CHAPTER 11

ネットワーク アクセスの許可または拒否

ここでは、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 10 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 モードと透過ファイアウォール 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。透過モードでは、拡張アクセス リスト（レイヤ 3 トラフィック）と EtherType アクセス リスト（レイヤ 2 トラフィック）の両方を使用できます。

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。

この章で説明する内容は、次のとおりです。

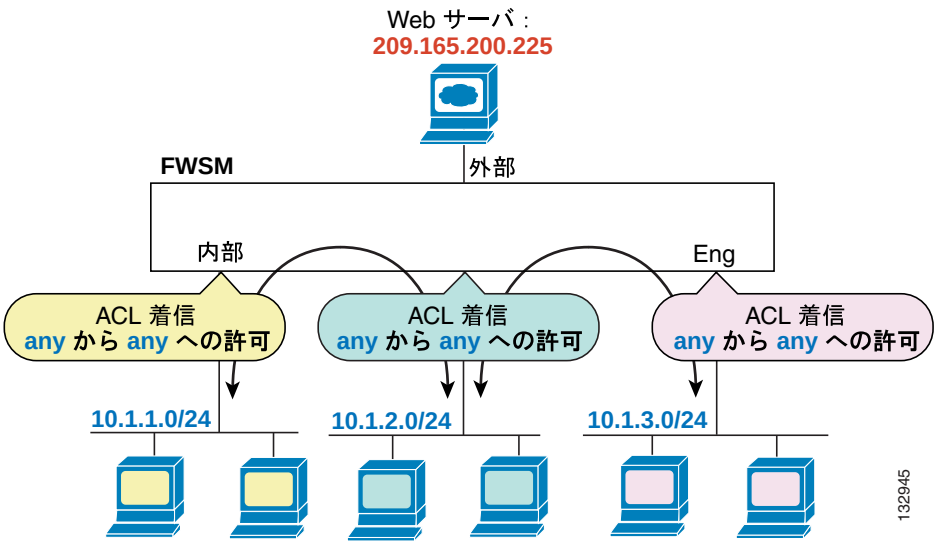
着信および発信アクセス リストの概要

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 リストを結合することによって制御できます。FWSM から出ていくトラフィックは、宛先インターフェイスに発信アクセス リストを結合することによって制御できます。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。そうしないと、FWSM はそのインターフェイスに届いたあらゆるトラフィックを自動的に廃棄します。デフォルトでは、発信アクセス リストを使用して制限しないかぎり、トラフィックは FWSM のすべてのインターフェイスから出ていくことが可能です。発信アクセス リストによって、着信アクセス リストですでに設定されているものに制限を加えます。

（注）　「着信」および「発信」とは、インターフェイス上でのアクセス　リストの適用方法を意味します。FWSM のインターフェイスに入ってくるトラフィックにアクセス リストを適用するのか、それとも FWSM のインターフェイスから出ていくトラフィックにアクセス リストを適用するのかという意味です。セキュリティ レベル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流れ（一般に、着信といいます）または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流れ（一般に、発信といいます）を表すわけではありません。

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 11-1 を参照）。

図 11-1　着信アクセス リスト



この例に対応するコマンドは、次のとおりです。

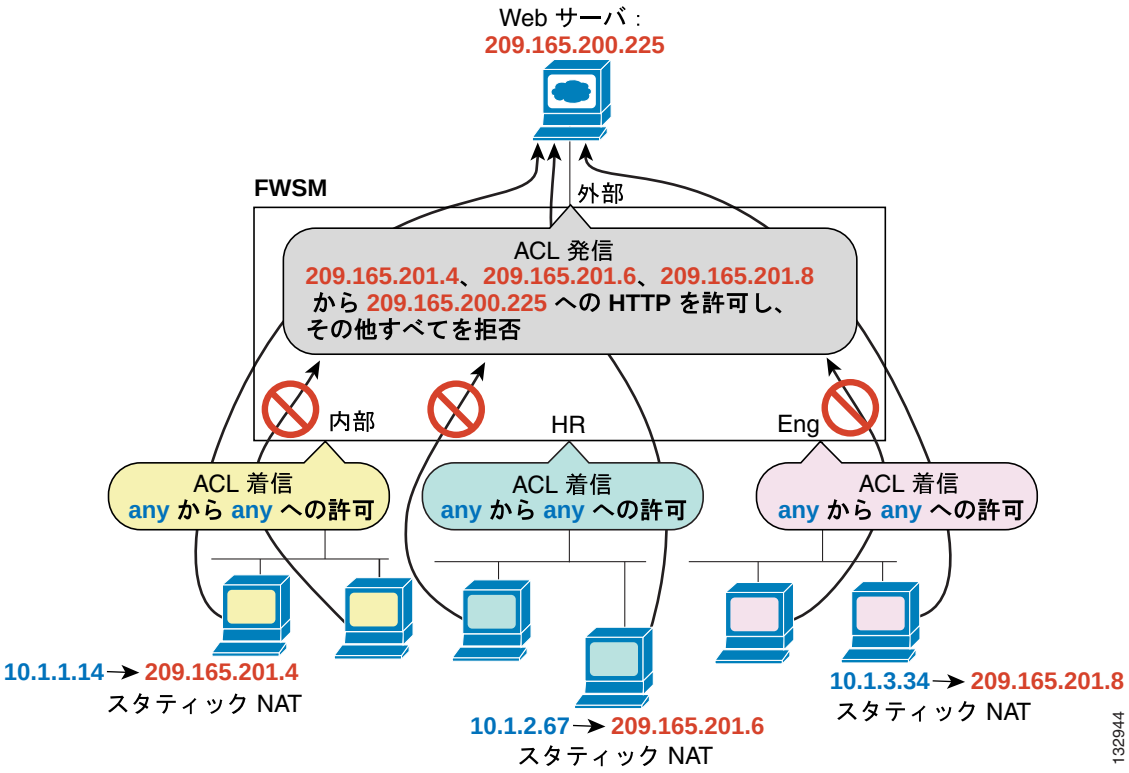
```
hostname(config)# access-list INSIDE extended permit ip any any
hostname(config)# access-group INSIDE in interface inside

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 11-1 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 IP アドレス」（p.10-3）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 11-2　発信アクセス リスト



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 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.11-2）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 アクセス リストを使用できます。ダイナミック 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 からのすべてのトラフィックを拒否し、ダイナミック アクセス リストが 10.0.0.0 からのすべてのトラフィックを許可する場合、そのユーザに対してはダイナミック アクセス リストがインターフェイス アクセス リストに優先されます。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」（p.15-8）を参照してください。**per-user-override** キーワードは、着信アクセス リストに対してのみ使用できます。

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、透過モードの 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
```

Web サーバの NAT を設定することも必要です。

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、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
```