コンソールポート、Telnet、および SSH の処理、およびリセットボタン

この章の内容は、次のとおりです。

コンソールポート、Telnet、および SSH に関する注意事項と制約事項

- トランスポートマップがイーサネット管理インターフェイスに適用されるとき、トランスポート マップでの Telnet および Secure Shell（SSH）設定は、他のすべての Telnet および SSH 設定をオーバーライドします。
- イーサネット管理インターフェイスを開始するユーザの認証には、ローカルユーザ名とパスワードだけを使用できます。持続性 Telnet または持続性 SSH を使用してイーサネット管理インターフェイス経由でデバイスにアクセスするユーザーは、AAA 認証を使用できません。
- アクティブな Telnet または SSH セッションがあるイーサネット管理インターフェイスにトランスポート マップを適用すると、アクティブ セッションが切断される可能性があります。しかし、インターフェイスからトランスポートマップを削除すると、アクティブな Telnet セッションまたは SSH セッションの接続は切断されません。
- 診断バナーおよび待機バナーの設定は任意ですが、設定することを推奨します。バナーは、特に Telnet または SSH 試行ステータスをユーザに示すインジケータとして役立ちます。

コンソール ポート

デバイス上のコンソールポートは、EIA/TIA-232 非同期、フロー制御なしのシリアル接続で、RJ-45 コネクタを使用します。コンソールポートは、デバイスへのアクセスに使用され、ルートプロセッサの前面パネルに位置しています。

コンソールポートを使用したデバイスへのアクセスについては、Cisco IOS XE ソフトウェアの使用を参照してください。

コンソールポートの処理

コンソール ポートを使用してルータにアクセスする場合は、自動的に Cisco IOS Command-Line Interface （CLI）へ誘導されます。

コンソールポートを介したルータへのアクセス試行で、CLI に接続する前にブレーク信号を送った場合（**Ctrl-C** または **Ctrl-Shift-6** を押すか、Telnet プロンプトで **send break** コマンドを入力）、非 RPIOS サブパッケージにアクセス可能であれば、診断モードに誘導されます。これらの設定を変更するには、コンソール ポートに設定したトランスポート マップをコンソール インターフェイスに適用します。

コンソールポートのトランスポートマップの設定

このタスクでは、デバイス上のコンソール ポート インターフェイスにトランスポートマップを設定する方法について説明します。

手順

ステップ 1 **enable**

例：

```
Router> 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：

```
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 **transport-map type console** *transport-map-name*

例：

```
Router(config)# transport-map type console consolehandler
```

コンソール接続を処理するためのトランスポート マップを作成して名前を付け、トランスポート マップ コンフィギュレーション モードを開始します。

ステップ 4 **connection wait** [**allow** [**interruptible**] | **none** [**disconnect**]]

例：

```
Router(config-tmap)# connection wait none
```

コンソール接続を処理する方法を、このトランスポート マップで指定します。

- **allow interruptible**：コンソール接続は Cisco IOS VTY 回線が使用可能になるのを待機します。また、ユーザは Cisco IOS VTY 回線が使用可能になるのを待機しているコンソール接続に割り込むことにより、診断モードを開始できます。これがデフォルト設定です。

  （注）
  Ctrl+C キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。

- **none**：コンソール接続はただちに診断モードを開始します。

ステップ 5 （任意） **banner** [**diagnostic** | **wait**] *banner-message*

例：

```
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to Diagnostic Mode--
X
Router(config-tmap)#
```

（オプション）診断モードを開始しているユーザ、またはコンソール トランスポート マップ設定のために Cisco IOS VTY 回線を待機しているユーザに表示されるバナー メッセージを作成します。

- **diagnostic**：コンソール トランスポート マップ設定のために診断モードに誘導されたユーザに表示されるバナー メッセージを作成します。

  （注）
  Ctrl+C キーまたは **Ctrl+Shift+6** キーを入力すると、ユーザは待機中の接続に割り込むことができます。

- **wait**：Cisco IOS VTY が使用可能になるのを待機しているユーザに表示されるバナー メッセージを作成します。

- *banner-message*：同じデリミタで開始および終了するバナー メッセージ。

ステップ 6 **exit**

例：

```
Router(config-tmap)# exit
```

トランスポート マップ コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードを再開します。

ステップ 7 **transport type console** *console-line-number* **input** *transport-map-name*

例：

```
Router(config)# transport type console 0 input consolehandler
```

トランスポート マップで定義された設定をコンソール インターフェイスに適用します。

このコマンドの *transport-map-name* は、**transport-map type console** コマンドで定義された *transport-map-name* と一致する必要があります。

例

次に、コンソール ポートのアクセス ポリシーを設定し、コンソール ポート 0 に接続するためにトランスポート マップを作成する例を示します。

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

コンソールポートおよび SSH の処理設定の表示

コンソールポート、SSH、および Telnet の処理設定を表示するには、次のコマンドを使用します。

- **show transport-map**
- **show platform software configuration access policy**

トランスポート マップ設定を表示するには、**show transport-map** コマンドを使用します。

show transport-map [**all** | **name** *transport-map-name* | **type** [**console** [**ssh**]]

このコマンドは、ユーザ EXEC モードまたは特権 EXEC モードで使用可能です。

例

次に、デバイスで設定されたトランスポートマップの例（コンソールポート（consolehandler）、持続性 SSH（sshhandler）、持続性 Telnet トランスポート（telnethandler））を示します。

```
Router# show transport-map all
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

bshell banner:

Welcome to Diagnostic Mode


Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0/0/0

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:
Welcome to Diagnostic Mode



Router# show transport-map type console
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode


Router# show transport-map type persistent ssh
Transport Map:
Name: sshhandler
Type: Persistent SSH Transport

Interface:
GigabitEthernet0
```

```
Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for IOS prompt

Bshell banner:

Welcome to Diagnostic Mode


SSH:
Timeout: 120
Authentication retries: 5
RSA keypair: sshkeys



Router# show transport-map name consolehandler
Transport Map:
Name: consolehandler
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable
Wait banner:

Waiting for the IOS CLI

Bshell banner:

Welcome to Diagnostic Mode
```

着信コンソール ポート、SSH、および Telnet 接続の処理に関する現行設定を表示するには、**show platform software configuration access policy** コマンドを使用します。このコマンドの出力には、各接続タイプ（Telnet、SSH、およびコンソール）の現在の待機ポリシーと、現在設定されているバナーの情報が示されます。

show transport-map コマンドとは異なり、**show platform software configuration access policy** コマンドは診断モードで使用可能です。このため、トランスポートマップ設定情報が必要であるにもかかわらず Cisco IOS CLI にアクセスできない場合に、このコマンドを入力できます。

例

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait
Shell banner:
Wait banner :

Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
```

```
Rule : wait with interrupt
Shell banner:
Wait banner :
```

例

この例では、SSH 用の新しいトランスポートマップが設定される前と後の両方で発行される **show platform software configuration access policy** コマンドを示します。設定時に、持続性 SSH トランスポート マップの接続ポリシーとバナーが設定され、SSH のトランスポート マップがイネーブル化されます。

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process


Method : ssh
Rule : wait
Shell banner:
Wait banner :

Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# transport-map type persistent ssh sshhandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
Welcome to Diag Mode
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS
X
Router(config-tmap)# rsa keypair-name sshkeys
Router(config-tmap)# transport interface gigabitethernet 1
Router(config-tmap)# exit
Router(config)# transport type persistent ssh input sshhandler
Router(config)# exit

Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt
Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS process
```

```
Method : ssh
Rule : wait with interrupt
Shell banner:
Welcome to Diag Mode

Wait banner :
Waiting for IOS


Method : console
Rule : wait with interrupt
Shell banner:
Wait banner :
```

リセットボタンの概要

リセットボタン機能は、すべての Cisco 8300 シリーズ セキュアルータにデフォルトで設定されています。リセットボタンを使用すると、設定不備が原因で応答しなくなったり、ユーザーがログイン情報を間違ってログインできなくなったりしたときに、Cisco 8300 シリーズ セキュアルータを回復できます。

リセットボタン機能について

デフォルトでは、リセットボタンの機能は有効になっています。この機能を無効にするには、**no service password-recovery strict** コマンドを使用します。

デバイスが初期化されているときに、前面パネルのリセットボタンを押すと、この機能をトリガーできます。

次の表では、サービスパスワード回復ありとサービスパスワード回復なしの条件で、さまざまな組み合わせでのリセットボタン機能の動作を示します。

表 1 : Service password-recovery

リセットボタンを押す（ステータス）				動作			
番No	**ゴールデンイメージ**	**ゴールデン構成**	**スタートアップ構成**	**イメージ**	**Config**	**追加情報**	
1	あり	あり	あり	ゴールデン	ゴールデン	-	
2	あり	あり	なし	ゴールデン	ゴールデン	-	

3	あり	なし	あり	ゴールデン	PnP	スタートアップの削除
4	あり	なし	なし	ゴールデン	PnP	-
5	なし	あり	あり	標準	ゴールデン	-
6	なし	あり	なし	標準	ゴールデン	-
7	なし	なし	あり	標準	PnP	スタートアップの削除
8	なし	なし	なし	標準	PnP	-

表 *2 : No service password-recovery*

リセットボタンを押す（ステータス）				動作		
番No	**ゴールデンイメージ**	**ゴールデン構成**	**スタートアップ構成**	**イメージ**	**Config**	**追加情報**
1	あり	NVRAM内	あり	ゴールデン	PnP	消去
2	あり	ブートフラッシュ内	あり	ゴールデン	ゴールデン	消去
3	あり	NVRAM内	なし	ゴールデン	PnP	消去
4	あり	ブートフラッシュ内	なし	ゴールデン	ゴールデン	消去
5	あり	なし	あり	ゴールデン	PnP	消去
6	あり	なし	なし	ゴールデン	PnP	消去
7	なし	NVRAM内	あり	標準	PnP	消去

8	なし	ブートフラッシュ内	あり	標準	ゴールデン	消去
9	なし	NVRAM内	なし	標準	PnP	消去
10	なし	ブートフラッシュ内	なし	標準	ゴールデン	消去
11	なし	なし	あり	標準	PnP	消去
12	なし	なし	なし	標準	PnP	消去

リセットボタン機能を有効にするための前提条件

- デバイスの ROMmon バージョンが 17.18（1.5r）以上であることを確認します。
- golden.bin イメージと golden.cfg を必ず設定してください。

コントローラモードのリセットボタンに関する制約事項

- リセットボタンを使用すると、すべての SD-WAN 設定を消去したり、Cisco 8300 シリーズセキュアルータのデフォルト設定として使用可能な ciscosdwan.cfg 設定を適用したりできます。リセットボタンは、最初に golden.bin イメージを起動しようとします（使用可能な場合）。golden.bin イメージが使用できない場合、次にデフォルトのブートアップ設定を試行します。リセット機能では、golden.bin イメージは必須ではありません。
- デバイスが起動を開始している場合は、リセットボタンを押す必要があります。システムが ROMMON モードまたは IOS モードに設定されている場合、リセット機能は動作しません。

リセットボタン機能を有効にする方法

ここでは、Cisco 8100 シリーズセキュアルータでリセットボタン機能を有効にする方法について説明します。

手順の概要

1. **configure terminal**
2. **service password-recovery**
3. **no service password-recovery**
4. **exit**
5. **no service recovery-service strict**

手順の詳細

手順

	コマンドまたはアクション	目的
ステップ 1	**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 2	**service password-recovery** 例： `Device(config)# service password-recovery`	デバイスでパスワード回復サービスを設定します。
ステップ 3	**no service password-recovery** 例： `Device(config)# no service password-recovery`	応答しないデバイスを回復できます。ただし、すべてのユーザー設定とキーが削除されるため、デバイスは再設定されます。 （注） IOS NVRAM の startup-config ファイルが削除されないように、リカバリメカニズムとしてデバイスに golden.bin と golden.cfg の設定があることを確認します。
ステップ 4	**exit** 例： `Device(config)# exit`	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 5	**no service recovery-service strict** 例： `Device(config)# no service recovery-service strict`**exit**	デバイスでリセットボタン機能を無効にします。 （注） Cisco IOS XE 17.18.x リリース以降では、デバイスに golden.bin や golden.cfg の設定があっても、**no service recovery-service strict** コマンドを使用するとデバイスを回復できないため、シスコへの返品許可（RMA）を通じた返品や交換が必要になります。

リセットボタン機能の有効化と無効化

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# service password-recovery
Executing this command enables the password recovery mechanism.
Device(config)#
```

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no service password-recovery strict

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.

Are you sure you want to continue? [yes]: yes
Device(config)#
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。