Cisco IOSのパスワード暗号化に関する事実の理解

内容

[はじめに](#)

[背景](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)
- [表記法](#)

[ユーザ パスワード](#)

- [enable secretおよびenable passwordコマンド](#)
- [enable secret をサポートしている Cisco IOS イメージを調べる方法](#)
- [その他のパスワード](#)

[コンフィギュレーション ファイル](#)

[アルゴリズム変更の可能性について](#)

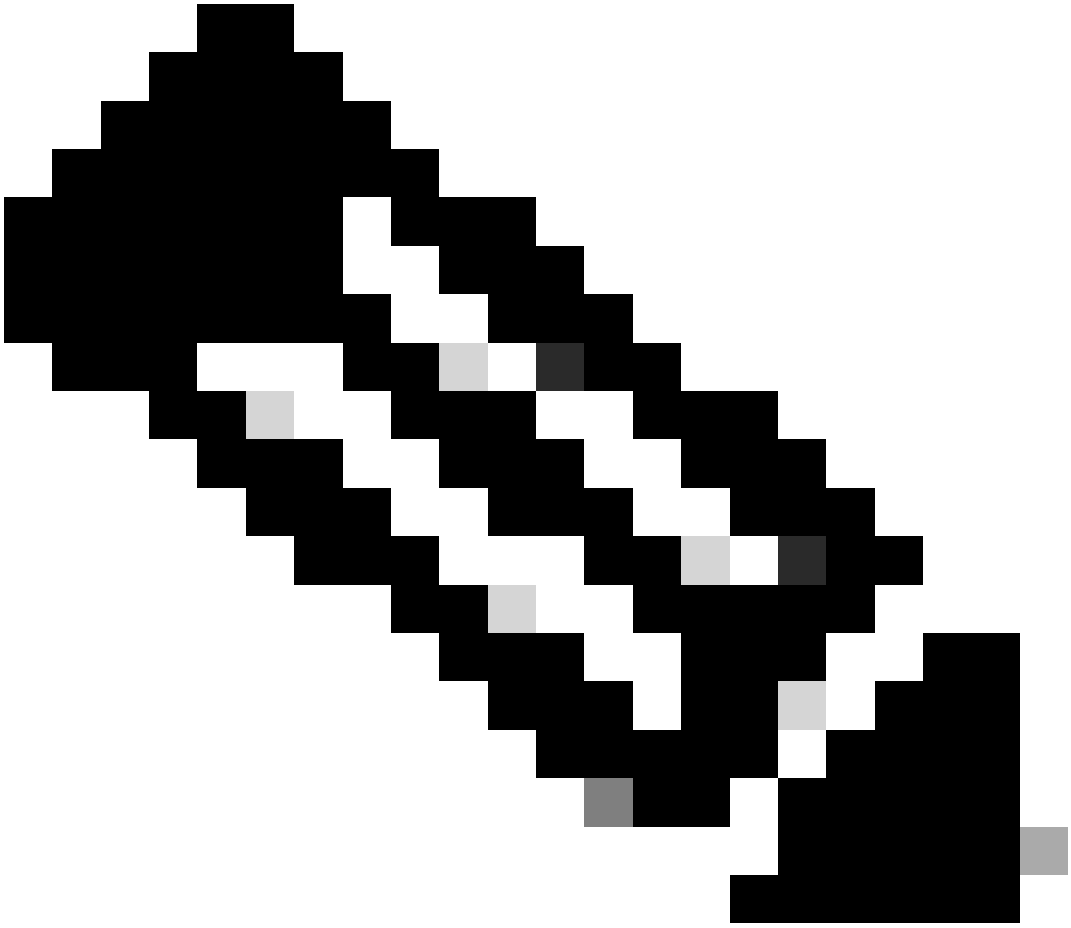
[関連情報](#)

はじめに

このドキュメントでは、Ciscoパスワード暗号化の背後にあるセキュリティモデルと、その暗号化のセキュリティ制限について説明します。

背景

シスコ コンフィギュレーション ファイル内のユーザ パスワード (およびその他のパスワード) を復号化するためのプログラムが、シスコ以外の情報源から公開されています。プログラムは、 **enable secret** コマンドで設定されたパスワードを復号化しません。シスコユーザの間でプログラムが引き起こした予想外の懸念から、多くのユーザがシスコのパスワード暗号化を利用して、意図したよりも高いセキュリティを実現しているのではないかと疑われるようになりました。



注：シスコでは、すべてのCisco IOS®デバイスで認証、許可、アカウンティング(AAA)セキュリティモデルを実装することを推奨しています。AAA ではローカル、RADIUS、および TACACS+ の各データベースを使用できます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

表記法の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

ユーザ パスワード

Cisco IOSコンフィギュレーションファイルにあるユーザパスワード、およびその他のほとんどのパスワード(**enable secret**は含まれません)は、最新の暗号化規格では非常に脆弱な方式で暗号化されています。

シスコでは復号化プログラムの配布を行っていませんが、インターネット上で一般に公開されているCisco IOSパスワード用の復号化プログラムは少なくとも2種類あります。このようなプログラムの最初の公開は1995年初めでした。暗号に詳しい者であればだれでも簡単に新しいプログラムを作成できると考えられます。

Cisco IOS で使用しているユーザ パスワードの方式は、周到かつ巧妙な攻撃から守ることを意図して作られていませんでした。暗号化スキームは、単純なスヌーピングまたはスニッフィングによるパスワードの盗難を回避するように設計されています。コンフィギュレーションファイルに対するパスワードクラッキング作業を行う何者かから保護する意図はありません。

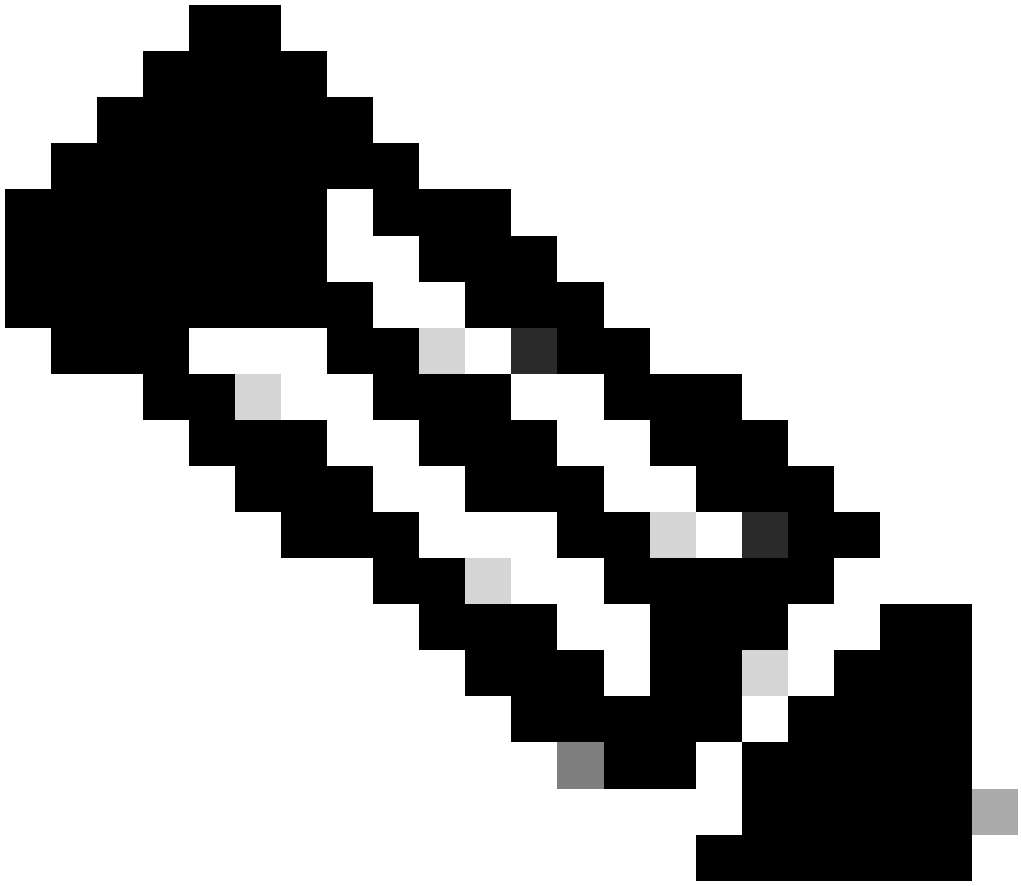
暗号化アルゴリズムが脆弱であるため、ユーザがパスワードを含むコンフィギュレーションファイルを機密情報として扱うのは、クリアテキストのパスワードリストを扱う場合と同じ方法というのがシスコの考え方です。

enable secretおよび**enable password**コマンド

enable password

コマンドの使用は推奨されなくなりました。セキュリティを強化するには、enable secretコマンドを使用します。**enable password**コマンドをテストできる唯一のインスタンスは、enable secretコマンドをサポートしていないブートモードでデバイスが動作している場合です。

イネーブルシークレットはMD5アルゴリズムでハッシュ処理されます。シスコが把握する限り、コンフィギュレーション ファイルの内容をもとに enable secret を復元することは不可能です（明らかな辞書攻撃によるものは除きます）。



注：これはenable secretで設定されたパスワードにのみ適用され、 **enable password**で設定されたパスワードには適用されません。実際には、2 つのコマンドの違いは使用されている暗号化の強度が大きく異なることだけです。

enable secret をサポートしている Cisco IOS イメージを調べる方法

ブートイメージが**enable secret** コマンドをサポートしているかどうかを確認するには、通常の動作モード（フルCisco IOSイメージ）で**show version** コマンドを使用してブートイメージを調べます。増加している場合は、 **enable password**を削除します。ブートイメージが **enable secret**をサポートしていない場合は、次の点に注意してください。

- 物理的なセキュリティを確保し、デバイスをブートイメージにリロードできないようにしている場合は、イネーブルパスワードを使用する必要はありません。

- デバイスに物理的にアクセスできるユーザがいれば、ブートイメージにアクセスすることなく、デバイスのセキュリティを簡単に破ることができます。

  enable password

  - をenable secretと同じ値に設定した場合、enable secretは **enable password**と同じように攻撃されやすくなります。

  - ブートイメージが **enable secret**をサポートしていないために異なる値**enable password** を設定した場合、**enable secret** コマンドをサポートしていないROM上でまれにしか使用されない新しいパスワードを、ルータ管理者が覚えておく必要があります。別のイネーブルパスワードを使用すると、管理者はソフトウェアのアップグレードのためにダウンタイムを強制するときにパスワードを記憶する必要があります。これがブートモードにログインする唯一の理由です。

その他のパスワード

Cisco IOSコンフィギュレーションファイルでは、ほとんどすべてのパスワードやその他の認証文字列が、ユーザパスワードに使用される脆弱で復元可能な方式で暗号化されています。

特定のパスワードの暗号化に使用された方式を確認するには、コンフィギュレーションファイルで暗号化された文字列の前の数字を確認します。その数字が7であれば、パスワードは脆弱なアルゴリズムで暗号化されています。数字が5の場合、パスワードはより強力なMD5アルゴリズムでハッシュされています。

たとえば、次の設定コマンドでは、

```
<#root>
```

enable secret 5 1iUjJ$cDZ03KKGh7mHfX2RSbDqP.

enable secret が MD5 でハッシュ処理されています。それに対して、次のコマンドでは、

<#root>

username jdoe password 7 07362E590E1B1C041B1E124C0A2F2E206832752E1A01134D

パスワードは、脆弱で復元可能なアルゴリズムで暗号化されています。

コンフィギュレーション ファイル

設定情報を電子メールで送信する場合は、タイプ7のパスワードから設定を消去します。show tech-supportコマンドを使用すると、デフォルトで情報が消去されます。**show tech-support** コマンドの出力例を次に示します。

<#root>

```
...
 hostname routerA
 !
 aaa new-model
 aaa authentication login default local
 aaa authentication ppp default if-needed local
```

enable secret 5 <removed>

!

```
username jdoe password 7 <removed>
username headquarters password 7 <removed>
username hacker password 7 <removed>
```

...

コンフィギュレーションファイルをTrivial File Transfer Protocol（TFTP；トリビアルファイル転送プロトコル）サーバに保存する場合は、ファイルが使用されていないときにそのファイルの特権を変更するか、ファイアウォールの背後に配置します。

アルゴリズム変更の可能性について

シスコでは、Cisco IOS ユーザ パスワードに対してより強固な暗号化アルゴリズムを近い将来サポートする予定はありません。シスコが今後このような機能を導入することを決定した場合、この機能を利用するユーザには管理上の負担が増えることは明らかです。

通常のケースでは、ユーザパスワードをenable secretに使用されるMD5ベースのアルゴリズムに切り替えることはできません。これは、MD5は単方向ハッシュであり、暗号化されたデータからはパスワードをまったく復元できないためです。特定の認証プロトコル（特にCHAP）をサポートするには、システムがユーザパスワードのクリアテキストにアクセスする必要があります。そのため、クリアテキストは可逆的なアルゴリズムで保存する必要があります。

キー管理の問題により、データ暗号規格(DES)などのより強力で復元可能なアルゴリズムに切り替えることは、簡単ではありません。パスワードの暗号化にDESを使用するようにCisco IOSを変更することは簡単ですが、すべてのCisco IOSシステムが同じDESキーを使用している場合、この方法ではセキュリティ上の利点はありません。また、システムごとに異なるキーを使用した場合は、すべての Cisco IOS ネットワーク管理者に管理上の負担がかかり、システム間でのコンフィギュレーション ファイルの移植性が失われます。より強力で復元可能なパスワード暗号化に対するユーザの要求は少ない。

関連情報

- **Password Recovery Procedures**

- **Cisco IOS デバイスの強化ガイド**

- **テクニカルサポート - Cisco Systems**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。