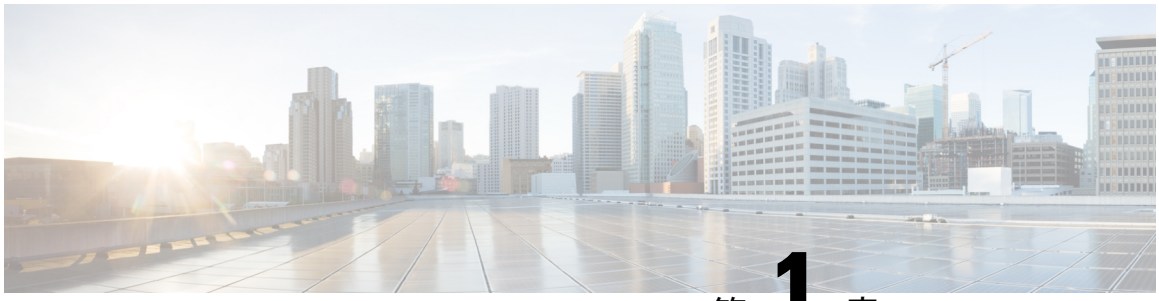
Cisco IOS XE Gibraltar 16.10.x TACACS+ コンフィギュレーション ガイド

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

最初にお読みください

Cisco IOS XE 16 に関する重要な情報

現行の Cisco IOS XE Release 3.7.0E（Catalyst スイッチング用）および Cisco IOS XE Release 3.17S（アクセスおよびエッジルーティング用）の 2 つのリリースは、単一バージョンのコンバージドリリース Cisco IOS XE 16 に進化（マージ）しました。これにより、スイッチングおよびルーティング ポートフォリオにおける広範なアクセス製品およびエッジ製品を 1 つのリリースでカバーします。

機能情報

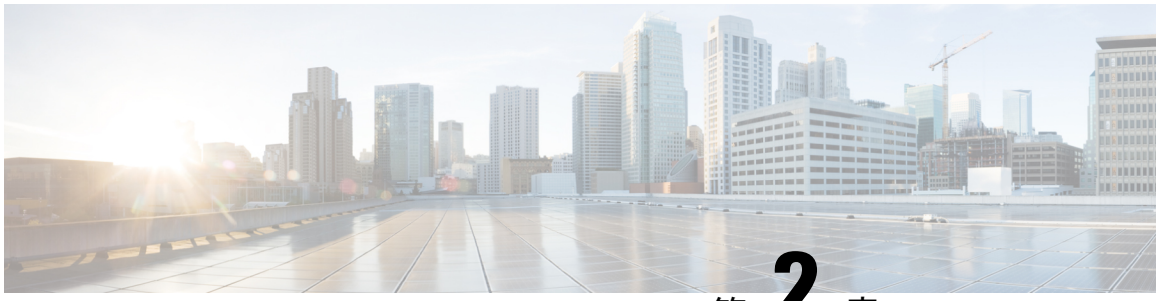
機能のサポート、プラットフォームのサポート、およびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco.com のアカウントは必要ありません。

参考資料

- 『Cisco IOS Command References, All Releases』

マニュアルの入手方法およびテクニカル サポート

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。



第 2 章

TACACS の設定

この章では、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できるようにするために、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、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

TACACS に関する情報

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+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。ネットワーク アクセス サーバに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

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+ を使用すると、単一のアクセス コントロール サーバ（TACACS+ デーモン）で、各サービス（認証、許可、アカウンティング）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提供できます。

TACACS+の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。アクセス サーバおよびルーティングのシスコ ファミリおよび（ルータとアクセス サーバ両方の）Cisco IOS および Cisco IOS XE ユーザ インターフェイスは、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 ポイントによって、従来の「低機能な」端末、端末エミュレータ、ワークステーション、パーソナル コンピュータ（PC）、およびルータと、適切なアダプタ（たとえば、モデムまたは ISDN アダプタ）を併用して、Point-to-Point Protocol（PPP）、Serial Line Internet Protocol（SLIP）、Compressed SLIP（CSLIP）、または AppleTalk Remote Access（ARA）プロトコルを使用する通信が可能になります。つまり、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、および相互接続したネットワークに対して、接続を提供できます。ネットワーク アクセス サーバを介して接続されているエンティティは、ネットワーク アクセス クライアントと呼ばれます。たとえば、音声グレードの回路で PPP を実行する PC は、ネットワーク アクセス クライアントです。AAA セキュリティ サービスを介して管理される TACACS+ は、次のサービスを提供できます。

- 認証：ログインとパスワードのダイアログ、チャレンジ/レスポンス、メッセージングのサポートを介して、認証を詳細に制御できます。

認証機能には、ユーザに任意のダイアログを実行する機能があります（たとえば、ログインとパスワードの指定後に、自宅住所、母親の旧姓、サービス タイプ、社会保険番号などの複数の質問をユーザに試行する機能）。さらに、TACACS+認証サービスは、ユーザ画面へのメッセージ送信をサポートします。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。

- 認可：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+認可機能を使用して、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、ネットワーク アクセス サーバと TACACS+ デーモンの間に認証機能を提供します。また、ネットワーク アクセス サーバと TACACS+ デーモン間のすべてのプロトコル交換は暗号化されるため、機密性を確保できます。

TACACS+ デーモン ソフトウェアを実行するシステムで、ネットワーク アクセス サーバで TACACS+ 機能を使用する必要があります。

独自の TACACS+ ソフトウェアを開発することに関心があるユーザ向けに、シスコでは、TACACS+ プロトコル仕様をドラフトの RFC として使用できるようにしています。

TACACS の動作

ユーザが TACACS+ を使用してネットワーク アクセス サーバに対して認証を受けることで、単純な ASCII ログインを試行すると、一般的に、次のプロセスが発生します。

1. 接続が確立すると、ネットワーク アクセス サーバは TACACS+ デーモンに接続してユーザ名のプロンプトをを取得します。また、そのプロンプトはユーザに表示されます。ユーザがユーザ名を入力すると、ネットワーク アクセス サーバは TACACS+ デーモンに接続し、パスワード プロンプトを取得します。ネットワーク アクセス サーバはユーザに対してパスワードプロンプトを表示します。ユーザがパスワードを入力すると、パスワードは TACACS+ デーモンに送信されます。

（注） TACACS+ によって、デーモンとユーザとの間で対話できるようになり、デーモンはユーザの認証に必要な情報を取得できるようになります。通常、この処理は、ユーザ名とパスワードの組み合わせのプロンプトを表示することで完了しますが、TACACS+ デーモンの制御下で、母親の旧姓など、他のアイテムを含めることができます。

1. ネットワーク アクセス サーバは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
    1. ACCEPT：ユーザは認証され、サービスを開始できます。認可を必須にするようにネットワーク アクセス サーバが設定されている場合、この時点で認可が開始されます。
    2. REJECT：ユーザは認証に失敗しました。ユーザは以降のアクセスを拒否される可能性があります。または、TACACS+ デーモンに応じてログイン シーケンスを再試行するようにプロンプトが表示されます。
    3. ERROR：認証中のある時点でエラーが発生しました。エラーは、デーモン、またはデーモンとネットワーク アクセス サーバ間のネットワーク接続で発生する可能性があります。ERROR 応答を受信すると、通常、ネットワーク アクセス サーバはユーザを認証する代替方式を使用しようとします。
    4. CONTINUE：ユーザは、さらに認証情報の入力を求められます。
2. PAP ログインは、ASCII ログインに似ていますが、ユーザによる入力ではなく、PAP プロトコルパケットでユーザ名とパスワードがネットワーク アクセス サーバに到達するため、ユーザにはプロンプトが表示されません。PPP CHAP ログインは、原則もにています。

ネットワーク アクセス サーバで認可をイネーブルにしている場合、認証の後に、ユーザは追加の認可段階を実行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。

1. TACACS+ の認可が必要な場合も、TACACS+ デーモンに接続します。また、TACACS+ デーモンは、ACCEPT または REJECT 認可応答を返します。ACCEPT 応答が返される場合、この応答には、そのユーザに関する EXEC または NETWORK セッションを指示する

ために使用される属性の形式のデータが含まれます。これによって、ユーザがアクセスできるサービスを判断します。この場合のサービスは次のとおりです。

1. Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
2. 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）

TACACS の設定方法

（注） Cisco IOS XE リリース 3.2S では、**tacacs-server host** コマンドは **tacacs server** コマンドに置き換えられました。**tacacs server** コマンドの詳細については、『*Security Command Reference*』を参照してください。

TACACS+ をサポートするようにルータを設定するには、次のタスクを実行する必要があります。

- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。TACACS+ を使用する予定がある場合、AAA を設定する必要があります。**aaa new-model** コマンドの使用の詳細については、「AAA の概要」の章を参照してください。
- **tacacs-server host** コマンドを使用して、1 つ以上の TACACS+ デーモンの IP アドレスを指定します。**tacacs-server key** コマンドを使用して、ネットワーク アクセス サーバと TACACS+ デーモンの間のすべてのやり取りを暗号化するために使用する暗号化キーを指定します。TACACS+ デーモンでも、この同じキーを設定する必要があります。
- **aaa authentication** 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、認証に TACACS+ を使用する方式リストを定義します。**aaa authentication** コマンドの使用の詳細については、「認証の設定」の章を参照してください。
- line および interface コマンドを使用して、定義済みの方式リストを多様なインターフェイスに適用します。詳細については、「認証の設定」の章を参照してください。
- 必要に応じて、**aaa authorization** グローバル コマンドを使用して、ネットワーク アクセス サーバの認可を設定します。回線またはインターフェイスごとに設定できる認証とは異なり、認可は、ネットワーク アクセス サーバ全体のグローバル設定です。**aaa authorization** コマンドの使用の詳細については、「認可の設定」の章を参照してください。
- 必要に応じて、**aaa accounting** コマンドを使用して TACACS+ 接続のアカウンティングをイネーブルにします。**aaa accounting** コマンドの使用の詳細については、「アカウンティングの設定」の章を参照してください。

TACACS サーバ ホストの指定

tacacs-server host コマンドを使用すると、TACACS+ サーバを保守する 1 つまたは複数の IP ホストの名前を指定できます。TACACS+ ソフトウェアは、指定した順序でホストを検索するため、この機能は、希望のデーモン リストを設定する場合に役立ちます。

（注） **tacacs-server host** コマンドは、間もなく廃止される予定です。**tacacs-server host** コマンドの代わりに **server** コマンドを使用できます。

TACACS+ホストを指定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tacacs-server host hostname [single-connection] [port integer] [timeout integer] [key string]`	TACACS+ ホストを指定します。

tacacs-server host コマンドを使用して、次のオプションも設定できます。

- **single-connection** キーワードを使用して、単一接続を指定します。通信が必要になるたびに、ルータの接続を開き、TCP 接続を閉じるのではなく、single-connection オプションによって、ルータとデーモン間の単一のオープンな接続を保守します。この方法はデーモンが処理できる TACACS 操作数が多くなるため、効率的です。

（注） この処理を有効にするには、デーモンが single-connection モードをサポートする必要があります。サポートしていない場合、ネットワーク アクセス サーバとデーモン間の接続が動作しなくなるか、不要なエラーを受信します。

- **port** *integer* 引数を使用して、TACACS+ デーモンに接続するときに使用される TCP ポート番号を指定します。デフォルト ポート番号は 49 です。
- **timeout** *integer* 引数を使用して、ルータがタイムアウトしてエラー宣言するまで、デーモンからの応答を待つ期間（秒）を指定します。

（注） **tacacs-server host** コマンドによるタイムアウト値の指定は、このサーバに関する **tacacs-server timeout** コマンドで設定されたデフォルトのタイムアウト値よりも優先されます。

- **key** *string* 引数を指定して、ネットワーク アクセス サーバと TACACS+ デーモン間のすべてのトラフィックを暗号化および復号化するための暗号キーを指定します。

（注） **tacacs-server host** コマンドによる暗号キーの指定は、このサーバに関するグローバル コンフィギュレーションの **tacacs-server key** コマンドで設定されたデフォルト キーよりも優先されます。

tacacs-server host コマンドのパラメータの一部は、**tacacs-server timeout** コマンドおよび **tacacs-server key** コマンドによるグローバル設定よりも優先されるため、このコマンドを使用して個別の TACACS+ 接続を一意に設定することで、ネットワークのセキュリティを強化できます。

TACACS 認証キーの設定

グローバル TACACS+ 認証キーおよび暗号化キーを設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
`Router(config)# tacacs-server key key`	TACACS+ デーモンで使用する、一致する暗号キーを設定します。

（注） 暗号化が成功するには、TACACS+ デーモンに同じキーを設定する必要があります。

AAA サーバ グループの設定

AAA サーバ グループを使用するようにルータを設定すると、既存のサーバ ホストをグループ化できます。これによって、設定したサーバホストのサブセットを選択し、それを特定のサービスに使用できます。サーバ グループは、グローバル サーバ ホスト リストと併せて使用されます。サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

サーバ グループには複数のホスト エントリを含めることができます。ただし、各エントリの IP アドレスが一意である必要があります。そのサーバ グループにある異なる 2 つのホスト エントリが 1 つのサービス（アカウンティングなど）に設定されている場合、設定されている 2 番めのホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウンティング サービスの提供に失敗すると、2番めのホストエントリを使用してアカウンティング サービスを提供するように、ネットワーク アクセス サーバが試行します（試行される TACACS+ ホスト エントリの順番は、設定されている順序に従います）。

サーバ グループ名を使用してサーバホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバは、グローバル コンフィギュレーション モードに存在します。

手順の概要

1. Router(config)# **tacacs-server host** *name* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]
2. Router(config-if)# **aaa group server**{**radius** | **tacacs+**} *group-name*
3. Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **tacacs-server host** *name* [**single-connection**] [**port** *integer*] [**timeout** *integer*] [**key** *string*]	サーバ ホストの IP アドレスを指定および定義してから、AAA サーバ グループを設定します。**tacacs-server host** コマンドの詳細については、この章の「TACACS サーバ ホストの指定」セクションを参照してください。
ステップ 2	Router(config-if)# **aaa group server**{**radius** | **tacacs+**} *group-name*	グループ名を指定して AAA サーバ グループを定義します。グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または TACACS+ です。このコマンドでは、サーバ グループのサブコンフィギュレーション モードにルータを配置します。
ステップ 3	Router(config-sg)# **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]	特定の TACACS+ サーバを定義済みのサーバ グループと関連付けます。**auth-port** *port-number* オプションを使用して、認証専用の UDP ポートを設定します。**acct-port** *port-number* オプションを使用して、アカウンティング専用の UDP ポートを設定します。 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。 （注） グループの各サーバは、**tacacs-server host** コマンドを使用して事前に定義する必要があります。

DNIS に基づく AAA サーバ グループの選択の設定

Cisco IOS XE ソフトウェアを使用すると、セッションの Dialed Number Identification Service（DNIS）番号に基づき、特定の AAA サーバ グループに対してユーザを認証できます。すべての電話回線（通常の自宅電話または商用の T1/PRI 回線）を、複数の電話番号と関連付けることができます。DNIS 番号は、ユーザ宛てに発信された番号を示します。

たとえば、複数の顧客で同じ電話番号を共有する場合に、電話を受ける前に発信元を知りたいことがあります。DNIS を使用すると、応答するときに発信元の顧客がわかるため、電話に応答する方法をカスタマイズできます。

ISDN または内部モデムと接続する Cisco ルータは、DNIS 番号を受信できます。この機能を使用すると、顧客ごとに異なる TACACS+ サーバ グループを割り当て可能です（つまり、DNIS 番号ごとに異なる TACACS+ サーバ）。さらに、サーバ グループを使用して、複数の AAA サービスに同じサーバ グループを指定できます。また、各 AAA サービスに個別のサーバ グループを指定できます。

Cisco IOS XE ソフトウェアには、認証サービスとアカウンティング サービスを複数の方法で実装できる柔軟性があります。

- グローバル：AAA サービスは、グローバル コンフィギュレーション アクセス リスト コマンドを使用して定義され、特定のネットワーク アクセス サーバ上のすべてのインターフェイスに、全般的に適用されます。
- インターフェイス別：AAA サービスは、インターフェイス コンフィギュレーション コマンドを使用して定義され、特定のネットワーク アクセス サーバに設定されているインターフェイスにだけ適用されます。
- DNIS マッピング：DNIS を使用して、AAA サーバが AAA サービスを提供するように指定します。

複数の AAA コンフィギュレーション方式を同時に設定できるため、シスコでは、AAA サービスを提供するサーバまたはサーバ グループを決定するために、優先順位を設定しました。優先順位は次のとおりです。

- DNIS 別：AAA サービスを提供するサーバ グループを DNIS によって指定するようネットワーク アクセス サーバを設定している場合、この方式がその他の AAA 選択方式よりも優先されます。
- インターフェイス別：サーバから AAA サービスを提供する方法をアクセス リストによって決定するように、インターフェイスごとにネットワーク アクセス サーバを設定している場合、この方式が他のグローバル コンフィギュレーション AAA アクセス リストよりも優先されます。
- グローバル：セキュリティ サーバが AAA サービスを提供する方法を決定するために、グローバル AAA アクセス リストを使用してネットワーク アクセス サーバを設定する場合、この方式には最も低い優先度が使用されます。

（注） DNIS に基づいて AAA サーバ グループの選択を設定する前に、各 AAA サーバ グループに関連付けられたリモート セキュリティ サーバを設定する必要があります。「TACACS サーバ ホストの指定」および「AAA サーバ グループの設定」を参照してください。

サーバ グループの DNIS に基づいて、特定の AAA サーバ グループを選択するようにルータを設定するには、DNIS マッピングを設定します。DNIS 番号を使用して、サーバ グループをグループ名とマッピングするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa dnis map enable**
2. Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*
3. Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **aaa dnis map enable**	DNIS マッピングをイネーブルにします。
ステップ 2	Router(config)# **aaa dnis map** *dnis-number* **authentication ppp group** *server-group-name*	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、認証に使用されます。
ステップ 3	Router(config)# **aaa dnis map** *dnis-number* **accounting network** [**none** | **start-stop** | **stop-only**] **group** *server-group-name*	DNIS 番号を定義済みの AAA サーバ グループにマッピングします。このサーバ グループのサーバは、アカウンティングに使用されます。

TACACS 認証の指定

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。詳細については、「認証の設定」の章を参照してください。

TACACS 認可の指定

AAA 認可により、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+ を介する認可は、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+ 認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。詳細については、「認可の設定」の章を参照してください。

TACACS アカウンティングの指定

AAA アカウンティングを使用すると、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。AAA によって TACACS+ アカウンティングは容易になるため、アカウンティング方式として TACACS+ を指定して、**aaa accounting** コマンドを発行する必要があります。詳細については、「アカウンティングの設定」の章を参照してください。

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。サポートされる TACACS+ の AV ペアのリストについては、「TACACS 属性値ペア」の章を参照してください。

TACACS の設定例

TACACS 認証の例

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。

TACACS 認可の例

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認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認可を設定します。認証リストとは異なり、この認可リストは、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。

TACACS アカウンティングの例

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。

TACACS サーバ グループの例

次に、3 つの異なる TACACS+ サーバ メンバを使用してサーバ グループを作成する例を示します。

```
aaa group server tacacs tacgroup1
server 172.16.1.1
server 172.16.1.21
server 172.16.1.31
```

DNIS に基づく AAA サーバ グループの選択の設定例

次に、特定の AAA サービスを提供するために、DNIS に基づいて TACACS+ サーバ グループを選択する例を示します。

```
! This command enables AAA.
aaa new-model
!
! The following set of commands configures the TACACS+ servers that will be associated
! with one of the defined server groups.
tacacs-server host 172.16.0.1
tacacs-server host 172.17.0.1
tacacs-server host 172.18.0.1
tacacs-server host 172.19.0.1
tacacs-server host 172.20.0.1
tacacs-server key abcdefg
! The following commands define the sg1 TACACS+ server group and associate servers
! with it.
aaa group server tacacs sg1
  server 172.16.0.1
  server 172.17.0.1
! The following commands define the sg2 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg2
  server 172.18.0.1
! The following commands define the sg3 TACACS+ server group and associate a server
! with it.
aaa group server tacacs sg3
  server 172.19.0.1
! The following commands define the default-group TACACS+ server group and associate
! a server with it.
aaa group server tacacs default-group
  server 172.20.0.1
!
! The next set of commands configures default-group tacacs server group parameters.
aaa authentication ppp default group default-group
aaa accounting network default start-stop group default-group
!
! The next set of commands enables DNIS mapping and maps DNIS numbers to the defined
! RADIUS server groups. In this configuration, all PPP connection requests using DNIS
! 7777 are sent to the sg1 server group. The accounting records for these connections
! (specifically, start-stop records) are handled by the sg2 server group. Calls with a
! DNIS of 8888 use server group sg3 for authentication and server group default-group
! for accounting. Calls with a DNIS of 9999 use server group default-group for
! authentication and server group sg3 for accounting records (stop records only). All
! other calls with DNIS other than the ones defined use the server group default-group
! for both authentication and stop-start accounting records.
aaa dnis map enable
aaa dnis map 7777 authentication ppp group sg1
aaa dnis map 7777 accounting network start-stop group sg2
aaa dnis map 8888 authentication ppp group sg3
aaa dnis map 9999 accounting network stop-only group sg3
```

TACACS デーモンの設定例

次に、TACACS+ デーモンの設定例を示します。実際に TACACS+ デーモンで使用する正確な構文は、この例の構文と異なる可能性があります。

```
user = mci_customer1 {
 chap = cleartext “some chap password”
 service = ppp protocol = ip {
inacl#1=”permit ip any any precedence immediate”
inacl#2=”deny igrp 0.0.1.2 255.255.0.0 any”
 }
```

その他の参考資料

ここでは、TACACS+ の設定機能に関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
TACACS+ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索し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

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	Link
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/en/US/support/index.html

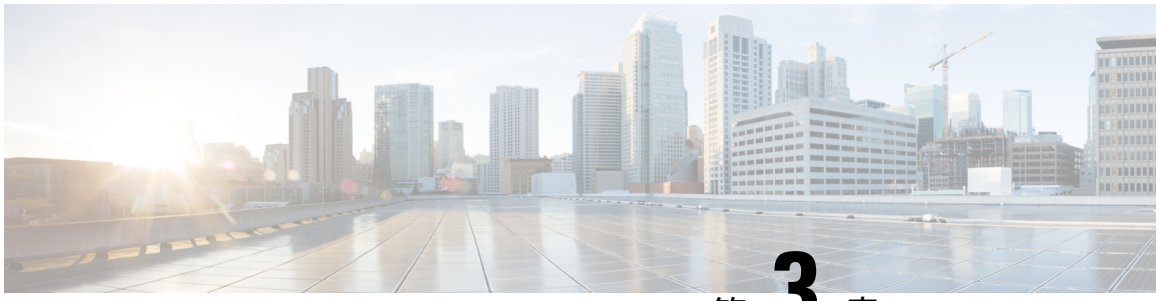
TACACS の設定に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : TACACS+* の設定に関する機能情報

機能名	リリース	機能情報
TACACS+		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、認証および認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、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできます。 次のコマンドが導入または変更されました：**tacacs-server host**、**tacacs-server key**、**aaa authentication**、 **aaa accounting**、**aaa group server tacacs+**。
DNIS に基づく AAA サーバ グループ		DNIS に基づく AAA サーバ グループを使用すると、セッションの着信番号識別サービス（DNIS）番号に基づき、特定の AAA サーバ グループに対してユーザを認証できます。 次のコマンドが導入または変更されました。**aaa dnis map enable**、**aaa dnis map authentication group**、**aaa dnis map accounting**



第 3 章

TACACS サーバの Per VRF

TACACS+ サーバの Per VRF 機能により、TACACS+ サーバで Per Virtual ルーティングおよび転送（Per VRF）の認証、認可、アカウンティング（AAA）を設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

TACACS サーバの Per VRF の前提条件

- TACACS+ サーバ アクセスが必要です。
- TACACS+、AAA および Per VRF AAA、およびグループ サーバ設定の経験が必要です。

TACACS サーバの Per VRF の制限事項

- TACACS+ サーバの Per VRF を設定する前に、ルータで VRF インスタンスをグローバルにイネーブルにする必要があります。

TACACS サーバの Per VRF に関する情報

TACACS サーバの Per VRF の概要

TACACS+ サーバの Per VRF 機能を使用すると、TACACS+ サーバで Per VRF AAA を設定できます。Cisco IOS XE リリース 2.2 よりも前のリリースでは、この機能は RADIUS サーバでのみ使用できました。

TACACS サーバの Per VRF の設定方法

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。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **interface** *interface-name*
7. **ip vrf forwarding** *vrf-name*
8. **ip address** *ip-address mask* [**secondary**]
9. **exit**
10. **aaa group server tacacs+** *group-name*
11. **server-private** {*ip-address* | *name*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [**0** | **7**] *string*]
12. **ip vrf forwarding** *vrf-name*
13. **ip tacacs source-interface** *subinterface-name*
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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： `Router# 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： `Router (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： `Router (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： `Router (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： `Router (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： `Router (config-if)# ip vrf forwarding cisco`	インターフェイスに VRF を設定します。
ステップ 8	**ip address** *ip-address mask* [**secondary**] 例： `Router (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： `Router (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。

	コマンドまたはアクション	目的
ステップ 10	**aaa group server tacacs+** *group-name* 例： `Router (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： `Router (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： `Router (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： `Router (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： `Router (config-sg-tacacs)# exit`	server-group コンフィギュレーション モードを終了します。

TACACS サーバの Per VRF の確認

Per VRF TACACS+ 設定を確認するには、次の手順を実行します。

（注） **debug** コマンドは、任意の順番で使用できます。

注意 デバッグ CLI をイネーブルにすると、ルータのパフォーマンスが低下する可能性があります。多数のセッションに対して **debug** コマンドを使用することはお勧めしません。

手順の概要

1. **enable**

2. **debug tacacs authentication**
3. **debug tacacs authorization**
4. **debug tacacs accounting**
5. **debug tacacs packets**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> 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	**debug tacacs authentication** 例： `Router# debug tacacs authentication`	AAA/TACACS+ 認証に関する情報を表示します。
ステップ 3	**debug tacacs authorization** 例： `Router# debug tacacs authorization`	AAA/TACACS+ 認可に関する情報を表示します。
ステップ 4	**debug tacacs accounting** 例： `Router# debug tacacs accounting`	説明可能なイベントが発生したときに、その情報を表示します。
ステップ 5	**debug tacacs packets** 例： `Router# debug tacacs packets`	TACACS+ パケットに関する情報を表示します。

TACACS サーバの Per VRF の設定例

TACACS サーバの Per VRF の設定例

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
```

その他の参考資料

次のセクションでは、TACACS+ サーバの Per VRF に関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
TACACS+ の設定	「Configuring TACACS+」モジュール。
Per VRF AAA	「Per VRF AAA」モジュール。
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	Title
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	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

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

テクニカル サポート

説明	Link
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/cisco/web/support/index.html

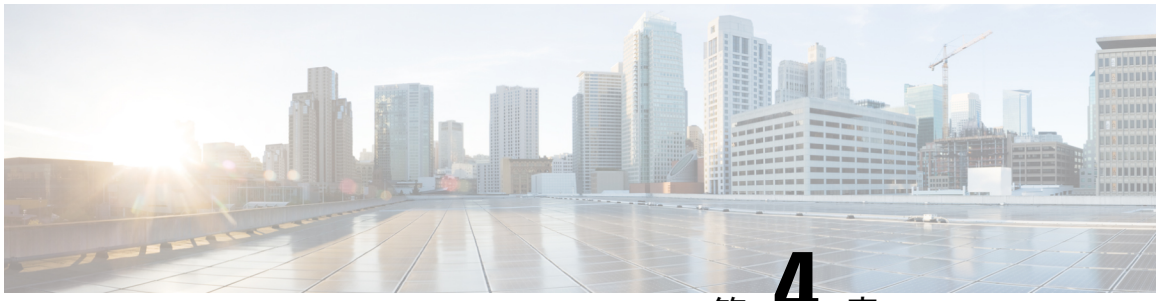
TACACS サーバの Per VRF の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2 : Per VRF for TACACS+ Servers* の機能情報

機能名	リリース	機能情報
Per VRF for TACACS+ Servers	Cisco IOS XE Release 2.2	TACACS+ サーバの Per VRF 機能により、TACACS+ サーバで Per Virtual ルーティングおよび転送（Per VRF）の認証、認可、アカウンティング（AAA）を設定できます。 Cisco IOS XE リリース 2.2 では、Cisco ASR 1000 シリーズ アグリゲーション サービス ルータにこの機能が実装されました。 次のコマンドが導入または変更されました：**ip tacacs source-interface**、**ip vrf forwarding (server-group)**、**server-private (TACACS+)**。



第 4 章

TACACS の属性値ペア

Terminal Access Controller Access Control System Plus（TACACS+）の属性値（AV）ペアは、TACACS+ デーモンに保存されるユーザ プロファイルで特定の認証、認可、およびアカウンティング要素を定義するために使用されます。この章では、現在サポートされている TACACS+ AV ペアの一覧を示します。

TACACS の属性値ペアに関する情報

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 *3*：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	IOS XE 2.1
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。	yes
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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
callback- dialstring	コールバックの電話番号を設定します（例：callback-dialstring=408-555-1212）。値は NULL またはダイヤルストリングです。NULL 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。	yes
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。	yes
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。	yes
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。	yes

属性	説明	IOS XE 2.1
cmd=x	シェル（EXEC）コマンド。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。	yes
data-service	service=outbound および protocol=ip で使用されます。	yes
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。	yes
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。	yes
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。	yes
gw-password	L2TP トンネル認証時のホーム 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。	yes
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。	yes
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。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。	yes
inacl=x	インターフェイス 入力アクセス リストの ASCII 識別名。service=ppp および protocol=ip と使用されます。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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
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。service=ppp および protocol=vpdn で使用されます。	yes
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。	yes
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 と併用。 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	yes
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。	yes
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。	yes
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。	yes
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。	yes

属性	説明	IOS XE 2.1
nas-password	L2TP トンネル認証時のネットワーク 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。	yes
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。	yes
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）。	yes
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）。	yes
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。	yes
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。	yes
outacl=x	インターフェイス 出力アクセス リストの ASCII 識別名。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。	yes
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 と使用されます。	yes

属性	説明	IOS XE 2.1
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 と使用されます。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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 と併用されます。	yes

属性	説明	IOS XE 2.1
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。 ネットワーク認証中、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*、および *gateway* は通常のドット付き 10 進表記での記述を想定されていて、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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
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 と使用されます。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。これは、**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。	yes
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。	yes

属性	説明	IOS XE 2.1
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）。	yes

TACACS+の設定の詳細については、「TACACS+の設定」の章を参照してください。TACACS+の認証および認可の設定について詳しくは、「認証の設定」および「認可の設定」の章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 XE リリースを指定しています。

表 *4:* サポートされる *TACACS+* アカウンティング *AV* ペア

属性	説明	IOS XE 2.1
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。	yes
bytes_in	この接続中に転送される入力バイト数です。	yes
bytes_out	この接続中に転送される出力バイト数です。	yes
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。	yes
cmd	ユーザが実行したコマンドです。	yes
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。	yes
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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
Fax-Dsn-Address	DSN の送信先のアドレスを示します。	yes
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。	yes
Fax-Mdn-Address	MDN の送信先のアドレスを示します。	yes
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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
paks_in	この接続中に転送される入力パケット数です。	yes
paks_out	この接続中に転送される出力パケット数です。	yes
port	ユーザがログインしたポートです。	yes
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。	yes

属性	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
priv_level	処理に関連付けられた権限レベルです。	yes
protocol	処理に関連付けられたプロトコルです。	yes
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。	yes
service	ユーザが使用するサービスです。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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 *5 : Disconnect Cause Extensions*

原因コード	説明	IOS XE 2.1
1000 – 理由なし	接続解除の理由はありません。	yes
1001 – 接続解除なし	イベントは接続解除されませんでした。	yes
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。	yes
1003 – コール接続解除	コールが接続解除されました。	yes
1004 – CLID 認証失敗	Calling line ID（CLID）認証が失敗しました。	yes
1009 – モデム使用不可	モデムが使用できません。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

原因コード	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

原因コード	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

原因コード	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

原因コード	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
1150 – Radius 接続解除	RADIUS サーバが接続解除を要求しました。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes

原因コード	説明	IOS XE 2.1
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	yes
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。	no
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。	no

原因コード	説明	IOS XE 2.1
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no

原因コード	説明	IOS XE 2.1
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no

原因コード	説明	IOS XE 2.1
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no

原因コード	説明	IOS XE 2.1
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no
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。	no

原因コード	説明	IOS XE 2.1
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。	no
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。	no
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。	no
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。	no
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。	no

TACACS+ アカウンティングの設定の詳細については、「TACACS+ 機能の設定」モジュールを参照してください。