



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 2950 または Catalyst 2955 スイッチでネットワーク 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。

ACL は物理インターフェイス用または管理インターフェイス用に作成できます。管理インターフェイスは、管理 VLAN として、または SNMP (簡易ネットワーク管理プロトコル)、Telnet、Web トラフィックなどのように CPU に直接送られるトラフィックとして定義されます。スイッチに Standard Software Image (SI; 標準ソフトウェアイメージ) または Enhanced Software Image (EI; 拡張ソフトウェアイメージ) がインストールされている場合は、管理インターフェイス用の ACL を作成できます。ただし、ACL を物理インターフェイスに適用するには、スイッチに EI をインストールしておく必要があります。



(注)

物理インターフェイスに適用する ACL の場合、マスクは 1 つという制限があります。また、一部のキーワードはサポートされません。詳細は、「[物理インターフェイスに ACL を適用する場合の注意事項](#)」(p.28-6) を参照してください。



(注)

この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンス、『*Cisco IOS IP and IP Routing Configuration Guide*』Release 12.1 の「Configuring IP Services」および『*Cisco IOS IP and IP Routing Command Reference*』Release 12.1 を参照してください。

この章の内容は、次のとおりです。

- [ACL の概要](#) (p.28-2)
- [ACL の設定](#) (p.28-7)
- [ACL 情報の表示](#) (p.28-23)
- [ACL の設定例](#) (p.28-25)

ACL は、CLI (コマンドライン インターフェイス) を使用して設定できます。

セキュリティ ウィザードを使用して、スイッチで着信トラフィックをフィルタリングすることもできます。フィルタリングは、ネットワーク アドレス、TCP アプリケーション、または UDP アプリケーションに基づいて行うことができます。フィルタリング条件と一致したパケットを廃棄するかまたは転送するかを選択できます。このウィザードを使用するには、ネットワークがどのように設計され、フィルタリング装置でインターフェイスがどのように使用されているかを把握する必要があります。セキュリティ ウィザードでの具体的な設定手順については、ウィザードのオンラインヘルプを参照してください。

ACL の概要

パケット フィルタリングにより、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装置に使用させるネットワークを制限できます。ACL を使用すると、スイッチを通過するトラフィックをフィルタリングし、指定されたインターフェイスでパケットを許可または拒否できます。ACL は、パケットに適用される許可条件および拒否条件を収集し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 リストの 1 つ 1 つの条件と突き合わせます。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。

レイヤ 2 スイッチでアクセス リストを設定することによって、ネットワークに基本的なセキュリティを備えることができます。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、ネットワークのあらゆる部分に伝送される可能性があります。ACL を使用すると、ネットワークの各部分にアクセスできるホストを制御したり、スイッチのインターフェイスで転送またはブロックするトラフィックのタイプを決定できます。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できます。ACL を設定することによって、着信トラフィックをブロックすることもできます。

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。

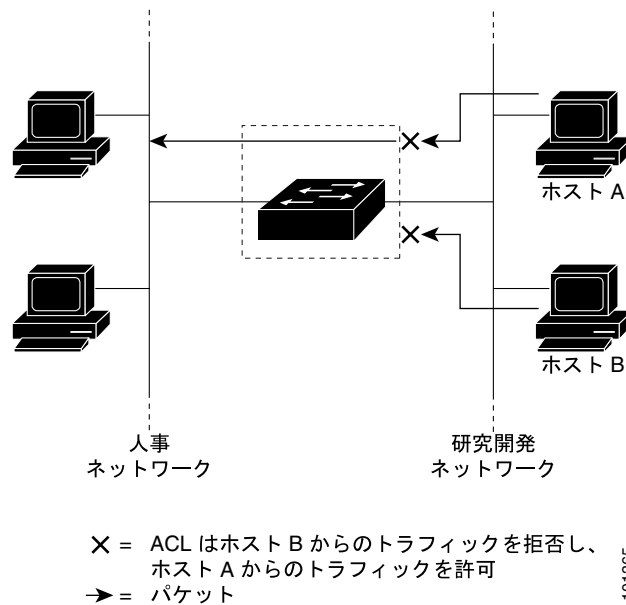
スイッチは物理インターフェイスにおいて、着信方向で次のタイプの ACL をサポートします。

- IP ACL は IP、TCP、および UDP トラフィックをフィルタリングします。
- イーサネットまたは MAC (メディア アクセス制御) ACL はレイヤ 2 トラフィックをフィルタリングします。
- MAC 拡張アクセス リストでは、送信元 MAC アドレス、宛先 MAC アドレス、および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、宛先アドレス、および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します。

スイッチは、所定のインターフェイスで設定されている機能に対応するアクセス リストを調べます。パケットがインターフェイスのスイッチに届くと、そのインターフェイス上のすべての着信機能に対応付けられた ACL が検証されます。

ACL はパケットが ACL エントリとどのように一致したかによって、パケットの転送を許可または拒否します。たとえば ACL を使用すると、あるホストにはネットワークの一部へのアクセスを許可するが、別のホストには同じ部分へのアクセスを阻止できます。図 28-1 では、スイッチの入力に適用された ACL によって、ホスト A は人事ネットワークにアクセスすることが許可され、ホスト B は同じネットワークへのアクセスが阻止されます。

図 28-1 ACL によるネットワークへのトラフィック制御



101365

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、Internet Control Message Protocol (ICMP) タイプおよび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、レイヤ 4 情報をテストする ACE は、通常の方法では、フラグメント IP パケットの大部分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 情報をテストする場合は、照合ルールを次のように変更します。

- 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みなされます。
- 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 つの分割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 deny tcp any any
```



(注)

この例の 1 番めおよび 2 番めの ACE で、宛先アドレスのあとに *eq* キーワードが指定されています。これは、TCP 宛先ポートのうち、それぞれ Simple Mail Transfer Protocol (SMTP; 簡易メール転送プロトコル) および Telnet に対応する well-known 番号の有無をテストするという意味です。

- パケット A は、ホスト 10.2.2.2 のポート 65000 から SMTP ポートのホスト 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。残りのフラグメントも最初の ACE と一致します。SMTP ポート情報の有無に関わらず、最初の ACE はフラグメントに適用された時点で、レイヤ 3 情報だけを調べるためです (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、最初のフラグメントは 2 番めの ACE (拒否) と一致します。すべてのレイヤ 3 情報とレイヤ 4 情報があるためです。パケットの残りのフラグメントは、レイヤ 4 情報がないので、2 番めの ACE と一致しません。
- 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 3 番めの ACE (拒否) と一致します。他のフラグメントもすべて、3 番めの ACE と一致します。この ACE はレイヤ 4 情報を調べず、すべてのフラグメントに含まれているレイヤ 3 情報から、ホスト 10.1.1.3 に送信中であることが認識され、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。

ACP の概要

スイッチで ACL を設定する前に、Access Control Parameter (ACP; アクセス制御パラメータ) を十分に理解しておく必要があります。ACP はスイッチの CLI コマンド出力ではマスクと呼ばれます。

各 ACE に、マスクとルールが 1 つずつあります。分類フィールド、すなわちマスクは、動作の実行対象となるフィールドです。特定のマスクに対応付けられた具体的な値をルールといいます。

パケットは、次のレイヤ 2、レイヤ 3、およびレイヤ 4 フィールドで分類できます。

- レイヤ 2 フィールド
 - 送信元 MAC アドレス (48 ビット全部を指定)
 - 宛先 MAC アドレス (48 ビット全部を指定)
 - Ethertype (16 ビットの Ethertype フィールド)
 これらのフィールドを任意に組み合わせて、または同時に全部使用して、フローを定義できます。
- レイヤ 3 フィールド
 - IP 送信元アドレス (32 の IP 送信元アドレス ビットをすべて指定してフローを定義するか、またはユーザ定義のサブネットを指定します。指定する IP サブネットに制限はありません)
 - IP 宛先アドレス (32 の IP 宛先アドレス ビットをすべて指定してフローを定義するか、またはユーザ定義のサブネットを指定します。指定する IP サブネットに制限はありません)
 これらのフィールドを任意に組み合わせて、または同時に全部使用して、フローを定義できます。

- レイヤ 4 フィールド
 - TCP (TCP 送信元ポート番号、宛先ポート番号、または両方を同時に指定できます)
 - UDP (UDP 送信元ポート番号、宛先ポート番号、または両方を同時に指定できます)



(注)

マスクは、複数のレイヤ 3 およびレイヤ 4 フィールドを組み合わせるか、または複数のレイヤ 2 フィールドを組み合わせるものに行うことができます。レイヤ 2 フィールドをレイヤ 3 またはレイヤ 4 フィールドと組み合わせることはできません。

マスクには次の 2 種類があります。

- ユーザ定義マスク ユーザが定義するマスク
- システム定義マスク 任意のインターフェイスに次のマスクを設定できます。

```
Switch (config-ext-nacl)# permit tcp any any
Switch (config-ext-nacl)# deny tcp any any
Switch (config-ext-nacl)# permit udp any any
Switch (config-ext-nacl)# deny udp any any
Switch (config-ext-nacl)# permit ip any any
Switch (config-ext-nacl)# deny ip any any
Switch (config-ext-nacl)# deny any any
Switch (config-ext-nacl)# permit any any
```



(注)

IP 拡張 ACL (名前付きと番号制の両方) では、レイヤ 4 のシステム定義マスクをレイヤ 3 のユーザ定義マスクより先行させることはできません。たとえば、`permit tcp any any` または `deny udp any any` といったレイヤ 4 のシステム定義マスクを `permit ip 10.1.1.1 any` などのレイヤ 3 ユーザ定義マスクより前に指定することはできません。この組み合わせを設定した場合、レイヤ 2 インターフェイスでは ACL を使用できません。それ以外であれば、システム定義マスクとユーザ定義マスクのあらゆる組み合わせをセキュリティ ACL で使用できます。

スイッチの ACL の設定は、他のシスコ Catalyst スイッチとの一貫性があります。ただし、スイッチでの ACL の設定には、重要な制限事項があります。

システム全体で定義できるユーザ定義マスクは 4 つだけです。ユーザ定義マスクは、セキュリティまたは Quality of Service (QoS; サービス品質) のどちらにも使用できますが、QoS とセキュリティ間で共用することはできません。ACL は必要な数だけいくつでも設定できます。ただし、4 種類を超えるマスクを設定した ACL がインターフェイスに適用されると、エラーメッセージが表示されます。エラーメッセージの詳細は、このリリースに対応するシステムメッセージガイドを参照してください。

表 28-1 に、スイッチにおける ACL の制限事項を示します。

表 28-1 ACL の制限事項の概要

制限事項	許容数
1 つの ACL で使用できるユーザ定義マスクの数	1
1 つのインターフェイスで使用できる ACL の数	1
セキュリティおよび QoS 用として 1 台のスイッチで使用できるユーザ定義マスクの総数	4

物理インターフェイスに ACL を適用する場合の注意事項

物理インターフェイスに ACL を適用する場合は、次に示す設定時の注意事項に従ってください。

- 1 つのインターフェイスに結合できるのは、次の制限のある ACL だけです。
 - ギガビットイーサネットポートが、ポートごとに 1 ACL あたり最大 100 の ACE をサポートしている場合
 - ファストイーサネットポートが、8 個のファストイーサネットポートに対して 1 ACL あたり最大 75 の ACE をサポートしている場合。この場合、ポート 1 ~ 8 が合計 75 の ACE をサポートし、ポート 9 ~ 16 が合計 75 の ACE をサポートすることになります。

ポート範囲上で ACE 制限を越えると、スイッチは `Error:Out of Rule Resources` メッセージを戻します。

詳細については、このリリースに対応するコマンドリファレンスの `ip access-group` インターフェイスコマンドを参照してください。

- ACL 内のすべての ACE に同じユーザ定義マスクを設定する必要があります。ただし、ACE には同じマスクを使用するさまざまなルールを設定できます。1 つのインターフェイスで使用できるユーザ定義マスクは 1 種類ですが、システム定義マスクは任意の数だけ適用できます。システム定義マスクの詳細については、「[ACP の概要](#)」(p.28-4) を参照してください。

ACL 内の同一マスクの例を示します。

```
Switch (config)# ip access-list extended acl2
Switch (config-ext-nacl)# permit tcp 10.1.1.1 0.0.0.0 any eq 80
Switch (config-ext-nacl)# permit tcp 20.1.1.1 0.0.0.0 any eq 23
```

この例では、最初の ACE によって、宛先 TCP ポート番号 80 を指定してホスト 10.1.1.1 から送られてきたすべての TCP パケットが許可されます。2 番目の ACE によって、宛先 TCP ポート番号 23 を指定してホスト 20.1.1.1 から送られてきたすべての TCP パケットが許可されます。どちらの ACE も同じマスクを使用しているため、スイッチはこの ACL をサポートします。

- 物理インターフェイスに ACL を適用する場合、一部のキーワードはサポートされません。また、マスクに関して一定の制限が ACL に適用されます。このような ACL の作成手順については、「[番号制標準 ACL の作成](#)」(p.28-9) および「[番号制拡張 ACL の作成](#)」(p.28-10) を参照してください。



(注)

上記の制約を受けずに、管理インターフェイスに ACL を適用することもできます。詳細については、『*Cisco IOS IP and IP Routing Configuration Guide*』 Release 12.1 の「Configuring IP Services」および『*Cisco IOS IP and IP Routing Command Reference*』 Release 12.1 を参照してください。

ACL の設定

ここでは、次の事項について説明します。

- 「サポート対象外の機能」(p.28-7)
- 「標準および拡張 IP ACL の作成」(p.28-7)
- 「名前付き MAC 拡張 ACL の作成」(p.28-18)
- 「MAC アクセス グループの作成」(p.28-19)

レイヤ 2 インターフェイス上で ACL を設定する手順は、シスコ ルータ上で ACL を設定する場合と同じです。ここで、手順を簡単に説明します。ルータ ACL を設定する場合の詳細については、『Cisco IP and IP Routing Configuration Guide』Release 12.1 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 and IP Routing Command Reference』Release 12.1 を参照してください。スイッチでサポートされない Cisco IOS 機能の一覧については、「サポート対象外の機能」(p.28-7) を参照してください。

サポート対象外の機能

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 28-2 を参照)
- ブリッジ グループ ACL
- IP アカウンティング
- 発信方向での ACL サポート
- 着信および発信レート制限 (QoS ACL を除く)
- ヘッダー長が 5 バイト未満の IP パケット
- 再帰 ACL
- 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)
- ICMP ベースのフィルタリング
- Interior Gateway Routing Protocol (IGMP) ベースのフィルタリング

標準および拡張 IP ACL の作成

ここでは、スイッチの IP ACL を作成する方法について説明します。スイッチはパケットをアクセス リストの 1 つ 1 つの条件と照合します。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条件の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。

ACL の使用手順は、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することによって、ACL を作成します。

ステップ 2 インターフェイスまたは端末回線に ACL を適用します。

ソフトウェアがサポートする IP アクセス リストの種類は、次のとおりです。

- 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。



(注) MAC 拡張アクセス リストでは、送信元 MAC アドレス、宛先 MAC アドレス、および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します。詳細は、「名前付き MAC 拡張 ACL の作成」(p.28-18) を参照してください。

次に、アクセス リストとその使用手順について説明します。

ACL 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 28-2 に、アクセス リスト番号および対応するタイプを示し、さらに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、IP 標準および IP 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 28-2 アクセス リスト番号

ACL 番号	タイプ	サポート
1 ~ 99	IP 標準アクセス リスト	する
100 ~ 199	IP 拡張アクセス リスト	する
200 ~ 299	プロトコル タイプ コード アクセス リスト	しない
300 ~ 399	DECnet アクセス リスト	しない
400 ~ 499	XNS 標準アクセス リスト	しない
500 ~ 599	XNS 拡張アクセス リスト	しない
600 ~ 699	AppleTalk アクセス リスト	しない
700 ~ 799	48 ビット MAC アドレス アクセス リスト	しない
800 ~ 899	IPX 標準アクセス リスト	しない
900 ~ 999	IPX 拡張アクセス リスト	しない
1000 ~ 1099	IPX SAP アクセス リスト	しない
1100 ~ 1199	拡張 48 ビット MAC アドレス アクセス リスト	しない
1200 ~ 1299	IPX サマリー アドレス アクセス リスト	しない
1300 ~ 1999	IP 標準アクセス リスト (拡張範囲)	する
2000 ~ 2699	IP 拡張アクセス リスト (拡張範囲)	する




(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個々のエントリを削除できるという利点があります。

番号制標準 ACL の作成



(注) 管理インターフェイスに適用する ACL の作成手順については、『Cisco IOS IP and IP Routing Configuration Guide』Release 12.1 の「Configuring IP Services」および『Cisco IOS IP and IP Routing Command Reference』Release 12.1 を参照してください。このような ACL を適用できるのは、管理インターフェイスに限定されます。

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

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>access-list access-list-number {deny permit remark} {source source-wildcard host source any}</code>	送信元アドレスとワイルドカードを使用することによって、標準 IP ACL を定義します。 <i>access-list-number</i> 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。 <i>source</i> 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。 <ul style="list-style-type: none"> ドット付き 10 進表記で 32 ビットの値 キーワード any は 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形です。 <i>source-wildcard</i> の入力は不要です。 キーワード host は、 <i>source</i> 0.0.0.0 という <i>source</i> および <i>source-wildcard</i> の省略形です。 (任意) <i>source-wildcard</i> によって、ワイルドカード ビットが <i>source</i> に適用されます (最初のリスト項目を参照)。  (注) <code>log</code> オプションは、スイッチではサポートされません。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除する場合は、`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 を個別に削除することはできません。



(注) ACL を作成するときには、ACL の末尾に到達するまでに 1 つも一致しなかった場合、デフォルトで、すべてのパケットに対する暗黙の拒否ステートメントが ACL の末尾に組み込ま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、それ以外のあらゆる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
    deny   171.69.198.102
    permit any
```

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

物理インターフェイスでは、次の IP プロトコルがサポートされます(プロトコルキーワードはカッコ内の太字)。Internet Protocol (**ip**)、Transmission Control Protocol (**tcp**)、または User Datagram Protocol (**udp**) です。

サポートされるパラメータは、次のカテゴリに分けられます。

- TCP
- UDP

表 28-3 に、ACE で使用できるフィルタリングパラメータをプロトコルタイプ別に示します。

表 28-3 ACE でサポートされるフィルタリングパラメータ (IP プロトコル別)

フィルタリングパラメータ ¹	TCP	UDP
レイヤ 3 パラメータ		
IP Type of Service (ToS; サービスタイプ) バイト ²	–	–
Differentiated Services Code Point (DSCP)	X	X
IP 送信元アドレス	X	X
IP 宛先アドレス	X	X
フラグメント	–	–
TCP または UDP	X	X
レイヤ 4 パラメータ		
送信元ポート演算子	X	X
送信元ポート	X	X
宛先ポート演算子	X	X
宛先ポート	X	X
TCP フラグ	–	–

1. プロトコル欄の X は、そのフィルタリングパラメータがサポートされることを意味します。
2. minimize-monetary-cost ToS ビットはサポートされません。

各プロトコルに関連する固有のキーワードの詳細については、『Cisco IP and IP Routing Command Reference』 Release 12.1 を参照してください。



(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ません。さらに、minimize-monetary-cost ToS ビットに基づくフィルタリングをサポートしません。

番号制拡張アクセス リストで ACE を作成する場合、リスト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 を選択して追加および削除することはできません。



(注) 管理インターフェイスに適用する ACL の作成手順については、『Cisco IOS IP and IP Routing Configuration Guide』Release 12.1 の「Configuring IP Services」および『Cisco IOS IP and IP Routing Command Reference』Release 12.1 を参照してください。ACL を適用できるのは、管理インターフェイスまたは SNMP、Telnet、Web トラフィックなどの CPU に限られます。

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

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

	コマンド	目的
ステップ 2	access-list <i>access-list-number</i> { deny permit remark } <i>protocol</i> { <i>source source-wildcard</i> host <i>source</i> any } [<i>operator port</i>] { <i>destination destination-wildcard</i> host <i>destination</i> any } [<i>operator port</i>] [dscp <i>dscp-value</i>] [time-range <i>time-range-name</i>]	<p>拡張 IP アクセス リストおよびアクセス条件を定義します。</p> <p><i>access-list-number</i> は、100 ~ 199 または 2000 ~ 2699 の 10 進数です。</p> <p>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。</p> <p><i>protocol</i> には、IP プロトコルの名前または番号を入力します (IP、TCP、または UDP)。あらゆる Internet Protocol (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。</p> <p><i>source</i> は、パケットの送信元であるネットワークまたはホストの番号です。</p> <p><i>source-wildcard</i> によって、ワイルドカード ビットが <i>source</i> に適用されます。</p> <p><i>destination</i> は、パケットの送信先ネットワークまたはホストの番号です。</p> <p>宛先ポートまたは送信元ポートを定義します。</p> <ul style="list-style-type: none"> • <i>operator</i> に使用できるのは eq (equal) だけです。 • <i>source source-wildcard</i> の後ろに演算子を指定した場合、送信元ポートと定義したポートが同じ場合に条件が一致します。 • <i>destination destination-wildcard</i> の後ろに演算子を指定した場合、宛先ポートと定義したポートが同じ場合に条件が一致します。 • <i>port</i> は、TCP ポートまたは UDP ポートを表す 10 進数または名前です。指定できる番号は 0 ~ 65535 です。 • TCP ポート名は、TCP トラフィック専用です。 • UDP ポート名は、UDP トラフィック専用です。 <p><i>destination-wildcard</i> によって、ワイルドカード ビットが <i>destination</i> に適用されます。</p> <p><i>source</i>、<i>source-wildcard</i>、<i>destination</i>、および <i>destination-wildcard</i> は、次の 3 とおりの指定が可能です。</p> <ul style="list-style-type: none"> • 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 <i>source</i> および <i>source-wildcard</i> またはあらゆる送信元ホストを表わす省略形としてのキーワード any。 • キーワード host の後ろにドット付き 10 進表記で 32 ビットの値。これは、<i>source</i> 0.0.0.0 という <i>source</i> および <i>source-wildcard</i> を持つ単一ホストを表わす省略形です。 <p>dscp サポートされる 13 の DSCP 値 (0、8、10、16、18、24、26、32、34、40、46、48、および 56) のいずれかとパケットを照合する場合に入力します。または疑問符 (?) を入力すると、使用できる値のリストが表示されます。</p> <p>time-range キーワードは任意です。このキーワードについては、「ACL への時間範囲の適用」(p.28-15) を参照してください。</p>
ステップ 3	show access-lists [<i>number</i> <i>name</i>]	アクセス リストの設定を確認します。
ステップ 4	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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 を個別に削除することはできません。

ネットワーク 171.69.198.0 のあらゆるホストからネットワーク 172.20.52.0 のあらゆるホストへの Telnet アクセスを禁止し、他のあらゆる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(宛先アドレスの後ろに `eq` キーワードを指定すると、TCP 宛先ポート番号が Telnet と同じかどうかテストされます)。

```
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
    deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
    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。ACL に ACE を追加することはできませんが、ACE を 1 つでも削除すると、ACL 全体が削除されます。



(注)

ACL を作成するときには、アクセス リストの末尾に到達するまでに 1 つも一致しなかった場合、デフォルトで、すべてのパケットに対する暗黙の拒否ステートメントがアクセス リストの末尾に組み込ま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 がマスクとして使用されます。

ACL の作成後、「[端末回線または物理インターフェイスへの ACL の適用](#)」(p.28-21) で説明するように、回線またはインターフェイスに ACL を適用する必要があります。

名前付き標準および拡張 ACL の作成

番号ではなく英数字の文字列 (名前) で、IP 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 IP 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 リストを使用するコマンドのすべてが名前付き ACL を許可す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に注意してください。


- 標準 ACL と拡張 ACL に同じ名前を指定することはできません。
- 「[標準および拡張 IP ACL の作成](#)」(p.28-7) で説明したとおり、番号制 ACL を使用することもできます。

■ ACL の設定

名前を使用して名前付き標準アクセス リストを作成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip access-list standard {name / access-list-number}</code>	名前を使用して標準 IP アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。  (注) 名前は、1 ~ 99 の番号にすることができます。
ステップ 3	<code>deny {source source-wildcard host source any}</code> または <code>permit {source source-wildcard host source any}</code>	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が廃棄するのかが決定付ける、拒否条件または許可条件を 1 つまたは複数指定します。 <ul style="list-style-type: none"> • <code>host source</code> は、<code>source 0.0.0.0</code> という <code>source</code> および <code>source-wildcard</code> を表します。 • <code>any</code> は、<code>0.0.0.0 255.255.255.255</code> という <code>source</code> および <code>source-wildcard</code> を表します。  (注) <code>log</code> オプションは、スイッチではサポートされません。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意)コンフィギュレーション ファイルに設定を保存します。

名前を使用して名前付き拡張 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip access-list extended {name / access-list-number}</code>	名前を使用して拡張 IP アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。  (注) 名前は、100 ~ 199 の番号にすることができます。

	コマンド	目的
ステップ 3	<code>{deny permit} protocol {source source-wildcard host source any} [operator port] {destination destination-wildcard host destination any} [operator port] [dscp dscp-value] [time-range time-range-name]</code>	<p>アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。</p> <p>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.28-10) を参照してください。</p> <ul style="list-style-type: none"> <code>host source</code> は、<code>source 0.0.0.0</code> という <code>source</code> および <code>source-wildcard</code> を表します。<code>host destination</code> は、<code>destination 0.0.0.0</code> という <code>destination</code> および <code>destination-wildcard</code> を表します。 <code>any</code> は、<code>0.0.0.0 255.255.255.255</code> という <code>source</code> および <code>source-wildcard</code> または <code>destination</code> および <code>destination-wildcard</code> を表します。 <p><code>dscp</code> サポートされる 13 の DSCP 値 (0、8、10、16、18、24、26、32、34、40、46、48、および 56) のいずれかとパケットを照合する場合に入力します。または疑問符 (?) を入力すると、使用できる値のリストが表示されます。</p> <p><code>time-range</code> キーワードは任意です。このキーワードについては、「ACL への時間範囲の適用」(p.28-15) を参照してください。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

標準 ACL および拡張 ACL を作成するときには、ACL の末尾に到達するまでに 1 つも一致しなかった場合、デフォルトで、あらゆるものに対する暗黙の拒否 (deny) ステートメントが ACL の末尾に組み込ま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 がマスクとみなされます。

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 を選択して特定の ACL に追加することはできません。ただし、`no permit` コマンドおよび `no deny` コマンドを使用すると、名前付き ACL から ACE を削除できます。次に、名前付き ACL 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。

ACL の作成後、「端末回線または物理インターフェイスへの ACL の適用」(p.28-21) で説明するように、回線またはインターフェイスに ACL を適用する必要があります。

ACL への時間範囲の適用

`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ことによって、曜日および時刻に基づく拡張 ACL を実装できます。最初に、時間範囲の名前、曜日および時刻を定義し、次に ACL 内の名前前で時間範囲を参照してアクセス リストに制限を適用します。時間範囲を使用すると、ACL の許可 (permit) または拒否 (deny) ステートメントをいつ有効にするかを定義できます。「標準および拡張 IP ACL の作成」(p.28-7) および「名前付き標準および拡張 ACL の作成」(p.28-13) で説明した、名前付きおよび番号制拡張 ACL の手順で、`time-range` キーワードおよび引数を参照してください。

時間範囲を使用する利点は多数ありますが、その一部を紹介します。

- アプリケーションなど、(IP アドレス マスク ペアおよびポート番号で識別される)リソースに対するユーザ アクセスの許可または拒否をきめ細かく制御できます。
- ログイン メッセージを制御できます。ACL エントリは、常時ではなく、決まった時刻にトラフィックを記録できます。したがって、ピーク時に生成された多数のログを解析しなくても、簡単にアクセスを拒否できます。



(注) 時間範囲は、スイッチのシステム クロックに依存します。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。詳細は、「システム日時の管理」(p.7-2) 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>time-range time-range-name</code>	意味のある名前(<i>workhours</i> など)で時間範囲を特定し、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、英字から始める必要があります。
ステップ 3	<code>absolute [start time date] [end time date]</code> または <code>periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm</code> または <code>periodic { weekdays weekend daily } hh:mm to hh:mm</code>	適用する機能がいつ動作可能になるかを指定します。次のコマンドを組み合わせて使用できます。periodic ステートメントは複数使用できますが、absolute ステートメントは 1 つしか使用できません。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。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show time-range</code>	時間範囲の設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

設定した時間範囲を削除するには、`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。

複数の項目を別々の時間で動作可能にする場合は、上記ステップを繰り返してください。

次に、*workhours*（営業時間）および休業日の時間範囲を設定し、設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2000
Switch(config-time-range)# absolute start 00:00 1 Jan 2000 end 23:59 1 Jan 2000
Switch(config-time-range)# exit
Switch(config)# time-range thanksgiving_2000
Switch(config-time-range)# absolute start 00:00 22 Nov 2000 end 23:59 23 Nov 2000
Switch(config-time-range)# exit
Switch(config)# time-range christmas_2000
Switch(config-time-range)# absolute start 00:00 24 Dec 2000 end 23:50 25 Dec 2000
Switch(config-time-range)# end
Switch# show time-range
time-range entry: christmas_2000 (inactive)
    absolute start 00:00 24 December 2000 end 23:50 25 December 2000
time-range entry: new_year_day_2000 (inactive)
    absolute start 00:00 01 January 2000 end 23:59 01 January 2000
time-range entry: thanksgiving_2000 (inactive)
    absolute start 00:00 22 November 2000 end 23:59 23 November 2000
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 内の名前（*workhours* など）で、その時間範囲を参照する必要があります。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、定義された休日の間はあらゆる送信元あらゆる宛先への 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_2000
Switch(config)# access-list 188 deny tcp any any time-range thanksgiving_2000
Switch(config)# access-list 188 deny tcp any any time-range christmas_2000
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
    deny tcp any any time-range new_year_day_2000 (inactive)
    deny tcp any any time-range thanksgiving_2000 (active)
    deny tcp any any time-range christmas_2000 (inactive)
    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_2000
Switch(config-ext-nacl)# deny tcp any any time-range thanksgiving_2000
Switch(config-ext-nacl)# deny tcp any any time-range christmas_2000
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list deny_access
    deny tcp any any time-range new_year_day_2000 (inactive)
    deny tcp any any time-range thanksgiving_2000 (inactive)
    deny tcp any any time-range christmas_2000 (inactive)
Extended IP access list may_access
    permit tcp any any time-range workhours (inactive)
```

エントリに関するコメントを ACL に組み込む方法

remark コマンドを使用すると、エントリに関するコメント (remark) を任意の IP 標準 / 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 (permit) ステートメントまたは拒否 (deny) 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 (permit) または拒否 (deny) 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、矛盾の原因となります。

IP 番号制標準または拡張 ACL の場合、アクセス リストに関するコメントを組み込むには、**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 ワークステーションにアクセスを許可し、Smith 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
```

名前付き IP ACL のエントリに関しては、**remark** アクセス リスト 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 のサブネットに発信 Telnet を使用させません。

```
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
```

名前付き MAC 拡張 ACL の作成

MAC アドレスおよび名前付き MAC 拡張 ACL を使用すると、物理レイヤ 2 のインターフェイス上で、レイヤ 2 トラフィックをフィルタリングできます。手順については、他の名前付き拡張アクセス リストを設定する場合と同様です。



(注) 名前付き MAC 拡張 ACL は、**mac access-group** イネーブル EXEC コマンドの一部として使用します。

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、このリリースに対応するコマンド リファレンスを参照してください。



(注) SNAP でカプセル化されたパケットとゼロ以外の Organizational Unique Identifier (OUI) との照合は、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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>mac access-list extended name</code>	名前を使用して、拡張 MAC アクセス リストを定義します。
ステップ 3	<code>{deny permit} {any host source MAC address} {any host destination MAC address} [aarp amber appletalk dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat larc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp]</code>	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、 any (すべての) 送信元 MAC アドレスまたは特定の host 送信元 MAC アドレス、および any (すべての) 宛先 MAC アドレスの 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。 <code>aarp amber appletalk dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat larc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp</code> (非 IP プロトコル)
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show access-lists [number name]</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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。

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-list
Extended MAC access list mac1
    deny any any decnet-iv
    permit any any
```

MAC アクセス グループの作成

MAC アクセス グループを作成し、インターフェイスに 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを特定し、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レイヤ 2 インターフェイスでなければなりません。
ステップ 3	<code>mac access-group {name} {in}</code>	MAC アクセス リスト名を使用することによって、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。
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show mac-access group</code>	スイッチに適用される MAC ACL を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスに ACL 2 を適用し、このインターフェイスに入ってくるパケットをフィルタリングする例を示します。

```
Switch(config)# interface gigabitethernet0/1  
Router(config-if)# mac access-group 2 in
```



(注)

mac access-group インターフェイス コンフィギュレーション コマンドが有効なのは、レイヤ 2 インターフェイスに適用された場合のみです。

着信 ACL の場合、スイッチはパケットの受信後、そのパケットを ACL と比較して調べます。ACL でパケットが許可されている場合、スイッチはパケットの処理を続けます。ACL でパケットが拒否された場合、スイッチはそのパケットを廃棄します。MAC ACL は IP パケットと非 IP パケットの両方に適用されます。

インターフェイスに未定義の ACL を適用した場合、スイッチは ACL がインターフェイスに適用されなかったものとして、すべてのパケットを許可します。ネットワーク セキュリティ目的で未定義の ACL を使用する場合は、この動作に注意してください。

端末回線または物理インターフェイスへの ACL の適用



(注) 物理インターフェイスに ACL を適用する前に、「物理インターフェイスに ACL を適用する場合の注意事項」(p.28-6) を参照してください。

ACL は任意の管理インターフェイスに適用できます。管理インターフェイスに適用する ACL の作成手順については、『Cisco IOS IP and IP Routing Configuration Guide』Release 12.1 の「Configuring IP Services」および『Cisco IOS IP and IP Routing Command Reference』Release 12.1 を参照してください。



(注) 物理インターフェイス上の ACL に適用される制約は、管理インターフェイス上の ACL には適用されません。

ACL の作成後、1 つまたは複数の管理インターフェイスまたは端末回線に作成した ACL を適用できます。ACL を適用できるのは着信インターフェイスです。ここでは、端末回線とネットワークインターフェイスの両方について、作業手順を紹介します。次の注意事項を考慮してください。

- 回線へのアクセスを制御する場合は、番号制 IP ACL または MAC 拡張 ACL を使用する必要があります。
- インターフェイスへのアクセスを制御する場合は、名前付きまたは番号制 ACL を使用できます。
- すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。
- 管理インターフェイスに ACL を適用した場合、ACL は SNMP、Telnet、Web トラフィックなど、CPU へ送られるパケットだけをフィルタリングします。

端末回線への ACL の適用

仮想端末回線と ACL に指定されたアドレス間の着信接続を制限するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>line [console vty] line-number</code>	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。 コンソール端末回線として <code>console</code> と入力します。コンソールポートは DCE です。 リモート コンソール アクセス用の仮想端末として、 <code>vty</code> と入力します。 <code>line-number</code> 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	<code>access-class access-list-number {in}</code>	(装置に対する) 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	<code>end</code>	イネーブル EXEC モードに戻ります。

■ 端末回線または物理インターフェイスへの ACL の適用

	コマンド	目的
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

物理インターフェイスへの ACL の適用

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、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>interface interface-id</code>	設定するインターフェイスを特定し、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、レイヤ 2 または管理インターフェイスにするか、または管理インターフェイス VLAN ID にしなければなりません。
ステップ 3	<code>ip access-group {access-list-number / name} {in}</code>	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	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	アクセス リストの設定を表示します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

インターフェイスにアクセス リスト 2 を適用し、このインターフェイスに入ってくるパケットをフィルタリングする例を示します。

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



(注) `ip access-group` インターフェイス コンフィギュレーション コマンドが有効なのは、管理インターフェイスまたはレイヤ 2 物理インターフェイスに適用された場合だけです。インターフェイスのポート チャネルに ACL を適用することはできません。

着信 ACL の場合、スイッチはパケットの受信後、そのパケットを ACL と比較して調べます。ACL でパケットが許可されている場合、スイッチはパケットの処理を続けます。ACL でパケットが拒否された場合、スイッチはそのパケットを廃棄します。

インターフェイスに未定義の ACL を適用した場合、スイッチは ACL がインターフェイスに適用されなかったものとして、すべてのパケットを許可します。ネットワーク セキュリティで未定義の ACL を使用する場合は、この動作に注意してください。

ACL 情報の表示

スイッチ上で設定されている ACL を表示できます。また、物理インターフェイスおよび管理インターフェイスに適用された ACL を表示できます。ここでは、次の事項について説明します。

- [ACL の表示 \(p.28-23\)](#)
- [アクセス グループの表示 \(p.28-24\)](#)

ACL の表示

show コマンドを使用すると、既存の ACL を表示できます。

アクセス リストを表示するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	<code>show access-lists [number / name]</code>	すべての IP および MAC アドレス アクセス リストまたは特定のアクセス リスト (番号制または名前付き) について情報を表示します。
ステップ 2	<code>show ip access-list [number / name]</code>	すべての IP アドレス アクセス リストまたは特定の IP ACL (番号制または名前付き) について情報を表示します。

すべての標準および拡張 ACL を表示する例を示します。

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

IP の標準および拡張 ACL だけを表示する例を示します。

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

アクセス グループの表示



(注) この機能を使用できるのは、スイッチで EI が稼働している場合に限られます。

レイヤ 3 インターフェイスに ACL を適用するには、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで IP がイネーブルに設定されている場合、**show ip interface interface-id** イネーブル EXEC コマンドを使用すると、インターフェイスの入力および出力アクセス リストとともに、他のインターフェイス特性を表示できます。インターフェイスで IP がイネーブルになっていない場合、アクセス リストは表示されません。

次に、VLAN 1 に設定されたすべてのアクセス グループを表示する例を示します。

```
Switch# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.20.30.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is permit Any
  Inbound access list is 13
```

(テキスト出力は省略)

次に、インターフェイスに設定されたすべてのアクセス グループを表示する例を示します。

```
Switch# show ip interface fastethernet0/9
FastEthernet0/9 is down, line protocol is down
  Inbound access list is ip1
```

あらゆる状況で確実に、設定されているすべてのアクセス グループを表示するには、**show running-config** イネーブル EXEC コマンドを使用するのが唯一の方法です。1 つのインターフェイスについて ACL の設定を表示する場合は、**show running-config interface interface-id** コマンドを使用します。

次に、インターフェイス GigabitEthernet 0/1 の ACL 設定を表示する例を示します。

```
Switch# show running-config interface gigabitethernet0/1
Building configuration...

Current configuration :112 bytes
!
interface GigabitEthernet0/1
 ip access-group 11 in
 snmp trap link-status
 no cdp enable
end!
```

ACL の設定例

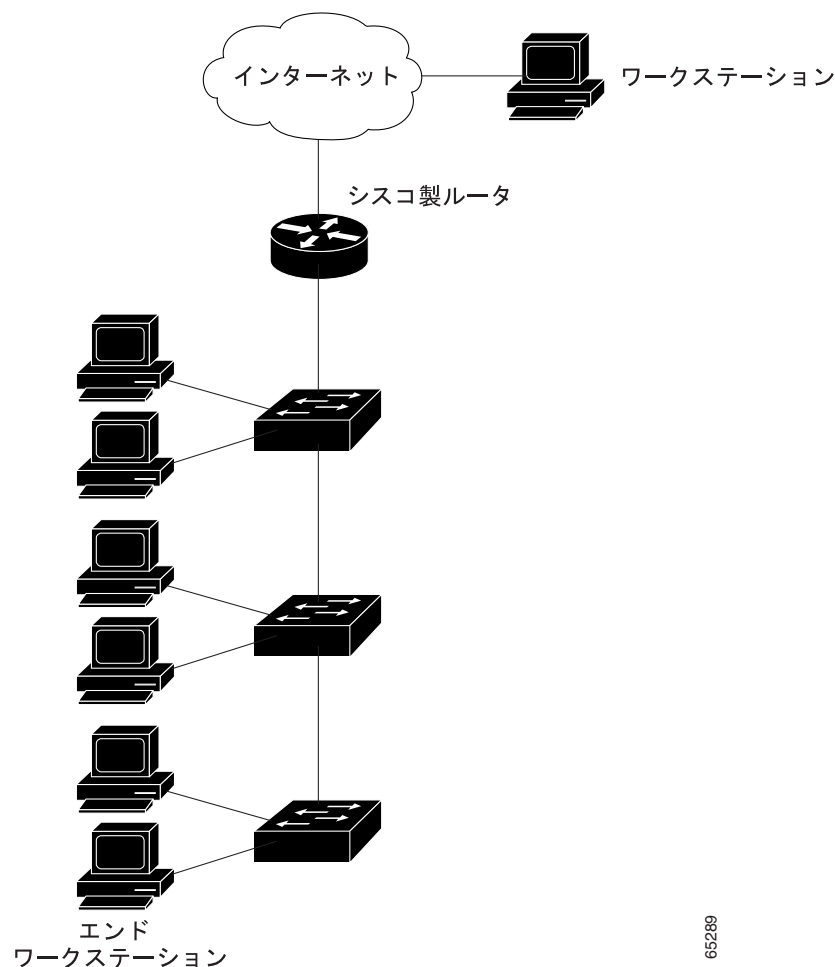
ACL のコンパイル手順については、『*Security Configuration Guide*』および『*Cisco IOS IP and IP Routing Configuration Guide*』 Release 12.1 の「IP Services」の章を参照してください。

図 28-2 は、複数のスイッチをシスコ製ルータに接続し、ネットワークで結んだ小規模なオフィスの例です。ホストは WAN リンクを使用し、インターネットを介してネットワークに接続されています。

次の目的で、スイッチの ACL を使用します。

- 標準 ACL を作成し、アドレス 172.20.128.64 の特定のインターネット ホストからのトラフィックをフィルタリングします。
- 拡張 ACL を作成し、トラフィックのフィルタリングによって、すべてのインターネット ホストに対する HTTP アクセスを拒否し、他のあらゆるタイプのアクセスを許可します。

図 28-2 スイッチ ACL によるトラフィックの制御



標準 ACL を使用して、アドレス 172.20.128.64 の特定のインターネット ホストへの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 0.0.0.0
Switch(config)# end
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 6 in
```

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

```
Switch(config)# access-list 106 deny tcp any any eq 80
Switch(config)# access-list 106 permit ip any any
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip access-group 106 in
```

番号制 ACL の例

次の例では、スイッチはネットワーク 36.0.0.0 のサブネット上のアドレスを受け入れ、56.0.0.0 のサブネットからのパケットをすべて拒否します。ACL はインターフェイスに入るパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# access-list 2 deny 56.0.0.0 0.255.255.255
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL の例

次に示す拡張 ACL の使用例では、ネットワークがインターネットに接続されていて、ネットワーク上のすべてのホストがインターネット上のすべてのホストに、TCP Telnet および SMTP 接続できるようにします。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 102 in
```

SMTP は、接続の一端で TCP ポート 25 を使用し、もう一端ではランダムなポート番号を使用します。接続が有効な間は常に、同じポート番号が使用されます。インターネットからのメール パケットは、宛先ポートが 25 です。スイッチの背後のセキュリティ システムが常にポート 25 のメール接続を受け付けるので、着信サービスが制御されます。

名前付き ACL の例

marketing_group の ACL により、宛先アドレスおよびワイルドカード 171.69.0.0 0.0.255.255 へのすべての TCP Telnet トラフィックが許可され、それ以外の TCP トラフィックは拒否されます。他の IP トラフィックは許可されます。

```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit ip any any
```

ACL は、着信トラフィックに適用された Marketing_group ACL というポートを許可するために適用されます。

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group marketing_group in
...
```

コメント付き IP ACE エントリの例

次の番号制 ACL の例では、Jones ワークステーションにアクセスを許可し、Smith 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
```

次の番号制 ACL の例では、Winter および Smith ワークステーションに対して、Web ブラウジングが許可されません。

```
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
```

次の名前付き ACL の例では、Jones サブネットはアクセスが許可されません。

```
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
```

次の名前付き ACL の例では、Jones サブネットに発信 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
```

