

目次

概要

[SSH 端末回線アクセス \(別名、リバース Telnet \) はどのように設定するのですか。](#)

[Catalyst 2900 では SSH はサポートされていますか。](#)

[どのプラットフォームとコードバージョンで SSH がサポートされているかを識別するにはどうすればよいのですか。](#)

[ルータから特定の SSH コマンドを削除しようとしたが、SSH をイネーブルにするには、RSA キーを作成するようという指示が繰り返し表示されます。なぜでしょうか。](#)

[Cisco IOS® SSH バージョン 2 は Digital Signature Standard \(DSS \) をサポートしますか。](#)

[Cisco IOS SSH サーバでは、エージェント転送がサポートされていますか。](#)

[Cisco IOS SSH サーバでどんなクライアント認証 メカニズムがサポートされますか。](#)

[Local: Corrupted check bytes on input というエラーは何を意味するのですか。](#)

[Blowfish の Cisco IOS サポート SSH は暗号化しますか。](#)

[生成することを試みるとき暗号キーを使用してルータの SSH アクセスのための RSA キーはコンフィギュレーションモードの rsa コマンドを、受け取りますこのエラーを生成します: %^。それはルータがルータのための SSH アクセスをイネーブルにするために RSA キーを生成しないようにしません。この問題の解決方法を次に説明します。](#)

[暗号画像はトリプル DES または AES のような暗号と SSH を使用するために強い暗号をサポートしますか。](#)

[これらのメッセージはログでルータの SSH を設定することを試みるとき見られます: SSH2_13:](#)

[RSA sign: および SSH2_13: -1。どうすれば、これを解決できるのですか。](#)

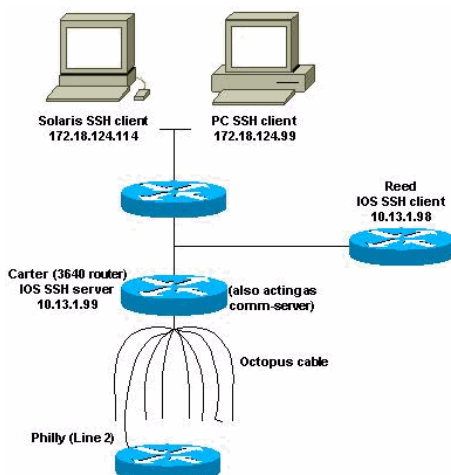
関連情報

概要

このドキュメントでは Secure Shell (SSH) に関する FAQ に回答しています。

Q. SSH 端末回線アクセス (別名、リバース Telnet) はどのように設定するのですか。

A. これは Cisco IOS® ソフトウェア リリース 12.2.2.T のいくつかのプラットフォームで最初に導入されました。



```
Router (config)#line line-number [ending-line-number] Router (config-line)#no exec Router (config-
```

```
line)#login {local | authentication listname Router(config-line)#rotary group Router(config-
line)#transport input {all | ssh} Router(config-line)#exit Router(config)#ip ssh port portnum
rotary group !--- Line 1 SSH Port Number 2001line 1 no exec login authentication default rotary
1 transport input ssh!--- Line 2 SSH Port Number 2002line 2 no exec login authentication default
rotary 2 transport input ssh!--- Line 3 SSH Port Number 2003line 3 no exec login authentication
default rotary 3 transport input ssh ip ssh port 2001 rotary 1 3
```

コマンド リファレンス :

```
ip ssh port ip ssh port portnum rotary group no ip ssh port portnum rotary group
```

- `portnum` は SSH が接続する必要がある 2001 年のようなポートを規定します。
- **ロータリグループ**は が定義されたロータリーその規定する 有効な名前を捜す必要があります。

Q. Catalyst 2900 では SSH はサポートされていますか。

A. いいえ。サポートされていません。

Q. どのプラットフォームとコードバージョンで SSH がサポートされているかを識別するにはどうすればよいのですか。

A. [Feature Navigator](#) ([>登録](#)ユーザ専用) を参照し、SSH 機能を指定してください。

Q. ルータから特定の SSH コマンドを削除しようとしたが、SSH をイネーブルにするには、RSA キーを作成するようという指示が繰り返し表示されます。なぜでしょうか。

A. この問題の例を次に示します。

```
804#configure terminalEnter configuration commands, one per line. End with CNTL/Z.804(config)#no
ip ssh time-out 120Please create RSA keys to enable SSH.804(config)#no ip ssh authenPlease
create RSA keys to enable SSH.804(config)
```

これは Cisco Bug ID [CSCdv70159](#) ([登録](#)ユーザ専用) で報告されている問題です。

Q. Cisco IOS® SSH バージョン 2 は Digital Signature Standard (DSS) をサポートしますか。

A. Cisco IOS SSH バージョン 2 は DSS をサポートしません。

Q. Cisco IOS SSH サーバでは、エージェント転送がサポートされていますか。

A. Cisco IOS SSH は、エージェント転送をサポートしていません。Cisco IOS SSH は、流通しているすべての SSH 実装と相互運用できます。

Q. Cisco IOS SSH サーバでどんなクライアント認証 メカニズムがサポートされますか。

A. Cisco IOS SSH バージョン 2 (SSHv2) はキーボード対話型およびパスワードベース 認証方式をサポートします。これらの認証方式に加えて、RSA 主要特点 (Cisco IOS ソフトウェア リリース 15.0(1)M から利用可能な開始) のための SSHv2 機能拡張はクライアント および サーバのための RSA ベースの公開キー 認証をサポートします。Cisco IOS SSH サーバによってサポー

トされる認証機構のその他の情報に関しては[セキュアシェルバージョン2サポート](#)を参照して下さい。

Q. Local: Corrupted check bytes on input というエラーは何を意味するのですか。

A. Corrupted checkbytes (チェックバイトの破損)は、受信したSSHパケットが完全性チェックに失敗したことを意味します。これは通常、不適切な復号化が原因です。また、不適切なキーを使用したことも原因です。不適切なキーは、暗号化されたSSHパケットのドロップによって発生します。送信されているはずの暗号化パケットがドロップされたか、復号化されているはずの受信暗号化パケットがドロップされたかのいずれかです。

Q. Blowfish の Cisco IOS サポート SSH は暗号化しますか。

A. Cisco IOS は Blowfish 暗号の SSH をサポートしません。SSH クライアントがそのようなサポートされていない暗号を送信するとき、ルータディスプレイデバッグメッセージは[SSH クライアント送信サポートされていない \(Blowfish\) 暗号](#)で述べました。

Q. 生成することを試みるときに rsa コマンドを *^。それはルータがルータのための SSH アクセスをイネーブルにするために RSA キーを生成しないようにしません。この問題の解決方法を次に説明します。

A. このエラーはルータで使用されるイメージが暗号キー生成する rsa コマンドをサポートしないと現われます。このコマンドはセキュリティイメージでだけサポートされます。このエラーを解決するために使用される適切な一連の Cisco IOS ルータのセキュリティイメージを使用して下さい。

Q. 暗号画像はトリプル DES または AES のような暗号と SSH を使用するために強い暗号をサポートしますか。

A. はい。暗号画像 サポート強い暗号だけ。SSH をトリプル DES または AES のような暗号と使用するために Cisco デバイスの暗号画像を持たなければなりません。

Q. これらのメッセージはログでルータの SSH を設定することを試みるとき見られます: SSH2 13: RSA_sign: および SSH2 13: -1。どうすれば、この問題を解決できますか。

A. これらのログメッセージは Cisco バグ ID [CSCsa83601](#) ([登録ユーザのみ](#)) および [CSCtc41114](#) ([登録ユーザのみ](#)) が見られた原因です。詳細については、これらのバグを参照してください。

関連情報

- [SSH サポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)