CHAPTER 13

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 20 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.10-5）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 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。

ここでは、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 13-1 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 13-1　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	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の通過も許可しません。 **（注）** また、管理アクセス用の FWSM 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 23 章「管理アクセスの設定」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 規則でのトラフィック識別	拡張	AAA 規則では、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 コントロール	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、FWSM 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。
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	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検査などがあります。
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。

ACE の順序

アクセス リストは 1 つまたは複数の Access Control Entry（ACE; 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。

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 リスト限定）。

ACE の順序は重要です。FWSM でパケットを転送するか廃棄するかを決定する場合、FWSM 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。一致するものが見つかると、残りの ACE は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

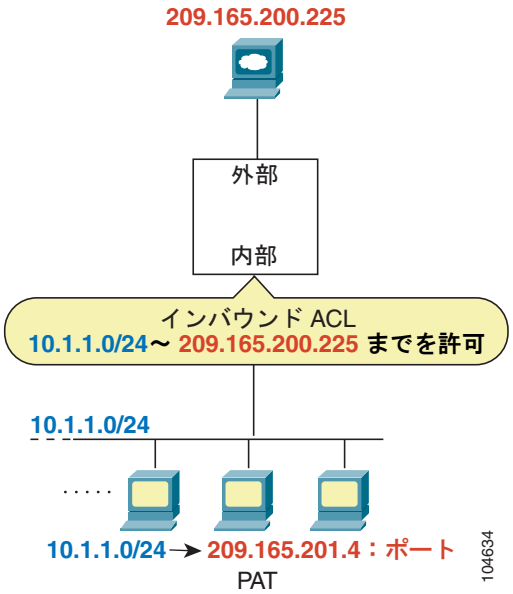
アクセス リストの末尾に暗黙拒否が指定されているため、明示的に許可しないかぎり、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、FWSM を通過してネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

NAT 使用時のアクセス リスト用の 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。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。使用されるアドレスを決定するのは、方向ではなく、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対して 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 13-1 を参照）。

図 13-1　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

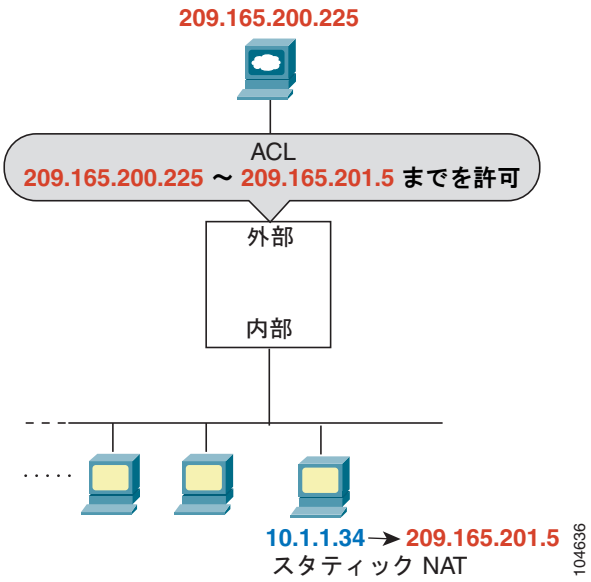


この例について、次のコマンドを参照してください。

```
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 13-2 を参照）。

図 13-2　アクセス リストの IP アドレス：宛先アドレスに NAT を使用

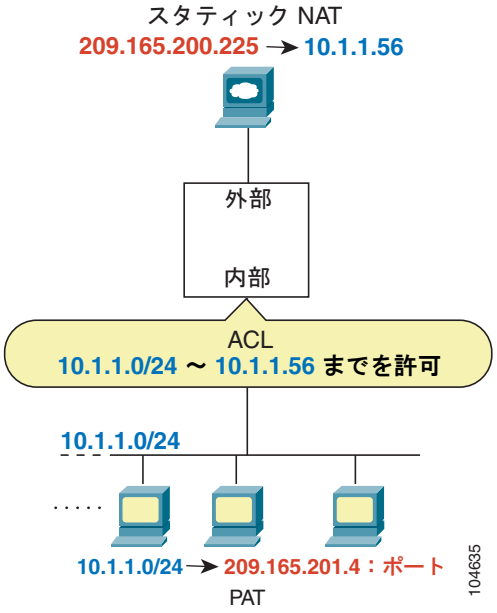


この例について、次のコマンドを参照してください。

```
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 13-3 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 13-3　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
```

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、**access-list** コマンドが最後に入力されてから少し待機したあとで、アクセス リストをコミットします。コミットの開始後に ACE を入力した場合、FWSM はこのコミットを打ち切り、少し待機したあとでアクセス 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。

（注）　各アクセス リストの変更後とネットワーク プロセッサへの以降のコミット後にこのメッセージが表示されないようにするには、**np acl-notify disable** コマンドを入力します。このコマンドはローカルであり、スタートアップ コンフィギュレーションに保存されていないため、フェールオーバーによってピアに複製されません。したがって、リロードを実行するごとにこのコマンドを入力し直す必要があります。

メモリ限度の超過については、「ACE の最大数」を参照してください。

ACE の最大数

FWSM はシステム全体で最大数の ACE をサポートしています。ルールの制限（ACE のルールを含む）と別のタイプのルールの詳細については、「ルールの制限」（P.A-6）を参照してください。

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。また、アクセス リストのタイプによっては、システムでサポートできる実際の制限値が最大値よりも小さくなります。

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 を追加した場合に、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 ログ 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 で構成され、ACE を挿入する行番号、送信元アドレスと宛先アドレス、ACE の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、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.13-12）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.13-26）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.13-24）を参照してください。

ルーテッド モードとトランスペアレント モードの両方のモードの TCP および UDP 接続では、トラフィックを戻すのにアクセス リストを使用する必要はありません。この理由として、FWSM は確立済みの双方向接続ですべての戻りトラフィックを許可するためです。ただし、ICMP などのコネクションレス型プロトコルでは、FWSM 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 エンジンでは、ICMP セッションは双方向接続として処理されます。

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 15 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 13-2 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 13-2　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	変更点
DHCP	UDP ポート 67 および 68	DHCP サーバがイネーブルの場合、FWSM 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	—
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 ～ 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.E-11）を参照してください。

単一のアドレスを指定するには、IP アドレスの前に **host** キーワードを入力します。この場合、マスクを入力しないでください。すべてのアドレスを指定するには、アドレスおよびマスクの代わりに **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 ポートおよび UDP ポート」（P.E-12）を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk には、それぞれ TCP の定義が 1 つと UDP の定義が 1 つ必要です。TACACS+ には、TCP のポート 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**：より小さい
- **gt**：より大きい
- **eq**：等しい
- **neq**：等しくない
- **range**：値の範囲。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.13-15）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**）（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.13-15）を参照してください。

ネットワーク マスクを指定する場合に使用する方式は、Cisco IOS ソフトウェア **access-list** コマンドの方式と異なります。FWSM 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 のマスクでは、ワイルドカード ビット（0.0.0.255 など）を使用します。

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** キーワードなしで 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。

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 FWSM 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
```

次のアクセス リストの例は、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しないようにします。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
```

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、それ以外のすべてのトラフィックは、明示的に許可されない限り拒否されます。

```
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 リストを適用するインターフェイス上の）すべてのホストが、アドレス 209.165.201.29 の Web サイトにアクセスできないようにします。その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

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。ここでは、次の内容について説明します。

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 Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）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）であるため、FWSM はトランク ポート BPDU を受信します。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、FWSM により、発信 VLAN を使用してペイロードが修正されます。

（注）　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。

双方向にアクセス リストを適用

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拒否は IP トラフィックと ARP トラフィックに影響しない

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拒否は IPv4 トラフィックと ARP トラフィックに影響しません。たとえば、EtherType 8037 を許可すると、アクセス リストの末尾にある暗黙拒否は、拡張アクセス リストですでに許可されている IP トラフィックをブロックしません。IPv4 トラフィックと ARP トラフィックは、EtherType アクセス リストで制御することができません。

同じインターフェイス上で拡張アクセス リストと EtherType アクセス リストを使用

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、ラベル配布プロトコルおよびタグ配布プロトコルの TCP 接続が FWSM を経由して確立されるようにしてください。これには、FWSM 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、FWSM 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 では、MPLS ルータが、パケットの転送に使用されるラベル（アドレス）をネゴシエートできます）。

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、FWSM 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

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 にアクセスして、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 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でだけ使用します。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。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。

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。ここでは、次の内容について説明します。

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。

たとえば、送信元の数が 100 の 1 つのネットワーク オブジェクト グループ、宛先の数が 100 の 1 つのネットワーク オブジェクト グループ、およびポートの数が 5 の 1 つのポート オブジェクト グループがあるとします。この場合に送信元から宛先へのポートを許可すると、拡張アクセス リスト内の ACE の数が 50,000（5 x 100 x 100）になります。

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.E-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手順は、次のとおりです。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.10-5）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手順は、次のとおりです。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.E-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手順は、次のとおりです。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.E-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.13-13）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、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。その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。コメントにより、アクセス リストが理解しやすくなります。

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** の番号を指定した場合を除き、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 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
```

アクセス リスト グループ最適化

アクセス リスト最適化機能では、重複した ACE と競合した ACE の結合や削除によって、アクセス リストのセマンティックに影響を与えることなくグループ当たりの ACE の数が削減されます。

ここでは、次の内容について説明します。

アクセス リスト グループ最適化の機能

最適化の実行中に、2 つのルールを結合できるかどうかを判別するために、4 つのケース（サブセット、スーパーセット、隣接、および重複）が検査されます。

- サブセット：ルール x がルール y のサブセットである場合、ルール x はルール y に下位結合されます。

  最適化前

  ```
  access-list test extended permit tcp 10.1.1.1 255.255.255.255 any eq 80 [rule x]
  access-list test extended permit tcp 10.1.1.0 255.255.255.0 any  [rule y]
  ```

  最適化後

  ```
  access-list test extended permit tcp 10.1.1.0 255.255.255.0 any [rule y]
  ```

- スーパーセット：ルール x がルール y のスーパーセットである場合、ルール y はルール x に上位結合されます。

  最適化前

  ```
  access-list test extended permit udp 10.1.1.0 255.255.255.0 any [rule x]
  access-list test extended permit udp 10.1.1.1 255.255.255.255 any [rule y]
  ```

  最適化後

  ```
  access-list test extended permit udp 10.1.1.0 255.255.255.0 any [rule x]
  ```

- 隣接：ルール x がルール y に隣接している場合、ルール y はルール x に上位結合されます。

  最適化前

  ```
  access-list test extended permit ip 10.1.1.0 255.255.255.128 any [rule x]
  access-list test extended permit ip 10.1.1.128 255.255.255.128 any [rule y]
  ```

  最適化後

  ```
  access-list test extended permit ip 10.1.1.0 255.255.255.0 any [rule x]
  ```

- 重複：ルール x がルール y と重複している場合、ルール y はルール x に上位結合されます。

  最適化前

  ```
  access-list test extended permit tcp any any range 50 100 [rule x]
  access-list test extended permit tcp any any range 60 120 [rule y]
  ```

  最適化後

  ```
  access-list test extended permit tcp any any range 50 120 rule x]
  ```

（注）　重複した 2 つのルール間のアクセス リストに競合したルールが存在する場合、これらのルールの結合はできません。

- 許可 / 拒否 : ルール x がルール y およびルール z と重複しており、ルール y に異なる権限 / アクションが定義されている場合、ルール x とルール z は、両方のルールに同じ権限 / アクションが定義されている場合でも結合できません。

  最適化前

  ```
  access-list test extended permit tcp any any range 50 100 [rule x]
  access-list test extended deny tcp any any range 80 130 [rule y]
  access-list test extended permit tcp any any range 60 120 [rule z]
  ```

  最適化後

  ```
  access-list test extended permit tcp any any range 50 100 [rule x]
  access-list test extended deny tcp any any range 80 130 [rule y]
  access-list test extended permit tcp any any range 60 120 [rule z]
  ```

- ロギング（default キーワードと disable キーワード）:「log default」キーワードが定義されたルール x と「log disable」キーワードが定義されたルール y が重複している場合、ルール x とルール y は、両方のルールに「permit」アクションが定義されている場合に限り結合できます。

  最適化前

  ```
  access-list test extended permit tcp any any range 50 100 log default [rule x]
  access-list test extended permit tcp any any range 80 130 log disable [rule y]
  ```

  最適化後

  ```
  access-list test extended permit tcp any any range 50 130 log default [rule x]
  ```

  最適化前

  ```
  access-list test extended deny tcp any any range 50 100 log default [rule x]
  access-list test extended deny tcp any any range 80 130 log disable [rule y]
  ```

  最適化後

  ```
  access-list test extended deny tcp any any range 50 100 log default [rule x]
  access-list test extended deny tcp any any range 80 130 log disable [rule y]
  ```

- ロギング（syslog レベル / 時間範囲 / 非アクティブ）: ログ レベル、時間範囲、または非アクティブが定義されたルールは、他のルールと結合できません。このルールは、ブロッキング ルールになることもあります。

  最適化前

  ```
  access-list test extended permit tcp any any range 50 100 [rule x]
  access-list test extended permit tcp any any range 80 130 log critical [rule y]
  access-list test extended permit tcp any any range 60 120 [rule z]
  ```

  最適化後

  ```
  access-list test extended permit tcp any any range 50 100 [rule x]
  access-list test extended permit tcp any any range 80 130 log critical [rule y]
  access-list test extended permit tcp any any range 60 120 [rule z]
  ```

（注）　アクセス リスト最適化が適用されるのは、静的な拡張アクセス リストだけです。動的なアクセス リストは最適化されません。また、アクセス リストが AAA、ポリシー NAT、およびフィックスアップ モジュールに結合された場合は、これらのルールの 2 つのコピーがシステム内に同時に存在することになります。最適化されたコピーは、アクセス リストがアクセス グループに結合された場合に使用され、最適化されていない元のコピーは、AAA、ポリシー NAT、およびフィックスアップに使用されます。

アクセス リスト グループ最適化の設定

アクセス リスト グループ最適化を設定する手順は、次のとおりです。

ステップ 1　アクセス リスト グループ最適化をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# access-list optimization enable
```

アクセス リスト グループ最適化をディセーブルにする場合は、そのコマンドの **no** 形式を使用します。

ステップ 2　最適化されたアクセス リストに関する情報を表示するには、次のコマンドを使用します。

```
hostname(config)# show access-list [id] [optimization [detail] [range low high]]
```

id 引数は、特定のアクセス リストを示します。**detail** キーワードは、最適化の詳細を示します。**range** キーワードには、特定のアクセス リストの範囲を low 引数と high 引数で指定できます。

ステップ 3　最適化された実行コンフィギュレーションを指定の場所にコピーするには、次のコマンドを使用します。

```
hostname(config)# copy optimized-running-config [url | running-config | startup-config | system]
```

url 引数には、コピーする送信元ファイルまたは宛先ファイルを指定します（disk:、*ftp:*、または tftp:）。

（注）　**copy optimized-running-config** コマンドは実行コンフィギュレーションを上書きするため、設定を保存した場合に、実行コンフィギュレーションから object-group アクセス リストの行が失われる可能性があります。通常、最適化されたコンフィギュレーションに含まれる通常 ACE は、オブジェクト グループの ACE よりも多いため、この操作により、実行コンフィギュレーションのサイズが増大する可能性があります。また、多数のアクセス リストが設定に含まれている場合は、この処理によって、サイズが 3 MB を超える大規模な設定ファイルが生成されることがあります。したがって、このコマンドは、スタートアップ コンフィギュレーションのサイズ制限を超えないことが確実な場合に使用してください。

次に、最適化されたアクセス リスト設定の例を示します。

元のアクセス リスト設定を表示します。

```
hostname(config)# sh access-list test
access-list test; 13 elements
access-list test line 1 extended permit tcp host 10.1.1.6 host 10.1.1.20 eq www (hitcnt=0) 0x1d3335f6
access-list test line 2 extended permit tcp any host 10.1.1.90 eq ssh (hitcnt=0) 0x9f0b14e0
access-list test line 3 extended permit tcp any host 10.1.1.90 eq ftp (hitcnt=0) 0x7d023e5f
access-list test line 4 extended permit tcp any object-group dns-servers eq domain 0xb4b0751d
access-list test line 4 extended permit tcp any host 10.10.10.5 eq domain (hitcnt=0) 0x9664696e
access-list test line 4 extended permit tcp any host 10.10.10.6 eq domain (hitcnt=0) 0xde9a7aec
access-list test line 4 extended permit tcp any host 10.10.10.7 eq domain (hitcnt=0) 0x5847c29a
access-list test line 4 extended permit tcp any host 10.10.10.8 eq domain (hitcnt=0) 0xa4246eba
```

```
access-list test line 4 extended permit tcp any host 10.10.10.9 eq domain (hitcnt=0) 0x85fc0e4a
access-list test line 5 extended permit udp any any eq domain (hitcnt=0) 0xbaf2384c
access-list test line 6 extended permit tcp 10.1.1.0 255.255.255.0 any (hitcnt=0) 0xd07a176b
access-list test line 7 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 8 extended permit udp any any neq domain (hitcnt=0) 0x8e2ee97e
access-list test line 9 extended permit tcp any host 10.10.10.5 (hitcnt=0) 0xaa819def
```

アクセス リスト グループ最適化をイネーブルにします。

```
hostname(config)# access-list optimization enable
ACL group optimization is enabled
hostname(config)#
Access Lists Optimization Complete
Access Rules Download Complete: Memory Utilization: < 1%
```

（注） 最適化をイネーブルにすると、ルールが最適化されて NP にダウンロードされます。最適化されていない元のルールは非アクティブになります。ルールの追加/削除は、最適化されていない元のアクセス リストで実行する必要があります。新しいルールを追加/削除すると、最適化処理が繰り返された後、最適化が終了したことを示す「アクセス リスト最適化完了」メッセージが表示されます。この処理期間中のアクセス リスト情報には、最適化処理が完了するまで正確でないものもあります。

最適化されていない（元の）アクセス リストをもう一度表示します。

```
hostname(config)# show access-list test
access-list test; 13 elements
access-list test line 1 extended permit tcp host 10.1.1.6 host 10.1.1.20 eq www (hitcnt=*) 0x1d3335f6
access-list test line 2 extended permit tcp any host 10.1.1.90 eq ssh (hitcnt=*) 0x9f0b14e0
access-list test line 3 extended permit tcp any host 10.1.1.90 eq ftp (hitcnt=*) 0x7d023e5f
access-list test line 4 extended permit tcp any object-group dns-servers eq domain 0xb4b0751d
access-list test line 4 extended permit tcp any host 10.10.10.5 eq domain (hitcnt=*) 0x9664696e
access-list test line 4 extended permit tcp any host 10.10.10.6 eq domain (hitcnt=*) 0xde9a7aec
access-list test line 4 extended permit tcp any host 10.10.10.7 eq domain (hitcnt=*) 0x5847c29a
access-list test line 4 extended permit tcp any host 10.10.10.8 eq domain (hitcnt=*) 0xa4246eba
access-list test line 4 extended permit tcp any host 10.10.10.9 eq domain (hitcnt=*) 0x85fc0e4a
access-list test line 5 extended permit udp any any eq domain (hitcnt=*) 0xbaf2384c
access-list test line 6 extended permit tcp 10.1.1.0 255.255.255.0 any (hitcnt=0) 0xd07a176b
access-list test line 7 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 8 extended permit udp any any neq domain (hitcnt=*) 0x8e2ee97e
access-list test line 9 extended permit tcp any host 10.10.10.5 (hitcnt=0) 0xaa819def
```

（注） 一部のヒット カウント値はアスタリスク「*」で表されます。アスタリスクは、そのルールが別のルールと結合されているため、ヒット カウント値が正確でないことを示します。最適化されたルールのヒット カウントは、結合されたルールと削除されたルールのすべてのヒット カウントを累積した値になります。結合されたルールまたは削除されたルールごとにヒット カウントを求める方法はありません。

最適化されたアクセス リストを表示します。

```
hostname(config)# show access-list test optimization
access-list test;
13 elements before optimization
7 elements after optimization

Reduction rate = 46%

access-list test line 2 extended permit tcp any host 10.1.1.90 range ftp ssh (hitcnt=0) 0x9f0b14e0
access-list test line 4 extended permit tcp any 10.10.10.6 255.255.255.254 eq domain (hitcnt=0)
0xde9a7aec
access-list test line 4 extended permit tcp any 10.10.10.8 255.255.255.254 eq domain (hitcnt=0)
0xa4246eba
access-list test line 5 extended permit udp any any (hitcnt=0) 0xbaf2384c
access-list test line 6 extended permit tcp 10.1.1.0 255.255.255.0 any (hitcnt=0) 0xd07a176b
access-list test line 7 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 10 extended permit tcp any host 10.10.10.5 (hitcnt=0) 0xaa819def
```

最適化されたアクセス リストの詳細を表示します。

```
hostname(config)# show access-list test optimization detail
access-list test;
13 elements before optimization
7 elements after optimization

Reduction rate = 46%

SUBSET rules   : 2
ADJACENT rules : 5

access-list test line 1 extended permit tcp host 10.1.1.6 host 10.1.1.20 eq www (hitcnt=0) 0x00000000
[Merged to 6: SUBSET]
access-list test line 2 extended permit tcp any host 10.1.1.90 range ftp ssh (hitcnt=0) 0x9f0b14e0
[(3)]
access-list test line 3 extended permit tcp any host 10.1.1.90 eq ftp (hitcnt=0) 0x00000000 [Merged to
2: ADJACENT]
access-list test line 4 extended permit tcp any object-group dns-servers eq domain 0xb4b0751d
access-list test line 4.1 extended permit tcp any host 10.10.10.5 eq domain (hitcnt=0) 0x00000000
[Merged to 9: SUBSET]
access-list test line 4.2 extended permit tcp any 10.10.10.6 255.255.255.254 eq domain (hitcnt=0)
0xde9a7aec  [(4.3)]
access-list test line 4.3 extended permit tcp any host 10.10.10.7 eq domain (hitcnt=0) 0x00000000
[Merged to 4.2: ADJACENT]
access-list test line 4.4 extended permit tcp any 10.10.10.8 255.255.255.254 eq domain (hitcnt=0)
0xa4246eba  [(4.5)]
access-list test line 4.5 extended permit tcp any host 10.10.10.9 eq domain (hitcnt=0) 0x00000000
[Merged to 4.4: ADJACENT]
access-list test line 5 extended permit udp any any (hitcnt=0) 0xbaf2384c  [(8.1,8.2)]
access-list test line 6 extended permit tcp 10.1.1.0 255.255.255.0 any (hitcnt=0) 0xd07a176b  [(1)]
access-list test line 7 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 8.1 extended permit udp any any lt domain (hitcnt=0) 0x00000000 [Merged to 5:
ADJACENT]
access-list test line 8.2 extended permit udp any any gt domain (hitcnt=0) 0x00000000 [Merged to 5:
ADJACENT]
access-list test line 9 extended permit tcp any host 10.10.10.5 (hitcnt=0) 0xaa819def  [(4.1)]
```

（注） ルール情報の中には、結合された時点で変更されるものもあります。ルール 2 は、ルール 3 と結合されたために変更されました。最適化されていない元のルール 2 を表示する場合、ユーザは（たとえば、**show access-list test** コマンドを使用して）最適化されていない（元の）アクセス リストを参照する必要があります。

最適化されたアクセス リストの範囲 2 ～ 5 を表示します。

```
hostname(config)# show access-list test optimization range 2 5
access-list test;
13 elements before optimization
7 elements after optimization

Reduction rate = 46%

access-list test line 2 extended permit tcp any host 10.1.1.90 range ftp ssh (hitcnt=0) 0x9f0b14e0
access-list test line 4 extended permit tcp any 10.10.10.6 255.255.255.254 eq domain (hitcnt=0)
0xde9a7aec
access-list test line 4 extended permit tcp any 10.10.10.8 255.255.255.254 eq domain (hitcnt=0)
0xa4246eba
access-list test line 5 extended permit udp any any (hitcnt=0) 0xbaf2384c
```

最適化されたアクセス リストの範囲 6 ～ 9 の詳細を表示します。

```
hostname(config)# show access-list test optimization detail range 6 9
access-list test;
13 elements before optimization
7 elements after optimization

Reduction rate = 46%

SUBSET rules   : 2
ADJACENT rules : 5

access-list test line 6 extended permit tcp 10.1.1.0 255.255.255.0 any (hitcnt=0) 0xd07a176b  [(1)]
access-list test line 7 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 8.1 extended permit udp any any lt domain (hitcnt=0) 0x00000000 [Merged to 5:
ADJACENT]
```

```
access-list test line 8.2 extended permit udp any any gt domain (hitcnt=0) 0x00000000 [Merged to 5:
ADJACENT]
access-list test line 9 extended permit tcp any host 10.10.10.5 (hitcnt=0) 0xaa819def  [(4.1)]
```

最適化が現在実行中のアクセス リストを表示します。

```
hostname(config)# show running-config access-list test optimization
access-list test extended permit tcp any host 10.1.1.90 range ftp ssh
access-list test extended permit tcp any 10.10.10.6 255.255.255.254 eq domain
access-list test extended permit tcp any 10.10.10.8 255.255.255.254 eq domain
access-list test extended permit udp any any
access-list test extended permit tcp 10.1.1.0 255.255.255.0 any
access-list test extended permit icmp any any
access-list test extended permit tcp any host 10.10.10.5
```

元のアクセス リストを、最適化されたアクセス リストに置き換えます。

```
hostname(config)# copy optimized-running-config running-config

Destination filename [running-config]?

hostname(config)#
Access Lists Optimization Complete
Access Rules Download Complete: Memory Utilization: < 1%
```

（注） アクセス リスト最適化を常時イネーブルにすると、計算リソースとメモリ リソースが無駄に消費されることがあります。最適化されたアクセス リストの結合方法に問題がない場合は、元のアクセス リストを、最適化されたアクセス リストに置き換えることができます。このアクションを実行すると、元のアクセス リストがすべて消去される点に注意してください。最適化されたアクセス リストをコピーしたら、アクセス リスト最適化をディセーブルにすることができます。これは、最適化されたアクセス リストを新たにコピーしても、さらに最適化されることがないためです。

アクセス リスト グループ最適化をディセーブルにします。

```
hostname(config)# no access-list optimization enable
Disabling ACL optimization will cause ACL rules get increased.
The non optimized rules might be more than the partition rule max
and might cause memory exhaustion to lose partial or all the
access-list configuration after disabling the optimization.
Please save a copy of your current optimized access-list config
before committing this command.
Continue ? [Y]es/[N]o:
ACL group optimization is disabled
hostname(config)# Access Rules Download Complete: Memory Utilization: < 1%

hostname(config)#
```

（注） アクセス リスト最適化をディセーブルにする場合は、最適化されていない元のルールの数（ほとんどの場合、最適化されたルールの数よりも多くなります）が、これらのルールを保存できるメモリの量を超えることがある点に注意してください。この状況でディセーブル化を行うと、いくつかのルールが削除されます。この場合は、アクセス リスト グループ最適化をディセーブルにする前に、元の設定のバックアップを取っておくことを推奨します。

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。ここでは、次の内容について説明します。

- 「時間範囲の追加」（P.13-25）
- 「時間範囲の ACE への適用」（P.13-26）

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 1 つあたり複数の periodic エントリを使用できます。**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 8:00 a.m. です。20:00 は 8:00 p.m. です。

- 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. です。20:00 は 8:00 p.m. です。

  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

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.13-6）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。

ここでは、次の内容について説明します。

- 「アクセス リスト ロギングの概要」（P.13-26）
- 「ACE ロギングの設定」（P.13-27）
- 「拒否フローの管理」（P.13-28）

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 ログ メッセージ 106023 を生成します。この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、拒否されたパケットに関して膨大な数のシステム ログ メッセージが生成されることがあります。代わりに、システム ログ メッセージ 106100 を使用したロギングをイネーブルにすることを推奨します。これにより、各 ACE の統計情報を入手し、生成されるシステム ログ 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 ログ 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で、パケットが ACE と一致した場合、FWSM 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。FWSM は、最初のヒット時と各間隔の終了時に、その間隔での合計ヒット数を示すシステム ログ メッセージを生成します。各間隔の終わりに、FWSM 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、FWSM はそのフロー エントリを削除します。

（注） ACL では SYN パケットだけが拒否されるため、別のタイプのパケットが入ってきた場合、そのパケットはアクセス リストのヒット カウンタに示されません。SYN パケット以外のタイプの TCP パケット（RST、SYN-ACK、ACK、PSH、および FIN）は、アクセス リストで廃棄される前に FWSM で廃棄されます。SYN パケットの場合にかぎり、Adaptive Security Algorithm（ASA; アダプティブ セキュリティ アルゴリズム）でセッションを作成できるため、SYN パケットだけがアクセス リストで評価されます。

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。

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。

システム ログ 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 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.13-6）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は、**inactive** キーワードを最後のキーワードとして使用します。

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。デフォルト値は 6 です。
- **interval** *secs* : システム ログ メッセージの時間間隔（秒単位）を 1 ～ 600 の範囲内で指定します。デフォルト値は 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
```

outside-acl の最初の ACE でパケットが許可された場合、FWSM は次のようなシステム ログ 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。

```
%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 でパケットが拒否された場合、FWSM は次のようなシステム ログ 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 のロギングをイネーブルにした場合に、パケットが ACE と一致すると、FWSM は一定の間隔で受信した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 64 K です。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、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）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、FWSM 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、FWSM 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 ログ 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 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。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示すシステム ログ 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 には、1 ～ 3600 の範囲内の値を入力します。300 がデフォルトです。