S コマンド

この章では、**show** コマンドを除く S で始まる Cisco NX-OS セキュリティ コマンドについて説明します（show コマンドは、第 2 章「show コマンド」で説明します）。

sap modelist

Cisco TrustSec Security Association Protocol（SAP）の動作モードを設定するには、**sap modelist** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sap modelist {**gcm-encrypt** | **gmac** | **no-encap** | **none**}

no sap modelist {**gcm-encrypt** | **gmac** | **no-encap** | **none**}

構文の説明

gcm-encrypt	Galois/Counter Mode（GCM）暗号化と認証モードを指定します。
gmac	GCM 認証モードを指定します。
no-encap	暗号化および Security Group Tag（SGT）を挿入しないように指定します。
none	認証または暗号化なしの SGT のカプセル化を指定します。

デフォルト

gcm-encrypt

コマンド モード

Cisco TrustSec 802.1X コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown**/**no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスに Cisco TrustSec SAP 動作モードを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# sap modelist gmac
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスのデフォルトの Cisco TrustSec SAP 動作モードに戻す例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no sap modelist gmac
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts dot1x	インターフェイスの Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

sap pmk

Cisco TrustSec Security Association Protocol（SAP）の Pairwise Master Key（PMK）を手動で設定するには、**sap** コマンドを使用します。SAP 設定を削除するには、このコマンドの **no** 形式を使用します。

sap pmk [*key* | **use-dot1x**} [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **none**}]

no sap

構文の説明

key	鍵の値。この値は、偶数で構成される 16 進文字列です。最大 32 文字まで指定可能です。
use-dot1x	ピア デバイスが Cisco TrustSec 802.1X 認証または許可をサポートせず、SAP データ パス暗号化と認証をサポートするように指定します。
modelist	（任意）SAP 動作モードを指定します。
gcm-encrypt	Galois/Counter Mode（GCM）暗号化と認証モードを指定します。
gmac	GCM 認証モードを指定します。
no-encap	暗号化および Security Group Tag（SGT）を挿入しないように指定します。
none	認証または暗号化なしの SGT のカプセル化を指定します。

デフォルト

gcm-encrypt

コマンド モード

Cisco TrustSec 手動コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(3)	**use-dot1x** キーワードが追加されました。
4.0(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、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown**/**no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスに Cisco TrustSec SAP を手動で設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスから Cisco TrustSec SAP 設定を手動で削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no sap
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec 手動コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

send-lifetime

デバイスが別のデバイスとの鍵の交換時に鍵を送信する時間間隔を指定するには、**send-lifetime** コマンドを使用します。時間間隔を削除するには、このコマンドの **no** 形式を使用します。

send-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

構文の説明

local	（任意）デバイスが、設定された時間をローカル時間として扱うように指定します。デフォルトでは、デバイスは *start-time* 引数および *end-time* 引数を UTC として扱います。
start-time	鍵がアクティブになる時刻および日付。 *start-time* 引数の値の詳細については、「使用上のガイドライン」を参照してください。
duration *duration-value*	（任意）ライフタイムの長さを秒単位で指定します。最大の長さは、2147483646 秒です（約 68 年）。
infinite	（任意）鍵が期限切れにならないように指定します。
end-time	（任意）鍵が非アクティブになる時刻および日付。 *end-time* 引数の有効値の詳細については、「使用上のガイドライン」を参照してください。

デフォルト

infinite

コマンド モード

鍵コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

このコマンドには、ライセンスは不要です。

デフォルトでは、デバイスはすべての時間範囲のルールを UTC として扱います。

デフォルトでは、デバイスが別のデバイスとの鍵の交換時に鍵を送信する時間間隔（送信ライフタイム）は、infinite です。つまり、鍵は期限切れになりません。

start-time 引数および *end-time* 引数の両方には、次の形式の時間と日付のコンポーネントが必要です。

hour[:*minute*[:*second*]] *month day year*

24 時間表記で指定します。たとえば、24 時間表記では 8:00 a.m. は 8:00 で、8:00 p.m. は 20:00 です。最小の有効な *start-time* 値は 00:00:00 Jan 1 1970 で、最大の有効な *start-time* 値は 23:59:59 Dec 31 2037 です。

例

次に、2008 年 6 月 13 日の午前零時に開始され、2008 年 8 月 12 日の午後 11 時 59 分 59 秒に終了する送信ライフタイムを作成する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2008 23:59:59 Aug 12 2008
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
accept-lifetime	鍵の受け入れライフタイムを設定します。
key	鍵を設定します。
key chain	キーチェーンを設定します。
key-string	鍵のストリングを設定します。
show key chain	キーチェーンの設定を表示します。

server

RADIUS サーバ グループ、TACACS+ サーバ グループ、または LDAP 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*}

構文の説明

ipv4-address	*A.B.C.D* 形式のサーバの IPv4 アドレス
ipv6-address	*X:X:X::X* 形式のサーバの IPv6 アドレス
hostname	サーバ名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。

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
LDAP サーバ グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
5.0(2)	LDAP サーバ グループのサポートが追加されました。
4.0(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

サーバ グループには、最大 64 のサーバを設定できます。

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。TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。LDAP 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 ldap** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンド、**tacacs-server host** コマンド、または **ldap-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+** コマンドを使用し、LDAP を設定する前に、**feature ldap** コマンドを使用する必要があります。

このコマンドには、ライセンスは不要です。

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

次に、LDAP サーバ グループにサーバを追加する例を示します。

```
switch# configure terminal
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)# server 10.10.3.3
```

次に、LDAP サーバ グループからサーバを削除する例を示します。

```
switch# configure terminal
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-ldap)# no server 10.10.3.3
```

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 ldap-server groups	LDAP サーバ グループ情報を表示します。
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。
feature tacacs+	TACACS+ をイネーブルにします。
tacacs-server host	TACACS+ サーバを設定します。
feature ldap	LDAP をイネーブルにします。
ldap-server host	LDAP サーバを設定します。

service dhcp

DHCP リレー エージェントをイネーブルにするには、**service dhcp** コマンドを使用します。DHCP リレー エージェント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。

service dhcp

no service dhcp

構文の説明

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

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	このコマンドは廃止予定で、**ip dhcp relay** コマンドに置き換えられます。
4.0(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

このコマンドには、ライセンスは不要です。

例

次に、DHCP スヌーピングをグローバルにイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# service dhcp
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp relay address	インターフェイスの DHCP サーバの IP アドレスを設定します。
ip dhcp relay information option	DHCP パケットの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

service-policy input

コントロール プレーンにコントロール プレーン ポリシー マップを付加するには、**service-policy input** コマンドを使用します。コントロール プレーン ポリシー 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。

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

構文の説明

policy-map-name	コントロール プレーン ポリシー マップの名前

デフォルト

なし

コマンド モード

コントロール プレーン コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

このコマンドは、デフォルトの Virtual Device Context（VDC; 仮想デバイス コンテキスト）でだけ使用できます。

コントロール プレーンに割り当てることができるのは、1 つのコントロール プレーン ポリシー マップだけです。コントロール プレーンに新しいコントロール プレーン ポリシー マップを割り当てるには、古いコントロール プレーン ポリシー マップを削除する必要があります。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーンにコントロール プレーン ポリシー マップを割り当てる例を示します。

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp)# service-policy input PolicyMapA
```

次に、コントロール プレーンからコントロール プレーン ポリシー マップを削除する例を示します。

```
switch# configure terminal
switch(config)# control-plane
switch(config-cp)# no service-policy input PolicyMapA
```

関連コマンド

コマンド	説明
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

set cos

コントロール プレーン ポリシー マップの IEEE 802.1Q Class of Service（CoS; サービス クラス）値を設定するには、**set cos** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set cos [**inner**] *cos-value*

no set cos [**inner**] *cos-value*

構文の説明

inner	（任意）Q-in-Q 環境には inner 802.1Q を指定します。
cos-value	コントロール プレーン ポリシー マップの CoS の数値。範囲は 0 ～ 7 です。

デフォルト

0

コマンド モード

ポリシー マップ クラス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

このコマンドは、デフォルトの仮想デバイス コンテキスト（VDC）でだけ使用できます。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーン ポリシー マップの CoS 値を設定する例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set cos 4
```

次に、コントロール プレーン ポリシー マップのデフォルトの CoS 値に戻す例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set cos 4
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

set dscp（ポリシー マップ クラス）

コントロール プレーン ポリシー マップに IPv4 パケットおよび IPv6 パケットの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定するには、**set dscp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set dscp [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}

no set dscp [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}

構文の説明

tunnel	（任意）トンネル カプセル化に DSCP を設定します。
dscp-value	コントロール プレーン ポリシー マップの CoS の数値。範囲は 0 ～ 63 です。
af11	相対的優先転送 11 DSCP（001010）を指定します。
af12	相対的優先転送 12 DSCP（001100）を指定します。
af13	相対的優先転送 13 DSCP（001110）を指定します。
af21	相対的優先転送 21 DSCP（010010）を指定します。
af22	相対的優先転送 22 DSCP（010100）を指定します。
af23	相対的優先転送 23 DSCP（010110）を指定します。
af31	相対的優先転送 31 DSCP（011010）を指定します。
af32	相対的優先転送 32 DSCP（011100）を指定します。
af33	相対的優先転送 33 DSCP（011110）を指定します。
af41	相対的優先転送 41 DSCP（100010）を指定します。
af42	相対的優先転送 42 DSCP（100100）を指定します。
af43	相対的優先転送 43 DSCP（100110）を指定します。
cs1	クラス セレクタ 1（precedence 1）DSCP（001000）を指定します。
cs2	クラス セレクタ 2（precedence 2）DSCP（010000）を指定します。
cs3	クラス セレクタ 3（precedence 3）DSCP（011000）を指定します。
cs4	クラス セレクタ 4（precedence 4）DSCP（100000）を指定します。
cs5	クラス セレクタ 5（precedence 5）DSCP（101000）を指定します。
cs6	クラス セレクタ 6（precedence 6）DSCP（110000）を指定します。
cs7	クラス セレクタ 7（precedence 7）DSCP（111000）を指定します。
ef	完全優先転送 DSCP（101110）を指定します。
default	デフォルトの DSCP（000000）を指定します。

デフォルト

default

コマンド モード

ポリシー マップ クラス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

このコマンドは、デフォルトの仮想デバイス コンテキスト（VDC）でだけ使用できます。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーン ポリシー マップの DHCP 値を設定する例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set dscp 4
```

次に、コントロール プレーン ポリシー マップのデフォルトの DHCP 値に戻す例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set dscp 4
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

set precedence（ポリシー マップ クラス）

コントロール プレーン ポリシー マップに IPv4 および IPv6 パケットの precedence 値を設定するには、**set precedence** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set precedence [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}

no set precedence [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}

構文の説明

tunnel	（任意）トンネル カプセル化に precedence を設定します。
prec-value	コントロール プレーン ポリシー マップの DSCP precedence の数値。範囲は 0 ～ 7 です。
critical	precedence 値 5 に等しい critical precedence を指定します。
flash	precedence 値 3 に等しい flash precedence を指定します。
flash-override	precedence 値 4 に等しい flash override precedence を指定します。
immediate	precedence 値 2 に等しい immediate precedence を指定します。
internet	precedence 値 6 に等しい internet precedence を指定します。
network	precedence 値 7 に等しい network precedence を指定します。
priority	precedence 値 1 に等しい priority precedence を指定します。
routine	precedence 値 0 に等しい routine precedence を指定します。

デフォルト

0 または **routine**

コマンド モード

ポリシー マップ クラス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

このコマンドは、デフォルトの仮想デバイス コンテキスト（VDC）でだけ使用できます。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーン ポリシー マップの CoS 値を設定する例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set precedence critical
```

次に、コントロール プレーン ポリシー マップのデフォルトの CoS 値に戻す例を示します。

```
switch# configure terminal
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set precedence critical
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

source-interface

特定の RADIUS サーバ グループまたは TACACS+ サーバ グループでソース インターフェイスを割り当てるには、**source-interface** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

source-interface *interface*

no source-interface

構文の説明

interface	ソース インターフェイス。サポートされるインターフェイス タイプは、**ethernet**、**loopback**、および **mgmt 0** です。

デフォルト

デフォルトは、グローバル ソース インターフェイスです。

コマンド モード

RADIUS コンフィギュレーション
TACACS+ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

ip radius source-interface コマンドまたは **ip tacacs source-interface** コマンドによって割り当てられたグローバル ソース インターフェイスを上書きする **source-interface** コマンド。

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。

このコマンドには、ライセンスは不要です。

例

次に、ip-acl-01 という 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# configure terminal
switch(config)# ip radius source-interface mgmt 0
switch(config-radius)# source-interface ethernet 2/1
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ 機能をイネーブルにします。
ip radius source-interface	Cisco NX-OS デバイス上で設定された RADIUS グループで、グローバル ソース インターフェイスを設定します。
ip tacacs source-interface	Cisco NX-OS デバイス上で設定された TACACS+ グループで、グローバル ソース インターフェイスを設定します。
show radius-server groups	RADIUS サーバ グループ設定を表示します。
show tacacs-server groups	TACACS+ サーバ グループ設定を表示します。

ssh

Cisco NX-OS デバイス上に Secure Shell（SSH; セキュア シェル）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*]

構文の説明

username	（任意）SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がありません。
ipv4-address	リモート デバイスの IPv4 アドレス。
hostname	リモート デバイスのホスト名。ホスト名では、大文字と小文字が区別されます。
vrf *vrf-name*	（任意）SSH セッションで使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名を指定します。VRF 名では、大文字と小文字が区別されます。

デフォルト

デフォルト VRF

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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 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 セッションの IPv6 アドレスを使用するには、**ssh6** コマンドを使用します。

Cisco NX-OS ソフトウェアは、最大で 60 の並列の SSH セッションおよび Telnet セッションをサポートしています。

Cisco NX-OS デバイスのブート モードから、リモート デバイスへの SSH セッションを作成する予定がある場合、リモート デバイスのホスト名を取得し、リモート デバイスで SSH サーバをイネーブルにして、Cisco NX-OS にキックスタート イメージのみがロードされていることを確認する必要があります。

このコマンドには、ライセンスは不要です。

例

次に、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
The authenticity of host '10.10.1.1 (10.10.1.1)' can't be established.
RSA key fingerprint is 9b:d9:09:97:f6:40:76:89:05:15:42:6b:12:48:0f:d6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.1' (RSA) to the list of known hosts.
User Access Verification
Password:
```

次に、Cisco NX-OS デバイスのブート モードから、リモート デバイスへの SSH セッションを作成する例を示します。

```
switch(boot)# ssh user1@10.10.1.1
```

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。
copy scp:	Secure Copy Protocol（SCP）を使用して、Cisco NX-OS デバイスからリモート デバイスにファイルをコピーします。
feature ssh	SSH サーバをイネーブルにします。
ssh6	IPv6 アドレスを使用して SSH セッションを開始します。

ssh key

仮想デバイス コンテキスト（VDC）の Secure Shell（SSH; セキュア シェル）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**]

構文の説明

dsa	Digital System Algorithm（DSA）SSH サーバ鍵を指定します。
force	（任意）SSH 鍵の交換を強制します。
rsa	RSA 公開鍵暗号法の 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。範囲は 768 ～ 2048 です。

デフォルト

1024 ビットの長さ

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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 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、**no feature ssh** コマンドを使用してまず SSH サーバをディセーブルにする必要があります。

このコマンドには、ライセンスは不要です。

例

次に、DSA を使用して SSH サーバ鍵を作成する例を示します。

```
switch# configure terminal
switch(config)# ssh key dsa
generating dsa key(1024 bits).....
..
generated dsa key
```

次に、デフォルトの鍵の長さで RSA を使用して SSH サーバ鍵を作成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

次に、指定した鍵の長さで RSA を使用して SSH サーバ鍵を作成する例を示します。

```
switch# configure terminal
switch(config)# ssh key rsa 768
generating rsa key(768 bits).....
.
generated rsa key
```

次に、force オプションで DSA を使用して SSH サーバ鍵を交換する例を示します。

```
switch# configure terminal
switch(config)# no feature ssh
switch(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
switch(config)# feature ssh
```

次に、DSA SSH サーバ鍵を削除する例を示します。

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key dsa
switch(config)# feature ssh
```

次に、すべての SSH サーバ鍵を削除する例を示します。

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key
switch(config)# feature ssh
```

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。
feature ssh	SSH サーバをイネーブルにします。

ssh login-attempts

ユーザが Secure Shell（SSH）セッションにログインを試みることができる最大回数を設定するには、**ssh login-attempts** コマンドを使用します。設定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 login-attempts *number*

no ssh login-attempts

構文の説明

number	最大ログイン試行回数。指定できる範囲は 1 ～ 10 です。

デフォルト

3

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

ログイン試行の合計数には、公開鍵認証、証明書ベースの認証、パスワードベースの認証による試行が含まれます。

このコマンドには、ライセンスは不要です。

ユーザは許可されたログイン試行の最大回数を超えると、セッションが切断されます。

例

次に、ユーザが SSH セッションにログインを試みることができる最大回数を設定する例を示します。

```
switch# config t
switch(config)# ssh login-attempts 5
```

次に、SSH ログイン試行設定をディセーブルにする例を示します。

```
switch# config t
switch(config)# no ssh login-attempts
```

関連コマンド

コマンド	説明
show running-config security all	SSH ログイン試行の設定済みの最大回数を表示します。

ssh server enable

仮想デバイス コンテキスト（VDC）の Secure Shell（SSH; セキュア シェル）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

構文の説明

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

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.1(2)	このコマンドは廃止予定で、**feature ssh** コマンドに置き換えられます。
4.0(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 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。

このコマンドには、ライセンスは不要です。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch# config t
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 t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
```

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。

ssh6

Cisco NX-OS デバイス上に IPv6 による Secure Shell（SSH; セキュア シェル）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*]

構文の説明

username	（任意）SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がありません。
ipv6-address	リモート デバイスの IPv6 アドレス。
hostname	リモート デバイスのホスト名。
vrf *vrf-name*	（任意）SSH セッションで使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名を指定します。VRF 名では、大文字と小文字が区別されます。

デフォルト

デフォルト VRF

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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 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 セッションを開始するために IPv4 アドレスを使用するには、**ssh** コマンドを使用します。

Cisco NX-OS ソフトウェアは、最大で 60 の並列の SSH セッションおよび Telnet セッションをサポートしています。

このコマンドには、ライセンスは不要です。

例

次に、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 host2 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。

コマンド	説明
ssh	IPv4 アドレスを使用して SSH セッションを開始します。
feature ssh	SSH サーバをイネーブルにします。

statistics per-entry

IP、MAC Access Control List（ACL; アクセス コントロール リスト）、または VLAN アクセスマップ エントリの各エントリで許可または拒否されたパケット数の統計情報の記録を開始するには、**statistics per-entry** コマンドを使用します。エントリ単位の統計情報の記録を停止するには、このコマンドの **no** 形式を使用します。

statistics per-entry

no statistics per-entry

構文の説明

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

IP アクセスリスト コンフィギュレーション
IPv6 アクセスリスト コンフィギュレーション
MAC アクセスリスト コンフィギュレーション
VLAN アクセスマップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(3)	**statistics** から **statistics per-entry** にコマンドが変更されました。
4.0(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

IPv4、IPv6、MAC ACL、または VLAN ACL がパケットに適用されるとデバイスが判別すると、ACL 内のすべてのエントリの条件に対してパケットのテストが実行されます。ACL エントリは、適用可能な **permit** コマンドおよび **deny** コマンドで設定するルールから抽出されます。最初の一致ルールは、パケットが許可または拒否されるかを判別します。**statistics per-entry** コマンドを入力して、ACL の各エントリで許可または拒否されるパケット数の記録を開始します。

DHCP スヌーピング機能がイネーブルに設定されている場合、統計情報はサポートされません。

デバイスは、暗黙ルールの統計情報を記録しません。これらのルールの統計情報を記録するには、各暗黙ルールの一致するルールを明示的に設定する必要があります。暗黙ルールの詳細については、次のコマンドを参照してください。

- **ip access-list**
- **ipv6 access-list**
- **mac access-list**

エントリ単位の統計情報を表示するには、**show access-lists** コマンドまたは適用可能な次のコマンドを使用します。

- **show ip access-lists**
- **show ipv6 access-lists**
- **show mac access-lists**

エントリ単位の統計情報を消去するには、**clear access-list counters** コマンドまたは適用可能な次のコマンドを使用します。

- **clear ip access-list counters**
- **clear ipv6 access-list counters**
- **clear mac access-list counters**
- **clear vlan access-list counters**

このコマンドには、ライセンスは不要です。

例

次に、ip-acl-101 という名前の IPv4 ACL に対するエントリ単位の統計情報の記録を開始する例を示します。

```
switch(config)# ip access-list ip-acl-101
switch(config-acl)# statistics per-entry
switch(config-acl)#
```

次に、ip-acl-101 という名前の IPv4 ACL に対するエントリ単位の統計情報の記録を停止する例を示します。

```
switch(config)# ip access-list ip-acl-101
switch(config-acl)# no statistics per-entry
switch(config-acl)#
```

次に、vlan-map-01 という名前の VLAN アクセス マップのエントリ 20 の ACL でエントリごとの統計情報の記録を開始する例を示します。

```
switch(config)# vlan access-map vlan-map-01 20
switch(config-access-map)# statistics per-entry
switch(config-access-map)#
```

次に、vlan-map-01 という名前の VLAN アクセス マップのエントリ 20 の ACL でエントリごとの統計情報の記録を停止する例を示します。

```
switch(config)# vlan access-map vlan-map-01 20
switch(config-access-map)# no statistics per-entry
switch(config-access-map)#
```

関連コマンド

コマンド	説明
show access-lists	すべての IPv4、IPv6、および MAC ACL、または特定の ACL を表示します。
clear access-list counters	すべての IPv4、IPv6、および MAC ACL、または特定の ACL のエントリ単位の統計情報を消去します。

storm-control level

トラフィック ストーム制御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したり、デフォルトの設定に戻したりするには、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**

構文の説明

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。
percentage	抑制レベルの割合。範囲は 0 ～ 100% です。
.fraction	（任意）抑制レベルの端数。範囲は 0 ～ 99 です。

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(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

storm-control level コマンドを入力して、インターフェイス上のトラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、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 ストーム制御モードにトラフィック ストーム制御レベルを適用します。

3 つすべての抑制モードで共有されている抑制レベルは、1 つだけです。たとえば、ブロードキャスト レベルを 30 に設定し、マルチキャスト レベルを 40 に設定する場合、両方のレベルがイネーブルにされ、40 に設定されます。

端数の抑制レベルを入力する場合、ピリオド（.）が必要になります。

抑制レベルは、合計帯域幅の割合です。100% 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（端数）パーセントのしきい値は、指定されたすべての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。

廃棄カウントを表示するには、**show interfaces counters broadcast** コマンドを使用します。

指定したトラフィック タイプの抑制をオフにするには、次のいずれかの方式を使用します。

- 指定したトラフィック タイプのレベルを 100% に設定する。

- このコマンドの **no** 形式を使用する。

このコマンドには、ライセンスは不要です。

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、抑制しきい値レベルを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# storm-control broadcast level 30
```

次に、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# configure terminal
switch(config)# interface ethernet 1/1
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制御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。

switchport port-security

レイヤ 2 イーサネット インターフェイスまたはレイヤ 2 ポートチャネル インターフェイスのポート セキュリティをイネーブルにするには、**switchport port-security** コマンドを使用します。ポート セキュリティ設定を削除するには、このコマンドの **no** 形式を使用します。

switchport port-security

no switchport port-security

構文の説明

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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、インターフェイス単位でポート セキュリティがディセーブルにされています。

switchport port-security コマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとしてインターフェイスを設定する必要があります。

switchport port-security コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

レイヤ 2 ポートチャネル インターフェイスの任意のメンバー ポート上でポート セキュリティをイネーブルにする場合、デバイス上では、ポートチャネル インターフェイスのポート セキュリティをディセーブルにはできません。これを行うには、まず、ポートチャネル インターフェイスからすべてのセキュア メンバー ポートを削除します。メンバー ポートでポート セキュリティをディセーブルにしたあとで、必要に応じて、ポートチャネル インターフェイスを再度追加できます。

インターフェイスでポート セキュリティをイネーブルにすると、セキュア MAC アドレスの学習のデフォルト方式（ダイナミック方式）もイネーブルになります。スティッキ学習方式をイネーブルにするには、**switchport port-security mac-address sticky** コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット 2/1 インターフェイスのポート セキュリティをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security
switch(config-if)#
```

次に、ポートチャネル 10 インターフェイスのポート セキュリティをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 10
switch(config-if)# switchport port-security
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security aging time

動的に学習したセキュア MAC アドレスのエージング タイムを設定するには、**switchport port-security aging time** コマンドを使用します。デフォルトのエージング タイムである 1440 分に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security aging time *minutes*

no switchport port-security aging time *minutes*

構文の説明

minutes	デバイスがアドレスをドロップするまでの動的に学習されたセキュア MAC アドレスのエージング タイム。有効値は、1 ～ 1440 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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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

デフォルトのエージング タイムは、1440 分です。

switchport port-security aging time コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとして動作するよう、インターフェイスを設定します。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット 2/1 インターフェイス上に 120 分のエージング タイムを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging time 120
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security aging type

動的に学習したセキュア MAC アドレスのエージング タイプを設定するには、**switchport port-security aging type** コマンドを使用します。デフォルトのエージング タイプ（absolute エージング）に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security aging type {**absolute | inactivity**}

no switchport port-security aging type {**absolute | inactivity**}

構文の説明

absolute	動的に学習されたセキュア MAC アドレスのエージングが、デバイスがアドレスの学習を開始した時点からの時間に基づくように指定します。
inactivity	動的に学習されたセキュア MAC アドレスのエージングが、デバイスが現在のインターフェイスで MAC アドレスから最後にトラフィックを受信した時点からの時間に基づくように指定します。

デフォルト

absolute

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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

デフォルトのエージング タイプは、absolute エージングです。

switchport port-security aging type コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとして動作するよう、インターフェイスを設定します。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット 2/1 インターフェイス上に [inactivity] のエージング タイプを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging type inactivity
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	ポート セキュリティにレイヤ 2 インターフェイスを設定します。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security mac-address

インターフェイスにスタティック セキュア MAC アドレスを設定するには、**switchport port-security mac-address** コマンドを使用します。インターフェイスからスタティック セキュア MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address *address* [**vlan** *vlan-ID*]

no switchport port-security mac-address *address* [**vlan** *vlan-ID*]

構文の説明

address	現在のインターフェイスにスタティック セキュア MAC アドレスとして指定する MAC アドレス
vlan *vlan-ID*	（任意）MAC アドレスからのトラフィックが許可される VLAN を指定します。有効な VLAN ID は、1 ～ 4096 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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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

デフォルトのスタティック セキュア MAC アドレスはありません。

switchport port-security mac-address コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとして動作するよう、インターフェイスを設定します。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット 2/1 インターフェイスにスタティック セキュア MAC アドレスとして 0019.D2D0.00AE を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	ポート セキュリティにレイヤ 2 インターフェイスを設定します。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security mac-address sticky

レイヤ 2 イーサネット インターフェイスまたはレイヤ 2 ポートチャネル インターフェイスのセキュア MAC アドレスを学習するスティッキ方式をイネーブルにするには、**switchport port-security mac-address sticky** コマンドを使用します。スティッキ方式をディセーブルにし、ダイナミック方式に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address sticky

no switchport port-security mac-address sticky

構文の説明

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

デフォルトでは、セキュア MAC アドレスを学習するスティッキ方式がディセーブルです。

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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

switchport port-security mac-address sticky コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとして動作するよう、インターフェイスを設定します。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット 2/1 インターフェイスのセキュア MAC アドレスを学習するスティッキ方式をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security maximum

レイヤ 2 イーサネット インターフェイスまたはレイヤ 2 ポートチャネル インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定するには、**switchport port-security maximum** コマンドを使用します。ポート セキュリティ設定を削除するには、このコマンドの **no** 形式を使用します。

switchport port-security maximum *number* [**vlan** *vlan-ID*]

no switchport port-security maximum *number* [**vlan** *vlan-ID*]

構文の説明

maximum *number*	セキュア MAC アドレスの最大数を指定します。*number* 引数の有効値に関する詳細については、「使用上のガイドライン」を参照してください。
vlan *vlan-ID*	（任意）最大値が適用される VLAN を指定します。**vlan** キーワードを省略する場合、最大値がインターフェイスの最大値として適用されます。

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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

デフォルトのインターフェイスの最大値は、1 つのセキュア MAC アドレスです。

インターフェイスでポート セキュリティをイネーブルにすると、セキュア MAC アドレスの学習のデフォルト方式（ダイナミック方式）もイネーブルになります。スティッキ学習方式をイネーブルにするには、**switchport port-security mac-address sticky** コマンドを使用します。

switchport port-security maximum コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとして動作するよう、インターフェイスを設定します。

デフォルトの VLAN の最大値はありません。

システム全体の、設定不可のセキュア MAC アドレスが最大 4096 あります。

このコマンドには、ライセンスは不要です。

アクセス ポートおよびトランク ポートの最大値

アクセス ポートして使用されるインターフェイスの場合、1 つのセキュア MAC アドレスにデフォルトのインターフェイスの最大値を使用することを推奨します。

トランク ポートして使用されるインターフェイスの場合、インターフェイスに使用できる実際のホスト数を反映する数にインターフェイスの最大値を設定します。

インターフェイスの最大値、VLAN の最大値、およびデバイスの最大値

インターフェイスに設定するすべての VLAN の最大値の合計は、インターフェイスの最大値を超えません。たとえば、インターフェイスの最大値を 10 セキュア MAC アドレス、VLAN 1 に対する VLAN の 最大値 を 5 セキュア MAC アドレスでトランクポート インターフェイスを設定する場合、VLAN 2 に設定するセキュア MAC アドレスの最大数も 5 になります。VLAN 2 に対して 6 セキュア MAC アドレスの最大値を設定しようとすると、デバイスはコマンドを受け入れません。

例

次に、イーサネット 2/1 インターフェイス上に 10 セキュア MAC アドレスのインターフェイスの最大値を設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security maximum 10
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security violation

セキュリティ違反イベントがインターフェイス上で発生するときにデバイスが実行する処理を設定するには、**switchport port-security violation** コマンドを使用します。ポート セキュリティ違反処理の設定を削除するには、このコマンドの **no** 形式を使用します。

switchport port-security violation {**protect | restrict | shutdown**}

no switchport port-security violation {**protect | restrict | shutdown**}

構文の説明

protect	パケットが通常セキュリティ違反イベントをトリガーするときに、デバイスがセキュリティ違反を発生させないように指定します。代わりに、セキュリティ違反をトリガーするアドレスは認識されますが、アドレスからのいかなるトラフィックもドロップされます。以降のアドレス認識は停止されます。
restrict	デバイスが、セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップするように指定します。アドレス認識は、インターフェイス上で 100 のセキュリティ違反が発生するまで継続されます。セキュリティ違反後、アドレスから最初に認識されるトラフィックはドロップされます。 100 のセキュリティ違反の発生後、デバイスは、インターフェイス上での認識をディセーブルにし、セキュアな MAC アドレス以外のアドレスからのすべての入力トラフィックをドロップします。さらに、デバイスでは、各セキュリティ違反に対して SNMP トラップが生成されます。
shutdown	セキュリティ違反をトリガーしているパケットを受信すると、デバイスがインターフェイスをシャットダウンするように指定します。インターフェイスは、errdisable 状態です。これがデフォルトの処理です。インターフェイスを再度イネーブルにしたあと、セキュア MAC アドレスを含めて、ポート セキュリティ設定は維持されます。

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

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.2(1)	レイヤ 2 ポートチャネル インターフェイスのサポートが追加されました。
4.0(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

デフォルトのセキュリティ違反処理は、インターフェイスをシャットダウンすることです。

switchport port-security violation コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用して、レイヤ 2 インターフェイスとして動作するよう、インターフェイスを設定します。

次の 2 つのいずれかのイベントが発生したときにポート セキュリティはセキュリティ違反をトリガーします。

- セキュア MAC アドレス以外のアドレスから入力トラフィックがインターフェイスに着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超えてしまう場合

  VLAN とインターフェイスの両方の最大値が設定されていて、どちらかの最大数を超える場合。たとえば、ポート セキュリティが設定されている単一のインターフェイスについて、次のように想定します。

  - VLAN 1 の最大アドレス値は 5 です。
  - このインターフェイスの最大アドレス値は 10 です。

  デバイスは、次のいずれかが発生すると違反を検出します。

  - VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンド トラフィックが VLAN 1 のインターフェイスに着信した場合
  - このインターフェイス上のアドレスをすでに 10 個学習していて、11 番目のアドレスからのインバウンド トラフィックがこのインターフェイスに着信した場合
- あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

（注） あるセキュア ポートでセキュア MAC アドレスが設定または学習されたあと、同じ VLAN 内の別のポート上でこのセキュア MAC アドレスが検出された場合に発生する一連のイベントを、MAC の移行違反と呼びます。

セキュリティ違反が発生すると、デバイスは、該当するインターフェイスのポート セキュリティ設定に指定されている処理を実行します。デバイスが実行できる処理は次のとおりです。

- シャットダウン：違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。インターフェイスは、errdisable 状態です。これがデフォルトの処理です。インターフェイスを再度イネーブルにしたあと、セキュア MAC アドレスを含めて、ポート セキュリティ設定は維持されます。

  シャットダウン後にデバイスが自動的にインターフェイスを再度イネーブルするように設定するには、**errdisable** グローバル コンフィギュレーション コマンドを使用します。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再度イネーブルにすることもできます。
- 制限：セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップします。アドレス認識は、インターフェイス上で 100 のセキュリティ違反が発生するまで継続されます。セキュリティ違反後、アドレスから最初に認識されるトラフィックはドロップされます。

  100 のセキュリティ違反の発生後、デバイスは、インターフェイス上での認識をディセーブルにし、セキュアな MAC アドレス以外のアドレスからのすべての入力トラフィックをドロップします。さらに、デバイスでは、各セキュリティ違反に対して SNMP トラップが生成されます。
- 保護：さらなる違反の発生を防止します。セキュリティ違反をトリガーするアドレスは認識されますが、アドレスからのいかなるトラフィックもドロップされます。以降のアドレス認識は停止されます。

セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにしたインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合、デバイスはトラフィックを受信したインターフェイスに対して処理を実行します。

このコマンドには、ライセンスは不要です。

例

次に、保護処理でセキュリティ違反イベントに応答するようにインターフェイスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security violation protect
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。