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。

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。
- 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。
- デバイスは、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。

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ています。

（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、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。

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 コマンダで終了します。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。

スイッチ スタック内のスタック マスターで、SSL セッションが強制終了されます。

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 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

セキュア コピー プロトコルは、このマニュアルで使用できるほど SSH に深く関連しているでしょうか。私はこのトピックにあるすべての項目を前提条件または制約事項に移動しました。

セキュア コピー プロトコル（SCP）機能は、device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）の設定が必要なため、device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。

セキュア コピーの動作方法

セキュア コピー（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、認可、アカウンティング（AAA）認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） Cisco 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セットアップ

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： `デバイス> 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： `デバイス# 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： `デバイス(config)# hostname your_hostname`	デバイスのホスト名および IP ドメイン名を設定します。 （注） この手順を実行するのは、デバイスを 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：	デバイスのホスト ドメインを設定します。

	コマンドまたはアクション	目的
	デバイス(config)# **ip domain-name your_domain**	
ステップ 5	**crypto key generate rsa** 例： デバイス(config)# **crypto key generate rsa**	デバイス上でローカルおよびリモート認証用に SSH サーバを有効にし、RSA キー ペアを生成します。デバイスの RSA キー ペアを生成すると、SSH が自動的に有効になります。 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。 （注） この手順を実行するのは、デバイスを SSH サーバとして設定する場合だけです。
ステップ 6	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： デバイス# **show running-config**	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： デバイス# **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、この手順が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **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： デバイス# **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： デバイス(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： デバイス(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、デバイスは CLI

	コマンドまたはアクション	目的
		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：
	`デバイス(config)# line vty 1 10`
	または
	`デバイス(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* 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。
		• デバイスが非 SSH Telnet 接続を阻止するように指定します。これにより、ルータは SSH 接続に限定されます。

ステップ 6	**end** **例**： `デバイス(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** **例**： `デバイス# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： デバイス# **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 クライアントの呼び出し

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。

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、認可、アカウンティング（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ス SSH の設定

SSH サーバ上でリバース 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、回線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**：	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。

	コマンドまたはアクション	目的
	`Device(config-line)# transport input ssh`	• 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。
ステップ 9	**ssh -l** *userid* **:** {*number*} {*ip-address*} 例： `Device# ssh -l lab:1 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。 • *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、下のステップ 10 に示すように、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： `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 1 200`	設定用の回線を特定して、回線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	**rotary** *group* 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 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。

	コマンドまたはアクション	目的
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** *userid* **:rotary** {*number*} {*ip-address*} 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。 • *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。

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： `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 client** 例：	SSH クライアントに関するデバッギング メッセージを表示します。

	コマンドまたはアクション	目的
	`Device# debug ip ssh client`	

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ギング 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。
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、認可を実行して、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*	ユーザ名をベースとした認証システムを構築します。

	コマンドまたはアクション	目的
	例： `Device(config)# username superuser privilege 2 password 0 superpassword`	（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： `Device(config)# ip scp server enable`	SCP サーバ側機能を有効にします。
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、特権 EXEC モードに戻ります。
ステップ 9	**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 10	**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、セキュア コピー（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

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。

ターミナル サーバの設定

```
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
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』

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/support

セキュア シェルの設定に関する機能情報

リリース	機能情報
Cisco IOS リリース 15.0(2)EX	この機能が導入されました。
Cisco IOS リリース 15.2(5)E	（注） Cisco IOS リリース 15.2(5)E 以降では、セキュア シェル バージョン 1（SSHv1）が廃止されます。
Cisco IOS 15.2(1)E	セキュア シェル（SSH）のバージョン 1 と 2 に対してサポートされているリバース SSH 拡張機能は、SSH を有効にしなければならない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いようにリバース SSH を設定する代替手段を提供します。この機能は、ロータリー グループの制限も排除します。 この機能は、CAT4500-X、CAT4500E-SUP6E、CAT4500E-SUP6L-E、CAT4500E-SUP7E、CAT4500E-SUP7L-E でサポートされていました。 **ssh** コマンドが導入されました。