CHAPTER 16

アクセス リストでのトラフィックの識別

この章では、アクセス リストでトラフィックを識別する方法について説明します。この章では、次の事項について説明します。

IPv6 アクセス リストの詳細については、「IPv6 アクセス リストの設定」（P.12-6）を参照してください。

アクセス リストの概要

アクセス リストは、1 つまたは複数のアクセス コントロール エントリで構成されます。ACE は許可または拒否のルールを指定する、アクセス リストの個々のエントリであり、プロトコル、送信元 IP アドレス、宛先 IP アドレス、またはネットワークに適用されます。任意で、送信元ポートと宛先ポートにも適用されます。

アクセス リストは、さまざまな機能で使用されます。モジュラ ポリシー フレームワークを使用する機能では、アクセス リストによってトラフィック クラス マップ内のトラフィックを識別できます。モジュラ ポリシー フレームワークの詳細については、第 21 章「モジュラ ポリシー フレームワークの使用」を参照してください。

この項では、次のトピックについて取り上げます。

アクセス リストのタイプ

表 16-1 に、アクセス リストのタイプと、それらの一般的な使用目的の一部を示します。

表 16-1　アクセス リストのタイプと一般的な使用目的

アクセス リストの使用目的	アクセス リストのタイプ	説明
IP トラフィックのネットワーク アクセスの制御（ルーテッド モードおよびトランスペアレント モード）	拡張	セキュリティ アプライアンスでは、拡張アクセス リストにより明示的に許可されている場合を除き、低位のセキュリティ インターフェイスから高位のセキュリティ インターフェイスへのトラフィックは認められません。 **（注）** また、管理アクセス用のセキュリティ アプライアンス インターフェイスにアクセスする場合は、ホスト IP アドレスを許可するアクセス リストは不要です。必要なのは、第 40 章「システム アクセスの管理」の説明に従って管理アクセスを設定することだけです。
AAA ルールでのトラフィック識別	拡張	AAA ルールでは、アクセス リストを使用してトラフィックを識別します。
所定のユーザに関する IP トラフィックのネットワーク アクセス制御	拡張、ユーザごとに AAA サーバからダウンロード	ユーザに適用するダイナミック アクセス リストをダウンロードするように RADIUS サーバを設定できます。または、セキュリティ アプライアンス上に設定済みのアクセス リストの名前を送信するようにサーバを設定できます。
NAT（ポリシー NAT および NAT 免除）のアドレス識別	拡張	ポリシー NAT を使用すると、拡張アクセス リストで送信元アドレスと宛先アドレスを指定することにより、アドレスを変換するローカル トラフィックを指定できます。
VPN アクセスの確立	拡張	VPN コマンドで拡張アクセス リストを使用できます。
モジュラ ポリシー フレームワークのトラフィック クラス マップ内でのトラフィック識別	拡張 EtherType	アクセス リストを使用すると、クラス マップ内のトラフィックを識別できます。このマップは、モジュラ ポリシー フレームワークをサポートする機能に使用されます。モジュラ ポリシー フレームワークをサポートする機能には、TCP および一般的な接続設定やインスペクションなどがあります。
トランスペアレント ファイアウォール モードの場合、IP 以外のトラフィックのネットワーク アクセスの制御	EtherType	トラフィックを EtherType に基づいて制御するためのアクセス リストを設定できます。
OSPF ルート再配布の指定	標準	標準アクセス リストには、宛先アドレスだけが含まれています。標準アクセス リストを使用して、OSPF ルートの再配布を制御できます。
WebVPN のフィルタリング	Webtype	URL をフィルタリングするように Webtype アクセス リストを設定できます。

アクセス コントロール エントリの順序

アクセス リストは、1 つ以上のアクセス コントロール エントリで構成されます。アクセス リストのタイプに応じて、送信元アドレス、宛先アドレス、プロトコル、ポート（TCP または UDP の場合）、ICMP タイプ（ICMP の場合）、または EtherType を指定できます。

特定のアクセス リスト名に対して入力した各 ACE は、そのアクセス リストの末尾に追加されます。

ACE の順序は重要です。セキュリティ アプライアンス でパケットを転送するか廃棄するかを決定する場合、セキュリティ アプライアンス は各 ACE に対して、エントリの指定順にパケットをテストします。一致が見つかると、ACE はそれ以上チェックされません。たとえば、アクセス リストの先頭にすべてのトラフィックを明示的に許可する ACE を作成した場合、残りのステートメントはチェックされません。

ACE をディセーブルにするには、**access-list** コマンドで **inactive** キーワードを指定します。

アクセス コントロールによる暗黙的な拒否

アクセス リストの最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、セキュリティ アプライアンスを通過してネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

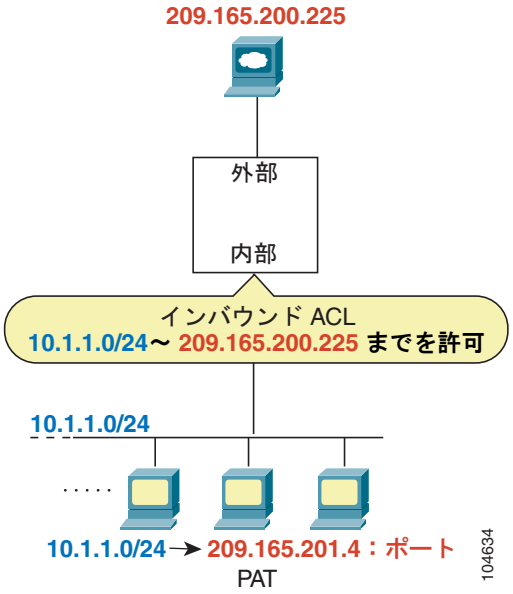
EtherType アクセス リストの場合、アクセス リストの末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、アクセス リストの末尾にある暗黙的な拒否によって、拡張アクセス リストで以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE とのすべてのトラフィックを*明示的*に拒否する場合、IP と ARP のトラフィックが拒否されます。

NAT 使用時にアクセス リストで使用する IP アドレス

NAT を使用する場合、アクセス リストに対して設定する IP アドレスは、アクセス リストが付加されるインターフェイスによって異なります。インターフェイスに接続されるネットワーク上で有効なアドレスを使用する必要があります。使用されるアドレスは宛先によって決まるのではなく、インターフェイスによってだけ決まるというガイドラインは、着信アクセス リストと発信アクセス リストの両方に当てはまります。

たとえば、内部インターフェイスの着信方向に対してアクセス リストを適用する場合、外部アドレスへのアクセス時に、内部送信元アドレスに対して NAT を実行するように セキュリティ アプライアンスを設定します。内部インターフェイスにアクセス リストが適用されるので、送信元アドレスは変換されていない元のアドレスになります。外部アドレスが変換されないので、アクセス リストで使用する宛先アドレスは実アドレスです（図 16-1 を参照）。

図 16-1　　アクセス リストの IP アドレス：送信元アドレスに NAT を使用

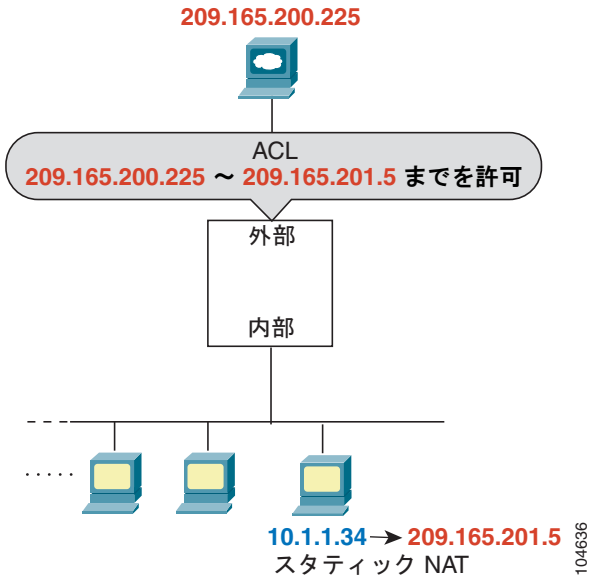


この例について、次のコマンドを参照してください。

```
hostname(config)# access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 host
209.165.200.225
hostname(config)# access-group INSIDE in interface inside
```

外部ホストから内部ホストにアクセスできるようにする場合は、外部インターフェイス上で着信アクセス リストを適用できます。アクセス リストに内部ホストの変換後のアドレスを指定する必要があります。これが外部ネットワーク上で使用できるアドレスであるためです（図 16-2 を参照）。

図 16-2　アクセス リストの IP アドレス：宛先アドレスに NAT を使用

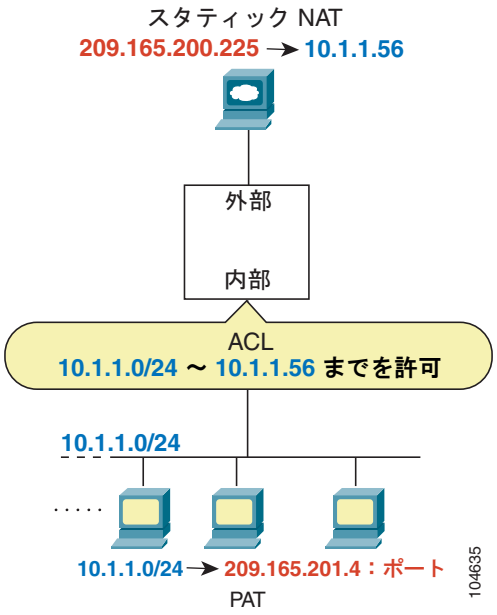


この例について、次のコマンドを参照してください。

```
hostname(config)# access-list OUTSIDE extended permit ip host 209.165.200.225 host
209.165.201.5
hostname(config)# access-group OUTSIDE in interface outside
```

両方のインターフェイスで NAT を実行する場合は、個々のインターフェイスに見せるアドレスを覚えておいてください。図 16-3 では、外部サーバがスタティック NAT を使用するので、変換されたアドレスが内部ネットワークに表示されます。

図 16-3　　アクセス リストの IP アドレス：送信元アドレスと宛先アドレスに NAT を使用



この例について、次のコマンドを参照してください。

```
hostname(config)# access-list INSIDE extended permit ip 10.1.1.0 255.255.255.0 host
10.1.1.56
hostname(config)# access-group INSIDE in interface inside
```

拡張アクセス リストの追加

この項では、アクセス リストを追加する方法について説明します。次の項目を取り上げます。

- 「拡張アクセス リストの概要」（P.16-6）
- 「トランスペアレント ファイアウォールを通過できるブロードキャスト トラフィックとマルチキャスト トラフィック」（P.16-7）
- 「拡張 ACE の追加」（P.16-8）

拡張アクセス リストの概要

拡張アクセス リストは、1 つ以上の ACE で構成されます。このリストには、行番号を指定して ACE、送信元アドレス、および宛先アドレスを挿入できます。また、ACE タイプによっては、プロトコル、ポート（TCP または UDP の場合）、または ICMP タイプ（ICMP の場合）も挿入できます。これらのすべてのパラメータを **access-list** コマンドで指定できます。また、各パラメータに対応するオブジェクト グループを使用することもできます。ここでは、コマンド内でパラメータを指定する方法について説明します。オブジェクト グループを使用する場合は、「オブジェクト グループ化機能によるアクセス リストの簡略化」（P.16-13）を参照してください。

ACE の末尾に追加できるロギング オプションについては、「アクセス リスト アクティビティのロギング」（P.16-22）を参照してください。時間範囲オプションについては、「拡張アクセス リストのアクティベーションのスケジュール設定」（P.16-20）を参照してください。

TCP 接続と UDP 接続では、リターン トラフィックを許可するアクセス リストは必要ありません。これは、ASA によって、確立された双方向接続のすべてのリターン トラフィックが許可されるためです。ただし、ICMP などのコネクションレス型プロトコルでは、セキュリティ アプライアンスは単方向のセッションを確立します。そのため、アクセス リストで双方向の ICMP を許可するか（アクセス リストを送信元と宛先のインターフェイスに適用する）、ICMP のインスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用できます。アクセス リストのインターフェイスへの適用の詳細については、第 18 章「ネットワーク アクセスの許可または拒否」を参照してください。

（注） アクセス リスト コンフィギュレーションを変更する場合、既存の接続がタイムアウトするのを待たずに新しいアクセス リスト情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

トランスペアレント ファイアウォールを通過できるブロードキャスト トラフィックとマルチキャスト トラフィック

ルーテッド ファイアウォール モードでは、ブロードキャスト トラフィックとマルチキャスト トラフィックはアクセス リストで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルや DHCP（DHCP リレーを設定している場合を除く）などがあります。トランスペアレント ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。この機能は、たとえば、ダイナミック ルーティングが許可されていないマルチ コンテキスト モードで特に有用です。

（注） これらの特殊なタイプのトラフィックはコネクションレス型であるため、拡張アクセス リストを両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

表 16-2 に、トランスペアレント ファイアウォールの通過を許可できる一般的なトラフィック タイプを示します。

表 16-2　トランスペアレント ファイアウォールの特殊トラフィック

トラフィック タイプ	プロトコルまたはポート	注意事項
DHCP	UDP ポート 67 および 68	DHCP サーバがイネーブルの場合、セキュリティ アプライアンスは DHCP パケットの通過を拒否します。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—

表 16-2　トランスペアレント ファイアウォールの特殊トラフィック （続き）

トラフィック タイプ	プロトコルまたはポート	注意事項
マルチキャスト ストリーム	UDP ポートは、アプリケーションによって異なります。	マルチキャスト ストリームは、常に Class D アドレス（224.0.0.0 to 239.x.x.x）に送信されます。
RIP（v1 または v2）	UDP ポート 520	—

拡張 ACE の追加

任意のアクセス リスト名を指定して **access-list** コマンドを入力すると、**line** の番号を指定した場合を除き、そのアクセス リストの末尾に ACE が追加されます。

次のコマンドを入力して、ACE を追加します。

```
hostname(config)# access-list access_list_name [line line_number] [extended]
{deny | permit} protocol source_address mask [operator port] dest_address mask
[operator port | icmp_type] [inactive]
```

ヒント　コンフィギュレーションを確認するときに名前をわかりやすくするために、アクセス リスト名は大文字で入力してください。インターフェイスを示すアクセス リスト名（INSIDE など）、または作成された目的を示すアクセス リスト名（NO_NAT、VPN など）を指定できます。

通常、プロトコルとして **ip** キーワードを指定しますが、他のプロトコルも受け付けることができます。プロトコル名のリストについては、「プロトコルとアプリケーション」（P.D-11）を参照してください。

1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。

送信元ポートと宛先ポートは、**tcp** または **udp** プロトコルの場合にかぎり指定できます。使用できるキーワードおよび予約済みポート割り当てのリストについては、「TCP ポートと UDP ポート」（P.D-12）を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

*演算子*を使用して、送信元または宛先に使用させるポート番号を一致させます。使用できる演算子は、次のとおりです。

- **lt**：より小さい
- **gt**：より大きい
- **eq**：等しい
- **neq**：等しくない
- **range**：値の包括的な範囲。この演算子を使用するときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。

  ```
  range 100 200
  ```

ICMP タイプは **icmp** プロトコルの場合にだけ指定できます。ICMP はコネクションレス型プロトコルなので、アクセス リストを使用して（送信元インターフェイスと宛先インターフェイスにアクセス リストを適用することによって）双方向で ICMP を使用できるようにするか、または ICMP インスペク

ション エンジンをイネーブルにする必要があります（「ICMP タイプ オブジェクト グループの追加」（P.16-16）を参照）。ICMP インスペクション エンジンでは、ICMP セッションはステートフル接続として処理されます。ping を制御するには、**echo-reply**（**0**）（セキュリティ アプライアンスからホストへ）または **echo**（**8**）（ホストからセキュリティ アプライアンスへ）を指定します。ICMP タイプのリストについては、「ICMP タイプ オブジェクト グループの追加」（P.16-16）を参照してください。

ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。セキュリティ アプライアンスでは、ネットワーク マスク（たとえば、Class C マスクの 255.255.255.0）が使用されます。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。

ACE を非アクティブ状態にするには、**inactive** キーワードを使用します。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能を使用すると、非アクティブな ACE のレコードをコンフィギュレーション内に保持して、再度イネーブルにしやすくすることができます。

ACE を削除するには、設定に表示されるコマンド構文文字列全体を使用して **no access-list** コマンドを入力します。

```
hostname(config)# no access-list access_list_name [line line_number] [extended]
{deny | permit} protocol source_address mask [operator port] dest_address mask
[operator port | icmp_type] [inactive]
```

削除するエントリがアクセス リストの唯一のエントリである場合は、アクセス リスト全体が削除されます。

次の例を参照してください。

次のアクセス リストは、このアクセス リストを適用するインターフェイスのすべてのホストがセキュリティ アプライアンスを通過することを許可しています。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のサンプル アクセス リストでは、192.168.1.0/24 上のホストが 209.165.201.0/27 ネットワークにアクセスすることが禁止されます。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

一部のホストのみにアクセスを制限する場合は、制限された permit ACE を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次のアクセス リストでは、すべてのホスト（アクセス リスト適用先のインターフェイス上にあるすべてのホスト）がアドレス 209.165.201.29 の Web サイトにアクセスすることが禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

EtherType アクセス リストの追加

トランスペアレント ファイアウォール モード限定

この項では、EtherType アクセス リストを追加する方法について説明します。次の項目を取り上げます。

EtherType アクセス リストの概要

EtherType アクセス リストは EtherType を指定する 1 つまたは複数の ACE からなります。この項では、次のトピックについて取り上げます。

サポートされている EtherType

EtherType ACE は、16 ビットの 16 進数で指定されたあらゆる EtherType を制御します。

EtherType アクセス リストでは、Ethernet V2 フレームがサポートされています。

802.3 形式フレームでは、type フィールドではなく length フィールドが使用されるため、アクセス リストでは処理されません。

唯一の例外は、アクセス リストで処理される BPDU です。BPDU は SNAP でカプセル化され、セキュリティ アプライアンス は BPDU を処理できるように設計されています。

セキュリティ アプライアンスでは、トランク ポート（シスコ専用）BPDU が受信されます。トランク BPDU のペイロードには VLAN 情報が含まれるので、BPDU を許可すると、セキュリティ アプライアンス により、発信 VLAN を使用してペイロードが修正されます。

IP および ARP だけの暗黙的な許可

セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの IPv4 トラフィックは、アクセス リストとは無関係に、トランスペアレント ファイアウォールを自動的に通過できます。ARP は、アクセス リストに関係なく、両方向ともトランスペアレント ファイアウォールを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。

ただし、IPv4 と ARP 以外の EtherType のトラフィックを許可するには、高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへのトラフィックである場合でも EtherType アクセス リストを適用する必要があります。

EtherType はコネクションレス型なので、双方向にトラフィックを流す場合は、両方のインターフェイスにアクセス リストを適用する必要があります。

アクセス リストの末尾にある暗黙的および明示的拒否 ACE

EtherType アクセス リストの場合、アクセス リストの末尾にある暗黙的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、アクセス リストの末尾にある暗黙的な拒否によって、拡張アクセス リストで以前許可（または高位のセキュリティ インターフェイス

から低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE とのすべてのトラフィックを*明示的*に拒否する場合、IP と ARP のトラフィックが拒否されます。

IPv6 の未サポート

EtherType ACE は、IPv6 トラフィックを許可しません。これは、IPv6 EtherType を指定した場合も同じです。

同じインターフェイス上での拡張アクセス リストと EtherType アクセス リストの使用

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用することもできます。

MPLS の許可

MPLS を許可する場合は、Label Distribution Protocol（LDP; ラベル配布プロトコル）および Tag Distribution Protocol（TDP; タグ配布プロトコル）の TCP 接続がセキュリティ アプライアンスを経由して確立されるようにしてください。これには、セキュリティ アプライアンス インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、セキュリティ アプライアンスに接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。*interface* は、セキュリティ アプライアンスに接続されているインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

EtherType ACE の追加

EtherType ACE を追加するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name ethertype {permit | deny} {ipx | bpdu |
mpls-unicast | mpls-multicast | any | hex_number}
```

hex_number は、0x600 以上の 16 ビット 16 進数で指定できる任意の EtherType です。EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt にアクセスして、RFC 1700「Assigned Numbers」を参照してください。

ACE を削除するには、設定に表示されるコマンド構文文字列全体を使用して **no access-list** コマンドを入力します。

```
hostname(config)# no access-list access_list_name [line line_number] [extended]
{deny | permit} protocol source_address mask [operator port] dest_address mask
[operator port | icmp_type] [inactive]
```

EtherType ACE を削除するには、設定に表示されるコマンド構文文字列全体を使用して **no access-list** コマンドを入力します。

```
ehostname(config)# no access-list access_list_name ethertype {permit | deny} {ipx | bpdu |
mpls-unicast | mpls-multicast | any | hex_number}
```

（注）　EtherType アクセス リストに **deny all** が設定されている場合、すべてのイーサネット フレームが廃棄されます。その場合でも、オートネゴシエーションなどの物理プロトコル トラフィックだけは許可されます。

任意のアクセス リスト名を指定して **access-list** コマンドを入力すると、そのアクセス リストの末尾に ACE が追加されます。

ヒント　コンフィギュレーションを確認するときに名前をわかりやすくするために、*access_list_name* は大文字で入力してください。インターフェイスを示すアクセス リスト名（INSIDE など）、または目的を示すアクセス リスト名（MPLS、IPX など）を指定できます。

たとえば、次のサンプル アクセス リストでは、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

次のアクセス リストでは、一部の EtherType に セキュリティ アプライアンス の通過を許可しますが、IPX は拒否します。

```
hostname(config)# access-list ETHER ethertype deny ipx
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次のアクセス リストでは、EtherType 0x1256 が指定されたトラフィックを拒否しますが、それ以外はすべて、両方のインターフェイスについて許可します。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

標準アクセス リストの追加

シングル コンテキスト モードだけ

標準アクセス リストでは、OSPF ルートの宛先 IP アドレスを指定します。このアクセス リストは、OSPF 再配布のルート マップに使用できます。標準アクセス リストをインターフェイスに適用してトラフィックを制御することはできません。

次のコマンドで標準 ACE を追加します。アクセス リストの末尾に別の ACE を追加する場合は、同じアクセス リスト名を指定して **access-list** コマンドをもう 1 つ入力します。「ルート マップの定義」（P.9-8）を参照してアクセス リストを適用します。

次のコマンドを入力して、ACE を追加します。

```
hostname(config)# access-list access_list_name standard {deny | permit} {any | ip_address
mask}
```

ACE を削除するには、設定に表示されるコマンド構文文字列全体を使用して **no access-list** コマンドを入力します。

```
hostname(config)# no access-list access_list_name standard {deny | permit} {any |
ip_address mask}
```

次に、アクセス リストで 192.168.1.0/24 へのルートを識別する例を示します。

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

Webtype アクセス リストの追加

WebVPN のフィルタリングをサポートするコンフィギュレーションにアクセス リストを追加するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name webtype {deny | permit} url [url_string | any]
```

Webtype アクセス リストを削除するには、設定に表示される構文文字列全体を使用して **no access-list** コマンドを入力します。

```
hostname(config)# access-list access_list_name webtype {deny | permit} url [url_string | any]
```

ACE の末尾に追加できるロギング オプションについては、「アクセス リスト アクティビティのロギング」（P.16-22）を参照してください。

オブジェクト グループ化機能によるアクセス リストの簡略化

ここでは、オブジェクトをグループ化してアクセス リストの作成/管理を簡素化する方法について説明します。

この項では、次のトピックについて取り上げます。

オブジェクト グループ化の機能

類似のオブジェクトをグループとしてまとめることによって、オブジェクトごとに個別に ACE を入力しなくても、ACE でオブジェクト グループを使用できます。次のタイプのオブジェクト グループを作成できます。

- プロトコル
- ネットワーク
- サービス

- ICMP タイプ

たとえば、次の 3 つのオブジェクト グループを考えてみます。

- MyServices：内部ネットワークにアクセスできるサービス要求の TCP および UDP ポート番号を指定します。
- TrustedHosts：最大範囲のサービスとサーバにアクセスできるホストおよびネットワークのアドレスを指定します。
- PublicServers：最大限のアクセス権を与えるサーバのホスト アドレスを指定します。

上記のグループを作成すると、1 つの ACE を使用して、信頼できるホストが公開サーバのグループにサービス要求を許可することが可能になります。

オブジェクト グループを他のオブジェクト グループにネストすることもできます。

（注） 拡張アクセス リストには ACE のシステム限度が適用されます。ACE でオブジェクト グループを使用した場合、実際に入力する ACE の数は少なくなりますが、拡張 ACE の数はオブジェクト グループを使用しなかった場合と同じになります。オブジェクト グループは通常、手動で追加する場合より多くの ACE を作成します。手動で ACE を作成する場合の方がオブジェクト グループよりアドレスを集約する傾向があるからです。アクセス リストの拡張 ACE の数を表示するには、**show access-list** *access_list_name* コマンドを入力します。

オブジェクト グループの追加

この項では、オブジェクト グループを追加する方法について説明します。

この項では、次のトピックについて取り上げます。

- 「プロトコル オブジェクト グループの追加」（P.16-14）
- 「ネットワーク オブジェクト グループの追加」（P.16-15）
- 「サービス オブジェクト グループの追加」（P.16-16）
- 「ICMP タイプ オブジェクト グループの追加」（P.16-16）

プロトコル オブジェクト グループの追加

プロトコル オブジェクト グループを追加または変更するには、次の手順に従います。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式で削除するまで残ります。

プロトコル グループを追加するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、プロトコル グループを追加します。

```
hostname(config)# object-group protocol grp_id
```

grp_id は、最大 64 文字の文字列です。

プロンプトがプロトコル コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-protocol)# description text
```

説明には、最大 200 文字を使用できます。

ステップ 3　プロトコルごとに次のコマンドを入力して、グループのプロトコルを定義します。

```
hostname(config-protocol)# protocol-object protocol
```

protocol は、特定の IP プロトコルを表す識別番号（1 ～ 254）または識別キーワード（**icmp**、**tcp**、または **udp**）です。すべての IP プロトコルを含めるには、キーワード **ip** を使用します。指定が可能なプロトコルのリストについては、「プロトコルとアプリケーション」（P.D-11）を参照してください。

たとえば、TCP、UDP、および ICMP に対応するプロトコル グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group protocol tcp_udp_icmp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object icmp
```

ネットワーク オブジェクト グループの追加

ネットワーク オブジェクト グループを追加または変更するには、次の手順に従います。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式で削除するまで残ります。

（注）　ネットワーク オブジェクト グループは、アクセス リストのタイプに応じて IPv4 アドレスおよび IPv6 アドレスをサポートします。IPv6 アクセス リストの詳細については、「IPv6 アクセス リストの設定」（P.12-6）を参照してください。

ネットワーク グループを追加するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、ネットワーク グループを追加します。

```
hostname(config)# object-group network grp_id
```

grp_id は、最大 64 文字の文字列です。

プロンプトがネットワーク コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-network)# description text
```

説明には、最大 200 文字を使用できます。

ステップ 3　ネットワークまたはアドレスごとに次のコマンドを入力して、グループのネットワークを定義します。

```
hostname(config-network)# network-object {host ip_address | ip_address mask}
```

たとえば、3 人の管理者の IP アドレスからなるネットワーク グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group network admins
hostname(config-network)# description Administrator Addresses
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.34
```

サービス オブジェクト グループの追加

サービス オブジェクト グループを追加または変更するには、次の手順に従います。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式で削除するまで残ります。

サービス グループを追加するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、サービス グループを追加します。

```
hostname(config)# object-group service grp_id {tcp | udp | tcp-udp}
```

grp_id は、最大 64 文字の文字列です。

追加するサービス（ポート）に対応するプロトコルを指定します。**tcp**、**udp**、または **tcp-udp** キーワードのいずれかになります。DNS（ポート 53）のように、サービスが同じポート番号で TCP と UDP の両方を使用する場合は、**tcp-udp** キーワードを入力します。

プロンプトがサービス コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-service)# description text
```

説明には、最大 200 文字を使用できます。

ステップ 3　ポートまたはポート範囲ごとに次のコマンドを入力して、グループのポートを定義します。

```
hostname(config-service)# port-object {eq port | range begin_port end_port}
```

使用できるキーワードおよび予約済みポート割り当てのリストについては、「プロトコルとアプリケーション」（P.D-11）を参照してください。

たとえば、DNS（TCP/UDP）、LDAP（TCP）、および RADIUS（UDP）からなるサービス グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group service services1 tcp-udp
hostname(config-service)# description DNS Group
hostname(config-service)# port-object eq domain

hostname(config-service)# object-group service services2 udp
hostname(config-service)# description RADIUS Group
hostname(config-service)# port-object eq radius
hostname(config-service)# port-object eq radius-acct

hostname(config-service)# object-group service services3 tcp
hostname(config-service)# description LDAP Group
hostname(config-service)# port-object eq ldap
```

ICMP タイプ オブジェクト グループの追加

ICMP タイプ オブジェクト グループを追加または変更するには、次の手順を実行します。グループを追加した後、同じグループ名でこの手順を繰り返し、追加のオブジェクトを指定することで、必要に応じてさらにオブジェクトを追加できます。既存のオブジェクトを再入力する必要はありません。設定済みのコマンドは、コマンドの **no** 形式で削除するまで残ります。

ICMP タイプ グループを追加するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、ICMP タイプ グループを追加します。

```
hostname(config)# object-group icmp-type grp_id
```

grp_id は、最大 64 文字の文字列です。

プロンプトが ICMP タイプ コンフィギュレーション モードに変わります。

ステップ 2　（任意）次のコマンドを入力して、説明を追加します。

```
hostname(config-icmp-type)# description text
```

説明には、最大 200 文字を使用できます。

ステップ 3　タイプごとに次のコマンドを入力して、グループの ICMP タイプを定義します。

```
hostname(config-icmp-type)# icmp-object icmp_type
```

ICMP タイプのリストについては、「ICMP タイプ」（P.D-16）を参照してください。

たとえば、（ping を制御する）echo-reply および echo からなる ICMP タイプ グループを作成する場合は、次のコマンドを入力します。

```
hostname(config)# object-group icmp-type ping
hostname(config-service)# description Ping Group
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object echo-reply
```

オブジェクト グループのネスト

オブジェクト グループを同じタイプの別のオブジェクト グループにネストする場合は、「オブジェクト グループの追加」（P.16-14）に従って、ネストするグループを先に作成します。次に、次の手順を実行します。

ステップ 1　次のコマンドを入力して、別のオブジェクト グループをネストするオブジェクト グループを追加または編集します。

```
hostname(config)# object-group {{protocol | network | icmp-type} grp_id | service grp_id
{tcp | udp | tcp-udp}}
```

ステップ 2　次のコマンドを入力して、ステップ 1 で指定したオブジェクト グループの中に指定のグループを追加します。

```
hostname(config-group_type)# group-object grp_id
```

ネストするグループは、同じタイプである必要があります。

ネストしたグループ オブジェクトと通常のオブジェクトは、単一のオブジェクト グループ内でさまざまに組み合わせることができます。

各部門の権限のあるユーザからなるネットワーク オブジェクト グループを作成する例を示します。

```
hostname(config)# object-group network eng
hostname(config-network)# network-object host 10.1.1.5
hostname(config-network)# network-object host 10.1.1.9
```

```
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network hr
hostname(config-network)# network-object host 10.1.2.8
hostname(config-network)# network-object host 10.1.2.12

hostname(config-network)# object-group network finance
hostname(config-network)# network-object host 10.1.4.89
hostname(config-network)# network-object host 10.1.4.100
```

その後、3 つすべてのグループを次のようにネストします。

```
hostname(config)# object-group network admin
hostname(config-network)# group-object eng
hostname(config-network)# group-object hr
hostname(config-network)# group-object finance
```

ACE では次のように管理オブジェクト グループを指定するだけです。

```
hostname(config)# access-list ACL_IN extended permit ip object-group admin host
209.165.201.29
```

アクセス リストでのオブジェクト グループの使用

アクセス リストでオブジェクト グループを使用するには、通常のプロトコル（*protocol*）、ネットワーク（*source_address mask* など）、サービス（*operator port*）、または ICMP タイプ（*icmp_type*）の各パラメータを **object-group** *grp_id* パラメータで置き換えます。

たとえば、**access-list** {**tcp** | **udp**} コマンドで使用できるすべてのパラメータにオブジェクト グループを使用する場合は、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name [line line_number] [extended] {deny |
permit} {tcp | udp} object-group nw_grp_id [object-group svc_grp_id] object-group
nw_grp_id [object-group svc_grp_id] [log [[level] [interval secs] | disable | default]]
[inactive | time-range time_range_name]
```

すべてのパラメータにオブジェクト グループを使用する必要はありません。たとえば、送信元アドレスにオブジェクト グループを使用すれば、宛先アドレスはアドレスとマスクで特定できるといったことが可能です。

次に示す、オブジェクト グループを使用しない通常のアクセス リストでは、内部ネットワーク上のいくつかのホストがいくつかの Web サーバへのアクセスを禁止されます。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
```

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

2 つのネットワーク オブジェクト グループ（内部ホスト用に 1 つ、Web サーバ用に 1 つ）を作成すると、コンフィギュレーションが簡略化され、簡単に修正してホストを追加できるようになります。

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

オブジェクト グループの表示

現在設定されているオブジェクト グループを表示するには、次のコマンドを入力します。

```
hostname(config)# show object-group [protocol | network | service | icmp-type | id grp_id]
```

パラメータを指定しないでコマンドを入力すると、設定されているすべてのオブジェクト グループが表示されます。

次に、**show object-group** コマンドの出力例を示します。

```
hostname# show object-group
object-group network ftp_servers
  description: This is a group of FTP servers
  network-object host 209.165.201.3
  network-object host 209.165.201.4
object-group network TrustedHosts
  network-object host 209.165.201.1
  network-object 192.168.1.0 255.255.255.0
  group-object ftp_servers
```

オブジェクト グループの削除

オブジェクト グループを削除するには、次のいずれかのコマンドを入力します。

（注） アクセス リストで使用中のオブジェクト グループは、削除することも空にすることもできません。

- 特定のオブジェクト グループを削除する場合は、次のコマンドを入力します。

  ```
  hostname(config)# no object-group grp_id
  ```

- 指定したタイプのオブジェクト グループをすべて削除する場合は、次のコマンドを入力します。

  ```
  hostname(config)# clear object-group [protocol | network | services | icmp-type]
  ```

  タイプを入力しない場合、すべてのオブジェクト グループが削除されます。

アクセス リストへのコメントの追加

拡張アクセス リスト、EtherType アクセス リスト、標準アクセス リストを含む任意のアクセス リストに、エントリについてのコメントを追加できます。コメントにより、アクセス リストが理解しやすくなります。

最後に入力した **access-list** コマンドの後にコメントを追加するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name remark text
```

いずれかの **access-list** コマンドの前にコメントを入力すると、コメントはアクセス リストの最初の行に表示されます。

no access-list *access_list_name* コマンドを使用してアクセス リストを削除すると、コメントもすべて削除されます。

テキストは 100 文字まで指定できます。テキストの先頭にスペースを入力できます。末尾のスペースは無視されます。

たとえば、各 ACE の前にコメントを追加すると、アクセス リスト内のその位置にコメントが入ります。コメント テキストの前にダッシュ（-）を入力すると、ACE との区別が容易になります。

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

拡張アクセス リストのアクティベーションのスケジュール設定

ACE に時間範囲を適用して、各 ACE を特定の時刻および曜日にアクティブ化するようにスケジューリングできます。この項では、次のトピックについて取り上げます。

- 「時間範囲の追加」（P.16-20）
- 「時間範囲の ACE への適用」（P.16-21）

時間範囲の追加

時間範囲を追加して時間ベースのアクセス リストを実装するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、時間範囲名を指定します。

```
hostname(config)# time-range name
```

ステップ 2　時間範囲として、定期時間範囲または絶対間範囲のどちらかを指定します。

（注） ACL を非アクティブにするための指定の終了時刻の後、約 80 ～ 100 秒の遅延が発生する場合があります。たとえば、指定の終了時刻が 3:50 の場合、この 3:50 は終了時刻に含まれているため、コマンドは、3:51:00 ～ 3:51:59 の間に呼び出されます。コマンドが呼び出された後、セキュリティ アプライアンスは現在実行されているすべてのタスクを終了し、コマンドに ACL を無効にさせます。

time-range コマンドごとに、複数の定期的なエントリが許可されます。**time-range** コマンドに **absolute** 値と **periodic** 値の両方を指定した場合、**periodic** コマンドは **absolute** 開始時間の到達後にだけ評価され、**absolute** 終了時間の到達後には評価されません。

- 定期時間範囲：

  ```
  hostname(config-time-range)# periodic days-of-the-week time to [days-of-the-week] time
  ```

  days-of-the-week には次の値を指定できます。

  - **monday**、**tuesday**、**wednesday**、**thursday**、**friday**、**saturday**、および **sunday**
  - **daily**
  - **weekdays**
  - **weekend**

  time の形式は、*hh*:*mm* です。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。

- 絶対時間範囲：

  ```
  hostname(config-time-range)# absolute start time date [end time date]
  ```

  time の形式は、*hh*:*mm* です。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。

  date の形式は、*day month year* です。たとえば、**1 january 2006** と指定します。

次に、2006 年 1 月 1 日の午前 8 時に始まる絶対的な時間範囲の例を示します。終了時刻も終了日も指定されていないため、時間範囲は事実上無期限になります。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

次に、平日の午前 8 時～午後 6 時に毎週繰り返される定期的な時間範囲の例を示します。

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

時間範囲の ACE への適用

時間範囲を ACE に適用するには、次のコマンドを入力します。

```
hostname(config)# access-list access_list_name [extended] {deny | permit}...[time-range
name]
```

access-list コマンド構文の詳細については、「拡張アクセス リストの追加」（P.16-6）を参照してください。

（注） ACE のロギングもイネーブルにするには、**log** キーワードを **time-range** キーワードの前に使用します。**inactive** キーワードを使用して ACE をディセーブルにする場合は、**inactive** キーワードを最後のキーワードとして使用します。

次の例では、「Sales」という名前のアクセス リストを「New_York_Minute」という名前の時間範囲にバインドしています。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

アクセス リスト アクティビティのロギング

ここでは、拡張アクセス リストと Webtype アクセス リストにアクセス リスト ロギングを設定する方法について説明します。

この項では、次のトピックについて取り上げます。

アクセス リスト ロギングの概要

デフォルトでは、拡張 ACE または Webtype ACE でトラフィックが定義されている場合、セキュリティ アプライアンスは、拒否されたパケットごとに次の形式のシステム メッセージ 106023 を生成します。

```
%ASA|PIX-4-106023: Deny protocol src [interface_name:source_address/source_port] dst
interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_id
```

セキュリティ アプライアンス が攻撃を受けた場合、拒否されたパケットを示すシステム メッセージの数が非常に大きくなることがあります。代わりに、システム メッセージ 106100 を使用するロギングをイネーブルにすることをお勧めします。このメッセージは各 ACE の統計情報を示すもので、これを使用することにより、生成されるシステム メッセージの数を制限できます。または、すべてのロギングをディセーブルにする方法もあります。

（注） ロギング メッセージは、アクセス リストの ACE によってのみ生成されます。アクセス リストの末尾にある暗黙的な拒否によって生成されることはありません。拒否されたすべてのトラフィックでメッセージが生成されるようにする場合は、次のように、アクセス リストの末尾に暗黙的な ACE を手動で追加します。

```
hostname(config)# access-list TEST deny ip any any log
```

拡張 **access-list** コマンドの末尾に **log** オプションを指定すると、次の動作を設定できます。

- メッセージ 106023 の代わりにメッセージ 106100 をイネーブルにする。
- すべてのロギングをディセーブルにする。
- メッセージ 106023 を使用するデフォルト ロギングに戻る。

システム メッセージ 106100 は次の形式をとります。

```
%ASA|PIX-n-106100: access-list acl_id {permitted | denied} protocol
interface_name/source_address(source_port) -> interface_name/dest_address(dest_port)
hit-cnt number ({first hit | number-second interval})
```

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。セキュリティ アプライアンスは、最初のヒットがあったとき、および各間隔の終わりにシステム メッセージを生成し、その間隔におけるヒットの合計数を示します。各間隔の終わりに、セキュリティ アプライアンスはヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、セキュリティ アプライアンスはそのフロー エントリを削除します。

フローは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートで定義されます。同じ 2 つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。ロギング フローの数を制限するには、「拒否フローの管理」（P.16-24）を参照してください。

確立された接続に属する、許可されたパケットをアクセス リストでチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可された場合でも、すべてのパケットが記録されます。拒否されたパケットはすべて記録されます。

このシステム メッセージの詳細については、『*Cisco Security Appliance Logging Configuration and System Log Messages*』を参照してください。

アクセス コントロール エントリのロギングの設定

ACE のロギングを設定するには、**log** オプションに関する次の情報を参照してください。

```
hostname(config)# access-list access_list_name [extended] {deny | permit}...[log [[level]
[interval secs] | disable | default]]
```

access-list コマンドの完全な構文については、「拡張アクセス リストの追加」（P.16-6）および「Webtype アクセス リストの追加」（P.16-13）を参照してください。

引数を指定せずに **log** オプションを入力すると、システム ログ メッセージ 106100 はデフォルト レベル（6）とデフォルト間隔（300 秒）でイネーブルになります。次のオプションを参照してください。

- *level*：0 ～ 7 の重大度。デフォルトは 6 です。
- **interval** *secs*：システム メッセージ間の時間間隔（秒）。1 ～ 600 で指定します。デフォルトは 300 です。この値は、非アクティブなフローを削除するためのタイムアウト値としても使用されます。
- **disable**：すべてのアクセス リスト ロギングをディセーブルにします。
- **default**：メッセージ 106023 のロギングをイネーブルにします。この設定は、**log** オプションがない場合と同じです。

次に、アクセス リストの設定例を示します。

```
hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600
hostname(config)# access-list outside-acl permit ip host 2.2.2.2 any
hostname(config)# access-list outside-acl deny ip any any log 2
hostname(config)# access-group outside-acl in interface outside
```

パケットが outside-acl の最初の ACE によって許可された場合、セキュリティ アプライアンスは次のシステム メッセージを生成します。

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

この接続の 20 個の後続パケットは、外部インターフェイスに到達しますが、そのトラフィックをアクセス リストでチェックする必要はなく、ヒット数も増加しません。

10 分と指定したインターバルの間に、同じホストでさらにもう 1 つ接続が開始された場合（送信元ポートと宛先ポートは同じまま）、ヒット カウントは 1 だけ増え、10 分のインターバルの最後に次のようなメッセージが表示されます。

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345)->
inside/192.168.1.1(1357) hit-cnt 2 (600-second interval)
```

パケットが 3 番目の ACE によって拒否された場合、セキュリティ アプライアンスは次のシステム メッセージを生成します。

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

5 分のインターバル（デフォルト）の試行回数が 20 回だった場合、5 分経過後に次のようなメッセージが表示されます。

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 21 (300-second interval)
```

拒否フローの管理

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、セキュリティ アプライアンスはフロー エントリを作成して、指定された時間内で受信したパケットの数を追跡します。セキュリティ アプライアンスでは、ACE 用のロギング フローを最大 32 K 保持できます。どの時点でも大量のフローが同時に存在する可能性があります。メモリと CPU のリソースが無限に消費されないように、セキュリティ アプライアンス は同時に存在する*拒否*フロー数を制限します。この限度が設定されるのは、（許可フローではなく）拒否フローだけです。これは、拒否フローが攻撃を示す可能性があるためです。制限に達すると、セキュリティ アプライアンスは既存の拒否フローが期限切れになるまでロギング用の新しい拒否フローを作成しません。

たとえば、DoS 攻撃（サービス拒絶攻撃）が開始された場合、セキュリティ アプライアンスは大量の拒否フローを短時間のうちに作成する可能性があります。拒否フロー数を制限することにより、メモリおよび CPU リソースが無制限に消費されないようになります。

拒否フローの最大数に達すると、セキュリティ アプライアンスは次のようなシステム メッセージ 106100 を発行します。

```
%ASA|PIX-1-106101: The number of ACL log deny-flows has reached limit (number).
```

拒否フローの最大数を設定し、拒否フロー アラート メッセージ（106101）のインターバルを設定する場合は、次のコマンドを入力します。

- セキュリティ アプライアンス がロギングを停止するまで 1 つのコンテキストで許可される拒否フローの最大数を設定するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list deny-flow-max number
  ```

  number には、1 ～ 4096 の範囲内の値を入力します。デフォルト値は 4096 です。

- 拒否フローが最大数に達したことを示すシステム メッセージ（番号 106101）間の時間間隔を設定するには、次のコマンドを入力します。

  ```
  hostname(config)# access-list alert-interval secs
  ```

  seconds には、1 ～ 3600 の範囲内の値を入力します。デフォルト値は 300 です。