traffic-export から zone security まで

username

ユーザ名に基づいた認証システムを確立するには、グローバル コンフィギュレーション モードで **username** コマンドを使用します。 確立されたユーザ名ベースの認証を削除するには、このコマンドの **no** 形式を使用します。

username *name* [**aaa attribute list** *aaa-list-name*]

username *name* [**access-class** *access-list-number*]

username *name* [**autocommand** *command*]

username *name* [**callback-dialstring** *telephone-number*]

username *name* [**callback-line [tty]** *line-number* [*ending-line-number*]]

username *name* [**callback-rotary** *rotary-group-number*]

username *name* **[dnis]**

username *name* **[mac]**

username *name* **[nocallback-verify]**

username *name* **[noescape]**

username *name* **[nohangup]**

username *name* [**nopassword**| **password** *password*| **password** *encryption-type encrypted-password*]

username *name* [**one-time** {**password** {**0**| **7**| *password*}| **secret** {**0**| **5**| *password*}}]

username *name* [**password** *secret*]

username *name* [**privilege** *level*]

username *name* [**secret** {**0**| **5**| *password*}]

username *name* [**user-maxlinks** *number*]

username [lawful-intercept] *name* [**privilege** *privilege-level*| **view** *view-name*] **password** *password*

no username *name*

構文の説明

name	ホスト名、サーバ名、ユーザ ID、またはコマンド名。 *name* 引数には 1 つの単語だけ使用できます。 空白や二重引用符は使用できません。
aaa attribute list *aaa-list-name*	指定された認証、許可、アカウンティング（AAA）メソッド リストを使用します。
access-class *access-list-number*	（任意）ライン コンフィギュレーション モードで使用可能な **access-class** コマンドで指定されたアクセス リストを上書きする発信アクセス リストを指定します。 これはユーザ セッション中に使用されます。

autocommand *command*	（任意）ユーザがログインした後に、自動的に指定されたコマンドが発行されるようにします。 コマンドが完了すると、セッションが終了します。 コマンドの長さは任意で、埋め込みスペースが含まれる可能性があるため、**autocommand** キーワードを使用したコマンドは、行の最後のオプションである必要があります。
callback-dialstring *telephone-number*	（任意）非同期コールバックの場合のみ：DCE デバイスに渡すための電話番号を指定できます。
callback-line *line-number*	（任意）非同期コールバックの場合のみ：コールバック用の特定のユーザ名をイネーブルにする、端末回線（または連続したグループの最初の行）の相対番号。 番号付けはゼロから始まります。
ending-line-number	（任意）コールバック用の特定のユーザ名をイネーブルにする、連続したグループの最後の行の相対番号。 キーワード（**tty** など）を省略すると、line-number および ending-line-number は相対ではなく絶対回線番号になります。
tty	（任意）非同期コールバックの場合のみ：標準非同期回線。
callback-rotary *rotary-group-number*	（任意）非同期コールバックの場合のみ：コールバック用に特定のユーザ名をイネーブルにする、ロータリーグループ番号を指定できます。 ロータリーグループの次の使用可能な回線が選択されます。 範囲は 1 ～ 100 です。
dnis	着信番号識別サービス（DNIS）経由で取得されると、パスワードは必要ではありません。
mac	MAC アドレスが、ローカルで実行される MAC フィルタリング用のユーザ名として使用できるようになります。
nocallback-verify	（任意）指定された回線上の EXEC コールバックで、認証が必要ないことを指定します。

noescape	（任意）ユーザが接続しているホストで、そのユーザがエスケープ文字を使用することを防ぎます。
nohangup	（任意）自動コマンド（**autocommand** キーワードで設定）が完了した後に、Cisco IOS ソフトウェアがユーザを切断することを防ぎます。代わりに、ユーザは別の EXEC プロンプトを受け取ります。
nopassword	このユーザがログインするためにパスワードは必要はありません。これは通常、**autocommand** キーワードと組み合わせて使用するには最も有用なキーワードです。
password	パスワードが *name* 引数にアクセスするように指定します。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。
password	ユーザが入力するパスワード。
encryption-type	（任意）直後に続くテキストを暗号化するかどうかと、暗号化する場合は使用する暗号化の種類を定義する 1 桁の数字。定義されている暗号化タイプは、後続するテキストは暗号化されない 0 と、テキストがシスコにより定義された暗号化アルゴリズムを使用して暗号化される 7 です。
encrypted-password	ユーザが入力する暗号化パスワード。
one-time	ユーザ名とパスワードは 1 回だけ有効であることを指定します。この設定は、デフォルトのクレデンシャルがユーザ設定に残ることを防ぐために使用されます。
0	非暗号化パスワードまたは秘密キー（設定に依存）が続くことを指定します。
7	非表示のパスワードが続くことを指定します。
5	非表示の秘密が続くことを指定します。
secret	ユーザの秘密を指定します。

secret	チャレンジ ハンドシェイク認証プロトコル（CHAP）認証の場合、ローカル ルータまたはリモート デバイスの秘密を指定します。 秘密はローカル ルータに保存するときに暗号化されます。 秘密は、11 文字までの任意の ASCII 文字の文字列で構成されます。 指定可能なユーザ名とパスワードの組み合わせに制限はないため、認証できるリモート デバイスの数は任意です。
privilege *privilege-level*	（任意）ユーザの特権レベルを設定します。 有効な範囲は、1 ～ 15 です。
user-maxlinks *number*	ユーザに許可されるインバウンド リンクの最大数。
lawful-intercept	（任意）シスコ デバイス上で合法的傍受ユーザを設定します。
name	ホスト名、サーバ名、ユーザ ID、またはコマンド名。 *name* 引数には 1 つの単語だけ使用できます。 空白や二重引用符は使用できません。
view *view-name*	（任意）CLI ビューの場合のみ：**parser view** コマンドで指定されたローカル AAA データベースと CLI ビュー名を関連付けます。
password *password*	CLI ビューにアクセスするためのパスワード。

コマンド デフォルト

ユーザ名に基づく認証システムは確立されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。

リリース	変更内容
11.1	このコマンドが変更されました。 次のキーワードと引数が追加されました。 • **callback-dialstring** *telephone-number* • **callback-rotary** *rotary-group-number* • **callback-line** [**tty**] *line-number* [*ending-line-number* • **nocallback-verify**
12.3(7)T	このコマンドが変更されました。 次のキーワードと引数が追加されました。 • **lawful-intercept** • **view** • *view-name*
12.2(33)SRB	このコマンドが変更されました。 次のキーワードと引数が、Cisco IOS Release 12.2(33)SRB に統合されました。 • **lawful-intercept** • **view** • *view-name*
12.2(33)SB	このコマンドが変更されました。 次のキーワードと引数が、Cisco IOS Release 12.2(33)SB に統合されました。 • **lawful-intercept** • **view** • *view-name*
Cisco IOS XE Release 2.1	このコマンドが、Cisco IOS XE Release 2.1 に統合されました。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
12.4	このコマンドが変更されました。 次のキーワードが、Cisco IOS Release 12.4 に統合されました。 • **one-time** • **secret** • **0**、**5**、**7**

リリース	変更内容
15.1(1)S	このコマンドが変更されました。 **nohangup** キーワードのサポートがセキュア シェル（SSH）から除外されました。
Cisco IOS XE Release 3.2SE	このコマンドが変更されました。 **mac** キーワードが追加されました。

使用上のガイドライン

username コマンドは、ユーザ名認証またはパスワード認証（またはその両方）をログインの目的のみで指定します。

複数の **username** コマンドを、単一のユーザに対するオプションを指定するために使用できます。

ローカル ルータが通信し、認証を要求する各リモート システムにユーザ名エントリを追加します。 リモート デバイスは、ローカル ルータに対してユーザ名エントリを持っている必要があります。 このエントリは、そのリモート デバイスに対するローカル ルータのエントリと同じパスワードを持っている必要があります。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。 たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する「info」ユーザ名を定義できます。

username コマンドは、CHAP の設定の一部として必要です。 ローカル ルータが認証を要求する各リモート システムにユーザ名エントリを追加します。

（注） リモート CHAP チャレンジに対するローカル ルータの応答をイネーブルにするには、1 つの **username** *name* エントリは、別のルータに割り当て済みの **hostname** エントリと同じである必要があります。

- 特権レベル 1 のユーザがより上位の権限レベルを開始する状況を避けるために、1 以外でユーザ単位の特権レベルを設定します（たとえば、0 または 2 ～ 15）。
- ユーザ単位の特権レベルは、仮想端末の特権レベルよりも優先されます。

Cisco IOS Release 15.1(1)S 以降のリリースでは、 **nohangup** キーワードは、SSH ではサポートされません。 **username** *user* **autocommand** *command-name* コマンドが設定されており、SSH が使用されている場合は、設定されているコマンドが実行された後にセッションが切断されます。 SSH のこの動作は Telnet の動作とは逆で、Telnet の動作では、ユーザが Telnet を終了するまで Telnet は継続的に認証を要求し、コマンドを実行し続けます。

CLI および合法的傍受ビュー

CLI ビューおよび合法的傍受ビューの両方とも、特定のコマンドと設定情報へのアクセスを制限します。 合法的傍受ビューを使用すれば、ユーザは、コールとユーザに関する情報を保存する簡易ネットワーク管理プロトコル（SNMP）コマンドの特別なセットである TAP-MIB 内に保持された合法的傍受コマンドへのアクセスを保護できます。

lawful-intercept キーワードを使用して指定されたユーザは、別の特権レベルまたはビュー名が明示的に指定されていない場合、デフォルトで合法的傍受ビューに配置されます。

secret 引数に値が指定されておらず **debug serial-interface** コマンドがイネーブルの場合、リンクが確立されたときにエラーが表示され、CHAP チャレンジは実行されません。 CHAP デバッグ情報は、**debug ppp negotiation**、**debug serial-interface**、および**debug serial-packet** コマンドを使用することで利用できます。 **debug** コマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

例

次に、ログイン プロンプトで入力し、ルータの現在のユーザをリストする UNIX の **who** コマンドに似たサービスを実装する例を示します。

```
username who nopassword nohangup autocommand show users
```

次に、パスワードを使用する必要のない情報サービスを実装する例を示します。 コマンドは次の形式になります。

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

次に、すべての TACACS+ サーバで障害が発生しても機能する ID を実装する例を示します。 コマンドは次の形式になります。

```
username superuser password superpassword
```

次に、「server_1」のインターフェイス シリアル 0 で CHAP をイネーブルにする例を示します。また、「server_r」という名前のリモート サーバのパスワードも定義します。

```
hostname server_1
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次に、暗号化されたパスワードを表示した **show running-config** コマンドの出力を示します。

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

次の例では、特権レベル 1 ユーザが、1 よりも高い特権レベルへのアクセスを拒否されています。

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

次に、user2 に対するユーザ名ベースの認証を削除する例を示します。

```
no username user2
```

関連コマンド

コマンド	説明
arap callback	ARA クライアントが ARA クライアントからのコールバックを要求できるようにします。

コマンド	説明
callback forced-wait	Cisco IOS ソフトウェアが、要求元クライアントに対するコールバックを開始する前に待機するように強制します。
debug ppp negotiation	PPP の始動時に、PPP オプションをネゴシエートするために送信された PPP パケットを表示します。
debug serial-interface	シリアル接続障害に関する情報を表示します。
debug serial-packet	**debug serial interface** コマンドを使用して取得したものよりも詳細なシリアルインターフェイスのデバッグ情報を表示します。
ppp callback（**DDR**）	DTR インターフェイスではないダイヤラ インターフェイスが、コールバックを要求するクライアントとして、またはコールバック要求を受け入れるコールバック サーバとして機能できるようにします。
ppp callback（**PPP クライアント**）	PPP クライアントが非同期インターフェイスにダイヤルインして、コールバックを要求できるようにします。
show users	ルータのアクティブ回線に関する情報を表示します。

username secret

不可逆的な暗号化を使用してユーザパスワードを暗号化するには、グローバル コンフィギュレーション モードで **username secret** コマンドを使用します。

username *name* **secret** {**0** *password*| **5** *secret-string*| **4** *secret-string*}

構文の説明

name	ユーザ名。
0	非暗号化シークレットを指定します。
password	クリアテキスト パスワード。
5 *secret-string*	暗号化されたユーザ パスワードとして保存される、メッセージ ダイジェスト アルゴリズム 5（MD5）で暗号化された秘密テキスト ストリング。
4 *secret-string*	暗号化されたユーザ パスワードとして保存される、SHA256 で暗号化された秘密テキスト ストリング。

コマンド デフォルト

ユーザ名に基づく認証システムは確立されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
12.0(18)S	このコマンドが導入されました。
12.1(8a)E	このコマンドが Cisco IOS Release 12.1(8a)E に統合されました。
12.2(8)T	このコマンドが Cisco IOS Release 12.2(8)T に統合されました。
12.2(14)SX	このコマンドのサポートが Supervisor Engine 720 に追加されました。
12.2(17d)SXB	Supervisor Engine 2 上のこのコマンドのサポートが Cisco IOS Release 12.2(17d)SXB に拡張されました。

リリース	変更内容
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。
15.0(1)S	このコマンドが Cisco IOS Release 15.0(1)S に統合されました。 暗号化タイプ **0**、**4**、および **5** が追加されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

username secret コマンドを使用して、ユーザ名および MD5 で暗号化されたユーザ パスワードを設定します。 MD5 暗号化は、取得不可能な強力な暗号化方式です。したがって、チャレンジ ハンドシェイク認証プロトコル（CHAP）などのクリアテキスト パスワードを必要とするプロトコルでは MD5 暗号化を使用できません。

username secret コマンドは、ユーザ名パスワードに追加のセキュリティ レイヤを提供します。 また、不可逆的な MD5 暗号化を使用してパスワードを暗号化し、暗号化されたテキストを保存することにより、さらにセキュリティが向上します。 追加された MD5 暗号化のレイヤは、パスワードがネットワークを越える、または TFTP サーバに格納される環境で便利です。

ルータ コンフィギュレーション ファイルからコピーした暗号化パスワードをこのコマンドに貼り付ける場合は、暗号化タイプとして MD5 を使用します。

このコマンドを使用すると、指定された取得不可能なユーザ名に対して拡張パスワード セキュリティがイネーブルになります。 このコマンドは、パスワードの MD5 カプセル化をイネーブルにします。 MD5 暗号化は強力な暗号化方式です。 CHAP などのクリアテキスト パスワードを必要とするプロトコルと MD5 との併用はできません。

このコマンドは、特殊な取り扱いが必要なユーザ名を定義する場合に便利です。 たとえば、このコマンドを使用すると、パスワードが不要で、ユーザを汎用の情報サービスに接続する「info」ユーザ名を定義できます。

username コマンドは、ログインだけを目的としてユーザ名または秘密の認証を行います。 *name* 引数に指定できるのは、1 ワードだけです。 スペースと引用符は使用できません。 複数の **username** コマンドを使用して、単一ユーザのオプションを指定できます。

例

次に、ユーザ名「abc」を設定し、クリアテキスト パスワード「xyz」で MD5 暗号化をイネーブルにする例を示します。

```
username abc secret 0 xyz
```

次に、ユーザ名「cde」を設定し、ユーザ名のパスワードとして保存される MD5 暗号化テキスト ストリングを入力する例を示します。

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

次に、ユーザ名「xyz」を設定し、ユーザ名のパスワードとして保存される MD5 暗号化テキストストリングを入力する例を示します。

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
enable secret	enable password コマンドよりも強化したセキュリティ レイヤを指定します。
username	ユーザ名をベースとした認証システムを構築します。