CHAPTER 10

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。アクセス リストはさまざまな機能で使用します。Modular Policy Framework を使用する機能の場合、アクセス リストを使用してトラフィック クラス マップ内のトラフィックを識別できます。Modular Policy Framework の詳細については、第 18 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。この章で説明する内容は、次のとおりです。

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.9-7) 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 Access Control Entry（ACE; アクセス制御エントリ）からなります。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。

このセクションでは、次の内容について説明します。

アクセス リストのタイプ

表 10-1 に、アクセス リストのタイプと一般的な用途を示します。

表 10-1　アクセス リストのタイプと一般的な用途

アクセス リストの用途	アクセス リストのタイプ	説明
IP トラフィック（ルーテッド/透過モード）のネットワーク アクセスの制御	拡張	FWSM は、拡張アクセス リストで明示的に許可されていないかぎり、どのようなトラフィックも通過させません。 （注）　管理アクセス用に FWSM インターフェイスにアクセスするために、アクセス リストでホスト IP アドレスを許可する必要はありません。第 21 章「管理アクセスの設定」に従って管理アクセスを設定するだけで済みます。
AAA ルールの対象トラフィックの特定	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特定します。
特定ユーザの IP トラフィックについてネットワーク アクセスの制御	拡張、ユーザ別に 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。RADIUS サーバは FWSM ですでに設定済みのアクセス リストの名前を送信することもできます。
NAT（ポリシー NAT および NAT 除外）の対象アドレスの特定	拡張	ポリシー NAT では、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って、アドレス変換対象のローカル アドレスを特定します。
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。
トラフィック クラス マップでの Modular Policy のトラフィックの識別	拡張 EtherType	Modular Policy Framework をサポートする機能では、アクセス リストを使用してクラス マップ内のトラフィックを識別できます。Modular Policy Framework をサポートする機能には、TCP、一般的な接続設定、インスペクションなどがあります。

表 10-1　アクセス リストのタイプと一般的な用途（続き）

アクセス リストの用途	アクセス リストのタイプ	説明
透過ファイアウォール モードにおける IP 以外のトラフィックのネットワーク アクセス制御	EtherType	EtherType に基づいてトラフィックを制御するアクセス リストを設定できます。
OSPF ルート再分配の指定	標準	標準アクセス リストには、宛先アドレスのみが含まれます。標準アクセス リストを使用して、OSPF ルートの再分配を制御できます。

ACE の順序

アクセス リストは 1 つまたは複数の ACE からなります。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。

任意のアクセス リスト名に入力した各 ACE は、ACE で行番号を指定した場合を除き、アクセス リストの末尾に追加されます（拡張アクセス リストのみ）。

ACE の順序は重要です。FWSM がパケットを転送するかまたは廃棄するかを決定する場合、FWSM は各 ACE に対して、エントリが指定された順番どおりにパケットをテストします。一致すると、それ以上、ACE は確認されません。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許可する ACE を設定した場合は、後ろのステートメントはいっさい確認されません。

ACE を非アクティブ状態にすることで、ACE をディセーブルにできます。

アクセス リストの暗黙拒否

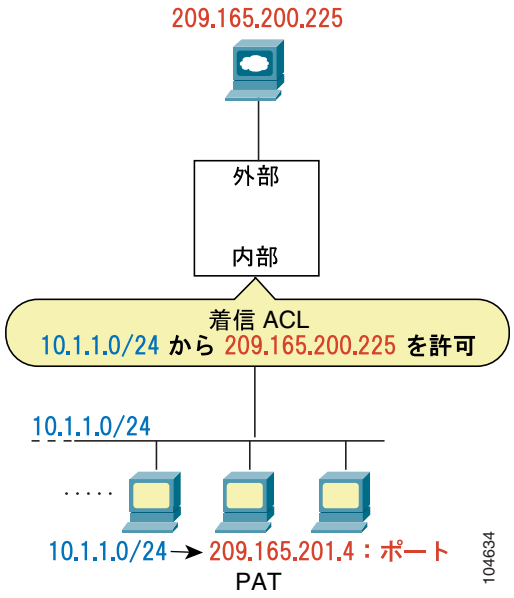
アクセス リストはリストの末尾に暗黙の拒否があるので、明示的に許可しないかぎり、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、FWSM を通過してネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

NAT 使用時のアクセス リスト用 IP アドレス

NAT を使用する場合、アクセス リストに指定する IP アドレスは、アクセス リストを結合するインターフェイスによって決まります。インターフェイスに接続した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。この注意事項は着信アクセス グループと発信アクセス グループの両方に当てはまります。使用するアドレスは方向によって左右されません。アドレスを決定付けるのはインターフェイスだけです。

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 NAT を実行するように FWSM 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 10-1 を参照）。

図 10-1　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

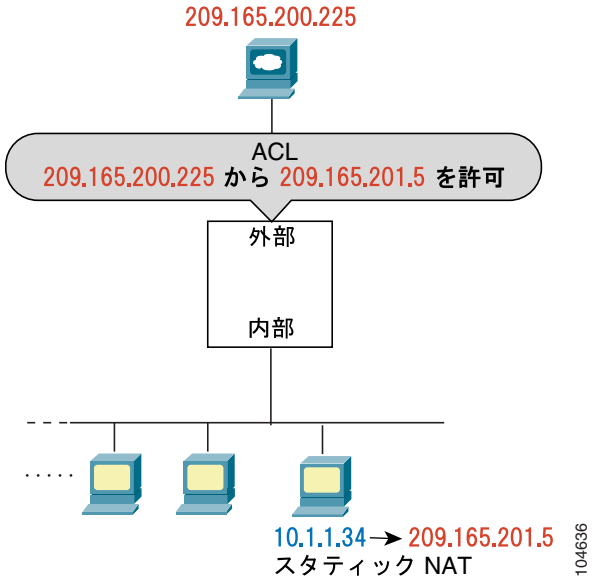


この例に対応するコマンドは、次のとおりです。

```
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 10-2 を参照）。

図 10-2　アクセス リストの IP アドレス：宛先アドレスに NAT を使用

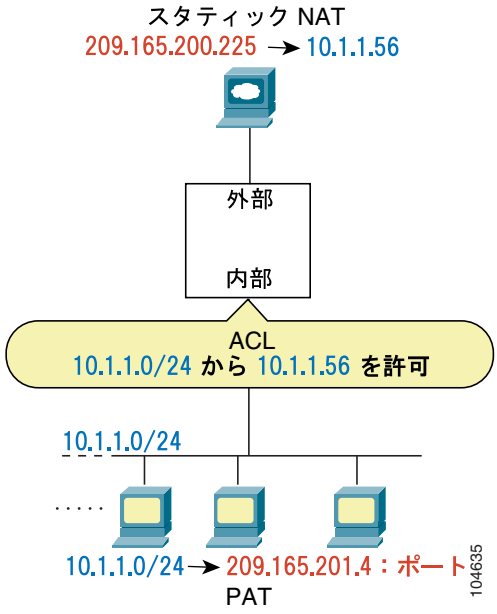


この例に対応するコマンドは、次のとおりです。

```
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 10-3 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 10-3　アクセス リストの IP アドレス：送信元および宛先アドレスに NAT を使用



この例に対応するコマンドは、次のとおりです。

```
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
```

アクセス リストのコミット

アクセス リストに ACE が追加されると、FWSM はネットワーク プロセッサにアクセス リストをコミットすることによって、そのアクセス リストをアクティブにします。FWSM は、最後の **access-list** コマンドが入力されたあと、短い時間待ってからアクセス リストをコミットします。コミット開始後に ACE を入力すると、FWSM はこのコミットを打ち切り、短い待機時間のあとにアクセス リストを再コミットします。FWSM がアクセス リストをコミットすると、次のようなメッセージが表示されます。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

約 60 K の ACE で構成される大きなアクセス リストの場合、大きさにより、コミットに 3 ～ 4 分かかることがあります。

メモリ限度の超過については、「ACE の最大数」（p.10-6）を参照してください。

ACE の最大数

FWSM は、シングルモードの場合、システム全体で最大 80 K、マルチモードで 142 K のルールをサポートします。ルールには ACE、ポリシー NAT に使用される ACE、フィルタ、AAA、ICMP、Telnet、SSH、HTTP、および確立されたルールが含まれます。

アクセス リストによっては、他のアクセス リストよりメモリを多く使用します。大きいポート番号範囲やオーバーラップしたネットワーク（たとえば、ある ACE で 10.0.0.0/8 を指定し、別の ACE で 10.1.1.0/24 を指定して、ACE のネットワークがオーバーラップする場合など）を使用するアクセス リストがこれに該当します。アクセス リストのタイプによって、システムがサポートできる実際の限度は 80 K 未満（シングルモード）または 142 K（マルチモード）未満になります。

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い場合と同じになり、拡張 ACE カウントがシステム限度に近づきます。アクセス リストに指定されている拡張 ACE の数を確認するには、**show access-list** コマンドを入力します。

ACE を追加して、FWSM がアクセス リストをコミットすると、コンソールに次のようなメッセージで使用メモリが表示されます。

```
Access Rules Download Complete: Memory Utilization: < 1%
```

メモリ限度を超えると、エラー メッセージとシステム メッセージ（106024）が表示され、このコミットで追加されたすべてのアクセス リストがコンフィギュレーションから削除されます。前回のコミットで正常にコミットされた 1 組のアクセス リストだけが使用されます。たとえば、プロンプトに 1000 個の ACE をペーストし、最後の ACE でメモリ限度を超えた場合、1000 個の ACE がすべて拒否されます。

拡張アクセス リストの追加

ここでは、拡張アクセス リストの追加方法について説明します。内容は次のとおりです。

拡張アクセス リストの概要

拡張アクセス リストは 1 つまたは複数の ACE からなり、ACE を挿入する行番号、送信元アドレスおよび宛先アドレス、ACE タイプに応じてプロトコル、ポート（TCP/UDP の場合）、または ICMP タイプ（ICMP の場合）を指定できます。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。または、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、「オブジェクトのグループ化によるアクセス リストの簡素化」（p.10-13）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.10-23）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リング」（p.10-21）を参照してください。

TCP/UDP 接続に関しては、トラフィックを戻すためにアクセス リストを使用する必要はありません。FWSM は、確立済みの双方向接続でのすべての戻りトラフィックを許可するからです。ただし、ICMP などのコネクションレス型プロトコルの場合、FWSM は単方向セッションを確立するため、アクセス リストで（アクセス リストを送信元インターフェイスと宛先インターフェイスに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 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各方向に、各タイプ（拡張および 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。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 11 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 リストの設定を変更し、既存の接続がタイムアウトする前に新しいアクセス リスト情報を使用したい場合、**clear local-host** コマンドを使用して接続を消去できます。

透過ファイアウォールを通過できる特殊な IP トラフィック

ルーテッド ファイアウォール モードでは、一部の IP トラフィック タイプはアクセス リストで許可されていてもブロックされます。サポートされないダイナミック ルーティング プロトコル、DHCP（DHCP リレーを設定している場合を除く）などです。透過ファイアウォール モードでは、すべての IP トラフィックの通過を許可します。このような特殊なトラフィック タイプはコネクションレス型であり、両方のインターフェイスにアクセス リストを適用しなければならないので、戻りトラフィックの通過が可能です。

表 10-2 に、透過ファイアウォールを通過させることができる一般的なトラフィック タイプを示します。

表 10-2　透過ファイアウォールの特殊なトラフィック

トラフィック タイプ	プロトコルまたはポート	説明
BGP	TCP ポート 179	—
DHCP	UDP ポート 67 および 68	DHCP サーバをイネーブルにした場合、FWSM は DHCP パケットを通過させません。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
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応じて変動	マルチキャスト ストリームの宛先は常にクラス D アドレス（224.0.0.0 ～ 239.x.x.x）です。
RIP（v1 または v2）	TCP 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** の番号を指定する場合を除き、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、「プロトコルおよびアプリケーション」（p.D-13）を参照してください。

単一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、マスクは入力しません。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** プロトコルに対してのみ指定できます。使用できるキーワードおよび well-known ポートの割り当てについては、「TCP ポートおよび UDP ポート」（p.D-14）を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk はいずれも、TCP 用の定義と UDP 用の定義が 1 つずつ必要です。TACACS+ は、TCP ポート 49 の定義が 1 つ必要です。

*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** — less than（より小さい）
- **gt** — greater than（より大きい）
- **eq** — equal to（等しい）
- **neq** — not equal to（等しくない）

- **range** — 指定された値を含めた範囲。この演算子を使用する場合は、次の例のように、2 つのポート番号を指定します。

  ```
  range 100 200
  ```

ICMP タイプは **icmp** プロトコルに対してのみ指定できます。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.10-16] を参照）。ICMP インスペクション エンジンは、ICMP セッションをステートフル接続として扱います。ping を制御するには、**echo-reply**（**0**）（FWSM からホストへ）または **echo**（**8**）（ホストから FWSM 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.10-16）を参照してください。

ネットワーク マスクを指定する方法は、Cisco IOS ソフトウェアの **access-list** コマンドとは異なります。FWSM ではネットワーク マスクを使用します（クラス C マスクには 255.255.255.0 など）。Cisco IOS ではマスクはワイルドカード ビットを使用します（0.0.0.255 など）。

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全 ACE を入力します。この機能によってコンフィギュレーション内の非アクティブな ACE を記録し、再イネーブルを容易にすることができます。

次の例を参照してください。

次のアクセス リストは、（アクセス リストが適用されるインターフェイス上の）すべてのホストに FWSM の通過を許可します。

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

次のアクセス リストの例は、192.168.1.0/24 上のホストに対して、ネットワーク 209.165.201.0/27 へのアクセスを阻止します。それ以外のすべてのアドレスは許可されます。

```
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
```

アクセスを一部のホストだけに限定する場合は、制限付き許可 ACE を入力します。デフォルトでは、他のすべてのトラフィックは明示的に許可しないかぎり拒否されます。

```
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 リストは、（アクセス リストが適用されるインターフェイス上の）すべてのホストに対して、アドレス 209.165.201.29 の Web サイトへのアクセスを制限します。その他のすべてのトラフィックは許可されます。

```
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

透過ファイアウォール モード限定

ここでは、EtherType アクセス リストの追加方法について説明します。内容は次のとおりです。

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。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 ACE は IPv4 パケットまたは ARP パケットには影響しません。EtherType アクセス リストは、イーサネット V2 フレームをサポートします。802.3 フォーマットのフレームは、タイプ フィールドではなく長さ フィールドを使用するので、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 リストで処理する BPDU です。BPDU は SNAP でカプセル化され、FWSM は BPDU を処理できるように設計されています。

FWSM のポートはトランク ポート（シスコ独自）なので、FWSM はトランク ポート BPDU を受信します。トランク BPDU にはペイロード内に VLAN 情報が含まれるので、BPDU を許可した場合、FWSM は発信 VLAN を使用してペイロードを変更します。フェールオーバーを使用する場合は、ブリッジング ループを防止するために、EtherType アクセス リストで両方のインターフェイスの BPDU を許可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。

MPLS を許可する場合、LDP および TDP TCP 接続が FWSM を介して確立されるようにする必要があります。これは、FWSM に接続された両方の MPLS ルータが、LDP または TDP セッションのルータ ID として FWSM に接続されたルータ インターフェイス上の IP アドレスを使用するように設定することによって行います（LDP および TDP によって、MPLS ルータはパケット転送用ラベル「アドレス」のネゴシエーションができます）。

Cisco IOS ルータ上で、プロトコル（LDP または TDP）に応じたコマンドを入力します。*interface* は FWSM に接続された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
```

インターフェイスの各方向に、各タイプ（拡張および 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。

EtherType ACE の追加

次のコマンドを入力して、EtherType ACE を追加します。

```
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、RFC 1700 「Assigned Numbers」を参照してください。

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、次のアクセス リストの例では、内部インターフェイスを起点とする一般的な EtherType を許可します。

```
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 FWSM 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

標準アクセス リストは、宛先 IP アドレスを識別する一部のコマンドにのみ使用します。たとえば、標準アクセス リストを使用して、OSPF 再分配用のルート マップで使用する OSPF ルートの宛先アドレスを識別します。トラフィックを制御するインターフェイスに標準アクセス リストを適用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。

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}
```

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
```

オブジェクトのグループ化によるアクセス リストの簡素化

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。内容は次のとおりです。

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

例として、次の 3 つのオブジェクト グループを取り上げます。

- 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/UDP ポート番号を指定します。
- TrustedHosts — 最大範囲のサービスおよび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。

これらのグループを作成したあとで、ACE を 1 つだけ使用して、信頼できるホストがパブリック サーバのグループに対して、特定のサービス要求を行うことができるようにします。

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 リストに指定されている拡張 ACE の数を確認するには、**show access-list** コマンドを入力します。

オブジェクト グループの追加

ここでは、オブジェクト グループの追加方法について説明します。内容は次のとおりです。

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手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。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** 形式を指定して削除しないかぎり維持されます。

プロトコル グループを追加する手順は、次のとおりです。

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
```

説明に使用できる文字数は最大 200 文字です。

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 プロトコルを指定する場合は、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、「プロトコルおよびアプリケーション」（p.D-13）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手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。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** 形式を指定して削除しないかぎり維持されます。

（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.9-7）を参照してください。

ネットワーク グループを追加する手順は、次のとおりです。

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
```

説明に使用できる文字数は最大 200 文字です。

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手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。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** 形式を指定して削除しないかぎり維持されます。

サービス グループを追加する手順は、次のとおりです。

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
```

説明に使用できる文字数は最大 200 文字です。

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 well-known ポートの割り当てのリストについては、「プロトコルおよびアプリケーション」（p.D-13）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手順は、次のとおりです。グループを追加したあと、同じグループ名で次の手順を繰り返し、他のオブジェクトを指定することによって、オブジェクトを必要なだけ追加できます。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** 形式を指定して削除しないかぎり維持されます。

ICMP タイプ グループを追加する手順は、次のとおりです。

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
```

説明に使用できる文字数は最大 200 文字です。

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 のタイプ」（p.D-17）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.10-13）に従って、ネストするグループを先に作成します。さらに、次の作業を行います。

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、同じタイプでなければなりません。

1 つのオブジェクト グループの中で、ネストされたグループ オブジェクトと標準オブジェクトを混在させて照合できます。

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
```

さらに、3 つのグループを 1 つにネストします。

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

次のように、ACE で管理（admin）オブジェクト グループを指定するだけで済むようになります。

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

アクセス リストでオブジェクト グループを使用する方法

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、標準プロトコル（*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*）パラメータを **object-group** *grp_id* パラメータに置き換えます。

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]
```

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。

次のオブジェクト グループを使用しない標準アクセス リストは、内部ネットワーク上の複数のホストに対して、複数の Web サーバへのアクセスを制限します。その他のすべてのトラフィックは許可されます。

```
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
```

内部ホストと Web サーバ用に 1 つずつ、2 つのネットワーク オブジェクト グループを作成すると、設定が簡素化され、ホストを追加するときの変更が容易になります。

```
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 グループを削除したり、または空にしたりすることはできません。

- 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]
  ```

  タイプを入力しなかった場合は、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 リストをはじめ、あらゆるアクセス リストでエントリに関するコメントを追加できます。コメントによってアクセス リストがわかりやすくなります。

次のコマンドを入力して、アクセス リストにコメントを追加します。

```
hostname(config)# access-list access_list_name [line line_number] remark text
```

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

clear configure 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。

テキストは最大 100 文字の長さまで入力できます。テキストの先頭に先行スペースを入力することもできます。後続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リング

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。このセクションでは、次の内容について説明します。

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。

time-range コマンドごとに複数の定期エントリを入力できます。**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のみ評価され、**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 に対して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 8:00 a.m で 20:00 は 8:00 p.m になります。
- 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 8:00 a.m で 20:00 は 8:00 p.m になります。

  date の形式は*日月年*で、**1 january 2006** のようになります。

次に、2006 年 1 月 1 日 8:00 a.m. に始まる絶対時間範囲の例を示します。終了日時を指定しないため、時間範囲は無期限に有効です。

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

次に、平日の 8:00 a.m. から 6:00 p.m. の週の定期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

次のコマンドを入力して、時間範囲を ACE に適用します。

```
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.10-7）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場合、**time-range** キーワードの前に **log** キーワードを使用します。**inactive** キーワードを使用して ACE をディセーブルにする場合、最後のキーワードとして **inactive** キーワードを使用します。

次に、「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結合する例を示します。

```
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。

内容は次のとおりです。

アクセス リスト ロギングの概要

デフォルトでは、拡張 ACE によってトラフィックが拒否された場合、FWSM は拒否されたパケットごとにシステム メッセージ 106023 を生成します。メッセージの形式は次のとおりです。

```
%XXX-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
```

FWSM が攻撃を受けると、拒否パケットに関するシステム メッセージの数が膨大になりかねません。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推奨します。各 ACE の統計情報が得られ、生成されるシステム メッセージ数を制限できます。または、すべてのロギングをディセーブルにすることもできます。

（注）　ロギング メッセージを生成するのは、アクセス リストで指定された ACE だけです。アクセス リストの末尾の暗黙拒否はメッセージを生成しません。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のロギングに戻す

システム メッセージ 106100 の形式は、次のとおりです。

```
%XXX-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のときに、パケットが ACE と一致すると、FWSM は一定の間隔で受信パケット数を追跡するフロー エントリを作成します。FWSM は、最初のヒットと各インターバルの最後にシステム メッセージを生成し、インターバルの間のヒット総数を示します。インターバルが終了するたびに、FWSM はヒット カウントを 0 にリセットします。インターバルの間にパケットが ACE と一致しなかった場合、FWSM はフロー 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、およびポートによって定義されます。同じ 2 つのホスト間でも、新しい接続では送信元ポートが異なる可能性があり、接続用に新しいフローが作成されるので、フローの増加分が同じではないことがあります。

確立済みの接続に属する許可パケットは、改めてアクセス リストと照合する必要はありません。最初のパケットだけを記録し、ヒット カウントに含めます。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。

システム メッセージの詳細については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Logging Configuration and System Log Messages*』を参照してください。

ACE ロギングの設定

ACE ロギングを設定する場合は、次の **log** オプションの説明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 コマンド構文の詳細については、「拡張アクセス リストの追加」（p.10-7）を参照してください。

（注） ACE の時間範囲もイネーブルにする場合、**time-range** キーワードの前に **log** キーワードを使用します。**inactive** キーワードを使用して ACE をディセーブルにする場合、最後のキーワードとして **inactive** キーワードを使用します。

引数を指定しないで **log** オプションを入力した場合は、システム ログ メッセージ 106100 がデフォルトのレベル（6）、デフォルトのインターバル（300 秒）でイネーブルになります。次のオプションを指定できます。

- *level* — 重大度レベル 0 ～ 7。デフォルトは 6 です。
- **interval** *secs* — 秒数で指定するシステム メッセージの時間間隔（1 ～ 600）。デフォルトは 300 です。アクティブではないフローを削除するタイムアウト値としても、この値を使用します。
- **disable** — すべてのアクセス リスト ロギングがディセーブルになります。
- **default** — メッセージ 106023 でのロギングがイネーブルになります。この設定は、**log** オプションを指定しないのと同じことです。

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
```

outside-acl の最初の ACE によってパケットが許可された場合、FWSM は次のようなシステム メッセージを生成します。

```
%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)
```

この接続ではさらに 20 のパケットが外部インターフェイスに届きますが、トラフィックをアクセス リストと照合する必要はなく、ヒット カウントも増えません。

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。

```
%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)
```

3 番めの ACE によってパケットが拒否された場合、FWSM は次のようなシステム メッセージを生成します。

```
%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。

```
%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のときに、パケットが ACE と一致すると、FWSM は一定の間隔で受信パケット数を追跡するフロー エントリを作成します。FWSM が ACE に使用するロギング フローは、最大で 32 K です。多数のフローが同時に存在可能です。メモリおよび CPU リソースが無限に消費されないように、FWSM 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）攻撃を示す可能性のある拒否フローだけです。この限度に達した場合、FWSM は既存のフローがタイムアウトするまで、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、ある人が DoS 攻撃を開始した場合、FWSM は短時間に大量の拒否フローを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って、メモリおよび CPU リソースが無限に消費されることがなくなります。

拒否フローの最大数に達すると、FWSM はシステム メッセージ 106100 を発行します。

```
%XXX-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。

- FWSM がロギングを停止するまでに、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場合は、次のコマンドを入力します。

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

  number は 1 ～ 4096 です。4096 がデフォルトです。
- 拒否フローの最大数に達したことを伝えるシステム メッセージ（106101）の発行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 は 1 ～ 3600 です。300 がデフォルトです。