

ルータおよびスイッチでの SSH の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[SSH v2 ネットワーク構成図](#)

[認証のテスト](#)

[SSH 非実装時の認証テスト](#)

[SSH 実装時の認証テスト](#)

[オプションのコンフィギュレーション セット](#)

[非 SSH 接続の防止](#)

[IOS ルータやスイッチの SSH クライアントとしての設定](#)

[RSA ベースのユーザー認証を実行する SSH サーバーとしての IOS ルータのセットアップ](#)

[SSH 端末回線アクセスの追加](#)

[サブネットへの SSH アクセスを制限する](#)

[SSH バージョン 2 の設定](#)

[banner コマンド出力のバリエーション](#)

[バナーコマンドオプション](#)

[Telnet](#)

[SSHv2](#)

[ログインバナーを表示できない](#)

[debug コマンドと show コマンド](#)

[debug 出力例](#)

[ルータのデバッグ](#)

[サーバのデバッグ](#)

[誤った設定](#)

[データ暗号標準 \(DES\) でコンパイルされていない SSH クライアントからの SSH](#)

[不適切なパスワード](#)

[ルータのデバッグ](#)

[SSH クライアントによるサポート対象外の \(Blowfish\) 暗号の送信](#)

[ルータのデバッグ](#)

["%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for" エラーの取得](#)

[ヒント](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco IOS® ソフトウェアを実行する Cisco ルータまたはスイッチで

Secure Shell (SSH) を設定し、デバッグする方法について説明します。

前提条件

要件

使用される Cisco IOS イメージは SSH をサポートするために k9(crypto) イメージである必要があります。たとえば、c3750e-universalk9-tar.122-35.SE5.tar は k9 (暗号) イメージです。

使用するコンポーネント

このドキュメントの情報は、Cisco IOS 3600 ソフトウェア (C3640-IK9S-M)、リリース 12.2(2)T1 に基づくものです。

SSH は、次の Cisco IOS プラットフォームおよびイメージに導入されています。

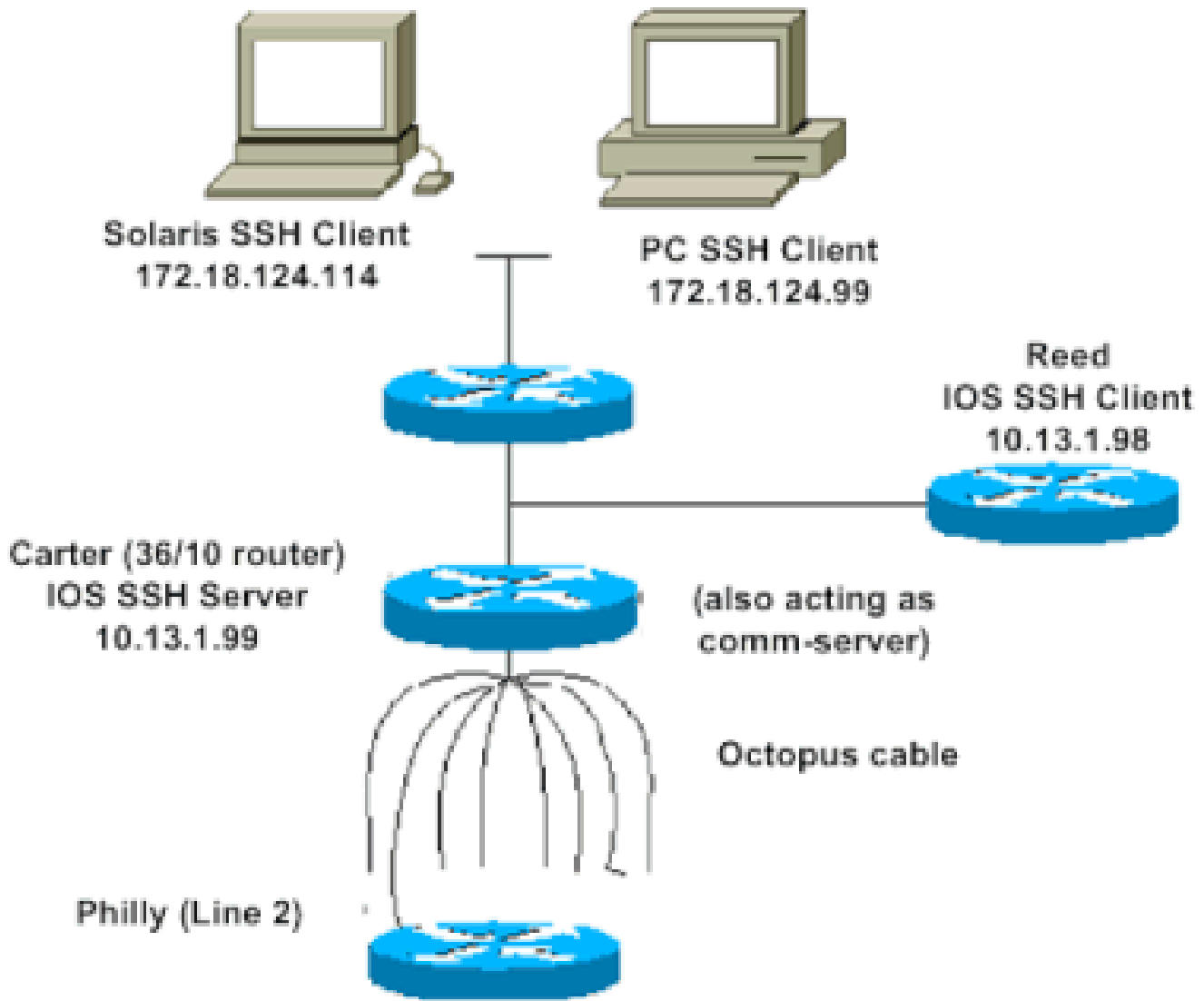
- SSH 端末回線アクセス (リバース Telnet と呼ばれる) は、Cisco IOS ソフトウェアリリース 12.2.2.T 以降の Cisco IOS プラットフォームおよびイメージに導入されました。
- SSH バージョン 2.0 (SSH v2) のサポートは、Cisco IOS ソフトウェアリリース 12.1(19)E 以降の Cisco IOS プラットフォームおよびイメージに導入されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

表記法

詳細については、[シスコのテクニカルティップスの表記法](#)を参照してください。


SSH v2 ネットワーク構成図



認証のテスト

SSH 非実装時の認証テスト

最初に、SSH を追加する前に、ルータ Carter で認証処理が動作することを確認するために、SSH を実装しない状態で認証をテストします。認証は、ローカル ユーザ名とパスワードを使用するか、TACACS+ または RADIUS が動作する Authentication、Authorization、および Accounting (AAA; 認証、認可、アカウントिंग) サーバを使用して行えます (SSH が実装されていると、回線パスワードによる認証は行えません)。次に、ローカル認証の例を示します。この認証により、ユーザー名 cisco とパスワード cisco を使用してルータに Telnet 接続できます。

 注：このドキュメント全体で、VTY は仮想端末タイプを示すために使用されます。

!--- The aaa new-model command causes the local username and password on the router to be used in the a

```
aaa new-model
username cisco password 0 cisco
```

```
line vty 0 4
transport input telnet
```

!--- Instead of aaa new-model, you can use the login local command.

SSH 実装時の認証テスト

SSH を使用した認証をテストするには、以前のステートメントに追加して、Carter で SSH を有効にし、PC および UNIX ステーションから SSH をテストする必要があります。

```
ip domain-name rtp.cisco.com
```

!--- Generate an SSH key to be used with SSH.

```
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
```

この時点で、`show cry key mypubkey rsa` コマンドを実行すると、生成されたキーが表示されます。SSH の設定を追加した後、PC と UNIX の端末からルータにアクセスできることをテストします。

オプションのコンフィギュレーション セット

非 SSH 接続の防止

非 SSH 接続を防止する場合は、行の下に `transport input ssh` コマンドを追加して、ルータを SSH 接続だけに制限します。通常の (非 SSH) Telnet は拒否されます。

```
line vty 0 4
```

!--- Prevent non-SSH Telnets.

```
transport input ssh
```

非 SSH ユーザーがルータ Carter に Telnet できないことを確認するためにテストします。

IOS ルータやスイッチの SSH クライアントとしての設定

Cisco IOS ルータで SSH のサポートを有効にするには、次の 4 つのステップを実行する必要があります。

1. `hostname` コマンドを設定します。

2. DNS ドメインを設定します。
3. SSH キーを生成します。
4. VTY の SSH トランスポートのサポートを有効にします。

1つのデバイスを他方の SSH クライアントとして動作させるには、Reed と呼ばれる 2 番目のデバイスに SSH を追加します。この操作により、これらのデバイスはクライアントとサーバーの関係になり、Carter がサーバーとして機能し、Reed がクライアントとして機能します。Reed 上の Cisco IOS SSH クライアント設定は、Carter 上の SSH サーバ設定と同じものがが必要です。

!--- Step 1: Configure the hostname if you have not previously done so.

```
hostname carter
```

!--- The aaa new-model command causes the local username and password on the router to be used in the a

```
aaa new-model  
username cisco password 0 cisco
```

!--- Step 2: Configure the DNS domain of the router.

```
ip domain-name rtp.cisco.com
```

!--- Step 3: Generate an SSH key to be used with SSH.

```
crypto key generate rsa  
ip ssh time-out 60  
ip ssh authentication-retries 2
```

!--- Step 4: By default the vty transport is Telnet. In this case, Telnet is disabled and only SSH is s

```
line vty 0 4  
transport input ssh
```

!--- Instead of aaa new-model, you can use the login local command.

これをテストするには、次のコマンドを発行して、Cisco IOS SSH クライアント (Reed) から Cisco IOS SSH サーバー (Carter) に SSH 接続します。

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

RSA ベースのユーザー認証を実行する SSH サーバーとしての IOS ルータのセットアップ

RSA ベースのユーザー認証を実行するように SSH サーバーを設定するには、次の手順を実行します。

1. ホスト名を指定します。

```
Router(config)#hostname <host name>
```

2. デフォルトのドメイン名を定義します。

```
Router(config)#ip domain-name <Domain Name>
```

3. RSA キー ペアを生成します。

```
Router(config)#crypto key generate rsa
```

4. ユーザーおよびサーバー認証用の SSH-RSA キーを設定します。

```
Router(config)#ip ssh pubkey-chain
```

5. SSH ユーザー名を設定します。

```
Router(conf-ssh-pubkey)#username <user name>
```

6. リモートピアの RSA 公開キーを指定します。

```
Router(conf-ssh-pubkey-user)#key-string
```

7. SSH キーのタイプとバージョンを指定します。(この手順は任意です)。

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa <key ID>
```

8. 現在のモードを終了し、特権 EXEC モードに戻ります。

```
Router(conf-ssh-pubkey-data)#end
```

SSH 端末回線アクセスの追加

送信 SSH 端末回線認証が必要な場合は、Philly への comm server として動作する、Carter 経由の送信リバース Telnet に SSH を設定でき、その設定をテストできます。

```
ip ssh port 2001 rotary 1
line 1 16
  no exec
  rotary 1
  transport input ssh
  exec-timeout 0 0
  modem InOut
  stopbits 1
```

Philly が Carter ポート 2 に接続されている場合は、次のコマンドを使用して、Reed から Carter を介して Philly への SSH 接続を設定できます。

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

Solaris からは、次のコマンドが使用できます。

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

サブネットへの SSH アクセスを制限する


SSH 接続を特定のサブネットワークに制限し、サブネットワーク外 IP からのその他すべての SSH 接続試行がドロップされるようにする必要があります。

この設定は、次の手順を使用して実行できます。

1. その特定のサブネットワークからのトラフィックを許可するアクセス リストを定義します。
。
2. `access-class` を備える VTY ライン インターフェイスへのアクセスを制限します。

次に設定例を示します。この例では、10.10.10.0 255.255.255.0 サブネットへの SSH アクセスのみが許可され、その他のアクセスは拒否されます。

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255
Router(config)#line vty 5 15
Router(config-line)#transport input ssh
Router(config-line)#access-class 23 in
Router(config-line)#exit
```

 注：SSH アクセスをロックダウンする同じ手順がスイッチプラットフォームにも使用されます。

SSH バージョン 2 の設定

```
carter(config)#ip ssh version 2
```

banner コマンド出力のバリエーション

banner コマンドの出力は、Telnet と SSH 接続の異なるバージョンの間では異なります。この表では、さまざまな接続タイプで、さまざまな banner コマンド オプションが、どのように動作するのかを説明しています。

バナーコマンドオプション	Telnet	SSH v2
バナーログ	デバイスにログインする前に表示されます。	デバイスにログインする前に表示されます。
banner motd	デバイスにログインする前に表示されます。	デバイスへのログイン後に表示されます。
banner exec	デバイスへのログイン後に表示されます。	デバイスへのログイン後に表示されます。

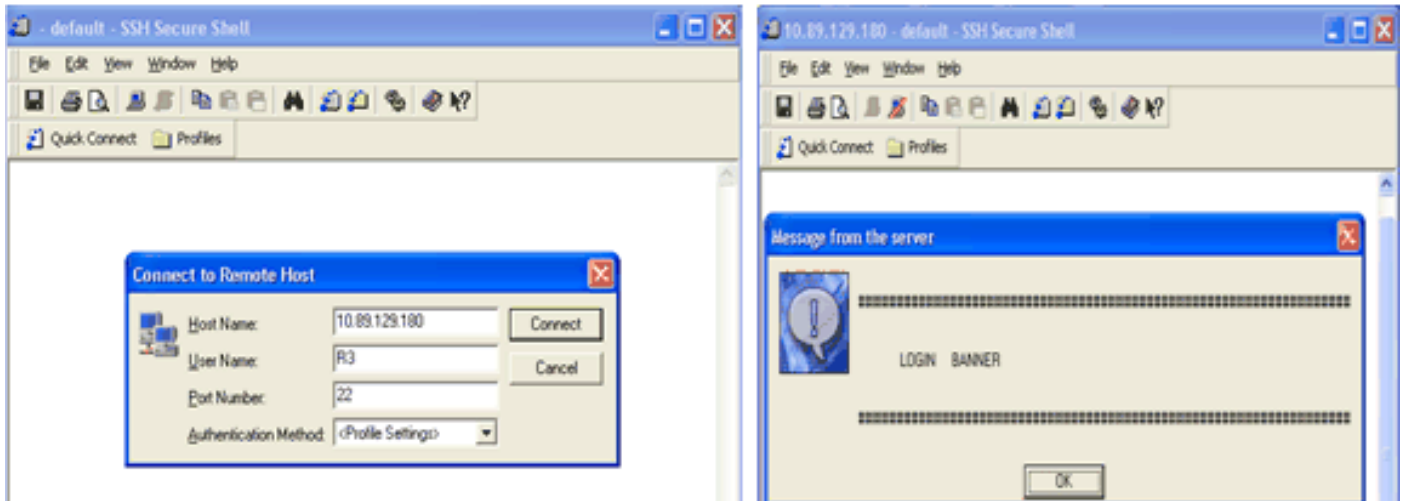
 注：SSH バージョン 1 は推奨されなくなりました。

ログイン バナーが表示されない

SSH バージョン 2 は、ログインバナーをサポートします。シスコルータとの SSH セッションを開始すると、SSH クライアントがユーザー名を送信したときにログインバナーが表示されます。たとえば、セキュアシェル (SSH) クライアントを使用すると、ログインバナーが表示されます。PuTTY SSH クライアントを使用する場合、ログインバナーは表示されません。これは、SSH

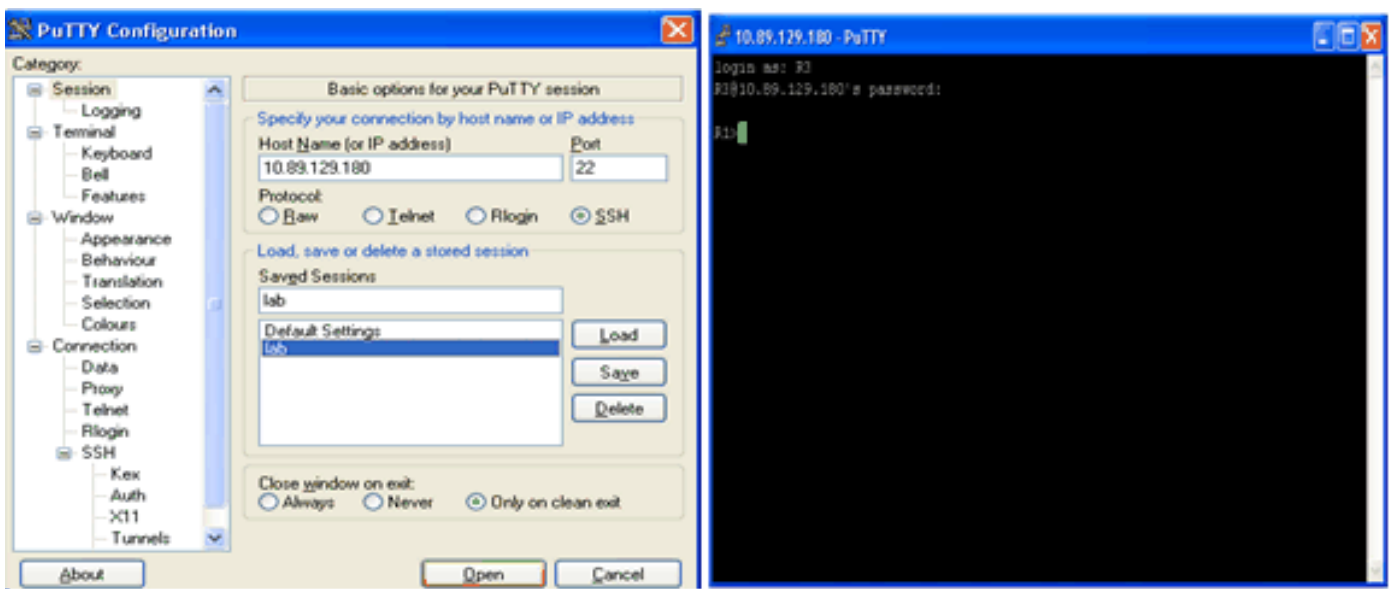
がデフォルトでユーザー名を送信し、PuTTY がデフォルトでユーザー名を送信しないためです。

SSH クライアントには、SSH 対応デバイスへの接続を開始するためのユーザー名が必要です。ホスト名とユーザー名を入力しないと、Connect ボタンは有効になりません。次の画像は、SSH がルータに接続するときログインバナーが表示されることを示しています。その後、バナーはパスワードの入力を求めます。



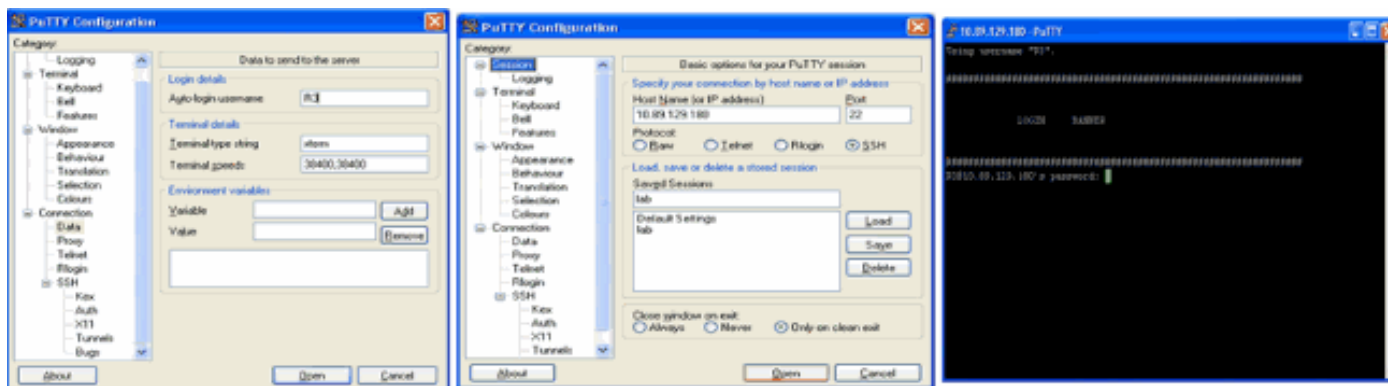
パスワードを求めるバナープロンプト

PuTTY クライアントでは、ルータへの SSH 接続を開始するのに、ユーザー名は必要ありません。この画像は、PuTTY クライアントがルータに接続したときに、ユーザー名とパスワードの入力が求められることを示しています。ログインバナーは表示されません。



ルータへの SSH 接続

このスクリーンショットは、PuTTY がユーザー名をルータに送信するように設定されている場合に、ログインバナーが表示されることを示しています。



Category → Connection → Data

ルータへのユーザー名の送信

debug コマンドと show コマンド

debug コマンドを発行する前に、[Debug コマンドについての重要な情報](#)を参照してください。特定の show コマンドは、[アウトプットインタープリタツール](#)（お客様に対してのみ登録）でサポートされており、このツールを使用して show コマンド出力の分析を表示できます。

- debug ip ssh : SSH のデバッグメッセージを表示します。
- show ssh : SSH サーバー接続のステータスを表示します。

```
carter#show ssh
Connection    Version Encryption    State                Username
0             2.0      DES              Session started     cisco
```

- show ip ssh : SSH のバージョンおよび設定データを表示します。

```
carter#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

debug 出力例

ルータのデバッグ

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-2.0-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
```

```
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_SMSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
    length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

サーバのデバッグ

 注：これは Solaris マシンの出力です。

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99
rtp-evergreen#/opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 2.0,
    remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
    and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
cisco@10.13.1.99's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
    could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.
```

誤った設定

次のセクションでは、いくつかの誤った設定からのデバッグの出力例を示しています。

データ暗号標準 (DES) でコンパイルされていない SSH クライアントからの SSH 不適切なパスワード

ルータのデバッグ

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-2.0-1.2.26
00:26:52: SSH0: SSH_MSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_MSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_MSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

SSH クライアントによるサポート対象外の (Blowfish) 暗号の送信

ルータのデバッグ

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-2.0-W1.0
00:39:26: SSH0: SSH_MSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

"%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for" エラーの取得

ドメイン名またはホスト名を変更すると、このエラーメッセージが表示されることがあります。
回避策は次のとおりです。

- RSA キーがゼロ化し、キーを再生成します。

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

- 前の回避策が機能しなかった場合、次の手順を試してください。
 1. すべての RSA キーをゼロ化します。
 2. デバイスをリロードします。
 3. 新規にラベルが付けられた SSH キーを作成します。

ヒント

- SSH コンフィギュレーション コマンドが違法なコマンドとして拒否される場合、ルータで RSA キー ペアが正しく生成されていません。ホスト名とドメインが指定されていることを確認します。次に、`crypto key generate rsa` コマンドを使用して RSA キーペアを生成し、SSH サーバーを有効にします。
- RSA キーペアを設定すると、次のエラーメッセージが表示されることがあります。
 1. No hostname specified.

ルータのホスト名を設定するには、`hostname` グローバル コンフィギュレーション コマンドを使用する必要があります。
 2. No domain specified.

ルータのホストドメインを設定するには、`ip domain-name` グローバル コンフィギュレーション コマンドを使用する必要があります。
- 許可されるSSH接続の数は、ルータに `vtty` 設定された最大数に制限されます。各SSH接続は `vtty` ソースを使用します。

SSH では、ルータで AAA によって設定されるローカルセキュリティまたはセキュリティプロトコルが、ユーザー認証に使用されます。AAA を設定する場合は、コンソールが AAA で実行されないようにする必要があります。コンソールで AAA を無効にするには、グローバル コンフィギュレーション モードでキーワードを適用します。

No SSH server connections running:

```
carter#show ssh %No SSHv2 server connections running.
```

この出力は、SSH サーバがディセーブルであるか、または正しくイネーブルになっていないことを示しています。SSH がすでに設定されている場合、デバイスの SSH サーバを再設定することを推奨します。デバイスで SSH サーバを再設定するには、次の手順を実行します。

- RSA キーペアを削除します。RSA キーペアを削除すると、SSH サーバは自動的に無効になります。

```
carter(config)#crypto key zeroize rsa
```



注：SSH v2 を有効にする場合は、ビットサイズが 768 以上のキーペアを生成することが重要です。



注意：設定を保存した後に、このコマンドを取り消すことはできません。また、RSA キーが削除された後は、RSA キーを再生成して CA の相互運用性を再設定し、CA 証明書を取得し、独自の証明書を再度要求しない限り、証明書または CA を使用したり、他の IP セキュリティ (IPSec) ピアとの証明書交換に参加したりすることはできません。

2. デバイスのホスト名とドメイン名を再設定します。

```
carter(config)#hostname hostname
```

```
carter(config)#ip domain-name domainname
```

3. ルータの RSA キーペアを生成します。生成すると、SSH が自動的に有効になります。

```
carter(config)#crypto key generate rsa
```



注：このコマンドの使用方法の詳細については、『[crypto key generate rsa - Cisco IOS Security Command Reference, Release 12.3](#)』を参照してください。



注：SSH2 0: Unexpected mesg type received というエラーメッセージが表示されることがあります。ルータが認識できないパケットを受信したことが原因です。この問題を解決するには、SSH の RSA キーを生成する際に、キーの長さを増やします。

4. SSH サーバを設定します。

5. SSH サーバ用にシスコルータ/スイッチを有効にして設定するには、SSH パラメータを設定する必要があります。SSH パラメータを設定しない場合、デフォルト値が使用されます。

```
ip ssh {[timeout seconds] | [authentication-retries integer]}
```

```
carter(config)# ip ssh
```

関連情報

- [SSH 製品に関するサポート ページ](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。