



C コマンド

この章のコマンドは、Cisco MDS 9000 ファミリのマルチレイヤディレクタおよびファブリック スイッチに対応しています。ここでは、コマンドモードに関係なく、すべてのコマンドがアルファベット順に記載されています。各コマンドの適切なモードを確認するには、「[CLI コマンドモードの概要](#)」(p.1-3) を参照してください。詳細については、『*Cisco MDS 9000 Family CLI Configuration Guide*』を参照してください。

callhome

Call Home 機能を設定するには、**callhome** コマンドを使用します。

callhome

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 デイセーブル

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	1.0(2)	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 Call Home 設定コマンドは、(config-callhome) サブモードで使用できます。

Call Home メッセージは、緊急アラームが発生した場合に備えて、サポート スタッフまたは企業の連絡用に使用します。

連絡情報を設定した場合、Call Home 機能をイネーブルにする必要があります。操作を開始するために、Call Home 機能には **enable** コマンドが必要です。Call Home 機能をディセーブルにした場合、すべての入力イベントが無効となります。



(注) Call Home 機能をディセーブルにしている場合でも、各 Call Home イベントの基本的な情報は Syslog に送信されます。

user-def-cmd コマンドを使用すると、Call Home メッセージにコマンドによる出力を添付してから送信するようコマンドを定義できます。指定できるのは **show** コマンドだけであり、アラートグループと関連付ける必要があります。1 つアラートグループに 5 つのコマンドを指定できます。無効なコマンドは拒否されます。



(注) カスタマイズした **show** コマンドは、フルテキストおよび XML アラートグループに対してのみサポートされます。ショートテキストのアラートグループ (short-txt-destination) では、128 バイトのテキストのみ使用できるため、カスタマイズした **show** コマンドはサポートされません。

アラートの送信時に **show** コマンドを実行するように指定するには、コマンドとアラートグループを関連付けてください。アラートが送信されると、Call Home はアラートグループとアラートタイプを関連付け、**show** コマンドの出力をアラートメッセージに添付します。



(注) non-Cisco-TAC アラートグループ用の宛先ファイルに、事前に定義された **show** コマンドが指定されていて、Cisco-TAC アラートグループとは異なることを確認してください。

次に、連絡情報を割り当てる例を示します。

```
switch# config terminal
config terminal
switch# snmp-server contact personname@companyname.com
switch(config)# callhome
switch(config-callhome)# email-contact username@company.com
switch(config-callhome)# phone-contact +1-800-123-4567
switch(config-callhome)# streetaddress 1234 Picaboo Street, Any city, Any state,
12345
switch(config-callhome)# switch-priority 0
switch(config-callhome)# customer-id Customer1234
switch(config-callhome)# site-id Site1ManhattanNY
switch(config-callhome)# contract-id Company1234
```

次に、アラート グループ ライセンス用のユーザ定義の **show** コマンドを設定する例を示します。

```
switch(config-callhome)# alert-group license user-def-cmd "show license usage"
```



(注)

show コマンドを二重引用符で囲む必要があります。

次に、アラート グループ ライセンス用のユーザ定義の **show** コマンドを削除する例を示します。

```
switch(config-callhome)# no alert-group license user-def-cmd "show license usage"
```

関連コマンド

コマンド	説明
alert-group	ユーザ定義の show コマンドにより Call Home アラート グループをカスタマイズします。
callhome test	ダミーのテスト メッセージを設定された 1 つまたは複数の宛先へ送信します。
show callhome	設定された Call Home 情報を表示します。

callhome test

Call Home メッセージの生成をシミュレートするには、**callhome test** コマンドを使用します。

callhome test [inventory]

シンタックスの説明	inventory	ダミーの Call Home インベントリを送信します。
------------------	------------------	------------------------------

デフォルト	なし
--------------	----

コマンドモード	EXEC モード
----------------	----------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン **callhome test** コマンドで、メッセージの生成をシミュレートできます。

例 次に、設定された 1 つまたは複数の宛先へテスト メッセージを送信する例を示します。

```
switch# callhome test
trying to send test callhome message
successfully sent test callhome message
```

次に、設定された 1 つまたは複数の宛先へテスト インベントリ メッセージを送信する例を示します。

```
switch# callhome test inventory
trying to send test callhome message
successfully sent test callhome message
```

関連コマンド	コマンド	説明
	callhome	Call Home 機能を設定します。
	show callhome	設定された Call Home 情報を表示します。

cd

デフォルト ディレクトリまたはファイル システムを変更するには、**cd** コマンドを使用します。

```
cd {directory | bootflash:[directory] | slot0:[directory] | volatile:[directory]}
```

シンタックスの説明

<i>directory</i>	ファイル システム上のディレクトリ名
bootflash:	ファイル システム上のブートフラッシュの URI またはエイリアス
slot0:	スロット 0 ファイル システムの URI またはエイリアス
volatile:	volatile ファイル システムの URI またはエイリアス

デフォルト

初期のデフォルト ファイル システムは、flash: です。flash: という名前がついた物理的なデバイスがないプラットフォームの場合、flash: キーワードというエイリアスがデフォルトのフラッシュ デバイスになります。

ファイル システムにディレクトリを指定しない場合、デフォルトはそのファイル システムのルート ディレクトリとなります。

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。

使用上のガイドライン

任意のファイル システム引数を持つすべての EXEC コマンドの場合、任意のファイル システム引数が省略されると、**cd** コマンドに指定されたファイル システムが使用されます。たとえば、ファイル システムのファイル リストを表示する **dir** コマンドには、任意のファイル システム引数が含まれます。この引数を省略した場合、システムは **cd** コマンドに指定されたファイル システムのファイルを一覧表示します。

例

次に、デフォルト ファイル システムに、slot0: に挿入されたフラッシュ メモリ カードを設定する例を示します。

```
switch# pwd
bootflash:/
switch# cd slot0:
switch# pwd
slot0:/
```

関連コマンド

コマンド	説明
copy	コピー元からコピー先へファイルをコピーします。
delete	フラッシュ メモリ デバイスのファイルを削除します。
dir	ファイル システムのファイルの一覧を表示します。
pwd	cd コマンドの現在の設定を表示します。
show file systems	使用できるファイル システムおよびそのエイリアス プレフィクス名を一覧表示します。
undelete	クラス A またはクラス B のフラッシュ ファイル システム上で削除されたファイルを復元します。

cdp

Cisco Discovery Protocol (CDP) のパラメータをグローバルに設定するには、**cdp** コマンドを使用します。工場出荷時の設定に戻すには、このコマンドの **no** 形式を使用します。

```
cdp {enable | advertise {v1 | v2} | holdtime holdtime-seconds | timer timer-seconds}
```

```
no cdp {enable | advertise | holdtime holdtime-seconds | timer timer-seconds}
```

シンタックスの説明	enable	スイッチ上のすべてのインターフェイスで CDP をグローバルにイネーブルにします。
	advertise	実行する EXEC コマンドを指定します。
	v1	CDP バージョン 1 を指定します。
	v2	CDP バージョン 2 を指定します。
	holdtime	CDP パケットでアドバタイズされるホールドタイムを設定します。
	holdtime-seconds	ホールドタイムを秒で指定します。デフォルトは 180 秒です。有効範囲は 10 ~ 255 秒です。
	timer	リフレッシュ タイム インターバルを設定します。
	timer-seconds	インターバル時間を秒で指定します。デフォルトは 60 秒です。有効範囲は 5 ~ 255 秒です。

デフォルト

CDP はイネーブルです。

ホールドタイムのデフォルトのインターバルは、180 秒です。

リフレッシュ タイム インターバルは 60 秒です。

コマンド モード

コンフィギュレーション モード

コマンド履歴

リリース	変更内容
1.1(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

cdp enable コマンドは、CDP 機能をスイッチ レベルまたはインターフェイス レベルでイネーブルにします。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。インターフェイス リンクが確立されると、CDP はデフォルトでイネーブルになります。

CDP バージョン 1 (v1) およびバージョン 2 (v2) が、Cisco MDS 9000 ファミリ スイッチでサポートされています。他のバージョン番号を持つ CDP パケットは、受信時にそのまま廃棄されます。

例 次に、スイッチの CDP プロトコルをディセーブルにする例を示します。インターフェイスで CDP がディセーブルになると、1つのパケットが送信され、各受信デバイスのスイッチの状態を消去します。

```
switch(config)# no cdp enable
Operation in progress. Please check global parameters
switch(config-console)#
The following example enables (default) the CDP protocol on the switch. When CDP is
enabled on an interface, one packet is sent immediately. Subsequent packets are sent
at the configured refresh time
switch(config)# cdp enable
Operation in progress. Please check global parameters
switch(config)#
```

次に、ギガビット イーサネット インターフェイス 8/8 を設定して、このインターフェイスの CDP プロトコルをディセーブルにする例を示します。インターフェイスで CDP がディセーブルになると、1つのパケットが送信され、各受信デバイスのスイッチの状態を消去します。

```
switch(config)# interface gigbitethernet 8/8
switch(config-if)# no cdp enable
Operation in progress. Please check interface parameters
switch(config-console)#
```

次に、選択したインターフェイスの CDP プロトコルをイネーブル (デフォルト) にする例を示します。CDP がこのインターフェイスでイネーブルになると、1つのパケットが直ちに送信されます。後続のパケットは、設定されたリフレッシュ タイムに合わせて送信されます。

```
switch(config-if)# cdp enable
Operation in progress. Please check interface parameters
switch(config)#
```

次に、CDP プロトコルのリフレッシュ タイム インターバル (秒) をグローバルに設定する例を示します。デフォルトは 60 秒です。有効範囲は 5 ~ 255 秒です。

```
switch# config terminal
switch(config)# cdp timer 100
switch(config)#
```

次に、CDP パケットでアドバタイズされたホールド タイム (秒) をグローバルに設定する例を示します。デフォルトは 180 秒です。有効範囲は 10 ~ 255 秒です。

```
switch# config terminal
switch(config)# cdp holdtime 200
switch(config)#
```

次に、CDP バージョンをグローバルに設定する例を示します。デフォルトのバージョンは 2 (v2) です。有効なオプションは v1 および v2 です。

```
switch# config terminal
switch(config)# cdp advertise v1
switch(config)#
```

関連コマンド

コマンド	説明
clear cdp	グローバルまたはインターフェイス特定の CDP 設定を消去します。
show cdp	構成された CDP 設定およびパラメータを表示します。

cfs distribute

スイッチの Cisco Fabric Services (CFS) 配信をイネーブルまたはディセーブルにするには、コンフィギュレーション モードで **cfs distribute** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

cfs distribute

no cfs distribute

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 CFS 配信はイネーブルです。

コマンド モード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	2.1(1a)	このコマンドが導入されました。

使用上のガイドライン デフォルト設定では、CFS が配信モードになっています。また、配信モードでは、ファブリック全体の配信がイネーブルです。アプリケーションは、自身のファブリック内の CFS に対応したすべてのスイッチにデータまたは設定を配信できます。この設定が操作の通常モードです。

CFS 配信がディセーブルのときに、**no cfs distribute** コマンドを使用すると、次の問題が発生します。

- スwitchの CFS および CFS を使用するアプリケーションは、物理的な接続があったとしても残りのファブリックから隔離されます。
- すべての CFS の操作は隔離されたスイッチに制限されます。
- すべての CFS コマンドは、スイッチが物理的に隔離されたかのように機能し続けます。
- 他のスイッチで実行された他の CFS の操作（たとえば、ロック、確定、廃棄）は、隔離されたスイッチにはまったく反映されません。
- ファイバチャネルおよび IP の両方を介した CFS 配信がディセーブルになります。

例 次に、CFS 配信をディセーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no cfs distribute
```

次に、CFS 配信を再度イネーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs distribute
```

関連コマンド	コマンド	説明
	show cfs status	CFS 配信がイネーブルかディセーブルかを表示します。

cfs ipv4 distribute

この機能を使用するアプリケーション向けに IPv4 を介した Cisco Fabric Services (CFS) 配信をイネーブルにするには、コンフィギュレーションモードで **cfs ipv4** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

cfs ipv4 distribute

no cfs ipv4 distribute

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 CFS 配信はイネーブルです。
CFS over IP はディセーブルです。

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(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 同様のマルチキャストアドレスを持つすべての CFS over IP 対応スイッチにより、1 つの CFS over IP ファブリックが構成されます。ネットワーク トポロジの変更を検知するためのキープアライブメカニズムといった CFS プロトコル特有の配信では、IP マルチキャストアドレスを使用して情報の送受信を行います。

このコマンドを使用する場合は、次の注意事項に従ってください。

- IP およびファイバチャネルの両方を介してスイッチに到達可能である場合、アプリケーションデータはファイバチャネルを介して配信されます。
- IP を介した CFS がイネーブルになっている場合は IPv4 配信または IPv6 配信のどちらかを選択できます。
- 同じスイッチ上で IPv6 配信および IPv4 配信の両方をイネーブルにすることはできません。
- IPv4 配信がイネーブルになっているスイッチは、IPv6 配信がイネーブルになっているスイッチを検知できません。これらのスイッチは互いに接続していても、2 つの別々のファブリックに存在するかのように動作します。

例 次に、CFS IPv4 配信をディセーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no cfs ipv4 distribute
This will prevent CFS from distributing over IPv4 network.
Are you sure? (y/n) [n]
```

次に、CFS IPv4 配信を再度イネーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs ipv4 distribute
```

関連コマンド	コマンド	説明
	cfs ipv4 mcast-address	IPv4 を介した CFS 配信の IPv4 マルチキャストアドレスを設定します。
	show cfs status	CFS 配信がイネーブルかディセーブルかを表示します。

cfs ipv4 mcast-address

IPv4 を介した Cisco Fabric Services (CFS) 配信の IPv4 マルチキャストアドレスを設定するには、コンフィギュレーションモードで **cfs ipv4 mcast-address** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
cfs ipv4 mcast-address ipv4-address
```

```
no cfs ipv4 mcast-address ipv4-address
```

シンタックスの説明	ipv4-address	説明
		IPv4 を介した CFS 配信の IPv4 マルチキャストアドレスを設定します。有効な IPv4 アドレスの範囲は、239.255.0.0 から 239.255.255.255 と、239.192.0.0 から 239.251.251.251 です。

デフォルト	マルチキャストアドレス : 239.255.70.83.

コマンドモード	コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(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前に、**cfs ipv4 distribute** コマンドを使用して IPv4 を介した CFS 配信をイネーブルにします。

同様のマルチキャストアドレスを持つすべての CFS over IP 対応スイッチにより、1 つの CFS over IP ファブリックが構成されます。ネットワーク トポロジの変更を検知するためのキープアライブメカニズムといった CFS プロトコル特有の配信では、IP マルチキャストアドレスを使用して情報の送受信を行います。



(注) アプリケーションデータの CFS 配信には、ダイレクトユニキャストを使用します。

CFS over IP マルチキャストアドレスの値を設定できます。デフォルトの IPv4 マルチキャストアドレスは 239.255.70.83 です。

例 次に、CFS over IPv4 の IP マルチキャストアドレスを設定する例を示します。

```
switch# config t
switch(config)# cfs ipv4 mcast-address 239.255.1.1
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

次に、IPv4 を介した CFS 配信のデフォルト IPv4 マルチキャストアドレスに戻す例を示します。CFS のデフォルトの IPv4 マルチキャストアドレスは 239.255.70.83 です。

```
switch(config)# no cfs ipv4 mcast-address 10.1.10.100
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure?(y/n) [n] y
```

関連コマンド

コマンド	説明
<code>cfs ipv4 distribute</code>	IPv4 を介した CFS 配信をイネーブルまたはディセーブルにします。
<code>show cfs status</code>	CFS 配信がイネーブルかディセーブルかを表示します。

cfs ipv6 distribute

この機能を使用するアプリケーション向けに IPv6 を介した Cisco Fabric Services (CFS) 配信をイネーブルにするには、コンフィギュレーションモードで **cfs ipv6 distribute** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

cfs ipv6 distribute

no cfs ipv6 distribute

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 CFS 配信はイネーブルです。
CFS over IP はディセーブルです。

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(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 同様のマルチキャストアドレスを持つすべての CFS over IP 対応スイッチにより、1 つの CFS over IP ファブリックが構成されます。ネットワーク トポロジの変更を検知するためのキープアライブメカニズムといった CFS プロトコル特有の配信では、IP マルチキャストアドレスを使用して情報の送受信を行います。

このコマンドを使用する場合は、次の注意事項に従ってください。

- IP およびファイバチャネルの両方を介してスイッチに到達可能である場合、アプリケーションデータはファイバチャネルを介して配信されます。
- IP を介した CFS がイネーブルになっている場合は IPv4 配信または IPv6 配信のどちらかを選択できます。
- 同じスイッチ上で IPv6 配信および IPv4 配信の両方をイネーブルにすることはできません。
- IPv4 配信がイネーブルになっているスイッチは、IPv6 配信がイネーブルになっているスイッチを検知できません。これらのスイッチは互いに接続していても、2 つの別々のファブリックに存在するかのように動作します。

例 次に、CFS IPv6 配信をディセーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# no cfs ipv6 distribute
This will prevent CFS from distributing over IPv6 network.
Are you sure? (y/n) [n]
```

次に、CFS IPv6 配信を再度イネーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs ipv6 distribute
```

関連コマンド	コマンド	説明
	<code>cfs ipv6 mcast-address</code>	IPv6 を介した CFS 配信の IPv6 マルチキャストアドレスを設定します。
	<code>show cfs status</code>	CFS 配信がイネーブルかディセーブルかを表示します。

cfs ipv6 mcast-address

IPv6 を介した Cisco Fabric Services (CFS) 配信の IPv6 マルチキャストアドレスを設定するには、コンフィギュレーションモードで **cfs ipv6 mcast-address** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
cfs ipv6 mcast-address ipv6-address
```

```
no cfs ipv6 mcast-address ipv6-address
```

シンタックスの説明	<code>ipv6-address</code>	IPv6 を介した CFS 配信の IPv6 マルチキャストアドレスを設定します。IPv6 管理スコープ範囲は [ff15::/16, ff18::/16] です。
-----------	---------------------------	--

デフォルト マルチキャストアドレス : ff15::efff:4653.

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(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前に、**cfs ipv6 distribute** コマンドを使用して IPv6 を介した CFS 配信をイネーブルにします。

同様のマルチキャストアドレスを持つすべての CFS over IP 対応スイッチにより、1 つの CFS over IP ファブリックが構成されます。ネットワーク トポロジの変更を検知するためのキープアライブメカニズムといった CFS プロトコル特有の配信では、IP マルチキャストアドレスを使用して情報の送受信を行います。



(注) アプリケーションデータの CFS 配信には、ダイレクトユニキャストを使用します。

IPv6 の CFS over IP マルチキャストアドレスの値を設定できます。デフォルトの IPv6 マルチキャストアドレスは ff15::efff:4653 です。IPv6 管理スコープ範囲の例は、ff15::0000:0000 から ff15::ffff:ffff または ff18::0000:0000 から ff18::ffff:ffff です。

例

次に、CFS over IPv6 の IP マルチキャスト アドレスを設定する例を示します。

```
switch# config t
switch(config)# cfs ipv6 mcast-address ff13::e244:4754
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

次に、IPv6 を介した CFS 配信のデフォルト IPv6 マルチキャスト アドレスに戻す例を示します。CFS のデフォルトの IPv6 マルチキャスト アドレスは ff13:7743:4653 です。

```
switch(config)# no cfs ipv6 ff13::e244:4754
Distribution over this IP type will be affected
Change multicast address for CFS-IP ?
Are you sure? (y/n) [n] y
```

関連コマンド

コマンド	説明
cfs ipv6 distribute	IPv6 を介した CFS 配信をイネーブルまたはディセーブルにします。
show cfs status	CFS 配信がイネーブルかディセーブルかを表示します。

cfs region

領域を作成してアプリケーション配信の範囲を選択したスイッチに制限するには、コンフィギュレーション モードで **cfs region** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

cfs region region-id

no cfs region region-id

シンタックスの説明	<i>region-id</i>	アプリケーションを領域に割り当てます。合計で 200 のリージョンがサポートされます。
デフォルト	なし	
コマンドモード	コンフィギュレーションモード	
コマンド履歴	リリース	変更内容
	3.2(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 1 つのアプリケーションは、指定したスイッチ上の 1 つの領域にしか属することができません。領域 ID を作成してそれをアプリケーションに適用することで、アプリケーション配信は同様の ID を持つスイッチに制限されます。

Cisco Fabric Services (CFS) 領域により、アプリケーション スコープから孤立した配信領域を作成することができます。現在、領域は物理的なスコープ アプリケーションに対してのみサポートされます。領域の設定が行われていない場合、アプリケーションはデフォルト領域に属します。デフォルトの領域の領域 ID は 0 です。このコマンドにより、領域がサポートされていなかった旧リリースとの互換性が保たれます。アプリケーションがある領域に割り当てられている場合は、コンフィギュレーション チェックによりダウングレードが発生しないようにします。Fabric Manager は CFS 領域をサポートします。

例 次に、領域 ID を作成する例を示します。

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs region 1
```

次に、領域にアプリケーションを割り当てる例を示します。

```
switch# cfs region 1
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs region 1
switch(config-cfs-region)# ntp
```



(注) 領域に割り当てられたアプリケーションは、CFS に登録する必要があります。

次に、領域に割り当てられているアプリケーションを削除する例を示します。

```
switch# cfs region 1
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cfs region 1
switch(config-cfs-region)# no ntp
```

The following example shows how to remove all the applications from a region.

```
switch(config)# no cfs region 1
WARNING: All applications in the region will be moved to default region.
Are you sure? (y/n) [n] y
```

関連コマンド

コマンド	説明
show cfs regions	全設定済アプリケーションとピアを表示します。

channel mode active

ポートチャネル インターフェイスでチャンネル モードをイネーブルにするには、**channel mode active** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

channel mode active

no channel mode

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 イネーブル

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 サブモード

コマンド履歴	リリース	変更内容
	2.0(x)	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、ポート チャネル インターフェイスに関連付けられたチャンネル グループのすべてのメンバー ポートのプロトコル動作を決定します。

例 次に、ポートチャネル インターフェイスでチャンネルをディセーブルにする例を示します。

```
switch# config terminal
switch(config)# interface port-channel 10
switch(config-if)# no channel mode active
```

関連コマンド	コマンド	説明
	show interface port-channel	ポートチャネル インターフェイス情報を表示します。

channel-group

ポートチャネル グループにポートを追加するには、**channel-group** コマンドを使用します。ポートを削除するには、コマンドの **no** 形式を使用します。

```
channel-group {port-channel-number force | auto}
```

```
no channel-group {port-channel-number force | auto}
```

シンタックスの説明	
<i>port-channel-number</i>	ポートチャネル番号を指定します。有効範囲は1～256です。
force	ポートの追加時に force オプションを使用することを指定します。
auto	ポートチャネルの自動作成をイネーブルにします。

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 サブモード

コマンド履歴	リリース	変更内容
	3.0(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 なし

例 次に、ポートチャネルの自動作成をイネーブルにする例を示します。

```
switch# config terminal
switch(config)# interface fc3/9
switch(config-if)# channel-group auto
```

関連コマンド	コマンド	説明
	show interface port-channel	ポートチャネル インターフェイス情報を表示します。

cimserver

Common Information Model (CIM) パラメータを設定するには、**cimserver** コマンドを使用します。工場出荷時の設定に戻すには、このコマンドの **no** 形式を使用します。

```
cimserver
  {certificate {bootflash:filename | slot0:filename | volatile:filename} |
  clearcertificate filename |
  enable |
  enablehttp |
  enablehttps}

no cimserver
  {certificate {bootflash:filename | slot0:filename | volatile:filename} |
  clearcertificate filename
  enable
  enablehttp
  enablehttps}
```

シンタックスの説明

certificate	Secure Socket Layer (SSL) 証明書をインストールします。
bootflash:	内部ブートフラッシュ メモリの場所を指定します。
slot0:	コンパクトフラッシュ メモリまたは PCMCIA カードの場所を指定します。
volatile:	揮発性ファイル システムの場所を指定します。
filename	.pem という拡張子の付いたライセンス ファイルの名前です。
clearcertificate	以前インストールした SSL 証明書を消去します。
enable	CIM サーバをイネーブルにして開始します。
enablehttp	CIM サーバの HTTP (非セキュア) プロトコルをイネーブルにします — (デフォルト)。
enablehttps	CIM サーバの HTTPS (セキュア) プロトコルをイネーブルにします。

デフォルト

なし

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
1.3(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

CIM クライアントは、CIM サーバにアクセスする必要があります。CIM をサポートするクライアントなら、どれでもクライアントになることができます。

例

次に、.pem 拡張子の付いた名前のファイルで指定された SSL 証明書をインストールする例を示します。

```
switch# config terminal
switch(config)# cimserver certificateName bootflash:simserver.pem
```

次に、指定した SSL 証明書を消去する例を示します。

```
switch(config)# cimserver clearCertificateName bootflash:simserver.pem
```

次に、HTTPS (セキュア プロトコル) をイネーブルにする例を示します。

```
switch(config)# cimserver enablehttps
```

次に、HTTPS をディセーブルにする (デフォルト) 例を示します。

```
switch(config)# no cimserver enablehttps
```

次に、CIM サーバをイネーブルにする例を示します。

```
switch(config)# cimserver enable
```

次に、CIM サーバをディセーブルにする (デフォルト) 例を示します。

```
switch(config)# no cimserver enable
```

次に、HTTP をイネーブルにしてスイッチ デフォルトに戻す例を示します。

```
switch(config)# cimserver enablehttp
```

次に、HTTP をディセーブルにしてスイッチ デフォルトに戻す例を示します。

```
switch(config)# no cimserver enablehttp
```

関連コマンド

コマンド	説明
show csimserver	設定した CIM の設定およびパラメータを表示します。

cimserver clearcertificate

cimserver 証明書を消去するには、コンフィギュレーション モードで **cimserver clearcertificate** コマンドを使用します。

cimserver clearcertificate

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 コンフィギュレーション モード

リリース	変更内容
3.3(1a)	このコマンドが導入されました。

使用上のガイドライン 証明書の名前は指定する必要がありません。

例 次に、cimserver 証明書を消去する例を示します。

```
switch# config  
Enter configuration commands, one per line. End with CNTL/Z.  
switch(config)# cimserver clearcertificate
```

コマンド	説明
show cimserver certificate name	cimserver 証明書ファイル名を表示します。

cimserver loglevel

cimserver のログレベルでのフィルタを設定するには、コンフィギュレーション モードで **cimserver loglevel** コマンドを使用します。

cimserver loglevel *filter value*

シンタックスの説明	<i>filter value</i>	cimserver ログ フィルタ レベルを指定します。有効範囲は 1 ~ 5 です。
	1	loglevel プロパティの現在値を trace (追跡) に設定します。
	2	loglevel プロパティの現在値を information (情報) に設定します。
	3	loglevel プロパティの現在値を warning (警告) に設定します。
	4	loglevel プロパティの現在値を severe (重大) に設定します。
	5	loglevel プロパティの現在値を fatal (致命的) に設定します。

デフォルト なし

コマンドモード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	3.3(1a)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、cimserver のログレベルの例を示します。

```
switch# config
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cimserver loglevel 2
Current value for the property logLevel is set to "INFORMATION" in CIMServer.
```

関連コマンド	コマンド	説明
	show cimserver logs	cimserver ログを表示します。

class

設定で、Quality of Service (QoS; サービス品質) ポリシー マップ クラスを選択するには、QoS ポリシー マップ コンフィギュレーション サブモードで **class** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
class class-map-name
```

```
no class class-map-name
```

シンタックスの説明	<i>class-map-name</i>	設定する QoS ポリシー クラス マップ を選択します。
-----------	-----------------------	-------------------------------

デフォルト	ディセーブル
-------	--------

コマンド モード	QoS ポリシー マップ コンフィギュレーション サブモード
----------	--------------------------------

コマンド履歴	リリース	変更内容
	1.3(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 QoS ポリシー マップ クラスを設定する前に、次の内容を実行してください。

- **qos enable** コマンドを使用して QoS データ トラフィック機能をイネーブルにする。
- **qos class-map** コマンドを使用して QoS クラス マップを設定します。
- **qos policy-map** コマンドを使用して QoS ポリシー マップを設定する。

QoS ポリシー マップ クラスの設定後には、Differentiated Services Code Point (DSCP) およびこのクラス マップと照合するフレームのプライオリティを設定できます。

例 次に、作成する QoS ポリシー マップ クラスを選択する例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# qos enable
switch(config)# qos class-map class-map1
switch(config)# qos policy-map policyMap1
switch(config-pmap)# class class-map1
switch(config-pmap-c)#
```

関連コマンド	コマンド	説明
	qos enable	スイッチの QoS データ トラフィック機能をイネーブルにします。
	qos class-map	QoS クラス マップを設定します。
	qos policy-map	QoS ポリシー マップを設定します。
	dscp	QoS ポリシー マップ クラスの DSCP を設定します。
	priority	QoS ポリシー マップ クラスのプライオリティを設定します。
	show qos	現在の QoS 設定を表示します。

clear accounting log

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

clear accounting log

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、アカウントティング ログを消去する例を示します。

```
switch# clear accounting session
```

関連コマンド	コマンド	説明
	show accounting log	アカウントティング ログの内容を表示します。

clear arp-cache

Address Resolution Protocol (ARP) キャッシュ テーブルのエントリを消去するには、EXEC モードで **clear arp-cache** コマンドを使用します。

clear arp-cache

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 ARP テーブルはデフォルトで空になっています。

コマンド モード EXEC モード

リリース	変更内容
1.0(2)	このコマンドが導入されました。

例 次に、ARP キャッシュ テーブル エントリを消去する例を示します。

```
switch# clear arp-cache
```

コマンド	説明
show arp	ARP エントリを表示します。

clear callhome session

Call Home の Cisco Fabric Services (CFS) セッション コンフィギュレーションおよびロックを消去するには、**clear callhome session** コマンドを使用します。

clear callhome session

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、Call Home セッション コンフィギュレーションおよびロックを消去する例を示します。

```
switch# clear callhome session
```

関連コマンド	コマンド	説明
	show callhome	Call Home 情報を表示します。

clear cdp

グローバルまたはインターフェイス特定の Cisco Discovery Protocol (CDP) 設定を削除するには、**clear cdp** コマンドを使用します。

```
clear cdp {counters | table} [interface {gigabitethernet slot/port | mgmt 0}]
```

シンタックスの説明		
counters		CDP をグローバルに、またはインターフェイス ベースごとにイネーブルにします。
table		実行する EXEC コマンドを指定します。
interface		インターフェイスの CDP パラメータを表示します。
gigabitethernet		ギガビット イーサネット インターフェイスを指定します。
<i>slot/port</i>		スロット番号およびポート番号をスラッシュ (/) で区切り、指定します。
mgmt 0		イーサネット管理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 コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	1.1(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、指定のインターフェイスまたはすべてのインターフェイス（管理およびギガビットイーサネットインターフェイス）に対して実行できます。

例 次に、すべてのインターフェイスの CDP トラフィック カウンタを消去する例を示します。

```
switch# clear cdp counters
switch#
```

次に、指定のギガビットイーサネットインターフェイスの CDP エントリを消去する例を示します。

```
switch# clear cdp table interface gigabitethernet 4/1
switch#
```

関連コマンド	コマンド	説明
	cdp	グローバルまたはインターフェイス特定の CDP 設定およびパラメータを設定します。
	show cdp	構成された CDP 設定およびパラメータを表示します。

clear cores

スイッチのすべてのコア ダンプを消去するには、EXEC モードで **clear cores** コマンドを使用します。

clear cores

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン システム ソフトウェアは、サービスおよびスロットごとに、最新のコアを 2、3 保持して、アクティブ スーパーバイザ モジュールに存在する他のすべてのコアを消去します。

例 次に、スイッチのすべてのコア ダンプを消去する例を示します。

```
switch# clear cores
```

関連コマンド	コマンド	説明
	show cores	作成されたコア ダンプを表示します。

clear counters (EXEC mode)

インターフェイス カウンタを消去するには、EXEC モードで **clear counters** コマンドを使用します。

```
clear counters {all | interface {fc | mgmt | port-channel | sup-fc | vsan} number}
```

シンタックスの説明		
all		すべてのインターフェイス カウンタを消去します。
interface		指定のインターフェイスのインターフェイス カウンタを消去します。
type		インターフェイス タイプを指定します。「使用上の注意事項」のキーワード テーブルを参照してください。
number		消去するスロット番号またはインターフェイス番号を指定します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン 次のテーブルに、**clear counters** インターフェイス タイプのキーワードおよび番号の範囲を示します。

キーワード	インターフェイス タイプ	番号
<i>fc</i>	ファイバチャネル	1～2 または 1～9 (スロット)
<i>gigabitethernet</i>	ギガビット イーサネット	1～2 または 1～9 (スロット)
<i>mgmt</i>	管理	0-0 (管理インターフェイス)
<i>port-channel</i>	ポートチャネル	1～128 (ポートチャネル)
<i>sup-fc</i>	帯域内	0-0 (帯域内インターフェイス)
<i>vsan</i>	VSAN	1～4093 (VSAN ID)

このコマンドは、**show interface** コマンドの出力に表示されるカウンタを消去します。

例 次に、VSAN (仮想 SAN) インターフェイスのカウンタを消去する例を示します。

```
switch# clear counters interface vsan 13
```

関連コマンド	コマンド	説明
	show interface	インターフェイス情報を表示します。

clear counters (SAN extension N port configuration mode)

SAN 拡張チューナー N ポート カウンタを消去するには、**clear counters** コマンドを使用します。

```
clear counters
```

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 SAN 拡張 N ポート コンフィギュレーション サブモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、SAN 拡張チューナー N ポート カウンタを消去する例を示します。

```
switch# san-ext-tuner
switch(san-ext)# nwwn 10:00:00:00:00:00:00:00
switch(san-ext)# nport pwwn 12:00:00:00:00:00:00:56 vsan 13 interface gigabitethernet
1/2
switch(san-ext-nport)# clear counters
```

関連コマンド	コマンド	説明
	show san-ext-tuner	SAN 拡張チューナー情報を表示します。

clear crypto ike domain ipsec sa

Internet Protocol Security (IPSec) の Internet Key Exchange (IKE) トンネルを消去するには、**clear crypto ike domain ipsec sa** コマンドを使用します。

```
clear crypto ike domain ipsec sa [tunnel-id]
```

シンタックスの説明	<i>tunnel-id</i>	トンネル ID を指定します。範囲は 1 ~ 2147483647 です。
-----------	------------------	---------------------------------------

デフォルト	なし
-------	----

コマンドモード	EXEC モード
---------	----------

コマンド履歴	リリース	変更内容
	2.0(x)	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、**crypto ike enable** コマンドを使用して IKE プロトコルをイネーブルにする必要があります。

トンネル ID が指定されていない場合、すべての IKE トンネルが消去されます。

例 次に、すべての IKE トンネルを消去する例を示します。

```
switch# clear crypto ike domain ipsec sa
```

関連コマンド	コマンド	説明
	crypto ike domain ipsec	IKE 情報を設定します。
	crypto ike enable	IKE プロトコルをイネーブルにします。
	show crypto ike domain ipsec	IPSec ドメインの IKE 情報を表示します。

clear crypto sa domain ipsec

Internet Protocol Security (IPSec) のセキュリティ アソシエーションを消去するには、**clear crypto sa domain ipsec** コマンドを使用します。

```
clear crypto sa domain ipsec interface gigabitethernet slot/port {inbound | outbound} sa sa-index
```

シンタックスの説明		
interface gigabitethernet <i>slot/port</i>		ギガビットイーサネットインターフェイスを指定します。
inbound		消去する入力アソシエーションを指定します。
outbound		消去する出力アソシエーションを指定します。
sa sa-index		セキュリティ アソシエーション インデックスを指定します。有効範囲は 1 ~ 2147483647 です。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン セキュリティ アソシエーションを消去するには、**crypto ipsec enable** コマンドを使用して IPSec をイネーブルにする必要があります。

例 次に、インターフェイスのセキュリティ アソシエーションを消去する例を示します。

```
switch# clear crypto sa domain ipsec interface gigabitethernet 1/2 inbound sa 1
```

関連コマンド	コマンド	説明
	show crypto sad domain ipsec	IPSec セキュリティ アソシエーション データベース情報を表示します。

clear debug-logfile

デバッグ ログファイルを削除するには、EXEC モードで **clear debug-logfile** コマンドを使用します。

clear debug-logfile *filename*

シンタックスの説明	<i>filename</i>	消去するログファイル名（最大 80 文字）です。ログ ファイルの最大サイズは、1024 バイトです。
-----------	-----------------	--

デフォルト	なし
-------	----

コマンド モード	EXEC モード
----------	----------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

例 次に、デバッグ ログファイルを消去する例を示します。

```
switch# clear debug-logfile debuglog
```

関連コマンド	コマンド	説明
	show debug logfilw	ログファイルの内容を表示します。

clear device-alias

デバイスエイリアス情報を消去するには、**clear device-alias** コマンドを使用します。

```
clear device-alias {session | statistics}
```

シンタックスの説明	session	statistics
	セッション情報を消去します。	デバイスエイリアス統計情報を消去します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、デバイスエイリアスセッションを消去する例を示します。

```
switch# clear device-alias session
```

関連コマンド	コマンド	説明
	show device-alias	デバイスエイリアスデータベース情報を表示します。

clear dpvm

Dynamic Port VSAN Membership (DPVM; ダイナミック ポート VSAN メンバシップ) 情報を消去するには、**clear dpvm** コマンドを使用します。

```
clear dpvm {auto-learn [pwwn pwwn-id] | session}
```

シンタックスの説明	パラメータ	説明
	auto-learn	自動的に学習した (自動学習) DPVM エントリを消去します。
	pwwn <i>pwwn-id</i>	pWWN ID を指定します。フォーマットは、 <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。ここで、 <i>h</i> は 16 進数の数です。
	session	DPVM セッションおよびロックを消去します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	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、**dpvm enable** コマンドを使用して DPVM をイネーブルにする必要があります。

例 次に、単一自動学習エントリを消去する例を示します。

```
switch# clear dpvm auto-learn pwwn 21:00:00:20:37:9c:48:e5
```

次に、すべての自動学習エントリを消去する例を示します。

```
switch# clear dpvm auto-learn
```

次に、セッションを消去する例を示します。

```
switch# clear dpvm session
```

関連コマンド	コマンド	説明
	dpvm enable	DPVM をイネーブルにします。
	show dpvm	DPVM データベース情報を表示します。

clear fabric-binding statistics

VSAN（仮想 SAN）がイネーブルである Fibre Connection（FICON）のファブリック バインディング統計情報を消去するには、EXEC モードで **clear fabric-binding statistics** コマンドを使用します。

```
clear fabric-binding statistics vsan vsan-id
```

シンタックスの説明	vsan vsan-id	FICON がイネーブルの VSAN を指定します。VSAN ID の有効範囲は、1 ~ 4093 です。
-----------	---------------------	---

デフォルト	なし
-------	----

コマンドモード	EXEC モード
---------	----------

コマンド履歴	リリース	変更内容
	1.1(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	なし
------------	----

例	次に、VSAN 1 の既存のファブリック バインディング統計情報を消去する例を示します。
---	--

```
switch# clear fabric-binding statistics vsan 1
```

関連コマンド	コマンド	説明
	show fabric-binding efmd statistics	既存のファブリック バインディング統計情報を表示します。

clear fcanalyzer

リモート キャプチャに設定されたホストの一覧をすべて消去するには、EXEC モードで **clear fcanalyzer** コマンドを使用します。

clear fcanalyzer

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	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、設定されたホストの一覧のみ消去します。既存の接続は切断されません。

例 次に、リモート キャプチャに設定されたホストの一覧すべてを消去する例を示します。

```
switch# clear fcanalyzer
```

関連コマンド	コマンド	説明
	show fcanalyzer	リモート キャプチャに設定されたホストの一覧を表示します。

clear fcflow stats

ファイバチャネルフロー統計情報を消去するには、EXEC モードで **clear fcflow stats** コマンドを使用します。

clear fcflow stats [**aggregated**] **module** *module-number* **index** *flow-number*

シンタックスの説明		
aggregated		ファイバチャネルフローの集約統計情報を消去します。
module		指定モジュールの統計情報を消去します。
<i>module-number</i>		モジュール番号を指定します。
Index		指定フローインデックスのファイバチャネルフローカウンタを消去します。
<i>flow-number</i>		フローインデックス番号を指定します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

例 次に、モジュール 2 のフローインデックス 1 に対する集約ファイバチャネルフロー統計情報を消去する例を示します。

```
switch(config)# # clear fcflow stats aggregated module 2 index 1
```

関連コマンド	コマンド	説明
	show fcflow	fcflow 統計情報を表示します。

clear fcns statistics

ネームサーバ統計情報を消去するには、EXEC モードで **clear fcns statistics** コマンドを使用します。

```
clear fcns statistics vsan vsan-id
```

シンタックスの説明	vsan vsan-id	1 ~ 4093 の範囲にある指定の VSAN (仮想 SAN) に対して、Fabric Configuration Server (FCS) 統計情報が消去されます。
------------------	---------------------	--

デフォルト	なし
--------------	----

コマンドモード	EXEC モード
----------------	----------

コマンド履歴	リリース	変更内容
	1.0(3)	このコマンドが導入されました。

例 次に、ネームサーバ統計情報を消去する例を示します。

```
switch# show fcns statistics

Name server statistics for vsan 1
=====
registration requests received = 0
deregistration requests received = 0
queries received = 23
queries sent = 27
reject responses sent = 23
RSCNs received = 0
RSCNs sent = 0

switch# clear fcns statistics vsan 1

switch# show fcns statistics

Name server statistics for vsan 1
=====
registration requests received = 0
deregistration requests received = 0
queries received = 0
queries sent = 0
reject responses sent = 0
RSCNs received = 0
RSCNs sent = 0
switch#
```

関連コマンド	コマンド	説明
	show fcns statistics	ネームサーバ統計情報を表示します。

clear fcs statistics

ファイバ設定のサーバ統計情報を消去するには、EXEC モードで **clear fcs statistics** コマンドを使用します。

```
clear fcs statistics vsan vsan-id
```

シンタックスの説明	vsan vsan-id	1 ~ 4093 の範囲にある指定の VSAN（仮想 SAN）に対して、Fabric Configuration Server（FCS）統計情報が消去されます。
デフォルト	なし	
コマンドモード	EXEC モード	
コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。
例	次に、VSAN（仮想 SAN）10 のファブリック設定のサーバ統計情報を消去する例を示します。 switch# clear fcs statistics vsan 10	
関連コマンド	コマンド	説明
	show fcs statistics	ファブリック設定のサーバ統計情報を表示します。

clear fctimer session

fctimer Cisco Fabric Services (CFS) セッション コンフィギュレーションおよびロックを消去するには、**clear fctimer session** コマンドを使用します。

clear fctimer session

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、fctimer セッションを消去する例を示します。

```
switch# clear fctimer session
```

関連コマンド	コマンド	説明
	show fctimer	fctimer 情報を表示します。

clear fc-redirect config vt

スイッチの FC リダイレクト設定を削除するには、**clear fc-redirect config** コマンドを使用します。

```
clear fc-redirect config vt vt-pwwn [local-switch-only]
```

シンタックスの説明	vt vt-pwwn	削除する設定の VT pWWN を指定します。
	local-switch-only	(任意) この設定はローカルでのみ削除されます。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.2(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、アプリケーションを使用して設定を削除できない場合の最後の選択肢として使用されます。

このコマンドは、SME/DMM などのアプリケーションにより作成される FC リダイレクトに関するすべての設定（アクティブな設定を含めて）を削除します。これにより、データ損失につながる可能性があります。このコマンドを入力すると、ホスト サーバは個々のインテリジェント サービスアプリケーションを渡すことでストレージレイと直接通信を行い、データの破損を引き起こします。このコマンドは、アプリケーション（DMM/SME）から削除できずに残った設定があればそれを消去するための最後の選択肢として使用してください。このコマンドは、スイッチが稼動していないときに使用してください。

例 次に、スイッチ上の FC リダイレクト設定を消去する例を示します。

```
switch# clear fc-redirect config vt 2f:ea:00:05:30:00:71:64
Deleting a configuration MAY result in DATA CORRUPTION.
Do you want to continue? (y/n) [n] y
```

関連コマンド	コマンド	説明
	show fc-redirect active-configs	スイッチのアクティブな設定すべてを表示します。

clear fc-redirect decommission-switch

スイッチの既存のすべての FC リダイレクト設定を削除し、スイッチにこれ以上 FC リダイレクト設定がされないようにするには、**clear fc-redirect decommission-switch** コマンドを使用します。

clear fc-redirect decommission-switch

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.2(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、write erase の後に使用します。このコマンドは、スイッチを FC リダイレクト設定がされているファブリックから別のファブリックに移動するためにも使用できます。このコマンドの使用後、スイッチを別のファブリックで使用するには、スイッチをファブリックから切断してからリブートします。

例 次に、スイッチの FC リダイレクトを解放する例を示します。

```
switch# clear fc-redirect decommission-switch
This Command removes any FC-Redirect configuration and disables
FC-Redirect on this switch. Its usage is generally recommended in
the following cases:
  1) After 'write erase'
  2) When removing the switch from the fabric.
If NOT for the above, Decommissioning a switch MAY result in
DATA CORRUPTION.

Do you want to continue? (Yes/No) [No] Yes

Please check the following before proceeding further:
  1) Hosts / targets connected locally are NOT involved in any
     FC-Redirect configuration.
  2) No application running on this switch created an FC-Redirect
     Configuration
Please use the command 'show fc-redirect active-configs' to check
these.

Do you want to continue? (Yes/No) [No] Yes
switch#
```

関連コマンド	コマンド	説明
	show fc-redirect active-configs	スイッチの全アクティブ コンフィギュレーションを表示します。

clear ficon

指定 VSAN（仮想 SAN）の Fibre Connection（FICON）情報を消去するには、**clear ficon** コマンドを使用します。

```
clear ficon vsan vsan-id [allegiance | timestamp]
```

シンタックスの説明	パラメータ	説明
	vsan <i>vsan-id</i>	FICON がイネーブルの VSAN を指定します。VSAN ID の有効範囲は、1 ~ 4093 です。
	allegiance	FICON デバイスの義務を消去します。
	timestamp	FICON VSAN の特定タイムスタンプを消去します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.3(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 **clear ficon vsan vsan-id allegiance** コマンドは、現在実行しているセッションを中断します。

例 次に、VSAN 1 の現在のデバイスの義務を消去する例を示します。

```
switch# clear ficon vsan 1 allegiance
```

次に、VSAN 20 の VSAN クロックを消去する例を示します。

```
switch# clear ficon vsan 20 timestamp
```

関連コマンド	コマンド	説明
	show ficon	設定された FICON の詳細を表示します。

clear fspf counters

Fabric Shortest Path First (FSPF) 統計情報を消去するには、EXEC モードで **clear fspf counters** コマンドを使用します。

```
clear fspf counters vsan vsan-id [interface type]
```

シンタックスの説明

vsan	VSAN (仮想 SAN) でカウンタを消去します。
vsan-id	VSAN ID の有効範囲は、1 ~ 4093 です。
interface type	(任意) インターフェイスでカウンタを消去します。インターフェイスタイプはファイバチャネルが fc 、およびポートチャネルが port-channel です。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスが指定されていない場合、VSAN (仮想 SAN) のすべてのカウンタが消去されます。インターフェイスが指定されている場合、指定のインターフェイスのカウンタが消去されます。

例

次に、VSAN 1 の FSPF 統計情報を消去する例を示します。

```
switch# clear fspf counters vsan 1
```

次に、VSAN 1 のスロット 9 ポート 32 のファイバチャネルインターフェイスに対し、FSPF 統計情報を消去する例を示します。

```
switch# clear fspf counters vsan 1 interface fc 9/32
```

関連コマンド

コマンド	説明
show fspf	特定の VSAN に対するグローバルな FSPF 統計情報を表示します。

clear install failure-reason

MDS 9124 ファブリック スイッチでの In-Service Software Upgrade (ISSU) 中に作成されたアップグレードエラー理由ログを消去するには、**clear install failure-reason** コマンドを使用します。



注意

アップグレードエラー理由ログを消去すると、ISSU エラー時のデバッグに役立つ情報が何もなくなります。

clear install failure-reason

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

EXEC モード

コマンド履歴

リリース	変更内容
3.1(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、Cisco MDS 9124 ファブリック スイッチでのみサポートされます。

例

The following example removes all upgrade failure reason logs on a Cisco MDS 9124 Fabric Switch.

```
switch# clear install failure-reason
```

関連コマンド

コマンド	説明
show install all status	Cisco MDS 9124 ファブリック スイッチでの ISSU のステータスを表示します。
show install all failure-reason	ISSU エラー時にアップグレードを進めることができない理由を表示します。

clear ip access-list counters

IP アクセス リスト カウンタを消去するには、EXEC モードで **clear access-list counters** コマンドを使用します。

clear ip access-list counters *list-name*

シンタックスの説明	<i>list-name</i>	IP アクセス リスト名を指定します (最大 64 文字)。
デフォルト	なし	
コマンド モード	EXEC モード	
コマンド履歴	リリース	変更内容
	1.1(1)	このコマンドが導入されました。
例	次に、IP アクセス リストのカウンタを消去する例を示します。 <pre>switch# clear ip access-list counters adminlist</pre>	
関連コマンド	コマンド	説明
	show ip access-list	IP アクセス リスト情報を表示します。

clear ips arp

Address Resolution Protocol (ARP) キャッシュを消去するには、EXEC モードで **clear ips arp** コマンドを使用します。

```
clear ips arp {address ip-address| interface gigabitethernet module-number}
```

シンタックスの説明	説明
address	fcflow (ファイバチャネルフロー) 集約統計情報を消去します。
<i>ip-address</i>	ピア IP アドレスを入力します。
interface gigabitethernet	ギガビットイーサネットインターフェイスを指定します。
<i>module-number</i>	ギガビットイーサネットインターフェイスのスロットおよびポートを指定します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.1(1)	このコマンドが導入されました。

例 ARP キャッシュは、2つの方法で消去できます。ARP キャッシュ内の1つのエントリのみ消去するか、または ARP キャッシュ内のすべてのエントリを消去するかです。

次に、Address Resolution Protocol (ARP) キャッシュ エントリを1つ消去する例を示します。

```
switch# clear ips arp address 10.2.2.2 interface gigabitethernet 8/7
arp clear successful
```

次に、すべての ARP キャッシュ エントリを消去する例を示します。

```
switch# clear ips arp interface gigabitethernet 8/7
arp clear successful
```


clear ips stats

IP ストレージ統計情報を消去するには、EXEC モードで **clear ips stats** コマンドを使用します。

```
clear ips stats {all [interface gigabitethernet slot/port] |
  buffer interface gigabitethernet slot/port |
  dma-bridge interface gigabitethernet slot/port |
  icmp interface gigabitethernet slot/port |
  ip interface gigabitethernet slot/port |
  ipv6 traffic interface gigabitethernet slot/port |
  mac interface gigabitethernet slot/port |
  tcp interface gigabitethernet slot/port}
```

シンタックスの説明

all	すべての IPS 統計情報を消去します。
interface gigabitethernet <i>slot/port</i>	ギガビットイーサネットインターフェイスを消去します。 スロット番号およびポート番号を指定します。
buffer	IP ストレージバッファ情報を消去します。
dma-bridge	Direct Memory Access (DMA; ダイレクトメモリアクセス) 統計情報を消去します。
icmp	Internet Control Message Protocol (ICMP) 統計情報を消去します。
ip	IP 統計情報を消去します。
ipv6	IPv6 統計情報を消去します。
mac	メディアアクセス制御 (MAC) 統計情報を消去します。
tcp	TCP 統計情報を消去します。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
3.0(1)	このコマンドが導入されました。

例

次に、指定のインターフェイスの IPS 統計情報をすべて消去する例を示します。

```
switch# clear ips all interface gigabitethernet 8/7
switch#
```

clear ips stats fabric interface

Cisco MDS 9000 18/4 ポート マルチ サービス モジュールの IPS ラインカード上の指定した iSCSI または FCIP インターフェイスを消去するには、**clear ips stats fabric interface** コマンドを使用します。

```
clear ips stats fabric interface [iscsi slot/port | fcip N]
```

シンタックスの説明	iscsi slot/port	(任意) iSCSI インターフェイスの Data Path Processor (DPP) ファブリック統計情報を消去します。
	fcip N	(任意) FCIP インターフェイスの DPP ファブリック統計情報を消去します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.2(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 なし

例 次に、指定した iSCSI または FCIP インターフェイスの統計情報を消去する例を示します。

```
switch# clear ips stats fabric interface fcip ?
<1-255>  Fcip interface number
switch# clear ips stats fabric interface fcip 1
switch#
switch# clear ips stats fabric interface iscsi 1/1
switch#
```

関連コマンド	コマンド	説明
	show ips stats fabric interface	Cisco MDS 9000 18/4 ポート マルチ サービス モジュールの IPS ラインカード上の指定した iSCSI または FCIP インターフェイスのファブリック関連の統計情報を表示します。

clear ipv6 access-list

IPv6 Access Control List (ACL; アクセス制御リスト) 統計情報を消去するには、**clear ipv6 access-list** コマンドを使用します。

```
clear ipv6 access-list [list-name]
```

シンタックスの説明	access-list	ACL の概要を表示します。
	<i>list-name</i>	ACL 名を指定します。最大文字サイズは 64 です。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.1(0)	このコマンドが導入されました。

使用上のガイドライン IPv6 ACL 統計情報を消去するために、**clear ipv6 access-list** コマンドを使用します。

例 次に、IPv6 ACL の情報を表示する例を示します。

```
switch# clear ipv6 access-list testlist
switch#
```

関連コマンド	コマンド	説明
	ipv6 access-list	IPv6 ACL を設定します。
	show ipv6	IPv6 設定情報を表示します。

clear ipv6 neighbors

IPv6 ネイバ キャッシュ テーブルを消去するには、**clear ipv6 neighbors** コマンドを使用します。

clear ipv6 neighbors

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.1(0)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、IPv6 ネイバ キャッシュ テーブルをフラッシュする例を示します。

```
switch# clear ipv6 neighbors
switch#
```

関連コマンド	コマンド	説明
	ipv6 nd	IPv6 近隣探索コマンドを設定します。
	show ipv6 neighbors	IPv6 ネイバ設定情報を表示します。

clear islb session

保留中の iSLB 設定を消去するには、**clear islb session** コマンドを使用します。

clear islb session

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.0(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 保留中の iSLB 設定を消去するために **clear islb session** コマンドを使用します。管理権限を持つユーザであれば、どのスイッチからでもこのコマンドを実行できます。

例 次に、保留中の iSLB 設定を消去する例を示します。

```
switch# clear islb session
```

関連コマンド	コマンド	説明
	islb abort	保留中の iSLB 設定を廃棄します。
	show islb cfs-session status	iSLB セッションの詳細を表示します。
	show islb pending	iSLB の保留中の設定を表示します。
	show islb pending-diff	iSLB 未決定コンフィギュレーションの差異を表示します。
	show islb session	iSLB セッション情報を表示します。
	show islb status	iSLB CFS ステータスを表示します。
	show islb vrrp	iSBL VRRP ロードバランス情報を表示します。

clear ivr fcdomain database

IVR fcdomain データベースを消去するには、EXEC モードで **clear ivr fcdomain database** コマンドを使用します。

clear ivr fcdomain database

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.1(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、すべての IVR fcdomain データベース情報を消去する例を示します。

```
switch# clear ivr fcdomain database
```

関連コマンド	コマンド	説明
	show ivr fcdomain database	IVR fcdomain データベース エントリ情報を表示します。

clear ivr service-group database

Inter-VSAN Routing (IVR) サービス グループ データベースを消去するには、**clear ivr service-group database** コマンドを使用します。

clear ivr service-group database

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 EXEC モード

リリース	変更内容
3.0(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 なし

例 次に、IVR サービス グループ データベースを消去する例を示します。

```
switch# clear ivr service-group database
```

コマンド	説明
show ivr service-group database	IVR サービス グループ データベースを表示します。

clear ivr zone database

Inter-VSAN Routing (IVR) のゾーン データベースを消去するには、EXEC モードで **clear ivr zone database** コマンドを使用します。

clear ivr zone database

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.3(1)	このコマンドが導入されました。

例 次に、設定されたすべての Inter-VSA Zone (IVZ;VSA 間ゾーン) 情報を消去する例を示します。
 switch# **clear ivr zone database**

clear license

ライセンスをアンインストールするには、EXEC モードで **clear license** コマンドを使用します。

clear license *filename*

シンタックスの説明	<i>filename</i>	アンインストールするライセンス ファイルを指定します。
------------------	-----------------	-----------------------------

デフォルト	なし
--------------	----

コマンドモード	EXEC モード
----------------	----------

コマンド履歴	リリース	変更内容
	1.3(2)	このコマンドが導入されました。

例 次に、特定のライセンスを消去する例を示します。

```
switch# clear license Ficon.lic
Clearing license Ficon.lic:
SERVER this_host ANY
VENDOR cisco
# An example fcports license
INCREMENT SAN_EXTN_OVER_IP cisco 1.000 permanent 1 HOSTID=VDH=ABCD \
  NOTICE=<LicFileID>san_extn2.lic</LicFileID><LicLineID>1</LicLineID> \
  SIGN=67CB2A8CCAC2

Do you want to continue? (y/n) y
Clearing license ..done
switch#
```

関連コマンド	コマンド	説明
	show license	ライセンス情報を表示します。

clear line

Virtual Terminal Line (VTY; 仮想端末回線) セッションを消去するには、EXEC モードで **clear line** コマンドを使用します。

```
clear line vty-name
```

シンタックスの説明	<i>vtty-name</i>	VTY 名を指定します (最大 64 文字)。
-----------	------------------	-------------------------

デフォルト	なし
-------	----

コマンドモード	EXEC モード
---------	----------

コマンド履歴	リリース	変更内容
	1.2(1)	このコマンドが導入されました。

例 次に、Address Resolution Protocol (ARP) キャッシュ エントリを 1 つ消去する例を示します。

```
switch# clear line Aux
arp clear successful
```

関連コマンド	コマンド	説明
	show line	回線情報を表示します。

clear logging

Syslog 情報を削除するには、EXEC モードで **clear logging** コマンドを使用します。

```
clear logging {logfile | nvram | onboard information [module slot] | session}
```

シンタックスの説明	
logfile	ログファイルメッセージを消去します。
nvram	NVRAM（不揮発性 RAM）ログを消去します。
onboard information	On-Board-Failure Logging（OBFL; オンボード障害ロギング）情報を消去します。information のタイプには、 boot-uptime 、 cpu-hog 、 device-version 、 endtime 、 environmental-history 、 error-stats 、 exception-log 、 interrupt-stats 、 mem-leak 、 miscellaneous-error 、 module 、 obfl-history 、 obfl-log 、 register-log 、 stack-trace 、 starttime 、 status 、 system-health があります。
module slot	指定したモジュールの OBFL 情報を消去します。
session	ロギングセッションを消去します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。
	3.0(1)	onboard 、 module 、および session オプションが追加されました。

例 次に、デバッグ ログ ファイルを消去する例を示します。

```
switch# clear logging logfile
```

次に、オンボード システム ヘルス ログ ファイルを消去する例を示します。

```
switch# clear logging onboard system-health
!!!WARNING! This will clear the selected logging buffer!!
Do you want to continue? (y/n) [n]
```

関連コマンド	コマンド	説明
	show logging	ロギング情報を表示します。

clear ntp

Network Time Protocol (NTP) 情報を消去するには、EXEC モードで **clear ntp** コマンドを使用します。

```
clear ntp {session | statistics {all-peers | io | local | memory}}
```

シンタックスの説明

session	NTP Cisco Fabric Services (CFS) セッション コンフィギュレーションおよびロックを消去します。
statistics	NTP 統計情報を消去します。
all-peers	すべてのピアの I/O 統計情報を消去します。
io	I/O デバイスの I/O 統計情報を消去します。
local	ローカル デバイスの I/O 統計情報を消去します。
memory	メモリの I/O 統計情報を消去します。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、すべてのピアの NTP 統計情報を消去する例を示します。

```
switch# clear ntp statistics all-peers
```

次に、I/O デバイスの NTP 統計情報を消去する例を示します。

```
switch# clear ntp statistics io
```

次に、ローカル デバイスの NTP 統計情報を消去する例を示します。

```
switch# clear ntp statistics local
```

次に、メモリの NTP 統計情報を消去する例を示します。

```
switch# clear ntp statistics memory
```

関連コマンド

コマンド	説明
show ntp	設定されたサーバおよびピア アソシエーションを表示します。

clear port-security

スイッチのポートセキュリティ情報を消去するには、EXEC モードで **clear port-security** コマンドを使用します。

```
clear port-security {database auto-learn {interface fc slot/port | port-channel port} | session |
statistics} vsan vsan-id
```

シンタックスの説明	パラメータ	説明
	database	ポートセキュリティのアクティブ コンフィギュレーション データベースを消去します。
	session	ポートセキュリティ Cisco Fabric Services (CFS) コンフィギュレーション セッションおよびロックを消去します。
	statistics	ポートセキュリティ カウンタを消去します。
	auto-learn	指定のインターフェイスまたは VSAN (仮想 SAN) の自動学習されたエントリを消去します。
	interface fc slot/port	指定インターフェイスのエントリを消去します。
	port-channel port	指定のポートチャネルのエントリを消去します。有効範囲は 1 ~ 128 です。
	vsan vsan-id	指定 VSAN ID のエントリを消去します。有効範囲は 1 ~ 4093 です。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.2(1)	このコマンドが導入されました。
	2.0(x)	session オプションが追加されました。

使用上のガイドライン アクティブ データベースは読み取り専用です。 **clear port-security database** コマンドは、競合解決時に使用できます。

例 次に、指定の VSAN のポートセキュリティ データベースから既存の統計情報をすべて消去する例を示します。

```
switch# clear port-security statistics vsan 1
```

次に、VSAN 内で指定されたインターフェイスのアクティブ データベースで、学習されたエントリを消去する例を示します。

```
switch# clear port-security database auto-learn interface fc1/1 vsan 1
```

次に、VSAN 全体のアクティブ データベースで学習されたエントリを消去する例を示します。

```
switch# clear port-security database auto-learn vsan 1
```

関連コマンド	コマンド	説明
	show port-security	設定されたポートセキュリティ情報を表示します。

clear processes log

スイッチのログ ファイルを消去するには、EXEC モードで **clear processes log** コマンドを使用します。

```
clear processes log {all | pid pid-number}
```

シンタックスの説明	パラメータ	説明
	all	ログ ファイルをすべて消去します。
	pid	特定のプロセスのログ ファイルを消去します。
	<i>pid-number</i>	プロセス ID (0 ~ 2147483647) を指定します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、スイッチのすべてのログ ファイルを消去する例を示します。

```
switch# clear processes log all
```

関連コマンド	コマンド	説明
	show processes	プロセスまたはハイ アベイラビリティ アプリケーションの詳細実行情報、またはログ情報を表示します。

clear qos statistics

Quality of Services (QoS; サービス品質) 統計情報カウンタを消去するには、EXEC モードで **clear qos statistics** コマンドを使用します。

clear qos 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 EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、QoS カウンタを消去する例を示します。

```
switch# clear qos statistics
```

関連コマンド	コマンド	説明
	show qos statistics	現在の QoS 設定(プライオリティの高いフレームの数など)を表示します。

clear radius session

Remote Authentication Dial-In User Service (RADIUS) Cisco Fabric Services (CFS) セッション コンフィギュレーションおよびロックを消去するには、**clear radius session** コマンドを使用します。

clear radius session

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、RADIUS セッションを消去する例を示します。

```
switch# clear radius session
```

関連コマンド	コマンド	説明
	show radius	RADIUS CFS 配信ステータスおよびその他の詳細を表示します。

clear rlir

Registered Link Incident Report (RLIR) を消去するには、EXEC モードで **clear rlir** コマンドを使用します。

```
clear rlir {history | recent {interface fc slot/port | portnumber port-number} | statistics vsan vsan-id}
```



(注)

Cisco Fabric Switch for HP c-Class BladeSystem と Cisco Fabric Switch for IBM BladeCenter では、構文が次のように異なります。

```
interface bay port | ext port
```

シンタックスの説明

history	RLIR リンクのインシデント履歴を消去します。
recent	最近のリンク インシデントを消去します。
interface fc slot/port bay port ext port	指定インターフェイスのエントリを消去します。 Cisco Fabric Switch for HP c-Class BladeSystem および Cisco Fabric Switch for IBM BladeCenter 上の指定のインターフェイスのエントリを消去します。
portnumber port-number	リンク インシデントのポート番号を表示します。
statistics	RLIR 統計情報を消去します。
vsan vsan-id	消去対象の RLIR 統計情報の VSAN ID を指定します。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.3(1)	このコマンドが導入されました。
3.1(2)	interface bay ext オプションが追加されました。

使用上のガイドライン

なし

例

次に、指定の VSAN の既存の統計情報をすべて消去する例を示します。

```
switch# clear rlir statistics vsan 1
```

次に、リンク インシデント履歴を消去する例を示します。

```
switch# clear rlir history
```

次に、指定のインターフェイスの最近の RLIR 情報を消去する例を示します。

```
switch# clear rlir recent interface fc 1/2
```

次に、指定のポート番号の最近の RLIR 情報を消去する例を示します。

```
switch# clear rlir recent portnumber 16
```

関連コマンド	コマンド	説明
	show rscn	RSCN 情報を表示します。

clear rmon alarms

実行コンフィギュレーションからすべての 32 ビットの Remote Monitoring (RMON; リモート モニタリング) アラームを消去するには、**clear rmon alarms** コマンドを使用します。

clear rmon alarms

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1a)	このコマンドが導入されました。

使用上のガイドライン 変更を永続的なものにするには、スタートアップ コンフィギュレーションに変更を保存する必要があります。

例 次に、実行コンフィギュレーションからすべての 32 ビット RMON アラームを消去する例を示します。

```
switch# clear rmon alarms
switch#
```

関連コマンド	コマンド	説明
	clear rmon hcalarms	すべての 64 ビット RMON アラームを消去します。
	clear rmon all-alarms	すべての 32 ビットおよび 64 ビット RMON アラームを消去します。
	clear rmon log	RMON ログ情報を消去します。

clear rmon all-alarms

実行コンフィギュレーションから、すべての 32 ビットおよび 64 ビット RMON アラームを消去するには、**clear rmon all-alarms** コマンドを使用します。

clear rmon all-alarms

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1a)	このコマンドが導入されました。

使用上のガイドライン 変更を永続的なものにするには、スタートアップ コンフィギュレーションに変更を保存する必要があります。

例 次に、実行コンフィギュレーションからすべての 32 ビットおよび 64 ビット RMON アラームを消去する例を示します。

```
switch# clear rmon all-alarms
switch#
```

関連コマンド	コマンド	説明
	clear rmon alarms	すべての 32 ビット RMON アラームを消去します。
	clear rmon hcalarms	すべての 64 ビット RMON アラームを消去します。
	clear rmon log	RMON ログ情報を消去します。

clear rmon hcalarms

実行コンフィギュレーションから、すべての 64 ビット RMON アラームを消去するには、**clear rmon hcalarms** コマンドを使用します。

clear rmon hcalarms

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1a)	このコマンドが導入されました。

使用上のガイドライン 変更を永続的なものにするには、スタートアップ コンフィギュレーションに変更を保存する必要があります。

例 次に、実行コンフィギュレーションからすべての 64 ビット RMON アラームを消去する例を示します。

```
switch# clear rmon hcalarms
switch#
```

関連コマンド	コマンド	説明
	clear rmon alarms	すべての 32 ビット RMON アラームを消去します。
	clear rmon all-alarms	すべての 32 ビットおよび 64 ビット RMON アラームを消去します。
	clear rmon log	RMON ログ情報を消去します。

clear rmon log

スイッチの RMON ログからすべてのエントリを消去するには、**clear rmon log** コマンドを使用します。

clear rmon 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 EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1a)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、スイッチの RMON ログからすべてのエントリを消去する例を示します。

```
switch# clear rmon log
switch#
```

関連コマンド	コマンド	説明
	clear rmon alarm	すべての 32 ビット RMON アラームを消去します。
	clear rmon hcalarms	すべての 64 ビット RMON アラームを消去します。
	clear rmon all-alarms	すべての 32 ビットおよび 64 ビット RMON アラームを消去します。

clear role session

認証ロール Cisco Fabric Services (CFS) セッション コンフィギュレーションおよびロックを消去するには、**clear role session** コマンドを使用します。

clear role session

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、認証ロール CFS セッションを消去する例を示します。

```
switch# clear role session
```

関連コマンド	コマンド	説明
	show role	ロール コンフィギュレーション情報を表示します。

clear rscn session vsan

指定の VSAN（仮想 SAN）の Registered State Change Notification（RSCN）セッションを消去するには、**clear rscn session vsan** コマンドを使用します。

```
clear rscn session vsan vsan-id
```

シンタックスの説明	<i>vsan-id</i>	RSCN セッションを消去する VSAN を指定します。VSAN ID の有効範囲は、1 ~ 4093 です。
------------------	----------------	---

デフォルト	なし
--------------	----

コマンドモード	EXEC モード
----------------	----------

コマンド履歴	リリース	変更内容
	3.0(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	なし
-------------------	----

例	次に、VSAN 1 の RSCN セッションを消去する例を示します。
----------	------------------------------------

```
switch# clear rscn session vsan 1
```

関連コマンド	コマンド	説明
	rscn	RSCN を設定します。
	show rscn	RSCN 情報を表示します。

clear rscn statistics

指定の VSAN（仮想 SAN）の Registered State Change Notification（RSCN）を消去するには、EXEC モードで **clear rscn statistics** コマンドを使用します。

```
clear rscn statistics vsan vsan-id
```

シンタックスの説明	vsan	VSAN で消去される RSCN 統計情報を指定します。
	vsan-id	RSCN 統計情報を消去する VSAN の ID を指定します。

デフォルト	なし
-------	----

コマンドモード	EXEC モード
---------	----------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン	なし
------------	----

例	次に、VSAN 1 の RSCN 統計情報を消去する例を示します。
---	-----------------------------------

```
switch# clear rscn statistics 1
```

関連コマンド	コマンド	説明
	show rscn	RSCN 情報を表示します。

clear santap module

SANTap 情報を消去するには、**clear santap module** コマンドを使用します。

```
clear santap module slot-number {avt avt-pwwn [lun avt-lun] | itl target-pwwn host-pwwn | session session-id}
```

シンタックスの説明	説明
<i>slot-number</i>	Storage Services Module (SSM; ストレージ サービス モジュール) のモジュール番号を指定します。有効値は 1 ~ 13 です。
avt <i>avt-pwwn</i>	Appliance Virtual Target (AVT) pWWN を削除します。フォーマットは <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。
lun <i>avt-lun</i>	AVT LUN を削除します。フォーマットは、 <i>0xhhhh[:hhhh[:hhhh[:hhhh]]]</i> です。
itl <i>target-pwwn host-pwwn</i>	SANTap Initiator Target LUN (ITL) 3 ビットバイトを削除します。 <i>target-pwwn</i> および <i>host-pwwn</i> のフォーマットは、 <i>hh:hh:hh:hh:hh:hh:hh:hh</i> です。
session <i>session-id</i>	セッションを消去します。セッション ID の有効値は 0 ~ 2147483647 です。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.0(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 なし

例 次に、SANTap セッションを削除する例を示します。

```
switch# clear santap module 13 session 2020
```

関連コマンド	コマンド	説明
	santap module	機器が設定されている SSM と VSAN 間のマッピングを設定します。
	show santap module	SANTap 機能の設定および統計情報を表示します。

clear ssm-nvram santap module

スーパーバイザのフラッシュに格納されている特定のスロットの SANTap 設定を消去するには、コンフィギュレーション モードで **clear ssm-nvram santap module** コマンドを使用します。

```
clear ssm-nvram santap module slot
```

シンタックスの説明	<i>slot</i>	指定したスロット内のモジュールの SANTap 設定を表示します。
デフォルト	なし	
コマンド モード	EXEC モード	
コマンド履歴	リリース	変更内容
	3.2(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	なし	
例	次に、スロット 2 の SANTap コンフィギュレーションを消去する例を示します。 switch# <code>clear ssm-nvram santap module 2</code>	
関連コマンド	コマンド	説明
	<code>ssm enable feature</code>	SSM で SANTap 機能をイネーブルにします。

clear scheduler logfile

コマンドスケジューラ ログファイルを消去するには、**clear scheduler logfile** コマンドを使用します。

clear scheduler logfile

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、コマンドスケジューラ ログファイルを消去する例を示します。

```
switch# clear scheduler logfile
```

関連コマンド	コマンド	説明
	show scheduler	コマンドスケジューラ情報を表示します。

clear screen

端末の画面を消去するには、EXEC モードで **clear screen** コマンドを使用します。

clear screen

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、端末画面を消去する例を示します。

```
switch# clear screen
```

clear scsi-flow statistics

SCSI フロー統計情報カウンタを消去するには、**clear scsi-flow statistics** コマンドを使用します。

```
clear scsi-flow statistics flow-id flow-id
```

シンタックスの説明	flow-id <i>flow-id</i>	SCSI フロー ID 番号を設定します。						
デフォルト	なし							
コマンドモード	EXEC モード							
コマンド履歴	リリース 2.0(2)	変更内容 このコマンドが導入されました。						
使用上のガイドライン	なし							
例	次に、SCSI フロー ID 3 の SCSI フロー統計情報カウンタを消去する例を示します。 <pre>switch# clear scsi-flow statistics flow-id 3</pre>							
関連コマンド	<table><thead><tr><th>コマンド</th><th>説明</th></tr></thead><tbody><tr><td>scsi-flow flow-id</td><td>SCSI フロー サービスを設定します。</td></tr><tr><td>show scsi-flow</td><td>SCSI フロー設定およびステータスを表示します。</td></tr></tbody></table>	コマンド	説明	scsi-flow flow-id	SCSI フロー サービスを設定します。	show scsi-flow	SCSI フロー設定およびステータスを表示します。	
コマンド	説明							
scsi-flow flow-id	SCSI フロー サービスを設定します。							
show scsi-flow	SCSI フロー設定およびステータスを表示します。							

clear sdv

指定の SAN Device Virtualization (SDV; SAN デバイス バーチャライゼーション) パラメータを消去するには、EXEC モードで **clear sdv** コマンドを使用します。

```
clear sdv {database vsan vsan-id | session vsan vsan-id | statistics vsan vsan-id}
```

シンタックスの説明

database	SDV データベースを消去します。
vsan vsan-id	VSAN (仮想 SAN) 数を指定します。有効範囲は 1 ~ 4093 です。
session	SDV セッションを消去します。
statistics	SDV 統計情報を消去します。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
3.1(2)	このコマンドが導入されました。

使用上のガイドライン

なし

例

次に、SDV 統計情報を消去する例を示します。

```
switch# clear sdv statistics vsan 2
```

関連コマンド

コマンド	説明
sdv enable	SAN デバイス バーチャライゼーションをイネーブルまたはディセーブルにします。
show sdv statistics	SAN デバイス バーチャライゼーションの統計情報を表示します。

clear snmp hostconfig

実行コンフィギュレーションからすべての SNMP ホストを消去するには、**clear snmp hostconfig** コマンドを使用します。

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.3(1a)	このコマンドが導入されました。

使用上のガイドライン 変更を永続的なものにするには、スタートアップ コンフィギュレーションに変更を保存する必要があります。

例 次に、SNMP ホスト リストを消去する例を示します。

```
switch# clear snmp hostconfig
switch#
```

関連コマンド	コマンド	説明
	show snmp host	SNMP ステータスおよび設定情報を表示します。

clear ssh hosts

信頼性のある Secure Shell (SSH; セキュア シェル) ホストを消去するには、EXEC モードで **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 EXEC モード

コマンド履歴	リリース	変更内容
	1.2(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 なし

例 次に、NVRAM（不揮発性 RAM）および揮発性ストレージからリセット要因情報を消去する例を示します。

```
switch# clear ssh hosts
```

関連コマンド	コマンド	説明
	show ssh hosts	SSH ホスト情報を表示します。

clear system reset-reason

NVRAM（不揮発性 RAM）および揮発性ストレージに格納された `reset-reason` 情報を消去するには、EXEC モードで `clear system reset-reason` コマンドを使用します。

`clear system reset-reason`

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.3(2a)	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、次のように使用します。

- Cisco MDS 9500 シリーズ スイッチでは、このコマンドはアクティブおよびスタンバイ スーパーバイザ モジュールの NVRAM および揮発性ストレージに保存されているリセット要因情報を消去します。
- Cisco MDS 9200 シリーズ スイッチでは、このコマンドはアクティブ スーパーバイザ モジュールの NVRAM および揮発性ストレージに保存されているリセット要因情報を消去します。

例 次に、信頼性のある Secure Shell（SSH; セキュア シェル）ホストを消去する例を示します。

```
switch# clear system reset-reason
```

関連コマンド	コマンド	説明
	<code>show system reset-reason</code>	システムの <code>reset-reason</code> 情報を表示します。

clear tacacs+ session

Terminal Access Controller Access Control System Plus (TACACS+) Cisco Fabric Servers (CFS) セッション コンフィギュレーションおよびロックを消去するには、**clear tacacs+ session** コマンドを使用します。

clear tacacs+ session

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 EXEC モード

コマンド履歴	リリース	変更内容
	2.0(x)	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、**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。

例 次に、TACACS+ セッションを消去する例を示します。

```
switch# clear tacacs+ session
```

関連コマンド	コマンド	説明
	show tacacs+	TACACS+ CFS 配信ステータスおよびその他の詳細を表示します。
	tacacs+ enable	TACACS+ をイネーブルにします。

clear tlport alpa-cache

Address Resolution Protocol (ARP) キャッシュの内容全体を消去するには、EXEC モードで **clear tlport alpa-cache** コマンドを使用します。

clear tlport alpa-cache

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.3(5)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、Translative Loop (TL) ポート Arbitrated Loop Physical Address (ALPA) キャッシュを消去する例を示します。

```
switch# clear tlport alpa-cache
```

関連コマンド	コマンド	説明
	show tlport alpa-cache	TL ポート ALPA キャッシュ情報を表示します。

clear user

信頼性のある Secure Shell (SSH; セキュア シェル) ホストを消去するには、EXEC モードで **clear user** コマンドを使用します。

```
clear user username
```

シンタックスの説明	<i>username</i>	消去するユーザ名を指定します。
デフォルト	なし	
コマンドモード	EXEC モード	
コマンド履歴	リリース	変更内容
	1.2(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	なし	
例	次に、指定のユーザをログアウトさせる例を示します。 switch# <code>clear user vsam</code>	
関連コマンド	コマンド	説明
	<code>show users</code>	ユーザ情報を表示します。

clear vrrp

指定の仮想ルータのすべてのソフトウェア カウンタを消去するには、EXEC モードで **clear vrrp** コマンドを使用します。

```
clear vrrp {statistics [ipv4 | ipv6] vr number interface {gigabitethernet slot/port | mgmt 0 |
port-channel portchannel-id | vsan vsan-id}}
```

シンタックスの説明

statistics	グローバル Virtual Router Redundancy Protocol (VRRP) 統計情報を消去します。
ipv4	IPv4 仮想ルータの統計情報を消去します。
ipv6	IPv6 仮想ルータの統計情報を消去します。
vr number	特定の仮想ルータの統計情報を消去して、VR 番号を 1 ~ 255 の間で指定します。
interface	インターフェイスを消去します。
gigabitethernet slot/port	指定のギガビットイーサネットインターフェイスを消去します。
mgmt 0	管理インターフェイスを指定します。
port-channel port-channel-number	指定のポートチャネル インターフェイスを消去します。ポートチャネル インターフェイスの ID は、1 ~ 128 の間で指定します。
vsan vsan-id	指定の VSAN (仮想 SAN) を消去します。VSAN ID の有効範囲は、1 ~ 4093 です。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。
3.0(1)	ipv4 および ipv6 引数が追加されました。

使用上のガイドライン

なし

例

次に、VSAN 2 上の仮想ルータ 7 に対するすべてのソフトウェア カウンタを消去する例を示します。

```
switch# clear vrrp vr 7 interface vsan2
```

関連コマンド

コマンド	説明
show vrrp	VRRP 設定情報を表示します。
vrrp	VRRP をイネーブルにします。

clear zone

指定の VSAN（仮想 SAN）のゾーンサーバにあるすべての設定情報を消去するには、EXEC モードで **clear zone** コマンドを使用します。

```
clear zone {database | lock | statistics {lun-zoning | read-only-zoning}} vsan vsan-id
```

シンタックスの説明

database	ゾーンサーバデータベース情報を消去します。
lock	ゾーンサーバデータベース ロックを消去します。
statistics	ゾーンサーバ統計を消去します。
lun-zoning	Logical Unit Number (LUN) ゾーニング関連統計を消去します。
read-only-zoning	読み取り専用のゾーニング関連統計を消去します。
vsan	VSAN（仮想 SAN）のゾーン情報を消去します。
vsan-id	VSAN ID の有効範囲は、1 ~ 4093 です。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。
3.0(1)	lock オプションが追加されました。

使用上のガイドライン

clear zone database コマンドを実行したあと、次にスイッチを開始する場合に実行中のコンフィギュレーションが使用されるようにするため、ユーザは確実に **copy running-config startup-config** コマンドを実行する必要があります。

リモートスイッチから **clear zone lock** コマンドを使用すると、そのリモートスイッチのロックのみが消去されます。ロックを行ったスイッチから **clear zone lock** コマンドを使用すると、VSAN のすべてのロックが消去されます。



(注)

ロックを行ったスイッチのセッション ロックを消去する方法として、**no zone commit vsan** コマンドを使用することを推奨します。

例

次に、VSAN 1 のゾーンサーバ内の設定情報をすべて消去する例を示します。

```
switch# clear zone database vsan 1
```

関連コマンド

コマンド	説明
show zone	設定されたインターフェイスのゾーン情報を表示します。

cli alias name

コマンドエイリアス名を定義するには、コンフィギュレーションサブモードで **cli alias name** コマンドを使用します。ユーザ定義のコマンドエイリアスを削除するには、コマンドの **no** 形式を使用します。

cli alias name *command definition*

no cli alias name *command*

シンタックスの説明

<i>command</i>	エイリアス コマンド名を指定します。最大文字サイズは 30 です。
<i>definition</i>	エイリアス コマンド定義を指定します。最大文字サイズは 80 です。

デフォルト

alias コマンド

コマンドモード

コンフィギュレーションサブモード

コマンド履歴

リリース	変更内容
3.0(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

コマンドエイリアスを定義するときには、次の注意事項に従ってください。

- コマンドエイリアスは、すべてのユーザセッションに対してグローバルです。
- コマンドエイリアスは再起動後も変わりません。
- エイリアス化するコマンドは、省略しないですべて入力する必要があります。
- コマンド エイリアス変換は常にすべてのコンフィギュレーション モードまたはサブモードのすべてのキーワードの中で最優先されます。
- コマンド エイリアスのサポートはスイッチング モジュールではなく、スーパーバイザ モジュールでのみ利用できます。
- コマンドエイリアスの設定は、他のユーザセッションでただちに有効になります。
- **show cli alias** のエイリアスであるデフォルトのコマンドエイリアス **alias** は変更できません。
- コマンドエイリアスのネスティングは最大深度 1 まで許容されます。1 つのコマンドエイリアスは、有効なコマンドを参照する必要がある別のコマンドエイリアスを参照できますが、その他のコマンドエイリアスは参照できません。
- コマンドエイリアスは必ず、コマンドラインの最初のコマンドキーワードを置き換えます。
- EXEC モードまたはコンフィギュレーション サブモードでコマンド エイリアスを定義できません。

例

次に、コンフィギュレーションサブモードでコマンドエイリアスを定義する例を示します。

```
switch# config t
switch(config)# cli alias name gigint interface gigabitethernet
switch(config)# cli alias name shintbr show interface brief
switch(config)# cli alias name shfcintup "shintbr| include up | include fc"
```

デフォルトのコマンドエイリアス **alias** を使用すると、スイッチ上で定義されているコマンドエイリアスを表示できます。

次に、スイッチ上で定義されているコマンドエイリアスを表示する例を示します。

```
switch# alias
CLI alias commands
=====
alias :show cli alias
gigint :interface gigabitethernet
shintbr :show interface brief
shfcintup :shintbr | include up | include fc
```

関連コマンド

コマンド	説明
alias	show cli alias のデフォルトのエイリアス コマンドを表示します。
show cli alias	設定されたすべてのエイリアスを表示されます。

cli var name (EXEC)

CLI セッション期間のみ維持される CLI セッション変数を定義するには、EXEC モードまたはコンフィギュレーションサブモードで **cli var name** コマンドを使用します。

cli var name name value

ユーザ定義のセッション CLI 変数を削除するには、コマンドの **no** 形式を使用します。

cli no var name name

シンタックスの説明	name	変数名を指定します。最大文字サイズは 31 です。
	value	変数値を指定します。最大文字サイズは 80 です。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.0(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 CLI セッション変数は次のように使用されます。

- コマンドラインに直接入力します。
- 子スクリプトに渡し、**run-script** コマンドを使用して開始します。親シェルで定義された変数を子の **run-script** コマンドプロセスで使用できます。
- **run-script** コマンドのコマンドライン引数として渡します。
- 構文 \$(variable) を使用して参照します。

CLI 変数には、次の制限があります。

- ネストされた参照を使用して、別の変数から変数を参照することはできません。

例 次に、セッションのユーザ定義の CLI 変数を作成する例を示します。

```
switch# cli var name testinterface 3/4
```

次に、セッションのユーザ定義の CLI 変数を削除する例を示します。

```
switch# cli no var name testinterface 3/4
```

関連コマンド	コマンド	説明
	cli no var name	ユーザ定義のセッション CLI 変数を削除します。
	show cli variables	すべての CLI 変数を表示します (セッションおよびシステムで固定)。

cli var name (configuration)

CLI セッションおよびスイッチのリロード後も維持される CLI 変数を定義するには、コンフィギュレーション サブモードで **cli var name** コマンドを使用します。ユーザ定義の固定 CLI 変数を削除するには、コマンドの **no** 形式を使用します。

```
cli var name name value
```

```
no cli var name name
```

シンタックスの説明	name	変数名を指定します。最大文字サイズは 31 です。
	value	変数値を指定します。最大文字サイズは 80 です。

デフォルト なし

コマンドモード コンフィギュレーション サブモード

コマンド履歴	リリース	変更内容
	3.0(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 CLI 変数の使用方法は、次のとおりです。

- コマンドラインに直接入力します。
- 子スクリプトに渡し、**run-script** コマンドを使用して開始します。親シェルで定義された変数を子の **run-script** コマンドプロセスで使用できます。
- **run-script** コマンドのコマンドライン引数として渡します。
- 構文 `$(variable)` を使用して参照します。

CLI 変数には、次の制限があります。

- ネストされた参照を使用して、別の変数から変数を参照することはできません。

例 次に、ユーザ定義の固定 CLI 変数を作成する例を示します。

```
switch# config t
switch(config)# cli var name mgmtport mgmt 0
```

関連コマンド	コマンド	説明
	show cli variables	すべての CLI 変数を表示します (セッションおよびシステムで固定)。

clock

タイムゾーンおよび夏時間を設定するには、コンフィギュレーションモードで **clock** コマンドを使用します。この夏時間調整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。

clock {**summer-time** *summer-time-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes* | **timezone** *timezone-name hours-offset minute-offset*}

no clock {**summer-time** *summer-time-name start-week start-day start-month start-time end-week end-day end-month end-time offset-minutes* | **timezone** *timezone-name hours-offset minute-offset*}

シンタックスの説明

summer-time	夏時間のタイムゾーン名を指定します。
<i>summer-time-name</i>	夏時間のゾーン名を指定します。有効範囲は1～8文字です。
<i>start-week end-week</i>	開始の週および終了の週を指定します。有効範囲は1(1週目)～5(5週目)です。
<i>start-day end-day</i>	開始の日および終了の日を指定します。有効範囲は1～5(日曜日から土曜日)です。
<i>start-month end-month</i>	開始の月および終了の月を指定します。有効範囲は1～8文字(January から December)です。
<i>start-time end-time</i>	開始時間および終了時間を指定します。有効範囲は00:00～23:59です。
<i>offset-minutes</i>	夏時間オフセットを指定します。有効範囲は1～1440分です。
timezone	タイムゾーン名を指定します。
<i>timezone-name</i>	タイムゾーン名を指定します。有効範囲は1～8文字です。
<i>hours-offset</i>	オフセットタイムを時間単位で指定します。有効範囲は0～23です。数字の前に-23のようにダッシュを付けてください。
<i>minutes-offset</i>	オフセットタイムを分単位で指定します。有効範囲は0～59です。数字の前に-59のようにダッシュを付けてください。

デフォルト

Coordinated Universal Time (UTC; 協定世界時間) は GMT (グリニッジ平均時) と同じです。

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。
3.1(1)	timezone の新しい引数一式が追加されました。

使用上のガイドライン

適切な夏時間のゾーン名を指定してください。指定されていない場合は、デフォルト名が使用されます。

hours-offset 引数には、たとえば **-23** のように数字の前にダッシュを使用して指定します。
minutes-offset 引数には、たとえば **-59** のように数字の前にダッシュを使用して指定します。

例

次に、開始時刻が3月の第2週の日曜日午前2時で、終了時刻が11月の第1週の日曜日午前2時である太平洋夏時間を設定する例を示します。

```
switch# config t
switch# clock summer-time PDT 2 sunday march 02:00 1 sunday november 02:00 60
```

次に、タイムゾーンを太平洋標準時間に設定する例を示します。

```
switch# config t
switch(config)# clock timezone PST 0 0
```

関連コマンド

コマンド	説明
clock set	スイッチの時間を変更します。
show clock	現在の日付と時刻を表示します。
show run	他の設定情報とともに、変更したタイムゾーン設定を表示します。

clock set

Cisco MDS 9000 ファミリ スイッチ上のシステム時間を変更するには、EXEC モードで **clock set** コマンドを使用します。

```
clock set HH:MM:SS DD Month YYYY
```

シンタックスの説明

<i>HH</i>	軍用時間のフォーマット（15 は PM3 時）で、時間を 2 桁で指定します。
<i>MM</i>	分（58）を 2 桁で指定します。
<i>SS</i>	秒（15）を 2 桁で指定します。
<i>DD</i>	日付（12）を 2 桁で指定します。
<i>Month</i>	月を言葉で指定します（August）
<i>YYYY</i>	年（2002）を 4 桁で指定します。

デフォルト

なし

コマンドモード

EXEC モード

コマンド履歴

リリース	変更内容
1.0(2)	このコマンドが導入されました。

使用上のガイドライン

システムが、Network Time Protocol (NTP) クロックのような他の有効な時間装置と同期を取っている場合、またはスイッチにカレンダー機能が搭載されている場合、通常、システムクロックを設定する必要はありません。他の時間装置を使用できない場合、このコマンドを使用してください。このコマンドで指定された時間は、設定のタイムゾーンと関連します。

clock set コマンドによる変更は、システムがリセットしたあとも維持されます。

例

次に、**clock set** コマンドを表示する例を示します。

```
switch# clock set 15:58:15 12 August 2002
Mon Aug 12 15:58:00 PDT 2002
```

cloud discover

手動またはオンデマンドのクラウド検出を開始するには、**cloud discover** コマンドを使用します。

```
cloud discover [interface {gigabitethernet slot/port | port-channel port-channel-number}]
```

シンタックスの説明	interface	クラウド検出を行うインターフェイスを指定します。
	gigabitethernet slot/port	ギガビットイーサネットインターフェイスを指定します。
	port-channel port-channel-number	ポートチャネルインターフェイスを指定します。ポートチャネル数の有効範囲は、1～256です。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	3.0(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、Cisco MDS 9124 スイッチ、Cisco Fabric Switch for HP c-Class BladeSystem、Cisco Fabric Switch for IBM BladeCenter でサポートされていません。

例 次に、手動またはオンデマンドのクラウド検出を開始する例を示します。

```
switch# cloud discover
```

次に、ギガビットイーサネットインターフェイス 2/2 に対して手動またはオンデマンドのクラウド検出を開始する例を示します。

```
switch# cloud discover interface gigabitethernet 2/2
```

関連コマンド	コマンド	説明
	cloud discovery	クラウドディスカバリを設定します。
	cloud-discovery enable	クラウドメンバシップのディスカバリをイネーブルにします。
	show cloud discovery	クラウドに関する検出情報を表示します。
	show cloud membership	クラウドのメンバーに関する情報を表示します。

cloud discovery

クラウド検出を設定するには、コンフィギュレーション モードで **cloud discovery** コマンドを使用します。設定を削除するには、コマンドの **no** 形式を使用します。

```
cloud discovery {auto | fabric distribute | message icmp}
```

```
no cloud discovery {auto | fabric distribute | message icmp}
```

シンタックスの説明

auto	ファブリックの自動検出をイネーブルにします。
fabric distribute	クラウド検出のファブリック配信をイネーブルにします。
message icmp	検出メッセージの送信方法として Internet Control Message Protocol (ICMP) を設定します。

デフォルト

自動

コマンドモード

コンフィギュレーション モード

コマンド履歴

リリース	変更内容
3.0(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

iSNS サーバは、CFS を使用してすべてのスイッチにクラウドおよびメンバシップ情報を配信します。したがって、ファブリック内のすべてのスイッチのクラウドビューは同じです。



(注)

自動検出がディセーブルになっている場合は、インターフェイスの変更によって検出されないクラウドに属するメンバーが作成されます。新しいクラウドは形成されません。



(注)

このコマンドは、Cisco MDS 9124 スイッチではサポートされません。

例

次に、クラウドの自動検出をイネーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cloud discovery auto
```

次に、クラウドの自動検出のファブリック配信をイネーブルにする例を示します。

```
switch(config)# cloud discovery fabric distribute
```

次に、クラウドの自動検出のファブリック配信をディセーブルにする例を示します。

```
switch(config)# no cloud discovery fabric distribute
```

関連コマンド	コマンド	説明
	cloud discover	手動の、オンデマンドクラウドディスカバリを開始します。
	cloud-discovery enable	クラウドメンバシップのディスカバリをイネーブルにします。
	show cloud discovery	クラウド検出情報を表示します。
	show cloud membership	クラウドのメンバーに関する情報を表示します。

cloud-discovery enable

クラウドのメンバシップの検出をイネーブルにするには、コンフィギュレーション モードで **cloud-discovery** コマンドを使用します。クラウドのメンバシップの検出をディセーブルにするには、コマンドの **no** 形式を使用します。

cloud-discovery enable

no cloud-discovery 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 コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	3.0(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、Cisco MDS 9124 スイッチではサポートされません。

例 次に、クラウドのメンバシップの検出をイネーブルにする例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# cloud-discovery enable
```

次に、クラウドのメンバシップの検出をディセーブルにする例を示します。

```
switch(config)# no cloud-discovery enable
```

関連コマンド	コマンド	説明
	cloud discover	手動の、オンデマンドクラウドディスカバリを開始します。
	cloud discovery	クラウドディスカバリを設定します。
	show cloud	クラウド検出およびメンバシップの情報を表示します。

cluster

クラスタ機能を設定するには、**cluster** コマンドを使用します。

cluster enable

シンタックスの説明	enable	クラスタをイネーブルまたはディセーブルにします。
デフォルト	なし	
コマンドモード	コンフィギュレーションモード	
コマンド履歴	リリース	変更内容
	3.2(2)	このコマンドが導入されました。
使用上のガイドライン	なし	
例	次に、Cisco SME クラスタリングをイネーブルにする例を示します。 <pre>switch# config terminal switch(config)# cluster enable switch(config)#</pre>	
関連コマンド	コマンド	説明
	show sme cluster	Cisco SME クラスタの情報を表示します。

code-page

EBCDIC（拡張 2 進化 10 進コード）フォーマットを設定するには、**code-page** コマンドを使用します。この設定をディセーブルにするか、またはデフォルトの設定に戻すには、コマンドの **no** 形式を使用します。

code-page brazil | france | international-5 | italy | japan | spain-latinamerica | uk | us-canada

シンタックスの説明

code-page	Fibre Connection (FICON) がイネーブルの VSAN（仮想 SAN）上で、コードページを設定します。
brazil	brazil EBCDIC フォーマットを設定します。
france	france EBCDIC フォーマットを設定します。
international-5	international-5 EBCDIC フォーマットを設定します。
italy	italy EBCDIC フォーマットを設定します。
japan	japan EBCDIC フォーマットを設定します。
spain-latinamerica	spain-latinamerica EBCDIC フォーマットを設定します。
uk	uk EBCDIC フォーマットを設定します。
us-canada	us-canada EBCDIC フォーマットを設定します。

デフォルト

なし

コマンド モード

コンフィギュレーション モード

コマンド履歴

リリース	変更内容
1.3(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

この設定は任意のものです。使用する EBCDIC（拡張 2 進化 10 進コード）フォーマットがわからない場合は、**us-canada** オプション（デフォルト）のままにすることを推奨します。

例

次に、**italy** EBCDIC フォーマットを設定する例を示します。

```
switch(config)# ficon vsan 2
switch(config-ficon)# code-page italy
```

次に、**us-canada** EBCDIC フォーマットを使用した工場出荷時の状態に戻す例を示します。

```
switch(config-ficon)# no code-page
```

関連コマンド

コマンド	説明
show ficon	設定された FICON の詳細を表示します。
ficon vsan vsan-id	指定の VSAN（仮想 SAN）上で FICON をイネーブルにします。

commit

処理中の Call Home コンフィギュレーションセッションに、関連性のある設定中の内容を適用するには、Call Home コンフィギュレーションサブモードで **commit** コマンドを使用します。

commit

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 Call Home コンフィギュレーションサブモード

コマンド履歴	リリース	変更内容
	2.0(1b)	このコマンドが導入されました。

使用上のガイドライン Cisco Fabric Services (CFS) 配信をイネーブルにしてから Call Home コンフィギュレーションを実行してください。

例 次に、Call Home コンフィギュレーションコマンドを実行する例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# commit
```

関連コマンド	コマンド	説明
	callhome	Call Home 機能を設定します。
	callhome test	ダミーのテストメッセージを設定された 1 つまたは複数の宛先へ送信します。
	show callhome	設定された Call Home 情報を表示します。

contract-id

Call Home 機能でカスタマーのサービス契約 ID を設定するには、**contract-id** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

```
contract-id customer-id
```

```
no contract-id customer-id
```

シンタックスの説明	<i>contract-id</i>	(任意) カスタマーのサービス契約 ID を設定します。契約番号に最大 64 文字まで使用できます。
-----------	--------------------	--

デフォルト	なし
-------	----

コマンド モード	Call Home コンフィギュレーション サブモード
----------	-----------------------------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン	なし
------------	----

例 次に、Call Home コンフィギュレーションで契約 ID を設定する例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# contract-id Customer1234
```

関連コマンド	コマンド	説明
	callhome	Call Home 機能を設定します。
	callhome test	ダミーのテスト メッセージを設定された 1 つまたは複数の宛先へ送信します。
	show callhome	設定された Call Home 情報を表示します。

configure terminal

コンフィギュレーション モードを開始するには、EXEC モードで **configure terminal** コマンドを使用します。

configure terminal

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 EXEC モード

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン なし

例 次に、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)#
```

次に、コマンドの省略フォーマットを使用してコンフィギュレーション モードにする例を示します。

```
switch# config terminal
switch(config)#
```

copy

システム ソフトウェアのバックアップを保存するには、EXEC モードで **copy** コマンドを使用します。

copy *source-URL destination-URL*

シンタックスの説明

<i>source-URL</i>	コピー元ファイルまたはディレクトリの URL、またはエイリアス
<i>destination-URL</i>	コピーしたファイルまたはディレクトリの宛先 URL、またはエイリアス

次のテーブルに、コピー元およびコピー先 URL のエイリアスを一覧表示します。

running-config	スイッチで現在実行されている設定を指定します。 system:running-config キーワードは現在の実行コンフィギュレーション ファイルを意味します。
startup-config	初期化中 (起動時) に使用される設定を指定します。NVRAM (不揮発性 RAM) からスタートアップ コンフィギュレーションをコピーできます。 nvram:startup-config キーワードは、初期化中に使用するコンフィギュレーション ファイルを意味します。
bootflash:	内部ブートフラッシュ メモリの場所を指定します。
log:	ログ ファイル システムの場所を指定します。
slot0:	コンパクトフラッシュ メモリまたは PCMCIA カードの場所を指定します。
volatile:	揮発性ファイル システムの場所を指定します。
system:	実行コンフィギュレーションを含むシステムのメモリ場所を指定します。
fabric	実行コンフィギュレーション (ソース) ファイルにあるすべてのリモート スイッチを、スタートアップ コンフィギュレーション (コピー先) ファイルにコピーするには、Cisco Fabric Services (CFS) を使用して、ファブリック全体のスタートアップ コンフィギュレーションの更新を指定します。このコマンドの構文は次のとおりです。 copy running-config startup-config fabric
tftp:	Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) ネットワーク サーバの場所を指定します。このエイリアスの構文は、 tftp:[[/location]/directory]/filename です。
ftp:	FTP (ファイル転送プロトコル) ネットワーク サーバの場所を指定します。このエイリアスの構文は、 ftp:[[/location]/directory]/filename です。
scp:	Secure Copy (scp) ネットワーク サーバの場所を指定します。このエイリアスの構文は、 scp:[[/location]/directory]/filename です。
sftp:	Secure Trivial File Transfer Protocol (SFTP) ネットワーク サーバの場所を指定します。このエイリアスの構文は、 sftp:[[/location]/directory]/filename です。
log:	同一のディレクトリに保存されているログ ファイルの場所を指定します。
debug:	デバッグ パーティションに保存されているデバッグ ファイルの場所を指定します。
nvram:	スイッチの NVRAM (不揮発性 RAM) を指定します。
core:	スイッチングまたはスーパーバイザ モジュールから、外部フラッシュ (スロット 0) または TFTP サーバへのコアの場所を指定します。
<i>filename</i>	フラッシュ ファイル名を指定します。
sup-1	スーパーバイザ モジュールの数です。sup-1 はスロット 5 スーパーバイザ (アクティブ) で、sup-2 はスロット 6 スーパーバイザ (スタンバイ) です。
sup-2	

デフォルト

なし

コマンドモード EXEC モード

コマンド履歴

リリース	変更内容
1.3(4)	コマンドが変更されました。
2.1(1a)	fabric キーワードおよびその機能が追加されました。

使用上のガイドライン

このコマンドは、ソフトウェアの実行コピーとバックアップのコピーを同一にします。

ファイルのコピーはアクティブなスーパーバイザからスタンバイ スーパーバイザに対して実行され、スタンバイからアクティブへの方向では実行されません。

このコマンドは、127.x.x.x IP アドレスを許可しません。

コピー機能は、ディレクトリで必要なスペースが確保できない場合、正常に完了しません。はじめに、必要なディレクトリへ移動して (例: **cd bootflash:**)、利用できるスペースを確認してください (例: **dir bootflash:**)。

コピー処理は全体で、数分かかる場合があります。

外部からファイルを直接スタンバイ スーパーバイザにコピーしないでください。外部からファイルをコピーする場合、必ずアクティブなスーパーバイザにコピーしてから、スタンバイ スーパーバイザにファイルを保存します。

コアは、(アクティブ スーパーバイザ モジュール、スタンバイ スーパーバイザ モジュール、または任意のスイッチング モジュールから) 外部フラッシュ (スロット 0) または TFTP サーバに、次の 2 つの方法のうちいずれかで保存できます。

- オンデマンド — 指定されたプロセス ID に基づいたファイルを単一でコピーします。
- 定期的 — ユーザが設定した頻度でコア ファイルを定期的にコピーします。

copy log:messages コマンドを使用して、ログファイルを異なる場所にコピーできます。

デバッグ パーティションには、トラブルシューティングの目的でソフトウェアが生成したデバッグ ファイルが含まれます。

running-config startup-config fabric パラメータを使用すると、CFS を使用して、強制的にファイバチャネル ファブリック内のすべてのスイッチの実行コンフィギュレーション (ソース) をスタートアップ コンフィギュレーション (コピー先) にコピーさせることができます。



(注)

リモート スイッチが **copy running-config startup-config fabric** 処理に失敗している場合、最初のスイッチもスタートアップ コンフィギュレーションの保存に失敗していることとなります。つまり、リモート スイッチと最初のスイッチは両方ともスタートアップ コンフィギュレーションの保存に失敗していることとなります (旧スタートアップ コンフィギュレーションに戻ります)。ネットワーク内の他のスイッチはすべて成功していることとなります。

例

次に、スタートアップ コンフィギュレーションに、使用しているコンフィギュレーション ファイルを保存する例を示します。

```
switch# copy system:running-config nvram:startup-config
```

次に、slot0 ディレクトリの samplefile というファイルを mystorage ディレクトリにコピーする例を示します。

```
switch# copy slot0:samplefile slot0:mystorage/samplefile
```

次に、現在のディレクトリ レベルからファイルをコピーする例を示します。

```
switch# copy samplefile mystorage/samplefile
```

現在のディレクトリが slot0:mydir の場合、このコマンドは slot0:mydir/samplefile から slot0:mydir/mystorages/samplefile にコピーします。

次に、外部コンパクトフラッシュからコンフィギュレーション ファイルをダウンロードし、実行コンフィギュレーションに適用する例を示します。

```
switch copy slot0:dns-config.cfg system:running-config
```

次に、外部コンパクトフラッシュに、実行コンフィギュレーション ファイルを保存する例を示します。

```
switch# copy system:running-config slot0:dns-config.cfg
```

次に、外部コンパクトフラッシュに、スタートアップ コンフィギュレーション ファイルを保存する例を示します。

```
switch# copy system:startup-config slot0:dns-config.cfg
```

次に、CFS を使用して、ファブリック内のすべてのスイッチの実行コンフィギュレーション (ソース) ファイルをスタートアップ コンフィギュレーション (コピー先) ファイルにコピーさせる例を示します。

```
switch# copy running-config startup-config fabric
[#####] 100%
switch#
```



(注)

リモート スイッチが **copy running-config startup-config fabric** 処理に失敗している場合、最初のスイッチもスタートアップ コンフィギュレーションの保存に失敗していることとなります。つまり、リモート スイッチと最初のスイッチは両方ともスタートアップ コンフィギュレーションの保存に失敗していることとなります (旧スタートアップ コンフィギュレーションに戻ります)。ネットワーク内の他のスイッチはすべて成功していることとなります。

次に、バイナリ設定のバックアップ コピーを作成する例を示します。

```
switch# copy nvram:startup-config nvram:snapshot-config
```

次に、アクティブなスーパーバイザ上のブートフラッシュのイメージを、スタンバイ スーパーバイザのブートフラッシュにコピーする例を示します。

```
switch# copy bootflash:myimage bootflash://sup-2/myimage
```

次に、ブートフラッシュにある実行コンフィギュレーションのコピーを作成する例を示します。

```
switch# copy system:running-config bootflash:my-config
```

次に、ブートフラッシュにあるスタートアップ コンフィギュレーションのコピーを作成する例を示します。

```
switch# copy nvram:startup-config bootflash:my-config
```

関連コマンド

コマンド	説明
cd	デフォルトのディレクトリまたはファイル システムを変更します。
dir	ファイル システムのファイルの一覧を表示します。
reload	オペレーティング システムをリロードします。
show version	実行コンフィギュレーション ファイルのバージョンを表示します。

copy licenses

インストールされたライセンス ファイルのバックアップを保存するには、EXEC モードで **copy licenses** コマンドを使用します。

copy licenses *source-URL destination-URL*

シンタックスの説明	<i>source-URL</i>	<i>destination-URL</i>
	コピー元ファイルまたはディレクトリの URL、またはエイリアス	コピーしたファイルまたはディレクトリの宛先 URL、またはエイリアス

次のテーブルに、コピー元およびコピー先 URL のエイリアスを一覧表示します。

bootflash:	内部ブートフラッシュ メモリの場所を指定します。
slot0:	コンパクトフラッシュ メモリまたは PCMCIA カードの場所を指定します。
volatile:	揮発性ファイル システムの場所を指定します。
filename	拡張子が tar のライセンス ファイルの名前を指定します。

デフォルト なし

コマンドモード EXEC モード

コマンド履歴	リリース	変更内容
	1.3(4)	このコマンドが導入されました。

使用上のガイドライン コピー機能は、ディレクトリに必要なスペースが確保できない場合、正常に完了しません。はじめに、必要なディレクトリへ移動して（例：**cd bootflash:**）、利用できるスペースを確認してください（例：**dir bootflash:**）。

ライセンス ファイルは、インストール後すぐ、**write erase** コマンドを実行する直前にバックアップを行うよう推奨します。

例 次に、Enterprise.tar という名前のファイルを bootflash: ディレクトリに保存する例を示します。

```
switch# copy licenses bootflash:/Enterprise.tar
Backing up license done
```

関連コマンド	コマンド	説明
	cd	デフォルトのディレクトリまたはファイル システムを変更します。
	dir	ファイル システムのファイルの一覧を表示します。
	install license	ライセンス ファイルをインストールします。

copy ssm-nvram standby-sup

Storage Services Module (SSM; ストレージサービス モジュール) NVRAM のコンテンツをスタンバイ スーパーバイザ 2 モジュールにコピーするには、EXEC モードで **copy ssm-nvram standby-sup** コマンドを使用します。

copy ssm-nvram standby-sup

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 EXEC モード

コマンド履歴	リリース	変更内容
	3.0(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、スーパーバイザ 1 モジュールからスーパーバイザ 2 モジュールに移行する場合にのみ使用してください。スイッチの両方のモジュールが同じ場合は、このコマンドの代わりに **copy** コマンドを使用してください。

例 次に、SSM NVRAM のコンテンツをスタンバイ スーパーバイザ 2 モジュールにコピーする例を示します。

```
switch# copy ssm-nvram standby-sup
```

関連コマンド	コマンド	説明
	copy	システム ソフトウェアのバックアップを保存します。

crypto ca authenticate

CA 証明書を関連付けて認証を行い、その CA 証明書（または証明書チェーン）を設定するには、コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。これは Privacy Enhanced Mail (PEM; プライバシー エンハンスド メール) 符号化形式の CA 証明書または証明書チェーンが利用できるようになっていることを前提としています。

crypto ca authenticate trustpoint-label

シンタックスの説明	<i>trustpoint-label</i>	トラスト ポイント名を指定します。最大文字サイズは 64 です。
デフォルト		なし
コマンドモード		コンフィギュレーション モード
コマンド履歴	リリース	変更内容
	3.0(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、CA の公開鍵を含む CA の自己署名証明書を取得することでスイッチに対して CA を認証します。CA は自身の証明書に署名をしているため、このコマンドの実行時に CA 管理者に連絡して CA の公開鍵を手動で認証する必要があります。

CA サポートをスイッチに初めて設定する場合には、このコマンドが必要です。CA 認証を行う前に、まず **crypto ca trustpoint** コマンドを使用してトラスト ポイントを作成します。CA 証明書のフィンガープリント（証明書の MD5 または SHA ハッシュ）は通常 CA により発行されます。CA の認証時に、証明書のフィンガープリントが表示されます。管理者は、このフィンガープリントと CA により発行されたフィンガープリントを比較して、一致する場合にのみ CA 証明書を受け入れます。

認証される CA が Subordinate CA (SCA; 下位認証局) である場合（つまり自己署名ではない場合）、別の CA により認証され、次にこの別の CA がまた別の CA により認証され、というように自己署名 CA に到達するまで認証が行われます。この場合、最初の SCA にはそれを認証する CA チェーンがあるとされます。CA 認証中に、チェーン全体を提供する必要があります。サポートされる CA 証明書チェーンの最大長は、10 です。

トラスト ポイント CA は、信頼された CA としてスイッチに設定されている CA です。ローカルで信頼されている CA またはその下位の CA により署名されているピア証明書を取得した場合は、すべて受け入れられます。



(注)

crypto ca trustpoint コマンドを使用して設定されたトラスト ポイントは、**copy running-config startup-config** コマンドを使用して明示的に保存された場合にのみ維持されます。トラスト ポイントがスタートアップ コンフィギュレーションですでに保存されている場合は、そのトラスト ポイントに関連する証明書および Certificate Revocation List (CRL; 証明書失効リスト) は自動的に維持されます。逆に、トラスト ポイントがスタートアップ コンフィギュレーションで保存されなかった場合は、そのトラスト ポイントに関連する証明書および CRL は、スイッチのリポート後に対応するトラスト ポイントがない状態では存在しないため自動的に維持されません。

設定された証明書、CRL、およびキー ペアが維持されていることを確認するには、実行している設定をスタートアップ コンフィギュレーションに必ず保存してください。

例

次に、admin-ca という CA 証明書を認証する例を示します。

```
switch# config terminal
switch(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIC4jCCAoygAwIBAgIQBWD5Iay0GZRPSRIljK0ZejanBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYWlhbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAkIO
MRIwEAYDVQQQIEw1LYXJuYXRha2ExEjAQBgNVBACTCUJhbmdbG9yZTEOMAwGA1UE
ChMFQ2l2Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWwFuZGt1QG9pc2NvLmNvbTELMakGA1UEBhMCSU4xEjAQBgNVBAGTCUth
cm5hdGFrYTESMBAGA1UEBxMjQ2MzFsb3JlMQ4wDAYDVQQKEwVDAxNjBzETMBEG
A1UECXMkbnV0c3RvcnFmZTESMBAGA1UEAxMjQXBhcm5hIENBMFwvDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzlunccNM87ypyzwuoSNZXOMpeRXXI
OzyBAGiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyYjRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwOC6gLiYqZmlsZTovL1xccc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTlIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaQNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfg1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
```

Do you accept this certificate? [yes/no]:y

関連コマンド

コマンド	説明
crypto ca trustpoint	トラスト ポイントを設定します。
show crypto ca certificates	設定済トラスト ポイント証明書を表示します。
show crypto ca trustpoints	トラスト ポイント設定を表示します。

crypto ca crl request

CA からダウンロードした新しい Certificate Revocation List (CRL; 証明書失効リスト) を設定するには、コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

```
crypto ca crl request trustpoint-label source-file
```

シンタックスの説明	
<i>trustpoint-label</i>	トラスト ポイント名を指定します。最大文字サイズは 64 です。
<i>source-file</i>	CRL の場所を bootflash: ファイル名の形式で指定します。最大文字サイズは 512 です。

デフォルト なし

コマンドモード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	3.0(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 Cisco MDS SAN-OS では、トラスト ポイントの CRL を事前にダウンロードし、**crypto ca crl request** コマンドを使用してこの CRL を証明書ストアにキャッシュできます。IPSec/IKE または SSH によるピア証明書の確認中には、すでに CRL がローカルに設定されており、CRL を使用した失効チェックが設定されている場合にのみ、発行元 CA の CRL が参照されます。それ以外で、他の失効チェック方式も設定されていない場合には、CRL チェックは実行されず、証明書は失効していないものと見なされます。この CRL チェックのモードは、オプションの CRL と呼ばれます。

これ以外の失効チェックのモードは、ベストエフォートの CRL または必須 CRL と呼ばれます。これらのモードでは、CRL がローカルで見つからない場合は、CA から自動的に取得しようとします。これらのモードは、MDS SAN-OS Release 3.0(1) ではサポートされません。

指定された CRL ファイルには、Privacy Enhanced Mail (PEM; プライバシー エンハンスド メール) 形式または Distinguished Encoding Rules (DER) 形式の最新の CRL が含まれています。



(注)

crypto ca trustpoint コマンドを使用して設定されたトラスト ポイントは、**copy running-config startup-config** コマンドを使用して明示的に保存された場合にのみ維持されます。トラスト ポイントがスタートアップ コンフィギュレーションですでに保存されている場合は、そのトラスト ポイントに関連する証明書および Certificate Revocation List (CRL; 証明書失効リスト) は自動的に維持されます。逆に、トラスト ポイントがスタートアップ コンフィギュレーションで保存されなかった場合は、そのトラスト ポイントに関連する証明書および CRL は、スイッチのリブート後に対応するトラスト ポイントがない状態では存在しないため自動的に維持されません。

設定された証明書、CRL、およびキー ペアが維持されていることを確認するには、実行している設定をスタートアップ コンフィギュレーションに必ず保存してください。

例 次に、トラスト ポイントの CRL を設定するか、現在の CRL を置き換える例を示します。

```
switch# config t
switch(config)# crypto ca crl request admin-ca bootflash:admin-ca.crl
```

関連コマンド	コマンド	説明
	revocation-check	トラスト ポイントの失効チェック方式を設定します。
	show crypto ca crl	設定されている CRL を表示します。

crypto ca enroll

このトラスト ポイント CA 用に作成された、スイッチの RSA キー ペアの証明書を要求するには、コンフィギュレーションモードで **crypto ca enroll** コマンドを使用します。

crypto ca enroll trustpoint-label

シンタクスの説明	trustpoint-label	トラスト ポイント名を指定します。最大文字サイズは 64 です。
----------	------------------	----------------------------------

デフォルト なし

コマンドモード コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	3.0(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 アイデンティティを証明書の形式で取得するために、MDS スイッチをトラスト ポイント CA に登録できます。スイッチを複数のトラスト ポイントに登録することで、各トラスト ポイントから別々のアイデンティティ証明書を取得できます。

トラスト ポイントに登録する場合は、認証対象の RSA キー ペアを指定する必要があります。登録要求を生成する前に、このキー ペアを生成してトラスト ポイントに関連付ける必要があります。トラスト ポイント、キー ペア、およびアイデンティティ証明書間の関連付けを無効するには、関連付けを必ず次の順序で削除します。まずアイデンティティ証明書を削除し、次にキー ペアの関連付けを解除して CA 証明書を削除し、最後にトラスト ポイント自体を削除します。

認証された CA に対応する各トラスト ポイントからアイデンティティ証明書を取得する要求を生成するには、**crypto ca enroll** コマンドを使用します。生成される Certificate Signing Request (CSR) は、Public-Key Cryptography Standards (PKCS) #10 規格であり、PEM 形式で表示されます。これをカット アンド ペーストして、電子メールまたは CA Web サイトから対応する CA に送信します。CA 管理者は証明書を発行し、Web サイト経由で、または電子メールで送信して利用できるようにします。取得したアイデンティティ証明書は、**crypto ca import trustpoint-label certificate** コマンドを使用して対応するトラスト ポイントにインポートする必要があります。

チャレンジパスワードは設定に保存されません。このパスワードは、証明書を失効する必要がある場合に必要となるため、覚えておく必要があります。

例

次に、承認された CA の証明書要求を生成する例を示します。

```
switch# config t
switch(config)# crypto ca enroll myCA
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Password:nbv123
The subject name in the certificate will be: Vegas-1.cisco.com
Include the switch serial number in the subject name? [yes/no]:no
Include an IP address in the subject name [yes/no]:yes
ip address:172.22.31.162
The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5MqNIgJ2kt8r141KY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjucXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhhVpj+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsGSIb3DQEJ
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEBBQADgYEAKT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PftNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2bktExiI6U188nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

関連コマンド

コマンド	説明
<code>crypto ca import trustpoint-label certificate</code>	CA から取得したアイデンティティ証明書をトラストポイントにインポートします。
<code>crypto key generate rsa</code>	RSA キーペアを生成します。
<code>rsakeypair</code>	RSA キーペアの詳細を設定し、トラストポイントと関連付けます。
<code>show crypto key mypubkey rsa</code>	すべての RSA 公開鍵の設定を表示します。

crypto ca export

トラスト ポイントの RSA キー ペアおよび関連する証明書（アイデンティティおよび CA）を Public-Key Cryptography Standards（PKCS）#12 形式ファイルで別の場所にエクスポートするには、コンフィギュレーション モードで **crypto ca export** コマンドを使用します。

```
crypto ca export trustpoint-label pkcs12 destination-file-url pkcs12-password
```

シンタックスの説明		
<i>trustpoint-label</i>		トラスト ポイント名を指定します。最大文字サイズは 64 です。
pkcs12 <i>destination-file-url</i>		宛先ファイルを bootflash: ファイル名の形式で指定します。最大文字サイズは 512 です。
<i>pkcs12-password</i>		エクスポート ファイル内の RSA 秘密鍵を保護するために使用するパスワードを指定します。最大文字サイズは 64 です。

デフォルト なし

コマンドモード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	3.0(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 バックアップの目的で、アイデンティティ証明書を関連する RSA キー ペアおよび CA 証明書とともに、PKCS #12 形式ファイルにエクスポートできます。スイッチでのシステム クラッシュから回復するために、証明書および RSA キー ペアを後でインポートできます。

例 次に、証明書およびキー ペアを PKCS #12 形式でエクスポートする例を示します。

```
switch# config terminal
switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

関連コマンド	コマンド	説明
	crypto ca import <i>trustpoint-label</i> certificate	CA から取得したアイデンティティ証明書をトラスト ポイントにインポートします。
	crypto ca import <i>trustpoint-label</i> pkcs12	アイデンティティ証明書および関連する RSA キー ペアと CA 証明書（チェーン）をトラスト ポイントにインポートします。
	crypto key generate rsa	RSA キー ペアを生成します。
	rsa keypair	RSA キー ペアの詳細を設定し、トラスト ポイントと関連付けます。
	show crypto key mypubkey rsa	RSA 公開鍵の設定を表示します。

crypto ca import

アイデンティティ証明書のみを PEM 形式でインポートしたり、アイデンティティ証明書および関連する RSA キー ペアと CA 証明書（または証明書チェーン）を Public-Key Cryptography Standards (PKCS) #12 形式でインポートするには、コンフィギュレーション モードで **crypto ca import** コマンドを使用します。

```
crypto ca import trustpoint-label {certificate | pkcs12 source-file-url pkcs12-password}
```

シンタックスの説明	trustpoint-label	トラスト ポイント名を指定します。最大文字サイズは 64 です。
	pkcs12 source-file-url	宛先ファイルを bootflash: ファイル名の形式で指定します。最大文字サイズは 512 です。
	pkcs12-password	インポートされた PKCS #12 ファイルで RSA 秘密鍵を保護するために使用されたパスワードを指定します。最大文字サイズは 64 です。

デフォルト なし

コマンド モード コンフィギュレーション モード

コマンド履歴	リリース	変更内容
	3.0(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 コマンドの最初の形式である **crypto ca import trustpoint-label certificate** は、トラスト ポイントで以前に生成され、CA に送信された登録要求に応じて、CA から取得されたアイデンティティ証明書をインポートする（つまりカット アンド ペーストする）ために使用されます。管理者は、証明書をカット アンド ペーストするよう求められます。

コマンドの 2 番目の形式である **crypto ca import trustpoint-label pkcs12 source-file-url pkcs12-password** は、空のトラスト ポイントに完全なアイデンティティ情報（つまり、アイデンティティ証明書および関連する RSA キー ペアと CA 証明書または証明書チェーン）をインポートするために使用されます。システムがダウンしたときに設定をリストアする場合に、このコマンドは便利です。



(注) **crypto ca trustpoint** コマンドを使用して設定されたトラスト ポイントは、**copy running-config startup-config** コマンドを使用して明示的に保存された場合にのみ維持されます。トラスト ポイントがスタートアップ コンフィギュレーションですでに保存されている場合は、そのトラスト ポイントに関連する証明書および Certificate Revocation List (CRL; 証明書失効リスト) は自動的に維持されます。逆に、トラスト ポイントがスタートアップ コンフィギュレーションで保存されなかった場合は、そのトラスト ポイントに関連する証明書および CRL は、スイッチのリブート後に対応するトラスト ポイントがない状態では存在しないため自動的に維持されません。

設定された証明書、CRL、およびキー ペアが維持されていることを確認するには、実行している設定をスタートアップ コンフィギュレーションに必ず保存してください。

例 次に、以前に作成および送信された登録依頼に応じて CA から取得されたアイデンティティ証明書
をインストールする例を示します。

```
switch# config t
switch(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6ggAwIBAgIKCj00oQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmrRrZUBjaXNjby5jb20xCzAJBgNVBAYTAK1OMRIwEAYD
VQQIEw1LYXJlYXRha2ExEjAQBGNVBAcTCUJhbmdbG9yZTEOMAwGA1UEChMFQ21z
Y28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJlYXNjby5jb20w
NTEwMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwGjAYBgNVBAMTEVZlZ2FzLzE2
Y21zY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfk5eJSmNCQujGpzcKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYA8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/Bsw
GYIRVmVnYXMTMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBGNVHSMEGcQwgcGAFCCo8kaDG6wjTEVNjskyYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZiIhvcNAQkBFhFhbWVfZGt1QGNpc2NvLmNvbTELMakGA1UE
BhMCSU4xEjAQBGNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMjQmFuZ2Fsb3JlMQ4w
DAYDVQQKEWVdaXNjbyETMBEGA1UECXMkbnV0c3RvcnFnZTESMBAGA1UEAxMjQXBh
cm5hIENBghAFYNKJrLQZLE9JEiWMrRl6MGsGA1UdHwRkMGiWlqAsocGKGH0dHA6
Ly9zc2UtdmGvQ2VydeVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAUocYgKkZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJlYXNjby5jb20wNTEwMTIwMzEyNDBa
AQEEfjB8MDSGCCsGAQUFBzAChi9odHRwOi8vc3N1LTA4L0N1cnRfbnJvbGwvc3N1
LTA4X0FwYXJlYXNjbyMENBmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xc3N1LTA4
XEN1cnRfbnJvbGwvc3N1LTA4X0FwYXJlYXNjbyMENBmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbE7GNLh9xeOTWBNbm24U69ZSuDdcOcUzUUTgrpnTqVpPyejtSyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
```

次に、証明書およびキーペアを PKCS #12 形式ファイルでエクスポートする例を示します。

```
switch# config t
witch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123
```

関連コマンド

コマンド	説明
<code>crypto ca export trustpoint-label pkcs12</code>	トラストポイントの RSA キーペアおよび関連する証明書をエクスポートします。
<code>crypto ca enroll</code>	トラストポイントの Certificate Signing Request (CSR) を生成します。
<code>crypto key generate rsa</code>	RSA キーペアを生成します。
<code>rsakeypair</code>	トラストポイントの RSA キーペアの詳細を設定します。
<code>show crypto ca certificates</code>	アイデンティティ証明書および CA 証明書の詳細を表示します。
<code>show crypto key mypubkey rsa</code>	RSA 公開鍵の設定を表示します。

crypto ca test verify

証明書ファイルを検証するには、コンフィギュレーション モードで **crypto ca test verify** コマンドを使用します。

crypto ca test verify *certificate-file*

シンタックスの説明	<i>certificate-file</i>	証明書のファイル名を bootflash: ファイル名の形式で指定します。最大文字サイズは 512 です。
-----------	-------------------------	--

デフォルト	なし
-------	----

コマンドモード	コンフィギュレーション モード
---------	-----------------

コマンド履歴	リリース	変更内容
	3.0(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 **crypto ca test verify** コマンドはテスト用コマンドです。このコマンドは、設定されている信頼された CA を使用して、必要に応じて失効チェック設定に従って Certificate Revocation List (CRL; 証明書失効リスト) または OCSP を参照することで、指定の PEM 形式の証明書を検証します。

例 次に、証明書ファイルを検証する例を示します。ステータス コード 0 が確認できれば、検証は成功です。

```
switch(config)# crypto ca test verify bootflash:id1.pem
verify status oode:0
verify error msg:
```

関連コマンド	コマンド	説明
	show crypto ca certificates	設定済トラスト ポイント証明書を表示します。

crypto ca trustpoint

スイッチが信頼するトラスト ポイント CA を作成して、トラスト ポイント コンフィギュレーションサブモードを開始するには、**crypto ca trustpoint** コマンドを使用します。トラスト ポイントを削除するには、コマンドの **no** 形式を使用します。

crypto ca trustpoint *trustpoint-label*

no crypto ca trustpoint *trustpoint-label*

シンタックスの説明	<i>trustpoint-label</i>	トラスト ポイント名を指定します。最大文字サイズは 64 です。
デフォルト		なし
コマンド モード		コンフィギュレーション モード
コマンド履歴	リリース	変更内容
	3.0(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	<p>トラスト ポイントには次の特徴があります。</p> <ul style="list-style-type: none"> • トラスト ポイントは、MDS スイッチが任意のアプリケーションについてピア証明書を検証するために信頼する 1 つの CA に相当します。 • CA は、crypto ca authenticate コマンドを使用して、CA 認証プロセスを使用するトラスト ポイントに明示的に関連付けられている必要があります。 • MDS スイッチは多数のトラスト ポイントを保持することができ、スイッチ上のアプリケーションはすべてそのトラスト ポイント CA のいずれかから発行されたピア証明書を信頼できます。 • トラスト ポイントは、特定のアプリケーションには限定されません。 • MDS スイッチは、それ自身のアイデンティティ証明書を取得するためにトラスト ポイント CA に任意で登録されます。
------------	---

1 つまたは複数のトラスト ポイントをアプリケーションに指定する必要はありません。すべてのアプリケーションは、どのトラスト ポイントから発行された証明書でも、証明書の目的がアプリケーションの要件を満たしている限りは使用できる必要があります。

トラスト ポイントからの保証証明書や、トラスト ポイントに関連付けられるキー ペアは 1 つあれば十分です。CA が指定したアイデンティティ (名前) を検証するのは 1 度だけであり、同じサブジェクト名を持つ複数の証明書を発行することはありません。1 つの CA について複数のアイデンティティ証明書が必要な場合は、CA が同じサブジェクト名の複数の証明書を発行できるように、同じ CA に別のトラスト ポイントを定義し、別のキー ペアをそれに関連付け、これに対して検証を行います。



(注)

no crypto ca trustpoint コマンドを使用してトラスト ポイントを削除する前に、まずアイデンティティ証明書および CA 証明書 (または証明書チェーン) を削除してから、RSA キー ペアのトラスト ポイントとの関連付けを解除します。トラスト ポイントが証明書とともに誤って削除されないようにするため、スイッチはこの動作を強制します。

例 次に、スイッチが信頼するトラストポイント CA を宣言して、トラストポイント 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 terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)#
```

次に、トラストポイント CA を削除する例を示します。

```
switch# config terminal
switch(config)# no crypto ca trustpoint admin-ca
```

関連コマンド

コマンド	説明
<code>crypto ca authenticate</code>	認証局の証明書を認証します。
<code>crypto ca enroll</code>	トラストポイントの Certificate Signing Request (CSR) を生成します。
<code>show crypto ca certificates</code>	アイデンティティ証明書および CA 証明書の詳細を表示します。
<code>show crypto ca trustpoints</code>	トラストポイント設定を表示します。

crypto global domain ipsec security-association lifetime

Internet Protocol Security (IPSec) のグローバルパラメータを設定するには、**crypto global domain ipsec security-association lifetime** コマンドを使用します。デフォルトの設定に戻すには、コマンドの **no** 形式を使用します。

```
crypto global domain ipsec security-association lifetime {gigabytes number | kilobytes number |
megabytes number | seconds number}
```

```
no crypto global domain ipsec security-association lifetime {gigabytes | kilobytes | megabytes |
seconds}
```

シンタックスの説明

gigabytes number	ボリュームベースのキー存続期間をギガバイトで指定します。有効範囲は 1 ～ 4095 です。
kilobytes number	ボリュームベースのキー存続期間をキロバイトで指定します。有効範囲は 2560 ～ 2147483647 です。
megabytes number	ボリュームベースのキー存続期間をメガバイトで指定します。有効範囲は 3 ～ 4193280 です。
seconds number	時間ベースのキー存続期間を秒で指定します。有効範囲は 120 ～ 86400 です。

デフォルト

450 ギガバイトおよび 3600 秒

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
2.0(x)	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、**crypto ipsec enable** コマンドを使用して IPSec をイネーブルにする必要があります。

IPSec クリプトマップ コンフィギュレーション サブモードで **set** コマンドを使用すれば、個々の IPSec クリプトマップに対してグローバルセキュリティアソシエーションの継続時間値を上書きできます。

例

次に、IPSec の前にシステムデフォルトを設定する例を示します。

```
switch# config terminal
switch(config)# crypto global domain ipsec security-association lifetime gigabytes
500
```

関連コマンド

コマンド	説明
crypto ipsec enable	IPSec をイネーブルにします。
set (IPSec クリプトマップ コンフィギュレーション サブモード)	IPSec クリプトマップ エントリ パラメータを設定します。
show crypto global domain ipsec	IPSec のグローバル属性を表示します。

crypto ike domain ipsec

Internet Key Exchange (IKE) コンフィギュレーションサブモードにするには、**crypto ike domain ipsec** コマンドを使用します。

crypto ike domain ipsec

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 コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン IKE プロトコル属性を設定するには、**crypto ike enable** コマンドを使用して IKE をイネーブルにする必要があります。



(注) このコマンドは、Cisco MDS 9124 スイッチ、Cisco Fabric Switch for HP c-Class BladeSystem、Cisco Fabric Switch for IBM BladeCenter でサポートされていません。

例 次に、IKE コンフィギュレーションモードにする例を示します。

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)#
```

関連コマンド	コマンド	説明
	crypto ike enable	IKE プロトコルをイネーブルにします。
	show crypto ike domain ipsec	IPSec ドメインの IKE 情報を表示します。

crypto ike domain ipsec rekey sa

IPSec ドメインの IKE クリプトセキュリティ アソシエーション(SA)のキーを変更するには、**crypto ike domain ipsec rekey sa** コマンドを使用します。

crypto ike domain ipsec rekey sa *sa-index*

シンタックスの説明	<i>sa-index</i>	SA インデックスを指定します。有効範囲は 1 ~ 2147483647 です。
-----------	-----------------	--

デフォルト	なし
-------	----

コマンドモード	EXEC モード
---------	----------

コマンド履歴	リリース	変更内容
	2.0(x)	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、**crypto ike enable** コマンドを使用して IKE をイネーブルにする必要があります。



(注) このコマンドは、Cisco MDS 9124 スイッチではサポートされません。

例 次に、IKE クリプト SA のキーを変更する例を示します。

```
switch# crypto ike domain ipsec rekey sa 100
```

関連コマンド	コマンド	説明
	crypto ike enable	IKE プロトコルをイネーブルにします。
	show crypto ike domain ipsec	IPSec ドメインの IKE 情報を表示します。

crypto ike enable

Internet Key Exchange (IKE) をイネーブルにするには、**crypto ike enable** コマンドを使用します。IKE をディセーブルにするには、コマンドの **no** 形式を使用します。

crypto ike enable

no crypto ike 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 コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン Internet Protocol Security (IPSec) がディセーブルになっていないかぎり、IKE プロトコルをディセーブルにはできません。

IKE プロトコルのコンフィギュレーションおよび確認コマンドは、IKE プロトコルがスイッチでイネーブルの場合にのみ使用できます。この機能をディセーブルにした場合、関連するすべての設定は自動的に廃棄されます。



(注) このコマンドは、Cisco MDS 9124 スイッチではサポートされません。

例 次に、IKE プロトコルをイネーブルにする例を示します。

```
switch# config terminal
switch(config)# crypto ike enable
```

関連コマンド	コマンド	説明
	clear crypto ike domain ipsec sa	IKE プロトコル情報および IKE セキュリティアソシエーション (SA) を消去します。
	crypto ipsec enable	IPSec をイネーブルにします。
	show crypto ike domain ipsec	IPSec ドメインの IKE 情報を表示します。

crypto ipsec enable

Internet Protocol Security (IPSec) をイネーブルにするには、**crypto ipsec enable** コマンドを使用します。IPSec をディセーブルにするには、コマンドの **no** 形式を使用します。

crypto ipsec enable

no crypto ipsec 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 コンフィギュレーションモード

コマンド履歴	リリース	変更内容
	2.0(x)	このコマンドが導入されました。

使用上のガイドライン IPSec をイネーブルにするには、**crypto ike enable** コマンドを使用して Internet Key Exchange (IKE) プロトコルをイネーブルにする必要があります。

IPSec のコンフィギュレーションおよび確認コマンドは、IPSec がスイッチでイネーブルの場合のみ使用できます。この機能をディセーブルにした場合、関連するすべてのコンフィギュレーションは自動的に廃棄されます。



(注)

このコマンドは、Cisco MDS 9124 スイッチ、Cisco Fabric Switch for HP c-Class BladeSystem、Cisco Fabric Switch for IBM BladeCenter でサポートされていません。

例 次に、IPSec をイネーブルにする例を示します。

```
switch# config terminal
switch(config)# crypto ipsec enable
```

関連コマンド	コマンド	説明
	show crypto global domain ipsec	IPSec クリプト グローバル情報を表示します。
	show crypto map domain ipsec	IPSec クリプトマップ情報を表示します。
	show crypto transform-set domain ipsec	IPSec クリプト トランスフォーム セット情報を表示します。

crypto key generate rsa

RSA キー ペアを生成するには、コンフィギュレーション モードで **crypto key generate rsa** コマンドを使用します。

```
crypto key generate rsa [label key-pair-label] [exportable] [modulus key-pair-size]
```

シンタックスの説明

label <i>key-pair-label</i>	キー ペア名を指定します。最大文字サイズは 64 です。
exportable	キー ペアをエクスポート可能に設定します。
modulus <i>key-pair-size</i>	キー ペアのサイズを指定します。サイズの範囲は 512 ~ 2048 です。

デフォルト

デフォルトでは、**key** はエクスポートできません。
デフォルトの **label** は、スイッチの FQDN です。
デフォルトの **modulus** は 512 です。

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
3.0(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

1 つ以上の RSA キー ペアを生成し、アイデンティティ証明書を取得するために MDS スイッチが登録されている別々のトラスト ポイントに各 RSA キー ペアを関連付けることができます。アイデンティティは、1 つのキー ペアと 1 つのアイデンティティ証明書で構成され、MDS スイッチが必要とするアイデンティティは、CA ごとに 1 つだけです。

Cisco MDS SAN-OS では、RSA キー ペアを生成する場合にキー サイズ (modulus) を設定できます。デフォルトのキー サイズは 512 です。modulus の有効値は 512、768、1024、1536、2048 です。

また、RSA キー ペアのラベルも設定できます。デフォルトのキー ペアのラベルは、FQDN です。

例

次に、newkeypair という RSA キー ペアを設定する例を示します。

```
switch# config terminal
switch(config)# crypto key generate rsa label newkeypair
```

次に、testkey という RSA キー ペアをサイズ 768 でエクスポート可能に設定する例を示します。

```
switch# config terminal
switch(config)# crypto key generate rsa label testkey exportable modulus 768
```

次に、デフォルトのラベルとしてスイッチ名を、デフォルトのモジュールとして 512 を使用して、エクスポート可能な RSA キーを生成する例を示します。

```
switch# config terminal
switch(config)# crypto key generate rsa exportable
```

関連コマンド

コマンド	説明
crypto key zeroize rsa	RSA キー ペア設定を削除します。
rsakeypair	トラスト ポイントの RSA キー ペアの詳細を設定します。
show crypto key mypubkey rsa	設定された RSA キー ペアに関する情報を表示します。

crypto key zeroize rsa

スイッチから RSA キー ペアを削除するには、コンフィギュレーション モードで **crypto key zeroize rsa** コマンドを使用します。

```
crypto key zeroize rsa key-pair-label
```

シンタックスの説明	<i>key-pair-label</i>	削除する RSA キー ペアを指定します。最大文字サイズは 64 です。
-----------	-----------------------	--------------------------------------

デフォルト	なし
-------	----

コマンド モード	コンフィギュレーション モード
----------	-----------------

コマンド履歴	リリース	変更内容
	3.0(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 何らかの方法で RSA キー ペアが信用できなくなったことがわかり、それ以上使用するべきではない場合には、キー ペアを削除する必要があります。

スイッチの RSA キー ペアを削除してから、CA 管理者にスイッチの証明書を CA で失効するよう依頼します。スイッチの証明書を最初に要求したときに作成したチャレンジパスワードを知らせる必要があります。

キー ペアを削除する前に、このキー ペアに対応するアイデンティティ証明書が存在していて、トラスト ポイントからキー ペアへの関連付けを解除する場合は、さまざまなトラスト ポイントにあるアイデンティティ証明書を削除します。これは、トラスト ポイントに存在するアイデンティティ証明書のキー ペアを誤って削除しないようにするためです。



(注)

トラスト ポイント設定、証明書、およびキー ペア設定は、スタートアップ コンフィギュレーションに保存してある場合のみ維持されます。このコンフィギュレーション動作と矛盾せず、削除も同様に動作します。つまり、削除をスタートアップ コンフィギュレーションに保存した場合のみ維持されます。

証明書およびキー ペアの削除を維持するには、**copy running-config startup-config** コマンドを使用します。

例 次に、testkey という RSA キー ペアを削除する例を示します。

```
switch# config terminal
switch(config)# crypto key zeroize rsa testkey
```

関連コマンド	コマンド	説明
	crypto key generate rsa	RSA キー ペアを設定します。
	rsaakeypair	トラスト ポイントの RSA キー ペアの詳細を設定します。
	show crypto key mypubkey rsa	設定された RSA キー ペアに関する情報を表示します。

crypto map domain ipsec (configuration mode)

Internet Protocol Security (IPSec) クリプトマップを指定し、IPSec クリプトマップ コンフィギュレーション モードにするには、**crypto map domain ipsec** コマンドを使用します。IPSec クリプトマップ または IPSec クリプトマップ の特定エントリを削除するには、コマンドの **no** 形式を使用します。

```
crypto map domain ipsec map-name seq-number
```

```
no crypto map domain ipsec map-name [seq-number]
```

シンタックスの説明

<i>map-name</i>	マップ名を指定します。最大 63 文字まで可能です。
<i>seq-number</i>	マップ エントリのシーケンス番号を指定します。有効範囲は 1 ~ 65535 です。

デフォルト

なし

コマンドモード

コンフィギュレーションモード

コマンド履歴

リリース	変更内容
2.0(x)	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、**crypto ipsec enable** コマンドを使用して IPSec をイネーブルにする必要があります。

シーケンス番号は、IPSec クリプトマップ エントリが適用される順番を決定します。

例

次に、IPSec クリプトマップ IPsecMap のエントリ 1 を指定し、IPSec クリプトマップ コンフィギュレーション モードにする例を示します。

```
switch# config terminal
switch(config)# crypto map domain ipsec IPsecMap 1
switch(config-crypto-map-ip)#
```

次に、IPSec クリプトマップ エントリを削除する例を示します。

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap 1
```

次に、IPSec クリプトマップ 全体を削除する例を示します。

```
switch# config terminal
switch(config)# no crypto map domain ipsec IPsecMap
```

関連コマンド

コマンド	説明
crypto ipsec enable	IPSec をイネーブルにします。
crypto transform-set domain ipsec	IPSec クリプトマップのトランスフォーム セットを設定します。
set (IPSec クリプトマップ コンフィギュレーション サブモード)	IPSec クリプトマップ エントリ パラメータを設定します。
show crypto map domain ipsec	IPSec クリプトマップ情報を表示します。

crypto map domain ipsec (interface configuration submode)

ギガビットイーサネットインターフェイスで Internet Protocol Security (IPSec) クリプトマップを設定するには、インターフェイス コンフィギュレーション サブモードで **crypto map domain ipsec** コマンドを使用します。IPSec クリプトマップを削除するには、コマンドの **no** 形式を使用します。

crypto map domain ipsec *map-name*

no crypto map domain ipsec

シンタックスの説明	<i>map-name</i>	マップ名を指定します。最大 63 文字まで可能です。
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 サブモード	
コマンド履歴	リリース	変更内容
	2.0(x)	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、 crypto ipsec enable コマンドを使用して IPSec をイネーブルにする必要があります。	
	シーケンス番号は、クリプトマップが適用される順番を決定します。	
例	次に、ギガビットイーサネットインターフェイスの IPSec クリプトマップを指定する例を示します。	
	<pre>switch# config terminal switch(config)# interface gigabitethernet 1/2 switch(config-if)# crypto map domain ipsec IPsecMap</pre>	
関連コマンド	コマンド	説明
	crypto ipsec enable	IPSec をイネーブルにします。
	show crypto map domain ipsec	IPSec クリプトマップ情報を表示します。
	show interface	インターフェイス情報を表示します。

crypto transform-set domain ipsec

Internet Protocol Security (IPSec) トランスフォーム セットを作成および設定するには、**crypto transform-set domain ipsec** コマンドを使用します。IPSec トランスフォーム セットを削除するには、コマンドの **no** 形式を使用します。

```
crypto transform-set domain ipsec set-name {esp-3des | esp-des} [esp-aes-xcbc-mac | esp-md5-hmac | esp-sha1-hmac]
```

```
crypto transform-set domain ipsec set-name esp-aes {128 | 256} [ctr {esp-aes-xcbc-mac | esp-md5-hmac | esp-sha1-hmac} | esp-aes-xcbc-mac | esp-md5-hmac | esp-sha1-hmac]
```

```
crypto transform-set domain ipsec set-name [{esp-3des | esp-des} [esp-aes-xcbc-mac | esp-md5-hmac | esp-sha1-hmac]]
```

```
crypto transform-set domain ipsec set-name esp-aes [{128 | 256} [ctr {esp-aes-xcbc-mac | esp-md5-hmac | esp-sha1-hmac} | esp-aes-xcbc-mac | esp-md5-hmac | esp-sha1-hmac]]
```

シンタックスの説明

<i>set-name</i>	トランスフォーム セット名を指定します。最大 63 文字まで可能です。
esp-3des	3DES 暗号 (128 ビット) を使用する Encapsulating Security Protocol (ESP) トランスフォームを指定します。
esp-des	DES 暗号 (56 ビット) を使用する ESP トランスフォームを指定します。
esp-aes-xcbc-mac	AES-XCBC-MAC 認証を使用する ESP トランスフォームを指定します。
esp-md5-hmac	MD5-HMAC 認証を使用する ESP トランスフォームを指定します。
esp-sha1-hmac	SHA1-HMAC 認証を使用する ESP トランスフォームを指定します。
esp-aes	Advanced Encryption Standard (AES) 暗号 (128 または 256 ビット) を使用する ESP トランスフォームを指定します。
128	AES 128 ビット暗号を使用する ESP トランスフォームを指定します。
256	AES 256 ビット暗号を使用する ESP トランスフォームを指定します。
ctr	カウンタ モードで AES を指定します。

デフォルト

なし

AES のデフォルト モードは、Cyber Block Chaining (CBC) です。

コマンドモード

コンフィギュレーション モード

コマンド履歴

リリース	変更内容
2.0(x)	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、**crypto ipsec enable** コマンドを使用して IPSec 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て、既存の IPSec トランスフォーム セットを変更できます。トランスフォーム セット定義を変更した場合、そのトランスフォーム セットを参照するクリプトマップ エントリ のみに変更が適用されます。既存のセキュリティ アソシエーションには変更が適用されませんが、続くネゴシエーションでは使用され、新規セキュリティ アソシエーションが確立されます。新しい設定をすぐに反映させたい場合は、**clear crypto sa domain ipsec** コマンドを使用してセキュリティ アソシエーション データベースのすべてまたは一部を消去します。

■ **crypto transform-set domain ipsec****例**

次に、IPSec トランスフォーム セットを設定する例を示します。

```
switch# config terminal  
switch(config)# crypto transform-set domain ipsec Set1 esp-aes 128
```

関連コマンド

コマンド	説明
clear crypto sa domain ipsec	セキュリティ アソシエーションを消去します。
crypto ipsec enable	IPSec をイネーブルにします。
show crypto transform-set domain ipsec	IPSec クリプト トランスフォーム セット情報を表示します。

customer-id

Call Home 機能でカスタマー ID を設定するには、Call Home コンフィギュレーション サブモードで **customer-id** コマンドを使用します。この機能をディセーブルにするには、コマンドの **no** 形式を使用します。

customer-id *customer-id*

no customer *customer-id*

シンタックスの説明	<i>customer-id</i>	(任意) カスタマー ID を指定します。最大の長さは 64 文字の英数字で、フォーマットは自由です。
------------------	--------------------	---

デフォルト	なし
--------------	----

コマンドモード	Call Home コンフィギュレーション サブモード
----------------	-----------------------------

コマンド履歴	リリース	変更内容
	1.0(2)	このコマンドが導入されました。

使用上のガイドライン	なし
-------------------	----

例 次に、Call Home コンフィギュレーションでカスタマー ID を設定する例を示します。

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# customer-id Customer1234
```

関連コマンド	コマンド	説明
	callhome	Call Home 機能を設定します。
	callhome test	ダミーのテスト メッセージを設定された 1 つまたは複数の宛先へ送信します。
	show callhome	設定された Call Home 情報を表示します。

■ customer-id