



# ACL 管理性を使用した IP アクセス リスト データの表示及びクリア

このモジュールでは、IP アクセス リスト内のエン트리および各エントリに一致したパケットの数の表示方法について説明します。ユーザは、ACL 管理性機能を使用して、グローバルに、または、インターフェイスごとのおよび着信または発信トラフィック方向ごとにこれらの統計情報を取得できます。ネットワークデバイスのさまざまなインターフェイス上の着信または発信トラフィックパターンの詳細表示は、特定のインターフェイスへの攻撃に対してデバイスの保護に役立ちます。このモジュールでは、また、アクセス リスト エントリに一致するパケットの数が 0 から再開されるカウンタをクリアする方法について説明します。

- [機能情報の確認 \(1 ページ\)](#)
- [ACL 管理性を使用した IP アクセス リスト データの表示及びクリアに関する情報 \(2 ページ\)](#)
- [IP アクセス リスト データを表示およびクリアする方法 \(2 ページ\)](#)
- [ACL 管理性を使用した IP アクセス リスト データの表示及びクリアのための設定例 \(5 ページ\)](#)
- [その他の参考資料 \(7 ページ\)](#)
- [IP アクセス リスト情報の表示およびカウンタのクリアに関する機能情報 \(8 ページ\)](#)

## 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

# ACL 管理性を使用した IP アクセス リスト データの表示 及びクリアに関する情報

## ACL 管理性の利点

Cisco IOS リリース 12.4(6)T 以前では、Cisco IOS ソフトウェア内の ACL インフラストラクチャは、ACL 内の各 ACE に対するグローバル統計情報を維持するだけでした。この方法によって、1 つの ACL が複数のインターフェイスに適用される場合、維持された ACE 統計情報は、その ACL が適用されるすべてのインターフェイス上で一致（ヒット）する着信および発信パケットの合計数となります。

ただし、ACE の統計情報がインターフェイスごとおよび着信または発信トラフィック方向ごとに維持される場合、ネットワークデバイスの様々なインターフェイスにおける着信および発信トラフィックパターンの特定の詳細および ACE の効率性を表示できます。このような情報は、特定のインターフェイス上に着信する攻撃に対するデバイスの保護に役立ちます。

## インターフェイス レベルの ACL 統計情報のサポート

Cisco IOS リリース 12.4(6)T により、Cisco IOS ソフトウェア内の ACL インフラストラクチャは、インターフェイスごとの、および ACL に対する着信または発信トラフィック方向ごとの ACE 統計情報の保守、表示、およびクリアをサポートするよう、拡張されます。このサポートは、『インターフェイス レベルの統計情報のサポート』と呼ばれます。



(注) 同じアクセス グループ ACL が他の機能によっても使用された場合、保持されているインターフェイス統計情報は、パケット一致が他の機能によって検出される際に、更新されません。この例では、ACL のために維持される、すべてのインターフェイス レベル統計情報の合計は、その ACL に対するグローバル統計情報を集約していない場合があります。

## IP アクセス リスト データを表示およびクリアする方法

この項には、IP アクセスリストおよび各リストに一致（ヒット）するパケットの数を表示し、IP アクセス リスト カウンタをクリアするための次の手順が含まれます。



- (注) 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。詳細については、「IP アクセスリストの概要」の「IP アクセスリストロギング」を参照して下さい。

## グローバル IP ACL 統計情報の表示

ルータ上のすべての IP アクセス リストと一致したパケット数を表示するには、次の作業を行います。

### 手順の概要

1. **enable**
2. **show ip access-list** [*access-list-number* | *access-list-name*]

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： <pre>Router&gt; enable</pre>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>show ip access-list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ] 例： <pre>Router# show ip access-list limited</pre>	IP アクセス リスト情報を表示します。 <ul style="list-style-type: none"> <li>• この例では、「名前付きアクセスリストを指定します」を使用するすべてのインターフェイスの統計情報を表示します。</li> </ul>

## インターフェイス レベル IP ACL 統計情報の表示

このセクションでは、インターフェイスに ACL 用の着信または発信トラフィック方向ごとの IP ACE の統計情報を表示する方法について説明します。この機能は、ACL 管理性と呼ばれています。



- (注)
- ACL 管理性サポート対象：
    - 非分散型プラットフォーム ソフトウェアでスイッチングされるだけです。
    - 標準と拡張の静的に設定された ACL と脅威緩和サービス (TMS) ダイナミック ACE です。
  - ACL 管理性サポート対象外：
    - ファイアウォールおよび認証プロキシなど、再帰かつユーザ設定のダイナミック ACL およびダイナミック ACE ブロック。
    - 仮想テンプレートおよび仮想アクセス インターフェイス。

&gt;

### 手順の概要

1. **enable**
2. **show ip access-list interface interface-name [in|out]**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： <pre>Router&gt; enable</pre>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>show ip access-list interface interface-name [in out]</b> 例： <pre>Router# show ip access-list interface FastEthernet 0/0 in</pre>	IP アクセス リスト情報を表示します。 <ul style="list-style-type: none"> <li>• この例では、FastEthernet インターフェイスに着信するトラフィックに関する統計情報を表示します。</li> <li>• ACL のインターフェイス レベルの統計情報に関するデバッグ情報を表示するには、<b>debug ip access-list intstats</b> コマンドを使用します。</li> </ul>

## アクセス リスト カウンタのクリア

システムは、アクセスリストの各行に一致 (ヒット) するパケットの数を数えます。カウンタは、**show access-lists EXEC** コマンドで表示されます。この作業を行い、アクセスリストのカウンタをクリアします。アクセスリストに一致するゼロから始まるパケットの数を決定しようとする場合に、これを行うことができます。

## 手順の概要

1. **enable**
2. **clear ip access-list counters** {*access-list-number* | *access-list-name*}

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Router> enable	特権 EXEC モードをイネーブルにします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>clear ip access-list counters</b> { <i>access-list-number</i>   <i>access-list-name</i> } 例：  Router# clear access-list counters corpmark	IP アクセス リストのカウンタをクリアします。

## ACL 管理性を使用した IP アクセス リスト データの表示及びクリアのための設定例

### グローバル IP ACL 統計情報を表示する例

次に、ACL 150 のグローバル統計情報を表示する例を示します。

```
Router# show ip access-list 150

Extended IP access list 150
 10 permit ip host 10.1.1.1 any (3 matches)
 30 permit ip host 10.2.2.2 any (27 matches)
```

### 入力統計情報を表示する例

次の例は、アクセスリスト 150（ACL 番号）に関連付けられているインターフェイス FastEthernet 0/1 から集めた着信パケットの統計情報を示しています。

```
Router#
 show ip access-list interface FastEthernet 0/1 in
Extended IP access list 150 in
 10 permit ip host 10.1.1.1 any (3 matches)
 30 permit ip host 10.2.2.2 any (12 matches)
```

## 出力統計情報を表示する例

次の例は、FastEthernet 0/0 インターフェイスから集めた出力パケットに関する統計情報を示しています。

```
Router#
show ip access-list interface FastEthernet 0/0 out
Extended IP access list myacl out
  5 deny ip any 10.1.0.0 0.0.255.255
 10 permit udp any any eq snmp (6 matches)
```

## 入出力統計情報を表示する例



(注) 方向を指定しないと、そのインターフェイスに適用された入出力 ACL が表示されます。

次の例の表示から集めた入出力統計情報は、FastEthernet 0/0 を実行します。

```
Router#
show ip access-list interface FastEthernet 0/0
Extended IP access list 150 in
 10 permit ip host 10.1.1.1 any
 30 permit ip host 10.2.2.2 any (15 matches)
Extended IP access list myacl out
  5 deny ip any 10.1.0.0 0.0.255.255
 10 permit udp any any eq snmp (6 matches)
```

## IP アクセスリスト用のグローバルおよびインターフェイス統計情報のクリアの例

次の例では、IP ACL 150 のグローバルおよびインターフェイスの統計情報をクリアします。

```
Router#
clear ip access-list counters 150
```

## すべての IP アクセス リスト用のグローバルおよびインターフェイス統計情報のクリアの例

次の例では、すべての IP ACL のグローバルおよびインターフェイスの統計情報をクリアします。

```
Router#
clear ip access-list counters
```

## その他の参考資料

### 関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『 <a href="#">Cisco IOS Master Commands List, All Releases</a> 』
セキュリティコマンド	『 <a href="#">Cisco IOS Security Command Reference</a> 』

### 標準

標準	タイトル
この機能がサポートする新しい規格または変更された規格はありません。	--

### MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFC

RFC	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

## テクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## IP アクセス リスト情報の表示およびカウンタのクリアに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 1: ACL 管理性を使用した IP アクセス リスト データの表示及びクリアのための機能情報

機能名	リリース	機能情報
ACL 管理性	Cisco IOS XE Release 3.9S	ACL 管理性機能により、ユーザは、インターフェイスおよびアクセス コントロール リスト (ACL) に対する入力や出力トラフィック方向ごとのアクセス コントロール エントリ (ACE) の統計情報を表示およびクリアすることができます。