



# パスワードおよび権限レベルによるスイッチアクセスの制御

- [パスワードおよび権限によるスイッチアクセスの制御の制約事項 \(1 ページ\)](#)
- [パスワードおよび権限レベルに関する情報 \(1 ページ\)](#)
- [パスワードおよび権限レベルでスイッチアクセスを制御する方法 \(4 ページ\)](#)
- [スイッチアクセスのモニタリング \(18 ページ\)](#)
- [パスワードおよび権限レベルの設定例 \(18 ページ\)](#)

## パスワードおよび権限によるスイッチアクセスの制御の制約事項

パスワードおよび権限によるスイッチアクセスの制御の制約事項は、次のとおりです。

- **boot manual** 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、スイッチを手動で起動するように設定している場合は、パスワード回復をディセーブルにできません。このコマンドは、スイッチの電源の再投入後、ブートローダプロンプト (*switch:*) を表示させます。

## パスワードおよび権限レベルに関する情報

### デフォルトのパスワードおよび権限レベル設定

ネットワークで端末のアクセスコントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワークデバイスへのアクセスが制限されます。権限レベルによって、ネットワークデバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

次の表に、デフォルトのパスワードおよび権限レベル設定を示します。

表 1: デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
イネーブルパスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です (特権 EXEC レベル)。パスワードは、コンフィギュレーションファイル内では暗号化されていない状態です。
イネーブル シークレット パスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です (特権 EXEC レベル)。パスワードは、暗号化されてからコンフィギュレーションファイルに書き込まれます。
回線パスワード	パスワードは定義されていません。

## 追加のパスワードセキュリティ

セキュリティレベルを強化するために、特にネットワークを超えるパスワードや Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバーに保存されたパスワードについて、グローバルコンフィギュレーションコマンド **enable password** または **enable secret** を使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード (デフォルト設定) または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

**enable secret** コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

パスワードの暗号化をイネーブルにすると、ユーザー名パスワード、認証キーパスワード、イネーブル コマンドパスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

### マスクされたシークレットパスワード



(注) この機能は、Cisco Catalyst 3560-CX シリーズ スイッチでのみサポートされています。

**enable secret** コマンドを使用すると、パスワードは暗号化されますが、パスワードを入力するときに端末に表示されます。端末でパスワードをマスクするには、**masked-secret** 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。このパスワードの暗号化タイプは、デフォルトではタイプ 9 です。

このコマンドを使用して、コモンライテリアポリシーのマスクされたシークレットパスワードを設定できます。

## パスワードの回復

スイッチに物理的にアクセスできるエンドユーザは、デフォルトで、スイッチの電源投入時にブートプロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。この機能がイネーブルの場合、エンドユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブートプロセスに割り込むことができます。パスワード回復をディセーブルにしても、ブートプロセスに割り込んでパスワードを変更できますが、コンフィギュレーションファイル (config.text) および VLAN データベース ファイル (vlan.dat) は削除されます。

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーションファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーションファイルのバックアップ コピーを保存しないでください。VTP (VLAN トランッキング プロトコル) トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

パスワードの回復を再びイネーブルにするには、**service password-recovery** 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。

## 端末回線の Telnet 設定

初めてスイッチに電源を投入すると、自動セットアッププログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。さらに、セットアッププログラムは、パスワードによる Telnet アクセス用にスイッチを設定することを要求します。セットアッププログラムの実行中にこのパスワードを設定しなかった場合は、端末回線に対する Telnet パスワードを設定するときに設定できます。

## ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

## 権限レベル

シスコデバイスでは、権限レベルを使用して、スイッチ動作の異なるレベルに対してパスワードセキュリティを提供します。デフォルトでは、Cisco IOS ソフトウェアは、パスワードセキュリティの 2 つのモード (権限レベル) で動作します。ユーザ EXEC (レベル 1) および特権 EXEC (レベル 15) です。各モードに、最大 16 個の階層レベルからなるコマンドを設定で

きます。複数のパスワードを設定することにより、ユーザグループ別に特定のコマンドへのアクセスを許可することができます。

### 回線の権限レベル

ユーザは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ラインコンフィギュレーションコマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっている場合、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル2のセキュリティを割り当て、レベル2のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル3のセキュリティを割り当て、そのパスワードを限られたユーザグループに配布することもできます。

### コマンド権限レベル

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル15に設定すると、**show** コマンドと **show ip** コマンドは、異なるレベルに個別に設定しない限り、権限レベルは自動的に15に設定されます。

# パスワードおよび権限レベルでスイッチ アクセスを制御する方法

## スタティック 有効パスワードの設定または変更

イネーブルパスワードは、特権EXECモードへのアクセスを制御します。スタティックイネーブルパスワードを設定または変更するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **enable password *password***
4. **end**
5. **show running-config**
6. **copy running-config startup-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	<b>enable</b> 例： スイッチ> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： スイッチ# <b>configure terminal</b>	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	<b>enable password password</b> 例： スイッチ(config)# <b>enable password secret321</b>	特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。 デフォルトでは、パスワードは定義されません。 <i>password</i> には、1～25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符 (?) は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようになります。 <ol style="list-style-type: none"> <li>1. <b>abc</b> を入力します。</li> <li>2. Ctrl+v を入力します。</li> <li>3. <b>?123</b> を入力します。</li> </ol> システムからイネーブルパスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。
ステップ 4	<b>end</b> 例： スイッチ(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例：	入力を確認します。

	コマンドまたはアクション	目的
	スイッチ# <code>show running-config</code>	
ステップ 6	<b>copy running-config startup-config</b> 例： スイッチ# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## 暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特権 EXEC モード (デフォルト) または指定された特権レベルにアクセスするためにユーザーが入力する必要がある暗号化パスワードを確立するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを使用します。
  - `enable password [level level] {password encryption-type encrypted-password}`
  - `enable secret [level level] {password encryption-type encrypted-password}`
4. **service password-encryption**
5. **end**
6. **show running-config**
7. **copy running-config startup-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	<b>enable</b> 例： スイッチ> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 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
<b>ステップ 3</b>	次のいずれかを使用します。 <ul style="list-style-type: none"> <li>• <code>enable password [level level] {password encryption-type encrypted-password}</code></li> <li>• <code>enable secret [level level] {password encryption-type encrypted-password}</code></li> </ul> 例 : スイッチ(config)# <code>enable password example102</code>  または スイッチ(config)# <code>enable secret level 1 password secret123sample</code>	<ul style="list-style-type: none"> <li>• 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。</li> <li>• シークレットパスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。               <ul style="list-style-type: none"> <li>• (任意) <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です (特権 EXEC モード権限)。</li> <li>• <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。</li> <li>• (任意) <i>encryption-type</i> には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。</li> </ul> </li> </ul> <p>(注) 暗号化タイプを指定してクリアテキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。</p>
<b>ステップ 4</b>	<b>service password-encryption</b>  例 :  スイッチ(config)# <code>service password-encryption</code>	<p>(任意) パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。</p> <p>暗号化を行うと、コンフィギュレーションファイル内でパスワードが読み取り可能な形式になるのを防止できます。</p>

	コマンドまたはアクション	目的
ステップ 5	<b>end</b> 例：  スイッチ(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例：  スイッチ# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  スイッチ# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## マスクされたシークレットパスワードの設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを使用します。
  - **username namemasked-secret**
  - **username namecommon-criteria-policy policy-name masked-secret**
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	<b>enable</b> 例：  Device> <b>enable</b>	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	<b>configure terminal</b> 例：  Device# <b>configure terminal</b>	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
ステップ 3	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <b>username namemasked-secret</b></li> <li>• <b>username namecommon-criteria-policy policy-name masked-secret</b></li> </ul> <p>例：</p> <pre>Device(config)# username cisco masked-secret</pre> <p>または</p> <pre>Device(config)# username common-criteria-policy test-policy masked-secret</pre>	<ul style="list-style-type: none"> <li>• マスクされたシークレットパスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。</li> <li>• コモンクライテリアポリシーのマスクされたシークレットパスワードを定義します。</li> <li>• マスクされたシークレットパスワードは 5 文字以上にする必要があります。マスクされたシークレットパスワードの最大長は 256 文字です。デフォルトでは、パスワードは定義されません。</li> </ul>
ステップ 4	<p><b>end</b></p> <p>例：</p> <pre>Device(config)# end</pre>	<p>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。</p>

## パスワード回復のディセーブル化

パスワードの回復をディセーブルにしてスイッチのセキュリティを保護するには、次の手順を実行します。

### 始める前に

パスワード回復をディセーブルにする場合は、エンドユーザがブート プロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーション ファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーション ファイルのバックアップ コピーを保存しないでください。VTP (VLAN トランッキング プロトコル) トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **system disable password recovery switch {all | <1-9>}**
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	<b>enable</b> 例： スイッチ> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： スイッチ# <b>configure terminal</b>	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	<b>system disable password recovery switch {all  &lt;1-9&gt;}</b> 例： スイッチ(config)# <b>system disable password recovery switch all</b>	パスワード回復をディセーブルにします。  • <b>all</b> ：スタック内のスイッチで設定を行います。 • <b>&lt;1-9&gt;</b> ：選択したスイッチ番号で設定を行います。  この設定は、フラッシュメモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイルシステムには含まれません。また、ユーザーがアクセスすることはできません。
ステップ 4	<b>end</b> 例： スイッチ(config)# <b>end</b>	特権 EXEC モードに戻ります。

## 次のタスク

**disable password recovery** を削除するには、**no system disable password recovery switch all** 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。

## 端末回線に対する Telnet パスワードの設定

接続された端末回線に対する Telnet パスワードを設定するには、ユーザー EXEC モードで次の手順を実行します。

## 始める前に

- エミュレーション ソフトウェアを備えた PC またはワークステーションをスイッチ コンソール ポートに接続するか、または PC をイーサネット管理ポートに接続します。

- コンソールポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドラインプロンプトが表示されるまで、Return キーを何回か押す必要があります。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **line vty 0 15**
4. **password *password***
5. **end**
6. **show running-config**
7. **copy running-config startup-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	<b>enable</b> 例： スイッチ> <b>enable</b>	(注) パスワードが特権 EXEC モードへのアクセスに必要な場合は、その入力が求められます。  特権 EXEC モードを開始します。
ステップ 2	<b>configure terminal</b> 例： スイッチ# <b>configure terminal</b>	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	<b>line vty 0 15</b> 例： スイッチ(config)# <b>line vty 0 15</b>	Telnet セッション（回線）の数を設定し、ライン コンフィギュレーション モードを開始します。  コマンド対応スイッチでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ 4	<b>password <i>password</i></b> 例： スイッチ(config-line)# <b>password abcxyz543</b>	1 つまたは複数の回線に対応する Telnet パスワードを設定します。  <i>password</i> には、1 ～ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。

	コマンドまたはアクション	目的
ステップ 5	<b>end</b> 例：  スイッチ(config-line)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例：  スイッチ# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  スイッチ# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ユーザ名とパスワードのペアの設定

ユーザー名とパスワードのペアを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **username name [ privilege level] { password encryption-type password}**
4. 次のいずれかを使用します。
  - **line console 0**
  - **line vty 0 15**
5. **login local**
6. **end**
7. **show running-config**
8. **copy running-config startup-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	<b>enable</b> 例：  スイッチ> <b>enable</b>	特権 EXEC モードを有効にします。  • 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
ステップ 2	<b>configure terminal</b> 例： スイッチ# <b>configure terminal</b>	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	<b>username name [ privilege level] { password encryption-type password}</b> 例： スイッチ (config)# <b>username adamsample privilege 1 password secret456</b> スイッチ (config)# <b>username 111111111111 mac attribute</b>	各ユーザのユーザ名、権限レベル、パスワードを設定します。 <ul style="list-style-type: none"> <li>• <b>name</b> には、ユーザー ID を 1 ワードで指定するか、または MAC アドレスを指定します。スペースと引用符は使用できません。</li> <li>• ユーザ名と MAC フィルタの両方に対し、最大 12000 のクライアントを個別に設定できます。</li> <li>• (任意) <b>level</b> には、アクセス権を得たユーザーに設定する権限レベルを指定します。指定できる範囲は 0～15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。</li> <li>• <b>encryption-type</b> には、暗号化されていないパスワードが後ろに続く場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。</li> <li>• <b>password</b> には、スイッチへアクセスするためにユーザーが入力しなければならないパスワードを指定します。パスワードは 1～25 文字で、埋め込みスペースを使用でき、<b>username</b> コマンドの最後のオプションとして指定します。</li> </ul>
ステップ 4	次のいずれかを使用します。 <ul style="list-style-type: none"> <li>• <b>line console 0</b></li> <li>• <b>line vty 0 15</b></li> </ul> 例： スイッチ (config)# <b>line console 0</b> または スイッチ (config)# <b>line vty 15</b>	ライン コンフィギュレーション モードを開始し、コンソール ポート (回線 0) または VTY 回線 (回線 0～15) を設定します。

## コマンドの特権レベルの設定

	コマンドまたはアクション	目的
ステップ 5	<b>login local</b> 例：  スイッチ(config-line)# <b>login local</b>	ログイン時のローカルパスワードチェックをイネーブルにします。認証は、ステップ 3 で指定されたユーザ名に基づきます。
ステップ 6	<b>end</b> 例：  スイッチ(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b> 例：  スイッチ# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例：  スイッチ# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## コマンドの特権レベルの設定

コマンドの権限レベルを設定するには、次の手順を実行します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **privilege mode level level command**
4. **enable password level level password**
5. **end**
6. **copy running-config startup-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	<b>enable</b> 例：	特権 EXEC モードを有効にします。  • 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
	スイッチ> <b>enable</b>	
ステップ 2	<b>configure terminal</b> 例： スイッチ# <b>configure terminal</b>	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	<b>privilege mode level level command</b> 例： スイッチ(config)# <b>privilege exec level 14 configure</b>	コマンドの特権レベルを設定します。  <ul style="list-style-type: none"> <li>• <i>mode</i> には、グローバル コンフィギュレーション モードの場合は <b>configure</b> を、EXEC モードの場合は <b>exec</b> を、インターフェイス コンフィギュレーション モードの場合は <b>interface</b> を、ライン コンフィギュレーション モードの場合は <b>line</b> をそれぞれ入力します。</li> <li>• <i>level</i> の範囲は 0 ~ 15 です。レベル 1 が通常のユーザー EXEC モード権限です。レベル 15 は、<b>enable</b> パスワードによって許可されるアクセスレベルです。</li> <li>• <i>command</i> には、アクセスを制限したいコマンドを指定します。</li> </ul>
ステップ 4	<b>enable password level level password</b> 例： スイッチ(config)# <b>enable password level 14 SecretPswd14</b>	権限レベルをイネーブルにするためのパスワードを指定します。  <ul style="list-style-type: none"> <li>• <i>level</i> の範囲は 0 ~ 15 です。レベル 1 が通常のユーザー EXEC モード権限です。</li> <li>• <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。</li> </ul>
ステップ 5	<b>end</b> 例： スイッチ(config)# <b>end</b>	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
ステップ 6	<b>copy running-config startup-config</b> 例： スイッチ# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 回線のデフォルト特権レベルの変更

指定した回線のデフォルトの権限レベルを変更するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **line vty line**
4. **privilege level level**
5. **end**
6. **copy running-config startup-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	<b>enable</b> 例： スイッチ> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： スイッチ# <b>configure terminal</b>	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	<b>line vty line</b> 例： スイッチ(config)# <b>line vty 10</b>	アクセスを制限する仮想端末回線を選択します。
ステップ 4	<b>privilege level level</b> 例：	回線のデフォルト特権レベルを変更します。 <i>level</i> の範囲は 0 ~ 15 です。レベル 1 が通常のコピー EXEC モード権限です。レベル 15 は、 <b>enable</b>



	コマンドまたはアクション	目的
	スイッチ(config)# <b>privilege level 15</b>	パスワードによって許可されるアクセス レベルです。
ステップ 5	<b>end</b> 例：  スイッチ(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>copy running-config startup-config</b> 例：  スイッチ# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

#### 次のタスク

ユーザーは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ラインコンフィギュレーションコマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっている場合は、ユーザはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

## 権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、ユーザー EXEC モードで次の手順を実行します。

#### 手順の概要

1. **enable level**
2. **disable level**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable level</b> 例：  スイッチ> <b>enable 15</b>	指定された特権レベルにログインします。  この例で、レベル 15 は特権 EXEC モードです。  <i>level</i> に指定できる範囲は 0 ~ 15 です。

	コマンドまたはアクション	目的
ステップ 2	<b>disable level</b> 例： スイッチ# <b>disable 1</b>	指定した特権レベルを終了します。 この例で、レベル 1 はユーザ EXEC モードです。 <i>level</i> に指定できる範囲は 0 ~ 15 です。

## スイッチ アクセスのモニタリング

表 2: DHCP 情報を表示するためのコマンド

<b>show privilege</b>	権限レベルの設定を表示します。
-----------------------	-----------------

## パスワードおよび権限レベルの設定例

### 例：スタティック イネーブルパスワードの設定または変更

次に、イネーブルパスワードを `1lu2c3k4y5` に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モードアクセス）。

```
スイッチ(config)# enable password 1lu2c3k4y5
```

### 例：暗号化によるイネーブルおよびイネーブルシークレットパスワードの保護

次に、権限レベル 2 に対して暗号化パスワード `$1$FaD0$Xyti5Rkls3LoyxzS8` を設定する例を示します。

```
スイッチ(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

### 例：マスクされたシークレットパスワードの設定

次に、マスクされたシークレットパスワードを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username cisco masked-secret
Enter secret: *****
Confirm secret: *****
```

次に、コモンクライテリアポリシーのマスクされたシークレットパスワードを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# username cisco common-criteria-policy test-policy masked-secret
Enter secret: *****
Confirm secret: *****
```

## 例：端末回線に対する Telnet パスワードの設定

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
スイッチ(config)# line vty 10
スイッチ(config-line)# password let45me67in89
```

## 例：コマンドの権限レベルの設定

ここで、**configure** コマンドを権限レベル 14 に設定する方法、レベル 14 のコマンドを使用する場合にユーザーが入力するパスワードとして *SecretPswd14* を定義する方法を示します。

```
スイッチ(config)# privilege exec level 14 configure
スイッチ(config)# enable password level 14 SecretPswd14
```

■ 例：コマンドの権限レベルの設定

## 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。