セキュア シェルの設定

この章は、次の項で構成されています。

セキュア シェルの概要

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。

セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にデバイス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。
- 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。**hostname** と **ip domain-name** コマンドをグローバル コンフィギュレーション モードで使用します。

セキュア シェルの設定に関する制約事項

セキュア シェル用に IR1101 を設定するための制約事項は、次のとおりです。

- ルータは RSA 認証をサポートしています。

- 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、データ暗号規格（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。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。

（注） 3DES 暗号化はより強力であるため、シスコでは強く推奨しています。

詳細については、https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.htmlの Cisco IOS-XE デバイス強化ガイドを参照してください。

- 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す。
- IR1101 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。
- 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。シスコが優れたセキュリティのため推奨しているセキュア シェル バージョン 2 でサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。

SSH とルータ アクセス

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。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。

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

デバイスを 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）。
- **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 hostname 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 IP 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。

関連タスク

SSH を実行するための IR1101 の設定 （4 ページ）

セキュア シェルの設定方法

SSH を実行するための IR1101 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。詳細については、次の関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `IR1101> 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： `IR1101# 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： `IR1101(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： `IR1101(config)# ip domain-name your_domain_name`	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： `IR1101(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	**end** 例： `IR1101(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `IR1101# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `IR1101# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） デバイスを SSH サーバとして設定する場合にのみ、この手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `IR1101> 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：	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。

	コマンドまたはアクション	目的
	`IR1101# configure terminal`	
ステップ 3	**ip ssh version** [2] 例： `IR1101(config)# ip ssh version 2`	（任意）SSH バージョン 2 を実行するように device 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 4	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}
	例：
	`IR1101(config)# ip ssh timeout 90`
	`ip ssh 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、デバイスは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 5	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**
	例：
	`IR1101(config)# line vty 1 10`
	または
	`IR1101(config-line)# 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* 引数と *ending_line_number* 引数の有効な範囲は 0 ～ 15 です。
		• device で SSH 以外の Telnet 接続を防ぎ、デバイスを SSH 接続のみに限定するように指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `IR1101(config-line)# end`	回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `IR1101# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `IR1101# copy running-config startup-config`	（任意）コンフィギュレーションファイルに設定を保存します。

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。

ルータのローカル認証および許可の設定

ローカル モードで AAA を実装するようにスイッチを設定すると、サーバがなくても動作するように AAA を設定できます。ルータは、認証と許可を処理します。この設定ではアカウンティング機能は使用できません。

ローカル モードで AAA を実装するようにルータを設定して、サーバがなくても動作するように AAA を設定するには、次の手順を実行します。

（注） AAA 方式を使用して HTTP アクセスに対しルータのセキュリティを確保するには、ip http authentication aaa グローバル コンフィギュレーション コマンドでを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しルータのセキュリティは確保しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `IR1101> 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： `IR1101# 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	aaa new-model 例： `IR1101(config)# aaa new-model`	AAA の有効化
ステップ 4	aaa authentication login default local 例： `IR1101(config)# aaa authentication login default local`	ローカル ユーザ名データベースを使用するログイン認証を設定します。default キーワードにより、ローカル ユーザ データベース認証がすべてのポートに適用されます。
ステップ 5	aaa authorization exec local 例： `IR1101(config-line)# aaa authorization exec local`	ユーザの AAA 許可を設定し、ローカルデータベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 6	aaa authorization network local 例： `IR1101(config-line)# aaa authorization network local`	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	**username** *name* **privilege** *level* **password** *encryption-type password* 例： `IR1101(config-line)# username your_user_name privilege 1 password 7 secret567`	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。 **1.** *name* には、ユーザ ID を 1 ワードで指定します。スペースと引用符は使用できません。

	コマンドまたはアクション	目的
		2. （任意）*level* には、アクセス権を得たユーザに設定する権限レベルを指定します。指定できる範囲は 0 ～ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 **3.** encryption-type には、暗号化されていないパスワードが後ろに続く場合は0を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 **4.** password には、ユーザがスイッチにアクセスする場合に入力する必要のあるパスワードを指定します。パスワードは 1 ～ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ 8	**end** 例： `IR1101(config-line)# end`	回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。
ステップ 9	**show running-config** 例： `IR1101# show running-config`	入力を確認します。
ステップ 10	**copy running-config startup-config** 例： `IR1101# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

セキュア コピーに関する情報

セキュア コピー（SCP）機能は、ルータ設定またはルータ イメージ ファイルをコピーするセキュアで認証された方法を提供します。SCP は、セキュア シェル（SSH）、アプリケーション、および Berkeley r ツールのセキュアな代替手段を提供するプロトコルに依存します。

セキュア コピーの前提条件

セキュア シェル（SSH）用にデバイスを設定するための前提条件は、次のとおりです。

- SCP を有効にする前に、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 に依存して安全な伝送を行っているため、ルータには RSA キー 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、およびアカウンティング（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。

セキュア コピーの設定に関する制約事項

- SCP を有効にする前に、ルータ上で SSH、認証、および認可を正しく設定する必要があります。
- 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。

セキュアコピーの設定

シスコの IR1101 にセキュア コピー（SCP）サーバ側機能の設定をするには、次の手順を実行します。

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。

	コマンドまたはアクション	目的
ステップ 3	**aaa new-model** 例： `Device(config)# aaa new-model`	ログイン時の AAA 認証を設定します。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default group tacacs+`	AAA アクセス コントロール システムをイネーブルにします。
ステップ 5	**username** *name* [**privilege** *level*] **password** *encryption-type encrypted-password* 例： `Device(config)# username superuser privilege 2 password 0 superpassword`	ユーザ名をベースとした認証システムを構築します。 （注） TACACS+ や RADIUS などのネットワークベースの認証メカニズムが設定されている場合は、この手順を省略できます。
ステップ 6	**ip scp server enable** 例： `Device(config)# ip scp server enable`	SCP サーバ側機能を有効にします。
ステップ 7	**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 8	**show running-config** 例： `Device# show running-config`	（任意）SCP サーバ側機能を表示します。
ステップ 9	**debug ip scp** 例： `Device# debug ip scp`	（任意）SCP 認証問題を解決します。

例

IR1101# **copy scp <*somefile*> your_username@remotehost:/<*some/remote/directory*>**

その他の参考資料

ここでは、SSH 機能に関する関連資料について説明します。

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』： https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf
RADIUS、TACACS+、Secure Shell、802.1x および AAA の設定。	『Security and VPN Configuration Guide, Cisco IOS XE 17.x』： https://www.cisco.com/c/en/us/td/docs/routers/ios/config/17-x/sec-vpn/b-security-vpn.html

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。