



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。

- [セキュア シェルを設定するための前提条件 \(1 ページ\)](#)
- [セキュア シェルの設定に関する制約事項 \(2 ページ\)](#)
- [セキュア シェルの設定について \(2 ページ\)](#)
- [セキュア シェルの設定方法 \(5 ページ\)](#)
- [セキュア シェルの設定例 \(16 ページ\)](#)
- [セキュア シェルに関するその他の参考資料 \(18 ページ\)](#)
- [セキュア シェルの設定の機能履歴 \(18 ページ\)](#)

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 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。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウントिंग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、およびアカウントिंग (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 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。

セキュア シェルの設定に関する制約事項

セキュア シェル用にデバイス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、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。
- **device** 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。
- 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。
- 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。
- 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。
- FreeRADIUS over RADSEC でクライアントを認証するには、1024 ビットよりも長い RSA キーを生成する必要があります。その場合は、**crypto key generate rsa general-keys exportable label label-name** コマンドを使用します。

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 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

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。

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

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、シスコソフトウェアの SSH サーバではデフォルトでサポートされていません。

SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンドで終了します。クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システム クロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

Secure Copy Protocol 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 にはセキュア シェル (SSH) が必要です (Berkeley の 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 許可が必要なため、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。

Secure Copy Protocol

Secure Copy Protocol (SCP) 機能は、デバイスの設定やスイッチ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 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 では認証、許可、およびアカウンティング

(AAA) の許可が必要なため、デバイスはユーザが正しい権限レベルを保有しているかどうかを特定できます。セキュア コピー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。

Secure Copy の動作方法

Secure Copy (SCP) は一連の Berkeley の r-tools (Berkeley 大学独自のネットワーキングアプリケーションセット) に基づいて設計されているため、その動作内容は Remote Copy Protocol (RCP) と類似しています。ただし、SCP はセキュアシェル (SSH) のセキュリティに対応している点は除きます。加えて、SCP では、ユーザが正しい権限レベルを持っていることをデバイス上で判断できるように、認証、許可、およびアカウントिंग (AAA) の許可を設定する必要があります。

SCP を使用すると、**copy** コマンドを使用して Cisco IOS ファイルシステム (IFS) 内の任意のファイルのコピーをデバイスとの間で実行できるのは、特権レベルが 15 のユーザのみになります。許可された管理者はワークステーションからこの操作を実行することもできます。



(注) シスコソフトウェアと一緒に pscp.exe ファイルを使用している場合は、SCP オプションを有効にします。

リバース Telnet

リバース Telnet を使用すると、特定のポート範囲に Telnet を実行したり、端末または補助回線に接続することができます。リバース Telnet は、他のシスコ デバイスのコンソールへの端末回線を複数内蔵したシスコ デバイスとの接続によく使用されていました。Telnet を使用すると、特定の回線上のターミナル サーバに Telnet することによって、どの場所からでも簡単にデバイス コンソールに到達できます。この Telnet アプローチは、デバイスへのすべてのネットワーク接続が切断されている場合でも、そのデバイスの設定に使用できます。また、リバース Telnet は、シスコ デバイスに接続されたモデムをダイヤルアウトに使用することもできます (通常は、ロータリー デバイスと一緒に使用します)。

リバース SSH

リバース Telnet は SSH を使用して実現できます。リバース Telnet と違って、SSH はセキュアな接続を提供します。リバース SSH 拡張機能は、SSH の設定を容易にします。この機能を使用すれば、SSH を有効にする端末または補助回線ごとに別々の回線を設定する必要がなくなります。以前のリバース SSH 設定方法では、アクセスできるポートの数が 100 に制限されていました。リバース SSH 拡張機能では、ポートの数に制限がありません。

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。 <ul style="list-style-type: none"> 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。 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、 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 : Device(config)# end	特権 EXEC モードに戻ります。

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 : 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 version [1 2] 例 : Device(config)# ip ssh version 1	(任意) SSH バージョン 1 または SSH バージョン 2 を実行するようにデバイスを設定します。 • 1 : SSH バージョン 1 を実行するようにデバイスを設定します。 • 2 : SSH バージョン 2 を実行するようにデバイスを設定します。 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

	コマンドまたはアクション	目的
		<p>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。</p>
ステップ 4	<p>ip ssh {timeout seconds authentication-retries number}</p> <p>例 :</p> <pre>Device(config)# ip ssh timeout 90 authentication-retries 2</pre>	<p>SSH 制御パラメータを設定します。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p> <ul style="list-style-type: none"> • 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。 <p>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。</p>
ステップ 5	<p>次のいずれかまたは両方を使用します。</p> <ul style="list-style-type: none"> • line vty line_number [ending_line_number] • transport input ssh <p>例 :</p> <pre>Device(config)# line vty 1 10</pre> <p>または</p>	<p>(任意) 仮想端末回線設定を設定します。</p> <ul style="list-style-type: none"> • 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 には、回線のペアを指定します。指定できる範囲は 0 ~ 15 です。 • 非 SSH Telnet によるデバイスへの接続を許可しない設定です。これに

	コマンドまたはアクション	目的
	Device(config-line)# transport input ssh	より、ルータは SSH 接続に限定されます。
ステップ 6	end 例： Device(config-line)# end	特権 EXEC モードに戻ります。

トラブルシューティングのヒント

- セキュア シェル (SSH) コンフィギュレーション コマンドが不正なコマンドとして拒否された場合は、デバイスの Rivest, Shamir, Adleman (RSA) キー ペアが適切に生成されていません。ホスト名およびドメインを指定していることを確認します。次に、**crypto key generate rsa** コマンドを使用して RSA キーペアを生成し、SSH サーバを有効にします。
- RSA キー ペアを設定すると、次のエラー メッセージが表示されることがあります。
 - No hostname specified
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、デバイスのホスト名を設定する必要があります。
 - No domain specified
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、デバイスのホストドメインを設定する必要があります。
- 使用できる SSH 接続数は、デバイスに設定されている vty の最大数までに制限されます。各 SSH 接続は vty リソースを使用します。
- SSH では、デバイスで AAA によって設定されるローカルセキュリティまたはセキュリティ プロトコルが、ユーザ認証に使用されます。認証、許可、およびアカウントिंग (AAA) を設定する場合、コンソールで AAA のユーザ認証を無効にする必要があります。デフォルトでコンソールの AAA 認可はディセーブルです。コンソールで AAA 許可が有効になっている場合は、AAA の設定段階で **no aaa authorization console** コマンドを設定して無効にします。

コンソール アクセス用のリバーズ SSH の設定

SSH サーバ上でリバーズ SSH コンソール アクセスを設定するには、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。
ステップ 3	line line-number ending-line-number 例： Device# line 1 3	設定用の回線を特定して、ライン コンフィギュレーションモードに入ります。
ステップ 4	no exec 例： Device(config-line)# no exec	回線上の EXEC 処理を無効にします。
ステップ 5	login authentication listname 例： Device(config-line)# login authentication default	回線のログイン認証メカニズムを定義します。 (注) 認証方式はユーザ名とパスワードを使用する必要があります。
ステップ 6	transport input ssh 例： Device(config-line)# transport input ssh	デバイスの特定の回線への接続に使用されるプロトコルを定義します。 • リバース SSH 拡張機能の場合は、 ssh キーワードを使用する必要があります。
ステップ 7	exit 例： Device(config-line)# exit	ライン コンフィギュレーション モードを終了します。
ステップ 8	exit 例： Device(config)# exit	グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	ssh -l userid : {number} {ip-address} 例 : <pre>Device# ssh -l lab:1 router.example.com</pre>	SSHサーバを実行しているリモートネットワークワーキング デバイスにログインするときに使用されるユーザ ID を指定します。 <ul style="list-style-type: none"> • userid : ユーザ ID。 • : : ポート番号と端末 IP アドレスが userid 引数に続くことを示します。 • number : 端末番号または補助回線番号。 • ip-address : ターミナルサーバの IP アドレス。 (注) リバース SSH の代替手段をモデム アクセス用に設定する場合は、 userid 引数、 :rotary {number} {ip-address} デリミタ、および引数が必須です。

モデム アクセス用のリバース SSH の設定

この設定では、リバース SSH がダイヤルアウト回線に使用されるモデム上で設定されます。ダイヤルアウトモデムのいずれかに到達するには、任意の SSH クライアントを使用して SSH セッションを開始し、ロータリーデバイスから次に使用可能なモデムに到達します。

手順

	コマンドまたはアクション	目的
ステップ 1	enable 例 : <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • 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 : <pre>Device# configure terminal</pre>	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	line <i>line-number</i> <i>ending-line-number</i> 例 : Device# line 1 200	設定用の回線を特定して、ラインコンフィギュレーションモードに入ります。
ステップ 4	no exec 例 : Device(config-line)# no exec	回線上の EXEC 処理を無効にします。
ステップ 5	login authentication <i>listname</i> 例 : Device(config-line)# login authentication default	回線のログイン認証メカニズムを定義します。 (注) 認証方式はユーザ名とパスワードを使用する必要があります。
ステップ 6	rotary <i>group</i> 例 : Device(config-line)# rotary 1	1つ以上の仮想端末回線または1つの補助ポート回線からなる回線グループを定義します。
ステップ 7	transport input ssh 例 : Device(config-line)# transport input ssh	デバイスの特定の回線への接続に使用されるプロトコルを定義します。 • リバーズ SSH 拡張機能の場合は、 ssh キーワードを使用する必要があります。
ステップ 8	exit 例 : Device(config-line)# exit	ラインコンフィギュレーションモードを終了します。
ステップ 9	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ます。
ステップ 10	ssh -l <i>userid</i> :rotary { <i>number</i> } { <i>ip-address</i> } 例 : Device# ssh -l lab:rotary1 router.example.com	SSH サーバを実行しているリモート ネットワーキングデバイスにログインするときに使用されるユーザ ID を指定します。 • <i>userid</i> : ユーザ ID。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • <code>:</code> : ポート番号と端末 IP アドレスが <code>userid</code> 引数に続くことを示します。 • <code>number</code> : 端末番号または補助回線番号。 • <code>ip-address</code> : ターミナルサーバの IP アドレス。 <p>(注) リバース SSH の代替手段をモデム アクセス用に設定する場合は、<code>userid</code> 引数、<code>:rotary {number} {ip-address}</code> デリミタ、および引数が必須です。</p>

クライアント上でのリバース SSH のトラブルシューティング

クライアント（リモート デバイス）上でリバース SSH 設定の問題を解決するには、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 : <pre>Device> enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	debug ip ssh client 例 : <pre>Device# debug ip ssh client</pre>	SSH クライアントに関するデバッグメッセージを表示します。

サーバ上でのリバース SSH のトラブルシューティング

ターミナル サーバ上でリバース SSH 設定の問題を解決するには、次の手順を実行します。各ステップは、互いに独立しているため、任意の順序で設定できます。

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	debug ip ssh 例： Device# debug ip ssh	SSH サーバに関するデバッグメッセージを表示します。
ステップ 3	show ssh 例： Device# show ssh	SSH サーバ接続のステータスを表示します。
ステップ 4	show line 例： Device# show line	端末回線のパラメータを表示します。

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。

セキュアコピーの設定

シスコ デバイスに Secure Copy (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。
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	aaa authorization {network exec commands level reverse-access configuration} {default list-name} [method1 [method2...]] 例： Device(config)# aaa authorization exec default group tacacs+	ネットワークへのユーザアクセスを制限するパラメータを設定します。 (注) exec キーワードは、許可を実行して、ユーザが EXEC シェルの実行を許可されているかどうかを判断します。したがって、SCP を設定するときに exec キーワードを使用する必要があります。
ステップ 6	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 7	ip scp server enable 例：	SCP サーバ側機能を有効にします。

	コマンドまたはアクション	目的
	Device(config)# ip scp server enable	
ステップ 8	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 9	debug ip scp 例： Device# debug ip scp	(任意) SCP 認証問題を解決します。

セキュア シェルの設定例

例：ローカル認証を使用したセキュア コピーの設定

次の例は、Secure Copy (SCP) のサーバ側機能の設定方法を示しています。この例では、ローカルに定義されたユーザ名とパスワードを使用します。

```
! AAA authentication and authorization must be configured properly in order for SCP to work.
aaa new-model
aaa authentication login default local
aaa authorization exec default local
username user1 privilege 15 password 0 lab
! SSH must be configured and functioning properly.
ip scp server enable
```

例：ネットワークベース認証を使用した SCP サーバ側の設定

次の例は、ネットワークベースの認証メカニズムを使用した SCP のサーバ側機能の設定方法を示しています。

```
! AAA authentication and authorization must be configured properly for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
! SSH must be configured and functioning properly.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```


リバース SSH コンソール アクセスの例

ターミナル サーバの設定

次の設定例は、リバース SSH が端末回線 1 ～ 3 のコンソール アクセス用に設定されていることを示しています。

```
line 1 3
  no exec
  login authentication default
  transport input ssh
```

クライアント設定

SSH クライアント上で設定された次のコマンドは、それぞれ、回線 1、2、および 3 とのリバース SSH セッションを形成します。

```
ssh -l lab:1 router.example.com
ssh -l lab:2 router.example.com
ssh -l lab:3 router.example.com
```

リバース SSH モデム アクセスの例

次の設定例では、ダイヤルアウト回線の 1 ～ 200 がモデム アクセス用のロータリー グループ 1 にグループ分けされています。

```
line 1 200
  no exec
  login authentication default
  rotary 1
  transport input ssh
  exit
```

次のコマンドは、リバース SSH がロータリー グループの最初の空き回線に接続されることを表示します。

```
ssh -l lab:rotary1 router.example.com
```

例 : SSH の設定およびステータスのモニタリング

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
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst Micro Switches)</i>

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <p>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。</p>	http://www.cisco.com/support

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 Release 15.2(7)E3k	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> [英語] からアクセスします。

