



# アクセス コントロール リストのロギングの設定

この章では、拡張 ACL および Web-type ACL の ACL ロギングを設定する方法と、拒否フローを管理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。

- 「ACL ロギングの設定」 (P.23-1)
- 「拒否フローの管理」 (P.23-5)

## ACL ロギングの設定

この項は、次の内容で構成されています。

- 「ACL アクティビティのロギングに関する情報」 (P.23-1)
- 「ACL ロギングのライセンス要件」 (P.23-2)
- 「ガイドラインと制限事項」 (P.23-2)
- 「デフォルト設定」 (P.23-3)
- 「ACL ロギングの設定」 (P.23-3)
- 「ACL のモニタリング」 (P.23-4)
- 「ACL ロギングの設定例」 (P.23-4)
- 「ACL ロギングの機能履歴」 (P.23-5)

## ACL アクティビティのロギングに関する情報

デフォルトでは、拡張 ACE または Webtype ACE でトラフィックが定義されている場合、ASA は、拒否されたパケットごとに次の形式の syslog メッセージ 106023 を生成します。

```
%ASA|PIX-4-106023: Deny protocol src [interface_name:source_address/source_port] dst  
interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_id
```

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場合があります。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 ACE 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。または、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。



(注)

ログギング メッセージは、ACL の ACE によってのみ生成されます。ACL の末尾にある暗黙的な拒否によって生成されることはありません。拒否されたすべてのトラフィックによってメッセージが生成されるようにする場合は、次の例に示すように、手動で ACL の末尾に暗黙的な ACE を追加します。

```
hostname(config)# access-list TEST deny ip any any log
```

拡張 **access-list** コマンドの末尾の **log** オプションを使用すると、次の動作を設定できます。

- メッセージ 106023 の代わりにメッセージ 106100 をイネーブルにする。
- すべてのログギングをディセーブルにする。
- メッセージ 106023 を使用するデフォルト ログギングに戻る。

syslog メッセージ 106100 では、次の形式が使用されます。

```
%ASA|PIX-n-106100: access-list acl_id {permitted | denied} protocol
interface_name/source_address(source_port) -> interface_name/dest_address(dest_port)
hit-cnt number ({first hit | number-second interval})
```

メッセージ 106100 のログ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、指定された時間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。

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。ログギングフローの数を制限するには、「拒否フローの管理」(P.23-5) を参照してください。

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グギングされ、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グギングされ、拒否されたパケットはすべてログギングされません。

この syslog 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。

## ACL ログギングのライセンス要件

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 モードおよび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

ACE ロギングによって、拒否されたパケットに対して `syslog` メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、`deny` ACE が存在する必要があります。

## デフォルト設定

表 23-1 に、拡張 ACL パラメータのデフォルト設定値を示します。

表 23-1 デフォルトの拡張 ACL パラメータ

パラメータ	デフォルト
<code>log</code>	<code>log</code> キーワードを指定する場合、 <code>syslog</code> メッセージ 106100 のデフォルト レベルは 6 (通知) になり、デフォルトの間隔は 300 秒になります。

## ACL ロギングの設定

この項では、ACL ロギングの設定方法について説明します。



(注)

ACL コマンドの完全な構文については、「[拡張 ACL の設定](#)」(P.19-4) および「[Web-type ACL の使用](#)」(P.22-2) を参照してください。

ACE のロギングを設定するには、次のコマンドを入力します。

コマンド	目的
<pre>access-list access_list_name [extended] {deny   permit}...[log [[level] [interval secs]   disable   default]]</pre> <p><b>例 :</b></p> <pre>hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600</pre>	<p>ACE のロギングを設定します。</p> <p><b>access-list access_list_name</b> 構文では、ロギングを設定する ACL を指定します。</p> <p><b>extended</b> オプションは、ACE を追加します。</p> <p><b>deny</b> キーワードは、条件が一致した場合にパケットを拒否します。一部の機能 (NAT など) では、拒否 ACE を許可しません (詳細については、ACL を使用する各機能のコマンド マニュアルを参照してください)。</p> <p><b>permit</b> 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。</p> <p>引数を指定せずに <b>log</b> オプションを入力すると、<b>syslog</b> 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。次のオプションを参照してください。</p> <ul style="list-style-type: none"> <li>• <b>level</b> : 0 ~ 7 の重大度。デフォルトは 6 です。</li> <li>• <b>interval secs</b> : <b>syslog</b> 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、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。</li> <li>• <b>disable</b> : すべての ACL ロギングをディセーブルにします。</li> <li>• <b>default</b> : メッセージ 106023 のロギングをイネーブルにします。この設定は、<b>log</b> オプションがない場合と同じです。</li> </ul> <p>コマンド オプションの詳細については、『<i>Cisco Security Appliance Command Reference</i>』の <b>access-list</b> コマンドを参照してください。</p>

## 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。

コマンド	目的
<b>show access-list</b>	ACL エントリを番号で表示します。
<b>show running-config access-list</b>	現在実行中の ACL コンフィギュレーションを表示します。

## ACL ロギングの設定例

ここでは、ACL ロギングのサンプル コンフィギュレーションを示します。

次の ACL を設定できます。

```
hostname(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval 600
hostname(config)# access-list outside-acl permit ip host 2.2.2.2 any
hostname(config)# access-list outside-acl deny ip any any log 2
hostname(config)# access-group outside-acl in interface outside
```

パケットが **outside-acl** の最初の ACE によって許可された場合、ASA は次の **syslog** メッセージを生成します。

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

この接続の 20 個の後続パケットは、外部インターフェイスに到達しますが、そのトラフィックを ACL でチェックする必要はなく、ヒット数も増加しません。

指定した 10 分間のうちに同じホストによる接続が 1 つ以上開始された場合（かつ、送信元ポートと宛先ポートが変わっていない場合）、ヒット数は 1 増加し、10 分間の終わりに次の **syslog** メッセージが表示されます。

```
%ASA|PIX-7-106100: access-list outside-acl permitted tcp outside/1.1.1.1(12345)->
inside/192.168.1.1(1357) hit-cnt 2 (600-second interval)
```

パケットが 3 番目の ACE によって拒否された場合、ASA は次の **syslog** メッセージを生成します。

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 1 (first hit)
```

5 分間（デフォルト）のうちにさらに 20 回の試行が行われた場合、5 分間の終わりに次の **syslog** メッセージが表示されます。

```
%ASA|PIX-2-106100: access-list outside-acl denied ip outside/3.3.3.3(12345) ->
inside/192.168.1.1(1357) hit-cnt 21 (300-second interval)
```

## ACL ログギングの機能履歴

表 23-2 に、この機能のリリース履歴を示します。

表 23-2 ACL ログギングの機能履歴

機能名	リリース	機能情報
ACL ログギング	7.0(1)	syslog メッセージ 106100 を使用するログギングをイネーブルにできます。このメッセージは各 ACE 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。 <b>access-list</b> コマンドが導入されました。
ACL タイムスタンプ	8.3(1)	ASA から、アクセス規則に対する最後のヒットのタイムスタンプが報告されます。

## 拒否フローの管理

この項は、次の内容で構成されています。

- 「拒否フローの管理に関する情報」 (P.23-6)
- 「拒否フローの管理のライセンス要件」 (P.23-6)
- 「ガイドラインと制限事項」 (P.23-6)
- 「拒否フローの管理」 (P.23-7)
- 「拒否フローのモニタリング」 (P.23-7)
- 「拒否フローの管理の機能履歴」 (P.23-8)

## 拒否フローの管理に関する情報

メッセージ 106100 のログिंग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、指定された時間内で受信したパケットの数を追跡します。ASA では、ACE 用のログングフローを最大 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グング用の新しい拒否フローを作成しません。

たとえば、DoS 攻撃（サービス拒絶攻撃）が開始された場合、ASA は大量の拒否フローを短時間のうちに作成する可能性があります。拒否フロー数を制限することにより、メモリおよび CPU リソースが無制限に消費されなくなります。

拒否フローの最大数に達すると、ASA は次のような syslog メッセージ 106100 を発行します。

```
%ASA|PIX-1-106101: The number of ACL log deny-flows has reached limit (number).
```

**access-list alert-interval** コマンドは、syslog メッセージ 106001 を生成する時間間隔を設定します。syslog メッセージ 106001 は、ASA が拒否フローの最大数に達したことを警告するものです。拒否フローの最大数に達した場合、最後の 106001 メッセージが生成されてから 6 秒以上経過すると、別の syslog メッセージ 106001 が生成されます。

## 拒否フローの管理のライセンス要件

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 モードおよび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

ASA では、同時拒否フロー数に対してだけ制限が設定されます（許可フローには設定されません）。

## デフォルト設定

表 23-1 に、拒否フローの管理のデフォルトの設定を示します。

表 23-3 拒否フローの管理のデフォルト パラメータ

パラメータ	デフォルト
<i>numbers</i>	<i>numbers</i> 引数には、拒否フローの最大数を指定します。デフォルトは 4096 です。
<i>secs</i>	<i>secs</i> 引数には、syslog メッセージ間の時間を秒単位で指定します。デフォルトは 300 です。

## 拒否フローの管理

拒否フローの最大数の設定、および拒否フロー アラート メッセージ (106100) 間の間隔の設定には、次のコマンドを入力します。

コマンド	目的
<code>access-list deny-flow-max number</code>  例： hostname(config)# access-list deny-flow-max 3000	拒否フローの最大数を設定します。  <i>numbers</i> 引数には、最大数を指定します。指定可能な範囲は 1 ~ 4096 です。デフォルトは 4096 です。

拒否フローが最大数に達したことを示す syslog メッセージ (番号 106101) 間の時間間隔を設定するには、次のコマンドを入力します。

コマンド	目的
<code>access-list alert-interval secs</code>  例： hostname(config)# access-list alert-interval 200	syslog メッセージ間の時間を秒単位で設定します。  <i>secs</i> 引数には、拒否フローが最大数に達したことを示すメッセージ間の時間間隔を指定します。有効な値は 1 ~ 3600 秒です。デフォルトは 300 秒です。

## 拒否フローのモニタリング

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。

コマンド	目的
<code>show access-list</code>	アクセス リスト エントリを番号で表示します。
<code>show running-config access-list</code>	現在実行中の ACL コンフィギュレーションを表示します。

## 拒否フローの管理の機能履歴

表 23-2 に、この機能のリリース履歴を示します。

表 23-4 拒否フローの管理の機能履歴

機能名	リリース	機能情報
拒否フローの管理	7.0(1)	拒否フローの最大数と拒否フロー アラート メッセージ間の間隔を設定できます。 <b>access-list deny-flow</b> および <b>access-list alert-interval</b> コマンドが導入されました。