



スイッチベースの認証の設定

この章では、Cisco ME 3400E スイッチでスイッチベースの認証を設定する方法について説明します。

- 「スイッチへの不正アクセスの防止」(P.8-1)
- 「特権 EXEC コマンドへのアクセスの保護」(P.8-2)
- 「TACACS+ によるスイッチ アクセスの制御」(P.8-10)
- 「RADIUS によるスイッチ アクセスの制御」(P.8-17)
- 「Kerberos によるスイッチ アクセスの制御」(P.8-32)
- 「スイッチのローカル認証および許可の設定」(P.8-36)
- 「Secure Shell のためのスイッチの設定」(P.8-37)
- 「SCP のためのスイッチの設定」(P.8-42)

スイッチへの不正アクセスの防止

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

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

- 最低限のセキュリティとして、各スイッチポートでパスワードおよび権限を設定します。このパスワードは、スイッチでローカルに保存されます。ユーザがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。詳細については、「[特権 EXEC コマンドへのアクセスの保護](#)」(P.8-2) を参照してください。
- 追加のセキュリティレイヤとして、ユーザ名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベル（対応する権利および権限付き）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.8-7) 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する際に、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティサーバ上のデータベースに保存できます。これにより、複数のネットワークデバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。詳細については、「[TACACS+ によるスイッチアクセスの制御](#)」(P.8-10) を参照してください。

特権 EXEC コマンドへのアクセスの保護

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



(注)

ここで説明す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。

- 「デフォルトのパスワードおよび権限レベル設定」 (P.8-2)
- 「スタティック イネーブル パスワードの設定または変更」 (P.8-3)
- 「暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護」 (P.8-3)
- 「パスワード回復のディセーブル化」 (P.8-5)
- 「端末回線に対する Telnet パスワードの設定」 (P.8-6)
- 「ユーザ名とパスワードのペアの設定」 (P.8-7)
- 「複数の権限レベルの設定」 (P.8-7)

デフォルトのパスワードおよび権限レベル設定

表 8-1 に、デフォルトのパスワードおよび権限レベル設定を示します。

表 8-1 デフォルトのパスワードおよび権限レベル

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

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 <i>password</i>	<p>特権 EXEC モードのアクセス用に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。</p> <p>デフォルトでは、パスワードは定義されていません。</p> <p><i>password</i> には、1 ~ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符 (?) は、パスワードを作成する場合に、疑問符の前にキーの組み合わせ Ctrl+v キーを押せば使用できます。たとえば、パスワード abc?123 を作成するときは、次のようにします。</p> <p>abc を入力します。</p> <p>Ctrl+v キーを押します。</p> <p>?123 を入力します。</p> <p>システムからイネーブル パスワードを入力するよう求められた場合、疑問符の前に Ctrl+v キーを押す必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。</p>
ステップ 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	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p> <p>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 ファイル内では読み取ることができる状態です。</p>

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 **11u2c3k4y5** に変更する例を示します。パスワードは暗号化されておらず、レベル 15 のアクセスが与えられます (従来の特権 EXEC モード アクセス)。

```
Switch(config)# enable password 11u2c3k4y5
```

暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

追加のセキュリティ レイヤを、特にネットワークを越えるパスワードや Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバに保存されているパスワードに対して設定する場合には、**enable password** または **enable secret** の各グローバル コンフィギュレーション コマンドを使用できます。両コマンドはともに同じ働きをします。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード (デフォルト設定) または特定の権限レベルにアクセスするには、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムを使用しているため、**enable secret** コマンドを使用することを推奨します。

■ 特権 EXEC コマンドへのアクセスの保護

enable secret コマンドは **enable password** コマンドに優先します。2 つのコマンドが同時に有効になることはありません。

イネーブルおよびイネーブル シークレット パスワードに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} または enable secret [level level] {password encryption-type encrypted-password}	<p>特権 EXEC モードのアクセス用に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。</p> <p>または</p> <p>シークレット パスワードを定義し、非可逆暗号方式を使用して保存します。</p> <ul style="list-style-type: none"> • (任意) <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルトレベルは 15 です (特権 EXEC モード権限)。 • <i>password</i> には、1 ~ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。 • (任意) <i>encryption-type</i> には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか指定できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチ コンフィギュレーションからコピーしたものです。 <p>(注) 暗号化タイプを指定してクリア テキスト パスワードを入力した場合は、再度特権 EXEC モードを開始することはできません。暗号化されたパスワードが不明になった場合、どのような方法でも回復できません。</p>
ステップ 3 service password-encryption	<p>(任意) パスワードを定義するとき、またはコンフィギュレーションを保存するときに、パスワードを暗号化します。</p> <p>暗号化によって、コンフィギュレーション ファイルのパスワードが読み取り不能になります。</p>
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) コンフィギュレーション ファイルに設定を保存します。

イネーブル パスワードおよびイネーブル シークレット パスワードの両方が定義されている場合、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。

特定の権限レベルのパスワードを定義するには、キーワード **level** を使用します。レベルを指定してパスワードを設定したら、そのレベルでアクセスする必要のあるユーザだけにそのパスワードを付与してください。さまざまなレベルでアクセス可能なコマンドを指定する場合は、**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.8-7)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、認証鍵パスワード、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]** 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。

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、スイッチに物理アクセスするすべてのエンドユーザは、スイッチの電源投入時にブートプロセスを中断して新しいパスワードを入力することで、失われたパスワードを回復できます。

パスワード回復ディセーブル機能では、この機能の一部をディセーブルにすることにより、スイッチパスワードへのアクセスを防止します。この機能がイネーブルな場合、エンドユーザはシステムをデフォルト設定に戻すことに同意するだけで、ブートプロセスを中断することができます。パスワード回復をディセーブル化しても、ブート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.txt) および VLAN (仮想 LAN) 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、エンドユーザがブートプロセスを中断してシステムをデフォルト値に戻す場合に備えて、セキュアサーバ上にコンフィギュレーションファイルのバックアップコピーを保管しておいてください。スイッチ上にコンフィギュレーションファイルのバックアップコピーを保管しないでください。また、セキュアサーバ上に VLAN データベースファイルのバックアップコピーも保管しておくことを推奨します。スイッチがシステムのデフォルト設定に戻ると、XMODEM プロトコルを使用して、保存したファイルを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.46-3) 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、フラッシュメモリのブートローダがアクセスできる領域および Cisco IOS イメージに保存されます。ただし、ファイルシステムの領域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設定している場合は、パスワード回復をディセーブルにできません。このコマンドにより、スイッチの電源再投入後に、ブート ロード プロンプト (*switch:*) が表示されます。

端末回線に対する Telnet パスワードの設定

初めてスイッチに電源を投入すると、自動セットアップ プログラムが起動して IP 情報を割り当て、引き続き使用するためのデフォルト設定を作成します。セットアップ プログラムは、パスワードによる Telnet アクセス用にスイッチを設定するように求めてきます。このとき、セットアップ プログラムを使用して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。

スイッチを Telnet アクセス用に設定するには、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 ソフトウェアをインストールした PC またはワークステーションと、スイッチのコンソール ポートを接続します。 コンソール ポートのデフォルトのデータ特性は、9600 ボー、8 データビット、1 ストップ ビット、パリティなしです。コマンドライン プロンプトを表示させるため、Return キーを数回押さなければならない場合があります。
ステップ 2	enable password <i>password</i>	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は、最大 16 のセッションが可能です。0 および 15 を指定することは、使用できる 16 個の Telnet セッションを全部設定することを意味します。
ステップ 5	password <i>password</i>	1 つまたは複数の回線の Telnet パスワードを入力します。 <i>password</i> には、1 ~ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。
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。 コマンド line vty 0 15 の下にパスワードが表示されます。
ステップ 8	copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

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。

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

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。この認証システムは、ログインユーザ名とパスワードを要求します。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>username name [privilege level] {password encryption-type password}</code>	各ユーザのユーザ名、権限レベル、パスワードを入力します。 <ul style="list-style-type: none"> <code>name</code> には、ユーザ ID を 1 ワードで指定します。スペースや引用符は使用できません。 (任意) <code>level</code> には、アクセス後ユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では、ユーザ EXEC モードでのアクセスとなります。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。 <code>encryption-type</code> には、暗号化されていないパスワードがあとに続く場合は 0 を指定します。暗号化されたパスワードがあとに続く場合は 7 を指定します。 <code>password</code> には、ユーザがスイッチにアクセスする場合に入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<code>username</code> コマンドの最後のオプションとして指定します。
ステップ 3	<code>line console 0</code> または <code>line vty 0 15</code>	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	<code>login local</code>	ログイン時のローカル パスワード チェックをイネーブルにします。認証は、ステップ 2 で指定されたユーザ名に基づきます。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	設定を確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

特定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。パスワードチェックをディセーブルにし、パスワードなしでの接続を可能にするには、`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 ソフトウェアは、デフォルトで、ユーザ EXEC と特権 EXEC という 2 種類のパスワードセキュリティ モードを備えています。各モードについて、コマンドの階層レベルを最大 16 まで設定できます。複数のパスワードを設定することにより、さまざまなユーザ グループに対して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、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル 2 のセキュリティを割り当て、レベル 2 のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセスをより制限されたものにしたい場合は、レベル 3 のセキュリティを割り当て、そのパスワードを限られたユーザ グループに配布することもできます。

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」(P.8-8)
- 「回線に対するデフォルトの権限レベルの変更」(P.8-9)
- 「権限レベルへのログインおよび終了」(P.8-9)

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。 <ul style="list-style-type: none"> • <i>mode</i> には、グローバル コンフィギュレーション モードの場合は configure を、EXEC モードの場合は exec を、インターフェイス コンフィギュレーション モードの場合は interface を、ライン コンフィギュレーション モードの場合は line を、それぞれ入力します。 • <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限用です。レベル 15 は、enable パスワードによって許可されるアクセス レベルです。 • <i>command</i> には、アクセスを制限したいコマンドを指定します。
ステップ 3 enable password level level password	権限レベルのイネーブル パスワードを指定します。 <ul style="list-style-type: none"> • <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限用です。 • <i>password</i> には、1 ~ 25 文字の英数字の文字列を指定します。文字列は数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されていません。
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。 show running-config コマンドはパスワードとアクセス レベルの設定を表示します。 show privilege 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) コンフィギュレーション ファイルに設定を保存します。

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル 15 に設定すると、**show** コマンドおよび **show ip** コマンドは、個々に別のレベルに設定しないかぎり、自動的にレベル 15 に設定されます。

特定のコマンドについて、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。

configure コマンドを権限レベル 14 に設定し、レベル 14 コマンドを使用する場合にユーザが入力す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
```

回線に対するデフォルトの権限レベルの変更

回線に対する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	回線のデフォルト権限レベルを変更します。 <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限用です。レベル 15 は、 enable パスワードによって許可されるアクセス レベルです。
ステップ 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。 show running-config コマンドはパスワードとアクセス レベルの設定を表示します。 show privilege 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) コンフィギュレーション ファイルに設定を保存します。

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

回線の権限レベルをデフォルトに戻すには、**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および終了

特定の権限レベルにログインし、特定の権限レベルを終了するには、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	特定の権限レベルにログインします。 <i>level</i> に指定できる範囲は 0 ~ 15 です。
ステップ 2	disable level	特定の権限レベルを終了します。 <i>level</i> に指定できる範囲は 0 ~ 15 です。

TACACS+ によるスイッチ 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について説明します。TACACS+ は、詳細なアカウント情報収集、認証および許可プロセスに対して柔軟な管理を行います。TACACS+ は、Authentication, Authorization, Accounting (AAA; 認証、認可、アカウント管理) 機能が拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用します。



(注)

ここで説明す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.8-10)
- 「TACACS+ の動作」 (P.8-12)
- 「TACACS+ の設定」 (P.8-12)
- 「TACACS+ 設定の表示」 (P.8-17)

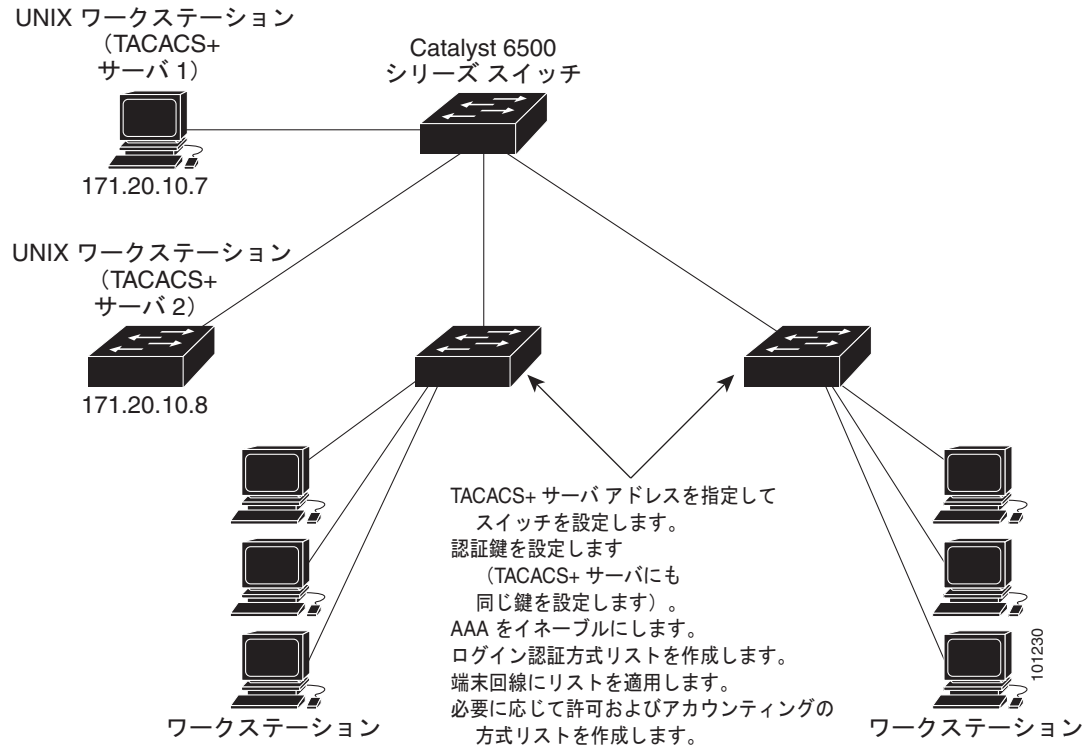
TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザの検証を集中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、通常 UNIX または Windows NT ワークステーション上で稼動する TACACS+ デモンのデータベースで管理されます。スイッチに TACACS+ 機能を設定するには、TACACS+ サーバにアクセスして設定する必要があります。

TACACS+ は、個別のモジュール型認証、認可、およびアカウント管理機能を備えています。TACACS+ により、単一のアクセス制御サーバ (TACACS+ デモン) が各サービス (認証、認可、アカウント管理) を個別に提供できます。各サービスを固有のデータベースに結合し、デモンの機能に応じてそのサーバまたはネットワークで利用できる他のサービスを使用することができます。

TACACS+ の目的は、1 つ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方式を提供することです。スイッチは、他のシスコ製ルータやアクセス サーバとともにネットワーク アクセス サーバにすることができます。ネットワーク アクセス サーバは、単一のユーザ、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との接続を実現します (図 8-1 を参照)。

図 8-1 一般的な TACACS+ ネットワーク構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワード ダイアログ、チャレンジおよび応答、メッセージ サポートによって認証の総合的な制御を行います。

認証機能では、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が入力されたあと、自宅の住所、母親の旧姓、サービス タイプ、社会保険番号などのいくつかの質問をすることによりユーザを試す）。TACACS+ 認証サービスは、ユーザ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間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：オートコマンド、アクセス制御、セッション期間、プロトコル サポートの設定といった、ユーザ セッション内のユーザ機能についてきめ細かい制御を行います。また、TACACS+ 許可機能によって、ユーザが実行できるコマンドを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て TACACS+ デーモンに送信します。ネットワークの管理者は、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活動状況を追跡したり、ユーザ課金用の情報を提供したりすることができます。アカウンティング レコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP [ポイントツーポイント プロトコル] など）、パケット数、およびバイト数が記録されます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモンとの間の認証を行い、スイッチと TACACS+ デーモンとの間のプロトコル交換をすべて暗号化することにより機密保持を実現します。

スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼動するシステムが必要です。

TACACS+ の動作

ユーザが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立すると、スイッチは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これがユーザに表示されます。ユーザがユーザ名を入力すると、スイッチは TACACS+ デーモンに接続してパスワードプロンプトを取得します。スイッチが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、そのパスワードが TACACS+ デーモンに送信されます。

TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。デーモンは、ユーザ名とパスワードの組み合わせを入力するよう指示しますが、ユーザの母親の旧姓など、その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 TACACS+ デーモンから次のいずれかの応答を受信します。
 - **ACCEPT** : ユーザが認証され、サービスを開始できます。許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、この時点で許可処理が開始されます。
 - **REJECT** : ユーザは認証されません。TACACS+ デーモンに応じて、ユーザはアクセスを拒否されるか、ログインシーケンスを再試行するよう求められます。
 - **ERROR** : デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。**ERROR** 応答が表示された場合は、スイッチは、通常別の方法でユーザを認証しようとします。
 - **CONTINUE** : ユーザは、さらに認証情報の入力を求められます。

認証後、スイッチで許可がイネーブルになっている場合、ユーザは追加の許可フェーズに入ります。ユーザはまず、TACACS+ 認証を正常に終了しなければ TACACS+ 許可に進めません。

3. TACACS+ 許可が必要な場合は、再度 TACACS+ デーモンに接続し、デーモンが **ACCEPT** または **REJECT** の許可応答を返します。**ACCEPT** 応答が返された場合は、その応答には、そのユーザの **EXEC** または **NETWORK** セッション宛てのアトリビュートの形式のデータ、およびユーザがアクセスできるサービスが含まれます。
 - Telnet、Secure Shell (SSH; セキュア シェル)、rlogin、または特権 EXEC サービス
 - 接続パラメータ (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)

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について説明します。少なくとも、TACACS+ デーモンを保持するホスト (複数可) を特定し、TACACS+ 認証の方式リストを定義する必要があります。任意で TACACS+ 許可およびアカウントの方式リストを定義することもできます。方式リストは、ユーザの認証、認可、およびアカウントを維持するための順序と方式を定義します。方式リストを使用すると、使用するセキュリティプロトコルを 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。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、アカウントの維持を行います。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方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストを使い果たすまで続きます。

aaa authorization console グローバル コンフィギュレーション コマンドによって、AAA および TACACS+ をコンソール ポート上で動作させることが可能です。

このコマンドについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter0918_6a00800ca6d8.html#wp1019867

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」 (P.8-13)
- 「TACACS+ サーバ ホストの特定と認証鍵の設定」 (P.8-13)
- 「TACACS+ ログイン認証の設定」 (P.8-14)
- 「特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定」 (P.8-16)
- 「TACACS+ アカウンティングの開始」 (P.8-16)

TACACS+ のデフォルト設定

TACACS+ と AAA は、デフォルトでディセーブルに設定されています。

セキュリティの失効を防止するために、ネットワーク管理アプリケーションを使用して TACACS+ を設定することは不可能です。TACACS+ をイネーブルに設定すると、CLI を使用してスイッチにアクセスするユーザを認証します。



(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 に設定された HTTP 接続を許可します。

TACACS+ サーバ ホストの特定と認証鍵の設定

認証用に 1 つのサーバを使用することも、既存のサーバ ホストをグループ化するために AAA サーバグループを使用するよう設定することもできます。設定済みサーバ ホストのサブセットを選択してサーバをグループ化し、特定のサービスに使用することが可能です。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、選択されたサーバホストの IP アドレスのリストを含んでいます。

IP ホストまたは TACACS+ サーバを保持するホストを特定し、任意で暗号鍵を設定するには、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 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>tacacs-server host hostname [port integer] [timeout integer] [key string]</code>	<p>TACACS+ サーバを保持する IP ホストまたはホストを識別します。このコマンドを複数回入力すると、優先ホストのリストが作成されます。ソフトウェアは、指定された順序でホストを検索します。</p> <ul style="list-style-type: none"> • <code>hostname</code> には、ホストの名前または IP アドレスを指定します。 • (任意) <code>port integer</code> には、サーバのポート番号を指定します。デフォルトはポート 49 です。指定できる範囲は 1 ~ 65535 です。 • (任意) <code>timeout integer</code> には、スイッチがデーモンからの応答を待つ時間を秒数で指定します。これを過ぎるとスイッチは時間切れとなりエラーを宣言します。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) <code>key string</code> には、スイッチと TACACS+ デーモンとの間のすべてのトラフィックを暗号化および暗号解除するための暗号鍵を指定します。暗号化が成功するには TACACS+ デーモンに同じ鍵を設定する必要があります。
ステップ 3 <code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
ステップ 4 <code>aaa group server tacacs+ group-name</code>	(任意) グループ名で AAA サーバ グループを定義します。 このコマンドによって、スイッチはサーバ グループ サブコンフィギュレーション モードになります。
ステップ 5 <code>server ip-address</code>	(任意) 特定の TACACS+ サーバを定義済みサーバ グループに対応付けます。AAA サーバ グループの各 TACACS+ サーバに対してこのステップを繰り返します。 グループの各サーバは、ステップ 2 で定義されている必要があります。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show tacacs</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

指定された 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。設定リストからサーバ 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作成してから、さまざまなポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行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（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストが明示的に定義されたポートを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

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るので、最初の方式が失敗した場合のバックアップ システムが確保されます。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すまで続きます。この処理のある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のユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行さ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 <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2 <code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
ステップ 3 <code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • <code>login authentication</code> 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されるデフォルトのリストを作成するには、キーワード default の後ろにデフォルト状況で使用す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。 • <code>list-name</code> には、作成するリストの名前として使用する文字列を指定します。 • <code>method1...</code> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> • 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、<code>enable password</code> 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あらかじめ定義しておく必要があります。 • group tacacs+ : TACACS+ 認証を使用します。この認証方式を使用するには、TACACS+ サーバをあらかじめ設定しておく必要があります。詳細については、「TACACS+ サーバホストの特定と認証鍵の設定」(P.8-13) 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、回線パスワードをあらかじめ設定しておく必要があります。<code>password password</code> 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しておく必要があります。<code>username password</code> 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 : 大文字と小文字を区別するローカル ユーザ名データベースを認証に使用します。<code>username name password</code> 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 <code>line [console tty vty] line-number [ending-line-number]</code>	ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。
ステップ 5 <code>login authentication {default list-name}</code>	<p>回線または回線セットに対して、認証リストを適用します。</p> <ul style="list-style-type: none"> • default を指定する場合は、<code>aaa authentication login</code> コマンドで作成したデフォルトのリストを使用します。 • <code>list-name</code> には、<code>aaa authentication login</code> コマンドで作成したリストを指定します。
ステップ 6 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 7 <code>show running-config</code>	設定を確認します。
ステップ 8 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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。ログインの TACACS+ 認証をディセーブルにするかデフォルト値に戻す場合は、**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。

特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

AAA 許可は、ユーザが利用できるサービスを制限します。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

aaa authorization グローバル コンフィギュレーション コマンドにキーワード **tacacs+** を付けて使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

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

- TACACS+ を使用して認証を行った場合は、特権 EXEC アクセス許可に TACACS+ を使用します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。



(注)

許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ユーザには、許可が省略されません。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、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+	ネットワーク関連のすべてのサービス要求に対するユーザ TACACS+ 許可をスイッチに設定します。
ステップ 3	aaa authorization exec tacacs+	特権 EXEC アクセスの有無を、ユーザ TACACS+ 許可によって判別するようにスイッチを設定します。 キーワード exec を指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返されることがあります。
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) コンフィギュレーション ファイルに設定を保存します。

許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+ アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスするサービスと、ユーザが消費するネットワーク リソースを追跡します。AAA アカウンティングがイネーブルに設定されていると、スイッチは、アカウンティング レコードの形式でユーザの活動状況を TACACS+ セキュリティ サーバにレポートします。

各アカウントレコードには、アカウントの AV のペアが含まれ、セキュリティ サーバ上に保存されます。このデータを分析し、ネットワーク管理、クライアントへの課金、または監査に使用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに関する TACACS+ 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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa accounting network start-stop tacacs+</code>	ネットワーク関連のすべてのサービス要求に対する TACACS+ アカウンティングをイネーブルにします。
ステップ 3	<code>aaa accounting exec start-stop tacacs+</code>	TACACS+ アカウンティングにより、特権 EXEC プロセスの開始時に記録開始アカウンティング通知、終了時に記録停止通知を送信するように設定します。
ステップ 4	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	設定を確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

アカウント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。

TACACS+ 設定の表示

TACACS+ サーバ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 によるスイッチ アクセスの制御

ここでは、RADIUS (Remote Authentication Dial-In User Service) をイネーブルにして設定する方法について説明します。RADIUS は、詳細なアカウント情報を収集し、認証および許可プロセスに対して柔軟な管理を行います。RADIUS は AAA を介して機能します。RADIUS をイネーブルするには AAA コマンドを使用します。



(注)

ここで説明す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。

- 「RADIUS の概要」 (P.8-18)
- 「RADIUS の動作」 (P.8-19)
- 「RADIUS の設定」 (P.8-20)
- 「RADIUS 設定の表示」 (P.8-32)

RADIUS の概要

RADIUS は分散型クライアント/サーバ システムで、不正なアクセスからネットワークを保護します。RADIUS クライアントは、サポートされているシスコ製ルータおよびスイッチ上で稼動し、中央 RADIUS サーバに認証要求を送信します。中央 RADIUS サーバには、すべてのユーザの認証およびネットワーク サービス アクセス情報が格納されています。RADIUS ホストは、通常、シスコ (Cisco Secure Access Control Server バージョン 3.0)、Livingston、Merit、Microsoft などのソフトウェア製造元の RADIUS サーバ ソフトウェアが稼動するマルチユーザ 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。

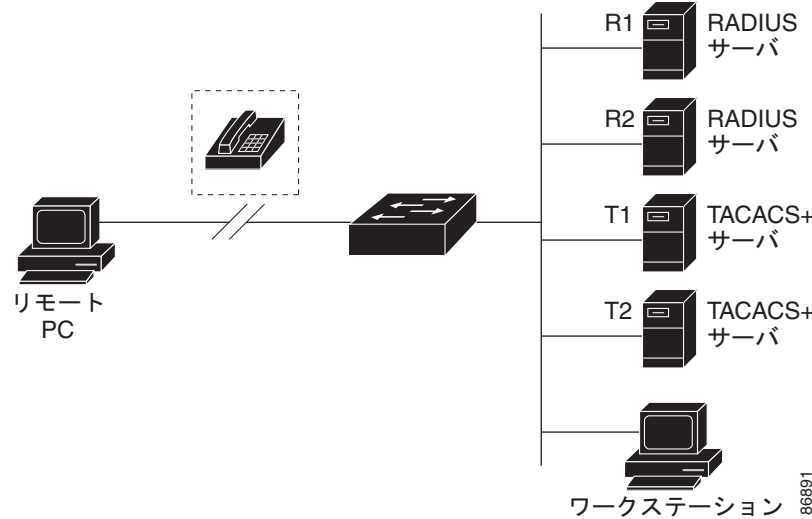
RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセス サーバが、1 つの RADIUS サーバベース セキュリティ データベースを使用します。複数のベンダーのアクセス サーバからなる IP ベースのネットワークでは、ダイヤルイン ユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、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ています。
- 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。たとえば、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。あるケースでは、RADIUS を Enigma のセキュリティ カードと併用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアントを含むシスコ製スイッチをネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。図 8-2 (P.8-19) を参照してください。
- ユーザが 1 つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1 つのホスト、Telnet などの 1 つのユーティリティ、または IEEE 802.1X などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、第 9 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 アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース (時間、パケット、バイトなど) の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス制御およびアカウンティング ソフトウェアのフリーウェア バージョンを使用して、特殊なセキュリティ および請求のニーズを満たすこともできます。

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

- マルチプロトコル アクセス環境。RADIUS は、AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP; NetBIOS フレーム制御プロトコル)、NetWare Asynchronous Services Interface (NASI; NetWare 非同期サポート インターフェイス)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製デバイスへの認証には使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

図 8-2 RADIUS から TACACS+ サービスへの移行



RADIUS の動作

RADIUS サーバによってアクセス制御されているスイッチに、ユーザがログインして認証を試みると、次のイベントが発生します。

1. ユーザ名とパスワードの入力を求めるプロンプトが表示されます。
2. ユーザ名と暗号化されたパスワードが、ネットワークを介して RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
 - 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るプロンプトが表示されるか、アクセスが拒否されます。
 - c. CHALLENGE : ユーザからの追加データが要求されます。
 - d. CHALLENGE PASSWORD : ユーザは新しいパスワードを選択するよう要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用される追加データがバンドルされています。RADIUS 許可がイネーブルになっている場合、ユーザはまず、RADIUS 認証に成功しなければ RADIUS 許可に進めません。ACCEPT または REJECT パケットの追加データには、次の項目が含まれています。

- Telnet、SSH、rlogin、または特権 EXEC サービス
- 接続パラメータ (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)

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について説明します。少なくとも、RADIUS サーバソフトウェアが稼動するホスト（複数可）を特定し、RADIUS 認証の方式リストを定義する必要があります。任意で RADIUS 許可およびアカウントिंगの方式リストを定義することもできます。

方式リストは、ユーザの認証、認可、およびアカウントを維持するための順序と方式を定義します。方式リストを使用すると、使用するセキュリティプロトコル（TACACS+ やローカル ユーザ名検索など）を 1 つまたは複数指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。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、アカウントの維持を行います。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方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストを使い果たすまで続きます。

スイッチに RADIUS 機能を設定するには、RADIUS サーバにアクセスして設定する必要があります。ここでは、次の設定情報について説明します。

- 「RADIUS のデフォルト設定」 (P.8-20)
- 「RADIUS サーバホストの特定」 (P.8-20) (必須)
- 「RADIUS ログイン認証の設定」 (P.8-23) (必須)
- 「AAA サーバグループの定義」 (P.8-25) (任意)
- 「ユーザイネーブルアクセスおよびネットワーク サービス用の RADIUS 許可の設定」 (P.8-27) (任意)
- 「RADIUS アカウンティングの開始」 (P.8-28) (任意)
- 「すべての RADIUS サーバに対する設定」 (P.8-29) (任意)
- 「ベンダー固有の RADIUS アトリビュート用にスイッチを設定する方法」 (P.8-29) (任意)
- 「ベンダー固有の RADIUS サーバ通信用にスイッチを設定する方法」 (P.8-30) (任意)
- 「RADIUS ロード バランシングの設定」 (P.8-31) (任意)

RADIUS のデフォルト設定

RADIUS と AAA は、デフォルトでディセーブルに設定されています。

セキュリティの失効を防止するために、ネットワーク管理アプリケーションを使用して RADIUS を設定することは不可能です。RADIUS をイネーブルに設定すると、CLI を使用して、スイッチにアクセスするユーザを認証します。

RADIUS サーバホストの特定

スイッチと RADIUS サーバ間の通信には、次の要素が関係します。

- 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 スtring
- タイムアウト時間
- 再送信回数

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と各 UDP ポート番号、あるいは IP アドレスと各 UDP ポート番号で識別されます。IP アドレスと UDP ポート番号の組み合わせによって一意の識別子が作成され、特定の AAA サービスを提供する RADIUS ホストとしてさまざまなポートを個別に定義できます。この一意の識別子によって、サーバ上の複数の UDP ポートに同じ IP アドレスで RADIUS 要求を送信できるようになります。

同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス（たとえば、アカウントティング）を設定している場合、あとから設定されたホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。この例では、最初のホスト エントリがアカウントティング サービスを提供できない場合は、スイッチは同じデバイス上に設定された 2 番目のホスト エントリでアカウントティング サービスを試行します（RADIUS のホスト エントリは、設定された順序で試行されます）。

RADIUS サーバおよびスイッチは、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 デーモンが稼動するホストと、そのスイッチを共有するシークレット テキスト（キー） ストリングを指定する必要があります。

タイムアウト、再送信回数、および暗号化鍵の値は、すべての RADIUS サーバに対してグローバルにサーバ単位で設定することも、グローバルな設定とサーバ単位の設定を組み合わせることもできます。この設定を、スイッチと通信するすべての RADIUS サーバに対してグローバルに適用するには、3 つの特別なグローバル 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。特定の RADIUS サーバにこれらの値を適用するには、**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。

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するよう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.8-25) を参照してください。

サーバ単位での 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	aaa new-model	AAA 認証をイネーブルにします。

コマンド	目的
ステップ 3 radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>]	<p>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。</p> <ul style="list-style-type: none"> (任意) auth-port <i>port-number</i> には、認証要求の UDP 宛先ポートを指定します。 (任意) acct-port <i>port-number</i> には、アカウント要求の UDP 宛先ポートを指定します。 (任意) timeout <i>seconds</i> には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでのインターバルを指定します。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 コマンドの設定を上書きします。radius-server host コマンドでタイムアウトを設定しない場合は、radius-server timeout コマンドの設定が使用されます。 (任意) retransmit <i>retries</i> には、サーバが応答しないか、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 コマンドで再送信の値を設定しない場合は、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 <i>string</i> には、スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。 <p>(注) key は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。鍵は、必ず radius-server host コマンドの最後の項目として設定します。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。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。</p> <p>1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定され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、再送信回数、および暗号化鍵の値を設定します。</p>
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) コンフィギュレーション ファイルに設定を保存します。

特定の 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、ある RADIUS サーバを認証用に、別の RADIUS サーバをアカウント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
```

次の例は、RADIUS サーバとして *host1* を設定し、認証およびアカウントの両方にデフォルトポートを使用する方法を示します。

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



(注) さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー スtring 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 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作成してから、さまざまなポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行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（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストが明示的に定義されたポートを除いて、自動的にすべてのポートに適用されます。

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るので、最初の方式が失敗した場合のバックアップ システムが確保されます。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すまで続きます。この処理のある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のユーザ名データベースがユーザ アクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行さ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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。

コマンド	目的
ステップ 3 <code>aaa authentication login {default list-name} method1 [method2...]</code>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> • <code>login authentication</code> 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されるデフォルトのリストを作成するには、キーワード default の後ろにデフォルト状況で使用す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。 • <code>list-name</code> には、作成するリストの名前として使用する文字列を指定します。 • <code>method1...</code> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。 <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> – 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あらかじめ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 サーバをあらかじめ設定しておく必要があります。詳細については、「RADIUS サーバホストの特定 (P.8-20)」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、回線パスワードをあらかじめ設定しておく必要があります。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しておく必要があります。username name password グローバル コンフィギュレーション コマンドを使用します。 – local-case : 大文字と小文字を区別するローカル 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 <code>line [console tty vty] line-number [ending-line-number]</code>	<p>ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。</p>
ステップ 5 <code>login authentication {default list-name}</code>	<p>回線または回線セットに対して、認証リストを適用します。</p> <ul style="list-style-type: none"> • default を指定する場合は、aaa authentication login コマンドで作成したデフォルトのリストを使用します。 • <code>list-name</code> 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 <code>end</code>	<p>特権 EXEC モードに戻ります。</p>
ステップ 7 <code>show running-config</code>	<p>設定を確認します。</p>
ステップ 8 <code>copy running-config startup-config</code>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

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。ログインの RADIUS 認証をディセーブルにするかデフォルト値に戻す場合は、**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。

AAA サーバ グループの定義

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するよう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、特定のサービスに使用できます。サーバ グループには、グローバル サーバホスト リストを使用します。このリストは、選択したサーバ ホストの IP アドレスのリストです。

サーバ グループには、各エントリが一意の識別子 (IP アドレスと UDP ポート番号の組み合わせ) を持っていれば、同じサーバに対して複数のホスト エントリを組み込むことができます。また、特定の AAA サービスを提供する RADIUS ホストとして、さまざまなポートを個別に定義できます。同一の RADIUS サーバ上の 2 つの異なるホスト エントリを同じサービス (たとえば、アカウントिंग) を設定すると、設定された 2 番めのホスト エントリは、最初のエントリの代替バックアップとして機能します。

定義済みのグループ サーバに特定のサーバを対応付けるには、**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特定したり、任意の **auth-port** および **acct-port** の各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識別したりできます。

AAA サーバ グループを定義して特定の RADIUS サーバに対応付けるには、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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>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。</p> <ul style="list-style-type: none"> （任意）<code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。 （任意）<code>acct-port port-number</code> には、アカウント要求の UDP 宛先ポートを指定します。 （任意）<code>timeout seconds</code> には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでのインターバルを指定します。指定できる範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドの設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトを設定しない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。 （任意）<code>retransmit retries</code> には、サーバが応答しないか、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。<code>radius-server host</code> コマンドで再送信の値を設定しない場合は、<code>radius-server retransmit</code> 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）<code>key string</code> には、スイッチと RADIUS サーバ上で稼動する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。 <p>(注) <code>key</code> は文字列であり、RADIUS サーバで使用されている暗号化キーと一致する必要があります。鍵は、必ず <code>radius-server host</code> コマンドの最後の項目として設定します。先頭のスペースは無視されますが、<code>key</code> の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。</p> <p>1 つの IP アドレスに対応する複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定され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、再送信回数、および暗号化鍵の値を設定します。</p>
ステップ 3	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	<code>aaa group server radius group-name</code>	<p>グループ名で AAA サーバ グループを定義します。</p> <p>このコマンドによって、スイッチはサーバ グループ コンフィギュレーション モードになります。</p>
ステップ 5	<code>server ip-address</code>	<p>特定の RADIUS サーバを定義済みサーバ グループに対応付けます。AAA サーバ グループの RADIUS サーバごとに、このステップを繰り返します。</p> <p>グループの各サーバは、ステップ 2 で定義されている必要があります。</p>
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。

	コマンド	目的
ステップ 7	<code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。
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.8-23) を参照してください。

特定の 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、同一の RADIUS サーバ上の 2 つの異なるホスト エントリに同じサービスを設定しています。2 番目のホスト エントリは、最初のエントリの代替バックアップとして機能します。

```
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 サービス用の RADIUS 許可の設定

AAA 許可は、ユーザが利用できるサービスを制限します。AAA 許可がイネーブルに設定されていると、スイッチはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

`aaa authorization` グローバル コンフィギュレーション コマンドにキーワード `radius` を指定して使用すると、特権 EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

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

- RADIUS を使用して認証を行った場合は、特権 EXEC アクセス許可に RADIUS を使用します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。



(注)

許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ユーザには、許可が省略されません。

特権 EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、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	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可をスイッチに設定します。
ステップ 3	aaa authorization exec radius	特権 EXEC アクセスの有無を、ユーザ RADIUS 許可によって判別するようにスイッチを設定します。 キーワード exec を指定すると、ユーザ プロファイル情報 (autocommand 情報など) が返されることがあります。
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) コンフィギュレーション ファイルに設定を保存します。

許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 アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスするサービスと、ユーザが消費するネットワーク リソースを追跡します。AAA アカウンティングがイネーブルに設定されていると、スイッチは、アカウンティング レコードの形式でユーザの活動状況を 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、アカウンティングの AV のペアが含まれ、セキュリティ サーバ上に保存されます。このデータを分析し、ネットワーク管理、クライアントへの課金、または監査に使用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに関する RADIUS 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	ネットワーク関連のすべてのサービス要求に関する RADIUS 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	RADIUS アカウンティングにより、特権 EXEC プロセスの開始時に記録開始アカウンティング通知、特権 EXEC プロセスの終了時に記録停止通知を送信するように設定します。
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) コンフィギュレーション ファイルに設定を保存します。

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。

すべての RADIUS サーバに対する設定

スイッチとすべての RADIUS サーバ間のグローバル通信コンフィギュレーションを設定するには、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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server key string</code>	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tring 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化 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。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 3	<code>radius-server retransmit retries</code>	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。デフォルトは 3 で、指定できる範囲は 1 ~ 1000 です。
ステップ 4	<code>radius-server timeout seconds</code>	スイッチが、RADIUS 要求に対する応答を待って要求を再送信するまでの秒数を指定します。デフォルトは 5 秒で、指定できる範囲は 1 ~ 1000 です。
ステップ 5	<code>radius-server deadtime minutes</code>	認証要求に応答しない RADIUS サーバをスキップする時間を指定します。これにより、要求がタイムアウトするまで待たずに、次の設定サーバを試行することができます。デフォルトは 0 で、指定できる範囲は 1 ~ 1440 分です。
ステップ 6	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 7	<code>show running-config</code>	設定を確認します。
ステップ 8	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

再送信、タイムアウト、デッドタイム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 アトリビュート用にスイッチを設定する方法

Internet Engineering Task Force (IETF) ドラフト規格では、ベンダー固有のアトリビュート (アトリビュート 26) を使用して、スイッチと RADIUS サーバとの間のベンダー固有情報の通信方式を定めています。Vendor-Specific Attribute (VSA; ベンダー固有アトリビュート) を使用すると、ベンダーは、汎用に適さない独自の拡張アトリビュートをサポートできます。シスコの実装 RADIUS では、仕様で推奨されたフォーマットを使用して 1 つのベンダー固有オプションをサポートします。シスコのベンダー ID は 9 で、サポート対象のオプションにはベンダータイプ 1 が設定されており、*cisco-avpair* と名前が付けられています。この値は次のフォーマットの文字列です。

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

protocol は、特定のタイプの許可に対応するシスコ プロトコル アトリビュートの値です。*attribute* と *value* は、シスコ TACACS+ 仕様で定義されている適正な AV のペアです。*sep* は、必須アトリビュートの場合は「=」、オプションのアトリビュートの場合は「*」です。TACACS+ 許可で利用できるすべての機能は、RADIUS にも使用できます。

たとえば、次の AV ペアは、IP 許可時 (PPP の IPCP アドレス割り当て時) に、シスコの複数の名前付き 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"
```

RADIUS によるスイッチ アクセスの制御

次の例は、スイッチからログインしているユーザに、特権 EXEC コマンドへの直接アクセスを可能にする方法を示します。

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

次の例は、RADIUS サーバ データベース内の許可 VLAN を指定する方法を示しています。

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

次の例は、この接続中に ASCII 形式の入力 ACL をインターフェイスに適用する方法を示しています。

```
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 deernet-iv"
```

次の例は、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する方法を示しています。

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

その他のベンダーにも、独自に一意のベンダー ID、オプション、および対応する VSA が割り当てられます。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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>radius-server vsa send [accounting authentication]</code>	<p>スイッチが、RADIUS IETF アトリビュート 26 に定義されている VSA を認識して使用できるようにします。</p> <ul style="list-style-type: none"> （任意）キーワード accounting を使用して、認識される VSA の集合をアカウントング アトリビュートに限定します。 （任意）キーワード authentication を使用して、認識される VSA の集合を認証アトリビュートに限定します。 <p>キーワードなしでこのコマンドを入力すると、アカウントングおよび認証の両方の VSA が使用されます。</p>
ステップ 3	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	設定を確認します。
ステップ 5	<code>copy running-config startup-config</code>	（任意）コンフィギュレーション ファイルに設定を保存します。

RADIUS アトリビュートの完全リスト、または VSA 26 の詳細については、『Cisco IOS Security Configuration Guide』 Release 12.2 の付録「RADIUS Attributes」を参照してください。

ベンダー固有の RADIUS サーバ通信用にスイッチを設定する方法

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバとの間のベンダー固有情報の通信方式を規定していますが、一部のベンダーは、固有の方法で RADIUS アトリビュートを機能拡張しています。Cisco IOS ソフトウェアは、ベンダー固有仕様の RADIUS アトリビュートのサブセットをサポートします。

前述したように、RADIUS（ベンダー固有または IETF のドラフト準拠）を設定するには、RADIUS サーバ デーモンが稼動しているホスト、および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。

ベンダー固有の 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、ベンダー固有の実装 RADIUS を使用していることを明確にします。
ステップ 3	radius-server key string	スイッチとベンダー固有の 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。スイッチおよび RADIUS サーバは、このテキスト 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。 (注) key は文字列であり、RADIUS サーバで使用されている暗号化鍵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せん。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で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) コンフィギュレーション ファイルに設定を保存します。

ベンダー固有の 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。鍵を削除するには、**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、ベンダー固有の RADIUS ホストを指定して、スイッチとサーバの間で *rad124* という秘密鍵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
```

RADIUS ロード バランシングの設定

この機能を使用すれば、アクセスおよび認証要求を、サーバ グループ内のすべての RADIUS サーバに均等に分散できます。詳細については、『Cisco IOS Security Configuration Guide』Release 12.2 の「RADIUS Server Load Balancing」の章を参照してください。

http://www.ciscosystems.com/en/US/docs/ios/12_2sb/feature/guide/sbrldbl.html

RADIUS 設定の表示

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

Kerberos によるスイッチ アクセスの制御

ここでは、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。Kerberos セキュリティ システムは、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します。この機能を使用するには、スイッチ ソフトウェアの暗号化（暗号化をサポートする）バージョンをスイッチにインストールする必要があります。この機能を使用するには、その許可を取得し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードする必要があります。詳細については、このリリースのリリース 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.8-32)
- 「Kerberos の動作」 (P.8-34)
- 「Kerberos の設定」 (P.8-35)

Kerberos の設定例については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章にある「Kerberos Configuration Examples」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html#wp1001396

ここで説明するコマンドの構文および使用方法の詳細については、この URL にある『Cisco IOS Security Command Reference』 Release 12.2 の「Security Server Protocols」の章にある「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 の構成例および『Cisco IOS Security Command Reference』 Release 12.2 では、信頼できるサードパーティとして Cisco ME スイッチを使用しています。このスイッチは Kerberos に対応し、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを使用したユーザ認証ができます。

Kerberos の概要

Kerberos はマサチューセッツ工科大学 (MIT) が開発した秘密鍵による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) という暗号化アルゴリズムを暗号化と認証に使用し、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という概念を使ってユーザとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティを *Key Distribution Center* (KDC; 鍵発行局) と呼びます。

Kerberos は、ユーザが誰であるか、そのユーザが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC (つまり信頼できる Kerberos サーバ) がユーザにチケットを発行します。このチケットには有効期限があり、ユーザ証明書のキャッシュに保存されます。

Kerberos サーバは、ユーザ名やパスワードの代わりにチケットを使ってユーザとネットワーク サービスを認証します。



(注) Kerberos サーバには、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを用いてユーザを認証できる Cisco ME スイッチを使用できます。

Kerberos の証明書発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザを 1 回認証すると、ユーザ証明書が有効な間は（他のパスワードの暗号化を行わずに）セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、(UNIX サーバや PC などの) 他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

このソフトウェア リリースでは、Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh (リモート シェル プロトコル)

表 8-2 に、一般的な Kerberos 関連用語とその定義を示します。

表 8-2 Kerberos の用語

用語	定義
認証	ユーザやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ネットワークやスイッチにおいてユーザがどのような権限を有しているか、またどのような動作を実行できるかを、スイッチが識別する手段
証明書	認証チケット (TGT ¹ やサービス証明書など) を表す総称。Kerberos 証明書で、ユーザまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバを信頼することにした場合、ユーザ名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの認証レベル ラベル。ほとんどの Kerberos プリンシパルは、「 <i>user@REALM</i> 」という形式です (たとえば、 <i>smith@EXAMPLE.COM</i>)。Kerberos インスタンスのある Kerberos プリンシパルは、「 <i>user/instance@REALM</i> 」という形式です (たとえば、 <i>smith/admin@EXAMPLE.COM</i>)。Kerberos インスタンスは、認証が成功した場合のユーザの許可レベルを指定するのに使用できます。各ネットワーク サービスのサーバは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。 (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とします。 (注) Kerberos レルム名はすべて大文字とします。
KDC ²	ネットワーク ホストで稼動する Kerberos サーバおよびデータベース プログラムで構成される KDC。
Kerberos 対応	Kerberos 証明書のインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語。

表 8-2 Kerberos の用語 (続き)

用語	定義
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。Kerberos サーバを信頼して、ユーザまたはネットワーク サービスに対する別のユーザまたはネットワーク 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とします。
Kerberos サーバ	ネットワーク ホストで稼動しているデーモン。ユーザおよびネットワーク サービスはそれぞれ Kerberos サーバに ID を登録します。ネットワーク サービスは Kerberos サーバにクエリーを送信して、他のネットワーク サービスの認証を得ます。
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 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス証明書を暗号解除して認証します。Kerberos 5 以前のバージョンでは、KEYTAB は SRVTAB ⁴ と呼ばれています。
プリンシパル	Kerberos ID とも呼ばれ、Kerberos サーバに基づき、ユーザが誰であるか、サービスが何であるかを表します。 (注) Kerberos プリンシパル名はすべて小文字とします。
サービス証明書	ネットワーク サービスの証明書。KDC から証明書が発行されると、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。ユーザ TGT ともパスワードを共有します。
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 以降のバージョンでは、SRVTAB は KEYTAB と呼びます。
TGT	身分証明書のこと、KDC が認証済みユーザに発行する証明書。TGT を受け取ったユーザは、KDC が表した Kerberos レルム内のネットワーク サービスに対して認証を得ることができます。

1. TGT = Ticket Granting Ticket (身分証明書)
2. KDC = Key Distribution Center (鍵発行局)
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 サーバには、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを用いてリモート ユーザを認証できる Cisco ME スイッチを使用できます。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモート ユーザは、3 つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

Kerberos サーバとしての Cisco ME スイッチを使用してネットワーク サービスに対して認証を得る手順は、次のとおりです。

1. 「境界スイッチに対する認証の取得」(P.8-35)
2. 「KDC からの TGT の取得」(P.8-35)
3. 「ネットワーク サービスに対する認証の取得」(P.8-35)

境界スイッチに対する認証の取得

ここでは、リモート ユーザが通過しなければならない最初のセキュリティ レイヤについて説明します。ユーザは、まず境界スイッチに対して認証を得なければなりません。その後、このプロセスは次のように進みます。

1. ユーザが、境界ルータへの Kerberos 非対応 Telnet 接続を確立します。
2. ユーザ名とパスワードの入力を求めるプロンプトが表示されます。
3. スイッチが、このユーザの TGT を KDC に要求します。
4. KDC がユーザ 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 の暗号解除を試行します。
 - 暗号解除に成功したら、ユーザはスイッチに対して認証を得ます。
 - 暗号解除に成功しなかった場合、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/オフに注意)、別のユーザ名とパスワードを入力してステップ 2 をやり直します。

境界スイッチに対して Kerberos 非対応 Telnet セッションを確立し認証を得たリモート ユーザは、ファイアウォールの内側に入ることに成功しましたが、ネットワーク サービスへのアクセス権を取得するには、さらに KDC に対して直接認証を得る必要があります。KDC が発行する TGT はスイッチに保存されているので、スイッチにログインしないと、追加の認証用に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 ユーザが通過しなければならない 2 番目のセキュリティ レイヤについて説明します。ユーザは、ネットワークにアクセスするために、ここで KDC の認証を得て KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章の「Obtaining a TGT from a KDC」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html#wp1000999

ネットワーク サービスに対する認証の取得

ここでは、リモート ユーザが通過しなければならない 3 番目のセキュリティ レイヤについて説明します。TGT を持つユーザは、ここで Kerberos レalm内のネットワーク サービスに対する認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfkerb.html#wp1001010

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を得るには、Kerberos レalm内のホストと KDC を設定して、ユーザおよびネットワーク サービスと通信を行って互いに認証し合う必要があります。これを実行するには、互いを識別する必要があります。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レalm内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザ用のエントリも作成します。

ホストおよびユーザのエントリを追加または作成する場合は、次のガイドラインに従ってください。

- Kerberos プリンシパル名はすべて小文字とします。
- Kerberos インスタンス名はすべて小文字とします。
- Kerberos レルム名はすべて大文字とします。



(注)

Kerberos サーバには、ネットワーク セキュリティ サーバとして設定可能で、Kerberos プロトコルを用いてユーザを認証できる Cisco ME スイッチを使用できます。

Kerberos 認証済みサーバクライアント システムを設定する手順は、次のとおりです。

- 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。

設定については、『Cisco IOS Security Configuration Guide』 Release 12.2 の「Security Server Protocols」の章にある「Kerberos Configuration Task List」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7ad.html

スイッチのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても AAA が動作するように設定できます。この場合、スイッチが認証および許可の処理を行います。この設定ではアカウント機能は利用できません。

スイッチをローカル AAA 用に設定するには、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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>aaa authentication login default local</code>	ローカルの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。キーワード default により、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 4	<code>aaa authorization exec local</code>	ユーザ AAA 許可を設定し、ローカル データベースを確認し、EXEC シェルをユーザに実行可能にします。
ステップ 5	<code>aaa authorization network local</code>	ネットワーク関連のすべてのサービス要求に関する AAA 許可を設定します。

コマンド	目的
ステップ 6 <code>username name [privilege level] {password encryption-type password}</code>	ローカル データベースを開始し、ユーザ名ベースの認証システムを設定します。 ユーザごとにこのコマンド入力を繰り返します。 <ul style="list-style-type: none"> <code>name</code> には、ユーザ ID を 1 ワードで指定します。スペースや引用符は使用できません。 (任意) <code>level</code> には、アクセス後ユーザに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では、ユーザ EXEC モードでのアクセスとなります。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 <code>encryption-type</code> には、暗号化されていないパスワードがあとに続く場合は 0 を、暗号化されたパスワードがあとに続く場合は 7 を指定します。 <code>password</code> には、ユーザがスイッチにアクセスする場合に入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<code>username</code> コマンドの最後のオプションとして指定します。
ステップ 7 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 8 <code>show running-config</code>	設定を確認します。
ステップ 9 <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

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。許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。

Secure Shell のためのスイッチの設定

ここでは、SSH 機能を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、スイッチに暗号化ソフトウェア イメージをインストールする必要があります。この機能を使用するには、その許可を取得し、Cisco.com から暗号化ソフトウェア ファイルをダウンロードする必要があります。詳細については、このリリースのリリース 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 の概要」(P.8-38)
- 「SSH の設定」(P.8-39)
- 「SSH の設定およびステータスの表示」(P.8-41)

SSH の設定例については、『Cisco IOS Security Configuration Guide』Cisco IOS Release 12.2 の「Configuring Secure Shell」の章にある「SSH Configuration Examples」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html



(注)

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、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。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080087e33.html

SSH の概要

SSH は、デバイスへの安全なリモート接続を提供するプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。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。

ここでは、次の内容について説明します。

- 「SSH サーバ、統合クライアント、およびサポート対象バージョン」(P.8-38)
- 「制限事項」(P.8-39)

SSH サーバ、統合クライアント、およびサポート対象バージョン

SSH 機能には、スイッチで稼動するアプリケーションである、SSH サーバおよび SSH 統合クライアントがあります。SSH サーバが稼動するスイッチとの接続には、SSH クライアントを使用できます。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他社製の SSH クライアントと連動します。また SSH クライアントも、このリリースでサポートされる SSH サーバおよび他社製の 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、DES 暗号化アルゴリズム、トリプル DES (3DES) 暗号化アルゴリズム、およびパスワードベースのユーザ認証をサポートします。

また 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+ によるスイッチ アクセスの制御」(P.8-10) を参照してください)
- RADIUS (詳細については、「RADIUS によるスイッチ アクセスの制御」(P.8-17) を参照してください)
- ローカル認証および許可 (詳細については、「スイッチのローカル認証および許可の設定」(P.8-36) を参照してください)



(注)

このソフトウェア リリースでは、IP Security (IPSec) をサポートしていません。

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, and Adelman (RSA) 認証をサポートします。
- SSH は、シェル実行アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、DES (56 ビット) および 3DES (168 ビット) の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、Advanced Encryption Standard (AES) 対称暗号化アルゴリズムをサポートしません。

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.8-39)
- 「スイッチでの SSH 実行の設定」(P.8-39) (必須)
- 「SSH サーバの設定」(P.8-40) (スイッチを SSH サーバとして設定している場合にだけ必要)

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 サーバにより生成された RSA 鍵ペアは、SSHv2 サーバで使用できます。また、その逆も可能です。
- **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、CLI エラーメッセージが表示される場合、RSA 鍵ペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。詳細については、「[スイッチでの SSH 実行の設定](#)」(P.8-39) を参照してください。
- RSA 鍵ペアを生成するときに、「ホスト名が指定されていません」というメッセージが表示される場合があります。表示される場合は、**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 鍵ペアを生成するときに、「ドメイン名が指定されていません」というメッセージが表示される場合があります。表示される場合は、**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。
- ローカルの AAA 方式を設定する場合は、コンソール上で AAA がディセーブルであることを確認してください。

スイッチでの SSH 実行の設定

スイッチに SSH の実行を設定するには、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。この手順は必須です。詳細については、このリリースのリリース ノートを参照してください。
2. スイッチに、ホスト名および IP ドメイン名を設定します。この手順は、スイッチを SSH サーバとして設定している場合にだけ実行します。
3. スイッチに RSA 鍵ペアを生成します。これにより自動的に SSH がイネーブルになります。この手順は、スイッチを SSH サーバとして設定している場合にだけ実行します。

4. ローカルまたはリモート アクセスにユーザ認証を設定します。この手順は必須です。詳細については、「[スイッチのローカル認証および許可の設定](#)」(P.8-36) を参照してください。

ホスト名および IP ドメイン名を設定して、RSA 鍵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 サーバとして設定している場合に必要です。

	コマンド	目的
ステップ 1	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>hostname hostname</code>	スイッチにホスト名を設定します。
ステップ 3	<code>ip domain-name domain_name</code>	スイッチにホスト ドメインを設定します。
ステップ 4	<code>crypto key generate rsa</code>	スイッチのローカルおよびリモート認証に関して、SSH サーバをイネーブルにして、RSA 鍵ペアを生成します。 モジュール サイズを 1024 ビット以上にすることを推奨します。 RSA 鍵ペアを生成すると、モジュールの長さを入力するよう求められます。モジュールの長さが長い方がセキュリティは高くなりますが、生成および使用に時間がかかります。
ステップ 5	<code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<code>show ip ssh</code> または <code>show ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。 スイッチ上の SSH サーバのステータスを表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

RSA 鍵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 鍵ペアを削除すると、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	<code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<code>ip ssh version [1 2]</code>	(任意) スイッチに SSH バージョン 1 または 2 を実行するよう設定します。 <ul style="list-style-type: none"> 1: スイッチに SSH バージョン 1 を実行するよう設定します。 2: スイッチに SSH バージョン 2 を実行するよう設定します。 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 サーバにより SSH クライアントがサポートする最新の SSH バージョンが選択されます。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。

コマンド	目的
ステップ 3 <code>ip ssh {timeout seconds authentication-retries number}</code>	<p>SSH 制御パラメータを設定します。</p> <ul style="list-style-type: none"> タイムアウト値を秒単位で指定します。デフォルトでは 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。接続が確立されると、スイッチはデフォルトの CLI ベース セッションのタイムアウト値を使用します。 <p>デフォルトでは、複数の CLI ベース セッションに関する暗号化 SSH 接続を最大 5 つまで同時にネットワーク上で使用できます (セッション 4 に対してセッション 0)。シェル実行が開始されると、CLI ベースセッションのタイムアウト値がデフォルトの 10 分に戻ります。</p> <ul style="list-style-type: none"> 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。デフォルトは 3 で、指定できる範囲は 0 ~ 5 です。 <p>両方のパラメータを設定する場合は、このステップを繰り返します。</p>
ステップ 4 <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5 <code>show ip ssh</code> または <code>show ssh</code>	<p>SSH サーバのバージョンおよび設定情報を表示します。</p> <p>スイッチ上の SSH サーバ接続のステータスを表示します。</p>
ステップ 6 <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

デフォルトの SSH 制御パラメータに戻るには、`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 の設定およびステータスの表示

SSH サーバの設定およびステータスを表示するには、表 8-3 に示される特権 EXEC コマンドを 1 つまたは複数使用します。

表 8-3 SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
<code>show ip ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。
<code>show ssh</code>	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、『Cisco IOS Security Command Reference』 Cisco IOS Release 12.2 の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。URL は次のとおりです。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800ca7cd.html

SCP のためのスイッチの設定

Secure Copy Protocol (SCP) 機能は、スイッチ設定またはスイッチ イメージ ファイルをセキュアな認証方法でコピーすることができます。SCP は、Secure Shell (SSH; セキュア シェル) に依存します。SSH は、Berkeley r-tool をセキュアにしたアプリケーションおよびプロトコルです。

SSH を動作させるには、RSA 公開鍵と秘密鍵のペアがスイッチで必要です。セキュアな転送のために SSH に依存している SCP も同様です。

SSH は AAA 認証にも依存しており、したがって SCP は AAA 許可に依存するため、正しい設定が必要になります。

- SCP をイネーブルにする前に、SSH、認証、認可をスイッチで正しく設定します。
- SCP はセキュアな転送のために SSH に依存するので、ルータでは RSA 鍵ペアが必要です。



(注)

SCP を使用する場合、copy コマンドにパスワードは入力できません。プロンプトが表示されてから、パスワードを入力します。

Secure Copy について

Secure Copy 機能を設定するには、次の概念を理解する必要があります。

- SCP の動作は、SCP がセキュリティのために SSH に依存している点を除いて、Berkeley の r-tool スイートからできた remote copy (rcp) と同様です。また、SCP でも AAA の設定が必須であるため、ルータはユーザに正しい権限レベルがあるかどうか判断できます。
- 適切に許可されたユーザは、SCP を使用して、copy コマンドにより、スイッチにまたはスイッチから Cisco IOS File System (IFS) 内の任意のファイルをコピーできます。許可された管理者も、ワークステーションからこの操作を実行できます。

SCP の設定方法および確認方法については、次の URL にある『Cisco IOS New Features』 Cisco IOS Release 12.2 の「Secure Copy Protocol」の章を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087b18.html