# パスワード、特権、およびログインによるセキュリティ設定

Cisco IOS ベースのネットワーキング デバイスには、デバイスで実行されているオペレーティング システムだけを使用して、基本的なセキュリティを実装できる機能が複数あります。たとえば、次のような機能があります。

- ネットワーキングデバイスのステータスを変更できるコマンドと、デバイスの監視に使用されるコマンドに対するアクセスを制御する CLI セッションの複数の認可レベル
- CLI セッションにパスワードを割り当てる機能
- ユーザがユーザ名を使用してネットワーキングデバイスにログインする操作を必須にする機能
- CLI セッション用に新しい認可レベルを作成するコマンドの特権レベルを変更する機能

このモジュールは、使用しているネットワーキングデバイスについて、基本レベルのセキュリティを実装する手順です。基本レベルのセキュリティを実装するために使用できる、最もシンプルなオプションを中心に説明します。セキュリティ オプションを設定せずにネットワークにネットワーキング デバイスをインストールした場合、またはこれからネットワーキング デバイスをインストールする予定で、基本的なセキュリティを実装する方法を理解する必要がある場合、このドキュメントが役立ちます。


- パスワード、特権、およびログインによるセキュリティ設定の制約事項 （2 ページ）
- パスワード、特権、およびログインによるセキュリティ設定について （2 ページ）
- パスワード、特権、およびログインによるセキュリティの設定方法 （17 ページ）
- パスワード、特権、およびログインによるセキュリティ設定の設定例 （40 ページ）
- 次の作業 （43 ページ）
- その他の参考資料 （44 ページ）
- パスワード、特権、およびログインによるセキュリティ設定に関する機能情報 （45 ページ）

# パスワード、特権、およびログインによるセキュリティ設定の制約事項

任意のローカルまたはリモートの認証、許可、アカウンティング（AAA）セキュリティ機能を使用するようにネットワーキングデバイスを設定しないでください。このドキュメントでは、ネットワーク デバイスでローカルで設定できる非 AAA セキュリティ機能のみを説明します。

ネットワーク デバイスでローカルで実行できる AAA セキュリティ機能の設定方法、または TACACS+ や RADIUS サーバを使用したリモート AAA セキュリティの設定方法については、『*Securing User Services Configuration Guide Library*』を参照してください。

## 可逆的パスワードタイプの制約事項とガイドライン

- パスワードタイプ 0 およびタイプ 7 は廃止されました。したがって、コンソール、Telnet、SSH、webUI、NETCONF への管理者ログインに使用されるパスワードタイプ 0 およびタイプ 7 は、パスワードタイプ 8 またはタイプ 9 に移行する必要があります。
- ISG および Dot1x の CHAP、EAP などのローカル認証でユーザー名とパスワードがタイプ 0 およびタイプ 7 の場合、アクションは不要です。
- イネーブルパスワードタイプ 0 およびタイプ 7 は、パスワードタイプ 8 またはタイプ 9 に移行する必要があります。

## 不可逆的パスワードタイプの制約事項とガイドライン

- パスワードタイプ 5 は廃止されました。パスワードタイプ 5 は、より強力なパスワードタイプ 8 またはタイプ 9 に移行する必要があります。
- ユーザー名シークレット パスワード タイプ 5 およびイネーブル シークレット パスワード タイプ 5 の場合は、タイプ 8 または 9 に移行します。
- シークレット パスワード タイプ 4 はサポートされていません。

# パスワード、特権、およびログインによるセキュリティ設定について

## セキュリティ スキームを作成する利点

ネットワークの優れたセキュリティ スキームの基礎は、ネットワーキング デバイスのユーザ インターフェイスを不正アクセスから保護することです。ネットワーキング デバイス上のユー

ザインターフェイスに対するアクセスを保護することで、ネットワークの安定を妨げ、ネットワーク セキュリティを危険にさらすような設定の変更を不正ユーザが行うことを回避できます。

このドキュメントで説明するCisco IOS XEの機能をさまざまな方法で組み合わせて、実際の各ネットワーク デバイスに固有のセキュリティ スキームを作成できます。次に、いくつかの設定例を示します。

- コマンドを実行可能なレベルを非管理特権レベルまで下げることで、非管理ユーザに対して、ネットワーキングデバイスで使用できる管理コマンドの一部の実行を許可できます。この処理は、次のシナリオに役立ちます。
  - ISPで、窓口のテクニカルサポートスタッフが、新規顧客の新規インターフェイスをイネーブルにするタスク、または接続がトラフィックのパスを停止した顧客の接続をリセットするタスクなどを実行できるようにする場合。その実行方法の例については、例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定 （42 ページ）を参照してください。
  - 窓口のテクニカル サポート スタッフが、ターミナル サーバから不正に接続解除されたコンソール ポート セッションをクリアする機能を実行できるようにする場合。その実行方法の例については、例：ユーザがリモート セッションをクリア可能にするデバイスの設定 （40 ページ）を参照してください。
  - 窓口のテクニカル サポート スタッフが、ネットワーク デバイスの設定を変更ではなく表示し、ネットワークの問題を解決する機能を実行できるようにする場合。その実行方法の例については、例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定 （41 ページ）を参照してください。

# Cisco IOS XE CLI モード

シスコ デバイスの設定を支援するために、Cisco IOS XE コマンドライン インターフェイスは、さまざまなコマンド モードに分かれています。各コマンド モードには、ルータとネットワークの動作を設定、メンテナンス、モニタリングするための独自のコマンドセットがあります。常に使用可能なコマンドは、モードによって異なります。システムプロンプト（デバイスプロンプト）で疑問符（**?**）を入力すると、各コマンドモードで使用できるコマンドのリストを取得できます。

特定のコマンドを使用すると、コマンドモードを変更できます。ユーザがモードにアクセスする標準の順序は、ユーザEXECモード、特権EXECモード、グローバル コンフィギュレーション モード、特定のコンフィギュレーション モード、コンフィギュレーション サブモード、およびコンフィギュレーション サブモードです。

（注） Cisco IOS XE ソフトウェア ベースのネットワーク デバイスのデフォルト設定で使用できるのは、ユーザEXECモード（ローカルおよびリモートCLIセッションの場合）と特権EXECモードへのアクセスを保護するパスワードを設定する操作だけです。ここでは、ユーザー名、パスワード、および**privilege**コマンドを組み合わせて他のモードへのアクセスおよびコマンドを保護することで、追加のセキュリティレベルを提供する方法について説明します。

ほとんどの EXEC モード コマンドは、現在の設定ステータスを表示する **show** コマンドまたは **more** コマンドや、カウンタやインターフェイスをクリアする **clear** コマンドのように、1 回限りのコマンドです。EXEC モードのコマンドは、ルータをリブートすると保持されません。

特権 EXEC モードから、グローバル コンフィギュレーション モードに入ることができます。このモードでは、一般的なシステム特性を設定するためのコマンドを実行できます。また、グローバル コンフィギュレーション モードを使用して特定のコンフィギュレーション モードを開始することもできます。グローバル コンフィギュレーション モードを含むコンフィギュレーション モードでは、実行コンフィギュレーションを変更できます。後で設定を保存すると、ルータをリブートしてもこれらのコマンドが保持されます。

グローバル コンフィギュレーション モードから、さまざまなプロトコル固有または機能固有のコンフィギュレーション モードを開始できます。CLI 階層では、グローバル コンフィギュレーション モードのみからこれらのコンフィギュレーション モードを開始できます。たとえば、インターフェイス コンフィギュレーション モードは、共通して使用されるコンフィギュレーション モードです。

コンフィギュレーション モードから、コンフィギュレーション サブモードを開始できます。コンフィギュレーション サブモードは、特定のコンフィギュレーション モードの範囲内で特定の機能を設定するために使用します。たとえば、この章では、インターフェイス コンフィギュレーション モードのサブモードであるサブインターフェイス コンフィギュレーション モードについて説明します。

*ROM* モニタ モードは、ルータが適切にブートできない場合に使用される別のモードです。システム（ルータ、スイッチ、またはアクセス サーバー）のブート時に適切なシステム イメージが見つからない場合、システムは ROM モニター モードを開始します。ROM モニター（ROMMON）モードには、起動時にブート シーケンスに割り込むことでもアクセスできます。ROMMON には使用できるセキュリティ機能がないため、このドキュメントでは説明していません。

## ユーザ EXEC モード

ルータでセッションを開始するときは、通常、EXEC モードの 2 つあるアクセス レベルの 1 つであるユーザ *EXEC* モードから始めます。セキュリティのために、ユーザー EXEC モードで使用できる EXEC コマンドは制限されています。このアクセス レベルは、ルータのステータスを確認するなど、ルータの設定を変更しない作業のために予約されています。

デバイスの設定で、ユーザのログインが必須の場合、そのログインプロセスはユーザ名とパスワードが必須になります。接続が拒否されるまでにパスワードを 3 回入力できます。

ユーザ EXEC モードは、デフォルトで特権レベル 1 に設定されています。特権 EXEC モードは、デフォルトで特権レベル 15 に設定されています。ユーザ EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 1 で実行されます。デフォルトで、特権レベル 1 の EXEC コマンドは、特権レベル 15 で使用できるコマンドのサブセットです。特権 EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 15 で実行されます。**privilege** コマンドを使用すると、1 ～ 15 の任意の特権レベルにコマンドを移動できます。

一般に、ユーザ EXEC コマンドでは、リモート デバイスへの接続、端末回線の一時的な設定変更、基本的なテストの実行、システム情報の表示を行うことができます。

使用可能なユーザ EXEC コマンドの一覧を表示するには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| `Device(config)# ?` | ユーザ EXEC モード コマンド リストを表示します |

ユーザ EXEC モード プロンプトは、デバイスのホスト名と、それに続く山カッコ（>）で構成されます。次に例を示します。

```
Device>
```

**setup** EXEC コマンドで初期設定時に変更していなければ、通常はデフォルトのホスト名は Router です。また、ホスト名の変更には、 **hostname** グローバル コンフィギュレーション コマンドを使用します。

（注） Cisco IOS XE のドキュメントの例では、「デバイス」のデフォルト名を使用することを想定しています。さまざまなデバイス（アクセス サーバ）が異なるデフォルト名を使用できます。デバイス（ルータ、アクセスサーバー、またはスイッチ）に、**hostname** コマンドで名前が設定されている場合、デフォルトの名前の代わりにその名前がプロンプトに表示されます。

ユーザーEXECモードで使用できるコマンドの一覧を表示するには、次の例に示すように疑問符（**?**）を入力します。

```
Device> ?

Exec commands:
 <1-99>           Session number to resume
 connect          Open a terminal connection
 disconnect       Disconnect an existing telnet session
 enable           Turn on privileged commands
 exit             Exit from Exec mode
 help             Description of the interactive help system
 lat              Open a lat connection
 lock             Lock the terminal
 login            Log in as a particular user
 logout           Exit from Exec mode and log out
 menu             Start a menu-based user interface
 mbranch          Trace multicast route for branch of tree
 mrbranch         Trace reverse multicast route to branch of tree
 mtrace           Trace multicast route to group
 name-connection  Name an existing telnet connection
 pad              Open a X.29 PAD connection
 ping             Send echo messages
 resume           Resume an active telnet connection
 show             Show running system information
 systat           Display information about terminal lines
 telnet           Open a telnet connection
 terminal         Set terminal line parameters
 tn3270           Open a tn3270 connection
```

```
trace           Trace route to destination
where           List active telnet connections
x3              Set X.3 parameters on PAD
```

コマンドの一覧は、使用しているソフトウェア機能セットおよびプラットフォームによって異なります。

（注） コマンドは、大文字、小文字、または大文字と小文字を混在させて入力できます。大文字と小文字の区別があるのはパスワードだけです。ただし、Cisco IOS XE のマニュアルの表記法では、コマンドは常に小文字になっています。

## 特権 EXEC モード

すべてのコマンドにアクセスするには、EXEC モードの第 2 レベルのアクセスである特権 *EXEC* モードを開始する必要があります。特権 EXEC モードを開始するには、通常、パスワードが必要です。特権 EXEC モードでは、任意の EXEC コマンドを入力できます。これは、特権 EXEC モードが、ユーザー EXEC モード コマンドのスーパーセットであるためです。

多くの特権 EXEC モード コマンドは操作パラメータを設定するため、不正使用を防ぐために、特権 EXEC レベル アクセスをパスワードで保護する必要があります。特権 EXEC コマンド セットには、ユーザ EXEC モードに含まれているこれらのコマンドが含まれます。また、特権 EXEC モードでは、**configure** コマンドを使用することで各種コンフィギュレーション モードにアクセスでき、**debug** などの高度なテストコマンドも含まれています。

特権 EXEC モードは、デフォルトで特権レベル 15 に設定されています。ユーザ EXEC モードは、デフォルトで特権レベル 1 に設定されています。詳細については、ユーザ EXEC モード（4 ページ）を参照してください。特権 EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 15 で実行されます。ユーザ EXEC モードでネットワーキング デバイスにログインしている場合、システムは特権レベル 1 で実行されます。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです。**privilege** コマンドを使用すると、1 ～ 15 の任意の特権レベルにコマンドを移動できます。特権レベルおよび **privilege** コマンドの詳細については、Cisco IOS XE の特権レベル （15 ページ） を参照してください。

特権 EXEC モード プロンプトは、デバイスのホスト名と、それに続くポンド記号（#）で構成されます。次に例を示します。

```
Device#
```

特権 EXEC モードにアクセスするには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| `Device> enable`<br>`Password`<br>`Device# exit`<br>`Device>` | 特権 EXEC モードをイネーブルにします。<br>• 特権 EXEC モードのパスワードを選択すると、enable コマンドの発行後にパスワードの入力が求められます。<br>• 特権 EXEC モードを終了するには、exit コマンドを使用します。 |

（注） 特権 EXEC モードは、モードの開始に、**enable** コマンドを使用するため、「イネーブルモード」とも呼ばれます。

システムでパスワードが設定されている場合、特権EXECモードへのアクセスが許可される前にパスワードを入力するよう求められます。パスワードは画面には表示されません。また、大文字と小文字が区別されます。イネーブル パスワードが設定されていない場合、特権 EXEC モードには、ローカル CLI セッション（コンソール ポートに接続された端末）からしかアクセスできません。

Telnet 接続など、リモート接続上のルータで特権 EXEC モードへのアクセスを試行しても、特権 EXEC モードのパスワードを設定していない場合は、**% No password set** エラーメッセージが表示されます。リモート接続の詳細については、リモート CLI セッション （11 ページ）を参照してくださいシステム管理者は、**enable secret** または **enable password** グローバル コンフィギュレーション コマンドを使用して、特権 EXEC モードへのアクセスを制限するパスワードを設定します。特権EXECモードのパスワード設定の詳細については、特権EXECモードへのアクセスの保護 （22 ページ） を参照してください。

ユーザ EXEC モードに戻るには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| `Device# disable` | 特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。 |

次に、特権 EXEC モードにアクセスするプロセスの例を示します。

```
Device> enable
Password:<letmein>
Device#
```

入力してもパスワードが表示されませんが、ここでは説明のために表示しています。特権EXECモードで使用できるコマンドの一覧を表示するには、プロンプトで**?** コマンドを発行します。次の項で説明するように、特権 EXEC モードからグローバル コンフィギュレーション モードにアクセスできます。

（注） 特権 EXEC コマンド セットには、ユーザ EXEC モードで使用できるすべてのコマンドが含まれているため、一部のコマンドはどちらのモードでも実行できます。Cisco IOS XE のドキュメントでは、ユーザ EXEC モードまたは特権 EXEC モードで入力できるコマンドは、EXEC モードコマンドと呼ばれます。ユーザまたは特権とドキュメントに特記されていない場合、どちらのモードでもそのコマンドを入力できることを示します。

## グローバル コンフィギュレーション モード

「グローバル」という言葉は、システム全体に影響する特性や機能を示すために使用されています。グローバル コンフィギュレーション モードは、システムをグローバルに設定したり、インターフェイスやプロトコルなどの特定の要素を設定したりする目的で、特定のコンフィギュレーションモードを開始するために使用します。グローバルコンフィギュレーションモードを開始するには、**configure terminal** 特権 EXEC コマンドを使用します。

グローバル コンフィギュレーション モードにアクセスするには、特権 EXEC モードで次のコマンドを入力します。

| コマンド | 目的 |
|---|---|
| `Device# configure terminal` | 特権 EXEC モードで、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。 |

次に、特権 EXEC モードからグローバル コンフィギュレーション モードを開始するプロセスの例を示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#
```

システム プロンプトが変わり、グローバル コンフィギュレーション モードに入ったことが示されることに注意してください。グローバルコンフィギュレーションモードのプロンプトは、デバイスのホスト名と、それに続く（config）およびポンド記号（#）で構成されます。特権 EXEC モードで使用できるコマンドの一覧を表示するには、プロンプトで **?** コマンドを発行します。

グローバルコンフィギュレーションモードでコマンドを入力すると、すぐに実行コンフィギュレーション ファイルが更新されます。つまり、設定に対する変更は、有効なコマンドの後で Enter キーまたは Return キーを押すたびに有効になります。ただし、これらの変更は、**copy running-config startup-config** EXEC モードコマンドを発行するまで、スタートアップ コンフィギュレーション ファイルに保存されません。この動作は、このマニュアルの後の項で詳しく説明します。

上記の例のように、コントロール（Ctrl）キーと「z」キーを同時に押すと、システムダイアログでコンフィギュレーションセッションを終了するプロンプトが表示されます。これらのキー操作で、**^Z** が画面に出力されます。実際にコンフィギュレーション セッションを終了するには、Ctrl+Z キーの組み合わせ、**end** コマンド、または Ctrl+C キーの組み合わせを使用できま

す。現在のコンフィギュレーションセッションを終了することをシステムに示すための方法としては、**end** コマンドが推奨されます。

**注意** 有効なコマンドを入力してから、コマンド ラインの最後で Ctrl+Z キーを使用すると、そのコマンドが実行コンフィギュレーション ファイルに追加されます。つまり、Ctrl+Z キーを使用することは、終了前に Enter（復帰）キーを押すことと同じです。このような理由から、**end** コマンドを使用してコンフィギュレーションセッションを終了するほうが安全です。また、改行信号を送信せずにコンフィギュレーション セッションを終了するには、Ctrl+C キーの組み合わせを使用できます。

また、**exit** コマンドを使用して、グローバル コンフィギュレーション モードから EXEC モードに戻ることもできますが、使用できるのはグローバル コンフィギュレーション モードだけです。Ctrl+Z キーを押すか **end** コマンドを入力することにより、どのコンフィギュレーション モードまたはコンフィギュレーション サブモードにいるかにかかわらず、常に EXEC モードに戻ることができます。

グローバル コンフィギュレーション コマンド モードを終了して特権 EXEC モードに戻るには、次のいずれかのコマンドを使用します。

| コマンド | 目的 |
|---|---|
| `Device(config)# end`<br>または<br>`Device(config)# ^Z` | 現在のコンフィギュレーション セッションを終了して、特権 EXEC モードに戻ります。 |
| `Device(config)# exit` | 現在のコマンド モードを終了して、前のモードに戻ります。たとえば、グローバル コンフィギュレーション モードから特権 EXEC モードに戻ります。 |

グローバル コンフィギュレーション モードから、いくつかのプロトコル固有、プラットフォーム固有、機能固有のコンフィギュレーション モードを開始できます。

次のセクションで説明されているインターフェイス コンフィギュレーション モードは、グローバル コンフィギュレーション モードから入ることができるコンフィギュレーション モードの例です。

## インターフェイス コンフィギュレーション モード

グローバル コンフィギュレーション モードから開始する特定のコンフィギュレーション モードの一例が、インターフェイス コンフィギュレーション モードです。

多くの機能は、インターフェイスごとにイネーブルになります。インターフェイス コンフィギュレーション コマンドは、イーサネット、FDDI、シリアル ポートなど、インターフェイスの動作を変更します。インターフェイス コンフィギュレーション コマンドは常に、インター

フェイスタイプを定義する **interface** グローバル コンフィギュレーション コマンドの後に指定します。

帯域幅やクロック レートなど、一般的なインターフェイス パラメータに影響があるインターフェイス コンフィギュレーション コマンドの詳細については、Release 12.2 の『*Cisco IOS Interface Configuration Guide*』を参照してください。プロトコル固有のコマンドについては、該当する Cisco IOS XE ソフトウェア コマンド リファレンスを参照してください。

インターフェイス コンフィギュレーション コマンドにアクセスし、その一覧を表示するには、次のコマンドを使用します。

| コマンド | 目的 |
|---|---|
| `Device(config)# interface type number` | 設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。 |

次に、シリアル インターフェイス 0 についてユーザがインターフェイス 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。新しいプロンプト、*hostname*（config-if）# は、インターフェイス コンフィギュレーション モードを示しています。

```
Device(config)# interface serial 0
Device(config-if)#
```

インターフェイス コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。

コンフィギュレーション サブモードは、他のコンフィギュレーション モード（グローバル コンフィギュレーション モード以外）から開始されるコンフィギュレーション モードです。コンフィギュレーション サブモードは、コンフィギュレーション モード内の特定の要素を設定するためにあります。コンフィギュレーション サブモードの 1 つの例は、次の項で説明するサブインターフェイス コンフィギュレーション モードです。

## サブインターフェイス コンフィギュレーション モード

インターフェイス コンフィギュレーション モードから、サブインターフェイス コンフィギュレーション モードに入ることができます。サブインターフェイス コンフィギュレーション モードは、インターフェイス コンフィギュレーション モードのサブモードの 1 つです。サブインターフェイス コンフィギュレーション モードでは、1 つの物理インターフェイスに複数の仮想インターフェイス（別名サブインターフェイス）を設定できます。サブインターフェイスは、さまざまなプロトコルにとって個別の物理インターフェイスのように見えます。

サブインターフェイスの設定方法の詳細については、Cisco IOS XE ソフトウェア マニュアル セットの特定のプロトコルの該当するドキュメンテーション モジュールを参照してください。

サブインターフェイス コンフィギュレーション モードにアクセスするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

| コマンド | 目的 |
| --- | --- |
| `Device(config-if)# interface type number` | 設定する仮想インターフェイスを指定し、サブインターフェイス コンフィギュレーション モードを開始します。 |

次の例では、シリアル ライン 2 のサブインターフェイスで、フレーム リレー カプセル化を設定します。シリアルインターフェイス 2 のサブインターフェイス 1 であることを示すため、サブインターフェイスは「2.1」として識別されます。新しいプロンプトの *hostname*（config-subif）#は、サブインターフェイス コンフィギュレーション モードを示します。サブインターフェイスは、1 つ以上のフレーム リレー PVC をサポートするように設定できます。

```
Device(config)# interface serial 2
Device(config-if)# encapsulation frame-relay
Device(config-if)# interface serial 2.1
Device(config-subif)#
```

サブインターフェイス コンフィギュレーション モードを終了しインターフェイス コンフィギュレーション モードに戻るには、**exit** コマンドを入力します。コンフィギュレーション セッションを終了し特権 EXEC モードに戻るには、Ctrl+Z キーを押すか、**end** コマンドを入力します。

# Cisco IOS XE CLI セッション

## ローカル CLI セッション

ローカル CLI セッションでは、ネットワーク デバイスのコンソール ポートへの直接アクセスが要求されます。ローカル CLI セッションは、ユーザ EXEC モードで開始されます。ネットワーキング デバイスの設定とおよび管理に必要なすべてのタスクは、ローカル CLI セッションを使用して実行できます。ローカル CLI セッションを確立する最も一般的な方式は、PC 上のシリアルポートを、ネットワーキング デバイスのコンソール ポートに接続し、PC で端末エミュレーション アプリケーションを起動する方法です。必要とされるケーブルとコネクタの種類および PC 上の端末エミュレーション アプリケーションの設定は、設定しているネットワーク デバイスの種類によって異なります。ローカル CLI セッションでネットワーキング デバイスを設定する方法の詳細については、そのデバイスのマニュアルを参照してください。

## リモート CLI セッション

リモート CLI セッションは、PC などのホストとネットワーク上のルータなどのネットワーク デバイス間で、Telnet やセキュア シェル（SSH）などのリモート端末アクセス アプリケーションを使用して作成されます。ローカル CLI セッションは、ユーザ EXEC モードで開始されます。ネットワーク デバイスの設定とおよび管理に必要なほとんどのタスクは、リモート CLI セッションを使用して実行できます。例外は、ROM モニタ モードのときのネットワーク デバイスとの通信や、（コンソール ポートで新しい OS イメージをアップロードすることによる、破壊されたオペレーティング システム（OS）の復元など）、コンソール ポートと直接的に通信するタスクです。

このドキュメントでは、リモート Telnet セッションのセキュリティを設定する方法について説明します。Telnet は、ネットワーキング デバイスでリモート CLI セッションにアクセスする際に最も一般的な方式です。

（注） ただし、SSH の方が Telnet よりも安全な方式です。SSH には、PC などのローカル管理デバイスと、管理しているネットワーキング デバイスとの間のセッション トラフィックを暗号化する機能があります。SSH を使用してセッション トラフィックを暗号化すると、ハッカーがトラフィックを傍受しても、トラフィックをデコードできなくなります。SSH を使用する詳細については、「Secure Shell Version 2 Support」フィーチャ モジュールを参照してください。

## 端末回線はローカルおよびリモート CLI セッションに使用される

シスコ ネットワーク デバイスでは、ローカルおよびリモート CLI セッションを管理するソフトウェア コンポーネントを参照するため語線を使用します。**line console 0** グローバル コンフィギュレーション コマンドを使用してライン コンフィギュレーション モードを開始し、パスワードなど、コンソール ポートのオプションを設定します。

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# password password-string
```

リモート CLI セッションでは、仮想テレタイプ（VTY）の行である回線を使用しています。**line vty** *line-number* [*ending-line-number*] グローバル コンフィギュレーション コマンドを使用してライン コンフィギュレーション モードを開始し、パスワードなど、リモート CLI セッションのオプションを設定します。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config-line)# password password-string
```

# Cisco IOS XE EXEC モードへのアクセスの保護

Cisco IOS XE では、次へのアクセスを保護するパスワードを設定できます。

## ユーザ EXEC モードへのアクセスの保護

ネットワーク デバイスの安全な環境の構築に向けた第一歩は、ローカルおよびリモート CLI セッションのパスワードを設定することで、ユーザ EXEC モードへのアクセスを保護することです。

ローカル CLI セッションでユーザ EXEC モードに対するアクセスを保護するには、コンソール ポートでパスワードを設定します。ローカル CLI セッションのパスワードの設定と確認 （20 ページ）を参照してください。

リモート CLI セッションでユーザ EXEC モードに対するアクセスを保護するには、仮想端末回線（VTY）でパスワードを設定します。リモート CLI セッションのパスワード設定方法の手順については、「リモート CLI セッションのパスワードの設定と確認 （17 ページ）」を参照してください。

## 特権 EXEC モードへのアクセスの保護

ネットワーキング デバイスのセキュア環境を作成するための第 2 段階は、特権 EXEC モードに対するアクセスをパスワードで保護することです。特権 EXEC モードに対するアクセスを保護する方式は、ローカルおよびリモートの CLI セッションと同じです。

特権 EXEC モードに対するアクセスを保護するには、そのモード用のパスワードを設定します。特権 EXEC モードを開始するコマンドが **enable** なので、このパスワードもイネーブルパスワードと呼ばれることがあります。

| コマンド | 目的 |
|---|---|
| **enable**<br><br>`Device> enable`<br><br>`Password`<br><br>`Device#` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。パスワードはターミナル ウィンドウに表示されません。<br>• プロンプト文字列の末尾の「>」は、特権 EXEC モードにいることを示す「#」に変更されました。 |

# Cisco IOS XE のパスワード暗号化レベル

ネットワーク デバイスで設定するパスワードの中には、プレーン テキストで設定に保存されるものもあります。これは、ディスクにコンフィギュレーション ファイルのコピーを保存すると、コンフィギュレーション ファイルを読み取ることで、ディスクへのアクセス権を持つ誰もが、パスワードがわかることを意味します。次の種類のパスワードは、デフォルトでプレーン テキストで設定に保存されます。

- ローカル CLI セッションのコンソール パスワード
- リモート CLI セッションの仮想端末回線のパスワード
- パスワードを設定するため、デフォルトの方法を使用したユーザ名のパスワード
- **enable password** *password* コマンドで設定されるときの特権 EXEC モードのパスワード
- RIPv2 と EIGRP で使用されている認証キー チェーン パスワード
- BGP ネイバーを認証するための BGP パスワード
- OSPF ネイバーの認証に使用する OSPF 認証キー
- ISIS ネイバーを認証するための ISIS パスワード

ルータの設定ファイルからのこの引用文は、クリアテキストとして保存されたパスワードと認証キーの例を示しています。

```
!
enable password O9Jb6D
!
username username1 password 0 kV9sIj3
!
key chain trees
 key 1
  key-string willow
!
interface Ethernet1/0.1
 ip address 172.16.6.1 255.255.255.0
 ip router isis
 ip rip authentication key-chain trees
 ip authentication key-chain eigrp 1 trees
 ip ospf authentication-key j7876
 no snmp trap link-status
 isis password u7865k
!
line vty 0 4
 password V9jA5M
!
```

**service password-encryption** コマンドを使用することで、これらのクリアテキストのパスワードをコンフィギュレーション ファイルで暗号化できます。パスワードを暗号化するのに **service password-encryption** コマンドによって使用された暗号化アルゴリズムは、公で使用可能なツールを使用して暗号化されるテキストストリングを作成するため、これは最小レベルのセキュリティにすぎないと見なされる必要があります。また、**service password-encryption** コマンドを使用後、コンフィギュレーション ファイルのどのような電子または文書でのコピーに対するアクセスも保護する必要があります。

パスワードがリモートデバイスに送信されるとき、**service password-encryption** コマンドではパスワードを暗号化しません。ネットワークに対するアクセス権があるネットワーク トラフィック アナライザを使用するユーザは、デバイス間でパケットを送信するときに、パケットからこのようなパスワードをキャプチャできます。コンフィギュレーション ファイルでのクリアテキストパスワードの暗号化の詳細については、「クリア テキスト パスワードのパスワード暗号化の設定 （24 ページ）」を参照してください。

クリア テキスト パスワードを使用する Cisco IOS XE 機能の多くは、より安全な MD5 アルゴリズムを使用するように設定することもできます。MD5 アルゴリズムによって、暗号化がはるかに難しいコンフィギュレーション ファイル内でテキストストリングが作成されます。MD5 アルゴリズムは、リモートデバイスにパスワードを送信しません。これによって、トラフィック アナライザのユーザが、内部ネットワークのトラフィックをキャプチャしてパスワードを検出することを防ぎます。

ネットワーキング デバイスのコンフィギュレーション ファイルにパスワード文字列とともに保存されている数字によって、使用されているパスワード暗号化の種類を判断できます。下記のコンフィギュレーションの引用文での数字 5 は、イネーブル シークレット パスワードは MD5 アルゴリズムを使用して暗号化されていること示しています。

enable secret 5 $1$fGCS$rkYbR6.Z8xo4qCl3vghWQ0

下記の引用文での数字 7 は、**service password-encryption** コマンドによって使用された、より安全でないアルゴリズムを使用してイネーブルパスワードが暗号化されたことを示しています。

!

enable password 7 00081204

# Cisco IOS XE CLI セッションのユーザ名

これらのパスワードを設定して、ユーザ EXEC モードおよび特権 EXEC モードへのアクセスを保護した後に、個々のユーザにネットワーク デバイスの CLI セッションへのアクセスを制限するためのユーザ名を設定することで、ネットワーク デバイスのセキュリティ レベルをさらに強化できます。

ネットワーキング デバイスの管理に使用するユーザ名は、次のような追加オプションを使用して変更できます。

『 *Cisco IOS Security Command Reference*』を参照してください。**username** コマンドの設定方法の詳細については、（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

# Cisco IOS XE の特権レベル

Cisco IOS XE ベースのネットワーク デバイスのデフォルト設定では、ユーザ EXEC モードに特権レベル 1 を、特権 EXEC に特権レベル 15 を使用します。特権レベル 1 のユーザ EXEC モードで実行できるコマンドは、特権レベル 15 の特権 EXEC モードで実行できるコマンドのサブセットです。

**privilege** コマンドは、1 つの特権レベルから別の特権レベルへコマンドを移動するのに使用されます。たとえば、一部の ISP では、窓口のテクニカル サポート スタッフに対して、新しい顧客の接続をアクティブ化するインターフェイスをイネーブルまたはディセーブルにする機能、およびトラフィックの送信を終了した接続を再起動する機能を許可しています。このオプションの設定方法の例については、例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定 （42 ページ）を参照してください。

**privilege** コマンドは、ユーザー名に特権レベルを割り当てるために使用できるため、ユーザーがこのユーザー名でログインすると、セッションは、**privilege** コマンドで指定された特権レベルで実行されます。たとえば、テクニカルサポートスタッフに対して、設定を変更することなくネットワークの問題を解決できるように、ネットワークデバイス設定を閲覧できるようにする場合、ユーザー名を作成し、特権レベル 15 を使用してユーザー名を設定し、**show running-config** コマンドを自動的に実行するように設定できます。ユーザがそのユーザ名でログインすると、実行コンフィギュレーションが自動的に表示されます。ユーザがコンフィギュレーションの最後の行を表示すると、ユーザのセッションは自動的にログアウトされます。このオプションの設定方法の例については、例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定 （41 ページ）を参照してください。

このようなコマンドの特権は、TACACS+ および RADIUS による AAA を使用するときにも実装できます。たとえば、TACACS+ には、ユーザ別またはグループ別にルータ コマンドの認可を制御する方法が 2 つあります。1 つ目の方法では、コマンドに特権レベルを割り当て、指定した特権レベルでユーザが認可されているかどうかについて、TACACS+ サーバを使用するルータで確認します。2 つ目の方法では、ユーザ別またはグループ別に、明示的に許可するコマンドを TACACS+ サーバに指定します。TACACS+ および RADIUS による AAA の実装の詳細については、『How to Assign Privilege Levels with TACACS+ and RADIUS』のテクニカル ノートを参照してください。

# Cisco IOS XE のパスワード設定

Cisco IOS XE ソフトウェアでは、パスワードが意図したとおりに正確に入力されたことを確認するため、設定するパスワードの再入力を求めるプロンプトを採用していません。新しいパスワードおよび既存のパスワードへの変更は、パスワード コンフィギュレーション コマンド文字列の末尾に、Enter キーを入力すると、ただちに有効になります。新しいパスワードを入力し、ネットワーク デバイスのスタートアップ コンフィギュレーション ファイルに設定を保存し、特権 EXEC モードを出たときに間違えた場合、間違えたことを認識する前に、デバイスを管理できなくなっていることがわかる場合があります。

発生する可能性のある一般的な状況は次のとおりです。

- コンソール ポートでローカル CLI セッションのパスワード設定時に間違えます。
  - リモート CLI セッションでネットワーク デバイスに対するアクセスを適切に設定した場合、コンソール ポートで Telnet をして、パスワードを再設定できます。
- リモート Telnet または SSH セッションのパスワード設定時に間違えます。
  - ローカル CLI セッションでネットワーキング デバイスに対するアクセスを適切に設定した場合、端末に接続して、リモート CLI セッションのパスワードをリセットできます。
- 特権 EXEC モードでパスワード（イネーブル パスワードまたはイネーブル シークレット パスワード）を設定するときに誤入力しました。
  - 失われたパスワードの復元手順を実行する必要があります。
- ユーザ名パスワード設定するときに誤入力し、ネットワーキング デバイスからそのユーザ名を使用してログインするように求められました。
  - 別のアカウント名へのアクセス権を持っていない場合、失われたパスワード復元手順を実行する必要があります。

忘失パスワードの復元手順を実行する必要がないようにするには、ネットワーキング デバイスに対して 2 つの CLI セッションを開き、特権 EXEC モードでその一方を開いたままで、他のセッションを使用してパスワードをリセットします。2 つの CLI セッションまたは 2 種類のデバイスを実行するときに、同じデバイス（PC または端末）を使用できます。この手順には、ローカルの CLI セッションとリモート CLI セッションを使用するか、2 つのリモート CLI セッションを使用できます。パスワードの設定に使用する CLI セッションを、パスワードが適切に変更されたことを確認するために利用することもできます。最初の設定で誤入力した場合、特

権EXECモードで開いておいたもう一方のCLIセッションはパスワードを変更するときにも利用できます。

実行コンフィギュレーションで行ったパスワードの変更は、そのパスワードが適切に変更されたことを確認できるまで、スタートアップコンフィギュレーションに保存しないでください。パスワードの設定時に誤入力したことに気づき、上記のような第2のCLIセッションの手法を使用して問題を解決できなかった場合、スタートアップコンフィギュレーションに保存されている以前のパスワードに戻すように、ネットワーキング デバイスの電源を再投入します。

## AES パスワード暗号化およびマスター暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）をイネーブルにすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能をイネーブルにし、パスワード暗号化および復号化に使用されるマスター暗号キーを設定する必要があります。AESパスワード暗号化を有効にしてマスターキーを設定すると、タイプ6パスワード暗号化を無効にしない限り、サポートされているアプリケーションの既存および新規作成されたクリアテキストパスワードがすべて、タイプ6暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ6暗号化パスワードに変換するようにデバイスを設定することもできます。

AESパスワード暗号化機能とマスター暗号キーが設定されている場合、タイプ0およびタイプ7 のパスワードはタイプ 6 に自動変換できます。

（注） タイプ 6 のユーザー名とパスワードには、Cisco IOS リリース 16.10.1 とのみ下位互換性があります。Cisco IOS リリース 16.10.1 より前のリリースバージョンにダウングレードすると、タイプ 6 のユーザー名とパスワードは拒否されます。自動変換後、管理者パスワードがダウングレード中に拒否されないようにするには、パスワードを移行します。

# パスワード、特権、およびログインによるセキュリティの設定方法

## ユーザ EXEC モードへのアクセスの保護

### リモート CLI セッションのパスワードの設定と確認

このタスクを実行すると、リモートCLIセッションのパスワードが割り当てられます。このタスクを完了すると、この次にリモート CLI セッションを起動するときに、ネットワーク デバイスからパスワードの入力が求められます。

Cisco IOS XE ベースのネットワーク デバイスでは、リモート CLI セッション用に設定されたパスワードが必要になります。リモートCLIセッション用に設定されたパスワードがないデバ

イスでリモートCLIセッションを開始しようとすると、パスワードが必要で、設定されていないことを示すメッセージが表示されます。リモートCLIセッションは、リモートホストによって終了されます。

### 始める前に

以前にリモート CLI セッションのパスワードを設定していない場合、コンソール ポートに接続している端末、または端末エミュレーション アプリケーションを実行する PC を使用して、ローカル CLI セッションでこのタスクを実行する必要があります。

ネットワーキング デバイス上のコンソール ポートに使用される設定によって、端末、または端末エミュレーションアプリケーションを設定する必要があります。ほとんどのシスコのネットワーク デバイスのコンソール ポートには、次の設定が必要です。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、およびフロー制御は"none"に設定します。これらの設定が端末で機能しない場合は、ネットワーク デバイスのマニュアルを参照してください。

このタスクの確認手順（手順6）を実行するには、ネットワーキングデバイスに、動作状態のインターフェイスが必要です。インターフェイスは有効な IP アドレスを持っている必要があります。

（注） 以前にリモート CLI セッションのパスワードを設定していない場合、コンソール ポートに接続している端末を使用して、ローカル CLI セッションでこのタスクを実行する必要があります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **line vty** *line-number* [*ending-line-number*]
4. **password** *password*
5. **end**
6. **telnet** *ip-address*
7. **exit**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例： | 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。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device# configure terminal` | |
| ステップ 3 | **line vty** *line-number* [*ending-line-number*]<br>例：<br>`Device(config)# line vty 0 4` | ライン コンフィギュレーション モードを開始します。 |
| ステップ 4 | **password** *password*<br>例：<br>`Device(config-line)# password H7x3U8` | 引数 *password* は、ライン パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。<br>• 最初の文字を数値にはできません。<br>• ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。<br>• パスワードは大文字と小文字が区別されます。 |
| ステップ 5 | **end**<br>例：<br>`Device(config-line)# end` | 現在のコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 6 | **telnet** *ip-address*<br>例：<br>`Device# telnet 172.16.1.1` | 動作状態（インターフェイスがアップ、ラインプロトコルがアップ）のネットワーキング デバイスで、インターフェイスの IP アドレスを使用して、現在の CLI セッションからネットワーキング デバイスとのリモート CLI セッションを開始します。<br>• プロンプトが表示されたら、手順 4 で設定したパスワードを入力します。<br>（注） この手順は、ネットワーキング デバイス自体からネットワーキング デバイスへのリモート Telnet セッションを開始するため、再帰的 Telnet セッションの開始とも呼ばれます。 |
| ステップ 7 | **exit**<br>例：<br>`Device# exit` | ネットワーキング デバイスとのリモート CLI セッション（再帰的 Telnet セッション）を終了します。 |

### トラブルシューティングのヒント

合法的傍受ビューにアクセス可能なすべてのユーザーに関する情報を表示するには、**show users lawful-intercept** コマンドを発行します（このコマンドは、認可された合法的傍受ビュー ユーザしか使用できません）。

### 次の作業

ローカル CLI セッションのパスワードの設定と確認 （20 ページ）に進みます。

## ローカル CLI セッションのパスワードの設定と確認

このタスクを実行すると、コンソール ポートでのローカル CLI セッション用のパスワードが割り当てられます。このタスクを完了した後に、コンソール ポートでローカル CLI セッションを起動すると、ネットワーキング デバイスからパスワードの入力が求められます。

このタスクは、コンソールポートを使用するローカルCLIセッションまたはリモートCLIセッションで実行できます。パスワードを適切に設定したことを確認するオプションの手順を実行する場合、コンソール ポートでローカル CLI セッションを使用して、このタスクを実行する必要があります。

### 始める前に

ローカル CLI セッション パスワードを確認するオプションの手順を実行する場合、ローカル CLIセッションを使用してこのタスクを実行する必要があります。ネットワーク デバイスのコンソール ポートに、端末または端末エミュレーション プログラムが稼働している PC を接続する必要があります。ネットワーキング デバイス上のコンソール ポートに使用される設定によって、端末を設定する必要があります。ほとんどのシスコのネットワーク デバイスのコンソール ポートには、次の設定が必要です。9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、およびフロー制御は "none" に設定します。これらの設定が端末で機能しない場合は、ネットワーク デバイスのマニュアルを参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **password** *password*
5. **end**
6. **exit**
7. Enter キーを押します。

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device> enable` | |
| ステップ 2 | **configure terminal**<br>例：<br>`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 | **line console 0**<br>例：<br>`Device(config)# line console 0` | ライン コンフィギュレーション モードを開始し、設定しているラインとしてコンソール ポートを選択します。 |
| ステップ 4 | **password** *password*<br>例：<br>`Device(config-line)# password Ji8F5Z` | 引数 *password* は、ライン パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。<br>• 最初の文字を数値にはできません。<br>• ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。<br>• パスワードは大文字と小文字が区別されます。 |
| ステップ 5 | **end**<br>例：<br>`Device(config-line)# end` | 現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 6 | **exit**<br>例：<br>`Device# exit` | 特権 EXEC モードを終了します。 |
| ステップ 7 | Enter キーを押します。 | （任意）コンソール ポートでローカル CLI セッションを開始します。<br>• プロンプトが表示されたら、ステップ 4 で設定したパスワードを入力して、適切に設定されたことを確認します。<br>（注） この手順を実行できるのは、このタスクの実行にローカル CLI セッションを使用している場合だけです。 |

### トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら次に何をするのかについては、パスワード、特権、およびログインによるセキュリティ設定の設定例に進みます。

### 次の作業

特権 EXEC モードへのアクセスの保護 （22 ページ）に進みます。

# 特権 EXEC モードへのアクセスの保護

## イネーブル パスワードの設定と確認

シスコは特権 EXEC モードのパスワード設定に **enable password** コマンドを使用することを推奨しなくなりました。**enable password** コマンドを使用して入力したパスワードは、ネットワークデバイスのコンフィギュレーションファイルにプレーンテキストとして保存されます。ネットワークデバイスのコンフィギュレーション ファイルに含まれる **enable password** コマンドのパスワードを暗号化するには、**service password-encryption** コマンドを使用します。ただし、**service password-encryption** コマンドで使用される暗号化レベルは、インターネットで入手できるツールを使用して復号できます。

シスコでは、**enable password** コマンドを使用する代わりに、**enable secret** コマンドを使用することを推奨します。設定したパスワードが、強力な暗号化方式で暗号化されるためです。パスワード暗号化問題の詳細については、Cisco IOS XE のパスワード暗号化レベル （13 ページ）を参照してください。**enable secret** コマンドの設定については、イネーブル シークレット パスワードの設定と確認 （25 ページ）を参照してください。

（注） このタスクを正常に実行するため、ネットワークデバイスでは、**enable secret** コマンドを使用してパスワードを設定しないでください。**enable secret** コマンドを使用して特権 EXEC モードのパスワードを既に設定している場合、設定されたパスワードは、このタスクで**enable password** コマンドを使用して設定するパスワードより優先されます。

**enable secret** コマンドと **enable** *password* コマンドに同じパスワードを使用することはできません。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **enable password** *password*
4. **end**
5. **exit**
6. **enable**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`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 | **enable password** *password*<br>例：<br>`Device(config)# enable password t6D77CdKq` | 引数 *password* は、イネーブル パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。<br>• 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。<br>• 先頭の文字に数字は指定できません。<br>• 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。<br>• パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次の手順を実行します。<br>  • abc と入力します。<br>  • Crtl-v キーを押します。<br>  • ?123 と入力します。 |
| ステップ 4 | **end**<br>例：<br>`Device(config)# end` | 現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 5 | **exit**<br>例：<br>`Device# exit` | 特権 EXEC モードを終了します。 |
| ステップ 6 | **enable**<br>例： | 特権 EXEC モードをイネーブルにします。<br>• 手順 3 で設定したパスワードを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device> enable` | |

### トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら、次に何をするのかについては、特権EXECモードの忘失パスワードまたは誤設定パスワードの復元セクションに進みます。

### 次の作業

クリア テキスト パスワードのパスワード暗号化の設定 （24 ページ）で説明した手順を使用して、ネットワーキング デバイスのコンフィギュレーション ファイルにクリア テキストで保存されているイネーブル パスワードを暗号化します。

## クリア テキスト パスワードのパスワード暗号化の設定

Cisco IOS XEは、一部の機能について、ネットワーク デバイスのコンフィギュレーション ファイルにクリアテキストでパスワードを保存します。たとえば、ローカルおよびリモートのCLIセッションのパスワード、およびルーティングプロトコルのネイバー認証のパスワードなどです。コンフィギュレーション ファイルのアーカイブ コピーにアクセスできれば、誰でもクリア テキストで保存されているパスワードを発見できるため、クリア テキスト パスワードはセキュリティ リスクです。**service password-encryption** コマンドを使用して、ネットワークデバイスのコンフィギュレーション ファイルに含まれるクリアテキストコマンドを暗号化できます。詳細については、Cisco IOS XE のパスワード暗号化レベル （13 ページ）を参照してください。

ネットワーキング デバイスのコンフィギュレーション ファイルにクリア テキストとして保存されているパスワードについて、パスワード暗号化を設定するには、次の手順を実行します。

### 始める前に

このコマンドの結果を即時に確認するために、クリア テキスト パスワードを使用する機能が1つ以上、ネットワーキング デバイスに設定されている必要があります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **service password-encryption**
4. **end**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ1 | **enable**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device> enable` | |
| ステップ 2 | **configure terminal**<br>例：<br>`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 | **service password-encryption**<br>例：<br>`Device(config)# service password-encryption` | すべてのクリア テキスト パスワード（ユーザ名パスワード、認証キー パスワード、特権コマンド パスワード、コンソールおよび仮想端末ライン アクセス パスワード、および Border Gateway Protocol ネイバーパスワード）について、パスワード暗号化をイネーブルにします。 |
| ステップ 4 | **end**<br>例：<br>`Device(config)# end` | 現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

## イネーブル シークレット パスワードの設定と確認

シスコは、**enablenable** *password* コマンドの代わりに **enable secret** コマンドを使用して特権 EXEC モードのパスワードを設定することを推奨しています。**enable secret** コマンドで作成されたパスワードは、より安全な MD5 アルゴリズムで暗号化されます。

（注） **enable secret** コマンドと **enable** *password* コマンドに同じパスワードを使用することはできません。

### 手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかの手順を実行します。
   - **enable secret** *password*
   - **enable secret 5** *previously-encrypted-password*
4. **end**
5. **exit**
6. **enable**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`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 | 次のいずれかの手順を実行します。<br>• **enable secret** *password*<br>• **enable secret 5** *previously-encrypted-password*<br>例：<br>`Device(config)# enable secret t6D77CdKq`<br>例：<br>`Device(config)# enable secret 5 $1$/x6H$RhnDI3yLC4GA01aJnHLQ4/` | 引数 *password* は、**enable secret** パスワードを指定する文字列です。次の規則が *password* 引数に適用されます。<br>• 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。<br>• 先頭の文字に数字は指定できません。<br>• 先頭にスペースを指定できますが、無視されます。ただし、中間および末尾のスペースは認識されます。<br>• パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、abc?123 というパスワードを作成するには、次の手順を実行します。<br>• abc と入力します。<br>• Crtl-v キーを押します。<br>• ?123 と入力します。<br>または<br>前に暗号化した文字列の前に数字 5 を入力することで、以前に暗号化した特権 EXEC モードのパスワードを設定します。この方式を使用するには、**enable secret** コマンドによって以前に暗号化されたコンフィギュレーション ファイルから、パスワードの正確なコピーを入力する必要があります。 |
| ステップ 4 | **end**<br>例： | 現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config)# end` | |
| ステップ 5 | **exit**<br>例：<br>`Device# exit` | 特権 EXEC モードを終了します。 |
| ステップ 6 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードをイネーブルにします。<br>• 手順 3 で設定したパスワードを入力します。 |

### トラブルシューティングのヒント

新しいパスワードを受け入れられなかったら次に何をするのかについては、パスワード、特権、およびログインによるセキュリティ設定の設定例に進みます。

### 次の作業

ローカルおよびリモートのCLIセッションのパスワードを設定し終わり、ユーザ名や特権レベルなど、追加のセキュリティ機能を設定する場合、CLIセッションとコマンドへのアクセスを管理するセキュリティ オプションの設定 （29 ページ）に進みます。

## ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定

レベル 15 より低い特権レベルで **show running-config** コマンドを使用してデバイスの実行コンフィギュレーションにアクセスするには、次の作業を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **privilege exec all level** *level command-string*
4. **file privilege** *level*
5. **privilege configure all level** *level command-string*
6. **end**
7. **show privilege**
8. **show running-config**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例： | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device> enable` | |
| ステップ 2 | **configure terminal**<br>例：<br>`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 | **privilege exec all level** *level command-string*<br>例：<br>`Device(config)# privilege exec all level 5 show running-config` | 指定されたコマンドの特権レベルを、1 つの権限レベルから別の特権レベルに変更します。 |
| ステップ 4 | **file privilege** *level*<br>例：<br>`Device(config)# file privilege 5` | 特権レベルのユーザが、ファイル システムを含むコマンドをデバイスで実行できるようにします。 |
| ステップ 5 | **privilege configure all level** *level command-string*<br>例：<br>`Device(config)# privilege configure all level 5 logging` | 特権レベルのユーザが、特定のコンフィギュレーション コマンドを表示できるようにします。たとえば、特権レベル 5 のユーザが、実行コンフィギュレーションでロギング コンフィギュレーション コマンドを表示できるようにします。 |
| ステップ 6 | **end**<br>例：<br>`Device(config)# end` | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 7 | **show privilege**<br>例：<br>`Device# show privilege` | 現在の特権レベルを表示します。 |
| ステップ 8 | **show running-config**<br>例：<br>`Device# show running-config` | 指定された特権レベルの現在の実行コンフィギュレーションを表示します。 |

**例**

**show running-config** コマンドの次の出力は、実行コンフィギュレーションのロギング コンフィギュレーション コマンドを表示します。15 未満の特権レベルを持つユーザーは、**privilege configure all level** *level command-string* コマンドを設定した後、実行コンフィギュレーションを表示できます。

```
Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

# CLI セッションとコマンドへのアクセスを管理するセキュリティ オプションの設定

ここでは、特権EXECモードで使用できる全コマンドに対してはアクセス権が持たないユーザが、特権 EXEC モード コマンドのサブセットを使用できるように、ネットワーキング デバイスを設定するタスクについて説明します。

このようなタスクは、複数レベルのネットワーク サポート スタッフがいて、各レベルのスタッフに、異なるサブセットの特権 EXEC モード コマンドに対するアクセス権を付与したい会社に役立ちます。

このタスクでは、特権EXECモードで使用できる全コマンドに対してはアクセス権を持たないユーザは、窓口のテクニカル サポート スタッフと呼びます。

ここでは、次の手順について説明します。

## 窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定

このタスクでは、窓口のテクニカル サポート スタッフ ユーザ用にネットワーキング デバイスを設定する方法について説明します。通常、窓口のテクニカル サポート スタッフは、ネットワーキング デバイスの特権 EXEC モードで（特権レベル 15）使用できる全コマンドの実行は許可されていません。また、特権EXECモードに割り当てられているパスワード、またはネットワーキング デバイスに設定されている他の役割に対してアクセス権が付与されていないため、権限がないコマンドを実行できません。

**privilege** コマンドは、ある特権レベルのコマンドを別の特権レベルに移動するために使用されます。この操作で、ネットワークデバイスに追加レベルの管理が作成されます。このような操作は、さまざまなスキルレベルを持つ、さまざまなレベルのネットワーク サポート スタッフがいる会社の場合に必要です。

Cisco IOS XE デバイスのデフォルトの設定では、2 種類のユーザが CLI にアクセスできます。1つ目のユーザは、ユーザEXECモードだけにアクセスできるユーザです。2つ目のユーザは、特権EXECモードにアクセスできるユーザです。ユーザEXECモードへのアクセスが許可され

ているだけのユーザは、ネットワーク デバイスの設定を表示または変更したり、ネットワーク デバイスの稼働状態を変更することはできません。一方、特権EXECモードにアクセスできるユーザは、CLI に許可されているネットワーキング デバイスを変更できます。

この作業では、通常特権レベル 15 で動作する 2 つのコマンドは、特権コマンドを使用して特権レベル 7 にリセットされます。窓口のテクニカル サポート スタッフ ユーザが 2 つのコマンドを実行できるようにするためです。特権レベルをリセットする 2 つのコマンドは、**clear counters** コマンドと **reload** コマンドです。

- **clear counters** コマンドは、受信されたパケット、送信されたパケット、およびエラーなどの統計情報のために、インターフェイスのカウンタフィールドをリセットするために使用されます。窓口のテクニカル サポート スタッフ ユーザがネットワーク デバイス間で、またはネットワークに接続しているリモートユーザとの間で、インターフェイスに関する接続の問題を解決しているときに、インターフェイスの統計情報をゼロにリセットしたり、インターフェイスの統計情報カウンタの値が変化するかを見るため、一定の時間インターフェイスを監視するのに役立ちます。
- **reload** コマンドは、ネットワークデバイスのリブートシーケンスを開始するのに使用します。窓口のテクニカル サポート スタッフによる一般的な reload コマンドの使用方法の 1 つは、メンテナンス ウィンドウでネットワーク デバイスをリブートすることです。この操作によって、高い権限レベルのユーザが以前にネットワーク デバイスのファイル システムにコピーした新しいオペレーティング システムがロードされます。

窓口のテクニカル サポート ユーザー ロールの特権レベルに割り当てられている **enable secret** パスワードを知る権限を持つユーザーは、窓口のテクニカルサポートユーザーとしてそのネットワークデバイスにアクセスできます。ネットワークデバイスのユーザ名を設定し、ユーザによるユーザ名とパスワードの把握を必須にして、新たなセキュリティ レベルを追加できます。追加レベルのセキュリティとしてユーザ名を設定する方法については、「」を参照してください。 窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定 （34 ページ）

（注） ネットワークデバイスでは、**aaa new-model** コマンドをイネーブルにしないでください。コンソールポートでのローカル CLI セッションの場合、またはリモート CLI セッションの場合、**login local** コマンドを設定しないでください。

（注） このタスクの手順では、わかりやすくするために、各手順に関係する構文に使用しています。これらのコマンドと併用できるその他の引数いては、お使いの Cisco IOS リリースの Cisco IOS コマンド リファレてください。

**注意** コマンドの特権レベルをデフォルトにリセットする場合、**privilege** コしないでください。コンフィギュレーションが適切なデフォルト状態ます。コマンドをデフォルトの特権レベルに戻すには、**privilege** コマを使用します。たとえば、コンフィギュレーションから **privilege exe** 削除し、**reload** コマンドをデフォルトの特権レベル 15 に戻すには、コマンドを使用します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **enable secret level** *level password*
4. **privilege exec level** *level command-string*
5. **end**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを開始します。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**<br>例：<br>`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 | **enable secret level** *level password*<br>例： | 特権レベル 7 の新しいイネーブル シークレット パスワードを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Device(config)# enable secret level 7 Zy72sKj` | |
| ステップ 4 | **privilege exec level** *level command-string*<br>例：<br>`Device(config)# privilege exec level 7 clear counters` | **clear counters** コマンドの特権レベルを、特権レベル 15 から特権レベル 7 に変更します。 |
| ステップ 5 | **end**<br>例：<br>`Device(config)# end` | グローバル コンフィギュレーション モードを終了します。 |

## 窓口のテクニカル サポート スタッフ用の設定の確認

ここでは、ネットワーキング デバイスが窓口のテクニカル サポート スタッフ用に適切に設定されていることを確認するタスクについて説明します。

### 始める前に

次のコマンドは、このタスクのために特権レベル 7 で実行するように変更済みです。

- **clear counters**
- **reload**

### 手順の概要

1. **enable** *level password*
2. **show privilege**
3. **clear counters**
4. **clear ip route** *
5. **reload in time**
6. **reload cancel**
7. **disable**
8. **show privilege**

### 手順の詳細

**ステップ 1** **enable** *level password*

level 引数に指定した特権レベルで、ネットワーキング デバイスにログインします。

例：

```
Device> enable 7 Zy72sKj
```

### ステップ 2 show privilege

現在の CLI セッションの特権レベルを表示します。

例：

```
Device# show privilege

Current privilege level is 7
```

### ステップ 3 clear counters

clear counters コマンドは、インターフェイスのカウンタをクリアします。このコマンドは、特権レベル 15 から特権レベル 7 に変更されました。

例：

```
Device# clear counters

Clear "show interface" counters on all interfaces [confirm]
Device#
02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console
```

### ステップ 4 clear ip route *

**clear** コマンドの *ip route* 引数文字列は、特権レベル 15 から特権レベル 7 に変更されていないため、使用できません。

例：

```
Device# clear ip route *
                                                                    ^
% Invalid input detected at '^' marker.
```

### ステップ 5 reload in time

reload コマンドによって、ネットワーキング デバイスはリブートされます。

例：

```
Device# reload in

10
Reload scheduled in 10 minutes by console
Proceed with reload? [confirm]

Device#

***
*** --- SHUTDOWN in 0:10:00 ---
***
02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20
```

### ステップ 6 reload cancel

**reload cancel** によって、以前に **reload in** *time* コマンドで設定したリロードが終了します。

例：

```
Device# reload cancel

***
*** --- SHUTDOWN ABORTED ---
***
04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED:  Scheduled reload cancelled at 15:38:46 PST Sun Mar 27
 2005
```

**ステップ 7** **disable**

現在の特権レベルを終了し、特権レベル 1 に戻します。

例：

```
Device# disable
```

**ステップ 8** **show privilege**

現在の CLI セッションの特権レベルを表示します。

例：

```
Device> show privilege

Current privilege level is 1
```

### トラブルシューティングのヒント

設定が希望どおりに機能しないため、設定から privilege コマンドを削除する場合、コマンドをデフォルトの特権レベルに戻すには、**privilege** コマンドに **reset** キーワードを使用します。たとえば、コンフィギュレーションから **privilege exec level** *reload* コマンドを削除し、**reload** コマンドをデフォルトの特権レベル 15 に戻すには、**privilege exec reset** *reload* コマンドを使用します。

### 次の作業

窓口のテクニカルサポートスタッフがログイン名を使用することを必須にして、セキュリティレベルを追加する場合、窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定 （34 ページ）に進みます。

## 窓口のテクニカル サポート スタッフのユーザ名を必須にするデバイスの設定

このタスクでは、窓口のテクニカルサポートスタッフが、admin のログイン名を使用してネットワーキング デバイスにログインすることを必須にするように、ネットワーキング デバイスを設定します。このタスクで設定された admin ユーザ名には、特権レベル 7 が割り当てられています。この名前を使用してログインするユーザは、前のタスクで特権レベル 7 に再割り当て

されたコマンドを実行できます。ユーザがユーザ名 admin で正常にログインすると、CLI セッションは自動的に特権レベル 7 に入ります。

Cisco IOS XE リリース 2.3 よりも前のリリースでは、2 種類のパスワードがユーザー名に関連付けられていました。タイプ 0 は、ルータの特権モードにアクセスできるすべてのユーザーから確認できるクリアテキストパスワードです。また、タイプ 7 は、**service password encryption** コマンドで暗号化されたパスワードです。

Cisco IOS XE リリース 2.3 以降のリリースでは、**username** コマンドに新しい **secret** キーワードを使用することで、ユーザー名のパスワードに Message Digest 5（MD5）暗号化を設定できます。

### 始める前に

次のコマンドは、このタスクのために特権レベル 7 で実行するように変更済みです。

- **clear counters**
- **reload**

コマンドの特権レベルを変更する手順については、窓口のテクニカル サポート スタッフ用のネットワーク デバイスの設定 （29 ページ）を参照してください。

（注） **username** コマンドの MD5 暗号化は、Cisco IOS XE リリース 2.3 よりも前の Cisco IOS ソフトウェアバージョンではサポートされません。

ネットワーキング デバイスでは、aaa-new model コマンドをイネーブルにしないでください。コンソールポートでのローカル CLI セッションの場合、またはリモート CLI セッションの場合、**login local** コマンドを設定しないでください。

（注） このタスクの手順では、わかりやすくするために、各手順に関係する構文に使用しています。これらのコマンドと併用できるその他の引数いては、お使いの Cisco IOS XE リリースの Cisco IOS コマンド リファ照してください。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **username** *username* **privilege** *level* **secret** *password*
4. **end**
5. **disable**
6. **login** *username*
7. **show privilege**
8. **clear counters**

9. **clear** *ip route* *
10. **reload in** *time*
11. **reload cancel**
12. **disable**
13. **show privilege**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Device> enable` | 特権 EXEC モードを開始します。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**<br>例：<br>`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 | **username** *username* **privilege** *level* **secret** *password*<br>例：<br>`Device(config)# username admin privilege 7 secret Kd65xZa` | ユーザ名を作成し、*password* テキスト ストリングに MD5 暗号化を適用します。 |
| ステップ 4 | **end**<br>例：<br>`Device(config)# end` | グローバル コンフィギュレーション モードを終了します。 |
| ステップ 5 | **disable**<br>例：<br>`Device# disable` | 現在の特権レベルを終了し、ユーザ EXEC モードに戻します。 |
| ステップ 6 | **login** *username*<br>例：<br>`Device> login admin` | ユーザにログインします。プロンプトが表示されたら、手順3で設定したユーザ名とパスワードを入力します。 |
| ステップ 7 | **show privilege**<br>例：<br>`Device# show privilege`<br>`Current privilege level is 7` | **show privilege** コマンドで、CLI セッションの特権レベルが表示されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 8 | **clear counters**<br>例：<br>`Device# clear counters`<br>`Clear "show interface" counters on all interfaces [confirm]`<br>`Device#`<br>`02:41:37: %CLEAR-5-COUNTERS: Clear counter on all interfaces by console` | **clear counters** コマンドでインターフェイスカウンタがクリアされます。このコマンドは、特権レベル 15 から特権レベル 7 に変更されました。 |
| ステップ 9 | **clear** *ip route* *<br>例：<br>`Device# clear ip route *`<br>`^`<br>`% Invalid input detected at '^' marker.` | **clear** コマンドの *ip route* 引数文字列は、特権レベル 15 から特権レベル 7 に変更されていないため、使用できません。 |
| ステップ 10 | **reload in** *time*<br>例：<br>`Device# reload in`<br>`10`<br>`Reload scheduled in 10 minutes by console`<br>`Proceed with reload? [confirm]`<br>`Device#`<br>`***`<br>`*** --- SHUTDOWN in 0:10:00 ---`<br>`***`<br>`02:59:50: %SYS-5-SCHEDULED_RELOAD: Reload requested for 23:08:30 PST Sun Mar 20` | reload コマンドによって、ネットワーキングデバイスはリブートされます。 |
| ステップ 11 | **reload cancel**<br>例：<br>`Device# reload cancel`<br>`***`<br>`*** --- SHUTDOWN ABORTED ---`<br>`***`<br>`04:34:08: %SYS-5-SCHEDULED_RELOAD_CANCELLED: Scheduled reload cancelled at 15:38:46 PST Sun Mar 27 2005` | **reload cancel** コマンドによって、以前に **reload in** *time* コマンドで設定したリロードが終了します。 |
| ステップ 12 | **disable**<br>例：<br>`Device# disable` | 現在の特権レベルを終了し、ユーザ EXEC モードに戻します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 13 | **show privilege**<br>例：<br>`Device> show privilege`<br>`Current privilege level is 1` | 現在のCLIセッションの特権レベルを表示します。 |

# ローカルセッションの忘失パスワードおよび誤設定パスワードの復元

コンソール ポートでローカル CLI セッションの忘失パスワードおよび誤設定パスワードを復元するために使用できる方式は3つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

## ネットワーク デバイスがリモート CLI セッションを許可するように設定されている

ローカルCLIセッションの忘失パスワードまたは誤設定パスワードを復元する最速の方式は、ネットワーキング デバイスとリモート CLI セッションを確立し、ローカル CLI セッションのパスワードの設定と確認（20ページ）を繰り返す方法です。この手順を実行するには、リモートCLIセッションを許可するようにネットワーキング デバイスを設定し、さらにリモートCLIセッションのパスワードを知っている必要があります。

## ネットワーク デバイスがリモート CLI セッションを許可するように設定されていない

- ネットワーキング デバイスに対するリモート セッションを確立できず、誤設定したローカル CLI セッション パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前のローカル CLI セッション パスワードが復元されます。

**注意** ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

# リモートセッションの忘失パスワードおよび誤設定パスワードの復元

忘失または誤設定したリモート CLI セッション パスワードから復元するために使用できる方式は3つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

## ネットワーク デバイスがローカル CLI セッションを許可するように設定されている

リモート CLI セッションの忘失パスワードまたは誤設定パスワードを復元する最速の方式は、ネットワーキング デバイスとローカル CLI セッションを確立し、リモート CLI セッションのパスワードの設定と確認 （17 ページ）を繰り返す方法です。この手順を実行するには、ローカル CLI セッションを許可するようにネットワーキング デバイスを設定し、さらにローカル CLI セッションのパスワードを知っている必要があります。

## ネットワーク デバイスがローカル CLI セッションを許可するように設定されていない

- ネットワーキング デバイスに対するローカル CLI セッションを確立できず、誤設定したリモート CLI セッション パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前のリモート CLI セッション パスワードが復元されます。

⚠

**注意** ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

# 特権 EXEC モードの忘失パスワードまたは誤設定パスワードの復元

忘失または誤設定した特権 EXEC モード パスワードから復元するために使用できる方式は 2 つあります。使用する方式は、ネットワーキング デバイスの現在の設定によって変わります。

## 誤設定された特権 EXEC モードのパスワードが保存されていない

- 誤設定した特権 EXEC モード パスワードをスタートアップ コンフィギュレーションに保存していない場合、ネットワーキング デバイスを再起動できます。ネットワーキング デバイスを再起動すると、スタートアップ コンフィギュレーション ファイルが読み込まれます。以前の特権 EXEC モード パスワードが復元されます。

⚠

**注意** ネットワーキング デバイスの再起動によって、トラフィックの転送が停止されます。また、DHCP サーバ サービスなど、ネットワーキング デバイスで実行されているすべてのサービスが中断されます。必要な操作は、ネットワークのメンテナンスに割り当てられた期間中に、ネットワーキング デバイスを再起動することだけです。

# パスワード、特権、およびログインによるセキュリティ設定の設定例

## 例：暗号化事前共有キーの設定

次に示すのは、タイプ6の事前共有キーが暗号化された場合の設定例です。この中には、ユーザに対して表示されるプロンプトやメッセージも含まれています。

```
Device(config)# password encryption aes
New key:
Confirm key:
Device (config)#

01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Device (config)# exit
```

## 例：ユーザがリモートセッションをクリア可能にするデバイスの設定

次に、管理者以外のユーザがリモートCLIセッションの仮想端末（VTY）回線をクリアできるように、ネットワーキング デバイスを設定する例を示します。

最初の項は、この例の実行コンフィギュレーションの抜粋です。ここでは、この例を使用する方法を示します。

次の項は、実行コンフィギュレーションの抜粋です。

```
!
privilege exec level 7 clear line
!
no aaa new-model
!
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege exec level 7 clear line
!
! the privilege exec level 7 clear command below is entered automatically
! when you enter the privilege exec level 7 clear line command above, do
! not enter it again
!
privilege exec level 7 clear
!
```

次の項では、**login**コマンドを使用して、ユーザーがadminのユーザー名を使用してネットワークデバイスにログインする場合を示します。

```
R1> login
Username: admin
Password:
```

次の項では、**show privilege** コマンドを使用して、現在の特権レベルが 7 であることを示します。

```
R1# show privilege

Current privilege level is 7
R1#
```

次の項では、**show user** コマンドを使用して、現在、2 ユーザー（admin と root）がネットワークデバイスにログインしていることを示します。

```
R1# show user

    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
   2 vty 0     root       idle                 00:00:17 172.16.6.2
  Interface    User               Mode         Idle     Peer Address
```

次の項では、**clear line** *2* コマンドを使用して、ユーザー名 root に使用されているリモート CLI セッションを終了します。

```
R1# clear line  2

[confirm]
 [OK]
```

次の項では、**show user** コマンドを使用して、ネットワークデバイスに現在ログインしているユーザーは admin だけであることを示します。

```
R1# show user
    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

# 例：ユーザが実行コンフィギュレーションを表示可能にするデバイスの設定

### 特権レベル 15 を持つユーザ

次に、管理者以外のユーザ（特権EXECモードへのアクセスなし）が、実行コンフィギュレーションを自動的に表示できるようにネットワーキングデバイスを設定する例を示します。この例では、ユーザ名を特権レベル 15 に設定する必要があります。コンフィギュレーション ファイルの多くのコマンドは、特権レベル 15 へのアクセス権を持つユーザだけが表示できるためです。

この点を解決するには、**show running-config** コマンドの実行中、一時的に特権レベル 15 へのユーザーアクセスを許可し、コンフィギュレーション ファイルの表示後に、CLIセッションを終了します。この例では、設定ファイルの表示後に、ネットワーキング デバイスが CLI セッションを自動的に終了します。その他の設定手順は必要ありません。

**注意** **username** コマンドに **noescape** キーワードを含める必要があります。これは、コンフィギュレーション ファイルの表示を終了し、特権レベル 15 で実行するセッションを終了するエスケープ文字をユーザーが入力しないようにするためです。

```
!
!
username viewconf privilege 15 noescape secret 5 $1$zA9C$TDWD/Q0zwp/5xRwRqdgc/.
username viewconf autocommand show running-config
!
```

### レベル 15 より低い特権レベルを持つユーザ

次の例は、レベル 15 より低い特権レベルを持つユーザが、実行コンフィギュレーションを表示可能にするネットワーク デバイスの設定方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# privilege exec all level 5 show running-config
Device(config)# file privilege 5
Device(config)# privilege configure all level 5 logging
Device(config)# end
Device# show privilege

Current privilege level is 5

Device# show running-config

Building configuration...

Current configuration : 128 bytes
!
boot-start-marker
boot-end-marker
!
no logging queue-limit
logging buffered 10000000
no logging rate-limit
!
!
!
end
```

# 例：ユーザがインターフェイスをシャットダウンおよびイネーブル化することを可能にするデバイスの設定

次に、管理者以外のユーザが、インターフェイスをシャットダウンおよびイネーブルにできるように、ネットワーキング デバイスを設定する例を示します。

最初の項は、この例の実行コンフィギュレーションの抜粋です。ここでは、この例を使用する方法を示します。

次の項は、実行コンフィギュレーションの抜粋です。

```
!
no aaa new-model
!
username admin privilege 7 secret 5 $1$tmIw$1aM7sadKhWMpkVTzxNw1J.
!
privilege interface all level 7 shutdown
privilege interface all level 7 no shutdown
privilege configure level 7 interface
privilege exec level 7 configure terminal
!
! the privilege exec level 7 configure command below is entered automatically
! when you enter the privilege exec level 7 configure terminal command above, do
! not enter it again
!
privilege exec level 7 configure
!
```

次の項では、**login** コマンドを使用して、ユーザーが admin のユーザー名を使用してネットワークデバイスにログインする場合を示します。

```
R1> login
Username: admin
Password:
```

次の項では、**show privilege** コマンドを使用して、現在の特権レベルが 7 であることを示します。

```
R1# show privilege
Current privilege level is 7
```

次の項では、**show user** コマンドを使用して、ネットワークデバイスに現在ログインしているユーザーは admin だけであることを示します。

```
R1# show user
    Line       User       Host(s)              Idle       Location
*  0 con 0     admin      idle                 00:00:00
  Interface    User               Mode         Idle     Peer Address
```

次の項は、admin ユーザがインターフェイスをシャットダウンおよびイネーブルにできる権限を持つことを示します。

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface ethernet 1/0
R1(config-if)# shutdown
R1(config-if)# no shutdown
R1(config-if)# exit
R1#
```

# 次の作業

ネットワーキングデバイスのセキュリティの基本を設定したら、次のように高度なオプションを考慮できます。

- ロールベースのCLIアクセス：ネットワークマネージャが、さまざまなレベルのテクニカルサポートスタッフに、異なるレベルのCLIコマンドのアクセスを付与する場合、ロールベースのCLIアクセス機能には、（このドキュメントで説明する）**privilege** コマンドよりも包括的なオプションセットが用意されています。
- AAA セキュリティ：多くのシスコ ネットワーク デバイスは、認証、許可、およびアカウンティング（AAA）機能を使用して、高度なレベルのセキュリティを提供しています。ネットワーキング デバイスで AAA を使用し、リモート TACACS+ または RADIUS サーバを併用することで、このドキュメントで説明しているすべてのタスクと、他のより高度なセキュリティ機能を実装できます。ネットワーク デバイスのローカルで実行できる AAA セキュリティ機能を設定する方法、またはTACACS+やRADIUSサーバを使用してリモート AAA セキュリティを設定する方法については、『*Cisco IOS XE Security Configuration Guide:Securing User Services* リリース 2』を参照してください。

# その他の参考資料

ここでは、パスワードによるセキュリティの設定、およびネットワーキングデバイスでのCLIセッションのログイン ユーザ名に関連する関連資料について説明します。

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| CLI コマンドおよび設定情報に対するユーザ アクセスの管理 | 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』Release 2 の「Role-Based CLI Access」 |
| AAA セキュリティ機能 | 『*Cisco IOS XE Security Configuration Guide: Securing User Services*』Release 2 |
| TACACS+ およびRADIUS での特権レベルの割り当て | 『How to Assign Privilege Levels with TACACS+ and RADIUS』 |

### 標準

| 標準 | タイトル |
|---|---|
| この機能によってサポートされる新しい RFC または変更された RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。 | -- |

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。 | 選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

### RFC

| RFC | タイトル |
|---|---|
| この機能によってサポートされる新しい RFC または変更された RFC はありません。また、この機能による既存 RFC のサポートに変更はありません。 | -- |

### シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| 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。<br>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。<br>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。 | http://www.cisco.com/en/US/support/index.html |

# パスワード、特権、およびログインによるセキュリティ設定に関する機能情報

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 に移動します。Cisco.com のアカウントは必要ありません。

**表 *1*:ネットワーク デバイス上の *CLI* セッションでのパスワード、特権レベル、およびログイン ユーザ名によるセキュリティ設定に関する機能情報**

| 機能名 | リリース | 機能の設定情報 |
|---|---|---|
| 強化されたパスワード セキュリティ | | Enhanced Password Security 機能を使用すると、ユーザ名のパスワードに MD5 暗号化を設定できます。MD5 暗号化は、暗号化されたパスワードの逆送信を不可能にする一方向ハッシュ関数であり、強力な暗号化保護を可能にします。MD5 暗号化を使用すると、クリアテキストパスワードを取得できません。MD5 で暗号化されたパスワードは、クリア テキスト パスワードを取得可能にすることを必須にするプロトコルでは使用できません。たとえば、チャレンジハンドシェーク認証プロトコル（CHAP）などのプロトコルです。 |

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。