CHAPTER 9

IP ACL の設定

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

ここでは、次の内容について説明します。

ACL の概要

ACL は、トラフィックをフィルタリングするためのルールを順序化したリストです。デバイスは、ある ACL がパケットに適用されると判断すると、そのルールと照合してパケットをテストします。最初に一致したルールによって、そのパケットを許可するか拒否するかが決まります。一致するものがなければ、デバイスはデフォルトのルールを適用します。デバイスは、許可されたパケットを処理し、拒否されたパケットはドロップします。詳細については、「暗黙ルール」（P.9-3）を参照してください。

ACL を使用することにより、ネットワークおよび特定のホストを不必要なトラフィックまたは望ましくないトラフィックから保護することができます。たとえば、ACL を使用すれば、高セキュリティ ネットワークからインターネットへの HTTP トラフィックを禁止できます。また、ACL を使用し、特定サイトへの 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、IP ACL 内で目的のサイトを識別するために、そのサイトの IP アドレスを使用します。

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 がトランク ポートに適用される場合、その ACL によってトランク ポートのすべての VLAN 上のトラフィックがフィルタリングされます。

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 IP 以外のトラフィックだけに適用されます。

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

ルールは、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、作成、変更、および削除するものです。ルールは実行コンフィギュレーション内にあります。ACL をインターフェイスに適用する場合、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場合、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。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。トラフィックと照合するルールの基準は、さまざまなオプションを使用して設定します。

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 4.0(4)SV1(3)*』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

各ルールでは、そのルールと一致するトラフィックの送信元および宛先を指定します。送信元と宛先は、特定のホスト、ネットワークまたはホスト グループ、あるいは任意のホストとして指定できます。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 4.0(4)SV1(3)*』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。

プロトコルはどれも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）のトラフィックを 115 として指定できます。

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 4.0(4)SV1(3)*』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。

追加のフィルタリング オプション

追加オプションを使用してトラフィックを識別することもできます。これらのオプションは、ACL のタイプによって異なります。以下のリストには、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 ポートおよび UDP ポート
  - ICMP のタイプとコード
  - IGMP タイプ
  - Precedence レベル
  - Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値
  - ACK、FIN、PSH、RST、SYN、または URG のビット セットを持つ 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
  - Class of Service（CoS; サービス クラス）

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 4.0(4)SV1(3)*』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）。シーケンス番号を使用することにより、次の ACL 作業を簡単に実行できます。

- 既存のルールの間への新しいルールの追加：シーケンス番号を指定することにより、新しいルールを入れる ACL 内の場所を指定できます。たとえば、100 番と 110 番のルールの間に新しいルールを 1 つ挿入する必要がある場合は、その新しいルールにシーケンス番号 105 を割り当てることができます。
- ルールの削除：シーケンス番号を使用しないと、ルールを削除するために次のようにルール全体を入力しなければなりません。

  ```
  n1000v(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  同じルールにシーケンス番号 101 が割り当ててあれば、次のコマンドを入力するだけでこのルールを削除できます。

  ```
  n1000v(config-acl)# no 101
  ```

- ルールの移動：シーケンス番号を使用すると、ACL 内で、あるルールを別の場所に移す必要がある場合、位置を正確に表すシーケンス番号を使用して、そのルールの第 2 インスタンスを追加してから、そのルールの元のインスタンスを削除すれば済みます。このようにすれば、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 内のルールに連続番号（100 と 101 など）が割り当てられていて、それらのルールの間に 1 つまたは複数のルールを挿入しなければならない場合に便利です。

統計情報

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。

始める前に

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 にログインしています。

手順の概要

1. **config t**
2. **ip access-list** *name*
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	**ip access-list** *name* 例： n1000v(config)# ip access-list acl-01 n1000v(config-acl)#	IP 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* 引数に指定できる文字数は、最大 64 文字です。
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 の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 の整数を指定できます。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』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 のルールの追加および削除を実行できます。既存のルールは変更できません。ルールを変更する場合は、そのルールを削除し、目的の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、現在のシーケンス番号では許容できない数のルールを追加する必要がある場合は、**resequence** コマンドを使用することにより、シーケンス番号を再割り当てできます。詳細については、「IP ACL のシーケンス番号の変更」（P.9-9）を参照してください。

始める前に

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 にログインしています。

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 のルールを作成します。シーケンス番号を使用すると、ACL 内のルールの位置を指定できます。シーケンス番号を使用しないと、最後のルールの後ろに追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定できます。 **permit** コマンドと **deny** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

	コマンド	目的
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** コマンドは、さまざまなトラフィック識別方法をサポートしています。詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』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。

始める前に

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 にログインしています。
- 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`	名前を指定した 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 のシーケンス番号の変更

IP ACL 内のルールに割り当てられているすべてのシーケンス番号を変更できます。

始める前に

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 にログインしています。

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 内のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。それ以降の各ルールには、前のルールよりも一定数だけ大きい番号が割り当てられます。番号の差異は、指定した増分によって決まります。*starting-sequence-number* 引数および *increment* 引数は、1 ～ 4294967295 の整数で指定できます。
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。

ポート ACL としての IP ACL 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。

始める前に

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 にログインしています。
- 各インターフェイスにポート ACL を 1 つ適用できます。
- 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.9-5）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、『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*』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。各インターフェイスにポート ACL を 1 つ適用できます。
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。
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	IPv4 ACL の設定を表示します。
show running-config interface	ACL を適用したインターフェイスの設定を表示します。

これらのコマンドの出力フィールドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

IP ACL の統計情報の表示とクリア

IP ACL の統計情報の表示またはクリアを行うには、次のいずれか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。

これらのコマンドの詳細については、『*Cisco Nexus 1000V Command Reference, Release 4.0(4)SV1(3)*』を参照してください。

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
```

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.9-12）
- 「標準規格」（P.9-13）

関連資料

関連項目	マニュアル タイトル
MAC ACL の概念	*「MAC ACL の概要」（P.10-1）*
ポート プロファイル	『*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.0(4)SV1(3)*』

標準規格

標準規格	タイトル
この機能でサポートされる新規または改訂された標準規格はありません。また、この機能による既存の標準規格サポートの変更はありません。	—

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
IP ACL	4.0	この機能が追加されました。