



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 \(2 ページ\)](#)
- [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 \(6 ページ\)](#)
- [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の設定例 \(19 ページ\)](#)
- [スイッチアクセスのモニタリング \(21 ページ\)](#)
- [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の機能履歴 \(22 ページ\)](#)

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

グローバル コンフィギュレーション モードで **boot manual** 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。

可逆的パスワードタイプの制約事項とガイドライン

- スタートアップ コンフィギュレーション にタイプ 6 のパスワードがあり、タイプ 6 のパスワードがサポートされていないバージョンにダウングレードすると、デバイスからロックアウトされる可能性があります。

不可逆的パスワードタイプの制約事項とガイドライン

- ユーザ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 は、より強力なパスワードタイプ 8 または 9 に移行する必要があります。詳細については、「[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 \(7 ページ\)](#)」を参照してください。

- プレーンテキストパスワードは、不可逆的暗号化パスワードタイプ 9 に変換されます。



注 これは、Cisco IOS Release 15.2(7)E3 以降のリリースでサポートされます。

パスワードおよび権限レベルに関する情報

次の各項では、パスワードと権限レベルについて説明します。

不正アクセスの防止

不正ユーザによる、デバイスの再設定や設定情報の閲覧を防止できます。一般的には、ネットワーク管理者からデバイスへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザや、シリアルポートを通じてネットワーク外から接続するユーザ、またはローカルネットワーク内の端末またはワークステーションから接続するユーザによるアクセスを制限します。

デバイスへの不正アクセスを防止するには、次のセキュリティ機能を1つまたは複数設定します。

- 最低限のセキュリティとして、各デバイスポートでパスワードおよび権限を設定します。このパスワードは、デバイスにローカルに保存されます。ユーザがポートまたは回線を通じてデバイスにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、デバイスにアクセスできません。
- 追加のセキュリティレイヤとして、ユーザ名とパスワードをペアで設定することもできます。このペアはデバイス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、デバイス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。
- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティサーバ上のデータベースに保存できます。これにより、複数のネットワークング デバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。詳細については、『Cisco IOS Login Enhancements』マニュアルを参照してください。

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、暗号化された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

マスクされていないシークレットパスワード

特にネットワーク間を行き交う、または TFTP サーバに保存されるパスワードに対してセキュリティレイヤを追加するには、グローバル コンフィギュレーション モードで **enable password** コマンドまたは **enable secret** コマンドのいずれかを使用できます。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 VTY 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

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。仮想端末プロトコル (VTP) 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、グローバル コンフィギュレーション モードで `service password-recovery` 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、別の権限レベルをイネーブルに設定することにより、**privilege level** 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。

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）を有効にできます。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有効にし、パスワードを暗号化および復号するためのマスター暗号キーを設定します。

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。

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

次の各項では、パスワードと権限レベルを使用したスイッチアクセスの制御方法に関するさまざまな設定例を示します。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	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	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	enable password password 例： Device(config)# enable password secret321	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> : 1 ~ 25 文字の英数字の文字列を指定します。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、次のようにします。 1. abc を入力します。 2. Ctrl+v を入力します。

	コマンドまたはアクション	目的
		<p>3. ?123 を入力します。</p> <p>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。</p>
ステップ 4	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 5	<p>show running-config</p> <p>例 :</p> <pre>Device# show running-config</pre>	入力を確認します。
ステップ 6	<p>copy running-config startup-config</p> <p>例 :</p> <pre>Device# copy running-config startup-config</pre>	(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) または任意の権限レベルにアクセスするためにユーザ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

	コマンドまたはアクション	目的
ステップ 1	<p>enable</p> <p>例 :</p> <pre>Device> enable</pre>	<p>特権 EXEC モードを有効にします。</p> <p>パスワードを入力します (要求された場合)。</p>
ステップ 2	<p>configure terminal</p> <p>例 :</p> <pre>Device configure terminal</pre>	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	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> enable password [level level] {unencrypted-password encryption-type encrypted-password} 	<ul style="list-style-type: none"> 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。

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> • enable secret [level level] {unencrypted-password encryption-type encrypted-password} <p>例 :</p> <pre>Device(config)# enable password level 12 example123</pre> <p>または</p> <pre>Device(config)# enable secret 9 \$9\$sMLBsTFXLnnHTk\$0L82</pre>	<ul style="list-style-type: none"> • 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。 • (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)。 • <i>unencrypted-password</i> には、1 ~ 25 文字の英数字の文字列を指定します。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。 • <i>encryption-type</i> の場合、enable password に使用可能なオプションはタイプ 0 と 7、enable secret に使用可能なオプションはタイプ 0、5、8、および 9 です。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。シークレット暗号化タイプ 9 はより安全であるため、アップグレードまたはダウングレード時に問題が発生しないように、タイプ 9 を選択することを推奨します。

	コマンドまたはアクション	目的
		(注)

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • シークレットパスワードの暗号化タイプを指定しない場合、パスワードはタイプ9に自動的に変換されます。 • 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、エラーが発生します。 • グローバル コンフィギュレーションモードで algorithm-type script コマンドを使用して、シークレットパスワードにタイプ9暗号化を手動で設定することもできます。次に例を示します。 <pre>Device(config)# username user1 algorithm-type script secret cisco</pre> または <pre>Device(config)# enable algorithm-type script secret cisco</pre> 特権 EXEC モードで write memory コマンドを実行し、タイプ9シークレットをスター

	コマンドまたはアクション	目的
		トアップ コンフィギュレーションに永続的に書き込みます。
ステップ 4	service password-encryption 例 : Device(config)# service password-encryption	(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。 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。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例 : Device# copy running-config startup-config	(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

	コマンドまたはアクション	目的
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。

	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"> • <code>username namemasked-secret</code> • <code>username namecommon-criteria-policy policy-name masked-secret</code> <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"> • 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。 • 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。 <ul style="list-style-type: none"> • 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。
ステップ 4	<p><code>end</code></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>

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の Telnet パスワードを設定するには、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

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

	コマンドまたはアクション	目的
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	line vty 0 15 例： Device(config)# line vty 0 15	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 device 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	password password 例： Device(config-line)# password abcxyz543	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> : 1 ~ 25 文字の英数字の文字列を指定します。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。
ステップ 5	end 例： Device(config-line)# end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例： Device# show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例： Device# copy running-config startup-config	(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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	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	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	username name [privilege level] { password encryption-type password} 例： Device(config)# username adamsample privilege 1 password secret456 Device(config)# username 111111111111 mac attribute	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"> • name：ユーザ 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。 • 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。 • level：（任意）ユーザがアクセス権を取得した後に持つ特権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。 • encryption-type：暗号化されていないパスワードが続くことを指定する場合は 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。 • password：デバイスにアクセスするためにユーザ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、username コマンドの最後のオプションとして指定します。
ステップ 4	次のいずれかを使用します。 <ul style="list-style-type: none"> • line console 0 	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）

	コマンドまたはアクション	目的
	• line vty 0 15 例： Device(config)# line console 0 または Device(config)# line vty 15	または vty 回線（回線 0～15）を設定します。
ステップ 5	login local 例： Device(config-line)# login local	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	end 例： Device(config-line)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例： Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例： Device# copy running-config startup-config	（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、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	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	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	privilege mode level level command 例：	コマンドの特権レベルを設定します。

	コマンドまたはアクション	目的
	Device(config)# privilege exec level 14 configure	<ul style="list-style-type: none"> • <i>mode</i> : グローバル コンフィギュレーション モードの場合は configure を、EXEC モードの場合は exec 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 interface を、ライン コンフィギュレーション モードの場合は line をそれぞれ入力します。 • <i>level</i> : 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。レベル 15 は、enable パスワードによって許可されるアクセスレベルです。 • <i>command</i> : アクセスを制限したいコマンドを指定します。
ステップ 4	enable password level level password 例 : Device(config)# enable password level 14 SecretPswd14	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"> • <i>level</i> : 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。 • <i>password</i> : 1 ~ 25 文字の英数字の文字列を指定します。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。
ステップ 5	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	copy running-config startup-config 例 : Device# copy running-config startup-config	(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

ユーザは、回線にログインし、別の権限レベルをイネーブルに設定することにより、**privilege level** 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。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。

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

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	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	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	line vty line 例： Device(config)# line vty 10	アクセスを制限する VTY を選択します。
ステップ 4	privilege level level 例： Device(config)# privilege level 15	回線のデフォルト特権レベルを変更します。 <i>level</i> : 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。レベル 15 は、 enable 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	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 6	copy running-config startup-config 例： Device# copy running-config startup-config	(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。

権限レベルへのログインおよび終了

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。

指定した権限レベルにログインし、指定した権限レベルを終了するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable level 例： Device> enable 15	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。 level : 範囲は 0 ~ 15 です。
ステップ 2	disable level 例： Device# disable 1	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。 level : 範囲は 0 ~ 15 です。

暗号化事前共有キーの設定

暗号化事前共有キーを設定するには、次の手順を実行します。

始める前に

この手順は、パスワードタイプ 6 への自動変換の前提条件です。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	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	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	key config-key password-encrypt [text] 例： Device(config)# key config-key password-encrypt	タイプ 6 の暗号キーをプライベート NVRAM に保存します。 <ul style="list-style-type: none"> （Enter キーを使用して）インタラクティブにキーボード操作を行う場合、暗号キーがすでに存在すれば、

	コマンドまたはアクション	目的
		<p>Old key、New key、Confirm key という3つのプロンプトが表示されます。</p> <ul style="list-style-type: none"> インタラクティブにキーボード操作を行う場合、暗号キーが存在しなければ、New key、Confirm key という2つのプロンプトが表示されます。 すでに暗号化されているパスワードを削除しようとする、次のプロンプトが表示されます。 <pre>WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:"</pre>
ステップ 4	password encryption aes 例 : <pre>Device(config)# password encryption aes</pre>	暗号化事前共有キーのイネーブル化
ステップ 5	end 例 : <pre>Device(config)# end</pre>	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。

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の設定例

次の項では、パスワードと権限レベルを使用したスイッチアクセスの制御の設定例を示します。

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

次の例は、イネーブルパスワードを `11u2c3k4y5` に変更する方法を示しています。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）。

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

```
Device> enable
Device# configure terminal
Device(config)# enable password 11u2c3k4y5
```

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 `1FaD0$Xyti5Rkls3LoyxzS8` を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# line vty 10
Device(config-line)# password let45me67in89
```

例：コマンドの権限レベルの設定

次の例は、**configure** コマンドを権限レベル 14 に設定し、ユーザがレベル 14 のコマンドを使用する場合に入力するパスワードとして *SecretPswd14* を定義する方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# line vty 10
Device(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
```

例：暗号化事前共有キーの設定

以下に、タイプ 6 の事前共有キーに暗号化を行った場合の設定例を示します。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> enable
Device# configure terminal
Device(config)# password encryption aes
Device(config)# key config-key password-encrypt
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)# end
```

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

コマンド	目的
show privilege	権限レベルの設定を表示します。
show running secret username	ユーザ名が作成され、デフォルトで type9 に暗号化されることを確認します。
show running secret enable	シークレットパスワードがデフォルトで type9 に暗号化されることを確認します。

パスワードおよび権限レベルによるスイッチ アクセスの制御の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS Release 15.2(7)E3k	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。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。