アクセス ルール

この章では、アクセス ルールを使用して ASA へのネットワーク アクセスや ASA を通過するネットワーク アクセスを制御する方法について説明します。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。

（注） 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、一般的な操作の設定ガイドに従って管理アクセスを設定することだけです。

ネットワーク アクセスの制御

アクセス ルールは、ASA の通過を許可するトラフィックを定義したものです。複数の異なるレイヤのルールを組み合わせてアクセス コントロール ポリシーを実装できます。

- インターフェイスに割り当てられる拡張アクセスルール（レイヤ3以上のトラフィック）：着信方向と発信方向のそれぞれで異なるルールセット（ACL）を適用できます。拡張アクセスルールでは、送信元と宛先のトラフィックの基準に基づいてトラフィックが許可または拒否されます。
- ブリッジ仮想インターフェイス（BVI、ルーテッドモード）に割り当てられている拡張アクセスルール（レイヤ3以上のトラフィック）：BVIを指定すると、着信方向と発信方向

のそれぞれで異なるルールセットを適用でき、ブリッジグループメンバーのインターフェイスにもルールセットを適用できます。BVIとメンバーのインターフェイスの両方にアクセスルールがあると、処理の順序は方向によって異なります。着信方向、メンバーのアクセス ルールが最初に、次に BVI のアクセス ルールが評価されます。発信方向、BVI ルールが最初に、メンバーのインターフェイスのルールが次に考慮されます。

- グローバルに割り当てられる拡張アクセス ルール：デフォルトのアクセス コントロールとして使用する単一のグローバル ルール セットを作成できます。グローバル ルールはインターフェイス ルールの後に適用されます。
- 管理アクセス ルール（レイヤ 3 以上のトラフィック）：インターフェイスに対するトラフィック（通常は管理トラフィック）を制御する単一のルールセットを適用できます。これらのルールは、CLI の「コントロール プレーン」アクセス グループに相当します。デバイスに対する ICMP トラフィックについては、代わりに ICMP ルールを設定できます。
- インターフェイスに割り当てられる EtherType ルール（レイヤ 2 のトラフィック）（ブリッジ グループ メンバーのインターフェイスのみ）：着信方向と発信方向のそれぞれで異なるルール セットを適用できます。EtherType ルールは、IP 以外のトラフィックのネットワーク アクセスを制御するルールです。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。また、ブリッジ グループ メンバーのインターフェイスに拡張アクセス ルールを適用して、レイヤ 3 以上のトラフィックを制御できます。

ルールに関する一般情報

次のトピックでは、アクセス ルールおよび EtherType ルールに関する一般的な情報を提供します。

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

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、特定の着信インターフェイス アクセス ルールが常に汎用のグローバル アクセス ルールよりも先に処理されます。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。

インバウンド ルールとアウトバウンド ルール

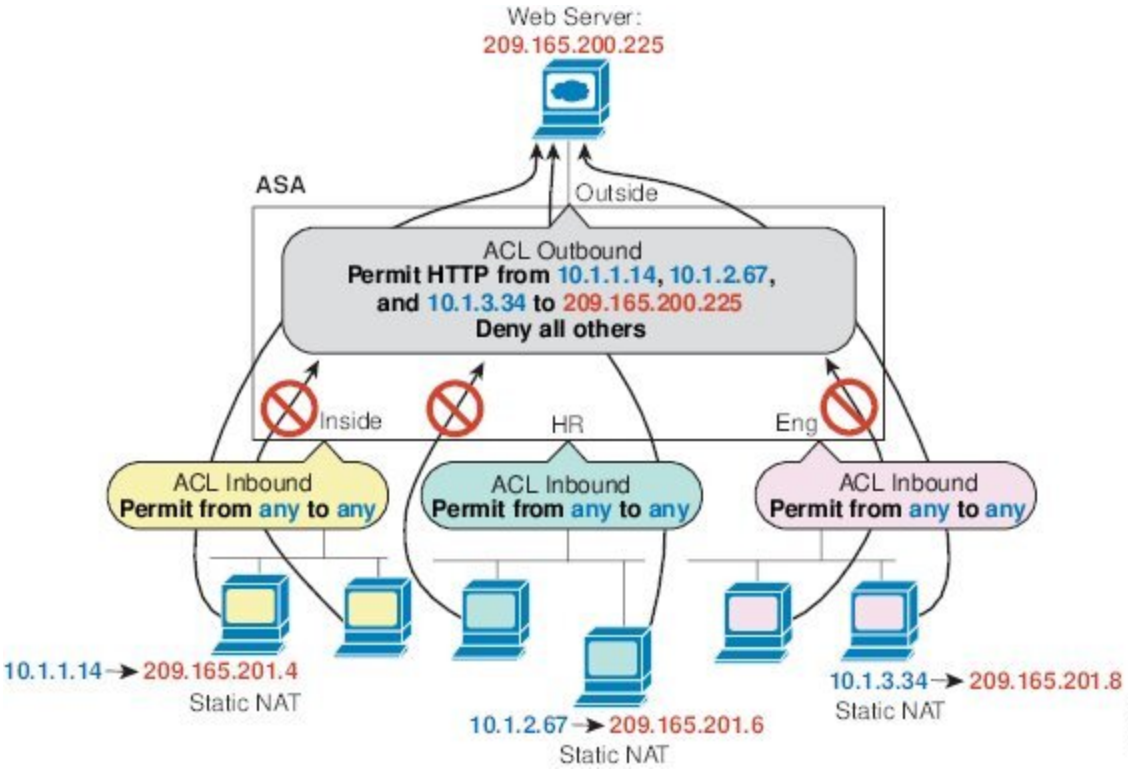
トラフィックの方向に基づいてアクセス ルールを設定できます。

- インバウンド：インバウンド 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 ルールおよび管理アクセス ルールは常にインバウンド ルールになります。
- アウトバウンド：アウトバウンドルールは、インターフェイスから送信されるトラフィックに適用されます。

（注） 「インバウンド」および「アウトバウンド」は、インターフェイスにおける ACL の適用対象を表したもので、前者は、インターフェイスにおいて ASA により受信されるトラフィックに ACL が適用されることを表し、後者はインターフェイスにおいて ASA から送信されるトラフィックに ACL が適用されることを表しています。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。

たとえば、内部ネットワーク上の特定のホストに限って、外部ネットワーク上の Web サーバーにアクセスできるようにする場合などには、アウトバウンド ACL が有用です。複数のインバウンド ACL を作成してアクセスを制限することもできますが、指定したホストだけアクセスを許可するアウトバウンド ACL を 1 つだけ作成する方が効率的です（次の図を参照してください）。他のすべてのホストは、アウトバウンド ACL により外部ネットワークから遮断されます。

図 *1 : Outbound ACL*



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
```

ルールの順序

ルールの順序が重要です。ASAにおいて、パケットを転送するかドロップするかの判断が行われる場合、ASAでは、パケットと各ルールとの照合が、適用されるACLにおけるそれらのルールの並び順に従って行われます。いずれかのルールに合致した場合、それ以降のルールはチェックされません。たとえば、先頭に作成したアクセスルールが、インターフェイスに対してすべてのトラフィックを明示的に許可するものであれば、それ以降のルールはチェックされません。

暗黙的な許可

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およびIPv6のユニキャスト トラフィックはデフォルトで許可されます。これには標準のルーテッド インターフェイスとルーテッドモードでのブリッジ仮想インターフェイス（BVI）間のトラフィックが含まれます。

ブリッジ グループ メンバーのインターフェイスでは、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この暗黙の許可が、同じブリッジ グループ内でのみインターフェイスに適用されます。ブリッジ グループ メンバーのインターフェイスとルーテッド インターフェイスまたは別のブリッジ グループのメンバーとの間には暗黙の許可はありません。

ブリッジ グループ メンバーのインターフェイス（ルーテッドまたはトランスペアレント モード）も次をデフォルトで許可します。

- 双方向の ARP。ARP トラフィックの制御には ARP インスペクションを使用します。アクセス ルールでは制御できません。
- 双方向の BPDU。（Ethertype ルールを使用してこれらを制御できます）

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 IP）のいずれかを使用する必要があります。

暗黙的な拒否

ACL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ーに、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ーを許可します。

管理（コントロール プレーン）の ACL は to-the-box トラフィックを管理していますが、インターフェイスの一連の管理ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

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 ルールですべてのトラフィックを明示的に拒否した場合は、IP と ARP のトラフィックが拒否され、物理的なプロトコルのトラフィック（自動ネゴシエーションなど）だけが許可されます。

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. ブリッジ グループ メンバーのインターフェイスでは、ブリッジ仮想インターフェイス（BVI）のアクセス ルール
3. グローバル アクセス ルール
4. 暗黙的な拒否

NAT とアクセス ルール

アクセス ルールは、NAT を設定している場合でも、アクセス ルールの一致に実際の IP アドレスを使用します。たとえば、内部サーバ 10.1.1.5 用の NAT を設定して、パブリックにルーティング可能な外部の IP アドレス 209.165.201.5 をこのサーバに付与する場合は、この内部サーバへのアクセスを外部トラフィックに許可するアクセス ルールの中で、サーバのマッピング アドレス（209.165.201.5）ではなく実際のアドレス（10.1.1.5）を参照する必要があります。

同一のセキュリティ レベル インターフェイスとアクセスルール

各インターフェイスにはセキュリティレベルがあり、アクセスルールが考慮される前にセキュリティレベルのチェックが実行されます。したがって、アクセスルールで接続を許可した場合でも、インターフェイスレベルでの同じセキュリティレベルのチェックにより、接続がブロックされる可能性があります。構成で同じセキュリティレベルの接続が許可されるようにすることで、許可/拒否の決定でアクセスルールが常に考慮されるようにする必要がある場合があります。

- 同じセキュリティレベルの入力インターフェイスと出力インターフェイス間の接続は、同じセキュリティトラフィックのインターフェイス間チェックの対象となります。

  これらの接続を許可するには、 **same-security-traffic permit inter-interface** コマンドを入力します。

  これらの接続を許可するには、**[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interface ）]**の順に選択し、**[同じセキュリティレベルで構成された2つ以上のインターフェイス間のトラフィックを有効にする（Enable traffic between two or more interfaces which are configured with the same security levels）]** オプションを選択します。

- 同じ入力インターフェイスと出力インターフェイスを持つ接続は、同じセキュリティトラフィックのインターフェイス内チェックの対象となります。

これらの接続を許可するには、**same-security-traffic permit intra-interface** コマンドを入力します。

これらの接続を許可するには、**[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interface）]** の順に選択し、**[同じインターフェイスに接続された2つ以上のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）]** オプションを選択します。

拡張アクセス ルール

この項では、拡張アクセス ルールについて説明します。

リターン トラフィックに対する拡張アクセス 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、UDP、および SCTP 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、（ACL 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。たとえば、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。

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 が含まれます。ダイナミック ルーティング プロトコルまたは DHCP リレーを、このトラフィックを許可するように設定する必要があります。

トランスペアレントまたはルーテッド ファイアウォール モードで同じブリッジ グループのメンバーであるインターフェイスでは、アクセス ルールを使用して IP トラフィックを許可することができます。

（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 ルールを着信および発信の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。

次の表に、同じブリッジ グループのメンバーであるインターフェイス間のアクセス ルールを使用して、ユーザーが許可できる一般的なトラフィック タイプを示します。

表 *1*: 同じブリッジ グループのメンバー間のアクセス ルールの特別なトラフィック

トラフィック タイプ	プロトコルまたはポート	注
DHCP	UDP ポート 67 および 68	DHCP サーバー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）に対するアクセス制御ルールは、**control-plane** オプションを使用して適用される管理アクセス 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 ACL 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。

通常のアクセス ルールとは異なり、インターフェイスの一連の管理ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

また、デバイスへの ICMP トラフィックは、ICMP ルールを使用して制御できます。デバイスを通過する ICMP トラフィックの制御には、通常の拡張アクセス ルールを使用します。

EtherType ルール

この項では、EtherType ルールについて説明します。

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 情報が含まれるため、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。
- Intermediate System to Intermediate System（IS-IS）。
- IEEE 802.2 論理リンク制御パケット。宛先サービス アクセス ポイントのアドレスに基づいてアクセスを制御できます。

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 EtherType 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 および Tag Distribution Protocol 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。

mpls ldp router-id *interface* **force**

または

tag-switching tdp router-id *interface* **force**

アクセス ルールのライセンス

アクセス制御ルールは特別なライセンスを必要としません。

ただし、ルール内でプロトコルとして **sctp** を使用する場合は、キャリア ライセンスが必要です。

アクセス制御に関するガイドライン

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 アドレスと IPv6 アドレスの組み合わせを含めることができます。

Per-User ACL の注意事項

- ユーザーごとの ACL では、**timeout uauth** コマンドの値が使用されますが、この値は AAA のユーザーごとのセッション タイムアウト値でオーバーライドできます。
- ユーザーごとの ACL 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。ユーザーごとの ACL の **log** オプションの効果はありません。

その他のガイドラインと制限事項

- 時間の経過とともにアクセスルールのリストが増え、多数の廃止されたルールが含まれるようになることがあります。最終的に、アクセスグループの ACL が非常に大きくなり、システム全体のパフォーマンスに影響を与える可能性があります。syslog メッセージの送信、フェールオーバー同期のための通信、SSH/HTTPS 管理アクセス接続の確立と維持などに問題がある場合は、アクセスルールのプルーニングが必要かもしれません。一般に、ルールリストを積極的に維持管理して、古いルール、ヒットしないルール、解決できなくなった FQDN オブジェクトなどを削除する必要があります。また、オブジェクトグループ検索の実装も検討してください。
- 新しい展開ではオブジェクトグループ検索はデフォルトで有効化されます。

  オブジェクト グループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下し、CPU 使用率は増加しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索を有効にした場合、ネットワーク オブジェクトまたはサービス オブジェクトは拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。このオプションを設定するには、**object-group-search access-control** コマンドを使用します。

  object-group-search threshold コマンドを使用してしきい値をイネーブルにし、パフォーマンスの低下を防止することができます。しきい値を使用した動作では、接続ごとに送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。一致件数が膨大になることを防ぐためにルールを設定します。

（注） オブジェクト グループの検索は、ネットワーク オブジェクトとサービス オブジェクトのみで動作します。セキュリティ グループまたはユーザ オブジェクトでは動作しません。ACL にセキュリティ グループが含まれている場合は、この機能を有効にしないでください。ACLが非アクティブになったり、その他の予期しない動作となる可能性があります。

- アクセス グループにトランザクション コミット モデルを使用することで、システムのパフォーマンスと信頼性を高めることができます。ただし、解決が頻繁に変わる可能性があるホスト名にFQDNオブジェクトを使用する場合は、アクセスグループが完全に解決されない可能性があるため、トランザクション コンパイル コミットは推奨されません。詳細については、一般的な操作設定ガイドの基本設定の章を参照してください。**asp rule-engine transactional-commit access-group** コマンドを使用します。

- ASDM では、ACL のルールの前にあるアクセス リストのコメントに基づいてルールの説明が設定されます。ASDMで新しいルールを作成した場合も、関連するルールの前にあるコメントが説明として設定されます。ただし、ASDMのパケットトレーサは、CLIの照合ルール後に設定されたコメントに一致します。

- 完全修飾ドメイン名（FQDN）ネットワークオブジェクトを送信元または宛先の基準として使用するには、データインターフェイスの DNS も設定する必要があります。

  FQDNによるアクセスの制御はベストエフォート型のメカニズムであることに注意してください。次の点を考慮してください。

  - DNS応答はスプーフィングされる可能性があるため、完全に信頼できる内部DNSサーバのみを使用します。

  - 一部のFQDNは、特に非常に人気の高いサーバーの場合、数千とはいかなくても、数百の IP アドレスを持つことがあり、それらが頻繁に変更されることがあります。システムはキャッシュされている DNS ルックアップの結果を使用するため、ユーザーはキャッシュに存在しないアドレスを取得する可能性があり、その接続はFQDNルールに合致しません。FQDN ネットワークオブジェクトを使用するルールは、100 未満のアドレスに解決される名前に対してのみ効果的に機能します。

    100 を超えるアドレスに解決される FQDN のネットワーク オブジェクト ルールを作成しないことを推奨します。接続のアドレスが解決され、デバイスのDNSキャッシュで使用可能である可能性は低いからです。

  - 人気のあるFQDNでは、異なるDNSサーバが異なるセットのIPアドレスを返す場合があります。したがって、ユーザが設定したものとは異なる DNS サーバを使用している場合、FQDNベースのアクセス制御ルールがクライアントで使用されているサイトのすべての IP アドレスに適用されないことがあり、ルールで意図した結果が得られません。

- 一部の FQDN DNS エントリには、非常に短い存続可能時間（TTL）値が設定されています。この結果、ルックアップテーブルで頻繁に再コンパイルが発生し、全体的なシステムパフォーマンスに影響を与える場合があります。

アクセス制御の設定

ここでは、アクセス コントロールを設定する方法について説明します。

アクセス グループの設定

アクセス グループを作成するには、まず、ACL を作成します。

ACL 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するには、次のコマンドを使用します。

access-group *access_list* { {**in** | **out**} **interface** *interface_name* [**per-user-override** | **control-plane**] | **global**}

インターフェイス固有のアクセス グループの場合は、次の手順を実行します。

- 拡張または EtherType ACL 名を指定します。ACL タイプ、インターフェイス、方向ごとに 1 つの access-group コマンドを設定し、1 つのコントロール プレーン ACL を設定できます。コントロール プレーン ACL は、拡張 ACL である必要があります。Ethertype ACL はブリッジ グループ メンバーのインターフェイスでのみ許可されます。ルーテッド モードのブリッジ グループでは、ブリッジ仮想インターフェイス（BVI）と各ブリッジ グループ メンバーのインターフェイスの両方に各方向の拡張 ACL を指定できます。
- **in** キーワードによって、ACL が着信トラフィックに適用されます。 **out** キーワードによって、ACL が発信トラフィックに適用されます。
- **interface** 名を指定します。
- per-user-override キーワードを使用すると（着信拡張 ACL の場合に限る）、ユーザー許可用にダウンロードしたダイナミック ユーザー ACL により、インターフェイスに割り当てられている ACL を上書きできます。たとえば、インターフェイス ACL 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 ACL が 10.0.0.0 からのトラフィックをすべて許可する場合、そのユーザーに関しては、ダイナミック ACL によってインターフェイス ACL が上書きされます。

  デフォルトでは、VPN リモート アクセス トラフィックはインターフェイス ACL と照合されません。ただし、**no sysopt connection permit-vpn** コマンドを使用してこのバイパスをオフにする場合、動作は、グループ ポリシーに適用される **vpn-filter** があるかどうか、および **per-user-override** オプションを設定するかどうかによって異なります。

  - **per-user-override** なし、**vpn-filter** なし：トラフィックはインターフェイス ACL と照合されます。

- **per-user-override** なし、**vpn-filter**：トラフィックはまずインターフェイス ACL と照合され、次に VPN フィルタと照合されます。
- **per-user-override**、**vpn-filter**：トラフィックは VPN フィルタのみと照合されます。

- 拡張 ACL 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。

  通常のアクセスルールとは異なり、インターフェイスの一連の管理（コントロールプレーン）ルールの末尾には暗黙の deny がありません。その代わりに、管理アクセス ルールに一致しない接続は通常のアクセス制御ルールで評価されます。

グローバル アクセス グループの場合は、global キーワードを指定して、すべてのインターフェイスの着信方向に拡張 ACL を適用します。

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

access-list コマンドでは、任意のホストからポート 80 を使用してホスト 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。

ICMP アクセス ルールの設定

デフォルトでは、IPv4 または IPv6 を使用して任意のインターフェイスに ICMP パケットを送信できます。ただし、次の例外があります。

- ASA は、ブロードキャスト アドレス宛ての ICMP エコー要求に応答しません。
- ASAは、トラフィックが着信するインターフェイス宛ての ICMP トラフィックにのみ応答します。ICMP トラフィックは、インターフェイス経由で離れたインターフェイスに送信できません。

デバイスを攻撃から保護するために、ICMP ルールを使用して、インターフェイスへの ICMP アクセスを特定のホスト、ネットワーク、または ICMP タイプに限定できます。ICMP ルールにはアクセスルールと同様に順序があり、パケットに最初に一致したルールのアクションが適用されます。

インターフェイスに対して any ICMP ルールを設定すると、ICMP ルールのリストの最後に暗黙の deny ICMP ルールが追加され、デフォルトの動作が変更されます。そのため、一部のメッセージ タイプだけを拒否する場合は、残りのメッセージ タイプを許可するように ICMP ルールのリストの最後に permit any ルールを含める必要があります。

ICMP到達不能メッセージタイプ（タイプ3）の権限を常に付与することを推奨します。ICMP到達不能メッセージを拒否すると、ICMPパスMTUディスカバリがディセーブルになり、IPsecおよびPPTPトラフィックが停止することがあります。また、IPv6のICMPパケットは、IPv6のネイバー探索プロセスに使用されます。

手順

ステップ1 ICMPトラフィックのルールを作成します。

icmp {**permit** | **deny**} {**host** *ip_address* | *ip_address mask* | **any**} [*icmp_type*] *interface_name*

icmp_type を指定しない場合、すべてのタイプにルールが適用されます。番号または名前を入力できます。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。

すべてのアドレス（**any**）、単一のホスト（**host**）、またはネットワーク（*ip_address mask*）にルールを適用できます。

ステップ2 ICMPv6（IPv6）トラフィックのルールを作成します。

ipv6 icmp {**permit** | **deny**} {**host** *ipv6_address* | *ipv6-network*/*prefix-length* | **any**} [*icmp_type*] *interface_name*

icmp_type を指定しない場合、すべてのタイプにルールが適用されます。

すべてのアドレス（**any**）、単一のホスト（**host**）、またはネットワーク（*ipv6-network*/*prefix-length*）にルールを適用できます。

ステップ3 （任意）トレース ルートの出力にASAが表示されるように、ICMPの到達不能メッセージに対するレート制限を設定します。

icmp unreachable rate-limit *rate* **burst-size** *size*

レート制限は1～100の範囲で設定できます。デフォルトは1です。バースト サイズは1～10です。応答のバーストサイズ数が送信されますが、後続の応答は、レート制限に達するまで送信されません。

例：

ASAをホップの1つとして表示するトレース ルートに対してASAの通過を許可するためには、**set connection decrement-ttl** コマンドをイネーブルにするほか、レート制限を大きくする必要があります。たとえば、次のポリシーでは、ASAを通過するすべてのトラフィックについて、レート制限を引き上げ、Time-to-Live（TTL; 存続可能時間）の値をデクリメントしています。

```
icmp unreachable rate-limit 50 burst-size 10
class-map global-class
  match any
policy-map global_policy
  class global-class
```

```
set connection decrement-ttl
```

例

次の例は、10.1.1.15 のホストを除くすべてのホストで内部インターフェイスへの ICMP の使用を許可する方法を示しています。

```
hostname(config)# icmp deny host 10.1.1.15 inside
hostname(config)# icmp permit any inside
```

次の例は、10.1.1.15 のアドレスを持つホストに内部インターフェイスへの ping だけを許可する方法を示しています。

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

次に、外部インターフェイスですべての ping 要求を拒否し、すべての packet-too-big メッセージを許可する（パス MTU ディスカバリをサポートするため）方法を示します。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次の例は、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する方法を示しています。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

アクセス ルールのモニタリング

ネットワーク アクセスをモニターするには、次のコマンドを入力します。

- **clear access-list** *id* **counters**

  アクセス リストのヒット数を消去します。

- **show access-list** [*name*]

  各 ACE の行番号とヒット カウントを含むアクセス リストを表示します。ACL 名を指定してください。そうしないと、すべてのアクセス リストが表示されます。

- **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 ACL を表示します。

アクセス ルールの syslog メッセージの評価

アクセス ルールに関するメッセージは、syslog イベントのビューア（ASDM のビューアなど）を使用して確認できます。

デフォルトのロギングを使用している場合、明示的に拒否されたフローに対する syslog メッセージ 106023 だけが表示されます。ルールのリストの最後にある「暗黙の deny」に一致するトラフィックは記録されません。

ASA が攻撃を受けた場合、拒否されたパケットを示す syslog メッセージの数が非常に大きくなることがあります。代わりに、syslog メッセージ 106100 を使用するロギングをイネーブルにすることをお勧めします。このメッセージは各ルール（許可ルールも含む）の統計情報を示すもので、これを使用することにより、生成される syslog メッセージの数を制限できます。また、特定のルールについて、すべてのロギングをディセーブルにする方法もあります。

メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフローエントリを作成して、指定された間隔内で受信したパケットの数を追跡します。ASA は、最初のヒットがあったとき、および各間隔の終わりに syslog メッセージを生成し、その間隔におけるヒットの合計数と最後のヒットのタイムスタンプを示します。各間隔の終わりに、ASA はヒット数を 0 にリセットします。1 つの間隔内で ACE と一致するパケットがなかった場合、ASA はそのフロー エントリを削除します。ルールのロギングの設定では、それぞれのルールについて、ログ メッセージの間隔のほか、シビラティ（重大度）も制御することができます。

フローは、送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびポートで定義されます。同じ 2 つのホスト間の新しい接続では、送信元ポートが異なる場合があるため、接続のための新しいフローが作成されると、同じフローの増加は示されない場合があります。

確立された接続に属する、許可されたパケットを ACL でチェックする必要はありません。最初のパケットだけがロギングされ、ヒット数に含められます。ICMP などのコネクションレス型プロトコルの場合は、許可されているパケットもすべてロギングされ、拒否されたパケットはすべてロギングされます。

これらのメッセージの詳細については、*syslog* メッセージ ガイドを参照してください。

ヒント メッセージ 106100 のロギングがイネーブルで、パケットが ACE と一致した場合、ASA はフロー エントリを作成して、指定された間隔内で受信したパケットの数を追跡します。ASA では、ACE 用のロギング フローを最大 32 K 保持できます。どの時点でも大量のフローが同時に存在する可能性があります。メモリおよび CPU リソースが無制限に消費されないようにするために、ASA は同時拒否フロー数に制限を設定します。この制限は、拒否フローに対してだけ設定されます（許可フローには設定されません）。これは、拒否フローは攻撃を示している可能性があるためです。制限に達すると、ASA は既存の拒否フローが期限切れになるまでロギング用の新しい拒否フローを作成せず、メッセージ 106101 を発行します。このメッセージの頻度は **access-list alert-interval** *secs* コマンドを使用して、拒否フローのキャッシュの最大数は **access-list deny-flow-max** *number* コマンドを使用して制御できます。

ネットワーク アクセスの許可または拒否の設定例

次に、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のいくつかを示します。

拡張 ACL の例

次の例は、内部サーバー1のネットワークオブジェクトを追加し、サーバーに対してスタティック NAT を実行し、内部サーバー 1 への外側からのアクセスをイネーブルにします。

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12

hostname(config)# access-list outside_access extended permit tcp any object inside-server1
 eq www
hostname(config)# access-group outside_access in interface outside
```

次の例では、すべてのホストに内部ネットワークと 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
```

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
```

EtherType の例

たとえば、次のサンプル ACL 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
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-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 nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

アクセス ルールの履歴

機能名	プラットフォーム リリース	説明
インターフェイス アクセス ルール	7.0(1)	ACL を使用した、ASA 経由のネットワーク アクセスの制御。 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。 次のコマンドが変更されました。 **access-group.**
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ー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。
EtherType ACL が IS-IS トラフィックをサポート	8.4(5)、9.1(2)	トランスペアレント ファイアウォール モードでは、ASA が EtherType ACL を使用して IS-IS トラフィックを渡すことができるようになりました。 **access-list ethertype** {**permit** | **deny**} **isis** コマンドが変更されました。

機能名	プラットフォーム リリース	説明
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。
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。 次のコマンドが変更されました。**access-list extended**、**access-list webtype** **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。
アクセス グループ ルール エンジンのトランザクション コミット モデル	9.1(5)	イネーブルの場合、ルールの編集の完了後、ルールの更新が適用されます。ルールの照合パフォーマンスへの影響はありません。 asp rule-engine transactional-commit、show running-config asp rule-engine transactional-commit、clear configure asp rule-engine transactional-commit の各コマンドが導入されました。
ACL およびオブジェクトを編集するためのコンフィギュレーション セッション アクセス ルール内でのオブジェクトおよび ACL の前方参照	9.3(2)	独立したコンフィギュレーション セッションで ACL およびオブジェクトを編集できるようになりました。オブジェクトおよび ACL を前方参照することも可能です。つまり、まだ存在していないオブジェクトや ACL に対するルールおよびアクセス グループを設定することができます。 clear config-session、clear session、configure session、forward-reference、show config-session の各コマンドが導入されました。

機能名	プラットフォーム リリース	説明
Stream Control Transmission Protocol（SCTP）のアクセス ルールのサポート	9.5(2)	**sctp** プロトコルを使用して、ポートの仕様を含むアクセス ルールを作成できるようになりました。 次のコマンドが変更されました。**access-list extended** 。
Ethertype ルールで、IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスがサポートされます。	9.6(2)	IEEE 802.2 論理リンク制御パケットの宛先サービス アクセス ポイントのアドレスに対する Ethertype のアクセス制御ルールを作成できるようになりました。この追加により、**bpdu** キーワードが対象トラフィックに一致しなくなります。**dsap 0x42** に対して **bpdu** ルールを書き換えます。 次のコマンドが変更されました。 **access-list ethertype**
ブリッジ グループ メンバーのインターフェイスで Ethertype ルールのルーテッド モード、およびブリッジ グループの仮想インターフェイス（BVI）の拡張アクセス ルールのサポート。	9.7(1)	Ethertype ACL を作成し、ルーテッド モードのブリッジ グループ メンバーのインターフェイスに適用できるようになりました。また、メンバー インターフェイスに加えて、ブリッジ仮想インターフェイス（BVI）に拡張アクセス ルールを適用することもできます。 次のコマンドが変更されました。**access-group**、**access-list ethertype**
EtherType アクセス制御リストの変更。	9.9(1)	EtherType アクセス コントロール リストは、Ethernet II IPX（EII IPX）をサポートするようになりました。さらに、DSAP キーワードに新しいキーワードが追加され、共通 DSAP 値（BPDU（0x42）、IPX（0xE0）、Raw IPX（0xFF）、および ISIS（0xFE））をサポートします。その結果、BPDU または ISIS キーワードを使用する既存の EtherType アクセス制御エントリは自動的に DSAP 仕様を使用するように変換され、IPX のルールは 3 つのルール（DSAP IPX、DSAP Raw IPX、および EII IPX）に変換されます。さらに、IPX を EtherType 値として使用するパケット キャプチャは廃止されました。これは、IPX が 3 つの個別の EtherType に対応するためです。 次のコマンドが変更されました：**access-list ethertype** キーワード **eii-ipx** および **dsap** {**bpdu** | **ipx** | **isis** | **raw-ipx**}が追加されました。**capture ethernet-typeipx** キーワードはサポートされなくなりました。
オブジェクト グループの検索しきい値がデフォルトで無効になりました。	9.12(1)	これまではオブジェクト グループの検索が有効になると、この機能によりしきい値が適用され、パフォーマンスの低下を防止していました。そのしきい値が、デフォルトで無効になりました。しきい値は、**object-group-search threshold** コマンドを使用して有効にできます。 **object-group-search threshold** コマンドが追加されました。

機能名	プラットフォーム リリース	説明
ACL とオブジェクトの前方参照は常に有効にです。さらに、アクセス制御のオブジェクトグループ検索がデフォルトで有効になりました。	9.18(1)	アクセスグループまたはアクセスルールを設定するときに、まだ存在していない ACL またはネットワークオブジェクトを参照できます。 さらに、オブジェクトグループ検索が新規展開のアクセス制御に対してデフォルトで有効になりました。デバイスをアップグレードしても、引き続きこのコマンドは無効になります。有効にする場合（推奨）、手動で行う必要があります。 **forward-reference enable** コマンドを削除し、**object-group-search access-control** のデフォルトを有効に変更しました。
オブジェクトグループ検索の最適化。	9.22(1)	オブジェクトグループ検索機能が拡張され、アクセスコントロールルールを評価して接続を照合する際のオブジェクトルックアップ時間が短縮され、CPU オーバーヘッドが削減されました。オブジェクトグループ検索の設定に変更はありません。最適化された動作は自動的に行われます。 デバイス CLI に次のコマンドが追加されました。または、コマンド出力が拡張されました。 **clear asp table network-object**、 **debug ac logs**、 **packet-tracer**、 **show access-list**、 **show asp table network-group**、 **show object-group**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。