IPv4 ACL チェーニング サポート

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、アクセス コントロール リスト（ACL）を分割することができます。このモジュールでは、IPv4 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。

IPv4 ACL チェーニング サポートの制限事項

- 単一のアクセス コントロール リスト（ACL）を、同じ方向の同じターゲットに対する共通、標準の両 ACL に使用することはできません。
- ACL チェーニングはセキュリティ ACL にのみ適用されます。サービス品質（QoS）、ファイアウォール サービス モジュール（FW）、ポリシーベース ルーティング（PBR）などのフィーチャ ポリシーではサポートされません。
- 共通 ACL ではターゲットごとの統計情報はサポートされません。

IPv4 ACL チェーニング サポートに関する情報

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、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。

IPv4 ACL チェーニング サポート

IPv4 ACL チェーニング サポートを使用して、アクセス コントロール リスト（ACL）を共通 ACL と顧客専用 ACL に分割したり、両 ACL を共通セッションにアタッチすることができます。この方法では、共通 ACL を 1 コピーのみ Ternary Content Addressable Memory（TCAM）にアタッチしこれを全ユーザーで共有することで、共通 ACE の維持が簡略化されます。

IPv4 ACL チェーニング機能により、次の 2 つの IPv4 ACL を 1 方向ごとに 1 つのインターフェイスでアクティブにできます。

- 共通
- 標準
- 共通と標準

（注） 1 つのインターフェイスで共通と標準の両 ACL を設定している場合、共通 ACL が標準 ACL に優先されます。

IPv4 ACL チェーニング サポートの設定方法

ACL チェーニングは、**ip traffic filter** コマンドの拡張によりサポートされます。

ip 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。

詳細については、『Security Configuration Guide: Access Control Lists Configuration Guide』の「*IPv6 ACL Chaining with a Common ACL*」セクションを参照してください。

共通 ACL を受け入れるインターフェイスの設定

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. **ip access-group** {**common** {*common-access-list-name* {*regular-access-list* | **acl**}} {**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（この場合、gigabitethernet interface）を設定し、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** {**common** {*common-access-list-name* {*regular-access-list*	**acl**}} {**in**	**out**}} 例： `Device(config)# ipv4 access-group common acl-p acl1 in`	インターフェイス固有の ACL とともに、共通 ACL を受け入れるようにインターフェイスを設定します。

	コマンドまたはアクション	目的
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。

IPv4 ACL チェーニング サポートの設定例

ここでは、共通アクセス コントロール リスト（ACL）の設定例を示します。

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
ipv4 access-group common  C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface gigabitethernet 0/0/0
ipv4 access-group common  C_acl ACL2 in
end
```

次に、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ない方法例を示します。

```
interface gigabitethernet 0/0/0
ipv4 access-group common  C_acl1 ACL1 in
end
change the common acl to C_acl2
interface gigabitethernet 0/0/0
no ipv4 access-group common  C_acl1  ACL1 in
end
interface gigabitethernet 0/0/0
ipv4 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 の削除方法を示します。

```
interface gigabitethernet 0/0/0
ipv4 access-group common C_acl1 ACL1 in
end
```

IPv4 ACL チェーニング サポートの追加参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 ACL チェーニング サポート	
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

IPv4 ACL チェーニング サポートに関する機能情報

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 : IPv4 ACL* チェーニング サポートに関する機能情報

機能名	リリース	機能情報
IPv4 ACL チェーニング サポート	Cisco IOS XE リリース 3.11S Cisco IOS XE リリース 3.6E	IPv4 ACL チェーニング サポートは、アクセス コントロール リスト（ACL ）を明示的に共通およびユーザー固有の ACL に分割して、両方の ACL をデバイス上でのトラフィック フィルタリングのためのセッション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。 次のコマンドが導入または変更されました。**ip access-group command**

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。