



## セキュアストレージについて

セキュアストレージ機能では、重要な設定情報を暗号化して保護できます。VPN、IPSec とその他の非対称キーペア、事前共有秘密、タイプ6のパスワード暗号化キーおよび特定のクレデンシャルを暗号化します。インスタンス固有の暗号キーは、危険にさらされることを防ぐためにハードウェアのトラストアンカーに保管されます。

デフォルトでは、この機能はハードウェアのトラストアンカーを備えたプラットフォームで有効です。この機能は、ハードウェアのトラストアンカーがないプラットフォームではサポートされません。

- [サポートされるプラットフォーム \(1 ページ\)](#)
- [セキュアストレージの有効化 \(4 ページ\)](#)
- [セキュアストレージの無効化 \(5 ページ\)](#)
- [暗号化のステータスの確認 \(6 ページ\)](#)
- [プラットフォームイメージの旧バージョンへのダウングレード \(6 ページ\)](#)
- [セキュアストレージの概要の機能情報 \(7 ページ\)](#)

## サポートされるプラットフォーム

Cisco IOS リリース 15.6(3) M1 以降、次の Cisco 880 シリーズプラットフォームでセキュアストレージがサポートされています。

表 1: セキュアストレージでサポートされるプラットフォーム : Cisco サービス統合型ルータ 880 PID

C881-K9
C887VA-K9
C886VA-K9
C887VAM-K9
C886VAJ-K9
C888-K9

Cisco IOS リリース 15.6(3)M1 以降、次の Cisco 890 シリーズプラットフォームでセキュアストレージがサポートされています。

表 2: セキュアストレージでサポートされるプラットフォーム : **Cisco サービス統合型ルータ 890 PID**

C891FW-E-K9
C891F-K9
C891FW-A-K9
C891-24X-K9

Cisco IOS リリース 15.6(3)M1 以降、次の Cisco 800M シリーズプラットフォームでセキュアストレージがサポートされています。

表 3: セキュアストレージでサポートされるプラットフォーム : **Cisco サービス統合型ルータ 800M PID**

C841M-4X/K9
C886VA-K9
C841M-8X/K9

Cisco IOS XE リリース 16.6.1 以降、次の ISR 4000 シリーズプラットフォームでセキュアストレージがサポートされています。

表 4: セキュアストレージでサポートされるプラットフォーム : **Cisco サービス統合型ルータ 4000 PID**

ISR4431
ISR4221
ISR4321
ISR4331
ISR4351
ISR4451-X

Cisco IOS XE リリース 16.6.1 以降、次の ASR 1000 プラットフォームでセキュアストレージがサポートされています。

表 5: セキュアストレージでサポートされるプラットフォーム : **Cisco ASR 1000** シリーズ アグリゲーション サービスルータ **PID**

ASR1000-RP3
ASR1001-X
ASR1001-HX
ASR1002-HX

Cisco IOS XE リリース 16.9.1 以降、次の Cisco 1000 シリーズプラットフォームでセキュアストレージがサポートされています。

表 6: セキュアストレージでサポートされるプラットフォーム : Cisco 1000 シリーズ PID

C1101-4P
C1111-8P
C1111-4P
C1112-8P
C1113-8P
C1113-8PM
C1116-4P
C1117-4P
C1117-4PM
C1101-4PLTEP
C1111-8PLTEEA
C1111-8PLTELA
C1111-4PLTEEA
C1111-4PLTELA
C1112-8PLTEEA
C1113-8PLTEEA
C1113-8PLTELA
C1113-8PMLTEEA
C1116-4PLTEEA
C1117-4PLTEEA
C1117-4PLTELA
C1117-4PMLTEEA
C1111-8PWY
C1111-4PWX
C1112-8PWE
C1113-8PWA

C1113-8PWB
C1113-8PWE
C1116-4PWE
C1117-4PWE
C1117-4PWA
C1117-4PWZ
C1117-4PMWE
C1111-8PLTEEAWX
C1111-8PLTELAZY
C1112-8PLTEAWE
C1113-8PLTEEAWA
C1113-8PLTEEAWB
C1113-8PLTEEAWC
C1113-8PLTELAZY
C1116-4PLTEEAWC
C1117-4PMLTEEA
C1117-4PLTEEAWC
C1117-4PLTEEAWA
C1117-4PLTELAZY
C1117-4PMLTEEAWC
C1101-4PLTEPWX

## セキュアストレージの有効化

### 始める前に

デフォルトでは、この機能はプラットフォームで有効です。この手順は、無効になっているプラットフォームで使用します。

### 手順の概要

#### 1. Config terminal

2. service private-config-encryption
3. do write memory

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Config terminal 例： router#config terminal	コンフィギュレーション モードを開始します。
ステップ 2	service private-config-encryption 例： router(config)# service private-config-encryption	プラットフォームでセキュリティストレージ機能を有効にします。
ステップ 3	do write memory 例： router(config)# do write memory	private-config ファイルを暗号化し、暗号化フォーマットで保存します。

#### 例

次に、セキュア ストレージをイネーブルにする例を示します。

```
router#config terminal
router(config)# service private-config-encryption
router(config)# do write memory
```

## セキュア ストレージの無効化

#### 始める前に

プラットフォームでセキュア ストレージ機能を無効にするには、次のタスクを実行します。

#### 手順の概要

1. Config terminal
2. no service private-config-encryption
3. do write memory

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Config terminal 例：	コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	<code>router#config terminal</code>	
ステップ 2	<code>no service private-config-encryption</code> 例 : <code>router(config)# no service private-config-encryption</code>	プラットフォームでセキュリティストレージ機能を無効にします。
ステップ 3	<code>do write memory</code> 例 : <code>router(config)# do write memory</code>	<code>private-config</code> ファイルを復号し、プレーンフォーマットで保存します。

### 例

次に、セキュアストレージをディセーブルにする例を示します。

```
router#config terminal
router(config)# no service private-config-encryption
router(config)# do write memory
```

## 暗号化のステータスの確認

暗号化のステータスを確認するには、**show parser encrypt file status** コマンドを使用します。次のコマンド出力は、機能は利用できるが、ファイルが暗号化されていないことを示します。ファイルは「プレーンテキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Plain Text
Encryption Version: Ver1
```

次のコマンド出力は、機能は有効で、ファイルが暗号化されていることを示します。ファイルは「暗号テキスト」形式です。

```
router#show parser encrypt file status
Feature: Enabled
File Format: Cipher Text
Encryption Version: Ver1
```

## プラットフォームイメージの旧バージョンへのダウングレード

セキュアストレージがサポートされていない旧バージョンにプラットフォームイメージをダウングレードする場合は、サポートされているバージョンでこの機能を事前に無効にする必要があります。

旧バージョンにダウングレードする前にこの機能を無効にしないと、`private-config` ファイルが暗号化形式になります。ファイルが暗号化形式になっていることを示す、次の Syslog メッセージが生成されます。

```
%PARSER-4-BADCFG: Unexpected end of configuration file.
```

ファイルが「プレーンテキスト」の場合、Syslog メッセージは生成されません。

## セキュアストレージの概要の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 7: Cisco TrustSec の概要の機能情報

機能名	リリース	機能情報
セキュアなストレージ	Cisco IOS XE Fuji 16.9.1	セキュアなストレージのサポートが ASR および ISR プラットフォームに導入されました。



## 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。