Telnet コマンド、SSH コマンド、および Slogin コマンド

この章は、次の項で構成されています。

ip telnet server

リモート Telnet クライアントからの接続要求を受け入れる Telnet サーバとしてデバイスを有効にするには、**ip telnet server** グローバル コンフィギュレーション モード コマンドを使用します。リモート Telnet クライアントでは、Telnet 接続を介してデバイスを設定できます。

デバイス上の Telnet サーバ機能を無効にするには、このコマンドの no 形式を使用します。

構文

ip telnet server

no ip telnet server

デフォルト設定

無効

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デバイスでリモート SSH クライアントとリモート Telnet クライアントの両方からの接続要求を受け入れるようにすることができます。リモート クライアントからデバイスへの接続には（Telnet ではなく）SSH を使用することを推奨します。SSH はセキュア プロトコルですが、Telnet はそうではないからです。デバイスを SSH サーバとして有効にするには、**ip ssh server** コマンドを使用します。

例

次の例では、Telnet サーバからデバイスを設定できるようにしています。

```
switchxxxxxx(config)# ip telnet server
```

ip SSH logging

SSHセッションのセットアップとシャットダウンに関連するトラップの送信を有効または無効にするには、グローバル コンフィギュレーション モードでip ssh loggingを使用します。デフォルト設定に戻すには、このコマンドのno形式を使用します。

構文

ip ssh logging [enable | disable]

no ip ssh logging

パラメータ

- **enable** ：デバイスでSSHロギングを有効にします。
- **disable** ：デバイスでSSHロギングを無効にします。

デフォルト設定

デフォルトでは、SSHセッションロギングは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、デバイスでSSHロギングを有効にします。SSHロギングは、SSHセッションのセットアップと切断の進行状況を追跡する手段です。SSHセッションのセットアップと切断の進行状況は、プロセスの一部として生成されるSYSLOGメッセージを使用して追跡されます。SSHロギングが無効になっている場合、SSHのセットアップまたは切断プロセスの一部としてSYSLOGメッセージは生成されません。

例

次に、デバイスでSSHロギングを有効にする例を示します。

```
switchxxxxxx(config)# ip ssh logging enable
```

ip ssh server

ip ssh server グローバル コンフィギュレーション モード コマンドは、デバイスを SSH サーバとして有効にし、リモート SSH クライアントからの接続要求を受け入れることができるようにします。リモート SSH クライアントでは、SSH 接続を介してデバイスを管理できます。

デバイスで SSH サーバ機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh server

no ip ssh server

デフォルト設定

SSH サーバ機能はデフォルトでは無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

デバイスは、SSH サーバとして、暗号キーを自動的に生成します。

新しい SSH サーバ キーを生成するには、**crypto key generate dsa** コマンドおよび **crypto key generate rsa** コマンドを使用します。

例

次の例では、デバイスを SSH サーバとして設定しています。

```
switchxxxxxx(config)# ip ssh server
```

ip ssh port

ip ssh port グローバル コンフィギュレーション モード コマンドは、SSH サーバで使用する TCP ポートを指定します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

ip ssh port *port-number*

no ip ssh port

パラメータ

- ***port-number***：SSH サーバで使用する TCP ポート番号を指定します。（範囲：1ー59999）。

デフォルト設定

デフォルトの TCP ポート番号は 22 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 モード

例

次の例では、TCP ポート番号 808 を SSH サーバで使用することを指定しています。

```
switchxxxxxx(config)# ip ssh port 808
```

ip ssh password-auth

受信 SSH セッションのパスワード認証を有効にするには、**ip ssh password-auth** グローバル コンフィギュレーション モード コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh password-auth

no ip ssh password-auth

デフォルト設定

受信 SSH セッションのパスワード認証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、リモートSSHクライアントのローカルSSHサーバによるパスワード キー認証が有効になります。

ローカル SSH サーバは有効になっているすべての SSH 認証方式をアドバタイズし、リモート SSH クライアントがそれらのいずれかを選択します。

リモート SSH クライアントが公開キーによって正常に認証された後も、クライアントがデバイスへの管理アクセスを取得するためには、クライアントを引き続き AAA 認証する必要があります。

SSH 認証方式が有効でない場合、リモート SSH クライアントはデバイスに対する管理アクセスを取得する前に AAA 認証される必要があります。

例

次の例では、SSH クライアントのパスワード認証を有効にしています。

```
switchxxxxxx(config)# ip ssh password-auth
```

ip ssh pubkey-auth

受信 SSH セッションの公開キー認証を有効にするには、**ip ssh pubkey-auth** グローバル コンフィギュレーション モード コマンドを使用します。

この機能を無効にするには、このコマンドの **no** 形式を使用します。

構文

ip ssh pubkey-auth [**auto-login**]

no ip ssh pubkey-auth

パラメータ

- **auto-login**：デバイス管理の AAA 認証（CLI ログイン）が必要ないことを指定します。デフォルトでは、SSH 認証後、ログインが必要です。

デフォルト設定

受信 SSH セッションの公開キー認証は無効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドを使用すると、リモート SSH クライアントのローカル SSH サーバによる公開キー認証が有効になります。

ローカル SSH サーバは有効になっているすべての SSH 認証方式をアドバタイズし、リモート SSH クライアントがそれらのいずれかを選択します。

リモート SSH クライアントが公開キーによって正常に認証された後も、クライアントがデバイスへの管理アクセスを取得するためには、クライアントを引き続き AAA 認証する必要があります。ただし、auto-login パラメータを指定した場合を除きます。

SSH 認証方式が有効でない場合、リモート SSH クライアントはデバイスに対する管理アクセスを取得する前に AAA 認証される必要があります。

公開キーによる SSH 認証に **auto-login** キーワードを指定した場合、SSH 認証が正常に完了し、使用された SSH の名前がローカル ユーザ データベースで検出されると、管理アクセスが付与されます。デバイス管理の AAA 認証は、ユーザに対して透過的です。ユーザ名がローカル ユーザ データベース内にない場合、ユーザは警告メッセージを受信し、SSH 認証とは関係なくデバイス管理の AAA 認証を通過する必要があります。

auto-login キーワードを指定しないと、管理アクセスは、ユーザが SSH 認証とデバイス管理の AAA 認証の両方を個別に受けて通過した場合にのみ付与されます。有効な SSH 認証方式がない場合、管理アクセスは、ユーザがデバイス管理によって AAA 認証された場合にのみ付与さ

れます。SSH 認証方式がないというのは、SSH は有効になっているものの、公開キーによる SSH 認証もパスワードも有効になっていないということです。

例

次の例では、SSH クライアントの認証を有効にしています。

```
switchxxxxxx(config)# ip ssh pubkey-auth
```

crypto key pubkey-chain ssh

crypto key pubkey-chain ssh グローバル コンフィギュレーション モード コマンドは、SSH 公開キー チェーン コンフィギュレーション モードを開始します。このモードは、SSH クライアント公開キーなどデバイスの公開キーを手動で指定する場合に使用します。

構文

crypto key pubkey-chain ssh

デフォルト設定

キーが存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、SSH クライアント公開キーを手動で指定する場合に使用します。

例

次の例では、SSH 公開キー チェーン コンフィギュレーション モードを開始して、ユーザ 'bob' に対して SSH 公開キー チェーンの RSA キー ペアを手動で設定しています。

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
```

user-key

user-key SSH 公開キー文字列コンフィギュレーション モード コマンドは、ユーザ名と手動で設定した SSH 公開キーを関連付けます。

SSH ユーザと関連する公開キーを削除するには、**no user-key** コマンドを使用します。

構文

user-key *username* {**rsa** | **dsa**}

no user-key *username*

パラメータ

- ***username***：リモート SSH クライアントのユーザ名を指定します。（長さ：1 ～ 48 文字）
- **rsa**：RSA キー ペアを手動で設定することを指定します。
- **dsa**：DSA キー ペアを手動で設定することを指定します。

デフォルト設定

SSH 公開キーは存在しません。

コマンド モード

SSH 公開キー文字列コンフィギュレーション モード

使用上のガイドライン

このコマンドを入力すると、ユーザに関連付けられた既存のキー（ある場合）は削除されます。このキーをユーザに設定するには、このコマンドの後に key-string コマンドを入力する必要があります。

例

次の例では、SSH 公開キー チェーン bob の SSH 公開キーを手動で設定しています。

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
```

key-string

key-string SSH 公開キーストリング コンフィギュレーション モード コマンドを使用して、SSH 公開キーを手動で指定します。

構文

key-string *[***row** key-string]

パラメータ

- **row**：SSH 公開キーを行ごとに指定します。行の最大長は、160 文字です。
- ***key-string***：UU でエンコードされた DER 形式のキーを指定します。UU エンコードされた DER 形式は、OpenSSH で使用される authorized_keys ファイルと同じ形式です。

デフォルト設定

キーが存在しません。

コマンド モード

SSH 公開キー文字列コンフィギュレーション モード

使用上のガイドライン

row パラメータを指定しない **key-string** SSH 公開キー文字列コンフィギュレーション モード コマンドは、次にどの SSH 公開キーを対話式に設定するかを指定する場合に使用します。文字を含めずに行を入力してコマンドを完了します。

key-string row SSH 公開キー文字列コンフィギュレーション モード コマンドは、SSH 公開キーを行ごとに指定する場合に使用します。各行は、**key-string row** コマンドで始める必要があります。

UU エンコードされた DER 形式は、OpenSSH で使用される authorized_keys ファイルと同じ形式です。

例

次の例では、SSH 公開キー クライアント 'bob' の公開キー文字列を入力しています。

```
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string
AAAAB3NzaC1yc2EAAAADAQABAAABAQCvTnRwPWl
Al4kpqIw9GBRonZQZxjHKcqKL6rMlQ+
ZNXfZSkvHG+QusIZ/76ILmFT34v7u7ChFAE+
Vu4GRfpSwoQUvV35LqJJk67IOU/zfwOl1g
kTwml75QR9gHujS6KwGN2QWXgh3ub8gDjTSq
muSn/Wd05iDX2IExQWu08licglk02LYciz
+Z4TrEU/9FJxwPiVQOjc+KBXuR0juNg5nFYsY
0ZCk0N/W9a/tnkm1shRE7Di71+w3fNiOA
```

```
6w9o44t6+AINEICBCCA4YcF6zMzaT1wefWwX6f+
Rmt5nhhqdAtN/4oJfce166DqVX1gWmN
zNR4DYDvSzg0lDnwCAC8Qh
Fingerprint: a4:16:46:23:5a:8d:1d:b5:37:59:eb:44:13:b9:33:e9
switchxxxxxx(config)# crypto key pubkey-chain ssh
switchxxxxxx(config-keychain)# user-key bob rsa
switchxxxxxx(config-keychain-key)# key-string row AAAAB3Nza
switchxxxxxx(config-keychain-key)# key-string row C1yc2
```

show ip ssh

show ip ssh 特権 EXEC モード コマンドは、SSH サーバ設定を表示します。

構文

show ip ssh

コマンド モード

特権 EXEC モード

例

次に、SSH サーバの設定を表示する例を示します。

```
switchxxxxxx# show ip ssh
SSH server enabled. Port: 22
SSH session logging is disabled
RSA key was generated.
DSA (DSS) key was generated.
SSH Public Key Authentication is enabled with auto-login.
SSH Password Authentication is enabled.
Active incoming sessions:
```

IP Address	SSH Username	Version	Cipher	Auth Code
---	---	---	---	---
172.16.0.1	John Brown	1.5	3DES	HMAC-SHA1
182.20.2.1	Bob Smith	1.5	3DES	Password

次の表に、この出力で表示される重要なフィールドの説明を示します。

フィールド	説明
IP Address	クライアント アドレス
SSH Username	ユーザ名
Version	SSH バージョン番号
Cipher	暗号化タイプ（3DES、Blowfish、RC4）
Auth Code	認証コード（HMAC MD5、HMAC SHA1）またはパスワード

show crypto key pubkey-chain ssh

show crypto key pubkey-chain ssh 特権 EXEC モード コマンドを使用すると、デバイスに保存されている SSH 公開キーが表示されます。

構文

show crypto key pubkey-chain ssh [**username** *username*] [**fingerprint** {**bubble-babble** | **hex**}]

パラメータ

- **username** *username*：リモート SSH クライアントのユーザ名を指定します。（長さ：1 ～ 48 文字）
- **fingerprint** {**bubble-babble** | **hex**}：フィンガープリントの表示形式を指定します。次の値が可能です。

  bubble-babble：フィンガープリントが Bubble Babble 形式で表示されることを指定します。

  hex：フィンガープリントを 16 進形式で表示することを指定します。

デフォルト設定

デフォルトのフィンガープリント形式は 16 進数です。

コマンド モード

特権 EXEC モード

例

次の例では、デバイスに保存されている SSH 公開キーを表示します。

```
switchxxxxxx# show crypto key pubkey-chain ssh
Username       Fingerprint
-----------    -----------------------------------------------------------
bob            9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
john           98:F7:6E:28:F2:79:87:C8:18:F8:88:CC:F8:89:87:C8
switchxxxxxx# show crypto key pubkey-chain ssh username bob
Username       Fingerprint
-----------    -----------------------------------------------------------
bob            9A:CC:01:C5:78:39:27:86:79:CC:23:C5:98:59:F1:86
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。