



## セキュリティ（ACL）の拡張機能

セキュリティ（ACL）の拡張機能では、1つのボックスで設定できる ACL、ACE、またはこれらの両方の数を制限するオプションが用意されています。ボックスで ACL または ACE の数を制限することにより、ボックスのパフォーマンスに悪影響を与える可能性のある TCAM スペースの枯渇または過使用を防ぐことができます。

- [機能制限（1 ページ）](#)
- [セキュリティ（ACL）の拡張機能の設定（2 ページ）](#)
- [ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報（3 ページ）](#)

## 機能制限

- `acl-ace-limit` の設定は、ACL ごとであり、ボックスのすべての ACL に適用されます。
- `acl-limit` および `acl-ace-limit` は、`global-ace-limit` と同時に使用できません。`acl-limit` と `acl-ace-limit` が設定されている場合、`global-ace-limit` は設定できず、`global-ace-limit` が設定されている場合、`acl-limit` と `acl-ace-limit` は設定できません。  
設定する制限は、ボックスの既存の ACL/ACE の数未満にはできません。
- `acl-limit`、`acl-ace-limit`、または `global-ace-limit` 設定は、デバイスの起動中に内部で作成された ACL/ACE に適用されます。
- オブジェクト グループ ACE（ogace）拡張を備えた ACL は、このリリースではサポートされていません。お客様の要件に基づいて、これは詳しく調査できます。各 ogace は1つの ace としてカウントされます。
- `acl-limit`、`acl-ace-limit`、または `global-ace-limit` 設定は、すべての静的 ACL および動的に作成されたすべての ACL に適用されます（ただし、テンプレート ACL は除きます）。
- 設定可能な `acl-limit`、`acl-ace-limit`、または `global-ace-limit` によって、TCAM スペースの過使用や枯渇が発生しなくなるという訳ではありません。ラボでの事前テストから、ボックスでサポートできる正確な設定可能制限を認知しておく必要があります。

- ボックスで設定されているすべての ACL がインターフェイスに適用されるということが前提であり、これは TCAM スペースに影響します。
- ボックスが設定可能な `acl-limit`、`acl-ace-limit`、または `global-ace-limit` に到達し、かつクライアントが動的 ACL/ACE を作成しようとする、その要求は拒否され、`syslog` エラーメッセージが出力されます。これに応じて障害を処理するのはユーザーの責任です。

## セキュリティ (ACL) の拡張機能の設定

V4 および V6 に対して ACL および ACE 制限を設定するには：

```
enable
configure terminal
access-list acl-limit 10
access-list acl-ace-limit 12
access-list global-ace-limit 14
end
```



(注) `acl-limit` および `acl-ace-limit` は、`global-ace-limit` と同時に使用できません。

### 特記事項

- 設定可能な最大 ACL 制限の範囲は  $1 \sim 2^{16}$  です。
- 設定可能な ACL あたりの最大 ACE 制限の範囲は  $1 \sim 2^{32}$  です。
- 設定可能な最大グローバル ACE 制限の範囲は  $1 \sim 2^{32}$  です。
- `acl-ace-limit` 設定は、すでに設定されているすべての ACL、およびこれから設定されるすべての ACL に適用されます。

### セキュリティ (ACL) の拡張機能の設定の確認

`show access-list acl-limit` コマンドを使用すると、設定されている ACL と ACE の数を表示できます。

```
Device# show access-list acl-limit
Max ACLs configurable:      50
Number of ACLs configured: 10

Max aces/ACL configurable: 10

Max aces configurable:     100
Number of aces configured: 67
```

# ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報

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: ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報

機能名	リリース	機能情報
ホップバイ ホップ フィルタリングに対応するための IPv6 ACL の拡張	Cisco IOS リリース XE 3.4S Cisco IOS リリース XE 3.5S Cisco IOS リリース XE 3.6S Cisco IOS リリース XE 3.3SG	これによって、ホップバイホップ拡張ヘッダーを含む IPv6 トラフィックを制御できます。  次のコマンドが導入または変更されました。 <b>deny</b> (IPv6)、 <b>permit</b> (IPv6)。



## 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。