

Secure Shell (SSH) に関する FAQ

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にという指示が繰り返し表示されます。なぜなのでしょう。](#)

[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に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: 無効な入力%の「^」マーカーで検出する。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: 見つけれないプライベートキーおよび SSH2 13: シグニチャ作成は、ステータス -1 失敗しました。どうすれば、これを解決できるのですか。](#)

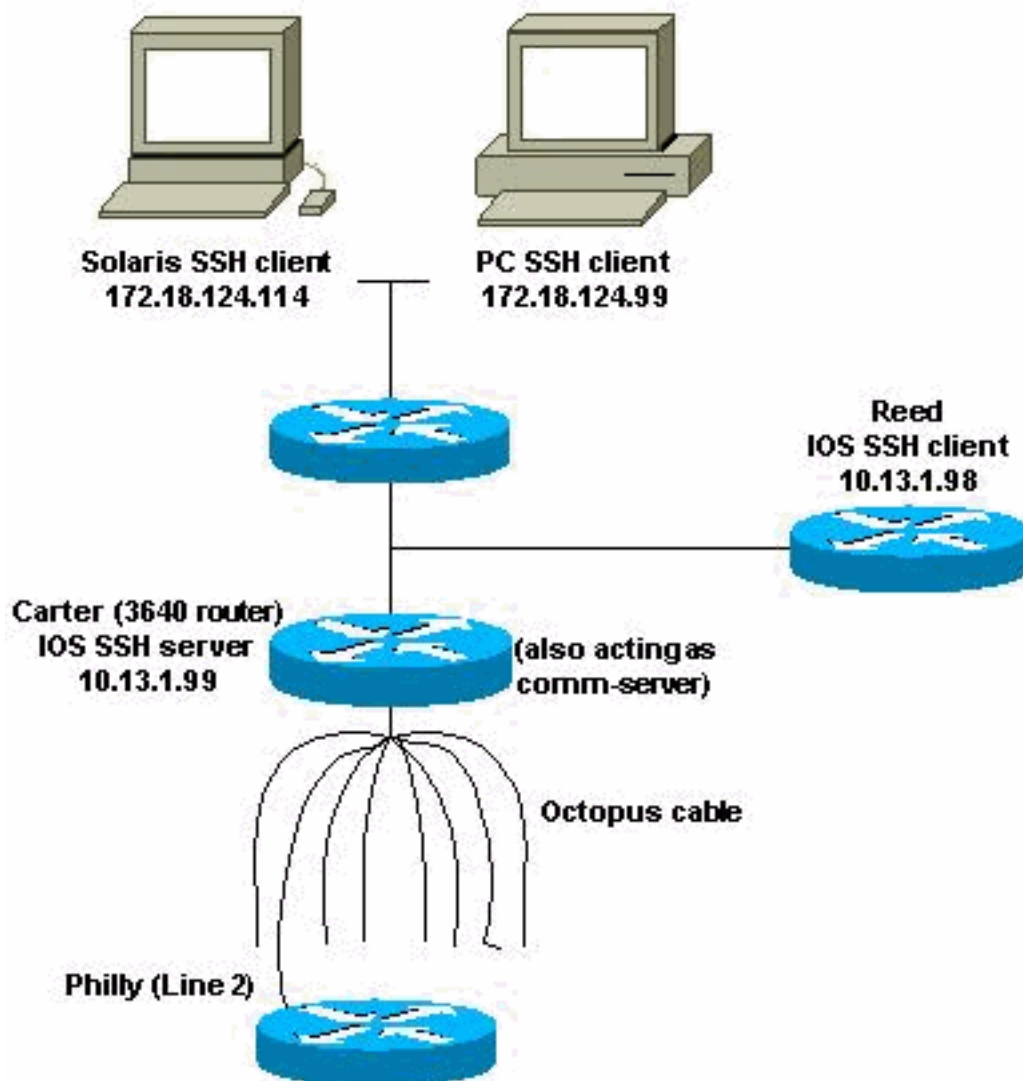
関連情報

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。Cisco IOS[®] SSH コードは Cisco オリジナル コードです。

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。

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 2001 line 1 no exec login authentication default rotary 1 transport
input ssh !--- Line 2 SSH Port Number 2002 line 2 no exec login authentication default rotary 2
transport input ssh !--- Line 3 SSH Port Number 2003 line 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 - 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-定義されたロータリ-その有効な名前を捜す必要があります規定します。

Catalyst 2900 では SSH はサポートされていますか。

いいえ。サポートされていません。

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。

[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。

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。

この問題の例はここに示されています:

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

Cisco バグ ID [CSCdv70159](#) ([登録ユーザのみ](#)) に出会いました。

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 バージョン 2 は DSS をサポートしません。

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 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。

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。

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 主要特点のための SSHv2 拡張は (Cisco IOS ソフトウェア リリース 15.0(1)M およびそれ以降で利用可能な) 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ついては[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。

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

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。

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

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。

生成することを試みるときに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。

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。

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。

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。

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。

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](#)