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 の ACL を意味します。

この章は、次の項で構成されています。

ACL について

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。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、そのすべてのルールの条件にパケットを照合し、テストします。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。一致するものがなければ、デバイスは適用可能な暗黙のルールを適用します。デバイスは、許可されたパケットの処理を続行し、拒否されたパケットはドロップします。

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。

ACL のタイプと適用

セキュリティ トラフィック フィルタリングには次のタイプの ACL を使用できます。

IPv4 ACL
Cisco Nexus® 3550-T デバイスは、IPv4 ACL を IPv4 トラフィックだけに適用します。

IP には次の種類のアプリケーションがあります。

ルータ ACL
レイヤ 3 トラフィックのフィルタリング

VTY ACL
仮想テレタイプ（VTY）トラフィックのフィルタリング

Note 次のインターフェイスの ACL で指定された条件に基づいて入力トラフィックをフィルタリングするために、入力ポリシーのみを Cisco Nexus® 3550-T スイッチで構成できます。

- 物理層 3 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
- Switch Virtual Interface（SVI）

次の表に、セキュリティ ACL の適用例の概要を示します。

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
ルータ ACL	• VLAN インターフェイス • 物理層 3 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 • 管理インターフェイス	• IPv4 ACL

ACL の適用順序

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 Ingress ルータ ACL のみを適用します。

パケットが入力 VLAN 内でブリッジされる場合、ルータ ACL は適用されません。

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。ACL の設定によっては、ルールよりも ACL エントリの方が数が多くなることがあります。特に、ルールを設定するときにオブジェクト グループを使用してポリシーベース ACL を実装する場合などです。

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。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。

IP ACL のプロトコル

IPv4 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 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。

IPv4 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。

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。

IP ACL の暗黙ルール

IP 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。

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
```

この暗黙ルールによって、デバイスは不一致 IP トラフィックを確実に拒否します。

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。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。

- 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
  - ICMP タイプおよびコード
  - IGMP タイプ

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しいルールを追加

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。

ルールの削除

シーケンス番号を使用しない場合は、ルールを削除するために、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
```

ルールの移動

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、Cisco NX-OS では、ACL 内ルールのシーケンス番号を再割り当てできます。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 NX-OS では、入力方向でのみ論理演算子をサポートします。

このデバイスは、論理演算ユニット（LOU）というレジスタに、演算子とオペランドの組み合わせを格納します。各タイプの演算子は、次のように LOU を使用します。

eq
LOU には格納されません。

gt
1 LOU を使用します。

lt
1 LOU を使用します。

range
1 LOU を使用します。

IP ACL に対する Session Manager のサポート

Session Manager は IP ACL の構成をサポートしています。この機能を使用すると、ACL の構成を調べて、その構成に必要とされるリソースが利用可能であるかどうかを、リソースを実行中の構成にコミットする前に確認できます。

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。

IP 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。

- 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、1,000 以上のルールが含まれている ACL に対して特に推奨されます。

- 異なるシーケンス番号を持つ重複した ACL エントリは、設定で許可されます。ただし、これらの重複エントリはハードウェア アクセス リストにプログラムされません。
- 最大 62 の一意の ACL を設定できます。各 ACL は、1 つのラベルを持ちます。同じ ACL が複数のインターフェイスで設定される場合、同じラベルが共有されます。ただし、各 ACL が一意のエントリを持つ場合、ACL のラベルは共有されず、そのラベルの上限は 62 です。
- 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。
  - IP オプションがある IPv4 パケット（他の 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）

  レート制限を行うことで、リダイレクト パケットによってスーパーバイザ モジュールに過剰な負荷がかかるのを回避します。

  を展開します。
- VTY ACL 機能はすべての VTY 回線のすべてのトラフィックを制限します。異なる VTY 回線に異なるトラフィックの制限を指定できません。どのルータの ACL も VTY ACL として設定できます。
- 出力 VTY ACL（アウトバウンド方向の VTY 回線に適用される IP ACL）は、ファイル転送プロトコル（TFTP、FTP、SCP、SFTPなど）が出力 VTY ACL 内で明示的に許可されていない限り、スイッチがファイル転送プロトコルによってファイルをコピーするのを禁止します。
- 未定義の ACL をインターフェイスに適用すると、システムは空の ACL と見なし、すべてのトラフィックを許可します。
- ACL ロギングはサポートされていません。
- DoS 攻撃を防ぐため、IPv4 ACL フローの総数はユーザ定義の最大値に制限されます。この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- レイヤ 3 の物理または論理インターフェイスに適用されるルータ ACL がマルチキャスト トラフィックとマッチしません。マルチキャスト トラフィックをブロックする必要がある場合は、代わりに PACL を使用します。
- レイヤ 3 物理インターフェイスおよび SVI では、入力 RACL だけがサポートされます。

IP ACL のデフォルト設定

次の表に、IP ACL パラメータのデフォルト設定を示します。

Table 2: 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。
IP ACL エントリ	1024
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 ACL を作成して、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。

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。
		Note
		ACL が有効な場合、TCP および UDP パケットのみが Cisco Nexus® 3550-T ハードウェアで処理されます。

ステップ 2	次のコマンドを入力します。 **ip 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。

	Command or Action	Purpose
ステップ 3	[*sequence-number*] {**permit** | **deny**} *protocol* {*source-ip-prefix* | *source-ip-mask*} {*destination-ip-prefix* | *destination-ip-mask*}	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。 IPv4 アクセス リストの場合、送信元と接続先の IPv4 プレフィックスを指定できます。これは、最初の連続するビットでのみ一致します。または、アドレスのいずれかのビットに一致する送信元と接続先の IPv4 ワイルドカード マスクを指定できます。
ステップ 4	(Optional) 次のコマンドを入力します。 **show ip 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 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

IP ACL の変更

既存の IPv4 ACL のルールの追加と削除は実行できますが、既存のルールを変更することはできません。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。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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	次のコマンドを入力します。 **ip access-list** *name*
	Example:
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		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	(Optional) [*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** `switch(config-acl)# 100 permit ip 192.168.2.0/24 any`	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。
ステップ 4	(Optional) **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** `switch(config-acl)# no 80`	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。
ステップ 5	(Optional) 次のコマンドを入力します。 **show ip 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 6	(Optional) **copy running-config startup-config** **Example:** `switch(config-acl)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

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。

Before you begin

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。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。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`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	**resequence** {**ip** | **ipv4**} **access-list** *name starting-sequence-number increment* **Example:** `switch(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	(Optional) **show ip access-lists** *name* **Example:** `switch(config)# show ip access-lists acl-01`	IP ACL の設定を表示します。
ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

IP ACL の削除

IP ACL をデバイスから削除できます。

Before you begin

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。削除できるのは、現在適用されている ACL 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。デバイスは削除された ACL を空であると見なします。MAC ACL が構成されているインターフェイスを探すには、summary キーワードを指定して **show ip access-lists** コマンドを使用します。

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。

ステップ 2	次のコマンドを入力します。 **no ip access-list** *name* **Example:** `switch(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	(Optional) 次のコマンドを入力します。 **show ip access-lists** *name* **summary** **Example:** `switch(config)# show ip access-lists acl-01 summary`	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	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

ルータ ACL としての IP ACL の適用

IPv4 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
- VLAN インターフェイス
- 管理インターフェイス

これらのインターフェイス タイプに適用された ACL はルータ ACL と見なされます。

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。

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。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interface ethernet** *slot*/*port*[**.** *number*]
	• **interface port-channel** *channel-number*
	• **interface vlan** *vlan-id*
	• **interface mgmt** *port*
	Example:
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		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	次のコマンドを入力します。 **ip access-group** *access-list* {**in** | **out**} **Example:** `switch(config-if)# ip access-group acl1 in`	IPv4 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 4	(Optional) **show running-config aclmgr** **Example:** `switch(config-if)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch(config-if)# copy running-config startup-config`	実行中の構成を、スタートアップ構成にコピーします。

IP ACL の設定の確認

IP ACL の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。
show running-config aclmgr [**all**]	IP ACL の設定および IP ACL が適用されるインターフェイスを含めて、ACL の実行コンフィギュレーションを表示します。 **Note** 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、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 **Note** 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とユーザー定義による ACL の両方が表示されます。

IP ACL の設定例

acl-01 という名前の IPv4 ACL を作成し、これをポート ACL としてイーサネット インターフェイス 2/1（レイヤ 2 インターフェイス）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 ethernet 2/1
  ip port access-group acl-01 in
```

次に、single-source という名前の VTY ACL を作成し、それを VTY 回線上の入力 IP トラフィックに対して適用する例を示します。この ACL は、通過するすべての TCP トラフィックを許可し、その他のすべての IP トラフィックをドロップします。

```
ip access-list single-source
  permit tcp 192.168.7.5/24 any
  exit
  line vty
  ip access-class single-source in
  show ip access-lists
```

オブジェクト グループの設定の確認

オブジェクト グループの設定情報を表示するには、次のいずれかのコマンドを使用します。

コマンド	目的
show object-group	オブジェクト グループの設定を表示します。
show {**ip** } **access-lists** *name* [**expanded**]	ACL設定の拡張統計情報を表示します。
show running-config aclmgr	オブジェクト グループを含めて、ACL の設定を表示します。

時間範囲設定の確認

時間範囲の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show time-range	時間範囲の設定を表示します。
show running-config aclmgr	すべての時間範囲を含めて、ACL の設定を表示します。

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。