



FIPS モードでのセキュアな操作

- [FIPS 140-2 の概要 \(1 ページ\)](#)
- [FIPS 140-2 の設定 \(2 ページ\)](#)
- [キーのゼロ化 \(2 ページ\)](#)
- [FIPS モードの無効化 \(3 ページ\)](#)
- [FIPS 設定を確認する \(3 ページ\)](#)
- [FIPS モードでのセキュアな動作に関する追加情報 \(5 ページ\)](#)

FIPS 140-2 の概要

連邦情報処理標準規格 (FIPS) 140-2、暗号モジュールセキュリティ要件は、暗号モジュールに対する米国およびカナダ政府の要求条件を定義しています。FIPS 140-2 は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。FIPS 140-2 標準および検証プログラムの詳細については、米国国立標準技術研究所 (NIST) の Web サイトを参照してください。 <http://csrc.nist.gov/groups/STM/index.html>

Cisco Catalyst シリーズスイッチの FIPS 140-2 コンプライアンスレビュー (CR) ドキュメントは、次の Web サイトに掲載されています。

<https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html>

「認定日」列のリンクをクリックして、CR 証明書を表示します。

セキュリティポリシー ドキュメントでは、FIPS の実装、ハードウェアの設置、ファームウェア初期化、および FIPS 操作のためのソフトウェア設定手順について説明します。 [NIST Computer Security Resource Center](#) の FIPS 140-2 統合検証証明書およびセキュリティポリシー ドキュメントにアクセスできます。この Web サイトから [Search] ウィンドウを開きます。[Vendor] フィールドに「Cisco」と入力し、[Search] をクリックします。表示されるウィンドウには、FIPS 準拠のシスコプラットフォームのリストが表示されます。リストから目的のプラットフォームをクリックして、セキュリティポリシーと統合証明書を取得します。



重要 このドキュメントでは、Cisco Catalyst スイッチの一般的な FIPS モードの動作について説明します。プラットフォーム固有の FIPS 140-2 実装の詳細については、プラットフォームの [FIPS 14-2 セキュリティ ポリシー ドキュメント](#) を参照してください。

FIPS 140-2 の設定

次に、Cisco Catalyst スイッチの FIPS 動作モードを有効にする一般的な手順を示します。詳細な設定手順については、必要なデバイスの [FIPS 140-2 セキュリティ ポリシー ドキュメント](#) を参照してください。

手順

ステップ 1 (任意) FIPS 140-2 ログイングを有効にします。

例：

```
Device(config)# logging console errors
```

ステップ 2 許可キーを設定します。

例：

```
Device(config)# fips authorization-key key
```

(注)

スタックの各メンバーに同じ認証キーを設定して、セキュアなスタック構成を有効にします。

key は 128 ビット、つまり 16 HEX バイトキーであることに注意してください。

次のタスク

FIPS を有効にした後、システムを再起動して FIPS モードでの動作を開始します。

キーのゼロ化

FIPS の重要な要件は、FIPS 動作モード中に安全でない状態がトリガーされた場合にキーとパスワードをゼロ化する機能です。

グローバル コンフィギュレーション モードで **no fips authorization-key** コマンドを使用して、FIPS 認証キーを削除できます。このコマンドは、フラッシュからキーを削除します。リブートすると、システムは FIPS モードで動作しなくなります。

セキュリティ違反がある場合は、**fips zeroize** コマンドを使用して、実行コンフィギュレーション、信頼アンカーモジュール、FIPS 認証キー、すべての ISE サーバー証明書、およびフラッシュ内の IOS イメージを含むすべてのデータを削除します。

このコマンドが実行されると、システムが再起動します。



注意 FIPS ゼロ化は、すべてのデータが失われる時の重要な手順です。慎重に使用してください。

セッションキーは、プログラムに従って、プロトコルを使用してゼロ化されます。

```
Device(config)#fips zeroize
```

```
**Critical Warning** - This command is irreversible  
and will zeroize the FVPK by Deleting the IOS  
image and config files, please use extreme  
caution and confirm with Yes on each of three  
iterations to complete. The system will reboot  
after the command executes successfully  
Proceed ?? (yes/[no]):
```

FIPS モードの無効化

no fips authorization-key コマンドを使用して FIPS モードを無効にできます。

no fips authorization-key コマンドは、フラッシュから認証キーを削除します。認証キーは、スイッチをリロードするまで使用できることを明記してください。

認証キーを完全に削除して FIPS モードを無効にするには、スイッチをリロードします。

```
Device> enable  
Device# config terminal  
Device(config)# no fips authorization-key  
Device(config)# end
```

FIPS 設定を確認する

FIPS 設定情報を表示するには、**show fips status** コマンドを使用します。

ハッシュされた FIPS キーを表示するには、**show fips authorization-key** コマンドを使用します。



(注) FIPS 設定情報は、**show running-config** コマンドを使用してアクティブな設定を一覧表示する場合、または**show startup-config** コマンドを使用してスタートアップコンフィギュレーションを一覧表示する場合には表示されません。

次に、**show** コマンドの出力例を示します。

```
Device# show fips authorization-key

FIPS: Stored key (16) : 11111111111111111111111111111111

Device#show romvar

ROMMON variables:
PS1="switch: "
BOARDID="24666"
SWITCH_NUMBER="1"
TERMLINES="0"
MOTHERBOARD_ASSEMBLY_NUM="73-18506-02"
MOTHERBOARD_REVISION_NUM="04"
MODEL_REVISION_NUM="P2A"
POE1_ASSEMBLY_NUM="73-16123-03"
POE1_REVISION_NUM="A0"
POE1_SERIAL_NUM="FOC21335EF2"
POE2_ASSEMBLY_NUM="73-16123-03"
POE2_REVISION_NUM="A0"
POE2_SERIAL_NUM="FOC21335EF3"
IMAGE_UPGRADE="no"
MAC_ADDR="F8:7B:20:77:F7:80"
MODEL_NUM="C9300-48UN"
MOTHERBOARD_SERIAL_NUM="FOC21351BC3"
BAUD="9600"
SYSTEM_SERIAL_NUM="FCW2138L0AF"
USB_SERIAL_NUM="FOC213609Y5"
STKPWR_SERIAL_NUM="FOC21360HTS"
STKPWR_ASSEMBLY_NUM="73-11956-08"
STKPWR_REVISION_NUM="B0"
USB_ASSEMBLY_NUM="73-16167-02"
USB_REVISION_NUM="A0"
TAN_NUM="68-101202-01"
TAN_REVISION_NUMBER="23"
VERSION_ID="P2A"
CLEI_CODE_NUMBER="ABCDEFGHJIJ"
ECI_CODE_NUMBER="123456"
TAG_ID="E20034120133FC00062B0965"
IP_SUBNET_MASK="255.255.0.0"
TEMPLATE="access"
TFTP_BLKSIZE="8192"
ENABLE_BREAK="yes"
TFTP_SERVER="10.8.0.6"
DEFAULT_GATEWAY="10.8.0.1"
IP_ADDRESS="10.8.3.33"
CRASHINFO="crashinfo:crashinfo_RP_00_00_20180420-020851-PDT"
CALL_HOME_DEBUG="00000000000000"
IP_ADDR="172.21.226.35/255.255.255.0"
DEFAULT_ROUTER="10.5.49.254"
RET_2_RTS=""
FIPS_KEY="5AC9BCA165E85D9FA3F2E5FC96AD98E8F943FBAB79B93E78"
MCP_STARTUP_TRACEFLAGS="00000000:00000000"
AUTOREBOOT_RESTORE="0"
MANUAL_BOOT="yes"
<output truncated>
Device#
```

FIPS モードでのセキュアな動作に関する追加情報

標準および RFC

標準/RFC	タイトル
FIPS 140-2	暗号モジュールのセキュリティ要件

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	http://www.cisco.com/cisco/web/support/index.html

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。