TACACS+ の設定

TACACS+は、ユーザによるルータまたはネットワークアクセスサーバへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。TACACS+は、認証および許可プロセスについて詳細なアカウンティング情報と柔軟な管理コントロールを提供します。TACACS+は、認証、許可、およびアカウンティング（AAA）を通じて効率化され、AAAコマンドでのみ有効化できます。

TACACS+ の前提条件

TACACS+によるデバイスアクセスのセットアップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

1. デバイスにTACACS+サーバアドレスを設定します。
2. 認証キーを設定します。
3. TACACS+サーバでステップ2からキーを設定します。
4. 認証、許可、およびアカウンティング（AAA）をイネーブルにします。
5. ログイン認証方式リストを作成します。
6. 端末回線にリストを適用します。
7. 認証およびアカウンティング方式のリストを作成します。

TACACS+によるデバイスアクセス制御のための前提条件は、次のとおりです。

- デバイス上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバにアクセスする必要があります。また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- デバイス上で TACACS+ を使用するには、TACACS+ デーモンソフトウェアが稼働するシステムが必要です。
- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 使用するデバイス上で許可をイネーブルにする必要があります。
- ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。
- このセクションに記載されている AAA コマンドのいずれかを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト（1 つまたは複数）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。また、任意で TACACS+ 認可およびアカウンティングの方式リストを定義できます。
- 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を明示的に定義されたインターフェイスを除いて、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。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 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。

TACACS+ の制約事項

TACACS+ をイネーブルにするには、AAA コマンドを使用する必要があります。

TACACS+ の概要

TACACS+ およびスイッチ アクセス

ここでは、TACACS+ について説明します。TACACS+ は詳細なアカウンティング情報を提供し、認証および許可プロセスを柔軟に管理します。TACACS+ は、認証、許可、およびアカウ

ンティング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

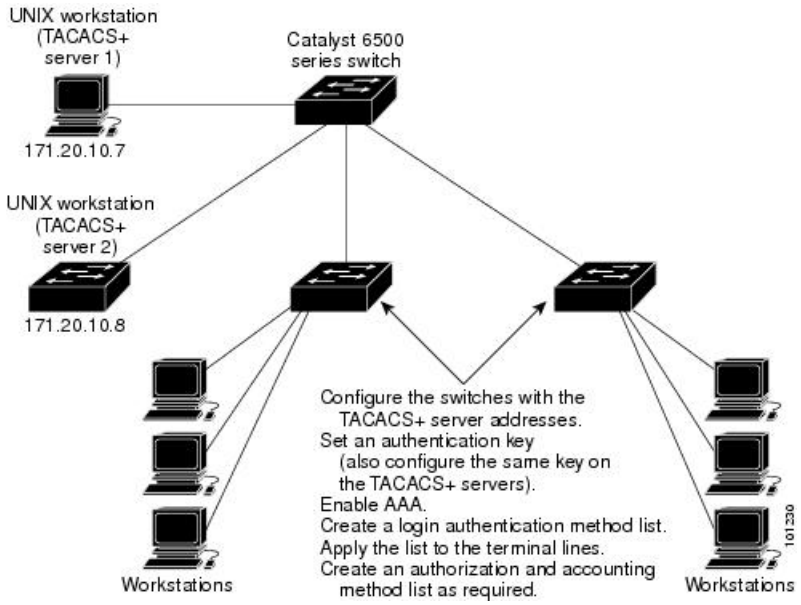
TACACS+ の概要

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+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

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 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 サーバにできます。

図 *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完全制御を行います。

  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が入力された後、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します）。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：autocommand、アクセスコントロール、セッション期間、プロトコルサポートの設定といった、ユーザセッション時のユーザ機能についてきめ細かく制御します。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、および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トラッキングしたり、ユーザ課金用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、開始時刻および終了時刻、実行されたコマンド（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+デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

TACACS+ の動作

ユーザが、TACACS+ を使用しているデバイスに対して簡易 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. 接続が確立されると、デバイスは TACACS+ デーモンに接続してユーザ名プロンプトを取得し、これをユーザに表示します。ユーザがユーザ名を入力すると、デバイスは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。デバイスによってパスワードプロンプトが表示され、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求めますが、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. デバイスは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

   - 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デバイス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に求められます。
   - ERROR：デーモンによる認証サービスのある時点で、またはデーモンとデバイス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、デバイスは、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、デバイス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 TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3. TACACS+ 許可が必要な場合は、再び 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、そ

のユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。

- Telnet、セキュア シェル（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、およびユーザ タイムアウトを含む）

方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、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、許可、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、方式リストの方式をすべて試し終わるまで続きます。

VTY 回線で方式リストを設定する場合、対応する方式リストを AAA に追加する必要があります。次の例は、VTY 回線の下に方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

次の例は、AAA で方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

VTY 回線で方式リストを設定しない場合、デフォルトの方式リストを AAA に追加する必要があります。次の例は、方式リストを使用しない VTY 設定を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
```

次の例は、デフォルトの方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

TACACS の AV ペア

ネットワーク アクセス サーバが TACACS+ 認可機能およびアカウンティング機能を実装するには、各ユーザ セッションで TACACS+ の属性と値（AV）ペアを送受信します。

TACACS+ 認証および認可の AV ペア

次の表で、サポートされている TACACS+ 認証および認可の AV ペアの一覧と説明を示し、実装されている Cisco IOS リリースを指定しています。

表 *1*：サポートされている *TACACS+* 認証および認可の *AV* ペア

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
acl=x	接続アクセス リストを表す ASCII 数。service=shell の場合のみ使用されます。	あり	あり	あり	あり	あり	あり	あり
addr=x	ネットワーク アドレス。service=slip、service=ppp、および protocol=ip で使用されます。SLIP または PPP/IP 経由で接続する際にリモート ホストが使用する IP アドレスを含みます。たとえば、addr=10.2.3.4 となります。	あり	あり	あり	あり	あり	あり	あり
addr-pool=x	リモート ホスト アドレスの取得元とするローカル プールの名前を指定します。service=ppp および protocol=ip と使用されます。 **addr-pool** はローカル プーリングと連動して動作することに注意してください。ローカル プールの名前を指定します。これはネットワーク アクセス サーバで事前設定する必要があります。**ip-local pool** コマンドを使用して、ローカル プールを宣言します。次に例を示します。 ip address-pool local ip local pool boo 10.0.0.1 10.0.0.10 ip local pool moo 10.0.0.1 10.0.0.20 その後、TACACS+ を使用して addr-pool=boo または addr-pool=moo を返し、このリモート ノードのアドレスの取得元にするアドレス プールを指示することができます。	あり	あり	あり	あり	あり	あり	あり
autocmd=x	EXEC 起動時に実行する autocommand を指定します（たとえば autocmd=telnet example.com）。service=shell の場合のみ使用されます。	あり	あり	あり	あり	あり	あり	あり
callback- dialstring	コールバックの電話番号（例：callback-dialstring= 408-555-1212）を設定します。値はヌルまたはダイヤルストリングです。ヌル値は、サービスで他の手段を通じてダイヤル ストリングを取得することもできることを示します。service=arap、service=slip、service=ppp、service=shell で使用されます。ISDN では無効です。	なし	あり	あり	あり	あり	あり	あり
callback-line	コールバックで使用する TTY 回線の数（例：callback-line=4）です。service=arap、service=slip、service=ppp、service=shell で使用されます。ISDN では無効です。	なし	あり	あり	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
callback-rotary	コールバックで使用するロータリー グループの数（0 ～ 100 の範囲）です（例：callback-rotary=34）。service=arap、service=slip、service=ppp、service=shell で使用されます。ISDN では無効です。	なし	あり	あり	あり	あり	あり	あり
cmd-arg=x	シェル（EXEC）コマンドに渡す引数です。実行されるシェル コマンドの引数を示します。cmd-arg 属性を複数指定でき、順序依存です。 （注） この TACACS+ AV ペアは、RADIUS 属性 26 で使用できません。	あり	あり	あり	あり	あり	あり	あり
cmd=x	シェル（EXEC）コマンドです。実行するシェル コマンドのコマンド名を示します。この属性は、サービスが「シェル」と等しい場合に指定する必要があります。ヌル値は、シェル自身が参照されることを示します。 （注） この TACACS+ AV ペアは、RADIUS 属性 26 で使用できません。	あり	あり	あり	あり	あり	あり	あり
data-service	service=outbound および protocol=ip で使用されます。	なし	なし	なし	なし	なし	あり	あり
dial-number	ダイヤルする番号を定義します。service=outbound および protocol=ip で使用されます。	なし	なし	なし	なし	なし	あり	あり
dns-servers=	Microsoft PPP クライアントにより、IPCP ネゴシエーション中にネットワーク アクセス サーバから要求される可能性がある DNS サーバ（プライマリまたはセカンダリ）を識別します。service=ppp および protocol=ip で使用されます。DNS サーバを特定する IP アドレスはドット付き 10 進表記で入力します。	なし	なし	なし	あり	あり	あり	あり
force-56	チャネルの 64 K すべてが使用可能に見える場合でも、ネットワーク アクセス サーバが 56 K の部分のみを使用するかどうかを指定します。この属性をオンにするには、「true」値（force-56=true）を使用します。他の値は、false として扱われます。service=outbound および protocol=ip で使用されます。	なし	なし	なし	なし	なし	あり	あり
gw-password	L2F トンネル認証中のホーム ゲートウェイのパスワードを指定します。service=ppp および protocol=vpdn で使用されます。	なし	なし	あり	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
idletime=x	値を分単位で設定します。その時間が経過すると、アイドルセッションが終了します。ゼロ値はタイムアウトなしを示します。	なし	あり	あり	あり	あり	あり	あり
inacl#<n>	現在の接続期間に使用されるインターフェイスにインストールされ適用される、入力アクセスリストのASCIIアクセス リスト識別名です。service=ppp および protocol=ip、service service=ppp および protocol =ipx で使用されます。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	なし	なし	なし	あり	あり	あり	あり
inacl=x	インターフェイス 入力アクセス リストの ASCII 識別名です。service=ppp および protocol=ip で使用されます。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	あり	あり	あり	あり	あり	あり	あり
interface-config#<n>	仮想プロファイルを使用してユーザ固有の AAA インターフェイス設定情報を指定します。等号（=）が付いている情報は、すべてのCisco IOSインターフェイス コンフィギュレーション コマンドとして使用できます。この属性は複数インスタンスが許可されますが、各インスタンスは固有の番号を持つ必要があります。service=ppp および protocol=lcp で使用されます。 （注） 「interface-config=」属性はこの属性に置き換えられます。	なし	なし	なし	あり	あり	あり	あり
ip-addresses	トンネルのエンドポイントで使用できるIPアドレスの、スペースで区切ったリストです。service=ppp および protocol=vpdn で使用されます。	なし	なし	あり	あり	あり	あり	あり
l2tp-busy-disconnect	LNS の vpdn-group で、事前にコピーするよう設定された仮想テンプレートを使用している場合、この属性は、接続先の事前にコピーされたインターフェイスが検索されない、新しいL2TPセッションのディスポジションを制御します。属性が true（デフォルト）の場合、セッションが LNS により切断されます。そうでない場合は、新しいインターフェイスが仮想テンプレートからコピーされます。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウ サイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
l2tp-drop-out-of-order	正しくない順序で受信したデータ パケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データ パケット上でシーケンス番号が送信されるわけではありません。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-hello- interval	hello キープアライブ インターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-tos-reflect	LNS でトンネルに入るパケットに対して、IP ToS フィールドを各ペイロード パケットの IP ヘッダーからトンネル パケットの IP ヘッダーにコピーします。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-tunnel- authen	この属性を設定すると、L2TP トンネル認証が実行されます。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-tunnel-password	L2TP トンネル認証および AVP 隠蔽に使用される共有秘密です。service=ppp および protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
l2tp-udp- checksum	これは認可属性で、L2TP がデータ パケットに対して UDP チェックサムを実行する必要があるかどうかを定義します。有効な値は「yes」と「no」です。デフォルトは「no」です。service=ppp と protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
link- compression=	PPP リンクで「stac」圧縮をオンまたはオフのどちらにするかを定義します。service=ppp で使用されます。 リンク圧縮は、次のように、数値で定義します。 • 0：なし • 1：Stac • 2：Stac-Draft-9 • 3：MS-Stac	なし	なし	なし	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
load-threshold= <n>	マルチリンク バンドルに対して他のリンクを追加または削除する発信元の負荷のしきい値を設定します。負荷がこの指定した値を超えると、追加リンクが追加されます。負荷が指定の値を下回ると、リンクが削除されます。service=ppp および protocol=multilink で使用されます。<n> の範囲は、1 から 255 です。	なし	なし	なし	あり	あり	あり	あり
map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップ クラスで設定される情報の参照を許可します。service=outbound および protocol=ip で使用されます。	なし	なし	なし	なし	なし	あり	あり
max-links=<n>	ユーザがマルチリンクで保持できるリンク数を制限します。service=ppp および protocol=multilink で使用されます。<n> の範囲は、1 から 255 です。	なし	なし	なし	あり	あり	あり	あり
min-links	MLP に対するリンクの最小数を設定します。service=ppp と protocol=multilink、protocol=vpdn で使用されます。	なし	なし	なし	なし	なし	あり	あり
nas-password	L2F トンネル認証でのネットワーク アクセス サーバのパスワードを指定します。service=ppp および protocol=vpdn で使用されます。	なし	なし	あり	あり	あり	あり	あり
nocallback-verify	コールバック検証が必要かを指定します。このパラメータで有効な値は 1 のみです（例：nocallback-verify=1）。service=arap、service=slip、service=ppp、service=shell で使用されます。コールバックに認証がありません。ISDN では無効です。	なし	あり	あり	あり	あり	あり	あり
noescape=x	ユーザがエスケープ文字を使用できないようにします。service=shell で使用されます。true または false のどちらかです（例：noescape=true）。	あり	あり	あり	あり	あり	あり	あり
nohangup=x	service=shell で使用されます。nohangup オプションを指定します。このオプションで EXEC シェルの終了後、ユーザに他のログイン（ユーザ名）プロンプトを表示します。true または false のどちらかです（例：nohangup=false）。	あり	あり	あり	あり	あり	あり	あり
old-prompts	プロバイダーが以前のシステム（TACACS および拡張 TACACS）と同じプロンプトを TACACS+ で表示できます。これにより、管理者は、TACACS または拡張 TACACS から TACACS+ に、ユーザが気づくことなくアップグレードできます。	あり	あり	あり	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
outacl#<n>	現在の状態である限りインターフェイスにインストールされ、適用されるインターフェイス出力アクセス リストの ASCII アクセス リスト識別情報です。service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	なし	なし	なし	あり	あり	あり	あり
outacl=x	インターフェイス 出力アクセス リストの ASCII 識別名です。service=ppp および protocol=ip、service service=ppp および protocol=ipx で使用されます。SLIP または PPP/IP の IP 出力アクセス リストが含まれます（outacl=4 など）。このアクセスリスト自身はルータで事前設定する必要があります。ユーザ単位のアクセス リストは、現在 ISDN インターフェイスでは使用できません。	あり（PPP/IP のみ）	あり	あり	あり	あり	あり	あり
pool-def#<n>	ネットワーク アクセス サーバで IP アドレス プールを定義します。service=ppp および protocol=ip で使用されます。	なし	なし	なし	あり	あり	あり	あり
pool-timeout=	pool-def とともに、ネットワーク アクセス サーバ上の IP アドレス プールを定義します。IPCP アドレス ネゴシエーション中、IP プール名がユーザに指定されている場合（addr-pool 属性を参照）、指定された名前のプールがネットワーク アクセス サーバで定義されているかチェックされます。その場合、プールに IP アドレスがあるか参照します。service=ppp および protocol=ip で使用されます。	なし	なし	あり	あり	あり	あり	あり
port-type	ユーザを認証するためにネットワーク アクセス サーバで使用されている物理ポートのタイプを示します。 物理ポートは、次のように数値で示されます。 • 0：非同期 • 1：同期 • 2：ISDN 同期 • 3：ISDN 非同期（V.120） • 4：ISDN-非同期（V.110） • 5：仮想 service=any および protocol=aaa で使用されます。	なし	なし	なし	なし	なし	あり	あり
ppp-vj-slot-compression	VJ 圧縮パケットを PPP リンク経由で送信する際に、Cisco ルータでスロット圧縮しないように指示します。	なし	なし	なし	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
priv-lvl=x	EXEC に割り当てられる権限レベルです。service=shell で使用されます。権限レベルの範囲は 0 ～ 15 で、15 が最高です。	あり	あり	あり	あり	あり	あり	あり
protocol=x	サービスのサブセットのプロトコルです。たとえば、任意の PPP NCP などです。現在知られている値は、**lcp**、**ip**、**ipx**、**atalk**、**vines**、**lat**、**xremote**、**tn3270**、**telnet**、**rlogin**、**pad**、**vpdn**、**osicp**、**deccp**、**ccp**、**cdp**、**bridging**、**xns**、**nbf**、**bap**、**multilink**、および **unknown** です。	あり	あり	あり	あり	あり	あり	あり
proxyacl#<n>	ダウンロード可能なユーザ プロファイル（ダイナミック ACL）を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。service=shell および protocol=exec で使用されます。	なし	なし	なし	なし	なし	あり	あり
route	インターフェイスに適用されるルートを指定します。service=slip、service=ppp、および protocol=ip で使用されます。 ネットワークの許可中、route 属性はユーザ単位のスタティック ルートの指定に使用でき、TACACS+ により次のようにインストールされます。 route=”*dst_address mask* [*gateway*]” これは、一時的に適用されるスタティック ルートを示します。*dst_address*、*mask*、*gateway* は、通常のドット付き 10 進表記での記述を想定されており、よく使用されるネットワークアクセスサーバの **ip route** コンフィギュレーション コマンドと同じ意味を持ちます。 *gateway* を省略すると、ピアのアドレスがゲートウェイになります。ルートは接続が終了すると消去されます。	なし	あり	あり	あり	あり	あり	あり
route#<n>	ルート AV ペアと同様にインターフェイスに適用されるルートを指定しますが、このルートは番号が付けられて複数のルートを適用できます。service=ppp と protocol=ip、および service=ppp と protocol =ipx で使用されます。	なし	なし	なし	あり	あり	あり	あり
routing=x	ルーティング情報をインターフェイスに伝播し、このインターフェイスから受け入れるかどうかを指定します。service=slip、service=ppp、および protocol=ip で使用されます。機能上、SLIP および PPP コマンドの /routing フラグと同等です。true または false のいずれか（例：routing=true）です。	あり	あり	あり	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
rte-fltr-in#<n>	現在の接続中に、現在のインターフェイスのルーティングアップデートにインストールし、適用する入力アクセスリストの定義を指定します。service=ppp と protocol=ip、および service=ppp と protocol =ipx で使用されます。	なし	なし	なし	あり	あり	あり	あり
rte-fltr-out#<n>	現在の接続中に、現在のインターフェイスのルーティングアップデートにインストールし、適用する出力アクセスリストの定義を指定します。service=ppp と protocol=ip、および service=ppp と protocol =ipx で使用されます。	なし	なし	なし	あり	あり	あり	あり
sap#<n>	接続中にインストールされるスタティック サービス アドバタイジング プロトコル（SAP）エントリを指定します。service=ppp および protocol=ipx で使用されます。	なし	なし	なし	あり	あり	あり	あり
sap-fltr-in#<n>	現在の接続中に、現在のインターフェイスにインストールし、適用する入力 SAP フィルタ アクセス リストの定義を指定します。service=ppp および protocol=ipx で使用されます。	なし	なし	なし	あり	あり	あり	あり
sap-fltr-out#<n>	現在の接続中に、現在のインターフェイスにインストールし、適用する出力 SAP フィルタ アクセス リストの定義を指定します。service=ppp および protocol=ipx で使用されます。	なし	なし	なし	あり	あり	あり	あり
send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル（PAP または CHAP）を定義します。service=any および protocol=aaa で使用されます。	なし	なし	なし	なし	なし	あり	あり
send-secret	NAS が発信コールの接続のリモート エンドからの chap/pap 要求に応答する際に必要なパスワードを指定します。service=ppp および protocol=ip で使用されます。	なし	なし	なし	なし	なし	あり	あり
service=x	プライマリ サービスです。このサービスの認証またはアカウンティングを要求していることを示すサービス属性を指定します。現在の値は、**slip**、**ppp**、**arap**、**shell**、**tty-daemon**、**connection**、および **system** です。この属性は常に含める必要があります。	あり	あり	あり	あり	あり	あり	あり
source-ip=x	VPDN トンネルの一部として生成されたすべての VPDN パケットの発信元 IP アドレスとして使用されます。これは、Cisco **vpdn outgoing** グローバル コンフィギュレーション コマンドと同じ意義を持ちます。	なし	なし	あり	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
spi	登録中にホーム エージェントがモバイル ノードの認証で必要とする認証情報を伝送します。この情報は、**ip mobile secure host <addr>** コンフィギュレーション コマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーション コマンドはそのまま含まれます。これにはセキュリティ パラメータ インデックス（SPI）、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。service=mobileip および protocol=ip で使用されます。	なし	なし	なし	なし	なし	あり	あり
timeout=x	EXEC または ARA セッションを切断するまでの分数です（例：timeout=60）。ゼロ値はタイムアウトなしを示します。service=arap で使用されます。	あり	あり	あり	あり	あり	あり	あり
tunnel-id	個々のユーザ MID が生成されるトンネルの認証に使用するユーザ名を指定します。**vpdn outgoing** コマンドの *remote name* と同様です。service=ppp および protocol=vpdn で使用されます。	なし	なし	あり	あり	あり	あり	あり
wins-servers=	IPCP ネゴシエーション中に、ネットワーク アクセス サーバから Microsoft PPP クライアントにより要求される可能性がある Windows NT サーバを特定します。service=ppp および protocol=ip で使用されます。各 Windows NT サーバを特定する IP アドレスはドット付き 10 進表記で入力します。	なし	なし	なし	あり	あり	あり	あり
zonelist=x	数字の zonelist の値です。service=arap で使用されます。ARA 向けの AppleTalk zonelist です（例：zonelist=5）。	あり	あり	あり	あり	あり	あり	あり

TACACS+ と、TACACS+ 認証および認可の設定に使用する資料については、「TACACS+ の設定」モジュールを参照してください。

TACACS アカウンティング AV ペア

次の表で、サポートされている TACACS+ アカウンティングの AV ペアの一覧と説明を示し、実装されている Cisco IOS リリースを指定しています。

表 *2*：サポートされる *TACACS+* アカウンティング *AV* ペア

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
Abort-Cause	ファクス セッションが中断した場合、中断の信号を送信したシステム コンポーネントを示します。中断する可能性のあるシステム コンポーネントには、FAP（Fax Application Process）、TIFF（TIFF リーダーまたは TIFF ライター）、fax-mail クライアント、fax-mail サーバ、ESMTP クライアント、ESMTP サーバなどがあります。	なし	なし	なし	なし	なし	あり	あり
bytes_in	この接続中に転送される入力バイト数です。	あり	あり	あり	あり	あり	あり	あり
bytes_out	この接続中に転送される出力バイト数です。	あり	あり	あり	あり	あり	あり	あり
Call-Type	ファクスのアクティビティのタイプを、fax receive または fax send のどちらかで記述します。	なし	なし	なし	なし	なし	あり	あり
cmd	ユーザが実行したコマンドです。	あり	あり	あり	あり	あり	あり	あり
data-rate	この AV ペアは名前が変更されました。nas-rx-speed を参照してください。							
disc-cause	接続がオフラインになった理由を特定します。Disconnect-Cause 属性は、アカウンティング終了記録で送信されます。また、この属性で、認証が実行される前に接続が切断された場合、最初に開始レコードを生成せずに終了レコードが生成されます。Disconnect-Cause 値とその意味の一覧については、次の表（接続解除原因の拡張）を参照してください。	なし	なし	なし	あり	あり	あり	あり
disc-cause-ext	disc-cause 属性が、接続がオフラインになったベンダー固有の理由をサポートするよう拡張します。	なし	なし	なし	あり	あり	あり	あり
elapsed_time	処理の経過時間（秒）です。デバイスが実時間を保持していない場合に有用です。	あり	あり	あり	あり	あり	あり	あり
Email-Server-Address	オンランプ fax-mail メッセージを処理する E メール サーバの IP アドレスを示します。	なし	なし	なし	なし	なし	あり	あり
Email-Server-Ack-Flag	オンランプ ゲートウェイが fax-mail メッセージを受け入れる E メール サーバから肯定確認応答を受信したことを示します。	なし	なし	なし	なし	なし	あり	あり
event	ルータの状態変化を記述した、アカウンティング パケットに含める情報です。記述されたイベントは、アカウンティング開始およびアカウンティング終了です。	あり	あり	あり	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
Fax-Account-Id-Origin	**mmoip aaa receive-id** コマンドまたは **mmoip aaa send-id** コマンドについて、アカウント ID の発信元がシステム管理者によって定義されたものとして示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Auth-Status	このファクス セッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、success、failed、bypassed、または unknown です。	なし	なし	なし	なし	なし	あり	あり
Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。	なし	なし	なし	なし	なし	あり	あり
Fax-Coverpage-Flag	カバー ページがこのファクス セッションのオフランプ ゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。	なし	なし	なし	なし	なし	あり	あり
Fax-Dsn-Address	DSN の送信先のアドレスを示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Mdn-Address	MDN の送信先のアドレスを示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Mdn-Flag	メッセージ配信通知（MDN）がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Modem-Time	モデムがファクスデータを送信した時間（x）、およびファクス セッションの合計時間（y）を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクス セッションが 15 秒であったことを示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Msg-Id=	Store and Forward Fax 機能によって割り当てられた一意のファクス メッセージ識別番号を示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Pages	このファクス セッション中に送信または受信したページ数を示します。このページ数には、カバー ページも含まれます。	なし	なし	なし	なし	なし	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
Fax-Process-Abort-Flag	ファクス セッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。	なし	なし	なし	なし	なし	あり	あり
Fax-Recipient-Count	このファクス送信の受信者数を示します。E メール サーバがセッション モードをサポートするまで、この数字は 1 にする必要があります。	なし	なし	なし	なし	なし	あり	あり
Gateway-Id	ファクス セッションを処理したゲートウェイの名前を示します。この名前は、hostname.domain-name の形式で表示されます。	なし	なし	なし	なし	なし	あり	あり
mlp-links-max	アカウンティング レコードが生成された時点で特定のマルチリンク セッションにあるリンク数を示します。	なし	なし	なし	あり	あり	あり	あり
mlp-sess-id	セッションが終了した時のマルチリンク バンドルの ID 番号をレポートします。この属性は、マルチリンク バンドルの一部のセッションに適用されます。この属性は、認証応答パケットで送信されます。	なし	なし	なし	あり	あり	あり	あり
nas-rx-speed	接続のライフタイムでの平均ビット/秒値を指定します。この属性は、アカウンティング終了記録で送信されます。	なし	なし	なし	あり	あり	あり	あり
nas-tx-speed	2 つのモデムによってネゴシエートされた送信速度を報告します。	なし	なし	なし	あり	あり	あり	あり
paks_in	この接続中に転送される入力パケット数です。	あり	あり	あり	あり	あり	あり	あり
paks_out	この接続中に転送される出力パケット数です。	あり	あり	あり	あり	あり	あり	あり
port	ユーザがログインしたポートです。	あり	あり	あり	あり	あり	あり	あり
Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。	なし	なし	なし	なし	なし	あり	あり
pre-bytes-in	認証前の入力バイト数を記録します。この属性は、アカウンティング終了記録で送信されます。	なし	なし	なし	あり	あり	あり	あり
pre-bytes-out	認証前の出力バイト数を記録します。この属性は、アカウンティング終了記録で送信されます。	なし	なし	なし	あり	あり	あり	あり
pre-paks-in	認証前の入力パケット数を記録します。この属性は、アカウンティング終了記録で送信されます。	なし	なし	なし	あり	あり	あり	あり

属性	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2
pre-paks-out	認証前の出力パケット数を記録します。Pre-Output-Packets 属性は、アカウンティング終了記録で送信されます。	なし	なし	なし	あり	あり	あり	あり
pre-session-time	コールが最初に接続された時から認証が完了した時までの時間長を秒で指定します。	なし	なし	なし	あり	あり	あり	あり
priv_level	処理に関連付けられた権限レベルです。	あり	あり	あり	あり	あり	あり	あり
protocol	処理に関連付けられたプロトコルです。	あり	あり	あり	あり	あり	あり	あり
reason	システム変更により発生したイベントを記述した、アカウンティングパケットに含める情報です。記述されるイベントは、システムのリロード、システムのシャットダウン、またはアカウンティングが再設定（オンまたはオフ）された場合です。	あり	あり	あり	あり	あり	あり	あり
service	ユーザが使用するサービスです。	あり	あり	あり	あり	あり	あり	あり
start_time	処理を開始する時刻（エポック（1970 年 1 月 1 日 12:00 a.m.）からの秒数で指定）。この情報を受信するよう、クロックを設定する必要があります。	あり	あり	あり	あり	あり	あり	あり
stop_time	処理を停止する時刻（エポックからの秒数で指定）。この情報を受信するよう、クロックを設定する必要があります。	あり	あり	あり	あり	あり	あり	あり
task_id	同じ（一意の）task_id 番号を持つ同じイベントに対する開始レコードと終了レコードです。	あり	あり	あり	あり	あり	あり	あり
timezone	このパケットに含まれるすべてのタイムスタンプの時間帯（省略形）です。	あり	あり	あり	あり	あり	あり	あり
xmit-rate	この AV ペアは名前が変更されました。nas-tx-speed を参照してください。							

次の表で、Disconnect Cause Extended（disc-cause-ext）属性の原因のコードと説明の一覧を示しています。

表 3 : Disconnect Cause Extensions

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1000 – 理由なし	接続解除の理由はありません。	なし	なし	なし	なし	あり	あり	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1001 – 接続解除なし	イベントは接続解除されませんでした。	なし	なし	なし	なし	あり	あり	あり	あり
1002 - 不明	接続解除の理由が不明です。このコードは、リモート接続が停止している場合に表示されることがあります。	なし	なし	なし	なし	あり	あり	あり	あり
1003 – コール接続解除	コールが接続解除されました。	なし	なし	なし	なし	あり	あり	あり	あり
1004 – CLID 認証失敗	Calling line ID（CLID）認証が失敗しました。	なし	なし	なし	なし	あり	あり	あり	あり
1009 – モデム使用不可	モデムが使用できません。	なし	なし	なし	なし	あり	あり	あり	あり
1010 – キャリアなし	モデムで、データ キャリア検出（DCD）が検出されませんでした。このコードは、最初のモデム接続で切断が発生した場合に表示されます。	なし	なし	なし	なし	あり	あり	あり	あり
1011 – キャリアのロスト	モデムで DCD は検出されましたが、非アクティブになっています。このコードは、最初のモデム接続で切断が発生した場合に表示されます。	なし	なし	なし	なし	あり	あり	あり	あり
1012 – モデム結果なし	結果コードが解析できません。このコードは、最初のモデム接続で切断が発生した場合に表示されます。	なし	なし	なし	なし	あり	あり	あり	あり
1020 – TS ユーザ退出	ユーザがターミナルサーバから正常に退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1021 – アイドル タイムアウト	アイドルタイマーの時間切れのため、ターミナルサーバからユーザが退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1022 – TS Telnet 退出	ユーザが、Telnet セッションから正常に退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1023 – TS IP アドレスなし	リモート ホストが IP アドレスを保持していないか、ダイナミック プールが割り当てられていないため、ユーザはシリアル ライン インターネット プロトコル（SLIP）または PPP にスイッチできませんでした。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1024 – TS TCP の raw 退出	ユーザが、raw TCP セッションから正常に退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1025 – TS パスワード不良	ユーザが 3 回、正しいパスワードの入力に失敗したため、ログイン処理が終了しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1026 – TS raw TCP なし	raw TCP オプションがイネーブルになっていません。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1027 – TS CNTL-C	ユーザが「Ctrl C」と入力したためログイン プロセスが終了しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の接続解除に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1028 – TS セッション終了	ターミナル サーバ セッションが終了しました。このコードは、ターミナルサーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1029 – TS Vconn 終了	ユーザがバーチャル コネクションを終了しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1030 – TS Vconn 終了	バーチャル コネクションが終了しました。このコードは、ターミナルサーバセッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1031 – TS Rlogin 退出	ユーザが Rlogin セッションから正常に退出しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1032 – TS Rlogin オプション無効	ユーザが無効な Rlogin オプションを選択しました。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1033 – TS 不十分なリソース	アクセス サーバにターミナル サーバ セッションを行う十分なリソースがありません。このコードは、ターミナル サーバ セッション中のイミディエート Telnet および raw TCP の切断に関連しています。	なし	なし	なし	なし	あり	あり	あり	あり
1040 – PPP LCP タイムアウト	PPP リンク コントロール プロトコル（LCP）ネゴシエーションがピアからの応答を待機している間にタイム アウトしました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1041 – PPP LCP 失敗	PPP LCP ネゴシエーションで収束に失敗しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1042 – PPP Pap 失敗	PPP パスワード認証プロトコル（PAP）認証が失敗しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1043 – PPP CHAP 失敗	PPP チャレンジ ハンドシェーク認証プロトコル（CHAP）認証が失敗しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1044 – PPP リモート失敗	リモート サーバからの認証が失敗しました。このコードは、PPP セッションと関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1045 – PPP 終了の受信	ピアが PPP 終了要求を送信しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
PPP LCP 終了（1046）	LCP がオープン状態にある時に、LCP が上位層から終了要求を受信しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1047 – PPP NCP なし	NCP がオープンでないため、LCP が終了しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1048 – PPP MP エラー	ユーザに追加するマルチリンク PPP バンドルを特定できなかったため、LCP は終了しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1049 – PPP 最大チャネル	アクセス サーバが MP セッションにこれ以上チャネルを追加できなかったため、LCP が終了しました。このコードは、PPP 接続と関係しています。	なし	なし	なし	なし	あり	あり	あり	あり
1050 – TS テーブルが満杯	raw TCP または Telnet 内部セッション テーブルが満杯です。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	なし	なし	なし	なし	あり	あり	あり	あり
1051 – TS リソースが満杯	内部リソースが満杯です。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	なし	なし	なし	なし	あり	あり	あり	あり
1052 – TS 無効な IP アドレス	Telnet ホストの IP アドレスが無効です。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	なし	なし	なし	なし	あり	あり	あり	あり
1053 – TS ホスト名不良	アクセスサーバがホスト名を解決できませんでした。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	なし	なし	なし	なし	あり	あり	あり	あり
1054 – TS ポート不良	アクセス サーバが不良または欠落したポート番号を検出しました。このコードは、イミディエート Telnet および raw TCP の切断に関連し、この表の前のほうに記載した Telnet および TCP コードよりも詳細な情報が含まれています。	なし	なし	なし	なし	あり	あり	あり	あり
1060 – TCP リセット	ホストで TCP 接続がリセットされました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1061 – TCP 接続拒否	ホストで TCP 接続が拒否されました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1062 – TCP タイムアウト	TCP 接続がタイムアウトしました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1063 – TCP 外部ホストの終了	外部ホストで TCP 接続が終了しました。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1064 – TCP ネット到達不能	TCP ネットワークが到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1065 – TCP ホスト到達不能	TCP ホストが到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1066 – TCP ネット管理到達不能	TCP ネットワークが管理的に到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1067 – TCP ホスト管理到達不能	TCP ホストが管理的に到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1068 – TCP ポート到達不能	TCP ポートが到達不能でした。TCP スタックが、イミディエート Telnet または raw TCP セッション中に、この切断コードを返す場合があります。	なし	なし	なし	なし	あり	あり	あり	あり
1100 – セッション タイムアウト	PPP リンクでアクティビティがないため、セッションがタイム アウトしました。このコードは、すべてのセッション タイプに適用されます。	なし	なし	なし	なし	あり	あり	あり	あり
1101 – セキュリティ障害	セキュリティ上の理由によりセッションが失敗しました。このコードは、すべてのセッション タイプに適用されます。	なし	なし	なし	なし	あり	あり	あり	あり
1102 – コールバック	コールバックのためセッションが終了しました。このコードは、すべてのセッション タイプに適用されます。	なし	なし	なし	なし	あり	あり	あり	あり
1120 – 非サポート	プロトコルがディセーブルまたは非サポートのため、片側がコールを拒否しました。このコードは、すべてのセッション タイプに適用されます。	なし	なし	なし	なし	あり	あり	あり	あり
1150 – Radius 接続解除	RADIUS サーバが接続解除を要求しました。	なし	なし	なし	なし	あり	あり	あり	あり
1151 – ローカル管理者接続解除	ローカル管理者が接続解除しました。	なし	なし	なし	なし	あり	あり	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1152 – SNMP 接続解除	簡易ネットワーク管理プロトコル（SNMP）が接続解除しました。	なし	なし	なし	なし	あり	あり	あり	あり
1160 – V110 リトライ	V110 同期で許可されたリトライ回数を超えました。	なし	なし	なし	なし	あり	あり	あり	あり
1170 – PPP 認証タイムアウト	認証がタイムアウトしました。このコードは、PPP セッションに適用されます。	なし	なし	なし	なし	あり	あり	あり	あり
1180 – ローカル ハングアップ	ローカルがハングアップした結果、コールが接続解除しました。	なし	なし	なし	なし	あり	あり	あり	あり
1185 – リモート ハングアップ	リモート エンドがハングアップしたため、コールが接続解除しました。	なし	なし	なし	なし	あり	あり	あり	あり
1190 – T1 休止	伝送している T1 回線が休止したため、コールが接続解除しました。	なし	なし	なし	なし	あり	あり	あり	あり
1195 – コール期間	コール期間が、アクセス サーバの Max Call Mins または Max DS0 Mins パラメータで許可された時間を越えたため、コールが接続解除しました。	なし	なし	なし	なし	あり	あり	あり	あり
1600 - VPDN ユーザ接続解除	ユーザが接続解除しました。この値は、バーチャル プライベート ダイヤルアップ ネットワーク（VPDN）セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1601 - VPDN 搬送波消失	搬送波消失が発生しました。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1602 – VPDN リソースなし	リソースがありません。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1603 – VPDN 制御パケット不良	制御パケットが無効です。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1604 – VPDN 管理者接続解除	管理者が接続解除しました。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1605 – VPDN トンネル ダウン/確立失敗	トンネルがダウンしているか、確立に失敗しました。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1606 – VPDN ローカル PPP 接続解除	ローカル PPP が接続解除しました。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1607 – VPDN ソフト停止/セッション制限	VPN トンネルで新しいセッションを確立できませんでした。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1608 – VPDN コール リダイレクト	コールがリダイレクトされました。このコードは、VPDN セッションに適用されます。	なし	なし	なし	なし	なし	なし	あり	あり
1801 – Q850 未割り当て番号	番号が割り当てられていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1802 – Q850 ルートなし	このコードを送信している機器が、認識されていない特定の中継ネットワークを使用したコールのルート要求を受信しました。このコードを送信している機器は、その中継ネットワークが存在しないか、その特定の中継ネットワークが存在していても、このコードを送信している機器で機能していないため、中継ネットワークを認識していません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1803 – Q850 宛先へのルートなし	コールが選択した経路で通過するネットワークが、目的の宛先で機能していないため、着信側に到達できません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1806 – Q850 チャネル受け入れ不能	直近で識別されたチャネルがこのコールで使用する送信エンティティに受け入れられません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1816 – Q850 正常な消去	このコールに関係するユーザの誰かが、コールを消去するよう要求したためコールが消去されました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1817 – Q850 ユーザ ビジー	ユーザビジー状態になっているため、着信側が他のコールを受けられません。このコードは、着信側のユーザまたはネットワークで生成されることがあります。ユーザにより生成された場合、ユーザの機器がこのコールに対応できます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1818 – Q850 ユーザ応答なし	割り当てられた所定の時間内に、着信側が、コール確立メッセージに対してアラートまたは接続表示によって応答しないときに使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1819 – Q850 ユーザ応答なし	着信側にアラートが送信されましたが、所定の時間内に接続表示による応答がありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1821 – Q850 コール却下	このコードを送信している機器は、ビジーまたは非対応ではないためこのコールを受けられますが、このコールを受けたくありません。このコードはネットワークにより生成されることもあり、この場合、このコールが補足サービスの制約により消去されたことを示します。診断フィールドには、補足サービスの追加情報や却下の理由が含まれている場合があります。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1822 – Q850 番号の変更	着信側を示す番号が割り当てられていません。新しい着番号が、任意で診断フィールドに含まれている場合があります。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1827 – Q850 宛先故障	宛先へのインターフェイスが正常に機能していないため、ユーザが指示した宛先に到達できません。「正常に機能していない」とは、シグナリング メッセージをリモート側に配信できなかったことを意味しています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1828 – Q850 無効な番号形式	着番号が有効な形式でないか、完全でないため、着信側に到達できません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1829 – Q850 ファシリティ拒否	このコードは、ユーザが要求した補足サービスがネットワークで提供されていない場合に返されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1830 – Q850 状態問い合わせへの応答	このコードは、STATUS ENQUIRY メッセージよりも先に受領したために STATUS メッセージが生成された場合に、STATUS メッセージに含まれています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1831 – Q850 未指定の原因	他のコードが適用されない場合に適用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1834 – Q850 使用可能な回線なし	コールを処理できる回線またはチャネルがありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1838 – Q850 ネットワーク障害	ネットワークが正常に機能しておらず、この状態が比較的長期間続く見込みです。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1841 – Q850 一時障害	ネットワークが正常に機能していませんが、この状態は長期間続かない見込みです。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1842 – Q850 ネットワーク輻輳	ネットワークが輻輳しています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1843 – Q850 アクセス情報破棄	このコードは、ネットワークがアクセス情報をリモート ユーザの要求に従って配信できなかったことを示します。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1844 – Q850 要求チャネルが使用不可能	このコードは、要求エンティティにより指定された回線またはチャネルが、インターフェイスの片側から提供できなかった場合に返されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1845 – Q850 コール プリエンプション	コールがプリエンプションされました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1847 – Q850 リソースが使用不可能	このコードは、リソース使用不可クラスの他のコードが適用されない場合にのみ、リソース使用不可イベントをレポートするために使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1850 – Q850 未登録ファシリティ	登録されているファシリティではありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1852 – Q850 発信コール除外	発信側が、発信非公開ユーザ グループ コールで非公開ユーザ グループのメンバーであっても、このメンバーに対して発信コールが許可されていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
Q850 着信コール除外（1854）	着信側が、着信非公開ユーザ グループ コールで非公開ユーザ グループのメンバーであっても、このメンバーに対して着信コールが許可されていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1858 – Q850 ベアラー機能が使用不可	ユーザが、このコードを生成した機器に実装されているベアラ機能を要求しましたが、その時点で使用できませんでした。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1863 – Q850 サービス使用不可	このコードは、サービスまたはオプション使用不可クラスの他のコードが適用されない場合にのみ、サービスまたはオプション使用不可イベントのレポートに使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1865 – Q850 ベアラー機能未実装	このコードを送信した機器は、要求されたベアラ機能をサポートしていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1866 – Q850 チャネル未実装	このコードを送信した機器は、要求されたチャネル タイプをサポートしていません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1869 – Q850 ファシリティ未実装	ユーザが要求した補足サービスがネットワークで提供できません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1881 – Q850 無効コール参照値	このコードを送信した機器は、ユーザネットワーク インターフェイスで現在使用されていないコール参照値が含まれたメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1882 – Q850 チャネルが存在しない	直近で識別されたチャネルがこのコールで使用する送信エンティティに受け入れられません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1888 – Q850 互換性がない宛先	このコードを送信中の機器が、対応できない下位レイヤの互換性または他の互換性属性を持つコールを確立するよう要求されました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1896 – Q850 必須情報要素が喪失	このコードを送信中の機器が、メッセージが処理される前にメッセージに存在しなければならない情報要素が失われているメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1897 – Q850 存在しないメッセージ タイプ	このコードを送信中の機器が、定義されていないメッセージであるか、定義されてはいるがこのコードを送信した機器で実装されていないため認識されないメッセージタイプのメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1898 – Q850 無効なメッセージ	このコードは、無効なメッセージ クラスの他のコードが適用されない場合に無効なメッセージをレポートするために使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1899 – Q850 情報要素不良	情報要素が認識されません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1900 – Q850 無効要素が含まれる	このコードを送信中の機器が、未実装の情報要素を受信しました。ただし、この情報要素の 1 つまたは複数のフィールドがこのコードを送信した機器で実装されていない方法で符号化されています。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1901 – Q850 誤った状態のメッセージ	受信したメッセージが、コール ステートと互換性がありません。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1902 – Q850 タイマーの期限切れからの回復	エラー処理手順に関連付けられたタイマーの期限切れによって、手順が初期化されました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1903 – Q850 情報要素エラー	このコードを送信中の機器が、情報要素識別名またはパラメータ名が定義されていないか、定義されてはいるがこのコードを送信した機器で実装されていないため、認識されない情報要素またはパラメータが含まれるメッセージを受信しました。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり

原因コード	説明	11.0	11.1	11.2	11.3	12.0	12.1	12.2	12.3
1911 – Q850 プロトコル エラー	このコードは、プロトコル エラー クラスの他のコードが適用されない場合にのみ、プロトコル エラー イベントをレポートするために使用されます。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり
1927 – Q850 未指定のインターネットワーキング イベント	行った処理に対してコードを提供しないネットワークでインターワーキングした場合にエラーになります。このコードは、ISDN または ISDN 経由のモデム コールに適用されます。	なし	なし	なし	なし	なし	なし	なし	あり

TACACS+ 設定オプション

認証用に 1 つのサーバを使用するように設定することも、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に設定することもできます。サーバをグループ化して設定済みサーバホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。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、選択されたサーバ ホストの IP アドレスのリストが含まれています。

TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ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。

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

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、デバイス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。

TACACS+ 認証

TACACS+ デーモンを指定し、関連する TACACS+ 暗号キーを定義したら、TACACS+ 認証の方式リストを定義する必要があります。TACACS+ 認証は AAA を介して実行されるため、認証方式として TACACS+ を指定して、**aaa authentication** コマンドを発行する必要があります。

TACACS+ 許可

AAA 許可により、ユーザによるネットワーク アクセスを制限するパラメータを設定することができます。TACACS+ を介する許可は、コマンド、ネットワーク接続、および EXEC セッションに適用できます。AAA によって TACACS+ 許可が容易になるため、認可方式として TACACS+ を指定して、**aaa authorization** コマンドを発行する必要があります。

TACACS+ Accounting

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワーク リソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、デバイスはユーザの活動状況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の Attribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトでは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、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。TACACS+ をイネーブルに設定した場合、CLI を通じ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 に設定された HTTP 接続を許可します。

TACACS+ を設定する方法

TACACS+ サーバ ホストの指定および認証キーの設定

TACACS+ サーバ ホストを特定し、認証キーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa group server tacacs+** *group-name* 例： `Device(config)# aaa group server tacacs+ your_server_group`	（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、device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* 例： `Device(config)# server 10.1.2.3`	（任意）特定の TACACS+ サーバを定義済みサーバ グループに関連付けます。AAA サーバ グループの TACACS+ サーバごとに、このステップを繰り返します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

始める前に

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、各種ポートにそのリストを適用します。

（注） AAA 方式を使用して HTTP アクセスに対しデバイスのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでデバイスを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しデバイスのセキュリティは確保されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default tacacs+ local`	ログイン認証方式リストを作成します。 • **login authentication** コマンドに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として使用する文字列を指定します。 • *method1...* 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

	コマンドまたはアクション	目的
		用されます。前の方式が失敗した場合は使用されません。 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、あらかじめ **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+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバを設定しておく必要があります。 • *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、あらかじめ回線パスワードを定義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** *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、ユーザ名情報をデータベースに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。

	コマンドまたはアクション	目的
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line 2 4`	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 6	**login authentication** {**default** | *list-name*} 例： `Device(config-line)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **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。 • *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 7	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。

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 authorization グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、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できます。

（注） 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa authorization network tacacs+** 例： `Device(config)# 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して、ユーザが TACACS+ 許可を受けるようにデバイスを設定します。
ステップ 4	**aaa authorization exec tacacs+** 例： `Device(config)# aaa authorization exec tacacs+`	ユーザの特権 EXEC アクセスに対してユーザ TACACS+ 許可を行うことを設定します。 **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 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**aaa accounting network start-stop tacacs+** 例： `Device(config)# aaa accounting network start-stop tacacs+`	ネットワーク関連のすべてのサービス要求について、TACACS+アカウンティングをイネーブルにします。
ステップ 4	**aaa accounting exec start-stop tacacs+** 例： `Device(config)# aaa accounting exec start-stop tacacs+`	TACACS+アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

次のタスク

AAA サーバが到達不能な場合にルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステム アカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまで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場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合に、ルータとのコンソールセッションまたは 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。

AAA サーバが到達不能な場合のルータとのセッションの確立

aaa accounting system guarantee-first コマンドは、システムアカウントを最初のレコードとして保証します。これは、デフォルトの条件です。場合によっては、システムがリロードされるまで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場合があります。システムのリロードにかかる時間は 3 分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合に、ルータとのコンソールセッションまたは 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 サーバ上の Per VRF の設定

この手順の最初のステップは、AAA およびサーバ グループの設定、VRF ルーティング テーブルの作成、およびインターフェイスの設定に使用されます。ステップ 10 ～ 13 は、TACACS+ サーバ機能上での Per VRF の設定に使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip vrf** *vrf-name* 例： `Device(config)# ip vrf cisco`	VRF テーブルを設定し、VRF 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	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:1`	VRF インスタンスに対するルーティングおよびフォワーディング テーブルを作成します。
ステップ 5	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了します。
ステップ 6	**interface** *interface-name* 例： `Device(config)# interface Loopback0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip vrf forwarding** *vrf-name* 例：	インターフェイスに VRF を設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip vrf forwarding cisco`	
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Device(config-if)# ip address 10.0.0.2 255.0.0.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 10	**aaa group server tacacs+** *group-name* 例： `Device(config)# aaa group server tacacs+ tacacs1`	異なる TACACS+ サーバ ホストを別々のリストと方式にグループ化し、server-group コンフィギュレーション モードを開始します。
ステップ 11	**server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*] 例： `Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco`	グループ サーバに対するプライベート TACACS+ サーバの IP アドレスを設定します。
ステップ 12	**ip vrf forwarding** *vrf-name* 例： `Device(config-sg-tacacs+)# ip vrf forwarding cisco`	AAA TACACS+ サーバ グループの VRF リファレンスを設定します。
ステップ 13	**ip tacacs source-interface** *subinterface-name* 例： `Device(config-sg-tacacs+)# ip tacacs source-interface Loopback0`	すべての発信 TACACS+ パケットに対して、指定されたインターフェイスの IP アドレスを使用します。
ステップ 14	**exit** 例： `Device(config-sg-tacacs)# exit`	サーバグループ 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 モードを開始します。

TACACS+ のモニタリング

表 *4: TACACS+* 情報を表示するためのコマンド

コマンド	目的
show tacacs	TACACS+ サーバの統計情報を表示します。

TACACS+ の設定例

例：TACACS 認可

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してネットワークの許可を設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa authorization network default group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **aaa authorization** コマンドにより、TACACS+ を介するネットワークの許可を設定します。認証リストとは異なり、この許可リストは、ネットワーク アクセス サーバに対するすべての着信ネットワーク接続に常に適用されます。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

例：TACACS アカウンティング

次に、デフォルトの方式リストを使用して、PPP 認証用のセキュリティ プロトコルとして、TACACS+ を設定する例を示します。また、TACACS+ を介してアカウンティングを設定する方法も示します。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
aaa accounting network default stop-only group tacacs+
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **aaa accounting** コマンドにより、TACACS+ を介するネットワーク アカウンティングを設定します。この例では、ネットワーク接続が終了するたびに、終了したセッションについて説明するアカウンティング レコードが、TACACS+ デーモンに送信されます。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

例：TACACS 認証

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
aaa new-model
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap pap test
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、テスト方式リストをこの回線に適用します。

次に、PPP 認証のセキュリティ プロトコルとして TACACS+ を設定する例を示します。ただし、「test」方式リストの代わりに、「default」方式リストが使用されます。

```
aaa new-model
aaa authentication ppp default if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication chap default
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「default」を定義します。キーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
aaa new-model
```

```
aaa authentication pap MIS-access if-needed group tacacs+ local
tacacs-server host 10.1.2.3
tacacs-server key goaway
interface serial 0
 ppp authentication pap MIS-access
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアル インターフェイスに使用する方式リスト「MIS-access」を定義します。方式リスト「MIS-access」は、PPP 認証がすべてのインターフェイスに適用されることを示します。**if-needed** キーワードは、ユーザが ASCII ログイン手順を介してすでに認証済みの場合には PPP 認証が不要なのでスキップできることを示します。認証が必要な場合、キーワード **group tacacs+** は、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバ上のローカル データベースを使用して認証が試行されることを示します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.1.2.3 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号キーを「goaway」に定義します。
- **interface** コマンドで回線を選択します。**ppp authentication** コマンドは、デフォルト方式リストをこの回線に適用します。

次に、IP アドレスが 10.2.3.4 である TACACS+ デーモンと暗号キー「apple」の設定の例を示します。

```
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.2.3.4
tacacs-server key apple
```

前述の設定例の回線は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドで、デフォルトの方式リストを定義します。すべてのインターフェイスでの着信 ASCII ログイン（デフォルト）では、認証に TACACS+ を使用します。応答する TACACS+ サーバがない場合、ネットワーク アクセス サーバは、認証用のローカル ユーザ名データベースに含まれる情報を使用します。
- **tacacs-server host** コマンドにより、TACACS+ デーモンが 10.2.3.4 という IP アドレスを持っていると指定します。**tacacs-server key** コマンドにより、共有暗号キーが「apple」になるように定義します。

例：TACACS サーバの Per VRF の設定

次の出力例では、Per VRF AAA サービスにグループ サーバ **tacacs1** が設定されています。

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0
  ip vrf cisco
   rd 100:1
  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

TACACS+ に関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches)

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

TACACS+ の機能情報

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

表 *5 : TACACS+* の機能情報

機能名	リリース	機能情報
TACACS+	Cisco IOS Release 15.2(7)E1	この機能が導入されました。