アクセス コントロール リストの設定

この章は、次の項で構成されています。

ACL について

アクセス コントロール リスト（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。スイッチは、あるパケットに対してある ACL を適用するかどうかを判断するとき、そのパケットを ACL 内のすべてのルールの条件に対してテストします。一致する条件が最初に見つかった時点で、パケットを許可するか拒否するかが決まります。一致する条件が見つからないと、スイッチは適用可能なデフォルトのルールを適用します。許可されたパケットについては処理が続行され、拒否されたパケットはドロップされます。

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。

IP ACL のタイプと適用

Cisco Nexus デバイスは、セキュリティ トラフィック フィルタリング用に、IPv4 をサポートしています。スイッチでは、次の表に示すように、ポートの ACL、VLAN ACL、およびルータの ACL として、IP アクセス コントロール リスト（ACL）を使用できます。

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
ポート ACL	ACL は、次のいずれかに適用した場合、ポート ACL と見なされます。 • イーサネット インターフェイス • 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 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。	IPv4 ACL
ルータ ACL	• VLAN インターフェイス **Note** VLANインターフェイスを設定するには、先に VLAN インターフェイスをグローバルにイネーブルにする必要があります。 • 物理層 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
VLAN ACL（VACL）	アクセス マップを使用して ACL をアクションにアソシエートし、そのアクセス マップを VLAN に適用する場合、その ACL は VACL と見なされます。	IPv4 ACL
VTY ACL	VTY	IPv4 ACL

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. 出力ルータ ACL
5. 出力 VACL

ルール

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。

ルールは ACL で作成できます。ルールは、**permit** または **deny** コマンドを使用してアクセス リスト コンフィギュレーション モードで作成できます。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。

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。

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。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 ACL では、ICMP を名前で指定できます。

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。

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スイッチ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
```

この暗黙のルールによって、どの条件にも一致しない IP トラフィックは拒否されます。

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
```

すべての MAC ACL には、次の暗黙のルールがあります。

```
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。

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。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
- 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
- 確立済み TCP 接続

シーケンス番号

Cisco Nexus デバイスはルールのシーケンス番号をサポートします。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。

  ```
  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。

また、デバイスでは、ACL内ルールのシーケンス番号を再割り当てすることができます。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 Nexus デバイスは、演算子とオペランドの組み合わせを論理演算ユニット（LOU）というレジスタ内に格納し、IP ACL で指定された TCP および UDP ポート上で演算（より大きい、より小さい、等しくない、包含範囲）を行います。

Note range 演算子は境界値も含みます。

これらの LOU は、これらの演算を行うために必要な Ternary Content Addressable Memory（TCAM）エントリ数を最小限に抑えます。最大で 2 つの LOU を、インターフェイスの各機能で使用できます。たとえば入力 RACL で 2 つの LOU を使用し、QoS 機能で 2 つの LOU を使用できます。ACL 機能で 2 つより多くの算術演算が必要な場合、最初の 2 つの演算が LOU を使用し、残りのアクセス コントロール エントリ（ACE）は展開されます。

デバイスが演算子とオペランドの組み合わせを LOU に格納するかどうかの判断基準を次に示します。

- 演算子またはオペランドが、他のルールで使用されている演算子とオペランドの組み合わせと異なる場合、この組み合わせは LOU に格納されます。

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

- 演算子とオペランドの組み合わせがルール内の送信元ポートと宛先ポートのうちどちらに適用されるかは、LOUの使用方法に影響を与えます。同じ組み合わせの一方が送信元ポートに、他方が宛先ポートに別々に適用される場合は、2 つの同じ組み合わせが別々に格納されます。

  たとえば、あるルールによって、演算子とオペランドの組み合わせ「gt 10」が送信元ポートに、別のルールによって同じ組み合わせ「gt 10」が宛先ポートに適用される場合、両方の組み合わせが LOU の半分に格納され、結果として 1 つの LOU 全体が使用されることになります。このため、「gt 10」を使用するルールが追加されても、これ以上 LOU は使用されません。

ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

IPv4 TCAM はシングル幅です。

TCAM リージョン サイズには、次の注意事項と制約事項があります。

- デフォルトの ACL TCAM サイズに戻すには、no hardware profile tcam region コマンドを使用します。write erase コマンドを使用してからスイッチをリロードする必要はなくなりました。
- Cisco Nexus デバイスによっては、各 TCAM リージョンが異なる最小/最大/集約サイズ制限を持つ可能性があります。
- ARPACL TCAM のデフォルト サイズはゼロです。コントロール プレーン ポリシング（CoPP）ポリシーで ARP ACL を使用する前に、この TCAM のサイズをゼロ以外のサイズに設定する必要があります。
- また、VACL および出力 VLAN ACL（E-VACL）を同じ値に設定する必要があります。
- 全体の TCAM の深さは、出力と入力の場合は 4000 エントリで共有されています。これは、16 のエントリ ブロックに切り分けることができます。
- TCAM は、ACL 機能ごとに 256 の統計エントリをサポートします。
- 各方向に 32 の 64 の ACL L4OP がサポートされます。
- 各方向のラベルごとに 2 つの L4OP がサポートされます。各ラベルは、同じ ACL の複数のインターフェイスで共有できます。
- TCAM の切り分け後には、スイッチをリロードする必要があります。
- すべての既存の TCAM のサイズを 0 に設定することはできません。
- デフォルトでは、すべての IPv6 TCAM はディセーブルです（TCAM サイズは 0 に設定されます）。

表 *2 : ACL* リージョンによる *TCAM* サイズ

TCAM ACL リージョン	デフォルト サイズ	最小サイズ	インクリメンタルサイズ
SUP（入力）	112	48	16
PACL（入力）	400	0	16
VACL（入力）、VACL（出力）	640（入力）、640（出力）	0（入力）、0（出力）	16
RACL（入力）	1536	0	16
QOS（入力）、QOS（出力）	192（入力）、64（出力）	16（入力）、64（出力）	16
E-VACL（出力）	640	0	16
E-RACL（出力）	256	0	16
NAT	256	0	16

ACL のライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

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。

VACL の前提条件は次のとおりです。

- VACL に使用する IP 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。

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、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。

- レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
- IP オプションがある IPv4 パケット（追加された 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）
- 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。
- 1 つの VLAN アクセス マップでは、1 つの IP ACL だけを照合できます。
- 1 つの IP ACL に、複数の許可/拒否 ACE を設定することができます。
- 1 つの VLAN に適用できるアクセス マップは 1 つだけです。
- ワープ モードでの出力 RACL および VACL はサポートされていないため、適用しないでください。
- 出力 ACL は、マルチキャスト トラフィックには適用できません。
- 出力 ACL ロギングは、Cisco Nexus 3548 プラットフォームではサポートされていません。
- マルチキャスト トラフィックでは SVI での入力 RACL がサポートされていますが、トラフィックに必ず送信先または送信元となるマルチキャスト グループを定義する ACL に **log** キーワードが含まれている場合は、SVI での入力 RACL の適用はサポートされません。
- SVI のマルチキャスト トラフィックの入力 RACL ACE を照合するには、ACE にマルチキャスト DIP の照合を含める必要があります。また、これらの ACE をインストールする前に、**RACL - ハードウェア プロファイル tcam mcast racl-bridge を使用してブリッジング** コマンドを有効にする必要があります。
- PACL はワープ モードでは適用できません。
- SVI とレイヤ 3 インターフェイスの同じ入力 RACL では TCAM リソースを共有できないため、それぞれが個別に TCAM リソースを使用します。ただし、ACL 統計情報リソースは共有されます。アップグレード前に RACL TCAM をほとんど使い切っている場合、アップグレード後に RACL アプリケーションで障害が発生する可能性があります。その場合は、RACL TCAM を切り分けることができます。
- ARP ACL は Nexus 3500 プラットフォームではサポートされません。
- 物理または論理レイヤ 3 インターフェイスに適用される入力 RACL がサポートされています。入力 RACL をレイヤ 3 SVI に適用するには、ハードウェア プロファイル *tcam mcast racl-bridge* 構成を、マルチキャスト トラフィックを一致させるための回避策として使用できます。
- Cisco NX-OS リリース 7.0(3)I7(6) 以前から、Cisco NX-OS リリース 9.3(1) から 9.3(2) 以降にアップグレードし、デフォルトの lou しきい値構成を使用すると lou しきい値が 1 に設定されます。

- Cisco Nexus 3548 シリーズスイッチでは、sup-redirect ACL の方が SUP へのトラフィックよりも高いプライオリティを持っているため、ACL ログオプションを使用した RACL は有効になりません。

Wide IFACL のガイドラインと制限事項を次に示します：

- 入力マッチ VLAN が両方のフローで同じである場合、異なる **SET_VLAN ID** を持つ 2 つの異なるフローで同じ出力ポートは使用できません。
- ワイドフロー IFACL リダイレクト アクションは、トランク ポートでのみサポートされます。
- フローリダイレクト ポートでは、PACL 以外の ACL 機能はサポートされません。PACL エントリ（ワイドフローかどうかにはかかわりなく）は、PACL_WIDE TCAM リージョンが切り分けられている場合、通常の PACL のように ACL TCAM ではなく、FIBACL TCAM にインストールされます。
- ポート フラップの間、エントリは TCAM から削除されません。これらは、他のセキュリティ ACL と同様にそのまま残ります。
- CLI で提供されるポート範囲のマッチは、TCAM に書き込む前に L4 ポートの値とマスクで拡張され、LOU ハードウェア リソースは使用されません。ユーザーへの影響はなく、フローの既存の規模にも影響はありません。
- Redirect/Set-vlan/Strip-vlan および Drop アクションのみがサポートされています。PUNT アクションはサポートされません。
- log キーワードは、ワイド IFACL ACL ではサポートされていません。
- TCAM サイズに関係なく、最大 4000 のリダイレクト ACL がサポートされます。
- 統計情報を含む最大 4,000 の ACE をサポートできます。
- match および set/strip に許可される VLAN 範囲：1 ～ 4094。
- TCP フラグの ACE マッチはサポートされていません。
- TCAM 構成を **ifacl-wide** から **ifacl**に変更する前に、Wideflow ACL のすべての構成がインターフェイスから削除されていることを確認します。
- 入力パケットに、同じ VLAN マッチの Wideflow ACE がある場合、strip_vlan とともに VLAN マッチ条件があるかどうかにかかわらず、strip-vlan ACE に一致しないパケットであっても、VLAN ヘッダーが削除されます。

デフォルトの ACL 設定

次の表は、IP ACL パラメータのデフォルト設定をリスト表示しています。

Table 3: IP ACL のデフォルト パラメータ

パラメータ	デフォルト
IP ACL	デフォルトの IP ACL は存在しません。
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。

次の表に、VACL パラメータのデフォルト設定を示します。

Table 4: VACL のデフォルト パラメータ

パラメータ	デフォルト
VACL	デフォルトの IP ACL は存在しません。
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

スイッチに IPv4 ACL を作成し、その ACL にルールを追加できます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip access-list** *name*
3. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. （任意） switch(config-acl)# **statistics**
5. （任意） switch# **show ip access-lists** *name*
6. （任意） switch# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **ip access-list** *name*	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。
ステップ 3	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	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、特定の Cisco Nexus デバイスの『*Command Reference*』を参照してください。
ステップ 4	（任意） switch(config-acl)# **statistics**	ACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。
ステップ 5	（任意） switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 6	（任意） 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。

例

次に、IPv4 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# statistics
```

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **ip access-list** *name*
3. switch(config)# **ip access-list** *name*

4. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*
5. (Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}
6. (Optional) switch(config-acl)# [**no**] **statistics**
7. (Optional) switch# **show ip access-lists** *name*
8. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **ip access-list** *name*	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	switch(config)# **ip access-list** *name*	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 4	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination*	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 デバイスの『*Command Reference*』を参照してください。
ステップ 5	(Optional) switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	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 デバイスの『*Command Reference*』を参照してください。
ステップ 6	(Optional) switch(config-acl)# [**no**] **statistics**	ACL のルールと一致するパケットのグローバル統計をスイッチが維持するように設定します。 **no** オプションを指定すると、ACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 7	(Optional) switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 8	(Optional) 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。

Related Topics

IP ACL 内のシーケンス番号の変更 （13 ページ）

IP ACL の削除

スイッチから IP ACL を削除できます。

スイッチから IP ACL を削除する前に、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てください。削除できるのは、現在適用されている ACL だけです。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。スイッチは、削除対象の ACL が空であると見なします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no ip access-list** *name*
3. switch(config)# no **ip access-list** *name*
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **no ip access-list** *name*	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	switch(config)# no **ip access-list** *name*	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 4	(Optional) switch# **show running-config**	ACL の設定を表示します。削除された IP ACL は表示されないはずです。
ステップ 5	(Optional) 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。

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **resequence ip access-list** *name starting-sequence-number increment*
3. (Optional) switch# **show ip access-lists** *name*
4. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	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) switch# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 4	(Optional) 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。

mgmt0 への IP-ACL の適用

IPv4 ACL は、管理インターフェイス（mgmt0）に適用できます。

始める前に

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。

手順の概要

1. **configure terminal**
2. **interface mgmt** *port*
3. **ip access-group** *access-list* {**in** | **out**}
4. （任意） **show running-config aclmgr**
5. （任意） **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	**interface mgmt** *port*
	例：
	`switch(config)# interface mgmt0`
	`switch(config-if)#`
		管理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	（任意） **show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	ACL の設定を表示します。
ステップ 5	（任意） **copy running-config startup-config** 例： `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。

関連項目

- IP ACL の作成

ポート ACL としての IP ACL の適用

IPv4 ACL は、物理イーサネット インターフェイスまたは PortChannel 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 と見なされます。

Note 一部の設定パラメータは、ポート チャネルに適用されていると、メンバー ポートの設定に反映されません。

SUMMARY STEPS

1. switch# **configure terminal**

2. switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}
3. switch(config-if)# **ip port access-group** *access-list* **in**
4. (Optional) switch# **show running-config**
5. (Optional) switch# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **interface** {**ethernet** [*chassis*/]*slot*/*port* | **port-channel** *channel-number*}	指定したインターフェイスに対してインターフェイス 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	switch(config-if)# **ip port access-group** *access-list* **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 では、インバウンド フィルタリングだけがサポートされています。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	(Optional) switch# **show running-config**	ACL の設定を表示します。
ステップ 5	(Optional) 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。

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 と見なされます。

Note 論理演算ユニット（LOU）は、Out 方向に適用されたルータ ACL には使用できません。IPv4 ACL が Out 方向のルータ ACL として適用される場合、TCP/UDP ポート番号の論理演算子を持つアクセス制御エントリ（ACE）は複数の ACE に内部的に拡張され、In 方向に適用された同じ ACL と比較すると、より多くの TCAM エントリが必要になることがあります。

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。

SUMMARY STEPS

1. switch# **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - switch(config)# **interface ethernet** *slot*/*port*[**.** *number*]
   - switch(config)# **interface port-channel** *channel-number*[**.** *number*]
   - switch(config)# **interface tunnel** *tunnel-number*
   - switch(config)# **interface vlan** *vlan-ID*
   - switch(config)# **interface mgmt** *port*
3. switch(config-if)# **ip access-group** *access-list* {**in** | **out**}
4. (Optional) switch(config-if)# **show running-config aclmgr**
5. (Optional) switch(config-if)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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。 • switch(config)# **interface ethernet** *slot*/*port*[**.** *number*] • switch(config)# **interface port-channel** *channel-number*[**.** *number*] • switch(config)# **interface tunnel** *tunnel-number* • switch(config)# **interface vlan** *vlan-ID* • switch(config)# **interface mgmt** *port*	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	switch(config-if)# **ip access-group** *access-list* {**in**	**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。

	Command or Action	Purpose
ステップ 4	(Optional) switch(config-if)# **show running-config aclmgr**	ACL の設定を表示します。
ステップ 5	(Optional) 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 設定情報を表示するには、次のいずれかの作業を実行します。

Procedure

- switch# **show running-config**

  ACL の設定（IP ACL の設定と IP ACL が適用されるインターフェイス）を表示します。

- switch# **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。

- switch# **show running-config aclmgr**

  ACL の構成と ACL が適用されるインターフェイスを表示します。

Example

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 デバイスの『*Command Reference*』を参照してください。

IP ACL の統計情報のモニタリングとクリア

IP ACL に関する統計情報（各ルールに一致したパケットの数など）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の詳細については、Cisco Nexus デバイスの『*Command Reference*』を参照してください。

Note MAC アクセス リストは、非 IPv4 トラフィックだけに適用可能です。

Procedure

- switch# **show ip access-lists** *name*

  IP ACL の設定を表示します。IP ACL に statistics コマンドが指定されている場合は、show ip access-lists コマンドの出力に、各ルールに一致したパケットの数が表示されます。

- switch# **show ip access-lists** *name*

IP ACL の設定を表示します。IP ACL に statistics コマンドが指定されている場合は、show ip access-lists コマンドの出力に、各ルールに一致したパケットの数が表示されます。

- switch# **clear access-list counters** [*access-list-name*]

  すべての IP ACL、または特定の IP ACL の統計情報を消去します。

- switch# **clear ip access-list counters** [*access-list-name*]

  すべての IP ACL、または特定の IP ACL の統計情報を消去します。

VLAN ACL の概要

VLAN ACL（VACL）は、IP ACL の適用例の 1 つです。VACL を設定して、VLAN 内でブリッジされているすべてのパケットに適用できます。VACL は、セキュリティ パケットのフィルタリングだけに使用します。VACL は方向（入力または出力）で定義されることはありません。

VACL とアクセス マップ

VACL では、アクセス マップを使用して、IP ACL をアクションとリンクさせます。スイッチは、VACL で許可されているパケットに対して、設定済みのアクションを実行します。

VACL とアクション

アクセス マップ コンフィギュレーション モードでは、action コマンドを使用して、次のいずれかのアクションを指定します。

- フォワード：スイッチの通常の動作によって決定された宛先にトラフィックを送信します。
- ドロップ：トラフィックをドロップします。

統計

Cisco Nexus デバイスは、VACL 内の各ルールについて、グローバルな統計情報を保持できます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、その VACL が適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。

Note Cisco Nexus デバイスは、インターフェイス単位の VACL 統計情報はサポートしていません。

設定する各 VLAN アクセス マップごとに、VACL の統計情報をスイッチ内に保持するかどうかを指定できます。これにより、VACL によってフィルタリングされたトラフィックをモニタリングするため、あるいは VLAN アクセス マップの設定のトラブルシューティングを行うために、VACL 統計情報の収集のオン/オフを必要に応じて切り替えることができます。

VACL の設定

VACL の作成または変更

VACL を作成または変更できます。VACL の作成には、IP ACL を、一致したトラフィックに適用するアクションとアソシエートさせるアクセス マップの作成が含まれます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **vlan access-map** *map-name*
3. switch(config-access-map)# **match ip address** *ip-access-list*
4. switch(config-access-map)# **action** {**drop** | **forward**}
5. (Optional) switch(config-access-map)# [**no**] **statistics**
6. (Optional) switch(config-access-map)# **show running-config**
7. (Optional) switch(config-access-map)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **vlan access-map** *map-name*	指定したアクセスマップのアクセスマップ 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	switch(config-access-map)# **match ip address** *ip-access-list*	マップの IPv4 ACL を指定します。
ステップ 4	switch(config-access-map)# **action** {**drop** | **forward**}	スイッチが、ACL に一致したトラフィックに適用するアクションを指定します。
ステップ 5	(Optional) switch(config-access-map)# [**no**] **statistics**	VACL に規定されたルールに一致するパケットのグローバルな統計情報をスイッチ内に保持するように指定します。 **no** オプションを指定すると、VACL のグローバルな統計情報がスイッチ内に保持されなくなります。
ステップ 6	(Optional) switch(config-access-map)# **show running-config**	ACL の設定を表示します。
ステップ 7	(Optional) switch(config-access-map)# **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。

VACL の削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

VACL が VLAN に適用されているかどうかを確認してください。削除できるのは、現在適用されている VACL だけです。VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。スイッチは、削除対象の VACL が空であると見なします。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# **no vlan access-map** *map-name*
3. (Optional) switch(config)# **show running-config**
4. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# **no vlan access-map** *map-name*	指定したアクセス マップの VLAN アクセス マップの設定を削除します。
ステップ 3	(Optional) switch(config)# **show running-config**	ACL の設定を表示します。
ステップ 4	(Optional) 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。

VACL の VLAN への適用

VACL を VLAN に適用できます。

SUMMARY STEPS

1. switch# **configure terminal**
2. switch(config)# [**no**] **vlan filter** *map-name* **vlan-list** *list*
3. (Optional) switch(config)# **show running-config**
4. (Optional) switch(config)# **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
ステップ 1	switch# **configure terminal**	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	switch(config)# [**no**] **vlan filter** *map-name* **vlan-list** *list*	指定したリストによって、VACL を VLAN に適用します。 **no** オプションを使用すると、VACL の適用が解除されます。 **vlan-list** コマンドで指定できる VLAN は最大 32 個ですが、複数の **vlan-list** コマンドを設定すると、32 個を超える VLAN を指定できます。
ステップ 3	(Optional) switch(config)# **show running-config**	ACL の設定を表示します。
ステップ 4	(Optional) 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。

VACL の設定の確認

VACL 設定情報を表示するには、次のいずれかの作業を実行します。

Procedure

- switch# **show running-config aclmgr**

  VACL 関連の設定を含む、ACL の設定を表示します。

- switch# **show vlan filter**

  VLAN に適用されている VACL の情報を表示します。

- switch# **show vlan access-map**

  VLAN アクセス マップに関する情報を表示します。

VACL 統計情報の表示と消去

VACL 統計情報を表示または消去するには、次のいずれかの作業を実行します。

Procedure

- switch# **show vlan access-list**

  VACL の設定を表示します。VLAN アクセス マップに **statistics** コマンドが指定されている場合は、**show vlan access-list** コマンドの出力に、各ルールに一致したパケットの数が表示されます。

- switch# **clear vlan access-list counters**

  すべての VACL、または特定の VACL の統計情報を消去します。

VACL の設定例

次に、acl-ip-01 という名前の IP ACL によって許可されたトラフィックを転送するように VACL を設定し、その VACL を VLAN 50 ～ 82 に適用する例を示します。

```
switch# configure terminal
switch(config)# vlan access-map acl-ip-map
switch(config-access-map)# match ip address acl-ip-01
switch(config-access-map)# action forward
switch(config-access-map)# exit
 switch(config)# vlan filter acl-ip-map vlan-list 50-82
```

ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory（TCAM）リージョンのサイズを変更できます。

手順の概要

1. **configure terminal**
2. **hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*
3. **copy running-config startup-config**
4. switch(config)# **show hardware profile tcam region**
5. switch(config)# **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	**hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*	ACL TCAM リージョン サイズを変更します。

	コマンドまたはアクション	目的
		• **arpacl**：アドレス解決プロトコル（ARP）の ACL（ARPACL）TCAM リージョン サイズを設定します。 • **e-racl**：出力ルータ ACL（ERACL）TCAM リージョン サイズを設定します。 • **e-vacl**：出力の VLAN ACL（EVACL）TCAM リージョン サイズを設定します。 • **ifacl**：インターフェイス ACL（ifacl）TCAM リージョンサイズを設定します。エントリの最大数は 1500 です。 • **nat**：NAT TCAM リージョンのサイズを設定します。 • **qos**：Quality of Service（QoS）TCAM リージョン サイズを設定します。 • **qoslbl**：QoS ラベル（qoslbl）TCAM リージョン サイズを設定します。 • **racl**：ルータの ACL（RACL）TCAM リージョン サイズを設定します。 • **vacl**：VLAN ACL（VACL）TCAM リージョン サイズを設定します。 • *tcam_size*：TCAM サイズ。有効な範囲は 0 ～ 2,147,483,647 エントリです。 （注） **vacl** および **e-vacl** TCAM リージョンを同じサイズに設定する必要があります。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に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て、変更を継続的に保存します。
ステップ 4	switch(config)# **show hardware profile tcam region** 例： `switch(config)# show hardware profile tcam region`	スイッチの次回のリロード時に適用される TCAM サイズを表示します。
ステップ 5	switch(config)# **reload** 例： `switch(config)# reload`	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。 （注）

	コマンドまたはアクション	目的
		copy running-config to startup-config を保存した後、次回のリロード時に新しいサイズ値が有効になります。

例

次に、RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、スイッチで TCAM VLAN ACL を設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# hardware profile tcam region vacl 512
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

```
switch(config)# show hardware profile tcam region
         sup size =   16
        vacl size =  640
       ifacl size =  496
         qos size =  256
       rbacl size =    0
        span size =    0
        racl size = 1536
      e-racl size =  256
      e-vacl size =  640
      qoslbl size =    0
      arpacl size =    0
```

この例では、特定のリージョンの TCAM の使用率を判断する方法を示しています。この例には 5 つの RACL エントリがあります。

```
switch(config)# show system internal aclqos platform mtc info tcam 0 region racl
         racl TCAM configuration for asic id 0:
[        sup tcam]: range     0 -   47
[       vacl tcam]: range   512 - 1087
[      ifacl tcam]: range   112 -  511
[        qos tcam]: range  3712 - 3903
[      rbacl tcam]: range     0 -    0
[       span tcam]: range     0 -    0
[       racl tcam]: range  1984 - 3455 *
```

```
[     e-racl tcam]: range  3456 - 3711
[     e-vacl tcam]: range  1088 - 1727
[     qoslbl tcam]: range     0 -    0
[       ipsg tcam]: range     0 -    0
[     arpacl tcam]: range     0 -    0
[  ipv6-racl tcam]: range     0 -    0
[ipv6-e-racl tcam]: range     0 -    0
[   ipv6-sup tcam]: range     0 -    0
[   ipv6-qos tcam]: range     0 -    0
[        nat tcam]: range  1728 - 1983
[      e-qos tcam]: range  3904 - 3967
[        pbr tcam]: range     0 -    0
[   ipv6-pbr tcam]: range     0 -    0
[       copp tcam]: range    48 -  111

    TCAM [racl tcam]: [v:1, size:1472, start:1984 end:3455]
    In use tcam entries: 5
        3451-3455
    Link Local Entries:
    nat size =  256
```

デフォルトの TCAM リージョン サイズに戻す

手順の概要

1. **configure terminal**
2. switch(config)# **no hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*
3. （任意） **copy running-config startup-config**
4. switch(config)# **reload**

手順の詳細

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`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	switch(config)# **no hardware profile tcam region** {**arpacl** | **e-racl**} | **ifacl** | **nat** | **qos**} |**qoslbl** | **racl**} | **vacl** } *tcam_size*	デフォルト ACL TCAM サイズに設定を戻します。
ステップ 3	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	リブートおよびリスタート時に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て、変更を継続的に保存します。
ステップ 4	switch(config)# **reload**	スイッチをリロードします。

例

次に、デフォルトの RACL TCAM リージョンのサイズに戻す例を示します。

```
switch(config)# no hardware profile tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# copy running-configur startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

仮想端末回線の ACL の設定

仮想端末（VTY）回線とアクセス リストのアドレス間の IPv4 の着信接続と発信接続を制限するには、ライン コンフィギュレーション モードで **access-class** コマンドを使用します。アクセス制限を解除するには、このコマンドの **no** 形式を使用します。

VTY 回線で ACL を設定する場合には、次のガイドラインに従ってください。

- すべての VTY 回線にユーザーが接続できるため、すべての VTY 回線に同じ制約を設定する必要があります。
- エントリ単位の統計情報は、VTY 回線の ACL ではサポートされません。

始める前に

適用する ACL が存在しており、この適用に対して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てください。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **line vty**
3. switch(config-line)# **access-class access-list-number {in | out}**
4. （任意） switch(config-line)# **no access-class access-list-number {in | out}**
5. switch(config-line)# **exit**
6. （任意） switch# **show running-config aclmgr**
7. （任意） switch# **copy running-config startup-config**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch(config)# **line vty**
	例：
	`switch(config)# line vty`
	`switch(config-line)#`
		ライン 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	switch(config-line)# **access-class access-list-number {in | out}**
	例：
	`switch(config-line)# access-class ozi2 in`
	`switch(config-line)#access-class ozi3 out`
	`switch(config)#`
		着信または発信アクセス制限を指定します。

ステップ 4	（任意） switch(config-line)# **no access-class access-list-number {in | out}**
	例：
	`switch(config-line)# no access-class ozi2 in`
	`switch(config-line)# no access-class ozi3 out`
	`switch(config)#`
		着信または発信アクセス制限を削除します。

ステップ 5	switch(config-line)# **exit**
	例：
	`switch(config-line)# exit`
	`switch#`
		ライン コンフィギュレーション モードを終了します。

ステップ 6	（任意） switch# **show running-config aclmgr** 例： `switch# show running-config aclmgr`	スイッチの ACL の実行コンフィギュレーションを表示します。
ステップ 7	（任意） switch# **copy running-config startup-config** 例： `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。

例

次に、VTY 回線の in 方向に access-class ozi2 のコマンドを適用する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# line vty
```

```
switch(config-line)# access-class ozi2 in
switch(config-line)# exit
switch#
```

VTY 回線の ACL の確認

VTY 回線の ACL 設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config aclmgr	スイッチで設定された ACL の実行コンフィギュレーションを表示します。
show users	接続されているユーザーを表示します。
show access-lists *access-list-name*	エントリ単位の統計情報を表示します。

VTY 回線の ACL の設定例

次に、コンソール回線（ttyS0）および VTY 回線（pts/0 および pts/1）の接続ユーザーの例を示します。

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    ttyS0        Aug 27 20:45   .         14425 *
admin    pts/0        Aug 27 20:06 00:46       14176 (172.18.217.82) session=ssh
admin    pts/1        Aug 27 20:52   .         14584 (10.55.144.118)
```

次に、172.18.217.82 を除き、すべての IPv4 ホストへの VTY 接続を許可する例と、10.55.144.118、172.18.217.79、172.18.217.82、172.18.217.92 を除き、すべての IPv4 ホストへの VTY 接続を拒否する例を示します。

```
switch# show running-config aclmgr
!Time: Fri Aug 27 22:01:09 2010
version 5.0(2)N1(1)
ip access-list ozi
  10 deny ip 172.18.217.82/32 any
  20 permit ip any any
ip access-list ozi2
  10 permit ip 10.55.144.118/32 any
  20 permit ip 172.18.217.79/32 any
  30 permit ip 172.18.217.82/32 any
  40 permit ip 172.18.217.92/32 any

line vty
  access-class ozi in
  access-class ozi2 out
```

次に、ACL のエントリ単位の統計情報をイネーブルにして、IP アクセス リストを設定する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
switch(config)# ip access-list ozi2
switch(config-acl)# statistics per-entry
switch(config-acl)# deny tcp 172.18.217.83/32 any
```

```
switch(config-acl)# exit

switch(config)# ip access-list ozi
switch(config-acl)# statistics per-entry
switch(config-acl)# permit ip 172.18.217.20/24 any
switch(config-acl)# exit
switch#
```

次に、in および out 方向で VTY の ACL を適用する例を示します。

```
switch(config)# line vty
switch(config-line)# ip access-class ozi in
switch(config-line)# access-class ozi2 out
switch(config-line)# exit
switch#
```

次に、VTY 回線でアクセス制限を削除する例を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
switch(config)# line vty
switch(config-line)# no access-class ozi2 in
switch(config-line)# no ip access-class ozi2 in
switch(config-line)# exit
switch#
```

IP ポート ACL での Wideflow IFACL リダイレクトの構成

Cisco NX-OS リリース 10.3(2)F までは、Cisco Nexus 3548 シリーズ スイッチのタップ集約機能は、Openflow を使用してサポートされています。詳細については、 Cisco OpenFlow エージェントの構成を参照してください。

Cisco NX-OS リリース 10.3(3)F 以降では、Openflow はCisco Nexus 3548 シリーズ スイッチではサポートされていません。すべての openflow または Tap 集約機能に対応するために、wideflow 機能を使用した ACL リダイレクトが導入され、新しい match コマンドオプション（srcmac、dstmac、vlan）と新しいアクション（setvlan、strip-vlan）が追加されました。

Cisco NX-OS リリース 10.3(3)F 以降では、既存の IP ACL CLI のキーワード **wideflow** とともに新しい CLI オプションが追加されています。キーワード **wideflow** は新しい CLI オプションを保護しており、Cisco Nexus 3548 スイッチでのみ有効になります。

始める前に

Wideflow の新しいコマンド オプションを有効にするには、 **IFACL-WIDE TCAM** を構成する必要があります。これには、実行時構成をスタートアップ構成にコピーし、デバイスがリロードすることが必要です。ハードウェア プロファイルの転送モードは、リロード後に通常からフローリダイレクトに変更されます。詳細については、 OpenFlow 機能の実現を参照してください。

（注）
- IFACL から IFACL-WIDE TCAM に変更する場合は、既存のすべての IP アクセスリストがインターフェイスおよびグローバル構成から削除されていることを確認します。
- IFACL-WIDE TCAM に変更した後、レガシー ACL をインターフェイスに適用することはできません。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip access-list** *name*
3. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow**
4. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow dstmac** *destination MAC address*
5. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow srcmac** *source MAC address*
6. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow vlan**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip access-list** *name*	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。
ステップ 3	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow**	wideflow のオプションは次のとおりです。 • **dstmac**：宛先 MAC アドレスの構成。 • **srcmac**：発信元 MAC アドレスの構成。 • **vlan**：Vlan 番号の構成。
ステップ 4	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow dstmac** *destination MAC address*	**dstmac**のオプションは次のとおりです。 • **E.E.E**：接続先ワイルドカードビット（オプション 1）。 • **EE-EE-EE-EE-EE-EE**：接続先ワイルドカードビット（オプション 2）。

	コマンドまたはアクション	目的
		• **EE:EE:EE:EE:EE:EE**：接続先ワイルドカードビット（オプション 3）。 • **EEEE.EEEE.EEEE**：：接続先ワイルドカードビット（オプション 4）。
ステップ 5	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow srcmac** *source MAC address*	**srcmac**のオプションは次のとおりです。 • **E.E.E**：送信元 MAC アドレス（オプション 1）。 • **EE-EE-EE-EE-EE-EE**：送信元 MAC アドレス（オプション 2）。 • **EE:EE:EE:EE:EE:EE**：送信元 MAC アドレス（オプション 3）。 • **EEEE.EEEE.EEEE**：送信元MACアドレス（オプション 4）。 • **any**：任意の送信元アドレス。
ステップ 6	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect-ports* **wideflow vlan**	0 ～ 4095 の範囲の Vlan 番号を入力します。

例

次に、構成例を示します：

ステップ 1：スイッチが openflow forwarding-mode の場合は、次の手順を実行します。

（注） スイッチが normal 転送モードの場合は、ステップ 1 をスキップして、ステップ 2 に直接進みます。

- すべての openflow 構成を削除します。
- ハードウェア プロファイルの転送モードを normal に変更します。
- 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。
- スイッチをリロードします。

```
switch#configure terminal
switch(config)# no openflow
switch(config)# no feature openflow
switch(config)# [optional] no hardware profile openflow forward-pdu
```

```
switch(config)# hardware profile forwarding-mode normal
switch(config)# copy r s
switch(config)# reload
```

ステップ 2：Cisco Nexus リリース 10.3(3)F 以降のリリースにアップグレードします。

ステップ 3：Cisco Nexus リリース 10.3(3)F 以降のリリースでスイッチを起動した後、次のように **TCAM for IFACL-WIDE** を構成します。

```
switch# configure terminal
switch(config)# hardware profile tcam region ifacl 0
switch(config)# hardware profile tcam region ifacl-wide 4096
switch(config)# copy r s
switch(config)# reload
switch(config)# [optional] hardware profile flow-redirect forward-pdu
```

次に、redirect コマンドとwideflow コマンドを使用した IP アクセス リスト構成の例を示します。

```
switch# configure terminal
switch(config)# ip access-list ACL
switch(config-acl)# 10 permit ip host 1.1.1.1 host 1.1.1.2 dscp 52 redirect
Ethernet1/2,portchannel1 strip-vlan wideflow srcmac 00:16:3e:33:e1:84 0.0.0 dstmac
00:16:3e:4d:d6:dd 0.0.0 vlan 1000
switch(config-acl)# 20 permit icmp host 2.2.2.1 host 2.2.2.2 redirect
Ethernet1/34,portchannel2 wideflow
switch(config-acl)# 30 permit tcp host 3.3.3.1 host 3.3.3.2 dscp 28 redirect
Ethernet1/2,port-channel1 set-vlan 1002 wideflow srcmac 00:16:3e:12:e9:c4 0.0.0 dstmac
00:16:3e:0f:6a:48 0.0.0 vlan 1001
switch(config-acl)# 40 permit udp host 4.4.4.1 host 4.4.4.2 precedence 7 redirect
Ethernet1/2,port-channel1 wideflow srcmac 00:16:3e:07:aa:53 0.0.0 dstmac 00:16:3e:79:e4:a8
 0.0.0 vlan 1000
switch(config-acl)# 50 permit ethertype 0x0806 redirect Ethernet1/48 wideflow
```

次に、インターフェイスで redirect コマンドとwideflow コマンドを使用して IP ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# mode flow-redirect
switch(config-if)# ip port access-group ACL in
switch(config-if)# end
```

リダイレクト アクションの構成

CLI構文のリダイレクトアクションは、**wideflow**キーワードの前に存在する必要があります。**Wideflow** キーワードが欠落している場合、リダイレクト アクション設定は受け入れられません。このチェックは、ユーザーが コマンドを入力すると実行時に実行されます。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **ip access-list** *name*
3. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect*
4. switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect*

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	構成モードに入ります。
ステップ 2	switch(config)# **ip access-list** *name*	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。
ステップ 3	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect*	**[リダイレクト（redirect）]**のオプションは次のとおりです。 • **redirect**：インターフェイスにリダイレクトします。構文例：redirect Ethernet1/1,Ethernet1/2,port-channel1 • **Wideflow**：ワイドフロー オプション（必須）。
ステップ 4	switch(config-acl)# [*sequence-number*] {**permit** | **deny**} *protocol source destination* **redirect** *redirect*	次に、redirect **redirect**のオプション コマンドを示します。 • **redirect**：インターフェイスにリダイレクトします。構文例：redirect Ethernet1/1,Ethernet1/2,port-channel1 • **set-vlan**：リダイレクト ポート ビアで出力されるトラフィックの vlan 値。 • **strip-vlan**：リダイレクト ポートから vlan タグなしパケットを送信します。 • **Wideflow**：ワイドフロー オプション（必須）。

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。