CHAPTER 35

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-E または 3560-E スイッチ上でネットワーク セキュリティを設定する方法について説明します。コマンドおよび表の中では、ACL の意味でアクセス リストという言葉を使用しています。特に明記しないかぎり、*スイッチ*という用語は Catalyst 3750-E または 3560-E スタンドアロン スイッチおよび Catalyst 3750-E スイッチ スタックを意味します。

（注） この章に記載されている IP ACL の情報は、IP Version 4（IPv4）のものです。IPv6 ACL の詳細については、第 36 章「IPv6 ACL の設定」を参照してください。

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、このリリースに対応するコマンド リファレンス、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の章の「Configuring IP Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services,Release 12.4*』を参照してください。

Catalyst 3750-E および 3560-E スイッチはまた、Cisco TrustSec Security Group Tag（SCT）Exchange Protocol（SXP）もサポートします。この機能は、IP アドレスに対してではなく、デバイスのグループに対して ACL ポリシーを定義する Security Group Access Control List（SGACL; セキュリティ グループ ACL）をサポートします。SXP 制御プロトコルは、ハードウェアをアップグレードせずに SCT によってパケットをタギングするためのプロトコルで、Cisco TrustSec ドメイン エッジにあるアクセス レイヤ デバイスと、Cisco TrustSec ドメイン内の配信レイヤ デバイスの間で実行されます。Catalyst 3750-E および 3560-E スイッチは、Cisco TrustSec ネットワーク内でアクセス レイヤ スイッチとして動作します。

Cisco TrustSec の詳細については、次の URL にある『Cisco TrustSec Switch Configuration Guide』を参照してください。
http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

SXP に関する各項では、Catalyst 3750-E および 3560-E スイッチでサポートされている機能について説明します。

この章で説明する内容は、次のとおりです。

- 「ACL の概要」（P.35-2）
- 「IPv4 ACL の設定」（P.35-7）
- 「名前付き MAC 拡張 ACL の作成」（P.35-28）
- 「VLAN マップの設定」（P.35-31）
- 「ルータ ACL を VLAN マップと組み合せて使用する方法」（P.35-40）
- 「IPv4 ACL の設定の表示」（P.35-44）

ACL の概要

パケット フィルタリングによって、ネットワーク トラフィックを限定し、さらに特定のユーザまたはデバイスに使用させるネットワークを制限できます。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条件および拒否条件を集めて順番に並べたものです。パケットがインターフェイスに着信すると、スイッチはパケットのフィールドと適用される ACL を比較し、アクセス リストに指定されている条件に基づいて、転送に必要な許可がパケットに与えられているかどうかを調べます。スイッチはパケットをアクセス リスト内の条件に対して 1 つずつテストします。最初に一致した条件によって、スイッチがパケットを許可するかまたは拒否するかが決まります。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。いずれの条件とも一致しなかった場合、スイッチはパケットを拒否します。制限がない場合、スイッチはパケットを転送し、制限がある場合はパケットをドロップします。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、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。ACL を設定しないと、スイッチを通過するパケットはすべて、ネットワークのすべての部分に伝送される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送は許可し、Telnet トラフィックは許可しないといったことが可能です。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）を順番に指定したリストが含まれます。ACE ごとに、*permit* または *deny*、および ACE と一致するためにパケットが満たさなければならない一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって異なります。

スイッチは、次の IP ACL およびイーサネット（MAC（メディア アクセス コントロール））ACL をサポートします。

- IP ACL は、TCP、UDP、Internet Group Management Protocol（IGMP）、Internet Control Message Protocol（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は、非 IP トラフィックをフィルタリングします。

このスイッチでは、QoS（Quality of Service）分類 ACL もサポートされています。詳細については、「QoS ACL に基づく分類」（P.37-8）を参照してください。

ここでは、次の概要について説明します。

- 「サポートされる ACL」（P.35-2）
- 「分割トラフィックおよび非分割トラフィックの処理」（P.35-6）
- 「ACL およびスイッチ スタック」（P.35-7）

サポートされる ACL

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

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックのアクセスを制御します。スイッチでは、発信方向のポート ACL はサポートしません。1 つのレイヤ 2 インターフェイスには、1 つの IP アクセス リストと 1 つの MAC アクセス リストだけを適用できます。詳細については、「ポート ACL」（P.35-3）を参照してください。
- 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、特定の方向（着信または発信）のレイヤ 3 インターフェイスに適用されます。詳細については、「ルータ ACL」（P.35-4）を参照してください。

- 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、IPv4 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。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセス制御されます。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 ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。詳細については、「VLAN マップ」（P.35-5）を参照してください。

同じスイッチ上で入力ポート ACL、ルータ ACL、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 だけ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、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 マップだけによって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 だけ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、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 マップだけによってフィルタリングされます。

インターフェイスで IEEE 802.1Q トンネリングを設定している場合、トンネル ポートで受信した IEEE 802.1Q カプセル化 IP パケットは、MAC ACL によってフィルタリングされますが、IP ACL ではフィルタリングされません。これは、IEEE 802.1Q ヘッダー内のプロトコルをスイッチが認識しないからです。この制限事項は、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 17 章「IEEE 802.1Q トンネリングの設定」および第 17 章「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。

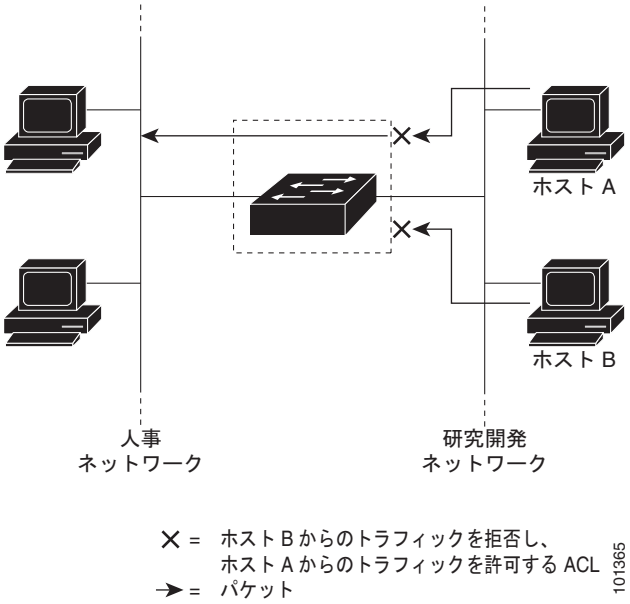
ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は、物理インターフェイス上でだけサポートされるため、EtherChannel インターフェイスではサポートされません。また、ポート ACL は着信方向のインターフェイス上にだけ適用できます。次のアクセス リストがサポートされています。

- 送信元アドレスを使用する標準 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

スイッチは、特定のインターフェイス上に設定されている着信方向のすべての機能に関連した ACL をテストし、パケットが ACL 内のエントリ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。この方法の場合、ACL は、ネットワークまたは一部のネットワークへのアクセスを制御します。図 35-1 に、ポート ACL を使用して、すべてのワークステーションが同一の VLAN にある場合のネットワーク アクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2 インターフェイスにだけ適用されます。

図 35-1　　ACL を使用したネットワーク トラフィックの制御



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 の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 リストの両方を適用すると、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、前に設定した ACL が新しい ACL に置き換えられます。

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 を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

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、照合されます。

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

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

ポート ACL の場合と同様、スイッチは特定の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 と照合します。ただし、ルータ ACL は双方向でサポートされています。パケットがインターフェイスのスイッチに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス制御が行えます。図 35-1 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が許可されますが、ホスト B は拒否されます。

VLAN マップ

VLAN ACL または VLAN マップを使用して、*すべて*のトラフィックをアクセス制御できます。VLAN との間でルーティングされる、またはスイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用します。

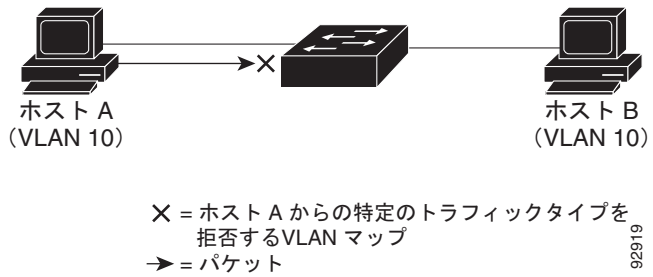
VLAN マップはセキュリティ パケット フィルタリングに使用してください。VLAN マップで方向（着信または発信）は定義されません。

VLAN マップを設定して、IPv4 トラフィックのレイヤ 3 アドレスを照合できます。

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 *できません*）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

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 35-2 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。各 VLAN には、VLAN マップを 1 つだけ適用できます。

図 35-2　VLAN マップによるトラフィックの制御



分割トラフィックおよび非分割トラフィックの処理

IP パケットは、ネットワークを通過中に分割されることがあります。分割された場合、TCP または UDP ポート番号、ICMP タイプ、コードなどのレイヤ 4 情報が格納されているのは、パケットの先頭部分が含まれるフラグメントだけです。他のいずれのフラグメントにも、この情報は格納されません。

一部の ACE はレイヤ 4 情報を調べないため、すべてのパケット フラグメントに適用できます。ただし、通常の方法では、レイヤ 4 情報をテストする ACE は分割された 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。フラグメントにレイヤ 4 情報が含まれず、ACE が一部のレイヤ 4 情報を調べる場合には、一致ルールが次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP、UDP などのプロトコル タイプを含む）を調べる許可 ACE は、格納されていないレイヤ 4 情報に関係なく、フラグメントに一致すると見なされます。
- レイヤ 4 情報を調べる拒否 ACE は、フラグメントにレイヤ 4 情報が格納されていないかぎり、フラグメントと一致することはありません。

次のコマンドで設定されたアクセス リスト 102 が 3 つのフラグメント パケットに適用されたとします。

```
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 1 番めおよび 2 番めの ACE で、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、それぞれ Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）および Telnet に対応する Well-known 番号の有無をテストするという意味です。

- パケット A は、ホスト 10.2.2.2 のポート 65000 から SMTP ポート上のホスト 10.1.1.1 へ送信される TCP パケットです。このパケットが分割される場合、最初のフラグメントは、すべてのレイヤ 4 情報が格納されているので、完全なパケットの場合と同様、最初の ACE（許可）と一致します。最初の ACE はフラグメント適用時にレイヤ 3 情報だけを調べるため、SMTP ポート情報の有無にかかわらず残りのフラグメントも最初の ACE と一致します。この例の情報は、パケットが TCP で宛先が 10.1.1.1 ということです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 から Telnet ポート上のホスト 10.1.1.2 へ送信される TCP パケットです。このパケットが分割される場合、すべてのレイヤ 3 情報とレイヤ 4 情報が存在するため、最初のフラグメントは 2 番めの ACE（拒否）と一致します。パケットの残りのフラグメントは、レイヤ 4 情報がないので、2 番めの ACE と一致しません。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たので、ホスト 10.1.1.2 は完全なパケットを再び組み立てることができず、パケット B は事実上、拒否されます。ただし、許可されたあとのフラグメントがパケットを再び組み立てるときに、ネットワーク帯域幅とホスト 10.1.1.2 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される場合、最初のフラグメントは 4 番めの ACE（拒否）と一致します。他のフラグメントもすべて、4 番めの ACE と一致します。この ACE はレイヤ 4 情報を調べず、すべてのフラグメントに含まれているレイヤ 3 情報から、ホスト 10.1.1.3 に送信中であったことが認識され、前の許可 ACE は別のホストをチェックしていたということがわかるためです。

ACL およびスイッチ スタック

スイッチ スタックの ACL サポート機能は、スタンドアロン スイッチの場合と同じです。ACL の設定情報は、スタック内のすべてのスイッチに伝播されます。スタック マスターを含むスタック内のすべてのスイッチは、情報を処理し、ハードウェアをプログラミングします（スイッチ スタックの詳細については、第 5 章「スイッチ スタックの設定」を参照してください）。

スタック マスターは、次に示す ACL 機能を実行します。

- ACL 設定を処理し、情報をすべてのスタック メンバーに伝播します。
- ACL 情報を、スタックに加入しているすべてのスイッチに配信します。
- 何らかの理由でパケットをソフトウェアで転送する必要がある場合（ハードウェア リソースが不足している場合など）、マスター スイッチはパケットに ACL を適用したあとにだけ、パケットを転送します。
- 処理する ACL 情報を使用して、ハードウェアをプログラミングします。

スタック メンバーは、次に示す ACL 機能を実行します。

- マスター スイッチから ACL 情報を受け取り、ハードウェアをプログラミングします。
- スタンバイ スイッチとして機能します。既存のマスター スイッチに障害が発生した場合、新規スタック マスターに選択されたスタック メンバーは、スタック マスターの役割を引き継ぐことができます。

スタック マスターに障害が発生し、新規スタック マスターが選択された場合、新規に選択されたマスターはバックアップされた実行コンフィギュレーションを解析し直します（第 5 章「スイッチ スタックの設定」を参照）。実行コンフィギュレーションの一部である ACL 設定も、この時に解析し直されます。新規スタック マスターは、ACL 情報をスタック内のすべてのスイッチに配信します。

IPv4 ACL の設定

スイッチに IPv4 ACL を設定する手順は、Cisco スイッチおよびルータに IPv4 ACL を設定する場合と同じです。ここでは、手順を簡単に説明します。ACL の設定に関する詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』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については、『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.4*』を参照してください。

スイッチがサポートしない Cisco IOS ルータ ACL 関連の機能は、次のとおりです。

- 非 IP プロトコル ACL（表 35-1（P.35-8）を参照）またはブリッジ グループ ACL
- IP アカウンティング
- 着信および発信レート制限（QoS ACL は除く）
- 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が使用する一部の特殊なダイナミック ACL は除く）
- 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 リストの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、次の設定情報について説明します。

- 「標準および拡張 IPv4 ACL の作成」（P.35-8）
- 「端末回線への IPv4 ACL の適用」（P.35-19）
- 「インターフェイスへの IPv4 ACL の適用」（P.35-20）
- 「IP ACL のハードウェアおよびソフトウェアの処理」（P.35-22）
- 「ACL のトラブルシューティング」（P.35-23）
- 「IPv4 ACL の設定例」（P.35-23）

標準および拡張 IPv4 ACL の作成

ここでは、IP ACL について説明します。ACL は許可条件と拒否条件を集めて順番に並べたものです。スイッチはパケットをアクセス リスト内の条件に対して 1 つずつテストします。最初に一致した条件によって、スイッチがパケットを許可するかまたは拒否するかが決まります。スイッチは最初に一致した時点でテストを中止するので、条件の指定順序が重要です。いずれの条件とも一致しなかった場合、スイッチはパケットを拒否します。

ソフトウェアは IPv4 用に、次に示すタイプの ACL、つまりアクセス リストをサポートします。

- 標準 IP アクセス リストでは、送信元アドレスを使用して照合します。
- 拡張 IP アクセス リストでは、送信元アドレスおよび宛先アドレスを使用して照合し、オプションとしてプロトコル タイプ情報を使用して、より細かな制御を行います。

ここでは、アクセス リストの概要、およびアクセス リストの作成方法について説明します。

- 「アクセス リスト番号」（P.35-8）
- 「ACL のロギング」（P.35-9）
- 「スマート ロギング」（P.35-9）
- 「番号制標準 ACL の作成」（P.35-10）
- 「番号制拡張 ACL の作成」（P.35-11）
- 「ACL 内の ACE シーケンスの再編集」（P.35-15）
- 「名前付き標準および拡張 ACL の作成」（P.35-15）
- 「ACL での時間範囲の使用法」（P.35-17）
- 「ACL へのコメントの挿入」（P.35-19）

アクセス リスト番号

ACL を表すために使用する番号は、作成するアクセス リストのタイプを示します。表 35-1 に、アクセス リスト番号と対応するアクセス リスト タイプ、およびスイッチがサポートするかどうかを示します。スイッチは、IPv4 標準および IPv4 拡張アクセス リスト（番号 1 ～ 199 および 1300 ～ 2699）をサポートします。

表 35-1　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
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

表 35-1　アクセス リスト番号 （続き）

アクセス リスト番号	タイプ	サポート
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）　番号制標準および拡張 ACL のほかに、サポートされている番号を使用することによって、名前付き標準および拡張 IP ACL を作成することもできます。標準 IP ACL の名前は 1 ～ 99、拡張 IP ACL の名前は 100 ～ 199 にできます。番号制リストの代わりに名前付き ACL を使用した場合、名前付きリストからエントリを個別に削除できるという利点があります。

ACL のロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、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。

スマート ロギング

スイッチでスマート ロギングがイネーブルであり、スマート ロギングで設定された ACL がレイヤ 2 インターフェイス（ポート ACL）に割り当てられている場合、ACL に従って拒否または許可されたパケットの内容は NetFlow 収集装置にも送信されます。スマート ロギングの詳細については、「スマート ロギングの設定」（P.32-15）を参照してください。

番号制標準 ACL の作成

番号制標準 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	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。
ステップ 2	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*] [**log** | **smartlog**]	送信元アドレスおよびワイルドカードを使用して、標準 IPv4 アクセス リストを定義します。 *access-list-number* は、1 ～ 99 または 1300 ～ 1999 の 10 進数です。 **deny** または **permit** を入力し、条件と一致した場合にアクセスを拒否するのか、それとも許可するのかを指定します。 *source* は、パケットが送られてくるネットワークまたはホストの送信元アドレスです。次のように指定されます。 • ドット付き 10 進表記で 32 ビットの値 • 0.0.0.0 255.255.255.255 という **source** および *source-wildcard* の省略形を表すキーワード *any*。source-wildcard の入力は不要です。 • **source** 0.0.0.0 という source および source-wildcard の省略形を表すキーワード *host* （任意）*source-wildcard* によって、ワイルドカード ビットが source 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。 （任意）**smartlog** を指定すると、拒否または許可されたパケットのコピーが NetFlow 収集装置に送信されます。 **（注）** ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。スマート ロギングは、レイヤ 2 インターフェイスに割り当てられた ACL でだけサポートされます。
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 全体を削除する場合は、**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。番号制アクセス リストから ACE を個別には削除できません。

（注） ACL を作成するときは、ACL の末尾に暗黙の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。標準アクセス リストで、対応する IP ホスト アドレスの ACL 仕様からマスクを省略した場合、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、それ以外のすべてのホストへのアクセスを許可する標準 ACL を作成し、その結果を表示する例を示します。

```
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 一致条件を指定されたエントリ、および 0.0.0.0 の無視（*don't care*）マスクを指定されたエントリが、リストの先頭（ゼロ以外の無視（*don't care*）マスクを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 リストの順序に常に書き換えられます。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 ファイルでは、ACE は必ずしも入力した順番に表示されません。

作成した番号制標準 IPv4 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.35-19）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.35-20）を参照）、または VLAN（「VLAN マップの設定」（P.35-31）を参照）に適用できます。

番号制拡張 ACL の作成

標準 ACL の場合、一致基準には送信元アドレスだけが使用されますが、拡張 ACL では送信元および宛先アドレスとともに、オプションとしてプロトコル タイプ情報を使用して照合できるので、より細かな制御が可能です。番号制拡張アクセス リストで ACE を作成する場合、ACL の作成後に追加したものは、リストの末尾に組み込まれることに注意してください。番号制リストの場合、リストを並べ替えたり、ACE を選択して追加したり削除したりはできません。

プロトコルによっては、そのプロトコルに適用される特定のパラメータおよびキーワードもあります。

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**）、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できます。

各プロトコルの特定のキーワードに関する詳細については、次のコマンド 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 12.4*』
- 『*Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols, Release 12.4*』
- 『*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast, Release 12.4*』

（注） スイッチは、ダイナミック アクセス リストまたは再帰アクセス リストをサポートしていません。また、minimize-monetary-cost 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していません。

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 IP というカテゴリにグループ化できます。

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	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。
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**] | **smartlog**] [**time-range** *time-range-name*] [**dscp** *dscp*] **（注）** **dscp** 値を入力した場合は、**tos** または **precedence** を入力できません。**dscp** を入力しない場合は、**tos** と **precedence** を両方とも入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* は、100 ～ 199 または 2000 ～ 2699 の 10 進数です。 **deny** または **permit** を入力し、条件と一致した場合にパケットを拒否するか、または許可するかを指定します。 *protocol* には、IP プロトコルの名前または番号を入力します。指定には **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 IP（ICMP、TCP、および UDP を含む）と照合する場合は、キーワード **ip** を使用します。 **（注）** このステップでは、ほとんどの IP プロトコルに対応するオプションを指定します。TCP、UDP、ICMP、および 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* によって、ワイルドカード ビットが source に適用されます。 *destination* は、パケットの宛先ネットワークまたはホストの番号です。 *destination-wildcard* によって、ワイルドカード ビットが destination に適用されます。 source、source-wildcard、destination、および destination-wildcard は、次の 3 つの方法で指定できます。 • ドット付き 10 進表記で 32 ビットの値 • 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あり、次の意味があります。 • **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て、パケットを照合します。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）、**network**（**7**）です。 • **fragments**：先頭以外のフラグメントをチェックします。 • **tos**：0 ～ 15 の番号または名前で指定された ToS レベルを使用して照合します。使用できる名前および番号は、**normal**（**0**）、**max-reliability**（**2**）、**max-throughput**（**4**）、**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。 • **smartlog**：拒否または許可されたパケットのコピーを NetFlow 収集装置に送信するためにスマート ロギングがグローバルでイネーブルな場合に指定します。 • **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.35-17）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。

	コマンド	目的
または	**access-list** *access-list-number* {**deny** | permit} *protocol* any any [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**log** [**log-input**] | **smartlog**] [**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、source と source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用するか、または destination と destination-wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。 送信元と宛先のアドレスおよび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**] | **smartlog**] [**time-range** *time-range-name*] [**dscp** *dscp*]	source と source-wildcard ワイルドカードの値 *source* 0.0.0.0 の省略形を使用するか、または destination と destination-wildcard の値 *destination* 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。 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。
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**] | **smartlog**] [**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 の説明にあ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* の後ろに入力した場合）または宛先ポート（*destination destination-wildcard* の後ろに入力した場合）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 ポート名を参照する場合は、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.4*』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だけを使用します。 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**：確立された接続と照合します。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照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または **urg**（緊急）です。
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**] | **smartlog**] [**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 の説明にあるパラメータと同じです。ただし、[*operator* [*port*]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP の場合、**flag** および **established** パラメータは無効です。

	コマンド	目的
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**] | **smartlog**] [**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 プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type* : ICMP メッセージ タイプ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-code* : ICMP メッセージ コード タイプ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名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 タイプ名およびコード名のリストを参照する場合は、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.4*』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**] | **smartlog**] [**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 プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type* : IGMP メッセージ タイプと照合するには、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場合は、**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。番号制アクセス リストから ACE を個別には削除できません。

次に、ネットワーク 171.69.198.0 のすべてのホストからネットワーク 172.20.52.0 のすべてのホストへの Telnet アクセスを禁止し、他のすべて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 の作成後に（端末から入力するなどして）追加したものは、リストの末尾に組み込まれます。番号制アクセス リストの特定の場所には、ACE を追加または削除できません。

（注） ACL を作成するときは、アクセス リストの末尾に暗黙の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。

作成した番号制拡張 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.35-19）を参照）、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.35-20）を参照）、または VLAN（「VLAN マップの設定」（P.35-31）を参照）に適用できます。

ACL 内の ACE シーケンスの再編集

アクセス リストのエントリのシーケンス番号は、新しく 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たり、適用する ACE の順番を変更したりできます。たとえば、ACL に新規 ACE を追加した場合、その ACE はリストの一番下に配置されます。その場合、シーケンス番号を変更することで、ACL 内の ACE を異なる場所に移動できます。

名前付き標準および拡張 ACL の作成

番号ではなく英数字のストリング（名前）で、IPv4 ACL を特定できます。名前付き ACL を使用すると、番号制アクセス リストの場合より多くの IPv4 アクセス リストをスイッチ上で設定できます。番号ではなく名前でアクセス リストを指定する場合、モードとコマンド構文が多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドが名前付きアクセス リストを受け入れるわけではありません。

（注）　標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ～ 99、拡張 IP ACL の名前は 100 ～ 199 にできます。番号制リストの代わりに名前付き ACL を使用した場合、名前付きリストからエントリを個別に削除できるという利点があります。

名前付き ACL を設定する前に、次の注意事項と制限事項を考慮してください。

- 番号制 ACL を受け入れるすべてのコマンドが、名前付き ACL を受け入れるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- 「標準および拡張 IPv4 ACL の作成」（P.35-8）で説明したとおり、番号制 ACL を使用することもできます。
- VLAN マップには、標準 ACL および拡張 ACL（名前付きまたは番号制）を使用できます。
- IPv4 の QoS ACL を使用する場合、**class-map** {**match-all** | **match-any**} *class-map-name* グローバル コンフィギュレーション コマンドを入力する場合に、次の **match** コマンドを使用できます。
  - **match access-group** *acl-name*

    （注）　ACL は、名前付き拡張 ACL にする必要があります。

  - **match input-interface** *interface-id-list*
  - **match ip dscp** *dscp-list*
  - **match ip precedence** *ip-precedence-list*

  match access-group *acl-index* コマンドは入力できません。

名前を使用して標準 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	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。
ステップ 2	**ip access-list standard** *name*	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前は、1 ～ 99 の番号にできます。
ステップ 3	**deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log** | **smartlog**] または **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] | **smartlog**]	アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する、拒否条件または許可条件を 1 つまたは複数指定します。 • **host** *source* : source と source-wildcard の値 *source* 0.0.0.0 • **any** : source と source-wildcard 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。

名前付き標準 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	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。
ステップ 2	**ip access-list extended** *name*	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前は、100 ～ 199 の番号にできます。
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** | **smartlog**] [**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、許可条件または拒否条件を指定します。**log** キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 プロトコルおよび他のキーワードの定義については、「番号制拡張 ACL の作成」（P.35-11）を参照してください。 • **host** *source* : source と source-wildcard の値 *source* 0.0.0.0 • **host** *destination* : destination と destination-wildcard の値 *destination* 0.0.0.0 • **any** : source と source-wildcard の値、または destination と destination-wildcard 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。
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。

名前付き拡張 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、対応する IP ホスト アドレスのアクセス リスト仕様に基づくマスクを指定しなかった場合、0.0.0.0 がマスクと見なされます。

ACL の作成後に行った追加は、リストの末尾に組み込まれます。ACE を選択的に特定の ACL に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、名前付き ACL からエントリを削除できます。次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

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

番号制 ACL ではなく名前付き ACL を使用する理由の 1 つは、名前付き ACL から行を選択して削除できるためです。

作成した名前付き ACL は、インターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.35-20）を参照）または VLAN（「VLAN マップの設定」（P.35-31）を参照）に適用できます。

ACL での時間範囲の使用法

time-range グローバル コンフィギュレーション コマンドを使用することによって、曜日および時刻に基づいて拡張 ACL を選択的に適用できます。最初に時間範囲の名前を定義して、時間範囲の時刻および日付、または曜日を設定します。この時間範囲名は、ACL を適用してアクセス リストに制限を設定するときに入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内、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、「標準および拡張 IPv4 ACL の作成」（P.35-8）および「名前付き標準および拡張 ACL の作成」（P.35-15）に記載されている、名前付きおよび番号制拡張 ACL の手順を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

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

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、ハードウェア メモリにロードされた結合済みの設定とマージする必要があるためです。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ます。したがって、信頼できるクロック ソースが必要です。Network Time Protocol（NTP）を使用してスイッチ クロックを同期させることを推奨します。詳細については、「システム日時の管理」（P.7-1）を参照してください。

ACL の時間範囲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	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。
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）を割り当てて、time-range コンフィギュレーション モードを開始します。名前にスペースまたは疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 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*	適用する機能がいつ動作可能になるかを指定します。 • 時間範囲には、**absolute** ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。 • 複数の **periodic** ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 設定例を参照してください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show time-range**	時間範囲の設定を確認します。
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。

複数の項目を別々の時間で有効にする場合は、上記の手順を繰り返してください。

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

```
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_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
   absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
   periodic weekdays 8:00 to 12:00
   periodic weekdays 13:00 to 17:00
```

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

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
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_2006 (inactive)
   20 permit tcp any any time-range workhours (inactive)
```

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

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
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_2006 (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（注釈）を任意の IP 標準または拡張 ACL に組み込むことができます。コメントを使用すると、ACL エントリの理解とスキャンが容易になります。1 つのコメント行は 100 文字までです。

コメントは許可（permit）ステートメントまたは拒否（deny）ステートメントの前後どちらにでも配置できます。コメントがどの許可ステートメントまたは拒否ステートメントの説明であるのかが明白になるように、コメントの位置には一貫性が必要です。たとえば、一部のコメントは対応する許可または拒否ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあるという状況は、混乱の原因となります。

番号制の 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、**no** 形式のコマンドを使用します。

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

```
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 through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリに関しては、**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、**no** 形式のコマンドを使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されていません。

```
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 IPv4 ACL の適用

番号制 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。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

インターフェイスへの ACL の適用の手順については、「インターフェイスへの IPv4 ACL の適用」（P.35-20）を参照してください。VLAN への ACL の適用については、「VLAN マップの設定」（P.35-31）を参照してください。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、特権 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。
ステップ 2	**line** [**console** | **vty**] *line-number*	設定する回線を特定し、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 Data Communications Equipment（DCE; データ通信装置）です。 • **vty**：リモート コンソール アクセス用の仮想端末を指定します。 *line-number* は、回線タイプを指定する場合、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ～ 16 です。
ステップ 3	**access-class** *access-list-number* {**in** | **out**}	（デバイスに対する）特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信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 IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。以下の注意事項に留意してください。

- ACL は着信レイヤ 2 インターフェイスにだけ適用してください。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*の方向に適用します。
- インターフェイスへのアクセスを制御する場合、名前付きまたは番号制 ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2（ポート）ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。レイヤ 2 ポートで受信する着信パケットは、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、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。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。
- プライベート VLAN が設定されている場合、プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。

（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ドロップされず、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。ポート ACL は例外です。ポート ACL は ICMP 到達不能メッセージを生成しません。

ICMP 到達不能メッセージは、ルータ ACL で **no ip unreachables** インターフェイス コマンドを使用してディセーブルにできます。

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

	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。
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、ポートにアクセス リスト 2 を適用して、ポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet1/0/1
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、パケットの受信後にスイッチは ACL を使用してパケットを調べます。ACL がパケットを許可すると、スイッチはパケットの処理を継続します。ACL がパケットを拒否すると、スイッチはパケットを廃棄します。

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、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。ACL がパケットを拒否すると、スイッチはパケットを廃棄します。

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

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断して処理を行い、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 のハードウェアおよびソフトウェアの処理

ACL の処理は主にハードウェアで実行されますが、トラフィック フローの中には CPU に転送してソフトウェア処理を行う必要があるものもあります。ハードウェアで ACL コンフィギュレーションを保存する容量がいっぱいになると、パケットは転送のために CPU に送信されます。ソフトウェア転送トラフィックの転送レートは、ハードウェア転送トラフィックより大幅に低くなります。

（注） スイッチまたはスタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、スイッチに着信した該当 VLAN 内のトラフィックだけです（ソフトウェアで転送される）。パケットのソフトウェア転送が発生すると、消費される CPU サイクル数に応じて、スイッチまたはスイッチ スタックのパフォーマンスが低下することがあります。

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 により多数のパケットが CPU へ送信されると、スイッチのパフォーマンスが低下する可能性があります。

show ip access-lists 特権 EXEC コマンドを入力しても、表示される一致カウントはハードウェアで制御されるアクセスのパケットを表示しません。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ドロップされます。*許可*ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が*許可*ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

ACL のトラブルシューティング

次の ACL マネージャ メッセージが表示され、[chars] がアクセスリスト名である場合、

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

スイッチのリソースが、ACL のハードウェア表現を作成するには不十分となっています。リソースには、ハードウェア メモリとラベル スペースが含まれますが、CPU メモリは含まれません。利用可能な論理演算ユニットまたは特殊なハードウェア リソースの不足によって、この問題が発生する可能性があります。論理演算ユニットは、TCP フラグの照合や、TCP、UDP、または SCTP ポート番号に関する **eq** 以外のテスト（**ne**、**gt**、**lt**、または **range**）に必要です。

次の回避策の 1 つを実行します。

- 使用するリソースを少なくするように ACL の設定を修正する。
- ACL の名前または番号を、使用されている英数字より若い英数字を使用して変更する。

特殊なハードウェア リソースを判断するには、**show platform layer4 acl map** 特権コマンドを入力します。スイッチに利用可能なリソースがない場合、インデックス 0 からインデックス 15 までが利用不能であることが表示されます。

リソースが不足している ACL の設定に関する詳細については、Bug Toolkit の『CSCsq63926』を参照してください。

たとえば、次の ACL をインターフェイスに適用する場合は次のとおりです。

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

また、次のメッセージが表示された場合は次のとおりです。

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグ関連の演算子が使用できません。この問題を回避するには、以下を実行します。

- **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、4 番目の ACE を 1 番目の ACE の前に移動します。

  ```
  permit tcp source source-wildcard destination destination-wildcard
  permit tcp source source-wildcard destination destination-wildcard range 5 60
  permit tcp source source-wildcard destination destination-wildcard range 15 160
  permit tcp source source-wildcard destination destination-wildcard range 115 1660
  ```

  または

- ACL の名前を、他の ACL より若い英数字の名前または番号に変更する（たとえば、ACL *79* から ACL *1* に変更）。

これで、この ACL 内の 1 番目の ACL をインターフェイスに適用できます。スイッチによって、ACE が、Opselect インデックス内の利用可能なマッピング ビットに割り当てられ、次に、ハードウェア メモリ内の同じビットを使用するフラグ関連演算子が割り当てられます。

IPv4 ACL の設定例

ここでは、IPv4 ACL の設定および適用例を示します。ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章の「Configuring IP Services」を参照してください。

- 「小規模ネットワークが構築されたオフィス用の ACL」（P.35-24）

- 「番号制 ACL」（P.35-25）
- 「拡張 ACL」（P.35-25）
- 「名前付き ACL」（P.35-26）
- 「IP ACL に適用される時間範囲」（P.35-26）
- 「コメント付き IP ACL エントリ」（P.35-27）
- 「ACL のロギング」（P.35-27）

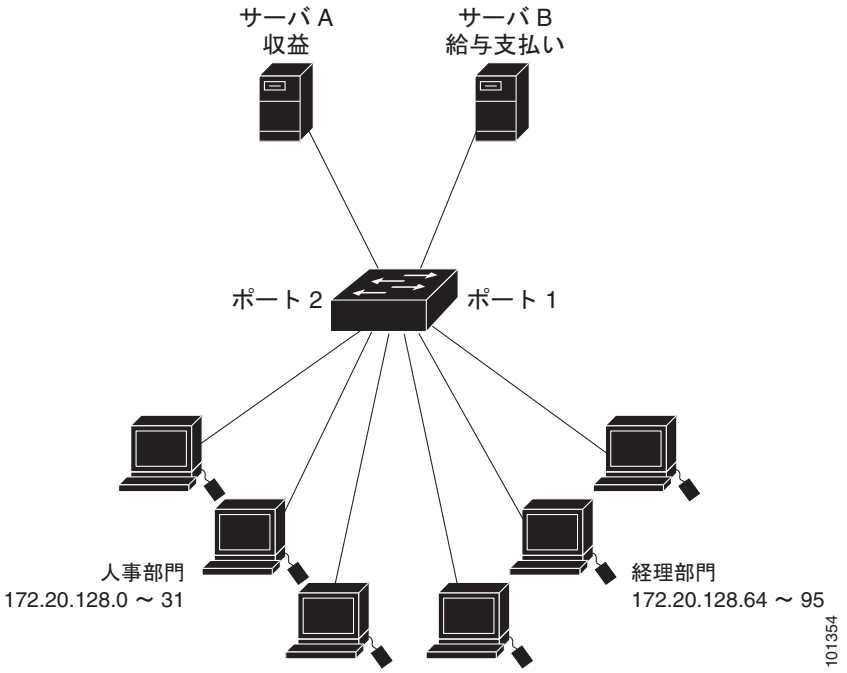
小規模ネットワークが構築されたオフィス用の ACL

図 35-3 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 35-3　　ルータ ACL によるトラフィックの制御



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

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

```
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
```

番号制 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。ACL はポートに着信す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 gigabitethernet2/0/1
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 gigabitethernet2/0/1
Switch(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、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 ホストには、専用メール ホストのメール（SMTP）ポート接続を除いて、ネットワーク上のホストへの TCP 接続は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、もう一方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。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
```

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

次の例では、ネットワークはアドレスが 128.88.0.0 のクラス B ネットワークで、メール ホストのアドレスは 128.88.1.2 です。**established** キーワードは、確立された接続を表示する TCP 専用のキーワードです。TCP データグラムに ACK または RST ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。スタック メンバー 1 のギガビット イーサネット インターフェイス 1 は、ルータをインターネットに接続するインターフェイスです。

```
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
```

名前付き 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、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
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
```

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

```
Switch(config)# interface gigabitethernet3/0/2
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

次の例では、月曜日から金曜日の午前 8 時～午後 6 時（18 時）の間、IP の HTTP トラフィックが拒否されます。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```
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 gigabitethernet2/0/1
Switch(config-if)# ip access-group strict in
```

コメント付き IP ACL エントリ

次に示す番号制 ACL の例では、Jones のワークステーションにアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
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
```

次に示す番号制 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
```

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

```
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
```

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

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

```
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

<output truncated>

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

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

```
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、一致した ACL やアクセス エントリの種類に応じて若干異なります。

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

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1
0001.42ef.a400) -> 10.1.1.61 (0/0), 1 packet
```

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

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

名前付き MAC 拡張 ACL の作成

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

（注）　レイヤ 3 インターフェイスには、名前付き 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 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ていません。

名前付き 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	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。
ステップ 2	**mac access-list extended** *name*	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	{**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、すべての（**any**）送信元 MAC アドレス、マスク付きの送信元 MAC アドレス、または特定のホスト（**host**）送信元 MAC アドレス、およびすべての（**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 *don't care* ビットの任意のマスクが付加されて、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。*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 802.1Q CoS 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 全体を削除する場合は、**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。名前付き MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、EtherType DECnet Phase IV トラフィックだけを拒否し、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 リストを作成して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。

- 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 ポートで受信する着信パケットは、常にポート ACL でフィルタリングされます。
- 同じレイヤ 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 IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換えられます。

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に 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	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。
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 リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は、着信方向だけをサポートします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show 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。

指定したアクセス 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、ポートにアクセス リスト *mac1* を適用して、ポートに着信す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
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だけ有効となります。このコマンドを EtherChannel ポート チャネルには使用できません。

パケットの受信後に、スイッチは着信 ACL とパケットを照合します。ACL がパケットを許可すると、スイッチはパケットの処理を継続します。ACL がパケットを拒否すると、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断して処理を行い、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 マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケット タイプ（IP または MAC）に対する match 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケット タイプに対する match コマンドがない場合、デフォルトでは、パケットが転送されます。

ここで使用す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、次のステップを実行します。

ステップ 1　VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。「標準および拡張 IPv4 ACL の作成」（P.35-8）および「VLAN マップの作成」（P.35-33）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** を入力することもできます。また、**match** コマンドを入力して、既知の MAC アドレスだけが格納された 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）　パケット タイプ（IP または MAC）に対する match 句が VLAN マップに設定されている場合で、そのマップ アクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。match 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。

ステップ 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、次の設定情報について説明します。

- 「VLAN マップの設定時の注意事項」（P.35-32）
- 「VLAN マップの作成」（P.35-33）
- 「VLAN への VLAN マップの適用」（P.35-36）
- 「ネットワークでの VLAN マップの使用法」（P.35-36）
- 「VACL ロギングの設定」（P.35-39）

VLAN マップの設定時の注意事項

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定*されていない*場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケット タイプ（IP または MAC）に対する match 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの match 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケット タイプに対する match 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- 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ていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまた MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケット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。
- プライマリおよびセカンダリ VLAN で VLAN マップを設定できます。ただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
  - ホスト ポートから混合ポートへのアップストリームで送信されるフレームの場合、セカンダリ VLAN に設定されている VLAN マップが適用されます。
  - 混合ポートからホスト ポートへのダウンストリームで送信されるフレームの場合、プライマリ VLAN に設定されている VLAN マップが適用されます。

  プライベート VLAN の特定の IP トラフィックをフィルタリングするには、VLAN マップをプライマリおよびセカンダリ VLAN の両方に適用します。プライベート VLAN の詳細については、第 16 章「プライベート VLAN の設定」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.35-36）を参照してください。

ルータ ACL および VLAN マップを組み合せて使用する方法については、「VLAN マップとルータ ACL の設定時の注意事項」（P.35-40）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、または削除するには、特権 EXEC モードで次の手順を実行します。

	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。
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）を指定します。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 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、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	**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（forward）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照合します（IP または MAC アドレスを使用）。パケットの照合は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセス リストに対してだけ照合されます。
ステップ 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。
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。マップ内のシーケンス エントリを 1 つ削除するには、**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 キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。

ACL および VLAN マップの例

次に、特定の目的のための 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ドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1*ACL を作成します。VLAN マップには IP パケットに対する match 句が存在するため、デフォルトのアクションでは、どの match 句とも一致しない IP パケットがすべてドロップされます。

```
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、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット（TCP でも UDP でもないパケット）がドロップされます。

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

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

```
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 パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合せて使用すると、次のようになります。

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

```
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）がドロップされます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合せて使用すると、次のようになります。

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

```
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	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。
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 のストリング（12、22、30）を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 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
```

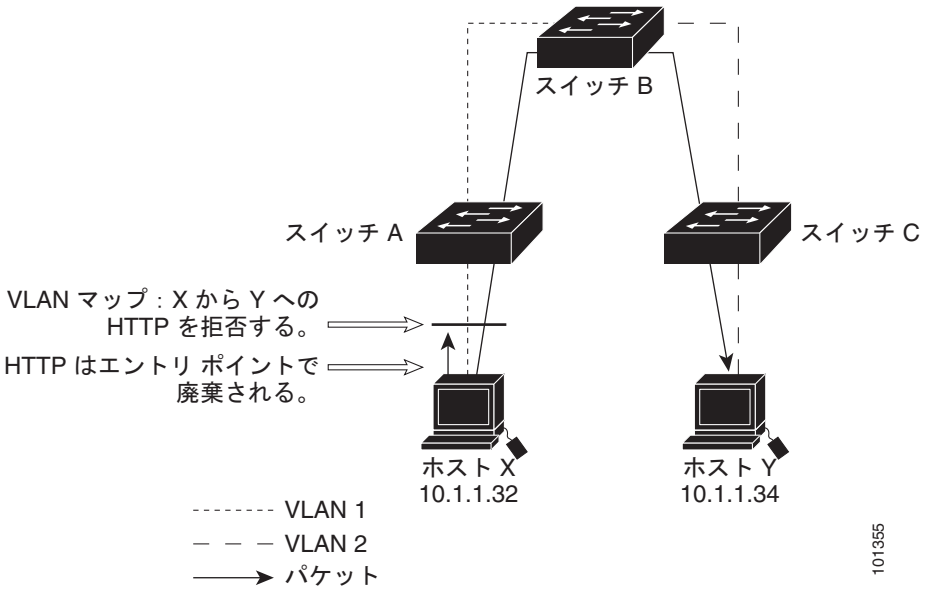
ネットワークでの VLAN マップの使用法

- 「ワイヤリング クローゼットの設定」（P.35-36）
- 「他の VLAN 上のサーバへのアクセス拒否」（P.35-38）

ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成では、ルーティングがスイッチ上でイネーブルにされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。図 35-4 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レイヤ 3 スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス制御できます。

図 35-4　ワイヤリング クローゼットの設定



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

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

```
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ドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
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。

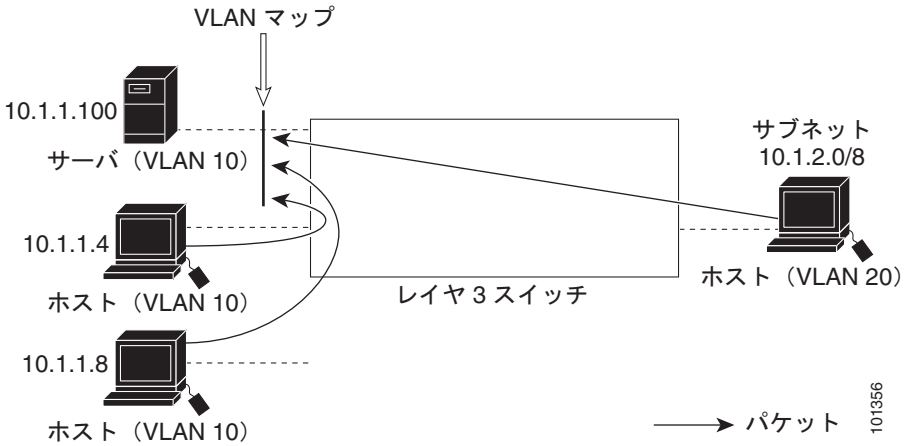
```
Switch(config)# vlan filter map2 vlan 1
```

他の VLAN 上の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 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 35-5 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 35-5　他の VLAN 上の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 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1-ACL を作成して、別の VLAN 内のサーバへのアクセスを拒否する例を示します。最後のステップでは、マップ SERVER1 を VLAN 10 に適用します。

ステップ 1　正しいパケットと一致する 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 パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```
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.
```

VACL ロギングの設定

VACL ロギングを設定する場合は、次の状況で拒否された IP パケットに対して Syslog メッセージが生成されます。

- 一致する最初のパケットを受信した場合
- 最後の 5 分間に一致するパケットを受信した場合
- 5 分経過する前にしきい値に達している場合

ログ メッセージはフロー単位で生成されます。フローは、同じ IP アドレスおよびレイヤ 4（UDP または TCP）ポート番号を持つパケットとして定義されます。フローで 5 分間パケットを受信しない場合、そのフローはキャッシュから削除されます。Syslog メッセージが生成されると、タイマーおよびパケット カウンタがリセットされます。

VACL ロギングの制限事項は次のとおりです。

- 拒否された IP パケットだけがロギングされます。
- 発信ポート ACL でロギングが必要なパケットは、VACL で拒否された場合、ロギングされません。

特権 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。
ステップ 2	**vlan access-map name** [*number*]	VLAN マップを作成します。VLAN マップに名前と番号（任意）を付けます。番号は、マップ内のエントリのシーケンス番号です。 シーケンス番号の範囲は 0 ～ 65535 です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 マップ名と番号（任意）を指定すると、アクセスマップ コンフィギュレーション モードが開始されます。
ステップ 3	**action drop log**	IP パケットを破棄およびロギングするよう VLAN アクセス マップを設定します。
ステップ 4	**exit**	VLAN アクセス マップ コンフィギュレーション モードを終了し、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 5	**vlan access-log** {**maxflow** *max_number* | **threshold** *pkt_count*}	VACL ロギング パラメータを設定します。 • **maxflow** *max_number*：ログ テーブル サイズを設定します。**maxflow** の値を 0 に設定すると、ログ テーブルの内容を削除できます。ログ テーブルがいっぱいの場合は、ロギングされたパケットがソフトウェアによって新しいフローから破棄されます。 値の範囲は、0 ～ 2048 です。デフォルト値は 500 です。 • **threshold** *pkt_count*：ロギングしきい値を設定します。5 分経過する前にフローのしきい値に達すると、ロギング メッセージが生成されます。 しきい値の範囲は 0 ～ 2147483647 です。デフォルトのしきい値は 0 であり、Syslog メッセージが 5 分ごとに生成されます。
ステップ 6	**exit**	特権 EXEC モードに戻ります。
ステップ 7	**show vlan access-map**	設定を確認します。
ステップ 8	**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。

no vlan access-map コマンドをシーケンス番号とともに使用してマップ順序を削除します。シーケンス番号なしでコマンドの **no** バージョンを使用してマップを削除します。

次に、IP パケットを廃棄およびロギングするよう、VLAN アクセス マップを設定する例を示します。ここでは、net_10 の許可エントリに一致する IP トラフィックが破棄およびロギングされます。

```
DomainMember(config)# vlan access-map ganymede 10
DomainMember(config-access-map)# match ip address net_10
DomainMember(config-access-map)# action drop log
DomainMember(config-access-map)# exit
```

次に、グローバル VACL ロギング パラメータを設定する例を示します。

```
DomainMember(config)# vlan access-log maxflow 800
DomainMember(config)# vlan access-log threshold 4000
```

（注） ここで使用するコマンドの構文および使用方法の詳細については、次の URL で入手可能な『*Cisco IOS LAN Switching Command Reference*』を参照してください。
http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_book.html

ルータ ACL を VLAN マップと組み合せて使用する方法

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できます。

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

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

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

- 「VLAN マップとルータ ACL の設定時の注意事項」（P.35-40）
- 「VLAN に適用されるルータ ACL と VLAN マップの例」（P.35-41）

VLAN マップとルータ ACL の設定時の注意事項

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

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

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

  または

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

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

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

VLAN に適用されるルータ ACL と VLAN マップの例

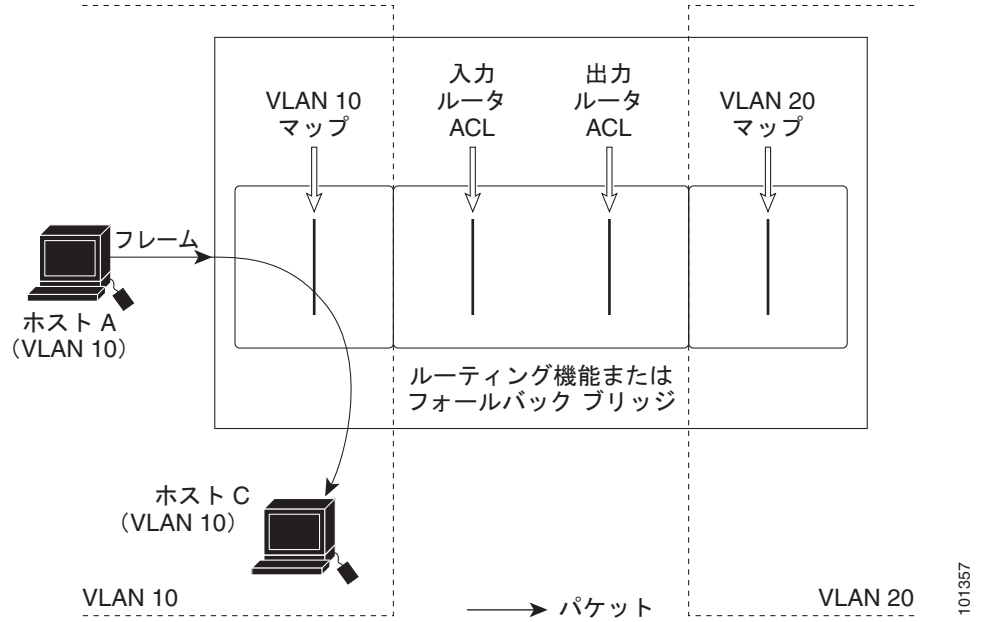
ここでは、ルータ ACL および VLAN マップを VLAN に適用し、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットを処理する例を示します。次の図ではそれぞれの宛先に転送されるパケットを示します。パケットのパスが VLAN マップや ACL を示す線と交差するポイントで、パケットを転送せずにドロップする可能性もあります。

- 「ACL およびスイッチド パケット」（P.35-41）
- 「ACL およびブリッジド パケット」（P.35-42）
- 「ACL およびルーテッド パケット」（P.35-43）
- 「ACL およびマルチキャスト パケット」（P.35-43）

ACL およびスイッチド パケット

図 35-6 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。フォールバック 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 マップだけが適用されます。

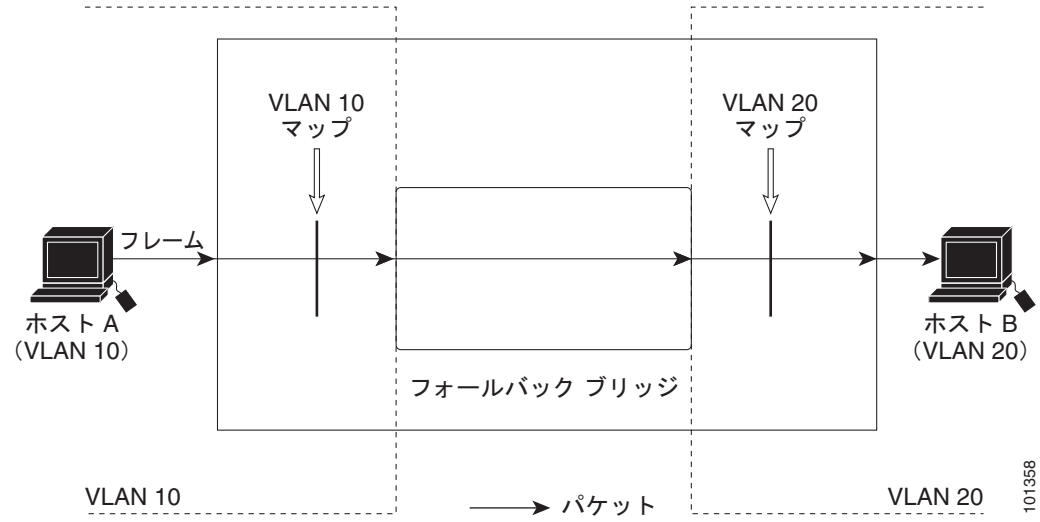
図 35-6　スイッチド パケットへの ACL の適用



ACL およびブリッジド パケット

図 35-7 に、フォールバック 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 だけが適用されます。また、非 IP および非 ARP パケットだけがフォールバック ブリッジド パケットとなります。

図 35-7　ブリッジド パケットへの ACL の適用

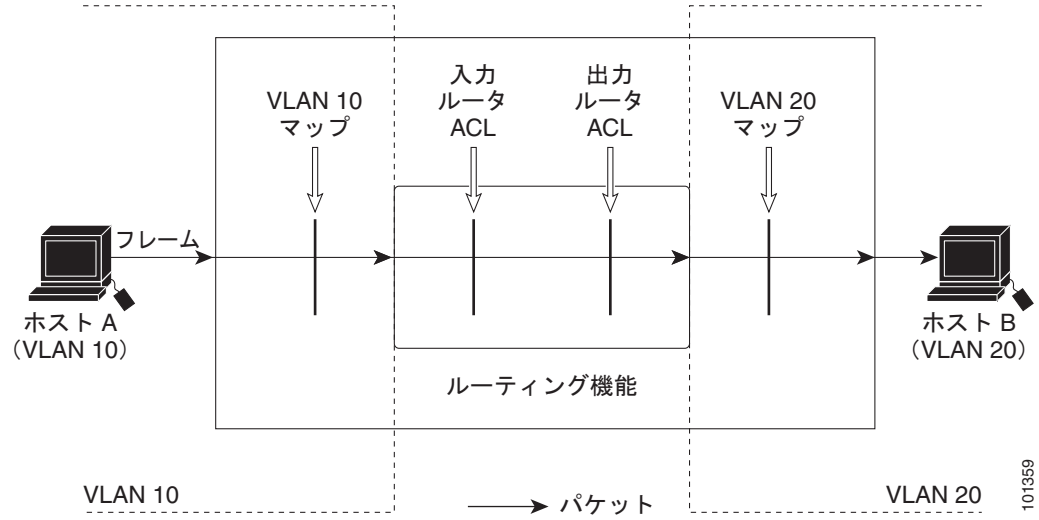


ACL およびルーテッド パケット

図 35-8 に、ルーテッド パケットに ACL を適用する方法を示します。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 35-8　ルーテッド パケットへの ACL の適用

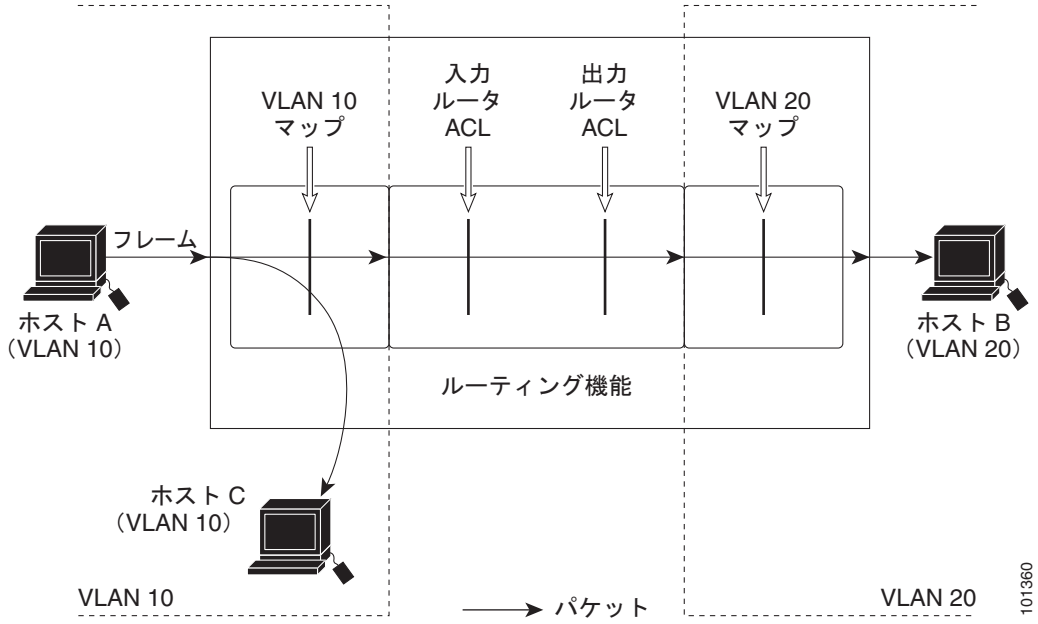


ACL およびマルチキャスト パケット

図 35-9 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 35-9 の VLAN 10 マップ）によってパケットがドロップされる場合、パケットのコピーは宛先に送信されません。

図 35-9　マルチキャスト パケットへの ACL の適用



IPv4 ACL の設定の表示

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された 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。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、特権 EXEC コマンドを使用します（表 35-2 を参照）。

表 35-2　アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [*number* | *name*]	現在の IP および MAC アドレス アクセス リストの 1 つまたは全体の内容、または特定のアクセス リスト（番号制または名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	現在の IP アクセス リスト全体、または特定の IP アクセス リスト（番号制または名前付き）の内容を表示します。
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 がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	スイッチまたは特定のインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたなど）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特定のレイヤ 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。

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 35-3 に記載された特権 EXEC コマンドを使用します。

表 35-3　VLAN マップ情報を表示するコマンド

コマンド	目的
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。