



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によるスイッチアクセス制御に関する情報 \(2 ページ\)](#)
- [パスワードおよび権限によるスイッチアクセスの設定方法 \(7 ページ\)](#)
- [パスワードおよび権限によるスイッチアクセスのモニター \(20 ページ\)](#)
- [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設定例 \(20 ページ\)](#)
- [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

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。

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7は、パスワードタイプ6に置き換えられます。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6に移行する必要があります。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。
- 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 \(8 ページ\)](#)」を参照してください。
- デバイスのスタートアップコンフィギュレーションに複雑なタイプ 9 シークレット (\$14\$ で始まるパスワード) がある場合、ダウングレードは複雑なタイプ 9 シークレットがサポートされているリリースでのみ実行できます。複雑なタイプ 9 シークレットは、Cisco IOS XE Gibraltar 16.11.2 以降のリリースでサポートされます。スタートアップコンフィギュレーションに複雑なタイプ 9 シークレットが含まれており、Cisco IOS XE Gibraltar 16.11.2 より前のリリース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。

複雑なタイプ 9 シークレットがサポートされていないリリースにダウングレードする前に、複雑なタイプ 9 シークレット (\$14\$ で始まるパスワード) またはタイプ 5 シークレット (\$1\$ で始まるパスワード) ではなく、タイプ 9 シークレット (\$9\$ で始まるパスワード) がスタートアップコンフィギュレーションに含まれていることを確認します。

デバイスが、Cisco IOS XE Fuji 16.9.x、Cisco IOS XE Gibraltar 16.10.x、または Cisco IOS XE Gibraltar 16.11.x から Cisco IOS XE Gibraltar 16.12.x へアップグレードされると、タイプ 5 シークレットは複雑なタイプ 9 シークレット (\$14\$ で始まるパスワード) に自動変換されます。たとえば、`username user1 secret 5 1dNmW$7jWhqdtZ2qBVz2R4CSZZC0` は `username user1 secret 9 14dNmW$QykGZEEGmiEGrE$C9D/fD0czicOtgaZAa1CTa2sgygi0Leyw3/cLqPY426` に自動変換されます。デバイスがアップグレードされたら、特権 EXEC モードで **write memory** コマンドを実行し、複雑なタイプ 9 シークレットをスター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。

- 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 XE Gibraltar 16.10.1 以降のリリースでサポートされています。

- 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。

パスワードおよび権限によるスイッチアクセス制御に関する情報

ここでは、パスワードおよび権限によるスイッチアクセス制御に関する情報を示します。

不正アクセスの防止

不正ユーザーによる、スイッチ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スイッチ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ーや、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ー、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ーによるアクセスを制限します。

スイッチ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、各スイッチ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、スイッチにローカルに保存されます。ユーザーがポートまたは回線を通じてスイッチ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、スイッチ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、ユーザー名とパスワードをペアで設定できます。このペアはスイッチ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。
- 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 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。

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스에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。

機能	デフォルト設定
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。

マスクされていないシークレットパスワード

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

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。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、**no system disable password recovery switch number|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 XE 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。ユーザー 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、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。

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7のパスワードはタイプ6に自動変換できます。



- (注)
- ユーザー名パスワードのタイプ 6 の暗号化パスワードは、Cisco IOS XE Gibraltar 16.10.1 以降のリリースでサポートされています。パスワードタイプ 6 への自動変換は、Cisco IOS XE Gibraltar 16.11.1 以降のリリースでサポートされています。
 - タイプ 6 のユーザー名とパスワードには Cisco IOS XE Gibraltar 16.10.x と下位互換性があります。Cisco IOS XE Gibraltar 16.10.1 より前のリリース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、管理者ログイン（管理アクセス）に使用されるパスワードを不可逆的なパスワードタイプに手動で移行します。

パスワードおよび権限によるスイッチアクセスの設定方法

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

	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。
ステップ 3	enable password <i>password</i> 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> 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

	コマンドまたはアクション	目的
		<p>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。</p> <ol style="list-style-type: none"> abc を入力します。 Ctrl+v を入力します。 ?123 を入力します。 <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	end 例 : 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。

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

	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"> • enable password [level <i>level</i>] {<i>unencrypted-password</i> <i>encryption-type encrypted-password</i>} • enable secret [level <i>level</i>] {<i>unencrypted-password</i> <i>encryption-type encrypted-password</i>} <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"> • 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。 • 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"> • (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。これは、Cisco IOS XE Gibraltar 16.10.1 以降のリリースで適用されます。 • 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 scrypt 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 scrypt secret cisco</pre> または

	コマンドまたはアクション	目的
		<pre>Device (config) # enable algorithm-type script secret cisco</pre> <p>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。</p>
ステップ 4	service password-encryption 例 : <pre>Device (config) # service password-encryption</pre>	<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>
ステップ 5	end 例 : <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

	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。
ステップ 3	system disable password recovery switch {all <1-9>} 例： Device (config)# system disable password recovery switch all	パスワード回復をディセーブルにします。 <ul style="list-style-type: none"> • <i>all</i> : スタック内のスイッチで設定を行います。 • <1-9> : 選択したスイッチ番号で設定を行います。 <p>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。</p>
ステップ 4	end 例： 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。

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

	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。
ステップ 3	line vty 0 98 例： Device(config)# line vty 0 98	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 99 のセッションが可能です。0 および 98 は、可能なすべての 99 Telnet セッションを設定していることを意味します。
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> 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。
ステップ 5	end 例： Device(config-line)# end	特権 EXEC モードに戻ります。

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。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	configure terminal 例： Device# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 3	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"> • <i>name</i> 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。 • 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。 • (任意) <i>level</i> 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。 • <i>encryption-type</i> に、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。非表示パスワードが後ろに続く場合は 7 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 6 を入力します。 • <i>password</i> には、デバイスにアクセスするためにユーザーが入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め

	コマンドまたはアクション	目的
		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 • line vty 0 98 例： Device(config)# line console 0 または Device(config)# line vty 0 98	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0～98）を設定します。
ステップ 5	end 例： Device(config-line)# end	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

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

	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。
ステップ 3	privilege mode level level command 例： Device(config)# privilege exec level 14 configure	コマンドの特権レベルを設定します。 <ul style="list-style-type: none"> • <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 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

	コマンドまたはアクション	目的
		<p>ギョレーションモードの場合は line をそれぞれ入力します。</p> <ul style="list-style-type: none"> • <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、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> には、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	<p>enable password level level password</p> <p>例 :</p> <pre>Device(config)# enable password level 14 SecretPswd14</pre>	<p>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。</p> <ul style="list-style-type: none"> • <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。 • <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。
ステップ 5	<p>end</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>

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

	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>

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例： Device# <code>configure terminal</code>	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)# <code>line vty 10</code>	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	privilege exec level level 例： Device(config-line)# <code>privilege exec level 15</code>	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 が通常のユーザー 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-line)# <code>end</code>	回線コンフィギュレーション モードを終了します。続いて、特権 EXEC モードに戻ります。

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、ユーザー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

	コマンドまたはアクション	目的
ステップ 1	enable level 例：	指定された特権レベルにログインします。

	コマンドまたはアクション	目的
	Device> enable 15	この例では、レベル 15 は特権 EXEC モードです。 level に指定できる範囲は 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。 この例では、レベル 1 はユーザー EXEC モードです。 level に指定できる範囲は 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。

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、Old key、New key、Confirm key という 3つのプロンプトが表示されます。 • 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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> 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によるスイッチアクセスのモニター

表 2: 特権レベル情報を表示するためのコマンド

コマンド	情報
show privilege	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によるスイッチアクセスの設定例

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）。

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

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 `9sMLBsTFXLnnHTk$0L82` を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret level 2 9 $9$sMLBsTFXLnnHTk$0L82
Device(config)# end
```

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
Device(config-line)# end
```

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)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
Device(config)# end
```

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
```

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、導入されたり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 XE Everest 16.5.1a	パスワードおよび権限によるスイッチ 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 IOS XE Gibraltar 16.11.1	タイプ0およびタイプ7のユーザー名とパスワードのタイプ6への自動変換	このリリース以降は、タイプ0および7のユーザー名とパスワードをタイプ6に自動変換できます。

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。

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。