CHAPTER 15

ネットワーク アクセスの許可または拒否

この章では、アクセス リストを使用して FWSM を通過するネットワーク アクセスを制御する方法について説明します。拡張アクセス リストまたは EtherType アクセス リストを作成する場合は、第 13 章「アクセス リストでのトラフィックの識別」を参照してください。

（注） ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの両方とも、アクセス リストを使用してネットワーク アクセスを制御します。トランスペアレント モードでは、拡張アクセス リスト（レイヤ 3 トラフィック用）と EtherType アクセス リスト（レイヤ 2 トラフィック用）の両方を使用できます。

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。

この章では、次の内容について説明します。

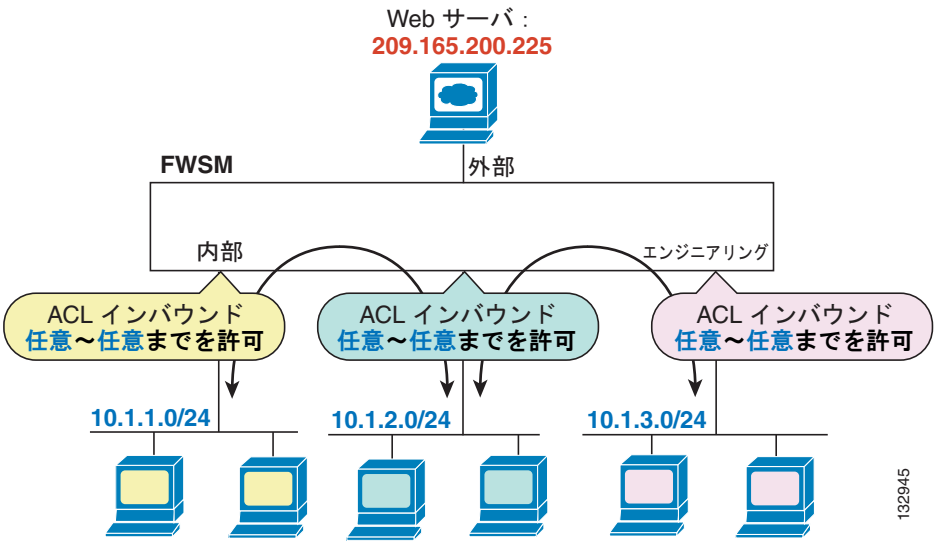
着信および発信アクセス リストの概要

FWSM のインターフェイス上を流れるトラフィックは、2 通りの方法で制御できます。FWSM に入ってくるトラフィックを制御する場合は、送信元インターフェイスに着信アクセス リストを結合します。FWSM から出ていくトラフィックを制御する場合は、宛先インターフェイスに発信アクセス リストを結合します。トラフィックが FWSM に入ってくるようにするには、インターフェイスに着信アクセス リストを結合する必要があります。これを実行しないと、FWSM はそのインターフェイスに届いたすべてのトラフィックを自動的に廃棄します。設定済みのインバウンド アクセス リストに制約を追加したアウトバウンド アクセス リストを使用して発信を制限しない限り、トラフィックは、デフォルトでは、すべてのインターフェイスで FWSM から発信することができます。

（注） 「着信」および「発信」という用語は、インターフェイス上の FWSM に入るトラフィックまたはインターフェイス上の FWSM を出るトラフィックのどちらにインターフェイス上のアクセス リストが適用されているかを意味します。これらの用語は、一般に着信と呼ばれる、セキュリティの低いインターフェイスから高いインターフェイスへのトラフィックの移動や、一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動を意味しません。

発信アクセス リストを使用して、アクセス リストの設定を簡素化する場合があります。たとえば、3 つの異なるインターフェイス上の 3 つの内部ネットワークが相互にアクセスできるようにする場合、各内部インターフェイス上ですべてのトラフィックを許可する単純な着信アクセス リストを作成します（図 15-1 を参照）。

図 15-1　着信アクセス リスト



この例について、次のコマンドを参照してください。

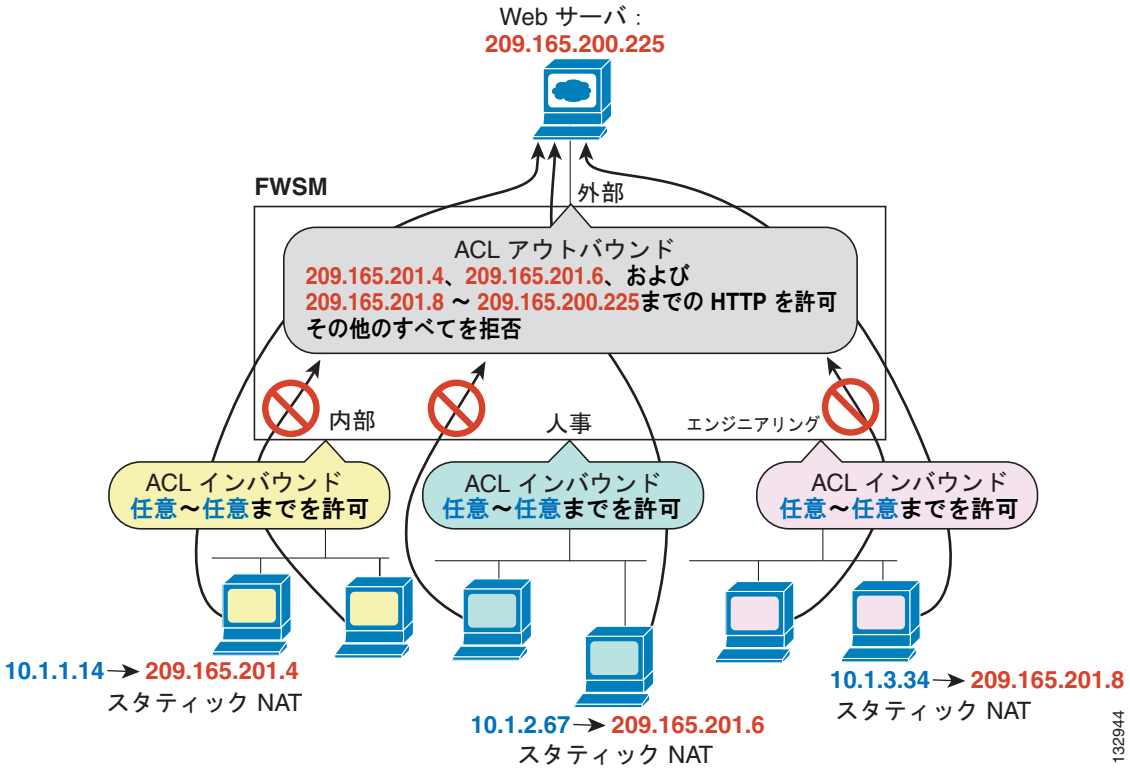
```
hostname(config)# access-list INSIDE extended permit ip any any
hostname(config)# access-group INSIDE in interface inside

hostname(config)# access-list HR extended permit ip any any
hostname(config)# access-group HR in interface hr

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

さらに、内部ネットワーク上の特定のホストだけが外部ネットワーク上の Web サーバにアクセスできるようにする場合、指定したホストだけを許可する、より制約の強化されたアクセス リストを作成し、外部インターフェイスの発信方向にそのアクセス リストを適用します（図 15-1 を参照）。NAT および IP アドレスについては、「NAT 使用時のアクセス リスト用の IP アドレス」（P.13-3）を参照してください。発信アクセス リストによって、その他のホストから外部ネットワークへの接続が禁止されます。

図 15-2　Outbound Access List



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 any any
hostname(config)# access-group INSIDE in interface inside

hostname(config)# access-list HR extended permit ip any any
hostname(config)# access-group HR in interface hr

hostname(config)# access-list ENG extended permit ip any any
hostname(config)# access-group ENG in interface eng

hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.4
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.6
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 209.165.201.8
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

アクセス リストのインターフェイスへの適用

次のコマンドを入力して、インターフェイスの着信方向と発信方向に拡張アクセス リストを適用します。

```
hostname(config)# access-group access_list_name {in | out} interface interface_name
[per-user-override]
```

インターフェイスの両方向に、各タイプ（拡張および EtherType）のアクセス リストを 1 つ適用できます。アクセス リストの方向の詳細については、「着信および発信アクセス リストの概要」（P.15-1）を参照してください。

per-user-override キーワードではダイナミックなアクセス リストを使用できます。ダイナミックなアクセス リストはユーザ許可用にダウンロードされ、インターフェイスに割り当てられたアクセス リストに優先されます。たとえば、インターフェイス アクセス リストが 10.0.0.0 からのトラフィックをすべて拒否し、ダイナミック アクセス リストが 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザに関しては、ダイナミック アクセス リストによってインターフェイス アクセス リストが上書きされます。ユーザ単位のアクセス リストの詳細については、「RADIUS 許可の設定」を参照してください。**per-user-override** キーワードは、着信アクセス リストにだけ使用できます。

コネクションレス型プロトコルで、双方向にトラフィックを流す場合は、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 リストを適用する必要があります。たとえば、トランスペアレント モードの EtherType アクセス リストで BGP を許可する場合、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。

IP アドレス 209.165.201.12（この IP アドレスは NAT の実行後に外部インターフェイス上で認識されます）の内部 Web サーバにアクセスできるようにするには、次のコマンドが必要です。

```
hostname(config)# access-list ACL_OUT extended permit tcp any host 209.165.201.12 eq www
hostname(config)# access-group ACL_OUT in interface outside
```

この Web サーバ用の NAT も設定する必要があります。

次のアクセス リストは、すべてのホストに対して、内部ネットワークと hr ネットワーク間の通信を許可しますが、外部ネットワークへのアクセスは一部のホストに限定して許可します。

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

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、それ以外はすべて拒否します。

```
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
```