CHAPTER 19

TACACS+ の設定

この章では、Cisco Nexus 4001I/4005I Switch Module for IBM BladeCenter 上で、Terminal Access Controller Access Control SystemPlus（TACACS+）プロトコルを設定する方法について説明します。

この章で説明する内容は、次のとおりです。

TACACS+ について

TACACS+ セキュリティ プロトコルを使用すると、スイッチへのアクセスを試みるユーザの検証を一元化できます。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実行されている TACACS+ デーモン上のデータベースで管理されます。設定済みの TACACS+ 機能をスイッチ上で使用するには、TACACS+ サーバへのアクセス権を持ち、このサーバを設定する必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。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。各サービスは固有のデータベースにアソシエートされており、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上で使用可能な他のサービスを利用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。スイッチ は、TACACS+ プロトコルを使用して集中型の認証を行います。

ここでは、次の内容について説明します。

- 「TACACS+ サーバのモニタリング」（P.19-3）

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、スイッチは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行する。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現する。RADIUS プロトコルはパスワードだけを暗号化します。

TACACS+ を使用したユーザ ログイン

ユーザが TACACS+ を使用して、スイッチに対し Password Authentication Protocol（PAP; パスワード認証プロトコル）によるログインを試行すると、次のプロセスが実行されます。

1. スイッチが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。

（注）　TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。この動作では通常、ユーザ名とパスワードの入力が要求されますが、ユーザの母親の旧姓など、その他の項目の入力が要求されることもあります。

2. スイッチが、TACACS+ デーモンから次のいずれかの応答を受信します。
   - ACCEPT：ユーザの認証に成功したので、サービスを開始します。スイッチがユーザの許可を要求している場合は、許可が開始されます。
   - REJECT：ユーザの認証に失敗しました。TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。
   - ERROR：認証中に、デーモン内、またはデーモンとスイッチ間のネットワーク接続でエラーが発生しました。スイッチが ERROR 応答を受信した場合、スイッチは代わりのユーザ認証方式を試します。

   スイッチで許可がイネーブルになっている場合は、この後、許可フェーズの処理が実行されます。TACACS+ 許可に進むには、まず TACACS+ 認証を正常に終了する必要があります。
3. TACACS+ 許可が必要な場合、スイッチは、再度、TACACS+ デーモンにアクセスします。デーモンは ACCEPT または REJECT 許可応答を返します。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

   サービスには次が含まれます。
   - Telnet、rlogin、Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）、Serial Line Internet Protocol（SLIP; シリアル ライン インターネット プロトコル）、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（IPv4 または IPv6）、アクセスリスト、ユーザ タイムアウト）

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

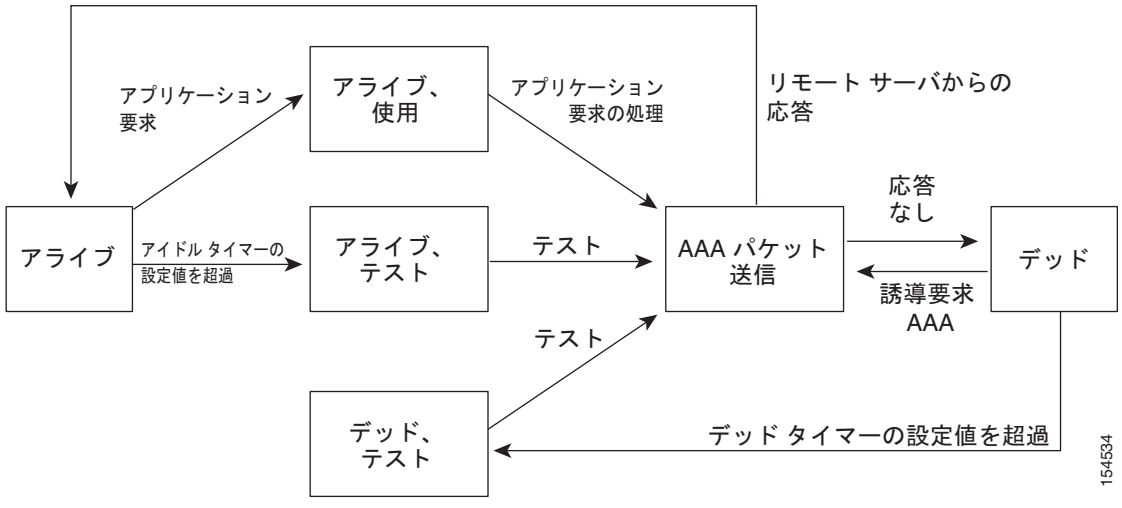
TACACS+ サーバに対してスイッチを認証するには、TACACS+ 事前共有キーを設定する必要があります。事前共有キーとは、スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。スイッチ上のすべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

グローバルな事前共有キーの設定は、個々の TACACS+ サーバの設定時に明示的に **key** オプションを使用することによって無効にできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を節約するため、スイッチは定期的に TACACS+ サーバをモニタリングし、TACACS+ サーバが応答を返す（アライブ）かどうかを調べることができます。スイッチは、応答を返さない TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。またスイッチは、定期的にデッド TACACS+ サーバをモニタリングし、それらが応答を返したらアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、TACACS+ サーバが稼動状態であることを確認します。TACACS+ サーバの状態がデッドまたはアライブに変わると、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが生成され、スイッチによって、パフォーマンスに影響が出る前に、障害が発生していることを知らせるエラー メッセージが表示されます。図 19-1 を参照してください。

図 19-1　TACACS+ サーバの状態



（注）　アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+ サーバ モニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 または IPv6IP アドレスまたはホスト名を取得していること。
- TACACS+ サーバから事前共有キーを取得していること。
- スイッチが、AAA サーバの TACACS+ クライアントとして設定されていること。

注意事項と制限事項

スイッチ上に設定できる TACACS+ サーバの最大数は 64 です。

TACACS+ の設定

ここでは、次の内容について説明します。

TACACS+ サーバの設定プロセス

TACACS+ サーバを設定する手順は、次のとおりです。

ステップ 1　TACACS+ をイネーブルにします。

「TACACS+ のイネーブル化」（P.19-5）を参照してください。

ステップ 2　TACACS+ サーバとスイッチとの接続を確立します。

「TACACS+ サーバ ホストの設定」（P.19-5）を参照してください。

ステップ 3　TACACS+ サーバの事前共有秘密キーを設定します。

「グローバルな事前共有キーの設定」（P.19-6）および「TACACS+ サーバの事前共有キーの設定」（P.19-7）を参照してください。

ステップ 4　必要に応じて、AAA 認証方式用に、TACACS+ サーバのサブセットを使用して TACACS+ サーバ グループを設定します。

「TACACS+ サーバ グループの設定」（P.19-7）および第 17 章「AAA の設定」を参照してください。

ステップ 5　必要に応じて、次のオプションのパラメータを設定します。

- デッドタイム間隔
- ログイン時に TACACS+ サーバの指定を許可
- タイムアウト間隔

  「グローバルな TACACS+ タイムアウト間隔の設定」（P.19-9）を参照してください。
- TCP ポート

  「TCP ポートの設定」（P.19-10）を参照してください。

ステップ 6　必要に応じて、定期的に TACACS+ サーバをモニタリングするよう設定します。

「TACACS+ サーバの定期的モニタリングの設定」（P.19-11）を参照してください。

TACACS+ のイネーブル化

デフォルトでは、スイッチで TACACS+ 機能はディセーブルに設定されています。TACACS+ 機能を明示的にイネーブルにして、認証用の設定コマンドおよび確認コマンドにアクセスする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバにアクセスするには、スイッチ上に、TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を設定する必要があります。すべての TACACS+ サーバ ホストは、デフォルトの TACACS+ サーバ グループに追加されます。最大 64 の TACACS+ サーバを設定できます。

設定済みの TACACS+ サーバに事前共有キーが設定されておらず、グローバル キーも設定されていない場合は、警告メッセージが表示されます。TACACS+ サーバ キーが設定されていない場合は、グローバル キー（設定されている場合）が該当サーバで使用されます（「グローバルな事前共有キーの設定」（P.19-6）および「TACACS+ サーバの事前共有キーの設定」（P.19-7）を参照）。

TACACS+ サーバ ホストを設定する前に、次の点を確認してください。

- TACACS+ がイネーブルになっていること（「TACACS+ のイネーブル化」（P.19-5）を参照）。
- リモート TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること。

TACACS+ サーバ ホストを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server host {ipv4-address | ipv6-address|host-name}`	TACACS+ サーバの IP アドレス（IPv4 または IPv6）、またはホスト名を指定します。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サーバ グループから TACACS+ サーバ ホストを削除できます。

グローバルな事前共有キーの設定

スイッチで使用するすべてのサーバについて、グローバル レベルで事前共有キーを設定できます。事前共有キーとは、スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

事前共有キーを設定する前に、次の点を確認してください。

- TACACS+ がイネーブルになっていること（「TACACS+ のイネーブル化」（P.19-5）を参照）。
- リモートの TACACS+ サーバの事前共有キー値を取得していること。

グローバルな事前共有キーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server key [0|7] key-value`	すべての TACACS+ サーバで使用する事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。キーの最大長は 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、グローバルな事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEfThUkO
switch(config)# exit
```

```
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバの事前共有キーの設定

TACACS+ サーバの事前共有キーを設定できます。事前共有キーとは、スイッチと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

TACACS+ 事前共有キーを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server host {ipv4-address|ipv6-address|host-name} key [0|7] key-value`	特定の TACACS+ サーバの事前共有キーを指定します。クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。デフォルトの形式はクリア テキストです。キーの最大長は 63 文字です。 この事前共有キーがグローバル共有キーの代わりに使用されます。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。 **（注）** 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ 事前共有キーを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて、TACACS+ プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループは随時設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。AAA サービスについては、第 17 章「AAA の設定」を参照してください。

TACACS+ サーバ グループを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# aaa group server tacacs+ group-name`	TACACS+ サーバ グループを作成し、そのグループの TACACS+ サーバ グループ 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	`switch(config-tacacs+)# server {ipv4-address|ipv6-address|host-name}`	TACACS+ サーバを、TACACS+ サーバ グループのメンバーとして設定します。 **ヒント** 指定した TACACS+ サーバが見つからない場合は、**tacacs-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	`switch(config-tacacs+)# deadtime minutes`	（任意）モニタリング デッド タイムを設定します。デフォルトは 0 分です。指定できる範囲は 0 ～ 1440 です。 **（注）** TACACS+ サーバ グループのデッド タイム間隔が 0 より大きい場合は、その値がグローバルなデッド タイム値より優先されます。
ステップ 5	`switch(config-tacacs+)# exit`	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	`switch(config)# show tacacs-server groups`	（任意）TACACS+ サーバ グループの設定を表示します。
ステップ 7	`switch(config)# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバ グループを設定する例を示します。

```
switch# configure terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# exit
switch(config)# show tacacs-server groups
switch(config)# copy running-config startup-config
```

ログイン時の TACACS+ サーバの指定

認証要求の送信先 TACACS+ サーバをユーザが指定できるようにスイッチを設定するには、directed-request オプションをイネーブルにします。デフォルトでは、スイッチは、デフォルトの AAA 認証方式に基づいて認証要求を転送します。このオプションをイネーブルにすると、ユーザは *username@hostname* としてログインできます。ここで、*hostname* は設定済みの RADIUS サーバの名前です。

（注） ユーザ指定のログインは、Telnet セッションでのみサポートされます。

ログイン時に TACACS+ サーバを指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server directed-request`	ログイン時に、ユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。デフォルトはディセーブルです。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server directed-request`	（任意）TACACS+ の directed request の設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

グローバルな TACACS+ タイムアウト間隔の設定

スイッチが、タイムアウト エラーを宣言する前に、すべての TACACS+ サーバからの応答を待機するグローバルなタイムアウト間隔も設定できます。タイムアウト間隔は、スイッチがタイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機する時間を決定します。

TACACS+ グローバル タイムアウト間隔を指定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server timeout` *seconds*	TACACS+ サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

サーバのタイムアウト間隔の設定

スイッチが、タイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。タイムアウト間隔は、スイッチがタイムアウト エラーを宣言する前に、TACACS+ サーバからの応答を待機する時間を決定します。

サーバのタイムアウト間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# switch(config)# tacacs-server host {ipv4-address|ipv6-address|host-name} timeout seconds`	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 （注）　特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。デフォルトでは、スイッチは、すべての TACACS+ 要求にポート 49 を使用します。

TCP ポートを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server host {ipv4-address|ipv6-address|host-name} port tcp-port`	TACACS+ アカウンティング メッセージ用の UDP ポートを指定します。デフォルトの TCP ポートは 49 です。指定できる範囲は 1 ～ 65535 です。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TCP ポートを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 port 2
switch(config)# exit
switch# show tacacs-server
switch# copy running-config startup-config
```

TACACS+ サーバの定期的モニタリングの設定

TACACS+ サーバの可用性をモニタリングできます。パラメータとして、サーバに使用するユーザ名とパスワード、およびアイドル タイマーがあります。アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、スイッチがテスト パケットを送信するかを指定します。このオプションを設定して、サーバを定期的にテストしたり、1 回だけテストを実行できます。

（注） ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。

テスト アイドル タイマーには、TACACS+ サーバがどのくらいの期間要求を受信しなかった場合に、スイッチがテスト パケットを送信するかを指定します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

TACACS+ サーバの定期的なモニタリングを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server host {ipv4-address | ipv6-address | host-name} test {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}`	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。 **（注）** TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	`switch(config)# tacacs-server dead-time minutes`	スイッチが、前回応答しなかった TACACS+ サーバをチェックするまでの時間（分）を指定します。デフォルト値は 0 分、指定できる範囲は 0 ～ 1440 分です。
ステップ 4	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 5	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 6	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

次に、TACACS+ サーバの定期的モニタリングを設定する例を示します。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
```

```
switch# show tacacs-server
switch# copy running-config startup-config
```

デッド タイム間隔の設定

すべての TACACS+ サーバのデッド タイム間隔を設定できます。デッド タイム間隔には、スイッチが TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。

（注）　デッド タイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デットとしてマークされません。デッド タイマーはグループ単位で設定できます（「TACACS+ サーバ グループの設定」（P.19-7）を参照）。

すべての TACACS+ サーバのデッド タイム間隔を設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# tacacs-server deadtime` *minutes*	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 分です。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# show tacacs-server`	（任意）TACACS+ サーバの設定を表示します。
ステップ 5	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバまたはサーバ グループの手動モニタリング

TACACS+ サーバまたはサーバ グループにテスト メッセージを手動で送信する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# test aaa server tacacs+` {*ipv4-address*|*ipv6-address*|*host-name*} [**vrf** *vrf-name*] *username password*	TACACS+ サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	`switch# test aaa group` *group-name username password*	TACACS+ サーバ グループにテスト メッセージを送信して可用性を確認します。

次に、手動でテスト メッセージを送信する例を示します。

```
switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group TacGroup user2 As3He3CI
```

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。

注意　TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

TACACS+ をディセーブルにする手順は、次のとおりです。

	コマンド	目的
ステップ 1	`switch# configure terminal`	コンフィギュレーション モードを開始します。
ステップ 2	`switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。
ステップ 3	`switch(config)# exit`	コンフィギュレーション モードを終了します。
ステップ 4	`switch# copy running-config startup-config`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

TACACS+ 統計情報の表示

スイッチが TACACS+ のアクティビティについて保持している統計情報を表示する手順は、次のとおりです。

コマンド	目的
`switch# show tacacs-server statistics {hostname|ipv4-address|ipv6-address}`	TACACS+ 統計情報を表示します。

このコマンドの出力に表示される各フィールドの詳細については、『*Cisco Nexus 4000I and 4005I Switch Module for IBM BladeCenter NX-OS Command Reference*』を参照してください。

TACACS+ の設定の確認

TACACS+ の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config tacacs [**all**]	実行コンフィギュレーションの TACACS+ 設定を表示します。
show startup-config tacacs	スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
show tacacs-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての TACACS+ サーバのパラメータを表示します。

TACACS+ の設定例

次に、TACACS+ を設定する例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config)# tacacs-server key 7 "ToIkLhPpG"
switch(config)# tacacs-server host 10.10.2.2 key 7 "ShMoMhT1"
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
switch(config-tacacs+)# use-vrf management
```

デフォルト設定

表 19-1 に、TACACS+ パラメータのデフォルト設定を示します。

表 19-1　TACACS+ のデフォルト パラメータ

パラメータ	デフォルト
TACACS+	ディセーブル
デッド タイマー間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test