CHAPTER 3

# Cisco Security Packet Analyzer 2400 シリーズ アプライアンスの設定

この章では、パケット アナライザ コマンドライン インターフェイス（CLI）を使用して、ネットワーク接続の確立や IP パラメータの設定を行うために Cisco Security Packet Analyzer 2400 シリーズ アプライアンス を設定する方法、およびその他の必要な管理タスクを実行する方法について説明します。この章ではまた、パケット アナライザ グラフィカル ユーザ インターフェイス（GUI）を開始する方法、およびさまざまなシステム管理タスクを実行する方法も説明します。

この章の内容は、次のとおりです。



パケット アナライザ 設定情報の詳細については、パケット アナライザ Web サーバ インターフェイスを使用するか、『*Network Analysis Module Command Reference*』を参照してください。

## 最初のログイン

最初に Cisco Security Packet Analyzer 2400 シリーズ アプライアンス の電源をオンにしてブートすると、接続されたコンソールにログイン プロンプトが表示されます。工場出荷時、Cisco Security Packet Analyzer 2400 シリーズ アプライアンスで root ユーザがあらかじめ設定されています。root ユーザのデフォルトのパスワードは *root* です。

（注） 最初のログイン セッション中に、ユーザ root のパスワードを変更する必要があります。

root ユーザは、パケット アナライザ のルート（読み取り/書き込み）レベルにアクセスし、パケット アナライザ コマンドライン インターフェイス（CLI）コマンドを入力できます。

初めて Cisco Security Packet Analyzer 2400 シリーズ アプライアンスにログインするには、Cisco Security Packet Analyzer アプライアンスとのコンソール セッションまたはシリアル セッションを開きます。でのセッションを開く例を示します。

（注）　初回ログイン後、パケット アナライザ アプライアンスへの **telnet** および **ssh** 接続をイネーブルにできます。

**ステップ 1**　パケット アナライザ ログイン プロンプトが表示されたら、**root** を入力して Enter を押します。

```
secpa.localdomain login: root
```

**ステップ 2**　パスワード プロンプトが表示されたら、**root** を入力して、Enter を押します。

ID とパスワードを入力すると、root のパスワードを変更するようプロンプトが表示されます。

```
secpa2400-209.localdomain login: root
Password: <secpa1>
Last login: Mon Aug 20 08:28:34 2012 from sjc-vpn2-1516.cisco.com on pts/1

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

System_Alert! Default password has not been changed!
Please enter a new root user password.
Enter new password:
```

**ステップ 3**　root ユーザの新しいパスワードを入力し、それを再度入力します。

```
Confirm new password:
Successfully changed password for user 'root'
```

パスワードを記録して、この情報を安全な場所に保管することを推奨します。設置場所のパスワード セキュリティ ポリシーに従って、このパスワードを定期的に変更する必要があります。ルート パスワードの変更（3-2 ページ）を参照してください。

# ルート パスワードの変更

この項では、初回ログイン セッション後に root ユーザのパスワードを変更する方法について説明します。root パスワードを変更するには、次の手順を実行します。

**ステップ 1**　Cisco Security Packet Analyzer アプライアンスのコンソール セッションまたはシリアル セッションを開きます。

**ステップ 2**　ユーザ名を求めるプロンプトが表示されたら、**root** を入力します。

Cisco Security Packet Analyzer 2400 アプライアンスでは、工場出荷時にデフォルトでユーザ **root** のパスワードが **root** に設定されています。

**ステップ 3**　パスワード入力を促されたときは、ユーザ root のパスワードを入力します。

root ユーザとしてログインすると、Cisco Security Packet Analyzer アプライアンスのルート レベルに読み取りおよび書き込みアクセスができ、CLI コマンドを入力して実行することができます。

```
root@hostname#
```

**ステップ 4**　次のコマンドを入力して、root ユーザのパスワードを変更します。

```
password  root

New password:
Confirm password:
```

**ステップ 5**　ユーザ root の新しいパスワードを入力し、確認します。

パスワードを記録して、この情報を安全な場所に保管することを推奨します。設置場所のパスワード セキュリティ ポリシーに従って、このパスワードを定期的に変更する必要があります。

**ステップ 6**　**exit** を入力してセッションを終了し、ログアウトします。

# 例

ここで紹介する例は、次のとおりです。

- パケット アナライザ ルート パスワードの変更：例（3-3 ページ）
- パケット アナライザ ルート パスワードの検証：例（3-3 ページ）

## パケット アナライザ ルート パスワードの変更：例

```
root@secpa2400-209.localdomain# password root
Enter new password:
Confirm new password:
Successfully changed password for user 'root'
```

## パケット アナライザ ルート パスワードの検証：例

```
nam1.company.com login: root
Password: <secpa1>
Terminal type: vt100

Cisco Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

root@nam1.company.com#
root@nam1.company.com# exit
```

# パケット アナライザ ルート パスワードのデフォルト値へのリセット

パケット アナライザ ルート パスワードをデフォルト値へリセットする方法の詳細については、『*Cisco Prime Network Analysis Module Software User Guide*』を参照してください。

# ネットワーク接続の確立

この項では、Cisco Security Packet Analyzer 2400 アプライアンスを設定して、ネットワーク接続を確立するために IPv4 環境で IP パラメータを設定する方法についてを説明します。

管理コンソールから Cisco Security Packet Analyzer 2400 アプライアンス にログインし、適切な設置場所の情報を使用して次の CLI コマンドを入力します。

---

ステップ 1　**ip address** コマンドを使用して、Cisco Security Packet Analyzer アプライアンス の IP アドレスを設定します。このコマンドの構文は次のとおりです。

**ip address** *ip-address subnet-mask*

**例**

```
root@localhost# ip address 172.20.104.126 255.255.255.248
```

ステップ 2　**ip gateway** コマンドを使用して、Cisco Security Packet Analyzer アプライアンス のデフォルト ゲートウェイ アドレスを設定できます。このコマンドの構文は次のとおりです。

**ip gateway** *ip-address*

**例**

```
root@localhost# ip gateway 172.20.104.123
```

ステップ 3　**exsession** コマンドを使用して、Telnet または SSH を使用した Cisco Security Packet Analyzer アプライアンス へのリモート ログインをイネーブルにできます。この（オプション）コマンドの構文は次のとおりです。

**exsession on**　*（Telnet の場合）*

または

**exsession on ssh**　*（SSH の場合）*

**例**

Telnet アクセスをイネーブルにするように Cisco Security Packet Analyzer アプライアンス を設定するには、次のコマンドを実行します。

```
root@localhost# exsession on
```

SSH アクセスをイネーブルにするように Cisco Security Packet Analyzer アプライアンスを設定するには、次のコマンドを実行します。

```
root@localhost# exsession on ssh
```

ステップ 4　**ip domain** コマンドを使用して、Cisco Security Packet Analyzer アプライアンス システムのドメイン名を設定できます。この（オプション）コマンドの構文は次のとおりです。

**ip domain** *name*

**例**

```
root@localhost# ip domain your_company.com
```

**ステップ 5**　**ip host** コマンドを使用して、Cisco Security Packet Analyzer アプライアンスシステムのホスト名を設定できます。

このコマンドの構文は次のとおりです。

**ip host** *name*

**例**

```
root@localhost# ip host secpa_machine
```

**ステップ 6**　（オプション）**ip nameserver** コマンドを使用して、Cisco Security Packet Analyzer アプライアンスに 1 つまたは複数のネーム サーバを設定するのが適切な場合もあります。

このコマンドの構文は次のとおりです。

**ip nameserver**　*ip-address [ip-address] [ip-address]*

**例**

```
root@localhost# ip nameserver 172.20.104.10
root@localhost# ip nameserver 172.20.104.10  172.20.104.20  172.20.104.30
```

# 設定の確認

Cisco Security Packet Analyzer アプライアンスのネットワーク接続の設定終了後に、接続の確認および Cisco Security Packet Analyzer アプライアンスに設定した IP パラメータの検証を行うことを推奨します。

**ステップ 1**　**ping** コマンドを使用して、Cisco Security Packet Analyzer アプライアンスとネットワーク デバイス間の接続を確認します。

このコマンドの構文は次のとおりです。

**ping** *{hostname | ip-address}*

**例**

```
root@localhost# ping secpa_machine.your_company.com
root@localhost# ping 172.20.104.10
```

次は、正常な接続を示す **ping** コマンドの例です。

```
root@secpa_machine.your_company.com# ping 172.20.104.10
PING 172.20.104.10 (172.20.104.10) 56(84) bytes of data.
64 bytes from 172.20.104.10: icmp_seq=1 ttl=254 time=1.27 ms
64 bytes from 172.20.104.10: icmp_seq=2 ttl=254 time=1.13 ms
64 bytes from 172.20.104.10: icmp_seq=3 ttl=254 time=1.04 ms
64 bytes from 172.20.104.10: icmp_seq=4 ttl=254 time=1.08 ms
64 bytes from 172.20.104.10: icmp_seq=5 ttl=254 time=1.11 ms

--- 172.20.104.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 1.043/1.129/1.278/0.090 ms
root@secpa_machine.your_company.com#
```

ステップ 2　**show ip** コマンドを使用して、Cisco Security Packet Analyzer アプライアンスの IP パラメータが適切に設定されたことを確認します。

このコマンドの構文は次のとおりです。

**show ip**

```
root@localhost# show ip root@nam1.company.com# show ip
```

次は、設定された Cisco Security Packet Analyzer アプライアンスを示す **show ip** コマンドの出力例です。

```
root@secpa-2400-96.cisco.com# show ip

==== IP/DNS Configuration ====
IPv4 Address/Netmask:    172.20.124.96 / 255.255.255.0
IPv4 Default Gateway:    172.20.124.47
IPv4 Broadcast:          172.20.124.255
IPv6 Address:            2001:20:1:100::96/64
IPv6 Default Gateway:    2001:20:1:100::1
Host Name:               appliance-2404-96.cisco.com
Nameserver(s):           171.70.168.183


==== Remote Access & Authentication ====
HTTP:                    Enabled (on port 80)
HTTPS:                   Disabled
SSH:                     Enabled (on port 22)
Telnet:                  Enabled (on port 23)
TACACS+:                 Disabled


==== File Sharing Services ====
SMB:                     Disabled
SFTP:                    Disabled
```

# Cisco Security Packet Analyzer Web サーバの有効化

この項では、Cisco Security Packet Analyzer Web サーバ、および Packet Analyzer グラフィカル ユーザ インターフェイス（GUI）へのブラウザベースのアクセスをイネーブルにする方法を説明します。

（注）　Packet Analyzer をイネーブルにして、HTTP サーバまたは HTTPS セキュア サーバとして機能させることができますが、同時に両方を機能させることはできません。

Packet Analyzer Web サーバをイネーブルにして、ブラウザベースのアクセスを準備するために、使用中の Web ブラウザが対象の Packet Analyzer ソフトウェア リリースをサポートしていることを確認します。

（注）　サポートするブラウザの一覧は、Cisco Security Packet Analyzer ソフトウェアリリース ノートを参照してください。

Packet Analyzer  Web サーバをイネーブルにするには、次のコマンドを入力します。

**ステップ 1**　Cisco Security Packet Analyzer アプライアンスへの Telnet または SSH セッションを開いて、パスワード プロンプトでパスワードを入力します。

**telnet** {ip-address | hostname}

または

**ssh** {ip-address | hostname}

**ステップ 2**　次のコマンドの 1 つを入力して、HTTP サーバまたは HTTPS セキュア サーバをイネーブルにします。

Packet Analyzer HTTP Web サーバをイネーブルにするには、次のようにします。

**ip http server enable**

Packet Analyzer HTTPS Web サーバをイネーブルにするには、次のようにします。

**ip http secure server enable**

Packet Analyzer より Web 管理者のユーザ名が要求されます。

```
Enabling HTTP server...

No web users are configured.
Please enter a web administrator user name [admin]: <CR>
```

Packet Analyzer Web サーバでは、少なくとも 1 人の Web 管理者が正しく設定されている必要があります。Packet Analyzer で Web ユーザ名とパスワードが要求されない場合は、少なくとも 1 人の Web 管理者が以前に設定されています。

**ステップ 3**　Web 管理者のユーザ名を入力します。別の方法としては、Enter を押して、デフォルトの Web 管理者のユーザ名である *admin* を使用します。

Packet Analyzer により Web 管理者のパスワードが要求されます。次に、正確さを確保するためパスワードを再入力するように要求されます。

```
New password: <adminpswd>

Confirm password: <adminpswd>
```

**ステップ 4**　Web 管理者のパスワードを入力し、確認します。

**（注）**　このマニュアルは、Cisco.com 経由で一般に公開されているため、このパスワードとすべてのデフォルトのパスワードをできるだけ早く変更することを推奨します。

**ステップ 5**　Packet Analyzer Web サーバ機能を確認するには、承認されたインターネット ブラウザを起動し、IP アドレスまたはホストおよびドメインの名前をブラウザのアドレス フィールドに入力します。

**（注）**　サポートするブラウザの一覧は、「Cisco Security Packet Analyzer ソフトウェアリリース ノート」を参照してください。

Cisco Security Packet Analyzer 2400 シリーズ アプライアンス Web サーバが正しく設定されている場合、Packet Analyzer ログイン ウィンドウにアクセスできます。

この時点で、Packet Analyzer Web サーバにログインできるユーザは、Web サーバのイネーブル時に設定した管理ユーザだけです。

# システムの状態の検証

インストール、アップグレード、またはダウングレードのステータスを確認したり、問題をトラブルシューティングするには、表 3-1、共通の診断コマンドおよび show コマンドに一覧表示されているコマンドを使用します。

(注)
- この項の表では、管理対象デバイスとネットワーク モジュールで共通のコマンドだけを記載します。
  - 使用可能なすべてのコマンドの一覧を表示するには、**?** をプロンプトで入力します（例：`user@secpa_host.domain# ?`）。
  - すべてのコマンド キーワード オプションの一覧を表示するには、**?** をコマンドの末尾に追加します（例：`secpa_host.domain# ip ?`）。
- 表では、コンフィギュレーション モード別にコマンドを記載しています。同じコマンドが複数のモードで利用できる場合は、モードによってコマンドの動作が異なることがあります。

(注)　多くの **show** コマンドには、診断出力を画面に表示したり、出力をファイルまたは URL に送信したりするためのキーワード オプションが含まれます。

*表 3-1　共通の診断コマンドおよびshow コマンド*

| コマンド | 目的 |
|---|---|
| **clear access-log** | Web アクセス ログをクリアします。 |
| **clear captured-data-files** | Packet Analyzer ローカル ドライブでキャプチャされたすべてのファイルを削除します。 |
| **clear monitoring-data** | Packet Analyzer 上のすべてのモニタリング データを削除します。 |
| **clear system-alerts** | システム アラートをクリアします。 |
| **clear system-passwords** | アプリケーション イメージのデフォルトの CLI パスワードを復元します。 |
| **ping** | 指定した IP アドレスまたはホスト名に ping を送信して、ネットワーク接続を確認します。 |
| **show access-log** | Web アクセス ログを表示します。 |
| **show application** | プロトコル グループ化情報を表示します。 |
| **show audit-trail** | Web GUI のログイン設定および CLI のアクセス設定を表示します。 |
| **show autocreate-data-source** | データ ソースの自動作成の設定を表示します。 |
| **show cdb** | CDB ファイルに関する情報を表示します。 |
| **show cdp settings** | CDP の設定を表示します。 |
| **show certificate** | インストールされた証明書を表示します。 |
| **show certificate-request** | 証明書署名要求を表示します。 |
| **show clock** | 現在のデータと時間を表示します。 |
| **show configuration** | **configure** コマンドを使用して入力した bootloader の現在の設定を表示します。 |

*表 3-1　共通の診断コマンドおよびshow コマンド(続き)*

| コマンド | 目的 |
|---|---|
| **show data-source** | データ ソースを表示します。 |
| **show date** | 現在のデータと時間を表示します。 |
| **show debug** | デバッグ情報を表示します。 |
| **show device** | リモート デバイスを表示します。 |
| **show email** | 電子メールの設定を表示します。 |
| **show entity** | エンティティ MIB 情報を表示します。 |
| **show flow-cache-sizes** | Packet Analyzer 内部キャッシュのサイズを表示します。 |
| **show ftp** | スケジュール レポートの FTP 設定を表示します。 |
| **show hosts** | hosts のエントリを表示します。 |
| **show inventory** | システムのインベントリ情報を表示します。 |
| **show ip** | IP パラメータを表示します。 |
| **show local-storage all** | すべての物理ディスクおよび仮想ドライブを表示します。 |
| **show local-storage physical** | すべての物理ディスクを表示します。 |
| **show local-storage progress** | ドライブ再構築の進行状況を表示します。 |
| **show local-storage virtual** | すべての仮想ドライブを表示します。 |
| **show log** | Packet Analyzer の設定、パッチ、レポート、およびアップグレードのログを表示します。 |
| **show memory** | インストールされたメモリの量、使用可能な量、およびシステムで現在使用されている量を表示します。 |
| **show monitor** | 設定した収集を表示します。 |
| **show patches** | インストールされたパッチを表示します。 |
| **show preferences** | Packet Analyzer Web インターフェイスの設定を表示します。 |
| **show protocol-feature** | 解析プロトコル機能の設定を表示します。 |
| **show remote-storage** | キャプチャ データを保管するためのリモート ストレージの設定を表示します。 |
| **show snmp** | SNMP パラメータを表示します。 |
| **show syslog-settings** | Packet Analyzer の Syslog 設定を表示します。 |
| **show system-alerts** | Packet Analyzer の障害や問題を表示します。 |
| **show tech-support** | シスコのテクニカル サポートが問題の診断に利用できるホストルータの情報を表示します。 |
| **show time** | Packet Analyzer のシステム時刻の設定を表示します。 |
| **show trap-dest** | Packet Analyzer のトラップ宛先の設定を表示します。 |
| **show version** | ルータ、ソフトウェア、ネットワーク モジュールの bootloader のバージョン情報とハードウェア、デバイスについての情報を表示します。 |
| **show waas** | WAAS デバイスおよびデータ ソースを表示します。 |
| **show web-publication** | Web パブリケーションの設定を表示します。 |
| **show web-users** | 現在のローカル Web ユーザのリストを表示します。 |

# 監視対象デバイスの設定

監視対象（または管理対象）デバイスの出力インターフェイスを Cisco Security Packet Analyzer 2400 シリーズ アプライアンスのモニタリング ポートに接続した後に、データをそのインターフェイスに送信するように監視対象デバイスも設定する必要があります。これを次の 2 つの手順で実行します。

- 監視対象デバイスのインターフェイスの設定
- 宛先ポートとして Cisco Security Packet Analyzer 2400 シリーズ アプライアンスを使用するようモニタ対象デバイスのポートを SPAN します。

## 監視対象デバイスのインターフェイスの設定

監視対象デバイスで、Cisco Security Packet Analyzer 2400 シリーズ アプライアンスへの接続をトランク ポートとして設定しますが、no negotiate オプションを使用します。監視対象デバイスで、no negotiate オプションを使用すると、スイッチまたはルータはアプライアンスのモニタリング ポートで Dynamic Trunk Protocol（DTP）を実行できません。

次の例で、アプライアンスのモニタリング ポートに接続されたスイッチポートを Te 7/29 として設定する方法を示します。

監視対象デバイスのコマンド ラインで、次のように CLI コマンドを入力します。

**show run interface ethernet 4/37**

```
n7k-4# show run int ethernet 4/37
!Command: show running-config interface Ethernet4/37
!Time: Mon Apr 27 09:49:03 2015

version 7.2(0)D1(1)

interface Ethernet4/37
  description "Connected to secpa data port"
  switchport
  switchport monitor
  mtu 9216
```

## SPAN セッションの作成

アプライアンスのモニタリング ポートに接続されたポートへのモニタリング対象デバイスのトラフィックを SPAN するためには SPAN セッションが必要です。モニタリング対象デバイスの CLI または パケット アナライザ アプライアンス GUI を使用して、SPAN セッションを作成できます。

パケット アナライザ GUI を使用して SPAN セッションを設定する方法の詳細については、『*Cisco Security Packet Analyzer User Guide*』を参照してください。

# Packet Analyzer への Telnet または SSH セッションの開始と終了

この手順では、Packet Analyzer への Telnet または SSH セッションを開始および終了します。Packet Analyzer のモニタリングとメンテナンスには通常、Packet Analyzer GUI を使用するので、この手順を実行することは稀です。ただし、Packet Analyzer GUI にアクセスできない場合は、Telnet または SSH を使用し、Packet Analyzer CLI からトラブルシューティングを実行する必要が生じることもあります。

Telnet または SSH アクセス用に Cisco Security Packet Analyzer 2400 シリーズ アプライアンス が適切に設定されていない場合（以下の 前提条件（3-11 ページ）セクションを参照）、Cisco Security Packet Analyzer 2400 シリーズ アプライアンスの接続先である管理対象デバイスへの Telnet セクションを開き、次に管理対象デバイスから Packet Analyzer コンソール セッションを開くことができます。

### 前提条件

- Packet Analyzer システム IP アドレスを設定します。オプションで、Packet Analyzer システム ホスト名を設定します。
- 次の ping テストのいずれかを実行して、Packet Analyzer ネットワーク接続を確認します。
  - ゲートウェイの背後のホストから Packet Analyzer システム IP アドレスに ping を実行します。
  - Packet Analyzer CLI から Packet Analyzer システム デフォルト ゲートウェイに ping を実行します。

### Telnet の前提条件

- Packet Analyzer CLI コマンド **exsession on** を入力します。

### SSH の前提条件

- Packet Analyzer CLI コマンド **exsession on ssh** を入力します。

### 手順の概要

1. **telnet** {*ip-address* | *hostname*}
   または
   **ssh** {*ip-address* | *hostname*}
2. ログイン プロンプトで **root** と入力します。
3. パスワード プロンプトで、パスワードを入力します。
   または
   パスワードを工場出荷時のデフォルト設定から変更していない場合は、ルート パスワードとして **root** を入力します。
4. Packet Analyzer CLI で、必要な作業を実行します。Packet Analyzer への Telnet または SSH セッションを終了して Cisco IOS CLI に戻るには、ステップ 5 およびステップ 6 を実行します。
5. **exit**
6. **logout**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **telnet** {*ip-address* \| *hostname*}<br>または<br>**ssh** {*ip-address* \| *hostname*}<br><br>**例:**<br>`host.domain# telnet 10.20.30.40`<br><br>**例:**<br>`host.domain# ssh 10.20.30.40` | Telnet をサポートするホストにログインします。<br>または<br>リモート ネットワーク デバイスとの暗号化されたセッションを開始します。<br>• Packet Analyzer システム IP アドレスまたは Packet Analyzer システム ホスト名を使用します。 |
| ステップ 2 | ログイン プロンプトで **root** と入力します。<br><br>**例:**<br>`login: root` | Packet Analyzer のルート（読み取り/書き込み）レベルにアクセスします。 |
| ステップ 3 | パスワード プロンプトで、パスワードを入力します。<br>または<br>パスワードを工場出荷時のデフォルト設定から変更していない場合は、ルート パスワードとして **root** を入力します。<br><br>**例:**<br>`Password: root` | |
| ステップ 4 | Packet Analyzer CLI で、必要な作業を実行します。Packet Analyzer への Telnet または SSH セッションを終了して Cisco IOS CLI に戻るには、ステップ 5 およびステップ 6 を実行します。 | Packet Analyzer CLI コマンドの使用方法については、 |
| ステップ 5 | **exit**<br><br>**例:**<br>`root@localhost(sub-custom-filter-capture)# exit`<br>`root@localhost#` | サブコマンド モードを終了します。<br>• コマンド モードに戻ります。 |
| ステップ 6 | **logout**<br><br>**例:**<br>`root@localhost# logout`<br><br>`Connection closed by foreign host.` | Packet Analyzer システムからログアウトします。 |

## 例

### Packet Analyzer システム IP アドレスを使用した Packet Analyzer への Telnet セッションの開始と終了

```
secpa_host> telnet 172.20.105.215
Trying 172.20.105.215 ...Open

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

login: root
Password: <password>
Terminal type: vt100

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

警告! Default password has not been changed!
root@secpa.company.com#
root@secpa.company.com# logout

[Connection to 172.20.105.215 closed by foreign host]
secpa_host>
```

### Packet Analyzer システム ホスト名を使用した Packet Analyzer への SSH セッションの開始と終了

```
host [/home/user] ssh -l root@namappl
root@namappl's password: <password>
Terminal type: vt100

Cisco Security Packet Analyzer 2400 (SEC-PA-2400-K9) Console, 6.2(2)
Copyright (c) 2012-2016 by Cisco Systems, Inc.

警告! Default password has not been changed!
root@secpa.company.com#
root@secpa.company.com# logout

Connection to secpa closed.
host [/home/user]
```

# CIMC の設定

Cisco Integrated Management Controller（CIMC）は Cisco UCS サーバの組み込み機能であり、リモートでサーバにアクセスし、サーバの設定、管理、モニタリングを行う Web ベース GUI または SSH ベースの CLI を提供します。Cisco Security Packet Analyzer 2400 シリーズ アプライアンスは Cisco UCS サーバ プラットフォームをベースにしているため、CIMC 機能が含まれています。

Packet Analyzer を使用するために必ずしも CIMC を設定する必要はありませんが、特定の管理タスクやトラブルシューティング タスクは CIMC を介してのみ実行できます。したがって、必要に応じてアクセスできるように CIMC に IP アドレスを設定することを強くお勧めします。

CIMC の IP アドレスを設定するには、Cisco Security Packet Analyzer アプライアンスを再起動し、F8 を押してプロンプトが表示されたら「Cisco IMC Configuration Utility」と入力します。[NIC mode] を [Shared LOM] に設定し、適切な IP と VLAN パラメータを設定します。CIMC 設定プロセスの詳細については、『*Cisco UCS C240 M3 Server Installation and Service Guide*』を参照してください。.

また、「M」というラベルの付いた UCS 管理ポートを使用して、専用の CIMC 接続を設定することもできます。

(注)　「M」というラベルが付いた UCS 管理ポートは、Packet Analyzer 管理ポート LAN 1 とは異なります。

# シリアル コンソール接続の設定

Packet Analyzer シリアル コンソールに接続する方法は 2 つあります。

- Serial over LAN（SoL）：CIMC の Web ベース GUI または SSH ベースの CLI を使用した Packet Analyzer シリアル コンソールへのアクセスを許可します。デフォルトでは、このアクセス方式が設定されています。
- 物理外部シリアル コンソール コネクタ（RJ-45）：直接のシリアル ケーブルまたはターミナル サーバを使用した Packet Analyzer シリアル コンソールへのアクセスを許可します。詳細については、外部 RJ-45 ポートを経由するシリアル コンソール アクセスの設定（3-14 ページ）を参照してください。

Packet Analyzer では com0 と com1 の 2 つのシリアル コンソール ポートがサポートされます。これらのポートのどちらを介しても Packet Analyzer CLI にアクセスできます。ただし、ブートアップ プロセスで完全な出力と双方向性を提供するのは、com0 ポートのみです。2 つのシリアル コンソール オプション（SoL または RJ-45 コネクタ）で同時に com0 を使用することはできないため、環境で通常使用するほうに com0 を割り当ててください。Packet Analyzer のデフォルトの設定では、SoL に com0 が割り当てられるため、SoL のアクセス方式を優先使用する場合は、何もする必要はありません。RJ-45 シリアル ポートに com0 を割り当てる場合は、「外部 RJ-45 ポートを経由するシリアル コンソール アクセスの設定」の手順に従います。

## 外部 RJ-45 ポートを経由するシリアル コンソール アクセスの設定

シリアル コネクタ（RJ-45）の位置については、図 5-2 を参照してください。

外部 RJ-45 ポート経由でシリアル コンソール アクセスを設定するには、次の手順に従います。

**ステップ 1**　CIMC GUI にログインします。

**ステップ 2**　[Server] タブをクリックし、[Remote Presence] をクリックします。

**ステップ 3**　[Serial over LAN] タブをクリックします。

**ステップ 4**　Serial over LAN を使用しない場合は、[Enabled] チェックボックスをオフにします。これにより、com0 が割り当てられた RJ-45 ポート経由でシリアル コンソールにアクセスできるようになります。また、主に RJ-45 シリアル コンソールを使用するものの、Packet Analyzer CLI にアクセスする 2 次的な方法として Serial over LAN も維持しておく場合は、Serial over LAN を有効にしたまま、[Com Port] を com1 に変更します。

**ステップ 5**　[Save Changes] ボタンをクリックします。

RJ-45 コンソール ポート経由でのコンソール アクセスが有効になります。コンソールへの接続時に 9600 ボー/bps、8-N-1 を使用するようにターミナル エミュレータまたはターミナル サーバを設定します。

状況によっては、シリアル コンソールが動作するために Packet Analyzer アプライアンスの電源の再投入が必要になることがあります。CIMC GUI から [Server] タブをクリックし、[Summary]、[Power Cycle Server] の順にクリックします。

# アプライアンスのシャットダウンと起動

Cisco Security Packet Analyzer 2400 シリーズ アプライアンスをシャットダウンするには、Packet Analyzer CLI **shutdown** コマンドを実行します。

電源ボタンを押すと Cisco Security Packet Analyzer 2400 シリーズ アプライアンスが再起動します。また、CIMC Web インターフェイスからサーバのスイッチをオンにすることもできます。