セキュア シェル（SSH）の設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

セキュア シェル（SSH）およびセキュア コピー プロトコル（SCP）用にスイッチを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに 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。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。 また、許可されている管理者もこの作業をワークステーションから実行できます。

関連トピック

セキュア コピー プロトコルの概念, （5 ページ）

SSH 用にスイッチを設定するための制約事項

セキュア シェル用にスイッチを設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、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でのみサポートされます。
- スイッチは、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。 ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- このソフトウェア リリースは、IP Security（IPSec）をサポートしていません。
- SCP を使用する場合、copy コマンドにパスワードを入力することはできません。 プロンプトが表示されたときに、入力する必要があります。

関連トピック

セキュア コピー プロトコルの概念, （5 ページ）

SSH に関する情報

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 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH およびスイッチ アクセス

SSH の設定例については、『*Cisco IOS Security Configuration Guide, Cisco IOS Release 12.4*』の「Other Security Features」の章の「Configuring Secure Shell」にある「SSH Configuration Examples」を参照してください。

IPv6 の SSH 機能は IPv4 における機能と同じです。 IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

（注） ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応したコマンド リファレンスおよび『*Cisco IOS Security Command Reference, Release 12.4*』と『*Cisco IOS IPv6 Command Reference*』の「Other Security Features」の章の「Secure Shell Commands」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

SSH 機能には SSH サーバおよび SSH 統合クライアントがあり、これらはスイッチ上で実行されるアプリケーションです。 SSH クライアントを使用すると、SSH サーバが稼働するスイッチに接続できます。 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。また、SSH クライアントは、このリリースでサポートされている SSH サーバおよび他社製の SSH サーバと使用します。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

SSH は、データ暗号規格（DES）暗号化アルゴリズム、Triple DES（3DES）暗号化アルゴリズム、およびパスワードベースの認証をサポートしています。

SSH は次のユーザ認証方式をサポートしています。

- TACACS+
- RADIUS

- ローカル認証および許可

関連トピック

スイッチのローカル認証および許可の設定
TACACS+ およびスイッチ アクセス
RADIUS およびスイッチ アクセス

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）。
- スタック マスターで SSH サーバが実行されている場合で、スタック マスターに障害が発生した場合、新しいスタック マスターでは、前のスタック マスターによって生成された RSA キー ペアが使用されます。
- **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。 詳細については、次の関連項目を参照してください。
- 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、**hostname** グローバル コンフィギュレーション 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、**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。

関連トピック

スイッチで SSH を実行するためのセットアップ, （5 ページ）
スイッチのローカル認証および許可の設定

セキュア コピー プロトコルの概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。 SCP には、Berkeley r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルであるセキュア シェル（SSH）が必要です。

SSH を動作させるには、スイッチに 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 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。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。 プロンプトが表示されたときに、入力する必要があります。

セキュア コピー プロトコルの概念

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。 SCP には、Berkeley r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルであるセキュア シェル（SSH）が必要です。

Secure Copy 機能を設定するには、SCP の概念を理解する必要があります。

SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。 また、SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。

SCP の設定および検証方法の詳細については、『*Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4*』の「Secure Copy Protocol」を参照してください。

関連トピック

セキュア シェル（SSH）およびセキュア コピー プロトコル（SCP）用にスイッチを設定するための前提条件, （1 ページ）

SSH 用にスイッチを設定するための制約事項, （2 ページ）

SSH の設定方法

スイッチで SSH を実行するためのセットアップ

SSH を実行するようにスイッチを設定するには、特権 EXEC モードで次の手順を実行します。

はじめる前に

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。詳細については、次の関連項目を参照してください。

手順の概要

1. **configure terminal**
2. **hostname** *hostname*
3. **ip domain-name** *domain_name*
4. **crypto key generate rsa**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**hostname** *hostname* 例： `Switch(config)# hostname your_hostname`	スイッチのホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
ステップ 3	**ip domain-name** *domain_name* 例： `Switch(config)# ip domain-name your_domain`	スイッチのホスト ドメインを設定します。
ステップ 4	**crypto key generate rsa** 例： `Switch(config)# crypto key generate rsa`	スイッチ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。 スイッチの 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。 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。

	コマンドまたはアクション	目的
		（注） この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。
ステップ 5	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

関連トピック

SSH 設定時の注意事項，（4 ページ）
スイッチのローカル認証および許可の設定

SSH サーバの設定

SSH サーバを設定するには、特権 EXEC モードで次の手順を実行します。

（注） この手順を実行するのは、スイッチを SSH サーバとして設定する場合だけです。

手順の概要

1. **configure terminal**
2. **ip ssh version** [**1** | **2**]
3. **ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}
4. 次のいずれかまたは両方を使用します。
   - **line vty***line_number*[*ending_line_number*]
   - **transport input ssh**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# 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 2	**ip ssh version** [**1** | **2**] 例： `Switch(config)# ip ssh version 1`	（任意）SSHv1 または SSHv2 を実行するようにスイッチを設定します。 • **1**：SSHv1 を実行するようにスイッチを設定します。 • **2**：SSHv2 を実行するようにスイッチを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。 たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 3	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} 例： `Switch(config)# ip ssh timeout 90 authentication-retries 2`	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。 指定できる範囲は 0 ～ 120 秒です。 このパラメータは、SSH ネゴシエーション フェーズに適用されます。 接続が確立されると、スイッチは CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。 実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。 デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 4	次のいずれかまたは両方を使用します。 • **line vty***line_number*[*ending_line_number*] • **transport input ssh**	（任意）仮想端末回線設定を設定します。 • ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。 *line_number* および *ending_line_number* に対して、1 回線ペアを指定します。 指定できる範囲は 0 ～ 15 です。 • スイッチで非 SSH Telnet 接続を回避するように設定します。 これにより、ルータは SSH 接続に限定されます。

	コマンドまたはアクション	目的

	例：
	`Switch(config)# line vty 1 10`
	または
	`Switch(config-line)# transport input ssh`	

ステップ 5	**end** 例： `Switch(config-line)# end`	特権 EXEC モードに戻ります。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *1*：*SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『*Cisco IOS Security Command Reference*』の「Other Security Features」の章の「Secure Shell Commands」を参照してください。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
セッションアウェアなネットワーキングに対するアイデンティティ コントロール ポリシーおよびアイデンティティ サービス テンプレートの設定。	Session Aware Networking Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ) http://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.html
RADIUS、TACACS+、Secure Shell、802.1X および AAA の設定。	Securing User Services Configuration Guide Library, Cisco IOS XE Release 3SE (Catalyst 3850 スイッチ) http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/xe-3se/3850/secuser-xe-3se-3850-library.html

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
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/support