CHAPTER 9

IP ACL の設定

この章では、IP アクセス コントロール リスト（ACL）を設定する手順について説明します。

この章は、次の内容で構成されています。

ACL について

ACL は、トラフィックをフィルタリングするための順番に並べられた一連のルールです。デバイスは、パケットを適用する ACL を決定する際に、パケットをルールに対してテストしていきます。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するルールがない場合は、そのデバイスでのデフォルト ルールが適用されます。デバイスは、許可されたパケットは処理し、拒否されたパケットは廃棄します。詳細については、「暗黙のルール」（P.9-3）を参照してください。

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。

ここでは、次の内容について説明します。

ACL のタイプと適用

ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。

レイヤ 2 トラフィックのフィルタリングでは、次のポート ACL のタイプがサポートされます。

- IP ACL：IPv4 ACL は IP トラフィックだけに適用されます。
- MAC ACL：MAC ACL は非 IP トラフィックにだけ適用されます。

ACL の適用順序

ACL は次の順序で適用されます。

1. 着信ポート ACL
2. 発信ポート ACL

ルールについて

ACL によるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。ルールは実行コンフィギュレーション内に表示されます。ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。

アクセスリスト コンフィギュレーション モードで **permit** または **deny** コマンドを使用すると、ACL にルールを作成できます。これにより、デバイス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。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。すべてのオプションの説明については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』の該当する **permit** および **deny** コマンドを参照してください。

ここでは、次の内容について説明します。

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。送信元と宛先の指定方法は、IP ACL と MAC ACL のどちらを設定するかによって異なります。送信元と宛先の指定方法については、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』の該当する **permit** および **deny** コマンドを参照してください。

プロトコル

IP ACL および MAC ACL では、トラフィックをプロトコルで識別できます。一部のプロトコルは名前で指定できます。たとえば、IP ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。MAC ACL では、プロトコルをそのプロトコルの Ethertype 番号（16 進数）で指定できます。たとえば、MAC ACL ルールの IP トラフィックの指定に 0x0800 を使用できます。

IP ACL では、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。たとえば、Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）を指定するには、115 を使用します。

各タイプの ACL に名前で指定できるプロトコルのリストは、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』の該当する **permit** および **deny** コマンドを参照してください。

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デバイスがトラフィックに適用するルールです。ACL のルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IP ACL には、不一致の IP トラフィックを拒否する次の暗黙ルールがあります。

```
deny ip 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
```

この暗黙ルールによって、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が確実に拒否されます。

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。これらのオプションは、ACL のタイプによって異なります。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- IP ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 4 プロトコル
  - TCP/UDP ポート
  - ICMP タイプおよびコード
  - IGMP タイプ
  - 優先レベル

  - DiffServ コード ポイント（DSCP）値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- MAC ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 3 プロトコル
  - VLAN ID
  - サービス クラス（CoS）

ルールに適用できるすべてのフィルタリング オプションについては、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』の該当する **permit** および **deny** コマンドを参照してください。

シーケンス番号

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。

  ```
  n1000v(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。

  ```
  n1000v(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。

さらに、ACL 内のルールにシーケンス番号を再割り当てすることも可能です。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。

統計

デバイスは IPv4 ACL および MAC ACL に設定する各ルールのグローバル統計を維持できます。1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計数が維持されます。

（注） インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。たとえば、すべての IPv4 ACL の末尾にある暗黙の **deny ip any any** ルールと一致するパケットのカウントはデバイスに維持されません。暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。詳細については、「暗黙のルール」（P.9-3）を参照してください。

IP 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。

注意事項および制約事項

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。

- ほとんどの場合、IP パケットの ACL 処理は、I/O モジュール上で実行されます。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。この場合、速度は遅くなります。
- ACL は、ポート チャネルではサポートされていません。

デフォルト設定

表 9-1 に、IP ACL パラメータのデフォルト設定値を示します。

表 9-1　IP ACL パラメータのデフォルト値

パラメータ	デフォルト
IP ACL	デフォルトでは IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙ルールが適用されます（「暗黙のルール」（P.9-3）を参照）。

IP ACL の設定

ここでは、次の内容について説明します。

IP ACL の作成

デバイスに IPv4 ACL を作成し、これにルールを追加できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **[no] ip access-list** {*name* | **match-local-traffic**}
3. [*sequence-number*] {**permit | deny**} *protocol source destination*
4. **statistics per-entry**
5. **show ip access-lists** *name*
6. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**[no] ip access-list** {*name* | **match-local-traffic**}
	
	例：
	`n1000v(config)# ip access-list acl-01`
	`n1000v(config-acl)#`
	
	例：
	`n1000v(config)# ip access-list match-local-traffic`
	`n1000v(config-acl)#`
		名前付き IP ACL（最大 64 文字）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。
		
		match-local-traffic オプションは、ローカルに生成されたトラフィックのマッチングをイネーブルにします。
		
		no オプションは指定されたアクセス リストを削除します。

	コマンド	目的
ステップ 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* 例： `n1000v(config-acl)# permit ip 192.168.2.0/24 any`	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、『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。
ステップ 4	**statistics per-entry** 例： `n1000v(config-acl)# statistics per-entry`	（任意）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	**show ip access-lists** *name* 例： `n1000v(config-acl)# show ip access-lists acl-01`	（任意）IP ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `n1000v(config-acl)# copy running-config startup-config`	（任意）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 の変更

既存の IPv4 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。詳細については、「IP ACL 内のシーケンス番号の変更」（P.9-10）を参照してください。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **ip access-list** *name*
3. [*sequence-number*] {**permit | deny**} *protocol source destination*
4. **no** {*sequence-number* | {**permit | deny**} *protocol source destination*}
5. [**no**] **statistics per-entry**
6. **show ip access-list** *name*
7. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** **例：** n1000v# config t n1000v(config)#	CLI 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-list** *name* **例：** n1000v(config)# ip access-list acl-01 n1000v(config-acl)#	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	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **例：** n1000v(config-acl)# 100 permit ip 192.168.2.0/24 any	（任意）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 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **例：** n1000v(config-acl)# no 80	（任意）指定したルールを IP ACL から削除します。 **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 1000V Command Reference, Release 4.2(1)SV1(5.1)*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** **例：** n1000v(config-acl)# statistics per-entry	（任意）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。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	**show ip access-lists** *name* **例：** n1000v(config-acl)# show ip access-lists acl-01	（任意）IP ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** **例：** n1000v(config-acl)# copy running-config startup-config	（任意）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 の削除

IP ACL をデバイスから削除できます。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- その 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ます。
- ACL を削除しても、適用されているインターフェイスの設定には影響しません。デバイスは削除された ACL を空であると見なします。

手順の概要

1. **config t**
2. **[no] ip access-list** *name*
3. **show ip access-list** *name* **summary**
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**no ip access-list** *name* **例：** `n1000v(config)# no ip access-list acl-01`	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	**show ip access-list** *name* **summary** **例：** `n1000v(config)# show ip access-lists acl-01 summary`	（任意）IP ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。

手順の概要

1. **config t**
2. **resequence ip access-list** *name starting-sequence-number increment*
3. **show ip access-lists** *name*
4. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**resequence ip access-list** *name starting-sequence-number increment* **例：** `n1000v(config)# resequence access-list ip acl-01 100 10`	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	**show ip access-lists** *name* **例：** `n1000v(config)# show ip access-lists acl-01`	（任意）IP ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** `n1000v(config)# copy running-config startup-config`	（任意）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 のポート ACL としての適用

IPv4 または ACL をレイヤ 2 インターフェイスの物理ポートに適用してポート ACL を設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。
- 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。詳細については、「IP ACL の作成」（P.9-6）または「IP ACL の変更」（P.9-7）を参照してください。
- IP ACL はポート プロファイルに設定することもできます。詳細については、「IP ACL のポート プロファイルへの追加」（P.9-12）の手順を参照してください。

手順の概要

1. **config t**
2. **interface vethernet** *port*
3. **ip port access-group** *access-list* [**in** | **out**]
4. **show running-config aclmgr**
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`n1000v# config t`
	`n1000v(config)#`
		CLI 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	**interface vethernet** *port*
	
	例：
	`n1000v(config)# interface vethernet 40`
	`n1000v(config-if)#`
		指定した vEthernet 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 3	**ip port access-group** *access-list* [**in** | **out**] 例： `n1000v(config-if)# ip port access-group acl-l2-marketing-group in`	インバウンドまたはアウトバウンド IPv4 ACL をインターフェイスに適用します。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	**show running-config aclmgr** 例： `n1000v(config-if)# show running-config aclmgr`	（任意）ACL の設定を表示します。

	コマンド	目的
ステップ 5	**copy running-config startup-config** **例：** `n1000v(config-if)# copy running-config startup-config`	（任意）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 のポート プロファイルへの追加

IP ACL をポート プロファイルに追加するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 「IP ACL の作成」（P.9-6）の手順に従ってこのポート プロファイルに追加する IP ACL をすでに作成しており、その IP ACL 名を知っていること。
- 既存のポート プロファイルを使用する場合は、すでにそのポート プロファイルを作成しており、名前を知っていること。
- 新しいポート プロファイルを作成する場合は、インターフェイス タイプ（イーサネットまたは vEthernet）およびそのプロファイルに付与する名前がわかっていること。
- ポート プロファイルの詳細については、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』を参照してください。
- このポート プロファイルに対して設定する IP アクセス コントロール リストの名前を知っていること。
- アクセス リストのパケット フローの方向を知っています。

手順の概要

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **ip port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

手順の詳細

	コマンド	説明
ステップ 1	**config t** **例：** n1000v# config t n1000v(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	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **例：** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	名前付きポート プロファイルのポート プロファイル 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 port access-group** *name* {**in** | **out**} **例：** n1000v(config-port-prof)# ip port access-group allaccess4 out	着信トラフィックまたは発信トラフィックのポート プロファイルに名前付き ACL を追加します。
ステップ 4	**show port-profile name** *profile-name* **例：** n1000v(config-port-prof)# show port-profile name AccessProf	（任意）確認のためにコンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** **例：** n1000v(config-port-prof)# copy running-config startup-config	（任意）リブート後に永続的な実行コンフィギュレーションを保存し、スタートアップ コンフィギュレーションにコピーして再起動します。

管理インターフェイスへの IP ACL の適用

管理インターフェイス mgmt0 に IPv4 または ACL を適用するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認または実行する必要があります。

- EXEC モードで CLI にログインしていること。
- 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。詳細については、「IP ACL の作成」（P.9-6）または「IP ACL の変更」（P.9-7）を参照してください。

手順の概要

1. **config t**
2. **interface mgmt0**
3. **[no] ip access-group** *access-list* **[in | out]**
4. **show ip access-lists** *access-list*
5. **copy running-config startup-config**

手順の詳細

	コマンド	目的
ステップ 1	**config t** 例： n1000v# config t n1000v(config)#	CLI 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	**interface mgmt0** 例： n1000v(config)# interface mgmt0 n1000v(config-if)#	管理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 3	**[no] ip access-group** *access-list* [**in** | **out**] 例： n1000v(config-if)# ip access-group telnet in n1000v(config-if)#	指定したインバウンド IPv4 ACL またはアウトバウンド IPv4 ACL をインターフェイスに適用します。 no オプションは指定された設定を削除します。
ステップ 4	**show ip access-lists** *access-list* 例： n1000v(config-if)# show ip access-lists telnet summary IP access list telnet statistics per-entry Total ACEs Configured:2 Configured on interfaces: mgmt0 - ingress (Router ACL) Active on interfaces: mgmt0 - ingress (Router ACL)	（任意）ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： n1000v(config-if)# copy running-config startup-config	（任意）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 の設定の確認

IP ACL の設定情報を表示するには、次のコマンドを使用します。

コマンド	目的
show running-config aclmgr	IP ACL の設定および IP ACL が適用されているインターフェイスを含めて、ACL の設定を表示します。
show ip access-lists [*name*]	すべての IPv4 アクセス コントロール リスト（ACL）または特定の IPv4 ACL を表示します。

コマンド	目的
show ip access-list [*name*] **summary**	設定済みのすべての IPv4 ACL または名前付き IPv4 ACL の要約を表示します。
show running-config interface	ACL が適用されたインターフェイスの設定を表示します。

IP ACL のモニタリング

IP ACL のモニタリングには、次のコマンドを使用します。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。IPv4 ACL に **statistics per-entry** コマンドが含まれている場合は、**show ip access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear ip access-list counters	すべての IPv4 ACL または特定の IPv4 ACL の統計情報をクリアします。

IP ACL の設定例

次に、acl-01 という名前の IPv4 ACL を作成し、これをポート ACL として vEthernet インターフェイス 40 に適用する例を示します。

```
ip access-list acl-01
    permit ip 192.168.2.0/24 any
interface vethernet 40
ip port access-group acl-01 in
```

次に、ローカルに生成されたトラフィックのアクセス リスト マッチングをイネーブルにする例を示します。

```
ip access-list match-local-traffic
```

その他の関連資料

IP ACL の実装に関する詳細情報については、次を参照してください。

- 「関連資料」（P.9-16）
- 「標準」（P.9-16）

関連資料

関連項目	参照先
ACL の概念。	*「ACL について」（P.9-1）*
インターフェイスの設定。	『*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(5.1)*』
ポート プロファイルの設定。	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*』
Cisco Nexus 1000V コマンドのすべてのコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上のガイドライン、および例。	『*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

IP ACL 機能の履歴

ここでは、IP ACL のリリース履歴を示します。

機能名	リリース	機能情報
mgmt0 インターフェイスの IP ACL	4.2(1) SV1(4)	
IP ACL	4.0(4)SV1(1)	この機能が導入されました。