CHAPTER 18

アクセス コントロール リストに関する情報

シスコの ASA は、アクセス コントロール リスト（ACL）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送受信を制限することにより、ネットワーク内でのアクセスをコントロールできます。この章では、ACL 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 ACL を追加する方法を示します。

ACL 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 ACL 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 ACL 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。

ACL 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、ACL 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、ファイアウォール コンフィギュレーション ガイドの Chapter 1, “Configuring a Service Policy Using the Modular Policy Framework,” を参照してください。

この章は、次の項で構成されています。

- 「ACL タイプ」（P.18-2）
- 「アクセス コントロール エントリの順序」（P.18-3）
- 「アクセス コントロールによる暗黙的な拒否」（P.18-3）
- 「NAT 使用時に ACL で使用する IP アドレス」（P.18-3）
- 「関連情報」（P.18-4）

ACL タイプ

ASA では、次の 5 つのタイプのアクセス リストを使用します。

- 標準 ACL：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。詳細については、第 21 章「標準アクセス コントロール リストの追加」を参照してください。
- 拡張 ACL：1 つまたは複数のアクセス コントロール エントリ（ACE）を使用します。このリストには、行番号を指定して ACE、送信元アドレス、および宛先アドレスを挿入できます。また、ACE タイプによっては、プロトコル、ポート（TCP または UDP の場合）、または IPCMP タイプ（ICMP の場合）も挿入できます。詳細については、第 19 章「拡張アクセス コントロール リストの追加」を参照してください。
- EtherType ACL：EtherType を指定する 1 つまたは複数の ACE を使用します。詳細については、第 20 章「EtherType アクセス コントロール リストの追加」を参照してください。
- Web-type ACL：クライアントレス SSL VPN のフィルタリングをサポートするコンフィギュレーションで使用されます。詳細については、第 22 章「Webtype アクセス コントロール リストの追加」を参照してください。

表 18-1 に、ACL のタイプとそれらの一般的な使用目的の一部を示します。

表 18-1　ACL のタイプと一般的な使用目的

ACL の使用目的	ACL タイプ	説明
IP トラフィックのネットワーク アクセスの制御（ルーテッド モードおよびトランスペアレント モード）	拡張	ASA では、拡張 ACL により明示的に許可されている場合を除き、低位のセキュリティ インターフェイスから高位のセキュリティ インターフェイスへのトラフィックは認められません。 **（注）** また、ASA 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 ACL は必要ありません。必要なのは、第 40 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。
AAA ルールでのトラフィック識別	拡張	AAA ルールでは、ACL を使用してトラフィックを識別します。
所定のユーザに関する IP トラフィックのネットワーク アクセス制御	拡張、ユーザごとに AAA サーバからダウンロード	ユーザに適用するダイナミック ACL をダウンロードするように RADIUS サーバを設定できます。または、ASA 上に設定済みの ACL の名前を送信するようにサーバを設定できます。
NAT（ポリシー NAT および NAT 免除）のアドレス識別	拡張	ポリシー NAT を使用すると、拡張 ACL で送信元アドレスと宛先アドレスを指定することにより、アドレスを変換するローカル トラフィックを指定できます。
VPN アクセスの確立	拡張	VPN コマンドで拡張 ACL を使用できます。
モジュラ ポリシー フレームワークのトラフィック クラス マップ内でのトラフィック識別	拡張 EtherType	ACL を使用すると、クラス マップ内のトラフィックを識別できます。このマップは、モジュラ ポリシー フレームワークをサポートする機能に使用されます。モジュラ ポリシー フレームワークをサポートする機能には、TCP および一般的な接続設定やインスペクションなどがあります。

表 18-1　ACL のタイプと一般的な使用目的 （続き）

ACL の使用目的	ACL タイプ	説明
トランスペアレント ファイアウォール モードの場合、IP 以外のトラフィックのネットワーク アクセスの制御	EtherType	EtherType に基づいてトラフィックを制御する ACL を設定できます。
OSPF ルート再配布の指定	標準	標準 ACL には、宛先アドレスだけが含まれています。標準 ACL を使用して、OSPF ルートの再配布を制御できます。
WebVPN のフィルタリング	Webtype	URL をフィルタリングするように Web-type ACL を設定できます。
IPV6 ネットワークのネットワーク アクセスの制御	IPv6	ACL を追加および適用して、IPv6 ネットワーク内のトラフィックを制御できます。

アクセス コントロール エントリの順序

1 つの ACL 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 ACL 名に対して入力した各 ACE は、その ACL の末尾に追加されます。ACL 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 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 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 ACL 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 ACL の末尾には、暗黙的な拒否文があります。そのため、明示的にトラフィックの通過を許可しない場合、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 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 ACL の場合、ACL 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、ACL の末尾にある暗黙的な拒否によって、拡張 ACL 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 ACL 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 ACL 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
- WCCP の **wccp redirect-list group-list** コマンド

次の機能は、ACL を使用しますが、これらの ACL は、インターフェイス上で認識される *マッピングされた*値を使用します。

- IPsec ACL
- capture コマンドの ACL
- ユーザ単位 ACL
- ルーティング プロトコル
- その他のすべての機能

関連情報

ACL の実装の詳細については、次の章を参照してください。

- *第 19 章「拡張アクセス コントロール リストの追加」*
- 第 20 章「EtherType アクセス コントロール リストの追加」
- 第 21 章「標準アクセス コントロール リストの追加」
- 第 22 章「Webtype アクセス コントロール リストの追加」
- ファイアウォール コンフィギュレーション ガイドの Chapter 6, “Configuring Access Rules,”