# Cisco ルータでの Telnet、コンソールおよび AUX ポートのパスワード設定例

## 目次



## はじめに

このドキュメントでは、ルータへの着信 EXEC 接続に対してパスワード保護を設定する設定例について説明しています。

## 前提条件

### 要件

このドキュメントに記載されている作業を実行するには、ルータの Command Line Interface ( CLI; コマンドライン インターフェイス ) へ特権 EXEC アクセスできる必要があります。 コマンド ラインの使用方法の詳細と、コマンド モードについては、『Cisco IOS ソフトウェアの使用方法』を参照してください。

ルータへのコンソールの接続手順については、ルータに同梱されている説明書、またはご使用の機器のオンライン ドキュメントを参照してください。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 2509 ルータ
- Cisco IOS(R) Software バージョン 12.2(19)

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

## 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

# 背景説明

ご使用になっているルータの Command Line Interface（CLI; コマンドライン インターフェイス）へのアクセスの制御や制限を行うためのパスワード保護の使用は、セキュリティ プラン全体に関わる基本的要素です。

認証されていないリモート アクセス（通常は Telnet）からのルータの保護は、必ず設定しなければならない最も一般的なセキュリティですが、認証されていないローカル アクセスからのルータの保護も見逃さないでください。

**注:** パスワード保護は、効率的かつ周到にネットワーク セキュリティを管理する際に使用する数多い手段の中の 1 つに過ぎません。 セキュリティ プランを実装する場合に検討する必要があるその他の要素には、ファイアウォール、アクセス リスト、機器への物理的アクセスがあります。

ルータへのコマンドライン アクセスまたは EXEC アクセスはさまざまな方法で実行可能ですが、いずれの場合でも、ルータへの着信接続は TTY 回線で実行されます。 次の **show line** 出力例で示すように、TTY 回線の主要タイプは 4 種類あります。

```
2509#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY               -    -      -    -    -      0       0     0/0       -
     1 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     2 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     3 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     4 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     5 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     6 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     7 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     8 TTY   9600/9600   -    -      -    -    -      0       0     0/0       -
     9 AUX   9600/9600   -    -      -    -    -      0       0     0/0       -
    10 VTY               -    -      -    -    -      0       0     0/0       -
    11 VTY               -    -      -    -    -      0       0     0/0       -
    12 VTY               -    -      -    -    -      0       0     0/0       -
    13 VTY               -    -      -    -    -      0       0     0/0       -
```

```
    14 VTY               -    -      -    -    -      0       0     0/0       -

2509#
```

CTY 回線タイプはコンソール ポートです。 いずれのルータ上でも、この回線タイプは、ルータ設定で **line con 0** として表示され、**show line** コマンド出力で **cty** として表示されます。 コンソール ポートは主として、コンソール端末を使用しているローカル システムのアクセスに使用されます。

TTY 回線は、着信または発信モデム、および端末接続に使用される非同期回線で、ルータ設定またはアクセス サーバ設定で **line x** として表示されることがあります。 固有の回線番号は、ルータまたはアクセス サーバに組み込まれたり取り付けられているハードウェアの機能です。

AUX 回線は補助ポートで、設定で **line aux 0** として表示されます。

VTY 回線はルータの仮想端末回線で、着信 Telnet 接続の制御だけに使われます。 この回線は、ソフトウェアの機能であり、この回線に関連するハードウェアは存在しないという点で仮想のものです。 この回線は、設定で **line vty 0 4** として表示されます。

上記の各回線タイプは、パスワード保護を使って設定できます。 回線は、全ユーザで 1 つのパスワードを使用するように設定することも、ユーザ固有のパスワードを使用するように設定することもできます。 ユーザ固有のパスワードは、ルータ上でローカルに設定することも、認証を行うため認証サーバを使用することもできます。

複数のパスワード保護を使って、複数の回線を設定できます。 実際、ルータでは、コンソール用に 1 つのパスワードを使用し、そのほかの着信接続にユーザ固有のパスワードを使用することが一般的です。

次に、**show running-config** コマンドからのルータ出力例を示します。

```
2509#show running-config
Building configuration...

Current configuration : 655 bytes
!
version 12.2
.
.
.
!--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

## 回線上でのパスワードの設定

回線上でパスワードを指定するには、回線設定モードで **password** コマンドを使用します。 ログイン時のパスワード チェックを有効にするには、回線設定モードで **login コマンド**を使用します。

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

### 設定手順

この例では、コンソールを使用する全ユーザに対して、パスワードが 1 つ設定されています。

1. 特権的な EXEC（または「イネーブルな」）プロンプトから設定モードに入り、次のコマンドを使って回線設定モードに切り替えます。 現在のモードを反映して、プロンプトが変化するという点に注意してください。

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#line con 0
router(config-line)#
```

2. パスワードを設定し、ログイン時のパスワード チェックを有効にします。

```
router(config-line)#password letmein
router(config-line)#login
```

3. 設定モードを終了します。

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

**注:** ユーザのログイン機能が確認されるまで、設定の変更を **line con 0** に保存しないでください。

**注:** 回線コンソールの設定で、**login** はログイン時のパスワード チェックを有効にするのに必要な設定コマンドです。 コンソール認証が機能するには、**password** コマンドと **login** コマンドの両方が必要です。

## 設定の確認

ルータ設定を調べて、コマンドが適切に入力されたことを確認します。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show running-config**：ルータの現在の設定を表示します。

```
router#show running-config
Building configuration...
...
!--- Lines omitted for brevity ! line con 0 password letmein
login
line 1 8
line aux 0
line vty 0 4
!
end
```

設定をテストするには、コンソールをログオフしてから、ルータ アクセス用のパスワードを使って再度ログインします。

```
router#exit

router con0 is now available

Press RETURN to get started.

User Access Verification
Password:
!--- Password entered here is not displayed by the router router>
```

**注:** ルータへの再ログインで障害が発生する場合に備えて、この試験を実行する前に、ルータへの別の接続（Telnet やダイヤルインなど）が確立されていることを確認してください。

## ログイン障害のトラブルシューティング

設定を保存していないまま、ルータへの再ログインができなくなった場合、ルータをリロードすれば、これまで行った設定変更が失われます。

設定変更を保存してからルータへのログインができなくなった場合、パスワードの回復を実行する必要があります。 ご使用になっているプラットフォーム固有の手順については、『パスワード回復手順』を参照してください。

# ローカル ユーザ固有のパスワードの設定

ユーザ名に基づいた認証システムを確立するには、グローバル設定モードで **username** コマンドを使用します。 ログイン時のパスワード チェックを有効にするには、回線設定モードで **login local** コマンドを使用します。

## 設定手順

この例では、Telnet を使って、VTY 回線上のルータへ接続しようとするユーザに対して、パスワードが設定されます。

1. 特権 EXEC ( または「イネーブル」 ) プロンプトから設定モードに入り、ルータへのアクセスを許可するユーザごとに、ユーザ名とパスワードの組み合わせを入力します。
```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#username russ password montecito
router(config)#username cindy password belgium
router(config)#username mike password rottweiler
```
2. 次のコマンドを使って、回線設定モードに切り替えます。 現在のモードを反映して、プロンプトが変化するという点に注意してください。
```
router(config)#line vty 0 4
router(config-line)#
```
3. ログイン時のパスワード チェックを設定します。
```
router(config-line)#login local
```
4. 設定モードを終了します。
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
**注:** CLI で名前を入力する際に自動 Telnet を無効にするには、使用する回線で **no logging preferred** を設定します。 **transport preferred none** でも同じ出力が表示され、**ip host** コマンドで設定された定義済みホストに対して自動 Telnet が無効にされます。 この場合、未定義のホストに対して自動 Telnet を停止させ、定義済みホストに対しては機能させる **no logging preferred** コマンドとは異なります。

## 設定の確認

ルータ設定を調べて、コマンドが適切に入力されたことを確認します。

- **show running-config**：ルータの現在の設定を表示します。
```
router#show running-config
Building configuration...
!
!--- Lines omitted for brevity ! username russ password 0 montecito
```

```
username cindy password 0 belgium
username mike password 0 rottweiler
!
!--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4 login local
!
end
```

この設定をテストするため、ルータへの Telnet 接続を確立する必要があります。 これはネットワークの別のホストから接続することによって実行できますが、**show interfaces** コマンドの出力で表示される up/up 状態にあるルータ上の任意のインターフェイスの IP アドレスに telnet 接続することによって、ルータ自体からテストすることもできます。**interface ethernet 0** のアドレスが 10.1.1.1 の場合の出力例を次に示します。

```
router#telnet 10.1.1.1
Trying 10.1.1.1 ... Open


User Access Verification


Username: mike
Password:
!--- Password entered here is not displayed by the router router
```

## ユーザ固有のパスワード障害のトラブルシューティング

ユーザ名とパスワードでは、大文字と小文字が区別されます。 ユーザ名またはパスワードの大文字と小文字を正しく区別しないで入力すると、ログインしようとするユーザが拒絶されます。

ユーザが固有のパスワードを使ってルータにログインできない場合、ルータ上でユーザ名とパスワードを再設定してください。

# AUX 回線パスワードの設定

AUX 回線上でパスワードを指定するには、回線設定モードで **password コマンド**を発行します。 ログイン時のパスワード チェックを有効にするには、回線設定モードで **login コマンド**を発行します。

## 設定手順

この例では、補助ポートを使用する全ユーザに対して、パスワードが 1 つ設定されています。

1. 補助ポートが使用する回線を確認するには、**show line コマンド**を発行します。

```
R1#show line

   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                  -    -     -    -     -     0      0     0/0       -
    65 AUX  9600/9600   -    -     -    -    -     0     1     0/0               -
    66 VTY                 -    -     -    -     -     0      0     0/0       -
    67 VTY                 -    -     -    -     -     0      0     0/0       -
```

2. この例では、補助ポートは回線 65 上にあります。 ルータの AUX 回線を設定するには、次のコマンドを発行します。

```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
```

```
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
R1#
```

## 設定の確認

ルータ設定を調べて、コマンドが適切に入力されたことを確認します。

- **show running-config コマンド**は、ルータの現在のコンフィギュレーションを表示します。

```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
 password cisco
 login
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

# ログイン用 AAA 認証の設定

ログイン用に認証、認可、アカウンティング（AAA）認証をイネーブルにするには、回線設定モードで **login authentication** コマンドを使用します。 AAA サービスも設定する必要があります。

## 設定手順

この例では、ユーザがルータに接続しようとすると、TACACS+ サーバからユーザのパスワードを取得するようにルータが設定されます。

**注:** ほかのタイプの AAA サーバ（RADIUS など）を使用するようにルータを設定する場合も同様です。 詳細は、『認証の設定』を参照してください。

**注:** このドキュメントでは、AAA サーバ自体の設定については触れません。 AAA サーバの設定については、『セキュリティ サーバ プロトコル』を参照してください。

1. 特権的な EXEC（または「有効な」）プロンプトから設定モードに入り、認証用に AAA サービスを使用するようにルータを設定します。

```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmein
```

2. 次のコマンドを使って、回線設定モードに切り替えます。 現在のモードを反映して、プロンプトが変化するという点に注意してください。

```
router(config)#line 1 8
router(config-line)#
```

3. ログイン時のパスワード チェックを設定します。

```
router(config)#line 1 8
router(config-line)#
```

4. 設定モードを終了します。

```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

## 設定の確認

ルータ設定を調べて、コマンドが適切に入力されたことを確認します。

- **show running-config**：ルータの現在の設定を表示します。

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
 login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

この特定の設定をテストするには、着信接続または発信接続を回線に反映する必要があります。モデム接続用の非同期回線設定については、『モデム - ルータ接続ガイド』を参照してください。

また、AAA 認証とその試験を実行するため、1 つまたは複数の VTY 回線を設定することもできます。

## AAA ログイン障害のトラブルシューティング

**debug** コマンドを発行する前に、『debug コマンドの重要な情報』を参照してください。

ログイン時の障害をトラブルシューティングするには、使用中の設定に対して **debug** コマンドを適切に使用する必要があります。

- debug aaa authentication
- debug radius
- debug kerberos

# 関連情報

- **認証の設定**
- Cisco IOS Debug コマンド リファレンス
- テクニカルサポート - Cisco Systems