CHAPTER 11

スイッチベース認証の設定

この章では、IE 3000 スイッチでのスイッチベース認証の設定方法について説明します。この章で説明する内容は、次のとおりです。

スイッチへの不正アクセスの防止

認可されていないユーザがスイッチの設定を変更したり、設定情報を表示したりすることを防止できます。通常、ネットワーク管理者にはスイッチへのアクセスを認可し、非同期ポートを通してネットワークの外部からダイヤルしてくるユーザ、シリアル ポートを通してネットワークの外部から接続してくるユーザ、またはローカル 端末またはワークステーションを通してネットワーク内から接続してくるユーザのアクセスは制限します。

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 つ以上設定する必要があります。

- 少なくとも、スイッチのポートごとにパスワードと権限を設定する必要があります。これらのパスワードは、スイッチにローカルに保存されます。ポートまたは回線を通してスイッチにアクセスしようとするユーザは、スイッチにアクセスする前に、そのポートまたは回線に対して指定されているパスワードを入力する必要があります。詳細については、「特権 EXEC コマンドへのアクセス保護」（P.11-2）を参照してください。
- セキュリティのレイヤを追加するには、ユーザ名とパスワードのペアを設定することもできます。この設定はスイッチにローカルに保存されます。これらのペアは回線またはポートに割り当てられ、各ユーザがスイッチにアクセスする前に、ユーザを認証します。権限レベルを定義してある場合は、ユーザ名とパスワードのペアごとに特定の権限レベル（および関連付けられている権利と権限）を割り当てることもできます。詳細については、「ユーザ名とパスワードのペアの設定」（P.11-6）を参照してください。

- ユーザ名とパスワードのペアを使用し、ローカルに保存するのではなくサーバに一元的に保存したい場合は、セキュリティ サーバのデータベースに保存できます。このようにすると、複数のネットワーキング装置が同じデータベースを使用して、ユーザ認証（および必要に応じて認可）の情報を取得できます。詳細については、「TACACS+ でのスイッチ アクセスの制御」（P.11-10）を参照してください。
- また、ログイン拡張機能をイネーブルにすることもできます。この機能は、失敗したログインの試行と成功しなかったログインの試行の両方をログに記録します。ログイン拡張機能は、一定の回数だけログインの試行が失敗したら、それ以降のログインの試行をブロックするように設定することもできます。詳細については、次の URL の『Cisco IOS Login Enhancements』ドキュメントを参照してください。
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html

特権 EXEC コマンドへのアクセス保護

ネットワーク内の端末アクセスを制御する簡単な方法に、パスワードを使用し、権限レベルを割り当てる方法があります。パスワード保護は、ネットワークまたはネットワーク装置へのアクセスを制限します。権限レベルは、ユーザがネットワーク装置にログインしたあとで入力できるコマンドを定義します。

（注）　この項で使用するコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

パスワードと権限レベルのデフォルト設定

表 11-1 に、パスワードと権限レベルのデフォルト設定を示します。

表 11-1　デフォルトのパスワードと権限レベル

機能	デフォルト設定
パスワードと権限レベルをイネーブルにする	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（特権 EXEC レベル）です。コンフィギュレーション ファイルではパスワードは暗号化されません。
シークレット パスワードと権限レベルをイネーブルにする	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（特権 EXEC レベル）です。パスワードはコンフィギュレーション ファイルに書き込まれる前に暗号化されます。
回線パスワード	パスワードは定義されていません。

スタティック イネーブル 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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**enable password** *password*	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ていません。 *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは使用できますが先行スペースは無視されます。パスワードを作成するとき、Crtl+v 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、次のようにします。 **abc** と入力します。 Crtl+v を押します。 **?123** と入力します。 システムでイネーブル パスワードの入力を求められたときは、疑問符の前に Ctrl+v を押す必要はなく、パスワード プロンプトで単に abc?123 と入力できます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。 イネーブル パスワードは暗号化されず、スイッチのコンフィギュレーション ファイルで読むことができます。

パスワードを削除するには、**no enable password** グローバル コンフィギュレーション コマンドを使用します。

次に、イネーブル パスワードを *l1u2c3k4y5* に変更する例を示します。パスワードは暗号化されず、レベル 15（従来の特権 EXEC モード アクセス）へのアクセスを提供します。

```
Switch(config)# enable password l1u2c3k4y5
```

イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化による保護

ネットワークで送受信されるパスワードまたは Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）サーバに保存されるパスワードについて、セキュリティをさらに強化するには、**enable password** または **enable 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。どちらのコマンドも同じことを行います。つまり、ユーザが特権 EXEC モード（デフォルト）または指定されている権限レベルにアクセスするために入力する必要がある暗号化されたパスワードを設定できます。

enable secret コマンドは改善された暗号化アルゴリズムを使用するので、こちらの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 つのコマンドをイネーブルにすることはできません。

イネーブル パスワードおよびイネーブル シークレット パスワードの暗号化を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted*-password}	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。
	または	または
	enable secret [**level** *level*] {*password* | *encryption-type encrypted*-password}	不可逆的な暗号化方式を使用して保存される、シークレット パスワードを定義します。 • （任意）*level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。デフォルトのレベルは 15（特権 EXEC モード権限）です。 • *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは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ていません。 • （任意）*encryption-type* には、シスコ独自の暗号化アルゴリズムを示すタイプ 5 だけを指定できます。暗号化タイプを指定する場合は、暗号化パスワード（別のスイッチの設定からコピーした暗号化パスワード）を指定する必要があります。 **（注）** 暗号化タイプを指定してから、クリア テキストのパスワードを入力すると、特権 EXEC モードを再び開始することができなくなります。暗号化パスワードを忘れた場合は、どのような方法でも回復できません。
ステップ 3	**service password-encryption**	（任意）パスワードを定義するとき、または設定を書き込むときに、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 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

イネーブル パスワードとイネーブル シークレット パスワードの両方が定義されている場合は、ユーザはイネーブル シークレット パスワードを入力する必要があります。

特定の権限レベルに対するパスワードを定義するには、**level** キーワードを使用します。レベルを指定してパスワードを設定したあと、権限レベルにアクセスする必要があるユーザだけに、パスワードを通知してください。各レベルでアクセスできるコマンドを指定するには、**privilege level** 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。詳細については、「複数の権限レベルの設定」（P.11-7）を参照してください。

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。

パスワードとレベルを削除するには、**no enable password** [**level** *level*] または **no enable secret** [**level** *level*] のいずれかのグローバル コンフィギュレーション コマンドを使用します。パスワードの暗号化をディセーブルにするには、**no service password-encryption** 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。

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。

```
Switch(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

パスワード回復のディセーブル化

デフォルトでは、スイッチに物理的にアクセスできるエンド ユーザは、スイッチの電源投入時に起動プロセスを中断して新しいパスワードを入力することにより、パスワードを失った状態から回復できます。

パスワード回復ディセーブル機能は、この機能の一部をディセーブルにすることで、スイッチのパスワードへのアクセスを保護します。この機能をイネーブルにすると、エンド ユーザは、システムをデフォルトの設定に戻すことに同意した場合にだけ、起動プロセスを中断できます。パスワード回復をディセーブルにすることにより、ユーザは起動プロセスを中断して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）と VLAN データベース ファイル（vlan.dat）は削除されます。

（注） パスワード回復をディセーブルにする場合は、エンド ユーザが起動プロセスを中断してシステムの設定をデフォルト値に戻す場合に備えて、コンフィギュレーション ファイルのバックアップ コピーをセキュア サーバに保存することを推奨します。スイッチには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。スイッチが VTP トランスペアレント モードで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 コピーもセキュア サーバに保存することを推奨します。スイッチがデフォルトのシステム設定に戻されたときは、Xmodem プロトコルを使用して、保存されているファイルをスイッチにダウンロードできます。詳細については、「パスワードを忘れた場合の回復」（P.52-3）を参照してください。

パスワード回復をディセーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**no service password-recovery**	パスワード回復をディセーブルにします。 この設定はフラッシュ メモリ内のブート 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、この領域はファイル システムの一部ではないので、ユーザはアクセスできません。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show version**	コマンド出力の最後の数行を調べて、設定を確認します。

パスワード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。

（注） **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、パスワード回復のディセーブル化はできません。このコマンドを実行すると、スイッチの電源をオフ/オンしたあとで、ブート ローダのプロンプト（*switch:*）が表示されます。

端末回線への Telnet パスワードの設定

スイッチの電源を初めて入れると、自動セットアップ プログラムが実行して、IP 情報を割り当て、継続的な使用のためのデフォルト設定を作成します。セットアップ プログラムでは、パスワードを使用して Telnet にアクセスするようにスイッチを設定することも求められます。セットアップ プログラムでこのパスワードを設定しなかった場合は、CLI（コマンドライン インターフェイス）を使用して設定できます。

Telnet アクセス用にスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1		エミュレーション ソフトウェアがインストールされている PC またはワークステーションを、スイッチのコンソール 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、8、1、パリティなしです。コマンドライン プロンプトを表示するため、Return キーを数回押す必要がある場合があります。
ステップ 2	**enable password** *password*	特権 EXEC モードを開始します。
ステップ 3	**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 4	**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。 コマンド対応スイッチで使用できるセッションの数は 16 です。0 および 15 は、使用可能な 16 の Telnet セッションをすべて設定することを意味します。
ステップ 5	**password** *password*	回線の Telnet パスワードを入力します。 *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは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ていません。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。 パスワードが **line vty 0 15** コマンドの下に表示されます。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

パスワードを削除するには、**no password** グローバル コンフィギュレーション コマンドを使用します。

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

```
Switch(config)# line vty 10
Switch(config-line)# password let45me67in89
```

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できます。この設定はスイッチにローカルに保存されます。これらのペアは回線またはポートに割り当てられ、各ユーザがスイッチにアクセスする前に、ユーザを認証します。権限レベルを定義してある場合は、ユーザ名とパスワードのペアごとに特定の権限レベル（および関連付けられている権利と権限）を割り当てることもできます。

ログイン ユーザ名とパスワードを要求するユーザ名ベースの認証システムを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ユーザごとにユーザ名、権限レベル、およびパスワードを入力します。 • *name* には、ユーザ ID として 1 語を指定します。スペースおよび引用符は使用できません。 • （任意）*level* には、ユーザがアクセスしたあとで割り当てられ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 は特権 EXEC モード アクセスです。レベル 1 はユーザ EXEC モード アクセスです。 • *encryption-type* には、暗号化されていないパスワードが後ろに続くことを指定する場合は 0 を入力します。非表示パスワードが後ろに続くことを指定する場合は 7 を入力します。 • *password* には、スイッチにアクセスするためにユーザ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 文字でなければならず、間にスペースを含むことができ、**username** コマンドで最後に指定するオプションである必要があります。
ステップ 3	**line console 0** または **line vty 0 15**	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。
ステップ 4	**login local**	ログイン時のローカル パスワード検査をイネーブルにします。認証は、ステップ 2 で指定したユーザ名に基づきます。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show running-config**	設定を確認します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

特定のユーザのユーザ名認証をディセーブルにするには、**no username** *name* 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。パスワード検査をディセーブルにし、パスワードを入力しないで接続できるようにするには、**no login** ライン コンフィギュレーション コマンドを使用します。

複数の権限レベルの設定

Cisco IOS ソフトウェアには、パスワード セキュリティのモードがデフォルトで 2 つあります。ユーザ EXEC モードと特権 EXEC モードです。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することができます。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。

たとえば、多くのユーザが **clear line** コマンドにアクセスできるようにするには、このコマンドにレベル 2 セキュリティを割り当て、レベル 2 パスワードを幅広く配布します。一方、**configure** コマンドにアクセスできるユーザを限定したい場合には、このコマンドにレベル 3 セキュリティを割り当て、限られたユーザ グループだけにパスワードを配布します。

ここでは、次の設定情報について説明します。

コマンドの権限レベルの設定

コマンド モードの権限レベルを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**privilege** *mode* **level** *level command*	コマンドの権限レベルを設定します。 • *mode* 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**、EXEC モードの場合は **exec**、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**、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。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって認可されるアクセスのレベルです。 • *command* には、アクセスを制限するコマンドを指定します。
ステップ 3	**enable password level** *level password*	権限レベルに対するイネーブル パスワードを指定します。 • *level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。 • *password* には、1 ～ 25 文字の英数字からなる文字列を指定します。先頭を数字にすることはできず、大文字と小文字の区別があり、スペースは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ていません。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	設定を確認します。 最初のコマンドは、パスワードおよびアクセス レベルの設定を表示します。2 番めのコマンドは、権限レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

コマンドを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すべてのコマンドも、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 に設定した場合、**show** コマンドや **show ip** コマンドも、別のレベルに個別に設定しない限り、権限レベル 15 に自動的に設定されます。

特定のコマンドをデフォルトの権限に戻すには、**no privilege** *mode* **level** *level command* 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。

次に、**configure** コマンドを権限レベル 14 に設定し、レベル 14 のコマンドを使用するためにユーザが入力する必要があるパスワードとして *SecretPswd14* を定義する例を示します。

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

回線のデフォルト権限レベルの変更

回線のデフォルトの権限レベルを変更するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**line vty** *line*	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 3	**privilege level** *level*	回線のデフォルトの権限レベルを変更します。 *level* に指定できる範囲は 0 ～ 15 です。レベル 1 は通常のユーザ EXEC モード権限です。レベル 15 は、**enable** パスワードによって認可されるアクセスのレベルです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** または **show privilege**	設定を確認します。 最初のコマンドは、パスワードおよびアクセス レベルの設定を表示します。2 番めのコマンドは、権限レベルの設定を表示します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ユーザは、回線にログインして別の権限レベルをイネーブルにすることで、**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した権限レベルを上書きできます。**disable** コマンドを使用すると、権限レベルを下げることができます。ユーザが高い権限レベルのパスワードを知っている場合は、そのパスワードを使用して、より高い権限レベルをイネーブルにできます。コンソール回線で回線の使用を制限するために、高レベルまたは権限レベルを指定する場合があります。

デフォルトの回線権限レベルに戻すには、**no privilege level** ライン コンフィギュレーション コマンドを使用します。

権限レベルへのログインと終了

指定した権限レベルにログインしたり、指定した権限レベルを終了したりするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**enable** *level*	指定した権限レベルにログインします。 *level* に指定できる範囲は 0 ～ 15 です。
ステップ 2	**disable** *level*	指定した権限レベルを終了します。 *level* に指定できる範囲は 0 ～ 15 です。

TACACS+ でのスイッチ アクセスの制御

ここでは、Terminal Access Controller Access Control System Plus（TACACS+）をイネーブルにして設定する方法を説明します。TACACS+ は詳細なアカウント情報を提供し、認証と認可のプロセスの管理を柔軟に制御できます。TACACS+ は、Authentication、Authorization、Accounting（AAA; 認証、認可、アカウンティング）によって促進され、AAA コマンドによってだけイネーブルにすることができます。

（注）　この項で使用しているコマンドの構文および使用方法の詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

- 「TACACS+ の概要」（P.11-10）
- 「TACACS+ の動作」（P.11-12）
- 「TACACS+ の設定」（P.11-12）
- 「TACACS+ の設定の表示」（P.11-17）

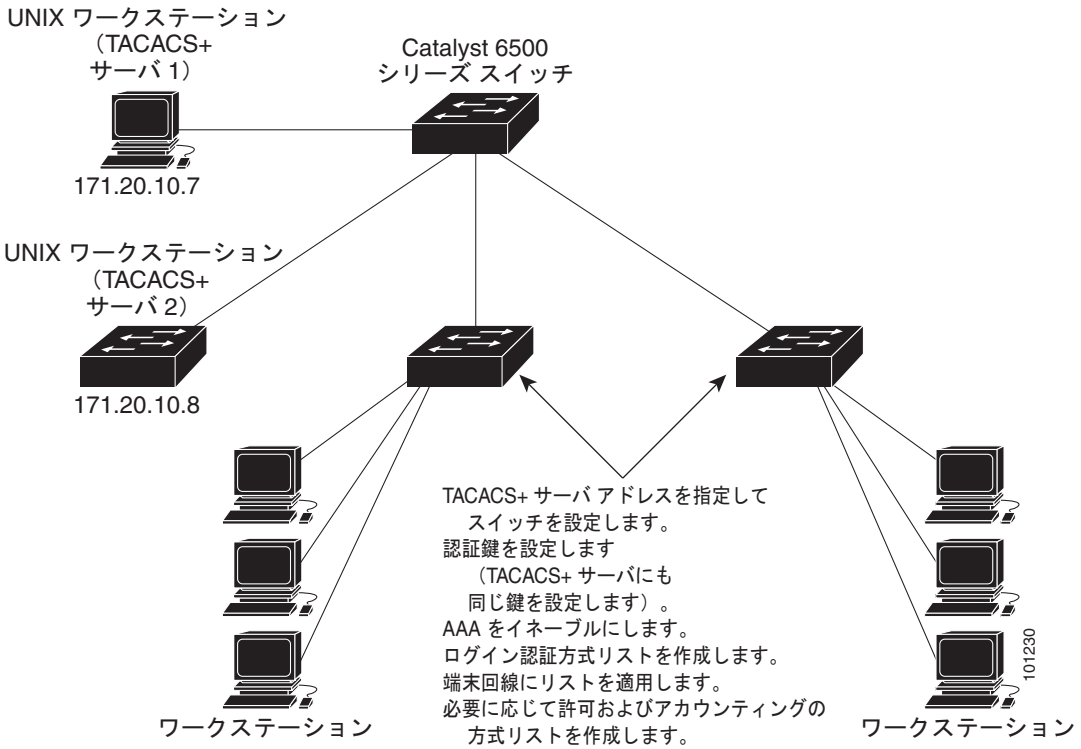
TACACS+ の概要

TACACS+ は、スイッチにアクセスを試みるユーザの検証を一元的に行うセキュリティ アプリケーションです。TACACS+ サービスは TACACS+ デーモンのデータベースで維持され、デーモンは通常は UNIX または Windows NT のワークステーション上で実行します。スイッチで TACACS+ の機能を設定するには、TACACS+ サーバにアクセスし、TACACS+ サーバを設定しておく必要があります。

TACACS+ は、独立したモジュール形式の認証、認可、アカウンティングの機能を備えています。TACACS+ では、単一のアクセス制御サーバ（TACACS+ デーモン）で、認証、認可、アカウンティングの各サービスを個別に提供できます。各サービスは専用のデータベースに結びつけられており、デーモンの機能に応じて、同じサーバ上またはネットワーク上で使用可能な他のサービスを利用できます。

TACACS+ の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理するための手段を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともに、ネットワーク アクセス サーバとして機能することができます。ネットワーク アクセス サーバは、図 11-1 で示すように、個別のユーザ、ネットワークまたはサブネットワーク、および相互接続されたネットワークへの接続を提供します。

図 11-1　一般的な TACACS+ ネットワークの設定



AAA セキュリティ サービスによって管理された TACACS+ は、次のサービスを提供できます。

- 認証：ログインおよびパスワード ダイアログ、チャレンジ アンド レスポンス、およびメッセージング サポートを通して、認証の完全な制御を提供します。

  認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードを提供されたあとで、自宅の住所、母親の旧姓、サービスのタイプ、社会保障番号などの質問で、ユーザの身元を確認できます）。TACACS+ の認証サービスは、ユーザの画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期限ポリシーのためにパスワードを変更する必要があることを、メッセージでユーザに通知できます。

- 認可：自動コマンド、アクセス制御、セッション期間、プロトコル サポートなどの設定をはじめとする、ユーザのセッションの間のさまざまなユーザ機能を、きめ細かく制御できます。また、ユーザが実行できるコマンドを TACACS+ の認可機能で制限することもできます。

- アカウンティング：課金、監査、レポートに使用する情報を収集し、TACACS+ デーモンに送信できます。ネットワーク マネージャは、アカウンティング機能を使用して、セキュリティ監査のためにユーザのアクティビティを追跡したり、ユーザ課金のための情報を提供したりできます。アカウンティング レコードには、ユーザ ID、開始および終了時刻、実行したコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間の認証を提供します。スイッチと TACACS+ デーモンの間でのプロトコル交換はすべて暗号化されるので、機密性が保証されます。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアを実行するシステムが必要です。

TACACS+ の動作

ユーザが TACACS+ を使用してスイッチの認証を受けることで簡単な ASCII ログインを試みると、次の処理が行われます。

1. 接続が確立されると、スイッチは TACACS+ デーモンと通信し、ユーザに対して表示するユーザ名プロンプトを取得します。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンと通信してパスワード プロンプトを取得します。スイッチがユーザに対してパスワード プロンプトを表示し、ユーザがパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

   デーモンがユーザを認証するために十分な情報を受け取るまで、TACACS+ はデーモンとユーザの間の対話を許可します。デーモンはユーザ名とパスワードの組み合わせの入力を求めますが、ユーザの母親の旧姓のような他の項目を含めることもできます。

2. スイッチは最終的に、次の応答のいずれかを TACACS+ デーモンから受け取ります。

   - ACCEPT：ユーザは認証され、サービスを開始できます。認可を必要とするようにスイッチが設定されている場合は、この時点で認可が開始します。
   - REJECT：ユーザは認証されませんでした。TACACS+ デーモンに応じて、ユーザのアクセスを拒否することも、ログイン シーケンスを再試行するようユーザに求めることもできます。
   - ERROR：デーモンとの認証の間のある時点で、またはデーモンとスイッチの間のネットワーク接続で、エラーが発生しました。ERROR 応答を受け取ったスイッチは、通常、代替方法を使用してユーザの認証を試みます。
   - CONTINUE：ユーザに追加の認証情報の入力を求めます。

   認証のあと、スイッチで認可がイネーブルになっている場合は、ユーザに対して追加の認可フェーズが実行されます。ユーザは、まず TACACS+ による認証が正常に完了してからでないと、TACACS+ による認可に進むことはできません。

3. TACACS+ による認可が必要な場合は、再び TACACS+ デーモンと通信し、認可に対する ACCEPT または REJECT の応答を受け取ります。ACCEPT 応答が返される場合、応答には、そのユーザに対する EXEC または NETWORK セッションを指示する属性、およびユーザがアクセスできるサービスの形式でデータが含まれます。これには、次のものがあります。

   - Telnet、Secure Shell（SSH; セキュア シェル）、rlogin、または特権 EXEC の各サービス
   - ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

TACACS+ の設定

ここでは、TACACS+ をサポートするようにスイッチを設定する方法を説明します。少なくとも、TACACS+ デーモンを維持するホストを識別し、TACACS+ による認証の方式リストを定義する必要があります。必要に応じて、TACACS+ による認可とアカウンティングの方式リストも定義できます。方式リストでは、ユーザの認証、認可、またはアカウントの保持に使用する手順と方式を定義します。方式リストを使用して、使用する 1 つまたは複数のセキュリティ プロトコルを指定でき、これにより、最初の方式が失敗した場合のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用して、ユーザの認証、認可、またはアカウントの保持を行います。その方式が応答しない場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リストの方式による通信が成功するか、方式をすべて試し終わるまで繰り返されます。

ここでは、次の設定情報について説明します。

TACACS+ のデフォルト設定

TACACS+ と AAA はデフォルトではディセーブルになっています。

セキュリティの問題を防ぐため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。イネーブルにすると、TACACS+ は CLI を使用してスイッチにアクセスするユーザを認証できます。

（注）　TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定されている HTTP 接続を認証します。

TACACS+ サーバ ホストの識別と認証キーの設定

単一のサーバまたは AAA サーバ グループを使用して既存のサーバ ホストを認証用にグループ化するように、スイッチを設定できます。サーバをグループ化することで、設定済みサーバ ホストのサブセットを選択し、それを特定のサービスに対して使用できます。サーバ グループは、グローバル サーバ ホスト リストとともに使用され、選択されているサーバ ホストの IP アドレスのリストを含みます。

IP ホストまたは TACACS+ サーバを維持するホストを識別し、必要に応じて暗号キーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	IP ホストまたは TACACS+ サーバを維持するホストを識別します。優先されるホストのリストを作成するには、このコマンドを複数回入力します。ソフトウェアは、ここで指定した順序でホストを検索します。 • *hostname* には、ホストの名前または IP アドレスを指定します。 • （任意）**port** *integer* には、サーバのポート番号を指定します。デフォルト値はポート 49 です。指定できる範囲は 1 ～ 65535 です。 • （任意）**timeout** *integer* には、スイッチが時間切れになってエラーを宣言するまでデーモンからの応答を待機する時間（秒単位）を指定します。デフォルト値は 5 秒です。指定できる範囲は 1 ～ 1000 秒です。 • （任意）**key** *string* には、スイッチと TACACS+ デーモンの間のすべてのトラフィックの暗号化と暗号化解除に使用する暗号キーを指定します。暗号化が成功するためには、TACACS+ デーモンでも同じキーを設定する必要があります。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 4	**aaa group server tacacs+** *group-name*	（任意）グループ名を指定して AAA のサーバ グループを定義します。 このコマンドは、スイッチをサーバ グループ サブコンフィギュレーション モードにします。
ステップ 5	**server** *ip-address*	（任意）特定の TACACS+ サーバと定義したサーバ グループを関連付けます。AAA サーバ グループ内の TACACS+ サーバごとに、このステップを繰り返します。 グループ内の各サーバは、ステップ 2 で先に定義しておく必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show tacacs**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定した TACACS+ サーバ名またはアドレスを削除するには、**no tacacs-server host** *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。コンフィギュレーション リストからサーバ グループを削除するには、**no aaa group server tacacs+** *group-name* 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。TACACS+ サーバの IP アドレスを削除するには、**no server ip-address** サーバ グループ サブコンフィギュレーション コマンドを使用します。

TACACS+ ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義したあと、そのリストをさまざまなポートに適用します。方式リストでは、実行する認証のタイプと、実行する手順を定義します。定義した認証方式を実行するには、特定のポートにリストを適用する必要があります。唯一の例外はデフォルトの方式リストです（名前は *default* です）。方式の名前付きリストが明示的に定義されているポート以外のすべてのポートには、デフォルトの方式リストが自動的に適用されます。定義された方式リストは、デフォルトの方式リストよりも優先されます。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定でき、これにより、最初の方式が失敗した場合の認証のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースがユーザ アクセスを拒否する応答を返した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前を示す文字列を指定します。 • *method1...* には、認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、前の認証方式が失敗した場合ではなく、エラーを返した場合にだけ使用されます。 次のいずれかの方式を選択します。 • **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、**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イネーブル パスワードを定義しておく必要があります。 • **group tacacs+**：TACACS+ による認証を使用します。この認証方式を使用するには、TACACS+ サーバを設定しておく必要があります。詳細については、「TACACS+ サーバ ホストの識別と認証キーの設定」（P.11-13）を参照してください。 • **line**：回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードを定義しておく必要があります。そのためには、**password** *password* ライン コンフィギュレーション コマンドを使用します。 • **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。そのためには、**username** *password* グローバル コンフィギュレーション コマンドを使用します。 • **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *name* **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、データベースにユーザ名情報を入力する必要があります。 • **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成されるデフォルト リストが使用されます。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** 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。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 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。ログインに対して TACACS+ による認証をディセーブルにするか、またはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

（注） AAA 方式を使用して HTTP アクセスに対してスイッチを保護するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、スイッチは AAA 方式で HTTP アクセスに対して保護されません。

ip http authentication コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

特権 EXEC アクセスおよびネットワーク サービスに対する TACACS+ による認可の設定

AAA 認可は、ユーザが使用できるサービスを制限します。AAA 認可をイネーブルにすると、スイッチは、ローカル ユーザ データベースまたはセキュリティ サーバにあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイルの情報によって許可される場合にだけ、要求したサービスにアクセスできます。

ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定するには、**aaa authorization** グローバル コンフィギュレーション コマンドで **tacacs+** キーワードを指定します。

aaa authorization exec tacacs+ local コマンドは、次の認可パラメータを設定します。

- 認証が TACACS+ を使用して実行された場合、特権 EXEC アクセスの認可には TACACS+ を使用します。
- 認証に TACACS+ が使用されなかった場合は、ローカル データベースを使用します。

（注） 認可が設定されている場合でも、CLI を使用してログインする認証済みのユーザに対しては、認可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに対して TACACS+ による認可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**aaa authorization network tacacs+**	ネットワーク関連サービスのすべての要求に対してユーザを TACACS+ で認可するようにスイッチを設定します。
ステップ 3	**aaa authorization exec tacacs+**	ユーザが特権 EXEC アクセスを行っている場合はユーザを TACACS+ で認可するようにスイッチを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

認可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* 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。

TACACS+ によるアカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザのアクティビティをアカウンティング レコードの形式で TACACS+ セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングに関する Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに保存されます。このデータを分析し、ネットワーク管理、クライアント課金、または監査に利用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに対して TACACS+ によるアカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**aaa accounting network start-stop tacacs+**	すべてのネットワーク関連サービス要求に対して TACACS+ によるアカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop tacacs+**	特権 EXEC プロセスの開始時に start-record アカウンティング通知を送信し、終了時に stop-record を送信するように、TACACS+ によるアカウンティングをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* 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。

AAA サーバが到達不能のときのセッション確立

aaa accounting system guarantee-first コマンドによって、システム アカウンティングが最初のレコードになります。これは、デフォルトの状態です。システムのリロード（場合によっては 3 分以上かかることがある）が行われるまで、ユーザがコンソールまたは端末接続でセッションを開始できないことがあります。

ルータがリロードされたときに AAA サーバが到達不能の場合、ルータとコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

TACACS+ の設定の表示

TACACS+ サーバの統計情報を表示するには、**show tacacs** 特権 EXEC コマンドを使用します。

RADIUS でのスイッチ アクセスの制御

ここでは、RADIUS をイネーブルにして設定する方法を説明します。RADIUS は詳細なアカウント情報を提供し、認証と認可のプロセスの管理を柔軟に制御できます。RADIUS は、AAA によって促進され、AAA コマンドによってだけイネーブルにすることができます。

（注）　この項で使用するコマンドの構文と使用方法の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

ここでは、次の設定情報について説明します。

RADIUS の概要

RADIUS は、不正アクセスに対してネットワークを保護する分散クライアント/サーバ システムです。RADIUS クライアントは、サポートされる Cisco ルータおよびスイッチで動作します。クライアントは、認証要求を中央の RADIUS サーバに送信します。サーバには、ユーザの認証とネットワーク サービス アクセスに関するすべての情報が存在します。RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server Version 3.0）、Livingston、Merit、Microsoft、またはその他のソフトウェア プロバイダーの RADIUS サーバ ソフトウェアを実行するマルチユーザ システムです。詳細については、RADIUS サーバのマニュアルを参照してください。

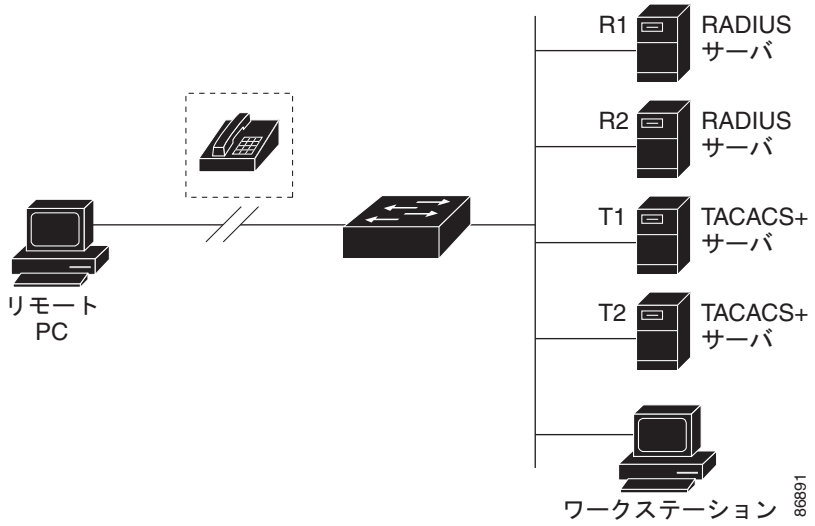
RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- 複数のベンダーのアクセス サーバが存在し、各サーバが RADIUS をサポートしているネットワーク。たとえば、複数のベンダーのアクセス サーバが、単一の RADIUS サーバベースのセキュリティ データベースを使用しているような場合です。複数のベンダーのアクセス サーバが存在する IP ベースのネットワークでは、ダイヤルイン ユーザは、Kerberos セキュリティ システムで動作するようにカスタマイズされた RADIUS サーバを使って認証されます。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。*スマート カード*アクセス制御システムを使用するアクセス環境などです。たとえば、RADIUS を Enigma のセキュリティ カードとともに使用して、ユーザを検証し、ネットワーク リソースへのアクセスを許可するような場合です。
- すでに RADIUS を使用しているネットワーク。RADIUS クライアントを含む Cisco スイッチをネットワークに追加できます。TACACS+ サーバに移行するときの最初のステップになる場合があります。図 11-2（P.11-19）を参照してください。
- ユーザがただ 1 つのサービスにアクセスする必要のあるネットワーク。RADIUS を使用すると、シングル ホスト、Telnet などの単一のユーティリティ、または IEEE 802.1x などのプロトコルを介したネットワークへのユーザ アクセスを制御できます。このプロトコルの詳細については、第 12 章「IEEE 802.1X ポートベースの認証の設定」を参照してください。
- リソースのアカウンティングが必要なネットワーク。RADIUS による認証または認可とは独立して、RADIUS によるアカウンティングを使用できます。RADIUS のアカウンティング機能を使用すると、サービスの開始時と終了時にデータを送信し、セッションの間に使用されたリソースの量（時間、パケット、バイトなど）を表示できます。インターネット サービス プロバイダーは、フリーウェアベース バージョンの RADIUS アクセス制御およびアカウンティング ソフトウェアを使用して、セキュリティや課金に関する特別なニーズを満たすことができます。

RADIUS は、次のようなネットワーク セキュリティ状況には適していません。

- マルチプロトコルのアクセス環境。RADIUS は、AppleTalk Remote Access（ARA）、NetBIOS Frame Control Protocol（NBFCP）、NetWare Asynchronous Services Interface（NASI）、または X.25 PAD による接続はサポートしません。
- スイッチ間またはルータ間の状況。RADIUS は双方向の認証には対応していません。RADIUS は、非シスコ デバイスが認証を必要とする場合に、ある装置から非シスコ デバイスへの認証を行うために使用できます。
- さまざまなサービスを使用するネットワーク。通常、RADIUS はユーザを 1 つのサービス モデルにバインドします。

図 11-2　RADIUS から TACACS+ サービスへの移行



RADIUS の動作

ユーザがログインし、RADIUS サーバでアクセス制御されているスイッチによる認証を試みると、次の処理が行われます。

1. ユーザは、ユーザ名とパスワードの入力を求められます。
2. ユーザ名と暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、次のいずれかの応答を RADIUS サーバから受け取ります。
   a. ACCEPT：ユーザは認証されます。
   b. REJECT：ユーザは、認証されずユーザ名とパスワードの再入力を求められるか、またはアクセスを拒否されます。
   c. CHALLENGE：チャレンジのためユーザからのデータがさらに必要です。
   d. CHALLENGE PASSWORD：応答はユーザに新しいパスワードの選択を要求しています。

ACCEPT または REJECT 応答は、特権 EXEC またはネットワーク認可に使用される追加データとバンドルされます。ユーザは、まず RADIUS による認証が正常に完了してからでないと、RADIUS による認可に進むことはできません（イネーブルになっている場合）。ACCEPT または REJECT パケットに含まれる追加データとしては次のものがあります。

- Telnet、SSH、rlogin、または特権 EXEC の各サービス
- ホストまたはクライアントの IP アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

RADIUS Change of Authorization

ここでは、使用できるプリミティブなどの RADIUS インターフェイスの概要、および Change of Authorization（CoA）の間におけるその使用方法について説明します。

概要

標準的な RADIUS インターフェイスは、通常はプル モデルで使用されます。つまり、要求はネットワークに接続された装置から送信されて、応答はクエリー対象のサーバから返送されます。Catalyst スイッチは、RFC 5176 で定義されている RADIUS Change of Authorization（CoA）拡張機能をサポートします。この機能は通常はプッシュ モデルで使用され、外部の認証、認可、アカウンティング（AAA）サーバまたはポリシー サーバからのセッションのダイナミックな再設定に対応しています。

Cisco IOS Release 12.2(52)SE 以降、スイッチは次のセッション単位の CoA 要求をサポートしています。

- セッションの再認証
- セッションの終了
- セッションの終了とポートのシャットダウン
- セッションの終了とポートのバウンス

この機能は、Cisco Secure Access Control Server（ACS）5.1 に統合されています。ACS の詳細については、次の URL を参照してください。
http://cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html

Catalyst スイッチでは、RADIUS インターフェイスはデフォルトでイネーブルになっています。ただし、次の属性についていくつか基本的な設定が必要です。

- セキュリティとパスワード：『*Catalyst 3750 Switch Software Configuration Guide, Cisco Release 12.2(50)SE*』の「Configuring Switch-Based Authentication」の章の「Preventing Unauthorized Access to Your Switch」の項を参照してください。
- アカウンティング：『*Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE*』の「Configuring Switch-Based Authentication」の章の「Starting RADIUS Accounting」の項を参照してください。

Change-of-Authorization 要求

RFC 5176 で説明されているように、Change of Authorization (CoA) 要求は、セッションの識別、ホストの再認証、およびセッションの終了に対応するために、プッシュ モデルで使用されます。このモデルは、1 つの要求（CoA-Request）と 2 つの応答コードで構成されます。

- CoA 確認応答（ACK）[CoA-ACK]
- CoA 非確認応答（NAK）[CoA-NAK]

要求は CoA クライアント（通常は RADIUS サーバまたはポリシー サーバ）から送信され、リスナーとして機能するスイッチに送られます。

ここでは、次の内容について説明します。

- 「CoA 要求の応答コード」
- 「CoA 要求コマンド」
- 「セッションの再認証」

RFC 5176 への準拠

Disconnect Request メッセージは、Packet of Disconnect（POD; パケット オブ ディスコネクト）とも呼ばれ、セッションを終了するためにスイッチによってサポートされます。

表 11-2 に、この機能のためにサポートされる Internet Engineering Task Force（IETF）属性を示します。

表 11-2　サポートされる IETF 属性

属性番号	属性名
24	State
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

表 11-3 に、Error-Cause 属性に設定される可能性のある値を示します。

表 11-3　Error-Cause の値

値	説明
201	残余セッション コンテキストが削除された
202	無効な EAP パケット（無視）
401	サポートされない属性
402	属性なし
403	NAS ID 不一致
404	無効な要求
405	サポートされないサービス
406	サポートされない拡張
407	無効な属性値
501	管理上禁止
502	要求をルーティングできない（プロキシ）
503	セッション コンテキストが見つからない
504	セッション コンテキストを削除できない
505	その他のプロキシ処理エラー
506	リソースを使用できない
507	要求が開始された
508	複数のセッションの選択はサポートされていない

前提条件

CoA インターフェイスを使用するには、セッションがすでにスイッチに存在している必要があります。CoA は、セッションを識別して接続解除要求を適用するために使用できます。更新は指定したセッションに対してだけ反映されます。

CoA 要求の応答コード

CoA 要求の応答コードを使用して、コマンドをスイッチに渡すことができます。表 11-4（P.11-23）に、サポートされるコマンドを示します。

セッションの識別

特定のセッションを対象とする接続解除要求および CoA 要求の場合、スイッチは次の属性の 1 つまたは複数に基づいてセッションを特定します。

- Calling-Station-Id（ホストの MAC アドレスを含む IETF 属性 31）
- Audit-Session-Id（Cisco Vendor-Specific Attribute（VSA; ベンダー固有属性））
- Acct-Session-Id（IETF 属性 44）

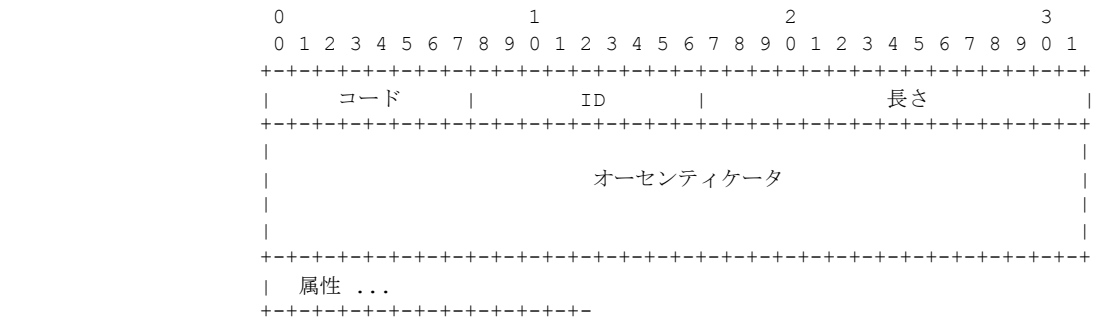
CoA メッセージに含まれるすべてのセッション識別属性がセッションと一致しない限り、スイッチは「無効な属性値」エラー コード属性を含む Disconnect-NAK または CoA-NAK を返します。

特定のセッションを対象とする接続解除要求および CoA 要求の場合、次のいずれかのセッション ID を使用できます。

- Calling-Station-ID（IETF 属性 31、MAC アドレスを含む必要があります）
- Audit-Session-ID（Cisco ベンダー固有属性）
- Accounting-Session-ID（IETF 属性 44）

複数のセッション識別属性がメッセージに含まれる場合、すべての属性がセッションと一致する必要があります。1 つでも一致しないものがある場合は、スイッチはエラーコード「*無効な属性値*」を含む切断否定確認応答（NAK）または CoA-NAK を返します。

RFC 5176 で定義されている CoA 要求コードのパケット形式は、コード、ID、長さ、オーセンティケータ、および属性の各フィールドで構成され、Type:Length:Value（TLV; タイプ : 長さ : 値）の形式になっています。



属性フィールドは、Cisco VSA の伝送に使用されます。

CoA ACK 応答コード

認可ステートが正常に変更されると、肯定確認応答（ACK）が送信されます。CoA ACK で返される属性は CoA 要求によって異なり、これについては個別の CoA コマンドで説明します。

CoA NAK 応答コード

否定確認応答（NAK）は認可ステートの変更が失敗したことを示し、失敗の理由を示す属性を含む場合があります。CoA が成功したかどうかを確認するには、**show** コマンドを使用します。

CoA 要求コマンド

ここでは、次の内容について説明します。

- 「セッションの再認証」
- 「セッションの終了」
- 「CoA Disconnect-Request」
- 「CoA Request: Disable Host Port」
- 「CoA Request: Bounce-Port」

Cisco IOS Release 12.2(52)SE 以降、スイッチは表 11-4 に示すコマンドをサポートします。

表 11-4　スイッチでサポートされる CoA コマンド

コマンド[1]	Cisco VSA
ホストの再認証	Cisco:Avpair="subscriber:command=reauthenticate"
セッションの終了	これは、VSA を必要としない標準の接続解除要求です。
ホスト ポートのバウンス	Cisco:Avpair="subscriber:command=bounce-host-port"
ホスト ポートのディセーブル化	Cisco:Avpair="subscriber:command=disable-host-port"

1. すべての CoA コマンドは、スイッチと CoA クライアントの間のセッション ID を含む必要があります。

セッションの再認証

AAA サーバは、通常、ID またはポスチャが不明のホストがネットワークに参加し、そのホストが制限付きアクセス認可プロファイル（ゲスト VLAN など）に関連付けられていると、セッション再認証要求を生成します。再認証要求により、クレデンシャルが不明のホストでも、適切な認可グループに配置できます。

セッションの認証を開始するために、AAA サーバは、*Cisco:Avpair="subscriber:command=reauthenticate"* という形式の Cisco ベンダー固有属性（VSA）と 1 つまたは複数のセッション識別属性を含む、標準の CoA-Request メッセージを送信します。

現在のセッションの状態により、このメッセージに対するスイッチの応答が決まります。セッションが現在 IEEE 802.1x によって認証されている場合、スイッチは Extensible Authentication Protocol over LAN（EAPOL）RequestId メッセージをサーバに送信することで応答します。

セッションが現在 MAC Authentication Bypass（MAB; MAC 認証バイパス）によって認証されている場合は、スイッチはアクセス要求をサーバに送信し、最初に成功した認証に使用したものと同じ ID 属性を渡します。

スイッチがコマンドを受信したときにセッションの認証が進行中の場合は、スイッチはプロセスを終了し、最初に試みるように設定されている方式で、認証手順を再開します。

セッションがまだ認可されていない場合、またはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認可されている場合は、再認証メッセージにより、最初に試みるように設定されている方式で、アクセス制御方式が再開されます。現在のセッションの認可は、再認証の結果が異なる認可になるまで維持されます。

セッションの終了

セッションを終了できる CoA 要求には 3 つの種類があります。CoA Disconnect-Request は、ホストのポートをディセーブルにしないでセッションを終了します。このコマンドは、指定したホストのオーセンティケータ ステート マシンを再初期化しますが、そのホストのネットワークへのアクセスは制限しません。

ホストのネットワークへのアクセスを制限するには、Cisco:Avpair="subscriber:command=disable-host-port" VSA を指定した CoA 要求を使用します。このコマンドは、あるホストがネットワーク上の問題の原因であることがわかっていて、そのホストのネットワーク アクセスを直ちにブロックする必要があるときに便利です。そのポートでのネットワーク アクセスを元に戻すときは、RADIUS 以外のメカニズムを使用して再びイネーブルにします。

プリンタのようにサプリカントを持たない装置で新しい IP アドレスを取得する必要がある場合は（VLAN を変更したあとなど）、ポートバウンス（ポートを一時的にディセーブルにしてから再びイネーブルにすること）を使用して、ホストのポートでのセッションを終了します。

CoA Disconnect-Request

このコマンドは標準 Disconnect-Request です。このコマンドはセッション指向なので、「セッションの識別」（P.11-22）で説明しているセッション識別属性を 1 つまたは複数含む必要があります。セッションを特定できない場合、スイッチは「セッション コンテキストが見つからない」というエラー コード属性が設定された Disconnect-NAK メッセージを返します。セッションが*特定された*場合は、スイッチはそのセッションを終了します。セッションが完全に削除されたあと、スイッチは Disconnect-ACK を返します。

Disconnect-ACK をクライアントに返す前にスイッチがスタンバイ スイッチにフェールオーバーした場合は、クライアントから要求が再送信されると、新しいアクティブ スイッチで処理が繰り返されます。再送信のあとでセッションが見つからない場合は、「セッション コンテキストが見つからない」というエラー コード属性を含む Disconnect-ACK が送信されます。

CoA Request: Disable Host Port

このコマンドは、次の新しい VSA を含む標準 CoA-Request メッセージで送信されます。

Cisco:Avpair="subscriber:command=disable-host-port"

このコマンドはセッション指向なので、「セッションの識別」（P.11-22）で説明しているセッション識別属性を 1 つまたは複数含む必要があります。セッションを特定できない場合、スイッチは「セッション コンテキストが見つからない」というエラー コード属性が設定された CoA-NAK メッセージを返します。セッションが特定された場合は、スイッチはホストしているポートをディセーブルにして、CoA-ACK メッセージを返します。

CoA-ACK をクライアントに返す前にスイッチで障害が発生した場合は、クライアントから要求が再送信されると、新しいアクティブ スイッチで処理が繰り返されます。CoA-ACK メッセージをクライアントに返したあと、操作が完了する前にスイッチで障害が発生した場合は、操作は新しいアクティブ スイッチで再開されます。

（注）　コマンド再送信後の Disconnect-Request のエラーは、元のコマンドが発行されたあとでスタンバイ スイッチがアクティブになる前に、切り替え前のセッション終了が成功したこと（Disconnect-ACK が送信されなかった場合）、または他の手段によるセッション終了（リンク障害など）による結果である場合があります。

CoA Request: Bounce-Port

このコマンドは、次の VSA を含む標準 CoA-Request メッセージで送信されます。

Cisco:Avpair="subscriber:command=bounce-host-port"

このコマンドはセッション指向なので、「セッションの識別」（P.11-22）で説明しているセッション識別属性を 1 つまたは複数含む必要があります。セッションを特定できない場合、スイッチは「セッション コンテキストが見つからない」というエラー コード属性が設定された CoA-NAK メッセージを返します。セッションが特定された場合は、スイッチはホストしているポートを 10 秒間だけディセーブルにしたあと、再びイネーブルにして（ポートバウンス）、CoA-ACK を返します。

CoA-ACK をクライアントに返す前にスイッチで障害が発生した場合は、クライアントから要求が再送信されると、新しいアクティブ スイッチで処理が繰り返されます。CoA-ACK メッセージをクライアントに返したあと、操作が完了する前にスイッチで障害が発生した場合は、操作は新しいアクティブ スイッチで再開されます。

RADIUS の設定

ここでは、RADIUS をサポートするようにスイッチを設定する方法を説明します。少なくとも、RADIUS サーバ ソフトウェアを実行しているホストを識別し、RADIUS による認証の方式リストを定義する必要があります。必要に応じて、RADIUS による認可とアカウンティングの方式リストも定義できます。

方式リストでは、ユーザの認証、認可、またはアカウントの保持に使用する手順と方式を定義します。方式リストを使用して、使用する 1 つまたは複数のセキュリティ プロトコルを指定でき（TACACS+ やローカル ユーザ名検索など）、これにより、最初の方式が失敗した場合のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用して、ユーザの認証、認可、またはアカウントの保持を行います。その方式が応答しない場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リストの方式による通信が成功するか、方式をすべて試し終わるまで繰り返されます。

スイッチで TACACS+ の機能を設定するには、RADIUS サーバにアクセスし、RADIUS サーバを設定しておく必要があります。

- 「RADIUS のデフォルト設定」（P.11-26）
- 「RADIUS サーバ ホストの識別」（P.11-26）（必須）
- 「RADIUS ログイン認証の設定」（P.11-28）（必須）
- 「AAA サーバ グループの定義」（P.11-30）（任意）
- 「ユーザ イネーブル アクセスおよびネットワーク サービスに対する RADIUS による認可の設定」（P.11-32）（任意）
- 「RADIUS によるアカウンティングの開始」（P.11-33）（任意）
- 「すべての RADIUS サーバに対する設定」（P.11-34）（任意）
- 「ベンダー固有の RADIUS 属性を使用するためのスイッチの設定」（P.11-34）（任意）
- 「ベンダー独自の RADIUS サーバ通信のためのスイッチの設定」（P.11-36）（任意）

- 「スイッチでの CoA の設定」（P.11-37）
- 「CoA 機能のモニタとトラブルシューティング」（P.11-38）
- 「RADIUS サーバのロード バランシングの設定」（P.11-38）（任意）

RADIUS のデフォルト設定

RADIUS と AAA はデフォルトではディセーブルになっています。

セキュリティの問題を防ぐため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。イネーブルにすると、RADIUS は CLI を使用してスイッチにアクセスするユーザを認証できます。

RADIUS サーバ ホストの識別

スイッチと RADIUS サーバの間の通信には、複数のコンポーネントが関係します。

- ホスト名または IP アドレス
- 認証宛先ポート
- アカウンティング宛先ポート
- キー文字列
- タイムアウト時間
- 再送信値

RADIUS セキュリティ サーバを識別するには、ホスト名または IP アドレス、ホスト名と特定の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号、または IP アドレスと特定の UDP ポート番号を使用します。IP アドレスと UDP ポート番号の組み合わせにより一意の ID が作成され、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。この一意の ID を使用して、同じ IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できます。

同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（アカウンティングなど）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。この例を使用すると、最初のホスト エントリがアカウンティング サービスの提供に失敗した場合は、`%RADIUS-4-RADIUS_DEAD` メッセージが表示されたあと、スイッチは同じ装置上でアカウンティング サービス用に設定されている第 2 のホスト エントリを試します。RADIUS ホスト エントリは、設定されている順序で試行されます。

RADIUS サーバとスイッチは、共有シークレット テキスト ストリングを使用してパスワードを暗号化し、応答を交換します。AAA セキュリティ コマンドを使用するように RADIUS を設定するには、RADIUS サーバ デーモンを実行しているホストと、そのホストがスイッチと共有している秘密テキスト（キー）文字列を指定する必要があります。

タイムアウト、再送信、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに、サーバごとに、またはグローバルとサーバごとの設定の組み合わせで設定できます。これらの設定をスイッチと通信するすべての RADIUS サーバにグローバルに設定するには、それぞれに一意の 3 つのグローバル コンフィギュレーション コマンド **radius-server timeout**、**radius-server retransmit**、および **radius-server key** を使用します。これらの値を特定の RADIUS サーバに適用するには、**radius-server host** 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）　1 つのスイッチにグローバル機能とサーバごとの機能（タイムアウト、再送信、キーの各コマンド）の両方を設定した場合は、タイマー、再送信、キー値のサーバごとのコマンドがグローバルなコマンドより優先されます。すべての RADIUS サーバでこれらの設定を行う方法については、「すべての

RADIUS サーバに対する設定」（P.11-34）を参照してください。

AAA サーバ グループを使用して既存のサーバ ホストを認証用にグループ化するように、スイッチを設定できます。詳細については、「AAA サーバ グループの定義」（P.11-30）を参照してください。

サーバごとの RADIUS サーバ通信を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**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 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、スイッチが再送信の前に RADIUS サーバの応答を待機する時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドの設定より優先されます。**radius-server host** コマンドでタイムアウトを設定しないと、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合またはサーバの応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数の値を設定しないと、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。キーは必ず **radius-server host** コマンドの最後の項目として設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 単一の IP アドレスに関連付けられている複数のホスト エントリを認識するようにスイッチを設定するには、必要な回数だけこのコマンドを入力し、そのたびに異なる UDP ポート番号を指定します。スイッチのソフトウェアは、ここで指定した順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

指定した RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* 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。

次に、1 つの RADIUS サーバを認証用に設定し、別のサーバをアカウンティング用に設定する例を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次に、*host1* を RADIUS サーバとして設定し、デフォルトのポートを認証とアカウンティングの両方に使用する例を示します。

```
Switch(config)# radius-server host host1
```

（注）　RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、およびサーバとスイッチの両方で共有されるキー文字列があります。詳細については、RADIUS サーバのマニュアルを参照してください。

RADIUS ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義したあと、そのリストをさまざまなポートに適用します。方式リストでは、実行する認証のタイプと、実行する手順を定義します。定義した認証方式を実行するには、特定のポートにリストを適用する必要があります。唯一の例外はデフォルトの方式リストです（名前は *default* です）。方式の名前付きリストが明示的に定義されているポート以外のすべてのポートには、デフォルトの方式リストが自動的に適用されます。

方式リストは、ユーザ認証のためクエリー送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定でき、これにより、最初の方式が失敗した場合の認証のバックアップ システムを設定できます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。このサイクルのいずれかの時点で認証が失敗した場合、つまりセキュリティ サーバまたはローカル ユーザ名データベースがユーザ アクセスを拒否する応答を返した場合には、認証プロセスは中止され、その他の認証方式が試みられることはありません。

ログイン認証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA をイネーブルにします。

	コマンド	目的
ステップ 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	ログイン認証方式リストを作成します。 • **login authentication** コマンドに名前付きリストが*指定されていない*場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 • *list-name* には、作成するリストの名前を示す文字列を指定します。 • *method1...* には、認証アルゴリズムが試みる実際の方式を指定します。追加の認証方式は、前の認証方式が失敗した場合ではなく、エラーを返した場合にだけ使用されます。 次のいずれかの方式を選択します。 – **enable**：イネーブル パスワードを認証に使用します。この認証方式を使用するには、**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イネーブル パスワードを定義しておく必要があります。 – **group radius**：RADIUS 認証を使用します。この認証方式を使用するには、RADIUS サーバを設定しておく必要があります。詳細については、「RADIUS サーバ ホストの識別」（P.11-26）を参照してください。 – **line**：回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードを定義しておく必要があります。そのためには、**password** *password* ライン コンフィギュレーション コマンドを使用します。 – **local**：ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力する必要があります。そのためには、**username** *name* **password** グローバル コンフィギュレーション コマンドを使用します。 – **local-case**：大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。**username** *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、データベースにユーザ名情報を入力する必要があります。 – **none**：ログインに認証を使用しません。
ステップ 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 5	**login authentication** {**default** | *list-name*}	認証リストを 1 つまたは複数の回線に適用します。 • **default** を指定すると、**aaa authentication login** コマンドで作成されるデフォルト リストが使用されます。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** 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。AAA 認証をディセーブルにするには、**no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 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。ログインに対して RADIUS 認証をディセーブルにするか、またはデフォルト値に戻すには、**no login authentication** {**default** | *list-name*} ライン コンフィギュレーション コマンドを使用します。

（注）　AAA 方式を使用して HTTP アクセスに対してスイッチを保護するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、スイッチは AAA 方式で HTTP アクセスに対して保護されません。

ip http authentication コマンドの詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

AAA サーバ グループの定義

AAA サーバ グループを使用して既存のサーバ ホストを認証用にグループ化するように、スイッチを設定できます。設定済みサーバ ホストのサブセットを選択し、それを特定のサービスに対して使用します。サーバ グループは、グローバル サーバ ホスト リストとともに使用します。このリストでは、選択されているサーバ ホストの IP アドレスがリストされています。

各ホスト エントリの ID（IP アドレスと UDP ポート番号の組み合わせ）が一意であれば、サーバ グループは同じサーバに対して複数のホスト エントリを含むこともでき、異なるポートを特定の AAA サービスを提供する RADIUS ホストとして個別に定義できます。同じ RADIUS サーバ上の異なる 2 つのホスト エントリを同じサービス（アカウンティングなど）用に設定した場合、2 番めに設定したホスト エントリは、最初のホスト エントリのフェールオーバー バックアップとして動作します。

特定のサーバと定義済みのグループ サーバを関連付けるには、**server** グループ サーバ コンフィギュレーション コマンドを使用します。IP アドレスでサーバを指定することも、オプションの **auth-port** および **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを指定することもできます。

AAA サーバ グループを定義し、それを特定の RADIUS サーバと関連付けるには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。 • （任意）**auth-port** *port-number* には、認証要求の UDP 宛先ポートを指定します。 • （任意）**acct-port** *port-number* には、アカウンティング要求の UDP 宛先ポートを指定します。 • （任意）**timeout** *seconds* には、スイッチが再送信の前に RADIUS サーバの応答を待機する時間を指定します。指定できる範囲は 1 ～ 1000 です。この設定は、**radius-server timeout** グローバル コンフィギュレーション コマンドの設定より優先されます。**radius-server host** コマンドでタイムアウトを設定しないと、**radius-server timeout** コマンドの設定が使用されます。 • （任意）**retransmit** *retries* には、サーバが応答しない場合またはサーバの応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。指定できる範囲は 1 ～ 1000 です。**radius-server host** コマンドで再送信回数の値を設定しないと、**radius-server retransmit** グローバル コンフィギュレーション コマンドの設定が使用されます。 • （任意）**key** *string* には、スイッチと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。キーは必ず **radius-server host** コマンドの最後の項目として設定してください。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。 単一の IP アドレスに関連付けられている複数のホスト エントリを認識するようにスイッチを設定するには、必要な回数だけこのコマンドを入力し、そのたびに異なる UDP ポート番号を指定します。スイッチのソフトウェアは、ここで指定した順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信、暗号キーの値を設定します。
ステップ 3	**aaa new-model**	AAA をイネーブルにします。
ステップ 4	**aaa group server radius** *group-name*	グループ名を指定して AAA のサーバ グループを定義します。 このコマンドは、スイッチをサーバ グループ コンフィギュレーション モードにします。
ステップ 5	**server** *ip-address*	特定の RADIUS サーバと定義したサーバ グループを関連付けます。AAA サーバ グループ内の RADIUS サーバごとに、このステップを繰り返します。 グループ内の各サーバは、ステップ 2 で先に定義しておく必要があります。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「RADIUS ログイン認証の設定」（P.11-28）を参照してください。

指定した RADIUS サーバを削除するには、**no radius-server host** *hostname* | *ip-address* 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。コンフィギュレーション リストからサーバ グループを削除するには、**no aaa group server radius** *group-name* 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。RADIUS サーバの IP アドレスを削除するには、**no server** *ip-address* サーバ グループ コンフィギュレーション コマンドを使用します。

次の例では、2 つの異なる RADIUS グループ サーバ（*group1* と *group2*）を認識するようにスイッチを設定しています。group1 では、同じサービスに対して設定されている同じ RADIUS サーバに 2 つの異なるホスト エントリがあります。2 番めのホスト エントリは、1 番めのエントリのフェールオーバー バックアップとして動作します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

ユーザ イネーブル アクセスおよびネットワーク サービスに対する RADIUS による認可の設定

AAA 認可は、ユーザが使用できるサービスを制限します。AAA 認可をイネーブルにすると、スイッチは、ローカル ユーザ データベースまたはセキュリティ サーバにあるユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザ プロファイルの情報によって許可される場合にだけ、要求したサービスにアクセスできます。

ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定するには、**aaa authorization** グローバル コンフィギュレーション コマンドで **radius** キーワードを指定します。

aaa authorization exec radius local コマンドは、次の認可パラメータを設定します。

- 認証が RADIUS を使用して実行された場合、特権 EXEC アクセスの認可には RADIUS を使用します。
- 認証に RADIUS が使用されなかった場合は、ローカル データベースを使用します。

（注）　認可が設定されている場合でも、CLI を使用してログインする認証済みのユーザに対しては、認可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに対して RADIUS による認可を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**aaa authorization network radius**	ネットワーク関連サービスのすべての要求に対してユーザを RADIUS で認可するようにスイッチを設定します。
ステップ 3	**aaa authorization exec radius**	ユーザが特権 EXEC アクセスを行っている場合はユーザを RADIUS で認可するようにスイッチを設定します。 **exec** キーワードを指定すると、ユーザ プロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 4	**end**	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

認可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* 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。

RADIUS によるアカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソースの量を追跡します。AAA アカウンティングをイネーブルにすると、スイッチはユーザのアクティビティをアカウンティング レコードの形式で RADIUS セキュリティ サーバに報告します。各アカウンティング レコードにはアカウンティングに関する Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに保存されます。このデータを分析し、ネットワーク管理、クライアント課金、または監査に利用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに対して RADIUS によるアカウンティングをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**aaa accounting network start-stop radius**	すべてのネットワーク関連サービス要求に対して RADIUS によるアカウンティングをイネーブルにします。
ステップ 3	**aaa accounting exec start-stop radius**	特権 EXEC プロセスの開始時に start-record アカウンティング通知を送信し、終了時に stop-record を送信するように、RADIUS によるアカウンティングをイネーブルにします。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

アカウンティングをディセーブルにするには、**no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* 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。

AAA サーバが到達不能のときのセッション確立

aaa accounting system guarantee-first コマンドによって、システム アカウンティングが最初のレコードになります。これは、デフォルトの状態です。システムのリロード（場合によっては 3 分以上かかることがある）が行われるまで、ユーザがコンソールまたは端末接続でセッションを開始できないことがあります。

ルータがリロードされたときに AAA サーバが到達不能の場合、ルータとコンソールまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

すべての RADIUS サーバに対する設定

スイッチとすべての RADIUS サーバの間のグローバルな通信設定を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**radius-server key** *string*	スイッチとすべての RADIUS サーバとの間で使用する共有シークレット テキスト ストリングを指定します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 3	**radius-server retransmit** *retries*	中止する前にスイッチがサーバに各 RADIUS 要求を送信する回数を指定します。デフォルト値は 3 で、指定できる範囲は 1 ～ 1000 です。
ステップ 4	**radius-server timeout** *seconds*	スイッチが RADIUS 要求を再送信する前に要求への応答を待機する秒数を指定します。デフォルト値は 5 秒で、指定できる範囲は 1 ～ 1000 です。
ステップ 5	**radius-server deadtime** *minutes*	認証要求に応答しない RADIUS サーバをスキップする分数を指定します。これにより、次に設定されているサーバを試行する前に要求の待機が時間切れになるのを防ぎます。デフォルト値は 0 で、指定できる範囲は 1 ～ 1440 分です。
ステップ 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config**	設定を確認します。
ステップ 8	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

再送信、タイムアウト、スキップ時間の設定をデフォルトに戻すには、これらのコマンドの **no** 形式を使用します。

ベンダー固有の RADIUS 属性を使用するためのスイッチの設定

Internet Engineering Task Force（IETF）のドラフト標準では、スイッチと RADIUS サーバの間でベンダー固有属性（属性 26）を使用してベンダー固有の情報を通信するための方法が指定されています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、仕様で推奨されている形式を使用して 1 つのベンダー固有属性をサポートしています。シスコのベンダー ID は 9、サポートされるオプションはベンダー タイプ 1 で、名前は *cisco-avpair* です。値は次の形式のストリングです。

```
protocol : attribute sep value *
```

protocol は、特定の認可タイプに対するシスコのプロトコル属性の値です。*attribute* および *value* はシスコの TACACS+ 仕様で定義されている適切な Attribute-Value（AV）ペアであり、*sep* は必須属性の場合は =、任意属性の場合は * です。TACACS+ による認可で使用可能なすべての機能セットを、RADIUS で使用できます。

たとえば、次の AV ペアは、（PPP IPCP アドレス割り当ての間の）IP 認可の間にシスコの *複数名 IP アドレス プール*機能をアクティブにします。

```
cisco-avpair= "ip:addr-pool=first"
```

次に、スイッチからログインするユーザがすぐに特権 EXEC コマンドにアクセスできるようにする例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

次に、RADIUS サーバ データベースで認可された VLAN を指定する例を示します。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

次に、この接続の期間だけインターフェイスに ASCII 形式の入力 ACL を適用する例を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次に、この接続の期間だけインターフェイスに ASCII 形式の出力 ACL を適用する例を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

他のベンダーは、それぞれが独自に一意のベンダー ID、オプション、および関連する VSA を定めています。ベンダー ID と VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

VSA を認識して使用するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**radius-server vsa send** [**accounting** | **authentication**]	RADIUS IETF 属性 26 で定義されている VSA を認識して使用するようにスイッチをイネーブルにします。 • （任意）認識されるベンダー固有属性のセットをアカウンティング属性だけに制限するには、**accounting** キーワードを使用します。 • （任意）認識されるベンダー固有属性のセットを認証属性だけに制限するには、**authentication** キーワードを使用します。 キーワードを指定しないでこのコマンドを入力すると、アカウンティングと認証の両方のベンダー固有属性が使用されます。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**show running-config**	設定を確認します。
ステップ 5	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

（注）　RADIUS 属性の詳細なリストまたはベンダー固有属性 26 の詳細については、Cisco.com のページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] >[Command References] にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の付録「RADIUS Attributes」を参照してください。

ベンダー独自の RADIUS サーバ通信のためのスイッチの設定

RADIUS に関する IETF のドラフト標準では、スイッチと RADIUS サーバの間でベンダー独自の情報を通信するための方法が指定されていますが、独自の方法で RADIUS 属性を拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自の RADIUS 属性のサブセットをサポートします。

すでに説明したように、RADIUS を設定するには（ベンダー独自か IETF ドラフト準拠かにかかわらず）、RADIUS サーバ デーモンを実行するホストと、ホストがスイッチと共有するシークレット テキスト ストリングを指定する必要があります。RADIUS ホストおよびシークレット テキスト ストリングを指定するには、**radius-server** 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。

ベンダー独自の RADIUS サーバ ホストおよび共有シークレット テキスト ストリングを指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、それが RADIUS のベンダー独自の実装を使用していることを示します。
ステップ 3	**radius-server key** *string*	スイッチとベンダー独自の RADIUS サーバの間で使用する共有シークレット テキスト ストリングを指定します。スイッチと RADIUS サーバはこの文字列を使用して、パスワードを暗号化し、応答を交換します。 **（注）** key は文字列であり、RADIUS サーバで使用されている暗号キーと一致する必要があります。先頭のスペースは無視されますが、key の中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show running-config**	設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

ベンダー独自の RADIUS ホストを削除するには、**no radius-server host** {*hostname* | *ip-address*} **non-standard** 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。キーをディセーブルにするには、**no radius-server key** 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。

次に、ベンダー独自の RADIUS ホストを指定し、スイッチとサーバの間で *rad124* の秘密キーを使用する例を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

スイッチでの CoA の設定

スイッチで CoA を設定するには、特権 EXEC モードで次の手順を実行します。この手順は必須です。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa server radius dynamic-author**	スイッチを認証、認可、アカウンティング（AAA）サーバとして設定し、外部ポリシー サーバとの相互通信を容易にします。
ステップ 4	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*]	ダイナミック認可ローカル サーバ コンフィギュレーション モードを開始し、装置が CoA および接続解除の要求を受け付ける RADIUS クライアントを指定します。
ステップ 5	**server-key** [**0** | **7**] *string*	装置と RADIUS クライアントの間で共有する RADIUS キーを設定します。
ステップ 6	**port** *port-number*	装置が設定済みの RADIUS クライアントからの RADIUS 要求を待ち受けるポートを指定します。
ステップ 7	**auth-type** {**any** | **all** | **session-key**}	スイッチが RADIUS クライアントに使用する認可のタイプを指定します。 クライアントが認可を受けるには、設定済みのすべての属性が一致する必要があります。
ステップ 8	**ignore session-key**	（任意）セッション キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 9	**ignore server-key**	（任意）サーバ キーを無視するようにスイッチを設定します。 **ignore** コマンドの詳細については、Cisco.com の『*Cisco IOS Intelligent Services Gateway Command Reference*』を参照してください。
ステップ 10	**authentication command bounce-port ignore**	（任意）CoA 要求を無視してセッションをホストしているポートを一時的にディセーブルにするようにスイッチを設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生し、変更を検出するためのサプリカントがエンドポイント上にないときに、ホストから DHCP の再ネゴシエーションをトリガーすることです。
ステップ 11	**authentication command disable-port ignore**	（任意）セッションをホストしているポートを管理的にシャットダウンすることを要求する非標準のコマンドを無視するように、スイッチを設定します。ポートをシャットダウンすると、セッションは終了します。 ポートを再びイネーブルにするには、標準の CLI コマンドまたは SNMP コマンドを使用します。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show running-config**	設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** 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。スイッチの AAA サーバ機能を無効にするには、**no aaa server radius dynamic authorization** 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。

CoA 機能のモニタとトラブルシューティング

次の Cisco IOS コマンドを使用して、スイッチの CoA 機能のモニタとトラブルシューティングを行います。

- **debug radius**
- **debug aaa coa**
- **debug aaa pod**
- **debug aaa subsys**
- **debug cmdhd** [**detail** | **error** | **events**]
- **show aaa attributes protocol radius**

RADIUS サーバのロード バランシングの設定

この機能を使用すると、アクセスと認証の要求を、サーバ グループ内のすべての RADIUS サーバに均等に配分できます。詳細については、次の場所にある『Cisco IOS Security Configuration Guide, Release 12.2』の「RADIUS Server Load Balancing」を参照してください。
http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrldldbl.html

RADIUS の設定の表示

RADIUS の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

Kerberos でのスイッチ アクセスの制御

ここでは、信頼できるサード パーティを使用してネットワーク リソースに対する要求を認証する Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。この機能を使用するには、暗号化バージョンのスイッチ ソフトウェアをスイッチにインストールする必要があります。

この機能を使用したり、暗号化ソフトウェアのファイルを Cisco.com からダウンロードしたりするには、許可を得る必要があります。詳細については、このリリースに対応するリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「Kerberos の概要」（P.11-39）
- 「Kerberos の動作」（P.11-41）
- 「Kerberos の設定」（P.11-42）

Kerberos の設定例については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Kerberos Configuration Examples」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080087df1.html

ここで使用するコマンドの構文および使用方法の詳細については、次の URL にある『*Cisco IOS Security Command Reference, Release 12.2*』の「Security Server Protocols」の章の「Kerberos Commands」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

（注）　Kerberos 設定例および『*Cisco IOS Security Command Reference, Release 12.2*』では、信頼できるサード パーティは、Kerberos をサポートし、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos の概要

Kerberos は、Massachusetts Institute of Technology（MIT）で開発された秘密キー ネットワーク認証プロトコルです。Data Encryption Standard（DES; データ暗号化規格）暗号アルゴリズムを使用して暗号化と認証を行い、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサード パーティの概念を使用して、ユーザとサービスのセキュアな検証を実行します。この信頼できるサード パーティは、*Key Distribution Center*（KDC; キー発行局）と呼ばれます。

Kerberos は、ユーザが自分で主張するとおりのユーザであり、ユーザが使用するネットワーク サービスがそのとおりのものであることを確認します。そのために、KDC つまり信頼できる Kerberos サーバはチケットをユーザに発行します。このチケットは有効期限が限られており、ユーザのクレデンシャル キャッシュに保存されます。Kerberos サーバは、ユーザ名とパスワードの代わりにチケットを使用して、ユーザとネットワーク サービスを認証します。

（注）　Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos のクレデンシャル方式は、*シングル ログオン*と呼ばれるプロセスを使用します。このプロセスは、ユーザを 1 回認証すると、そのユーザ クレデンシャルが受け付けられるすべての場所で（別のパスワードを暗号化することなく）セキュアな認証を許可します。

このソフトウェア リリースでは Kerberos 5 をサポートするので、すでに Kerberos 5 を使用している場合は、他のネットワーク ホスト（UNIX サーバや PC など）ですでに使用しているものと同じ Kerberos 認証データベースを KDC で使用できます。

このソフトウェア リリースの Kerberos は、次のネットワーク サービスをサポートします。

- Telnet
- rlogin
- remote shell protocol（rsh; リモート シェル プロトコル）

表 11-5 に Kerberos に関連する一般的な用語とその定義を示します。

表 11-5　Kerberos の用語

用語	定義
認証	ユーザまたはサービスが別のサービスに対して自分の身元を証明するプロセス。たとえば、クライアントがスイッチに対して認証したり、スイッチが別のスイッチに対して認証したりする場合があります。
認可	スイッチが、ネットワークまたはスイッチでユーザに与えられている権限およびユーザが実行できる処理を識別する手段。

表 11-5　Kerberos の用語 （続き）

用語	定義
クレデンシャル	TGT[1] やサービス クレデンシャルなどの認証チケットを表す一般的な用語。Kerberos クレデンシャルはユーザまたはサービスの ID を確認します。チケットを発行した Kerberos サーバをネットワーク サービスが信頼することにした場合、ユーザ名とパスワードを再入力する代わりにチケットを使用できます。クレデンシャルのデフォルトの有効期間は 8 時間です。
インスタンス	Kerberos プリンシパルの承認レベルのラベル。ほとんどの Kerberos プリンシパルの形式は *user@REALM*（たとえば smith@EXAMPLE.COM）です。Kerberos インスタンスを含む Kerberos プリンシパルの形式は *user/instance@REALM*（たとえば smith/admin@EXAMPLE.COM）です。Kerberos インスタンスを使用すると、認証が成功した場合にユーザの承認レベルを指定できます。各ネットワーク サービスのサーバでは Kerberos インスタンスの認可マッピングが実装され、適用されている場合がありますが、そのようにする必要はありません。 **（注）** Kerberos プリンシパルとインスタンスの名前は、すべて小文字にする*必要があります*。 **（注）** Kerberos レルム名は、すべて大文字にする*必要があります*。
KDC[2]	ネットワーク ホスト上で実行する Kerberos サーバとデータベース プログラムで構成されるキー発行局。
Kerberos 対応	Kerberos クレデンシャル インフラストラクチャをサポートするように変更されたアプリケーションおよびサービスを示す用語。
Kerberos レルム	Kerberos サーバに登録されたユーザ、ホスト、およびネットワーク サービスで構成されるドメイン。ユーザまたはネットワーク サービスは、Kerberos サーバを信頼することで、別のユーザやネットワーク サービスの ID を検証します。 **（注）** Kerberos レルム名は、すべて大文字にする*必要があります*。
Kerberos サーバ	ネットワーク ホスト上で実行しているデーモン。ユーザおよびネットワーク サービスは、自分の ID を Kerberos サーバに登録します。ネットワーク サービスは Kerberos サーバをクエリーして、他のネットワーク サービスに対して認証します。
KEYTAB[3]	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降では、ネットワーク サービスは、KEYTAB を使用して暗号化されたサービス クレデンシャルを復号化することで、クレデンシャルを認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB は SRVTAB[4] と呼ばれていました。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバでのユーザまたはサービスの身元です。 **（注）** Kerberos プリンシパル名は、すべて小文字にする*必要があります*。
サービス クレデンシャル	ネットワーク サービスのクレデンシャル。KDC から発行されるとき、このクレデンシャルは、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。パスワードはユーザの TGT とも共有されます。

表 11-5　Kerberos の用語 （続き）

用語	定義
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降では、SRVTAB は KEYTAB と呼ばれます。
TGT	KDC が認証済みのユーザに対して発行するクレデンシャルであるチケット認可チケット。TGT を受け取ったユーザは、KDC によって表される Kerberos レルム内のネットワーク サービスに対して認証できます。

1. TGT = Ticket Granting Ticket（チケット認可チケット）
2. KDC = Key Distribution Center（キー発行局）
3. KEYTAB = Key Table（キー テーブル）
4. SRVTAB = Server Table（サーバ テーブル）

Kerberos の動作

Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してリモート ユーザを認証できる IE 3000 スイッチです。さまざまな方法で Kerberos をカスタマイズできますが、ネットワーク サービスにアクセスを試みるリモート ユーザは、3 つのセキュリティ レイヤを通過してからでないと、ネットワーク サービスにアクセスできません。

IE 3000 スイッチを Kerberos サーバとして使用してネットワーク サービスに対して認証するには、リモート ユーザは次の手順を実行する必要があります。

1. 「境界スイッチに対する認証」（P.11-41）
2. 「KDC からの TGT の取得」（P.11-42）
3. 「ネットワーク サービスに対する認証」（P.11-42）

境界スイッチに対する認証

ここでは、リモート ユーザが通過する必要のある第 1 のセキュリティ レイヤについて説明します。ユーザは最初に境界スイッチに対して認証を行う必要があります。この処理は次のように行われます。

1. ユーザは、Kerberos 対応ではない Telnet 接続を境界スイッチに対して開きます。
2. スイッチは、ユーザにユーザ名とパスワードの入力を求めます。
3. スイッチは、このユーザに対する TGT を KDC に要求します。
4. KDC は、ユーザの ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザが入力したパスワードを使用して TGT の復号化を試みます。
   - 復号化が成功すると、ユーザはスイッチに対して認証されます。
   - 復号化が成功しない場合は、ユーザはユーザ名とパスワードを再入力するか（Caps Lock または Num Lock のオンまたはオフに注意してください）、または別のユーザ名とパスワードを入力して、ステップ 2 を繰り返します。

Kerberos 対応ではない Telnet セッションを開始して境界スイッチに対して認証するリモート ユーザは、ファイアウォールの内部にいますが、ネットワーク サービスにアクセスする前に、KDC に対して直接認証する必要があります。ユーザが KDC に対して認証する必要があるのは、KDC が発行する TGT はスイッチに格納され、ユーザがスイッチにログオンするまでは追加の認証に TGT を使用できないためです。

KDC からの TGT の取得

ここでは、リモート ユーザが通過する必要のある第 2 のセキュリティ レイヤについて説明します。ユーザは次に、ネットワーク サービスにアクセスするために、KDC に対して認証して TGT を KDC から取得する必要があります。

KDC に対して認証を行う方法については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Obtaining a TGT from a KDC」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

ネットワーク サービスに対する認証

ここでは、リモート ユーザが通過する必要のある第 3 のセキュリティ レイヤについて説明します。TGT を取得したユーザは次に、Kerberos レルム内にあるネットワーク サービスに対して認証する必要があります。

ネットワーク サービスに対して認証を行う方法については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Authenticating to Network Services」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

Kerberos の設定

リモート ユーザがネットワーク サービスに対して認証できるためには、ユーザおよびネットワーク サービスと通信して相互に認証するように、Kerberos レルム内のホストと KDC を設定する必要があります。そのためには、ユーザとネットワーク サービスを相互に識別する必要があります。ホストのエントリを KDC 上の Kerberos データベースに追加し、KDC によって生成された KEYTAB ファイルを Kerberos レルム内のすべてのホストに追加します。また、KDC データベースにユーザのエントリを作成します。

ホストおよびユーザのエントリを追加または作成するときは、次の注意事項に従ってください。

- Kerberos プリンシパル名は、すべて小文字にする*必要があります*。
- Kerberos インスタンス名は、すべて小文字にする*必要があります*。
- Kerberos レルム名は、すべて大文字にする*必要があります*。

（注） Kerberos サーバは、ネットワーク セキュリティ サーバとして設定され、Kerberos プロトコルを使用してユーザを認証できる IE 3000 スイッチです。

Kerberos で認証されたサーバ クライアント システムを設定するには、次の手順を実行します。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

手順については、次の URL にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Security Server Protocols」の「Kerberos Configuration Task List」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

ローカルな認証と認可のためのスイッチの設定

AAA をローカル モードで実装するようにスイッチを設定することで、サーバなしで動作するように AAA を設定できます。このように設定すると、スイッチが認証と認可を処理します。この設定ではアカウンティングは使用できません。

ローカル AAA 用にスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**aaa new-model**	AAA をイネーブルにします。
ステップ 3	**aaa authentication login default local**	ローカル ユーザ名データベースを使用するように、ログイン認証を設定します。**default** キーワードは、ローカル ユーザ データベース認証をすべてのポートに適用します。
ステップ 4	**aaa authorization exec local**	AAA によるユーザの認可を設定し、ローカル データベースをチェックし、ユーザに EXEC シェルの実行を許可します。
ステップ 5	**aaa authorization network local**	ネットワーク関連サービスのすべての要求に対してユーザを AAA で認可するように設定します。
ステップ 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	ローカル データベースに入り、ユーザ名に基づく認証システムを設定します。 ユーザごとにこのコマンドを繰り返します。 • *name* には、ユーザ ID として 1 語を指定します。スペースおよび引用符は使用できません。 • （任意）*level* には、ユーザがアクセスしたあとで割り当てられ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 は特権 EXEC モード アクセスです。レベル 0 はユーザ EXEC モード アクセスです。 • *encryption-type* には、暗号化されていないパスワードが後ろに続くことを指定する場合は 0 を入力します。非表示パスワードが後ろに続くことを指定する場合は 7 を入力します。 • *password* には、スイッチにアクセスするためにユーザ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 文字でなければならず、間にスペースを含むことができ、**username** コマンドで最後に指定するオプションである必要があります。
ステップ 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show running-config**	設定を確認します。
ステップ 9	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

AAA をディセーブルにするには、**no aaa new-model** 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。認可をディセーブルにするには、**no aaa authorization** {**network** | **exec**} *method1* 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） AAA 方式を使用して HTTP アクセスに対してスイッチを保護するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、スイッチは AAA 方式で HTTP アクセスに対して保護されません。

ip http authentication コマンドの詳細については、『*Cisco IOS Security Command Reference, Release 12.2*』を参照してください。

セキュア シェル用のスイッチの設定

ここでは、セキュア シェル（SSH）機能の設定方法について説明します。この機能を使用するには、暗号化ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用したり、暗号化ソフトウェアのファイルを Cisco.com からダウンロードしたりするには、許可を得る必要があります。詳細については、このリリースに対応するリリース ノートを参照してください。

ここでは、次の情報について説明します。

SSH の設定例については、次の URL にある『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*』の「Configuring Secure Shell」の「SSH Configuration Examples」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html

（注）　この項で使用しているコマンドの構文および使用方法の詳細については、次の URL にあるこのリリースのコマンド リファレンスおよび Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

SSH の概要

SSH は、装置に対するセキュアなリモート接続を提供するプロトコルです。SSH は装置の認証時に強力な暗号化を行うことにより、リモート接続に対して Telnet よりも高いセキュリティを提供します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートします。

この項で説明する内容は、次のとおりです。

SSH サーバ、統合クライアント、サポートされるバージョン

SSH の機能には、スイッチで実行するアプリケーションである SSH サーバと SSH 統合クライアントがあります。SSH クライアントを使用して、SSH サーバを実行するスイッチに接続できます。SSH サーバは、このリリースでサポートされる SSH クライアントおよびシスコ以外の SSH クライアントと連動します。また、SSH クライアントは、このリリースでサポートされる SSH サーバおよびシスコ以外の SSH サーバと連動します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは SSHv1 クライアントをサポートします。

SSH は、データ暗号化規格（DES）、Triple DES（3DES）暗号アルゴリズム、およびパスワードに基づくユーザ認証をサポートします。

SSH は、次のユーザ認証方式もサポートします。

- TACACS+（詳細については、「TACACS+ でのスイッチ アクセスの制御」（P.11-10）を参照してください）
- RADIUS（詳細については、「RADIUS でのスイッチ アクセスの制御」（P.11-17）を参照してください）
- ローカル認証と認可（詳細については、「ローカルな認証と認可のためのスイッチの設定」（P.11-43）を参照してください）

（注）　このソフトウェア リリースは IP セキュリティ（IPSec）はサポートしません。

制限事項

SSH には、次の制限事項が適用されます。

- スイッチは、Rivest、Shamir、Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバと SSH クライアントは、DES（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアだけでサポートされます。
- スイッチは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES; 高度暗号化規格）暗号化アルゴリズムをサポートします。ただし、対称暗号 AES によるキーの暗号化はサポートしません。

SSH の設定

ここでは、次の設定情報について説明します。

- 「設定時の注意事項」（P.11-45）
- 「SSH を実行するためのスイッチの設定」（P.11-46）（必須）
- 「SSH サーバの設定」（P.11-47）（スイッチを SSH サーバとして設定する場合に限り必要）

設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定するときは、次の注意事項に従ってください。

- SSHv1 サーバによって生成された RSA キー ペアは、SSHv2 サーバで使用できます。その逆の場合も同様です。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力したあとで CLI エラー メッセージが表示される場合は、RSA キー ペアが生成されていません。ホスト名とドメインを再設定したあと、**crypto key generate rsa** コマンドを入力してください。詳細については、「SSH を実行するためのスイッチの設定」（P.11-46）を参照してください。
- RSA キー ペアを生成するとき、[No host name specified] というメッセージが表示される場合があります。その場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キー ペアを生成するとき、[No domain specified] というメッセージが表示される場合があります。その場合は、**ip domain-name** 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 IP ドメイン名を設定する必要があります。

- ローカル認証および認可認証方式を設定するときは、コンソールで AAA がディセーブルになっていることを確認してください。

SSH を実行するためのスイッチの設定

SSH を実行するようにスイッチを設定するには、次の手順を実行します。

1. Cisco.com から暗号化ソフトウェア イメージをダウンロードします。このステップは必須です。詳細については、このリリースに対応するリリース ノートを参照してください。
2. スイッチのホスト名と IP ドメイン名を設定します。スイッチを SSH サーバとして設定する場合にだけ、この手順を実行してください。
3. スイッチの RSA キー ペアを生成します。SSH が自動的にイネーブルになります。スイッチを SSH サーバとして設定する場合にだけ、この手順を実行してください。
4. ローカルまたはリモート アクセス用にユーザ認証を設定します。このステップは必須です。詳細については、「ローカルな認証と認可のためのスイッチの設定」（P.11-43）を参照してください。

ホスト名と IP ドメイン名を設定し、RSA キー ペアを生成するには、特権 EXEC モードで次の手順を実行します。この手順は、スイッチを SSH サーバとして設定する場合に必要です。

	コマンド	目的
ステップ 1	**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 2	**hostname** *hostname*	スイッチのホスト名を設定します。
ステップ 3	**ip domain-name** *domain_name*	スイッチのホスト ドメインを設定します。
ステップ 4	**crypto key generate rsa**	スイッチでローカルおよびリモート認証用の SSH サーバをイネーブルにして、RSA キー ペアを生成します。 最小モジュール サイズを 1024 ビットにすることを推奨します。 RSA キーを生成するときに、モジュールの長さの入力を求められます。モジュールを長くするほど安全性は高くなりますが、生成および使用するときの時間が長くなります。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチの SSH サーバのステータスを表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

RSA キー ペアを削除するには、**crypto key zeroize rsa** 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。RSA キー ペアを削除すると、SSH サーバは自動的にディセーブルになります。

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**ip ssh version** [**1** | **2**]	（任意）SSH バージョン 1 または SSH バージョン 2 を実行するようにスイッチを設定します。 • **1**：SSH バージョン 1 を実行するようにスイッチを設定します。 • **2**：SSH バージョン 2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合は、SSH サーバは SSH クライアントがサポートする最新の SSH バージョンを選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}	SSH 制御パラメータを設定します。 • タイムアウト値を秒単位で指定します。デフォルト値は 120 秒です。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されたあとは、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク経由での複数の CLI ベース セッション用に、最大で 5 つの暗号化 SSH 接続を同時に使用できます（セッション 0 からセッション 4）。実行シェルが開始したあと、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントがサーバに対して再認証できる回数を指定します。デフォルト値は 3 で、指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定するときは、このステップを繰り返します。
ステップ 4	**line vty** *line_number* [*ending_line_number*] **transport input ssh**	（任意）仮想端末回線の設定を指定します。 • ライン コンフィギュレーション モードを開始して、仮想端末回線の設定を行います。*line_number* と *ending_line_number* には、回線のペアを指定します。指定できる範囲は 0 ～ 15 です。 • スイッチが SSH ではない Telnet 接続を拒否するように指定します。これにより、ルータを SSH 接続だけに制限します。
ステップ 5	**end**	特権 EXEC モードに戻ります。
ステップ 6	**show ip ssh** または **show ssh**	SSH サーバのバージョンおよび設定情報を表示します。 スイッチの SSH サーバ接続のステータスを表示します。
ステップ 7	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

デフォルトの SSH 制御パラメータに戻すには、**no ip ssh** {**timeout** | **authentication-retries**} 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。

SSH の設定とステータスの表示

SSH サーバの設定とステータスを表示するには、表 11-6 に示す 1 つまたは複数の特権 EXEC コマンドを使用します。

表 11-6　SSH サーバの設定とステータスを表示するためのコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、次の URL にある『*Cisco IOS Security Command Reference, Cisco IOS Release 12.2*』の「Other Security Features」の「Secure Shell Commands」を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cd.html

Secure Socket Layer HTTP 用のスイッチの設定

ここでは、HTTP 1.1 のサーバおよびクライアントに対して Secure Socket Layer（SSL）バージョン 3.0 のサポートを設定する方法を説明します。SSL は、サーバ認証、暗号化、メッセージ整合性、および HTTP クライアント認証の機能を備え、セキュアな HTTP 通信を可能にします。この機能を使用するには、暗号化ソフトウェア イメージをスイッチにインストールする必要があります。この機能を使用したり、暗号化ソフトウェアのファイルを Cisco.com からダウンロードしたりするには、許可を得る必要があります。暗号化イメージの詳細については、このリリースに対応するリリース ノートを参照してください。

ここでは、次の情報について説明します。

- 「セキュア HTTP サーバおよびクライアントの概要」（P.11-48）
- 「セキュア HTTP サーバおよびクライアントの設定」（P.11-50）
- 「セキュア HTTP のサーバとクライアントのステータスの表示」（P.11-54）

ここで使用する設定例やコマンドの構文および使用方法の詳細については、次の URL にある Cisco IOS Release 12.2(15)T の「HTTPS：HTTP Server and Client with SSL 3.0」の機能説明を参照してください。
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a008015a4c6.html

セキュア HTTP サーバおよびクライアントの概要

セキュアな HTTP 接続では、HTTP サーバとの間でやり取りされるデータは、インターネット上で送信される前に暗号化されます。SSL 暗号化を使用する HTTP が提供するセキュアな接続を使用すると、Web ブラウザからのスイッチの設定のような機能が可能になります。セキュア HTTP サーバおよびセキュア HTTP クライアントのシスコによる実装では、SSL バージョン 3.0 の実装とアプリケーション層の暗号化を使用します。HTTP over SSL は HTTPS と略されます。セキュアな接続の URL は、http:// ではなく https:// で始まります。

HTTP セキュア サーバ（スイッチ）の主な役割は、指定されているポート（デフォルトの HTTPS ポートは 443）で HTTPS 要求を待ち受けて、要求を HTTP 1.1 Web サーバに渡すことです。HTTP 1.1 サーバは要求を処理して応答（ページ）を HTTP セキュア サーバに返送し、HTTP セキュア サーバは元の要求に応答します。

HTTP セキュア クライアント（Web ブラウザ）の主な役割は、HTTPS ユーザ エージェント サービスに対する Cisco IOS アプリケーション要求に応答し、アプリケーションに対して HTTPS ユーザ エージェント サービスを実行し、応答をアプリケーションに戻すことです。

認証局のトラストポイント

Certificate Authority（CA; 認証局）は、証明書の要求を管理し、参加しているネットワーク装置に証明書を発行します。これらのサービスは、参加している装置のためにセキュリティ キーと証明書を一元的に管理します。特定の CA サーバは*トラストポイント*と呼ばれます。

接続が試みられると、HTTPS サーバは指定された CA トラストポイントから取得した認証済みの X.509v3 証明書をクライアントに発行することで、セキュアな接続を提供します。これに対し、クライアント（通常は Web ブラウザ）は、証明書を認証できる公開キーを持っています。

セキュアな HTTP 接続のために、CA トラストポイントを設定することを強く推奨します。HTTPS サーバを実行する装置に対して CA トラストポイントを設定しないと、サーバは自分自身を認証し、必要な RSA キー ペアを生成します。自己認証（自己署名）された証明書は十分なセキュリティを提供しないので、接続しているクライアントは証明書が自己認証されていることを示す通知を生成し、ユーザは接続を許可または拒否できます。このオプションは、内部ネットワーク トポロジ（テスト用など）に適しています。

CA トラストポイントを設定していない場合、セキュア HTTP 接続をイネーブルにすると、セキュア HTTP サーバ（またはクライアント）用の一時的または永続的な自己署名証明書が、自動的に生成されます。

- スイッチにホスト名およびドメイン名を設定していない場合は、一時的な自己署名証明書が生成されます。スイッチが再起動した場合、一時的な自己署名証明書は失われ、新しい一時的な自己署名証明書が割り当てられます。
- スイッチにホスト名とドメイン名を設定してある場合は、永続的な自己署名証明書が生成されます。この証明書は、スイッチを再起動した場合、またはセキュア HTTP サーバをディセーブルにした場合でもアクティブ状態のままになり、次にセキュア HTTP 接続を再びイネーブルにするとまだ存在しています。

（注） 認証局およびトラストポイントは、装置ごとに個別に設定する必要があります。他の装置からコピーしても、コピー先のスイッチでは無効になります。

自己署名証明書が生成されている場合、この情報は **show running-config** 特権 EXEC コマンドの出力に含まれます。次の例は、このコマンドからの出力で自己署名証明書が表示されている部分です。

```
Switch# show running-config
Building configuration...

<output truncated>

crypto pki trustpoint TP-self-signed-3080755072
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3080755072
 revocation-check none
 rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
 certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109

<output truncated>
```

セキュア HTTP サーバをディセーブルにし、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで、この自己署名証明書を削除できます。あとでセキュア HTTP サーバを再びイネーブルにすると、新しい自己署名証明書が生成されます。

（注）　*TP self-signed* に続く値は、装置のシリアル番号によって決まります。

オプションのコマンド（**ip http secure-client-auth**）を使用することで、HTTPS サーバからクライアントに X.509v3 証明書を要求できます。クライアントを認証すると、サーバがそれ自体で認証するよりもセキュリティが向上します。

認証局の詳細については、Cisco.com ページの [Documentation] > [Cisco IOS Software] > [12.2 Mainline] > [Command References] にある『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Configuring Certification Authority Interoperability」を参照してください。

CipherSuite

CipherSuite は、SSL 接続で使用する暗号化アルゴリズムとダイジェスト アルゴリズムを指定します。HTTPS サーバに接続するときに、クライアントの Web ブラウザはサポートされる CipherSuite のリストを提供し、クライアントとサーバはリストの中で両方がサポートするものから最善の暗号化アルゴリズムを使用するようにネゴシエートします。たとえば、Netscape Communicator 4.76 は、RSA 公開キー暗号化、MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC の U.S. セキュリティをサポートします。

可能な最善の暗号化を使用するには、Microsoft Internet Explorer Version 5.5（またはそれ以降）や Netscape Communicator Version 4.76（またはそれ以降）などの 128 ビット暗号化をサポートするクライアント ブラウザを使用する必要があります。SSL_RSA_WITH_DES_CBC_SHA CipherSuite は、128 ビット暗号化ではないので、他の CipherSuite よりもセキュリティが劣ります。

より安全で複雑な CipherSuite ほど、必要な処理時間が長くなります。次に、スイッチがサポートする CipherSuite を、ルータの処理（速度）が速いものから遅いものの順に示します。

1. SSL_RSA_WITH_DES_CBC_SHA：メッセージの暗号化には DES-CBC を使用し、メッセージのダイジェストには SHA を使用する RSA キー交換（RSA 公開キー暗号化）
2. SSL_RSA_WITH_RC4_128_MD5：RC4 128 ビット暗号化と MD5 のメッセージ ダイジェストを使用する RSA キー交換
3. SSL_RSA_WITH_RC4_128_SHA：RC4 128 ビット暗号化と SHA のメッセージ ダイジェストを使用する RSA キー交換
4. SSL_RSA_WITH_3DES_EDE_CBC_SHA：メッセージの暗号化には 3DES と DES-EDE3-CBC を使用し、メッセージのダイジェストには SHA を使用する RSA キー交換

RSA は（指定されている暗号化とダイジェスト アルゴリズムの組み合わせとともに）、キーの生成と、SSL 接続での認証の両方に使用されます。この使用方法は、CA トラストポイントが設定されているかどうかには関係ありません。

セキュア HTTP サーバおよびクライアントの設定

SSL のデフォルト設定

標準 HTTP サーバはイネーブルです。

SSL はイネーブルです。

CA トラストポイントは設定されていません。

自己署名証明書は生成されません。

SSL 設定時の注意事項

SSL がスイッチ クラスタで使用されると、SSL セッションはクラスタ コマンダで終了します。クラスタ メンバー スイッチは標準 HTTP を実行する必要があります。

CA トラストポイントを設定する前に、システム クロックを設定する必要があります。クロックが設定されていない場合は、日付が正しくないために証明書が拒否されます。

CA トラストポイントの設定

セキュアな HTTP 接続のために、正式な CA トラストポイントを設定することを推奨します。CA トラストポイントの方が自己署名証明書よりも安全です。

CA トラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**hostname** *hostname*	スイッチのホスト名を指定します（ホスト名をまだ設定していない場合に限り必要）。ホスト名はセキュリティ キーと証明書のために必要です。
ステップ 3	**ip domain-name** *domain-name*	スイッチの IP ドメイン名を指定します（IP ドメイン名をまだ設定していない場合に限り必要）。ドメイン名はセキュリティ キーと証明書のために必要です。
ステップ 4	**crypto key generate rsa**	（任意）RSA キー ペアを生成します。スイッチの証明書を取得するには、先に RSA キー ペアが必要です。RSA キー ペアは自動的に生成されます。このコマンドを使用すると、必要な場合にキーを再生成できます。
ステップ 5	**crypto ca trustpoint** *name*	CA トラストポイントのローカル設定名を指定して、CA トラストポイント コンフィギュレーション モードを開始します。
ステップ 6	**enrollment url** *url*	スイッチが証明書要求を送信する宛先の URL を指定します。
ステップ 7	**enrollment http-proxy** *host-name port-number*	（任意）HTTP プロキシ サーバ経由で CA から証明書を取得するようにスイッチを設定します。
ステップ 8	**crl query** *url*	Certificate Revocation List（CRL; 証明書失効リスト）を要求してピアの証明書が失効していないことを確認するように、スイッチを設定します。
ステップ 9	**primary**	（任意）トラストポイントを CA 要求のプライマリ（デフォルト）トラストポイントとして使用するように指定します。
ステップ 10	**exit**	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto ca authentication** *name*	CA の公開キーを取得して CA を認証します。ステップ 5 で使用したものと同じ名前を使用します。
ステップ 12	**crypto ca enroll** *name*	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キー ペアの署名付き証明書を要求します。

	コマンド	目的
ステップ 13	**end**	特権 EXEC モードに戻ります。
ステップ 14	**show crypto ca trustpoints**	設定を確認します。
ステップ 15	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

CA と関連付けられているすべての ID 情報および証明書を削除するには、**no crypto ca trustpoint** *name* 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。

セキュア HTTP サーバの設定

証明書に認証局を使用している場合は、HTTP サーバをイネーブルにする前に、前記の手順を使用してスイッチに CA トラストポイントを設定する必要があります。CA トラストポイントを設定していない場合は、セキュア HTTP サーバを初めてイネーブルにしたときに、自己署名証明書が生成されます。サーバを設定したあとは、標準とセキュアの両方の HTTP サーバに適用されるオプション（パス、適用するアクセス リスト、最大接続数、タイムアウト ポリシー）を設定できます。

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的

ステップ 1	**show ip http server status**	（任意）HTTP サーバのステータスを表示し、セキュア HTTP サーバ機能がソフトウェアでサポートされているかどうかを確認します。出力に次のいずれかの行が表示される必要があります。
		`HTTP secure server capability: Present`
		`or`
		`HTTP secure server capability: Not present`

ステップ 2	**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	**ip http secure-server**	ディセーブルになっている場合は、HTTPS サーバをイネーブルにします。HTTPS サーバはデフォルトでイネーブルになっています。
ステップ 4	**ip http secure-port** *port-number*	（任意）HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。有効なオプションは、443 または 1025 ～ 65535 の範囲の任意の値です。
ステップ 5	**ip http secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する必要がない場合は、サーバとクライアントに両方がサポートする CipherSuite をネゴシエートさせます。これはデフォルトです。
ステップ 6	**ip http secure-client-auth**	（任意）接続処理の間に認証用の X.509v3 証明書をクライアントに要求するように HTTP を設定します。デフォルトでは、クライアントはサーバに証明書を要求しますが、サーバはクライアントの認証を試みません。
ステップ 7	**ip http secure-trustpoint** *name*	X.509v3 セキュリティ証明書を取得し、クライアントの証明書接続を認証するために使用する CA トラストポイントを指定します。 **（注）**　このコマンドを使用する場合は、前記の手順に従って CA トラストポイントをすでに設定してあるものと見なされます。
ステップ 8	**ip http path** *path-name*	（任意）HTML ファイルのベース HTTP パスを設定します。このパスでは、ローカル システム上の HTTP サーバ ファイルの場所を指定します（通常はシステムのフラッシュ メモリにあります）。
ステップ 9	**ip http access-class** *access-list-number*	（任意）HTTP サーバへのアクセスを許可するために使用するアクセス リストを指定します。

	コマンド	目的
ステップ 10	**ip http max-connections** *value*	（任意）HTTP サーバに対して許可する同時接続の最大数を設定します。指定できる範囲は 1 ～ 16 です。デフォルト値は 5 です。
ステップ 11	**ip http timeout-policy idle** *seconds* **life** *seconds* **requests** *value*	（任意）定義されている状況で HTTP サーバへの接続を開いておくことのできる時間の長さを指定します。 • **idle**：データを受信しない、または応答を送信できない状態の最大時間。指定できる範囲は 1 ～ 600 秒です。デフォルト値は 180 秒（3 分）です。 • **life**：接続が確立されてからの最大時間。指定できる範囲は 1 ～ 86400 秒（24 時間）です。デフォルト値は 180 秒です。 • **requests**：持続している接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。
ステップ 12	**end**	特権 EXEC モードに戻ります。
ステップ 13	**show ip http server secure status**	HTTP セキュア サーバのステータスを表示して、設定を確認します。
ステップ 14	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

標準 HTTP サーバをディセーブルにするには、**no ip http server** 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。セキュア HTTP サーバをディセーブルにするには、**no ip http secure-server** 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。デフォルト設定に戻すには、**no ip http secure-port** および **no ip http secure-ciphersuite** 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。クライアント認証を不要にするには、**no ip http secure-client-auth** 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。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、https://*URL* と入力します。URL は、サーバ スイッチの IP アドレスまたはホスト名です。デフォルト ポート以外のポートを設定した場合は、URL の後ろにポート番号も指定する必要があります。次に例を示します。

```
https://209.165.129:1026
```
または

```
https://host.domain.com:1026
```

セキュア HTTP クライアントの設定

標準 HTTP クライアントとセキュア HTTP クライアントは、常にイネーブルになっています。セキュア HTTP クライアント証明書には、認証局が必要です。次の手順では、すでにスイッチに CA トラストポイントを設定してあるものと見なされます。CA トラストポイントが設定されておらず、リモート HTTPS サーバでクライアント認証が必要な場合は、セキュア HTTP クライアントへの接続は失敗します。

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**ip http client secure-trustpoint** *name*	（任意）リモート HTTP サーバがクライアントの認証を要求する場合は、使用する CA トラストポイントを指定します。このコマンドを使用する場合は、前記の手順を使用して CA トラストポイントをすでに設定してあるものと見なされます。クライアント認証が必要ない場合、またはプライマリ トラストポイントが設定されている場合は、このコマンドは任意です。

	コマンド	目的
ステップ 3	**ip http client secure-ciphersuite** {[**3des-ede-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**des-cbc-sha**]}	（任意）HTTPS 接続の暗号化に使用する CipherSuite（暗号化アルゴリズム）を指定します。特定の CipherSuite を指定する必要がない場合は、サーバとクライアントに両方がサポートする CipherSuite をネゴシエートさせます。これはデフォルトです。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ip http client secure status**	HTTP セキュア サーバのステータスを表示して、設定を確認します。
ステップ 6	**copy running-config startup-config**	（任意）設定をコンフィギュレーション ファイルに保存します。

クライアント トラストポイントの設定を削除するには、**no ip http client secure-trustpoint** *name* を使用します。クライアントに事前に設定されている CipherSuite の指定を削除するには、**no ip http client secure-ciphersuite** を使用します。

セキュア HTTP のサーバとクライアントのステータスの表示

SSL セキュア サーバおよびクライアントのステータスを表示するには、表 11-7 に示す特権 EXEC コマンドを使用します。

表 11-7　SSL セキュア サーバおよびクライアントのステータスを表示するためのコマンド

コマンド	目的
show ip http client secure status	HTTP セキュア クライアントの設定を表示します。
show ip http server secure status	HTTP セキュア サーバの設定を表示します。
show running-config	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

Secure Copy Protocol 用のスイッチの設定

Secure Copy Protocol（SCP）機能は、スイッチの設定またはスイッチのイメージ ファイルをコピーするためのセキュアで認証された方法を提供します。SCP は、Berkeley r-tools の代わりのセキュアな方式を提供するアプリケーションとプロトコルであるセキュア シェル（SSH）に依存します。

SSH を使用するには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは、セキュアな転送を SSH に依存する SCP と同じです。

SSH は AAA 認証に依存し、SCP も AAA 認可に依存するので、正しく設定する必要があります。

- SCP をイネーブルにする前に、スイッチに SSH、認証、および認可を正しく設定する必要があります。
- SCP はセキュアな転送を SSH に依存するので、ルータには Rivest、Shamir、Adelman（RSA）キー ペアが必要です。

（注） SCP を使用するときは、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときにパスワードを入力する必要があります。

セキュア コピーの概要

セキュア コピー機能を設定するには、次の概念を理解しておく必要があります。

SCP の動作は、Berkeley r-tools スイートに含まれるリモート コピー（rcp）の動作と似ていますが、SCP はセキュリティを SSH に依存します。また、SCP では、ユーザが正しい権限レベルを持っているかどうかをルータが判断できるように、認証、認可、アカウンティング（AAA）認可を設定する必要もあります。

適切な認可を持っているユーザは、SCP の **copy** コマンドを使用してスイッチとの間で Cisco IOS File System（IFS; IOS ファイル システム）の任意のファイルをコピーできます。認可された管理者は、ワークステーションからこれを行うこともできます。

SCP の設定および確認方法の詳細については、次の URL にある『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』の「Secure Copy Protocol」を参照してください。
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_secure_copy_ps6350_TSD_Products_Configuration_Guide_Chapter.html