CHAPTER 18

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 セキュリティ アプライアンス 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 16 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 モードの場合もトランスペアレント ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、ACL を使用します。トランスペアレント モードでは、拡張 ACL（レイヤ 3 トラフィックの場合）と EtherType ACL（レイヤ 2 トラフィックの場合）の両方を使用できます。

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。

この章は、次の項で構成されています。

着信アクセス リストおよび発信アクセス リストの概要

デフォルトでは、高セキュリティ インターフェイスから低セキュリティ インターフェイスへのトラフィックはすべて許可されます。アクセス リストを使用して、低セキュリティ インターフェイスからのトラフィックを許可したり、高セキュリティ インターフェイスからのトラフィックを制限したりできます。

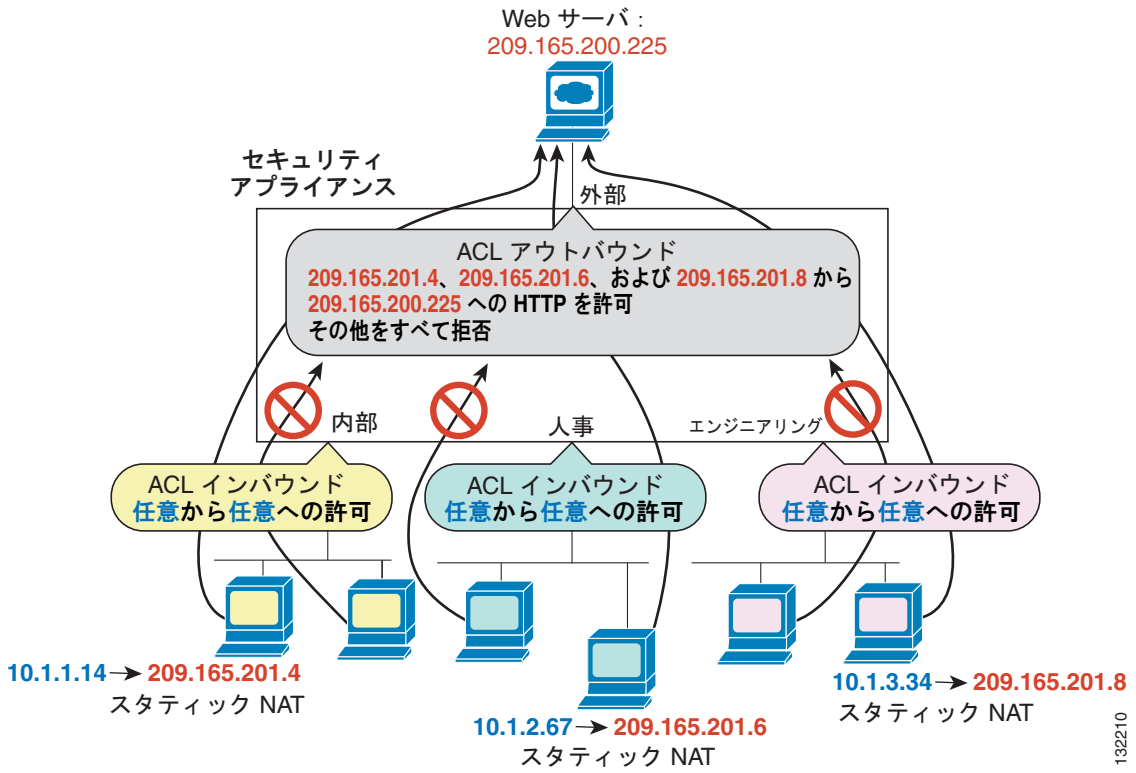
セキュリティ アプライアンスでは、次の 2 つのタイプのアクセス リストをサポートします。

- 着信：着信アクセス リストは、インターフェイスに入ってくるトラフィックに適用されます。
- 発信：発信アクセス リストは、インターフェイスから出ていくトラフィックに適用されます。

（注） 「着信」および「発信」という用語は、インターフェイス上のセキュリティ アプライアンスに入るトラフィックまたはインターフェイス上のセキュリティ アプライアンス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。

アクセス リストは、たとえば内部ネットワークの特定のホストにのみ外部ネットワークの Web サーバへのアクセスを許可する場合に便利です。複数の着信アクセス リストを作成してアクセスを制限せずに、発信アクセス リストを 1 つ作成して、指定したホストだけが許可されるようにすることができます（図 18-1 を参照）。NAT および IP アドレスについては、「NAT 使用時にアクセス リストで使用する IP アドレス」（P.16-3）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 18-1　　発信アクセス 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 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
```

インターフェイスへのアクセス リストの適用

拡張アクセス リストをインターフェイスの着信方向または発信方向に適用するには、次のコマンドを入力します。

```
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、「着信アクセス リストおよび発信アクセス リストの概要」（P.18-1）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。

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 リストによって、*任意*のホストが **inside** および **hr** ネットワークとの間で通信することができますが、最終行で表示しているように、指定のホスト（209.168.200.3 および 209.168.200.4）だけが外部ネットワークと通信できます。

```
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 セキュリティ アプライアンス 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
```