# IP アクセス リストの作成とインターフェイスへの適用

IP アクセス リストには、ネットワークを保護し、Quality of Service（QoS）係数の設定や**debug** コマンド出力の制限などのセキュリティ以外の目標を達成する際に多数の利点があります。ここでは、標準、拡張、名前付き、および番号付き IP アクセス リストの作成方法について説明します。アクセス リストは、名前または番号で参照できます。標準アクセス リストは、IP パケットの送信元アドレスのみに基づいてフィルタできます。拡張アクセス リストは、IP パケットの送信元アドレス、宛先アドレス、および他のフィールドに基づいてフィルタできます。

アクセス リストの作成後に有効にするには、何かに適用する必要があります。このモジュールでは、アクセス リストをインターフェイスに適用する方法について説明します。ただし、アクセス リストにはその他にも多数の用途があり、このモジュールで言及していますが、他のモジュールでも説明しています。多様なテクノロジーについては、他のコンフィギュレーション ガイドを参照してください。



# IP アクセス リストの作成およびインターフェイスへの適用の制限

IPv4 および IPv6 アクセス コントロール リスト（ACL）を設定する場合、次の制限事項が適用されます。

- Application Control Engine（ACE）固有のカウンタは、サポートされていません。
- レイヤ 3 IPv4 および Ipv6 ACL は、同じインターフェイスではサポートされません。

- レイヤ 3 Ipv4 または IPv6 ACL が適用されているイーサネット フローポイント（EFP）またはトランク EFP インターフェイスでは、MAC ACL はサポートされていません。
- IPv4 および IPv6 ACL は、EFP インターフェイスでは現在サポートされていません。IPv4 および IPv6 ACL は、物理インターフェイス、ブリッジ ドメイン インターフェイスおよびポート チャネル インターフェイスでサポートされています。
- レイヤ 4 ポートの範囲と機能は、Ternary Content Addressable Memory（TCAM）に展開されます。IPv4 ACL によって、レイヤ 1K TCAM に制限され、レイヤ 2 ACL スケールは、1K TCAM エントリに制限されます。
- オブジェクトグループ ACL（IPv4 および IPv6 ACL）は、Cisco ISR プラットフォームでサポートされています。
- **any options** コマンドはサポートされていません。
- Cisco IOS XE Cupertino リリース 17.7.1 以降、ACL は、管理インターフェイス Gigabit 0 でサポートされています。

# IPアクセスリストの作成とインターフェイスへの適用に関する情報

## IP アクセス リストを作成する際に役立つヒント

- アクセスリストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙的な **deny** ステートメントによってアクセスに緊急の問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。permit がないと、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- パケットは、ACL の最初の ACE に一致します。したがって、**permit ip any any** はすべてのパケットに一致し、以降の ACE はすべて無視されます。
- すべてのアクセス リストは暗黙的な **deny** ステートメントで終了しますが、明示的な **deny** ステートメント（たとえば **deny ip any any**）の使用を推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny**

ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。

- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用すると、適切なエントリが削除されます。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 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。
- このヒントは、アクセスリストの配置に適用されます。リソースを保存しようとすると、インバウンドアクセスリストでは常にフィルタ条件を適用した後に、ルーティングテーブルの検索を行います。アウトバウンドアクセスリストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

# アクセス リストの注釈

任意のIPアクセスリストのエントリについて、コメントまたは注釈を含めることができます。アクセス リストの注釈は、アクセス リスト エントリの前後にあるオプションの注釈です。エントリの内容がわかるので、エントリの目的を解釈する必要はありません。各注釈の長さは 100 文字に制限されます。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。注釈を追加する場所には一貫性があるようにしてください。注釈が関連する **permit** ステートメントや**deny** ステートメントの前にある場合と後にある場合とが混在すると、ユーザーが混乱する可能性があります。

後続の **deny** ステートメントの機能を説明する注釈の例を次に示します。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.16.2.88 any eq telnet
```

# その他の IP アクセス リスト機能

標準または拡張アクセス リストを作成する基本手順以外に、次のようにアクセス リストを強化できます。これらの各方法の詳細については、『*Refining an IP Access List module*』を参照してください。

- 拡張アクセス リストの **permit** ステートメントまたは **deny** ステートメントを有効にする日時を指定し、アクセスリストを細かくし、絶対的または定期的な期間に限定することができます。

- 名前付きまたは番号付きアクセスリストの作成後は、エントリを追加したり、エントリの順序を変更したりできます（これはアクセスリストのシーケンス番号再割り当てとも呼ばれます）。
- パケットの非初期フラグメントについてフィルタすることで、パケットをフィルタするときにより細かい精度を達成できます。

# IPアクセス リストの作成とインターフェイスへの適用方法

ここでは、名前または番号を使用して、標準または拡張アクセス リストを作成する一般的な方法について説明します。アクセス リストには高い柔軟性があります。この作業では、単純に1つの **permit** コマンドと 1 つの **deny** コマンドを使用して、それぞれのコマンド構文を指定します。あとは、必要な **permit** および **deny** コマンドの数とその順序を決めるだけです。

（注） このモジュールの最初の 2 つの作業として、1 つのアクセス リストを作成します。適切に機能するように、アクセス リストを適用する必要があります。インターフェイスにアクセス リストを適用する場合は、「インターフェイスへのアクセス リストの適用」タスクを実行します。

## 送信元アドレスに基づいてフィルタする標準アクセス リストの作成

送信元アドレスのみに基づいてフィルタする場合、簡易な標準アクセス リストで十分です。標準アクセス リストには名前付きと番号付きという 2 種類があります。名前付きアクセス リストを使用すると、番号よりも直感的な名前を使用してアクセス リストを特定できます。また、番号付きアクセス リストよりもサポートする機能が多数です。

### 送信元アドレスに基づいてフィルタする名前付きアクセス リストの作成

送信元アドレスのみに基づいてフィルタする必要がある場合、標準の名前付きアクセス リストを使用します。この作業では、1 つの **permit** ステートメントと 1 つの **deny** ステートメントを使用しますが、使用する実際のステートメントとその順序は、フィルタまたは許可する内容によって変わります。フィルタリングの目標を達成するように、**permit** および **deny** ステートメントを定義します。

**ステップ 1** **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

**ステップ 2** **configure terminal**

**例**：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

**ステップ 3** **ip access-list standard** *name*

**例**：

```
Device(config)# ip access-list standard R&D
```

名前を使用して標準IPアクセス リストを定義し、標準名前付きアクセス リストのコンフィギュレーション モードを開始します。

**ステップ 4** **remark** *remark*

**例**：

```
Device(config-std-nacl)# remark deny Sales network
```

（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。

- 注釈はアクセス リスト エントリの前または後に指定できます。
- この例の注釈では、後続のエントリがインターフェイスに対するSalesネットワークのアクセスを拒否することをネットワーク管理者に示しています（このアクセス リストは後でインターフェイスに適用される想定です）。

**ステップ 5** **deny** {*source* [*source-wildcard*] | **any**} [**log**]

**例**：

```
Device(config-std-nacl)# deny 172.16.0.0 0.0.255.255 log
```

（任意）送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を拒否します。

- *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、*source source-wildcard* の代わりに、キーワード **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ネットワーク 172.16.0.0 のすべてのホストは、アクセス リストへの合格が拒否されます。
- この例では、送信元アドレスを明示的に拒否し、**log** キーワードを指定しているため、その送信元からのパケットが拒否されるとロギングされます。これは、ネットワークまたはホスト上の誰かがアクセスしようとしたことを通知する方法の 1 つです。

**ステップ 6** **remark** *remark*

例：

```
Device(config-std-nacl)# remark Give access to Tester's host
```

（任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。

- 注釈はアクセス リスト エントリの前または後に指定できます。
- この注釈は、後続のエントリがインターフェイスに対する Tester のホスト アクセスを許可することをネットワーク管理者に示します。

**ステップ 7** **permit** {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config-std-nacl)# permit 172.18.5.22 0.0.0.0
```

送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を許可します。

- 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。ただし、最初のエントリにする必要はありません。
- *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、*source source-wildcard* の代わりに、キーワード **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ホスト 172.18.5.22 がアクセス リストに合格できます。

**ステップ 8** アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。

明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。

**ステップ 9** **end**

例：

```
Device(config-std-nacl)# end
```

標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

**ステップ 10** **show ip access-list**

例：

```
Device# show ip access-list
```

（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

# 送信元アドレスに基づいてフィルタする番号付きアクセス リストの作成

送信元アドレスのみに基づいてフィルタする必要があり、名前付きアクセス リストを使用しない場合、標準の番号付きアクセス リストを設定します。

IP 標準アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。この作業では、1 つの **permit** ステートメントと 1 つの **deny** ステートメントを使用しますが、使用する実際のステートメントとその順序は、フィルタまたは許可する内容によって変わります。フィルタリングの目標を達成するように、**permit** および **deny** ステートメントを定義します。

**ステップ 1** **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

**ステップ 2** **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

**ステップ 3** **access-list** *access-list-number permit* {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0
```

送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を許可します。

- 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。ただし、最初のエントリにする必要はありません。
- 標準 IP アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。
- source-wildcard を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、source source-wildcard の代わりに、キーワード any を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ホスト 172.16.5.22 がアクセス リストに合格できます。

**ステップ 4** **access-list** *access-list-number* **deny** {*source* [*source-wildcard*] | **any**} [**log**]

例：

```
Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0
```

送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を拒否します。

- *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。
- 必要に応じて、*source source-wildcard* の代わりに、省略形 **any** を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
- この例では、ホスト 172.16.7.34 はアクセス リストへの合格が拒否されます。

**ステップ 5** アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。

明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。

**ステップ 6** **end**

例：

```
Device(config)# end
```

グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

**ステップ 7** **show ip access-list**

例：

```
Device# show ip access-list
```

（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

# 拡張アクセス リストの作成

送信元アドレス以外の要素に基づいてフィルタする場合、拡張アクセスリストを作成する必要があります。拡張アクセスリストには名前付きと番号付きという2種類があります。名前付きアクセス リストを使用すると、番号よりも直感的な名前を使用してアクセス リストを特定できます。また、サポートする機能が多数です。

送信元アドレスまたは宛先アドレス以外の要素をフィルタする方法の詳細については、コマンド リファレンス マニュアルの構文の説明を参照してください。

## 名前付き拡張アクセス リストの作成

送信元アドレス、宛先アドレス、またはアドレスと他の IP フィールドの組み合わせをフィルタする場合、名前付き拡張アクセス リストを作成します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. **deny** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
5. **permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
6. アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。
7. **end**
8. **show ip access-list**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **ip access-list extended** *name*<br>例：<br>`Device(config)# ip access-list extended acl1` | 名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。 |
| ステップ 4 | **deny** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]<br>例：<br>`Device(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10 log` | （任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。<br>• *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。<br>• 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • 必要に応じて、キーワード **host** *source* を使用し、*source* 0.0.0.0 の送信元と送信元ワイルドカードを表示して、省略形 **host** *destination* を使用し、*destination* 0.0.0.0 の宛先と宛先ワイルドカードを表示します。<br>• この例では、すべての送信元のパケットは、宛先ネットワーク 172.18.0.0 へのアクセスが拒否されます。アクセスリストによって許可または拒否されるパケットに関するロギング メッセージは、**logging facility** コマンドに設定された設備に送信されます（たとえば、コンソール、端末、syslog）。つまり、パケットがアクセス リストに一致する場合は常に、パケットに関する情報を提供するロギング メッセージが設定された設備に送信されます。コンソールにロギングするメッセージのレベルは、**logging console** コマンドで制御します。 |
| ステップ 5 | **permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** \| **log-input**] [**time-range** *time-range-name*] [**fragments**]<br>例：<br>`Device(config-ext-nacl)# permit tcp any any` | ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。<br>• 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。<br>• *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。<br>• 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。<br>• この例では、任意の送信元から任意の宛先への TCP パケットが許可されています。<br>• **log-input** キーワードを使用して、ロギング出力に入力インターフェイス、送信元 MAC アドレス、または仮想回線を含めます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。 | 明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。 |
| ステップ 7 | **end**<br>例：<br>`Device(config-ext-nacl)# end` | 標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。 |
| ステップ 8 | **show ip access-list**<br>例：<br>`Device# show ip access-list` | （任意）現在の IP アクセス リストすべてのコンテンツが表示されます。 |

### RSP3 ポートの関連情報

ACL は、フラグメント化されたパケットに対してはサポートされていません。

## 番号付き拡張アクセス リストの作成

送信元アドレス、宛先アドレス、またはアドレスと他の IP フィールドの組み合わせに基づいてフィルタし、名前を使用しない場合、番号付き拡張アクセス リストを作成します。拡張 IP アクセス リストには、100 ～ 199 または 2000 ～ 2699 の番号を付けます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* **remark** *remark*
4. **access-list** *access-list-number* **permit** *protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
5. **access-list** *access-list-number* **remark** *remark*
6. **access-list** *access-list-number* **deny** *protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**]
7. アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。
8. **end**
9. **show ip access-list**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **access-list** *access-list-number* **remark** *remark*<br>例：<br>`Device(config)# access-list 107 remark allow Telnet packets from any source to network 172.69.0.0 (headquarters)` | （任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。<br>• 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。 |
| ステップ 4 | **access-list** *access-list-number* **permit** *protocol* {*source* [*source-wildcard*] \| **any**} {*destination* [*destination-wildcard*] \| **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** \| **log-input**] [**time-range** *time-range-name*] [**fragments**]<br>例：<br>`Device(config)# access-list 107 permit tcp any 172.69.0.0 0.0.255.255 eq telnet` | ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。<br>• 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。ただし、最初のエントリにする必要はありません。<br>• 拡張 IP アクセス リストには、100 ～ 199 または 2000 ～ 2699 の番号を付けます。<br>• *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。<br>• 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。<br>• TCP と他のプロトコルでは、その他の構文も使用できます。複雑な構文の場合、コマンド リファレンスの **access-list** コマンドを参照してください。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **access-list** *access-list-number* **remark** *remark*<br>例：<br>`Device(config)# access-list 107 remark deny all other TCP packets` | （任意）アクセス リスト エントリに関してユーザーにわかりやすいコメントを追加します。<br>• 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。 |
| ステップ 6 | **access-list** *access-list-number* **deny** *protocol* {*source* [*source-wildcard*] \| **any**} {*destination* [*destination-wildcard*] \| **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** \| **log-input**] [**time-range** *time-range-name*] [**fragments**]<br>例：<br>`Device(config)# access-list 107 deny tcp any any` | ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。<br>• *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。<br>• 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 |
| ステップ 7 | アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。 | 明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。 |
| ステップ 8 | **end**<br>例：<br>`Device(config)# end` | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。 |
| ステップ 9 | **show ip access-list**<br>例：<br>`Device# show ip access-list` | （任意）現在の IP アクセス リストすべてのコンテンツが表示されます。 |

# 物理インターフェイスへのアクセスリストの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
5. **ip access-list extended** *acl-name acl-number*

6. **end**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Device# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *type number*<br>例： | インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip access-group** {*access-list-number* \| *access-list-name*} {**in** \| **out**}<br>例：<br>`Device(config-if)# ip access-group acl1 in` | 指定したアクセス リストをインバウンド インターフェイスに適用します。<br>• 送信元アドレスをフィルタリングするには、インバウンド インターフェイスにアクセス リストを適用します。 |
| ステップ 5 | **ip access-list extended** *acl-name acl-number*<br>例： | 拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。<br>拡張 ACL コンフィギュレーション モードを有効にします。CLI は拡張 ACL コンフィギュレーション モードを開始します。このモードでは、後続のすべてのコマンドが現在の拡張アクセスリストに適用されます。<br>• ACL コンフィギュレーション モードから入力されたすべてのコマンドが適用されるアクセス リスト。英字で始まる最大 30 文字の英数字文字列を使用します。<br>• アクセス リスト コンフィギュレーション モードから入力されたすべてのコマンドが適用されるアクセスリスト。数字の識別子を使用します。拡張アクセスリストでは、有効範囲は 100 ～ 199 です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **end**<br>例：<br>`Device(config-if)# end` | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

# IP アクセスリストの作成と物理インターフェイスへの適用に関する設定例

## 例：ホスト送信元アドレスでのフィルタリング

次の例では、user1 に属するワークステーションがギガビットイーサネット 0/0/0 へのアクセスを許可され、user2 に属するワークステーションはアクセスを許可されていません。

```
interface gigabitethernet 0/0/0
 ip access-group workstations in
!
ip access-list standard workstations
 remark Permit only user1 workstation through
 permit 172.16.2.88
 remark Do not allow user2 workstation through
 deny 172.16.3.13
```

## 例：サブネット送信元アドレスでのフィルタリング

次の例では、user1 サブネットは、gigabitethernet インターフェイス 0/0/0 へのアクセスが許可されていませんが、Main サブネットは、アクセスが許可されています。

```
interface gigabitethernet 0/0/0
 ip access-group prevention in
!
ip access-list standard prevention
 remark Do not allow user1 subnet through
 deny 172.22.0.0 0.0.255.255
 remark Allow Main subnet
 permit 172.25.0.0 0.0.255.255
```

## 例：送信元と宛先のアドレスおよびIPプロトコルでのフィルタリング

次の設定例は、2 つのアクセス リストを持つインターフェイスを示します。一方のリストは発信パケット、もう一方のリストは着信パケットに適用されます。Internet-filter という標準アクセス リストは、送信元アドレスに基づいて発信パケットをフィルタします。インターフェイスから発信が許可されるパケットは、送信元が 172.16.3.4 である必要があります。

marketing-group という拡張アクセス リストは、着信パケットをフィルタします。このアクセス リストは、任意の送信元からネットワーク 172.26.0.0 への Telnet パケットを許可し、その他す

べての TCP パケットを拒否します。また、ICMP パケットはすべて許可します。1024 未満のポート番号を使用する、任意の送信元からネットワーク 172.26.0.0 への UDP パケットは拒否します。最後に、このアクセス リストはその他すべての IP パケットを拒否し、そのエントリによって許可または拒否されるパケットのロギングを実行します。

```
interface gigabitethernet 0/0/0
 ip address 172.20.5.1 255.255.255.0
 ip access-group Internet-filter out
 ip access-group marketing-group in
!
ip access-list standard Internet-filter
 permit 172.16.3.4
ip access-list extended marketing-group
 permit tcp any 172.26.0.0 0.0.255.255 eq telnet
 deny tcp any any
 permit icmp any any
 deny udp any 172.26.0.0 0.0.255.255 lt 1024
 deny ip any any
```

# 例：番号付きアクセスリストを使用した送信元アドレスでのフィルタリング

次の例では、ネットワーク 10.0.0.0 は、クラス A ネットワークで、2 番目のオクテットでサブネットを指定します。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク 10.0.0.0 アドレスの 3 番目および 4 番目のオクテットで特定のホストを指定します。Cisco IOS XE ソフトウェアは、アクセス リスト 2 を使用して、サブネット 48 上の 1 つのアドレスを受け入れ、そのサブネット上のその他のアドレスはすべて拒否します。最後の行は、その他すべてのネットワーク 10.0.0.0 サブネット上のアドレスを受け入れることを示します。

```
interface gigabitethernet 0/0/0
 ip access-group 2 in
!
access-list 2 permit 10.48.0.3
access-list 2 deny 10.48.0.0  0.0.255.255
access-list 2 permit 10.0.0.0  0.255.255.255
```

# 例：サブネットへの Telnet アクセスの防止

次の例では、user1 サブネットは、ギガビット イーサネット インターフェイス 0/0/0 から Telnet にアクセスできません。

```
interface gigabitethernet 0/0/0
 ip access-group telnetting out
!
ip access-list extended telnetting
 remark Do not allow user1 subnet to telnet out
 deny tcp 172.20.0.0 0.0.255.255 any eq telnet
 remark Allow Top subnet to telnet out
 permit tcp 172.33.0.0 0.0.255.255 any eq telnet
```

# 例：ポート番号を使用した TCP および ICMP に基づくフィルタリング

次の例では、acl1 という名前の拡張アクセス リストの最初の行で、1023 よりも大きい宛先ポートを持つ着信 TCP 接続を許可しています。2 行目で、ホスト 172.28.1.2 の Simple Mail Transfer Protocol（SMTP）ポートへの着信 TCP 接続を許可しています。最後の行では、エラー フィードバックのための着信 ICMP メッセージを許可しています。

```
interface gigabitethernet 0/0/0
 ip access-group acl1 in
!
ip access-list extended acl1
 permit tcp any 172.28.0.0 0.0.255.255 gt 1023
 permit tcp any host 172.28.1.2 eq 25
 permit icmp any 172.28.0.0 255.255.255.255
```

# 例：SMTP 電子メールと確立済み TCP 接続の許可

インターネットに接続されているネットワークがあり、イーサネット上のホストでインターネット上の任意のホストに対して TCP 接続を構成するとします。ただし、専用のメール ホストのメール（SMTP）ポートを除き、IP ホストから gigabitethernet 上のホストに対する TCP 接続を構成できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続の存続中は、この同じ 2 つのポート番号が使用されます。インターネットから着信するメール パケットは、25 という宛先ポートを持ちます。発信パケットは、ポート番号が予約されています。ルータの背後にあるセキュア システムは、ポート 25 でメール接続を常に受け入れるため、着信および発信サービスを個別に制御できます。発信インターフェイスまたは着信インターフェイスで、アクセス リストを設定できます。

次の例で、gigabitethernet ネットワークはアドレスが 172.18.0.0 の クラス B ネットワークで、メール ホストのアドレスは 172.18.1.2 です。**established** キーワードを使用するのは、TCP プロトコルで確立済み接続を指定する場合のみです。TCP データグラムに ACK または RST ビットが設定されている場合に一致が発生します。これは、パケットが既存の接続に属することを示します。

```
interface gigabitethernet 0/0/0
 ip access-group 102 in
!
access-list 102 permit tcp any 172.18.0.0 0.0.255.255 established
access-list 102 permit tcp any host 172.18.1.2 eq 25
```

# 例：ポート名に基づくフィルタによる Web へのアクセス回避

次の例では、w1 および w2 ワークステーションは Web アクセスが許可されていません。ネットワーク 172.20.0.0 上のその他のホストは Web アクセスが許可されています。

```
interface gigabitethernet0/0/0
 ip access-group no-web out
!
ip access-list extended no-web
```

```
 remark Do not allow w1 to browse the web
 deny host 172.20.3.85 any eq http
 remark Do not allow w2 to browse the web
 deny host 172.20.3.13 any eq http
 remark Allow others on our network to browse the web
 permit 172.20.0.0 0.0.255.255 any eq http
```

# 例：送信元アドレスでのフィルタリングおよびパケットのロギング

次の例では、アクセス リスト 1 および 2 を定義します。いずれのリストもロギングが有効です。

```
interface gigabitethernet 0/0/0
 ip address 172.16.1.1 255.0.0.0
 ip access-group 1 in

!
access-list 1 permit 172.25.0.0 0.0.255.255 log
access-list 1 deny 172.30.0.0 0.0.255.255 log
!
access-list 2 permit 172.27.3.4 log
access-list 2 deny 172.17.0.0 0.0.255.255 log
```

インターフェイスが 172.25.7.7 から 10 パケットを受信し、172.17.23.21 から 14 パケットを受信する場合、最初のログは次のようになります。

```
list 1 permit 172.25.7.7 1 packet
list 2 deny 172.17.23.21 1 packet
```

5 分後、コンソールは、次のログを受信します。

```
list 1 permit 172.25.7.7 9 packets
list 2 deny 172.17.23.21 13 packets
```

# 例：デバッグ出力の制限

次の設定例では、アクセス リストを使用して、**debug** コマンドの出力を制限します。**debug** の出力を制限すると、データ量が絞られ、目的のデータを探しやすくなるため、時間とリソースを節約できます。

```
Device(config)# ip access-list acl1
Device(config-std-nacl)# remark Displays only advertisements for LDP peer in acl1
Device(config-std-nacl)# permit host 10.0.0.44

Device# debug mpls ldp advertisements peer-acl acl1

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

# IPアクセスリストの作成とインターフェイスへの適用に関する追加参照資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| セキュリティ コマンド | • 『Cisco IOS Security Command Reference: Commands A to C』<br>• 『Cisco IOS Security Command Reference: Commands D to L』<br>• 『Cisco IOS Security Command Reference: Commands M to R』<br>• 『Cisco IOS Security Command Reference: Commands S to Z』 |
| • アクセス リスト エントリの順序<br>• 日または週の時刻に基づくアクセス リスト エントリ<br>• 非初期フラグメントを使用するパケット | 『Refining an IP Access List』 |
| IP オプション、TCP フラグ、または非隣接ポートに基づくフィルタリング | 『Creating an IP Access List for Filtering』 |
| ロギング関連のパラメータの制御 | 『Understanding Access Control List Loggingl』 |

### 標準および RFC

| 標準/RFC | タイトル |
|---|---|
| この機能によりサポートされる新規または変更された標準や RFC はありません。またこの機能による既存の標準や RFC のサポートに変更はありません。 | — |

### シスコのテクニカル 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。 | http://www.cisco.com/cisco/web/support/index.html |

# IPアクセス リストの作成とインターフェイスへの適用に関する機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

**表 *1: IP* アクセス リストの作成とインターフェイスへの適用に関する機能情報**

| 機能名 | リリース | 機能の設定情報 |
|---|---|---|
| ACL - アクセス コントロール リスト内の送信元アドレスと宛先アドレスの一致 | Cisco IOS XE リリース 3.5S | Cisco IOS XE リリース 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 |
| ACL - ICMP コード | Cisco IOS XE リリース 3.5S | Cisco IOS XE リリース 3.5S では、Cisco ASR 903 ルータのサポートが追加されました。 |
| ACL パフォーマンスの強化 | Cisco IOS XE リリース 2.1 | この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。<br>この機能について導入または変更されたコマンドはありません。 |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。