CHAPTER 16

アクセス ルールの設定

この章では、アクセス ルールを使用して、ASA 1000V 経由でのネットワーク アクセスを制御する方法について説明します。この章は次の項で構成されています。

- 「アクセス ルールに関する情報」（P.16-1）
- 「前提条件」（P.16-5）
- 「デフォルト設定」（P.16-5）
- 「アクセス ルールの設定」（P.16-5）
- 「アクセス ルールのモニタリング」（P.16-6）
- 「ネットワーク アクセスの許可または拒否の設定例」（P.16-6）

（注） また、ASA 1000V インターフェイスに管理アクセスの目的でアクセスするには、ホスト IP アドレスを許可するアクセス ルールは必要ありません。必要なのは、第 17 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。

アクセス ルールに関する情報

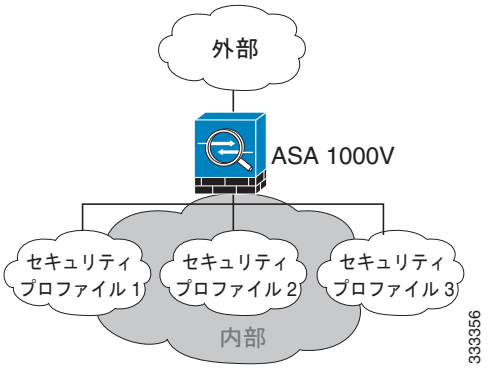
拡張アクセス リストをインターフェイスに適用するか、グローバルにすべてのインターフェイスに対して適用して、アクセス ルールを作成します。アクセス ルールは、プロトコル、送信元および宛先の IP アドレスまたはネットワーク、および任意で送信元ポートと宛先ポートに基づいてトラフィックを許可または拒否します。

この項は、次の内容で構成されています。

- 「暗黙的な許可」（P.16-2）
- 「インターフェイス アクセス ルールとグローバル アクセス ルールに関する情報」（P.16-2）
- 「暗黙の拒否」（P.16-3）
- 「着信ルールと発信ルール」（P.16-3）
- 「リターン トラフィックに対するアクセス ルール」（P.16-4）
- 「管理アクセス ルール」（P.16-5）

インターフェイスにアクセス ルールを適用する方法

外部インターフェイスに適用するアクセス ルールは、外部イーサネット インターフェイスを直接参照する必要があります。セキュリティ ポリシーの目的として、内部インターフェイスが別々のセキュリティ プロファイルに分かれます。内部インターフェイスに適用するアクセス ルールは、内部インターフェイスを直接参照するのではなく、特定のセキュリティ プロファイルを参照する必要があります。



セキュリティ プロファイルと外部の間のアクセスを制御できますが、セキュリティ プロファイル間のアクセスは制御できません。セキュリティ プロファイルで定義されているホストがすべて内部インターフェイス上にあるため、セキュリティ プロファイル間のトラフィックは ASA 1000V を通りません。このトラフィックは、必要に応じて、直接相互にまたは VSG を通じて到達できます。

暗黙的な許可

セキュリティ プロファイル インターフェイスから外部インターフェイスへの IPv4 トラフィックは、デフォルトで許可されます。

他のトラフィックのアクセスまたは制限には、拡張アクセス ルールを使用する必要があります。

インターフェイス アクセス ルールとグローバル アクセス ルールに関する情報

特定のインターフェイスにアクセス ルールを適用するか、またはすべてのインターフェイスにアクセス ルールをグローバルに適用できます。インターフェイス アクセス ルールと一緒にグローバル アクセス ルールを設定できます。この場合、特定のインターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも前に処理されます。

（注） グローバル アクセス ルールは、着信トラフィックだけに適用されます。「着信ルールと発信ルール」（P.16-3）を参照してください。

暗黙の拒否

アクセス リストの最後で暗黙の拒否が設定されるため、明示的に許可しない限り、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、ASA 1000V 経由での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。

グローバル アクセス ルールを設定すると、グローバル ルールが処理された*後*に、暗黙の拒否が置かれます。次の動作順序を確認してください。

1. インターフェイス アクセス ルール。
2. グローバル アクセス ルール。
3. 暗黙の拒否。

着信ルールと発信ルール

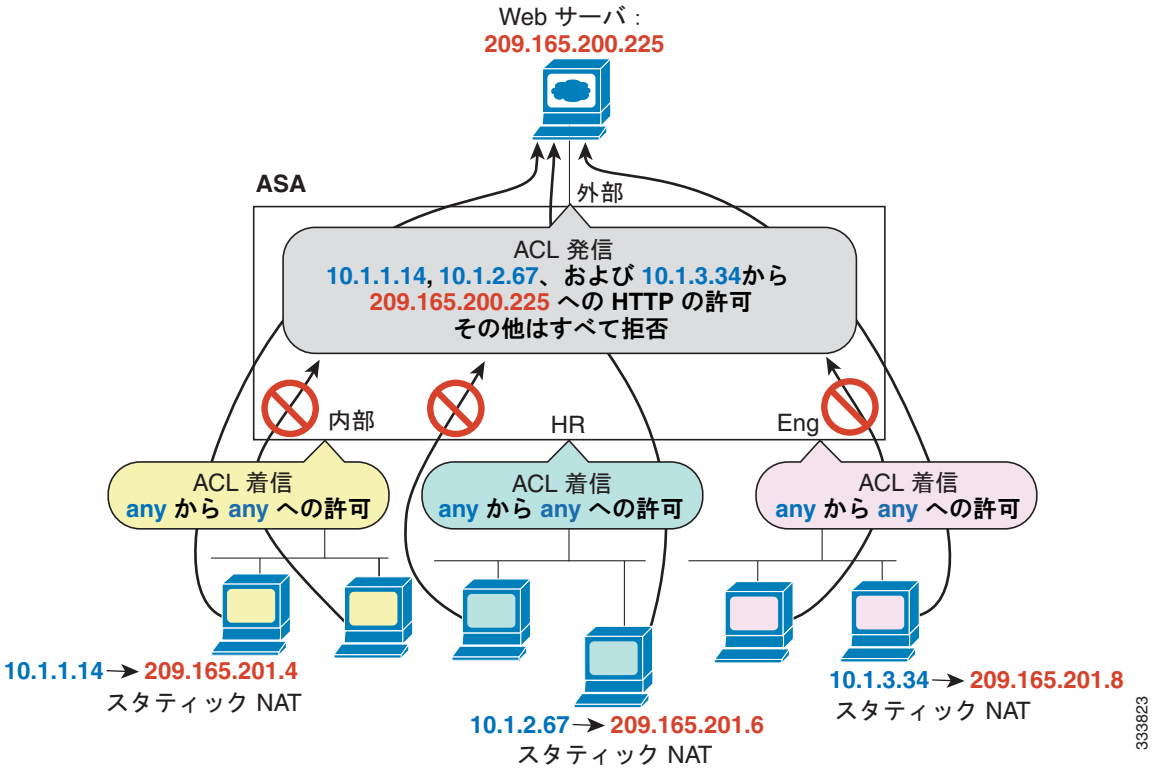
ASA 1000V では、次の 2 つのタイプのアクセス リストをサポートします。

- 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。グローバル アクセス ルールは常に受信です。
- 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 ASA 1000V に入るトラフィックまたはインターフェイス上の ASA 1000V 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するよりも、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 16-1 を参照）。発信アクセス リストは、他のホストが外部ネットワークに到達することを禁止します。

図 16-1　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 10.1.1.14
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

リターン トラフィックに対するアクセス ルール

TCP 接続および UDP 接続の場合、リターン トラフィックを許可するアクセス ルールは必要ありません。これは、ASA 1000V によって、確立された双方向接続のすべてのリターン トラフィックが許可されるためです。

ただし、ICMP などのコネクションレス型プロトコルについては、ASA 1000V は単方向セッションを確立します。したがって、（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で）アクセス ルールで双方向の ICMP を許可するか、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。ping を制御するには、**echo-reply** （**0**）（ASA 1000V からホストへ）または **echo**（**8**）（ホストから ASA 1000V へ）を指定します。

管理アクセス ルール

ASA 1000V宛ての管理トラフィックを制御するアクセス ルールを設定できます。To-the-box 管理トラフィック（**http**、**ssh**、**telnet** などのコマンドで定義されます）のアクセス コントロール ルールは、**control-plane** オプションで適用された管理アクセス ルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box アクセス リストで明示的に拒否されている場合でも着信が許可されます。

前提条件

アクセス ルールを作成するには、まず、アクセス リストを作成します。詳細については、第 9 章「拡張アクセス リストの追加」を参照してください。

デフォルト設定

「暗黙的な許可」（P.16-2）を参照してください。

アクセス ルールの設定

アクセス ルールを適用するには、次の手順を実行します。

手順の詳細

コマンド	目的
access-group *access_list* {{**in** | **out**} **interface** *interface_name* [**control-plane**] | **global**} **例：** `hostname(config)# access-group acl_out in interface outside`	アクセス リストをインターフェイスにバインドするか、グローバルに適用します。 拡張アクセス リストの名前を指定します。空のアクセス リストまたはコメントだけを含むアクセス リストは参照できません。 インターフェイス固有のルールの場合： • **in** キーワードは、着信トラフィックにアクセス リストを適用します。**out** キーワードは、発信トラフィックにアクセス リストを適用します。 • **interface** の名前を指定します。内部から外部へのトラフィックを制御するには、内部イーサネット インターフェイスではなく、セキュリティ プロファイル インターフェイスを指定します。 • ルールの対象が to-the-box トラフィックである場合、**control-plane** キーワードを指定します。 グローバル ルールの場合、すべてのインターフェイスの着信方向にアクセス リストを適用するには、**global** キーワードを指定します。

例

次の例は、**access-group** コマンドを使用する方法を示しています。

```
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

access-list コマンドでは、任意のホストからポート 80 を使用してグローバル アドレスにアクセスできるようにしています。**access-group** コマンドでは、外部インターフェイスに入るトラフィックに **access-list** コマンドを適用するように指定しています。

アクセス ルールのモニタリング

ネットワーク アクセスをモニタするには、次のコマンドを入力します。

コマンド	目的
show running-config access-group	インターフェイスにバインドされている現在のアクセス リストを表示します。

ネットワーク アクセスの許可または拒否の設定例

この項では、ネットワーク アクセスの許可または拒否の一般的な設定例を示します。

次の例は、IP アドレス 10.1.1.1 の内部 Web サーバへのアクセスをイネーブルにするために必要なコマンドを示しています。（この IP アドレスは実際のアドレスであり、NAT 処理の後は外部インターフェイスでは表示されなくなります）。

```
hostname(config)# access-list ACL_OUT extended permit tcp any host 10.1.1.1 eq www
hostname(config)# access-group ACL_OUT in interface outside
```

次の例では、セキュリティ プロファイル インターフェイスの「hr」および「eng」内のすべてのホストによる、Web トラフィック用の outside ネットワークへのアクセスを許可します。ASA 1000V は、eng と hr のインターフェイス間でルーティングできないため、これらの access-group コマンドは、セキュリティ プロファイル インターフェイスと外部インターフェイスの間だけで適用されます。

```
hostname(config)# access-list ANY extended permit tcp any any eq www
hostname(config)# access-group ANY in interface eng
hostname(config)# access-group ANY in interface hr
```

次の例では、サービス オブジェクト グループを使用して、セキュリティ プロファイル インターフェイス「Finance」で特定のサービスを許可します。

```
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destination eq http
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list FinanceAcl extended permit object-group myaclog any any
hostname(config)# access-group FinanceAcl in interface Finance
```