sa ipsec から sessions maximum まで

- server_（Diameter），2 ページ
- server（RADIUS），4 ページ
- server name（IPv6 TACACS+），7 ページ
- server-private（RADIUS），9 ページ
- server-private（TACACS+），12 ページ
- service password-encryption，15 ページ
- service password-recovery，17 ページ

server_（Diameter）

Diameter サーバを Diameter 認証、許可、アカウンティング（AAA）サーバ グループに関連付けるには、Diameter サーバ グループ コンフィギュレーション サブモードで **server** コマンドを使用します。 サーバ グループからサーバを削除するには、このコマンドの **no** 形式を入力します。

server *name*

no server *name*

構文の説明

name	Diameter サーバ名の指定に使用する文字列。 （注） このコマンドに指定した名前は、**diameter peer** コマンドを使用して定義した Diameter ピアの名前と一致する必要があります。

コマンド デフォルト

Diameter AAA サーバ グループに関連付けられているサーバはありません。

コマンド モード

Diameter サーバ グループ 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
12.4(9)T	このコマンドが導入されました。

使用上のガイドライン

server コマンドを使用して、Diameter サーバを Diameter サーバ グループに関連付けることができます。

例

次に、Diameter サーバを Diameter サーバ グループに関連付ける例を示します。

```
Router (config-sg-diameter)# server
 dia_peer_1
```

関連コマンド

コマンド	説明
aaa accounting	課金またはセキュリティ目的のために、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。
aaa authentication login	ログイン時の AAA 認証を設定します。
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 group server diameter	Diameter 用のサーバ グループを設定します。

server（RADIUS）

グループ サーバに対して、RADIUS サーバの IP アドレスを設定するには、サーバグループ コンフィギュレーション モードで **server** コマンドを使用します。 関連付けられたサーバを認証、許可、アカウンティング（AAA）グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

構文の説明

ip-address	RADIUS サーバ ホストの IP アドレスです。
auth-port *port-number*	（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）宛先ポートを指定します。 port-number 引数は、認証要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストは認証に使用されません。
acct-port *port-number*	（任意）アカウンティング要求に対する UDP 宛先ポートを指定します。 port number 引数は、アカウンティング要求に対するポート番号を指定します。 この値が 0 に設定されている場合、そのホストはアカウンティング サービスに使用されません。

コマンド デフォルト

ポート属性が定義されていない場合、デフォルトは次のようになります。

- 認証ポート：1645
- アカウンティング ポート：1646

コマンド モード

サーバグループ 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
12.0(5)T	このコマンドが導入されました。

リリース	変更内容
12.0(7)T	次の新しいキーワードと引数が追加されました。 • **auth-port** *port-number* • **acct-port** *port-number*
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(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

server コマンドを使用して、特定のサーバを定義済みのグループ サーバに関連付けることができます。 サーバを識別する方法は、AAA サービスを提供する方法に応じて 2 種類あります。 IP アドレスを使用して単純にサーバを識別する方法と、オプションの **auth-port** キーワードおよび **acct-port** キーワードを使用して複数のホスト インスタンスまたはエントリを識別する方法があります。

オプションのキーワードを使用すると、ネットワーク アクセス サーバにより、IPアドレスと特定の UDP ポート番号に基づいてグループ サーバに関連付けられている RADIUS セキュリティ サーバおよびホスト インスタンスが識別されます。 IPアドレスとUDPポート番号の組み合わせによって一意の ID を作成し、特定の AAA サービスを提供する RADIUS ホスト エントリとして各ポートを個々に定義できます。 1 台の RADIUS サーバ上にある異なる 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 番目のホスト 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、同じデバイスに設定されている 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 RADIUS 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）。

例

例

次に、同じ IP アドレスを持つ複数の RADIUS ホスト エントリを認識する、ネットワーク アクセス サーバの例を示します。 同じ RADIUS サーバ上にある 2 つのホスト エントリは、同じサービス（認証とアカウンティング）のために設定されています。 設定されている 2 番めのホスト エントリは、1 番めの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 （試行される RADIUS 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）。

```
! This command enables AAA.
aaa new-model
```

```
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

例

次の例では、ネットワーク アクセス サーバは異なる 2 つの RADIUS グループ サーバを認識するように設定されます。 一方のグループである group1 には、同じ RADIUS サーバ上に同じサービス用に設定された 2 つのホスト エントリがあります。 設定されている 2 番めのホスト エントリは、1 番めの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

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
   server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
   server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.31.0.1 auth-port 1645 acct-port 1646
```

関連コマンド

コマンド	説明
aaa group server	各種のサーバホストを別個のリストと別個の方式にグループ化します。
aaa new-mode l	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。

server name（IPv6 TACACS+）

IPv6 TACACS+ サーバを指定するには、TACACS+ グループ サーバ コンフィギュレーション モードで **server name** コマンドを使用します。 コンフィギュレーションから IPv6 TACACS+ サーバを削除するには、このコマンドの **no** 形式を使用します。

server name *server-name*

no server name *server-name*

構文の説明

server-name	使用する IPv6 TACACS+ サーバ。

コマンド デフォルト

サーバ名は指定されていません。

コマンド モード

TACACS+ グループ サーバ コンフィギュレーション（config-sg-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

このコマンドを設定する前に、**aaa group server tacacs** コマンドを設定する必要があります。

IPv6 TACACS+ サーバを指定するには、**server name** コマンドを入力します。

例

次に、server1 という名前の IPv6 TACACS+ サーバを指定する例を示します。

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

関連コマンド

コマンド	説明
aaa group server tacacs	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。

server-private（RADIUS）

グループ サーバに対して、プライベート RADIUS サーバの IP アドレスを設定するには、サーバ グループ コンフィギュレーション モードで **server-private** コマンドを使用します。 関連付けられたプライベート サーバを認証、許可、アカウンティング（AAA）グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private *ip-address* [**auth-port** *port-number*| **acct-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [**auth-port** *port-number*| **acct-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

構文の説明

ip-address	プライベート RADIUS サーバ ホストの IP アドレス。
auth-port *port-number*	（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。 デフォルト値は 1645 です。
acct-port *port-number*	（任意）アカウンティング要求用の UDP 宛先ポート。 デフォルト値は 1646 です。
non-standard	（任意）RADIUS サーバは、ベンダー固有の RADIUS 属性を使用しています。
timeout *seconds*	（任意）ルータが RADIUS サーバの応答を待機し、再送信するまでの時間間隔（秒単位）です。 この設定は、radius-server timeout コマンドのグローバル値を上書きします。 タイムアウト値が指定されていない場合は、グローバル値が使用されます。
retransmit *retries*	（任意）サーバが応答しない、または応答が遅い場合に、そのサーバに RADIUS 要求を再送信する回数。 この設定は、radius-server retransmit コマンドのグローバル値を上書きします。
key *string*	（任意）ルータと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キー。 このキーは、radius-server key コマンドのグローバル値を上書きします。 キー文字列を指定しない場合、グローバル値が使用されます。

コマンド デフォルト

server-private パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。

コマンド モード

サーバグループ 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
12.2(1)DX	このコマンドが Cisco 7200 シリーズおよび Cisco 7401ASR に導入されました。
12.2(2)DD	このコマンドが、Cisco IOS Release 12.2(2)DD に統合されました。
12.2(4)B	このコマンドが Cisco IOS Release 12.2(4)B に組み込まれました。
12.2(13)T	このコマンドが、Cisco IOS Release 12.2(13)T 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(33)SRC	このコマンドが、Cisco IOS Release 12.2(33)SRC 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。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。

使用上のガイドライン

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 Virtual Route Forwarding（VRF）間でのプライベート アドレスの重複を防止するために、プライベート サーバ（プライベート アドレスを持つサーバ）をサーバ グループ内に定義し、他のグループからは見えない状態にしておくことができます。この場合も、グローバル プール（デフォルトの「radius」サーバ グループ）にあるサーバは、IP アドレスとポート番号で参照できます。 このように、サーバ グループ内のサーバのリストには、グローバル コンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

（注） **radius-server directed-request** コマンドが設定されている場合、**server-private**（RADIUS）コマンドを設定して、プライベート RADIUS サーバをグループ サーバとして使用することはできません。

例

次に、sg_water RADIUS グループ サーバを定義し、これにプライベート サーバを関連付ける例を示します。

```
aaa group server radius sg_water
 server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
 server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

関連コマンド

コマンド	説明
aaa group server	各種のサーバ ホストを別個のリストと別個の方式にグループ化します。
aaa new-mode l	AAA アクセス コントロール モデルをイネーブルにします。
radius-server host	RADIUS サーバ ホストを指定します。
radius-server directed-request	ユーザが Cisco Network Access Server（NAS）にログインし、認証に RADIUS サーバを選択することを許可します。

server-private（TACACS+）

グループ サーバに対して、プライベート TACACS+ サーバの IPv4 または IPv6 アドレスを設定するには、サーバグループ コンフィギュレーション モードで **server-private** コマンドを使用します。関連付けられたプライベート サーバを認証、許可、アカウンティング（AAA）グループ サーバから削除するには、このコマンドの **no** 形式を使用します。

server-private {*ip-address*| *name*| *ipv6-address*} **[nat] [single-connection]** [**port** *port-number*] [**timeout** *seconds*] [**key** [**0**| **7**] *string*]

no server-private

構文の説明

ip-address	プライベート RADIUS または TACACS+ サーバ ホストの IP アドレス。
name	プライベート RADIUS または TACACS+ サーバ ホストの名前。
ipv6-address	プライベート RADIUS または TACACS+ サーバ ホストの IPv6 アドレス。
nat	（任意）リモート デバイスのポート ネットワーク アドレス変換（NAT）アドレスを指定します。このアドレスは TACACS+ サーバに送信されます。
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。
port *port-number*	（任意）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。
timeout *seconds*	（任意）タイムアウト値を指定します。この値によって、**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。

key [**0** | **7**]	（任意）認証および暗号キーを指定します。このキーは 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 **tacacs-server key** コマンドで設定されているキーが上書きされます。 • 番号が入力されていないか、0 が入力されている場合、入力されたストリングはプレーン テキストであると見なされます。7 が入力されている場合、入力されたストリングは暗号化テキストであると見なされます。
string	（任意）認証および暗号キーを指定する文字列。

コマンド デフォルト

server-private パラメータが指定されていない場合、グローバル コンフィギュレーションが使用されます。グローバル コンフィギュレーションが指定されていない場合、デフォルト値が使用されます。

コマンド モード

サーバグループ コンフィギュレーション（server-group）

コマンド履歴

リリース	変更内容
12.3(7)T	このコマンドが導入されました。
12.2(33)SRA1	このコマンドが、Cisco IOS Release 12.2(33)SRA1 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。
12.2(33)SXI	このコマンドが、Cisco IOS Release 12.2(33)SXI に統合されました。
12.2(54)SG	このコマンドが、Cisco IOS Release 12.2(54)SG に統合されました。
Cisco IOS XE Release 3.2S	このコマンドが変更されました。 引数 *ipv6-address* が追加されました。

使用上のガイドライン

server-private コマンドを使用して、特定のプライベート サーバを定義済みのサーバ グループに関連付けることができます。 Virtual Route Forwarding（VRF）間でのプライベート アドレスの重複を防止するために、プライベート サーバ（プライベート アドレスを持つサーバ）をサーバ グループ内に定義し、他のグループからは見えない状態にしておくことができます。この場合も、グローバル プール（デフォルトの「TACACS+」サーバ グループ）にあるサーバは、IP アドレスとポート番号で参照できます。このように、サーバ グループ内のサーバのリストには、グローバル コンフィギュレーションにおけるホストの参照情報とプライベート サーバの定義が含まれます。

例

次に、tacacs1 TACACS+ グループ サーバを定義し、これにプライベート サーバを関連付ける例を示します。

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

関連コマンド

コマンド	説明
aaa group server	各種のサーバ ホストを別個のリストと別個の方式にグループ化します。
aaa new-mode l	AAA アクセス コントロール モデルをイネーブルにします。
ip tacacs source-interface	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。
ip vrf forwarding（**server-group**）	AAA RADIUS または TACACS+ サーバ グループの VRF 参照を設定します。
tacacs-server host	TACACS+ サーバ ホストを指定します。

service password-encryption

パスワードを暗号化するには、グローバル コンフィギュレーション モードで **service password-encryption** コマンドを使用します。 デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

service password-encryption

no service password-encryption

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

パスワードは暗号化されません。

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。
12.2(33)SRA	このコマンドが、Cisco IOS Release 12.2(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。
12.2(33)SB	このコマンドが、Cisco IOS Release 12.2(33)SB に統合されました。

使用上のガイドライン

実際の暗号化プロセスは、現在の設定が保存されるとき、またはパスワードが設定されるときに行われます。 パスワードの暗号化は、ユーザ名パスワード、認証キーパスワード、特権コマンドパスワード、コンソールおよび仮想端末回線アクセスパスワード、およびボーダーゲートウェイプロトコル ネイバー パスワードを含む、すべてのパスワードに適用されます。 このコマンドは、主に未許可ユーザがコンフィギュレーション ファイル内のパスワードを閲覧するのを防ぐために役立ちます。

パスワードの暗号化をイネーブルにした場合、**more system:running-config** コマンドを入力すると、パスワードの暗号化された形式が表示されます。

注意 このコマンドでは、高レベルのネットワーク セキュリティは確保されません。 このコマンドを使用する場合は、その他のネットワーク セキュリティ手段も講じる必要があります。

（注） 暗号化パスワードを忘れた場合、回復はできません。 NVRAM を消去し、新しいパスワードを設定する必要があります。

例

次に、パスワードの暗号化を実行する例を示します。

```
service password-encryption
```

関連コマンド

コマンド	説明
enable password	さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。
key-string（認証）	キーの認証文字列を指定します。
neighbor password	2 つの BGP ピアの間の TCP 接続で MD5 認証をイネーブルにします。

service password-recovery

パスワード回復機能をイネーブルにするには、グローバル コンフィギュレーション モードで **service password-recovery** コマンドを使用します。 パスワード回復機能をディセーブルにするには、**no service password-recovery** コマンドを使用します。

service password-recovery

no service password-recovery

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

パスワード回復機能はイネーブルです。

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
12.3(8)YA	このコマンドが導入されました。
12.3(14)T	このコマンドが、Cisco IOS Release 12.3(14)T に統合されました。
15.1(1)SY	このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。

使用上のガイドライン

（注） このコマンドは、一部のプラットフォームでは使用できません。 Feature Navigator を使用して、お使いのプラットフォームで使用できるかどうかを確認してください。

no service password-recovery コマンドを使用してパスワード回復機能をディセーブルにする場合は、デバイスとは別の場所にシステム コンフィギュレーション ファイルのコピーを保存しておくことを推奨します。 VTP トランスペアレント モードで動作するデバイスを使用している場合、デバイスとは別の場所に、vlan.dat ファイルのコピーを保存することも推奨しています。

⚠

注意 no **service password-recovery** コマンドをコマンドラインに入力すると、パスワード回復がディセーブルになります。 パスワード回復機能をサポートしないイメージにダウングレードする場合は、ダウングレード後はパスワードを回復できなくなるため、ダウングレード前にこのコマンドをディセーブルにしてください。

このコマンドが設定されているときに、ROMMON を開始する方法をなくすため、コンフィギュレーション レジスタ ブート ビットをイネーブルにする必要があります。 Cisco IOS ソフトウェアは、ユーザによるコンフィギュレーション レジスタのブート フィールドの設定を防止する必要があります。

スタートアップ コンフィギュレーションを無視するビット 6、およびブレークをイネーブルにするビット 8 を設定する必要があります。

ルータの起動中は、Break キーをディセーブルにし、この機能をイネーブルにしている場合は、Cisco IOS ソフトウェアでディセーブルにする必要があります。

no service password-recovery コマンドを入力する前に、**config-register** 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、コンフィギュレーション レジスタが自動的に起動するようにしておくことが必要な場合もあります。 **show version** EXEC コマンドの最後の行は、コンフィギュレーション レジスタの設定を表示します。 **show version** EXEC コマンドを使用して現在のコンフィギュレーション レジスタ値を取得し、必要に応じて **config-register** コマンドを使用してルータが自動起動するように設定してから、**no service password-recovery** コマンドを入力します。

ディセーブルにすると、**no service password-recovery** コマンドでは次のコンフィギュレーション レジスタ値が無効になります。

- 0x0
- 0x2002（ビット 8 制限）
- 0x0040（ビット 6）
- 0x8000（ビット 15）

Catalyst スイッチ動作

パスワード回復メカニズムを再度イネーブル（デフォルト）にするには、**service password-recovery** コマンドを使用します。 このメカニズムでは、スイッチに物理的にアクセスするユーザは、スイッチの電源投入時に Mode ボタンを押してブート プロセスを中断し、新しいパスワードを割り当てることができます。 パスワード回復機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

パスワード回復メカニズムがディセーブルになると、ユーザがシステムをデフォルト設定に戻すことに同意した場合だけ、ブート プロセスを中断できます。 スイッチでパスワード回復がイネーブルか、ディセーブルかを確認するには、**show version** EXEC コマンドを使用します。

service password-recovery コマンドは、Catalyst 3550 ファスト イーサネット スイッチでだけ有効です。ギガビット イーサネット スイッチでは使用できません。

例

例

次に、（この例では自動起動に設定されている）コンフィギュレーション レジスタ設定を取得し、パスワード回復機能を無効にしてから、設定がシステムのリロード後も維持されることを確認する方法の例を示します。 **noconfirm** キーワードは、確認プロンプトにより起動プロセスが中断することを防止します。

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-03 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000
ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Router uptime is 10 minutes
System returned to ROM by reload at 16:28:11 UTC Thu Mar 6 2003
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2012
Router# configure terminal
Router(config)# no service password-recovery noconfirm
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload
Proceed with reload? [confirm] yes
00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.
```

次に、中断を確定する場合と、中断を確定しない場合に生じる状態を示します。

例

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
################################################################################################################################
 [OK] !The 5-second window starts.
telnet> send break
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
```

```
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "y" here.
Reset router configuration to factory default.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
 Importers, exporters, distributors and users are responsible for compliance with U.S. and
 local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
         --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up config is erased.
SETUP: new interface FastEthernet1 placed in "up" state
SETUP: new interface FastEthernet2 placed in "up" state
SETUP: new interface FastEthernet3 placed in "up" state
SETUP: new interface FastEthernet4 placed in "up" state
Press RETURN to get started!
Router> enable
Router# show startup configuration
startup-config is not present
Router# show running-config | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption !The "no service password-recovery" is disabled.
==========================================================================================
```

例

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
telnet> send break
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
##################################################################################################################################################
 [OK]
telnet> send break
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "n" here.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
```

```
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
Press RETURN to get started! !The Cisco IOS software boots as if it is not interrupted.
Router> enable
Router# show startup configuration
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
```

```
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
Router# show running-configuration | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
```

例

no service password-recovery コマンドは、ルータのコンフィギュレーション レジスタが自動起動するように設定されていることを想定しています。 **no service password-recovery** コマンドを入力する前に、コンフィギュレーション レジスタが自動起動以外に設定されている場合は、次の例のようなプロンプトが表示され、**config-register** 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設定を変更するように促されます。

```
Router(config)# no service password-recovery
Please setup auto boot using config-register first.
```

（注） このコマンドの動作により、意図しない結果が生じることを回避するには、**show version** コマンドを使用して、現在のコンフィギュレーション レジスタ値を取得します。 自動起動に設定されていない場合、**no service password-recovery** コマンドを入力する前に、**config-register** コマンドを使用して、ルータを自動起動に設定する必要があります。

パスワード回復をディセーブルにすると、ビット パターン値を 0x40、0x8000、または 0x0（自動起動をディセーブル化）に設定できません。 次に、パスワード回復をディセーブルにしたルータで、無効なコンフィギュレーション レジスタ設定が試行された場合に表示されるメッセージの例を示します。

```
Router(config)# config-register 0x2143
Password recovery is disabled, cannot enable diag or ignore configuration.
```

コマンドは無効なビット パターンをリセットし、無関係なビット パターンの変更を許可し続けます。 コンフィギュレーション レジスタの値は次回のシステム リロード時に 0x3 にリセットされます。これは、**show version** コマンドの出力の最後の行をチェックすることで確認できます。

```
Configuration register is 0x2012 (will be 0x3 at next reload)
```

例

次の例では、スイッチ上でパスワード回復をディセーブルにする方法を示します。ユーザはデフォルト設定に戻すことに同意する場合のみパスワードをリセットできます。

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

パスワード回復手順を実行する場合、スイッチに物理的にアクセスするユーザは、スイッチの電源投入時とポート 1X の上にある LED が消灯してから 1 ～ 2 秒後に Mode ボタンを押します。 ボタンを放すと、システムは初期化を続けます。 パスワード回復メカニズムがディセーブルの場合は、次のメッセージが表示されます。

```
The password-recovery mechanism has been triggered, but is currently disabled. Access to
the boot loader prompt through the password-recovery mechanism is disallowed at this point.
 However, if you agree to let the system be reset back to the default system configuration,
 access to the boot loader prompt can still be allowed.
Would you like to reset the system back to the default configuration (y/n)?
```

システムをデフォルト設定にリセットしないことを選択した場合は、**Mode** ボタンを押さないときと同じように、通常の起動プロセスが続行されます。 システムをデフォルト設定にリセットする場合、フラッシュ メモリ内のコンフィギュレーション ファイルが削除され、VLAN データベース ファイル flash:vlan.dat（存在する場合）が削除されます。

次に、パスワード回復がディセーブルのデバイスでの、**show version** コマンドの出力例を示します。

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 24-Oct-01 06:20 by xxx
Image text-base: 0x00003000, data-base: 0x004C1864
ROM: Bootstrap program is C3550 boot loader
flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on
Cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image
Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface
Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is disabled.
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

関連コマンド

コマンド	説明
config-register	コンフィギュレーション レジスタの設定を変更します。

コマンド	説明
show version	ハードウェアおよびファームウェアのバージョン情報を表示します。