C コマンド

この章では、C で始まる Cisco NX-OS Security コマンドについて説明します。

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 マップを指定するには、**class** コマンドを使用します。コントロール プレーン ポリシー マップからコントロール プレーン クラス 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。

class {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}

no class *class-map-name*

シンタックスの説明

class-map-name	クラス マップの名前
insert-before *class-map-name2*	（任意）コントロール プレーン ポリシー マップの別のコントロール プレーン クラス マップの前にコントロール プレーン クラス マップを挿入します。
class-default	デフォルト クラスを指定します。

デフォルト

なし

コマンド モード

ポリシー 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(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルト Virtual Device Context（VDC; バーチャル デバイス コンテキスト）でのみ使用できます。

このコマンドにライセンスは必要ありません。

例

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

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
swtich(config-pmap-c)
```

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

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# no class ClassMapA
```

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。

class-map type control-plane

コントロール プレーン クラス マップを作成または指定して、クラス マップ コンフィギュレーション モードを開始するには、**class-map type control-plane** コマンドを使用します。コントロール プレーン クラス 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。

class-map type control-plane [**match-all** | **match-any**] *class-map-name*

no class-map type control-plane [**match-all** | **match-any**] *class-map-name*

シンタックスの説明

match-all	（任意）クラス マップのすべての一致条件と一致するように指定します。
match-any	（任意）クラス マップの任意の一致条件と一致するように指定します。
class-map-name	クラス マップの名前。名前には英数字を使用します。大文字と小文字が区別され、最大 64 文字まで可能です。

デフォルト

match-any

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)	このコマンドが導入されました。

使用上のガイドライン

コントロール プレーン クラス マップの名前として、match-all、match-any、または class-default は使用できません。

このコマンドは、デフォルト VDC でのみ使用できます。

このコマンドにライセンスは必要ありません。

例

次に、コントロール プレーン クラス マップを指定して、クラス マップ 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 t
switch(config)# class-map type control-plane ClassMapA
switch(config-cmap)#
```

次に、コントロール プレーン クラス マップを削除する例を示します。

```
switch# config t
switch(config)# no class-map type control-plane ClassMapA
```

関連コマンド

コマンド	説明
show class-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。

clear access-list counters

すべてまたは 1 つの IPv4 Access Control List（ACL; アクセス コントロール リスト）および MAC ACL のカウンタをクリアするには、**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）デバイスがそのカウンタをクリアする 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。

デフォルト

なし

コマンド モード

特権 EXEC

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)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての IPv4 ACL および MAC ACL のカウンタをクリアする例を示します。

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

次に、acl-ipv4-01 という名前の IPv4 ACL のカウンタをクリアする例を示します。

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

関連コマンド

コマンド	説明
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL および MAC ACL に関する情報を表示します。

clear accounting log

アカウンティング ログをクリアするには、**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。

デフォルト なし

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)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、デフォルト VDC（VDC 1）でのみ機能します。

このコマンドにライセンスは必要ありません。

例 次に、アカウンティング ログをクリアする例を示します。

```
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 ログの内容を表示します。

clear copp statistics

コントロール プレーン ポリシング（CoPP）統計情報をクリアするには、**clear copp statistics** コマンドを使用します。

clear copp statistics

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 任意のコンフィギュレーション 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)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、デフォルト VDC でのみ使用できます。

このコマンドにライセンスは必要ありません。

例 次に、コントロール プレーン クラス マップを指定して、クラス マップ 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# clear copp statistics
```

関連コマンド

コマンド	説明
show policy-map interface control-plane	インターフェイスの CoPP 統計情報を表示します。

clear dot1x

802.1X オーセンティケータ インスタンスをクリアするには、**clear dot1x** コマンドを使用します。

clear dot1x {**all** | **interface ethernet** *slot*/*port*}

シンタックスの説明

all	すべての 802.1X オーセンティケータ インスタンスを指定します。
interface ethernet *slot*/*port*	指定のインターフェイスの 802.1X オーセンティケータ インスタンスを指定します。

デフォルト

なし

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)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、すべての 802.1X オーセンティケータ インスタンスをクリアする例を示します。

```
switch# clear dot1x all
```

次に、インターフェイスの 802.1X オーセンティケータ インスタンスをクリアする例を示します。

```
switch# clear dot1x interface ethernet 1/1
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

clear eou

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）セッションをクリアするには、**clear eou** コマンドを使用します。

clear eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *type*}

シンタックスの説明

all	すべての EAPoUDP セッションを指定します。
authentication	EAPoUDP 認証を指定します。
clientless	クライアントレス ポスチャ検証を使用して認証するセッションを指定します。
eap	EAPoUDP を使用して認証するセッションを指定します。
static	静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet *slot*/*port*	インターフェイスを指定します。
ip-address *ipv4-address*	IPv4 アドレスを A.B.C.D 形式で指定します。
mac-address *mac-address*	MAC アドレスを指定します。
posturetoken *type*	ポスチャ トークン名を指定します。

デフォルト

なし

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)	このコマンドが導入されました。

使用上のガイドライン

feature eou コマンドを使用して EAPoUDP をイネーブルにしてから、**clear eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、すべての EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou all
```

次に、静的に認証された EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou authentication static
```

次に、インターフェイスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou interface ethernet 1/1
```

次に、IP アドレスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou ip-address 10.10.1.1
```

次に、MAC アドレスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou mac-address 0019.076c.dac4
```

次に、ポスチャ トークンのタイプが Checkup である EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou posturetoken healthy
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

clear hardware rate-limiter

レート制限統計情報をクリアするには、**clear hardware rate-limiter** コマンドを使用します。

clear rate-limiter {**access-list-log** | **all** | **copy** | **layer-2 storm-control** | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**}

シンタックスの説明

access-list-log	アクセス リスト ロギング パケットのレート制限統計情報をクリアします。
all	すべてのレート制限統計情報をクリアします。
copy	コピーパケットのレート制限統計情報をクリアします。
layer-2 storm-control	レイヤ 2 ストーム制御パケットのレート制限統計情報をクリアします。
layer-3	レイヤ 3 パケットのレート制限を指定します。
control	レイヤ 3 制御パケットのレート制限統計情報をクリアします。
glean	レイヤ 3 グリーニング パケットのレート制限統計情報をクリアします。
mtu	レイヤ 3 最大伝送ユニット（maximum transmission unit; MTU）パケットのレート制限統計情報をクリアします。
multicast	レイヤ 3 マルチキャストのレート制限を指定します。
directly-connected	レイヤ 3 マルチキャスト直接接続パケットのレート制限統計情報をクリアします。
local-groups	レイヤ 3 マルチキャスト ローカル グループ パケットのレート制限統計情報をクリアします。
rpf-leak	レイヤ 3 マルチキャスト RPF リーク パケットのレート制限統計情報をクリアします。
ttl	レイヤ 3 Time-to-Live（TTL; 存続可能時間）パケットのレート制限統計情報をクリアします。
receive	受信パケットのレート制限統計情報をクリアします。

デフォルト

なし

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

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルト VDC でのみ使用できます。

このコマンドにライセンスは必要ありません。

例

次に、すべてのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter all
```

次に、アクセス リスト ロギング パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter access-list-log
```

次に、レイヤ 2 ストーム制御パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-2 storm-control
```

次に、レイヤ 3 グリーニング パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-3 glean
```

次に、レイヤ 3 マルチキャスト直接接続パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-3 multicast directly-connected
```

次に、受信パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter receive
```

関連コマンド

コマンド	説明
platform rate-limit	レート制限を設定します。
show hardware rate-limit	レート制限情報を表示します。

clear ip access-list counters

すべてまたは 1 つの IPv4 ACL のカウンタをクリアするには、**clear ip access-list counters** コマンドを使用します。

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

シンタックスの説明

access-list-name	（任意）デバイスがそのカウンタをクリアする IPv4 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。

デフォルト

なし

コマンド モード

特権 EXEC

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)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての IPv4 ACL のカウンタをクリアする例を示します。

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

次に、acl-ipv4-101 という名前の IP ACL のカウンタをクリアする例を示します。

```
switch# clear ip access-list counters acl-ipv4-101
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL および MAC ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL および 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 ACL に関する情報を表示します。

clear ip arp inspection log

Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP 検査）ログ バッファをクリアするには、**clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection 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。

デフォルト なし

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)	このコマンドが導入されました。

使用上のガイドライン このコマンドにライセンスは必要ありません。

例 次に、DAI ログ バッファをクリアする例を示します。

```
switch# clear ip arp inspection log
switch#
```

関連コマンド

コマンド	説明
ip arp inspection log-buffer	DAI ログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection log	DAI ログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。

clear ip arp inspection statistics vlan

指定の VLAN の DAI 統計情報をクリアするには、**clear ip arp inspection statistics vlan** コマンドを使用します。

clear ip arp inspection statistics vlan *vlan-list*

シンタックスの説明

vlan *vlan-list*	このコマンドによってその DAI 統計情報がクリアされる VLAN を指定します。*vlan-list* 引数では、単一の VLAN ID、VLAN ID の範囲、またはカンマで区切った ID と範囲を指定できます（「Examples」セクションを参照）。有効な VLAN ID は、1 ～ 4094 です。

デフォルト

なし

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)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、VLAN 2 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

次に、VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

次に、VLAN 2 および VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ログ バッファをクリアします。
ip arp inspection log-buffer	DAI ログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection vlan	指定リストの VLAN の DAI ステータスを表示します。

clear ip device tracking

IP デバイス トラッキング情報をクリアするには、**clear ip device tracking** コマンドを使用します。

clear ip device tracking {**all** | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*}

シンタックスの説明

all	すべての IP デバイス トラッキング情報をクリアします。
interface ethernet *slot*/*port*	インターフェイスの IP デバイス トラッキング情報をクリアします。
ip-address *ipv4-address*	A.B.C.D 形式の IPv4 アドレスの IP デバイス トラッキング情報をクリアします。
mac-address *mac-address*	XXXX.XXXX.XXXX 形式の MAC アドレスの IP トラッキング情報をクリアします。

デフォルト

なし

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
VDC ユーザ

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking all
```

次に、インターフェイスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking interface ethernet 1/1
```

次に、IP アドレスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking ip-address 10.10.1.1
```

次に、MAC アドレスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking mac-address 000c.30da.86f4
```

関連コマンド

コマンド	説明
ip device tracking	IP デバイス トラッキングをイネーブルにします。
show ip device tracking	IP デバイス トラッキング情報を表示します。

clear ip dhcp snooping binding

DHCP スヌーピング バインディング データベースをクリアするには、**clear ip dhcp snooping binding** コマンドを使用します。

clear ip dhcp snooping binding

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface ethernet** *slot*/*port*[**.***subinterface-number*]]

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface port-channel** *channel-number*[**.***subchannel-number*]]

シンタックスの説明

***vlan** vlan-id*	（任意）*vlan-id* 引数およびその後に続く追加のキーワードと引数によって指定された VLAN ID で識別されるエントリの DHCP スヌーピング バインディング データベースをクリアします。
mac-address *mac-address*	クリアするバインディング データベース エントリの MAC アドレスを指定します。ドット付き 16 進表記で *mac-address* 引数を入力します。
ip *ip-address*	クリアするバインディング データベース エントリの IPv4 アドレスを指定します。ドット付き 10 進表記で *ip-address* 引数を入力します。
***interface ethernet** slot/port*	（任意）クリアするバインディング データベース エントリのイーサネット インターフェイスを指定します。
.subinterface-number	（任意）イーサネット インターフェイスのサブインターフェイスの番号 **（注）** *port* 引数と *subinterface-number* 引数間には、ドット区切り文字が必要です。
***interface port-channel** channel-number*	（任意）クリアするバインディング データベース エントリのイーサネット ポートチャネルを指定します。
.subchannel-number	（任意）イーサネット ポートチャネルのサブチャネルの番号 **（注）** *channel-number* 引数と *subchannel-number* 引数間には、ドット区切り文字が必要です。

デフォルト

なし

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
VDC ユーザ

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	このコマンドは、特定のバインディング データベース エントリのクリアをサポートするように変更されました。オプションの **vlan** キーワードおよびそれに続く引数とキーワードが追加されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、DHCP スヌーピング バインディング データベースをクリアする例を示します。

```
switch# clear ip dhcp snooping binding
switch#
```

次に、DHCP スヌーピング バインディング データベースの特定のエントリをクリアする例を示します。

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9
interface ethernet 2/11
switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイスで 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 ip dhcp snooping binding	スタティック IP ソース エントリを含む、IP-MAC アドレス バインディングを表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

clear mac access-list counters

すべてまたは 1 つの MAC ACL のカウンタをクリアするには、**clear mac access-list counters** コマンドを使用します。

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

シンタックスの説明

access-list-name	（任意）デバイスがそのカウンタをクリアする MAC 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。

デフォルト

なし

コマンド モード

特権 EXEC

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)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての MAC ACL のカウンタをクリアする例を示します。

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

次に、acl-mac-0060 という名前の MAC ACL のカウンタをクリアする例を示します。

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL および MAC ACL のカウンタをクリアします。
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL および MAC ACL に関する情報を表示します。
show mac access-lists	1 つまたはすべての MAC ACL に関する情報を表示します。

clear port-security

動的に学習された単一のセキュア MAC アドレス、または特定のインターフェイスの動的に学習されたすべてのセキュア MAC アドレスをクリアするには、**clear port-security** を使用します。

clear port-security {**dynamic**} {**interface ethernet** *slot*/*port* | **address** *address*} [**vlan** *vlan-id*]

シンタックスの説明

dynamic	動的に学習されたセキュア MAC アドレスをクリアするように指定します。
interface ethernet *slot*/*port*	クリアする対象の動的に学習されたセキュア MAC アドレスのインターフェイスを指定します。
address *address*	クリアする単一の MAC アドレスを指定します。*address* は MAC アドレスです。
vlan *vlan-id*	クリアするセキュア MAC アドレスの VLAN を指定します。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

dynamic

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)	このコマンドが導入されました。

使用上のガイドライン

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してから、**clear port-security** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、動的に学習されたセキュア MAC アドレスをイーサネット 2/1 インターフェイスから削除する例を示します。

```
switch# config t
switch(config)# clear port-security dynamic interface ethernet 2/1
```

次に、動的に学習されたセキュア MAC アドレス 0019.D2D0.00AE を削除する例を示します。

```
switch# config t
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

関連コマンド

コマンド	説明
debug port-security	ポート セキュリティのデバッグ情報を指定します。
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 インターフェイスのポート セキュリティをイネーブルにします。

clear ssh hosts

VDC の Secure Shell（SSH; セキュア シェル）ホスト セッションをクリアするには、**clear ssh hosts** コマンドを使用します。

clear ssh hosts

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 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)	このコマンドが導入されました。

使用上のガイドライン このコマンドにライセンスは必要ありません。

例 次に、すべての SSH ホスト セッションをクリアする例を示します。

```
switch# clear ssh hosts
```

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。

clear user

VDC のユーザ セッションをクリアするには、**clear user** コマンドを使用します。

clear user *user-id*

シンタックスの説明

user-id	ユーザ ID

デフォルト

なし

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)	このコマンドが導入されました。

使用上のガイドライン

デバイスで現在のユーザ セッションを表示するには、**show users** コマンドを使用します。

このコマンドにライセンスは必要ありません。

例

次に、すべての SSH ホスト セッションをクリアする例を示します。

```
switch# clear user user1
```

関連コマンド

コマンド	説明
show users	ユーザ セッション情報を表示します。

cts device-id

Cisco TrustSec デバイス ID を設定するには、**cts device-id** コマンドを使用します。

cts device-id *device-id* **password** [**7**] *password*

シンタックスの説明

device-id	Cisco TrustSec デバイス ID 名。名前には英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。
7	（任意）パスワードを暗号化します。
password *password*	EAP-FAST 処理の間に使用するパスワードを指定します。名前には英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。

デフォルト

Cisco TrustSec デバイス ID はなし
クリア テキスト パスワード

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)	このコマンドが導入されました。

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。

Cisco TrustSec デバイス ID 名は、Cisco TrustSec ネットワーク クラウド内で一意でなければなりません。

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

例

次に、Cisco TrustSec デバイス ID を設定する例を示します。

```
switch# config t
swtich(config)# cts device-id DeviceA password Cisco321
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts credentials	Cisco TrustSec クレデンシャル情報を表示します。

cts dot1x

インターフェイスで Cisco TrustSec 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始するには、**cts dot1x** 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。

cts dot1x

no cts dot1x

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

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)	このコマンドが導入されました。

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後で、**shutdown**/**no shutdown** コマンド シーケンスを使用して、インターフェイスをイネーブルおよびディセーブルにして、設定を有効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、インターフェイスで Cisco TrustSec 認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスで Cisco TrustSec 認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts dot1x
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
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 設定情報を表示します。

cts manual

インターフェイスの Cisco TrustSec 手動設定を開始するには、**cts manual** コマンドを使用します。手動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。

cts manual

no cts manual

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 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)	このコマンドが導入されました。

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後で、**shutdown**/**no shutdown** コマンド シーケンスを使用して、インターフェイスをイネーブルおよびディセーブルにして、設定を有効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、インターフェイスの Cisco TrustSec 手動設定モードを開始する例を示します。

```
switch# config t
switch(config)# interface etherent 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

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

```
switch# config t
switch(config)# interface etherent 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
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 設定情報を表示します。

cts refresh role-based-policy

Cisco Secure ACS からダウンロードした Cisco TrustSec Security Group ACL（SGACL; セキュリティグループ ACL）ポリシーをリフレッシュするには、**cts refresh role-based-policy** コマンドを使用します。

cts refresh role-based-policy

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

任意のコンフィギュレーション 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)	このコマンドが導入されました。

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、インターフェイスの Cisco TrustSec 手動設定モードを開始する例を示します。

```
switch# cts refresh role-based-policy
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based policy	Cisco TrustSec SGACL ポリシー設定を表示します。

cts rekey

Cisco TrustSec ポリシーのインターフェイス キーを再生成するには、**cts rekey** コマンドを使用します

cts rekey ethernet *slot*/*port*

シンタックスの説明

ethernet *slot*/*port*	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

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)	このコマンドが導入されました。

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。

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

例

次に、Cisco TrustSec のインターフェイス キーを再生成する例を示します。

```
switch# cts rekey ethernet 2/3
```

関連コマンド

コマンド	説明
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 設定情報を表示します。

cts role-based access-list

Cisco TrustSec SGACL を作成また指定して、ロールベース ACL コンフィギュレーション モードを開始するには、**cts role-based access-list** コマンドを使用します。SGACL を削除するには、このコマンドの **no** 形式を使用します。

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

シンタックスの説明

list-name	SGACL の名前。名前には英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。

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
4.0(1)	このコマンドが導入されました。

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。

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

例

次に、Cisco TrustSec SGACL を作成して、ロールベース 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 t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

次に、Cisco TrustSec SGACL を削除する例を示します。

```
switch# config t
switch(config)# no cts role-based access-list MySGACL
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL 設定を表示します。

cts role-based enforcement

VLAN または Virtual Routing and Forwarding Instance（VRF; 仮想ルーティング / 転送インスタンス）で Cisco TrustSec SGACL 強制をイネーブルにするには、**cts role-based enforcement** 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。

cts role-based enforcement

no cts role-based enforcement

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

グローバル コンフィギュレーション
VLAN コンフィギュレーション
VRF 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)	このコマンドが導入されました。

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。

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

例

次に、デフォルト VRF で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# config t
switch(config)# cts role-based enforcement
```

次に、VLAN で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# config t
switch(config)# vlan 1
switch(config-vlan)# cts role-based enforcement
```

次に、非デフォルト VRF で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# config t
switch(config)# vrf context MyVRF
switch(config-vrf)# cts role-based enforcement
```

次に、Cisco TrustSec SGACL 強制をディセーブルにする例を示します。

```
switch# config t
switch(config)# no cts role-based enforcement
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based enable	Cisco TrustSec SGACL ポリシー強制の設定を表示します。

cts role-based sgt

SGACL と Cisco TrustSec Security Group Tag（SGT; セキュリティ グループ タグ）のマッピングを手動で設定するには、**cts role-based sgt** コマンドを使用します。SGACL と SGT のマッピングを削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **unknown**}
access-list *list-name*

no cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **unknown**}

シンタックスの説明

sgt-value	送信元 SGT の値。有効範囲は 0 ～ 65533 です。
any	任意の SGT を指定します。
unknown	未知の SGT を指定します。
dgt	宛先 SGT を指定します。
dgt-value	宛先 SGT の値。有効範囲は 0 ～ 65533 です。
access-list *list-name*	SGACL の名前を指定します。

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
4.0(1)	このコマンドが導入されました。

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。

SGT のマッピングを設定する前に SGACL を設定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、SGACL の SGT マッピングを設定する例を示します。

```
switch# config t
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

次に、SGACL の SGT マッピングを削除する例を示します。

```
switch# config t
switch(config)# no cts role-based sgt 3 sgt 10
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based policy	SGACL の Cisco TrustSec SGT マッピングを表示します。

cts role-based sgt-map

IP アドレスと Cisco TrustSec SGT のマッピングを手動で設定するには、**cts role-based sgt-map** コマンドを使用します。SGT を削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt-map *ipv4-address sgt-value*

no cts role-based sgt-map *ipv4-address*

シンタックスの説明

ipv4-address	IPv4 アドレス。形式は、*A.B.C.D* です。
sgt-value	SGT 値。有効範囲は 0 ～ 65533 です。

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
VLAN コンフィギュレーション
VRF 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)	このコマンドが導入されました。

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。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

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

例

次に、Cisco TrustSec SGT のマッピングを設定する例を示します。

```
switch# config t
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config-rbacl)#
```

次に、Cisco TrustSec SGT のマッピングを削除する例を示します。

```
switch# config t
switch(config)# no ccts role-based sgt-map 10.10.1.1
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based sgt-map	Cisco TrustSec SGT のマッピングを表示します。

cts sgt

Cisco TrustSec SGT を設定するには、**cts sgt** コマンドを使用します。

cts sgt *tag*

シンタックスの説明

tag	**0x***hhhh* 形式の 16 進値であるデバイスのローカル SGT。有効範囲は 0x0 ～ 0xffff です。

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
4.0(1)	このコマンドが導入されました。

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。

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

例

次に、デバイスの Cisco TrustSec SGT を設定する例を示します。

```
switch# config t
switch(config)# cts sgt 0x3
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts environment-data	Cisco TrustSec 環境データを表示します。

cts sxp connection peer

Cisco TrustSec の SGT Exchange Protocol（SXP）ピア接続を設定するには、**cts sxp connection peer** コマンドを使用します。SXP 接続を削除するには、このコマンドの **no** 形式を使用します。

cts sxp connection peer *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** [**default** | **none** | **required** *password*] **mode** {**speaker** | **listener**} [**vrf** *vrf-name*]

no cts sxp connection peer *peer-ipv4-addr* [**vrf** *vrf-name*]

シンタックスの説明

peer-ipv4-addr	ピア デバイスの IPv4 アドレス。
source *src-ipv4-addr*	（任意）送信元デバイスの IPv4 アドレスを指定します。
password	SXP 認証に使用するパスワード オプションを指定します。
default	（任意）SXP がデバイスのデフォルト SXP パスワードを使用するように指定します。
none	（任意）SXP がパスワードを使用しないように指定します。
required *password*	（任意）SXP がこのパスワードを使用するように指定します。
mode	ピア デバイスのモードを指定します。
speaker	ピアがスピーカとなるように指定します。
listener	ピアがリスナーとなるように指定します。
vrf *vrf-name*	（任意）ピアの VRF を指定します。

デフォルト

デバイスの設定済みデフォルト SXP パスワード
デバイスの設定済みデフォルト SXP 送信元 IPv4 アドレス
デフォルト VRF

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)	このコマンドが導入されました。

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。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

送信元 IPv4 アドレスを指定しない場合は、**cts sxp default source-ip** コマンドを使用してデフォルト SXP 送信元 IPv4 アドレスを設定する必要があります。

デフォルトをパスワード モードで指定する場合は、**cts sxp default password** コマンドを使用してデフォルト SXP パスワードを設定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、SXP ピア接続を設定する例を示します。

```
switch# config t
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default
mode listener
```

次に、SXP ピア接続を削除する例を示します。

```
switch# config t
switch(config)# no cts sxp connection peer 10.10.1.1
```

関連コマンド

コマンド	説明
cts sxp default password	デバイスのデフォルト SXP パスワードを設定します。
cts sxp default source-ip	デバイスのデフォルト SXP 送信元 IPv4 アドレスを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。

cts sxp default password

デバイスのデフォルト SGT SXP パスワードを設定するには、**cts sxp default password** コマンドを使用します。デフォルトを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password *password*

no cts sxp default password

シンタックスの説明

password	デフォルト SXP パスワード。パスワードには英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。

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
4.0(1)	このコマンドが導入されました。

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。

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

例

次に、デバイスのデフォルト SXP パスワードを設定する例を示します。

```
switch# config t
switch(config)# cts sxp default password Cisco654
```

次に、デフォルト SXP パスワードを削除する例を示します。

```
switch# config t
switch(config)# no cts sxp default password
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp default source-ip

デバイスのデフォルト SGT SXP 送信元 IPv4 アドレスを設定するには、**cts sxp default source-ip** 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。

cts sxp default source-ip *ipv4-address*

no cts sxp default source-ip *ipv4-address*

シンタックスの説明

ipv4-address	デバイスのデフォルト SXP IPv4 アドレス

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
4.0(1)	このコマンドが導入されました。

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。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

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

例

次に、デバイスのデフォルト SXP 送信元 IP アドレスを設定する例を示します。

```
switch# config t
switch(config)# cts sxp default source-ip 10.10.3.3
```

次に、デフォルト SXP 送信元 IP アドレスを削除する例を示します。

```
switch# config t
switch(config)# no cts sxp default source-ip
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp enable

デバイス上の SGT SXP ピアをイネーブルにするには、**cts sxp 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。

cts sxp enable

no cts sxp 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。

デフォルト ディセーブル

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
4.0(1)	このコマンドが導入されました。

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。

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

例 次に、SXP をイネーブルにする例を示します。

```
switch# config t
switch(config)# cts sxp enable
```

次に、SXP をディセーブルにする例を示します。

```
switch# config t
switch(config)# no cts sxp enable
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp reconcile-period

SGT SXP 復帰期間タイマーを設定するには、**cts sxp reconcile-period** 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。

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

シンタックスの説明

seconds	秒数。有効範囲は 0 ～ 64000 秒です。

デフォルト

60 秒（1 分）

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)	このコマンドが導入されました。

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。

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、NX-OS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。

（注） SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

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

例

次に、SXP 復帰期間を設定する例を示します。

```
switch# config t
switch(config)# cts sxp reconcile-period 120
```

次に、SXP 復帰期間をデフォルト値に戻す例を示します。

```
switch# config t
switch(config)# no cts sxp reconcile-period
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP 設定情報を表示します。

cts sxp retry-period

SGT SXP リトライ期間タイマーを設定するには、**cts sxp retry-period** 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。

cts sxp retry-period *seconds*

no cts sxp retry-period

シンタックスの説明

seconds	秒数。有効範囲は 0 ～ 64000 秒です。

デフォルト

120 秒（2 分）

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)	このコマンドが導入されました。

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。

SXP リトライ期間によって、NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。

（注） SXP リトライ期間を 0 秒に設定すると、タイマーがディセーブルになり、再試行は実行されません。

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

例

次に、SXP リトライ期間を設定する例を示します。

```
switch# config t
switch(config)# cts sxp retry-period 120
```

次に、SXP リトライ期間をデフォルト値に戻す例を示します。

```
switch# config t
switch(config)# no cts sxp retry-period
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。