CHAPTER 28

ACL によるネットワーク セキュリティの設定

この章では、Access Control List（ACL; アクセス コントロール リスト）を使用して、Catalyst 2950 または Catalyst 2955 スイッチにネットワーク セキュリティを設定する方法について説明します。ACL は、コマンドやテーブルでは *アクセス リスト*とも呼ばれます。

ACL は物理インターフェイスまたは管理インターフェイスに対して作成できます。管理インターフェイスは、管理 VLAN、または CPU に直接送信されるトラフィックとして定義されるもので、SNMP、Telnet、Web トラフィックなどがあります。スイッチにインストールされている 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）を使用して、管理インターフェイスに対して 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される ACL には、1 つのマスクの制約があり、いくつかのキーワードはサポートされていません。詳細については、「物理インターフェイスへの ACL 適用のガイドライン」（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完全な構文および使用の情報は、このリリースのコマンド リファレンス、および『*Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1*』の「Configuring IP Services」、および『*Cisco IOS IP and IP Routing Command Reference, Cisco IOS Release 12.1*』を参照してください。

この章で説明する内容は、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.28-21）
- 「ACL のコンパイル例」（P.28-22）

Command-line Interface（CLI; コマンドライン インターフェイス）を使用して ACL を設定できます。

また、セキュリティ ウィザードを使用してスイッチ上の着信トラフィックをフィルタできます。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 User Datagram Protocol（UDP）アプリケーションに基づいて行うことができます。フィルタリング基準を満たすパケットをドロップするか、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ているか、およびフィルタリング デバイス上でインターフェイスがどのように使用されるかを理解する必要があります。このウィザードの使用に関する詳しい設定手順については、セキュリティ 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 フィルタリングは、ネットワーク トラフィックを限定し、ネットワークの使用を特定のユーザまたはデバイスに制限します。ACL は、スイッチの通過時に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の順序付けられた集まりです。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内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。スイッチはパケットを 1 つずつ、アクセス リストの条件でテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。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ため、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。

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、レイヤ 2 スイッチにアクセス リストを設定します。ACL を設定しなければ、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あらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御できます。また、スイッチ インターフェイスで転送またはブロックされるトラフィックの種類を決定できます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を設定して着信トラフィックをブロックできます。

ACL には、Access Control Entry（ACE; アクセス コントロール エントリ）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある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変わります。

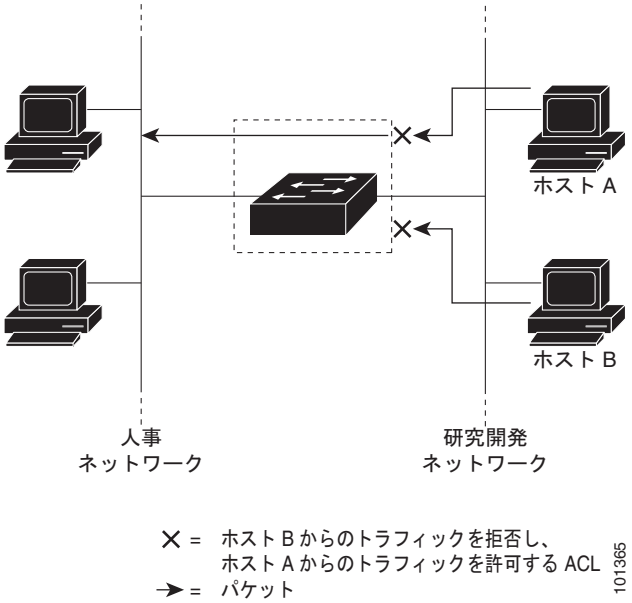
スイッチは、着信方向の物理インターフェイスにおいて、次のタイプの ACL をサポートしています。

- IP ACL は IP、TCP、および UDP トラフィックをフィルタします。
- イーサネットまたは MAC ACL はレイヤ 2 トラフィックをフィルタします。
- MAC 拡張アクセス リストは、送信元と宛先の MAC アドレス、およびオプションのプロトコル タイプ情報を使用して、照合処理を行います。
- 標準 IP アクセス リストでは、送信元アドレスを使用して照合します。
- 拡張 IP アクセス リストは、送信元と宛先のアドレス、およびオプションのプロトコル タイプ情報を使用して、照合処理を行います。

スイッチは、特定のインターフェイスに設定されている機能に関連付けられているアクセス リストを調べます。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。

ACL は、パケットが ACL 内のエントリとどのように一致したかに基づいてパケットの転送を許可または拒否します。たとえば ACL を使用して、あるホストにはネットワークの特定の場所へのアクセスを許可し、別のホストにはそのネットワークの同じ場所へのアクセスを禁止できます。図 28-1 では、スイッチへの入力に適用されている ACL により、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は拒否されます。

図 28-1　ACL によるネットワークへのトラフィックの制御



フラグメント化されたトラフィックとフラグメント化されていない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されることがあります。その場合、TCP または UDP のポート番号、Internet Control Message Protocol（ICMP）タイプ、コードなどのレイヤ 4 の情報が含まれるのは、パケットの最初の部分があるフラグメントだけです。他のフラグメントには、この情報はありません。

ACE には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE がレイヤ 4 情報をテストする場合は、照合の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 や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 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、フラグメントと一致しません。

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
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）　最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれ Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントに SMTP ポート情報が含まれていない場合でも、これらのフラグメントは最初の ACE と一致します。これは、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです（この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです）。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。
- 最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。
- フラグメント化されたパケット C は、ホスト 10.2.2.2 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。このパケットがフラグメント化された場合、最初のフラグメントが 3 番めの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なる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 3 番めの ACE と一致します。

アクセス コントロール パラメータについて

スイッチで ACL を設定する前に、Access Control Parameter（ACP; アクセス コントロール パラメータ）をよく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*とも呼ばれます。

各 ACE には 1 つのマスクと 1 つのルールがあります。Classification フィールドまたはマスクは、アクションを実行する対象のフィールドです。指定されたマスクに関連付けられる特定の値を*ルール*と呼びます。

パケットは、次の Layer 2、Layer 3、Layer 4 の各フィールドに分類できます。

- Layer 2 フィールド：
  - 送信元 MAC アドレス（48 ビットすべて指定）
  - 宛先 MAC アドレス（48 ビットすべて指定）
  - イーサタイプ（16 ビットのイーサタイプ フィールド）

  これらのフィールドの組み合わせまたはすべてを使用してフローを拒否できます。
- Layer 3 フィールド：
  - IP 送信元アドレス（フローを定義するには IP 送信元アドレスの 32 ビットをすべて指定するか、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 サブネットには制約はありません）

- IP 宛先アドレス（フローを定義するには、IP 宛先アドレスの 32 ビットをすべて指定するか、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 サブネットには制約はありません）

これらのフィールドの組み合わせまたはすべてを使用してフローを拒否できます。

- Layer 4 フィールド：
  - TCP（TCP の送信元または宛先ポート番号のいずれかを指定することも、同時に両方を指定することもできます）
  - UDP（UDP の送信元または宛先ポート番号のいずれかを指定することも、同時に両方を指定することもできます）

（注） マスクは、複数の Layer 3 および Layer 4 フィールドを組み合わせることも、複数の Layer 2 のフィールドにすることもできます。Layer 2 フィールドは、Layer 3 または Layer 4 の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 2 つのタイプがあります。

- ユーザ定義マスク：ユーザが定義したマスク。
- システム定義マスク：すべてのインターフェイスで設定できるマスク。

```
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（名前付きと番号付きの両方）では、レイヤ 4 のシステム定義マスクよりも、レイヤ 3 のユーザ定義マスクが優先されます。たとえば、レイヤ 4 システム定義マスク（**permit tcp any any** や **deny udp any any** など）よりも、レイヤ 3 のユーザ定義マスク（**permit ip 10.1.1.1 any**）が優先されます。この組み合わせを設定すると、ACL は、レイヤ 2 インターフェイス上で許可されません。他のすべてのシステム定義マスクとユーザ定義マスクの組み合わせは、セキュリティ ACL で許可されます。

スイッチ ACL の設定は、他の Cisco Catalyst スイッチと整合性が保たれます。ただし、スイッチ上で ACL を設定する場合には重要な制限があります。

システム全体で定義できるのは、4 つのユーザ定義マスクのみです。これらのマスクはセキュリティ、または Quality of Service（QoS）のいずれかで使用できますが、QoS とセキュリティで共有することはできません。ACL は必要な数だけ設定できます。ただし、5 つ以上のマスクを持つ ACL がインターフェイスに適用されると、システム エラー メッセージが表示されます。エラー メッセージの詳細については、*このリリースのシステム メッセージ ガイド*を参照してください。

表 28-1 に、スイッチの ACL の制約について概要を示します。

表 28-1　ACL の制約の概要

制約事項	数
ACL で許可されるユーザ定義マスクの数	1
インターフェイスで許可される ACL の数	1
スイッチでセキュリティおよび QoS に対して許可されるユーザ定義マスクの合計数	4

物理インターフェイスへの ACL 適用のガイドライン

ACL を物理インターフェイスに適用する場合は、次の設定ガイドラインに従います。

- インターフェイスに接続できるのは、次の制約を持つ 1 つの ACL のみです。
  - ギガビット イーサネットは、1 つのポートの ACL につき最大 100 の ACE をサポートします。
  - ファスト イーサネット ポートは、8 つのファスト イーサネット ポート間の 1 つの ACL につき最大 75 の ACE をサポートします。これは、ポート 1 ～ 8 は、合計 75 の ACE の組み合わせをサポートし、ポート 9 ～ 16 は合計 75 の ACE の組み合わせをサポートすることを意味します。

    一連のポートで ACE の制限を超えると、スイッチは `Error:Out of Rule Resources` メッセージを返します。

  詳細については、このリリースの *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。

- 同じ ACL 内のすべての ACE は同じユーザ定義マスクを持っている必要があります。ただし、ACE は、同じマスクを使用する異なるルールを持つことができます。あるインターフェイスでは、1 つのユーザ定義マスクのみ許可されますが、任意の数のシステム定義マスクを適用できます。システム定義マスクの詳細については、「アクセス コントロール パラメータについて」（P.28-4）を参照してください。

  この例は、ACL 内の同じマスクを示しています。

```
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 は、宛先 TCP ポート番号が 80 でホスト 10.1.1.1 から到着するすべての TCP パケットを許可します。2 番めの ACE は、宛先 TCP ポート番号が 23 でホスト 20.1.1.1 から到着するすべての TCP パケットを許可します。これらの 2 つの ACE は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。

- ACL を物理インターフェイスへ適用する場合に、いくつかのキーワードはサポートされません。またいくつかのマスクの制約が ACL に適用されます。これらの ACL の作成については、「番号付き標準 ACL の作成」（P.28-9）および 「番号付き拡張 ACL の作成」（P.28-10）を参照してください。

（注） ACL を管理インターフェイスに適用する場合は、これらの制約はありません。詳細については、『*Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1*』の「Configuring IP Services」および『*Cisco IOS IP and IP Routing Command Reference, Cisco IOS Release 12.1*』を参照してください。

ACL の設定

ここでは、次の内容について説明します。

- 「サポートされていない機能」（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.28-17）
- 「MAC アクセス グループの作成」（P.28-18）

レイヤ 2 インターフェイスにおける ACL の設定は、Cisco ルータにおける ACL の設定と同じです。ここでは、その設定手順を簡単に説明します。ルータ ACL の設定の詳細については、『*Cisco IP and IP Routing Configuration Guide, Cisco IOS 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, Cisco IOS Release 12.1*』を参照してください。スイッチでサポートされていない Cisco IOS 機能のリストは、「サポートされていない機能」（P.28-7）を参照してください。

サポートされていない機能

このスイッチは、Cisco IOS ルータの ACL に関連する次の機能をサポートしていません。

- 非 IP プロトコル ACL（表 28-2（P.28-8）を参照）
- ブリッジ グループ ACL
- IP アカウンティング
- 送信方向の ACL サポート
- 着信および発信レート制限（QoS ACL によるレート制限を除く）
- 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（スイッチのクラスタリング機能で使用される特別なダイナミック ACL を除く）
- 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

このセクションでは、スイッチ IP ACL の作成方法について説明します。スイッチはパケットを 1 つずつ、アクセス リストの条件でテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは、最初の一致が見つかると条件テストを終了するため、条件の順序が重要になります。一致する条件がない場合、スイッチはパケットを拒否します。

ACL を使用するには、次の手順を実行します。

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　その ACL をインターフェイスまたは端末回線に適用します。

ソフトウェアは、次のタイプの IP アクセス リストをサポートしています。

- 標準 IP アクセス リストでは、送信元アドレスを使用して照合します。
- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

（注）　MAC 拡張アクセス リストは、送信元と宛先の MAC アドレス、およびオプションのプロトコル タイプ情報を使用して、照合処理を行います。詳細については、「名前付き MAC 拡張 ACL の作成」（P.28-17）を参照してください。

次の項では、アクセス リストについて、およびそれらを使用する手順について説明します。

ACL 番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。表 28-2 に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。スイッチでは、IP 標準および IP 拡張アクセス リストがサポートされています（番号は 1 ～ 199、1300 ～ 2699）。

表 28-2　アクセス リスト番号

ACL 番号	タイプ	サポート状況
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 サマリー 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）　番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 ACL の作成

（注）　ACL を作成して管理インターフェイスへ適用する方法の詳細については、『*Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1*』の「Configuring IP Services」および『*Cisco IOS IP and IP Routing Command Reference, Cisco IOS Release 12.1*』を参照してください。これらの ACL は管理インターフェイスにのみ適用できます。

番号付き標準 IP 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** | **remark**} {*source source-wildcard* | **host** *source* | **any**}	送信元アドレスとワイルドカードを使用して標準 IP ACL を定義します。 *access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *source* 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送信元アドレスです。 • 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* の 0.0.0.0 255.255.255.255 の省略形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* 0.0.0.0 の *source* および *source-wildcard* の省略形としてのキーワード **host**。 （任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します（箇条書きの最初の項目を参照）。 **（注）　log** オプション はスイッチでサポートされていません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no access-list** *access-list-number* グローバル コンフィギュレーション コマンドを使用します。番号付きアクセス リストから個々の ACE は削除できません。

（注）　ACL を作成する場合には、ACL の末尾に暗黙的な deny ステートメントがデフォルトで追加され、ACL の終わりに到達するまで一致する条件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 リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、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、他のすべてのホストへのアクセスを許可し、結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
```

```
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    deny   171.69.198.102
    permit any
```

番号付き拡張 ACL の作成

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用して、オプションのプロトコル タイプ情報を使用して制御の精度を高めることができます。一部のプロトコルには、特定のパラメータやキーワードも適用されます。

次の IP プロトコルは物理インターフェイスでサポートされています（プロトコル キーワードを括弧内の太字で示します）。Internet Protocol（**ip**）、Transmission Control Protocol（**tcp**）、または User Datagram Protocol（**udp**）。

サポートされているパラメータは、次のカテゴリにグループ化できます。

- TCP
- UDP

表 28-3 に、ACE の各プロトコル タイプについて有効なフィルタリング パラメータを示します。

表 28-3　さまざまな IP プロトコルでサポートされているフィルタリング パラメータ ACE

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 タイプ オブ サービス（ToS）バイト[2]	–	–
Differentiated Services Code Point（DSCP; DiffServ コード ポイント）	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. プロトコル列の X は、フィルタリング パラメータのサポートを表します。
2. Type of Service（ToS; タイプ オブ サービス）の minimize monetary cost ビットはサポートしていません。

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

（注） このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、Type of Service（ToS; タイプ オブ サービス）の minimize-monetary-cost 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。

番号付き拡張アクセス リストに ACE を作成するときは、リストの作成後は、追加した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

（注）　ACL を作成して管理インターフェイスへ適用する方法の詳細については、『*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, Cisco IOS Release 12.1*』を参照してください。ACL は、SNMP、Telnet、Web トラフィックなどの管理インターフェイス、または CPU にのみ適用できます。

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 2	**access-list** *access-list-number* {**deny** | **permit** | **remark**} *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*]	拡張 IP アクセス リストおよびアクセス条件を定義します。 *access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は **deny**、許可する場合は **permit** を指定します。 *protocol* には、IP プロトコルの名前または番号として、**IP**、**TCP**、または **UDP** を入力します。すべてのインターネット プロトコル（TCP および UDP を含む）と一致するようにするには、キーワード **ip** を使用します。 *source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 *destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。 宛先または送信元のポートを定義します。 • *operator* には **eq**（等号）のみ使用できます。 • operator が *source source-wildcard* の後にある場合、送信元ポートが定義済みポートと一致したときに条件が満たされます。 • operator が *destination destination-wildcard* の後にある場合、宛先ポートが定義済みポートと一致したときに条件が満たされます。 • *port* は TCP ポートまたは UDP ポートの 10 進数または名前です。番号は、0 ～ 65535 です。 • TCP のポート名は TCP トラフィックにのみ使用します。 • UDP のポート名は UDP トラフィックにのみ使用します。 *destination-wildcard* は、ワイルドカード ビットを宛先アドレスに適用します。

	コマンド	目的
	access-list *access-list-number* {**deny** | **permit** | **remark**} *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*] （続き）	*source*、*source-wildcard*、*destination*、および *destination-wildcard* の値は、次の 3 つの形式で指定します。 • 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 の *source* および *source-wildcard* の省略形としてのキーワード **any**、または任意の送信元ホスト。 • *source* 0.0.0.0 の *source* および *source-wildcard* を持つ単一ホストの省略形としてのキーワード **host** と、それに続くドット付き 10 進表記の 32 ビット長の値。 **dscp**：パケットと照合する、サポートされた 13 の DSCP 値のいずれか（0、8、10、16、18、24、26、32、34、40、46、48、および 56）を入力するか、または疑問符（**?**）を入力して、使用できる値のリストを表示します。 **time-range** キーワードはオプションです。このキーワードの説明は、「ACL への時間範囲の適用」（P.28-14）を参照してください。
ステップ 3	**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 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 リストから個々の ACE は削除できません。

次に、ネットワーク 171.69.198.0 内の任意のホストからネットワーク 172.20.52.0 内の任意のホストへの Telnet アクセスを拒否し、それ以外のアクセスを許可する拡張アクセス リストを作成し、表示する例を示します（**eq** キーワードを宛先アドレスの後に指定すると、Telnet に対応する TCP 宛先ポート番号がチェックされます）。

```
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（端末からの入力などによって）追加したエントリは、リストの末尾に追加されます。ACL に ACE を追加することはできますが、いずれかの ACE を削除すると、ACL 全体が削除されます。

（注） ACL を作成すると、アクセス リストの末尾に暗黙的な deny ステートメントがデフォルトで追加され、アクセス リストの終わりに到達するまで一致する条件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 リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL を作成したら、「端末回線または物理インターフェイスへの ACL の適用」（P.28-19）で説明しているように、その ACL を回線またはインターフェイスに適用する必要があります。

名前付き標準 ACL および名前付き拡張 ACL の作成

IP ACL を識別する手段として、番号ではなく英数字の文字列（名前）を使用できます。名前付き ACL を使用すると、番号付きアクセス リストを使用した場合よりも多くの IP アクセス リストをスイッチ上に設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付き ACL で使用でき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 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、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 を設定するときには、次の注意事項および制限事項に留意してください。

- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- 「標準および拡張 IP ACL の作成」（P.28-7）で説明したとおり、番号付き ACL も使用できます。

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、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* | *access-list-number*}	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）　名前には、1 ～ 99 の番号を使用できます。
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、1 つ以上の条件を拒否または許可に指定し、パケットの転送またはドロップを決定します。 • **host** *source* は、*source* 0.0.0.0 の *source* および *source-wildcard* を表します。 • **any** は、0.0.0.0 255.255.255.255 の *source* および *source-wildcard* を表します。 （注）　**log** オプション はスイッチでサポートされていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show 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。

名前を使用して名前付き拡張 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* | *access-list-number*}	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）　名前には、100 ～ 199 の番号を使用できます。

	コマンド	目的
ステップ 3	{**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*]	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、「番号付き拡張 ACL の作成」（P.28-10）を参照してください。* • **host** *source* は、*source* 0.0.0.0 の *source* および *source-wildcard* を表し、***host*** *destination* は、*destination* 0.0.0.0 の *destination* および *destination-wildcard* を表します。 • **any** は、0.0.0.0 255.255.255.255 の *source* および *source-wildcard*、または *destination* および *destination-wildcard* を表します。 **dscp**：パケットと照合する、サポートされた 13 の DSCP 値のいずれか（0、8、10、16、18、24、26、32、34、40、46、48、および 56）を入力するか、または疑問符（**?**）を入力して、使用できる値のリストを表示します。 **time-range** キーワードはオプションです。このキーワードの説明は、「ACL への時間範囲の適用」（P.28-14）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 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。

標準および拡張 ACL を作成すると、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのものに適用されることに注意してください。標準 ACL では、関連付けられた 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すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。特定の ACL に対して ACE を選択的に追加することはできません。ただし、**no permit** および **no deny** コマンドを使用して、名前付き ACL から ACE を削除することができます。次の例は、名前付き ACL から個々の ACE を削除する方法を示します。

```
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 つとして、名前付き ACL では行を選択して削除できることがあります。

ACL を作成したら、「端末回線または物理インターフェイスへの ACL の適用」（P.28-19）で説明しているように、その ACL を回線またはインターフェイスに適用する必要があります。

ACL への時間範囲の適用

曜日および時刻に基づいて拡張 ACL を実装するには、**time-range** グローバル コンフィギュレーション コマンドを使用します。最初に、時間範囲の名前、および曜日と時刻を定義し、ACL 内で名前によってその時間範囲を参照し、アクセス リストに制約を適用します。時間範囲を使用して、ACL 内で実際にステートメントを許可または拒否するタイミングを定義することができます。**time-range** キーワードおよび引数については、「標準および拡張 IP ACL の作成」（P.28-7）および「名前付き標準 ACL および名前付き拡張 ACL の作成」（P.28-13）にある名前付きおよび番号付き拡張 ACL タスクの表を参照してください。

時間範囲を使用する利点のいくつかを次に示します。

- アプリケーションなどのリソースに対するユーザ アクセスを、より厳密に許可または拒否できます（IP アドレスとマスクのペア、およびポート番号で識別されます）。
- ロギング メッセージを制御できます。ACL のエントリでは、特定の時刻にトラフィックをロギングできますが、常時はロギングできません。そのため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

（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; ネットワーク タイム プロトコル）を使用してスイッチ クロックを同期させることを推奨します。詳細については、「システム日時の管理」（P.7-1）を参照してください。

ACL の時間範囲パラメータを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**time-range** *time-range-name*	意味のある名前（*workhours* などの）で time-range を識別し、time-range コンフィギュレーション モードを開始します。名前にスペースや疑問符は使用できません。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*	適用対象の機能がいつ動作可能になるかを指定します。これらのコマンドをいくつか組み合わせて使用します。**periodic** ステートメントは複数指定できます。**absolute** ステートメントは 1 つしか指定できません。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	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show time-range**	時間範囲の設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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。

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

この例は、*workhours* および会社の休日について時間範囲を設定し、設定を確認する方法を示しています。

```
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、時間範囲を実装する拡張 ACL 内で、名前（*workhours* など）によって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_2000
Switch(config)# access-list 188 deny tcp any any time-range thanskgiving_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 thanskgiving_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)
```

ACL 内のエントリに関するコメントの付加

remark コマンドを使用して、任意の IP 標準または拡張 ACL のエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは 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 permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または 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、混乱を招く可能性があります。

IP 番号付きの標準または拡張 ACL の場合は、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用して、アクセス リストに関するコメントを追加します。コメントを削除するには、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ていますが、Smith のワークステーションのアクセスは禁止されています。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリでは、**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、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 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
```

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 を使用して、物理レイヤ 2 インターフェイスでレイヤ 2 のトラフィックをフィルタすることができます。この手順は、他の名前付き拡張アクセス リストを設定する場合と類似しています。

（注）　名前付き MAC 拡張 ACL は、**mac access-group** 特権 EXEC コマンドの一部として使用されます。

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）　SNAP のカプセル化パケットと、ゼロ以外の Organizational Unique Identifier（OUI; 組織固有識別子）との照合はサポートしていません。

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*} {**any** | **host** *destination MAC address*} [**aarp** | **amber** | **appletalk** | **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**]	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、任意の（**any**）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、および任意の（**any**）宛先 MAC アドレスを許可（**permit**）するか、拒否（**deny**）するかを指定します。 （任意）次のオプションを入力することもできます。 **aarp** | **amber** | **appletalk** | **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**：（IP 以外のプロトコル）。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show access-lists** [*number* | *name*]	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no mac access-list extended** *name* グローバル コンフィギュレーション コマンドを使用します。名前付き 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アクセス リスト *mac1* を作成および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、MAC アクセス リストをインターフェイスに適用するには、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	**interface** *interface-id*	設定する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。 インターフェイスを、レイヤ 2 インターフェイスとして設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 リストの名前を使用して、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。
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**	スイッチに適用されている MAC ACL 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。

次に、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来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 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 コマンドは、レイヤ 2 インターフェイスに適用される場合のみ有効です。

着信 ACL の場合、スイッチはパケットの受信後に ACL とパケットを照合します。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継続します。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。MAC ACL は、IP および非 IP の両方のパケットに適用されます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じること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 を適用するには、その前に 「物理インターフェイスへの ACL 適用のガイドライン」（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で ACL を作成する方法の詳細については、『*Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1*』の「Configuring IP Services」、および『*Cisco IOS IP and IP Routing Command Reference, Cisco IOS 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。

作成した ACL は、1 つ以上の管理インターフェイス、または端末回線に適用できます。ACL は着信インターフェイスに適用できます。このセクションでは、端末回線およびネットワーク インターフェイスの両方に対してこのタスクを実行する方法について説明します。次の注意事項に留意してください。

- 回線に対するアクセスを制御する場合は、番号付きでない 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付きの 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、すべての仮想端末回線に同じ制約を設定する必要があります。
- ある管理インターフェイスに ACL を適用すると、その ACL は、SNMP、Telnet、Web トラフィックなど、CPU を対象としたパケットのみがフィルタされます。

端末回線への ACL の適用

仮想端末回線と ACL 内のアドレス間の着信接続を制限するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**line** [**console** | **vty**] *line-number*	設定する回線を指定し、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。 コンソールの端末回線に対しては **console** を入力します。コンソール ポートは DCE です。 リモート コンソール アクセスの仮想端末に対しては **vty** を入力します。 *line-number* は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。有効範囲は 0 ～ 16 です。

	コマンド	目的
ステップ 3	**access-class** *access-list-number* {**in**}	（デバイスへの）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接続および発信接続を制限します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	設定する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、レイヤ 2、または管理インターフェイス、または管理インターフェイス VLAN ID のいずれかにする必要があります。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in**}	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	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）コンフィギュレーション ファイルに設定を保存します。

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

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

（注）　**ip access-group** インターフェイス コンフィギュレーション コマンドは、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る場合のみ有効です。ACL は、インターフェイス ポート チャネルには適用できません。

着信 ACL の場合、スイッチはパケットの受信後に ACL とパケットを照合します。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継続します。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 ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

ACL 情報の表示

スイッチ上に設定されている ACL を表示したり、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ている ACL を表示できます。ここでは、次の内容について説明します。

- 「ACL の表示」（P.28-21）
- 「アクセス グループの表示」（P.28-22）

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、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	**show access-lists** [*number* | *name*]	すべての IP および MAC アドレス アクセス リストに関する情報、または特定の（番号付きまたは名前付きの）アクセス リストに関する情報を表示します。
ステップ 2	**show ip access-list** [*number* | *name*]	すべての IP アドレス アクセス リストに関する情報、または特定の（番号付きまたは名前付きの）IP ACL に関する情報を表示します。

次の例では、すべての標準および拡張 ACL が表示されます。

```
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
```

次の例では、IP 標準および拡張 ACL のみが表示されます。

```
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）　この機能は、スイッチが EI を実行している場合のみ使用可能です。

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。インターフェイス上で IP が有効になっている場合は、**show ip interface** ***interface-id*** 特権 EXEC コマンドを使用すると、インターフェイス上の入力および出力アクセス リストだけでなく、他のインターフェイス特性についても表示できます。インターフェイス上で IP が有効になっていない場合は、アクセス リストは表示されません。

次の例は、VLAN 1 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方法を示しています。

```
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
<information truncated>
```

次の例は、インターフェイス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方法を示しています。

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

すべての状況で設定されているすべてのアクセス グループを確実に表示できるのは、**show running-config** 特権 EXEC コマンドを使用する方法だけです。単一インターフェイスの ACL 設定を表示するには、**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 Gigabit Ethernet 0/1 の ACL の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 のコンパイル例

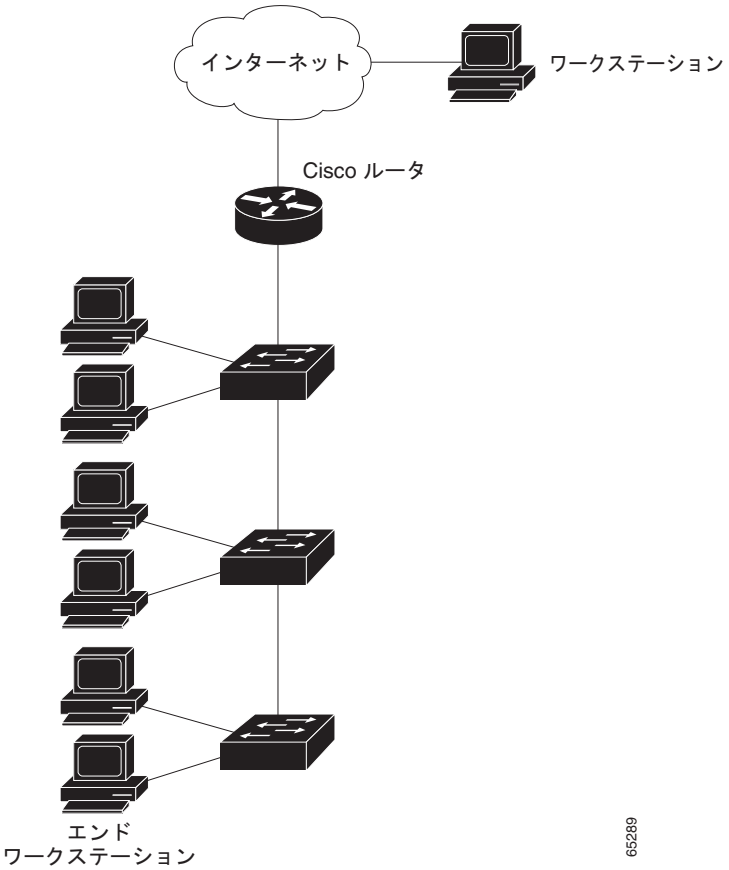
ACL のコンパイルの詳細については、『*Security Configuration Guide*』、および『*Cisco IOS IP and IP Routing Configuration Guide, Cisco IOS Release 12.1*』の「IP Services」を参照してください。

図 28-2 は、Cisco ルータに接続されたいくつかのスイッチを備えた、小規模なネットワーク オフィスを示しています。ホストは WAN リンクを使用し、インターネット経由でネットワークに接続されています。

次のために ACL を使用します。

- 標準 ACL を作成し、アドレスが 172.20.128.64 である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します。
- 拡張 ACL を作成し、すべてのインターネット ホストへの HTTP アクセスは拒否するが、他のタイプのアクセスはすべて許可するようトラフィックをフィルタします。

図 28-2　スイッチ ACL によるトラフィックの制御



次の例は、標準 ACL を使用して、アドレスが 172.20.128.64 である特定のインターネット ホストに対するアクセスを許可します。

```
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
```

次の例は、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します。この ACL は、それ以外のすべてのトラフィックを許可します。

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

番号付き ACL の例

次の例は、スイッチがネットワーク 36.0.0.0 サブネット上のアドレスを受け入れ、56.0.0.0 サブネットからのすべてのパケットを拒否することを示しています。次にこの ACL は、インターフェイス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 gigabitethernet0/1
Switch(config-if)# ip access-group 2 in
```

拡張 ACL の例

拡張 ACL を使用する別の例として、インターネットに接続されたネットワークがあり、ネットワーク上の任意のホストが、インターネット上の任意のホストと TCP Telnet および SMTP 接続を確立できるようにする場合を考えます。

```
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、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。スイッチの背後にある安全なシステムは、ポート 25 でメール接続を常に受け入れるため、着信サービスが制御されます。

名前付き ACL の例

marketing_group ACL は、宛先アドレスと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。この ACL は他のすべての IP トラフィックを許可します。

```
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
```

着信トラフィックに marketing_group ACL が適用されるポートを許可するよう、ACL が適用されます。

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

コメント付き IP ACL エントリの例

次に示す番号付き ACL 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ますが、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
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
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
```

次に示す名前付き ACL の例では、Jones のサブネットに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
```