CHAPTER 9

拡張アクセス リストの追加

この章では、拡張アクセス リスト（アクセス コントロール リストとも呼ばれます）を設定する方法について説明します。次の項を取り上げます。

- 「アクセス リストに関する情報」（P.9-1）
- 「ガイドラインと制限事項」（P.9-3）
- 「デフォルト設定」（P.9-3）
- 「拡張アクセス リストの設定」（P.9-3）
- 「拡張アクセス リストのモニタリング」（P.9-6）
- 「拡張アクセス リストの設定例」（P.9-6）
- 「関連情報」（P.9-8）

アクセス リストに関する情報

Cisco ASA 1000V は、アクセス リストによる基本的なトラフィック フィルタリング機能を備えています。この機能を使用すると、特定のトラフィックの出入りを防止して、ネットワーク内のアクセスを制御できます。この章では、アクセス リストについて説明し、ネットワーク コンフィギュレーションにアクセス リストを追加する方法を示します。

アクセス リストは、1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。ACE は、パケットを転送またはドロップするための許可ルールまたは拒否ルールを指定するアクセス リスト内の 1 つのエントリで、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。また、オプションで、送信元ポートおよび宛先ポートに適用される場合もあります。

すべてのルーテッド プロトコルおよびネットワーク プロトコル（IP や AppleTalk など）に対してアクセス リストを設定し、それらのプロトコルのパケットがルータを通過するときに、パケットをフィルタリングすることができます。

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 14 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。

この章は、次の内容で構成されています。

- 「アクセス コントロール エントリの順序」（P.9-2）
- 「アクセス コントロールによる暗黙的な拒否」（P.9-2）
- 「NAT 使用時にアクセス リストで使用する IP アドレス」（P.9-2）

アクセス コントロール エントリの順序

アクセス リストは、1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。特定のアクセス リスト名に対して入力した各 ACE は、そのアクセス リストの末尾に追加されます。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。

ACE の順序は重要です。ASA 1000V によりパケットを転送するかドロップするかが決定されるとき、ASA 1000V では、エントリがリストされている順序で各 ACE とパケットが照合されます。一致が見つかると、ACE はそれ以上チェックされません。たとえば、すべてのトラフィックを明示的に許可する ACE をアクセス リストの先頭に作成した場合、それより後の文はまったくチェックされず、パケットが転送されます。

アクセス コントロールによる暗黙的な拒否

すべてのアクセス リスト（拡張アクセス リストを除く）の末尾には、暗黙的な拒否文があります。そのため、トラフィックの通過を明示的に許可しない限り、トラフィックは拒否されます。たとえば、1 つまたは複数の特定のアドレス以外のすべてのユーザが ASA 1000V 経由でネットワークにアクセスできるようにするには、特定のアドレスを拒否してから、その他のすべてのアドレスを許可する必要があります。

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的な拒否は、IP トラフィックや ARP には影響しません。たとえば、EtherType 8037 を許可する場合、アクセス リストの末尾にある暗黙的な拒否によって、拡張アクセス リストで以前許可（または高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイスへ暗黙的に許可）した IP トラフィックがブロックされることはありません。ただし、EtherType ACE とのすべてのトラフィックを*明示的*に拒否する場合、IP と ARP のトラフィックが拒否されます。

NAT 使用時にアクセス リストで使用する IP アドレス

次の機能では、インターフェイスに表示されるアドレスがマッピング アドレスである場合でも、NAT を使用するときにはアクセス リストに*実際の* IP アドレスを指定する必要があります。

- **access-group** コマンド
- モジュラ ポリシー フレームワークの **match access-list** コマンド
- ボットネット トラフィック フィルタの **dynamic-filter enable classify-list** コマンド
- AAA の **aaa ... match** コマンド

次の機能はアクセス リストを使用していますが、これらのアクセス リストはインターフェイス上に表示されるマップリストを使用します。

- IPsec アクセス リスト
- capture コマンド アクセス リスト
- ユーザごとのアクセス リスト
- ルーティング プロトコル
- その他のすべての機能

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

- アクセス リスト名は、大文字で入力します。これによって、コンフィギュレーションで名前が見つけやすくなります。アクセス リストには、インターフェイスを表す名前（INSIDE など）や、作成する目的を表す名前（NO_NAT や VPN など）を付けることができます。
- 通常、プロトコルには **ip** キーワードを指定しますが、他のプロトコルも受け入れられます。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.B-5）を参照してください。
- TCP プロトコルまたは UDP プロトコルの場合に限り、送信元ポートおよび宛先ポートを指定できます。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 ポートと UDP ポート」（P.B-6）を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。
- ネットワーク マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの **access-list** コマンドとは異なることに注意してください。ASA 1000V 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 マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。

デフォルト設定

表 9-1 に、拡張アクセス リスト パラメータのデフォルトの設定を示します。

表 9-1　デフォルトの拡張アクセス リスト パラメータ

パラメータ	デフォルト
ACE logging	ACE ロギングは、拒否されたパケットについてシステム ログ メッセージ 106023 を生成します。拒否されたパケットをログに記録するには、deny ACE が存在している必要があります。
log	**log** キーワードが指定されている場合、システム ログ メッセージ 106100 のデフォルトの重大度は 6（情報）で、デフォルトの間隔は 300 秒です。

拡張アクセス リストの設定

この項では、アクセス コントロール エントリとアクセス リストを追加および削除する方法について説明します。次の項目を取り上げます。

- 「拡張アクセス リストの追加」（P.9-4）
- 「アクセス リストへのコメントの追加」（P.9-6）

拡張アクセス リストの追加

アクセス リストは、同じアクセス リスト ID を持つ 1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。アクセス リストを作成するには、まず ACE を作成し、リスト名を適用します。アクセス リストには複数のエントリを追加できますが、1 つのエントリを含むアクセス リストもリストと見なされます。

前提条件

（任意）「オブジェクトとグループの設定」（P.8-1）に従ってオブジェクトまたはオブジェクト グループを作成します。

ガイドライン

ACE を削除するには、**no access-list** コマンドを、コンフィギュレーションに表示されるコマンド構文のすべての文字列とともに入力します。アクセス リスト全体を削除するには、**clear configure access-list** コマンドを使用します。

手順の詳細

コマンド	目的
（IP トラフィックの場合、ポートなし） **access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {*protocol* | **object-group** *prot_grp_id*} {*source_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} {*dest_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] （TCP または UDP トラフィックの場合、ポートあり） **access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp** | **object-group** *prot_grp_id*} {*source_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [*operator port* | **object-group** *svc_grp_id*] {*dest_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [*operator port* | **object-group** *svc_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] （ICMP トラフィックの場合） **access-list** *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **icmp** {*source_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} {*dest_address mask* | **object** *nw_obj_id* | **object-group** *nw_grp_id*} [*icmp_type* | **object-group** *icmp_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] **例：** `hostname(config)# access-list ACL_IN extended permit ip any any`	拡張 ACE を追加します。 **line** *line_number* オプションは、ACE を挿入する行番号を指定します。行番号を指定しなかった場合は、アクセス リストの末尾に ACE が追加されます。行番号はコンフィギュレーションに保存されません。ACE の挿入場所を指定するだけです。 **deny** キーワードは、条件が一致した場合にパケットを拒否します。**permit** キーワードは、条件が一致した場合にパケットを許可します。 コマンドにプロトコル、IP アドレス、またはポートを直接入力する代わりに、**object** および **object-group** キーワードを使用して、ネットワーク オブジェクト（プロトコル、ネットワーク、ポート）、または ICMP オブジェクト グループを使用できます。オブジェクトの作成については、「オブジェクトとグループの設定」（P.8-1）を参照してください。 *protocol* 引数には、IP プロトコルの名前または番号を指定します。たとえば、UDP は 17、TCP は 6、EGP は 47 です。 *source_address* には、パケットの送信元のネットワークまたはホストの IP アドレスを指定します。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。 TCP および UDP プロトコルの場合に限り、*operator port* オプションによって送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。 • **lt**：小なり。 • **gt**：大なり。 • **dq**：同値。 • **neq**：非同値。 • **range**：値の包括的な範囲。この演算子を使用する場合は、2 つのポート番号を指定します（例：**range 100 200**）。 *dest_address* には、パケットの送信先のネットワークまたはホストの IP アドレスを指定します。1 つのアドレスを指定する場合は、IP アドレスの前に **host** キーワードを入力します。この場合は、マスクを入力しません。すべてのアドレスを指定する場合は、アドレスとマスクの代わりに **any** キーワードを入力します。 *icmp_type* 引数には、ICMP タイプを指定します（プロトコルが ICMP の場合）。 アクセス リストをアクティブにするときは、**time-range** キーワードを指定します。詳細については、「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ル設定」（P.8-14）を参照してください。 **inactive** キーワードは、ACE をディセーブルにします。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。この機能では、再イネーブル化を簡単にするために、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に保持できます。 **log** キーワードについては、第 10 章「アクセス リストのロギングの設定」を参照してください。

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、IPv6 アクセス リスト、標準アクセス リスト、Webtype アクセス リストを含む任意のアクセス リストに、エントリについての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。

最後に入力した **access-list** コマンドの後にコメントを追加するには、次のコマンドを入力します。

コマンド	目的
access-list *access_list_name* **remark** *text* **例：** `hostname(config)# access-list OUT remark - this is the inside admin address`	最後に入力した access-list コマンドの後にコメントを追加します。 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。 いずれかの **access-list** コマンドの前にコメントを入力すると、コメントはアクセス リストの最初の行に表示されます。 **no 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。

例

各 ACE の前にコメントを追加できます。コメントはその場所でアクセス リストに表示されます。コメントの開始位置にダッシュ（-）を入力すると、ACE と区別しやすくなります。

```
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
```

拡張アクセス リストのモニタリング

拡張アクセス リストをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show access list	アクセス リスト エントリを番号で表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

拡張アクセス リストの設定例

この項は、次の内容で構成されています。

- 「拡張アクセス リストの設定例（オブジェクトなし）」（P.9-7）
- 「拡張アクセス リストの設定例（オブジェクト使用）」（P.9-7）

拡張アクセス リストの設定例（オブジェクトなし）

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 ASA 1000V 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
```

次のサンプル アクセス リストでは、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することが禁止されます。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
```

選択したホストだけにアクセスを制限する場合は、限定的な許可 ACE を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
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 リストでは、すべてのホスト（アクセス リスト適用先のインターフェイス上にあるすべてのホスト）がアドレス 209.165.201.29 の Web サイトにアクセスすることが禁止されます。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
```

オブジェクト グループを使用する次のアクセス 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。他のトラフィックはすべて許可されます。

```
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
```

次の例では、あるネットワーク オブジェクト グループ（A）から別のネットワーク オブジェクト グループ（B）へのトラフィックを許可するアクセス リストを一時的にディセーブルにします。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベースのアクセス リストを実装するには、**time-range** コマンドを使用して、1 日および週の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲をアクセス リストにバインドします。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
```

拡張アクセス リストの設定例（オブジェクト使用）

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。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
```

関連情報

アクセス リストをインターフェイスに適用します。詳細については、「アクセス ルールの設定」（P.16-5）を参照してください。