CHAPTER 38

ACL によるネットワーク セキュリティの設定

この章では、Access Control List（ACL; アクセス制御リスト）（アクセス リストとも呼ばれる）を使用して、IE 3000 スイッチにネットワーク セキュリティを設定する手順について説明します。この章で言及される IP ACL は、IP バージョン 4（IPv4）ACL を指しています。IPv6 ACL の詳細については、第 44 章「IPv6 ACL の設定」を参照してください。

この章で使用しているコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」、および『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2* 』を参照してください。Cisco IOS のマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックの制限や、特定のユーザまたは装置によるネットワーク利用の制限に役立ちます。ACL は、ルータまたはスイッチを通過するトラフィックをフィルタリングし、指定したインターフェイスまたは VLAN を通るパケットを許可または拒否します。ACL とは、パケットに適用される許可条件と拒否条件を列挙したものです。インターフェイス上でパケットが受信されると、スイッチはパケット内の各フィールドと適用されているすべての ACL を比較し、アクセス リストで指定された基準に基づいて、そのパケットを転送するのに必要な許可があることを確認します。スイッチは、パケットをアクセス リスト内の各条件と 1 つずつ照合してテストします。最初の条件一致で、スイッチがパケットを受け入れるか拒否するかが決まります。最初の条件一致後にスイッチはテストを停止するため、リスト内の条件の順序が重要となります。どの条件も一致しない場合、スイッチはパケットを拒否します。制限がない場合はスイッチがパケットを転送しますが、そうでない場合はスイッチがパケットを廃棄します。スイッチは、VLAN 内でブリッジされるパケットを含め、転送するすべてのパケットに対して ACL を使用できます。

ルータまたはレイヤ 3 スイッチ上でアクセス リストを設定すると、ネットワークの基本的なセキュリティが実現されます。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のどの部分に対しても許可される可能性があります。ACL を使用すると、ネットワークのさまざまな部分にアクセスできる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

フィックのタイプを決定したりすることができます。たとえば、E メール トラフィックは転送を許可し、Telnet トラフィックは禁止するといった設定が可能です。ACL の設定により、インバウンド トラフィック、アウトバウンド トラフィック、またはその両方をブロックできます。

ACL には、Access Control Entry（ACE; アクセス制御エントリ）の順序指定リストが含まれています。各 ACE には、*許可*または*拒否*と、パケットがその ACE と一致するために満たす必要のある条件のセットが指定されます。*許可*または*拒否*の意味は、その ACL が使用されているコンテキストによって決まります。

このスイッチでは、IP ACL およびイーサネット（MAC）ACL がサポートされています。

- IP ACL は、Transmission Control Protocol（TCP; 伝送制御プロトコル）、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、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）を含む 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、Quality Of Service（QoS; サービス品質）分類の 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.39-8）を参照してください。

ここでは、次の概念情報について説明します。

- 「サポートされる ACL」（P.38-2）
- 「フラグメント化およびフラグメント解除されたトラフィックの処理」（P.38-5）

サポートされる ACL

（注）　ルータ ACL および VLAN マップは、IP サービス イメージが稼動しているスイッチ上でだけサポートされます。

- ポート ACL は、レイヤ 2 インターフェイスに着信す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、このスイッチで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は、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。詳細については、「ポート ACL」（P.38-3）を参照してください。
- ルータ ACL は、VLAN 間のルーテッド 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.38-4）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（ブリッジドおよびルーテッド）をアクセス制御します。VLAN マップを使用すると、同じ VLAN 内の装置間のトラフィックをフィルタリングできます。VLAN マップを設定すると、IPv4 のレイヤ 3 アドレスに基づいたアクセス制御を行います。サポートされていないプロトコルは、イーサネット ACE を使用する MAC アドレスを通じてアクセス制御されます。VLAN マップが VLAN に適用されると、VLAN に着信するすべてのパケット（ルーテッドまたはブリッジド）が VLAN マップと照合されます。パケットは、スイッチ ポートまたはルーティングされたあとのルーテッド ポートのいずれかを通して VLAN に入ることができます。詳細については、「VLAN マップ」（P.38-5）を参照してください。

ユーザは同一のスイッチ上で、入力ポート ACL、ルータ ACL、VLAN マップを使用できます。ただし、ポート ACL はルータ ACL や VLAN マップよりも優先されます。

- 入力ポート ACL と VLAN マップの両方が適用されている場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。その他のパケットには、VLAN マップのフィルタが適用されます。

- 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。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- 出力ルータ ACL および入力ポート ACL が SVI に存在している場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタが適用されます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- VLAN マップ、入力ルータ ACL、および入力ポート ACL が SVI に存在している場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけ適用されます。
- VLAN マップ、出力ルータ ACL、および入力ポート ACL が SVI に存在している場合、ポート ACL が適用されたポート上で受信された着信パケットには、ポート ACL のフィルタだけが適用されます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけ適用されます。

IEEE 802.1Q トンネリングがインターフェイス上で設定されている場合、トンネル ポートで受信された IEEE 802.1Q カプセル化 IP パケットには MAC ACL のフィルタを適用できますが、IP ACL のフィルタは適用できません。これは、スイッチが IEEE 802.1Q ヘッダー内部のプロトコルを認識しないためです。ルータ ACL、ポート ACL、および VLAN マップに、この制限が適用されます。IEEE 802.1Q トンネリングの詳細については、第 20 章「IEEE 802.1Q およびレイヤ 2 プロトコル トンネリングの設定」を参照してください。

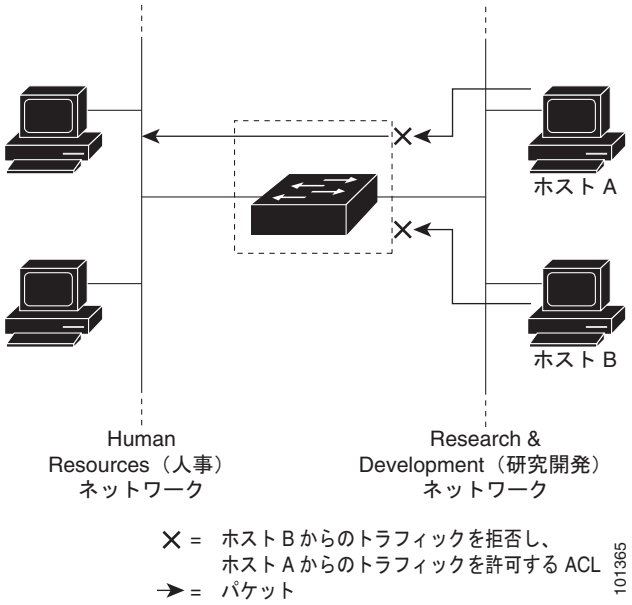
ポート ACL

ポート ACL は、スイッチ上のレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は EtherChannel インターフェイス上ではなく物理インターフェイス上でだけサポートされ、着信方向のインターフェイス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
- 送信元アドレスおよび宛先アドレスと、任意のプロトコル タイプ情報を使用する拡張 IP アクセス リスト
- 送信元 MAC アドレスおよび宛先 MAC アドレスと、任意のプロトコル 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、指定したインターフェイス上で設定されたすべての着信機能と関連付けられた ACL を検証し、パケットが ACL 内のエントリとどのように一致するかに基づいてパケット転送を許可または拒否します。このようにして、ACL は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を制御します。図 38-1 に、すべてのワークステーションが同一 VLAN 内にある場合に、ポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 入力に適用された ACL は、ホスト A から人事部のネットワークへのアクセスは許可しますが、ホスト B から同じネットワークへのアクセスは禁止します。ポート ACL は、着信方向のレイヤ 2 インターフェイスにしか適用できません。

図 38-1　　ACL によるネットワークへの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、ACL によってトランク ポート上に存在するすべての VLAN のトラフィックがフィルタリングされます。ポート ACL を音声 VLAN のポートに適用すると、ACL によってデータと音声の両方の VLAN のトラフィックがフィルタリングされます。

ポート ACL を使用すると、IP トラフィックは IP アクセス リストでフィルタリングし、非 IP トラフィックは MAC アドレスでフィルタリングすることができます。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、同じレイヤ 2 インターフェイスで IP トラフィックと非 IP トラフィックの両方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は、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストまたは MAC アクセス リストがレイヤ 2 インターフェイス上ですでに設定されている場合に、新しい IP アクセス リストまたは MAC アクセス リストをこのインターフェイスに適用すると、以前に設定されていた ACL は新しい ACL で置換されます。

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 を適用できます。ルータ ACL はインターフェイス上で特定の方向（着信または発信）に対して適用します。インターフェイス上の各方向で、1 つのルータ ACL を適用できます。

1 つの ACL をある特定インターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。複数の機能で 1 つのルータ ACL が使用されている場合は、その ACL が複数回検証されます。

IPv4 トラフィックに対して次のアクセス リストがサポートされています。

- 標準 IP アクセス リストでは、照合処理に送信元アドレスが使用されます。
- 拡張 IP アクセス リストでは、照合処理に送信元アドレスおよび宛先アドレスと、任意のプロトコル情報が使用されます。

ポート ACL と同様に、スイッチは指定のインターフェイス上で設定された機能と関連付けられた ACL を検証します。ただし、ルータ ACL は双方向で使用できますが、適用できるのは着信ポート ACL だけです。パケットがインターフェイス上でスイッチに入ってくると、そのインターフェイス上で設定されたすべての着信機能と関連付けられた ACL が検証されます。パケットがルーティングされたあと、ネクストホップに転送される前に、出力インターフェイス上で設定された発信機能と関連付けられた ACL がすべて検証されます。

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 38-1 では、ルータ入力に適用された ACL は、ホスト A から人事部のネットワークへのアクセスは許可しますが、ホスト B から同じネットワークへのアクセスは禁止します。

VLAN マップ

すべてのトラフィックをアクセス制御するには、VLAN ACL または VLAN マップを使用します。VLAN マップは、VLAN に（または VLAN から）ルーティングされる、あるいはスイッチの VLAN 内でブリッジされるすべてのパケットに適用できます。

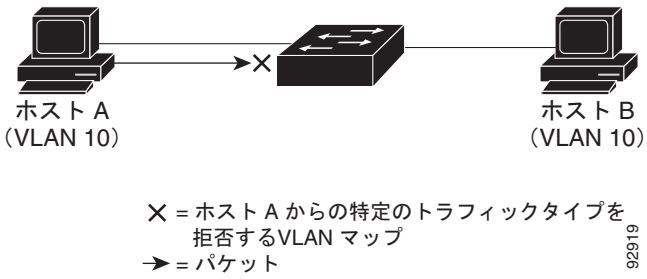
VLAN マップは、セキュリティ パケット フィルタリングに使用します。VLAN マップは方向（入力または出力）別では定義されません。

IPv4 トラフィックのレイヤ 3 アドレスと照合する VLAN マップを設定できます。

非 IP プロトコルはすべて、MAC VLAN マップを使用する MAC アドレスおよび Ethertype を通してアクセス制御されます（IP トラフィックは MAC VLAN マップではアクセス制御 *されません*）。スイッチを通過するパケットに対してだけ VLAN マップを適用できますが、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対しては VLAN マップを適用できません。

VLAN マップを使用すると、マップ内で指定されたアクションに基づいて、パケット転送が許可または拒否されます。図 38-2 に、VLAN マップを適用して、VLAN 10 内のホスト A からの特定タイプのトラフィックが転送されないようにする方法を示します。VLAN に適用できる VLAN マップは 1 つだけです。

図 38-2　VLAN マップによるトラフィック制御



フラグメント化およびフラグメント解除されたトラフィックの処理

IP パケットは、ネットワークを通過するときにフラグメント化できます。フラグメント化が行われた場合、TCP または UDP ポート番号、ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの先頭が格納されたフラグメントにだけ含まれます。他のすべてのフラグメントには、この情報はありません。

ACE の中には、レイヤ 4 情報を確認しないため、すべてのパケット フラグメントに適用できるものもあります。レイヤ 4 情報をテストする ACE は、標準の方法では、フラグメント化された IP パケット内の大半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 情報がなく、ACE が何らかのレイヤ 4 情報をテストする場合は、照合ルールが変更されます。

- 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）を確認する許可 ACE は、欠落しているレイヤ 4 情報の内容にかかわらず、フラグメントと一致するものと見なされます。
- レイヤ 4 情報を確認する拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、そのフラグメントとは一致しません。

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

```
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） この例の最初および 2 番めの ACE で、宛先アドレスのあとの *eq* キーワードは、TCP 宛先ポートの既知の番号がそれぞれ Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）および Telnet と一致しているかどうかをテストすることを意味します。

- パケット A は、ホスト 10.2.2.2、ポート 65000 から SMTP ポート上のホスト 10.1.1.1 に転送される TCP パケットです。すべてのレイヤ 4 情報が存在するため、このパケットがフラグメント化されている場合は、最初のフラグメントが完全なパケットであるかのように最初の ACE（許可）と一致します。最初の ACE はフラグメントに適用された際のレイヤ 3 情報をチェックするだけなので、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 と一致します。この例の情報では、パケットは TCP、宛先は 10.1.1.1 になっています。
- パケット B は、ホスト 10.2.2.2、ポート 65001 から Telnet ポート上のホスト 10.1.1.2 に転送されます。すべてのレイヤ 3 およびレイヤ 4 情報が存在するため、このパケットがフラグメント化されている場合は、最初のフラグメントが 2 番めの ACE（拒否）と一致します。パケット内の残りのフラグメントにはレイヤ 4 情報がないため、2 番めの ACE とは一致しません。代わりに、残りのフラグメントは 3 番めの ACE（許可）と一致します。

  最初のフラグメントは拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できません。このため、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は、パケットの再構成を試みる際に、ネットワーク上の帯域幅とホスト 10.1.1.2 のリソースを消費します。
- フラグメント化されたパケット C は、ホスト 10.2.2.2、ポート 65001 からホスト 10.1.1.3、ポート ftp に転送されます。このパケットがフラグメント化されている場合は、最初のフラグメントが 4 番めの ACE（拒否）と一致します。4 番めの ACE はレイヤ 4 情報をチェックせず、全フラグメント内のレイヤ 3 情報は全フラグメントがホスト 10.1.1.3 に送信されることを示しており、前の許可 ACE は別のホストをチェックしていたため、他のフラグメントもすべて 4 番めの ACE と一致します。

IPv4 ACL の設定

このスイッチで IP v4ACL を設定する方法は、他の Cisco スイッチおよびルータで IPv4 ACL を設定する方法と同じです。次に、このプロセスについて簡単に説明します。ACL の設定の詳細については、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」を参照してください。コマンドの詳細については、『*Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services, Release 12.2* 』を参照してください。Cisco IOS のマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References] から入手できます。

このスイッチでは、次の Cisco IOS ルータ ACL 関連機能はサポートされていません。

- 非 IP プロトコル ACL（表 38-1（P.38-8）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 を使用した場合を除く）
- 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

次に、このスイッチで IP ACL を使用するための手順を示します。

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。また、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.38-7）
- 「端末回線への IPv4 ACL の適用」（P.38-20）
- 「インターフェイスへの IPv4 ACL の適用」（P.38-20）
- 「IP ACL のハードウェアおよびソフトウェアの処理」（P.38-22）
- 「ACL のトラブルシューティング」（P.38-23）
- 「IPv4 ACL の設定例」（P.38-24）

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 とは、許可条件と拒否条件を列挙したものです。スイッチは、パケットをアクセス リスト内の各条件と 1 つずつ照合してテストします。最初の条件一致で、スイッチがパケットを受け入れるか拒否するかが決まります。最初の一致後にスイッチはテストを停止するため、条件の順序が重要となります。どの条件も一致しない場合、スイッチはパケットを拒否します。

ソフトウェアでは、次のタイプの ACL または IPv4 対応アクセス リストがサポートされています。

- 標準 IP アクセス リストでは、照合処理に送信元アドレスが使用されます。
- 拡張 IP アクセス リストでは、照合処理に送信元アドレスと宛先アドレスが使用され、さらに細かい制御を行う場合は任意でプロトコル タイプ情報も使用されます。

ここでは、アクセス リストとその作成手順について説明します。

- 「アクセス リスト番号」（P.38-8）

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 38-1 に、アクセス リスト番号とそれに対応するアクセス リスト タイプを示し、それらがスイッチでサポートされているかどうかを示します。このスイッチでは、IPv4 の標準および拡張アクセス リスト、番号 1 ～ 199 および 1300 ～ 2699 がサポートされています。

表 38-1　　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
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） 番号付きの標準および拡張 ACL に加えて、サポート対象の番号を使用して名前付きの標準および拡張 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、拡張 IP ACL の名前には 100 ～ 199 を使用できます。番号付きリストではなく名前付き ACL を使用することの利点は、名前付きリストから個別のエントリを削除できることです。

ACL ロギング

スイッチ ソフトウェアでは、標準の 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ギング メッセージを提供できます。つまり、パケットが ACL と一致すると、そのパケットの詳細を示すロギング メッセージがコンソールに送信されます。コンソールに記録されるメッセージのレベルは、syslog メッセージを制御する logging console コマンドで制御します。

（注）　ルーティングはハードウェアで行われ、ロギングはソフトウェアで行われるため、多数のパケットが **log** キーワードを含む*許可*または*拒否* ACE と一致する場合は、ソフトウェアがハードウェアの処理速度に対応できず、一部のパケットが記録されない可能性があります。

ACL をトリガーする最初のパケットによって、ロギング メッセージが直ちに表示され、後続のパケットは 5 分間隔で収集されたあと、表示または記録されます。ロギング メッセージには、アクセス リスト番号、パケットが許可されたか拒否されたか、パケットの送信元 IP アドレス、直前の 5 分間隔でこの送信元から許可または拒否されたパケットの数が含まれます。

番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、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**]	送信元アドレスとワイルドカードを使用して、標準 IPv4 アクセス リストを定義します。 *access-list-number* 値は、1 ～ 99 または 1300 ～ 1999 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にアクセスを拒否するのか許可するのかを指定します。 *source* 値は、パケットの送信元となるネットワークまたはホストのアドレスであり、次の形式で指定されます。 • ドット付き 10 進表記による 32 ビット長の値。 • *source* および *source-wildcard* 値 0.0.0.0 255.255.255.255 の略を意味するキーワード **any**。source-wildcard を入力する必要はありません。 • source および source-wildcard 値 *source* 0.0.0.0 の略を意味するキーワード **host**。 （任意）*source-wildcard* を使用して、ワイルドカード ビットを送信元に適用します。 （任意）**log** を入力すると、エントリと一致するパケットの詳細を示すロギング 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 コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。番号付きアクセス リストから個別の ACE は削除できません。

（注） ACL を作成する場合は、ACL の最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否暗黙の拒否文が、デフォルトで ACL の最後尾に含まれることに注意してください。標準アクセス リストで、関連 IP ホスト アドレス ACL の指定からマスクを省略した場合は、0.0.0.0 がマスクと見なされます。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、それ以外へのアクセスを許可し、結果を表示する標準 ACL を作成する例を示します。

```
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
```

スイッチは常に、標準アクセス リストの順序を上書きします。これにより、**host** が一致するエントリ、および *don't care* マスクが 0.0.0.0 に一致するエントリがリストの先頭に移動され、*don't care* マスクが 0 以外のどのエントリよりも上になります。このため、**show** コマンド出力とコンフィギュレーション ファイルでは、ACE は必ずしも入力順どおりには表示されません。

作成した番号付き標準 IPv4 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.38-20）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.38-20）を参照）、または VLAN（「VLAN マップの設定」（P.38-31）を参照）に適用できます。

番号付き拡張 ACL の作成

標準 ACL では送信元アドレスだけを照合に使用しますが、照合処理に拡張 ACL の送信元アドレスと宛先アドレスを使用でき、さらに細かい制御を行う場合は任意でプロトコル タイプ情報も使用できます。番号付き拡張アクセス リストで ACE を作成する場合は、ACL の作成後の追加はすべてリストの末尾に置かれることに注意してください。リストの順序の変更や、番号付きリストでの ACE の選択的な追加または削除を行うことはできません。

プロトコルの中には、特定のパラメータやキーワードをそのプロトコルに適用するものもあります。

次の IP プロトコルがサポートされています（カッコ内の太字がプロトコル キーワードです）。

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

（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すべて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の詳細については、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 12.2*』
- 『*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*』

これらのマニュアルは、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] から入手できます。

（注）　このスイッチでは、ダイナミックまたは再帰アクセス リストはサポートされていません。また、Type of Service（ToS; サービス タイプ）の minimize-monetary-cost ビットに基づいたフィルタリングもサポートされていません。

サポート対象パラメータは、TCP、UDP、ICMP、IGMP、その他の IP の各カテゴリに分類できます。

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**] [**time-range** *time-range-name*] [**dscp** *dscp*] （注）　**dscp** 値を入力した場合は、**tos** と **precedence** は入力できません。**dscp** がない場合は、**tos** と **precedence** の両方の値を入力できます。	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* 値は、100 ～ 199 または 2000 ～ 2699 の範囲の 10 進数値です。 **deny** または **permit** を入力して、条件が一致した場合にパケットを拒否するのか許可するのかを指定します。 *protocol* には、IP プロトコルの名前（**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、または **udp**）、または番号（IP プロトコル番号を示す 0 ～ 255 の範囲の整数）を入力します。任意のインターネット プロトコル（ICMP、TCP、および UDP を含む）を照合するには、キーワード **ip** を使用します。 （注）　この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の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* 値は、パケットの送信元となるネットワークまたはホストの番号です。 *source-wildcard* を使用して、ワイルドカード ビットを送信元に適用します。 *destination* 値は、パケットの送信先となるネットワークまたはホストの番号です。 *destination-wildcard* を使用して、ワイルドカード ビットを宛先に適用します。 source、source-wildcard、destination、および destination-wildcard は、次の形式で指定できます。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • シングル 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す。各キーワードの意味は次のとおりです。 • **precedence**：0 ～ 7 の数値または名前で指定された優先レベルを使用してパケットを照合します。指定可能な値は、**routine**（**0**）、***priority***（**1**）、**immediate**（**2**）、**flash**（**3**）、**flash-override**（**4**）、**critical**（**5**）、**internet**（6）、**network**（**7**）です。 • **fragments**：非初期フラグメントを確認します。 • **tos**：0 ～ 15 の数値または名前で指定されたサービス タイプ レベルを使用して照合する場合に入力します。指定可能な値は、**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の詳細を示すロギング メッセージを作成してコンソールに送信します。または、**log-input** を入力して、ログ エントリに入力インターフェイスを含めます。 • **time-range**：このキーワードの詳細については、「ACL での時間範囲の使用」（P.38-17）を参照してください。 • **dscp**：0 ～ 63 の数値で指定された DSCP 値を使用してパケットを照合します。使用可能な値のリストを表示する場合は、疑問符（?）を使用します。

	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**] [**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 および source wildcard 値 0.0.0.0 255.255.255.255 の略と、destination および destination wildcard 値 0.0.0.0 255.255.255.255 の略を使用して、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**] [**time-range** *time-range-name*] [**dscp** *dscp*]	source および source wildcard 値 *source* 0.0.0.0 の略と、destination および destination wildcard 値 *destination* 0.0.0.0 の略を使用して、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**] [**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。 パラメータはステップ 2a で説明されているパラメータと同じです。ただし、次の例外があります。 （任意）送信元ポート（*source source-wildcard* の後ろに置かれた場合）または宛先ポート（*destination destination-wildcard* の後ろに置かれた場合）を比較する場合は、*operator* および *port* を入力します。使用できる演算子には、**eq**（equal：一致）、**gt**（greater than：より大きい）、**lt**（less than：未満）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）があります。演算子にはポート番号が必要です（**range** にはスペースで区切った 2 つのポート番号が必要です）。 10 進数値（0 ～ 65535）の *port* 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、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」を参照してください。TCP をフィルタリングする場合は、TCP ポート番号またはポート名だけを使用します。 その他の任意のキーワードの意味は次のとおりです。 • **established**：確立された接続を照合します。これには、**ack** または **rst** フラグの照合と同じ機能があります。 • *flag*：指定された TCP ヘッダー ビットによって照合する場合は、次のいずれかのフラグを入力します。**ack**（acknowledge：確認応答）、**fin**（finish：終了）、**psh**（push：プッシュ）、**rst**（reset：リセット）、**syn**（synchronize：同期）、**urg**（urgent：緊急）
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が、[*operator* [*port*]] の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**] [**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 プロトコルに関して説明されてい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。任意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 メッセージのタイプ名およびコード名のリストについては、? を使用するか、『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「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 プロトコルに関して説明されているパラメータとほとんど同じですが、次に示す任意のパラメータが追加されています。 *igmp-type*：IGMP メッセージ タイプを照合するには、0 ～ 15 の数値、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 コンフィギュレーションを確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。番号付きアクセス リストから個別の ACE は削除できません。

次に、拡張アクセス リストを作成および表示して、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、それ以外はすべて許可する例を示します（宛先アドレスのあとの **eq** キーワードは、TCP 宛先ポート番号が Telnet と一致しているかどうかをテストすることを意味します）。

```
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 の作成後の追加（端末から入力される可能性がある）は、すべてリストの末尾に置かれます。番号付きアクセス リストでアクセス リスト エントリを選択的に追加または削除できません。

（注）　ACL を作成する場合は、アクセス リストの最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトでアクセス リストの最後尾に含まれることに注意してください。

作成した番号付き拡張 ACL は、端末回線（「端末回線への IPv4 ACL の適用」（P.38-20）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.38-20）を参照）、または VLAN（「VLAN マップの設定」（P.38-31）を参照）に適用できます。

ACL 内の ACE の順序変更

アクセス リスト内のエントリのシーケンス番号は、新しい ACL の作成時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 コマンドを使用すると、ACL 内のシーケンス番号を編集して、ACE の適用順序を変更することができます。たとえば、新しい ACE を ACL に追加すると、その ACE はリストの末尾に置かれます。シーケンス番号を変更すると、この ACE を ACL 内の別の位置に移動できます。

ip access-list resequence コマンドの詳細については、次の URL を参照してください。
http://preview.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a0080134a60.html

名前付き標準および拡張 ACL の作成

IPv4 ACL を番号ではなく英数字のストリング（名前）で識別することができます。名前付き ACL を使用して、番号付きアクセス リストを使用した場合よりも多くの IPv4 アクセス リストをルータに設定できます。番号ではなく名前でアクセス リストを識別する場合は、モードと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が名前付きアクセス リストを受け入れるとは限りません。

（注）　標準または拡張 ACL に付ける名前は、サポート対象のアクセス リスト番号範囲の数値でも構いません。つまり、標準 IP ACL の名前には 1 ～ 99、拡張 IP ACL の名前には 100 ～ 199 を使用できます。番号付きリストではなく名前付き ACL を使用することの利点は、名前付きリストから個別のエントリを削除できることです。

名前付き ACL を設定する場合は、次の注意事項および制限事項を考慮してください。

- 番号付き ACL を受け入れるすべてのコマンドが、名前付き ACL を受け入れるとは限りません。インターフェイス上のパケット フィルタとルート フィルタに関する ACL には名前を使用できます。VLAN マップも名前を受け入れます。
- 標準 ACL と拡張 ACL は同じ名前にできません。
- 番号付き ACL も使用可能です（「標準および拡張 IPv4 ACL の作成」（P.38-7）を参照）。
- VLAN マップでは、標準および拡張 ACL（名前付きまたは番号付き）を使用できます。

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。 名前には 1 ～ 99 の範囲の数値を使用できます。
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、パケットを転送するか廃棄する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 および source wildcard 値 *source* 0.0.0.0。 • **any**：source および source wildcard 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 コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。 名前には 100 ～ 199 の範囲の数値を使用できます。
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、許可条件または拒否条件を指定します。違反を含むアクセス リスト ロギング メッセージを取得するには、**log** キーワードを使用します。 プロトコルおよびその他のキーワードの定義については、「番号付き拡張 ACL の作成」（P.38-10）を参照してください。 • **host** *source*：source および source wildcard 値 *source* 0.0.0.0。 • ***host*** *destination*：destination および destination wildcard 値 *destination* 0.0.0.0。 • **any**：source および source wildcard、または destination および destination wildcard 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 コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。

標準および拡張 ACL を作成する場合は、ACL の最後尾に達する前に一致が見つからないときに、すべてのパケットに適用される暗黙の拒否文が、デフォルトで ACL の最後尾に含まれることに注意してください。標準 ACL で、関連 IP ホスト アドレス アクセス リストの指定からマスクを省略した場合は、0.0.0.0 がマスクと見なされます。

ACL の作成後の追加は、すべてリストの末尾に置かれます。特定の ACL に ACL エントリを選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアクセス リスト *border-list* から個別の ACE を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
```

番号付き 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 から行を選択的に削除できることです。

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.38-20）を参照）、または VLAN（「VLAN マップの設定」（P.38-31）を参照）に適用できます。

ACL での時間範囲の使用

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と、時刻や週に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲名を定義し、その時間範囲内の日時や曜日を設定します。次に、ACL を適用してアクセス リストへの制限を設定する際に、定義した時間範囲名を入力します。時間範囲を使用すると、ACL 内の permit または deny ステートメントが有効な時期（指定された時間帯や指定された曜日など）を定義できます。**time-range** キーワードおよび引数については、前述の「標準および拡張 IPv4 ACL の作成」（P.38-7）および「名前付き標準および拡張 ACL の作成」（P.38-15）の名前付き拡張 ACL および番号付き拡張 ACL の作業表を参照してください。

時間範囲を使用すると、次のような利点があります。

- （IP アドレス/マスクのペアとポート番号で識別される）アプリケーションなどのリソースへのユーザ アクセスの許可または拒否をより細かく制御できます。
- ロギング メッセージを制御できます。特定の時刻のトラフィックだけを記録するように ACL エントリを設定できます。このため、ピーク時に生成される多数のログを分析しなくても、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 リストは CPU のアクティビティをトリガーします。これは、このアクセス リストの新しい設定を他の機能や、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 リストを短時間に連続で（互いに数分以内で）有効化する設定は行わないよう注意してください。

（注） 時間範囲はスイッチのシステム クロックに依存するため、信頼できるクロック ソースが必要です。スイッチ クロックの同期には、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を使用す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わかりやすい名前（たとえば *workhours*）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。名前にはスペースまたは引用符を含めることはできません。また、名前の先頭は文字にする必要があります。
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*	適用対象の機能の動作可能時期を指定します。 • 時間範囲で使用できる **absolute** ステートメントは 1 つだけです。absolute ステートメントを複数設定した場合は、最後に設定したステートメントだけが実行されます。 • **periodic** ステートメントは複数入力できます。たとえば、平日と週末に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**	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）設定をコンフィギュレーション ファイルに保存します。

異なる時間に有効化する項目が複数ある場合は、これらの手順を繰り返します。

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、*workhours* の時間範囲を設定し、会社の休日を 2006 年 1 月 1 日に設定して、設定内容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 に時間範囲名を入力します。次に、定義された休日の時間中は任意の送信元から任意の宛先への TCP トラフィックを拒否し、業務時間中はすべての TCP トラフィックを許可する拡張アクセス リスト 188 を作成および確認する例を示します。

```
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 でのコメント付け

remark キーワードを使用すると、任意の IP 標準 ACL または IP 拡張 ACL 内のエントリに関するコメント（備考）を付けることができます。remark を使用すると、ACL がわかりやすく、またスキャンしやすくなります。各 remark 行は 100 文字以内に制限されています。

remark は、permit または deny ステートメントの前後どちらにでも設定できます。どの remark ステートメントがどの permit または deny ステートメントを説明しているかが明確になるように、remark の位置は一貫性を保ってください。たとえば、関連付けられている permit または deny ステートメントの前に付く remark と後ろに付く remark が混在していると、わかりにくくなってしまいます。

IP 番号付き標準 ACL または IP 番号付き拡張 ACL にコメントを付けるには、**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。remark を削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションのアクセスは許可され、Smith のワークステーションのアクセスは許可されません。

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

次の例では、Jones のサブネットによる発信 Telnet の使用が許可されません。

```
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

番号付き 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。名前付き ACL は回線に適用できません。ユーザはどの仮想端末回線にも接続を試行できるため、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。

ACL をインターフェイスに適用する手順については、「インターフェイスへの IPv4 ACL の適用」（P.38-20）を参照してください。ACL を VLAN に適用する方法については、「VLAN マップの設定」（P.38-31）を参照してください。

仮想端末回線と ACL 内のアドレス間の着信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* には、回線タイプの指定時に設定する連続グループ内で最初の回線番号が入ります。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（装置に対する）仮想端末回線とアクセス リスト内の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 コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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

次の注意事項を確認してください。

- レイヤ 2 ポートには、着信方向にだけ ACL を適用してください。
- レイヤ 3 インターフェイスでは、発信側または着信側のいずれかに ACL を適用してください。
- インターフェイスへのアクセスを制御する場合は、名前付きまたは番号付き ACL を使用できます。
- ACL を VLAN のメンバーであるポートに適用した場合、ポート ACL の方が VLAN インターフェイスに適用された ACL より優先されます。
- VLAN のメンバーになっているレイヤ 2 インターフェイスに ACL を適用すると、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レイヤ 3 ACL や VLAN に適用された VLAN マップよりも優先されます。ポート ACL は、レイヤ 2 ポートで受信した着信パケットを常にフィルタリングします。

- ルーティングがイネーブルでない状態で、レイヤ 3 インターフェイスに ACL を適用すると、CPU 宛てのパケット（SNMP、Telnet、Web トラフィックなど）だけがこの ACL によってフィルタリングされます。ACL をレイヤ 2 インターフェイスに適用する場合、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は、ルータ ACL はプライマリ VLAN SVI にだけ適用できます。ACL はプライマリ VLAN 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、デフォルトでルータがインターネット制御メッセージ プロトコル（ICMP）到達不能メッセージを送信します。アクセス グループによって拒否されたパケットはハードウェアで廃棄されるのではなく、ICMP 到達不能メッセージを生成できるようにスイッチの CPU にブリッジされます。

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	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*	設定対象とな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**}	指定のインターフェイス宛て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 コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定のアクセス 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、この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 gigabitethernet1/1
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）に適用する場合は、インターフェイスが IP アドレスで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 上のレイヤ 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。VLAN 内でブリッジされるパケットには影響しません。

着信 ACL では、スイッチは、パケットを受信すると、ACL と照合することでそのパケットを確認します。ACL がパケットを許可する場合、スイッチはパケットの処理を続行します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL では、スイッチは、パケットを受信してそれを制御されたインターフェイスへ送信したあと、ACL と照合することでそのパケットを確認します。ACL がパケットを許可する場合、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

パケットが入力インターフェイス上の ACL によって廃棄されたか出力インターフェイス上の ACL によって廃棄されたかに関係なく、パケットが廃棄されるたびに、デフォルトで入力インターフェイスが ICMP 到達不能メッセージを送信します。ICMP 到達不能メッセージは通常、入力インターフェイスあたり 1/2 秒につき 1 つまでに制限されていますが、**ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用すると、これを変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチはその ACL がインターフェイスに適用されていないかのように動作し、すべてのパケットを許可します。ネットワーク セキュリティ用に未定義の ACL を使用する場合は、この動作に注意してください。

IP ACL のハードウェアおよびソフトウェアの処理

ACL 処理は主にハードウェアで行われますが、ソフトウェア処理のために一部のトラフィック フローを CPU に転送する必要があります。ハードウェアが ACL 設定の格納容量に達すると、パケットが転送のために 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に比べると、大幅に小さくなります。

（注） スイッチがリソース不足状態になっているためにハードウェアで ACL 設定を実装できない場合は、そのスイッチに到着する対象 VLAN 内のトラフィックだけが影響を受けます（ソフトウェアで転送されます）。パケットのソフトウェア転送で消費される CPU サイクル数によっては、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。

ルータ ACL の場合は、次のような他の要因によってパケットが CPU に送信される可能性があります。

- **log** キーワードの使用
- ICMP 到達不能メッセージの生成

トラフィック フローの記録と転送の両方が行われる場合、転送はハードウェアによって行われますが、記録はソフトウェアによって行う必要があります。ハードウェアとソフトウェアのパケット処理能力は異なるため、記録される全フロー（許可フローと拒否フローの両方）の合計の帯域幅がかなり大きい場合は、転送されるパケットの一部を記録できない可能性があります。

ルータ ACL の設定をハードウェアで適用できない場合、ルーティングする必要のある VLAN に着信するパケットはソフトウェアではルーティングされますが、ハードウェアではブリッジされます。ACL によって大量のパケットが CPU に送信される場合は、スイッチ 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 コマンドの出力に表示されるマッチ カウントは、ハードウェアでアクセス制御されるパケットに対応しません。スイッチド パケットおよびルーテッド パケットの基本的なハードウェア ACL 統計情報を取得するには、**show access-lists hardware counters** 特権 EXEC コマンドを使用します。

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の場合、

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

スイッチには ACL のハードウェア表現を作成するためのリソースが不足していることになります。リソースにはハードウェア メモリやラベル スペースが含まれますが、CPU メモリは含まれません。この問題は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足が原因と考えられます。論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での **eq** 以外（**ne**、**gt**、**lt**、**range**）のテストで必要です。

次のいずれかの回避策を実行してください。

- ACL 設定を変更して使用するリソースを減らします。
- ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

特殊なハードウェア リソースを判別するには、**show platform layer4 acl map** 特権 EXEC コマンドをを入力します。スイッチに使用可能なリソースがない場合の出力には、インデックス 0 ～ インデックス 15 が使用可能でないことが示されます。

リソースが不十分な状態での ACL の設定の詳細については、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した場合で、

```
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
```

なおかつ次のメッセージが表示された場合は、

```
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ないことになります。この問題を回避するには、次のようにします。

- **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 番めの ACE を最初の 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

- 他の ACL よりも英数字順で先に表示される名前または番号に ACL の名前を変更します（たとえば、ACL *79* から ACL *1* に変更します）。

これで、ACL 内の最初の ACE をインターフェイスに適用できます。スイッチはこの ACE を Opselect インデックス内の使用可能なマッピング ビットに割り当てたあと、フラグ関連の演算子を割り当てて Ternary Content Addressable Memory（TCAM; 三値連想メモリ）内の同じビットを使用します。

ルータ ACL は次のように機能します。

- ハードウェアは標準および拡張 ACL（入力および出力）の許可アクションと拒否アクションを制御して、セキュリティ アクセス制御を実現します。
- **log** が指定されていない場合、セキュリティ ACL 内の *deny* ステートメントに一致するフローはハードウェアによって廃棄されます（*ip unreachables* がディセーブルに設定されている場合）。*permit* ステートメントと一致するフローは、ハードウェアでスイッチングされます。

- ルータ ACL 内の ACE に **log** キーワードを追加すると、ロギングだけの目的でパケットのコピーが CPU に送信されます。ACE が *permit* ステートメントの場合でも、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。

IPv4 ACL の設定例

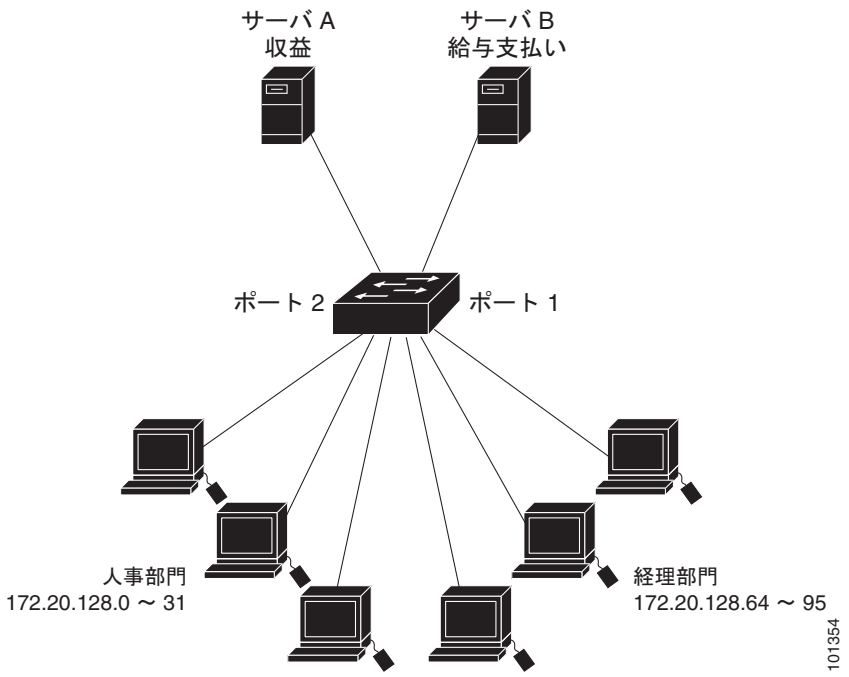
ここでは、IPv4 ACL の設定例と適用例を示します。ACL のコンパイルの詳細については、『*Cisco IOS Security Configuration Guide, Release 12.2*』および『*Cisco IOS IP Configuration Guide, Release 12.2*』にある「IP Addressing and Services」の「Configuring IP Services」を参照してください。

図 38-3 に、サーバ A に接続されたルーテッド ポート 2 と、サーバ B に接続されたルーテッド ポート 1 を使用した小規模なネットワーク オフィス環境を示します。サーバ A には全従業員がアクセスできる収益などの情報が格納されており、サーバ B には機密の給与支払いデータが格納されています。サーバ A にはユーザ全員がアクセスできますが、サーバ B のアクセスは制限されます。

ルータ ACL を使用してこれを実現するには、次のいずれかの方法を用います。

- 標準 ACL を作成して、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 を作成して、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 38-3　　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 からの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のルーテッド ポート 1 からのトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch #show access-lists
Standard IP access list 6
 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
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 への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 へのトラフィックに適用され、指定した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
 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 106 in
```

番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番めのオクテットはサブネットを指定するクラス A ネットワークです。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク 36.0.0.0 のアドレスの 3 番めと 4 番めのオクテットは、特定のホストを指定します。スイッチは、アクセス リスト 2 を使用してサブネット 48 上のアドレスを 1 つ受け入れ、このサブネット上の他のアドレスはすべて拒否します。リストの最後の行は、スイッチがネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスを受け入れることを示しています。この ACL はポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

次の例の最初の行は、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 のシンプル メール転送プロトコル（SMTP）ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface gigabitethernet0/1
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip access-group 102 in
```

この例で、ネットワークがインターネットに接続されている状態で、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 接続を形成できるようにするとします。ただし、IP ホストは、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への TCP 接続を形成できないようにします。

SMTP は、接続の一端では TCP ポート 25 を使用し、他端ではランダムなポート番号を使用します。接続の間は、同じポート番号が使用されます。インターネットからの着信メール パケットの宛先ポートは 25 です。発信パケットでは、ポート番号が逆になります。ネットワークのセキュア システムはポート 25 上のメール接続を常に受け入れるため、着信サービスと発信サービスは個別に制御されます。ACL は、発信インターフェイス上では入力 ACL として設定し、着信インターフェイス上では出力 ACL として設定する必要があります。

次の例のネットワークはアドレス 128.88.0.0 のクラス B ネットワークであり、メール ホスト アドレスは 128.88.1.2 です。**established** キーワードは TCP だけに使用され、確立された接続を示します。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われ、パケットが既存の接続に属していることを示します。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 gigabitethernet1/1
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 からのトラフィックをすべて許可します。

```
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、宛先のアドレスおよびワイルドカード 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、それ以外の TCP トラフィックをすべて拒否します。この ACL は、ICMP トラフィックを許可し、任意の送信元から 1024 より小さい宛先ポートの 171.69.0.0 ～ 179.69.255.255 の宛先アドレス範囲への UDP トラフィックを拒否し、それ以外の IP トラフィックをすべて拒否して、結果のログを表示します。

```
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 ポート上の着信トラフィックに適用されます。

```
Switch(config)# interface gigabitethernet1/1
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 上の HTTP トラフィックを拒否します。この例では、土曜日と日曜日の正午～午後 8 時（20 時）の間だけ 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 gigabitethernet1/1
Switch(config-if)# ip access-group strict in
```

コメント付き IP ACL エントリ

次の例の番号付き ACL では、Jones のワークステーションのアクセスは許可され、Smith のワークステーションのアクセスは許可されません。

```
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
```

次の例の番号付き ACL では、Winter および Smith のワークステーションでの Web 閲覧が許可されません。

```
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
```

次の例の名前付き ACL では、Jones のサブネットのアクセスが許可されます。

```
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
```

次の例の名前付き ACL では、Jones のサブネットによる発信 Telnet の使用が許可されません。

```
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 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** キーワードは、エントリと一致するパケットの詳細を示すロギング メッセージをコンソールに送信します。**log-input** キーワードは、ログ エントリに入力インターフェイスを含めます。

次の例の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は許可し、**log** キーワードを含めます。

```
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 gigabitethernet1/1
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
```

次の例の名前付き拡張アクセス リスト *ext1* は、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、UDP パケットはすべて拒否します。

```
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 gigabitethernet1/1
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 のロギング エントリはすべて `%SEC-6-IPACCESSLOG` で始まりますが、ACL の種類および一致するアクセス エントリによっては、形式が若干異なります。

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

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

log キーワードを使用した同じ種類のパケットのログ 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 上またはレイヤ 2 インターフェイス上の非 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。この手順は、他の名前付き拡張 ACL の設定手順と同様です。

（注）　名前付き MAC 拡張 ACL を、レイヤ 3 インターフェイスに適用できません。

mac access-list extended コマンドでサポートされる非 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 ストリングには表示されますが、**deny** および **permit** MAC アクセス リスト コンフィギュレーション モード コマンドの一致条件としてはサポートされていません。

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、**permit** または **deny** を、**すべての（any）**送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定の **host** 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 アドレスに指定します。 （任意）次のオプションも入力できます。 • *type mask*：Ethernet II または Subnetwork Access Protocol（SNAP; サブネットワーク アクセス プロトコル）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）。一致をテストする前に *don't care* ビットのマスクが EtherType に任意で適用されます。 • **lsap** *lsap mask*：IEEE 802.2 カプセル化を使用したパケットの LSAP 番号（10 進数、16 進数、または 8 進数）。*don't care* ビットのマスクが任意で付加されます。 • **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*：プライオリティの設定に使用する 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 コンフィギュレーションを表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。名前付き MAC 拡張 ACL から個別の ACE を削除することもできます。

次に、*mac1* という名前のアクセス リストを作成および表示して、EtherType DECnet Phase IV トラフィックだけを拒否し、それ以外のタイプのトラフィックはすべて許可する例を示します。

```
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 を作成したら、それをレイヤ 2 インターフェイスに適用して、このインターフェイスへの非 IP トラフィックをフィルタリングできます。MAC ACL の適用時は、次の注意事項を考慮してください。

- VLAN のメンバーになっているレイヤ 2 インターフェイスに ACL を適用すると、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レイヤ 3 ACL や VLAN に適用された VLAN マップよりも優先されます。レイヤ 2 ポート上で受信した着信パケットは常に、そのポート 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は、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アクセス リストは 1 つだけです。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、以前に設定されていた ACL は新しい ACL で置換されます。

MAC アクセス リストを適用してレイヤ 2 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	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。この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）を指定する必要があります。
ステップ 3	**mac access-group** {*name*} {**in**}	MAC アクセス リストを使用して、指定のインターフェイス宛てのアクセスを制御します。 ポート ACL は、着信方向でだけサポートされます。
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*]	こ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）設定をコンフィギュレーション ファイルに保存します。

指定のアクセス 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 MAC アクセス リスト *mac1* を適用して、この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 gigabitethernet1/1
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る場合だけ有効です。EtherChannel ポート チャネルにはこのコマンドを使用できません。

スイッチはパケットを受信すると、着信 ACL と照合することでそのパケットを確認します。ACL がパケットを許可する場合、スイッチはパケットの処理を続行します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチはその ACL が適用されていないかのように動作し、すべてのパケットを許可します。ネットワーク セキュリティ用に未定義の ACL を使用する場合は、この動作に注意してください。

VLAN マップの設定

ここでは、VLAN マップの設定する方法を説明します。これは、VLAN 内の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の ACL を含める必要があります。VLAN マップにそのパケット タイプ（IP または MAC）に対する match コマンドがある場合、デフォルトのアクションでは、マップ内のどのエントリとも一致しないパケットは廃棄されます。そのパケット 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。

この項で使用しているコマンドの構文と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、それを 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 に適用する標準または拡張 IPv4 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.38-7）および「VLAN マップの作成」（P.38-33）を参照してください。

ステップ 2　**vlan access-map** グローバル コンフィギュレーション コマンドを入力して、VLAN ACL マップ エントリを作成します。

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、任意で、**action**（**forward**（デフォルト）または **drop**）を入力します。また、**match** コマンドを入力して、（既知の MAC アドレスだけを格納した）IP パケットまたは非 IP パケットを指定し、このパケットを 1 つまたは複数の ACL（標準または拡張）と照合します。

（注）　VLAN マップが特定のパケット タイプ（IP または MAC）に対する match コマンドで設定されていて、マップ アクションが drop の場合は、このタイプと一致するパケットがすべて廃棄されます。VLAN マップに match コマンドがなく、設定されたアクションが drop の場合は、IP パケットとレイヤ 2 パケットがすべて廃棄されます。

ステップ 4　**vlan filter** グローバル コンフィギュレーション コマンドは、VLAN マップを 1 つまたは複数の VLAN に適用します。

ここでは、次の設定情報について説明します。

VLAN マップ設定時の注意事項

VLAN マップを設定する場合、次の注意事項に従ってください。

- インターフェイス上のトラフィックを拒否するよう設定された ACL がなく、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 マップ内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 マップ内の最初のエントリと照合してテストされます。パケットが一致する場合は、VLAN マップのその部分に対して指定されたアクションが実行されます。一致しない場合は、パケットはマップ内の次のエントリと照合してテストされます。
- VLAN マップに特定のパケット タイプ（IP または MAC）に対する match コマンドが少なくとも 1 つあり、パケットがこれらの match コマンドのいずれとも一致しない場合、デフォルトではそのパケットが廃棄されます。VLAN マップ内にそのパケット 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。
- ACL が多数設定されていると、システムの起動に時間が掛かる可能性があります。
- ロギングは VLAN マップではサポートされません。
- スイッチが IP アクセス リストまたは MAC アクセス リストをレイヤ 2 インターフェイスに適用させている状態で、ポートが属する VLAN に VLAN マップを適用した場合、ポート ACL は VLAN マップよりも優先されます。
- VLAN マップの設定をハードウェアで適用できない場合、この VLAN 内のすべてのパケットをソフトウェアによってブリッジおよびルーティングする必要があります。
- プライマリ VLAN およびセカンダリ VLAN では 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 VLAN とセカンダリ VLAN には、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 内でレイヤ 2 転送される場合、入力側と出力側で同じ VLAN マップが適用されます。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 マップは入力側で適用されます。
  - ホスト ポートからプロミスキャス 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 で設定された VLAN マップが適用されます。
  - プロミスキャス 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 で設定された 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、プライマリ VLAN とセカンダリ VLAN の両方に VLAN マップを適用する必要があります。プライベート VLAN の詳細については、第 19 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」（P.38-36）を参照してください。

ルータ ACL と VLAN マップの両方の使用については、「VLAN マップおよびルータ ACL 設定時の注意事項」（P.38-38）を参照してください。

VLAN マップの作成

各 VLAN マップは、順序指定された一連のエントリで構成されます。VLAN マップ エントリの作成、追加、削除を行うには、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、マップに名前と（任意で）番号を付けます。この番号は、マップ内のエントリのシーケンス番号になります。 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。マップの修正または削除時には、修正または削除するマップ 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 モードになります。
ステップ 3	**action** {**drop** | **forward**}	（任意）マップ エントリのアクションを設定します。デフォルトは forward です。
ステップ 4	**match** {**ip** | **mac**} **address** {*name* | *number*} [*name* | *number*]	（IP アドレスまたは MAC アドレスを使用している）パケットを 1 つまたは複数の標準または拡張アクセス リストと照合します。パケットは正しいプロトコル タイプのアクセス リストだけと照合されます。IP パケットは標準または拡張 IP アクセス リストと照合されます。非 IP パケットは名前付き MAC 拡張アクセス リストだけと照合されます。
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 コンフィギュレーションを表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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。マップ内から 1 つのシーケンス 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（forward）を適用するには、**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 キーワードや deny キーワードは使用しません。VLAN マップを使用してパケットを拒否するには、そのパケットと一致する ACL を作成し、アクションを drop に設定します。ACL 内の permit は一致と見なされます。ACL 内の deny は不一致と見なされます。

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

次に、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）と一致するパケットがすべて廃棄されます。最初に、任意の TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1*ACL を作成します。VLAN マップには IP パケットに対する match コマンドがあるため、デフォルトのアクションでは、どの match コマンドとも一致しない IP パケットは廃棄されます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
```

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

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*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、これまでのどの ACL とも一致しなかった IP パケット（つまり、TCP パケットでも UDP パケットでもないパケット）がすべて廃棄されます。

```
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 パケットに対してデフォルトのアクション drop と、MAC パケットに対してデフォルトのアクション forward が設定されています。このマップを標準 ACL 101 と、名前付き拡張アクセス リスト **igmp-match** および **tcp-match** とともに使用すると、次のような結果になります。

- UDP パケットはすべて転送されます。
- IGMP パケットはすべて廃棄されます。
- TCP パケットはすべて転送されます。
- その他の IP パケットはすべて廃棄されます。
- 非 IP パケットはすべて転送されます。

```
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 パケットに対してデフォルトのアクション drop と、IP パケットに対してデフォルトのアクション forward が設定されています。このマップを MAC 拡張アクセス リスト **good-hosts** および **good-protocols** とともに使用すると、次のような結果になります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットは転送されます。
- decnet-iv または vines-ip プロトコルを使用した MAC パケットは転送されます。
- その他の非 IP パケットはすべて廃棄されます。
- IP パケットはすべて転送されます。

```
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（IP および非 IP）に対してデフォルトのアクション drop が設定されています。このマップを例 2 および 3 のアクセス リスト **tcp-match** および **good-hosts** とともに使用すると、次のような結果になります。

- TCP パケットはすべて転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットは転送されます。
- その他の IP パケットはすべて廃棄されます。
- その他の MAC パケットはすべて廃棄されます。

```
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

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）、連続する範囲（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のスペースは任意です。
ステップ 3	**show running-config**	アクセス リスト コンフィギュレーションを表示します。
ステップ 4	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

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
```

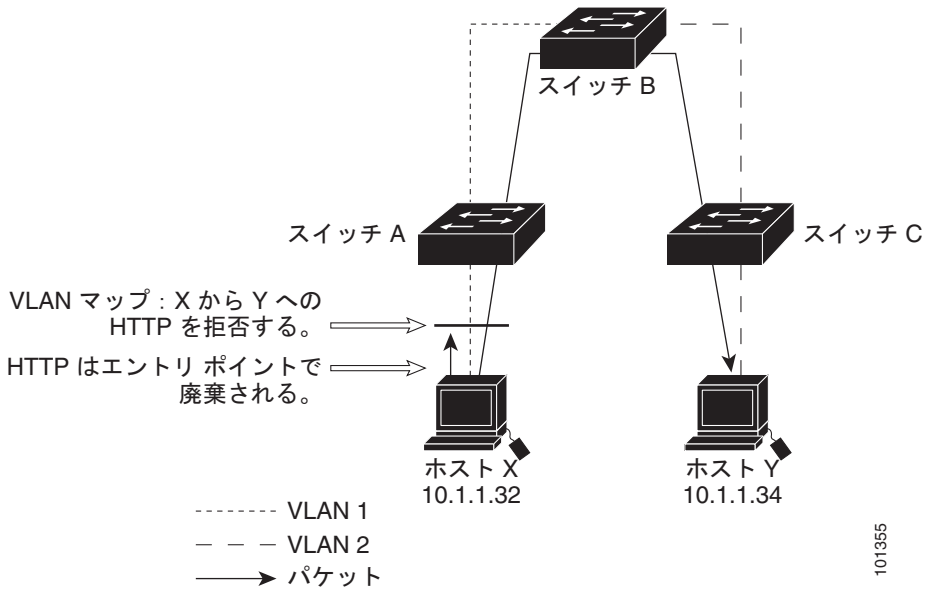
ネットワークでの VLAN マップの使用

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。

配線クローゼットの設定

配線クローゼットの設定では、スイッチ上でルーティングがイネーブルでない可能性があります。この設定でも、スイッチは VLAN マップと QoS 分類 ACL をサポートできます。図 38-4 では、ホスト X とホスト Y が異なる VLAN 内にあり、配線クローゼットのスイッチ A と C にそれぞれ接続されていると仮定します。ホスト X からホスト Y へのトラフィックは最終的にスイッチ B（ルーティングがイネーブルになっているレイヤ 3 スイッチ）によって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 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 38-4　　配線クローゼットの設定



HTTP トラフィックがホスト X からホスト Y にスイッチングされないようにするには、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 トラフィックをスイッチ A ですべて廃棄し、トラフィックをスイッチ B にブリッジしないように、スイッチ A 上の VLAN マップを設定できます。

まず、HTTP ポート上で任意の 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、VLAN アクセス マップ *map2* を作成して、*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 IP トラフィックはすべて転送されるようにします。

```
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。

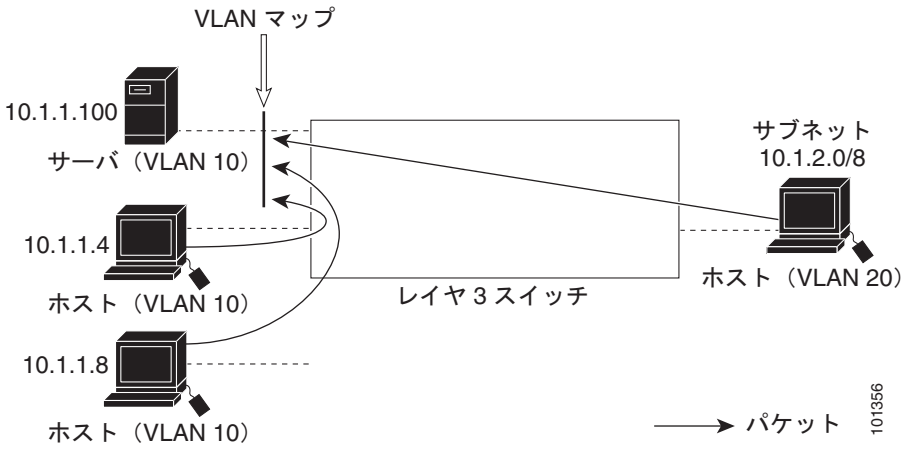
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN 上のサーバへのアクセスの拒否

別の VLAN 上の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 38-5 を参照）。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストがアクセスできないようにします。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 がアクセスできないようにします。

図 38-5　別の VLAN 上のサーバへのアクセスの拒否



次に、サブネット 10.1.2.0.8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 へのアクセスを拒否し、その他の IP トラフィックは許可する VLAN マップ SERVER 1 を作成して、別の VLAN 上のサーバへのアクセスを拒否する例を示します。最後に、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　この ACL を使用して、SERVER1_ACL と一致する IP パケットを廃棄し、ACL と一致しない IP パケットを転送する 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　この VLAN マップを VLAN 10 に適用します。

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

VLAN マップとルータ ACL の併用

ブリッジド トラフィックとルーテッド トラフィックの両方をアクセス制御する場合、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。入力と出力の両方のルーテッド VLAN インターフェイスでルータ ACL を定義し、ブリッジド トラフィックをアクセス制御する VLAN マップを定義できます。

パケット フローが ACL 内の VLAN マップの deny コマンドと一致する場合は、ルータ ACL の設定に関係なく、パケット フローが拒否されます。

（注）　ルータ ACL と VLAN マップを併用する際には、ルータ ACL でのロギングの必要があるパケットは、VLAN マップで拒否された場合、記録されません。

VLAN マップにパケット タイプ（IP または MAC）に対する match コマンドがあり、パケットがそのタイプと一致しない場合、デフォルトではそのパケットが廃棄されます。VLAN マップに match コマンドがなく、アクションが指定されていない状態で、パケットがどの VLAN マップ エントリとも一致しない場合は、そのパケットが転送されます。

ここでは、VLAN マップとルータ ACL の併用について説明します。

- 「VLAN マップおよびルータ ACL 設定時の注意事項」（P.38-38）
- 「VLAN に適用されたルータ ACL および VLAN マップの例」（P.38-39）

VLAN マップおよびルータ ACL 設定時の注意事項

次の注意事項は、同じ VLAN 上でルータ ACL *および*VLAN マップを使用する必要がある設定に適用されます。これらの注意事項は、ルータ ACL と VLAN マップを異なる VLAN 上にマッピングする設定には適用されません。

スイッチのハードウェアには、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。このため、ルータ ACL と VLAN マップが同じ VLAN 上で設定されている場合は、これらを結合する必要があります。ルータ ACL と VLAN マップを結合すると、ACE の数が大幅に増える可能性があります。

ルータ ACL と VLAN マップを同じ VLAN 上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ついて次の注意事項があります。

- VLAN インターフェイス上の各方向（入力および出力）に VLAN マップおよびルータの ACL を 1 つずつだけ設定できます。
- タイプが異なる場合の末尾のデフォルト アクションを除き、すべてのエントリのアクションを可能な限り単一にして ACL を記述するようにします。つまり、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 で複数のアクション（permit、deny）を定義する場合は、エントリ数を減らすために、アクション タイプごとにグループ化します。
- レイヤ 4 情報を ACL に含めないようにします。この情報を加えると、結合処理が複雑になります。完全なフロー（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）ではなく IP アドレス（送信元および宛先）に基づいて ACL をフィルタリングすると、最適な結合結果が得られます。可能な限り、IP アドレス内に *don't care* ビットを使用するのも効果的です。

  full-flow モードを指定する必要があり、ACL に IP ACE とレイヤ 4 情報を持つ TCP/UDP/ICMP ACE の両方が含まれている場合は、レイヤ 4 ACE をリストの末尾に置きます。これにより、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。

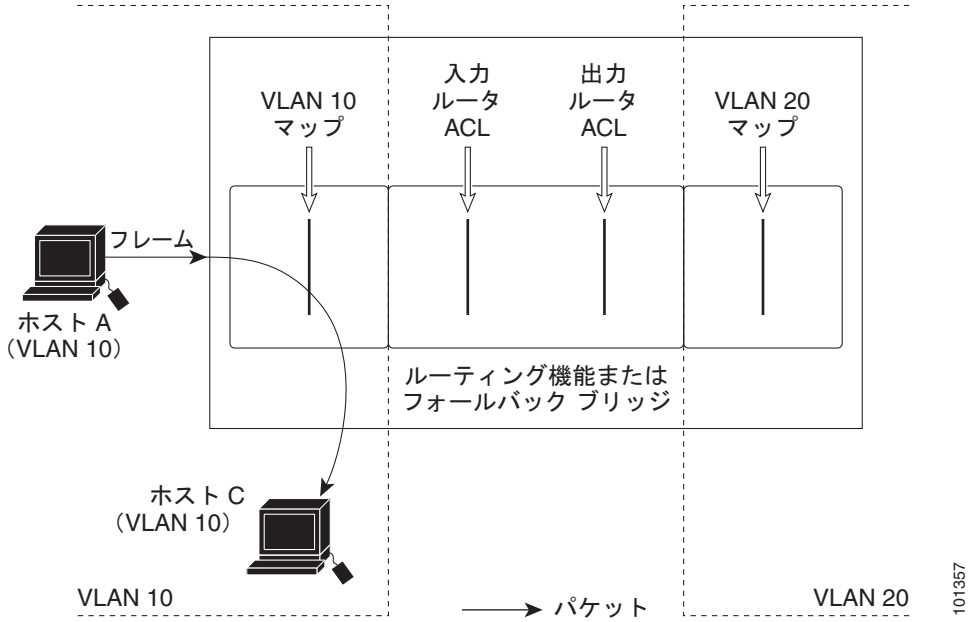
VLAN に適用されたルータ ACL および VLAN マップの例

ここでは、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 パケットを対象に、ルータ ACL と VLAN マップを VLAN に適用する例を示します。次の各図はパケットが宛先に転送される様子を示していますが、パケットのパスが VLAN マップまたは ACL を示す線を通過するたびに、パケットが転送されずに廃棄される可能性もあります。

ACL およびスイッチド パケット

図 38-6 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に 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。

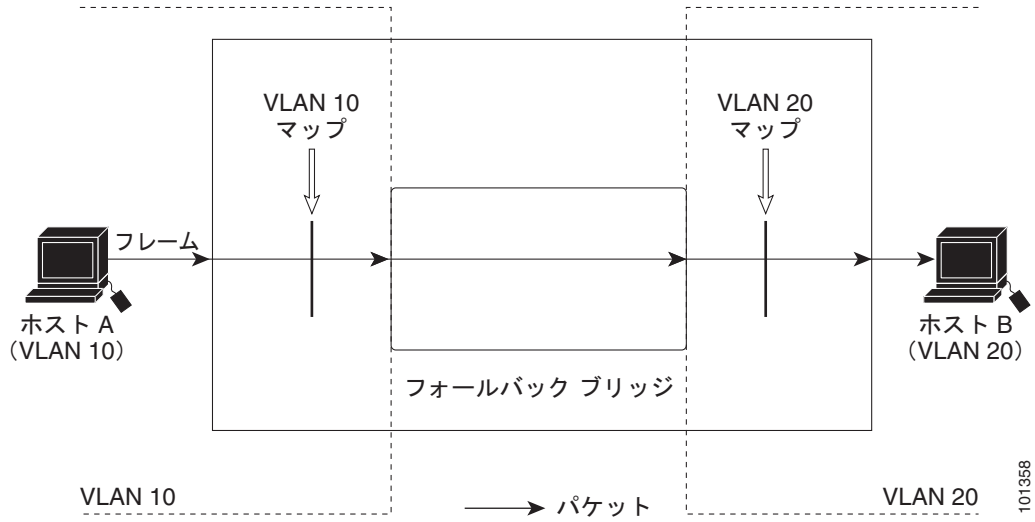
図 38-6　スイッチド パケットへの ACL の適用



ACL およびブリッジド パケット

図 38-7 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、レイヤ 2 ACL だけが入力 VLAN に適用されます。フォールバック ブリッジングが可能なのは、非 IP の非 ARP パケットだけです。

図 38-7　ブリッジド パケットへの ACL の適用

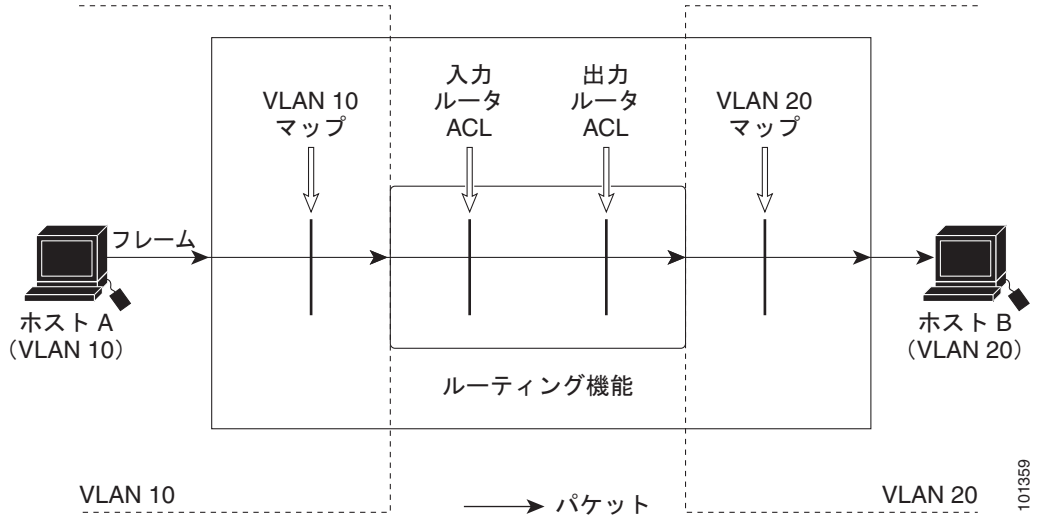


ACL およびルーテッド パケット

図 38-8 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 パケットの場合は、次の順序で ACL が適用されます。

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

図 38-8　ルーテッド パケットへの ACL の適用

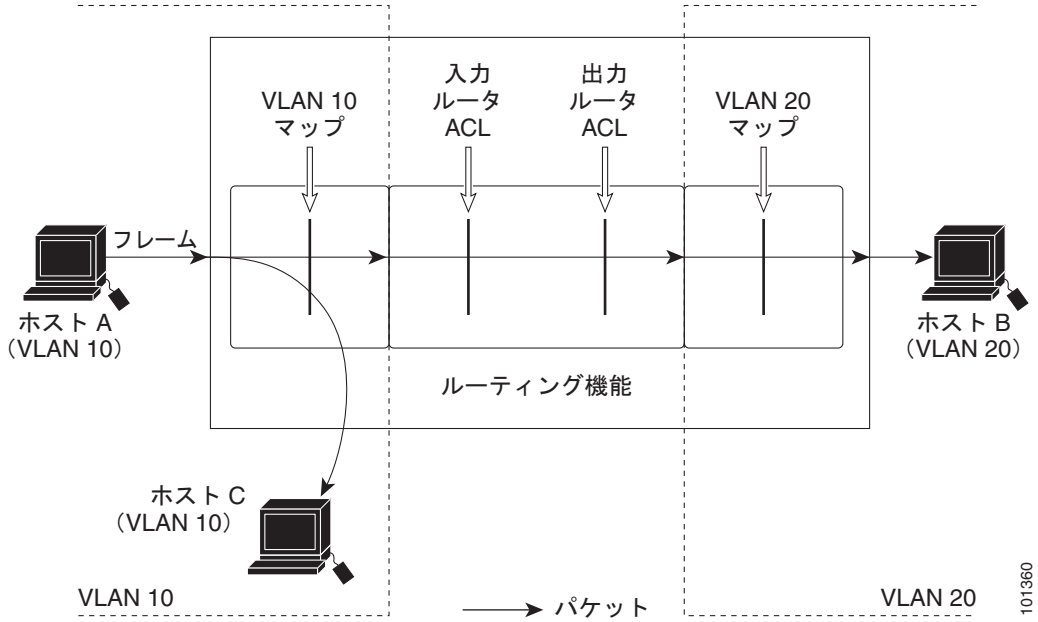


ACL およびマルチキャスト パケット

図 38-9 に、IP マルチキャスト用に複製されるパケットに 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 つの異なる種類のフィルタが適用されます。1 つは入力 VLAN 内の他のポートである宛先用のフィルタで、もう 1 つはパケットのルーティング先となった他の VLAN 内の宛先用のフィルタです。このパケットは複数の出力 VLAN にルーティングされる可能性があります。この場合、それぞれの宛先 VLAN に異なるルータ出力 ACL と VLAN マップが適用されます。

最終的な結果としては、一部の出力 VLAN ではパケットが許可され、他の VLAN では拒否される場合もあります。許可された宛先には、パケットのコピーが転送されます。ただし、入力 VLAN マップ（図 38-9 の VLAN 10）がパケットを廃棄した場合は、どの宛先もパケットのコピーを受信しません。

図 38-9　マルチキャスト パケットへの ACL の適用



IPv4 ACL 設定の表示

スイッチ上で設定された ACL や、インターフェイスおよび VLAN に適用されている 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 ACL をレイヤ 2 またはレイヤ 3 インターフェイスに適用した場合は、インターフェイス上のアクセス 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 を表示することもできます。この情報を表示するには 、表 38-2 に示す各特権 EXEC コマンドを使用します。

表 38-2　アクセス リストおよびアクセス グループを表示するためのコマンド

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（1 つまたはすべて）、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	現在のすべての IP アクセス リスト、または特定の IP アクセス リスト（番号付きまたは名前付き）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な設定およびステータスを表示します。インターフェイス上で IP がイネーブルになっていて、ACL が **ip access-group** インターフェイス コンフィギュレーション コマンドによって適用されている場合は、アクセス グループも表示されます。
show running-config [**interface** *interface-id*]	スイッチまたは指定したインターフェイスのコンフィギュレーション ファイルの内容を表示します。設定されたすべての MAC および IP アクセス リストや、インターフェイスに適用されているアクセス グループなどが表示されます。
show mac access-group [**interface** ***interface-i***d]	すべてのレイヤ 2 インターフェイスまたは指定したレイヤ 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。

また、VLAN アクセス マップまたは VLAN フィルタ に関する情報も表示できます。VLAN マップ情報を表示するには、表 38-3 に示す各特権 EXEC コマンドを使用します。

表 38-3　VLAN マップ情報を表示するためのコマンド

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や、指定された VLAN または VLAN アクセス マップに関する情報を表示します。