送信元ワイルドカード、宛先、宛先ワイルドカードは、次の 3 つの方法で指定することができます。 • 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 **any**（任意のホスト） • 単一のホスト 0.0.0.0 を表すキーワード **host** その他のキーワードは任意で、意味は次のとおりです。 • **precedence** — 0 ～ 7 の番号または名前で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、**routine**（0）、**priority**（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、および **network**（7）です。 • **fragments** — 先頭以外のフラグメントを確認します。 • **tos** — 0 ～ 15 の番号または名前で指定された 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、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、および **min-delay**（8）です。 • **log** — 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。**log-input** 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。 • **time-range** — 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.32-17）を参照してください。 • **dscp** — 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。
または	**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*]	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。 送信元 / 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。
または	**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*]	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。 送信元 / 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。

	コマンド	説明
ステップ 2b	**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*]	（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。 TCP の場合は **tcp** を入力します。 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。 （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**（等しい）、**gt**（より大きい）、**lt**（より小さい）、**neq**（等しくない）、**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）。 *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 ポート名を表示するには、疑問符（?）を入力するか、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章の「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。 その他のオプションのキーワードの意味は次のとおりです。 • **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	**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*]	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP の場合は、**udp** を入力します。 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*]] で指定する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。

	コマンド	説明
ステップ 2d	**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**] [**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の意味は次のとおりです。 • *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 タイプ名と ICMP メッセージのタイプおよびコード名を表示する場合は、疑問符（?）を入力するか、『*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	**access-list** *access-list-number* {**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	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リストの設定を確認します。
ステップ 5	**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。

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、それ以外のアクセスを許可する拡張アクセス リストを作成し、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。番号指定のアクセス 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。

作成した番号指定の拡張 ACL は、端末回線（「端末回線への IP ACL の適用」[p.32-20] を参照）、インターフェイス（「インターフェイスへの IP ACL の適用」[p.32-20] を参照）、または VLAN（「VLAN マップの設定」[p.32-31] を参照）に適用できます。

ACL での ACE の再順番付け

Cisco IOS Release 12.2(25)EY およびそれ以降では、新規 ACL を作成すると、アクセス リストのエントリのシーケンス番号は自動的に生成されます。ACL のシーケンス番号を編集し、ACE が適用される順番を変更するには、**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用します。たとえば、ACL に新規 ACE を追加した場合、リストの一番後ろに置かれます。シーケンス番号を変更することで、ACE を ACL 内の別の位置に移動できます。

ip access-list resequence コマンドに関する詳細は、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a60.html

名前指定の標準および拡張 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 リストの場合より多くの IP アクセス リストをルータに設定できます。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かぎりません。

（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。

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 を指定できるとはかぎりません。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することができます。
- 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.32-7] 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）を使用できます。

名前指定の標準 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**ip access-list standard** *name*	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）　名前は 1 ～ 99 の番号にすることができます。
ステップ 3	**deny** {*source* [***source-wildcard***] | **host** *source* | **any**} [**log**] または **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**]	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。 • **host** *source* — 送信元と送信元ワイルドカードの値 *source* 0.0.0.0 • **any** — 送信元と送信元ワイルドカードの値 0.0.0.0 255.255.255.255
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	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**	（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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**ip access-list extended** *name*	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）　名前は 100 ～ 199 の番号にすることができます。
ステップ 3	{**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*]	アクセス リスト コンフィギュレーション モードで、許可または拒否する条件を指定します。**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。 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.32-10）を参照してください。 • **host** *source* — 送信元と送信元ワイルドカードの値 *source* 0.0.0.0 • **host** *destination* — 宛先と宛先ワイルドカードの値 *destination* 0.0.0.0 • **any** — 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 0.0.0.0 255.255.255.255
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。

	コマンド	説明
ステップ 6	**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 の作成後に追加された ACE は、リストの末尾に配置されます。特定の ACL では個別に ACE 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。

作成した名前指定の ACL はインターフェイス（「インターフェイスへの IP ACL の適用」[p.32-20]を参照）または VLAN（「VLAN マップの設定」[p.32-31] を参照）に適用できます。

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間（指定期間内、指定曜日など）を定義することができます。**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.32-7）および「名前指定の標準および拡張 ACL の作成」（p.32-15）に記載されている、名前指定および番号指定の拡張 ACL の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一部を次に示します。

- 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することができます。

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、Ternary CAM（TCAM）にロードされた結合済みの設定と統合する必要があるためです。このため、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を行わないように、注意する必要があります。

（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; ネットワーク タイム プロトコル）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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**time-range** *time-range-name*	作成する時間範囲には意味のある名前（*workhours* 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	**absolute** [**start** *time date*] [**end** *time date*] または **periodic** *day-of-the-week hh:mm to* [*day-of-the-week*] *hh:mm* または **periodic** {**weekdays** | **weekend** | **daily**} *hh:mm to hh:mm*	時間範囲を適用する機能が作動する時間を指定します。 • 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することができます。 設定例を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show time-range**	設定した時間範囲を確認します。
ステップ 6	**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。

異なる時刻に有効となるように設定する項目が複数ある場合は、このステップを繰り返します。

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。

次に、営業時間（*workhours*）および 2005 年 1 月 1 日の休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_2003 (inactive)
   absolute start 00:00 01 January 2003 end 23:59 01 January 2003
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、時間範囲を実行できる拡張 ACL 内に、時間範囲名を入力します。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_2003 (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 deny_access
    10 deny tcp any any time-range new_year_day_2003 (inactive)
=Extended IP access list may_access
    10 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 に追加することができます。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、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、ステートメントのあと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、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ていますが、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ています。

```
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 のサブネットは発信 Telnet の使用が禁止されています。

```
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
```

端末回線への IP ACL の適用

番号指定の ACL を使用すると、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。端末回線には名前指定の 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、すべての仮想端末回線に同一の制限を設定する必要があります。

インターフェイスに ACL を適用する手順については、「インターフェイスへの IP ACL の適用」（p.32-20）を参照してください。VLAN に ACL を適用する手順については、「VLAN マップの設定」（p.32-31）を参照してください。

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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**line** [**console** | **vty**] *line-number*	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。 • **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、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。
ステップ 3	**access-class** *access-list-number* {**in** | **out**}	特定の仮想端末回線（デバイス側）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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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**	（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。

端末回線から ACL 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。

インターフェイスへの IP ACL の適用

ここでは、ネットワーク インターフェイスに IP ACL を適用する手順について説明します。レイヤ 3 インターフェイスの場合は、ACL を着信または発信のいずれかの方向に適用できます。レイヤ 2 インターフェイスの場合は、ACL を着信方向にのみ適用できます。次の注意事項を考慮してください。

- インターフェイスへのアクセスを制御する場合は、名前指定または番号指定の ACL を使用することができます。
- 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 2 ポートに着信したパケットは、常にポート ACL でフィルタリングされます。
- 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（簡易ネットワーク管理プロトコル）、Telnet、Web トラフィックなど、CPU で処理され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。

（注）　パケットがアクセス グループによって拒否された場合、デフォルトでは、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これらのパケットはハードウェアで廃棄されず、スイッチの CPU にブリッジングされて、ICMP 到達不能メッセージを生成します。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**interface** *interface-id*	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**}	指定したインターフェイスへのアクセスを制御します。 **out** キーワードは、レイヤ 2 インターフェイス（ポート ACL）ではサポートされていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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**	（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 gigabitethernet1/0/2
Switch(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、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 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、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に、スイッチはパケットを ACL と照合します。ACL によってパケットが許可された場合、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。

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することができます。

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で処理する必要があります。ハードウェアの容量が満杯になり、ACL 設定を保存できなくなると、パケットは CPU に送信されて転送されます。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。

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** キーワードを使用する。
- ICMP 到達不能メッセージを生成する。

トラフィック フローのロギングと転送の両方を行う場合、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能力が異なるため、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。

ルータ ACL の設定をハードウェアに適用できない場合、VLAN に着信したルーティング対象パケットはソフトウェアでルーティングされますが、ブリッジングはハードウェアで行われます。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。

show ip access-lists 特権 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。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 access-lists hardware counters** 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、アクセス制御のセキュリティを強化します。
- *ip unreachables* 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*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*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。

IP ACL の設定例

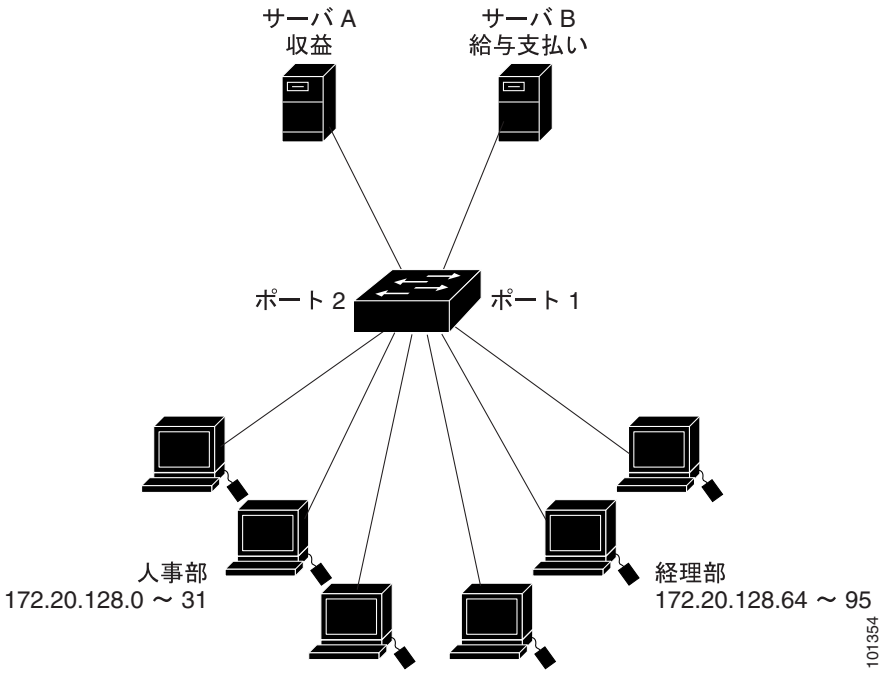
ここでは、IP ACL の設定例および適用例を示します。ACL の編集に関する詳細は、『*Cisco IOS Security Configuration Guide*』Release 12.2 および『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章の「Configuring IP Services」を参照してください。

図 32-3 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収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

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

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

図 32-3　ルータ ACL によるトラフィックの制御



次に、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する例を示します。この ACL は、指定された送信元アドレスからルーテッド ポート 1 を通って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
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 6 out
```

次に、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
    10 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet1/0/1
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 アドレス 36.0.0.0 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 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 はインターフェイス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 gigabitethernet1/0/1
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 gigabitethernet1/0/1
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があり、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考えます。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するとします。

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。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。指定されたインターフェイスは、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 gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

名前指定 ACL

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。

```
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て、その他の TCP トラフィックを拒否します。また、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。

```
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インターフェイスに適用されます。*Internet_filter* ACL は発信トラフィックに、*marketing_group* ACL は着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet1/0/2
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

次に、月曜から金曜の午前 8 時～午後 6 時（18:00）の間、IP の HTTP トラフィックを拒否する例を示します。また、土曜および日曜の正午～午後 8 時（20:00）の間のみ、UDP トラフィックを許可します。

```
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 fastethernet1/0/1
Switch(config-if)# ip access-group strict in
```

コメント付きの IP ACL エントリ

次に示す番号指定の 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
```

次に示す番号指定の ACL の例では、Winter および Smith のワークステーションは 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
```

次に示す名前指定の ACL の例では、Jones のサブネットは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
```

次に示す名前指定の ACL の例では、Jones のサブネットは発信 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

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 gigabitethernet1/0/1
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
```

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 gigabitethernet1/0/2
Switch(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、ACL 種類や一致したアクセス エントリ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 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、他の名前指定の拡張 ACL の場合と同様です。

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

mac access-list extended コマンドでサポートされている非 IPv4 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** はコマンドラインのヘルプに表示されますが、**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ません。

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

	コマンド	説明
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。
ステップ 2	**mac access-list extended** *name*	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 3	{**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*]	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（**any**）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（**host**）送信元 MAC アドレス、およびあらゆる（**any**）宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、**permit** または **deny** を指定します。 （任意）次のオプションを入力することもできます。 • *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。EtherType に適用される無視（*don't care*）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。 • **lsap** *lsap mask* — 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（*don't care*）ビットの任意のマスクが付加されます。 • **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** *cos* — プライオリティを設定するために使用される、0 ～ 7 の IEEE 802.1p サービス コスト番号
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	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**	（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 IPv4 トラフィックをフィルタリングすることができます。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。

- 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 2 ポートに着信したパケットは、常にポート ACL でフィルタリングされます。
- 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。IP アクセス リストは IPv4 パケットのみをフィルタリングし、MAC アクセス リストは非 IPv4 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、前に設定した ACL が新しい ACL に置き換わります。

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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**interface** *interface-id*	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	**mac access-group** {*name*} {**in**}	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	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show mac access-group** [**interface** *interface-id*]	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	**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。

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*} 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 gigabitethernet1/0/2
Switch(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。EtherChannel ポート チャネルでは、このコマンドを使用できません。

スイッチは受信したパケットを入力 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 が適用されていない場合と同様に処理を行い、すべてのパケットが許可されます。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 マップ内に該当タイプのパケット（IP または MAC）に対する match 句が存在する場合、デフォルトではマップ内のどのエントリにも一致しないパケットが廃棄されます。該当タイプのパケットに対する match 句が存在しない場合、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 MAC 拡張 ACL を作成します。「標準および拡張 IP ACL の作成」（p.32-7）および「VLAN マップの作成」（p.32-32）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、**action** として **forward**（デフォルト）または **drop** を任意で入力します。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 IPv4 パケットまたは非 IPv4 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）とパケットを照合することもできます。

（注）　VLAN マップがパケット タイプ（IP または MAC）の match 句で設定されており、マップ アクションが drop の場合は、該当するタイプのパケットがすべて廃棄されます。VLAN マップに match 句がなく、設定されているアクションが drop の場合は、すべての IP パケットおよびレイヤ 2 パケットが廃棄されます。

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。

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

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。

- トラフィックを拒否するように設定された ACL がインターフェイスに存在せず、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 マップではエントリの順序が重要です。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 句が 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 句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 句が 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。
- VLAN マップのロギングはサポートされません。
- 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をソフトウェアでブリッジングおよびルーティングする必要があります。
- 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 リストが適用されている場合に、ポートが属する VLAN に VLAN マップを適用した場合、このポートの ACL は VLAN マップよりも優先されます。
- 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.32-35）を参照してください。
- ルータ ACL および VLAN マップを組み合わせて使用する方法については、「注意事項」（p.32-38）を参照してください。

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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**vlan access-map** *name* [*number*]	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することができます。 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	**action** {**drop** | **forward**}	（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。
ステップ 4	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]	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 IPv4 パケットは、名前指定 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	**end**	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	説明
ステップ 6	**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**	（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 の permit キーワードは一致を意味します。ACL の deny キーワードは一致しないことを意味します。

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 句が存在するため、デフォルトではどの match 句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。*ip2* ACL 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。このマップでは、これ以前のどの ACL 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。

```
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
```

例 2

次の例の VLAN マップには、IP パケットの廃棄および MAC パケットの転送というデフォルト アクションがあります。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 IPv4 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 マップには、MAC パケットの廃棄および IP パケットの転送というデフォルト アクションがあります。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 IPv4 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 マップには、すべてのパケット（IPv4 および非 IPv4）が廃棄されるデフォルト アクションがあります。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、特権 EXEC モードで次の手順を実行します。

	コマンド	説明
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。
ステップ 2	**vlan filter** *mapname* **vlan-list** *list*	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	**show running-config**	アクセス リストの設定を表示します。
ステップ 4	**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 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。

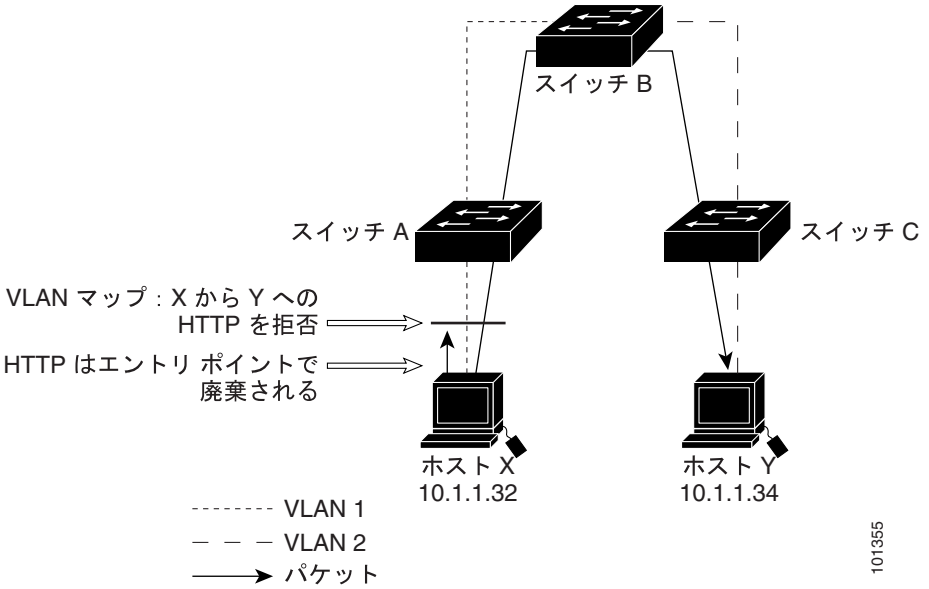
- ワイヤリング クローゼットの構成（p.32-35）
- 別の VLAN にあるサーバへのアクセスの拒否（p.32-37）

ワイヤリング クローゼットの構成

ワイヤリング 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 32-4 では、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 32-4　ワイヤリング 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 にブリッジングされず、すべてスイッチ A で廃棄されるようにスイッチ A の VLAN マップを設定することができます。

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。

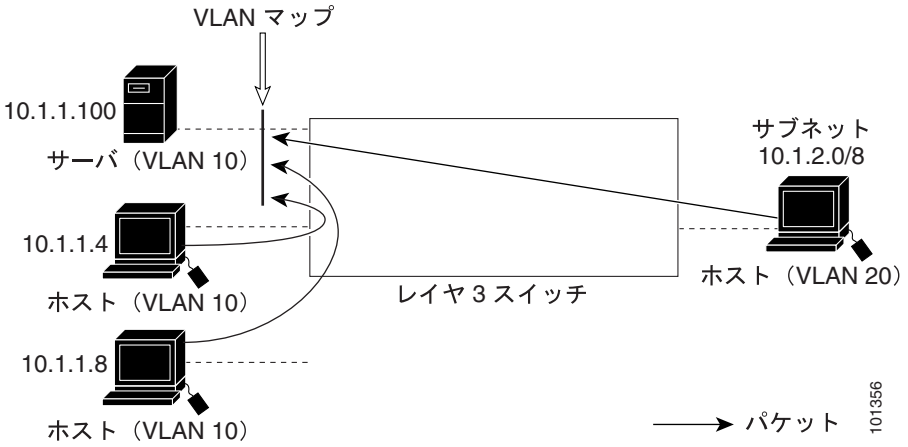
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN にあるサーバへのアクセスの拒否

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 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（図 32-5 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 32-5　別の VLAN にあるサーバへのアクセス拒否



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 へ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 を VLAN マップと組み合わせて使用する方法

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制御する VLAN マップを定義したりすることができます。

パケット フローが ACL 内 VLAN マップの deny 句と一致した場合、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。

パケット タイプ（IP または MAC）に対する match 句が VLAN マップに存在する場合、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 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。

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。

- 注意事項（p.32-38）
- VLAN に適用されるルータ ACL と VLAN マップの例（p.32-39）

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。

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 の数が膨大になる場合があります。

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 インターフェイスの方向（入力および出力）ごとに、設定できる VLAN マップおよびルータ ACL は 1 つのみです。
- 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。可能なかぎり、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。

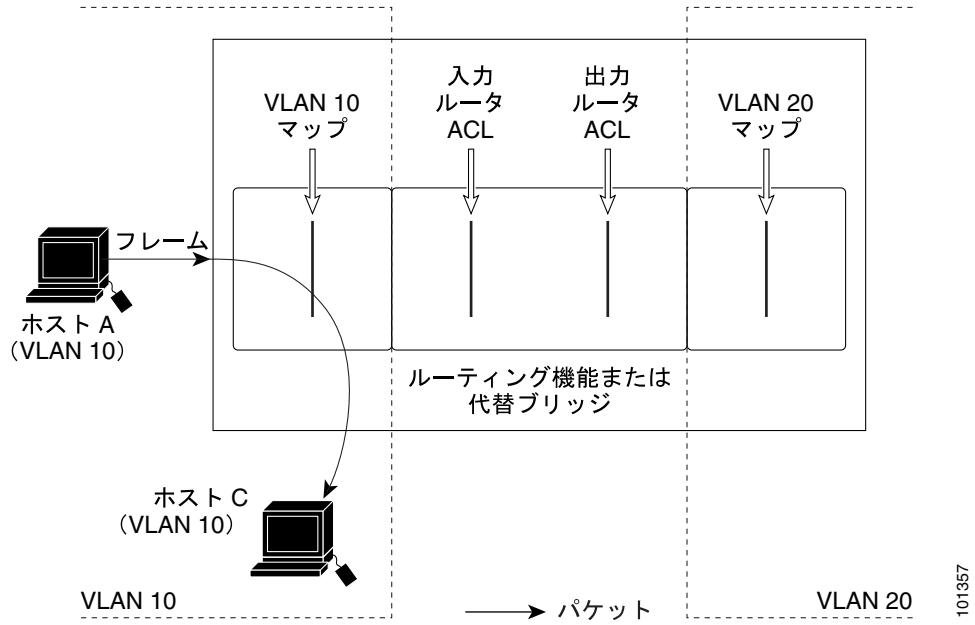
VLAN に適用されるルータ ACL と VLAN マップの例

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可能性もあります。

ACL およびスイッチド パケット

図 32-6 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。

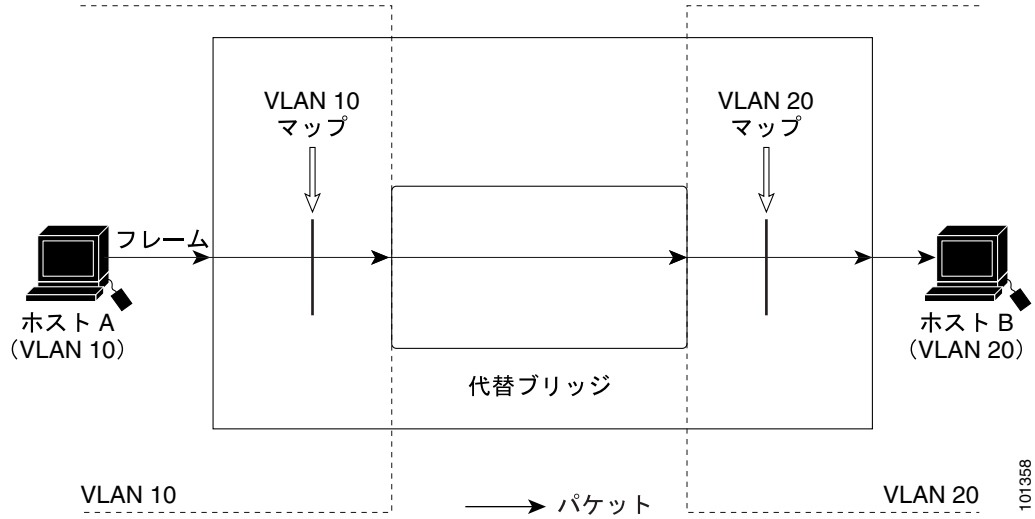
図 32-6　スイッチド パケットへの ACL の適用



ACL およびブリッジド パケット

図 32-7 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 IPv4 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 32-7　ブリッジド パケットへの ACL の適用

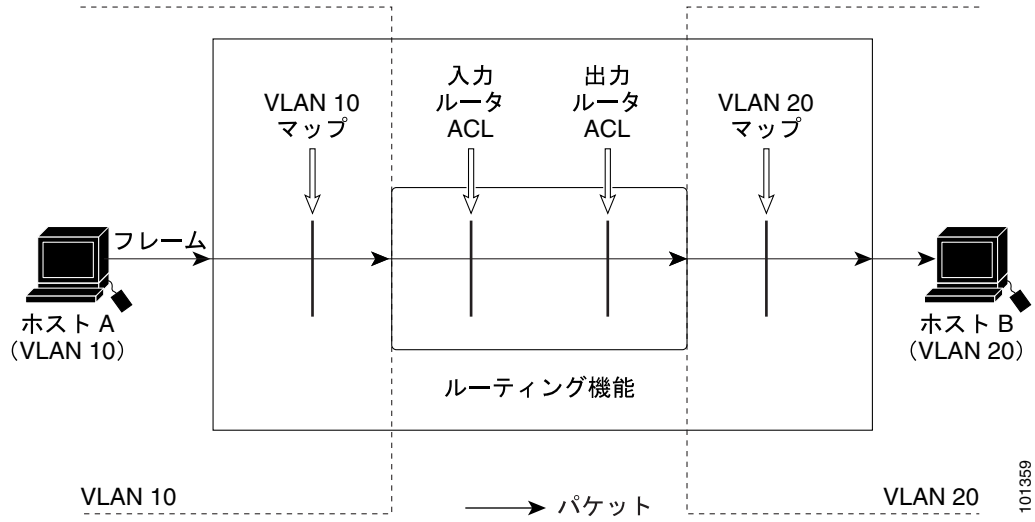


ACL およびルーテッド パケット

図 32-8 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 32-8　ルーテッド パケットへの ACL の適用

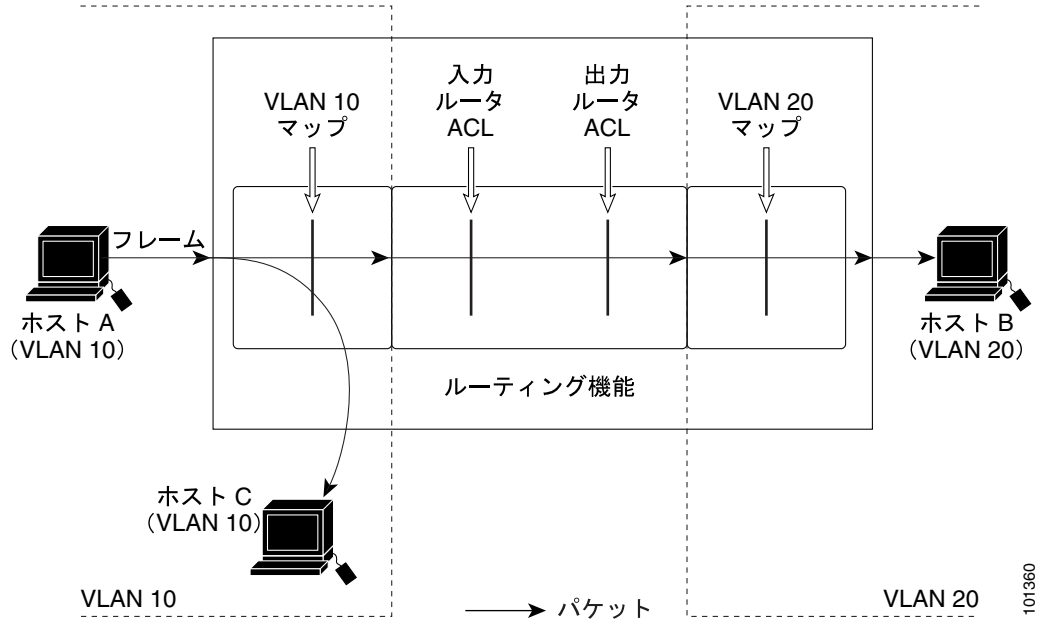


ACL およびマルチキャスト パケット

図 32-9 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る場合がありますが、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 32-9 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 32-9　マルチキャスト パケットへの ACL の適用



ACL の設定の表示

スイッチ上に設定されている ACL、およびインターフェイスや VLAN に適用された ACL を表示することができます。

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 グループを表示することができます。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、特権 EXEC コマンドを使用します（表 32-2 を参照）。

表 32-2　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	説明
show access-lists [*number* | *name*]	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。
show ip access-lists [*number* | *name*]	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。
show ip interface *interface-id*	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、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	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。
show mac access-group [**interface** *interface-id*]	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。

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することもできます。VLAN マップ情報を表示するには、表 32-3 に記載された特権 EXEC コマンドを使用します。

表 32-3　VLAN マップ情報を表示するコマンド

コマンド	説明
show vlan access-map [*mapname*]	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。
show vlan filter [**access-map** *name* | **vlan** *vlan-id*]	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。