IP ACL の設定

この章では、Cisco NX-OS デバイスの IP アクセス コントロール リスト（ACL）を設定する方法について説明します。

特に指定がなければ、IP ACL は IPv4 および IPv6 の ACL を意味します。

ACL の概要

アクセス コントロール リスト（ACL）とは、トラフィックのフィルタリングに使用する順序付きのルールセットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットを ACL 内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、拒否されたパケットはドロップされます。

ACLを使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACLを使用して、厳重にセキュリティ保護されたネットワークからインターネットにHTTPトラフィックが流入するのを禁止できます。また、特定のサイトへのHTTPトラフィックだけを許可することもできます。その場合は、サイトのIP アドレスが、IP ACL に指定されているかどうかによって判定します。

IP ACL のタイプと適用

Cisco Nexus デバイスは、セキュリティ トラフィック フィルタリングのために IPv4、IPv6、および MAC ACL をサポートします。スイッチでは、次の表に示すように、ポート ACL、およびルータ ACL として、IP アクセス コントロール リスト（ACL）を使用できます。

Table 1: セキュリティ ***ACL*** の適用

適用	サポートするインターフェイス	サポートする ACL のタイプ
ポート ACL	ACL は、次のいずれかに適用した場合、ポート ACL と見なされます。 • イーサネット インターフェイス • イーサネット ポート チャネル インターフェイス	IPv4 ACL IPv6 ACL MAC ACL
ルータ ACL	• 物理層 3 インターフェイス • レイヤ3イーサネットサブインターフェイス • レイヤ 3 イーサネット ポート チャネル インターフェイス • レイヤ 3 イーサネット ポート チャネル サブインターフェイス • 管理インターフェイス • Switched Virtual Interface（SVI）	IPv4 ACL IPv6 ACL
VTY ACL	VTY	IPv4 ACL IPv6 ACL

適用順序

デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。デバイスがトラフィックに適用する ACL はパスによって決まります。デバイスは、次の順序で ACL を適用します。

1. ポート ACL
2. 入力ルータ ACL

ルール

アクセス リスト コンフィギュレーション モードでルールを作成するには、**permit** または **deny** コマンドを使用します。スイッチは、許可ルール内の基準と一致するトラフィックを許可し、

拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。

プロトコル

IPv4およびMACのACLでは、トラフィックをプロトコルで識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 ACLでは、ICMPを名前で指定できます。

インターネット プロトコル番号を表す整数でプロトコルを指定できます。

暗黙のルール

IP ACLおよびMAC ACLには暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL内の他のルールと一致しない場合にスイッチがトラフィックに適用するルールです。

すべてのIPv4 ACLには、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙のルールによって、どの条件にも一致しないIPトラフィックは拒否されます。

すべてのIPv6 ACLには、次の暗黙のルールがあります。

```
deny ipv6 any any
```

すべてのMAC ACLには、次の暗黙のルールがあります。

```
deny any any protocol
```

この暗黙ルールによって、デバイスは、トラフィックのレイヤ2ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。IPv4 ACLには、次の追加フィルタリング オプションが用意されています。

- レイヤ4プロトコル
- TCP/UDPポート
- IGMPタイプ
- 確立済みTCP接続

シーケンス番号

Cisco Nexus デバイスはルールのシーケンス番号をサポートしています。入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

  ```
  switch(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

また、デバイスでは、ACL 内ルールのシーケンス番号を再割り当てすることができます。シーケンス番号の再割り当ては、ACL 内に、100、101 のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

TCP および UDP トラフィックの IP ACL ルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。

Cisco Nexus デバイスは、演算子とオペランドの組み合わせを論理演算ユニット（LOU）というレジスタ内に格納し、IP ACL で指定された TCP および UDP ポート上で演算（より大きい、より小さい、等しくない、包含範囲）を行います。

ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。

- ACL を設定するインターフェイス タイプについての知識が必要です。

ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- HTTP メソッド照合の拡張として、 tcp-option-length オプションが ACE 構文に追加され、パケットの TCP オプション ヘッダーの長さを指定できます。ACE には最大 4 つの tcp-option-length を構成できます。これには、TCP オプション長が 0 のものも含まれます。tcp-option-length オプションを構成しない場合、長さは 0 と見なされます。これは、TCP オプション ヘッダーのないパケットだけがこの ACE と一致することを意味します。この機能により、可変長の TCP オプション ヘッダーを持つパケットでも HTTP メソッドを照合できるようになり、柔軟性が向上します。
- ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。
- TCAM スペースが使用可能な限り、任意の数の ACL を構成できます。
- 出力 RACL は、リリース 7.x ではサポートされていません。ただし、構成がエラーや警告なしで許可される場合があります。
- 通常、IP パケットに対する ACL 処理は I/O モジュール上で実行されます。これには、ACL 処理を加速化するハードウェアを使用します。場合によっては、スーパーバイザ モジュールで処理が実行されることもあります。この場合、特に多数のルールが設定されている ACL を処理する際には、処理速度が遅くなることがあります。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。次のカテゴリのいずれかに属する IP パケットがレイヤ 3 インターフェイスから出る場合、これらのパケットはスーパーバイザ モジュールに送られて処理されます。
  - レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
  - IP オプションがある IPv4 パケット（追加された IP パケット ヘッダーのフィールドは、宛先アドレス フィールドの後）
  - 拡張 IPv6 ヘッダー フィールドがある IPv6 パケット
- 時間範囲を使用する ACL を適用すると、デバイスは、その ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリを更新します。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。時間範囲が有効で、アクティブな状態であることを確認します。

- すべての着信および発信トラフィックに **match-local-traffic** オプションを使用するには、最初に ソフトウェアで ACL を有効にする必要があります。
- 出力 RACL が構成された Cisco N3K-C36180YC-R スイッチの場合、7.x リリースから 9.x リリースにアップグレードする際、次の手順に従って RACL が維持され、アップグレードが問題なく完了していることを確認してください。

  1. **hardware access-list tcam region e-racl** コマンドを使用して、出力 RACL の TCAM エントリを追加します。
  2. 構成を保存してリロードします。
  3. 9.x リリースにアップグレードします。

  構成の詳細については、ACL TCAM リージョン （25 ページ）および ACL TCAM リージョン サイズの設定 （34 ページ）を参照してください。
- Cisco NX-OS リリース 9.3(2) 以降、Cisco Nexus 36180YC-R および 3636C-R では、ユーザー定義の MAC アドレス制限を 16 ー 256 の範囲で設定できます。
- Cisco NX-OS リリース 9.3(3) において、Cisco Nexus 3636C-R プラットフォーム スイッチは、出力 IPv6 RACL について次をサポートします：
  - レイヤ 4 プロトコル
  - TCP フラグ
  - フラグメント
  - ACL ログ
- Cisco NX-OS リリース 9.3(3) において、Cisco Nexus 3636C-R プラットフォーム スイッチは、次をサポートしません：
  - 出力のアトミック アップデート
  - 外部 TCAM の出力ルータ ACL
  - UDF を伴う出力 ルータ ACL
  - 出力と入力の両方のルータ ACL v6 カウンタ
  - l4 ops による出力および出力ルータ ACL IPv6
  - サブインターフェイスの出力ルータ ACL
  - IPv6 ICMP タイプおよびコードによる出力および入力ルータ ACL
  - tcp-flag を使用した IPv6 入力ルータ ACL
  - 追加オプション付きの IPv4 ルータ ACL
- Cisco NX-OS リリース 9.3(3) において、Cisco Nexus 3636C-R プラットフォーム スイッチは、出力 IPv4 RACL について次をサポートします：

- TCP フラグ
- ICMP のタイプとコード
- ACL ログ

- hardware profile acl-stats module xx コマンドを使用して ACL TCAM エントリのカウンタを有効にすると、show interface の input discard フィールドは常にゼロになります。この制限は、N3K-C3636C-R および N3K-C36180YC-R ライン カードを搭載した Cisco Nexus 3600 プラットフォーム スイッチにのみ適用されます。
- Cisco NX-OS リリース 9.3(5) において、IPv6 出力 ACL は、Cisco Nexus 3636C-R および 36180YC-R スイッチで以下をサポートします：
  - レイヤ 4 プロトコル
  - TCP フラグ
  - フラグメント
  - ACL ログ
  - IPv6 ヘッダーのフィールド

デフォルトの ACL 設定

次の表は、IP ACL パラメータのデフォルト設定をリスト表示しています。

***Table 2: IP ACL* のデフォルト パラメータ**

パラメータ	デフォルト
IP ACL	デフォルトの IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

次の表は、MAC ACL パラメータのデフォルト設定をリスト表示しています。

***Table 3: MAC ACL* のデフォルト パラメータ**

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

IP ACL の設定

IP ACL の作成

デバイスに IPv4 または IPv6 ACL を作成し、これにルールを追加できます。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。

SUMMARY STEPS

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **ip access-list** *name*
   - **ipv6 access-list** *name*
3. [*sequence-number*] {**permit** | **deny**} *protocol* {*source-ip-prefix* | *source-ip-mask*} {*destination-ip-prefix* | *destination-ip-mask*}
4. **statistics per-entry**
5. **hardware profile acl-stats module** *xx*
6. **reload**
7. 次のいずれかのコマンドを入力します。
   - **show ip access-lists** *name*
   - **show ipv6 access-lists** *name*
8. **copy running-config startup-config**
9. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

	Command or Action	Purpose

ステップ 2	次のいずれかのコマンドを入力します。
	• **ip access-list** *name*
	• **ipv6 access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。

ステップ 3	[*sequence-number*] {**permit** | **deny**} *protocol* {*source-ip-prefix* | *source-ip-mask*} {*destination-ip-prefix* | *destination-ip-mask*} **Example:** `switch(config-acl)# 10 permit ipv6 1::1 2::2 3::3 4::4`	IP ACL 内にルールを作成します。多数のルールを作成できます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、特定の Cisco Nexus デバイスのコマンド リファレンスを参照してください。
ステップ 4	**statistics per-entry** **Example:** `switch(config-acl)# statistics per-entry`	その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 5	**hardware profile acl-stats module** *xx* **Example:** `switch(config-acl)# hardware profile acl-stats module 1`	内部 TCAM と外部 TCAM の両方で ACL TCAM エントリのカウンタを有効にします。 **Note** このコマンドは、-R および -RX ライン カードと Cisco Nexus 3636C-R および 36180YC-R スイッチを備えた Cisco Nexus 9500 プラットフォームスイッチにのみ適用されます。カウンタを有効にすると、VLAN と SVI の統計情報は失われます。
ステップ 6	**reload** **Example:** `switch(config)# reload`	スイッチをリロードします。 **Note** **reload** コマンドは、Cisco Nexus 3636C-R および 36180YC-R スイッチでは必須です。
ステップ 7	次のいずれかのコマンドを入力します。 • **show ip access-lists** *name* • **show ipv6 access-lists** *name* **Example:** `switch(config-acl)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 8	**copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	Command or Action	Purpose
ステップ 9	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
```

次に、IPv6 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
```

IPv4 ACL ロギングの設定

Ipv4 ACL ロギング プロセスを設定するには、最初にアクセス リストを作成してから、指定された ACL を使用してインターフェイス上の IPv4 トラフィックのフィルタリングをイネーブルにし、最後に ACL ロギング プロセス パラメータを設定します。

手順の概要

1. **configure terminal**
2. **ip access-list** *name*
3. {**permit** | **deny**} **ip** *source-address destination-address* **log**
4. **exit**
5. **interface ethernet** *slot/port*
6. **ip access-group** *name* **in**
7. **exit**
8. **logging ip access-list cache interval** *interval*
9. **logging ip access-list cache entries** *number-of-flows*
10. **logging ip access-list cache threshold** *threshold*
11. **logging ip access-list detailed**
12. **hardware rate-limiter access-list-log** パケット
13. **acllog match-log-level** *severity-level*
14. （任意） **show logging ip access-list cache** [**detail**]

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**ip access-list** *name*
	例：
	`switch(config)# ip access-list logging-test`
	`switch(config-acl)#`
		IPv4 ACL を作成し、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。

ステップ 3	{**permit** | **deny**} **ip** *source-address destination-address* **log** 例： `switch(config-acl)# permit ip any 10.30.30.0/24 log`	条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。システムがルールに一致する各パケットに関する情報ロギング メッセージを生成できるようにするには、logキーワードを含める必要があります。 *Source-address* および *destination-address* 引数には、IP アドレスとネットワーク ワイルドカード、IP アドレスと可変長サブネット マスク、ホスト アドレス、または任意のアドレスを指定する **any** などがあります。

ステップ 4	**exit**
	例：
	`switch(config-acl)# exit`
	`switch(config)#`
		設定を更新し、IP ACL コンフィギュレーション モードを終了します。

ステップ 5	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 1/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 6	**ip access-group** *name* **in** 例： `switch(config-if)# ip access-group logging-test in`	指定された ACL を使用してインターフェイス上の IPv4 トラフィックのフィルタリングをイネーブルにします。着信トラフィックに ACL を適用できます。

ステップ 7	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定を更新し、インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 8	**logging ip access-list cache interval** *interval* 例： `switch(config)# logging ip access-list cache interval 490`	ACL ロギング プロセスのログ更新間隔（秒単位）を設定します。デフォルト値は300秒です。範囲は 5 ～ 86400 秒です。
ステップ 9	**logging ip access-list cache entries** *number-of-flows* 例： `switch(config)# logging ip access-list cache entries 8001`	ACL ロギング プロセスでモニタするフローの最大数を指定します。デフォルト値は8000です。サポートされる値の範囲は 0 ～ 1048576 です。
ステップ 10	**logging ip access-list cache threshold** *threshold* 例： `switch(config)# logging ip access-list cache threshold 490`	アラート期限が切れる前に、指定されたパケット数がログ記録された段階で、Syslog メッセージが生成されます。
ステップ 11	**logging ip access-list detailed** 例： `switch(config)# logging ip access-list detailed`	**show logging ip access-list cache** コマンドの出力で、ACL 名、ACE シーケンス番号、アクション、ACL の方向、ACL フィルタ タイプ、および ACL 適用インターフェイスが表示されるようにします。
ステップ 12	**hardware rate-limiter access-list-log** パケット 例： `switch(config)# hardware rate-limiter access-list-log 200`	ACL ロギングのためにスーパーバイザ モジュールにコピーされるパケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。 （注） Cisco Nexus NX-OS 7.0(3)F3(1) は、 **hardware rate-limiter access-list-log** コマンドをサポートしていません。
ステップ 13	**acllog match-log-level** *severity-level* 例： `switch(config)# acllog match-log-level 5`	ACL の一致を記録する最小シビラティ（重大度）レベルを指定します。デフォルトは 6（情報）です。範囲は 0（緊急）～ 7（デバッグ）です。
ステップ 14	（任意） **show logging ip access-list cache** [**detail**] 例： `switch(config)# show logging ip access-list cache`	送信元IPおよび宛先IPアドレス、送信元ポートおよび宛先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。**logging ip access-list detailed** コマンドを入力すると、出力には、ACL の名前、ACE のシーケンス番号、アクション、ACL の方向、ACL のフィルタ タイプ、そして ACL の適用インターフェイスも含まれるようになります。

IP ACL の変更

既存の IPv4 または IPv6 ACL に対してルールの追加または削除を行うことができます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# {**ip** | **ipv6**}**ip access-list** *name*
3. switch(config)# **ip access-list** *name*
4. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*
5. (Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}
6. (Optional) switch# **show ip access-lists** *name*
7. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **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 2	switch(config)# {**ip** | **ipv6**}**ip access-list** *name*	名前で指定した ACL の IP ACL 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	switch(config)# **ip access-list** *name*	名前で指定した ACL の IP ACL 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	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、Cisco Nexus デバイスの『*Command Reference*』を参照してください。
ステップ 5	(Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	指定したルールを IP ACL から削除します。

	Command or Action	Purpose
		permit コマンドと deny コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、Cisco Nexus デバイスの『*Command Reference*』を参照してください。
ステップ 6	(Optional) switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 7	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Related Topics

IP ACL 内のシーケンス番号の変更 （15 ページ）

IP ACL の削除

スイッチから IP ACL を削除できます。

スイッチから IP ACL を削除する前に、ACL がインターフェイスに適用されているかどうかを確認してください。削除できるのは、現在適用されている ACL だけです。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。スイッチは、削除対象の ACL が空であると見なします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no ip access-list** *name*
3. switch(config)# no **ip access-list** *name*
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **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 2	switch(config)# **no ip access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	switch(config)# no **ip access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。

	Command or Action	Purpose
ステップ 4	(Optional) switch# **show running-config**	ACL の設定を表示します。削除された IP ACL は表示されないはずです。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence ip access-list** *name starting-sequence-number increment*
3. (Optional) switch# **show ip access-lists** *name*
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **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 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	ACL内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	(Optional) switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 4	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

mgmt0 への IP-ACL の適用

管理インターフェイス（mgmt0）に適用できるのは、IPv4 と IPv6 の ACL です。

始める前に

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **ip access-group** *access-list* {**in** | **out**}
3. （任意） **show running-config aclmgr**
4. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**ip access-group** *access-list* {**in**	**out**} 例： `switch(config-if)#ip access-group acl-120 out`	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 3	（任意） **show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 4	（任意） **copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連項目

- IP ACL の作成

ポート ACL としての IP ACL の適用

IPv4 ACL は、物理イーサネット インターフェイスまたは PortChannel に適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。

Note 一部の設定パラメータは、ポート チャネルに適用されていると、メンバー ポートの設定に反映されません。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}
3. switch(config-if)# **ip port access-group** *access-list* **in**
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **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 2	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ip port access-group** *access-list* **in**	IPv4 ACL を、インターフェイスまたはポート チャネルに適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	(Optional) switch# **show running-config**	ACL の設定を表示します。
ステップ 5	(Optional) switch# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ルータ ACL としての IP ACL の適用

IPv4 ACL または IPv6 ACL は、次のタイプのインターフェイスに適用できます：

- 物理層 3 インターフェイスおよびサブインターフェイス
- レイヤ 3 イーサネット ポート チャネル インターフェイスおよびサブインターフェイス
- 管理インターフェイス

Before you begin

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

SUMMARY STEPS

1. switch# **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - switch(config)# **interface ethernet** *slot*/*port*[**.** *number*]
   - switch(config)# **interface port-channel** *channel-number*[**.** *number*]
   - switch(config)# **interface mgmt** *port*
3. 次のいずれかのコマンドを入力します。
   - switch(config-if)# **ip access-group** *access-list* {*in*}
   - switch(config-if)# **ipv6 traffic-filter** *access-list* {*in*}
4. (Optional) switch(config-if)# **show running-config aclmgr**
5. (Optional) switch(config-if)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **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 2	次のいずれかのコマンドを入力します。 • switch(config)# **interface ethernet** *slot*/*port*[**.** *number*] • switch(config)# **interface port-channel** *channel-number*[**.** *number*] • switch(config)# **interface mgmt** *port*	指定したインターフェイス タイプ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 3	次のいずれかのコマンドを入力します。 • switch(config-if)# **ip access-group** *access-list* {*in*} • switch(config-if)# **ipv6 traffic-filter** *access-list* {*in*}	IPv4 ACL または IPv6 ACL を、入力方向のトラフィックのレイヤ 3 インターフェイスに適用します。
ステップ 4	(Optional) switch(config-if)# **show running-config aclmgr**	ACL の設定を表示します。
ステップ 5	(Optional) switch(config-if)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイス MAC アドレスの設定と制限

SVI、レイヤ 3インターフェイス、ポート チャネル、レイヤ 3 サブインターフェイス、およびトンネル インターフェイスにスタティック MAC アドレスを設定できます。ポートおよびポート チャネルの範囲でスタティック MAC アドレスを設定することもできます。ただし、すべてのポートがレイヤ 3 にある必要があります。ポートの範囲内の 1 つのポートがレイヤ 2 にある場合でも、コマンドは拒否され、エラー メッセージが表示されます。

デフォルトでは、スイッチに設定できる MAC アドレスの最大数は 16 です。ただし、この制限を変更して、MAC アドレス数の範囲を 16 ー 256 に設定することができます。

vPC対応スイッチでの構成制限には、ローカルに構成されたユーザー定義のMACアドレスと、vPC ピアから同期されたユーザー定義の MAC アドレスの両方が含まれます。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. [**no**] **mac-address** *static router MAC address*
4. （任意） **show interface ethernet** *slot/port*
5. **mac address-table limit** *16-256* **user-defined**
6. （任意） **show mac address-table limit user-defined**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス設定モードを開始します。

ステップ 3	[**no**] **mac-address** *static router MAC address* 例： `switch(config-if)# mac-address 0019.D2D0.00AE`	インターフェイスに MAC アドレスを設定します。設定を削除するには、このコマンドの no 形式を使用します。MACアドレスは、サポートされている次の4つの形式のいずれかで入力できます。 • E.E.E • EE-EE-EE-EE-EE-EE • EE:EE:EE:EE:EE:EE

	コマンドまたはアクション	目的
		• EEEE.EEEE.EEEE （注） 次の無効なMACアドレスは入力しないでください。 • ヌルMACアドレス：0000.0000.0000 • ブロードキャストMACアドレス：FFFF.FFFF.FFFF • マルチキャストMACアドレス：0100.DAAA.ADDD

ステップ 4	（任意） **show interface ethernet** *slot/port*
	例：
	`switch(config-if)# show interface ethernet 2/1`
	`switch(config)#`
		インターフェイスのすべての情報を表示します。

ステップ 5	**mac address-table limit** *16-256* **user-defined**
	例：
	`switch(config)# mac address-table limit 200 user-defined`
	`switch(config)#`
		スイッチに設定できる MAC アドレスの最大数を設定します。

ステップ 6	（任意） **show mac address-table limit user-defined** 例： `switch(config)# show mac address-table limit user-defined`	スイッチに設定できる MAC アドレスの最大数を表示します。

例

インターフェイスの MAC アドレスを構成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/3
switch(config-if)# mac-address aaaa.bbbb.dddd
switch(config-if)# show interface ethernet 3/3
switch(config-if)#
switch(config)# mac address-table limit 100 user-defined
Warning: Configure the same User-Defined Mac Limit on the peer.
Warning: New Fhrp max group limit is 390
switch# show  mac address-table limit user-defined
User Defined Mac Limit: 100
FHRP Mac Limit: 390
==============
```

UDF ベースの MAC ACL の設定

この機能により、デバイスはユーザ定義フィールド（UDF）で照合し、一致するパケットを MAC ACL に適用できます。

Cisco NX-OS リリース 9.3(2) 以降では、Cisco Nexus 36180YC-R および 3636C-R プラットフォーム スイッチの UDF ベースで MAC アクセス リスト（ACL）を構成できます。

手順の概要

1. **configure terminal**
2. **udf** *udf-name offset-base offset length*
3. **hardware access-list tcam region ing-ifacl qualify** {**udf** *udf-name* }
4. **copy running-config startup-config**
5. **reload**
6. **mac access-list** *udf-acl*
7. **permit mac** *source destination* **udf** *udf-name value mask*
8. **interface port-channel** *channel-number*
9. **mac port access-group** *udf-access-list*
10. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**udf** *udf-name offset-base offset length* 例： `switch(config)# udf pktoff10 packet-start 10 2`	次のように UDF を定義します。 • *udf-name*：UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。 • *offset-base*：UDF オフセット ベースを {**packet-start**} のように指定します。 • オフセット：オフセット ベースからバイト オフセットの数を指定します。 • 長さ：オフセット からバイトの数を指定します。1 または 2 バイトのみがサポートされています。追加のバイトに一致させるためには、複数の UDF を定義する必要があります。

	コマンドまたはアクション	目的
		複数の UDF を定義できますが、シスコは必要な UDF のみ定義することを推奨します。
ステップ 3	**hardware access-list tcam region ing-ifacl qualify** {**udf** *udf-name* } 例： `switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10`	IPv4 または IPv6 ポート ACLに適用する ing-ifacl TCAM リージョンに UDF をアタッチします。 最大 18 個の UDF がサポートされます。 （注） UDF 修飾子が追加されると、TCAM リージョンはシングル幅から倍幅に拡大します。十分な空き領域があることを確認してください。そうでない場合、このコマンドは拒否されます。必要な場合、未使用のリージョンから TCAM スペースが減りますので、このコマンドを再入力します。詳細については、「ACL TCAM リージョン サイズの設定（34 ページ）」を参照してください。 （注） このコマンドの **no** 形式は、UDF を TCAM リージョンから切り離し、リージョンをシングル幅に戻します。
ステップ 4	必須: **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 5	必須: **reload** 例： `switch(config)# reload`	デバイスがリロードされます。 （注） UDF 設定は **copy running-config startup-config** + **reload** を入力した後のみ有効になります。

ステップ 6	**mac access-list** *udf-acl*
	例：
	`switch(config)# mac access-list udfacl`
	`switch(config-acl)#`
		MAC アクセス コントロール リスト（ACL）を作成して、MAC ACL コンフィギュレーション モードを開始します。

ステップ 7	**permit mac** *source destination* **udf** *udf-name value mask* 例： `switch(config-acl)# permit mac any any udf pktoff10 0x1234 0xffff`	MAC ACL を 設定して、外部パケット フィールドについて現在のアクセス コントロール エントリ（ACE）と併せて UDF で一致させるように設定します（例 2）。値とマスクの引数の範囲は 0x0～0xFFFF です。 シングル ACL は、UDFがある場合とない場合の両方とも、ACE を有することができます。各 ACE に

	コマンドまたはアクション	目的
		は一致する異なる UDF フィールドがあるか、すべての ACE を UDF の同じリストに一致させることができます。

ステップ 8	**interface port-channel** *channel-number*
	例：
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		レイヤ 2 のポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 9	**mac port access-group** *udf-access-list* 例： `switch(config-if)# mac port access-group udf-acl-01`	UDF ベース MAC ACL をインターフェイスに適用します。
ステップ 10	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IPv6 拡張ヘッダーの ACL の設定

この手順は、次のデバイスにのみ適用されます。

- Cisco Nexus 9504 および 9508 モジュラ シャーシ（N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R）
- Cisco Nexus 3600 プラットフォーム スイッチ（N3K-C36180YC-R および N3K-C3636C-R）

Cisco NX-OS リリース 9.3(7) 以降では、ここにリストされているデバイスで IPv6 ACL を設定する場合、拡張ヘッダーを含む IPv6 パケットの処理に関する新しいルールを含める必要があります。IPv6 拡張ヘッダーの詳細については、*Cisco Nexus 3600* シリーズ *NX-OS* ユニキャスト ルーティング構成ガイドの NX-OS リリース 9.3(x) 以降の「簡素化した IPv6 パケット ヘッダー」を参照してください。

（注） この手順で選択した許可ルールまたは拒否ルールは、パケットの他のフィールドに一致する他の ACL ルールに関係なく、少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットに適用されます。

手順の概要

1. **configure terminal**
2. **ipv6 access-list** *name*
3. **extension-header** {**permit-all** | **deny-all**}

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル構成モードを開始します。

ステップ 2	**ipv6 access-list** *name*
	例：
	`switch(config)# ipv6 access-list acl-01`
	`switch(config-acl)#`
		MAC ACL を作成して、ACL 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	**extension-header** {**permit-all** | **deny-all**}
	例：
	`switch(config-acl)# extension-header permit-all`
	`switch(config-acl)#`
		一致したパケットに必要なアクションを選択します。
		• **permit-all**：少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットが許可されます。
		• **deny-all**：少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットがドロップされます。

システム ACL について

36180YC-R および C3636C-Rスイッチでシステム ACL を構成することができます。システム ACL を使用すると、スイッチ内の同じアクセスリストを持つすべてのポートにレイヤ 2 ポート ACL（PACL）を設定できます。システム ACL を設定すると、TCAM の使用率が低下し、ポリシーの適用または変更中に時間とメモリの使用率が低下します。

システム ACL の設定については、次の注意事項と制限事項を参照してください。

- システム PACL は、レイヤ 2 インターフェイスでのみサポートされます。
- ACE 統計情報は、システム ACL ではまだサポートされていません。
- IPv6 は、システム ACL ではまだサポートされていません。
- システム ACL は、ブレークアウト ポートではサポートされません。
- Cisco Nexus 3600 プラットフォーム スイッチでのサービス品質、ACL、または TCAM カービング構成については、 Cisco Nexus 3600 NX-OS サービス品質構成ガイドを参照してください。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

IPv4 TCAM はシングル幅です。

IPv6、ポート ACL、およびルータ ACLを作成でき、QoS の IPv6 アドレスとマッチングできます。Cisco NX-OS は、3 つすべての TCAM を同時にサポートします。これらの新しい IPv6 TCAM を有効にするには、既存の TCAM を削除するか、サイズを小さくする必要があります。

TCAM リージョン サイズには、次の注意事項と制約事項があります。

- デフォルトの ACL TCAM サイズに戻すには、**no hardware access list tcam region** コマンドを使用します。デフォルトのサイズに戻す場合は、モジュールをリロードする必要があります。
- プラットフォームによっては、各 TCAM リージョンの最小/最大/集約サイズ制限が異なる場合があります。
- TCAMの総数は 16 です。
  - 大型 TCAM は 12 あり、それぞれに 160 ビット キー サイズのエントリが 2048 あります。
  - 小型 TCAM は 4 つあり、それぞれに 160 ビット キー サイズのエントリが 256 あります。
- TCAM リージョン RACL v6、QoS、CoPP、およびマルチキャストを 0 に設定することはできません。
- Redirect_v6、RACL v4 は TCAM を他の機能と共有できません。
- TCAM の切り分け後には、スイッチをリロードする必要があります。
- RACL v6、CoPP、およびマルチキャストにはデフォルトの TCAM サイズがあります。以下の Cisco 3600 ラインカードでは、リロード中にライン カード障害が発生しないように、これらの TCAM サイズをゼロ以外にする必要があります。
  - N3K-C3636C-R
  - N3K-C36180YC-R
- IPv6 RACL は IPv6 IFCAL で部分的に使用できます。これは、Cisco Nexus N3K-C36180YC-R および N3K-C3636C-R ライン カードに適用されます。

表 *4 : ACL* リージョンによる *TCAM* サイズ

TCAM ACL リージョン	デフォルト サイズ
PACL_IPv4 [ifacl]	1024
PACL_IPV6 [ipv6-ifacl]	1024

TCAM ACL リージョン	デフォルト サイズ
PACL_MAC [mac-ifacl]	2048
IPv4 ポート QOS [qos]	640
IPV6 ポート QoS [ipv6-qos]	256
IPv4 RACL [racl]	1024
IPv6 RACL [ipv6-racl]	1024
IPv4 L3 QoS [l3qos]	640
IPv6 L3 QoS [ipv6-l3qos]	256
SPAN [span]	96
入力 CoPP [copp]	128
リダイレクト v4	1024
リダイレクトv6	2048

TCAM リージョンの分割

システム ACL を設定する前に、まず TCAM リージョンを分割します。1k 未満の ACL を設定する場合は、TCAM リージョンを分割する必要がないことに注意してください。詳細については、「ACL TCAM リージョン サイズの設定 （34 ページ）」を参照してください。

（注） PACL IPv4、RACL IPv4、および RACL IPv6 が12k を超えていても構成できます。

システム ACL の設定

IPv4 ACL を作成したら、システム ACL を設定します。

始める前に

デバイスで IPv4 ACL を作成します。詳細については、「IP ACL の作成 （8 ページ）」を参照してください。

手順の概要

1. **config t**
2. **system acl**
3. **ip port access-group** <*pacl name*> **in**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**config t**	コンフィギュレーション モードを開始します。
ステップ 2	**system acl**	システムACLを設定します。
ステップ 3	**ip port access-group** <*pacl name*> **in**	インターフェイスにレイヤ 2 PACL を適用します。ポート ACL では、インバウンド フィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。

システム ACL の設定および show コマンドの例

システム ACL のshowコマンドについては、次の設定例を参照してください。

1K スケールのシステム PACL の設定（デフォルト TCAM を使用）

1K スケールのシステム PACL の設定については、次の例を参照してください（デフォルト TCAM を使用）。

ステップ 1：PACL を作成します。

```
config t
ip access-list PACL-DNA
    10 permit ip 1.1.1.1/32 any
    20 permit tcp 3.0.0.0/8 255.0.0.0 eq 1500
    25 deny udp any any eq 500
    26 deny tcp any eq 490 any
    …·· ….

    1000 deny any any
```

ステップ 2：PACL をシステム レベルに適用します。

```
configuration terminal
system acl
    ip port access-group PACL-DNA in
```

スイッチに設定されているシステム ACLを検証するには、**sh run aclmgr | sec system** コマンドを使用します。

```
switch# sh run aclmgr | sec system
system acl
 ip port access-group test in
switch#
```

スイッチに設定されている PACL を検証するには、**sh ip access-lists <name> [summary]** コマンドを使用します。

```
switch# sh ip access-lists test

IP access list test
        10 deny udp any any eq 27
        20 permit ip 1.1.1.1/32 100.100.100.100/32
        30 permit ip 1.2.1.1/32 100.100.100.100/32
        40 permit ip 1.3.1.1/32 100.100.100.100/32
        50 permit ip 1.4.1.1/32 100.100.100.100/32
        60 permit ip 1.5.1.1/32 100.100.100.100/32
        70 permit ip 1.6.1.1/32 100.100.100.100/32
        80 permit ip 1.7.1.1/32 100.100.100.100/32
        90 permit ip 1.8.1.1/32 100.100.100.100/32

switch# sh ip access-lists test summary
IPV4 ACL test
        Total ACEs Configured: 12279
        Configured on interfaces:
        Active on interfaces:
                - ingress
                - ingress

switch#
```

PACL IPv4（ifacl）TCAMリージョン サイズを検証するには、**show hardware access-list tcam region** コマンドを使用します。

```
switch# show hardware access-list tcam region
*********************************WARNING*********************************
*****************The output shows NFE tcam region info******************
***Please refer to 'show hardware access-list tcam template' for NFE2***
*************************************************************************
                             IPV4 PACL [ifacl] size = 12280
                          IPV6 PACL [ipv6-ifacl] size =    0
                            MAC PACL [mac-ifacl] size =    0
                             IPV4 Port QoS [qos] size =  640
                          IPV6 Port QoS [ipv6-qos] size =  256
                            MAC Port QoS [mac-qos] size =    0
                       FEX IPV4 PACL [fex-ifacl] size =    0
                  FEX IPV6 PACL [fex-ipv6-ifacl] size =    0
                    FEX MAC PACL [fex-mac-ifacl] size =    0
                     FEX IPV4 Port QoS [fex-qos] size =    0
                FEX IPV6 Port QoS [fex-ipv6-qos] size =    0
                  FEX MAC Port QoS [fex-mac-qos] size =    0
                             IPV4 VACL [vacl] size =    0
                          IPV6 VACL [ipv6-vacl] size =    0
                            MAC VACL [mac-vacl] size =    0
                           IPV4 VLAN QoS [vqos] size =    0
                       IPV6 VLAN QoS [ipv6-vqos] size =    0
                         MAC VLAN QoS [mac-vqos] size =    0
                             IPV4 RACL [racl] size =    0
                          IPV6 RACL [ipv6-racl] size =  128
                   IPV4 Port QoS Lite [qos-lite] size =    0
           FEX IPV4 Port QoS Lite [fex-qos-lite] size =    0
                  IPV4 VLAN QoS Lite [vqos-lite] size =    0
                   IPV4 L3 QoS Lite [l3qos-lite] size =    0
                         Egress IPV4 QoS [e-qos] size =    0
                    Egress IPV6 QoS [e-ipv6-qos] size =    0
                      Egress MAC QoS [e-mac-qos] size =    0
```

```
                              Egress IPV4 VACL [vacl] size =    0
                           Egress IPV6 VACL [ipv6-vacl] size =    0
                             Egress MAC VACL [mac-vacl] size =    0
                              Egress IPV4 RACL [e-racl] size =    0
                          Egress IPV6 RACL [e-ipv6-racl] size =    0
                    Egress IPV4 QoS Lite [e-qos-lite] size =    0
                                 IPV4 L3 QoS [l3qos] size =  640
                               IPV6 L3 QoS [ipv6-l3qos] size =  256
                                 MAC L3 QoS [mac-l3qos] size =    0
                                          Ingress System size =    0
                                           Egress System size =    0
                                             SPAN [span] size =   96
                                   Ingress COPP [copp] size =  128
                         Ingress Flow Counters [flow] size =    0
switch#
```

ACL 関連のテクニカル サポート情報を表示するには、**show tech-support aclmgr** および **show tech-support aclqos** コマンドを使用します。

```
show tech-support aclmgr
show tech-support aclqos
```

ACL ロギングの構成

ACL ロギング

Cisco Nexus デバイスは ACL ロギングをサポートしているため、特定のアクセス コントロール リスト（ACL）にヒットするフローをモニターできます。ACL エントリの機能を有効にするには、オプションの **log** キーワードを使用して特定の ACE を構成します。

ACL ロギング キャッシュの設定

手順の概要

1. switch# **configure terminal**
2. switch(config)# **logging ip access-list cache entries** *num_entries*
3. switch(config)# **logging ip access-list cache interval** *seconds*
4. switch(config)# **logging ip access-list cache threshold** *num_packets*
5. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **logging ip access-list cache entries** *num_entries*	ソフトウェア内にキャッシュする最大ログ エントリ数を設定します。範囲は 0 ～ 1000000 エントリです。デフォルト値は 8000 エントリです。
ステップ 3	switch(config)# **logging ip access-list cache interval** *seconds*	ログの更新の間隔を秒数で設定します。エントリがこの期間非アクティブである場合、そのエントリはキャッシュから削除されます。指定できる範囲は 5 ～ 86400 秒です。デフォルト値は 300 秒です。
ステップ 4	switch(config)# **logging ip access-list cache threshold** *num_packets*	エントリがログに記録されるまでに一致するパケット数を設定します。範囲は 0 ～ 1000000 パケットです。デフォルト値は 0 パケットです。つまり、パケットの一致数によってロギングがトリガーされることはありません。
ステップ 5	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、ログ エントリの最大数を 5000、間隔を 120 秒、しきい値を 500000 に設定する例を示します。

```
switch# configure terminal
switch(config)# logging ip access-list cache entries 5000
switch(config)# logging ip access-list cache interval 120
switch(config)# logging ip access-list cache threshold 500000
switch(config)# copy running-config startup-config
```

インターフェイスへの ACL ロギングの適用

イーサネット インターフェイスおよびポート チャネルに ACL ロギングを適用できます。

始める前に

- ACL を作成します。
- ロギング用に設定された少なくとも 1 つのアクセス コントロール エントリ（ACE）で IP アクセス リストを作成します。

- ACL ロギング キャッシュを設定します。
- ACL ログの一致レベルを設定します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **interface ethernet** *slot/port*
3. switch(config-if)# **ip access-group** *name* **in**
4. （任意） switch(config-if)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **interface ethernet** *slot/port*	イーサネット インターフェイスを指定します。
ステップ 3	switch(config-if)# **ip access-group** *name* **in**	指定されたインターフェイスにACLとログをアタッチします。ACL ロギングは、ACL がハードウェア上のインターフェイスに適用されると有効になります。
ステップ 4	（任意） switch(config-if)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、すべての入力トラフィックに対して acl1 で指定されたロギングにイーサネット インターフェイスを適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# ip access-group acl1 in
switch(config-if)# copy running-config startup-config
```

ACL ログの一致レベルの適用

手順の概要

1. switch# **configure terminal**
2. switch(config)# **acllog match-log-level** *number*

3. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **acllog match-log-level** *number*	ACL ログ（acllog）で記録されるエントリと一致するようにログ レベルを指定します。number は 0 ～ 7 までの値です。デフォルト値は 6 です。 （注） ログ メッセージは、ACL ログ ファシリティ（acllog）のログ レベルとログ ファイルのロギング重大度が、ACL ログの一致ログ レベル設定よりも大きいか同じ場合、ログに入力されます。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

例

次に、ACL ログに記録されるエントリのログ一致レベルを適用する例を示します。

```
switch# configure terminal
switch(config)# acllog match-log-level 3
switch(config)# copy running-config startup-config
```

ログ ファイルのクリア

ログ ファイルおよび NVRAM のメッセージは表示したり消去したりできます。

手順の概要

1. switch# **clear logging ip access-list cache**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **clear logging ip access-list cache**	アクセス制御リスト（ACL）キャッシュをクリアします。

ACL ロギング構成の確認

ACL ロギング構成情報を表示するには、次のいずれかの作業を実行します：

コマンド	目的
switch# **show hardware access-list tcam region**	デバイスで次のリロード時に適用される TCAM サイズを表示します。
switch# **show ip access-lists**	IPv4 ACL の設定を表示します。
switch# **show ipv6 access-lists**	IPv6 ACL の設定を表示します。
switch# **show logging ip access-list cache [detail]**	送信元IPおよび宛先IPアドレス、送信元ポートおよび宛先ポート情報、送信元インターフェイスなど、アクティブなログフローに関する情報を表示します。
switch# **show logging ip access-list status**	拒否フローの最大数、現在の有効なログ間隔と現在の有効なしきい値を表示します。
switch# **show startup-config acllog**	スタートアップ構成のアクセス制御リスト（ACL）ログ ファイルを表示します。
switch# **show startup-config aclmgr [all]**	スタートアップ構成のアクセス制御リスト（ACL）ログ ファイルを表示します。 （注） このコマンドは、スタートアップ コンフィギュレーションのユーザ設定 ACL を表示します。allオプションを使用すると、スタートアップ構成のデフォルト（CoPP構成）とユーザー定義による ACL の両方が表示されます。
switch# **show running-config acllog**	実行構成のアクセス制御リスト（ACL）ログ ファイルを表示します。

コマンド	目的
switch# **show running-config aclmgr [all]**	実行構成のアクセス制御リスト（ACL）ログファイルを表示します。IP ACL の構成および IP ACL が適用されるインターフェイスを含みます。 （注） このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。all オプションを使用すると、スタートアップ構成のデフォルト（CoPP 構成）とユーザー定義による ACL の両方が表示されます。

ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

（注） 小規模 TCAM（TCAM 12 ～ 15）のサイズは変更できません。

手順の概要

1. switch# **configure terminal**
2. **hardware access-list tcam region** { **ifacl** | {**ipv6-qos** | **qos**} | {**ipv6-racl** | **racl**} *tcam_size*
3. **copy running-config startup-config**
4. switch(config)# **show hardware access-list tcam region**
5. switch(config)# **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	**hardware access-list tcam region** { **ifacl** | {**ipv6-qos** | **qos**} | {**ipv6-racl** | **racl**} *tcam_size*	ACL TCAM リージョン サイズを変更します。 • **ifacl**：インターフェイス ACL（ifacl）TCAM リージョンサイズを設定します。エントリの最大数は 1500 です。

	コマンドまたはアクション	目的
		• **qos**：Quality of Service（QoS）TCAM リージョン サイズを設定します。 • **racl**：ルータの ACL（RACL）TCAM リージョン サイズを設定します。 • *tcam_size*：TCAM サイズ。指定できる範囲は 0 ～ 256、512、（256 の倍数）エントリです。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。
ステップ 4	switch(config)# **show hardware access-list tcam region** 例： `switch(config)# show hardware access-list tcam region`	スイッチの次回のリロード時に適用される TCAM サイズを表示します。
ステップ 5	switch(config)# **reload** 例： `switch(config)# reload`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） **copy running-config to startup-config** を保存した後、次回のリロード時に新しいサイズ値が有効になります。

例

次に、RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware access-list tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

```
switch(config)# show hardware accesslist tcam region | exclude "0"



      IPV4 PACL [ifacl] size = 1024
  IPV6 PACL [ipv6-ifacl] size = 1024
    MAC PACL [mac-ifacl] size = 2048
     IPV4 Port QoS [qos] size =  640
```

```
 IPV6 Port QoS [ipv6-qos] size =  256
        IPV4 RACL [racl] size = 2048
   IPV6 RACL [ipv6-racl] size = 1024
     IPV4 L3 QoS [l3qos] size =  640
IPV6 L3 QoS [ipv6-l3qos] size =  256
             SPAN [span] size =   96
     Ingress COPP [copp] size =  128
             Redirect v4 size =  1024
             Redirect v6 size =  2048
```

デフォルトの TCAM リージョン サイズに戻す

手順の概要

1. switch# **configure terminal**
2. switch(config)# **no hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*
3. （任意） switch(config)# **copy running-config startup-config**
4. switch(config)# **reload**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **no hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*	デフォルト ACL TCAM サイズに設定を戻します。
ステップ 3	（任意） switch(config)# **copy running-config startup-config**	リブートおよびリスタート時に実行構成をスタートアップ構成にコピーして、変更を継続的に保存します。
ステップ 4	switch(config)# **reload**	スイッチをリロードします。

例

次に、デフォルトの RACL TCAM リージョンのサイズに戻す例を示します。

```
switch(config)# no hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

仮想端末回線の ACL の設定

仮想端末（VTY）回線とアクセス リストのアドレス間の IPv4 の着信接続と発信接続を制限するには、ライン コンフィギュレーション モードで **access-class** コマンドを使用します。アクセス制限を解除するには、このコマンドの **no** 形式を使用します。

VTY 回線で ACL を設定する場合には、次のガイドラインに従ってください。

- すべての VTY 回線にユーザーが接続できるため、すべての VTY 回線に同じ制約を設定する必要があります。
- エントリ単位の統計情報は、VTY 回線の ACL ではサポートされません。

始める前に

適用する ACL が存在しており、この適用に対してトラフィックをフィルタリングするように設定されていることを確認してください。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **line vty**
3. switch(config-line)# **access-class access-list-number {in | out}**
4. （任意） switch(config-line)# **no access-class access-list-number {in | out}**
5. switch(config-line)# **exit**
6. （任意） switch# **show running-config aclmgr**
7. （任意） switch# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **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 2	switch(config)# **line vty**
	例：
	`switch(config)# line vty`
	`switch(config-line)#`
		ライン 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	switch(config-line)# **access-class access-list-number {in | out}** 例：	着信または発信アクセス制限を指定します。

	コマンドまたはアクション	目的
	switch(config-line)# access-class ozi2 in switch(config-line)#access-class ozi3 out switch(config)#	
ステップ 4	（任意） switch(config-line)# **no access-class access-list-number {in | out}** 例： switch(config-line)# no access-class ozi2 in switch(config-line)# no access-class ozi3 out switch(config)#	着信または発信アクセス制限を削除します。
ステップ 5	switch(config-line)# **exit** 例： switch(config-line)# exit switch#	ライン コンフィギュレーション モードを終了します。
ステップ 6	（任意） switch# **show running-config aclmgr** 例： switch# show running-config aclmgr	スイッチの ACL の実行コンフィギュレーションを表示します。
ステップ 7	（任意） switch# **copy running-config startup-config** 例： switch# copy running-config startup-config	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

例

次に、VTY 回線の in 方向に access-class ozi2 のコマンドを適用する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# line vty
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

VTY 回線の ACL の確認

VTY 回線の ACL 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config aclmgr	スイッチで設定された ACL の実行コンフィギュレーションを表示します。
show users	接続されているユーザーを表示します。
show access-lists *access-list-name*	エントリ単位の統計情報を表示します。

VTY 回線の ACL の設定例

次に、コンソール回線（ttyS0）および VTY 回線（pts/0 および pts/1）の接続ユーザーの例を示します。

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    ttyS0        Aug 27 20:45   .         14425 *
admin    pts/0        Aug 27 20:06 00:46       14176 (172.18.217.82) session=ssh
admin    pts/1        Aug 27 20:52   .         14584 (10.55.144.118)
```

次に、172.18.217.82 を除き、すべての IPv4 ホストへの VTY 接続を許可する例と、10.55.144.118、172.18.217.79、172.18.217.82、172.18.217.92 を除き、すべての IPv4 ホストへの VTY 接続を拒否する例を示します。

```
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
  10 deny ip 172.18.217.82/32 any
  20 permit ip any any
ip access-list ozi2
  10 permit ip 10.55.144.118/32 any
  20 permit ip 172.18.217.79/32 any
  30 permit ip 172.18.217.82/32 any
  40 permit ip 172.18.217.92/32 any


line vty
  access-class ozi in
  access-class ozi2 out
```

次に、ACL のエントリ単位の統計情報をイネーブルにして、IP アクセス リストを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit
switch#
```

次に、in および out 方向で VTY の ACL を適用する例を示します。

```
switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#
```

次に、VTY 回線でアクセス制限を削除する例を示します。

```
switch# configure terminal
```

```
Enter configuration commands, one per line. End
with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#
```

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。