



## D コマンド

この章では、D で始まる Cisco Nexus 1000V コマンドについて説明します。

### deadtime

到達不可能な RADIUS または TACACS+ サーバをスキップする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* 分単位の間隔です。0 ~ 1440 の値を指定できます。

#### 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 (**config-radius**)  
TACACS+ サーバグループ コンフィギュレーション (**config-tacacs+**)  
グローバル コンフィギュレーション (**config**)

#### サポートされるユーザの役割

network-admin

#### コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

設定する前に、**tacacs+ enable** コマンドを使用して TACACS+ をイネーブルにする必要があります。デッドタイムは、グローバルに設定してすべての RADIUS または TACACS+ サーバに適用することも、サーバグループごとに適用することもできます。

RADIUS または TACACS+ サーバ グループに対するデッドタイムの間隔がゼロ (0) より大きい場合は、その値がグローバルなデッドタイム値より優先されます。

デッドタイムの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。

デッドタイムの間隔が 0 分の場合、RADIUS および TACACS+ サーバは応答しなくても「応答なし」と指定されません。

## 例

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

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

次に、すべての TACACS+ サーバおよびサーバ グループのグローバルなデッドタイムの間隔を 5 分に設定する例を示します。

```
switch# config t
switch(config)# tacacs-server deadtime 5
switch(config)#
```

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

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

次に、デッドタイムの間隔をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# feature tacacs+
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
<b>aaa group server</b>	AAA サーバ グループを設定します。
<b>radius-server host</b>	RADIUS サーバを設定します。
<b>show radius-server groups</b>	RADIUS サーバ グループ情報を表示します。
<b>show tacacs-server groups</b>	TACACS+ サーバ グループ情報を表示します。
<b>tacacs+ enable</b>	TACACS+ をイネーブルにします。
<b>tacacs-server host</b>	TACACS+ サーバを設定します。

# debug logfile

指定のファイルに **debug** コマンドの結果を出力するには、**debug logfile** 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。

**debug logfile filename [size bytes]**

**no debug logfile filename [size bytes]**

シンタックスの説明	filename	debug コマンドの出力ファイルの名前を指定します。ファイル名は 64 文字以下の英数字で、大文字と小文字が区別されます。
	size bytes	(任意) ログ ファイルのサイズをバイト単位で指定します。指定できる範囲は 4096 ~ 4194304 です。

**デフォルト**  
 デフォルトのファイル名 : syslogd\_debugs  
 デフォルトのファイル サイズ : 4194304 バイト

**コマンド モード** 任意

**サポートされるユーザの役割** network-admin

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(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**  
 ログ ファイルは、log: ファイル システム ルート ディレクトリに作成されます。  
 ログ ファイルを表示するには、**dir log:** コマンドを使用します。

**例**  
 次に、デバッグ ログ ファイルを指定する例を示します。

```
switch# debug logfile debug_log
```

次に、デフォルトのデバッグ ログ ファイルに戻す例を示します。

```
switch# no debug logfile debug_log
```

関連コマンド	コマンド	説明
	<b>dir</b>	ディレクトリの内容を表示します。
	<b>show debug</b>	デバッグの設定を表示します。
	<b>show debug logfile</b>	デバッグ ログ ファイルの内容を表示します。

# debug logging

**debug** コマンド出力のロギングをイネーブルにするには、**debug logging** コマンドを使用します。デバッグのロギ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。

**debug logging**

**no debug logging**

**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。

**デフォルト** ディセーブル

**コマンドモード** 任意

**サポートされるユーザの役割** network-admin

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(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

**例** 次に、**debug** コマンドの出力のロギングをイネーブルにする例を示します。

```
switch# debug logging
```

次に、**debug** コマンドの出力のロギングをディセーブルにする例を示します。

```
switch# no debug logging
```

関連コマンド	コマンド	説明
	debug logfile	debug コマンド出力のログ ファイルを設定します。

# default switchport (port profile)

ポート プロファイルから特定のスイッチポート特性を削除するには、**default switchport** コマンドを使用します。

**default switchport {mode | access vlan | trunk {native | allowed} vlan | private-vlan {host-association | mapping [trunk]} | port-security}**

## シンタックスの説明

<b>mode</b>	ポート プロファイルからポート モードの特性を削除します。ポート モードはグローバルなデフォルトまたはインターフェイスのデフォルト（アクセスモード）に戻ります。これは、 <b>no switchport mode port-profile</b> コマンドを実行する場合と同等の効果があります。
<b>access vlan</b>	アクセス VLAN の設定を削除します。
<b>trunk allowedvlan</b>	トランキング許可 VLAN の特性を削除します。
<b>trunk native vlan</b>	トランキング ネイティブ VLAN の特性を削除します。
<b>private-vlan host-association</b>	PVLAN のホスト アソシエーションを削除します。
<b>private-vlan mapping</b>	PVLAN のマッピングを削除します。
<b>port-security</b>	ポート セキュリティの特性を削除します。

## デフォルト

なし

## コマンド モード

ポート プロファイル コンフィギュレーション (**config-port-prof**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

このコマンドの機能は、特定の **switchport** コマンドの **no** 形式を使用する場合と同等の効果があります。たとえば、次のコマンドの効果は同じです。

- **default switchport mode** コマンド = **no switchport mode** コマンド
- **default switchport access vlan** コマンド = **no switchport access vlan** コマンド
- **default switchport trunk native vlan** コマンド = **no switchport trunk native vlan** コマンド

## 例

次に、ポート プロファイル ポートをスイッチ アクセス ポートに戻す例を示します。

```
n1000v(config-port-prof)# default switchport mode
```

## ■ default switchport (port profile)

次に、ポート プロファイルのトランキング許可 VLAN の特性を削除する例を示します。

```
n1000v(config-port-prof)# default switchport trunk allowed vlan
```

次に、ポート プロファイルのプライベート VLAN ホスト アソシエーションを削除する例を示します。

```
n1000v(config-port-prof)# default switchport private-vlan host-association
```

次に、ポート プロファイルのポート セキュリティの特性を削除する例を示します。

```
n1000v(config-port-prof)# default switchport port-security
```

## 関連コマンド

コマンド	説明
<b>show port-profile</b>	ポート プロファイルに関する情報を表示します。

# default shutdown (port profile)

ポートプロファイルから管理ステータスの特性 (config 属性) を削除するには、**default shutdown** コマンドを使用します。このコマンドは、このポートプロファイルを継承するインターフェイスの管理ステータスを、グローバルまたはインターフェイスのデフォルト (通常、デフォルトの管理ステータスはシャットダウン) に設定します。

## default shutdown

**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。

**デフォルト** なし

**コマンドモード** ポートプロファイルコンフィギュレーション (**config-port-prof**)

**サポートされるユーザの役割** network-admin

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(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

**例** 次に、特定のポートプロファイルのポートをシャットダウン状態に変更する方法を示します。

```
n1000v# config t
n1000v# port-profile DataProfile
n1000v(config-port-prof)# default shutdown
n1000v(config-port-prof)# show port-profile name DataProfile
port-profile DataProfile
description:
status: enabled
capability uplink: no
capability l3control: no
system vlans: none
port-group: DataProfile
max-ports: 32
inherit:
config attributes:
  switchport mode access
evaluated config attributes:
  switchport mode access
assigned interfaces:
  Vethernet1switch(config-port-prof)#
```

■ default shutdown (port profile)

## 関連コマンド

コマンド	説明
<b>show port-profile</b>	ポート プロファイルの設定を表示します。

# default shutdown (interface)

インターフェイス レベルでの管理ステータスの上書きを削除するには、**default shutdown** コマンドを使用します。このコマンドでは、以前に入力された管理ステータスのすべての設定が削除されます。これにより、ポート プロファイルの設定が有効になります。

## default shutdown

**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。

**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 (**config-if**)

**サポートされるユーザの役割** network-admin

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(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

**例** 次に、ポートをシャットダウン状態に変更する例を示します。

```
n1000v# config t
n1000v(config)# interface ethernet 3/2
n1000v(config-if)# default shutdown
n1000v(config-if)#
```

関連コマンド	コマンド	説明
	<b>show running-config interface</b>	インターフェイスの設定を表示します。

# default switchport port-security (VEthernet)

スイッチポート ポート セキュリティ 特性のユーザ設定を VEthernet インターフェイスから削除するには、**default switchport port-security** コマンドを使用します。このコマンドを使用すると、そのインターフェイスのポート セキュリティがデフォルト（ディセーブル）に設定されます。

## default switchport port-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。

**デフォルト** ディセーブル

**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 (**config-if**)

**サポートされるユーザの役割** network-admin

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(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

**例** 次に、VEthernet 2 でポート セキュリティをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface veth 2
switch(config-if)# default switchport port-security
switch(config-if)#
```

関連コマンド	コマンド	説明
	<b>show running-config port-security</b>	ポート セキュリティの設定を表示します。
	<b>show port-security</b>	ポート セキュリティのステータスを表示します。

# delay

イーサネット インターフェイスにスループット遅延値情報を割り当てるには、**delay** コマンドを使用します。遅延値を削除するには、このコマンドの **no** 形式を使用します。

**delay value**

**no delay [value]**

## シンタックスの説明

*delay\_val* スループット遅延時間を 10 マイクロ秒単位で指定します。  
指定できる値は、1 ~ 16777215 です。

## 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 (**config-if**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

この値を設定しても、実際のイーサネット インターフェイスのスループット遅延時間は変化しません。この設定は情報設定のみを目的としています。

## 例

次に、スロット 3 のポート 1 にあるイーサネット インターフェイスに遅延時間を割り当てる例を示します。

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# delay 10000
switch(config-if)#
```

次に、遅延時間の設定を削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 3/1
switch(config-if)# no delay 10000
switch(config-if)#
```

## 関連コマンド

コマンド	説明
<b>show interface</b>	インターフェイスの設定情報を表示します。

# delete

ファイルを削除するには、**delete** コマンドを使用します。

**delete** [*filesystem:[//directory/] | directory/*]*filename*

シンタックスの説明	パラメータ	説明
<i>filesystem:</i>	(任意) ファイル システムの名前を指定します。有効な値は <b>bootflash</b> または <b>volatile</b> です。	
<i>//directory/</i>	(任意) ディレクトリの名前を指定します。ディレクトリ名では、大文字と小文字が区別されます。	
<i>filename</i>	ファイルの名前を指定します。大文字と小文字が区別されます。	

**デフォルト** なし

**コマンド モード** 任意

**サポートされるユーザの役割** network-admin

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(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** 削除するファイルを見つけるには、**dir** コマンドを使用します。

**例** 次に、ファイルを削除する例を示します

```
switch# delete bootflash:old_config.cfg
```

関連コマンド	コマンド	説明
	<b>dir</b>	ディレクトリの内容を表示します。

# 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]
```

```
no deny protocol source destination [dscp dscp | precedence precedence]
```

```
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]
```

## Internet Group Management Protocol (IGMP; 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]
```

## Internet Protocol v4 (IPv4)

```
[sequence-number] deny ip source destination [dscp dscp | precedence precedence]
```

## 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] destination [operator port [port]  
[dscp dscp | precedence precedence]
```

## シンタックスの説明

<i>sequence-number</i>	<p>(任意) <b>deny</b> コマンドのシーケンス番号です。指定すると、コマンドはアクセスリスト内の指定された番号の位置に挿入されます。シーケンス番号は、ACL 内のルールの順番を維持します。</p> <p>シーケンス番号の有効範囲は、1 から 4294967295 までの整数です。</p> <p>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。</p> <p>シーケンス番号を指定しない場合は、ルールは ACL の最後に追加され、直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が割り当てられます。</p> <p>ルールにシーケンス番号を再度割り当てるには、<b>resequence</b> コマンドを使用します。</p>
<i>protocol</i>	<p>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。有効な番号は、0 ~ 255 です。有効なプロトコル名として指定できるのは、次のキーワードです。</p> <ul style="list-style-type: none"> <li>• <b>icmp</b> : このルールが ICMP トラフィックだけに適用されることを指定します。このキーワードを使用する場合は、<i>protocol</i> 引数のすべての有効な値に対するキーワードに加えて、<i>icmp-message</i> 引数も使用できます。</li> <li>• <b>igmp</b> : このルールが IGMP トラフィックだけに適用されることを指定します。このキーワードを使用する場合は、<i>protocol</i> 引数のすべての有効な値に対するキーワードに加えて、<i>igmp-type</i> 引数も使用できます。</li> <li>• <b>ip</b> : このルールがすべての IPv4 トラフィックに適用されることを指定します。このキーワードを使用する場合は、他に使用できるキーワードと引数はすべての IPv4 プロトコルに適用されるものだけとなります。使用できるキーワードには次のものがあります。 <ul style="list-style-type: none"> <li>– <b>dscp</b></li> <li>– <b>precedence</b></li> </ul> </li> <li>• <b>tcp</b> : このルールが TCP トラフィックだけに適用されることを指定します。このキーワードを使用する場合は、<i>protocol</i> 引数のすべての有効な値に対するキーワードに加えて、<i>flags</i> および <i>operator</i> 引数も使用できます。</li> <li>• <b>udp</b> : このルールが UDP トラフィックだけに適用されることを指定します。このキーワードを使用する場合は、<i>protocol</i> 引数のすべての有効な値に対するキーワードに加えて、<i>operator</i> 引数も使用できます。</li> </ul>
<i>source</i>	<p>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方法の詳細については、「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。</p>
<i>destination</i>	<p>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方法の詳細については、「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。</p>

**dscp dscp**

(任意) 指定した 6 ビットの Diffserv 値が IP ヘッダーの DSCP フィールドに存在するパケットだけがこのルールに一致することを指定します。dscp 引数には、次の数値またはキーワードを指定できます。

- **0 ~ 63** : DSCP フィールドの 6 ビットと等価な 10 進数値です。たとえば、10 を指定すると、ルールに一致するのは DSCP フィールドのビットが 001010 であるパケットだけとなります。
- **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** : クラスセレクタ (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 (EF) (101110)

<b>precedence</b> <i>precedence</i>	<p>(任意) <i>precedence</i> 引数によって指定された値が IP プレシデンス フィールドに存在するパケットだけがこのルールに一致することを指定します。 <i>precedence</i> 引数には、次の数値またはキーワードを指定できます。</p> <ul style="list-style-type: none"> <li>• 0 ~ 7 : IP プレシデンス フィールドの 3 ビットと等価な 10 進数値です。たとえば、3 を指定すると、ルールに一致するのは DSCP フィールドのビットが 011 であるパケットだけとなります。</li> <li>• <b>critical</b> : プレシデンス 5 (101)</li> <li>• <b>flash</b> : プレシデンス 3 (011)</li> <li>• <b>flash-override</b> : プレシデンス 4 (100)</li> <li>• <b>immediate</b> : プレシデンス 2 (010)</li> <li>• <b>internet</b> : プレシデンス 6 (110)</li> <li>• <b>network</b> : プレシデンス 7 (111)</li> <li>• <b>priority</b> : プレシデンス 1 (001)</li> <li>• <b>routine</b> : プレシデンス 0 (000)</li> </ul>
<i>icmp-message</i>	<p>(ICMP のみ : 任意) ルールに一致する ICMP メッセージ タイプです。この引数には、0 ~ 255 の整数または「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」に記載されているキーワードの 1 つを指定できます。</p>
<i>igmp-message</i>	<p>(IGMP のみ : 任意) ルールに一致する IGMP メッセージ タイプです。 <i>igmp-message</i> 引数には、IGMP メッセージ番号 (0 ~ 15 の整数) を指定できます。次のキーワードの 1 つを指定することもできます。</p> <ul style="list-style-type: none"> <li>• <b>dvmp</b> : Distance Vector Multicast Routing Protocol (DVMP)</li> <li>• <b>host-query</b> : ホスト クエリ</li> <li>• <b>host-report</b> : ホスト レポート</li> <li>• <b>pim</b> : Protocol Independent Multicast (PIM)</li> <li>• <b>trace</b> : マルチキャスト トレース</li> </ul>

<i>operator port</i> [ <i>port</i> ]	<p>(任意：TCP および UDP のみ) ルールに一致するのは、<i>operator</i> 引数および <i>port</i> 引数の条件を満たす送信元ポートからのパケット、またはこれらの引数の条件を満たす宛先ポートへのパケットだけとなります。これらの引数が送信元ポートと宛先ポートのどちらに適用されるかは、<i>source</i> 引数と <i>destination</i> 引数のどちらの後に指定されたかによって決まります。</p> <p><i>port</i> 引数には、TCP ポートまたは UDP ポートの名前または番号を指定できません。有効な番号は、0 ~ 65535 の整数です。有効なポート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「TCP ポート名」および「UDP ポート名」を参照してください。</p> <p>2 番目の <i>port</i> 引数は、<i>operator</i> 引数が範囲となっている場合にだけ必要となります。</p> <p><i>operator</i> 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。</p> <ul style="list-style-type: none"> <li>• <b>eq</b> : パケットのポートが <i>port</i> 引数と等しい場合にだけ一致します。</li> <li>• <b>gt</b> : パケットのポートが <i>port</i> 引数より大きい場合にだけ一致します。</li> <li>• <b>lt</b> : ポートが <i>port</i> 引数より小さい場合にだけ一致します。</li> <li>• <b>neq</b> : パケットのポートが <i>port</i> 引数と等しくない場合にだけ一致します。</li> <li>• <b>range</b> : 2 つの <i>port</i> 引数が必要で、パケットのポートが最初の <i>port</i> 引数以上、2 番目の <i>port</i> 引数以下の場合にだけ一致します。</li> </ul>
<i>flags</i>	<p>(TCP のみ：任意) ルールに一致する TCP コントロール ビット フラグです。<i>operator</i> 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。</p> <ul style="list-style-type: none"> <li>• <b>ack</b></li> <li>• <b>fin</b></li> <li>• <b>psh</b></li> <li>• <b>rst</b></li> <li>• <b>syn</b></li> <li>• <b>urg</b></li> </ul>

**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 (**config-acl**)

**サポートされるユーザの役割**

network-admin

**コマンドの履歴**

リリース	変更内容
4.0(4)SV1(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**

デバイスは、IPv4 ACL をパケットに適用するときに、その ACL のすべてのルールについてパケットを評価します。ルールの条件をパケットが満たしていれば、そのルールが採用されます。複数のルールの条件を満たしている場合は、シーケンス番号が最も小さいルールが採用されます。

**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方法は、他の引数の指定方法には影響しません。ルールを設定するときは、次の方法を使用して *source* 引数と *destination* 引数を指定します。

- 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 を表すネットワーク ワイルドカードを使用して *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 を表す VLSM を使用して *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、ホスト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。

```
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* キーワードと 192.168.67.132 という IPv4 アドレスを使用して **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** キーワードを使用すると、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。

**ICMP メッセージタイプ**

*icmp-message* 引数には ICMP メッセージ番号 (0 ~ 255 の整数) を指定できます。次のキーワードの 1 つ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** : 禁止されていない

- **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-reply** : 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

*protocol* 引数に **tcp** を指定した場合は、*port* 引数に TCP ポート番号 (0 ~ 65535 の整数) を指定できます。次のキーワードの 1 つ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 サーバ (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**

*protocol* 引数に **udp** を指定した場合は、*port* 引数に UDP ポート番号 (0 ~ 65535 の整数) を指定できます。次のキーワードの 1 つ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) クライアント (68)
- bootps** : Bootstrap Protocol (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 サーバ (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** : Network Time Protocol (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.route、52)
- snmp** : Simple Network Management Protocol (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)
- ftp** : 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、**acl-lab-01** という名前で IPv4 ACL を設定する例を示します。この ACL のルールでは、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し、最後のルールでその他の IPv4 トラフィックを許可します。

```
switch# config t
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
<b>ip access-list</b>	IPv4 ACL を設定します。
<b>permit (IPv4)</b>	IPv4 ACL に許可ルールを設定します。
<b>remark</b>	IPv4 ACL にリマークを設定します。
<b>show ip access-list</b>	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。
<b>statistics per-entry</b>	ACL 内の各エントリに対する統計情報の収集をイネーブルにします。

# deny (MAC)

条件に一致するトラフィックを拒否する MAC 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

<i>sequence-number</i>	(任意) <b>deny</b> コマンドのシーケンス番号です。指定すると、コマンドはアクセスリスト内の指定された番号の位置に挿入されます。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、ルールは ACL の最後に追加され、直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が割り当てられます。  ルールにシーケンス番号を再度割り当てるには、 <b>resequence</b> コマンドを使用します。
<i>source</i>	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方法の詳細については、「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。
<i>destination</i>	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方法の詳細については、「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。
<i>protocol</i>	(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。
<i>cos cos-value</i>	(任意) <i>cos-value</i> 引数で指定された Class of Service (CoS; サービス クラス) 値が IEEE 802.1Q ヘッダーに含まれるパケットだけがこのルールに一致することを指定します。 <i>cos-value</i> 引数に指定できるのは、0 ~ 7 の整数です。
<i>vlan VLAN-ID</i>	(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がこのルールに一致することを指定します。 <i>VLAN-ID</i> 引数に指定できるのは、1 ~ 4094 の整数です。

## 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、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

MAC ACL コンフィギュレーション (**config-mac-acl**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

デバイスは、MAC ACL をパケットに適用するときに、その ACL のすべてのルールについてパケットを評価します。ルールの条件をパケットが満たしていれば、そのルールが採用されます。複数のルールの条件を満たしている場合は、シーケンス番号が最も小さいルールが採用されます。

## 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方法は、他の引数の指定方法には影響しません。ルールを設定するときは、次の方法を使用して *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 を使用して *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 であるすべてのホストの MAC アドレスを使用して *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** キーワードを使用すると、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。有効なキーワードには、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` という名前の MAC ACL を設定する例を示します。この ACL のルールでは、2 つの MAC アドレス グループ間のすべての非 IPv4 トラフィックを許可します。

```
switch# config t
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
<code>mac access-list</code>	MAC ACL を設定します。
<code>permit (MAC)</code>	MAC ACL に許可ルールを設定します。
<code>remark</code>	ACL にリマークを設定します。
<code>show mac access-list</code>	すべての MAC ACL または 1 つの MAC ACL を表示します。
<code>statistics per-entry</code>	ACL 内の各エントリに対する統計情報の収集をイネーブルにします。

# description (interface)

インターフェイスの説明を追加して、実行コンフィギュレーションに保存するには、**description** コマンドを使用します。インターフェイスの説明を削除するには、このコマンドの **no** 形式を使用します。

**description** *text*

**no description**

<b>シンタックスの説明</b>	<i>text</i>	インターフェイスについての説明です。最大文字数は 80 文字です。
------------------	-------------	-----------------------------------

<b>デフォルト</b>	なし
--------------	----

<b>コマンド モード</b>	インターフェイス コンフィギュレーション (config-if)
-----------------	----------------------------------

<b>サポートされるユーザの役割</b>	network-admin
----------------------	---------------

コマンドの履歴	リリース	変更内容
	4.0(4)SV1(1)	このコマンドが追加されました。

<b>使用上のガイドライン</b>	.
-------------------	---

<b>例</b>	次に、インターフェイスの説明を追加して実行コンフィギュレーションに保存する例を示します。 <pre>switch(config-if)# description Ethernet port 3 on module 1</pre> 次に、インターフェイスの説明を削除する例を示します。 <pre>switch(config-if)# no description Ethernet port 3 on module 1</pre>
----------	--

関連コマンド	コマンド	説明
	<b>interface vethernet</b>	仮想イーサネット インターフェイスを作成します。
	<b>interface port-channel</b>	ポート チャネル インターフェイスを作成します。
	<b>interface ethernet</b>	イーサネット インターフェイスを作成します。
	<b>interface mgmt</b>	管理インターフェイスを設定します。
	<b>show interface</b>	インターフェイスの説明を含むステータスを表示します。

# description (NetFlow)

フロー レコード、フロー モニタ、またはフロー エクスポートに説明を追加するには、**description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

**description** *line*

**no description**

## シンタックスの説明

*line* 63 文字以下の説明です。

## デフォルト

なし

## コマンド モード

NetFlow フロー レコード (config-flow-record)

NetFlow フロー エクスポート (config-flow-exporter)

Netflow フロー モニタ (config-flow-monitor)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

### 例

次に、フロー レコードに説明を追加する例を示します。

```
n1000v(config)# flow record RecordTest
n1000v(config-flow-record)# description Ipv4flow
```

次に、フロー エクスポートに説明を追加する例を示します。

```
n1000v# config t
n1000v(config)# flow exporter ExportTest
n1000v(config-flow-exporter)# description ExportHamilton
```

次に、フロー モニタに説明を追加する例を示します。

```
n1000v# config t
n1000v(config)# flow monitor MonitorTest
n1000v(config-flow-monitor)# description Ipv4Monitor
```

## 関連コマンド

コマンド	説明
<b>flow exporter</b>	Flexible NetFlow フロー エクスポートを作成します。
<b>flow record</b>	Flexible NetFlow フロー レコードを作成します。
<b>flow monitor</b>	Flexible NetFlow フロー モニタを作成します。
<b>show flow exporter</b>	NetFlow フロー エクスポートに関する情報を表示します。
<b>show flow record</b>	NetFlow フロー レコードに関する情報を表示します。
<b>show flow monitor</b>	NetFlow フロー モニタに関する情報を表示します。

# description (QoS)

QoS クラス マップおよびポリシー マップに説明を追加するには、**description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

**description** *text*

**no description** *text*

<b>シンタックスの説明</b>	<i>text</i> クラス マップまたはポリシー マップに関する 200 文字以下の説明です。
------------------	---

<b>デフォルト</b>	なし
--------------	----

<b>コマンド モード</b>	QoS クラス マップ コンフィギュレーション ( <b>config-cmap-qos</b> ) QoS ポリシー マップ コンフィギュレーション ( <b>config-pmap-qos</b> )
-----------------	---

<b>サポートされるユーザの役割</b>	network-admin
----------------------	---------------

<b>コマンドの履歴</b>	リリース	変更内容
	4.0(4)SV1(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

<b>例</b>	次に、ポリシー マップに説明を追加する例を示します。
----------	----------------------------

```
switch(config)# policy-map my_policy1
switch(config-pmap)# description this policy applies to input packets
switch(config-pmap)#
```

<b>関連コマンド</b>	コマンド	説明
	<b>class-map</b>	クラス マップを作成または修正します。
	<b>policy-map</b>	ポリシー マップを作成または変更します。

# description (role)

ロールの説明を追加するには、**description** コマンドを使用します。ロールの説明を削除するには、このコマンドの **no** 形式を使用します。

**description** *string*

**no description**

<b>シンタックスの説明</b>	ストリング      ロールについての説明です。文字列にはスペースを含むことができます。
------------------	--

<b>デフォルト</b>	なし
--------------	----

<b>コマンド モード</b>	ロール コンフィギュレーション ( <b>config-role</b> )
-----------------	--

<b>サポートされるユーザの役割</b>	network-admin
----------------------	---------------

<b>コマンドの履歴</b>	リリース	変更内容
	4.0(4)SV1(1)	このコマンドが追加されました。

<b>使用上のガイドライン</b>	なし
-------------------	----

<b>例</b>	次に、ロールに説明を追加する例を示します。 <pre>switch(config-role)# <b>description</b> admin</pre> 次に、ロールの説明を削除する例を示します。 <pre>switch(config-role)# <b>no description</b> admin</pre>
----------	--

<b>関連コマンド</b>	コマンド	説明
	<b>username</b>	ロールの割り当てを含む、ユーザ アカウントの作成を行います。
	<b>show role</b>	ロールの設定を表示します。

# description (SPAN)

SPAN セッションに説明を追加するには、**description** コマンドを使用します。説明を削除するには、このコマンドの **no** 形式を使用します。

**description** *string*

**no description**

## シンタックスの説明

ストリング 32 文字以下の英数字で説明を指定します。

## デフォルト

ブランク (説明なし)

## コマンド モード

SPAN モニタ コンフィギュレーション (**config-monitor**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

なし

## 例

次に、SPAN セッションに説明を追加する例を示します。

```
switch# config t
switch(config)# monitor session 8
switch(config-monitor)# description span_session_8a
switch(config-monitor)#
```

次に、SPAN セッションから説明を削除する例を示します。

```
switch# config t
switch(config)# monitor session 8
switch(config)# no description span_session_8a
switch(config-monitor)#
```

## 関連コマンド

コマンド	説明
<b>show monitor session</b>	セッションの情報を表示します。

# destination (NetFlow)

宛先 IP アドレスまたは VRF を NetFlow フロー エクスポートに追加するには、**destination** コマンドを使用します。IP アドレスまたは VRF を削除するには、このコマンドの **no** 形式を使用します。

```
destination {ipaddr | ipv6addr} [use-vrf vrf_name]
```

```
no destination
```

## シンタックスの説明

<i>ipaddr</i>	コレクタの宛先 IP アドレスです。
<i>ipv6addr</i>	コレクタの宛先 IPv6 アドレスです。
<b>use-vrf</b> <i>vrf_name</i>	(任意) オプションの VRF ラベルです。

## デフォルト

なし

## コマンド モード

NetFlow フロー エクスポート コンフィギュレーション (**config-flow-exporter**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

**例** 次に、NetFlow フロー エクスポートに宛先 IP アドレスを追加する例を示します。

```
switch# config t
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# destination 192.0.2.1
```

次に、フロー エクスポートから IP アドレスを削除する例を示します。

```
switch# config t
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# no destination 192.0.2.1
```

## 関連コマンド

コマンド	説明
<b>flow exporter</b>	Flexible NetFlow フロー エクスポートを作成します。
<b>flow record</b>	Flexible NetFlow フロー レコードを作成します。
<b>flow monitor</b>	Flexible NetFlow フロー モニタを作成します。

コマンド	説明
<b>show flow exporter</b>	NetFlow フロー エクスポータに関する情報を表示します。
<b>show flow record</b>	NetFlow フロー レコードに関する情報を表示します。
<b>show flow monitor</b>	NetFlow フロー モニタに関する情報を表示します。

# destination interface (SPAN)

コピーされたソース パケットの宛先として機能する SPAN セッションのポートを設定するには、**destination interface** コマンドを使用します。宛先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。

**destination interface** *type number(s)\_or\_range*

**no destination interface** *type number(s)\_or\_range*

## シンタックスの説明

<b>ethernet</b> <i>slot/port_or_range</i>	SPAN の宛先イーサネット インターフェイスを指定します。
<b>port-channel</b> <i>number(s)_or_range</i>	SPAN の宛先ポート チャネルを指定します。
<b>vethernet</b> <i>number(s)_or_range</i>	SPAN の宛先仮想イーサネット インターフェイスを指定します。

## デフォルト

なし

## コマンド モード

SPAN モニタ コンフィギュレーション (**config-monitor**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

SPAN の宛先ポートは、アクセス ポートまたはトランク ポートとしてすでに設定されている必要があります。

SPAN セッションは、デフォルトではシャットダウン状態で作成されます。

既存の SPAN セッションを作成すると、追加の設定はすべてそのセッションに追加されます。セッションから以前の設定を確実に消去するには、**no monitor session** コマンドを使用して先にセッションを削除します。

## 例

次に、コピーされたソース パケットの宛先となる SPAN セッションのイーサネット インターフェイス 2/5 および 3/7 を設定する例を示します。

```
switch# config t
switch(config)# monitor session 8
switch(config-monitor)# destination interface ethernet 2/5, ethernet 3/7
```

次に、宛先イーサネット インターフェイス 2/5 から SPAN の設定を削除する例を示します。

```
switch# config t  
switch(config)# monitor session 8  
switch(config-monitor)# no destination interface ethernet 2/5
```

## 関連コマンド

コマンド	説明
<b>show interface</b>	指定した宛先インターフェイスのインターフェイス トランキンク設定を表示します。
<b>show monitor</b>	イーサネットの SPAN 情報を表示します。
<b>monitor session</b>	指定した SPAN モニタ セッションを開始します。

# dir

ディレクトリまたはファイルの内容を表示するには、**dir** コマンドを使用します。

**dir [bootflash: | debug: | log: | volatile:]**

## シンタックスの説明

<b>bootflash:</b>	(任意) ディレクトリまたはファイル名を指定します。
<b>debug:</b>	(任意) 拡張フラッシュのディレクトリまたはファイル名を指定します。
<b>log:</b>	(任意) ログ フラッシュのディレクトリまたはファイル名を指定します。
<b>volatile:</b>	(任意) 揮発性フラッシュのディレクトリまたはファイル名を指定します。

## デフォルト

なし

## コマンドモード

任意

## サポートされるユーザの役割

network-admin  
network-operator

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

現在の作業ディレクトリを識別するには、**pwd** コマンドを使用します。  
現在の作業ディレクトリを変更するには、**cd** コマンドを使用します。

## 例

次に、bootflash: ディレクトリの内容を表示する例を示します。

```
switch# dir bootflash:
```

## 関連コマンド

コマンド	説明
<b>cd</b>	現在の作業ディレクトリを変更します。
<b>pwd</b>	現在の作業ディレクトリを表示します。

# domain id

ドメイン ID を割り当てるには、**domain id** コマンドを使用します。ドメイン ID を削除するには、このコマンドの **no** 形式を使用します。

**domain id** *number*

**no domain id**

## シンタックスの説明

*number*           ドメイン ID 番号を指定します。指定できるドメイン ID は 1 ～ 4095 です。

## デフォルト

なし

## コマンドモード

ドメイン コンフィギュレーション (**config-svs-domain**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

Cisco Nexus 1000V をインストールする際、セットアップユーティリティでは、ドメイン ID、コントロール VLAN、パケット VLAN など、ドメインの設定が求められます。

## 例

次に、ドメイン ID を割り当てる例を示します。

```
switch# config t
switch(config)# sve-domain
switch(config-svs-domain)# domain-id number 32
switch(config-svs-domain)#
```

次に、ドメイン ID を削除する例を示します。

```
switch# config t
switch(config)# sve-domain
switch(config-svs-domain)# no domain-id number 32
switch(config-svs-domain)#
```

## 関連コマンド

コマンド	説明
<b>show svs domain</b>	ドメインの設定を表示します。

# dscp (NetFlow)

Differentiated Services Codepoint (DSCP; DiffServ コードポイント) を NetFlow フロー エクスポートに追加するには、**dscp** コマンドを使用します。DSCP を削除するには、このコマンドの **no** 形式を使用します。

**dscp** *value*

**no dscp**

## シンタックスの説明

*value*            0 ～ 63 の範囲で DSCP を指定します。

## デフォルト

なし

## コマンド モード

NetFlow フロー エクスポート コンフィギュレーション (**config-flow-exporter**)

## サポートされるユーザの役割

network-admin

## コマンドの履歴

リリース	変更内容
4.0(4)SV1(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

なし

## 例

次に、NetFlow フロー エクスポートに DSCP を設定する例を示します。

```
switch# config t
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# dscp 2
switch(config-flow-exporter)#
```

次に、NetFlow フロー エクスポートから DSCP を削除する例を示します。

```
switch# config t
switch(config)# flow exporter ExportTest
switch(config-flow-exporter)# no dscp 2
switch(config-flow-exporter)#
```

## 関連コマンド

コマンド	説明
<b>flow exporter</b>	Flexible NetFlow フロー エクスポートを作成します。
<b>flow record</b>	Flexible NetFlow フロー レコードを作成します。
<b>flow monitor</b>	Flexible NetFlow フロー モニタを作成します。

コマンド	説明
<b>show flow exporter</b>	NetFlow フロー エクスポータに関する情報を表示します。
<b>show flow record</b>	NetFlow フロー レコードに関する情報を表示します。
<b>show flow monitor</b>	NetFlow フロー モニタに関する情報を表示します。

