SSH Terminal-Line アクセス

SSH Terminal-Line アクセス機能で、tty（text telephone）回線へのセキュアなアクセスを実現します。tty で、聞き取りおよび発話不良でも、電話を使用してメッセージを入力することで、通信できます。

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、「SSH Terminal-Line アクセスの機能情報」（P.9）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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

SSH Terminal-Line アクセスの前提条件

必要なイメージをルータにダウンロードします。Cisco IOS Release 12.1(1)T 以降のリリースから、Secure Shell（SSH; セキュア シェル）サーバはルータに IPSec（Data Encryption Standard（DES; データ暗号規格）または 3DES）暗号化ソフトウェア イメージを必要とします。Cisco IOS Release 12.1(3)T 以降のリリースから、SSH クライアントはルータに IPSec（DES または 3DES）暗号化ソフトウェア イメージを必要とします。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*, Release 12.4T』を参照してください。

SSH サーバは、ローカルのユーザ名およびパスワード、TACACS+ または RADIUS を使用して定義されるユーザ名およびパスワードの使用を必要とします。

（注） SSH Terminal-Line アクセス機能は、SSH が含まれるすべてのイメージで使用できます。

SSH Terminal-Line アクセスの制約事項

コンソール サーバ要件

セキュリティ保護されているサーバ アクセスを設定するには、そのロータリーの各回線を定義し、ユーザがそれらのデバイスにそれぞれアクセスする際にネットワークを介して SSH を使用するよう SSH を設定する必要があります。

メモリおよびパフォーマンスに対する影響

SSH を使用した反転 Telnet を置換すると、vty 処理での暗号化と暗号化プロセスの追加により、使用できる tty 回線のパフォーマンスが低下します（どの暗号化メカニズムも、通常のアクセスよりもメモリを多く使用します）。

SSH Terminal-Line アクセスに関する情報

SSH Terminal-Line アクセス 機能を設定するには、次の概念を理解しておく必要があります。

- 「SSH Terminal-Line アクセスの概要」（P.2）

SSH Terminal-Line アクセスの概要

Cisco IOS は、ユーザがルータ（特定のポート範囲経由）を介して tty（非同期）回線に接続するために Telnet を使用できる反転 Telnet をサポートしています。反転 Telnet で、ユーザは従来 Telnet ではサポートされていない、リモート デバイスのコンソール ポートへの接続を行えます。ただし、この方式は、Telnet トラフィックがすべて、ネットワーク上を暗号化されずに通過するため、ほとんどセキュリティ保護されていません。SSH Terminal-Line アクセス機能で、反転 Telnet を SSH に置き換えます。この機能は、tty 回線のデバイスにアクセスする際に暗号化を使用するよう設定でき、ユーザに強固なプライバシーとセッションの一体性をサポートする接続を提供します。

SSH は rsh、rlogin、rcp などの Berkeley r-tools スイートに安全に置換するアプリケーションおよびプロトコルです（Cisco IOS は rlogin をサポートします）。この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。現在、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。Cisco IOS ソフトウェアに実装されているのは SSH バージョン 1 のみです。

SSH Terminal-Line アクセス機能で、ユーザがルータを安全にアクセスし、次のタスクを実行するよう設定できます。

- 他のルータ、スイッチ、またはデバイスのコンソールまたはシリアル ポートに接続された複数の端末回線があるルータへの接続。
- 特定の回線上のターミナル サーバに安全に接続することで、任意の場所からのルータへの接続を簡素化。
- ダイヤルアウトを安全に行うために使用されるルータにモデムを取り付け可能。
- ローカルで定義したユーザ名とパスワード、TACACS+、RADIUS を使用して各回線の認証を要求。

（注） モジュールでのセッションを開始するために使用する **session slot** コマンドは、仮想 tty（vty）回線で受け入れられるためには Telnet が必要です。SSH に対してのみ vty 回線を制限する場合、モジュールとの通信にコマンドを使用できません。これは、ユーザがデバイスのモジュールに Telnet できるすべての Cisco IOS デバイスに適用されます。

SSH Terminal-Line アクセスの設定方法

ここでは、次の作業について説明します。

- 「SSH Terminal-Line アクセスの設定」（P.3）

SSH Terminal-Line アクセスの設定

次のタスクを実行して、Cisco ルータで安全なリバース Telnet をサポートするよう設定します。

（注） SSH がすでにルータで設定されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login** {**local** | **authentication** *listname*}
6. **rotary** *group*
7. **transport input** {**all** | **ssh**}
8. **exit**
9. **ip ssh port** *portnum* **rotary** *group*

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** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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** **例：** `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	**line** *line-number* [*ending-line-number*] **例：** `Router(config)# 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。 **（注）** ルータ コンソール コンフィギュレーションでは、各回線を独自のロータリーで定義し、SSH を各ロータリー上で待ち受けるよう設定する必要があります。 **（注）** ユーザ名とパスワードが必要な認証方式を、各回線で設定する必要があります。これは、ルータに保存されたローカルのユーザ名とパスワードや、TACACS+、RADIUS を使用することで行えます。回線パスワードとイネーブル パスワードは両方とも、SSH で使用するには不十分です。
ステップ 4	**no exec** **例：** `Router(config-line)# no exec`	各回線での exec 処理をディセーブルにします。
ステップ 5	**login** {**local** | **authentication** *listname*} **例：** `Router(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）** 認証方式で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：** `Router(config-line)# rotary 1`	1 つ以上で構成される回線グループを定義します。 **（注）** 使用するロータリーをすべて定義し、定義した各ロータリーは SSH がイネーブルの場合に使用される必要があります。
ステップ 7	**transport input** {**all** | **ssh**} **例：** `Router(config-line)# transport input ssh`	ルータ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
ステップ 8	**exit** **例：** `Router(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	**ip ssh port** *portnum* **rotary** *group* **例：** `Router(config)# ip ssh port 2000 rotary 1`	tty 回線へのセキュア ネットワーク アクセスをイネーブルにします。 • このコマンドを使用して、ロータリー *group* 引数とともに *portnum* 引数に接続します。引数は、回線または回線グループと関連付けられています。 **（注）** *group* 引数は、ステップ 6 で選択した **rotary** *group* 番号と対応している必要があります。

SSH Terminal-Line アクセスの確認

この機能が動作しているか確認するため、SSH クライアントを使用してルータに接続します。

SSH Terminal-Line アクセスの設定例

ここでは、次の設定例について説明します。

- 「SSH Terminal-Line アクセスの設定例」（P.5）
- 「コンソール（シリアル回線）ポートの SSH Terminal-Line アクセスの設定例」（P.6）

SSH Terminal-Line アクセスの設定例

次は、SSH Terminal-Line アクセス機能を、1 ～ 200 の回線でダイヤルアウトで使用するモデムに設定する方法の例です。任意のダイヤルアウト モデムを取得するには 任意の SSH クライアントを使用し、ルータのポート 2000 で SSH セッションを開始して、次に使用可能なモデムをロータリーから取得します。

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh
 exit
ip ssh port 2000 rotary 1
```

コンソール（シリアル回線）ポートの SSH Terminal-Line アクセスの設定例

次は、SSH Terminal-Line アクセス機能を、さまざまなデバイスのコンソールまたはシリアル回線インターフェイスにアクセスするよう設定する例です。このタイプのアクセスでは、各回線は独自のロータリーに設定され、各ロータリーは 1 つのポートで使用されます。この例では、回線 1 ～ 3 が使用されています。設定のポート（回線）マッピングを表 1 に示しています。

表 1　　ポート（回線）設定マッピング

回線番号	SSH ポート番号
1	2001
2	2002
3	2003

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh

ip ssh port 2001 rotary 1 3
```

その他の参考資料

次の項で、SSH Terminal-Line アクセス機能に関連した関連資料を示します。

関連資料

内容	参照先
SSH	『*Cisco IOS Security Configuration Guide: Securing User Services*』
SSH コマンド	『*Cisco IOS Security Command Reference*』
ダイヤル テクノロジー	『*Cisco IOS Dial Technologies Configuration Guide*』
ダイヤル コマンド	『*Cisco IOS Dial Technologies Command Reference*』
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
	—

MIB

MIB	MIB リンク
	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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
なし	—

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。 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。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・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 ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・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 ・トレーニング リソースへアクセスする ・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 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/techsupport

SSH Terminal-Line アクセスの機能情報

表 2 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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 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 2　SSH Terminal-Line アクセスの機能情報

機能名	リリース	機能情報
SSH Terminal-Line アクセス	12.2(4)JA 12.2(15)T 12.2(6th)S	SSH Terminal-Line アクセス機能で、tty（text telephone）回線へのセキュアなアクセスを実現します。tty で、聞き取りおよび発話不良でも、電話を使用してメッセージを入力することで、通信できます。 この機能は、Cisco IOS Release 12.2(4)JA で導入されました。 この機能は、Cisco IOS Release 12.2(15)T に統合されました。 この機能は、Cisco IOS Release 12.2(6th)S に統合されました。 次のコマンドが、導入または変更されました。**ip ssh port**。