CHAPTER 21

EtherType アクセス リストの追加

この章では、EtherType アクセス リストを設定する方法について説明します。次の項目を取り上げます。

EtherType アクセス リストに関する情報

EtherType アクセス リストは、EtherType を指定する 1 つまたは複数の Access Control Entry（ACE; アクセス コントロール エントリ）で構成されます。EtherType ルールは、16 ビットの 16 進数値で指定されるすべての EtherType および選択されたトラフィック タイプを制御します。詳細については、「サポートされている EtherType およびその他のトラフィック」（P.42-6）を参照してください。

EtherType アクセス リストを使用したアクセス ルールの作成については、第 42 章「アクセス ルールの設定」を参照してください。

EtherType アクセス リストのライセンス要件

次の表に、この機能のライセンス要件を示します。

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

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 モードで使用できます。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードでだけ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。

その他のガイドラインと制限事項

EtherType アクセス リストには、次のガイドラインと制限事項が適用されます。

- 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。
- 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、アクセス リストでは処理されません。
- サポート対象のトラフィックの詳細については、「サポートされている EtherType およびその他のトラフィック」（P.42-6）を参照してください。

デフォルト設定

アクセス リスト 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、拒否パケットが存在している必要があります。

アクセス リストにロギングを設定する場合、システム ログ メッセージ 106100 に対するデフォルトの重大度は 6（情報）です。

EtherType アクセス リストの設定

この項は、次の内容で構成されています。

EtherType アクセス リストの設定のタスク フロー

アクセス リストを作成して実装するには、次のガイドラインを使用します。

ステップ 1　「EtherType アクセス リストの追加」（P.21-3）に示すように、ACE を追加し、アクセス リスト名を適用して、アクセス リストを作成します。

ステップ 2　アクセス リスト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）。

EtherType アクセス リストの追加

EtherType に基づいてトラフィックを制御するアクセス リストを設定するには、次の手順を実行します。

手順の詳細

コマンド	目的
access-list *access_list_name* **ethertype** {**deny** | **permit**} {**ipx** | **bpdu** | **mpls-unicast** | **mpls-multicast** | **any** | *hex_number*} **例：** `hostname(config)# hostname(config)#` **`access-list ETHER ethertype permit ipx`**	EtherType ACE を追加します。 *access_list_name* 引数には、アクセス リストの名前または番号を示します。アクセス リスト名を指定すると、アクセス リストの末尾に ACE が追加されます。*access_list_name* は、大文字で入力します。これにより、コンフィギュレーションで名前が見つけやすくなります。アクセス リストには、インターフェイスを表す名前（INSIDE など）や、目的を表す名前（MPLS や PIX など）を付けることができます。 **permit** キーワードは、条件が一致した場合にアクセスを許可します。**deny** はアクセスを拒否します。 **ipx** キーワードは、IPX へのアクセスを指定します。 **bpdu** キーワードは、デフォルトで許可されているブリッジ プロトコル データ ユニットへのアクセスを指定します。 **deny** キーワードは、条件が一致した場合にアクセスを拒否します。EtherType アクセス リストに deny all が設定されている場合、すべてのイーサネット フレームが廃棄されます。その場合でも、オートネゴシエーションなどの物理プロトコル トラフィックだけは許可されます。 **mpls-multicast** キーワードは、MPLS マルチキャストへのアクセスを指定します。 **mpls-unicast** キーワードは、MPLS ユニキャストへのアクセスを指定します。 **any** キーワードは、任意のトラフィックへのアクセスを指定します。 *hex_number* 引数は、0x600 以上の 16 ビット 16 進数値で指定できる任意の EtherType です （EtherType のリストについては、http://www.ietf.org/rfc/rfc1700.txt で、RFC 1700「Assigned Numbers」を参照してください）。 **（注）** EtherType 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。

例

次のサンプル アクセス リストでは、Inside インターフェイスで発信される一般的なトラフィックが許可されます。

```
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
```

アクセス リストへのコメントの追加

拡張アクセス リスト、EtherType アクセス リスト、IPv6 アクセス リスト、標準アクセス リスト、Webtype アクセス リストを含む任意のアクセス リストに、エントリについてのコメントを追加できます。コメントにより、アクセス リスト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。

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。 いずれかの **access-list** コマンドの前にコメントを入力すると、コメントはアクセス リストの最初の行に表示されます。 **no access-list** *access_list_name* コマンドを使用してアクセス リストを削除すると、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。コメントはその場所でアクセス リストに表示されます。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
```

次の作業

アクセス リスト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）。

EtherType アクセス リストのモニタリング

EtherType アクセス リストをモニタするには、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	アクセス リスト エントリを番号で表示します。
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。

EtherType アクセス リストの設定例

次の例は、EtherType アクセス リストを設定する方法を示しています。

次のアクセス リストでは、一部の EtherType は ASA を通過することが許可されますが、IPX は拒否されます。

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

次のアクセス リストでは、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
```

EtherType アクセス リストの機能履歴

表 21-1 に、この機能のリリース履歴を示します。

表 21-1　EtherType アクセス リストの機能履歴

機能名	リリース	機能情報
EtherType アクセス リスト	7.0(1)	EtherType アクセス リストは、EtherType に基づいてトラフィックを制御します。 この機能および **access-list ethertype** コマンドが導入されました。