CHAPTER 20

拡張アクセス コントロール リストの追加

この章では、拡張アクセス コントロール リスト（ACL）を設定する方法について説明します。次の項で構成されています。

拡張 ACL に関する情報

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。1 つの拡張 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。各 ACE では、検出するトラフィックの送信元と宛先が指定されます。**access-list** コマンド内でパラメータを指定することも、オブジェクトまたはオブジェクト グループを作成して ACL の中で使用することもできます。

ACE 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 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。

ACE の順序は重要です。セキュリティ アプライアンスは、パケットを転送するかドロップするかを決定するときに、パケットが各 ACE に該当するかどうかを調べます。このときの順序は、エントリがリストされている順です。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は、残りのステートメントはチェックされません。

ACE を非アクティブ状態にすることで、ACE をディセーブルにできます。

NAT と ACL

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、必ず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。

（注）　ACL の移行に関する情報については、『*Cisco ASA 5500 Migration to Version 8.3 and Later*』を参照してください。

実際の IP アドレスを使用する機能

次のコマンドと機能では、実際の IP アドレスが ACL の中で使用されます。

- **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

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 は引き続き、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

アクセス リストのアクティベーションのスケジュール設定に関する情報

ACE に時間範囲を適用することで、アクセス リストの各 ACE が、1 日および週の特定の時刻にアクティブになるようにスケジュールを設定できます。

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。

拡張 ACL 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

ガイドラインと制限事項

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。

IDFW、FQDN、TrustSec の ACL をサポートしない機能

次の機能は ACL を使用しますが、IDFW、FQDN、または TrustSec の値が指定されている ACL を受け入れることができません。

- **route-map** コマンド
- 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

その他のガイドラインと制限事項

- ヒント：ACL の名前を大文字で入力すると、コンフィギュレーションの中で見つけやすくなります。ACL には、インターフェイスを表す名前（たとえば INSIDE）を付けることも、作成した目的を表す名前（たとえば NO_NAT や VPN）を付けることもできます。
- 通常、プロトコルには **ip** キーワードを指定しますが、他のプロトコルも受け入れられます。プロトコル名のリストについては、「プロトコルとアプリケーション」（P.B-11）を参照してください。
- TCP プロトコルまたは UDP プロトコルの場合に限り、送信元ポートおよび宛先ポートを指定できます。使用できるキーワードおよび予約済みポート割り当てのリストについては、「TCP ポートと UDP ポート」（P.B-12）を参照してください。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。

- 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。

デフォルト設定

表 20-1 に、拡張 ACL パラメータのデフォルト設定値を示します。

表 20-1　デフォルトの拡張 ACL パラメータ

パラメータ	デフォルト
ACE logging	ACE ロギングは、拒否されたパケットについてシステム ログ メッセージ 106023 を生成します。拒否されたパケットをログに記録するには、deny ACE が存在している必要があります。
log	**log** キーワードが指定されている場合、システム ログ メッセージ 106100 のデフォルトの重大度は 6（情報）で、デフォルトの間隔は 300 秒です。

拡張 ACL の設定

この項では、さまざまなタイプの ACE を ACL に追加する方法を説明します。説明する項目は次のとおりです。

- 「IP アドレスまたは完全修飾ドメイン名ベース ポリシーのための ACE の追加」（P.20-4）
- 「TCP または UDP ベース ポリシーのための ACE の追加（ポート指定あり）」（P.20-7）
- 「ICMP ベース ポリシーのための ACE の追加（ICMP タイプの指定あり）」（P.20-8）
- 「ユーザ ベース ポリシーのための ACE の追加（アイデンティティ ファイアウォール）」（P.20-9）
- 「セキュリティ グループ ベース ポリシーのための ACE の追加（TrustSec）」（P.20-10）
- 「ACL へのコメントの追加」（P.20-11）

IP アドレスまたは完全修飾ドメイン名ベース ポリシーのための ACE の追加

この項では、トラフィックを、IP アドレスまたは完全修飾ドメイン名（FQDN）に基づいて制御します。1 つの ACL は、同じ ACL ID 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。ACL を作成するには、まず ACE を 1 つ作成し、リスト名を適用します。エントリが 1 つだけの ACL もリストと見なされますが、リストには複数の ACE を追加できます。

前提条件

（任意）「ネットワーク オブジェクトとグループの設定」（P.18-2）に従ってネットワーク オブジェクトまたはオブジェクト グループを作成します。オブジェクトには、1 つの IP アドレス（ホスト、サブネット、または範囲）または FQDN を入れることができます。オブジェクト グループには、複数のオブジェクトまたはインライン エントリが含まれます。

ガイドライン

ACE を削除するには、**no access-list** コマンドを、コンフィギュレーションに表示されるコマンド構文のすべての文字列とともに入力します。ACL 全体を削除するには、**clear configure access-list** コマンドを使用します。

手順の詳細

コマンド	目的
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**]] [**inactive** | **time-range** *time_range_name*] **例：** `hostname(config)# access-list ACL_IN extended permit ip any any`	IP アドレスまたは FQDN ポリシーのための ACE を追加します。 • 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** キーワードは、条件が一致した場合にパケットを許可します。 • 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。TCP、UDP、または ICMP のサービス オブジェクトには、プロトコル*に加えて*、送信元や宛先のポートまたは ICMP タイプとコードも入れることができます。 – **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。 – *dest_ip_address mask*：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 any6 トラフィックを表します。 – **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。 • ロギング：**log** 引数では、ネットワーク アクセスに関して ACE に一致するパケットアクティブが見つかったとき（**access-group** コマンドで ACL が適用されます）のロギング オプションを設定します。 • アクティベーション：ACE をアクティブにする時間範囲を非アクティブにするか、またはイネーブルにします。時間範囲の定義方法については、**time-range** コマンドを参照してください。

TCP または UDP ベース ポリシーのための ACE の追加（ポート指定あり）

この項では、トラフィックを、IP アドレスまたは完全修飾ドメイン名（FQDN）および TCP または UDP ポートに基づいて制御します。1 つの ACL は、同じ ACL ID 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。ACL を作成するには、まず ACE を 1 つ作成し、リスト名を適用します。エントリが 1 つだけの ACL もリストと見なされますが、リストには複数の ACE を追加できます。

前提条件

- （任意）「ネットワーク オブジェクトとグループの設定」（P.18-2）に従ってネットワーク オブジェクトまたはオブジェクト グループを作成します。オブジェクトには、1 つの IP アドレス（ホスト、サブネット、または範囲）または FQDN を入れることができます。オブジェクト グループには、複数のオブジェクトまたはインライン エントリが含まれます。
- （任意）「サービス オブジェクトとサービス グループの設定」（P.18-5）に従ってサービス オブジェクトまたはグループを作成します。

ガイドライン

ACE を削除するには、**no access-list** コマンドを、コンフィギュレーションに表示されるコマンド構文のすべての文字列とともに入力します。ACL 全体を削除するには、**clear configure access-list** コマンドを使用します。

手順の詳細

コマンド	目的
access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} {**tcp** | **udp**} *source_address_argument* [*port_argument*] *dest_address_argument* [*port_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] **例：** `hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www`	IP アドレスまたは FQDN のポリシーのための ACE と、任意指定の TCP または UDP ポートを追加します。共通キーワードおよび引数については、「IP アドレスまたは完全修飾ドメイン名ベース ポリシーのための ACE の追加」（P.20-4）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。 *port_argument* では、送信元と宛先の一方または両方のポートを指定します。使用可能な引数は次のとおりです。 • *operator port*：*operator* は次のいずれかです。 – **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ときは、ポート番号を 2 つ指定します。たとえば、次のように指定します。 `range 100 200` *port* には、TCP または UDP ポートの番号（整数）または名前を指定できます。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** 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。

ICMP ベース ポリシーのための ACE の追加（ICMP タイプの指定あり）

この項では、トラフィックを、IP アドレスまたは完全修飾ドメイン名（FQDN）および ICMP タイプに基づいて制御します。1 つの ACL は、同じ ACL ID 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。ACL を作成するには、まず ACE を 1 つ作成し、リスト名を適用します。エントリが 1 つだけの ACL もリストと見なされますが、リストには複数の ACE を追加できます。

前提条件

- （任意）「ネットワーク オブジェクトとグループの設定」（P.18-2）に従ってネットワーク オブジェクトまたはオブジェクト グループを作成します。オブジェクトには、1 つの IP アドレス（ホスト、サブネット、または範囲）または FQDN を入れることができます。オブジェクト グループには、複数のオブジェクトまたはインライン エントリが含まれます。
- （任意）「ICMP グループの設定」（P.18-10）に従って、ICMP グループを作成します。

ガイドライン

ACE を削除するには、**no access-list** コマンドを、コンフィギュレーションに表示されるコマンド構文のすべての文字列とともに入力します。ACL 全体を削除するには、**clear configure access-list** コマンドを使用します。

手順の詳細

コマンド	目的
access-list *access_list_name* [**line** *line_number*] **extended** {**deny** | **permit**} **icmp** *source_address_argument dest_address_argument* [*icmp_argument*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]] [**inactive** | **time-range** *time_range_name*] **例：** `hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1`	IP アドレスまたは FQDN のポリシーのための ACE と、任意指定の TCP または UDP ポートを追加します。共通キーワードおよび引数については、「IP アドレスまたは完全修飾ドメイン名ベース ポリシーのための ACE の追加」（P.20-4）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。 *icmp_argument* では、ICMP タイプおよび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す。 • **object-group** *icmp_grp_id*：**object-group icmp** コマンドを使用して作成された ICMP オブジェクト グループを指定します。

ユーザ ベース ポリシーのための ACE の追加（アイデンティティ ファイアウォール）

アイデンティティ ファイアウォール機能を設定する場合は、ユーザ アイデンティティに基づいてトラフィックを制御できます。

前提条件

IDFW をイネーブルにするには、第 39 章「アイデンティティ ファイアウォールの設定」を参照してください。

手順の詳細

コマンド	目的
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**]] [**inactive** | **time-range** *time_range_name*] **例：** `hostname(config)# access-list v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0`	IP アドレスまたは FQDN のポリシーのための ACE と、任意指定のユーザ名やグループを追加します。共通キーワードおよび引数については、「IP アドレスまたは完全修飾ドメイン名ベース ポリシーのための ACE の追加」（P.20-4）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。 *user_argument* はアイデンティティ ファイアウォール機能とともに使用します。送信元アドレスに加えて、トラフィックを検出する条件となるグループまたはユーザを指定します。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。**any** を指定すると、ユーザ クレデンシャルを持つすべてのユーザが対象となり、**none** を指定するとユーザ クレデンシャルを持たないユーザが対象となります。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。 **（注）** 左にある構文には示されていませんが、TrustSec セキュリティ グループ引数も使用できます。

セキュリティ グループ ベース ポリシーのための ACE の追加（TrustSec）

Cisco TrustSec 機能を設定する場合は、セキュリティ グループに基づいてトラフィックを制御できます。

前提条件

TrustSec をイネーブルにするには、第 40 章「Cisco TrustSec と統合するための ASA の設定」を参照してください。

手順の詳細

コマンド	目的
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 v1 extended permit ip user LOCAL\idfw any 10.0.0.0 255.255.255.0`	IP アドレスまたは FQDN のポリシーのための ACE と、任意指定のセキュリティ グループを追加します。共通キーワードおよび引数については、「IP アドレスまたは完全修飾ドメイン名ベース ポリシーのための ACE の追加」（P.20-4）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。 *security_group_argument* は TrustSec 機能とともに使用します。送信元や宛先のアドレスに加えて、トラフィックを検出する条件となるセキュリティ 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。 **（注）**　左にある構文には示されていませんが、アイデンティティ ファイアウォール ユーザ引数も使用できます。

ACL へのコメントの追加

エントリに関するコメントを ACL に含めることができます。コメントを追加すると、ACL が理解しやすくなります。

最後に入力した **access-list** コマンドの後にコメントを追加するには、次のコマンドを入力します。

手順の詳細

コマンド	目的
access-list *access_list_name* **remark** *text* **例：** `hostname(config)# access-list OUT remark - this is the inside admin address`	最後に入力した access-list コマンドの後にコメントを追加します。 テキストは 100 文字まで指定できます。テキストの先頭にスペースを入力できます。末尾のスペースは無視されます。 **access-list** コマンドの前にコメントを入力すると、そのコメントが ACL の最初の行となります。 **no access-list** *access_list_name* コマンドを使って ACL を削除すると、コメントもすべて削除されます。

例

各 ACE の前にコメントを追加できます。コメントは ACL 内のその位置に表示されます。コメントの開始位置にダッシュ（-）を入力すると、ACE と区別しやすくなります。

```
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
```

拡張 ACL のモニタリング

拡張 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。

コマンド	目的
show access-list	ACE を番号順に表示します。
show running-config access-list	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。

拡張 ACL の設定例

この項は、次の内容で構成されています。

拡張 ACL（オブジェクトなし）の設定例

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 の例では、192.168.1.0/24 のホストが 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アクセス リストでは、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 ACL を実装するには、**time-range** コマンドを使用して、週および 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 ACL にバインドします。次の例では、「Sales」という名前の ACL を「New_York_Minute」という名前の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
```

拡張 ACL（オブジェクトを使用）の設定例

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-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
```

関連情報

多くの機能が ACL を使用します。ACL をインターフェイスに適用します。詳細については、「アクセス ルールの設定」（P.42-8）を参照してください。

拡張 ACL の機能履歴

表 20-2 に、この機能のリリース履歴を示します。

表 20-2　拡張 ACL の機能履歴

機能名	リリース	機能情報
拡張 ACL の有無	7.0(1)	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、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。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 ICMP タイプ（ICMP の場合）も挿入できます。 **access-list extended** コマンドが導入されました。
実際の IP アドレス	8.3(1)	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、必ず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。詳細については、「実際の IP アドレスを使用する機能」（P.20-2）を参照してください。
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 20-2　拡張 ACL の機能履歴 （続き）

機能名	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。