



# アクセスコントロールリスト

アクセスコントロールリスト (ACL) は、さまざまな機能で使用されます。ACL をアクセスルールとしてインターフェイスに適用するか、グローバルに適用すると、アプライアンスを通過するトラフィックが許可または拒否されます。ACL では、他の機能のために、機能を適用するトラフィックを選択し、制御サービスではなく照合サービスを実行します。

ここでは、ACL の基本と ACL を設定およびモニタする方法について説明します。アクセスルールとは、グローバルに、またはインターフェイスに適用される ACL のことです。これについては、「[アクセセルール](#)」で詳しく説明します。

- [ACL について \(1 ページ\)](#)
- [アクセス制御リストのライセンス \(6 ページ\)](#)
- [ACL のガイドライン \(7 ページ\)](#)
- [ACL の設定 \(8 ページ\)](#)
- [隔離されたコンフィギュレーションセッションでの ACL の編集 \(24 ページ\)](#)
- [ACL のモニタリング \(26 ページ\)](#)
- [ACL の履歴 \(27 ページ\)](#)

## ACL について

アクセスコントロールリスト (ACL) では、ACL のタイプに応じてトラフィック フローを 1 つまたは複数の特性 (送信元および宛先 IP アドレス、IP プロトコル、ポート、EtherType、その他のパラメータを含む) で識別します。ACL は、さまざまな機能で使用されます。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。

## ACL タイプ

ASA では、次のタイプの ACL が使用されます。

- **拡張 ACL** : 主に使用されるタイプです。この ACL は、サービスポリシー、AAA ルール、WCCP、ボットネットトラフィックフィルタ、VPN グループおよび DAP ポリシーを含むさまざまな機能で、トラフィックがデバイスを通るのを許可および拒否するアクセス

ルールとトラフィックの照合に使用されます。 [拡張 ACL の設定 \(10 ページ\)](#) を参照してください。

- **EtherType ACL** : EtherType ACL はブリッジグループメンバーのインターフェイスの非 IP レイヤ2 トラフィックにのみ適用されます。これらのルールを使用して、レイヤ2 パケット内の EtherType 値に基づいてトラフィックを許可または破棄できます。EtherType ACL では、デバイスでの非 IP トラフィックフローを制御できます。 [EtherType ACL の設定 \(23 ページ\)](#) を参照してください。
- **Webtype ACL** : クライアントレス SSL VPN トラフィックのフィルタリングに使用されます。この ACL では、URL または宛先アドレスに基づいてアクセスを拒否できます。 [Webtype ACL の設定 \(18 ページ\)](#) を参照してください。
- **標準 ACL** : 宛先アドレスだけでトラフィックを識別します。このタイプの ACL は、少数の機能 (ルートマップと VPN フィルタ) でしか使用されません。VPN フィルタでは拡張アクセスリストも使用できるので、標準 ACL の使用はルートマップだけにしてください。 [標準 ACL の設定 \(18 ページ\)](#) を参照してください。

次の表に、ACL の一般的な使用目的と使用するタイプを示します。

表 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。ルーテッドモードでは、ACL を使用して、ブリッジグループメンバーのインターフェイスと同じブリッジグループの外部のインターフェイスとの間のトラフィックを許可する必要があります。  (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、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。
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。
特定のユーザの IP トラフィックに対するネットワークアクセスコントロールの強化	拡張、ユーザごとに AAA サーバからダウンロード	ユーザに適用する動的 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。

ACLの使用目的	ACLタイプ	説明
VPN アクセスおよびフィルタリング	拡張 規格	リモート アクセスおよびサイト間 VPN のグループ ポリシーでは、標準または拡張 ACL がフィルタリングに使用されます。リモート アクセス VPN では、クライアントファイアウォール設定とダイナミックアクセスポリシーにも拡張 ACL が使用されます。
トラフィック クラス マップでのモジュラポリシーフレームワークのトラフィックの識別	拡張	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。
ブリッジグループメンバーのインターフェイスに対する非 IP トラフィックのネットワーク アクセスの制御	EtherType	ブリッジグループのメンバーであるすべてのインターフェイスの EtherType に基づいて、トラフィックを制御をする ACL を設定できます。
ルートフィルタリングおよび再配布の特定	規格 拡張	各種のルーティングプロトコルでは、IP アドレスのルートフィルタリングと（ルートマップを介した）再配布に ACL が使用されます（IPv4 アドレスの場合は標準 ACL が、IPv6 アドレスの場合は拡張 ACL がそれぞれ使用されます）。
クライアントレス SSL VPN のフィルタリング	Webtype	Webtype ACL は、URL と宛先をフィルタリングするように設定できます。

## ACL 名

各 ACL には、`outside_in`、`OUTSIDE_IN`、101 などの名前または数値 ID があります。名前は 241 文字以下にする必要があります。実行コンフィギュレーションを表示するときに名前を簡単に見つけられるように、すべて大文字にすることを検討してください。

ACL の目的を識別するのに役立つ命名規則を作成します。ASDM では、「`interface-name_purpose_direction`」などの命名規則が使用されます。たとえば、「外部」インターフェイスにインバウンド方向で適用される ACL の場合には、「`outside_access_in`」のようになります。

従来、ACL ID は数値でした。標準 ACL は、1～99 または 1300～1999 の範囲にありました。拡張 ACL は、100～199 または 2000～2699 の範囲にありました。ASA では、これらの範囲は強制されませんが、数値を使用する場合は、IOS ソフトウェアを実行するルータとの一貫性を保つために、これらの命名規則を引き続き使用することをお勧めします。

## 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ACEで構成されます。特定の行に明示的にACEを挿入しない限り、あるACL名について入力した各ACEはそのACLの末尾に追加されます。

ACEの順序は重要です。ASAは、パケットを転送するかドロップするかを決定するとき、エントリがリストされている順序で各ACEに対してパケットをテストします。一致が見つかる場合、ACEはそれ以上チェックされません。

したがって、一般的なルールの後に具体的なルールを配置した場合、具体的なルールは決してヒットしない可能性があります。たとえば、ネットワーク10.1.1.0/24を許可し、そのサブネット上のホスト10.1.1.15からのトラフィックをドロップする場合、10.1.1.15を拒否するACEは10.1.1.0/24を許可するACEの前に置く必要があります。10.1.1.0/24を許可するACEを先にすると、10.1.1.15は許可され、拒否ACEは決して一致しません。

拡張ACLでは、**access-list** コマンドで **line number** パラメータを使用して適切な場所にルールを挿入します。どの番号を使用すればよいか判断できるようにACLエントリとその行番号を表示するには、**show access-list name** コマンドを使用します。その他のタイプのACLの場合には、ACLを作成（できればASDMを使用）してACEの順序を変更します。

## 許可/拒否と一致/不一致

アクセスコントロールエントリでは、ルールに一致するトラフィックを「許可」または「拒否」します。グローバルアクセスルールやインターフェイスアクセスルールなど、トラフィックがASAの通過を許可されるか、ドロップされるかを決定する機能にACLを適用する場合、「許可」と「拒否」は文字どおりの意味を持ちます。

サービスポリシールールなどのその他の機能の場合、「許可」と「拒否」は実際には「一致」または「不一致」を意味します。この場合、ACLでは、アプリケーションインスペクションやサービスモジュールへのリダイレクトなど、その機能のサービスを受けるトラフィックを選択しています。「拒否される」トラフィックは、単にACLに一致せず、したがってサービスを受けないトラフィックのことです。

## アクセスコントロールによる暗黙的な拒否

through-the-box アクセスルールに使用するACLには末尾に暗黙のdenyステートメントがあります。したがって、インターフェイスに適用されるACLなどのトラフィック制御ACLでは、あるタイプのトラフィックを明示的に許可しない場合、そのトラフィックはドロップされます。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。

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。

サービス対象のトラフィックの選択に使用される ACL の場合は、明示的にトラフィックを「許可」する必要があります。「許可」されていないトラフィックはサービスの対象になりません。「拒否された」トラフィックはサービスをバイパスします。

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 で明示的にすべてのトラフィックを拒否すると、IP および ARP トラフィックが拒否されます。許可されるのは、自動ネゴシエーションなどの物理プロトコルトラフィックだけです。

## NAT 使用時に拡張 ACL で使用する IP アドレス

NAT または PAT を使用すると、アドレスまたはポートが変換され、通常は内部アドレスと外部アドレスがマッピングされます。変換されたポートまたはアドレスに適用される拡張 ACL を作成する必要がある場合は、実際の（変換されていない）アドレスまたはポートを使用するか、マッピングされたアドレスまたはポートを使用するかを決定する必要があります。要件は機能によって異なります。

実際のアドレスとポートが使用されるので、NAT コンフィギュレーションが変更されても ACL を変更する必要はなくなります。

### 実際の IP アドレスを使用する機能

次のコマンドおよび機能では、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、実際の IP アドレスを使用します。

- アクセス ルール（access-group コマンドで参照される拡張 ACL）
- サービス ポリシー ルール（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 フィルタのトラフィック分類（dynamic-filter enable classify-list コマンド）
- AAA ルール（aaa ... match コマンド）
- WCCP（wccp redirect-list group-list コマンド）

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。

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,outside) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
```

```
hostname(config)# access-group OUTSIDE in interface outside
```

### マッピング IP アドレスを使用する機能

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 プロトコルの ACL
- 他のすべての機能の ACL

## 時間ベース ACE

ルールが一定期間だけアクティブになるように、拡張 ACE と Webtype ACE に時間範囲オブジェクトを適用することができます。このタイプのルールを使用すると、特定の時間帯には許容できるものの、それ以外の時間帯には許容できないアクティビティを区別できます。たとえば、勤務時間中に追加の制限を設け、勤務時間後または昼食時にその制限を緩めることができます。逆に、勤務時間外は原則的にネットワークをシャットダウンすることもできます。

時間範囲オブジェクトが含まれていないルールでは、プロトコル、送信元、宛先、およびサービス基準が正確に同じ時間ベースのルールを作成することはできません。時間ベースではないルールは、重複した時間ベースのルールを常にオーバーライドします（冗長であるため）。



- (注) ACL を非アクティブにするための指定の終了時刻の後、約 80 ～ 100 秒の遅延が発生する場合があります。たとえば、指定の終了時刻が 3:50 の場合、この 3:50 は終了時刻に含まれているため、コマンドは、3:51:00 ～ 3:51:59 の間に呼び出されます。コマンドが呼び出された後、ASA は現在実行されているすべてのタスクを終了し、コマンドに ACL を無効にさせます。

## アクセス制御リストのライセンス

アクセス制御リストは特別なライセンスを必要としません。

ただし、エントリ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。

# ACLのガイドライン

## ファイアウォールモード

- 標準ACLと拡張ACLは、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ます。
- Webtype ACLは、ルーテッドモードのみでサポートされます。
- EtherType ACLは、ルーテッドおよびトランスペアレントモードで、ブリッジグループメンバーのインターフェイスに対してのみサポートされます。

## フェールオーバーとクラスタリング

コンフィギュレーションセッションは、フェールオーバーまたはクラスタユニット間で同期されません。あるセッションで変更をコミットすると、通常どおりすべてのフェールオーバーおよびクラスタユニットでその変更が反映されます。

## IPv6

- 拡張ACLとWebtype ACLでは、IPv4アドレスとIPv6アドレスを組み合わせて使用できます。
- 標準ACLでは、IPv6アドレスは使用できません。
- EtherType ACLでは、IPアドレスは使用しません。

## その他のガイドライン

- ネットワークマスクを指定するときは、指定方法がCisco IOSソフトウェアの **access-list** コマンドとは異なることに注意してください。ASAでは、ネットワークマスク（たとえば、Class Cマスクの255.255.255.0）が使用されます。Cisco IOSマスクでは、ワイルドカードビット（たとえば、0.0.0.255）が使用されます。
- 通常、ACLまたはオブジェクトグループに存在しないオブジェクトを参照したり、現在参照しているオブジェクトを削除したりすることはできません。**access-group** コマンド（アクセスルールを適用するコマンド）に存在しないACLを参照することもできません。ただし、このデフォルトの動作を変更し、オブジェクトまたはACLを作成する前にそれらを「前方参照」できるようにすることができます。オブジェクトまたはACLが作成されるまで、それらを参照するルールまたはアクセスグループは無視されます。事前参照をイネーブルにするには、**forward-reference enable** コマンドを使用します。
- （拡張ACLのみ）次の機能では、ACLを使用しますが、アイデンティティファイアウォール（個人またはグループ名を指定）、FQDN（完全修飾ドメイン名）、またはCisco TrustSec値を含むACLは使用できません。
  - VPNの **crypto map** コマンド

- VPN の `group-policy` コマンド、ただし、`vpn-filter` を除く
- WCCP
- DAP

## ACL の設定

次の各セクションでは、さまざまなタイプの ACL の設定方法について説明します。まず ACL の基本に関するセクションを読んで全体像を把握し、次に特定のタイプの ACL に関するセクションを読んで詳細を確認してください。

## 基本的な ACL 設定および管理オプション

1つの ACL は、同じ ACL ID または ACL 名を持つ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。新しい ACL を作成するには、新しい ACL 名で ACE を作成します。作成した ACE は、新しい ACL の最初のルールになります。

ACL の操作では、次のことを実行できます。

### ACL の内容を確認し、行番号とヒット数を決定する

ACL の内容を表示するには、`show access-list name` コマンドを使用します。各行は ACE で、行番号を含みます。行番号は、拡張 ACL に新しいエントリを挿入する場合に知っておく必要があります。情報には、各 ACE のヒットカウントも含まれます。ヒットカウントは、トラフィックがルールに一致した回数です。次に例を示します。

```
hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group
LOCAL\\usergroup any any (hitcnt=0) 0xb0f5b1e1
```

### ACE を追加する

ACE を追加するためのコマンドは `access-list name [line line-num] type parameters` です。行番号引数は、拡張 ACL でのみ使用できます。行番号を指定すると、ACE は ACL のその場所に挿入されます。その場所にあった ACE は、残りの ACE とともに下に移動します (つまり、ある行番号の位置に ACE を挿入しても、その行にあった古い ACE は置き換えられません)。行番号を指定しない場合、ACE は ACL の末尾に追加されます。使用可能なパラメータは、ACL のタイプによって異なります。詳細については、各 ACL タイプのトピックを参照してください。



## コメントを ACL に追加する（Webtype 以外のすべてのタイプ）

ACE の目的を説明するのに役立つ注釈を ACL に追加するには、**access-list name [line line-num] remark text** コマンドを使用します。ベスト プラクティスは、ACE の前に注釈を挿入することです。ASDM で設定を表示すると、注釈は、その注釈に続く ACE に関連付けられます。ACE の前に複数の注釈を入力してコメントを拡張できます。各注釈は 100 文字に制限されます。先頭にスペースを置いて注釈を強調することができます。行番号を指定しない場合、注釈は ACL の末尾に追加されます。たとえば、各 ACE を追加する前に注釈を追加できます。

```
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
```

## ACE または注釈を編集または移動する

ACE または注釈を編集または移動することはできません。代わりに、目的の値を持つ新しい ACE または注釈を（行番号を使用して）適切な場所に作成してから、古い ACE または注釈を削除します。ACE を挿入できるのは拡張 ACL だけなので、標準、Webtype、または EtherType の ACL の ACE を編集または移動する必要がある場合は、それらのタイプの ACL を再作成する必要があります。これは ASDM を使用して長い ACL を再編成するよりもはるかに簡単です。

## ACE または注釈を削除する

ACE または注釈を削除するには、**no access-list parameters** コマンドを使用します。入力する必要があるパラメータ文字列を表示するには、**show access-list** コマンドを使用します。この文字列は、削除する ACE または注釈に正確に一致する必要があります。ただし、**line line-num** 引数は除きます。この引数は、**no access-list** コマンドのオプションです。

## 注釈を含む ACL 全体を削除する

**clear configure access-list name** コマンドを使用します。注意してください。このコマンドでは、確認は求められません。名前を含めないと、ASA のすべてのアクセスリストが削除されます。

## ACL の名前を変更する

**access-list name rename new\_name** コマンドを使用します。

## ACL をポリシーに適用する

ACL を作成しただけでは、トラフィックには何の処理も実行されません。ポリシーに ACL を適用する必要があります。たとえば、**access-group** コマンドを使用してインターフェイスに拡張 ACL を適用すると、このインターフェイスを通過するトラフィックを拒否または許可できます。

## 拡張 ACL の設定

拡張 ACL は、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。拡張 ACL は、最も複雑で機能豊富な ACL タイプで、さまざまな機能に使用できます。拡張 ACL の最も注目すべき用途は、グローバルに、またはインターフェイスに適用され、デバイスを通過するのを拒否または許可されるトラフィックを決定するアクセスグループとしての使用です。ただし、拡張 ACL は、その他のサービスの適用対象のトラフィックを決定するのにも使用されます。

拡張 ACL は複雑であるため、次の各セクションでは、ACE を作成して特定のタイプのトラフィック照合を提供することに焦点を当てます。最初のセクションでは、基本的なアドレスベースの ACE と TCP/UDP ACE について説明し、残りのセクションの基礎を作ります。

### IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加

基本的な拡張 ACE では、IPv4 および IPv6 アドレスや、www.example.com などの完全修飾ドメイン名 (FQDN) を含む送信元アドレスと宛先アドレスに基づいてトラフィックを照合します。実際、どのタイプの拡張 ACE にも、送信元アドレスと宛先アドレスに関する詳細を含める必要があります。したがって、このトピックでは、最小限の拡張 ACE について説明します。



#### ヒント

ヒント：FQDN に基づいてトラフィックを照合する場合は、各 FQDN を表すネットワーク オブジェクトを作成する必要があります。

IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
source_address_argument dest_address_argument [log [[level] [interval secs] | disable | default]]
[time-range time_range_name] [inactive]
```

例：

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

次のオプションがあります。

- *access\_list\_name*：新規または既存の ACL の名前。
- 行番号：*line line\_number* オプションでは、ACE を挿入する位置の行番号を指定します。指定しない場合は、ACL の末尾に追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- プロトコル：*protocol\_argument* では、IP プロトコルを指定します。
  - *name* または *number*：プロトコルの名前または番号を指定します。**ip** を指定すると、すべてのプロトコルに適用されます。

- **object-group protocol grp\_id** : **object-group protocol** コマンドを使用して作成されたプロトコル オブジェクト グループを指定します。
  - **object service obj\_id** : **object service** コマンドを使用して作成されたサービス オブジェクトを指定します。オブジェクトには、ポートまたは ICMP タイプとコード仕様を含めることができます（必要に応じて）。
  - **object-group service grp\_id** : **object-group service** コマンドを使用して作成されたサービス オブジェクト グループを指定します。
- 送信元アドレス、宛先アドレス : *source\_address\_argument* ではパケットの送信元の IP アドレスまたは FQDN を指定し、*dest\_address\_argument* ではパケットの送信先の IP アドレスまたは FQDN を指定します。
- **host ip\_address** : IPv4 ホスト アドレスを指定します。
  - **ip\_address mask** : 10.100.10.0 255.255.255.0 などの IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
  - **ipv6-address/prefix-length** : IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。
  - **any**、**any4**、および **any6** : **any** は IPv4 と IPv6 トラフィックの両方を指定します。**any4** は IPv4 トラフィックのみを指定し、**any6** は IPv6 トラフィックのみを指定します。
  - **interface interface\_name** : ASA インターフェイスの名前を指定します。IP アドレスではなくインターフェイス名を使用して、トラフィックの送信元または宛先のインターフェイスに基づいてトラフィックを照合します。
  - **object nw\_obj\_id** : **object network** コマンドを使用して作成されたネットワーク オブジェクトを指定します。
  - **object-group nw\_grp\_id** : **object-group network** コマンドを使用して作成されたネットワーク オブジェクト グループを指定します。
- ログイング : **log** 引数では、ACE がネットワーク アクセス用の接続に一致するとき (**access-group** コマンドで ACL が適用されます) のログイング オプションを設定します。引数を指定せずに **log** オプションを入力すると、**syslog** メッセージ 106100 はデフォルトレベル (6) とデフォルト間隔 (300 秒) でイネーブルになります。ログ オプションは次のとおりです。
- **level** : 0 ~ 7 の重大度。デフォルトは 6 (情報) です。アクティブな ACE に対してこのレベルを変更する場合、新しいレベルは新規接続に適用され、既存の接続は引き続き前のレベルでログイングされます。
  - **interval secs** : **syslog** メッセージ間の時間間隔 (秒) 。1 ~ 600 で指定します。デフォルトは 300 です。この値は、ドロップ統計情報の収集に使用するキャッシュから非アクティブなフローを削除するためのタイムアウト値としても使用されます。
  - **disable** : すべての ACE ログイングをディセーブルにします。

- **default** : 拒否されたパケットに関するメッセージ 106023 のログをイネーブルにします。この設定は、**log** オプションを指定しないのと同じです。
- **時間範囲** : **time-range** *time\_range\_name* オプションでは、ACE がアクティブになっている時間帯と曜日を決定する時間範囲オブジェクトを指定します。時間範囲を指定しない場合、ACE は常にアクティブです。
- **アクティベーション** : ACE を削除せずにディセーブルにするには、**inactive** オプションを使用します。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。

## ポートベースの照合に使用する拡張 ACE の追加

ACE でサービス オブジェクトを指定する場合は、サービス オブジェクトに TCP/80 などのポートが指定されたプロトコルを含めることができます。または、ACE にポートを直接指定できます。ポートベースの照合を使用すると、プロトコルのすべてのトラフィックではなく、ポートベースのプロトコルの特定のタイプのトラフィックを対象にすることができます。

ポートベースの拡張 ACE は、プロトコルが **tcp**、**udp**、または **sctp** である基本的なアドレス照合 ACE です。ポート仕様を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} {tcp | udp | sctp}
source_address_argument [port_argument] dest_address_argument [port_argument] [log [[level] [interval
secs]] | disable | default] [time-range time-range-name] [inactive]
```

例 :

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

*port\_argument* オプションでは、送信元ポートまたは宛先ポートを指定します。ポートを指定しなかった場合は、すべてのポートが照合されます。使用可能な引数は次のとおりです。

- **operator port** : *port* は、整数またはポートの名前にできます。*operator* には次のいずれかを指定できます。
  - **lt** : より小さい
  - **gt** : より大きい
  - **eq** : 等しい
  - **neq** : 等しくない
  - **range** : 値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します (例 : **range 100 200**) 。



(注) DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

- **object-group service grp\_id : object-group service {tcp | udp | tcp-udp}** コマンドを使用して作成されたサービス オブジェクト グループを指定します。これらのオブジェクト タイプは推奨されなくなりました。

ポート引数としてプロトコルおよびポートがオブジェクト内で定義されている場合は、推奨される一般的なサービス オブジェクトは指定できません。[IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 \(10 ページ\)](#) で説明されているように、これらのオブジェクトはプロトコル引数の一部として指定します。

その他のキーワードの詳細と、サービスオブジェクトを使用してプロトコルおよびポートを指定する方法については、[IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 \(10 ページ\)](#) を参照してください。

## ICMP ベースの照合に使用する拡張 ACE の追加

ACE でサービス オブジェクトを指定する場合は、サービス オブジェクトに ICMP/ICMP6 プロトコルの ICMP タイプとコード仕様を含めることができます。または、ACE に ICMP タイプとコードを直接指定できます。たとえば、ICMP エコー要求 (ping) トラフィックをターゲットにできます。

ICMP 拡張 ACE は、プロトコルが **icmp** または **icmp6** である基本的なアドレス照合 ACE です。これらのプロトコルにはタイプおよびコード値があるため、ACE にタイプおよびコード仕様を追加できます。

プロトコルが ICMP または ICMP6 である IP アドレスまたは FQDN 照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} {icmp | icmp6}
source_address_argument dest_address_argument [icmp_argument] [log [[level] [interval secs]] | disable
| default]] [time-range time_range_name] [inactive]
```

例：

```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
hostname(config)# access-list abc extended permit icmp any any echo
```

*icmp\_argument* オプションでは、ICMP のタイプとコードを指定します。

- **icmp\_type [icmp\_code]** : ICMP タイプを名前または番号で指定し、そのタイプの ICMP コード (省略可能) を指定します。コードを指定しない場合は、すべてのコードが使用されません。
- **object-group icmp\_grp\_id** : (廃止予定) **object-group icmp-type** コマンドを使用して作成された ICMP/ICMP6 用のオブジェクト グループを指定します。

ICMP 引数としてプロトコルおよびタイプがオブジェクト内で定義されている場合は、推奨される一般的なサービス オブジェクトは指定できません。IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加（10 ページ）で説明されているように、これらのオブジェクトはプロトコル引数の一部として指定します。

他のキーワードの説明については、IP アドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加（10 ページ）を参照してください。

## ユーザベースの照合（アイデンティティファイアウォール）に使用する拡張 ACE の追加

ユーザベースの拡張 ACE は、ユーザ名またはユーザ グループを送信元の一一致条件に含める基本的なアドレス照合 ACE です。ユーザ ID に基づくルールを作成すると、ルールがスタティックなホストまたはネットワークアドレスに縛られるのを回避できます。たとえば、user1 のルールを定義し、アイデンティティファイアウォール機能によってそのユーザがあるホストにマッピングされているとします。さらに、このホストにある日 10.100.10.3 が割り当てられ、その翌日に 192.168.1.5 が割り当てられたとします。この場合でも、ユーザベースのルールは適用されます。

送信元アドレスと宛先アドレスは引き続き指定する必要があります。そのため、送信元アドレスは、ユーザに（通常は DHCP 経由で）割り当てられる可能性があるアドレスが含まれるように広く設定してください。たとえば、ユーザ「LOCAL\user1 any」は、割り当てられているアドレスに関係なく LOCAL\user1 ユーザに一致しますが、「LOCAL\user1 10.100.1.0/255.255.255.0」は、アドレスが 10.100.1.0/24 ネットワーク上にある場合にのみユーザに一致します。

グループ名を使用すると、学生、教師、マネージャ、エンジニアなどユーザのクラス全体に基づいてルールを定義できます。

ユーザまたはグループ照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument [user_argument] source_address_argument [port_argument] dest_address_argument [port_argument] [log [[level] [interval secs] | disable | default]] [time-range time_range_name] [inactive]
```

例：

```
hostname (config) # access-list v1 extended permit ip user LOCAL\idfw  
any 10.0.0.0 255.255.255.0
```

*user\_argument* オプションでは、送信元アドレスに加えて、トラフィックを照合するユーザまたはグループを指定します。使用可能な引数は次のとおりです。

- **object-group-user** *user\_obj\_grp\_id* : **object-group user** コマンドを使用して作成されたユーザ オブジェクト グループを指定します。
- **user** {[*domain\_nickname*]\*name* | **any** | **none**} : ユーザ名を指定します。ユーザ クレデンシャルを含むすべてのユーザを照合するには **any** を指定し、ユーザ名にマッピングされていないアドレスを照合するには **none** を指定してください。これらのオプションが特に役立つのは、**access-group** と **aaa authentication match** のポリシーを結合する場合です。

- **user-group** [domain\_nickname\\]user\_group\_name : ユーザグループ名を指定します。\\ はドメインとグループ名の区切りです。

他のキーワードの説明については、[IPアドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 \(10 ページ\)](#) を参照してください。



ヒント 特定の ACE にユーザと Cisco Trustsec セキュリティグループの両方を含めることができます。

## セキュリティグループベースの照合 (Cisco TrustSec) に使用する拡張 ACE の追加

セキュリティグループ拡張 ACE は、セキュリティグループまたはタグを送信元または宛先の一致条件に含める基本的なアドレス照合 ACE です。セキュリティグループに基づくルールを作成すると、ルールがスタティックなホストまたはネットワークアドレスに縛られるのを回避できます。送信元アドレスと宛先アドレスは引き続き指定する必要があります。そのため、アドレスは、ユーザに (通常は DHCP 経由で) 割り当てられる可能性があるアドレスが含まれるように広く設定してください。



ヒント このタイプの ACE を追加する前に、Cisco TrustSec 設定してください。

セキュリティグループ照合に使用する ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[security_group_argument] source_address_argument [port_argument] [security_group_argument]
dest_address_argument [port_argument] [log [[level]]] [interval secs] | disable | default] [inactive |
time-range time_range_name]
```

例 :

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security\_group\_argument オプションでは、送信元または宛先アドレスに加えて、トラフィックを照合するセキュリティグループを指定します。使用可能な引数は次のとおりです。

- **object-group-security** security\_obj\_grp\_id : **object-group security** コマンドを使用して作成されたセキュリティオブジェクトグループを指定します。
- **security-group** {name security\_grp\_id | tag security\_grp\_tag} : セキュリティグループの名前またはタグを指定します。

他のキーワードの説明については、[IPアドレスまたは完全修飾ドメイン名ベースの照合に使用する拡張 ACE の追加 \(10 ページ\)](#) を参照してください。



ヒント 特定の ACE にユーザと Cisco Trustsec セキュリティグループの両方を含めることができます。

## 拡張 ACL の例

次に示す ACL は ASA を通るすべてのホスト（ACL を適用するインターフェイス上の）を許可します。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次の ACL は、192.168.1.0/24 のホストが TCP ベースのトラフィックで 209.165.201.0/27 のネットワークにアクセスすることを拒否します。その他のアドレスはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

選択したホストだけにアクセスを制限する場合は、限定的な許可 ACE を入力します。デフォルトでは、明示的に許可しない限り、他のトラフィックはすべて拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次の ACL では、すべてのホスト（この ACL を適用するインターフェイス上の）からアドレス 209.165.201.29 の Web サイトへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

オブジェクトグループを使用する次の ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

次の例では、あるネットワーク オブジェクトグループ (A) から別のネットワーク オブジェクトグループ (B) へのトラフィックを許可する ACL を一時的にディセーブルにします。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

時間ベース ACE を実装するには、**time-range** コマンドを使用して、週おおよび 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACE にバインドします。次の例では、「Sales」ACL の ACE を「New\_York\_Minute」という時間範囲にバインドしています。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
```



```
209.165.201.1 time-range New_York_Minute
```

次の例では、IPv4/IPv6 混在 ACL が表示されています。

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

## アドレスを拡張 ACL のオブジェクトに変換する例

次に示す、オブジェクトグループを使用しない通常の ACL では、内部ネットワーク上のさまざまなホストについて、さまざまな Web サーバへのアクセスを禁止しています。他のトラフィックはすべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

2つのネットワーク オブジェクトグループ（内部ホスト用に1つ、Web サーバ用に1つ）を作成すると、コンフィギュレーションが簡略化され、簡単に修正してホストを追加できるようになります。

```
hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group
web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

## 標準 ACL の設定

標準 ACL は、ACL ID または名前が同じすべての ACE で構成されます。標準 ACL は、ルートマップや VPN フィルタなどの限られた数の機能に使用されます。標準 ACL では、IPv4 アドレスのみを使用して、宛先アドレスのみを定義します。

標準アクセスリスト エントリを追加するには、次のコマンドを使用します。

```
access-list access_list_name standard {deny | permit} {any4 | host ip_address | ip_address mask}
```

例：

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

次のオプションがあります。

- 名前：*access\_list\_name* 引数には、ACL の名前または番号を指定します。標準 ACL の従来の数値は 1～99 または 1300～1999 ですが、任意の名前または数値を使用できます。ACL がまだ存在しない場合は、新しい ACL を作成します。ACL が存在する場合、エントリは ACL の末尾に追加されます。
- 許可または拒否：**deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- 宛先アドレス：**any4** キーワードは、すべての IPv4 アドレスに一致します。**host** *ip\_address* 引数は、ホストの IPv4 アドレスに一致します。*ip\_address ip\_mask* 引数は、IPv4 サブネット (10.1.1.0 255.255.255.0 など) に一致します。

## Webtype ACL の設定

Webtype ACL は、クライアントレス SSL VPN トラフィックのフィルタリング、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザアクセスの制限に使用されます。フィルタを定義しない場合は、すべての接続が許可されます。Webtype ACL は、同じ ACL ID または ACL 名を持つすべての ACE で構成されます。

Webtype ACL では、URL または宛先アドレスに基づいてトラフィックを照合できます。単一の ACE でこれらの仕様を組み合わせることはできません。次の各セクションでは、各タイプの ACE について説明します。

### URL 照合に使用する Webtype ACE の追加

ユーザがアクセスしようとしている URL に基づいてトラフィックを照合するには、次のコマンドを使用します。

```
access-list access_list_name webtype {deny | permit} url {url_string | any} [log [[level] [interval secs]] | disable | default]] [time_range time_range_name] [inactive]
```

例：

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

次のオプションがあります。

- **access\_list\_name** : 新規または既存の ACL の名前。ACL がすでに存在する場合は、ACL の末尾に ACE が追加されます。
- 許可または拒否 : **deny** キーワードを指定すると、条件に一致した場合にパケットが拒否または免除されます。**permit** キーワードを指定すると、条件に一致した場合にパケットが許可または包含されます。
- **URL** : **url** キーワードでは、照合する URL を指定します。すべての URL ベースのトラフィックに一致させるには、**url any** を使用します。そうでない場合は、URL 文字列を入力します。URL 文字列には、ワイルドカードを含めることができます。以下では、URL の指定に関するヒントと制限事項をいくつか示します。
  - すべての URL に一致させるには、**any** を指定します。
  - 「Permit url any」と指定すると、「プロトコル://サーバ IP/パス」の形式の URL はすべて許可され、このパターンに一致しないトラフィック（ポート転送など）はブロックされます。暗黙的な拒否が発生しないよう、必要なポート（Citrix の場合はポート 1494）への接続を許可する ACE を使用してください。
  - スマートトンネルと ica プラグインは、**smart-tunnel://** と **ica://** のタイプにのみ一致するため、「permit url any」を使用した ACL によって影響を受けることはありません。
  - 使用できるプロトコルは、**cifs://**、**citrix://**、**citrixs://**、**ftp://**、**http://**、**https://**、**imap4://**、**nfs://**、**pop3://**、**smart-tunnel://**、および **smtp://** です。プロトコルでワイルドカードを使用することもできます。たとえば、**htt\*** は **http** および **https** に一致し、アスタリスク **\*** はすべてのプロトコルに一致します。たとえば、**\*://\*.example.com** は、**example.com** ネットワークへのすべてのタイプの URL ベースのトラフィックに一致します。
  - **smart-tunnel://** URL を指定すると、サーバ名だけを含めることができます。URL にパスを含めることはできません。たとえば、**smart-tunnel://www.example.com** は受け入れ可能ですが、**smart-tunnel://www.example.com/index.html** は受け入れ不可です。
  - アスタリスク (**\***) : 空の文字列を含む任意の文字列に一致します。すべての **http** URL に一致させるには、**http://\*\*** と入力します。
  - 疑問符 **?** は任意の 1 文字に一致します。
  - 角カッコ (**[]**) : 文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、**http://www.cisco.com:80/** と **http://www.cisco.com:81/** の両方に一致させるには、「**http://www.cisco.com:8[01]/**」と入力します。
- **ロギング** : **log** 引数では、パケットが ACE に一致した場合のロギングオプションを設定します。引数を指定せずに **log** オプションを入力すると、**syslog** メッセージ 106102 はデフォルトレベル (6) とデフォルト間隔 (300 秒) でイネーブルになります。ログオプションは次のとおりです。

- **level** : 0 ~ 7 の重大度。デフォルト値は 6 です。
- **interval secs** : syslog メッセージ間の時間間隔 (秒)。1 ~ 600 で指定します。デフォルトは 300 です。
- **disable** : すべての ACL ロギングをディセーブルにします。
- **default** : メッセージ 106103 のロギングをイネーブルにします。この設定は、**log** オプションを指定しないのと同じです。
- **時間範囲** : **time-range** *time\_range\_name* オプションでは、ACE がアクティブになっている時間帯と曜日を決定する時間範囲オブジェクトを指定します。時間範囲を指定しない場合、ACE は常にアクティブです。
- **アクティベーション** : ACE を削除せずにディセーブルにするには、**inactive** オプションを使用します。再度イネーブルにするには、**inactive** キーワードを使用せずに ACE 全体を入力します。

## IP アドレス照合に使用する Webtype ACE の追加

ユーザがアクセスしようとしている宛先アドレスに基づいてトラフィックを照合するには、次のコマンドを使用します。Webtype ACL には、URL 仕様に加えて 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。

IP アドレス照合に使用する Webtype ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name webtype {deny | permit} tcp dest_address_argument [operator port] [log
[[level] [interval secs] | disable | default]] [time_range time_range_name] [inactive]]
```

例 :

```
hostname(config)# access-list acl_company webtype permit tcp any
```

ここで説明していないキーワードの説明については、[URL 照合に使用する Webtype ACE の追加 \(18 ページ\)](#) を参照してください。このタイプの ACE に固有のキーワードと引数は次のとおりです。

- **tcp** : TCP プロトコル。Webtype ACL では、TCP トラフィックのみを照合します。
- **宛先アドレス** : *dest\_address\_argument* では、パケットの送信先の IP アドレスを指定します。
  - **host** *ip\_address* : IPv4 ホスト アドレスを指定します。
  - **dest\_ip\_address mask** : 10.100.10.0 255.255.255.0 など、IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
  - **ipv6-address/prefix-length** : IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。
  - **any**、**any4**、**any6** : **any** は IPv4 と IPv6 の両方のトラフィックを表し、**any4** は IPv4 トラフィックのみを表し、**any6** は IPv6 トラフィックのみを表します。

- *operator port* : 宛先ポート。ポートを指定しなかった場合は、すべてのポートが照合されます。*port* には、TCP ポートの番号（整数）または名前を指定できます。*operator* は次のいずれかになります。
  - **lt** : より小さい
  - **gt** : より大きい
  - **eq** : 等しい
  - **neq** : 等しくない
  - **range** : 値の包括的な範囲。この演算子を使用する場合は、2つのポート番号を指定します（例：**range 100 200**）。

## Webtype ACL の例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

次の例は、特定の Web ページへのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_file webtype deny url  
https://www.example.com/dir/file.html
```

次の例は、特定サーバ上にある任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

次の例は、Webtype ACL でワイルドカードを使用する方法を示しています。

- 次に、`http://www.example.com/layouts/1033` などの URL に一致させる例を示します。

```
access-list VPN-Group webtype permit url http://www.example.com/*
```

- 次に、`http://www.example.com/` や `http://www.example.net/` などの URL に一致させる例を示します。

```
access-list test webtype permit url http://www.example.*
```

- 次に、`http://www.example.com` や `ftp://wwwz.example.com` などの URL に一致させる例を示します。

```
access-list test webtype permit url *://ww?.e*co*/
```

- 次の例は、`http://www.cisco.com:80` や `https://www.cisco.com:81` などの URL に一致します。

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上記の例の範囲演算子「[]」は、文字 **0** または **1** がその場所で出現する可能性があることを示しています。

- 次に、`http://www.example.com` や `http://www.example.net` などの URL に一致させる例を示します。

```
access-list test webtype permit url http://www.[a-z]example?*/
```

上記の例に示した **range** 演算子「[]」は、**a** ~ **z** の範囲内の任意の 1 文字が出現可能であることを指定します。

- 次に、ファイル名またはパスのどこかに「**cgi**」が含まれる **http** または **https** URL に一致させる例を示します。

```
access-list test webtype permit url htt*://*/.*cgi?*
```



- (注) すべての **http** URL に一致させるには、「`http://*`」ではなく「`http://*/*`」と入力する必要があります。

次の例は、**Web-type ACL** を適用して、特定の **CIFS** 共有へのアクセスをディセーブルにする方法を示しています。

このシナリオでは、「**shares**」というルートフォルダに「**Marketing\_Reports**」および「**Sales\_Reports**」という 2 つのサブフォルダが格納されています。「**shares/Marketing\_Reports**」フォルダへのアクセスを明示的に拒否しようとしています。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

ただし、**ACL** の末尾に暗黙的な「**deny all**」があるため、上記の **ACL** を指定すると、ルートフォルダ（「**shares**」）とすべてのサブフォルダ（「**shares/Sales Reports**」と「**shares/Marketing Reports**」）にアクセスできなくなります。

この問題を修正するには、ルートフォルダと残りのサブフォルダへのアクセスを許可する新しい **ACL** を追加します。

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

## EtherType ACL の設定

EtherType ACL は、ブリッジグループメンバーのインターフェイスの非 IP レイヤ 2 トラフィックに適用されます。これらのルールを使用して、レイヤ 2 パケット内の EtherType 値に基づいてトラフィックを許可または破棄できます。EtherType ACL では、ブリッジグループを経由する非 IP トラフィックのフローを制御できます。802.3 形式フレームでは、`type` フィールドではなく `length` フィールドが使用されるため、ACL では処理されません。

EtherType ACE を追加するには、次のコマンドを使用します。

```
access-list access_list_name ethertype {deny | permit} {any | bpdu | dsap {hex_address | bpdu | ipx | isis | raw-ipx} | eii-ipx | ipx | isis | mpls-multicast | mpls-unicast | hex_number}
```

例：

```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

次のオプションがあります。

- `access_list_name`：新規または既存の ACL の名前。ACL がすでに存在する場合は、ACL の末尾に ACE が追加されます。
- 許可または拒否：`deny` キーワードを指定すると、条件に一致した場合にパケットが拒否されます。`permit` キーワードは、条件が一致した場合にパケットを許可します。
- トラフィック一致条件：次のオプションを使用してトラフィックを照合できます。
  - `any`：すべてのレイヤ 2 トラフィックと一致します。
  - `bpdu`：デフォルトで許可されるブリッジプロトコルデータユニット (dsap 0x42)。このキーワードは `dsap bpdu` に変換されます。
  - `dsap{hex_address|bpdu|ipx|isis|raw-ipx}`：IEEE 802.2 論理リンク制御 (LLC) パケットの宛先サービスアクセスポイントのアドレス。ユーザが許可または拒否するアドレスを 16 進数 (0x01 ~ 0xff) で含めます。また、次のキーワードを使用して共通の値のルールを作成することもできます。
    - `bpdu 0x42` では、ブリッジプロトコルデータユニット。
    - `ipx 0xe0` では、Internet Packet Exchange (IPX) 802.2 LLC。
    - `isis 0xfe` では、Intermediate System to Intermediate System (IS-IS)
    - `raw-ipx 0xff` では、Raw IPX 802.3 形式。
  - `eii-ipx`：Ethernet II IPX 形式、EtherType 0x8137。
  - `ipx`：Internetwork Packet Exchange (IPX)。このキーワードは、3つの個別のルールを設定するための `dsap ipx`、`dsap raw-ipx`、および `eii-ipx` のショートカットです。
  - `isis`：Intermediate System to Intermediate System (IS-IS) このキーワードは `dsap isis` に変換されます。

- **mpls-multicast** : MPLS マルチキャスト。
- **mpls-unicast** : MPLS ユニキャスト。
- **[hex\_number]** : 16 ビットの 16 進数 0x600 ~ 0xffff で指定できる任意の EtherType。EtherType のリストについては、<http://www.ietf.org/rfc/rfc1700.txt> にアクセスして、RFC 1700 「Assigned Numbers」を参照してください。

## EtherType ACL の例

次の例は、EtherType ACL の設定方法（インターフェイスへの適用方法を含む）を示しています。

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
```

## 隔離されたコンフィギュレーションセッションでの ACL の編集

アクセスルールまたは他の目的に使用する ACL を編集すると、その変更はすぐに実装され、トラフィックに影響を与えます。新しいルールがアクティブになるのはルールのコンパイルが完了した後のみとし、そのコンパイルは各 ACE を編集した後に発生することを、トランザクションコミットモデルによって保証するために、アクセスルールを使用できます。



ACL 編集の影響をさらに分離するには、「コンフィギュレーションセッション」で変更を行うことができます。このセッションは、変更内容を明示的にコミットする前に、複数の ACE やオブジェクトを編集できる隔離されたモードです。このため、デバイスの動作を変更する前に、目的のすべての変更が完了したことを確認できます。

### 始める前に

- `access-group` コマンドによって参照されるコマンドは編集できますが、その他のコマンドによって参照される ACL は編集できません。参照されない ACL を編集したり、新しいオブジェクトを作成したりすることもできます。
- オブジェクトとオブジェクトグループを作成または編集できますが、あるセッションで1つのオブジェクトまたはオブジェクトグループを作成する場合、同じセッションでそのオブジェクトまたはオブジェクトグループを編集することはできません。オブジェクトが希望どおりに定義されていない場合は、変更をコミットしてからオブジェクトを編集するか、セッション全体を廃棄してもう一度やり直す必要があります。
- `access-group` コマンド（アクセスルール）によって参照される ACL を編集する場合は、セッションをコミットするときにトランザクション コミット モデルが使用されます。このため、ACL は、古い ACL が新しい ACL に置き換えられる前に完全にコンパイルされません。
- ACL とオブジェクト名の前方参照をイネーブルにすると（`forward-reference enable` コマンド）、`access-group` コマンド（アクセスルール）によって参照される ACL を削除してから、その ACL を再作成できます。変更をコミットすると、コンパイルが完了した後に新しいバージョンの ACL が使用されます。存在しないオブジェクトを参照するルールを作成したり、アクセスルールで使用中のオブジェクトを削除したりすることもできます。ただし、NAT などの他のルールで使用されているオブジェクトを削除すると、コミットエラーが発生します。

### 手順

#### ステップ 1 セッションを開始します。

```
hostname#configure session session_name  
hostname(config-s)#
```

`session_name` がすでに存在する場合は、そのセッションを開きます。存在しない場合は、新しいセッションを作成します。

既存のセッションを表示するには、`show configuration session` コマンドを使用します。一度にアクティブにできるセッションは最大で3つです。古い未使用のセッションを削除する必要がある場合は、`clear configuration session session_name` コマンドを使用します。

他のユーザが編集中であるために既存のセッションを開くことができない場合は、セッションが編集中であることを示すフラグをクリアできます。この操作は、セッションが実際には編集

中でないことが確実な場合にのみ行ってください。フラグをリセットするには、**clear session session\_name access** コマンドを使用します。

**ステップ2** (コミットされたセッションのみ) 変更を行います。次の基本コマンドとそれらのパラメータのいずれかを使用できます。

- **access-list**
- **object**
- **object-group**

**ステップ3** セッションで実行することを決定します。使用できるコマンドは、前にセッションをコミット済みかどうかによって異なります。使用できる可能性があるコマンドは次のとおりです。

- **exit** : セッションを単に終了し、変更のコミットや廃棄は行わないため、後で戻ることができます。
- **commit [noconfirm [revert-save | config-save]]** : (コミットされていないセッションのみ) 変更を保存します。セッションを保存するかどうか尋ねられます。リバートセッションを保存 (**revert-save**) しておくと、**revert** コマンドで変更を元に戻すことができます。また、コンフィギュレーションセッションを保存 (**config-save**) しておくと、そのセッションで変更したすべての内容を、必要に応じて再度コミットできます。リバートセッションまたはコンフィギュレーションセッションを保存した場合は、変更はコミットされますが、セッションはアクティブのままになります。セッションを開いて、変更を元に戻したり同じ変更を再コミットしたりできます。**noconfirm** オプションと任意の適切な **save** オプションを指定すると、プロンプトが表示されないようにすることができます。
- **abort** : (コミットされていないセッションのみ) 変更を破棄し、セッションを削除します。セッションを保持する場合は、セッションを終了して **clear session session\_name configuration** コマンドを使用します。このコマンドは、セッションを削除せずに空にします。
- **revert** : (コミットされたセッションのみ) 変更を元に戻し、セッションをコミットする前のコンフィギュレーションに戻して、そのセッションを削除します。
- **show configuration session [session\_name]** : セッションで行った変更を表示します。

## ACLのモニタリング

ACLをモニタするには、次のいずれかのコマンドを入力します。

- **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-list [name]** : 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。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。

## ACLの履歴

機能名	リリース	説明
標準、拡張、Webtype ACL	7.0(1)	<p>ACLは、ネットワークアクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。拡張アクセスコントロールリストは、<b>through-the-box</b> アクセスコントロールとその他のいくつかの機能に使用されます。標準ACLは、ルートマップとVPNフィルタで使用されます。Webtype ACLは、クライアントレスSSL VPNフィルタリングで使用されます。EtherType ACLは、IP以外のレイヤ2トラフィックを制御します。</p> <p><b>access-list extended</b>、<b>access-list standard</b>、<b>access-list webtype</b>、<b>access-list ethertype</b> の各コマンドが導入されました。</p>
拡張ACLでの実際のIPアドレス	8.3(1)	<p>NATまたはPATを使用するときは、さまざまな機能で、ACLでのマッピングアドレスおよびポートの使用が不要になります。これらの機能については、変換されていない実際のアドレスとポートを使用する必要があります。実際のアドレスとポートが使用されるので、NATコンフィギュレーションが変更されてもACLを変更する必要はなくなります。</p>
拡張ACLでのアイデンティティファイアウォールのサポート	8.4(2)	<p>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。</p> <p><b>access-list extended</b> コマンドが変更されました。</p>
EtherType ACLがIS-ISトラフィックをサポート	8.4(5)、9.1(2)	<p>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トラフィックを制御できるようになりました。</p> <p><b>access-list ethertype {permit deny} isis</b> コマンドが変更されました。</p>
拡張ACLでのCisco TrustSecのサポート	9.0(1)	<p>Cisco 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。</p> <p><b>access-list extended</b> コマンドが変更されました。</p>

機能名	リリース	説明
拡張 ACL と Webytype ACL での IPv4 アドレスと IPv6 アドレスの統合	9.0(1)	<p>拡張 ACL と Webytype ACL で IPv4 アドレスと 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。</p> <p>次のコマンドが変更されました。 <b>access-list extended</b>、 <b>access-list webytype</b></p> <p><b>ipv6 access-list</b>、 <b>ipv6 access-list webytype</b>、 <b>ipv6-vpn-filter</b> の各コマンドが削除されました。</p>
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)	<p>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。</p> <p><b>access-list extended</b>、 <b>service-object</b>、 <b>service</b> の各コマンドが導入または変更されました。</p>
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)	<p>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。</p> <p><b>clear configuration session</b>、 <b>clear session</b>、 <b>configure session</b>、 <b>forward-reference</b>、 および <b>show configuration session</b> の各コマンドが導入されました。</p>
Stream Control Transmission Protocol (SCTP) の ACL のサポート	9.5(2)	<p><b>sctp</b> プロトコルを使用して、ポートの仕様を含む ACL ルールを作成できるようになりました。</p> <p>次のコマンドが変更されました。 <b>access-list extended</b>。</p>
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)	<p>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 Etherbyte 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、<b>bpdu</b> キーワードが対象トラフィックに一致しなくなります。<b>dsap 0x42</b> に対して <b>bpdu</b> ルールを書き換えます。</p> <p>次のコマンドが変更されました。 <b>access-list etherbyte</b></p>

機能名	リリース	説明
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)	<p>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。</p> <p>次のコマンドが変更されました。 <b>access-group</b>、<b>access-list ethertype</b></p>
EtherType アクセス制御リストの変更。	9.9(1)	<p>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。</p> <p>次のコマンドが変更されました：<b>access-list ethertype</b> キーワード <b>eii-ipx</b> および <b>dsap {bpdu   ipx   isis   raw-ipx}</b> が追加されました。<b>capture ethernet-typeipx</b> キーワードはサポートされなくなりました。</p>

