セキュアなストレージ

セキュアなストレージ

セキュアストレージ機能では、重要な設定情報を暗号化することによってそれらが保護されます。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などが入っています。セキュリティを確保するため、インスタンスに特有の暗号化キーがハードウェア トラスト アンカー内に格納されているため、不正アクセスや侵害を防止できます。

セキュアストレージの有効化

セキュアストレージはデフォルトでは無効になっています。セキュアストレージを有効にするには、次の操作を行います。

手順

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

プロンプトが表示されたらパスワードを入力します。

ステップ 2 **configure terminal**

例：

```
Device# configure terminal
```

グローバル コンフィギュレーション モードを開始します。

ステップ 3 **[no] service private-config-encryption**

例：

```
Device(config)# service private-config-encryption
```

デバイスでセキュアストレージ機能を有効にします。

デバイスでセキュアストレージを無効にするには、このコマンドの no 形式を使用します。

（注）
セキュアストレージを無効にすると、すべてのユーザーデータがプレーンテキストでNVRAMに保存されます。

ステップ 4 **end**

例：

```
Device(config)# end
```

特権 EXEC モードに戻ります。

ステップ 5 **write memory**

例：

```
Device# 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。

暗号化ステータスを確認するための設定例

暗号化ステータスが有効になっているかどうかを確認するための出力例を以下に示します。

```
Device# show parser encrypt file status
Feature:            Enabled
File Format:        Cipher text
Encryption Version: ver1
```

この例では、ファイル形式は 暗号テキスト として表示されています。これは、ファイルが暗号化されていて、セキュアストレージが有効になっていることを表しています。

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。