CHAPTER 22

標準アクセス コントロール リストの追加

この章では、標準アクセス リストを設定する方法について説明します。次の項目を取り上げます。

標準アクセス リストに関する情報

標準アクセス リストでは、OSPF ルートの宛先 IP アドレスを指定します。このアクセス リストは、OSPF 再配布のルート マップに使用できます。標準アクセス リストをインターフェイスに適用してトラフィックを制御することはできません。

標準アクセス リストのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

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。

- 「IPv6 のガイドライン」（P.22-2）
- 「その他のガイドラインと制限事項」（P.22-2）

コンテキスト モードのガイドライン

シングル コンテキスト モードでだけサポートされます。

ファイアウォール モードのガイドライン

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 モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドラインと制限事項

標準アクセス リストには、次のガイドラインと制限事項が適用されます。

- 標準 ACL では、OSPF ルートの宛先 IP アドレス（送信元アドレスではない）を指定します。このアクセス リストは、OSPF 再配布のルート マップに使用できます。標準 ACL をインターフェイスに適用してトラフィックを制御することはできません。
- アクセス リストの末尾に ACE を追加するには、同じアクセス リスト名を指定して別の **access-list** コマンドを入力します。
- **access-group** コマンドとともに **deny** キーワードを使用すると、パケットが ASA を通過できなくなります。デフォルトでは、ASA は、ユーザが特にアクセスを許可しない限り、送信元インターフェイスのパケットをすべて拒否します。
- 送信元、ローカル、または宛先アドレスを指定する場合は、次のガイドラインを使用します。
  - 4 つの部分からなるドット付き 10 進数形式の 32 ビットの数値を使用します。
  - キーワード **any** を 0.0.0.0.0.0.0.0 のアドレスおよびマスクの省略形として使用します。
  - **host** *ip_address* オプションを 255.255.255.255 のマスクの省略形として使用します。
- ACE をディセーブルにするには、**access-list** コマンドで **inactive** キーワードを指定します。

デフォルト設定

表 22-1 に、標準アクセス リスト パラメータのデフォルトの設定を示します。

表 22-1　標準アクセス リストのデフォルト パラメータ

パラメータ	デフォルト
deny	特にアクセスを許可しない限り、ASA によって発信元インターフェイス上のすべてのパケットが拒否されます。 アクセス リスト 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、拒否パケットが存在している必要があります。

標準アクセス リストの追加

この項は、次の内容で構成されています。

拡張アクセス リストの設定のタスク フロー

アクセス リストを作成して実装するには、次のガイドラインを使用します。

- ACE を追加し、アクセス リスト名を適用して、アクセス リストを作成します。「標準アクセス リストの追加」（P.22-3）を参照してください。
- 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.42-8）を参照してください。

標準アクセス リストの追加

OSPF ルートの宛先 IP アドレスを指定するアクセス リストを追加するには、次のコマンドを入力します。このアクセス リストは、OSPF 再配布のルート マップに使用できます。

コマンド	目的
`hostname(config)# access-list` *access_list_name* **standard** {**deny** | **permit**} {**any** | *ip_address mask*} **例：** `hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0`	標準アクセス リスト エントリを追加します。アクセス リストの末尾にもう 1 つ ACE を追加するには、同じアクセス リスト名を指定して別の **access-list** コマンドを入力します。 *access_list_name* 引数には、アクセス リストの名前または番号を指定します。 **any** キーワードは、任意のユーザへのアクセスを指定します。 **deny** キーワードは、条件が一致した場合にアクセスを拒否します。 **host** *ip_address* 構文は、ホスト IP アドレスへのアクセスを指定します。 *ip_address ip_mask* 引数は、特定の IP アドレスおよびサブネット マスクへのアクセスを指定します。 **line** *line-num* オプションでは、ACE を挿入する行番号を指定します。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。 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
```

次の作業

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.42-8）を参照してください。

アクセス リストのモニタリング

アクセス リストをモニタするには、次のいずれかのタスクを実行します。

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。

標準アクセス リストの設定例

次に、ASA 経由の IP トラフィックを拒否する方法の例を示します。

```
hostname(config)# access-list 77 standard deny
```

次に、条件に一致した場合に ASA 経由の IP トラフィックを許可する方法の例を示します。

```
hostname(config)# access-list 77 standard permit
```

次の例は、宛先アドレスを指定する方法を示しています。

```
hostname(config)# access-list 77 standard permit host 10.1.10.123
```

標準アクセス リストの機能履歴

表 22-2 に、この機能のリリース履歴を示します。

表 22-2　標準アクセス リストの機能履歴

機能名	リリース	機能情報
標準アクセス リスト	7.0(1)	標準アクセス リストでは、OSPF ルートの宛先 IP アドレスを指定します。このアクセス リストは、OSPF 再配布のルート マップに使用できます。 この機能および **access-list standard** コマンドが導入されました。