CHAPTER 6

セキュリティ コマンド

この章では、Cisco Nexus 5000 シリーズ スイッチで使用できる Cisco NX-OS セキュリティ コマンドについて説明します。

aaa accounting default

アカウンティングの Authentication, Authorization, and Accounting（AAA; 認証、許可、アカウンティング）メソッドを設定するには、**aaa accounting default** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa accounting default {**group** {*group-list*} | **local**}

no aaa accounting default {**group** {*group-list*} | **local**}

シンタックスの説明

group	サーバ グループをアカウンティングで使用するよう指定します。
group-list	1 つまたは複数の RADIUS サーバ グループを指定する空白で区切られたリストです。
local	ローカル データベースをアカウンティングで使用するよう指定します。

コマンドのデフォルト

ローカル データベース

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

group *group-list* メソッドは、RADIUS サーバまたは TACACS+ サーバの既定のセットを参照します。**radius-server host** コマンドを使用してホスト サーバを設定します。**aaa group server** コマンドを使用して、サーバの名前付きグループを作成します。

group メソッドか **local** メソッドまたはその両方を指定すると、アカウンティング認証に失敗します。

例

次に、AAA アカウンティングの RADIUS サーバを設定する例を示します。

```
switch(config)# aaa accounting default group
```

関連コマンド

コマンド	説明
aaa group server radius	AAA RADIUS サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login console

コンソール ログインの AAA 認証メソッドを設定するには、**aaa authentication login console** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login console {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

シンタックスの説明

group	認証のサーバ グループを指定するのに使用します。
group-list	RADIUS サーバまたは TACACS+ サーバ グループのスペースで区切られたリストを指定します。リストには次の内容が含まれます。 • 設定されたすべての RADIUS サーバの **radius** • 設定されたすべての TACACS+ サーバの **tacacs+** • 設定された RADIUS サーバまたは TACACS+ サーバ グループ名
none	（任意）認証でユーザ名を使用するよう指定します。
local	（任意）認証でローカル データベースを使用するよう指定します。

コマンドのデフォルト

ローカル データベース

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

group radius、**group tacacs+**、および **group** *group-list* メソッドでは、定義済みの RADIUS サーバまたは TACACS+ サーバのセットが参照されます。**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してこれらのホスト サーバを設定します。**aaa group server** コマンドを使用して、サーバの名前付きグループを作成します。

group メソッドまたは **local** メソッドを指定してそれが失敗した場合は、認証も失敗します。**none** メソッドを単体または **group** メソッドの後に指定すると、認証は常に成功します。

例

次に、AAA 認証コンソール ログイン メソッドを設定する例を示します。

```
switch(config)# aaa authentication login console group radius
```

次に、デフォルトの AAA 認証コンソール ログイン メソッドに戻す例を示します。

```
switch(config)# no aaa authentication login console group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login default

デフォルトの AAA 認証メソッドを設定するには、**aaa authentication login default** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

シンタックスの説明

group	サーバ グループを認証で使用するよう指定します。
group-list	次の内容を含む RADIUS サーバまたは TACACS+ サーバ グループのスペースで区切られたリストを指定します。 • 設定されたすべての RADIUS サーバの **radius** • 設定されたすべての TACACS+ サーバの **tacacs+** • 設定された RADIUS サーバまたは TACACS+ サーバ グループ名
none	（任意）認証でユーザ名を使用するよう指定します。
local	（任意）認証でローカル データベースを使用するよう指定します。

コマンドのデフォルト

ローカル データベース

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

group radius、**group tacacs+**、および **group** *group-list* メソッドでは、定義済みの RADIUS サーバまたは TACACS+ サーバのセットが参照されます。**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してこれらのホスト サーバを設定します。**aaa group server** コマンドを使用して、サーバの名前付きグループを作成します。

group メソッドまたは **local** メソッドを指定してそれが失敗した場合は、認証も失敗します。**none** メソッドを単体または **group** メソッドの後に指定すると、認証は常に成功します。

例

次に、AAA 認証コンソール ログイン メソッドを設定する例を示します。

```
switch(config)# aaa authentication login default group radius
```

次に、デフォルトの AAA 認証コンソール ログイン メソッドに戻す例を示します。

```
switch(config)# aaa authentication login default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login error-enable

AAA 認証失敗メッセージをコンソールに表示するよう設定するには、**aaa authentication login error-enable** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login error-enable

no aaa authentication login error-enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

ディセーブル

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカル ユーザ データベースにロール オーバーして処理されます。このような状況では、ログイン失敗メッセージの表示がイネーブルに設定されている場合、次のメッセージが表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

例

次に、AAA 認証失敗メッセージのコンソールでの表示をイネーブルにする例を示します。

```
switch(config)# aaa authentication login error-enable
```

次に、AAA 認証失敗メッセージのコンソールでの表示をディセーブルにする例を示します。

```
switch(config)# no aaa authentication login error-enable
```

関連コマンド

コマンド	説明
show aaa authentication	AAA 認証失敗メッセージ表示のステータスを表示します。

aaa authentication login mschap enable

ログイン時に Microsoft Challenge Handshake Authentication Protocol（MSCHAP）をイネーブルにするには、**aaa authentication login mschap enable** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login mschap enable

no aaa authentication login mschap enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

ディセーブル

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、MSCHAP 認証をイネーブルにする例を示します。

```
switch(config)# aaa authentication login mschap enable
```

次に、MSCHAP 認証をディセーブルにする例を示します。

```
switch(config)# no aaa authentication login mschap enable
```

関連コマンド

コマンド	説明
show aaa authentication	MSCHAP 認証のステータスを表示します。

aaa group server radius

RADIUS サーバ グループを作成し、RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。RADIUS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server radius *group-name*

no aaa group server radius *group-name*

シンタックスの説明

group-name	RADIUS サーバ グループ名です。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、RADIUS サーバ グループを作成し、RADIUS サーバ グループ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

次に、RADIUS サーバ グループを削除する例を示します。

```
switch(config)# no aaa group server radius RadServer
```

関連コマンド

コマンド	説明
show aaa groups	サーバ グループ情報を表示します。

action

パケットが VLAN Access Control List（VACL）の **permit** コマンドに一致するときのスイッチの動作を指定するには、**action** コマンドを使用します。**action** コマンドを削除するには、このコマンドの **no** 形式を使用します。

action {drop forward}

no action {drop forward}

シンタックスの説明

drop	スイッチがパケットをドロップするよう指定します。
forward	スイッチがパケットを宛先ポートに転送するよう指定します。

コマンドのデフォルト

なし

コマンド モード

VLAN アクセスマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

action コマンドは、パケットが **match** コマンドで指定された ACL の条件に一致する場合に、デバイスが実行するアクションを指定します。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の Internet Protocol Version 4（IPv4; インターネット プロトコル バージョン 4）ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
match	VLAN アクセス マップでトラフィックのフィルタリングを行う ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法に関する情報を表示します。
statistics	アクセス コントロール リストまたは VLAN アクセス マップの統計情報をイネーブルにします。

コマンド	説明
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	VLAN アクセス マップを 1 つまたは複数の VLAN に適用します。

clear access-list counters

すべての IPv4 Access Control List（ACL; アクセス コントロール リスト）または単独の IPv4 ACL のカウンタを消去するには、**clear access-list counters** コマンドを使用します。

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

シンタックスの説明

access-list-name	（任意）スイッチがカウンタを消去する IPv4 ACL の名前です。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、すべての IPv4 ACL のカウンタを消去する例を示します。

```
switch# clear access-list counters
```

次に、acl-ipv4-01 という名前の IPv4 ACL のカウンタを消去する例を示します。

```
switch# clear access-list counters acl-ipv4-01
```

関連コマンド

コマンド	説明
access-list	VTY 回線に IPv4 ACL を適用します。
ip access-group	インターフェイスに IPv4 ACL を適用します。
ip access-list	IPv4 ACL を設定します。
show access-lists	1 つまたはすべての IPv4、Internet Protocol Version 6（IPv6; インターネット プロトコル バージョン 6）、MAC ACL に関する情報を表示します。
show ip access-lists	1 つまたはすべての IPv4 に関する情報を表示します。

clear accounting log

アカウンティング ログを消去するには、**clear accounting log** コマンドを使用します。

clear accounting log

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、アカウンティング ログを消去する例を示します。

```
switch# clear accounting log
```

関連コマンド

コマンド	説明
show accounting log	アカウンティング ログを表示します。

deadtime

RADIUS または TACACS+ サーバ グループのデッド タイムの時間間隔を設定するには、**deadtime** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

deadtime *minutes*

no deadtime *minutes*

シンタックスの説明

minutes	時間間隔の分です。有効な範囲は 0 ～ 1440 分です。デッド タイムの設定をゼロにすると、タイマーがディセーブルになります。

コマンドのデフォルト

0 分

コマンド モード

RADIUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループのデッド タイムを 2 分に設定する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

次に、TACACS+ サーバ グループのデッド タイムを 5 分に設定する例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

次に、デッド タイムの時間間隔をデフォルトに戻す例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。

コマンド	説明
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

deny（IPv4）

条件に一致するトラフィックを拒否する IPv4 ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

一般的な構文

[*sequence-number*] **deny** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

no deny *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Group Management Protocol（インターネット グループ管理プロトコル）

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Protocol v4（IPv4）

[*sequence-number*] **deny ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

シンタックスの説明

sequence-number	（任意）スイッチにアクセス リストの番号ポジションへコマンドを挿入させる **deny** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、スイッチがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 ルールにシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。
protocol	ルールが一致するパケットのプロトコルの名前または番号です。有効な番号の範囲は、0 から 255 です。有効なプロトコル名は、次のキーワードです。 • **icmp**：ICMP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*icmp-message* 引数を使用できます。 • **igmp**：IGMP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*igmp-type* 引数を使用できます。 • **ip**：すべての IPv4 トラフィックに適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv4 プロトコルに共通して適用されるキーワードと引数だけです。使用できるキーワードには次のものがあります。 – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**：TCP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*flags* 引数、*operator* 引数、**portgroup** キーワード、および **established** キーワードを使用できます。 • **udp**：UDP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*operator* 引数と **portgroup** キーワードを使用できます。
source	ルールに一致する送信元 IPv4 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
destination	ルールに一致する宛先 IPv4 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。

dscp *dscp*	（任意）指定した 6 ビットのディファレンシエーティッド サービス値を IP ヘッダーの DSCP フィールドに持つパケットに対してだけ一致するように、ルールを指定します。*dscp* 引数には、次のキーワードを指定できます。 • 0 ～ 63：DSCP フィールドの 6 ビットに相当する 10 進数。たとえば、10 を指定すると、このルールは DSCP フィールドのビット列が 001010 のパケットにだけ一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低ドロップ確率（001010） • **af12**：AF クラス 1、中程度ドロップ確率（001100） • **af13**：AF クラス 1、高ドロップ確率（001110） • **af21**：AF クラス 2、低ドロップ確率（010010） • **af22**：AF クラス 2、中程度ドロップ確率（010100） • **af23**：AF クラス 2、高ドロップ確率（010110） • **af31**：AF クラス 3、低ドロップ確率（011010） • **af32**：AF クラス 3、中程度ドロップ確率（011100） • **af33**：AF クラス 3、高ドロップ確率（011110） • **af41**：AF クラス 4、低ドロップ確率（100010） • **af42**：AF クラス 4、中程度ドロップ確率（100100） • **af43**：AF クラス 4、高ドロップ確率（100110） • **cs1**：Class-Selector（CS）1、プレシデンス 1（001000） • **cs2**：CS2、プレシデンス 2（010000） • **cs3**：CS3、プレシデンス 3（011000） • **cs4**：CS4、プレシデンス 4（100000） • **cs5**：CS5、プレシデンス 5（101000） • **cs6**：CS6、プレシデンス 6（110000） • **cs7**：CS7、プレシデンス 7（111000） • **default**：デフォルト DSCP 値（000000） • **ef**：Expedited Forwarding（101110）

precedence *precedence*	（任意）*precedence* 引数によって指定された値を伴う IP プレシデンス フィールドを持つパケットだけに一致するようルールを指定します。*precedence* 引数には、次の数値またはキーワードを指定できます。 • 0 ～ 7 : IP プレシデンス フィールドの 3 ビットに相当する 10 進数。たとえば、3 を指定すると、このルールは DSCP フィールドのビット列が 011 のパケットにだけ一致します。 • **critical**：プレシデンス 5（101） • **flashl**：プレシデンス 3（011） • **flash-override**：プレシデンス 4（100） • **immediate**：プレシデンス 2（010） • **internet**：プレシデンス 6（110） • **network**：プレシデンス 7（111） • **priority**：プレシデンス 1（001） • **routine**：プレシデンス 0（000）
fragments	（任意）非先頭フラグメントであるパケットにだけ一致するようルールを指定します。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定した同じルールに指定できません。これらのオプションを評価するためにスイッチが必要とする情報は、先頭フラグメントにだけ含まれているためです。
log	（任意）スイッチが、ルールに一致する各パケットに関する情報メッセージを生成するように指定します。メッセージに含まれる情報は、次のとおりです。 • ACL 名 • パケットが許可されたか拒否されたか • プロトコルが TCP、UDP、ICMP または数値であるか • 発信元アドレスと宛先アドレス、必要に応じて発信元および宛先ポート番号
time-range *time-range-name*	（任意）このルールに適用される時間の範囲を指定します。**time-range** コマンドを使用すると、時間の範囲を設定できます。
icmp-message	（任意、IGMP 専用）指定した ICMP メッセージ タイプのパケットにだけ一致するルールです。この引数には、0 から 255 までの整数か、「使用上のガイドライン」セクションの「ICMP メッセージ タイプ」に一覧されたキーワードのうちの 1 つを指定できます。
igmp-message	（任意、IGMP 専用）指定した IGMP メッセージ タイプのパケットにだけ一致するルールです。*igmp-message* 引数には、IGMP メッセージ番号を 0 ～ 15 の整数で指定できます。また、次のキーワードのいずれかを指定することもできます。 • **dvmrp** : Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • **host-query**：ホスト クエリー • **host-report**：ホスト レポート • **pim**：Protocol Independent Multicast（PIM） • **trace**：マルチキャスト トレース

operator port [*port*]	（任意、TCP および UDP 専用）送信元ポートからのパケット、または *operator* および *port* 引数の条件を満たす宛先ポートに送られるパケットにだけ一致するルールです。これらの引数は、その後に *source* 引数を指定するか、または *destination* 引数を指定するかによって、送信元ポートまたは宛先ポートに適用されます。 *port* 引数は、名前、または TCP ポートか UDP ポートの番号です。有効な番号の範囲は、0 から 65535 の整数です。有効なポート名の一覧については、「使用上のガイドライン」セクションの「TCP ポート名」および「UDP ポート名」を参照してください。 2 番めの *port* 引数は、*operator* 引数が range のときにだけ必要です。 *operator* 引数は、次のキーワードのうち 1 つにする必要があります。 • **eq**：パケット内のポートが *port* 引数と等しい場合にだけ一致します。 • **gt**：パケット内のポートが *port* 引数より大きい場合にだけ一致します。 • **lt**：パケット内のポートが *port* 引数より小さい場合にだけ一致します。 • **neq**：パケット内のポートが *port* 引数と等しくない場合にだけ一致します。 • **range**：2 つの *port* 引数が必要で、パケット内のポートが最初の *port* 引数以上、2 番めの *port* 引数以下の場合にだけ一致します。
portgroup *portgroup*	（任意、TCP および UDP 専用）*portgroup* 引数によって指定された IP ポート グループ オブジェクトのメンバーである送信元ポートからのパケット、または同メンバーである宛先ポートへのパケットにだけ一致するよう指定します。その後、*source* 引数を指定するか、または *destination* 引数を指定するかによって、ポート グループ オブジェクトが送信元ポートまたは宛先ポートに適用されます。 **object-group ip port** コマンドを使用して、IP ポートグループ オブジェクトの作成と変更を行います。
flags	（任意、TCP 専用）特定の TCP コントロール ビット フラグ セットを持つパケットにだけ一致するルールです。*flags* 引数の値は、次の 1 つまたは複数のキーワードにする必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（任意、TCP 専用）確立された TCP 接続に属するパケットにだけルールが一致するよう指定します。スイッチは、ACK ビットまたは RST ビットが設定されている TCP パケットを、確立済みの接続に属しているものと見なします。

コマンドのデフォルト　新しく作成された IPv4 ACL にはルールは含まれません。

シーケンス番号を指定しない場合は、スイッチにより ACL の最後のルールのシーケンス番号に 10 を足したシーケンス番号がルールに割り当てられます。

コマンド モード　IPv4 ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン　スイッチが IPv4 ACL をパケットに適用する場合、ACL のすべてのルールについてパケットを評価します。スイッチは、パケットによって満たされた最初の条件を採用します。複数の条件が満たされる場合は、スイッチは最も小さいシーケンス番号のルールを採用します。

送信元と宛先

source 引数と *destination* 引数はいくつかの方法で指定できます。それぞれのルールで、これらの引数の 1 つを指定するのに使用するメソッドは、他の引数の指定方法には影響しません。ルールを設定する場合は、次のメソッドを使用して *source* 引数と *destination* 引数を指定します。

- IP アドレス グループ オブジェクト：IPv4 アドレス グループ オブジェクトを使用して、*source* 引数または *destination* 引数を指定できます。**object-group ip address** コマンドを使用して、IPv4 ポート グループの作成と変更を行います。構文は次のようになります。

  addrgroup *address-group-name*

  次に、lab-gateway-svrs という名前の IPv4 アドレス オブジェクト グループを使用して、*destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
  ```

- アドレスおよびネットワーク ワイルドカード：IPv4 アドレスの後にネットワーク ワイルドカードを使用して、ホストまたはネットワークを送信元または宛先として指定できます。構文は次のようになります。

  IPv4-address network-wildcard

  次に、IPv4 アドレスとサブネット 192.168.67.0 のネットワーク ワイルドカードを持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）：IPv4 アドレスの後に VLSM を使用して、ホストまたはネットワークを送信元または宛先として指定できます。構文は次のようになります。

  IPv4-address/prefix-len

  次に、IPv4 アドレスとサブネット 192.168.67.0 の VLSM を持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny udp 192.168.67.0/24 any
  ```

- ホスト アドレス：**host** キーワードと IPv4 アドレスを使用して、送信元または宛先としてホストを指定できます。構文は次のようになります。

  host *IPv4-address*

  これは、*IPv4-address*/32、および *IPv4-address* 0.0.0.0 と等しい構文です。

次に、**host** 192.168.67.132 の IPv4 アドレスを持つ *source* 引数を指定する例を示します。

```
switch(config-acl)# deny icmp host 192.168.67.132 any
```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先が任意の IPv4 アドレスであることを指定します。**any** キーワードを使用する例については、このセクションの例を参照してください。それぞれの例で、**any** キーワードを使用して送信元または宛先を指定する方法が示されています。

ICMP メッセージ タイプ

icmp-message 引数には、ICMP メッセージ番号を 0 ～ 255 の整数で指定できます。また、次のキーワードのいずれかを指定することもできます。

- **administratively-prohibited**：管理上禁止
- **alternate-address**：代替アドレス
- **conversion-error**：データグラム変換
- **dod-host-prohibited**：禁止ホスト
- **dod-net-prohibited**：禁止ネット
- **echo**：エコー（ping）
- **echo-reply**：エコー応答
- **general-parameter-problem**：パラメータの問題
- **host-isolated**：分離ホスト
- **host-precedence-unreachable**：プレシデンスが到達不可能なホスト
- **host-redirect**：ホスト リダイレクト
- **host-tos-redirect**：ToS ホスト リダイレクト
- **host-tos-unreachable**：ToS が到達不可能なホスト
- **host-unknown**：不明ホスト
- **host-unreachable**：到達不可能なホスト
- **information-reply**：情報応答
- **information-request**：情報要求
- **mask-reply**：マスク応答
- **mask-request**：マスク要求
- **mobile-redirect**：モバイル ホスト リダイレクト
- **net-redirect**：ネットワーク リダイレクト
- **net-tos-redirect**：ToS ネット リダイレクト
- **net-tos-unreachable**：ToS が到達不可能なネットワーク
- **net-unreachable**：到達不可能なネット
- **network-unknown**：不明ネットワーク
- **no-room-for-option**：パラメータが必要であるが空きスペースがない
- **option-missing**：パラメータが必要であるが存在しない
- **packet-too-big**：フラグメント化と DF セットが必要
- **parameter-problem**：すべてのパラメータの問題

- **port-unreachable**：到達不可能なポート
- **precedence-unreachable**：プレシデンス カットオフ
- **protocol-unreachable**：到達不可能なプロトコル
- **reassembly-timeout**：再アセンブリ タイムアウト
- **redirect**：すべてのリダイレクト
- **router-advertisement**：ルータ ディスカバリ アドバタイズメント
- **router-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元クエンチ
- **source-route-failed**：送信元ルート失敗
- **time-exceeded**：すべての time-exceeded メッセージ
- **timestamp-reply**：タイムスタンプ応答
- **timestamp-request**：タイムスタンプ要求
- **traceroute**：Traceroute
- **ttl-exceeded**：TTL 超過
- **unreachable**：すべての到達不能

TCP ポート名

tcp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で TCP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

bgp：ボーダー ゲートウェイ プロトコル（179）

chargen：文字ジェネレータ（19）

cmd：リモート コマンド（rcmd、514）

daytime：Daytime（13）

discard：廃棄（9）

domain：ドメイン ネーム サービス（53）

drip：ダイナミック ルーティング情報プロトコル（3949）

echo：エコー（7）

exec：EXEC（rsh、512）

finger：フィンガー（79）

ftp：FTP（21）

ftp-data：FTP データ接続（2）

gopher：Gopher（7）

hostname：NIC ホスト名サーバ（11）

ident：Ident プロトコル（113）

irc：インターネット リレー チャット（194）

klogin：Kerberos ログイン（543）

kshell：Kerberos シェル（544）

login：ログイン（rlogin、513）

lpd：プリンタ サービス（515）

nntp：Network News Transport Protocol（119）

pim-auto-rp：PIM Auto-RP（496）

pop2：Post Office Protocol v2（19）

pop3：Post Office Protocol v3（11）

smtp：Simple Mail Transport Protocol（25）

sunrpc：Sun Remote Procedure Call（111）

tacacs：TAC Access Control System（49）

talk：Talk（517）

telnet：Telnet（23）

time：Time（37）

uucp：Unix-to-Unix Copy Program（54）

whois：WHOIS/NICNAME（43）

www：World Wide Web（HTTP、8）

UDP ポート名

udp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で UDP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

biff：Biff（メール通知、comsat、512）

bootpc：Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）

bootps：ブートストラップ プロトコル（BOOTP）サーバ（67）

discard：廃棄（9）

dnsix：DNSIX セキュリティ プロトコル監査（195）

domain：ドメイン ネーム サービス（DNS、53）

echo：エコー（7）

isakmp：Internet Security Association および Key Management Protocol（5）

mobile-ip：モバイル IP 登録（434）

nameserver：IEN116 ネーム サービス（廃止、42）

netbios-dgm：NetBIOS データグラム サービス（138）

netbios-ns：NetBIOS ネーム サービス（137）

netbios-ss：NetBIOS セッション サービス（139）

non500-isakmp：Internet Security Association および Key Management Protocol（45）

ntp：ネットワーク タイム プロトコル（123）

pim-auto-rp：PIM Auto-RP（496）

rip：ルーティング情報プロトコル（ルータ、in.routed、52）

snmp：簡易ネットワーク管理プロトコル（161）

snmptrap：SNMP トラップ（162）

sunrpc：Sun Remote Procedure Call（111）

syslog：システム ロガー（514）

tacacs：TAC Access Control System（49）

talk：Talk（517）

tftp：Trivial File Transfer Protocol（69）

time：Time（37）

who：Who サービス（rwho、513）

xdmcp：X Display Manager Control Protocol（177）

例

次に、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP および UDP トラフィックを拒否するルールと、他のすべての IPv4 トラフィックを許可する最終ルールを使用して、acl-lab-01 という名前で IPv4 ACL を設定する例を示します。

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
permit（IPv4）	IPv4 ACL に許可ルールを設定します。
remark	IPv4 ACL にリマークを設定します。
show ip access-list	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。

deny（IPv6）

条件に一致するトラフィックを拒否する IPv6 ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。条件に一致するトラフィックを拒否する IPv6 ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

一般的な構文

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no deny *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number* | **no**] **deny icmp** *source destination* [*icmp-message*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Protocol v6（IPv6）

[*sequence-number*] **deny ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*]
[**fragments**] [**log**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol（SCTP）

[*sequence-number* | **no**] **deny sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*]
[**established**]

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number* | **no**] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

シンタックスの説明

sequence-number	（任意）デバイスにアクセス リストの番号ポジションへコマンドを挿入させる **deny** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、デバイスがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 ルールにシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。
protocol	ルールが一致するパケットのプロトコルの名前または番号です。有効な番号の範囲は、0 から 255 です。有効なプロトコル名は、次のキーワードです。 • **ahp**：Authentication Header Protocol（AHP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **esp**：Encapsulating Security Payload（ESP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **icmp**：ICMP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*icmp-message* 引数を使用できます。 • **ipv6**：すべての IPv6 トラフィックに適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **pcp**：Payload Compression Protocol（PCP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **sctp**：Stream Control Transmission Protocol（SCTP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*operator* 引数と **portgroup** キーワードを使用できます。 • **tcp**：TCP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*flags* 引数、*operator* 引数、**portgroup** キーワード、および **established** キーワードを使用できます。 • **udp**：UDP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*operator* 引数と **portgroup** キーワードを使用できます。
source	ルールに一致する送信元 IPv6 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。

destination	ルールに一致する宛先 IPv6 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
dscp *dscp*	（任意）指定した 6 ビットのディファレンシエーティッド サービス値を IPv6 ヘッダーの DSCP フィールドに持つパケットに対してだけ一致するように、ルールを指定します。*dscp* 引数には、次のキーワードを指定できます。 • 0 ～ 63：DSCP フィールドの 6 ビットに相当する 10 進数。たとえば、10 を指定すると、このルールは DSCP フィールドのビット列が 001010 のパケットにだけ一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低ドロップ確率（001010） • **af12**：AF クラス 1、中程度ドロップ確率（001100） • **af13**：AF クラス 1、高ドロップ確率（001110） • **af21**：AF クラス 2、低ドロップ確率（010010） • **af22**：AF クラス 2、中程度ドロップ確率（010100） • **af23**：AF クラス 2、高ドロップ確率（010110） • **af31**：AF クラス 3、低ドロップ確率（011010） • **af32**：AF クラス 3、中程度ドロップ確率（011100） • **af33**：AF クラス 3、高ドロップ確率（011110） • **af41**：AF クラス 4、低ドロップ確率（100010） • **af42**：AF クラス 4、中程度ドロップ確率（100100） • **af43**：AF クラス 4、高ドロップ確率（100110） • **cs1**：Class-Selector（CS）1、プレシデンス 1（001000） • **cs2**：CS2、プレシデンス 2（010000） • **cs3**：CS3、プレシデンス 3（011000） • **cs4**：CS4、プレシデンス 4（100000） • **cs5**：CS5、プレシデンス 5（101000） • **cs6**：CS6、プレシデンス 6（110000） • **cs7**：CS7、プレシデンス 7（111000） • **default**：デフォルト DSCP 値（000000） • **ef**：Expedited Forwarding（101110）
flow-label *flow-label-value*	（任意）*flow-label-value* 引数に指定した値を Flow Label ヘッダー フィールドに持つ IPv6 パケットにだけ一致するルールを指定します。 *flow-label-value* 引数には、0 ～ 1048575 の整数を指定できます。
fragments	（任意）非先頭フラグメント パケットにだけ一致するルールを指定します。デバイスは、フラグメント拡張ヘッダーにゼロ以外のフラグメント オフセットが含まれるパケットを、非先頭フラグメント パケットと見なします。TCP ポート番号などのレイヤ 4 オプションを指定するルールにはこのキーワードを指定できません。レイヤ 4 オプションを評価するには、先頭フラグメントにしか含まれない情報が必要になるからです。

log	（任意）デバイスが、ルールに一致する各パケットに関する情報メッセージを生成するように指定します。メッセージに含まれる情報は、次のとおりです。 • ACL 名 • パケットが許可されたか拒否されたか • プロトコルが TCP、UDP、ICMP または数値であるか • 発信元アドレスと宛先アドレス、必要に応じて発信元および宛先ポート番号
time-range *time-range-name*	（任意）このルールに適用される時間の範囲を指定します。**time-range** コマンドを使用すると、時間の範囲を設定できます。
icmp-message	（任意、ICMP 専用）ルールに一致する ICMPv6 メッセージ タイプ。この引数には、0 から 255 までの整数か、「使用上のガイドライン」セクションの「ICMPv6 メッセージ タイプ」に一覧されたキーワードのうちの 1 つを指定できます。
operator port [*port*]	（任意。TCP、UDP、および SCTP 専用）送信元ポートからのパケット、または *operator* および *port* 引数の条件を満たす宛先ポートに送られるパケットにだけ一致するルールです。これらの引数は、その後に *source* 引数を指定するか、または *destination* 引数を指定するかによって、送信元ポートまたは宛先ポートに適用されます。 *port* 引数は、名前、または TCP ポートか UDP ポートの番号です。有効な番号の範囲は、0 から 65535 の整数です。有効なポート名の一覧については、「使用上のガイドライン」セクションの「TCP ポート名」および「UDP ポート名」を参照してください。 2 番めの *port* 引数は、*operator* 引数が range のときにだけ必要です。 *operator* 引数は、次のキーワードのうち 1 つにする必要があります。 • **eq**：パケット内のポートが *port* 引数と等しい場合にだけ一致します。 • **gt**：パケット内のポートが *port* 引数より大きい場合にだけ一致します。 • **lt**：パケット内のポートが *port* 引数より小さい場合にだけ一致します。 • **neq**：パケット内のポートが *port* 引数と等しくない場合にだけ一致します。 • **range**：2 つの *port* 引数が必要で、パケット内のポートが最初の *port* 引数以上、2 番めの *port* 引数以下の場合にだけ一致します。
portgroup *portgroup*	（任意。TCP、UDP、および SCTP 専用）*portgroup* 引数によって指定された IP ポートグループ オブジェクトのメンバーである送信元ポートからのパケット、または同メンバーである宛先ポートへのパケットにだけ一致するよう指定します。その後、*source* 引数を指定するか、または *destination* 引数を指定するかによって、ポート グループ オブジェクトが送信元ポートまたは宛先ポートに適用されます。 **object-group ip port** コマンドを使用して、IP ポートグループ オブジェクトの作成と変更を行います。

established	（任意、TCP 専用）確立された TCP 接続に属するパケットにだけルールが一致するよう指定します。デバイスは、ACK ビットまたは RST ビットが設定されている TCP パケットを、確立済みの接続に属しているものと見なします。
flags	（任意、TCP 専用）特定の TCP コントロール ビット フラグ セットを持つパケットにだけ一致するルールです。*flags* 引数の値は、次の 1 つまたは複数のキーワードにする必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

コマンドのデフォルト　なし

コマンド モード　IPv6 ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン　新しく作成された IPv6 ACL にはルールは含まれません。

デバイスが IPv6 ACL をパケットに適用する場合、ACL のすべてのルールについてパケットを評価します。デバイスは、パケットによって満たされた最初の条件を採用します。複数の条件が満たされる場合は、デバイスは最も小さいシーケンス番号のルールを採用します。

このコマンドにライセンスは必要ありません。

送信元と宛先

source 引数と *destination* 引数はいくつかの方法で指定できます。それぞれのルールで、これらの引数の 1 つを指定するのに使用するメソッドは、他の引数の指定方法には影響しません。ルールを設定する場合は、次のメソッドを使用して *source* 引数と *destination* 引数を指定します。

- IPv6 アドレス グループ オブジェクト：IPv6 アドレス グループ オブジェクトを使用して、*source* 引数または *destination* 引数を指定できます。**object-group ipv6 address** コマンドを使用して、IPv6 アドレス グループ オブジェクトの作成と変更を行います。構文は次のようになります。

  addrgroup *address-group-name*

  次に、lab-svrs-1301 という名前の IPv6 アドレス オブジェクト グループを使用して、*destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny ipv6 any addrgroup lab-svrs-1301
  ```

- アドレスおよび可変長サブネット マスク（VLSM）：IPv6 アドレスの後に VLSM を使用して、ホストまたはネットワークを送信元または宛先として指定できます。構文は次のようになります。

IPv6-address/prefix-len

次に、IPv6 アドレスとネットワーク 2001:0db8:85a3:: の VLSM を持つ *source* 引数を指定する例を示します。

```
switch(config-acl)# deny udp 2001:0db8:85a3::/48 any
```

- ホスト アドレス：**host** キーワードと IPv6 アドレスを使用して、送信元または宛先としてホストを指定できます。構文は次のようになります。

  host *IPv6-address*

  この構文は、*IPv6-address*/128 に相当します。

  次に、**host** キーワードと 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 アドレスで *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先が任意の IPv6 アドレスであることを指定します。**any** キーワードを使用する例については、このセクションの例を参照してください。それぞれの例で、**any** キーワードを使用して送信元または宛先を指定する方法が示されています。

ICMPv6 メッセージ タイプ

icmp-message 引数には、ICMPv6 メッセージ番号を 0 ～ 255 の整数で指定できます。また、次のキーワードのいずれかを指定することもできます。

- **beyond-scope**：スコープ外の宛先
- **destination-unreachable**：宛先アドレスが到達不能
- **echo-reply**：エコー応答
- **echo-request**：エコー要求（ping）
- **header**：パラメータ ヘッダーの問題
- **hop-limit**：配送中のホップ数の限界の超過
- **mld-query**：Multicast Listener Discovery クエリー
- **mld-reduction**：Multicast Listener Discovery リダクション
- **mld-report**：Multicast Listener Discovery レポート
- **nd-na**：ネイバー ディスカバリのネイバー アドバタイズメント
- **nd-ns**：ネイバー ディスカバリのネイバー要求
- **next-header**：パラメータ ネクスト ヘッダーの問題
- **no-admin**：管理上禁止された宛先
- **no-route**：宛先へのルートがない
- **packet-too-big**：パケット サイズ超過
- **parameter-option**：パラメータ オプションの問題
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：到達不可能なポート
- **reassembly-timeout**：再アセンブリ タイムアウト
- **redirect**：ネイバー リダイレクト
- **renum-command**：ルータの再番号付けコマンド

- **renum-result**：ルータの再番号付けの結果
- **renum-seq-number**：ルータの再番号付けのシーケンス番号リセット
- **router-advertisement**：ネイバー ディスカバリのルータ アドバタイズメント
- **router-renumbering**：すべてのルータの再番号付け
- **router-solicitation**：ネイバー ディスカバリのルータ要求
- **time-exceeded**：すべての時間超過メッセージ
- **unreachable**：すべて到達不能

TCP ポート名

tcp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で TCP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

bgp：ボーダー ゲートウェイ プロトコル（179）

chargen：文字ジェネレータ（19）

cmd：リモート コマンド（rcmd、514）

daytime：Daytime（13）

discard：廃棄（9）

domain：ドメイン ネーム サービス（53）

drip：ダイナミック ルーティング情報プロトコル（3949）

echo：エコー（7）

exec：EXEC（rsh、512）

finger：フィンガー（79）

ftp：FTP（21）

ftp-data：FTP データ接続（2）

gopher：Gopher（7）

hostname：NIC ホスト名サーバ（11）

ident：Ident プロトコル（113）

irc：インターネット リレー チャット（194）

klogin：Kerberos ログイン（543）

kshell：Kerberos シェル（544）

login：ログイン（rlogin、513）

lpd：プリンタ サービス（515）

nntp：Network News Transport Protocol（119）

pim-auto-rp：PIM Auto-RP（496）

pop2：Post Office Protocol v2（19）

pop3：Post Office Protocol v3（11）

smtp：Simple Mail Transport Protocol（25）

sunrpc：Sun Remote Procedure Call（111）

tacacs：TAC Access Control System（49）

talk：Talk（517）

telnet：Telnet（23）

time：Time（37）

uucp：Unix-to-Unix Copy Program（54）

whois：WHOIS/NICNAME（43）

www：World Wide Web（HTTP、8）

UDP ポート名

udp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で UDP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

biff：Biff（メール通知、comsat、512）

bootpc：ブートストラップ プロトコル（BOOTP）クライアント（68）

bootps：ブートストラップ プロトコル（BOOTP）サーバ（67）

discard：廃棄（9）

dnsix：DNSIX セキュリティ プロトコル監査（195）

domain：ドメイン ネーム サービス（DNS、53）

echo：エコー（7）

isakmp：Internet Security Association および Key Management Protocol（5）

mobile-ip：モバイル IP 登録（434）

nameserver：IEN116 ネーム サービス（廃止、42）

netbios-dgm：NetBIOS データグラム サービス（138）

netbios-ns：NetBIOS ネーム サービス（137）

netbios-ss：NetBIOS セッション サービス（139）

non500-isakmp：Internet Security Association および Key Management Protocol（45）

ntp：ネットワーク タイム プロトコル（123）

pim-auto-rp：PIM Auto-RP（496）

rip：ルーティング情報プロトコル（ルータ、in.routed、52）

snmp：簡易ネットワーク管理プロトコル（161）

snmptrap：SNMP トラップ（162）

sunrpc：Sun Remote Procedure Call（111）

syslog：システム ロガー（514）

tacacs：TAC Access Control System（49）

talk：Talk（517）

tftp：Trivial File Transfer Protocol（69）

time：Time（37）

who：Who サービス（rwho、513）

xdmcp：X Display Manager Control Protocol（177）

例

次に、2001:0db8:85a3:: および 2001:0db8:69f2:: のネットワークから 2001:0db8:be03:2112:: ネットワークへ送信されるすべての TCP および UDP トラフィックを拒否するルールで、acl-lab13-ipv6 という名前の IPv6 ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

次に、IPv6 アドレス オブジェクト グループ eng_ipv6 から IPv6 アドレス オブジェクト グループ marketing_group へ送信されるすべての IPv6 トラフィックを拒否するルールで、ipv6-eng-to-marketing という名前の IPv6 ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# deny ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 ACL を設定します。
permit（IPv6）	IPv6 ACL に許可ルールを設定します。
remark	ACL にリマークを設定します。
time-range	時間の範囲を設定します。

deny（MAC）

条件に一致するトラフィックを拒否する Media Access Control（MAC; メディア アクセス制御）アクセス コントロール リスト（ACL）を作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

シンタックスの説明

sequence-number	（任意）スイッチにアクセス リストの番号ポジションへコマンドを挿入させる **deny** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、スイッチがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 ルールにシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。
source	ルールに一致する送信元 MAC アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
destination	ルールに一致する宛先 MAC アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
protocol	（任意）ルールに一致するプロトコル番号です。有効なプロトコル番号の範囲は 0x0 から 0xffff です。有効なプロトコル名のリストについては、「使用上のガイドライン」セクションの「MAC プロトコル」を参照してください。
cos *cos-value*	（任意）IEEE 802.1Q ヘッダーに *cos-value* 引数で指定された Class of Service（CoS; サービス クラス）値が含まれるパケットだけに一致するように、ルールを指定します。*cos-value* 引数は、0 から 7 までの整数となります。
vlan *vlan-id*	（任意）指定された VLAN ID が IEEE 802.1Q ヘッダーに含まれるパケットだけに一致するように、ルールを指定します。*vlan-id* 引数は、1 から 4094 までの整数となります。

コマンドのデフォルト

新しく作成された MAC ACL にはルールは含まれません。

シーケンス番号を指定しない場合は、スイッチにより ACL の最後のルールのシーケンス番号に 10 を足したシーケンス番号がルールに割り当てられます。

コマンド モード

MAC ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチが MAC ACL をパケットに適用する場合、ACL のすべてのルールについてパケットを評価します。スイッチは、パケットによって満たされた最初の条件を採用します。複数の条件が満たされる場合は、スイッチは最も小さいシーケンス番号のルールを採用します。

送信元と宛先

source 引数と *destination* 引数は 2 つの方法で指定できます。それぞれのルールで、これらの引数の 1 つを指定するのに使用するメソッドは、他の引数の指定方法には影響しません。ルールを設定する場合は、次のメソッドを使用して *source* 引数と *destination* 引数を指定します。

- アドレスとマスク：MAC アドレスの後にマスクを使用して、1 つのアドレスまたはアドレスのグループを指定できます。構文は次のようになります。

  MAC-address MAC-mask

  次に、MAC アドレス 00c0.4f03.0a72 を持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、MAC ベンダー コードが 00603e のすべての MAC アドレスを持つ *destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先が任意の MAC アドレスであることを指定できます。**any** キーワードを使用する例については、このセクションの例を参照してください。それぞれの例で、**any** キーワードを使用して送信元または宛先を指定する方法が示されています。

MAC プロトコル

protocol 引数は、MAC プロトコル番号またはキーワードを指定します。プロトコル番号は、先頭に 0x が付く 4 バイトの 16 進数です。有効なプロトコル番号の範囲は 0x0 から 0xffff です。有効なキーワードは、次のとおりです。

- **aarp**：Appletalk ARP（0x80f3）
- **appletalk**：Appletalk（0x809b）
- **decnet-iv**：DECnet Phase IV（0x6003）
- **diagnostic**：DEC Diagnostic Protocol（0x6005）
- **etype-6000**：EtherType 0x6000（0x6000）
- **etype-8042**：EtherType 0x8042（0x8042）
- **ip**：Internet Protocol v4（0x0800）
- **lat**：DEC LAT（0x6004）
- **lavc-sca**：DEC LAVC、SCA（0x6007）
- **mop-console**：DEC MOP リモート コンソール（0x6002）
- **mop-dump**：DEC MOP ダンプ（0x6001）
- **vines-echo**：VINES エコー（0x0baf）

例

次に、mac-ip-filter という名前で、2 つの MAC アドレスのグループ間ですべての非 IPv4 トラフィックを許可する MAC ACL を設定する例を示します。

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
switch(config-mac-acl)# permit any any
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
permit（MAC）	MAC ACL に拒否ルールを設定します。
remark	ACL にリマークを設定します。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

description（ユーザ ロール）

ユーザ ロールの説明を設定するには、**description** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

description *text*

no description

シンタックスの説明

text	ユーザ ロールを説明するテキスト ストリング。最大長は 128 文字です。

コマンドのデフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ユーザ ロールを説明するテキストに、ブランクのスペースを含めることができます。

例

次に、ユーザ ロールの説明を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

次に、ユーザ ロールから説明を削除する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no description
```

feature

ユーザ ロール機能グループの機能を設定するには、**feature** コマンドを使用します。ユーザ ロール機能グループの機能を削除するには、このコマンドの **no** 形式を使用します。

feature *feature-name*

no feature *feature-name*

シンタックスの説明

feature-name	**show role feature** コマンドの出力で一覧されるスイッチ機能名

コマンドのデフォルト

なし

コマンド モード

ユーザ ロール機能グループ コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで使用する有効な機能名の一覧を表示するには、**show role** feature コマンドを使用します。

例

次に、機能をユーザ ロール機能グループに追加する例を示します。

```
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

次に、ユーザ ロール機能グループから機能を削除する例を示します。

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

関連コマンド

コマンド	説明
role feature-group name	ユーザ ロール機能グループを作成または設定します。
show role feature-group	ユーザ ロール機能グループを表示します。

interface policy deny

ユーザ ロールのインターフェイス ポリシー コンフィギュレーション モードを開始するには、**interface policy deny** コマンドを使用します。ユーザ ロールのインターフェイス ポリシーをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

interface policy deny

no interface policy deny

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

すべてのインターフェイス

コマンド モード

ユーザ ロール コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールのインターフェイス ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

次に、ユーザ ロールのインターフェイス ポリシーをデフォルトに戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。

ip access-list

IPv4 アクセス コントロール リスト（ACL）を作成するか、特定の ACL の IP アクセス リスト コンフィギュレーション モードを開始するには、**ip access-list** コマンドを使用します。IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-list *access-list-name*

no ip access-list *access-list-name*

シンタックスの説明

access-list-name	IPv4 ACL の名前です。最大 64 文字まで使用できます。名前にスペースや引用符を含めることはできません。

コマンドのデフォルト

IPv4 ACL はデフォルトでは定義されていません。

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

IPv4 ACL を使用して IPv4 トラフィックのフィルタリングを行います。

ip access-list コマンドを使用すると、スイッチは IP アクセス リスト コンフィギュレーション モードを開始します。そこで IPv4 **deny** コマンドおよび **permit** コマンドを使用して ACL のルールを設定できます。指定された ACL が存在しない場合は、このコマンドを入力したときにスイッチが ACL を作成します。

ACL をインターフェイスに適用するには、**ip access-group** コマンドを使用します。

どの IPv4 ACL にも、最後のルールとして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。

IPv4 ACL には、ネイバー ディスカバリ プロセスを可能にする追加の暗黙のルールはありません。IPv6 ネイバー ディスカバリ プロセスに相当する IPv4 のプロセスである Address Resolution Protocol（ARP; アドレス解決プロトコル）は、個別のデータ リンク レイヤ プロトコルを使用します。デフォルトでは、IPv4 ACL はインターフェイス上での ARP パケットの送受信を暗黙的に許可します。

例

次に、ip-acl-01 という名前の IPv4 ACL の IP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
access-list	VTY 回線に IPv4 ACL を適用します。
deny（IPv4）	IPv4 ACL に拒否ルールを設定します。
ip access-group	インターフェイスに IPv4 ACL を適用します。
permit（IPv4）	IPv4 ACL に許可ルールを設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。

ip port access-group

IPv4 アクセス コントロール リスト（ACL）をポート ACL としてインターフェイスに適用するには、**ip port access-group** コマンドを使用します。IPv4 ACL をインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

シンタックスの説明

access-list-name	IPv4 ACL の名前で、最大 64 文字の英数字を使用できます。大文字小文字が区別されます。
in	ACL が着信トラフィックに適用されるよう指定します。

コマンドのデフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、インターフェイスには IPv4 ACL は適用されません。

ip port access-group コマンドを使用して、IPv4 ACL をポート ACL として次のインターフェイス タイプに適用できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 EtherChannel インターフェイス

IPv4 ACL を VLAN ACL として適用することもできます。詳細については、**match** コマンドを参照してください。

スイッチは、ポート ACL を着信トラフィックにだけ適用します。スイッチは、着信パケットを ACL のルールに対してチェックします。最初の一致ルールによりパケットが許可された場合、スイッチはそのパケットの処理を継続します。最初の一致ルールによりパケットが拒否された場合、スイッチはそのパケットをドロップし、ICMP ホスト到達不能メッセージを返します。

インターフェイスから削除されていない ACL をスイッチから削除すると、削除された ACL はそのインターフェイス上のトラフィックに影響しなくなります。

例

次に、ip-acl-01 という名前の IPv4 ACL をポート ACL としてイーサネット インターフェイス 1/2 に適用する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# ip port access-group ip-acl-01 in
```

次に、ip-acl-01 という名前の IPv4 ACL をイーサネット インターフェイス 1/2 から削除する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no ip port access-group ip-acl-01 in
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定のインターフェイスの実行コンフィギュレーションを表示します。

ipv6 access-list

IPv6 アクセス コントロール リスト（ACL）を作成するか、特定の ACL の IP アクセス リスト コンフィギュレーション モードを開始するには、**ipv6 access-list** コマンドを使用します。IPv6 ACL を削除するには、このコマンドの **no** 形式を使用します。

ipv6 access-list *access-list-name*

no ipv6 access-list *access-list-name*

シンタックスの説明

access-list-name	IPv6 ACL の名前です。最大 64 文字まで使用できます。名前にスペースや引用符を含めることはできません。

コマンドのデフォルト

デフォルトでは IPv6 ACL は定義されていません。

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 ACL を使用して IPv6 トラフィックのフィルタリングを行います。

ipv6 access-list コマンドを使用すると、スイッチは IP アクセス リスト コンフィギュレーション モードを開始します。そこで IPv6 **deny** コマンドおよび **permit** コマンドを使用して ACL のルールを設定できます。指定された ACL が存在しない場合は、このコマンドを入力したときにスイッチが ACL を作成します。

どの IPv6 ACL にも、最後のルールとして次の暗黙のルールがあります。

```
deny ipv6 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。

例

次に、ipv6-acl-01 という名前の IPv6 ACL の IP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# ipv6 access-list ipv6-acl-01
switch(config-ipv6-acl)#
```

関連コマンド

コマンド	説明
deny（IPv6）	IPv6 ACL に拒否ルールを設定します。
permit（IPv6）	IPv6 ACL に許可ルールを設定します。

ipv6 port traffic-filter

IPv6 アクセス コントロール リスト（ACL）をポート ACL としてインターフェイスに適用するには、**ipv6 port traffic-filter** コマンドを使用します。IPv6 ACL をインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

ipv6 port traffic-filter *access-list-name* **in**

no ipv6 port traffic-filter *access-list-name* **in**

シンタックスの説明

access-list-name	IPv6 ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
in	ACL を着信トラフィックに適用することを指定します。

コマンドのデフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、インターフェイスに適用される IPv6 ACL はありません。

ipv6 port traffic-filter コマンドを使用して、IPv6 ACL をポート ACL として次のインターフェイス タイプに適用できます。

- イーサネット インターフェイス
- EtherChannel インターフェイス

また、**ipv6 port traffic-filter** コマンドを使用して、IPv6 ACL をポート ACL として次のインターフェイス タイプに適用することもできます。

- VLAN インターフェイス

（注） 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。詳細については、**feature interface-vlan** コマンドを参照してください。

スイッチは、ポート ACL を着信トラフィックにだけ適用します。スイッチは、着信パケットを ACL のルールに対してチェックします。最初の一致ルールによりパケットが許可された場合、スイッチはそのパケットの処理を継続します。最初の一致ルールによりパケットが拒否された場合、スイッチはそのパケットをドロップし、ICMP ホスト到達不能メッセージを返します。

インターフェイスから削除されていない ACL をデバイスから削除すると、削除された ACL はそのインターフェイス上のトラフィックに影響しなくなります。

例

次に、ipv6-acl という名前の IPv6 ACL をイーサネット インターフェイス 1/3 に適用する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# ipv6 port traffic-filter ipv6-acl in
```

次に、ipv6-acl という名前の IPv6 ACL をイーサネット インターフェイス 1/3 から削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# no ipv6 port traffic-filter ipv6-acl in
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ipv6 access-lists	特定の IPv6 ACL またはすべての IPv6 ACL を表示します。

mac access-list

メディア アクセス制御（MAC）アクセス コントロール リスト（ACL）を作成するか、特定の ACL の MAC アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list** コマンドを使用します。MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac access-list *access-list-name*

no mac access-list *access-list-name*

シンタックスの説明

access-list-name	MAC ACL の名前です。

コマンドのデフォルト

デフォルトでは MAC ACL は定義されていません。

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

MAC ACL を使用して、非 IP トラフィックのフィルタリングを行います。パケット分類をディセーブルにしている場合は、MAC ACL を使用してすべてのトラフィックのフィルタリングを行うことができます。

mac access-list コマンドを使用すると、スイッチは MAC アクセス リスト コンフィギュレーション モードを開始します。そこで MAC **deny** コマンドおよび **permit** コマンドを使用して ACL のルールを設定できます。指定された ACL が存在しない場合は、このコマンドを入力したときにスイッチが ACL を作成します。

ACL をインターフェイスに適用するには、**mac access-group** コマンドを使用します。

どの MAC ACL にも、最後のルールとして次の暗黙のルールがあります。

```
deny any any protocol
```

この暗黙のルールにより、トラフィックのレイヤ 2 ヘッダーで指定されているプロトコルに関係なく、一致しないパケットは確実に拒否されます。

例

次に、mac-acl-01 という名前の MAC ACL の MAC アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に拒否ルールを設定します。
mac access-group	インターフェイスに MAC ACL を適用します。
permit（MAC）	MAC ACL に許可ルールを設定します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

mac port access-group

MAC アクセス コントロール リスト（ACL）をインターフェイスに適用するには、**mac port access-group** コマンドを使用します。MAC ACL をインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

シンタックスの説明

access-list-name	MAC ACL の名前で、最大 64 文字の英数字を使用できます。大文字小文字が区別されます。

コマンドのデフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、インターフェイスには MAC ACL は適用されません。

MAC ACL を非 IP トラフィックに適用します。パケット分類がディセーブルの場合、MAC ACL はすべてのトラフィックに適用されます。

mac port access-group コマンドを使用して、MAC ACL をポート ACL として次のインターフェイス タイプに適用できます。

- レイヤ 2 インターフェイス
- レイヤ 2 EtherChannel インターフェイス

MAC ACL を VLAN ACL として適用することもできます。詳細については、「match」（P.52）を参照してください。

スイッチは、MAC ACL を着信トラフィックにだけ適用します。スイッチが MAC ACL を適用する場合、ACL のルールについてパケットを評価します。最初の一致ルールによりパケットが許可された場合、スイッチはそのパケットの処理を継続します。最初の一致ルールによりパケットが拒否された場合、スイッチはそのパケットをドロップし、ICMP ホスト到達不能メッセージを返します。

インターフェイスから削除されていない ACL をスイッチから削除すると、削除された ACL はそのインターフェイス上のトラフィックに影響しなくなります。

例

次に、mac-acl-01 という名前の MAC ACL をイーサネット インターフェイス 1/2 に適用する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# mac port access-group mac-acl-01
```

次に、mac-acl-01 という名前の MAC ACL をイーサネット インターフェイス 1/2 から削除する例を示します。

```
switch(config)# interface ethernet 1/2
switch(config-if)# no mac port access-group mac-acl-01
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL を表示します。
show mac access-lists	特定の MAC ACL またはすべての MAC ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定のインターフェイスの実行コンフィギュレーションを表示します。

match

VLAN アクセス マップのトラフィック フィルタリングにアクセス コントロール リスト（ACL）を指定するには、**match** コマンドを使用します。VLAN アクセス マップから **match** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match {ip | ipv6 | mac} address *access-list-name*

no match {ip | ipv6 | mac} address *access-list-name*

シンタックスの説明

ip	指定されている ACL は IPv4 ACL です。
ipv6	IPv6 機能を設定します。
mac	指定されている ACL は MAC ACL です。
address *access-list-name*	ACL を指定します。

コマンドのデフォルト

デフォルトでは、スイッチはトラフィックを分類して、IPv4 ACL を IPv4 トラフィックに、MAC ACL を他のすべてのトラフィックに適用します。

コマンド モード

VLAN アクセスマップ コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

指定できる **match** コマンドは、アクセス マップごとに 1 つだけです。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップでトラフィックのフィルタリングを行うアクションを指定します。
show vlan access-map	すべての VLAN アクセス マップまたは VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法に関する情報を表示します。

コマンド	説明
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	VLAN アクセス マップを 1 つまたは複数の VLAN に適用します。

permit（IPv4）

条件に一致するトラフィックを許可する IPv4 アクセス コントロール リスト（ACL）ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

一般的な構文

[*sequence-number*] **permit** *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Group Management Protocol（インターネット グループ管理プロトコル）

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Protocol v4（IPv4）

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**log**] [**time-range** *time-range-name*]

シンタックスの説明

sequence-number	（任意）スイッチにアクセス リストの番号ポジションへコマンドを挿入させる **permit** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、スイッチがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 ルールにシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。
protocol	ルールが一致するパケットのプロトコルの名前または番号です。有効な番号の範囲は、0 から 255 です。有効なプロトコル名は、次のキーワードです。 • **icmp**：ICMP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*icmp-message* 引数を使用できます。 • **igmp**：IGMP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*igmp-type* 引数を使用できます。 • **ip**：すべての IPv4 トラフィックに適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv4 プロトコルに共通して適用されるキーワードと引数だけです。使用できるキーワードには次のものがあります。 – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**：TCP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*flags* 引数、*operator* 引数、**portgroup** キーワード、および **established** キーワードを使用できます。 • **udp**：UDP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*operator* 引数と **portgroup** キーワードを使用できます。
source	ルールに一致する送信元 IPv4 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
destination	ルールに一致する宛先 IPv4 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。

dscp *dscp*	（任意）指定した 6 ビットのディファレンシエーティッド サービス値を IP ヘッダーの DSCP フィールドに持つパケットに対してだけ一致するように、ルールを指定します。*dscp* 引数には、次のキーワードを指定できます。 • 0 ～ 63：DSCP フィールドの 6 ビットに相当する 10 進数。たとえば、10 を指定すると、このルールは DSCP フィールドのビット列が 001010 のパケットにだけ一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低ドロップ確率（001010） • **af12**：AF クラス 1、中程度ドロップ確率（001100） • **af13**：AF クラス 1、高ドロップ確率（001110） • **af21**：AF クラス 2、低ドロップ確率（010010） • **af22**：AF クラス 2、中程度ドロップ確率（010100） • **af23**：AF クラス 2、高ドロップ確率（010110） • **af31**：AF クラス 3、低ドロップ確率（011010） • **af32**：AF クラス 3、中程度ドロップ確率（011100） • **af33**：AF クラス 3、高ドロップ確率（011110） • **af41**：AF クラス 4、低ドロップ確率（100010） • **af42**：AF クラス 4、中程度ドロップ確率（100100） • **af43**：AF クラス 4、高ドロップ確率（100110） • **cs1**：Class-Selector（CS）1、プレシデンス 1（001000） • **cs2**：CS2、プレシデンス 2（010000） • **cs3**：CS3、プレシデンス 3（011000） • **cs4**：CS4、プレシデンス 4（100000） • **cs5**：CS5、プレシデンス 5（101000） • **cs6**：CS6、プレシデンス 6（110000） • **cs7**：CS7、プレシデンス 7（111000） • **default**：デフォルト DSCP 値（000000） • **ef**：Expedited Forwarding（101110）

precedence *precedence*	（任意）*precedence* 引数によって指定された値を伴う IP プレシデンス フィールドを持つパケットだけに一致するようルールを指定します。*precedence* 引数には、次の数値またはキーワードを指定できます。 • 0 ～ 7 : IP プレシデンス フィールドの 3 ビットに相当する 10 進数。たとえば、3 を指定すると、このルールは DSCP フィールドのビット列が 011 のパケットにだけ一致します。 • **critical**：プレシデンス 5（101） • **flashl**：プレシデンス 3（011） • **flash-override**：プレシデンス 4（100） • **immediate**：プレシデンス 2（010） • **internet**：プレシデンス 6（110） • **network**：プレシデンス 7（111） • **priority**：プレシデンス 1（001） • **routine**：プレシデンス 0（000）
fragments	（任意）非先頭フラグメントであるパケットにだけ一致するようルールを指定します。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定した同じルールに指定できません。これらのオプションを評価するためにスイッチが必要とする情報は、先頭フラグメントにだけ含まれているためです。
log	（任意）スイッチが、ルールに一致する各パケットに関する情報メッセージを生成するように指定します。メッセージに含まれる情報は、次のとおりです。 • ACL 名 • パケットが許可されたか拒否されたか • プロトコルが TCP、UDP、ICMP または数値であるか • 発信元アドレスと宛先アドレス、必要に応じて発信元および宛先ポート番号
time-range *time-range-name*	（任意）このルールに適用される時間の範囲を指定します。**time-range** コマンドを使用すると、時間の範囲を設定できます。
icmp-message	（任意、IGMP 専用）指定した ICMP メッセージ タイプのパケットにだけ一致するルールです。この引数には、0 から 255 までの整数か、「使用上のガイドライン」セクションの「ICMP メッセージ タイプ」に一覧されたキーワードのうちの 1 つを指定できます。
igmp-message	（任意、IGMP 専用）指定した IGMP メッセージ タイプのパケットにだけ一致するルールです。*igmp-message* 引数には、IGMP メッセージ番号を 0 ～ 15 の整数で指定できます。また、次のキーワードのいずれかを指定することもできます。 • **dvmrp**：ディスタンス ベクトル マルチキャスト ルーティング プロトコル（DVMRP） • **host-query**：ホスト クエリー • **host-report**：ホスト レポート • **pim**：Protocol Independent Multicast（PIM） • **trace**：マルチキャスト トレース

operator port [*port*]	（任意、TCP および UDP 専用）送信元ポートからのパケット、または *operator* および *port* 引数の条件を満たす宛先ポートに送られるパケットにだけ一致するルールです。これらの引数は、その後に *source* 引数を指定するか、または *destination* 引数を指定するかによって、送信元ポートまたは宛先ポートに適用されます。 *port* 引数は、名前、または TCP ポートか UDP ポートの番号です。有効な番号の範囲は、0 から 65535 の整数です。有効なポート名の一覧については、「使用上のガイドライン」セクションの「TCP ポート名」および「UDP ポート名」を参照してください。 2 番めの *port* 引数は、*operator* 引数が range のときにだけ必要です。 *operator* 引数は、次のキーワードのうち 1 つにする必要があります。 • **eq**：パケット内のポートが *port* 引数と等しい場合にだけ一致します。 • **gt**：パケット内のポートが *port* 引数より大きい場合にだけ一致します。 • **lt**：パケット内のポートが *port* 引数より小さい場合にだけ一致します。 • **neq**：パケット内のポートが *port* 引数と等しくない場合にだけ一致します。 • **range**：2 つの *port* 引数が必要で、パケット内のポートが最初の *port* 引数以上、2 番めの *port* 引数以下の場合にだけ一致します。
portgroup *portgroup*	（任意、TCP および UDP 専用）*portgroup* 引数によって指定された IP ポート グループ オブジェクトのメンバーである送信元ポートからのパケット、または同メンバーである宛先ポートへのパケットにだけ一致するよう指定します。その後、*source* 引数を指定するか、または *destination* 引数を指定するかによって、ポート グループ オブジェクトが送信元ポートまたは宛先ポートに適用されます。 **object-group ip port** コマンドを使用して、IP ポートグループ オブジェクトの作成と変更を行います。
flags	（任意、TCP 専用）特定の TCP コントロール ビット フラグ セットを持つパケットにだけ一致するルールです。*flags* 引数の値は、次の 1 つまたは複数のキーワードにする必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（任意、TCP 専用）確立された TCP 接続に属するパケットにだけルールが一致するよう指定します。スイッチは、ACK ビットまたは RST ビットが設定されている TCP パケットを、確立済みの接続に属しているものと見なします。

コマンドのデフォルト　新しく作成された IPv4 ACL にはルールは含まれません。

シーケンス番号を指定しない場合は、デバイスにより ACL の最後のルールのシーケンス番号に 10 を足したシーケンス番号がルールに割り当てられます。

コマンド モード　IPv4 ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン　スイッチが IPv4 ACL をパケットに適用する場合、ACL のすべてのルールについてパケットを評価します。スイッチは、パケットによって満たされた最初の条件を採用します。複数の条件が満たされる場合は、スイッチは最も小さいシーケンス番号のルールを採用します。

送信元と宛先

source 引数と *destination* 引数はいくつかの方法で指定できます。それぞれのルールで、これらの引数の 1 つを指定するのに使用するメソッドは、他の引数の指定方法には影響しません。ルールを設定する場合は、次のメソッドを使用して *source* 引数と *destination* 引数を指定します。

- IP アドレス グループ オブジェクト：IPv4 アドレス グループ オブジェクトを使用して、*source* 引数または *destination* 引数を指定できます。**object-group ip address** コマンドを使用して、IPv4 ポート グループの作成と変更を行います。構文は次のようになります。

  addrgroup *address-group-name*

  次に、lab-gateway-svrs という名前の IPv4 アドレス オブジェクト グループを使用して、*destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit ip any addrgroup lab-gateway-svrs
  ```

- アドレスおよびネットワーク ワイルドカード：IPv4 アドレスの後にネットワーク ワイルドカードを使用して、ホストまたはネットワークを送信元または宛先として指定できます。構文は次のようになります。

  IPv4-address network-wildcard

  次に、IPv4 アドレスとサブネット 192.168.67.0 のネットワーク ワイルドカードを持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび可変長サブネット マスク（VLSM）：IPv4 アドレスの後に VLSM を使用して、ホストまたはネットワークを送信元または宛先として指定できます。構文は次のようになります。

  IPv4-address/prefix-len

  次に、IPv4 アドレスとサブネット 192.168.67.0 の VLSM を持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit udp 192.168.67.0/24 any
  ```

- ホスト アドレス：**host** キーワードと IPv4 アドレスを使用して、送信元または宛先としてホストを指定できます。構文は次のようになります。

  host *IPv4-address*

  これは、*IPv4-address*/32、および *IPv4-address* 0.0.0.0 と等しい構文です。

  次に、**host** 192.168.67.132 の IPv4 アドレスを持つ *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit icmp host 192.168.67.132 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先が任意の IPv4 アドレスであることを指定します。**any** キーワードを使用する例については、このセクションの例を参照してください。それぞれの例で、**any** キーワードを使用して送信元または宛先を指定する方法が示されています。

ICMP メッセージ タイプ

icmp-message 引数には、ICMP メッセージ番号を 0 ～ 255 の整数で指定できます。また、次のキーワードのいずれかを指定することもできます。

- **administratively-prohibited**：管理上禁止
- **alternate-address**：代替アドレス
- **conversion-error**：データグラム変換
- **dod-host-prohibited**：禁止ホスト
- **dod-net-prohibited**：禁止ネット
- **echo**：エコー（ping）
- **echo-reply**：エコー応答
- **general-parameter-problem**：パラメータの問題
- **host-isolated**：分離ホスト
- **host-precedence-unreachable**：プレシデンスが到達不可能なホスト
- **host-redirect**：ホスト リダイレクト
- **host-tos-redirect**：ToS ホスト リダイレクト
- **host-tos-unreachable**：ToS が到達不可能なホスト
- **host-unknown**：不明ホスト
- **host-unreachable**：到達不可能なホスト
- **information-reply**：情報応答
- **information-request**：情報要求
- **mask-reply**：マスク応答
- **mask-request**：マスク要求
- **mobile-redirect**：モバイル ホスト リダイレクト
- **net-redirect**：ネットワーク リダイレクト
- **net-tos-redirect**：ToS ネット リダイレクト
- **net-tos-unreachable**：ToS が到達不可能なネットワーク
- **net-unreachable**：到達不可能なネット
- **network-unknown**：不明ネットワーク
- **no-room-for-option**：パラメータが必要であるが空きスペースがない
- **option-missing**：パラメータが必要であるが存在しない
- **packet-too-big**：フラグメント化と DF セットが必要
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：到達不可能なポート
- **precedence-unreachable**：プレシデンス カットオフ

- **protocol-unreachable**：到達不可能なプロトコル
- **reassembly-timeout**：再アセンブリ タイムアウト
- **redirect**：すべてのリダイレクト
- **router-advertisement**：ルータ ディスカバリ アドバタイズメント
- **router-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元クエンチ
- **source-route-failed**：送信元ルート失敗
- **time-exceeded**：すべての time-exceeded メッセージ
- **timestamp-reply**：タイムスタンプ応答
- **timestamp-request**：タイムスタンプ要求
- **traceroute**：Traceroute
- **ttl-exceeded**：TTL 超過
- **unreachable**：すべての到達不能

TCP ポート名

tcp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で TCP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

bgp：ボーダー ゲートウェイ プロトコル（179）

chargen：文字ジェネレータ（19）

cmd：リモート コマンド（rcmd、514）

daytime：Daytime（13）

discard：廃棄（9）

domain：ドメイン ネーム サービス（53）

drip：ダイナミック ルーティング情報プロトコル（3949）

echo：エコー（7）

exec：EXEC（rsh、512）

finger：フィンガー（79）

ftp：FTP（21）

ftp-data：FTP データ接続（2）

gopher：Gopher（7）

hostname：NIC ホスト名サーバ（11）

ident：Ident プロトコル（113）

irc：インターネット リレー チャット（194）

klogin：Kerberos ログイン（543）

kshell：Kerberos シェル（544）

login：ログイン（rlogin、513）

lpd：プリンタ サービス（515）

nntp：Network News Transport Protocol（119）

pim-auto-rp：PIM Auto-RP（496）

pop2：Post Office Protocol v2（19）

pop3：Post Office Protocol v3（11）

smtp：Simple Mail Transport Protocol（25）

sunrpc：Sun Remote Procedure Call（111）

tacacs：TAC Access Control System（49）

talk：Talk（517）

telnet：Telnet（23）

time：Time（37）

uucp：Unix-to-Unix Copy Program（54）

whois：WHOIS/NICNAME（43）

www：World Wide Web（HTTP、8）

UDP ポート名

udp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で UDP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

biff：Biff（メール通知、comsat、512）

bootpc：ブートストラップ プロトコル（BOOTP）クライアント（68）

bootps：ブートストラップ プロトコル（BOOTP）サーバ（67）

discard：廃棄（9）

dnsix：DNSIX セキュリティ プロトコル監査（195）

domain：ドメイン ネーム サービス（DNS、53）

echo：エコー（7）

isakmp：Internet Security Association および Key Management Protocol（5）

mobile-ip：モバイル IP 登録（434）

nameserver：IEN116 ネーム サービス（廃止、42）

netbios-dgm：NetBIOS データグラム サービス（138）

netbios-ns：NetBIOS ネーム サービス（137）

netbios-ss：NetBIOS セッション サービス（139）

non500-isakmp：Internet Security Association および Key Management Protocol（45）

ntp：ネットワーク タイム プロトコル（123）

pim-auto-rp：PIM Auto-RP（496）

rip：ルーティング情報プロトコル（ルータ、in.routed、52）

snmp：簡易ネットワーク管理プロトコル（161）

snmptrap：SNMP トラップ（162）

sunrpc：Sun Remote Procedure Call（111）

syslog：システム ロガー（514）

tacacs：TAC Access Control System（49）

talk：Talk（517）

tftp：Trivial File Transfer Protocol（69）

time：Time（37）

who：Who サービス（rwho、513）

xdmcp：X Display Manager Control Protocol（177）

例

次に、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP および UDP トラフィックを許可するルールを使用して、acl-lab-01 という名前で IPv4 ACL を設定する例を示します。

```
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

関連コマンド

コマンド	説明
deny（IPv4）	IPv4 ACL に拒否ルールを設定します。
ip access-list	IPv4 ACL を設定します。
remark	ACL にリマークを設定します。
show ip access-lists	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。

permit（IPv6）

条件に一致するトラフィックを許可する IPv6 ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

一般的な構文

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no permit *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*]
[**fragments**] [**log**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number* | **no**] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Protocol v6（IPv6）

[*sequence-number*] **permit ipv6** *source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol（SCTP）

[*sequence-number* | **no**] **permit sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Transmission Control Protocol（TCP; 伝送制御プロトコル）

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*]
[**established**]

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number* | **no**] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*]
destination [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*]

シンタックスの説明

sequence-number	（任意）デバイスにアクセス リストの番号ポジションへコマンドを挿入させる **permit** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、デバイスがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 ルールにシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。
protocol	ルールが一致するパケットのプロトコルの名前または番号です。有効な番号の範囲は、0 から 255 です。有効なプロトコル名は、次のキーワードです。 • **ahp**：Authentication Header Protocol（AHP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **esp**：Encapsulating Security Payload（ESP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **icmp**：ICMP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*icmp-message* 引数を使用できます。 • **ipv6**：すべての IPv6 トラフィックに適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **pcp**：Payload Compression Protocol（PCP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、このキーワード以外に使用できるのは、すべての IPv6 プロトコルに共通して適用されるキーワードと引数だけです。 • **sctp**：Stream Control Transmission Protocol（SCTP）トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*operator* 引数と **portgroup** キーワードを使用できます。 • **tcp**：TCP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*flags* 引数、*operator* 引数、**portgroup** キーワード、および **established** キーワードを使用できます。 • **udp**：UDP トラフィックにだけ適用されるルールを指定します。このキーワードを使用する場合、*protocol* 引数のすべての有効値で共通して使用できるキーワードに加えて、*operator* 引数と **portgroup** キーワードを使用できます。
source	ルールに一致する送信元 IPv6 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。

destination	ルールに一致する宛先 IPv6 アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
dscp *dscp*	（任意）指定した 6 ビットのディファレンシエーティッド サービス値を IPv6 ヘッダーの DSCP フィールドに持つパケットに対してだけ一致するように、ルールを指定します。*dscp* 引数には、次のキーワードを指定できます。 • 0 ～ 63：DSCP フィールドの 6 ビットに相当する 10 進数。たとえば、10 を指定すると、このルールは DSCP フィールドのビット列が 001010 のパケットにだけ一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低ドロップ確率（001010） • **af12**：AF クラス 1、中程度ドロップ確率（001100） • **af13**：AF クラス 1、高ドロップ確率（001110） • **af21**：AF クラス 2、低ドロップ確率（010010） • **af22**：AF クラス 2、中程度ドロップ確率（010100） • **af23**：AF クラス 2、高ドロップ確率（010110） • **af31**：AF クラス 3、低ドロップ確率（011010） • **af32**：AF クラス 3、中程度ドロップ確率（011100） • **af33**：AF クラス 3、高ドロップ確率（011110） • **af41**：AF クラス 4、低ドロップ確率（100010） • **af42**：AF クラス 4、中程度ドロップ確率（100100） • **af43**：AF クラス 4、高ドロップ確率（100110） • **cs1**：Class-Selector（CS）1、プレシデンス 1（001000） • **cs2**：CS2、プレシデンス 2（010000） • **cs3**：CS3、プレシデンス 3（011000） • **cs4**：CS4、プレシデンス 4（100000） • **cs5**：CS5、プレシデンス 5（101000） • **cs6**：CS6、プレシデンス 6（110000） • **cs7**：CS7、プレシデンス 7（111000） • **default**：デフォルト DSCP 値（000000） • **ef**：Expedited Forwarding（101110）
flow-label *flow-label-value*	（任意）*flow-label-value* 引数に指定した値を Flow Label ヘッダー フィールドに持つ IPv6 パケットにだけ一致するルールを指定します。 *flow-label-value* 引数には、0 ～ 1048575 の整数を指定できます。
fragments	（任意）非先頭フラグメント パケットにだけ一致するルールを指定します。デバイスは、フラグメント拡張ヘッダーにゼロ以外のフラグメント オフセットが含まれるパケットを、非先頭フラグメント パケットと見なします。TCP ポート番号などのレイヤ 4 オプションを指定するルールにはこのキーワードを指定できません。レイヤ 4 オプションを評価するには、先頭フラグメントにしか含まれない情報が必要になるからです。

log	（任意）デバイスが、ルールに一致する各パケットに関する情報メッセージを生成するように指定します。メッセージに含まれる情報は、次のとおりです。 • ACL 名 • パケットが許可されたか拒否されたか • プロトコルが TCP、UDP、ICMP または数値であるか • 発信元アドレスと宛先アドレス、必要に応じて発信元および宛先ポート番号
time-range *time-range-name*	（任意）このルールに適用される時間の範囲を指定します。**time-range** コマンドを使用すると、時間の範囲を設定できます。
icmp-message	（任意、ICMP 専用）ルールに一致する ICMPv6 メッセージ タイプ。この引数には、0 から 255 までの整数か、「使用上のガイドライン」セクションの「ICMPv6 メッセージ タイプ」に一覧されたキーワードのうちの 1 つを指定できます。
operator port [*port*]	（任意。TCP、UDP、および SCTP 専用）送信元ポートからのパケット、または *operator* および *port* 引数の条件を満たす宛先ポートに送られるパケットにだけ一致するルールです。これらの引数は、その後に *source* 引数を指定するか、または *destination* 引数を指定するかによって、送信元ポートまたは宛先ポートに適用されます。 *port* 引数は、名前、または TCP ポートか UDP ポートの番号です。有効な番号の範囲は、0 から 65535 の整数です。有効なポート名の一覧については、「使用上のガイドライン」セクションの「TCP ポート名」および「UDP ポート名」を参照してください。 2 番めの *port* 引数は、*operator* 引数が range のときにだけ必要です。 *operator* 引数は、次のキーワードのうち 1 つにする必要があります。 • **eq**：パケット内のポートが *port* 引数と等しい場合にだけ一致します。 • **gt**：パケット内のポートが *port* 引数より大きい場合にだけ一致します。 • **lt**：パケット内のポートが *port* 引数より小さい場合にだけ一致します。 • **neq**：パケット内のポートが *port* 引数と等しくない場合にだけ一致します。 • **range**：2 つの *port* 引数が必要で、パケット内のポートが最初の *port* 引数以上、2 番めの *port* 引数以下の場合にだけ一致します。
portgroup *portgroup*	（任意。TCP、UDP、および SCTP 専用）*portgroup* 引数によって指定された IP ポートグループ オブジェクトのメンバーである送信元ポートからのパケット、または同メンバーである宛先ポートへのパケットにだけ一致するよう指定します。その後、*source* 引数を指定するか、または *destination* 引数を指定するかによって、ポート グループ オブジェクトが送信元ポートまたは宛先ポートに適用されます。 **object-group ip port** コマンドを使用して、IP ポートグループ オブジェクトの作成と変更を行います。

established	（任意、TCP 専用）確立された TCP 接続に属するパケットにだけルールが一致するよう指定します。デバイスは、ACK ビットまたは RST ビットが設定されている TCP パケットを、確立済みの接続に属しているものと見なします。
flags	（任意、TCP 専用）特定の TCP コントロール ビット フラグ セットを持つパケットにだけ一致するルールです。*flags* 引数の値は、次の 1 つまたは複数のキーワードにする必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**

コマンドのデフォルト　なし

コマンド モード　IPv6 ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン　新しく作成された IPv6 ACL にはルールは含まれません。

デバイスが IPv6 ACL をパケットに適用する場合、ACL のすべてのルールについてパケットを評価します。デバイスは、パケットによって満たされた最初の条件を採用します。複数の条件が満たされる場合は、デバイスは最も小さいシーケンス番号のルールを採用します。

このコマンドにライセンスは必要ありません。

送信元と宛先

source 引数と *destination* 引数はいくつかの方法で指定できます。それぞれのルールで、これらの引数の 1 つを指定するのに使用するメソッドは、他の引数の指定方法には影響しません。ルールを設定する場合は、次のメソッドを使用して *source* 引数と *destination* 引数を指定します。

- IPv6 アドレス グループ オブジェクト：IPv6 アドレス グループ オブジェクトを使用して、*source* 引数または *destination* 引数を指定できます。**object-group ipv6 address** コマンドを使用して、IPv6 アドレス グループ オブジェクトの作成と変更を行います。構文は次のようになります。

  addrgroup *address-group-name*

  次に、lab-svrs-1301 という名前の IPv6 アドレス オブジェクト グループを使用して、*destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit ipv6 any addrgroup lab-svrs-1301
  ```

- アドレスおよび可変長サブネット マスク（VLSM）：IPv6 アドレスの後に VLSM を使用して、ホストまたはネットワークを送信元または宛先として指定できます。構文は次のようになります。

IPv6-address/prefix-len

次に、IPv6 アドレスとネットワーク 2001:0db8:85a3:: の VLSM を持つ *source* 引数を指定する例を示します。

```
switch(config-acl)# permit udp 2001:0db8:85a3::/48 any
```

- ホスト アドレス：**host** キーワードと IPv6 アドレスを使用して、送信元または宛先としてホストを指定できます。構文は次のようになります。

  host *IPv6-address*

  この構文は、*IPv6-address*/128 に相当します。

  次に、**host** キーワードと 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 アドレスで *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit icmp host 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 any
  ```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先が任意の IPv6 アドレスであることを指定します。**any** キーワードを使用する例については、このセクションの例を参照してください。それぞれの例で、**any** キーワードを使用して送信元または宛先を指定する方法が示されています。

ICMPv6 メッセージ タイプ

icmp-message 引数には、ICMPv6 メッセージ番号を 0 ～ 255 の整数で指定できます。また、次のキーワードのいずれかを指定することもできます。

- **beyond-scope**：スコープ外の宛先
- **destination-unreachable**：宛先アドレスが到達不能
- **echo-reply**：エコー応答
- **echo-request**：エコー要求（ping）
- **header**：パラメータ ヘッダーの問題
- **hop-limit**：配送中のホップ数の限界の超過
- **mld-query**：Multicast Listener Discovery クエリー
- **mld-reduction**：Multicast Listener Discovery リダクション
- **mld-report**：Multicast Listener Discovery レポート
- **nd-na**：ネイバー ディスカバリのネイバー アドバタイズメント
- **nd-ns**：ネイバー ディスカバリのネイバー要求
- **next-header**：パラメータ ネクスト ヘッダーの問題
- **no-admin**：管理上禁止された宛先
- **no-route**：宛先へのルートがない
- **packet-too-big**：パケット サイズ超過
- **parameter-option**：パラメータ オプションの問題
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：到達不可能なポート
- **reassembly-timeout**：再アセンブリ タイムアウト
- **redirect**：ネイバー リダイレクト
- **renum-command**：ルータの再番号付けコマンド

- **renum-result**：ルータの再番号付けの結果
- **renum-seq-number**：ルータの再番号付けのシーケンス番号リセット
- **router-advertisement**：ネイバー ディスカバリのルータ アドバタイズメント
- **router-renumbering**：すべてのルータの再番号付け
- **router-solicitation**：ネイバー ディスカバリのルータ要求
- **time-exceeded**：すべての時間超過メッセージ
- **unreachable**：すべて到達不能

TCP ポート名

tcp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で TCP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

bgp：ボーダー ゲートウェイ プロトコル（179）

chargen：文字ジェネレータ（19）

cmd：リモート コマンド（rcmd、514）

daytime：Daytime（13）

discard：廃棄（9）

domain：ドメイン ネーム サービス（53）

drip：ダイナミック ルーティング情報プロトコル（3949）

echo：エコー（7）

exec：EXEC（rsh、512）

finger：フィンガー（79）

ftp：FTP（21）

ftp-data：FTP データ接続（2）

gopher：Gopher（7）

hostname：NIC ホスト名サーバ（11）

ident：Ident プロトコル（113）

irc：インターネット リレー チャット（194）

klogin：Kerberos ログイン（543）

kshell：Kerberos シェル（544）

login：ログイン（rlogin、513）

lpd：プリンタ サービス（515）

nntp：Network News Transport Protocol（119）

pim-auto-rp：PIM Auto-RP（496）

pop2：Post Office Protocol v2（19）

pop3：Post Office Protocol v3（11）

smtp：Simple Mail Transport Protocol（25）

sunrpc：Sun Remote Procedure Call（111）

tacacs：TAC Access Control System（49）

talk：Talk（517）

telnet：Telnet（23）

time：Time（37）

uucp：Unix-to-Unix Copy Program（54）

whois：WHOIS/NICNAME（43）

www：World Wide Web（HTTP、8）

UDP ポート名

udp として *protocol* 引数を指定すると、*port* 引数には 0 ～ 65535 の整数で UDP ポート番号を指定できます。また、次のキーワードのいずれかを指定することもできます。

biff：Biff（メール通知、comsat、512）

bootpc：ブートストラップ プロトコル（BOOTP）クライアント（68）

bootps：ブートストラップ プロトコル（BOOTP）サーバ（67）

discard：廃棄（9）

dnsix：DNSIX セキュリティ プロトコル監査（195）

domain：ドメイン ネーム サービス（DNS、53）

echo：エコー（7）

isakmp：Internet Security Association および Key Management Protocol（5）

mobile-ip：モバイル IP 登録（434）

nameserver：IEN116 ネーム サービス（廃止、42）

netbios-dgm：NetBIOS データグラム サービス（138）

netbios-ns：NetBIOS ネーム サービス（137）

netbios-ss：NetBIOS セッション サービス（139）

non500-isakmp：Internet Security Association および Key Management Protocol（45）

ntp：ネットワーク タイム プロトコル（123）

pim-auto-rp：PIM Auto-RP（496）

rip：ルーティング情報プロトコル（ルータ、in.routed、52）

snmp：簡易ネットワーク管理プロトコル（161）

snmptrap：SNMP トラップ（162）

sunrpc：Sun Remote Procedure Call（111）

syslog：システム ロガー（514）

tacacs：TAC Access Control System（49）

talk：Talk（517）

tftp：Trivial File Transfer Protocol（69）

time：Time（37）

who：Who サービス（rwho、513）

xdmcp：X Display Manager Control Protocol（177）

例

次に、2001:0db8:85a3:: および 2001:0db8:69f2:: のネットワークから 2001:0db8:be03:2112:: ネットワークへ送信されるすべての TCP および UDP トラフィックを許可するルールで、acl-lab13-ipv6 という名前の IPv6 ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

次に、IPv6 アドレス オブジェクト グループ eng_ipv6 から IPv6 アドレス オブジェクト グループ marketing_group へ送信されるすべての IPv6 トラフィックを許可するルールで、ipv6-eng-to-marketing という名前の IPv6 ACL を設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

関連コマンド

コマンド	説明
deny（IPv6）	IPv6 ACL に拒否ルールを設定します。
ipv6 access-list	IPv6 ACL を設定します。
remark	ACL にリマークを設定します。

permit（MAC）

条件に一致するトラフィックを許可する MAC ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan vlan-id**]

no permit *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *vlan-id*]

no *sequence-number*

シンタックスの説明

sequence-number	（任意）スイッチにアクセス リストの番号ポジションへコマンドを挿入させる **permit** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、スイッチがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 ルールにシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。
source	ルールに一致する送信元 MAC アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
destination	ルールに一致する宛先 MAC アドレスです。この引数を指定するのに使用できるメソッドの詳細については、「使用上のガイドライン」セクションの「送信元と宛先」を参照してください。
protocol	（任意）ルールに一致するプロトコル番号です。有効なプロトコル番号の範囲は 0x0 から 0xffff です。有効なプロトコル名のリストについては、「使用上のガイドライン」セクションの「MAC プロトコル」を参照してください。
cos *cos-value*	（任意）IEEE 802.1Q ヘッダーに *cos-value* 引数で指定されたサービス クラス（CoS）値が含まれるパケットだけに一致するように、ルールを指定します。*cos-value* 引数は、0 から 7 までの整数となります。
vlan *vlan-id*	（任意）指定された VLAN ID が IEEE 802.1Q ヘッダーに含まれるパケットだけに一致するように、ルールを指定します。*vlan-id* 引数は、1 から 4094 までの整数となります。

コマンドのデフォルト

新しく作成された MAC ACL にはルールは含まれません。

シーケンス番号を指定しない場合は、スイッチにより ACL の最後のルールのシーケンス番号に 10 を足したシーケンス番号がルールに割り当てられます。

コマンド モード

MAC ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチが MAC ACL をパケットに適用する場合、ACL のすべてのルールについてパケットを評価します。スイッチは、パケットによって満たされた最初の条件を採用します。複数の条件が満たされる場合は、スイッチは最も小さいシーケンス番号のルールを採用します。

送信元と宛先

source 引数と *destination* 引数は 2 つの方法で指定できます。それぞれのルールで、これらの引数の 1 つを指定するのに使用するメソッドは、他の引数の指定方法には影響しません。ルールを設定する場合は、次のメソッドを使用して *source* 引数と *destination* 引数を指定します。

アドレスとマスク：MAC アドレスの後にマスクを使用して、1 つのアドレスまたはアドレスのグループを指定できます。構文は次のようになります。

```
MAC-address MAC-mask
```

次に、MAC アドレス 00c0.4f03.0a72 を持つ *source* 引数を指定する例を示します。

```
switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
```

次に、MAC ベンダー コードが 00603e のすべての MAC アドレスを持つ *destination* 引数を指定する例を示します。

```
switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
```

- 任意のアドレス：**any** キーワードを使用して、送信元または宛先が任意の MAC アドレスであることを指定できます。**any** キーワードを使用する例については、このセクションの例を参照してください。それぞれの例で、**any** キーワードを使用して送信元または宛先を指定する方法が示されています。

MAC プロトコル

protocol 引数は、MAC プロトコル番号またはキーワードを指定します。プロトコル番号は、先頭に 0x が付く 4 バイトの 16 進数です。有効なプロトコル番号の範囲は 0x0 から 0xffff です。有効なキーワードは、次のとおりです。

- **aarp**：Appletalk ARP（0x80f3）
- **appletalk**：Appletalk（0x809b）
- **decnet-iv**：DECnet Phase IV（0x6003）
- **diagnostic**：DEC Diagnostic Protocol（0x6005）
- **etype-6000**：Ethertype 0x6000（0x6000）
- **etype-8042**：Ethertype 0x8042（0x8042）
- **ip**：Internet Protocol v4（0x0800）
- **lat**：DEC LAT（0x6004）
- **lavc-sca**：DEC LAVC、SCA（0x6007）
- **mop-console**：DEC MOP リモート コンソール（0x6002）
- **mop-dump**：DEC MOP ダンプ（0x6001）
- **vines-echo**：VINES エコー（0x0baf）

例

次に、mac-ip-filter という名前で、2 つの MAC アドレスのグループ間ですべての非 IPv4 トラフィックを許可する MAC ACL を設定する例を示します。

```
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
ip
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に拒否ルールを設定します。
mac access-list	MAC ACL を設定します。
remark	ACL にリマークを設定します。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

permit interface

ユーザ ロールのインターフェイス ポリシー のインターフェイスを追加するには、**permit interface** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

permit interface *interface-list*

no permit interface

シンタックスの説明

interface-list	ユーザ ロールがアクセスを許可されているインターフェイスのリストです。

コマンドのデフォルト

すべてのインターフェイス

コマンド モード

インターフェイス ポリシー コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

permit interface 文を機能させるには、次の例にあるように、コマンド ルールを設定してインターフェイス アクセスを許可する必要があります。

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

例

次に、ユーザ ロール インターフェイス ポリシーのインターフェイスの範囲を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 8
```

次に、ユーザ ロール インターフェイス ポリシーのインターフェイスのリストを設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5
```

次に、ユーザ ロール インターフェイス ポリシーからインターフェイスを削除する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 1/2
```

関連コマンド

コマンド	説明
interface policy deny	ユーザ ロールのインターフェイス ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。

permit vlan

ユーザ ロール VLAN ポリシー に VLAN を追加するには、**permit vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

permit vlan *vlan-list*

no permit vlan

シンタックスの説明

vlan-list	ユーザ ロールがアクセスを許可されている VLAN のリストです。

コマンドのデフォルト

すべての VLAN

コマンド モード

VLAN ポリシー コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

permit vlan 文を機能させるには、次の例にあるように、コマンド **ルール**を設定して VLAN アクセスを許可する必要があります。

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

例

次に、ユーザ ロール VLAN ポリシーの VLAN の範囲を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

次に、ユーザ ロール VLAN ポリシーの VLAN のリストを設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

次に、ユーザ ロール VLAN ポリシーから VLAN を削除する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

関連コマンド

コマンド	説明
vlan policy deny	ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。

permit vrf

ユーザ ロール VRF ポリシーに Virtual Routing and Forwarding Instance（VRF; 仮想ルーティング/転送インスタンス）を追加するには、**permit vrf** コマンドを使用します。VRF を削除するには、このコマンドの **no** 形式を使用します。

permit vrf *vrf-list*

no permit vrf

シンタックスの説明

vrf-list	ユーザ ロールがアクセスを許可されている VRF のリストです。

コマンドのデフォルト

すべての VRF

コマンド モード

VRF ポリシー コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール VRF ポリシーの VRF 範囲を設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

関連コマンド

コマンド	説明
vrf policy deny	ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。

radius-server deadtime

Cisco Nexus 5000 シリーズ スイッチですべての RADIUS サーバのデッドタイム インターバルを設定するには、**radius-server deadtime** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

シンタックスの説明

minutes	デッドタイム インターバルの分数です。有効な範囲は 1 ～ 1440 分です。

コマンドのデフォルト

0 分

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

デッドタイム インターバルは、以前応答しなかった RADIUS サーバをスイッチがチェックする前の分数です。

（注） アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例

次に、すべての RADIUS サーバのグローバル デッドタイム インターバルを設定して、定期的なモニタリングを実行する例を示します。

```
switch(config)# radius-server deadtime 5
```

次に、すべての RADIUS サーバのグローバル デッドタイム インターバルをデフォルトに戻して、定期的なサーバ モニタリングをディセーブルにする例を示します。

```
switch(config)# no radius-server deadtime 5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server directed-request

ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにするには、**radius-server directed request** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server directed-request

no radius-server directed-request

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

設定された RADIUS サーバ グループに認証要求を送信します。

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ログイン中に *username@vrfname:hostname* を指定できます。*vrfname* は使用する VRF で *hostname* は設定された RADIUS サーバです。ユーザ名が認証用に RADIUS サーバに送信されます。

例

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにする例を示します。

```
switch(config)# radius-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できないようにする例を示します。

```
switch(config)# no radius-server directed-request
```

関連コマンド

コマンド	説明
show radius-server directed-request	転送された要求 RADIUS サーバ設定を表示します。

radius-server host

RADIUS サーバ パラメータを設定するには、**radius-server host** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

シンタックスの説明

hostname	RADIUS サーバ Domain Name Server（DNS）名です。最大 256 文字まで使用できます。
ipv4-address	*A*.*B*.*C*.*D* 形式の RADIUS サーバ IPv4 アドレスです。
ipv6-address	*X*:*X*:*X*:*X* 形式の RADIUS サーバ IPv6 アドレスです。
key	（任意）RADIUS サーバ事前共有秘密鍵を設定します。
0	（任意）RADIUS クライアントおよびサーバ間の通信を認証する、平文で指定された事前共有鍵を設定します。これはデフォルトです。
7	（任意）RADIUS クライアントおよびサーバ間の通信を認証する、暗号文で指定された事前共有鍵（7 で表示）を設定します。
shared-secret	RADIUS クライアントおよびサーバ間の通信を認証する事前共有鍵を設定します。最大長は 63 文字です。
pac	（任意）Cisco TrustSec と共に使用する RADIUS Cisco ACS サーバの保護されたアクセス資格情報の生成をイネーブルにします。
accounting	（任意）アカウンティングを設定します。
acct-port *port-number*	（任意）アカウンティング用の RADIUS サーバのポートを設定します。指定できる範囲は 0 ～ 65535 です。
auth-port *port-number*	（任意）認証用の RADIUS サーバのポートを設定します。指定できる範囲は 0 ～ 65535 です。
authentication	（任意）認証を設定します。
retransmit *count*	（任意）スイッチがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数を設定します。有効範囲は 1 ～ 5 回で、デフォルトは 1 回です。
test	（任意）RADIUS サーバにテスト パケットを送信するようパラメータを設定します。
idle-time *time*	サーバをモニタリングするための時間間隔を分で指定します。有効な範囲は 1 ～ 1440 分です。
password *password*	テスト パケット内のユーザ パスワードを指定します。最大文字サイズは 32 です。
username *name*	テスト パケット内のユーザ名を指定します。最大文字サイズは 32 です。
timeout *seconds*	RADIUS サーバへの再送信タイムアウト（秒単位）を設定します。デフォルトは 1 秒で、有効な範囲は 1 ～ 60 秒です。

コマンドのデフォルト

アカウンティング ポート：1813

認証ポート：1812

アカウンティング：イネーブル

認証：イネーブル

再送信回数：1

アイドル時間：0

サーバ モニタリング：ディセーブル

タイムアウト：5 秒

テスト ユーザ名：test

テスト パスワード：test

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

例

次に、RADIUS サーバ認証とアカウンティング パラメータを設定する例を示します。

```
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server key

RADIUS 共有秘密鍵を設定するには、**radius-server key** コマンドを使用します。共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

シンタックスの説明

0	（任意）RADIUS クライアントおよびサーバ間の通信を認証する、平文で指定された事前共有鍵を設定します。
7	（任意）RADIUS クライアントおよびサーバ間の通信を認証する、暗号文で指定された事前共有鍵を設定します。
shared-secret	RADIUS クライアントおよびサーバ間の通信を認証するのに使用する事前共有鍵を設定します。最大長は 63 文字です。

コマンドのデフォルト

平文認証

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

RADIUS 事前共有鍵を設定して、RADIUS サーバに対してスイッチを認証する必要があります。鍵の長さは 65 文字に制限されており、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。グローバル鍵は、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。**radius-server host** コマンドで **key** キーワードを使用することでこのグローバル鍵の割り当てを上書きできます。

例

次に、さまざまなシナリオを提供して RADIUS 認証を設定する例を示します。

```
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server retransmit

スイッチが RADIUS サーバで要求を試行する回数を指定するには、**radius-server retransmit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server retransmit *count*

no radius-server retransmit *count*

シンタックスの説明

count	スイッチがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数です。有効値は 1 ～ 5 回です。

コマンドのデフォルト

再送信 1 回

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、RADIUS サーバへの再送信回数を設定する例を示します。

```
switch(config)# radius-server retransmit 3
```

次に、RADIUS サーバへの再送信回数をデフォルトに戻す例を示します。

```
switch(config)# no radius-server retransmit 3
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server timeout

RADIUS サーバへの再送信間隔を指定するには、**radius-server timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout *seconds*

シンタックスの説明

seconds	RADIUS サーバに再送信する間隔の秒数です。有効な範囲は 1 ～ 60 秒です。

コマンドのデフォルト

1 秒

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、タイムアウト インターバルを設定する例を示します。

```
switch(config)# radius-server timeout 30
```

次に、時間間隔をデフォルトに戻す例を示します。

```
switch(config)# no radius-server timeout 30
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

remark

コメントを IPv4 または MAC アクセス コントロール リスト（ACL）に入力するには、**remark** コマンドを使用します。remark コマンドを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

シンタックスの説明

sequence-number	（任意）スイッチにアクセス リストの番号ポジションにコマンドを挿入させる **remark** コマンドのシーケンス番号です。シーケンス番号は、ACL 内のルールの順番を維持します。 シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。 デフォルトでは、ACL の最初のルールのシーケンス番号が 10 となります。 シーケンス番号を指定しない場合は、スイッチがルールを ACL の最後に追加して、その前のルールのシーケンス番号に 10 を足したシーケンス番号を割り当てます。 **resequence** コマンドを使用して、リマークとルールにシーケンス番号を再度割り当てます。
remark	リマークのテキストです。この引数は、最大 100 文字まで可能です。

コマンドのデフォルト

デフォルトでは、リマークは ACL に含まれません。

コマンド モード

IPv4 ACL コンフィギュレーション
MAC ACL コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

remark 引数は、最大 100 文字まで可能です。*remark* 引数に 101 文字以上を入力した場合、スイッチは最初の 100 文字を受け入れ、それ以外の文字はドロップします。

例

次に、IPv4 ACL でリマークを作成して結果を表示する例を示します。

```
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the lab
switch(config-acl)# show access-list acl-ipv4-01
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-list	すべての ACL または 1 つの ACL を表示します。

resequence

シーケンス番号をアクセス コントロール リスト（ACL）またはタイム レンジのすべてのルールに再割り当てするには、**resequence** コマンドを使用します。

resequence *access-list-type* **access-list** *access-list-name starting-number increment*

resequence time-range *time-range-name starting-number increment*

シンタックスの説明

access-list-type	ACL のタイプです。この引数の有効な値は、次のキーワードとなります。 • **arp** • **ip** • **mac**
access-list *access-list-name*	ACL 名を指定します。
time-range *time-range-name*	タイム レンジ名を指定します。
starting-number	ACL またはタイム レンジの最初のルールのシーケンス番号です。
increment	後続の各シーケンス番号にスイッチが加算する数です。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

resequence コマンドを使用すると、ACL のルールまたはタイム レンジにシーケンス番号を再割り当てすることができます。最初のルールの新しいシーケンス番号は、*starting-number* 引数によって決定されます。追加される各ルールは、*increment* 引数が決定する新しいシーケンス番号を受け取ります。最も大きいシーケンス番号が使用可能な最大シーケンス番号を超える場合は、シーケンシングが発生せず、次のメッセージが表示されます。

```
ERROR: Exceeded maximum sequence number.
```

最大シーケンス番号は 4294967295 です。

例

次に、開始シーケンス番号が 100 で番号が 10 ずつ増えていく ip-acl-01 という名前の IPv4 ACL のリシーケンスを行い、**show ip access-lists** コマンドを使用して、**resequence** コマンドの使用の前後でシーケンス番号を確認する例を示します。

```
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        7 permit tcp 128.0.0.0/16 any eq www
        10 permit udp 128.0.0.0/16 any
        13 permit icmp 128.0.0.0/16 any eq echo
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp 128.0.0.0/16 any eq www
        110 permit udp 128.0.0.0/16 any
        120 permit icmp 128.0.0.0/16 any eq echo
        130 deny igmp any any
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。

role feature-group name

ユーザ ロール機能グループを作成または指定して、ユーザ ロール機能グループ コンフィギュレーション モードを開始するには、**role feature-group name** コマンドを使用します。ユーザ ロール機能グループを削除するには、このコマンドの **no** 形式を使用します。

role feature-group name *group-name*

no role feature-group name *group-name*

シンタックスの説明

group-name	ユーザ ロール機能グループ名です。*group-name* は最大 32 文字までの英数字が可能で、大文字小文字が区別されます。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能グループを作成してユーザ ロール機能グループ コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

次に、ユーザ ロール機能グループを削除する例を示します。

```
switch(config)# no role feature-group name MyGroup
```

関連コマンド

コマンド	説明
feature-group name	ユーザ ロール機能グループを作成または指定して、ユーザ ロール機能グループ コンフィギュレーション モードを開始します。
show role feature-group	ユーザ ロール機能グループを表示します。

role name

ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始するには、**role name** コマンドを使用します。ユーザ ロールを削除するには、このコマンドの **no** 形式を使用します。

role name *role-name*

no role name *role-name*

シンタックスの説明

role name	ユーザ ロール名です。*role-name* は最大 16 文字までの英数字が可能で、大文字小文字が区別されます。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

Cisco Nexus 5000 シリーズ スイッチは、次のデフォルト ユーザ ロールを提供します。

- ネットワーク管理者：スイッチ全体への完全なリード/ライト アクセス
- スイッチ全体への完全なリード アクセス

デフォルトのユーザ ロールは、変更または削除できません。

例

次に、ユーザ ロールを作成してユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role MyRole
switch(config-role)#
```

次に、ユーザ ロールを削除する例を示します。

```
switch(config)# no role name MyRole
```

関連コマンド

コマンド	説明
show role	ユーザ ロールを表示します。

rule

ユーザ ロールのルールを設定するには、**rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

シンタックスの説明

number	ルールのシーケンス番号です。スイッチは、最も大きい値を持つルールを最初に適用し、次に降順で適用していきます。
deny	コマンドまたは機能へのアクセスを拒否します。
permit	コマンドまたは機能へのアクセスを許可します。
command *command-string*	コマンド ストリングを指定します。
read	リード アクセスを指定します。
read-write	リード/ライト アクセスを指定します。
feature *feature-name*	（任意）機能名を指定します。**show role feature** コマンドを使用して、スイッチの機能名を一覧します。
feature-group *group-name*	（任意）機能グループを指定します。

コマンドのデフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

ロールごとに最大 256 のルールを設定できます。

指定したルール番号は、ルールが適用される順番を決定します。ルールは降順で適用されます。たとえば、ロールに 3 つのルールがある場合、ルール 3、ルール 2、ルール 1 の順に適用されます。

例

次に、ユーザ ロールにルールを追加する例を示します。

```
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

次に、ユーザ ロールからルールを削除する例を示します。

```
switch(config)# role MyRole
switch(config-role)# no rule 10
```

関連コマンド

コマンド	説明
role name	ユーザ ロール名を作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールを表示します。

server

RADIUS または TACACS+ サーバ グループにサーバを追加するには、**server** コマンドを使用します。サーバ グループからサーバを削除するには、このコマンドの **no** 形式を使用します。

server {*ipv4-address* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

シンタックスの説明

ipv4-address	*A.B.C.D* 形式のサーバ IPv4 アドレスです。
ipv6-address	*X*:*X*:*X*::*X* 形式のサーバ IPv6 アドレスです。
hostname	サーバ名。最大 256 文字まで使用できます。

コマンドのデフォルト

なし

コマンド モード

RADIUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

サーバ グループに最大 64 のサーバを設定できます。

aaa group server radius コマンドを使用して RADIUS サーバ グループ コンフィギュレーション モードを開始するか、または **aaa group server tacacs+** コマンドを使用して TACACS+ サーバ グループ コンフィギュレーション モードを開始します。

サーバが見つからない場合は、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。

（注）　TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループにサーバを追加する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
```

次に、RADIUS サーバ グループからサーバを削除する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 10.10.1.1
```

次に、TACACS+ サーバ グループにサーバを追加する例を示します。

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

次に、TACACS+ サーバ グループからサーバを削除する例を示します。

```
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 10.10.2.2
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

show aaa accounting

AAA アカウンティング コンフィギュレーションを表示するには、**show aaa accounting** コマンドを使用します。

show aaa accounting

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例　次に、アカウンティング ログの設定を表示する例を示します。

```
switch# show aaa accounting
```

show aaa authentication

AAA 認証コンフィギュレーション情報を表示するには、**show aaa authentication** コマンドを使用します。

show aaa authentication login [**error-enable** | **mschap**]

シンタックスの説明

error-enable	（任意）認証ログイン エラー メッセージ イネーブル コンフィギュレーションを表示します。
mschap	（任意）認証ログイン MS-CHAP イネーブル コンフィギュレーションを表示します。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、設定されている認証パラメータを表示する例を示します。

```
switch# show aaa authentication
```

次に、認証ログイン エラー イネーブル コンフィギュレーションを表示する例を示します。

```
switch# show aaa authentication login error-enable
```

次に、認証ログイン MSCHAP コンフィギュレーションを表示する例を示します。

```
switch# show aaa authentication login mschap
```

show aaa groups

AAA サーバ グループ コンフィギュレーションを表示するには、**show aaa groups** コマンドを使用します。

show aaa groups

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例　次に、AAA グループ情報を表示する例を示します。

```
switch# show aaa groups
```

show access-lists

すべての IPv4 および MAC アクセス コントロール リスト（ACL）または特定の ACL を表示するには、**show access-lists** コマンドを使用します。

show access-lists [*access-list-name*]

シンタックスの説明

access-list-name	（任意）表示する ACL の名前です。

コマンドのデフォルト

access-list-name 引数を使用して ACL を指定しないかぎり、スイッチはすべての ACL を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチのすべての IPv4 および MAC ACL を表示する例を示します。

```
switch# show access-lists
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

show accounting log

アカウンティングのログ内容を表示するには、**show accounting log** コマンドを使用します。

show accounting log [*size*] [**start-time** *year month day HH*:*MM*:*SS*] [**end-time** *year month day HH*:*MM*:*SS*]

シンタックスの説明

size	（任意）表示するログのバイト単位のサイズです。有効な範囲は 0 ～ 250000 です。
start-time *year month day HH*:*MM*:*SS*	（任意）開始時刻を指定します。*year* 引数は *yyyy* 形式です。*month* は 3 文字の英語略称の月名です。有効な *day* 引数の範囲は 1 ～ 31 です。*HH*:*MM*:*SS* 引数は、標準的な 24 時間形式です。
end-time *year month day HH*:*MM*:*SS*	（任意）終了時刻を指定します。*year* 引数は *yyyy* 形式です。*month* は 3 文字の英語略称の月名です。有効な *day* 引数の範囲は 1 ～ 31 です。*HH*:*MM*:*SS* 引数は、標準的な 24 時間形式です。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、アカウンティング ログ全体を表示する例を示します。

```
switch# show accounting log
```

次に、400 バイトのアカウンティング ログを表示する例を示します。

```
switch# show accounting log 400
```

次に、2008 年 2 月 16 日 16:00:00 に開始するアカウンティング ログを表示する例を示します。

```
switch# show accounting log start-time 2008 Feb 16 16:00:00
```

次に、2008 年 2 月 1 日 15:59:59 に開始し、2008 年 2 月 29 日 16:00:00 に終了するアカウンティング ログを表示する例を示します。

```
switch# show accounting log start-time 2008 Feb 1 15:59:59 end-time 2008 Feb 29 16:00:00
```

関連コマンド

コマンド	説明
clear accounting log	アカウンティング ログを消去します。

show ip access-lists

すべての IPv4 ACL または特定の IPv4 ACL を表示するには、**show ip access-lists** コマンドを使用します。

show ip access-lists [*access-list-name*]

シンタックスの説明

access-list-name	（任意）表示する IPv4 ACL の名前です。

コマンドのデフォルト

access-list-name 引数を使用して ACL を指定しないかぎり、スイッチはすべての IPv4 ACL を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチのすべての IPv4 ACL を表示する例を示します。

```
switch# show ip access-lists
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

show ipv6 access-lists

すべての IPv6 ACL または特定の IPv6 ACL を表示するには、**show ipv6 access-lists** コマンドを使用します。

show ipv6 access-lists [*access-list-name*] [**expanded** | **summary**]

シンタックスの説明

access-list-name	（任意）IPv6 ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
expanded	（任意）オブジェクト グループの名前だけでなく、IPv6 アドレス グループやポート グループの内容も表示することを指定します。
summary	（任意）ACL 設定ではなく、ACL に関する情報を表示することを指定します。詳細については、「使用上のガイドライン」セクションを参照してください。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

access-list-name 引数を使用して ACL を指定しないかぎり、すべての IPv6 ACL が表示されます。

summary キーワードを使用すると、ACL 設定ではなく、ACL に関する情報を表示できます。表示される情報には、以下のものがあります。

- エントリ単位の統計情報が ACL に設定されているかどうか
- ACL 設定内のルールの数。この数は、デバイスにより ACL がインターフェイスに適用されるときのエントリの数を反映してはいません。ACL 内のルールでオブジェクト グループが使用されていると、適用時の ACL 内のエントリの数は、ルールの数よりも多くなる可能性があります。
- ACL が適用されるインターフェイス
- ACL がアクティブなインターフェイス

show ipv6 access-lists コマンドでは、次の条件の両方が満たされていると、ACL 内のエントリごとに統計情報が表示されます。

- ACL 設定に statistics per-entry コマンドが含まれている
- ACL が、管理上アップのインターフェイスに適用されている

例

次に、スイッチ上のすべての IPv6 ACL を表示する例を示します。

```
switch# show ipv6 access-lists
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 ACL を設定します。

show mac access-lists

すべてのメディア アクセス制御（MAC）ACL または特定の MAC ACL を表示するには、**show access-lists** コマンドを使用します。

show mac access-lists [*access-list-name*]

シンタックスの説明

access-list-name	（任意）表示する MAC ACL の名前です。

コマンドのデフォルト

access-list-name 引数を使用して ACL を指定しないかぎり、スイッチはすべての MAC ACL を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチのすべての MAC ACL を表示する例を示します。

```
switch# show mac access-lists
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。

show radius-server

RADIUS サーバ情報を表示するには、**show radius-server** コマンドを使用します。

show radius-server [*hostname* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** [*group-name*] | **sorted** | **statistics** *hostname* | *ipv4-address* | *ipv6-address*]

シンタックスの説明

hostname	（任意）RADIUS サーバの Domain Name Server（DNS）名です。最大文字サイズは 256 です。
ipv4-address	（任意）*A.B.C.D* 形式の RADIUS サーバ IPv4 アドレスです。
ipv6-address	（任意）*X:X::X:X* 形式の RADIUS サーバ IPv6 アドレスです。
directed-request	（任意）指定された要求設定を表示します。
groups [*group-name*]	（任意）設定されている RADIUS サーバ グループに関する情報を表示します。*group-name* を入力して、特定の RADIUS サーバ グループに関する情報を表示します。
sorted	（任意）RADIUS サーバ に関する情報を名前によるソート順に表示します。
statistics	（任意）RADIUS サーバの RADIUS 統計情報を表示します。ホスト名または IP アドレスが必要です。

コマンドのデフォルト

グローバル RADIUS サーバ設定を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

RADIUS 事前共有鍵は、**show radius-server** コマンド出力には表示されません。**show running-config radius** コマンドを使用して RADIUS 事前共有鍵を表示します。

例

次に、すべての RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server
```

次に、指定した RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server 10.10.1.1
```

RADIUS 要求設定を表示する例を示します。

```
switch# show radius-server directed-request
```

次に、RADIUS サーバ グループの情報を表示する例を示します。

```
switch# show radius-server groups
```

次に、指定した RADIUS サーバ グループの情報を表示する例を示します。

```
switch# show radius-server groups RadServer
```

次に、ソートされたすべての RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server sorted
```

次に、指定した RADIUS サーバの統計情報を表示する例を示します。

```
switch# show radius-server statistics 10.10.1.1
```

関連コマンド

コマンド	説明
show running-config radius	実行コンフィギュレーション ファイルの RADIUS 情報を表示します。

show role

ユーザ ロール コンフィギュレーションを表示するには、**show role** コマンドを使用します。

show role [**name** *role-name*]

シンタックスの説明

name *role-name*	（任意）特定のユーザ ロール名の情報を表示します。

コマンドのデフォルト

すべてのユーザ ロールの情報を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、特定のユーザ ロールの情報を表示する例を示します。

```
switch# show role name MyRole
```

次に、すべてのユーザ ロールの情報を表示する例を示します。

```
switch# show role
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを設定します。

show role feature

ユーザ ロール機能を表示するには、**show role feature** コマンドを使用します。

show role feature [**detail** | **name** *feature-name*]

シンタックスの説明

detail	（任意）すべての機能の詳細情報を表示します。
name *feature-name*	（任意）特定の機能の詳細情報を表示します。

コマンドのデフォルト

ユーザ ロール機能名のリストを表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能を表示する例を示します。

```
switch# show role feature
```

次に、すべてのユーザ ロール機能の詳細情報を表示する例を示します。

```
switch# show role feature detail
```

次に、特定のユーザ ロール機能の詳細情報を表示する例を示します。

```
switch# show role feature name boot-variable
```

関連コマンド

コマンド	説明
role feature-group	ユーザ ロールの機能グループを設定します。
rule	ユーザ ロールのルールを設定します。

show role feature-group

ユーザ ロール機能グループを表示するには、**show role feature-group** コマンドを使用します。

show role feature-group [**detail** | **name** *group-name*]

シンタックスの説明

detail	（任意）すべての機能グループの詳細情報を表示します。
name *group-name*	（任意）特定の機能グループの詳細情報を表示します。

コマンドのデフォルト

ユーザ ロール機能グループのリストを表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール機能グループを表示する例を示します。

```
switch# show role feature-group
```

次に、すべてのユーザ ロール機能グループに関する詳細情報を表示する例を示します。

```
switch# show role feature-group detail
```

次に、特定のユーザ ロール機能グループの情報を表示する例を示します。

```
switch# show role feature-group name SecGroup
```

関連コマンド

コマンド	説明
role feature-group	ユーザ ロールの機能グループを設定します。
rule	ユーザ ロールのルールを設定します。

show running-config aaa

実行コンフィギュレーションの認証、許可、アカウンティング（AAA）コンフィギュレーション情報を表示するには、**show running-config aaa** コマンドを使用します。

show running-config aaa [**all**]

シンタックスの説明

all	（任意）設定された情報とデフォルト情報を表示します。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、設定された実行コンフィギュレーションの AAA 情報を表示する例を示します。

```
switch# show running-config aaa
```

show running-config radius

実行コンフィギュレーションの RADIUS サーバ情報を表示するには、**show running-config radius** コマンドを表示します。

show running-config radius [**all**]

シンタックスの説明

all	（任意）デフォルトの RADIUS コンフィギュレーション情報を表示します。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、実行コンフィギュレーションの RADIUS 情報を表示する例を示します。

```
switch# show running-config radius
```

関連コマンド

コマンド	説明
show radius-server	RADIUS 情報を表示します。

show running-config security

実行コンフィギュレーションのユーザ アカウント、SSH サーバ、Telnet サーバ情報を表示するには、**show running-config security** コマンドを表示します。

show running-config security [**all**]

シンタックスの説明

all	（任意）デフォルトのユーザ アカウント、SSH サーバ、Telnet サーバ設定情報を表示します。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、実行コンフィギュレーションのユーザ アカウント、SSH サーバ、Telnet サーバを表示する例を示します。

```
switch# show running-config security
```

show ssh key

Secure Shell（SSH; セキュア シェル）サーバ鍵を表示するには、**show ssh key** コマンドを使用します。

show ssh key

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン　このコマンドは、**ssh server enable** コマンドを使用して SSH をイネーブルにしている場合にだけ使用できます。

例　次に、SSH サーバ鍵を表示する例を示します。

```
switch# show ssh key
```

関連コマンド

コマンド	説明
ssh server key	SSH サーバ鍵を設定します。

show ssh server

セキュア シェル（SSH）サーバ ステータスを表示するには、**show ssh server** コマンドを使用します。

show ssh server

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、SSH サーバ ステータスを表示する例を示します。

```
switch# show ssh server
```

関連コマンド

コマンド	説明
ssh server enable	SSH サーバをイネーブルにします。

show startup-config aaa

スタートアップ コンフィギュレーションの認証、許可、アカウンティング（AAA）コンフィギュレーション情報を表示するには、**show startup-config aaa** コマンドを使用します。

show startup-config aaa

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スタートアップ コンフィギュレーションの AAA 情報を表示する例を示します。

```
switch# show startup-config aaa
```

show startup-config radius

スタートアップ コンフィギュレーションの RADIUS コンフィギュレーション情報を表示するには、**show startup-config radius** コマンドを使用します。

show startup-config radius

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スタートアップ コンフィギュレーションの RADIUS 情報を表示する例を示します。

```
switch# show startup-config radius
```

show startup-config security

スタートアップ コンフィギュレーションのユーザ アカウント、SSH サーバ、Telnet サーバ設定情報を表示するには、**show startup-config security** コマンドを表示します。

show startup-config security

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スタートアップ コンフィギュレーションのユーザ アカウント、SSH サーバ、Telnet サーバを表示する例を示します。

```
switch# show startup-config security
```

show tacacs-server

TACACS+ サーバ情報を表示するには、**show tacacs-server** コマンドを表示します。

show tacacs-server [hostname | ip4-address | ip6-address] [directed-request | groups | sorted | statistics]

シンタックスの説明

hostname	（任意）TACACS+ サーバの Domain Name Server（DNS）名です。最大文字サイズは 256 です。
ipv4-address	（任意）*A.B.C.D* 形式の TACACS+ サーバ IPv4 アドレスです。
ipv6-address	（任意）*X:X:X::X* 形式の TACACS+ サーバ IPv6 アドレスです。
directed-request	（任意）指定された要求設定を表示します。
groups	（任意）設定されている TACACS+ サーバ グループに関する情報を表示します。
sorted	（任意）TACACS+ サーバに関する情報を名前によるソート順に表示します。
statistics	（任意）TACACS+ サーバの TACACS+ 統計情報を表示します。

デフォルト

グローバル TACACS+ サーバ設定を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ 事前共有鍵は、**show tacacs-server** コマンド出力には表示されません。**show running-config tacacs+** コマンドを使用して TACACS+ 事前共有鍵を表示します。

TACACS+ 情報を表示する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、すべての TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server
```

次に、指定した TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server 10.10.2.2
```

TACACS+ 要求設定を表示する例を示します。

```
switch# show tacacs-server directed-request
```

次に、TACACS+ サーバ グループの情報を表示する例を示します。

```
switch# show tacacs-server groups
```

次に、指定した TACACS+ サーバ グループの情報を表示する例を示します。

```
switch# show tacacs-server groups TacServer
```

次に、ソートされたすべての TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server sorted
```

次に、指定した TACACS+ サーバの統計情報を表示する例を示します。

```
switch# show tacacs-server statistics 10.10.2.2
```

関連コマンド

コマンド	説明
show running-config tacacs+	実行コンフィギュレーション ファイルの TACACS+ 情報を表示します。

show telnet server

Telnet サーバ ステータスを表示するには、**show telnet server** コマンドを使用します。

show telnet server

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、Telnet サーバ ステータスを表示する例を示します。

```
switch# show telnet server
```

関連コマンド

コマンド	説明
telnet server enable	Telnet サーバをイネーブルにします。

show user-account

スイッチのユーザ アカウントに関する情報を表示するには、**show user-account** コマンドを使用します。

show show user-account [*name*]

シンタックスの説明

name	（任意）指定したユーザ アカウントに関する情報だけを表示します。

コマンドのデフォルト

スイッチで定義されているすべてのユーザ アカウントに関する情報を表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

スイッチで定義されているすべてのユーザ アカウントに関する情報を表示する例を示します。

```
switch# show user-account
```

次に、特定のユーザ アカウントに関する情報を表示する例を示します。

```
switch# show user-account admin
```

show users

現在スイッチにログオンしているユーザを表示するには、**show users** コマンドを使用します。

show users

シンタックスの説明　このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト　なし

コマンド モード　EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

現在スイッチにログオンしているすべてのユーザを表示する例を示します。

```
switch# show users
```

関連コマンド

コマンド	説明
clear user	特定のユーザをログアウトします。
username	ユーザ アカウントを作成し、設定します。

show vlan access-list

特定の VLAN アクセス マップに関連付けられた IPv4 ACL または MAC ACL の内容を表示するには、**show vlan access-list** コマンドを使用します。

show vlan access-list *map-name*

シンタックスの説明

map-name	表示する VLAN アクセス リストです。

コマンドのデフォルト

なし

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

指定した VLAN アクセス マップについて、スイッチはアクセス マップ名とマップに関連付けられた ACL の内容を表示します。

例

次に、指定した VLAN アクセス マップに関連付けられた ACL の内容を表示する例を示します。

```
switch# show vlan access-list vlan1map
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を作成または設定します。
mac access-list	MAC ACL を作成または設定します。
show access-lists	VLAN アクセス マップの適用方法に関する情報を表示します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。
vlan access-map	VLAN アクセス マップを設定します。

show vlan access-map

すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示するには、**show vlan access-map** コマンドを使用します。

show vlan access-map [*map-name*]

シンタックスの説明

map-name	（任意）表示する VLAN アクセス マップです。

コマンドのデフォルト

map-name 引数を使用して特定のアクセス マップを選択しないかぎり、スイッチはすべての VLAN アクセス マップを表示します。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

表示される各 VLAN アクセス マップについて、スイッチはアクセス マップ名、**match** コマンドで指定された ACL、**action** コマンドで指定されたアクションを表示します。

show vlan filter コマンドを使用して、どの VLAN に VLAN アクセス マップが適用されるかを表示します。

例

次に、特定の VLAN アクセス マップを表示する例を示します。

```
switch# show vlan access-map vlan1map
```

次に、すべての VLAN アクセス マップを表示する例を示します。

```
switch# show vlan access-map
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップでトラフィックのフィルタリングを行うアクションを指定します。
match	VLAN アクセス マップでトラフィックのフィルタリングを行う ACL を指定します。
show vlan filter	VLAN アクセス マップの適用方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	VLAN アクセス マップを 1 つまたは複数の VLAN に適用します。

show vlan filter

VLAN アクセス マップ、コマンドの影響を受ける VLAN ID など、**vlan filter** コマンドのインスタンスに関する情報を表示するには、**show vlan filter** コマンドを使用します。

show vlan filter [**access-map** *map-name* | **vlan** *vlan-id*]

シンタックスの説明

access-map *map-name*	（任意）指定したアクセス マップが適用される VLAN への出力を制限します。
vlan *vlan-id*	（任意）指定した VLAN に適用されるアクセス マップだけに出力を制限します。

コマンドのデフォルト

access-map キーワードを使用してアクセス マップを指定するか、**vlan** キーワードを使用して VLAN ID を指定しないかぎり、VLAN に適用される VLAN アクセス マップのすべてのインスタンスが表示されます。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、スイッチのすべての VLAN アクセス マップ情報を表示する例を示します。

```
switch# show vlan filter
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップでトラフィックのフィルタリングを行うアクションを指定します。
match	VLAN アクセス マップでトラフィックのフィルタリングを行う ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	VLAN アクセス マップを 1 つまたは複数の VLAN に適用します。

ssh

IPv4 を使用してセキュア シェル（SSH）セッションを作成するには、**ssh** コマンドを使用します。

ssh [*username*@]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

シンタックスの説明

username	（任意）SSH セッションのユーザ名です。
ipv4-address	リモート ホストの IPv4 アドレスです。
hostname	リモート ホストのホスト名です。
vrf *vrf-name*	（任意）SSH セッションで使用する VRF 名を指定します。

コマンドのデフォルト

デフォルトの VRF です。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

IPv4 を使用して SSH セッションを開始する例を示します。

```
switch# ssh 10.10.1.1 vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh server enable	SSH サーバをイネーブルにします。
ssh6	IPv6 アドレッシングを使用して SSH セッションを開始します。

ssh6

IPv6 を使用してセキュア シェル（SSH）セッションを作成するには、**ssh6** コマンドを使用します。

ssh6 [*username*@]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*]

シンタックスの説明

username	（任意）SSH セッションのユーザ名です。
ipv6-address	リモート ホストの IPv6 アドレスです。
hostname	リモート ホストのホスト名です。
vrf *vrf-name*	（任意）SSH セッションで使用する VRF 名を指定します。

コマンドのデフォルト

デフォルトの VRF です。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

IPv6 を使用して SSH セッションを開始する例を示します。

```
switch# ssh 2001:0DB8::200C:417A vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh	IPv4 アドレッシングを使用して SSH セッションを開始します。
ssh server enable	SSH サーバをイネーブルにします。

ssh key

セキュア シェル（SSH）サーバ鍵を作成するには、**ssh key** コマンドを使用します。SSH サーバ鍵を削除するには、このコマンドの **no** 形式を使用します。

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

シンタックスの説明

dsa	Digital System Algorithm（DSA）SSH サーバ鍵を指定します。
force	（任意）以前のイベントが存在する場合に、DSA SSH 鍵イベントを強制的に生成します。
rsa	Rivest, Shamir, Adelman（RSA）公開鍵暗号 SSH サーバ鍵を指定します。
length	（任意）SSH サーバ鍵を作成するときに使用するビット数です。有効な範囲は 768 ～ 2048 です。

コマンドのデフォルト

1024 ビット長

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS ソフトウェアは SSH バージョン 2 をサポートしています。

SSH サーバ鍵を削除または交換する場合は、**no ssh server enable** コマンドを使用して最初に SSH サーバ鍵をディセーブルにする必要があります。

例

次に、デフォルトのキー長を使用して RSA サーバ鍵を作成する例を示します。

```
switch(config)# ssh key rsa
```

次に、指定したキー長を使用して RSA サーバ鍵を作成する例を示します。

```
switch(config)# ssh key rsa 768
```

次に、強制オプションを使用して RSA サーバ鍵を交換する例を示します。

```
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
switch(config)# ssh server enable
```

次に、DSA SSH サーバ鍵を削除する例を示します。

```
switch(config)# no ssh server enable
switch(config)# no ssh key dsa
switch(config)# ssh server enable
```

次に、すべての SSH サーバ鍵を削除する例を示します。

```
switch(config)# no ssh server enable
switch(config)# no ssh key
switch(config)# ssh server enable
```

関連コマンド

コマンド	説明
show ssh key	SSH サーバ鍵の情報を表示します。
ssh server enable	SSH サーバをイネーブルにします。

ssh server enable

セキュア シェル（SSH）サーバをイネーブルにするには、**ssh server enable** コマンドを使用します。SSH サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh server enable

no ssh server enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

イネーブル

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは SSH バージョン 2 をサポートしています。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch(config)# ssh server enable
```

次に、SSH サーバをディセーブルにする例を示します。

```
switch(config)# no ssh server enable
```

関連コマンド

コマンド	説明
show ssh server	SSH サーバ鍵の情報を表示します。

storm-control level

トラフィック ストーム コントロールの抑制レベルを設定するには、**storm-control level** コマンドを使用します。抑制モードをオフにするかデフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage*[**.***fraction*]

no storm-control {broadcast | multicast | unicast} level

シンタックスの説明

broadcast	ブロードキャスト トラフィックを指定します。
multicast	マルチキャスト トラフィックを指定します。
unicast	ユニキャスト トラフィックを指定します。
level *percentage*	抑制レベルのパーセンテージです。有効値は 0 ～ 100 パーセントです。
fraction	（任意）抑制レベルのフラクションです。有効な範囲は 0 ～ 99 です。

コマンドのデフォルト

すべてのパケットが渡されます。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

storm-control level コマンドを入力して、インターフェイスの抑制レベルをイネーブルにして、トラフィック ストーム コントロール レベルを設定し、インターフェイスでイネーブルにされているすべてのトラフィック ストーム コントロール モードにトラフィック ストーム コントロール レベルを適用します。

フラクショナル抑制レベルを入力する場合には、ピリオド（.）が必要です。

抑制レベルは、総帯域幅のパーセンテージです。100 パーセントのしきい値は、トラフィックに制限がないことを意味します。0 または 0.0（フラクショナル）パーセントのしきい値は、指定したトラフィックがポートでブロックされることを意味します。

show interfaces counters storm-control コマンドを使用して、廃棄カウントを表示します。

次のメソッドの 1 つを使用して、指定したトラフィック タイプの抑制をオフにします。

- 指定したトラフィック タイプのレベルを 100 パーセントに設定します。
- このコマンドの **no** 形式を使用します。

例

次に、ブロードキャスト トラフィックの抑制をイネーブルにして、抑制しきい値レベルを設定する例を示します。

```
switch(config-if)# storm-control broadcast level 30
```

マルチキャスト トラフィックの抑制モードをディセーブルにする例を示します。

```
switch(config-if)# no storm-control multicast level
```

関連コマンド

コマンド	説明
show interface	インターフェイスのストーム コントロール抑制カウンタを表示します。
show running-config	インターフェイスの設定を表示します。

tacacs-server deadtime

応答性について到達不能（非応答）TACACS+ サーバを監視する定期的な時間間隔を設定するには、**tacacs-server deadtime** コマンドを使用します。非応答 TACACS+ サーバのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

シンタックスの説明

time	時間間隔を分で指定します。指定できる範囲は 1 ～ 1440 です。

コマンドのデフォルト

0 分

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

時間間隔の設定をゼロにすると、タイマーがディセーブルになります。個別の TACACS+ サーバのデッド時間間隔がゼロ（0）よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。

デッド時間間隔が 0 分の場合、TACACS+ サーバがサーバ グループの一部でグループのデッド時間間隔が 0 分を超えていないかぎり、TACACS+ サーバ モニタリングは実行されません。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、デッド タイムの時間間隔を設定し、定期的なモニタリングをイネーブルにする例を示します。

```
switch(config)# tacacs-server deadtime 10
```

次に、デッド タイムの時間間隔をデフォルトに戻し、定期的なモニタリングをディセーブルにする例を示します。

```
switch(config)# no tacacs-server deadtime 10
```

関連コマンド

コマンド	説明
deadtime	非応答 RADIUS サーバ グループまたは TACACS+ サーバ グループをモニタリングする時間間隔を設定します。
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server directed-request

ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できるようにするには、**tacacs-server directed request** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server directed-request

no tacacs-server directed-request

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

設定された TACACS+ サーバ グループに認証要求を送信します。

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

ログイン中に *username@vrfname:hostname* を指定できます。*vrfname* は使用する VRF、*hostname* は設定された TACACS+ サーバです。ユーザ名が認証用にサーバに送信されます。

例

次に、ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できるようにする例を示します。

```
switch(config)# tacacs-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できないようにする例を示します。

```
switch(config)# no tacacs-server directed-request
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server directed request	指定要求 TACACS+ サーバ コンフィギュレーションを表示します。

tacacs-server host

TACACS+ サーバ ホスト パラメータを設定するには、**tacacs-server host** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **7**] *shared-secret*] [**port** *port-number*] [**test** {**idle-time** *time* | **password** *password* | **username** *name*}] [**timeout** *seconds*]

シンタックスの説明

hostname	TACACS+ サーバの Domain Name Server（DNS）名です。最大文字サイズは 256 です。
ipv4-address	*A.B.C.D* 形式の TACACS+ サーバ IPv4 アドレスです。
ipv6-address	*X:X:X::X* 形式の TACACS+ サーバ IPv6 アドレスです。
key	（任意）TACACS+ サーバ用の共有秘密鍵を設定します。
0	（任意）TACACS+ クライアントとサーバ間の通信を認証する、平文で指定された事前共有鍵（0 で表示）を設定します。これはデフォルトです。
7	（任意）TACACS+ クライアントおよびサーバ間の通信を認証する、暗号文で指定された事前共有鍵（7 で表示）を設定します。
shared-secret	TACACS+ クライアントとサーバ間の通信を認証する事前共有鍵を設定します。最大長は 63 文字です。
port *port-number*	（任意）認証用の TACACS+ サーバのポートを設定します。指定できる範囲は 1 ～ 65535 です。
test	（任意）TACACS+ サーバにテスト パケットを送信するようパラメータを設定します。
idle-time *time*	（任意）サーバをモニタリングするための時間間隔を分で指定します。時間の範囲は 1 ～ 1440 分です。
password *password*	（任意）テスト パケット内のユーザ パスワードを指定します。最大文字サイズは 32 です。
username *name*	（任意）テスト パケット内のユーザ名を指定します。最大文字サイズは 32 です。
timeout *seconds*	（任意）TACACS+ サーバ タイムアウト期間（秒単位）を設定します（TACACS+ サーバへの再送信を行う時間間隔）。有効な範囲は 1 ～ 60 秒です。

コマンドのデフォルト

アイドル時間：ディセーブル

サーバ モニタリング：ディセーブル

タイムアウト：1 秒

テスト ユーザ名：test

テスト パスワード：test

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

例

次に、TACACS+ サーバ ホスト パラメータを設定する例を示します。

```
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server key

グローバル TACACS+ 共有秘密鍵を設定するには、**tacacs-server key** コマンドを使用します。共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

シンタックスの説明

0	（任意）TACACS+ クライアントおよびサーバ間の通信を認証する、平文で指定された事前共有鍵を設定します。これはデフォルトです。
7	（任意）TACACS+ クライアントおよびサーバ間の通信を認証する、暗号文で指定された事前共有鍵を設定します。
shared-secret	TACACS+ クライアントとサーバ間の通信を認証する事前共有鍵です。最大長は 63 文字です。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有鍵を設定する必要があります。鍵の長さは 65 文字に制限されており、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。グローバル鍵を設定して、スイッチにあるすべての TACACS+ サーバ コンフィギュレーションで使用するようにできます。**tacacs-server host** コマンドで **key** キーワードを使用することでこのグローバル鍵の割り当てを上書きできます。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、TACACS+ サーバ共有鍵を設定する例を示します。

```
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

tacacs-server timeout

TACACS+ サーバへの再送信間隔を指定するには、**tacacs-server timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

シンタックスの説明

seconds	TACACS+ サーバへの再送信間隔の秒です。有効範囲は 1 ～ 60 秒です。

コマンドのデフォルト

1 秒

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、TACACS+ サーバ タイムアウト値を設定する例を示します。

```
switch(config)# tacacs-server timeout 3
```

次に、TACACS+ サーバ タイムアウト値をデフォルトに戻す例を示します。

```
switch(config)# no tacacs-server timeout 3
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show tacacs-server	TACACS+ サーバ情報を表示します。

telnet

Cisco Nexus 5000 シリーズ スイッチで IPv4 を使用して Telnet セッションを作成するには、**telnet** コマンドを使用します。

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

シンタックスの説明

ipv4-address	リモート スイッチの IPv4 アドレスです。
hostname	リモート スイッチのホスト名です。
port-number	（任意）Telnet セッションのポート番号です。指定できる範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）Telnet セッションで使用する VRF 名を指定します。

コマンドのデフォルト

ポート 23 がデフォルト ポートです。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

IPv6 アドレッシングで Telnet セッションを作成するには、**telnet6** コマンドを使用します。

例

IPv4 を使用して Telnet セッションを開始する例を示します。

```
switch# telnet 10.10.1.1 vrf management
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet server enable	Telnet サーバをイネーブルにします。
telnet6	IPv6 アドレッシングを使用して Telnet セッションを作成します。

telnet server enable

Telnet サーバをイネーブルにするには、**telnet server enable** コマンドを使用します。Telnet サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

telnet server enable

no telnet server enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

イネーブル

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、Telnet サーバをイネーブルにする例を示します。

```
switch(config)# telnet server enable
```

次に、Telnet サーバをディセーブルにする例を示します。

```
switch(config)# no telnet server enable
```

関連コマンド

コマンド	説明
show telnet server	Telnet サーバ ステータスを表示します。

telnet6

NX-OS デバイス上で IPv6 を使用して Telnet セッションを作成するには、**telnet6** コマンドを使用します。

telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

シンタックスの説明

ipv6-address	リモート デバイスの IPv6 アドレスです。
hostname	リモート デバイスのホスト名です。この名前は 64 文字以下の英数字で、大文字と小文字が区別されます。
port-number	（任意）Telnet セッションのポート番号です。有効範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）Telnet セッションで使用する Virtual Routing and Forwarding（VRF; 仮想ルーティングおよびフォワーディング）名を指定します。大文字と小文字が区別されます。

コマンドのデフォルト

ポート 23 がデフォルト ポートです。デフォルトの VRF が使用されます。

コマンド モード

EXEC モード

コマンドの履歴

リリース	変更内容
4.0(1a)N1(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、**telnet server enable** コマンドを使用して Telnet サーバをイネーブルにしておく必要があります。

IPv4 アドレッシングで Telnet セッションを作成するには、**telnet** コマンドを使用します。

例

IPv6 アドレスを使用して Telnet セッションを開始する例を示します。

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet	IPv4 アドレッシングを使用して Telnet セッションを作成します。
telnet server enable	Telnet サーバをイネーブルにします。

use-vrf

RADIUS サーバ グループまたは TACACS+ サーバ グループの仮想ルーティングおよびフォワーディング（VRF）インスタンスを指定するには、**use-vrf** コマンドを使用します。VRF インスタンスを削除するには、このコマンドの **no** 形式を使用します。

use-vrf *vrf-name*

no use-vrf *vrf-name*

シンタックスの説明

vrf-name	VRF インスタンス名を指定します。

コマンドのデフォルト

なし

コマンド モード

RADIUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

1 つのサーバ グループには、1 つの VRF インスタンスしか設定できません。

aaa group server radius コマンドを使用して RADIUS サーバ グループ コンフィギュレーション モードを開始するか、または **aaa group server tacacs+** コマンドを使用して TACACS+ サーバ グループ コンフィギュレーション モードを開始します。

サーバが見つからない場合は、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

例

次に、RADIUS サーバ グループの VRF インスタンスを指定する例を示します。

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf management
```

次に、TACACS+ サーバ グループの VRF インスタンスを指定する例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf management
```

次に、TACACS+ サーバ グループから VRF インスタンスを削除する例を示します。

```
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf management
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature tacacs+	TACACS+ をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ情報を表示します。
show tacacs-server groups	TACACS+ サーバ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。
vrf	VRF インスタンスを設定します。

username

ユーザ アカウントを作成し、設定するには、**username** コマンドを使用します。ユーザ アカウントを削除するには、このコマンドの **no** 形式を使用します。

username *user-id* [**expire** *date*] [**password** *password*] [**role** *role-name*]

username *user-id* **sshkey** {*key* | **filename** *filename*}

no username *user-id*

シンタックスの説明

user-id	ユーザ アカウントのユーザ ID です。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。
expire *date*	（任意）ユーザ アカウントの有効期限を指定します。*date* 引数の形式は、YYYY-MM-DD です。
password *password*	（任意）アカウントのパスワードを指定します。デフォルトは password です。
role *role-name*	（任意）ユーザに割り当てられるロールを指定します。
sshkey	（任意）ユーザ アカウントの SSH 鍵を指定します。
key	SSH 鍵ストリングです。
filename *filename*	SSH 鍵ストリングを含むファイル名を指定します。

コマンドのデフォルト

有効期限、パスワード、SSH 鍵はありません。

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは強力なパスワードしか受け入れません。強力なパスワードの特性には次のものがあります。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

注意　ユーザ アカウントのパスワードを指定していない場合、ユーザはアカウントにログインできません。

例

次に、パスワードを使用してユーザ アカウントを作成する例を示します。

```
switch(config)# username user1 password Ci5co321
```

次に、ユーザ アカウントの SSH 鍵を設定する例を示します。

```
switch(config)# username user1 sshkey file bootflash:key_file
```

関連コマンド

コマンド	説明
show user-account	ユーザ アカウントの設定を表示します。

vlan access-map

新しい VLAN アクセス マップを作成するか、または既存の VLAN アクセス マップを設定するには、**vlan access-map** コマンドを使用します。VLAN アクセス マップを削除するには、このコマンドの **no** 形式を使用します。

vlan access-map *map-name*

no vlan access-map *map-name*

シンタックスの説明

map-name	作成または変更する VLAN アクセス マップの名前です。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

各 VLAN アクセス マップには、1 つの **match** コマンドと 1 つの **action** コマンドを含めることができます。

例

次に、vlan-map-01 という名前で VLAN アクセス マップを作成して、そのマップに ip-acl-01 という名前の IPv4 ACL を割り当て、スイッチが ACL に一致するパケットを転送するよう指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップでトラフィックのフィルタリングを行うアクションを指定します。
match	VLAN アクセス マップでトラフィックのフィルタリングを行う ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法に関する情報を表示します。
vlan filter	VLAN アクセス マップを 1 つまたは複数の VLAN に適用します。

vlan filter

VLAN アクセス マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** コマンドを使用します。VLAN アクセス マップの適用を解除するには、このコマンドの **no** 形式を使用します。

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* [**vlan-list** *VLAN-list*]

シンタックスの説明

map-name	作成または変更する VLAN アクセス マップの名前です。
vlan-list *VLAN-list*	VLAN アクセス マップでトラフィックをフィルタリングする VLAN の ID を 1 つ以上指定します。 ハイフン（-）を使用して、VLAN ID 範囲の開始 ID と終了 ID を区切ります。たとえば、70 ～ 100 を使用します。 カンマ（,）を使用して、個別の VLAN ID と VLAN ID の範囲を区切ります。たとえば、20, 70 ～ 100, 142 を使用します。 **（注）** このコマンドの **no** 形式を使用する場合、*VLAN-list* 引数は任意となります。この引数を省略すると、スイッチはアクセス マップが適用されているすべての VLAN からアクセス マップを削除します。

コマンドのデフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

VLAN アクセス マップを 1 つまたは複数の VLAN に適用できます。

1 つの VLAN には、1 つの VLAN アクセス マップしか適用できません。

このコマンドの **no** 形式を使用すると、アクセス マップの適用時に指定した VLAN リストのすべてまたは一部に対して、VLAN アクセス マップの適用を解除できます。アクセス マップが適用されているすべての VLAN から適用を解除するには、*VLAN-list* 引数を省略します。現在アクセス マップが適用されている VLAN のサブセットに対して、アクセス マップの適用を解除するには、*VLAN-list* 引数を使用してアクセス マップを削除する VLAN を指定します。

例

次に、vlan-map-01 という名前の VLAN アクセス マップを 20 ～ 45 の VLAN に適用する例を示します。

```
switch(config)# vlan filter vlan-map-01 20-45
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップでトラフィックのフィルタリングを行うアクションを指定します。
match	VLAN アクセス マップでトラフィックのフィルタリングを行う ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。

vlan policy deny

ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始するには、**vlan policy deny** コマンドを使用します。ユーザ ロールの VLAN ポリシーをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

vlan policy deny

no vlan policy deny

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

すべての VLAN

コマンド モード

ユーザ ロール コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

次に、ユーザ ロールの VLAN ポリシーをデフォルトに戻す例を示します。

```
switch# configure terminal
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。

vrf policy deny

ユーザ ロールの仮想転送およびルーティング インスタンス（VRF）ポリシー コンフィギュレーション モードを開始するには、**vrf policy deny** コマンドを使用します。ユーザ ロールの VRF ポリシーをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

vrf policy deny

no vrf policy deny

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

コマンドのデフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション

コマンドの履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

次に、ユーザ ロールの VRF ポリシーをデフォルトに戻す例を示します。

```
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。