CHAPTER 30

ACL によるネットワーク セキュリティの設定

この章では、Access Control List（ACL; アクセス制御リスト）を使用して、Catalyst 2975 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*という用語はスタンドアロン スイッチおよびスイッチ 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 バージョン 4（IPv4）のものです。

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンド リファレンス、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章にある「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 のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References]）からご利用になれます。

この章で説明する内容は、次のとおりです。

ACL の概要

パケット フィルタリングによって、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廃棄します。スイッチは、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、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、転送またはブロックされるトラフィックの種類を決定できます。たとえば、電子メール トラフィックの転送は許可し、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 には Access Control Entry（ACE; アクセス制御エントリ）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 アクセス制御]）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、Quality of Service（QoS; サービス品質）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.32-8）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。

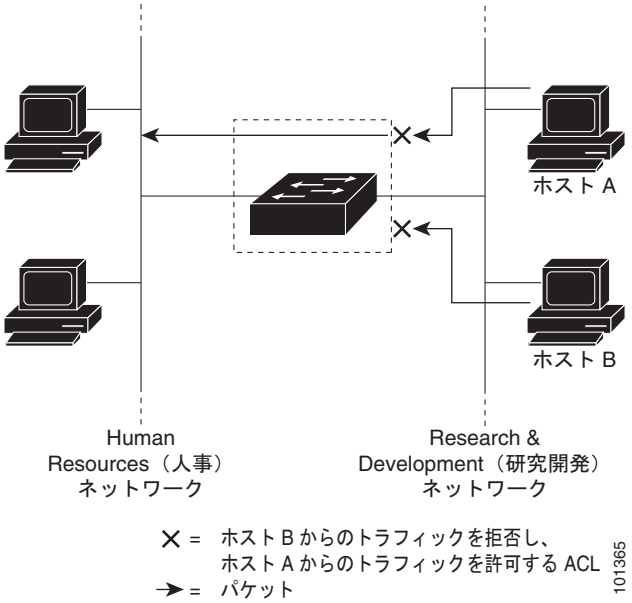
ポート ACL

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のみ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のみ適用できます。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 30-1 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のみ適用されます。

図 30-1　　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。

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、一致規則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 番目および 2 番目の 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）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 番目の 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 番目の ACE と一致しません。残りのフラグメントは 3 番目の ACE（許可）に一致します。

  最初のフラグメントが拒否されたので、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 番目の ACE（拒否）と一致します。他のフラグメントもすべて、4 番目の 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 6 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 を適用したあとにのみ、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 6 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、このとき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、シスコ製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は、『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。コマンドの詳細については、『*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 のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Configuration Guides] または [Command References]）からご利用になれます。

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 30-1（P.30-6）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）
- ACL のロギング

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。

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

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

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 30-1 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 30-1　　アクセス リスト番号

アクセス リスト番号	Type	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

表 30-1　アクセス リスト番号 （続き）

アクセス リスト番号	Type	サポート
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。

番号制標準 ACL の作成

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

	コマンド	目的
ステップ 1	**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*]	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。
ステップ 3	**end**	イネーブル 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.30-16）を参照）、およびインターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.30-17）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*

上記のマニュアルは、Cisco.com のホームページ（[Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References]）からご利用になれます。

（注） スイッチは、動的アクセス 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; サービス タイプ）ビットに基づくフィルタリングもサポートしていません。

サポートされているパラメータは、TCP、UDP、ICMP、IGMP、または他の IP のカテゴリにグループ化できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2a	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] （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。 *プロトコルには*、IP プロトコルの **ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、**udp** の名前または番号、もしくは IP プロトコル番号を表す 0 ～ 255 の整数を入力します 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。 • **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.30-14）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**] [**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**] [**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**] [**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 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときは、TCP ポートの番号または名前のみを使用します。 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。

	コマンド	目的
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**] [**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。
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**] [**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 12.2 の「Configuring IP Services」を参照してください。
ステップ 2e	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**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**	イネーブル 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 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.30-16）を参照）、およびインターフェイス（「インターフェイスへの IPv4 ACL の適用」（P.30-17））を参照）に適用できます。

ACL 内の ACE シーケンスの再編集

新しく ACL を作成すると、アクセス リスト内のエントリのシーケンス番号が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。

ip access-list resequence コマンドの詳細については、次の URL にアクセスしてください。

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

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。
- 標準 ACL と拡張 ACL に同じ名前を使用できません。
- 「標準および拡張 IPv4 ACL の作成」（P.30-6）で説明したとおり、番号制 ACL を使用することもできます。

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

	コマンド	目的
ステップ 1	**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**} または **permit** {*source* [*source-wildcard*] | **host** *source* | **any**}	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廃棄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**	イネーブル 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。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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**] [**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。 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.30-8）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**	イネーブル EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**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 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.30-17）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.30-6）および「名前付き標準および拡張 ACL の作成」（P.30-12）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。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新規設定を他の機能や、Ternary CAM（TCAM）にロードされた結合済みの設定と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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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 つのみ使用できます。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**	イネーブル 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.30-17）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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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**	イネーブル 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のみ適用してください。
- インターフェイスへのアクセスを制御する場合、名前付きまたは番号制 ACL を使用できます。

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

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in**}	指定したインターフェイスへのアクセスを制御します。
ステップ 4	**end**	イネーブル 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。

指定したアクセス グループを削除するには、**no ip access-group** {*access-list-number* | *name*} {**in**} 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
Switch(config-if)# ip access-group 2 in
```

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。

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。

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 イネーブル 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 イネーブル 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 マネージャのメッセージが表示され、[chars] が access-list の名前である場合、

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

ACL のハードウェア表示を作成するリソースが、スイッチに不足しています。リソースには、ハードウェア メモリとラベル スペースは含まれていますが、CPU メモリは含まれていません。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 リソースが不足していると、この問題が起こります。論理演算ユニットは、TCP、UDP、SCTP の各ポート番号における TCP フラグの一致または **eq** (**ne**、**gt**、**lt**、**range**) 以外のテストに必要です。

次のいずれかの回避策を使用してください。

- ACL の設定を修正して、使用するリソースを減らす。
- ACL の名前または番号を、その ACL の名前または番号よりも英数字的に先頭に近いものに変更する。

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** イネーブル EXEC コマンドを実行します。スイッチに利用できるリソースがない場合、索引 0 から索引 15 が利用できないと出力されます。

リソースが不足している場合の 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する場合

```
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
```

さらに、次のメッセージが表示される場合

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

フラグ関連の演算子は利用できません。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 番目の ACE を最初の ACE の前に移動する。

  ```
  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 の名前または番号を、他の ACL の名前または番号よりも英数字的に先頭に近いものに（たとえば、ACL *79* を ACL *1* に）変更する。

これで、ACL の最初の ACE をインターフェイスに適用できます。スイッチでは、ACE が、Opselect 索引内の利用可能なマッピング ビットに割り当てられたあと、同じビットを TCAM で使用するようフラグ関連の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 12.2、および『*Cisco IOS IP Configuration Guide*』Release 12.2 の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。

次に、標準 ACL を使用してアドレス 172.20.128.64 を持つ特定のインターネット ホストへのポート アクセスを許可する例を示します。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
   10 permit 172.20.128.64 wildcard bits 0.0.0.0
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 6 in
```

次に、拡張 ACL を使用してポート 80（HTTP）からのポート トラフィックを拒否する例を示します。ここでは、他のタイプのトラフィックはすべて許可します。

```
Switch(config)# access-list 106 deny tcp any any eq 80
Switch(config)# access-list 106 permit ip any any
Switch(config)# end
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 106 in
```

番号制 ACL

この ACL は、ネットワーク 36.0.0.0 サブネット上のアドレスを受け入れて、56.0.0.0 サブネットからのパケットをすべて拒否します。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 36.0.0.0 0.255.255.255
Switch(config)# access-list 2 deny 56.0.0.0 0.255.255.255
```

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL

この例では、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。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、着信サービスを制御できます。

```
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 gigabitethernet1/0/1
Switch(config-if)# ip access-group 102 in
```

名前付き ACL

次に、*marketing_group* という名前の拡張 ACL を作成する例を示します。*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。ここでは、他の IP トラフィックはすべて許可します。

```
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 ip any any
Switch(config-ext-nacl)# exit
```

marketing_group ACL は、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)# 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）の間のみ許可されます。

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

コメント付き IP ACL エントリ

次に示す番号指定 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
```

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。

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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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。

	コマンド	目的
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**	イネーブル 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。

- 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 パケットのみ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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
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、着信方向のみサポートします。
ステップ 4	**end**	イネーブル EXEC モードに戻ります。
ステップ 5	**show mac access-group** [**interface** *interface-i*d]	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のみ有効となります。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。

IPv4 ACL の設定の表示

スイッチ上に設定されている ACL、およびインターフェイスに適用された 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 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、イネーブル EXEC コマンドを使用します（表 30-2 を参照）。

表 30-2　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 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。