



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, on page 1](#)
- [IP ACL の前提条件, on page 6](#)
- [IP ACL の注意事項と制約事項 \(7 ページ\)](#)
- [IP ACL のデフォルト設定, on page 8](#)
- [IP ACL の設定, on page 9](#)
- [IP ACL の設定の確認, on page 14](#)
- [IP ACL の設定例, on page 15](#)
- [時間範囲の設定, on page 15](#)
- [時間範囲設定の確認, on page 20](#)

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 TCP および UDP 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 Cisco Nexus® 3550-T では、ルータおよび VTY ACL IP アプリケーションのみがサポートされています。



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 チャンネル インターフェイス

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	<ul style="list-style-type: none"> • 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 チャンネル インターフェイス • 管理インターフェイス 	<ul style="list-style-type: none"> • IPv4 ACL <p>Note 出力ルータ ACL は、Cisco Nexus® 3550-T スイッチのアップリンクポートではサポートされません。</p>

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。

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増えることがあります。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。

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

シーケンス番号

デバイスはルールของ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。

既存のルールの中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、それらのルールの中に 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。

時間範囲

時間範囲を使用して、ACL ルールが有効になる時期を制御できます。たとえば、インターフェイスに着信するトラフィックに特定の ACL を適用するとデバイスが判断し、その ACL のあるルールの時間範囲が有効になっていない場合、デバイスは、トラフィックをそのルールと照合しません。デバイスは、そのデバイスのクロックに基づいて時間範囲を評価します。

時間範囲を使用する ACL を適用すると、デバイスはその ACL で参照される時間範囲の開始時または終了時に影響する I/O モジュールをアップデートします。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。

IPv4 の ACL は時間範囲をサポートしています。デバイスがトラフィックに ACL を適用する場合、有効なルールは次のとおりです。

- 時間範囲が指定されていないすべてのルール
- デバイスがその ACL をトラフィックに適用した時点（秒）が時間範囲に含まれているルール

名前が付けられた時間範囲は再利用できます。多くの ACL ルールを設定する場合は、時間範囲を名前ですべて一度設定すれば済みます。時間範囲の名前は最大 64 の英文字で指定します。

時間範囲には、1 つまたは複数のルールで構成されます。これらのルールは次の 2 種類に分類できます。

絶対

特定の開始日時、終了日時、その両方を持つルール、またはそのどちらも持たないルール。絶対時間範囲のルールがアクティブかどうかは、開始日時または終了日時の有無によって、次のように決まります。

- 開始日時と終了日時が両方指定されている：この時間範囲ルールは、現在の時刻が開始日時よりも後で終了日時よりも前の場合にアクティブになります。
- 開始日時が指定され、終了日時は指定されていない：この時間範囲ルールは、現在の時刻が開始日時よりも後である場合にアクティブになります。
- 開始日時は指定されず、終了日時が指定されている：この時間範囲ルールは、現在の時刻が終了日時よりも前である場合にアクティブになります。

- 開始日時も終了日時も指定されていない：この時間範囲ルールは常にアクティブです。

たとえば、新しいサブネットへのアクセスを許可するようにネットワークを設定する場合、そのサブネットをオンラインにする予定日の真夜中からアクセスを許可するような時間範囲を指定し、この時間範囲をそのサブネットに適用する ACL ルールに使用します。デバイスはこのルールを含む ACL を適用する場合、開始日時が過ぎると、この時間範囲を使用するルールの適用を自動的に開始します。

定期

毎週1回以上アクティブになるルール。たとえば、定期時間範囲を使用すると、平日の営業時間中だけ、研究室のサブネットにアクセスできるようにすることができます。デバイスは、そのルールを含む ACL が適用されていて、時間範囲がアクティブな場合にだけ、この時間範囲を使用する ACL ルールを自動的に適用します。



Note デバイスは、時間範囲内のルールの順序に関係なく、時間範囲がアクティブかどうかを判断します。Cisco NX-OS は、時間範囲を編集できるように時間範囲内にシーケンス番号を入れます。

時間範囲には備考を含めることもできます。備考を使用すると、時間範囲にコメントを挿入できます。備考は、最大 100 文字の英数字で指定します。

デバイスは次の方法で時間範囲がアクティブかどうかを判断します。

- 時間範囲に絶対ルールが1つまたは複数含まれている：現在の時刻が1つまたは複数の絶対ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に定期ルールが1つまたは複数含まれている：現在の時刻が1つまたは複数の定期ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に絶対ルールと定期ルールが両方含まれている：現在の時刻が1つまたは複数の絶対ルールと1つ以上の定期ルールの範囲内にある場合に、その時間範囲はアクティブです。

時間範囲に絶対ルールと定期ルールが両方含まれている場合、定期ルールがアクティブになるのは、最低1つの絶対ルールがアクティブな場合だけです。

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。

- 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。
- 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のトラフィックは、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）

Cisco Nexus® 3550-T スイッチでは、リダイレクトされたパケットによってスーパーバイザモジュールが過負荷になるのを防ぐために、ストーム制御設定が使用されます。

ストーム制御については、[トラフィック ストーム制御の設定](#) を参照してください。

- 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。
- 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ことを禁止します。
- 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。
- IP トンネルは、ACL または QoS ポリシーをサポートしません。
- 出力方向の IPv4 ACL ロギングはサポートされていません。
- ACL ロギングは、**ip port access-group** コマンドで設定されたポート ACL と、**ip access-group** コマンドで設定されたルータ ACL にのみ適用されます。

- 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。
- IPv4 ACL ロギングによって生成される syslog エントリ数は、ACL ロギングプロセスで設定されたログレベルによって制限されています。Syslog エントリの数がこの制限を超えると、ロギング機能が一部のロギングメッセージをドロップする場合があります。したがって、IPv4 ACL ロギングは課金ツールや ACL との一致数を正確に把握するための情報源として使用しないでください。
- 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。この動作は、Cisco Nexus® 3550-T スイッチに適用されません。
- 複数のインターフェイスに同じ QoS ポリシーと ACL が適用された場合、ラベルが共有されるのは、QoS ポリシーが no-stats オプションで適用されたときだけです。
- HTTP メソッドに基づくアクセスリストは、Cisco Nexus® 3550-T プラットフォームスイッチおよび Cisco Nexus® 3550-T スイッチではサポートされていません。
- Cisco Nexus® 3550-T スイッチには次の注意事項と制限事項が適用されます。
 - RAACL は、マルチキャスト MAC 宛先アドレスを持つパケットでは照合できません。

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。
オブジェクトグループ	デフォルトではオブジェクトグループは存在しません。
時間範囲	デフォルトでは時間範囲は存在しません。

IP ACL の設定

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。

Before you begin

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: <pre>switch# configure terminal switch(config)#</pre>	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。 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: <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	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。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	<pre>[sequence-number] {permit deny} protocol {source-ip-prefix source-ip-mask} {destination-ip-prefix destination-ip-mask}</pre>	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。 <i>sequence-number</i> 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。

	Command or Action	Purpose
ステップ 4	(Optional) 次のコマンドを入力します。 show ip access-lists <i>name</i> 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。

既存のルールの中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

この機能を使用すると、ACL の設定を調べて、その設定に必要な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 <i>name</i> Example: switch(config)# ip access-list acl-01 switch(config-acl)#	名前指定した 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) [<i>sequence-number</i>] { permit deny } <i>protocol source destination</i> Example:	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

	Command or Action	Purpose
	switch(config-acl)# 100 permit ip 192.168.2.0/24 any	番号を指定しないと、ルールは ACL の末尾に追加されます。 <i>sequence-number</i> 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 { <i>sequence-number</i> { permit deny } <i>protocol source destination</i> } 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 <i>name</i> 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。

Before you begin

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

	Command or Action	Purpose
ステップ 2	resequence {ip ipv4} access-list name starting-sequence-number increment Example: <pre>switch(config)# resequence access-list ip acl-01 100 10</pre>	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。 <i>starting-sequence-number</i> 引数と <i>increment</i> 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: <pre>switch(config)# show ip access-lists acl-01</pre>	IP ACL の設定を表示します。
ステップ 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	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。

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: <pre>switch# configure terminal switch(config)#</pre>	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。 no ip access-list name Example:	名前指定した 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
	<pre>switch(config)# no ip access-list acl-01</pre>	
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: <pre>switch(config)# show ip access-lists acl-01 summary</pre>	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: <pre>switch(config)# copy running-config startup-config</pre>	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 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

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: <pre>switch# configure terminal switch(config)#</pre>	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。 <ul style="list-style-type: none"> • interface ethernet slot/port • interface port-channel channel-number Example: <pre>switch(config)# interface ethernet 1/3 switch(config-if)#</pre>	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。

	Command or Action	Purpose
ステップ 3	次のコマンドを入力します。 ip access-group access-list 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。

コマンド	目的
<code>show startup-config aclmgr [all]</code>	<p>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。</p> <p>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。</p>

IP ACL の設定例

次に、`acl-01` という名前の IPv4 ACL を作成して、これを RACL としてイーサネット インターフェイス 1/1 (レイヤ 3 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 1/1
  ip port access-group acl-01 in
```

時間範囲の設定

時間範囲の作成

デバイス上で時間範囲を作成し、これにルールを追加できます。

Procedure

	Command or Action	Purpose
ステップ 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	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。

	Command or Action	Purpose
ステップ 2	time-range name Example: <pre>switch(config)# time-range workday-daytime switch(config-time-range)#</pre>	時間範囲を作成し、時間範囲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] periodic weekday time to [weekday] time Example: <pre>switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59</pre>	指定開始日時と終了日時の間（両端を含める）の1日以上連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [sequence-number] periodic list-of-weekdays time to time Example: <pre>switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00</pre>	<i>list-of-weekdays</i> 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。 <i>list-of-weekdays</i> 引数の値には次のキーワードも使用できます。 <ul style="list-style-type: none"> • daily : 1 週間のすべての曜日 • weekdays : 月曜日から金曜日まで • weekend : 土曜日から日曜日まで
ステップ 5	(Optional) [sequence-number] absolute start time date [end time date] Example: <pre>switch(config-time-range)# absolute start 1:00 15 march 2013</pre>	start キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。 end キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	(Optional) [sequence-number] absolute [start time date] end time date Example: <pre>switch(config-time-range)# absolute end 23:59:59 31 may 2013</pre>	end キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。 start キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) show time-range name Example: <pre>switch(config-time-range)# show time-range workday-daytime</pre>	時間範囲の設定を表示します。
ステップ 8	(Optional) copy running-config startup-config Example: <pre>switch(config-time-range)# copy running-config startup-config</pre>	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。

時間範囲の変更

既存の時間範囲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。

既存のルールの中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。

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	time-range name Example: switch(config)# time-range workday-daytime switch(config-time-range)#	特定の時間範囲の時間範囲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] periodic weekday time to [weekday] time Example: switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59	指定開始日時と終了日時の間（両端を含める）の1日以上連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	(Optional) [sequence-number] periodic list-of-weekdays time to time Example: switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00	<i>list-of-weekdays</i> 引数で指定された曜日の、指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。 <i>list-of-weekdays</i> 引数の値には次のキーワードも使用できます。 <ul style="list-style-type: none"> • daily : 1 週間のすべての曜日 • weekdays : 月曜日から金曜日まで • weekend : 土曜日から日曜日まで
ステップ 5	(Optional) [sequence-number] absolute start time date [end time date] Example: switch(config-time-range)# absolute start 1:00 15 march 2013	start キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。 end キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。

	Command or Action	Purpose
ステップ 6	(Optional) <code>[sequence-number] absolute [start time date] end time date</code> Example: <pre>switch(config-time-range) # absolute end 23:59:59 31 may 2013</pre>	end キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。 start キーワードを省略すると、そのルールは終了日時を過ぎるまでずっと有効です。
ステップ 7	(Optional) no <code>{sequence-number periodic arguments . . . absolute arguments . . . }</code> Example: <pre>switch(config-time-range) # no 80</pre>	時間範囲から特定のルールを削除します。
ステップ 8	(Optional) show time-range name Example: <pre>switch(config-time-range) # show time-range workday-daytime</pre>	時間範囲の設定を表示します。
ステップ 9	(Optional) copy running-config startup-config Example: <pre>switch(config-time-range) # copy running-config startup-config</pre>	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。

時間範囲の削除

デバイスから時間範囲を削除できます。

Before you begin

その時間範囲が ACL ルールのいずれかに使用されているかどうかを確認します。削除できるのは、ACL ルールに使用されている時間範囲です。ACL ルールに使用されている時間範囲を削除しても、その ACL が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時間範囲を使用する ACL ルールを空であると見なします。

Procedure

	Command or Action	Purpose
ステップ 1	configure terminal Example: <pre>switch# configure terminal switch(config) #</pre>	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 time-range name Example: <pre>switch(config) # no time-range daily-workhours</pre>	名前を指定した時間範囲を削除します。

	Command or Action	Purpose
ステップ 3	(Optional) show time-range Example: switch(config-time-range)# show time-range	すべての時間範囲の設定を表示します。 削除された時間範囲は表示されません。
ステップ 4	(Optional) copy running-config startup-config Example: 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。

時間範囲のシーケンス番号の変更

時間範囲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。

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 time-range name starting-sequence-number increment Example: switch(config)# resequence time-range daily-workhours 100 10 switch(config)#	時間範囲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。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。
ステップ 3	(Optional) show time-range name Example: switch(config)# show time-range daily-workhours	時間範囲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。

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
<code>show time-range</code>	時間範囲の設定を表示します。
<code>show running-config aclmgr</code>	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。