CHAPTER 19

アクセス リストに関する情報

Cisco ASA 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 Access Control Entry（ACE; アクセス コントロール エントリ）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 36 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、次の項で構成されています。

アクセス リストのタイプ

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。

- 標準アクセス リスト：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。詳細については、第 22 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。
- 拡張アクセス リスト：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 20 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 アクセス リスト：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 21 章「EtherType アクセス リストの追加」を参照してください。
- Webtype アクセス リスト：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 23 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 19-1 に、アクセス リストのタイプと、それらの一般的な使用目的の一部を示します。

表 19-1　アクセス リストのタイプと一般的な使用目的

アクセス リストの使用目的	アクセス リストのタイプ	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、拡張アクセス リスト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、管理アクセス用の ASA インターフェイスにアクセスする場合は、ホスト IP アドレスを許可するアクセス リストは不要です。必要なのは、第 43 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、アクセス リスト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 アクセス リスト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 上に設定済みのアクセス リスト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、拡張アクセス リスト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 コマンドで拡張アクセス リストを使用できます。

表 19-1　アクセス リストのタイプと一般的な使用目的 （続き）

アクセス リストの使用目的	アクセス リストのタイプ	説明
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	アクセス リストを使用すると、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。
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	トラフィックを EtherType に基づいて制御するためのアクセス リストを設定できます。
OSPF ルート再配布の指定	標準	標準アクセス リストには、宛先アドレスだけが含まれています。標準アクセス リストを使用して、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 Webtype アクセス リストを設定できます。
IPV6 ネットワークのネットワーク アクセスの制御	IPv6	アクセス リスト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

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 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 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
- WCCP の **wccp redirect-list group-list** 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

関連情報

アクセス リストの実装の詳細については、このマニュアルの次の章を参照してください。

- 第 20 章「拡張アクセス コントロール リストの追加」
- 第 21 章「EtherType アクセス リストの追加」
- 第 22 章「標準アクセス コントロール リストの追加」
- 第 23 章「Webtype アクセス コントロール リストの追加」
- 第 42 章「アクセス ルールの設定」