共通 ACL による IPv6 ACL チェーニング

マルチアクセス コントロール リストとも呼ばれる ACL チェーニングにより、ACL を分割することができます。このマニュアルでは、IPv6 ACL チェーニング サポートによって ACL を共通 ACL とユーザー専用 ACL に明示的に分割する方法、および両 ACL をデバイスでのトラフィック フィルタリングのためにバインドする方法について説明します。この方法では、Ternary Content Addressable Memory（TCAM）内の共通 ACL は複数のターゲットにより共有され、これによりリソース使用量が削減されます。

共通 ACL による IPv6 ACL チェーニングに関する情報

ACL チェーニングの概要

パケット フィルタリング プロセスは、1 つのインターフェイスの 1 つの方向および 1 つのプロトコルごとに適用される単一のアクセス コントロール リスト（ACL）のみをサポートします。そのため、多数のインターフェイスに共通 ACL エントリが必要な場合、管理性と拡張性の問題が生じます。そのようなインターフェイスにはすべて重複アクセス コントロール エントリ（ACE）が設定されており、共通 ACE の変更はすべての ACL で行われる必要があります。

インターネット サービス プロバイダー（ISP）のエッジ ボックスの典型的な ACL には次の 2 組の ACE が含まれます。

- 共通 ISP 専用 ACE
- 顧客/インターフェイス専用 ACE

これらのアドレスブロックは、ISP の保護されたインフラストラクチャ ネットワークへのアクセスを拒否するため、および顧客の送信元アドレスブロックのみを許可することでスプーフィングを防ぐために行われます。この結果、インターフェイスごとに一意の ACL が設定され、

共通 ACL による IPv6 ACL チェーニング

ほとんどの ACE がデバイス上のすべての ACL で共通になります。ACL をプロビジョニングし、変更するのは非常に面倒ですが、ACE を変更すれば全ターゲットに影響を及ぼすことができます。

共通 ACL による IPv6 ACL チェーニング

IPv6 ACL チェーニングを使用して、トラフィック フィルタを次の ACL とチェーニングできます。

- 共通 ACL
- 専用 ACL
- 共通 ACL と専用 ACL

各アクセス コントロール リスト（ACL）は順に照合されます。たとえば、共通 ACL と専用 ACL の両方を指定している場合、パケットはまず共通 ACL に対して照合され、一致が見つからなければ専用 ACL に対して照合されます。

（注） 任意の IPv6 ACL を共通または専用 ACL としてトラフィック フィルタで設定できます。ただし、同じ ACL を同じトラフィック フィルタで共通と専用の両方として指定することはできません。

共通 ACL による IPv6 ACL チェーニングの設定方法

始める前に

IPv6 ACL チェーニングは、既存の IPv6 トラフィック フィルタ コマンド **ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] [**in** | **out**] の拡張機能を使用して、インターフェイス上で設定します。

（注） 次のいずれかを設定できます。

- 共通 ACL のみ。例：**ipv6 traffic-filter common** *common-acl*
- 特定の ACL のみ。例：**ipv6 traffic-filter** *common-acl*
- 両方の ACL。例：**ipv6 traffic-filter common** *common-acl specific-acl*

ipv6 traffic-filter コマンドは追加式ではありません。このコマンドを使用すると、このコマンドの以前のインスタンスが置き換えられます。たとえば、コマンド シーケンス **ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] **in** **ipv6 traffic-filter** [*specific-acl*] **in** は、共通 ACL とトラフィック フィルタをバインディングし、共通 ACL を削除してから、特定の ACL をバインディングします。

インターフェイスへの IPv6 ACL の設定

このタスクを実行すると、インターフェイス固有の ACL とともに、共通のアクセス コントロール リスト（ACL）を受け入れるようにインターフェイスを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*}
4. **ipv6 traffic filter** {*common-access-list-name* {**in** | **out**}}
5. **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** 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	**interface** *type number*} 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスのタイプおよび番号を指定し、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	**ipv6 traffic filter** {*common-access-list-name* {**in**	**out**}} 例： `Device(config)# ipv6 traffic-filter outbound out`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）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。

共通 ACL による IPv6 ACL チェーニングの設定例

特定の順序でなくても、次の組み合わせを設定できます。

- 共通 ACL。例： **ipv6 traffic-filter common** *common-acl* **in**
- 特定の ACL。例： **ipv6 traffic-filter** *specific-acl* **in**

- 両方の ACL。例： **ipv6 traffic-filter common** *common-acl* *specific-acl* **in**

例：共通 ACL を受け入れるインターフェイスの設定

次に、ACL を明示的に削除しないでインターフェイスで設定したアクセス コントロール リスト（ACL）を交換する方法例を示します。

```
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl ACL2 in
end
```

次の例では、共通 ACL をインターフェイスから削除する方法を示します。インターフェイスから共通 ACL を明示的に削除しないと、共通 ACL をインターフェイスで交換できません。

```
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl1 ACL1 in
end
change the common acl to C_acl2
interface gigabitethernet 0/0/0
no ipv6 access-group common  C_acl1  ACL1 in
end
interface gigabitethernet 0/0/0
ipv6 access-group common  C_acl2  ACL1 in
end
```

（注） 共通 ACL を再設定する際、ライン カードの他のインターフェイスが共通 ACL に取り付けられないことを確認する必要があります。

（注） 共通 ACL とインターフェイス ACL の両方をインターフェイスに取り付け、その一方をインターフェイスで再構成すると、他は自動的に削除されます。

次に、インターフェイス ACL を削除する方法を示します。

```
interface gigabitethernet 0/0/0
ipv6 access-group common C_acl1 ACL1 in
end
```

共通 ACL による IPv6 ACL チェーニングの追加情報

関連資料

関連項目	マニュアル タイトル
IPv4 ACL チェーニング サポート	『Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

共通 ACL による IPv6 ACL チェーニングに関する機能情報

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 :* 共通 *ACL* による *IPv6 ACL* チェーニングに関する機能情報

機能名	リリース	機能情報
共通 ACL による IPv6 ACL チェーニング	Cisco IOS XE リリース 3.11S Cisco IOS XE リリース 3.6E	ACL チェーニング機能（別名、マルチ ACL）により、IPv6 トラフィック フィルタのアクセス コントロール リスト（ACL ）を明示的にコモンおよびセッション単位の ACL に分割できます。このように、使用される共通のアクセス コントロール エントリ（ACE）は、Ternary Content Addressable Memory（TCAM）内のセッションごとに各 ACL エントリのリソース使用量を減らします。 次のコマンドが導入または変更されました。**ip access-group common**

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。