# セキュア シェルの設定

Secure Shell（SSH; セキュア シェル）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。ここでは、SSH バージョン 1 について説明します。SSH バージョン 2 については、「Secure Shell Version 2 Support」フィーチャ モジュールを参照してください。

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

## 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。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「セキュア シェルの設定に関する機能情報」（P.14）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、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。

## この章の構成

# SSH の設定に関する前提条件

SSH の設定前に、次のタスクを実行します。

- ルータに必要なイメージをダウンロードします SSH サーバには、Cisco IOS Release 12.1(1)T 以降のリリースの IPsec（Data Encryption Standard（DES）または 3DES）暗号化ソフトウェア イメージが必要です。SSH クライアントには、Cisco IOS Release 12.1(3)T 以降のリースの IPsec（DES または 3DES）暗号化ソフトウェア イメージが必要です。ソフトウェア イメージのダウンロードの詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』を参照してください。
- グローバル コンフィギュレーション モードで **hostname** コマンドと **ip domain-name** コマンドを使用して、ルータのホスト名とホスト ドメインを設定します。
- ルータの 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イネーブルになります。

  **（注）** RSA キー 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。

- ローカルまたはリモート アクセスのためにユーザ認証を設定します。Authentication, Authorization, and Accounting（AAA; 認証、認可、およびアカウンティング）の有無に関係なく、認証を設定できます。詳細については、「Configuring Authentication」、「Configuring Authorization」、および「Configuring Accounting」の各フィーチャ モジュールを参照してください。

# SSH の設定に関する制約事項

SSH には、次の制約事項があります。

- SSH サーバと SSH クライアントは、DES（56-bit）および 3DES（168-bit）データ暗号化ソフトウェア イメージでだけサポートされます。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。

# セキュア シェルの概要

ここでは、SSH の概要について説明します。



（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

## SSH サーバ

SSH サーバの機能によって、SSH クライアントは Cisco ルータに対してセキュアで暗号化された接続を実行できます。この接続には、インバウンド Telnet 接続の機能と似ています。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 IOS ソフトウェア認証と併用することで、強力な暗号化が可能になりました。Cisco IOS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと連携できます。

## SSH 統合クライアント

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提供するアプリケーションです。SSH クライアントによって、Cisco ルータは他の Cisco ルータ、または SSH サーバを実行する他のデバイスに対して、セキュアで暗号化された接続を実行できます。この接続には、接続が暗号化されている点を除き、アウトバウンド Telnet 接続と似た機能があります。SSH クライアントは、認証および暗号化により、非セキュアなネットワーク上でセキュアな通信ができます。

Cisco IOS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。SSH クライアントは、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、ルータに対する Telnet セッションの認証と同様に実行されます。SSH でサポートされるユーザ認証メカニズムには、RADIUS、TACACS+、およびローカルに保存されたユーザ名とパスワードがあります。

（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

SSH クライアントで使用できる RSA 認証は、Cisco IOS 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 認証のサポートを設定する手順については、「Secure Shell Version 2 Support」の章の「Configuring a Router for SSH Version 2 Using Private Public Key Pairs」の項を参照してください。

# SSH の設定方法

次のタスクを実行して、SSH を設定します。

- 「SSH サーバの設定」（P.4）（必須）
- 「SSH クライアントの呼び出し」（P.5）（任意）

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

# 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。このタスクによって、Cisco ルータで SSH をイネーブルにできます。

（注） SSH クライアント機能はユーザ EXEC モードで実行され、ルータの設定は特にありません。

（注） SSH コマンドは任意であり、SSH サーバをディセーブルにするとディセーブルになります。SSH パラメータを設定しない場合、デフォルト値が使用されます。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh** {**timeout** *seconds* | **authentication-retries** *integer*}

**手順の詳細**

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **ステップ 1** | **enable**<br><br>**例：**<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• プロンプトが表示されたら、パスワードを入力します。 |
| **ステップ 2** | **configure terminal**<br><br>**例：**<br>`Router# 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** {**timeout** *seconds* \| **authentication-retries** *integer*}<br><br>**例：**<br>`Router(config) # ip ssh timeout 30` | ルータで SSH コントロール パラメータを設定します。<br>• SSH コントロール変数の 1 つを選択します。<br>• *seconds* 引数に、120 秒以下のタイムアウト値を指定します。デフォルトは 120 です。この設定は、SSH のネゴシエーション フェーズに適用されます。EXEC セッションが開始されると、vty に設定された標準のタイムアウトが適用されます。<br>• デフォルトで、5 個の vty（0 ～ 4）が定義されているため、5 個のターミナル セッションが可能です。SSH がシェルを実行した後、vty タイムアウトが開始されます。vty タイムアウトのデフォルト値は 10 分です。 |
| | | • integer 引数で、5 回以下の認証の再試行回数を指定します。デフォルト値は 3 です。<br>**（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。<br>– **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。<br>– **ip ssh authentication-retries** *integer* コマンドを使用してルータに設定されている値に 1 を足した値。 |

# SSH クライアントの呼び出し

このタスクを実行して、SSH クライアントを呼び出します。

**手順の概要**

1. **enable**
2. **ssh -l** *username* **-vrf** *vrf-name ip-address*

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br><br>**例：**<br>`Router> enable` | （任意）特権 EXEC モードをイネーブルにします。<br>• プロンプトが表示されたら、パスワードを入力します。 |
| ステップ 2 | **ssh -l** *username* **-vrf** *vrf-name ip-address*<br><br>**例：**<br>`Router# ssh -l user1 -vrf vrf1 192.0.2.1` | （任意）Cisco IOS SSH クライアントを呼び出し、指定した Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）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

- SSH コンフィギュレーション コマンドが正規のコマンドとして拒否される場合、ルータの RSA キー ペアを適切に生成していません。ホスト名とドメインを指定してください。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 サーバをイネーブルにします。
- 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、ルータのホスト名を設定する必要があります。詳細については、「IPsec and Quality of Service」フィーチャ モジュールを参照してください。
  - 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、ルータのホスト ドメインを設定する必要があります。詳細については、「IPsec and Quality of Service」フィーチャ モジュールを参照してください。
- 使用できる SSH 接続数は、ルータに設定されている vty の最大数に制限されます。各 SSH 接続は vty リソースを使用します。
- SSH は、ユーザ認証のためにルータ上で AAA を介して設定されたローカル セキュリティまたはセキュリティ プロトコルを使用します。AAA を設定する場合、ユーザ認証のためにコンソールで AAA をディセーブル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 認可がイネーブルの場合、AAA コンフィギュレーション段階で **no aaa authorization console** コマンドを設定してディセーブルにします。

# SSH の設定例

ここでは、Cisco 7200、Cisco 7500、および Cisco 12000 ルータでの **show running-config** EXEC コマンドの出力である次の設定例を紹介します。


- 「Cisco 7200 シリーズ ルータ上の SSH：例」（P.7）
- 「Cisco 7500 シリーズ ルータ上の SSH：例」（P.8）
- 「Cisco 12000 シリーズ ルータ上の SSH：例」（P.10）
- 「SSH の確認：例」（P.11）

（注） 以降、特に明記していないかぎり、「SSH」という用語は「SSH バージョン 1」だけを示します。

（注） **crypto key generate rsa** コマンドは、**show running-config** の出力に表示されません。

# Cisco 7200 シリーズ ルータ上の SSH：例

次の例では、60 秒以下のタイムアウト、および 2 回以下の認証再試行回数を指定した SSH が Cisco 7200 に設定されています。SSH サーバ機能をルータに設定する前に、TACACS+ は認証の方式として指定されます。

```
hostname Router72K
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password password

username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter the ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 2

controller E1 2/0

controller E1 2/1

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no keepalive
no cdp enable

interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

no ip classless
ip route 192.168.1.0 255.255.255.0 10.1.10.1
ip route 192.168.9.0 255.255.255.0 10.1.1.1
```

```
ip route 192.168.10.0 255.255.255.0 10.1.1.1

map-list atm
ip 10.1.10.1 atm-vc 7 broadcast
no cdp run

tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7200kw
transport input none
line aux 0
line vty 0 4
password password

end
```

# Cisco 7500 シリーズ ルータ上の SSH：例

次の例では、60 秒以下のタイムアウト、および 5 回以下の認証再試行回数を指定した SSH が Cisco 7500 に設定されています。SSH サーバ機能をルータに設定する前に、RADIUS は認証の方式として指定されます。

```
hostname Router75K
aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password password

username username1 password 0 password1
username username2 password 0 password2
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 5

controller E1 3/0
channel-group 0 timeslots 1

controller E1 3/1
channel-group 0 timeslots 1
channel-group 1 timeslots 2

interface Ethernet0/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/1
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown
```

```
interface Ethernet0/0/2
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/3
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/1
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/3
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/4
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/5
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Serial2/0
ip address 10.1.1.2 255.0.0.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache

ip classless
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1

tacacs-server host 192.168.109.216 port 9000
```

```
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7500kw
transport input none
line aux 0
transport input all
line vty 0 4

end
```

# Cisco 12000 シリーズ ルータ上の SSH：例

次の例では、60 秒以下のタイムアウト、および 2 回以下の認証再試行回数を指定した SSH が Cisco 12000 に設定されています。SSH サーバ機能をルータに設定する前に、TACACS+ は認証の方式として指定されます。

```
hostname Router12K
aaa new-model
aaa authentication login default tacacs+ local
aaa authentication login aaa12000kw local
enable password password

username username1 password 0 password1
username username2 password 0 password2
redundancy
main-cpu
    auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh timeout 60
ip ssh authentication-retries 2

interface ATM0/0
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown

interface POS1/0
ip address 10.100.100.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
no keepalive
crc 16
no cdp enable

interface POS1/1
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/2
```

```
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/3
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS2/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
crc 16

interface Ethernet0
ip address 172.17.110.91 255.255.255.224
no ip directed-broadcast

router ospf 1
network 0.0.0.0 255.255.255.255 area 0.0.0.0

ip classless
ip route 0.0.0.0 0.0.0.0 172.17.110.65

logging trap debugging
tacacs-server host 172.17.116.138
tacacs-server key cisco

radius-server host 172.17.116.138 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa12000kw
transport input none
line aux 0
line vty 0 4

no scheduler max-task-time
no exception linecard slot 0 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end
```

# SSH の確認：例

SSH サーバがイネーブル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。

```
Router# 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。

```
Router# 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 をイネーブルにしたときのルータ上の SSH サーバ接続の例を示します。

```
Router# show ssh

Connection      Version     EncryptionStateUsername
    0   1.5 3DESSession Startedguest
```

次に、SSH がディセーブルの例を示します。

```
Router# show ssh

%No SSH server connections running.
```

# 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。

## 関連資料

| 内容 | 参照先 |
|---|---|
| Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング） | • 「*Configuring Accounting*」フィーチャ モジュール<br>• 「*Configuring Authentication*」フィーチャ モジュール<br>• 「*Configuring Authorization*」フィーチャ モジュール |
| IPsec | 「*IPsec and Quality of Service*」フィーチャ モジュール |
| SSH バージョン 2 | 「*Secure Shell Version 2 Support*」フィーチャ モジュール |
| ソフトウェア イメージのダウンロード | 『*Cisco IOS Configuration Fundamentals Configuration Guide*』 |

## 規格

| 規格 | タイトル |
|---|---|
| この機能がサポートする新しい規格または変更された規格はありません。また、この機能による既存規格のサポートに変更はありません。 | — |

# MIB

| MIB | MIB リンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。 | 選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。<br>http://www.cisco.com/go/mibs |

# RFC

| RFC | タイトル |
|---|---|
| この機能によってサポートされる新しい RFC や変更された RFC はありません。 | — |

# シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| 右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。<br>以下を含むさまざまな作業にこの Web サイトが役立ちます。<br>・テクニカル サポートを受ける<br>・ソフトウェアをダウンロードする<br>・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける<br>・ツールおよびリソースへアクセスする<br>- Product Alert の受信登録<br>- Field Notice の受信登録<br>- Bug Toolkit を使用した既知の問題の検索<br>・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する<br>・トレーニング リソースへアクセスする<br>・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する<br>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。 | http://www.cisco.com/cisco/web/support/index.html |

# セキュア シェルの設定に関する機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

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 を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。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。

**（注）** 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

**表 1　セキュア シェルの設定に関する機能情報**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| セキュア シェル | 12.0(5)S | Secure Shell（SSH; セキュア シェル）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。ここでは、SSH バージョン 1 について説明します。 |