セキュア シェルの設定

セキュア シェルの設定

セキュア シェル（SSH）は、Berkeley の r ツールへのセキュアな置換を提供するアプリケーションおよびプロトコルです。プロトコルは標準の暗号メカニズムを使用してセッションの安全を確保します。アプリケーションは Berkeley の rexec および rsh ツールと同様に使用できます。2 つのバージョンの SSH（SSH バージョン 1 と SSH バージョン 2）を使用できます。特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。SSH バージョン 2 については、「セキュアシェルバージョン 2 サポート」機能モジュールを参照してください。

セキュア シェルを設定するための前提条件

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman（RSA）の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- デバイスに必要なイメージをダウンロードします。セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェア イメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで **hostname** および **ip domain name** コマンドを使用して、デバイスのホスト名とホストドメインを設定します。
- デバイスの Rivest, Shamir and Adleman（RSA）キーペアを生成します。グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを入力すると、このキーペアによって SSH とリモート認証が自動的に有効になります。

（注） RSA キーのペアを削除するには、**crypto key zeroize rsa** グローバル コンフィギュレーション コマンドを使用します。RSA キー ペアを削除すると、SSH サーバは自動的にディセーブルになります。

- ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。認証、許可、アカウンティング（AAA）の有無に関係なく、認証を設定できます。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェア イメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。

セキュア シェルの設定に関する制約事項

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

- セキュアシェル（SSH）サーバと SSH クライアントは、Data Encryption Standard（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェア イメージのみでサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- 実行シェルは、唯一サポートされるアプリケーションです。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。
- SFTP サーバはサポートされていません。

セキュア シェルの設定について

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2（SSHv2）をサポートします。

SSH サーバ

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

セキュアシェル（SSH）サーバ機能を使用すると、SSHクライアントはシスコデバイスとの間で、セキュアな暗号化された接続を確立できます。この接続は、インバウンドTelnet接続の機能と同様です。SSH 以前は、セキュリティは Telnet のセキュリティに限定されていました。SSH を Cisco ソフトウェアの認証と併用することで、強力な暗号化が可能になります。Cisco ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用できます。

SSH 統合クライアント

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

セキュア シェル（SSH）統合クライアント機能は、SSHプロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いてTelnetのアウトバウンド接続と同様の機能を提供します。SSHクライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

シスコ ソフトウェアの SSH クライアントは、市販の一般的な SSH サーバと使用します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。ユーザ認証は、デバイスに対するTelnetセッションの認証と同様に実行されます。SSH がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service（RADIUS）、TACACS+、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

RSA 認証のサポート

セキュア シェル（SSH）クライアントで使用できるRivest、Shamir、Adleman（RSA）認証は、Cisco ソフトウェアの SSH サーバではデフォルトでサポートされていません。RSA 認証サポートの詳細については、「セキュアシェルバージョン2サポート」の「RSAペアを使用したSSHバージョン 2 のデバイス設定」セクションを参照してください。

SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSHプロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いてTelnetのアウトバウンド接続と同様の機能を提供します。SSHクライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSHサーバおよびSSH統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSHクライアントは、市販の一般的なSSHサーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対するTelnetセッションの認証と同様に実行されます。SSHは、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- SSHサーバがアクティブスイッチ上で動作しており、アクティブスイッチに障害が発生した場合、新しいアクティブスイッチは、以前のアクティブスイッチによって生成された RSA キーペアを使用します。
- **crypto key generate rsa**グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、グローバル コンフィギュレーション モードで **hostname** コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、グローバル コンフィギュレーション モードで **ip domain name** コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

セキュア シェルの設定方法

SSH を実行するためのデバイスの設定

SSH を実行するようにデバイスをセットアップするには、次の手順を実行してください。

始める前に

ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**hostname** *hostname* 例： `Device(config)# hostname your_hostname`	device のホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、device を SSH サーバとして設定する場合だけです。
ステップ 4	**ip domain name** *domain_name* 例： `Device(config)# ip domain name your_domain`	device のホストドメインを設定します。
ステップ 5	**crypto key generate rsa** 例： `Device(config)# crypto key generate rsa`	device 上でローカルおよびリモート認証用に SSH サーバをイネーブルにし、RSA キー ペアを生成します。device の RSA キー ペアを生成すると、SSH が自動的にイネーブルになります。 最小モジュラス サイズは、1024 ビットにすることを推奨します。

	コマンドまたはアクション	目的
		RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、device を SSH サーバとして設定する場合だけです。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ip ssh** 例： `Device# show ip ssh`	（任意）SSH サーバが有効であることを確認し、SSH 接続のバージョンおよび設定データを表示します。

SSH サーバの設定

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip ssh** { **time-out** *seconds* | **authentication-retries** *integer*} 例： `Device(config)# ip ssh time-out 30`	セキュアシェル（SSH）制御パラメータを設定します。 （注） このコマンドは、ユーザに表示するパスワード プロンプトの回数を設定するためにも使用できます。この数値は、次の 2 つの値の低い方です。

	コマンドまたはアクション	目的
		• **ssh -o numberofpasswordprompt** コマンドを使用してクライアントから提案された値。 • **ip ssh authentication-retries** *integer* コマンドを使用してデバイスに設定された値に 1 を加えた値。
ステップ 4	**ip ssh rekey** { **time** *time* | **volume** *volume*} 例： `Device(config)# ip ssh rekey time 108`	（任意）SSH の時間ベースのキー再生成またはボリュームベースのキー再生成を設定します。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ip ssh** 例： `Device# show ip ssh`	（任意）SSH サーバが有効であることを確認し、SSH 接続のバージョンおよび設定データを表示します。

SSH クライアントの呼び出し

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

セキュア シェル（SSH）クライアントを呼び出すには、次の作業を実行します。SSH クライアントはユーザ EXEC モードで実行されます。設定作業は特にありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**ssh -l** *username* **-vrf** *vrf-name* *ip-address* 例： `Device# ssh -l user1 -vrf vrf1 192.0.2.1`	SSH クライアントを呼び出し、指定した仮想ルーティングおよび転送（VRF）インスタンスの IP ホストまたはアドレスに接続します。

セキュア シェルの設定例

例：SSH サーバの設定

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

次に、サーバに設定されたセキュアシェル（SSH）制御パラメータの例を示します。この例では、30秒のタイムアウト間隔が指定されています。このタイムアウト間隔は、SSHネゴシエーションフェーズで使用されます。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh timeout 30
Device(config)# end
```

例：SSH クライアントの呼び出し

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

次の例では、指定された Virtual Routing and Forwarding（VRF）インスタンスの IP アドレス 192.0.2.1 に接続するためにセキュアシェル（SSH）クライアントが呼び出されています。

```
Device> enable
Device# ssh -1 user1 -vrf vrf1 192.0.2.1
```

例：SSH の確認

（注） 特に明記しない限り、「SSH」という用語は「SSH バージョン 1」のみを意味します。

セキュア シェル（SSH）サーバが有効であることを確認し、SSH接続のバージョンおよび設定データを表示するには、**show ip ssh** コマンドを使用します。次に、SSHがイネーブルの例を示します。

```
Device# show ip ssh

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

次に、SSH がディセーブルの例を示します。

```
Device# show ip ssh

%SSH has not been enabled
```

SSH サーバ接続のステータスを確認するには、**show ssh** コマンドを使用します。次に、SSH を有効にしたときのデバイス上の SSH サーバ接続の例を示します。

```
Device# show ssh

Connection      Version     Encryption State Username
 0 1.5 3DES Session Started  guest
```

次に、SSH がディセーブルの例を示します。

```
Device# show ssh

%No SSH server connections running.
```

セキュア シェルに関するその他の参考資料

関連資料

関連項目	マニュアル タイトル
SSH バージョン 2	『セキュリティ コンフィギュレーション ガイド』の「セキュアシェルバージョン 2 サポート」

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

セキュアシェルの設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.9.2	セキュア シェル	SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。