アクセス コントロール リストの設定

この章の内容は、次のとおりです。

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 HyperText Transfer Protocol（HTTP; ハイパー テキスト トランスファ プロトコル）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

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、IP アクセス コントロール リスト（ACL）をポート ACL、VLAN ACL、およびルータ ACL として、次の表に示すように使用することができます。

表 *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 IPv6 ACL
ルータ ACL	• VLAN インターフェイス （注） VLANインターフェイスを設定する前に、VLANインターフェイスをグローバルで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 IPv6 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

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
VTY ACL	VTY	IPv4 ACL IPv6 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

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。 スイッチは、許可ルールに指定された基準に一致するトラフィックを許可し、拒否ルールに指定された基準に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。

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、IPv6、および MAC の 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任意の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 には暗黙のルールがあります。暗黙のルールは、実行コンフィギュレーションには表示されていませんが、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。

すべての IPv6 ACL には、次の暗黙のルールがあります。

```
deny ipv6 any any

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

ICMPv6 のネイバー探索メッセージを拒否するルールを持つ IPv6 ACL を設定した場合を除き、最初の 4 つのルールによって、デバイスはネイバー探索アドバタイズメント メッセージと請求メッセージを許可するようになります。 5 つめのルールにより、デバイスは不一致の IPv6 トラフィックを拒否します。

（注） IPv6 の ACL に **deny ipv6 any any** というルールを明示的に設定すると、暗黙の permit ルールでトラフィックをまったく許可できなくなります。 **deny ipv6 any any** というルールを明示的に設定するものの、ICMPv6 ネイバー探索メッセージは許可したい場合は、5 つの暗黙のルールをすべて明示的に設定します。

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

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。 入力されたすべてのルールには、ユーザによって、またはスイッチによって自動的に、シーケンス番号が付けられます。 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。

スイッチは、演算子とオペランドの組み合わせを、Logical Operator Unit（LOU; 論理演算ユニット）と呼ばれるレジスタ内に格納します。

「eq」演算子で LOU を使用しても、LOU への格納は行われません。 range 演算子は境界値も含みます。

演算子とオペランドの組み合わせが LOU に格納され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。 ただし、IPv6 TCAM はダブル幅です。 たとえば、256 エントリの IPv6 TCAM を作成するには、IPv4 TCAM を 256 x 2（つまり 512）エントリ減らす必要があります。

IPv6 ポート ACL、VLAN ACL、ルータ ACL を作成して、QoS の IPv6 アドレスを照合できます。ただし、Cisco NX-OS ではすべてを同時に使用することをサポートしていません。 これらの新しい IPv6 TCAM をイネーブルにするには、既存の TCAM を削除するかサイズを縮小する必要があります。

TCAM リージョン サイズに関する注意事項および制約事項は次のとおりです。

- デフォルト 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。
- プラットフォームによっては、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。
- VACL および出力 VLAN ACL（E-VACL）のサイズには、同じ値を設定する必要があります。
- IPv4 と IPv6 の両方のアドレスは、ダブル幅の TCAM 内であっても共存できません。
- 合計 TCAM 深度は、入力が 2000、出力が 1000 であり、256 エントリのブロックに切り分けることができます。
- TCAM の切り分け後に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 サイズを 0 には設定できません。

- 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*** リージョン別 ***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	最大サイズ
SUP（入力）	128 x 2	128 x 2	N/A	128 x 2
SPAN（入力）	128	128	N/A	128
ARPACL（入力）	0	0	128	128
PACL（入力）	384	ARPACL がディセーブル = 128 ARPACL がイネーブル = 256	256	1664（連結）
VACL（入力）	512	0	256	
RACL（入力）	512	256	256	
QOS（入力）	256	256	256	
PACL_IPV6（入力）	0	0	256 x 2	
VACL_IPV6（入力）	0	0	256 x 2	
RACL_IPV6（入力）	0	0	256 x 2	
QOS_IPV6（入力）	0	0	256 x 2	
E-VACL（出力）	512	0	256	1024（連結）
E-RACL（出力）	512	0	256	
E-VACL_IPV6（出力）	0	0	256 x 2	
E-RACL_IPV6（出力）	0	0	256 x 2	

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	最大サイズ
QOSLBL（前ルックアップ）	256	256	256	512（連結）
IPSG（前ルックアップ）	256	256	256	
SUP_IPV6（前ルックアップ）	128 x 2	256 x 2	N/A	256 x 2

ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ACL を使用するためにライセンスは必要ありません。

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、この適用に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、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。

- 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）
- 時間範囲を使用する ACL を適用すると、デバイスは 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。
- すべての着信および発信トラフィックに **match-local-traffic** オプションを使用するには、まずソフトウェアで ACL をイネーブルにする必要があります。

VACL には、次の設定があります

- 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、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。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。
- VLAN ACL として適用される IPv4 ACL に、TCP/UDP ポート番号のための論理演算子を含む 1 つ以上の ACE が含まれている場合、ポート番号は入力方向では照合されますが、出力方向では無視されます。
- 1 つの VLAN アクセス マップは、1 つの IP ACL だけを照合できます。
- 1 つの IP ACL は、複数の許可/拒否 ACE を持てます。
- 1 つの VLAN には、1 つのアクセス マップだけを適用できます。

デフォルトの ACL 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。

表 *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。

次の表に、VACL パラメータのデフォルト設定を示します。

表 *4*：デフォルトの *VACL* 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 または IPv6 を作成し、それにルールを追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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*	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、『*Cisco Nexus 3000* シリーズ *Command Reference*』を参照してください。
ステップ 4	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な統計情報をスイッチが保持するように指定します。
ステップ 5	switch# **show** {**ip** | **ipv6**} **access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 6	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。

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
```

次に、IPv6 ACL を作成する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-01-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
```

IP ACL の変更

既存の IPv4 ACL または IPv6 ACL のルールの追加および削除を実行できます。 既存のルールは変更できません。 ルールを変更するには、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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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** | **ipv6**} **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 3000* シリーズ *Command Reference*』を参照してください。
ステップ 5	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*}	（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。

	コマンドまたはアクション	目的
		詳細については、『*Cisco Nexus 3000* シリーズ *Command Reference*』を参照してください。
ステップ 6	switch(config-acl)# [**no**] **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な統計情報をスイッチが保持するように指定します。 **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	switch#**show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 8	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。

関連トピック

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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** | **ipv6**} **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。

	コマンドまたはアクション	目的
ステップ 4	switch# **show running-config**	（任意） 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	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。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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	switch# **show** {**ip** | **ipv6**} **access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 4	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。

mgmt0 への IP ACL の適用

管理インターフェイス（mgmt0）に IPv4 ACL または IPv6 ACL を適用できます。

はじめる前に

適用するACLが存在し、この適用に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。

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	**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 または IPv6 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。

関連資料

- IP ACL の作成

IP ACL のポート ACL としての適用

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。

（注） 一部の設定パラメータは、PortChannel に適用されると、メンバ ポートの設定に反映されません。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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*}	特定のインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 3	switch(config-if)# **ip port access-group** *access-list* **in**	IPv4 ACL を、インターフェイスまたは PortChannel 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	switch# **show running-config**	（任意） ACL の設定を表示します。
ステップ 5	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。

ルータ ACL としての IP ACL の適用

IPv4 ACL または IPv6 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。

（注） 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 コントロール 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 エントリが必要な場合があります。

はじめる前に

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

	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	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	次のいずれかのコマンドを入力します。 • switch(config-if)# **ip access-group** *access-list* {**in** | **out**} • switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}	IPv4 ACL または IPv6 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	switch(config-if)# **show running-config aclmgr**	（任意） ACL の設定を表示します。
ステップ 5	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。

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。

- 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。

これらのコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 3000* シリーズ *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** または **show ipv6 access-list** コマンドを使用します。 このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 3000* シリーズ *Command Reference*』を参照してください。

（注） MAC アクセス リストは、非 IPv4 および非 IPv6 トラフィックだけに適用可能です。

- switch# **show** {**ip** | **ipv6**} **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** および **show ipv6 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#**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** {**ip** | **ipv6**} **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 によって許可されたパケットに設定されている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。

統計情報

スイッチは、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。

（注） Cisco Nexus 3000 シリーズ スイッチでは、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。

VACL を作成または変更する手順は、次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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 および IPv6 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	switch(config-access-map)# [**no**] **statistics**	（任意） その VACL のルールと一致するパケットのグローバルな統計情報をスイッチが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	switch(config-access-map)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 7	switch(config-access-map)# **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 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。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
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	switch(config)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 4	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。

VACL の VLAN への適用

VACL を VLAN に適用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	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** コマンドでは、最大 32 個の VLAN から構成される 1 つのリストを指定できますが、複数の **vlan-list** コマンドを設定すれば 32 個を超える VLAN を指定できます。
ステップ 3	switch(config)# **show running-config**	（任意） ACL の設定を表示します。
ステップ 4	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。

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。

- 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。

- 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

	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** | {**ipv6-e-racl** | **e-racl**} | **ifacl** | **ipsg** | {**ipv6-qos** | **qos**} |**qoslbl** | {**ipv6-racl** | **racl**} | **vacl** } *tcam_size*	ACL TCAM リージョン サイズを変更します。 • **arpacl**：アドレス解決プロトコル（ARP）ACL（ARPACL）TCAM リージョンのサイズを設定します。 • **e-racl**：出力ルータ ACL（ERACL）TCAM リージョンのサイズを設定します。 • **e-vacl**：出力 VLAN ACL（EVACL）TCAM リージョンのサイズを設定します。 • **ifacl**：インターフェイス ACL（ifacl）TCAM リージョンのサイズを設定します。 • **ipsg**：IP ソース ガード（IPSG）TCAM リージョンのサイズを設定します。 • **qos**：Quality of Service（QoS）TCAM リージョンのサイズを設定します。 • **qoslbl**：QoS ラベル（qoslbl）TCAM リージョンのサイズを設定します。 • **racl**：ルータ ACL（RACL）TCAM リージョンのサイズを設定します。 • **vacl**：VLAN ACL（VACL）TCAM リージョンの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 リージョンは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**	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。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **show hardware profile tcam region**	スイッチで次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**	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） **copy running-config to startup-config** を保存した後、次にリロードして初めて新しいサイズ値が有効になります。

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

次に、0 または 128 以外の値に ARP ACL TCAM 値を設定したときに表示されるエラー メッセージの例を示します。また、ARP ACL TCAM リージョンのサイズを変更し、その変更を確認する方法を示します。

```
switch(config)# hardware profile tcam region arpacl 200
ARPACL size can be either 0 or 128

switch(config)# hardware profile tcam region arpacl 128
To start using ARPACL tcam, IFACL tcam size needs to be changed.
Changing IFACL tcam size to 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'

switch(config)# show hardware profile tcam region
   sup size = 128
  vacl size = 512
 ifacl size = 256
   qos size = 256
 rbacl size = 0
  span size = 128
  racl size = 256
e-racl size = 512
e-vacl size = 512
qoslbl size = 512
  ipsg size = 512
arpacl size = 128
switch(config)#
```

次に、スイッチで TCAM VLAN ACL を設定する例を示します。

```
switch# configure sync
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-sync)# switch-profile s5010
Switch-Profile started, Profile ID is 1
switch(config-sync-sp)# hardware profile tcam region vacl 512
switch(config-sync-sp)# hardware profile tcam region e-vacl 512
switch(config-sync-sp)#
```

デフォルト TCAM リージョン サイズに戻す

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** | **arpacl** *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	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 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。

次に、デフォルト 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 または IPv6 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 回線の ACL を設定する場合は、次の注意事項に従います。

- すべての VTY 回線にユーザが接続できるため、すべての VTY 回線に同じ制限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。

はじめる前に

適用するACLが存在しており、この適用向けに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。

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	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)#`
		（任意）
		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	switch# **show running-config aclmgr** 例： `switch# show running-config aclmgr`	（任意） 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	switch# **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。

次に、VTY 回線の In 方向に access-class ozi2 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

次の例は、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 以外のすべての IPv4 ホストへの VTY 接続を許可し、10.55.144.118、172.18.217.79、172.18.217.82、172.18.217.92 以外のすべての 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# conf t
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、VTY の In および Out 方向に 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 回線のアクセス制限を削除する例を示します。

```
switch# conf t
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#
```