CHAPTER 10

IP ACL の設定

この章では、NX-OS デバイスの IP Access Control List（ACL; アクセス コントロール リスト）の設定方法を説明します。

（注） 特に指定がなければ、IP ACL は IPv4 ACL を意味しています。

この章の内容は次のとおりです。

ACL の概要

ACL は、トラフィックのフィルタリングに使用するルールを順序化したリストです。各ルールには、そのルールと一致するためにパケットが満たさなければならないひとまとまりの条件が指定されています。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、デバイスは適用可能な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の処理を続行し、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.10-6）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 のタイプとアプリケーション

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 ACLs — IPv4 トラフィックのみに適用されます。
- Media Access Control（MAC; メディア アクセス制御）ACL — IP 以外のトラフィックのみに適用されます。詳細については、「MAC ACL の概要」（p.11-2）を参照してください。
- セキュリティ グループ ACL（SGACL）— Cisco TrustSec によってタグ付けされたトラフィックに適用されます。詳細については、第 9 章「Cisco TrustSec の設定」を参照してください。

IPv4 ACL および MAC ACL には次の 3 つのアプリケーション タイプがあります。

- ポート ACL — レイヤ 2 トラフィックをフィルタリングします。
- ルータ ACL — レイヤ 3 トラフィックをフィルタリングします。
- VLAN ACLVLAN トラフィックをフィルタリングします。

表 10-1 に、セキュリティ ACL のアプリケーションの概要を示します。

表 10-1　セキュリティ ACL のアプリケーション

アプリケーション	サポートされるインターフェイス	サポートされる ACL タイプ
ポート ACL	• レイヤ 2 インターフェイス • レイヤ 2 イーサネット ポート チャネル インターフェイス 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。	• IPv4 ACL • MAC ACL
ルータ ACL	• VLAN インターフェイス（Switch Virtual Interface［SVI; スイッチ仮想インターフェイス］とも言う） （注）　VLAN インターフェイスを設定するには、その前に VLAN インターフェイスをグローバルにイネーブル化する必要があります。詳細については、『*Cisco NX-OS Interface Configuration Guide*』を参照してください。 • 物理レイヤ 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 • トンネル • 管理インターフェイス	• IPv4 ACL （注）　MAC ACL はレイヤ 3 インターフェイスではサポートされません。
VLAN ACL	• VLAN VLAN ACL についての詳細は、第 12 章「VLAN ACL の設定」を参照してください。	• IPv4 ACL • MAC 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、次の順序で ACL を適用します。

1. ポート ACL
2. 入力 VACL
3. 入力ルータ ACL
4. SGACL
5. 出力ルータ ACL
6. 出力 VACL

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。図 10-1 に、デバイスが ACL を適用する順序を示します。

図 10-1　ACL の適用順序

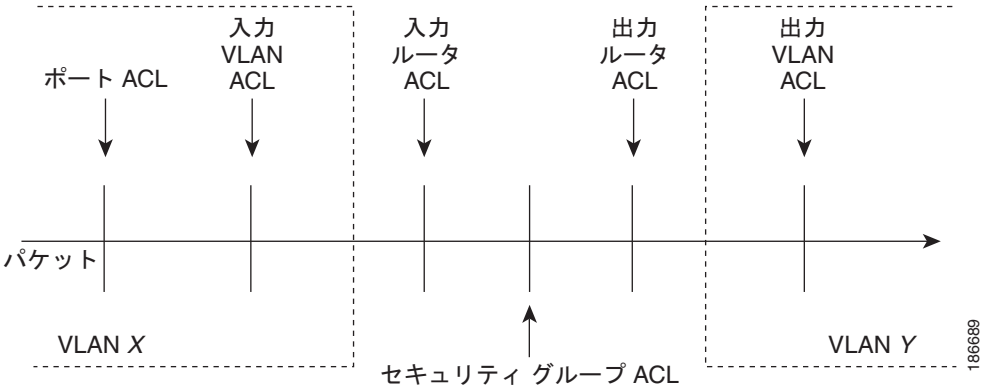
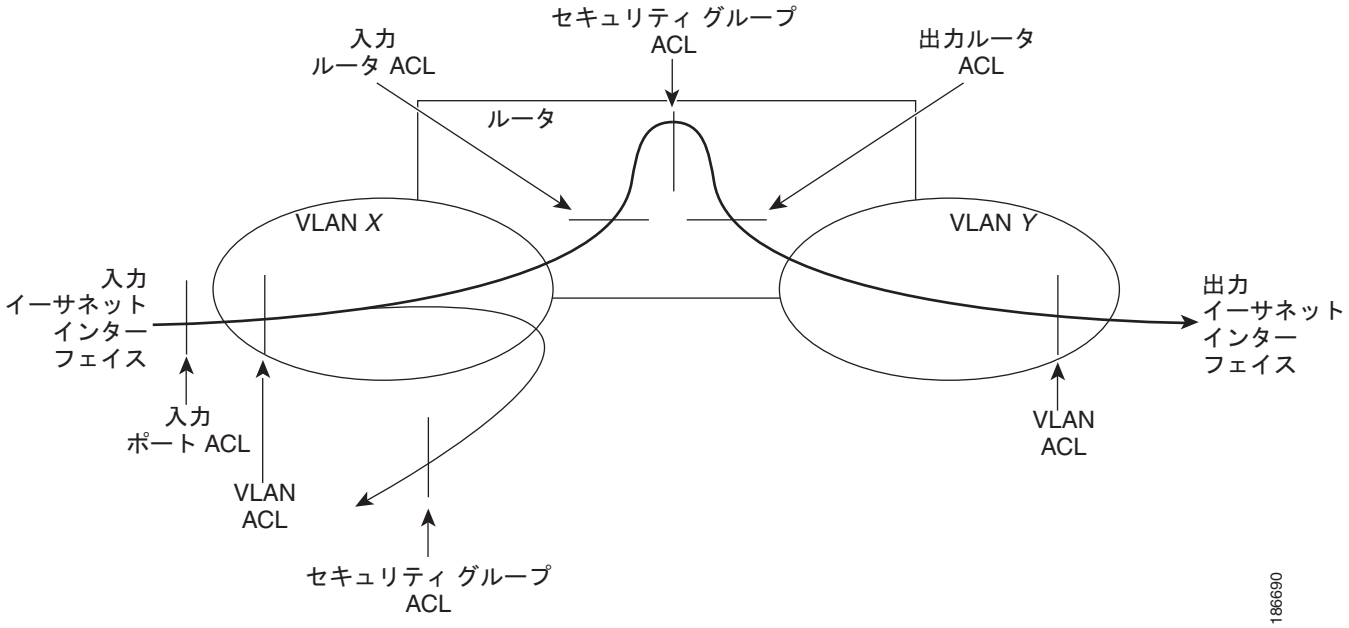


図 10-2 は、各 ACL の適用場所を示しています。赤いパスは送信元とは異なるインターフェイス上の宛先に送信されるパケットを表しています。青いパスは同じ VLAN 内でブリッジされるパケットを表しています。

デバイスは適用可能な ACL だけを適用します。たとえば、入力ポートがレイヤ 2 ポートの場合、VLAN インターフェイスである VLAN 上のトラフィックには、ポート ACL とルータ ACL が両方とも適用される可能性があります。さらに、その VLAN に VACL が適用される場合、デバイスはその VACL も適用します。

SGACL の詳細については、第 9 章「Cisco TrustSec の設定」を参照してください。

図 10-2　ACL とパケット フロー



ルールについて

アクセスリスト コンフィギュレーション モードで **permit** コマンドまたは **deny** コマンドを使用すると、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。

（注）　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についての説明は、『*Cisco NX-OS Security Command Reference*』の **permit** コマンドおよび **deny** コマンドの該当項目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、IPv4 ACL と MAC ACL のどちらを設定するの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 NX-OS Security Command Reference*』の該当する **permit** コマンドおよび **deny** コマンドを参照してください。

プロトコル

IPv4 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。便宜上、プロトコルを名前で指定することもできます。たとえば、IPv4 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。

IPv4 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 NX-OS Security Command Reference*』の該当する **permit** コマンドおよび **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。

すべての IPv4 ACL には、次の暗黙ルールがあります。

```
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。

すべての MAC ACL には、次の暗黙ルールがあります。

```
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。

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。

- IPv4 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
  - 確立済みの TCP 接続
- 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 NX-OS Security Command Reference*』の該当する **permit** コマンドおよび **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。

  ```
  switch(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。

  ```
  switch(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、NX-OS では 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。

論理演算子と論理演算ユニット

TCP トラフィックおよび UDP トラフィックの IP ACL ルールでは、ポート番号に基づいたトラフィック フィルタリングに論理演算子を使用できます。このデバイスは、Logical Operator Unit（LOU; 論理演算ユニット）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。Cisco Nexus 7000 シリーズ デバイスは 104 の LOU をサポートしています。

各タイプの演算子は、次のように LOU を使用します。

- eqLOU には格納されません。
- gt — 1/2 LOU を使用します。
- Lt — 1/2 LOU を使用します。
- Neq — 1/2 LOU を使用します。
- range — 1 LOU を使用します。

デバイスは、次の場合に演算子とオペランドの組み合わせを LOU に格納します。

- 演算子とオペランドのどちらかが、他のルールで使用されている演算子・オペランドの組み合わせとは異なっている場合、その組み合わせが LOU に格納されます。

  たとえば、演算子・オペランドの組み合わせ、「gt 10」と「gt 11」は、LOU の半分に別々に格納されます。組み合わせ「gt 10」と「lt 10」も、別々に格納されます。

- 演算子・オペランドの組み合わせがルール内の送信元ポートに適用されるか、宛先ポートに適用されるかによって 使用される LOU は変わってきます。同一の組み合わせでも、一方が送信元ポートに適用され、もう一方が宛先ポートに適用される場合は、別々に格納されます。

  たとえば、あるルールで演算子・オペランドの組み合わせ「gt 10」が送信元ポートに適用され、別のルールで「gt 10」が宛先ポートに適用される場合、それぞれが LOU の半分に格納されるので、LOU 全体が 1 つ使用されることになります。ほかに「gt 10」を使用するルールがあっても、これ以上 LOU は使用されません。

ロギング

ルールに一致するパケットに関する情報ログ メッセージの作成をイネーブルにできます。ログ メッセージには、パケットについての次の情報が含まれます。

- ACL 名
- デバイスがそのパケットを許可するか拒否するか
- プロトコル
- TCP、UDP、または ICMP のいずれのパケットか、あるいは、番号が付けられただけのパケットか
- 送信元と宛先のアドレス
- 送信元と宛先のポート番号（該当する場合）

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 ACL と MAC 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 1 度設定すればすみます。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。

- 絶対ルール — 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あとで終了日時より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あと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。

- 定期ルール — 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。

（注）　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。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 の英文字で指定します。

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 つまたは複数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。

PB ACL

デバイスは Policy-Based ACL（PBACL; ポリシーベース ACL）をサポートしています。PBACL を使用すると、オブジェクト グループ全体にアクセス コントロール ポリシーを適用できます。オブジェクト グループは、IP アドレスのグループまたは TCP ポートもしくは UDP ポートのグループです。ルール作成時に、IP アドレスやポートを指定するのではなく、オブジェクト グループを指定できます。

IPv4 ACL の設定にオブジェクト グループを使用すると、ルールの送信元または宛先に対してアドレスまたはポートの追加や削除を行う場合に、ACL を簡単にアップデートできます。たとえば、3 つのルールが同じ IP アドレス グループ オブジェクトを参照している場合は、3 つのすべてのルールを変更しなくても、オブジェクトに IP アドレスを追加すれば済みます。

PBACL を使用しても、インターフェイスに ACL を適用する際にその ACL が必要とするリソースは減りません。PBACL 適用時に、デバイスはオブジェクト グループを参照する各ルールを展開し、グループ内の各オブジェクトとルールが 1 対 1 になるようにします。あるルールに、送信元と宛先が両方ともオブジェクト グループとして指定されている場合、この PBACL を適用する際に作成されるルールの数は、送信元グループ内のオブジェクト数に宛先グループ内のオブジェクト数をかけた値になります。

ポート、ルータ、VLAN の ACL には、次のオブジェクト グループ タイプが適用されます。

- IPv4 アドレス オブジェクト グループ — IPv4 ACL ルールで送信元または宛先のアドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。
- プロトコル ポート オブジェクト グループ — IPv4 TCP および UDP ルールで送信元または宛先のポートの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**portgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

統計情報

このデバイスは IPv4 ACL および MAC ACL の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。

IP ACL 統計の表示については、「IP ACL の統計情報の表示とクリア」（p.10-19）を参照してください。MAC ACL 統計の表示については、「MAC ACL の統計情報の表示とクリア」（p.11-9）を参照してください。

IP ACL に対する Session Manager のサポート

Session Manager は IP ACL および MAC ACL の設定をサポートしています。この機能を使用すると、ACL の設定を調べて、設定の実行をコミットする前に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確認できます。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。

バーチャライゼーション サポート

Virtual Device Context（VDC; バーチャル デバイス コンテキスト）では、IP ACL および MAC ACL に次の事項が適用されます。

- ACL は各 VDC に固有です。ある VDC に作成した ACL を別の VDC に使用することはできません。
- ACL が複数の VDC に共有されることはないので、ACL 名は他の VDC に再利用できます。
- デバイスは、ACL やルールを VDC 単位では制限しません。

IP ACL のライセンス要件

この機能のライセンス要件は次の表のとおりです。

製品	ライセンス要件
NX-OS	IP ACLにはライセンスは必要ありません。ライセンス パッケージに含まれていない機能は、Cisco NX-OS システム イメージにバンドルされており、追加料金なしで利用できます。NX-OS のライセンス スキームに関する詳細は、『*Cisco NX-OS Licensing Guide*』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。

- 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、設定の実行をコミットする前に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確認できます。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。
- 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。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、I/O モジュールでの処理よりも速度が遅くなります。パケットがスーパーバイザ モジュールで処理されるのは、次の場合です。
  - 管理インターフェイス トラフィックが常にスーパーバイザ モジュールで処理される場合
  - レイヤ 3 インターフェイスに多数のルールで構成される出力 ACL が適用されている場合、そのインターフェイスを出る IP パケットは、スーパーバイザ モジュールに送信されることがあります。
- 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。
- IP ACL を VLAN インターフェイスに適用するためには、VLAN インターフェイスをグローバルにイネーブル化する必要があります。VLAN インターフェイスの詳細については、『*Cisco NX-OS Interfaces Configuration Guide*』を参照してください。

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。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **ip access-list** *name*
3. [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. **statistics**
5. **show ip access-lists** *name*
6. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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-list** *name*
	
	例：
	`switch(config)# ip access-list acl-01`
	`switch(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：** `switch(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 の間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 NX-OS Security Command Reference*』を参照してください。

	コマンド	目的
ステップ 4	**statistics** **例：** `switch(config-acl)# statistics`	（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：** `switch(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：** `switch(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。既存のルールを変更することはできません。ルールを変更したい場合は、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.10-15）を参照してください。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

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**
6. **show ip access-list** *name*
7. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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-list** *name*
	
	例：
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		名前を指定する ACL の IP ACL コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **例**： `switch(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 の間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 NX-OS Security Command Reference*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **例**： `switch(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 NX-OS Security Command Reference*』を参照してください。
ステップ 5	[**no**] **statistics** **例**： `switch(config-acl)# statistics`	（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**： `switch(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**： `switch(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。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

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。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 を空であるとみなします。

手順の概要

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

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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	**no ip access-list** *name* **例：** switch(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 running-config aclmgr** **例：** switch(config)# show running-config aclmgr	（任意）ACL の設定を表示します。削除された IP ACL は表示されません。
ステップ 4	**copy running-config startup-config** **例：** switch(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。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

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**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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 access-list** *name starting-sequence-number increment* **例：** switch(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。その後ろの各ルールには、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。

	コマンド	目的
ステップ 3	**show ip access-lists** *name* **例：** `switch(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：** `switch(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。

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。

- 物理レイヤ 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
- VLAN インターフェイス
- トンネル
- 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 とみなされます。

作業を開始する前に

適用する ACL が存在し、必要な方法で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ます。詳細については、「IP ACL の作成」（p.10-12）または「IP ACL の変更」（p.10-13）を参照してください。

手順の概要

1. **config t**
2. **interface *ethernet*** *slot/port*[**.***number*]

   interface *port-channel* *channel-number*[**.***number*]

   interface *tunnel* *tunnel-number*

   interface *vlan* *vlan-ID*

   interface *mgmt* *port*
3. **ip access-group** *access-list* {***in*** | ***out***}
4. **show running-config aclmgr**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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	**interface *ethernet*** *slot/port*[**.***number*] **例：** switch(config)# interface ethernet 2/3 switch(config-if)#	レイヤ 2 またはレイヤ 3 物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。レイヤ 3 サブインターフェイスのコンフィギュレーション モードを開始するには、*number* 引数を指定します。
	interface *port-channel* *channel-number*[**.***number*] **例：** switch(config)# interface port-channel 5 switch(config-if)#	ポート チャネル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。レイヤ 3 ポート チャネル インターフェイスのコンフィギュレーション モードを開始するには、*number* 引数を指定します。
	interface *tunnel* *tunnel-number* **例：** switch(config)# interface tunnel 13 switch(config-if)#	トンネル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。
	interface *vlan* *vlan-ID* **例：** switch(config)# interface vlan 11 switch(config-if)#	VLAN 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。
	interface *mgmt* *port* **例：** switch(config)# interface mgmt 0 switch(config-if)#	管理ポート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 access-group** *access-list* {***in*** | ***out***} **例：** switch(config-if)# ip access-group acl-120 out	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	**show running-config aclmgr** **例：** switch(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：** switch(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。

ポート ACL としての IP ACL の適用

IPv4 ACL は、レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）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 とみなされます。

作業を開始する前に

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。詳細については、「IP ACL の作成」（p.10-12）または「IP ACL の変更」（p.10-13）を参照してください。

手順の概要

1. **config t**
2. **interface *ethernet*** *slot/port*

   interface *port-channel* *channel-number*
3. **ip port access-group** *access-list* ***in***
4. **show running-config aclmgr**
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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	**interface *ethernet*** *slot/port* **例：** switch(config)# interface ethernet 2/3 switch(config-if)#	レイヤ 2 またはレイヤ 3 物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。
	interface *port-channel* *channel-number* **例：** switch(config)# interface port-channel 5 switch(config-if)#	ポート チャネル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*** **例：** switch(config-if)# ip port access-group acl-l2-marketing-group 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 でサポートされているのは、インバウンド フィルタリングだけです。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：** switch(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：** switch(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。

VACL としての IP ACL の適用

IP ACL は VACL として適用できます。IPv4 ACL を使用した VACL の作成方法については、「VACL の作成または変更」（p.12-5）を参照してください。

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 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	IP 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に関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

IP ACL の統計情報の表示とクリア

各ルールと一致したパケット数を含めて、IP ACL についての統計情報を表示するには、**show ip access-lists** コマンドを使用します。このコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

IPv4 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。IPv4 ACL に **statistics** 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。

これらのコマンドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

IP ACL の設定例

acl-01 という名前の IPv4 ACL を作成し、これをイーサネット 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 access-group acl-01 in
```

オブジェクト グループの設定

IPv4 ACL の ACL ルールに送信元と宛先のアドレスおよびプロトコル ポートを指定する際に、オブジェクト グループを使用できます。

ここでは、次の内容について説明します。

オブジェクト グループに対する Session Manager のサポート

Session Manager はオブジェクト グループの設定をサポートしています。この機能を使用すると、設定セッションを作成し、オブジェクト グループの設定変更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。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。

IPv4 アドレス オブジェクト グループの作成および変更

IPv4 アドレス グループ オブジェクトの作成および変更を実行できます。

手順の概要

1. **config t**
2. **object-group ip address** *name*
3. [*sequence-number*] {**host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*}

   no {*sequence-number* | **host** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*}
4. **show object-group** *name*
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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	**object-group ip address** *name*
	
	例：
	`switch(config)# object-group ip address ipv4-addr-group-13`
	`switch(config-ipaddr-ogroup)#`
		IPv4 アドレス オブジェクト グループを作成し、IPv4 アドレス オブジェクト グループ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	[*sequence-number*] {***host*** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*} **例**： `switch(config-ipaddr-ogroup)# host 10.99.32.6`	オブジェクト グループのエントリを作成します。作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または **host** コマンドを省略してホストのネットワークを指定します。
	no [*sequence-number* | ***host*** *IPv4-address* | *IPv4-address network-wildcard* | *IPv4-address/prefix-len*} **例**： `switch(config-ipaddr-ogroup)# no host 10.99.32.6`	オブジェクト グループのエントリを削除します。オブジェクト グループから削除するエントリごとに、**no** 形式の **host** コマンドを使用します。
ステップ 4	**show object-group** *name* **例**： `switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13`	(任意) オブジェクト グループの設定を表示します。
ステップ 5	**copy running-config startup-config** **例**： `switch(config-ipaddr-ogroup)# 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。

プロトコル ポート オブジェクト グループの作成および変更

プロトコル ポート オブジェクト グループの作成および変更を実行できます。

手順の概要

1. **config t**
2. **object-group ip port** *name*
3. [*sequence-number*] *operator port-number* [*port-number*]

   no {*sequence-number* | *operator port-number* [*port-number*]}
4. **show object-group** *name*
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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	**object-group ip port** *name*
	
	例：
	`switch(config)# object-group ip port NYC-datacenter-ports`
	`switch(config-port-ogroup)#`
		プロトコル ポート オブジェクト グループを作成し、ポート オブジェクト グループ コンフィギュレーション モードを開始します。

	コマンド	目的
ステップ 3	[*sequence-number*] *operator port-number* [*port-number*] 例： `switch(config-port-ogroup)# eq 80`	オブジェクト グループのエントリを作成します。作成するエントリごとに、次の演算子コマンドを 1 つ使用します。 • **eq** • **gt** • **lt** • **neq** • **range** （注）　**range** コマンドだけは、2 つの *port-number* 引数を必要とします。
	no {*sequence-number* | *operator port-number* [*port-number*]} 例： `switch(config-port-ogroup)# no eq 80`	オブジェクト グループからエントリを削除します。削除するエントリごとに、該当する演算子コマンドを **no** 形式で使用します。
ステップ 4	**show object-group** *name* 例： `switch(config-port-ogroup)# show object-group NYC-datacenter-ports`	(任意) オブジェクト グループの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-port-ogroup)# 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。

オブジェクト グループの削除

IPv4 アドレス オブジェクト グループまたはプロトコル オブジェクト グループを削除できます。

手順の概要

1. **config t**
2. **no object-group** {**ip address** | **ip port**} *name*
3. **show object-group**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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	**no object-group** {**ip address** | **ip port**} *name* **例：** switch(config)# no object-group ip address ipv4-addr-group-A7	指定したオブジェクト グループを削除します。
ステップ 3	**show object-group** **例：** switch(config)# show object-group	（任意）すべてのオブジェクト グループを表示します。削除されたオブジェクト グループは表示されません。
ステップ 4	**copy running-config startup-config** **例：** switch(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。

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 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。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

時間範囲の設定

ここでは、次の内容について説明します。

時間範囲に対する Session Manager のサポート

Session Manager は時間範囲の設定をサポートしています。この機能を使用すると、設定セッションを作成し、時間範囲の設定変更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。Session Manager についての詳細は、『*Cisco NX-OS System Management Guide*』を参照してください。

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。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **time-range** *name*
3. [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*
   [*sequence-number*] **periodic** [*list-of-weekdays*] *time* **to** *time*
   [*sequence-number*] **absolute** ***start*** *time date* [***end*** *time date*]
   [*sequence-number*] **absolute** [***start*** *time date*] ***end*** *time date*
4. **show time-range** *name*
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*
	
	例：
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		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。

	コマンド	目的
ステップ 3	[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **例：** `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 日以上の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。
	[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **例：** `switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00`	*list-of-weekdays* 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。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • ***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
	[*sequence-number*] **absolute start** *time date* [**end** *time date*] **例：** `switch(config-time-range)# absolute start 1:00 15 march 2008`	***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ルールを作成します。***end*** キーワードを省略すると、そのルールは開始日時を過ぎると常に有効になります。
	[*sequence-number*] **absolute** [start *time date*] **end** *time date* **例：** `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	***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常に有効です。
ステップ 4	**show time-range** *name* **例：** `switch(config-time-range)# show time-range workday-daytime`	（任意）時間範囲の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config-time-range)# 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。

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。既存のルールを変更することはできません。ルールを変更したい場合は、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、「時間範囲のシーケンス番号の変更」（p.10-28）を参照してください。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **time-range** *name*
3. [*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*
   [*sequence-number*] **periodic** [*list-of-weekdays*] *time* **to** *time*
   [*sequence-number*] **absolute** ***start*** *time date* [***end*** *time date*]
   [*sequence-number*] **absolute** [***start*** *time date*] ***end*** *time date*
   no {*sequence-number* | **periodic** . . . | **absolute** . . .}
4. **show time-range** *name*
5. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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*
	
	例：
	`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。

	コマンド	目的
ステップ 3	[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time* **例：** `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 日以上の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。
	[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time* **例：** `switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00`	*list-of-weekdays* 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。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • ***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
	[*sequence-number*] **absolute start** *time date* [**end** *time date*] **例：** `switch(config-time-range)# absolute start 1:00 15 march 2008`	***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ルールを作成します。***end*** キーワードを省略すると、そのルールは開始日時を過ぎると常に有効になります。
	[*sequence-number*] **absolute** [**start** *time date*] **end** *time date* **例：** `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	***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常に有効です。
	no {*sequence-number* | **periodic** *arguments. . .* | **absolute** *arguments. . .*} **例：** `switch(config-time-range)# no 80`	時間範囲から特定のルールを削除します。
ステップ 4	**show time-range** *name* **例：** `switch(config-time-range)# show time-range workday-daytime`	（任意）時間範囲の設定を表示します。
ステップ 5	**copy running-config startup-config** **例：** `switch(config-time-range)# 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。

時間範囲の削除

デバイスから時間範囲を削除できます。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

その時間範囲が ACL ルールのど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みなします。

手順の概要

1. **config t**
2. **no time-range** *name*
3. **show time-range**
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`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	**no time-range** *name* **例**： `switch(config)# no time-range daily-workhours`	名前を指定した時間範囲を削除します。
ステップ 3	**show time-range** **例**： `switch(config-time-range)# show time-range`	（任意）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	**copy running-config startup-config** **例**： `switch# 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。

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。

作業を開始する前に

正しい VDC 内にいることを確認します（あるいは、**switch to vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **config t**
2. **resequence time-range** *name starting-sequence-number increment*
3. **show time-range** *name*
4. **copy running-config startup-config**

詳細な手順

	コマンド	目的
ステップ 1	**config t** **例：** switch# config t 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* **例：** 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。その後ろの各ルールには、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。
ステップ 3	**show time-range** *name* **例：** switch(config)# show time-range daily-workhours	（任意）時間範囲の設定を表示します。
ステップ 4	**copy running-config startup-config** **例：** switch(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。

時間範囲の設定の確認

時間範囲の設定情報を表示するには、次の作業を実行します。

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。

これらのコマンドの出力フィールドに関する詳細は、『*Cisco NX-OS Security Command Reference*』を参照してください。

デフォルト設定

表 10-2 に IP ACL パラメータのデフォルト設定値を示します。

表 10-2　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。
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.10-6] を参照）。
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。

その他の参考資料

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.10-30）
- 規格（p.10-30）

関連資料

関連事項	タイトル
VACL の概念	VLAN ACL の概要（p.12-2）
IP ACL コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco NX-OS Security Command Reference*』
オブジェクト グループのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco NX-OS Security Command Reference*』
時間範囲のコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco NX-OS Security Command Reference*』

規格

規格	タイトル
この機能のサポート対象の規格には、新規規格も変更された規格もありません。また、この機能は既存の規格に対するサポートに影響を及ぼしません。	—