



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 ACL 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 ACL に関する情報」 (P.21-1)
- 「標準 ACL のライセンス要件」 (P.21-1)
- 「ガイドラインと制限事項」 (P.21-1)
- 「デフォルト設定」 (P.21-2)
- 「標準 ACL の追加」 (P.21-3)
- 「次の作業」 (P.21-4)
- 「ACL のモニタリング」 (P.21-4)
- 「標準 ACL の設定例」 (P.21-4)
- 「標準 ACL の機能の履歴」 (P.21-5)

標準 ACL に関する情報

標準 ACL では、OSPF ルートの宛先 IP アドレスを指定します。この ACL 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。

標準 ACL 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。

- 「コンテキスト モードのガイドライン」 (P.21-2)
- 「ファイアウォール モードのガイドライン」 (P.21-2)

- 「IPv6 のガイドライン」 (P.21-2)
- 「その他のガイドラインと制限事項」 (P.21-2)

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 ACL には、次の注意事項と制限が適用されます。

- 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。
- ACL の末尾に ACE を追加するには、同じ ACL 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 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 21-1 に、標準 ACL パラメータのデフォルト設定値を示します。

表 21-1 デフォルトの標準 ACL パラメータ

パラメータ	デフォルト
deny	<p>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。</p> <p>ACL 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。</p>

標準 ACL の追加

この項は、次の内容で構成されています。

- 「拡張 ACL 設定のタスク フロー」(P.21-3)
- 「標準 ACL の追加」(P.21-3)
- 「ACL へのコメントの追加」(P.21-4)

拡張 ACL 設定のタスク フロー

ACL 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、ACL 名を適用して、ACL を作成します。「標準 ACL の追加」(P.21-3) を参照してください。
- ACL をインターフェイスに適用します。詳細については、ファイアウォール コンフィギュレーション ガイドの“Configuring Access Rules” section on page 6-7 を参照してください。

標準 ACL の追加

OSPF ルートの宛先 IP アドレスを指定する ACL を追加するには、次のコマンドを入力します。この ACL 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
<pre>hostname(config)# access-list access_list_name standard {deny permit} {any ip_address mask}</pre> <p>例 :</p> <pre>hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0</pre>	<p>標準アクセス リスト エントリを追加します。ACL の末尾にもう 1 つ ACE を追加するには、同じ ACL 名を指定して別の access-list コマンドを入力します。</p> <p><i>access_list_name</i> 引数には、ACL の名前または番号を指定します。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p><i>ip_address ip_mask</i> 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。</p> <p>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。</p> <p>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。</p> <p>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。</p>

ACL へのコメントの追加

拡張 ACL、EtherType ACL、IPv6 ACL、標準 ACL、および Web-type ACL を含む ACL のエントリに関するコメントを追加できます。コメントを追加すると、ACL 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 <i>access_list_name</i> remark <i>text</i>	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。
例: hostname(config)# access-list OUT remark - this is the inside admin address	access-list コマンドの前にコメントを入力すると、そのコメントが ACL の最初の行となります。 no access-list <i>access_list_name</i> コマンドを使って ACL 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 ACL 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

ACL をインターフェイスに適用します。詳細については、ファイアウォール コンフィギュレーション ガイドの“[Configuring Access Rules](#)” section on page 6-7 を参照してください。

ACL のモニタリング

ACL 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	ACL 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 ACL 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 ACL の機能の履歴

表 21-2 に、この機能のリリース履歴を示します。

表 21-2 標準 ACL の機能の履歴

機能名	リリース	機能情報
標準 ACL	7.0(1)	標準 ACL 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。

