tacacs-server administration から title-color まで

tacacs server

IPv6 または IPv4 の TACACS+ サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tacacs server** コマンドを使用します。 設定を削除するには、このコマンドの **no** 形式を使用します。

tacacs server *name*

no tacacs server

構文の説明

name	プライベート TACACS+ サーバ ホストの名前。

コマンド デフォルト

TACACS+ サーバは設定されていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

tacacs server コマンドは、*name* 引数を使用して TACACS サーバを設定し、TACACS+ サーバ コンフィギュレーション モードを開始します。 この設定は、設定を終了し、TACACS+ サーバ コンフィギュレーション モードを終了すると適用されます。

例

次に、名前 server1 を使用して TACACS+ サーバ コンフィギュレーション モードを開始し、TACACS サーバを設定する例を示します。

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

関連コマンド

コマンド	説明
address ipv6（**TACACS+**）	TACACS+ サーバの IPv6 アドレスを設定します。

コマンド	説明
key（**TACACS+**）	TACACS+ サーバでサーバ単位の暗号キーを設定します。
port（**TACACS+**）	TACACS+ 接続に使用する TCP ポートを指定します。
send-nat-address（**TACACS+**）	クライアントの NAT 後のアドレスを TACACS+ サーバに送信します。
single-connection（**TACACS+**）	単一の TCP 接続を使用してすべての TACACS パケットを同じサーバに送信できるようにします。
timeout（**TACACS+**）	指定された TACACS サーバからの応答を待機する時間を設定します。

tacacs-server host

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 **tacacs-server host** コマンドを使用します。 指定された名前またはアドレスを削除するには、このコマンドの **no** 形式を使用します。

tacacs-server host{*host-name*| *host-ip-address*}[**key***string*][**[nat]**[**port**[*integer*]]**[single-connection]**[**timeout**[*integer*]]]

no tacacs-server host{*host-name*| *host-ip-address*}

構文の説明

host-name	ホストの名前。
host-ip-address	ホストの IP アドレス。
key	（任意）認証および暗号キーを指定します。 これは TACACS+ デーモンで使用されるキーと一致する必要があります。 このキーを指定すると、このサーバに限り、グローバル コマンド **tacacs-server key** で設定されているキーが上書きされます。
string	（任意）認証および暗号キーを指定する文字列。
nat	（任意）クライアントのポート ネットワーク アドレス変換（NAT）アドレスが TACACS+ サーバに送信されます。
port	（任意）TACACS+ サーバのポート番号を指定します。 この設定によって、デフォルトのポート 49 は上書きされます。
integer	（任意）サーバのポート番号です。 有効なポート番号の範囲は 1 ～ 65535 です。
single-connection	（任意）ルータと TACACS+ サーバ間で単一のオープンな接続を保守します。
timeout	（任意）タイムアウト値を指定します。 これによって、**tacacs-server timeout** コマンドで設定したグローバル タイムアウト値がこのサーバに限り上書きされます。

integer	（任意）タイムアウト間隔の整数値（秒単位）。 値は 1 ～ 1000 です。

コマンド デフォルト

TACACS+ ホストは指定されません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.1(11)、12.2(6)	**nat** キーワードが追加されました。
12.2(8)T	**nat** キーワードが、Cisco IOS Release 12.2(8)T に統合されました。
12.2(33)SRA	このコマンドが Cisco IOS Release 12.(33)SRA に統合されました。
12.2SX	このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。 このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャセット、プラットフォーム、およびプラットフォームハードウェアによって異なります。

使用上のガイドライン

複数の **tacacs-server host** コマンドを使用して、追加のホストを指定できます。 Cisco IOS ソフトウェアは、指定された順序でホストを検索します。 AAA/TACACS+ サーバを実行している場合のみ、**port**、**timeout**、**key**、**single-connection**、および **nat** キーワードを使用します。

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ルータ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。

single-connection キーワードは、単一の接続を指定します（CiscoSecure Release 1.0.1 以降でのみ有効）。 通信が必要になるたびに、ルータが TCP 接続を開閉するのではなく、single-connection オプションによって、ルータとサーバ間の単一のオープンな接続を保守します。 単一の接続のほうが、サーバがより多くの TACACS 操作を処理できるようになるため、より効率的です。

例

次に、Sea_Change という名前の TACACS+ ホストを指定する例を示します。

```
tacacs-server host Sea_Change
```

次に、認証、許可、アカウンティング（AAA）、AAA(AAA)の確認のために、ルータがポート番号51でSea_Cureという名前のTACACS+サーバホストに打診することを指定する例を示します。この接続における要求のタイムアウト値は3秒で、暗号キーはa_secretです。

```
tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

関連コマンド

コマンド	説明
aaa authentication	AAA 認証を指定するか、またはイネーブルにします。
aaa authorization	ネットワークへのユーザアクセスを制限するパラメータを設定します。
aaa accounting	課金またはセキュリティのために、要求されたサービスの AAA アカウンティングをイネーブルにします。
ppp	PPP を使用して非同期接続を開始します。
slip	SLIP を使用してリモート ホストへのシリアル接続を開始します。
tacacs-server key	アクセス サーバと TACACS+デーモンとのすべての TACACS+ 通信に使用される認証暗号キーを設定します。

telnet

Telnetをサポートしているホストにログインするには、ユーザEXECモードまたは特権EXECモードで **telnet** コマンドを使用します。

telnet *host* [*port*] [*keyword*]

構文の説明

host	ホスト名または IP アドレス。
port	（任意）10 進数の TCP ポート番号またはポート名。デフォルトはホストの Telnet のルータポート（10 進数値 23）。
keyword	（任意）次の表にリストされているキーワードいずれか 1 つ。

コマンド モード

ユーザ EXEC 特権 EXEC

コマンド履歴

リリース	変更内容
10.0	このコマンドが導入されました。
12.0(21)ST	**/ipv4** キーワードおよび **/ipv6** キーワードが追加されました。
12.1	**/quiet** キーワードが追加されました。
12.2(2)T	**/ipv4** キーワードおよび **/ipv6** キーワードが追加されました。
12.0(22)S	このコマンドが、Cisco IOS Release 12.0(22)S に統合されました。
12.2(14)S	このコマンドが、Cisco IOS Release 12.2(14)S に統合されました。
12.2(28)SB	このコマンドが、Cisco IOS Release 12.2(28)SB に統合されました。
12.2(25)SG	このコマンドが、Cisco IOS Release 12.2(25)SG に統合されました。
12.2(33)SXH	このコマンドが、Cisco IOS Release 12.2(33)SXH に統合されました。

リリース	変更内容
Cisco IOS XE Release 2.1	このコマンドは、Cisco ASR 1000 シリーズ ルータで追加されました。

使用上のガイドライン

次の表は、オプションの **telnet** コマンド キーワードのリストです。

表 *1* : ***telnet*** キーワード オプション

オプション	説明
/debug	Telnet デバッグ モードをイネーブルにします。
/encrypt kerberos	暗号化された Telnet セッションをイネーブルにします。 このキーワードは、Kerberos 対応 Telnet サブシステムがある場合にだけ使用できます。 Kerberos 証明書を使用して認証を実行する場合、このキーワードの使用により、リモート サーバとの暗号化ネゴシエーションが開始されます。暗号化ネゴシエーションが失敗すると、Telnet 接続がリセットされます。 暗号化ネゴシエーションが成功すると、Telnet 接続が確立され、暗号化モードで引き続き Telnet セッションが続行されます（セッションではすべての Telnet トラフィックが暗号化されます）。
/ipv4	IP プロトコルのバージョン 4 を指定します。IPv4 と IPv6 プロトコル スタックの両方をサポートするネットワークで IP プロトコルのバージョンが指定されていない場合、IPv6 が最初に試行され、次に IPv4 が試行されます。
/ipv6	IP プロトコルのバージョン 6 を指定します。IPv4 と IPv6 プロトコル スタックの両方をサポートするネットワークで IP プロトコルのバージョンが指定されていない場合、IPv6 が最初に試行され、次に IPv4 が試行されます。

オプション	説明
/line	Telnet 回線モードをイネーブルにします。 このモードでは、ユーザが **Enter** キーを押すまで Cisco IOS ソフトウェアはホストにデータを送信しません。 標準の Cisco IOS ソフトウェアのコマンド編集文字を使用して回線を編集できます。 **/line** キーワードはローカル スイッチです。リモート ルータには、モードの変更は通知されません。
/noecho	ローカル エコーをディセーブルにします。
/quiet	Cisco IOS ソフトウェアからのすべてのメッセージを画面上に表示しないようにします。
/route: *path*	ルース送信元ルーティングを指定します。 *path* 引数は、最終的な宛先で終了するネットワーク ノードを指定するホスト名または IP アドレスのリストです。
/source-interface	送信元インターフェイスを指定します。
/stream	*stream* 処理をオンにします。これにより、Telnet の制御シーケンスなしの raw TCP ストリームがイネーブルになります。 ストリーム接続は Telnet オプションを処理せず、UNIX 間コピー プログラム（UUCP）や他の非 Telnet プロトコルを実行するポート接続に適している場合があります。
port-number	ポート番号。
bgp	ボーダー ゲートウェイ プロトコル。
chargen	文字ジェネレータ。
cmd *rcmd*	リモート コマンド。
daytime	デイタイム。
discard	廃棄。
domain	ドメイン ネーム サービス。
echo	エコー。

オプション	説明
exec	EXEC
finger	フィンガ。
ftp	File Transfer Protocol（ファイル転送プロトコル）。
ftp-data	FTP データ接続（めったに使用しない）。
gopher	Gopher。
hostname	ホストネーム サーバ。
ident	Ident プロトコル。
irc	インターネット リレー チャット。
klogin	Kerberos ログイン。
kshell	Kerberos シェル。
login	ログイン（rlogin）。
lpd	印刷サービス。
nntp	ネットワーク ニュース トランスポート プロトコル。
pim-auto-rp	Protocol Independent Multicast（PIM）の自動ランデブー ポイント（RP）。
node	特定のローカルエリア トランスポート（LAT）ノードに接続します。
pop2	Post Office Protocol v2。
pop3	Post Office Protocol v3。
port	宛先ローカルエリア トランスポート（LAT）ポート名。
smtp	シンプル メール転送プロトコル。
sunrpc	Sun Remote Procedure Call。

オプション	説明
syslog	Syslog。
tacacs	TACACS セキュリティを指定します。
talk	Talk（517）。
Telnet	Telnet（23）。
time	Time（37）。
uucp	UNIX 間コピー プログラム（540）。
whois	ニックネーム（43）。
www	World Wide Web（HTTP、80）。

Cisco IOS の TCP/IP 実装では、端末接続を確立するために、**connect** または **telnet** コマンドを入力する必要はありません。 次の条件をすべて満たす場合に限り、学習されたホスト名だけを入力できます。

- ホスト名がルータのコマンド ワードとは異なる。
- 優先トランスポート プロトコルが **telnet** に設定されている。

利用可能なホストを一覧表示するには、**show hosts** コマンドを使用します。 すべての TCP 接続のステータスを表示するには、**show tcp** コマンドを使用します。

Cisco IOS ソフトウェアから各接続に論理名が割り当てられ、これらの名前を使用する複数のコマンドによって接続が識別されます。 論理名は、その名前が使用中の場合と、**name-connection** EXEC コマンドで接続名が変更された場合を除き、ホスト名と同じになります。 この名前が使用中の場合、Cisco IOS ソフトウェアによりヌル名が接続に割り当てられます。

Telnet ソフトウェアは Telnet シーケンス形式の特殊な Telnet コマンドをサポートします。このシーケンスは、一般的な端末制御機能をオペレーティング システム固有の機能にマッピングします。特殊な Telnet コマンドを発行するには、エスケープ シーケンスを入力してからコマンド文字を入力します。 デフォルトのエスケープ シーケンスは、Ctrl-^（Ctrl キーと Shift キーを押しながら数字の 6 キーを押す）です。 大文字のコマンド文字は Ctrl キーを押しながら、小文字のコマンド文字は Ctrl キーを離して入力するとそれぞれ入力できます。 次の表は、特殊な Telnet のエスケープ シーケンスを示します。

表 *2*：特殊な *Telnet* のエスケープ シーケンス

エスケープ シーケンス[1]	目的
Ctrl-^ b	ブレーク

エスケープ シーケンス[1]	目的
Ctrl-^ c	プロセスの割り込み（IP および IPv6）
Ctrl-^ h	文字の消去（EC）
Ctrl-^ o	出力の中断（AO）
Ctrl-^ t	そこにいますか。（AYT）
Ctrl-^ u	行の消去（EL）

1 キャレット（^）記号は、キーボードの Shift + 6 で入力します。

アクティブな Telnet セッション中の任意の時点で、システム プロンプトでエスケープ シーケンス キーを押してから疑問符を入力（Ctrl-^ **?**）すると、Telnet コマンドを一覧表示できます

次に、この一覧の例を示します。 この出力例では、最初のキャレット（^）記号は Ctrl キーを表し、2 番目のキャレット記号はキーボードの Shift + 6 を表しています。

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

複数の並列 Telnet セッションを開き、セッション間を切り替えることができます。 以降のセッションを開くには、最初に、エスケープ シーケンスで（デフォルトでは Ctrl-Shift-6、x [Ctrl^x] の順に押す）現在の接続を一時停止してシステム コマンド プロンプトに戻ります。 その後、**telnet** コマンドで新しい接続を開きます。

アクティブな Telnet セッションを終了するには、接続しているデバイスのプロンプトから次のいずれかのコマンドを入力します。

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

例

次に、ルータから host1 というリモート ホストに対して暗号化された Telnet セッションを確立する例を示します。

```
router>

telnet host1 /encrypt kerberos
```

次に、送信元システム host1 から example.com、10.1.0.11 の順にパケットをルーティングし、最後に *host1* に返す例を示します。

```
router>
telnet host1 /route:example.com 10.1.0.11 host1
```

次に、論理名 host1 のホストに接続する例を示します。

```
router>
host1
```

次に、ログインおよびログアウト時にCisco IOS ソフトウェアからの画面メッセージをすべて抑制する例を示します。

```
router>

telnet host2 /quiet
```

次に、接続がオプションの **/quiet** キーワードを使用して接続を確立したときに表示される、制限されたメッセージの例を示します。

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32
Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

関連コマンド

コマンド	説明
connect	Telnet、rlogin、または LAT をサポートするホストにログインします。
kerberos clients mandatory	**rsh**、**rcp**、**rlogin**、および **telnet** コマンドでリモート サーバと Kerberos プロトコルのネゴシエーションができない場合、これらのコマンドは失敗します。
name connection	接続に論理名を割り当てます。
rlogin	rlogin を使用して UNIX ホストにログインします。
show hosts	デフォルトのドメイン名、名前ルックアップ サービス、ネーム サーバ ホストのリスト、およびホスト名とアドレスのキャッシュされたリストを表示します。
show tcp	TCP 接続のステータスを表示します。

test aaa group

着信番号識別サービス（DNIS）または発信回線 ID（CLID）ユーザ プロファイルを RADIUS サーバに送信されたレコードに関連付けるか、または手動でロードバランシング サーバのステータスをテストするには、特権 EXEC モードで **test aaa group** コマンドを使用します。

DNIS and CLID User Profile

test aaa group {*group-name*| **radius**} *username password* **new-code** [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing

test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password* **new-code** [**count** *requests*] [**rate** *requests-per-second*] [**blocked** {**yes**| **no**}]

構文の説明

group-name	サーバ グループのグループ名で定義されている、RADIUS サーバのサブセット。
radius	認証に RADIUS サーバを使用します。
username	テスト ユーザの名前。 **注意** このコマンドを使用して手動で RADIUS ロードバランシング サーバの状態をテストする場合、テスト ユーザが正しく設定されていない場合に発生するセキュリティ上の問題を防止するために、テスト ユーザ（RADIUS サーバ上で定義されていないもの）を使用することを推奨します。
password	パスワード。
new-code	RADIUS サーバとの CLID または DNIS ユーザ プロファイル アソシエーションをサポートする、新しいコードまでのコード パス。
profile *profile-name*	（任意）aaa user profile コマンドで指定されたユーザ プロファイルを識別します。 ユーザ プロファイルを RADIUS サーバに関連付けるには、ユーザプロファイル名を識別する必要があります。

server *ip-address*	（任意）RADIUS サーバのロードバランシングのために、サーバ グループ内のどのサーバにテスト パケットを送信するかを指定します。
auth-port	（任意）認証要求に対するユーザ データグラム プロトコル（UDP）宛先ポート。
port-number	（任意）認証要求用のポート番号です。0 に設定されている場合、認証にホストは使用されません。指定しない場合、ポート番号はデフォルトの 1646 になります。
acct-port	（任意）アカウンティング要求用の UDP 宛先ポート。
port-number	（任意）アカウンティング要求用のポート番号です。0 に設定されている場合、アカウンティングにホストは使用されません。指定しない場合、ポート番号はデフォルトの 1646 になります。
count *requests*	（任意）サーバの各ポートに送信される認証およびアカウンティング要求の数。 有効な範囲は、1 ～ 50000 です。 デフォルト：1。
rate *requests-per-second*	（任意）サーバに送信される 1 秒あたりの要求の数。 範囲は 1 ～ 1000 です。 デフォルトは 10 です。
blocked {**yes** | **no**}	（任意）要求をブロッキング モードで送信するか、ノンブロッキング モードで送信するかを指定します。 **blocked** キーワードを使用せず 1 つの要求を送信する場合、デフォルトは **yes** です。複数の要求を送信する場合は、デフォルトは **no** です。

コマンド デフォルト

DNIS または CLID 属性値は、RADIUS サーバに送信されません。

RADIUS サーバ ロードバランシングの手動テスト

コマンド モード

RADIUS サーバ ロードバランシングのサーバ ステータス手動テストは実行されません。
特権 EXEC（#）

コマンド履歴

リリース	変更内容
12.2(4)T	このコマンドが導入されました。
12.2(28)SB	RADIUS ロード バランシング手動テスト機能を設定するために、次のキーワードと引数が追加されました。**server** *ip-address*、**auth-port** *port-number*、**acct-port** *port-number*、**count** *request*、**rate** *requests-per-second*、**blocked**。
12.4(11)T	このコマンドが Cisco IOS Release 12.4(11)T に統合されました。
12.2(31)ZV1	このコマンドは、認証が成功した場合に RADIUS 認証から返されるユーザ属性を表示するように拡張されました。
Cisco IOS XE Release 2.4	このコマンドが、Cisco IOS XE Release 2.4 に統合されました。

使用上のガイドライン

test aaa group コマンドは、次の目的に使用できます

- DNIS または CLID ネームド ユーザ プロファイルを RADIUS サーバに送信されるレコードに関連付けます。これにより、サーバが RADIUS レコードを受信した際に、DNIS または CLID 情報にアクセスできるようになります。
- RADIUS ロードバランシング サーバのステータスを確認します。

（注） **test aaa group** コマンドは、TACACS+ では機能しません。

例

次に、「prfl1」という名前の dnis = dnisvalue ユーザ プロファイルを設定し、**test aaa group** コマンドを使用して関連付ける例を示します。

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

次の例は、ユーザ名の「test」がユーザ プロファイルと一致しない場合の動作中の RADIUS ロード バランシング サーバからの応答を示しています。 サーバは、**test aaa group** コマンドで生成さ

れた AAA パケットに対する Access-Reject 応答を発行した時点で動作中であることが確認されます。

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication ]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

例

次に、test aaa コマンドを発行し認証が成功したときに、RADIUS サーバから返されるユーザ属性リストの例を示します。

```
Router# test aaa group radius viral viral new-code blocked no
AAA/SG/TEST: Sending 1 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
CLI-1#
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Authen Requests to Send    : 1
AAA/SG/TEST:      Authen Requests Processed  : 1
AAA/SG/TEST:      Authen Requests Sent       : 1
AAA/SG/TEST:      Authen Requests Replied    : 1
AAA/SG/TEST:      Authen Requests Successful : 1
AAA/SG/TEST:      Authen Requests Failed     : 0
AAA/SG/TEST:      Authen Requests Error      : 0
AAA/SG/TEST:      Authen Response Received   : 1
AAA/SG/TEST:      Authen No Response Received: 0
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Account Requests to Send    : 0
AAA/SG/TEST:      Account Requests Processed  : 0
AAA/SG/TEST:      Account Requests Sent       : 0
AAA/SG/TEST:      Account Requests Replied    : 0
AAA/SG/TEST:      Account Requests Successful : 0
AAA/SG/TEST:      Account Requests Failed     : 0
AAA/SG/TEST:      Account Requests Error      : 0
AAA/SG/TEST:      Account Response Received   : 0
AAA/SG/TEST:      Account No Response Received: 0
USER ATTRIBUTES
username             "Username:viral"
nas-ip-address       3.1.1.1
interface            "210"
service-type         1 [Login]
Framed-Protocol      3 [ARAP]
ssg-account-info     "S20.5.0.2"
ssg-command-code     0B 4C 32 54 50 53 55 52 46
Router
```

関連コマンド

コマンド	説明
aaa attribute	ユーザ プロファイルに DNIS または CLID 属性値を追加します。
aaa user profile	AAA ユーザ プロファイルを作成します。
load-balance	RADIUS-named サーバ グループに対して RADIUS サーバ ロード バランシングをイネーブルにします。
radius-server host	ロードバランシング用の RADIUS 自動テストをイネーブルにします。
radius-server load-balance	グローバル RADIUS サーバ グループに対して RADIUS サーバ ロードバランシングをイネーブルにします。

timeout（TACACS+）

指定された TACACS サーバからの応答を待機する時間を設定するには、TACACS+ サーバ コンフィギュレーション モードで **timeout** コマンドを使用します。 コマンド デフォルトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout *seconds*

構文の説明

seconds	（任意）合計時間（秒単位）。

コマンド デフォルト

待機時間は 5 秒です。

コマンド モード

TACACS+ サーバ コンフィギュレーション（config-server-tacacs）

コマンド履歴

リリース	変更内容
Cisco IOS XE Release 3.2S	このコマンドが導入されました。

使用上のガイドライン

timeout コマンドを使用して、TACACS サーバからの応答を待機する時間を秒単位で設定します。**timeout** コマンドが設定されている場合、指定された秒数は、5 秒のデフォルト時間を上書きします。

例

次に、待機時間を 10 秒に設定する例を示します。

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

関連コマンド

コマンド	説明
tacacs server	IPv6 または IPv4 に対して TACACS+ サーバを設定して、TACACS サーバ コンフィギュレーション モードを開始します。