CHAPTER 42

アクセス ルールの設定

この章では、アクセス ルールを使用して、ASA 経由でのネットワーク アクセスを制御する方法について説明します。この章は次の項で構成されています。

（注） ルーテッド ファイアウォール モードの場合もトランスペアレント ファイアウォール モードの場合も、ネットワーク アクセスを制御するには、アクセス ルールを使用します。トランスペアレント モードでは、アクセス ルール（レイヤ 3 トラフィックの場合）と EtherType ルール（レイヤ 2 トラフィックの場合）の両方を使用できます。

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アクセス ルールは必要ありません。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。

アクセス ルールに関する情報

拡張または EtherType アクセス リストを特定のインターフェイスに、またはすべてのインターフェイスに対してグローバルに適用することによって、アクセス ルールを作成します。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 モードでアクセス ルールを使用して、IP トラフィックを制御できます。アクセス ルールでは、プロトコル、送信元および宛先の IP アドレスまたはネットワーク、および任意で送信元ポートと宛先ポートに基づいてトラフィックが許可または拒否されます。

トランスペアレント モードの場合に限り、EtherType ルールによって非 IP トラフィックのネットワーク アクセスが制御されます。EtherType ルールでは、EtherType に基づいてトラフィックが許可または拒否されます。

この項は、次の内容で構成されています。

ルールに関する一般情報

この項では、アクセス ルールと EtherType ルールの両方について説明します。次の項目を取り上げます。

暗黙的な許可

ルーテッド モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 トラフィック。
- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv6 トラフィック。

トランスペアレント モードの場合、デフォルトでは次のタイプのトラフィックが許可されます。

- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv4 トラフィック。
- 高セキュリティ インターフェイスから低セキュリティ インターフェイスへの IPv6 トラフィック。
- 双方向の Address Resolution Protocol（ARP; アドレス解決プロトコル）。

（注）　ARP トラフィックは ARP インスペクションによって制御できますが、アクセス ルールによって制御することはできません。

- 双方向の Bridge Protocol Data Unit（BPDU; ブリッジ プロトコル データ ユニット）。

他のトラフィックには、拡張アクセス ルール（IPv4 および IPv6）、または EtherType ルール（非 IPv4/IPv6）のいずれかを使用する必要があります。

インターフェイス アクセス ルールとグローバル アクセス ルールに関する情報

アクセス ルールを特定のインターフェイスに適用するか、またはアクセス ルールをすべてのインターフェイスにグローバルに適用できます。インターフェイス アクセス ルールと一緒にグローバル アクセス ルールを設定できます。この場合、特定のインターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも前に処理されます。

（注）　グローバル アクセス ルールは、着信トラフィックにだけ適用されます。「着信ルールと発信ルール」（P.42-3）を参照してください。

同じインターフェイスでのアクセス ルールと EtherType ルールの使用

1 つのアクセス ルールと 1 つの EtherType ルールを各方向のインターフェイスに適用できます。

暗黙の拒否

アクセス リストの最後で暗黙的な拒否が設定されるため、明示的に許可しない限り、トラフィックは通過できません。たとえば、特定のアドレスを除くすべてのユーザに、ASA 経由でのネットワークにアクセスすることを許可する場合、特定のアドレスを拒否したうえで、他のすべてのユーザを許可します。

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。

グローバル アクセス ルールを設定すると、暗黙的な拒否はグローバル ルールが処理された *後*になります。次の動作の順序を参照してください。

1. インターフェイス アクセス ルール。
2. グローバル アクセス ルール。
3. 暗黙的な拒否。

着信ルールと発信ルール

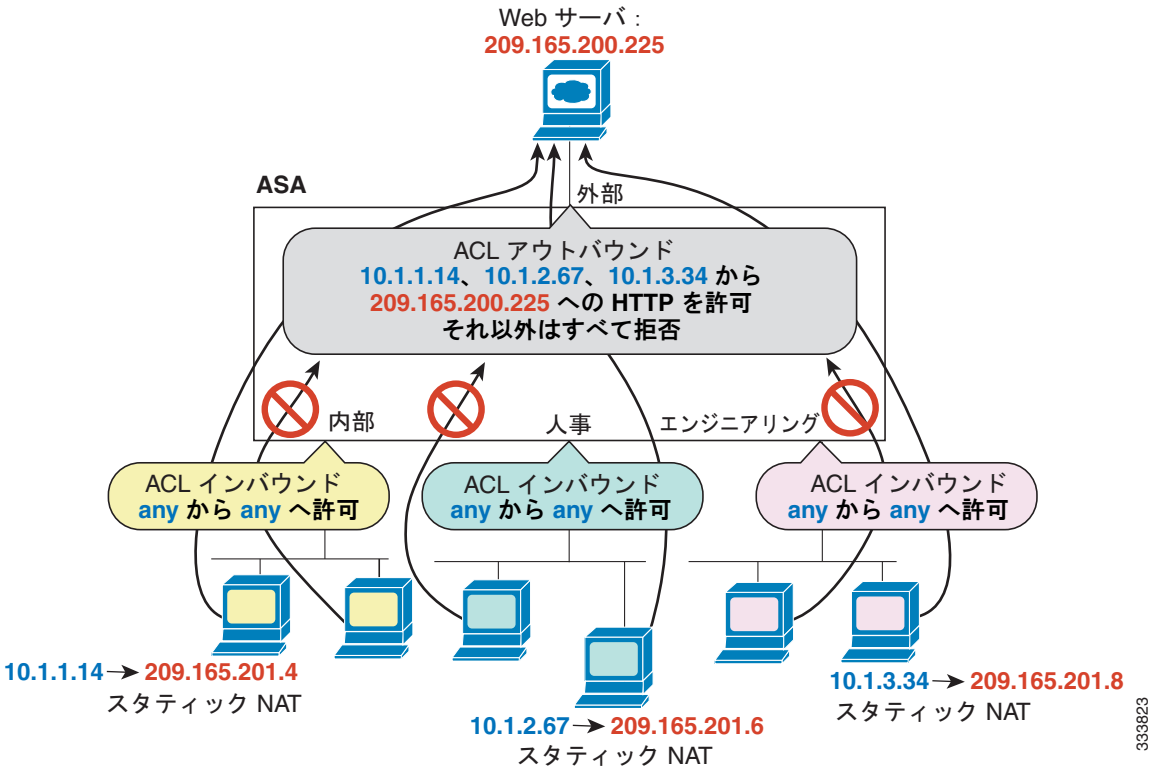
ASA では、次の 2 つのタイプのアクセス リストをサポートします。

- 着信：着信アクセス ルールは、インターフェイスに入ってくるトラフィックに適用されます。グローバル アクセス ルールは常に着信です。
- 発信：発信アクセス リストは、インターフェイスから出ていくトラフィックに適用されます。

（注） 「着信」および「発信」という用語は、インターフェイス上の ASA に入るトラフィックまたはインターフェイス上の ASA を出るトラフィックのどちらにインターフェイス上のアクセス リストが適用されているかを意味します。これらの用語は、一般に着信と呼ばれる、セキュリティの低いインターフェイスから高いインターフェイスへのトラフィックの移動や、一般に発信と呼ばれる、セキュリティの高いインターフェイスから低いインターフェイスへのトラフィックの移動を意味しません。

アクセス リストは、たとえば内部ネットワークの特定のホストにのみ外部ネットワークの Web サーバへのアクセスを許可する場合に便利です。複数の着信アクセス リストを作成してアクセスを制限するよりも、発信アクセス リストを 1 つ作成して、指定したホストだけが許可されるようにすることができます （図 42-1 を参照）。発信アクセス リストは、他のホストが外部ネットワークに到達することを禁止します。

図 42-1　発信アクセス リスト



この例について、次のコマンドを参照してください。

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67
host 209.165.200.225 eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34
host 209.165.200.225 eq www
hostname(config)# access-group OUTSIDE out interface outside
```

拡張アクセス ルールに関する情報

この項では、拡張アクセス ルールについて説明します。次の項目を取り上げます。

- 「リターン トラフィックに対するアクセス ルール」（P.42-4）
- 「アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可」（P.42-5）
- 「管理アクセス ルール」（P.42-5）

リターン トラフィックに対するアクセス ルール

ルーテッド モードとトランスペアレント モードの両方に対する TCP 接続および UDP 接続については、リターン トラフィックを許可するためのアクセス ルールは必要ありません。ASA は、確立された双方向接続のリターン トラフィックをすべて許可します。

ただし、ICMP などのコネクションレス型プロトコルについては、ASA は単方向セッションを確立します。したがって、（アクセス リストを送信元インターフェイスと宛先インターフェイスに適用することで）アクセス ルールで双方向の ICMP を許可するか、ICMP インスペクション エンジンをイネーブルにする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。ping を制御するには、**echo-reply**（**0**）（ASA からホストへ）または **echo**（**8**）（ホストから ASA へ）を指定します。

アクセス ルールを使用したトランスペアレント ファイアウォールを介したブロードキャストとマルチキャスト トラフィックの許可

ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセス ルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。トランスペアレント ファイアウォール モードでは、すべての IP トラフィックの通過を許可できます。この機能は、たとえば、ダイナミック ルーティングが許可されていないマルチ コンテキスト モードで特に有用です。

（注） これらの特殊なタイプのトラフィックはコネクションレス型であるため、アクセス ルールを両方のインターフェイスに適用して、リターン トラフィックの通過を許可する必要があります。

表 42-1 に、トランスペアレント ファイアウォールの通過を許可できる一般的なトラフィック タイプを示します。

表 42-1　トランスペアレント ファイアウォールの特殊トラフィック

トラフィックのタイプ	プロトコルまたはポート	注釈
DHCP	UDP ポート 67 および 68	DHCP サーバがイネーブルの場合、ASA は DHCP パケットの通過を拒否します。
EIGRP	プロトコル 88	—
OSPF	プロトコル 89	—
マルチキャスト ストリーム	UDP ポートは、アプリケーションによって異なります。	マルチキャスト ストリームは、常に Class D アドレス（224.0.0.0 to 239.x.x.x）に送信されます。
RIP（v1 または v2）	UDP ポート 520	—

管理アクセス ルール

ASA 宛ての管理トラフィックを制御するアクセス ルールを設定できます。To-the-box 管理トラフィック（**http**、**ssh**、**telnet** などのコマンドで定義されます）のアクセス コントロール ルールは、**control-plane** オプションで適用された管理アクセス ルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box アクセス リストで明示的に拒否されている場合でも着信が許可されます。

EtherType ルールに関する情報

この項では、EtherType ルールについて説明します。次の項目を取り上げます。

サポートされている EtherType およびその他のトラフィック

EtherType ルールは次を制御します。

- 一般的なタイプの IPX および MPLS ユニキャストまたはマルチキャストを含む、16 ビットの 16 進数値で示された EtherType。
- イーサネット V2 フレーム。
- デフォルトで許可される BPDU。BPDU は、SNAP でカプセル化されており、ASA は特別に BPDU を処理するように設計されています。
- トランク ポート（シスコ専用）BPDU。トランク BPDU のペイロードには VLAN 情報が含まれるので、BPDU を許可すると、ASA により、発信 VLAN を使用してペイロードが修正されます。

次のタイプのトラフィックはサポートされていません。

- 802.3 形式フレーム：type フィールドではなく length フィールドが使用されるため、ルールでは処理されません。

リターン トラフィックに対するアクセス ルール

EtherType はコネクションレス型であるため、トラフィックを両方向に通過させる必要がある場合は、両方のインターフェイスにルールを適用する必要があります。

MPLS の許可

MPLS を許可する場合は、Label Distribution Protocol（LDP; ラベル配布プロトコル）および Tag Distribution Protocol（TDP; タグ配布プロトコル）の TCP 接続が ASA を経由して確立されるようにしてください。これには、ASA インターフェイス上の IP アドレスを LDP セッションまたは TDP セッションの router-id として使用するように、ASA に接続されている両方の MPLS ルータを設定します（LDP および TDP を使用することにより、MPLS ルータは、転送するパケットに使用するラベル（アドレス）をネゴシエートできるようになります）。

Cisco IOS ルータで、使用プロトコル（LDP または TDP）に適したコマンドを入力します。*interface* は、ASA に接続されているインターフェイスです。

```
hostname(config)# mpls ldp router-id interface force
```

または

```
hostname(config)# tag-switching tdp router-id interface force
```

アクセス ルールのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

前提条件

アクセス ルールを作成するには、まず、アクセス リストを作成します。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」と第 21 章「EtherType アクセス リストの追加」を参照してください。

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

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

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。送信元アドレスと宛先アドレスには、IPv4 および IPv6 アドレスの組み合わせを含めることができます。

ユーザごとのアクセス リストのガイドライン

- ユーザごとのアクセス リストがパケットに関連付けられていない場合、インターフェイス アクセス ルールが適用されます。
- ユーザごとのアクセス リストでは、**timeout uauth** コマンドの値が使用されますが、この値は AAA のユーザごとのセッション タイムアウト値で上書きできます。
- ユーザごとのアクセス リストのためにトラフィックが拒否された場合、syslog メッセージ 109025 がログに記録されます。トラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとのアクセス リストの **log** オプションの効果はありません。

デフォルト設定

「暗黙的な許可」（P.42-2）を参照してください。

アクセス ルールの設定

アクセス ルールを適用するには、次の手順を実行します。

手順の詳細

コマンド	目的
access-group *access_list* {{**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**] | **global**} **例：** `hostname(config)# access-group acl_out in interface outside`	アクセス リストをインターフェイスにバインドするか、グローバルに適用します。 拡張または EtherType アクセス リスト名を指定します。インターフェイスごとのアクセス リスト タイプごとに 1 つの **access-group** コマンドを設定できます。空のアクセス リストまたはコメントだけを含むアクセス リストを参照できません。 インターフェイス固有のルールの場合： • **in** キーワードは、着信トラフィックにアクセス リストを適用します。**out** キーワードは、発信トラフィックにアクセス リストを適用します。 • **interface** 名を指定します。 • **per-user-override** キーワードを使用すると（着信アクセス リストの場合に限る）、ユーザ許可用にダウンロードしたダイナミック ユーザ アクセス リストにより、インターフェイスに割り当てられているアクセス リストを上書きできます。たとえば、インターフェイス アクセス リストが 10.0.0.0 からのトラフィックをすべて拒否し、ダイナミック アクセス リストが 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザに関しては、ダイナミック アクセス リストによってインターフェイス アクセス リストが上書きされます。ユーザごとのアクセス リストの詳細については、「RADIUS 許可の設定」（P.44-17）を参照してください。「ユーザごとのアクセス リストのガイドライン」（P.42-7）も参照してください。 • ルールの対象が to-the-box トラフィックである場合、**control-plane** キーワードを指定します。 グローバル ルールでは、すべてのインターフェイスのインバウンド方向にアクセス リストを適用するには、**global** キーワードを指定してください。

例

次の例は、**access-group** コマンドを使用する方法を示しています。

```
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

access-list コマンドでは、任意のホストからポート 80 を使用してグローバル アドレスにアクセスできるようにしています。**access-group** コマンドでは、外部インターフェイスに入るトラフィックに **access-list** コマンドを適用するように指定しています。

アクセス ルールのモニタリング

ネットワーク アクセスをモニタするには、次のコマンドを入力します。

コマンド	目的
show running-config access-group	インターフェイスにバインドされている現在のアクセス リストを表示します。

ネットワーク アクセスの許可または拒否の設定例

この項では、ネットワーク アクセスの許可または拒否の一般的な設定例を示します。

次の例は、IP アドレス 209.165.201.12 の内部 Web サーバへのアクセスをイネーブルにするために必要なコマンドを示しています。（この IP アドレスは実際のアドレスであり、NAT 処理の後は外部インターフェイスでは表示されなくなります）。

```
hostname(config)# access-list ACL_OUT extended permit tcp any host 209.165.201.12 eq www
hostname(config)# access-group ACL_OUT in interface outside
```

次の例では、すべてのホストに **inside** ネットワークと **hr** ネットワークの間での通信を許可しますが、外部ネットワークへのアクセスは特定のホストだけに許可されます。

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

たとえば、次のサンプル アクセス リストでは、内部インターフェイスで発信される一般的な EtherType が許可されます。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

次の例では、ASA を通過する一部の EtherType が許可されますが、それ以外はすべて拒否されます。

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次の例では、両方のインターフェイスで EtherType 0x1256 のトラフィックが拒否されますが、他のトラフィックはすべて許可されます。

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

次の例では、オブジェクト グループを使用して内部インターフェイスの特定のトラフィックを許可します。

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
```

```
hostname (config-service)# service-object tcp source range 3000 3010 destinatio$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

アクセス ルールの機能履歴

表 42-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 42-2　アクセス ルールの機能履歴

機能名	プラットフォーム リリース	機能情報
インターフェイス アクセス ルール	7.0(1)	ASA を経由するネットワーク アクセスを、アクセス リストを使用して制御します。 **access-group** コマンドが導入されました。
グローバル アクセス ルール	8.3(1)	グローバル アクセス ルールが導入されました。 **access-group** コマンドが変更されました。
アイデンティティ ファイアウォールのサポート	8.4(2)	アイデンティティ ファイアウォールのユーザおよびグループを発信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL はアクセス ルールや AAA ルールとともに、および VPN 認証に使用できます。 **access-list extended** コマンドが変更されました。
TrustSec のサポート	9.0(1)	TrustSec セキュリティ グループを送信元と宛先に使用できるようになりました。アイデンティティ ファイアウォール ACL をアクセス ルールとともに使用できます。 **access-list extended** コマンドが変更されました。

表 42-2　アクセス ルールの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
IPv4 および IPv6 の統合 ACL	9.0(1)	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。**any** キーワードは、IPv4 および IPv6 トラフィックを表すように変更されました。IPv4 のみのトラフィックを表す **any4** キーワードと、IPv6 のみのトラフィックを表す **any6** キーワードが追加されました。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 **access-list extended**、**access-list webtype** の各コマンドが変更されました。 **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。
ICMP コードによって ICMP トラフィックをフィルタリングするための拡張 ACL とオブジェクト機能拡張	9.0(1)	ICMP コードに基づいて ICMP トラフィックの許可または拒否ができるようになりました。 **access-list extended**、**service-object**、**service** の各コマンドが導入または変更されました。