デバイスを管理するための準備

Security Manager を使用してデバイスの管理を開始する前に、最低限の設定を行ってデバイスを準備する必要があります。次の各項では、さまざまなトランスポートプロトコルまたはデバイスタイプに必要な基本的なデバイス構成について説明します。

デバイスの通信要件について

Security Manager には、デバイスを管理するための多くの方法が用意されています。最も簡単なのは、Security Manager からデバイスに直接接続する方法です。Security Manager がデバイスにアクセスするのは、インベントリまたはポリシーのディスカバリ中、設定の展開中、または Security Manager でデバイス接続を要求するアクション（接続のテストなど）が行われた場合などです。

オフラインの方法を使用して、Security Manager インベントリにデバイスを追加したり、デバイスに設定変更を展開したりできるため、Security Manager で使用するためにデバイス通信設定を行うかどうかは任意に選択できます。ただし、通常は、オフラインまたはカスタマイズした設定展開ツールを実装するために、デバイスで基本的なデバイス通信設定を行う必要があります。

Security Manager では、特定のタイプのデバイスがデフォルトで使用するトランスポート プロトコルを設定する一方で、別のプロトコルに応答するように設定されたデバイスではそのデフォルトのプロトコルを変更できます。Security Manager は、そのタイプのデバイスで最もよく使用されるプロトコルがデフォルトのプロトコルとして設定されます。あるタイプのデバイスに対するデフォルトのデバイス通信設定を変更するには、[ツール（Tools）]>[Security Manager 管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します（詳細については、[Device Communication] ページを

参照してください）。特定のデバイスに対するトランスポート設定を変更するには、デバイスプロパティの表示または変更の説明に従って、そのデバイス プロパティを変更します。

Security Manager では、次のトランスポート プロトコルを使用できます。

- SSL（HTTPS）：Secure Socket Layer は HTTPS 接続であり、PIX ファイアウォール、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）、および Firewall Services Module（FWSM; ファイアウォール サービス モジュール）で使用される唯一のトランスポート プロトコルです。また、SSL は、Cisco IOS ソフトウェアリリース 12.3 以降を実行しているルータおよび IPS デバイスのデフォルトプロトコルです。

Cisco IOS ルータでトランスポート プロトコルとして SSL を使用する場合、ルータで SSH も設定する必要があります。Security Manager は、SSH 接続を使用して、SSL 展開中にインタラクティブ コマンド展開を処理します。

Cisco Security Manager は、Transport Layer Security（TLS）およびセキュアソケットレイヤ（SSL）プロトコルに OpenSSL を使用していました。バージョン 4.13 以降、Cisco Security Manager は OpenSSL バージョン 1.0.2 を Cisco SSL バージョン 6.x に置き換えました。Cisco SSL は、完全な FIPS 検証による FIPS 準拠を可能にし、高速で費用対効果の高い接続を実現します。Cisco SSL のコモンクライテリアモードにより、コンプライアンスが容易になります。OpenSSL と比較して、Cisco SSL は機能が進んでいます。Cisco SSL の製品セキュリティベースライン（PSB）要件により、ログイン情報とキーの管理、暗号化標準規格、スプーフィング対策機能、整合性と改ざん防止といったセキュリティの重要な側面が保証され、セッション、データ、ストリームの管理と運用が保護対象となります。

SSL の設定方法の詳細については、SSL（HTTPS）の設定 （3 ページ）を参照してください。

- SSH：セキュア シェルは、Catalyst スイッチおよび Catalyst 6500/7600 デバイスのデフォルトのトランスポート プロトコルです。また、Cisco IOS ルータでも SSH を使用できます。

SSH の設定方法の詳細については、SSH の設定 （7 ページ）を参照してください。

- Telnet：Telnet は、Cisco IOS ソフトウェア Release 12.1 および 12.2 を実行しているルータのデフォルト プロトコルです。また、Catalyst スイッチ、Catalyst 6500/7600 デバイス、および、Cisco IOS ソフトウェア Release 12.3 以降を実行しているルータでも Telnet を使用できます。Telnet の設定方法の詳細については、Cisco IOS ソフトウェアのマニュアルを参照してください。
- HTTP：IPS デバイスでは、HTTPS（SSL）の代わりに HTTP を使用できます。いずれのデバイス タイプでも、HTTP はデフォルト プロトコルではありません。
- SQL Anywhere：バージョン 4.20 まで、Security Manager は SQL Anywhere バージョン 12.x をデータベースとして使用していました。バージョン 4.21 以降、Security Manager は Sybase SQL Anywhere バージョン 17.0.10.5855 を使用しています。
- TMS：Token Management Server は、Security Manager でトランスポート プロトコルと同様に処理されますが、実際のトランスポート プロトコルではありません。TMS をルータのトランスポート プロトコルとして設定することにより、設定を TMS に展開するように Security Manager に指示します。TMS から設定を eToken にダウンロードし、その eToken

をルータの USB バスにプラグインして、設定を更新できます。TMS は、Cisco IOS ソフトウェア 12.3 以降を実行している特定のルータでのみ使用可能です。

設定を TMS に展開してルータにダウンロードする方法の詳細については、Token Management Server への設定の展開を参照してください。

また、Security Manager は、間接的な方法を使用して設定をデバイスに展開し、展開を管理するサーバ上の設定をデバイスにステージングすることもできます。さらに、これらの間接的な方法を使用すると、デバイスでダイナミック IP アドレスを使用することもできます。これらの方法はトランスポート プロトコルとしてではなく、デバイスの補助トランスポート プロトコルとして扱われます。次の間接的な方法を使用できます。

- AUS（Auto Update Server）：デバイスを Security Manager に追加するときに、Security Manager を管理している AUS サーバを選択できます。AUS は、PIX ファイアウォールおよび ASA デバイスで使用できます。

AUS サーバを使用するようにデバイスを設定する方法の詳細については、AUS または Configuration Engine の設定 （11 ページ）を参照してください。

- Configuration Engine：ルータを Security Manager に追加するときに、Security Manager を管理している Configuration Engine を選択できます。

Configuration Engine サーバを使用するようにデバイスを設定する方法の詳細については、AUS または Configuration Engine の設定 （11 ページ）を参照してください。

AUS サーバまたは Configuration Engine サーバを使用するデバイスを Security Manager に追加する方法の詳細については、次の項を参照してください。

- デバイス インベントリへのデバイスの追加
- Auto Update Server または Configuration Engine の追加、編集、または削除

SSL（HTTPS）の設定

多くのデバイスでは、デバイスとの通信に Secure Socket Layer（SSL）プロトコルを使用できます。これは HTTPS とも呼ばれます。このプロトコルを使用して設定を展開すると、Security Manager では設定ファイルが暗号化されてからデバイスに送信されます。

ここでは、デバイスで SSL を設定する方法について説明します。

- PIX ファイアウォール、ASA、および FWSM デバイスでの SSL（HTTPS）の設定 （4 ページ）
- Cisco IOS ルータでの SSL の設定 （5 ページ）

PIXファイアウォール、ASA、およびFWSMデバイスでのSSL（HTTPS）の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、PIX ファイアウォール、ASA、および FWSM デバイスでデバイス管理用のトランスポート プロトコルとして SSL を使用する前に実行する必要のあるタスクについて説明します。

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
hostname# config terminal
```

プロンプトに応答します。次にいくつかのヒントを示します。

- インタラクティブプロンプトを使用して事前設定するかを確認するプロンプトが表示されたら、**y** を入力します。
- 現在のイネーブル パスワードを入力します。
- タイム ゾーン、年、月、日、および時間を指定します。
- デバイスが次の場合は、それぞれ次の操作を実行します。
  - 新規のデバイス：ネットワーク インターフェイス IP アドレスと、デバイスの内部 IP アドレスに適用するネットワーク マスクを指定します。
  - 既存のデバイス：インターフェイス IP アドレスおよびマスクが正しいことを確認します。
- デバイスが次の場合は、それぞれ次の操作を実行します。
  - 新規のデバイス：ホスト名およびドメイン名を指定します。
  - 既存のデバイス：ホスト名およびドメイン名が正しいことを確認します。
- PIX Device Manager を実行するホストの IP アドレスの入力を要求された場合、Security Manager サーバの IP アドレスを指定します。
- 前述の変更をフラッシュに書き込むかどうかを確認するプロンプトが表示されたら、**yes** を入力します。

ステップ 2 ASA を設定している場合、ASA がサーバーとして機能するときに使用する SSL/TLS プロトコルのバージョンを指定します。バージョン 4.8 以降、Cisco Security Manager はすべての SSL/TLS プロトコルバージョンをサポートしています。最新の認定バージョンは TLS 1.2 です。

例：

```
hostname(config)# ssl server-version any
```

ステップ 3 HTTP サーバーをイネーブルにします。

例：

```
hostname(config)# http server enable
```

ステップ 4 デバイスとの HTTP 接続を開始することを認可されたホストまたはネットワークを指定します。

例：

```
hostname(config)# http
 ip_address
 [netmask
] [if_name
```

ステップ 5 現在の設定がフラッシュ メモリに保存されます。

例：

```
hostname(config)# write memory
```

ここで、

- ip_address：Cisco Security Manager サーバーの IP アドレス。
- netmask：IP アドレスのネットワークマスク。
- if_name：デバイスのインターフェイス名（デフォルトは **inside**）。このインターフェイスから Cisco Security Manager が HTTP 接続を開始します。

Cisco IOS ルータでの SSL の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、IOS デバイス、および IPS をサポートしますが、拡張機能はサポートしません。

ここでは、Cisco IOS ルータでデバイス管理用のトランスポート プロトコルとして SSL を使用する前に実行する必要のあるタスクについて説明します。

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
hostname# config terminal
```

ステップ 2 デバイスが新規の場合は、ホスト名とドメイン名を設定します。

例：

```
router(config)# hostname
 name

hostname(config)# ip domain-name
 your_domain
```

ステップ 3 レベル 15 の権限を設定します。SSL では、Cisco IOS ルータにログインするためにレベル 15 の権限が必要です。

例：

```
hostname(config)# username
 username
 privilege 15 password 0
 password
```

ステップ 4 ローカル認可または AAA 認可のどちらかをイネーブルにします。

- ローカル認可：認可に AAA を使用しているが、ローカル認可を使用する場合は、次のコマンドを使用して、ログイン時の AAA 認可および AAA 認証をディセーブルにします。list-name は、認可方式のリストに名前を付け、設定したユーザー名を使用してローカル認可をイネーブルにするために使用する文字列です。

例：

```
hostname(config)# no aaa authorization network
 list-name

hostname(config)# no aaa authentication login
 list-name
hostname(config)#ip http authentication local
```

ip http authentication local コマンドを入力しない場合、デフォルトのイネーブルパスワードが認証に使用されます。

- AAA 認可：次のコマンドを使用して、AAA 認証および認可をイネーブルにします。最後の 2 つのコマンドが必要になるのは、複数の AAA リストが定義されている場合だけです。list-name は、認可方式のリストに名前を付けるために使用される文字列です。これらのコマンドによって、HTTPS プロトコルを使用してデバイスに接続しようとするユーザが認証されます。

例：

```
hostname(config)#ip http authentication aaa

hostname(config)#ip http authentication aaa login-authentication
 list-name
hostname(config)# ip http authentication aaa exec-authorization
 list-name
```

ステップ 5 HTTPS サーバーをイネーブルにします。

例：

```
hostname(config)# ip http secure-server
```

ステップ 6 コンフィギュレーション モードを終了し、EXEC モードに戻ります。

例：

```
hostname(config)# exit
```

ステップ 7 デバイスで SSL が設定されていることを確認します。デバイスは「イネーブル」ステータスで応答する必要があります。

例：

```
hostname# show ip http server secure status
```

SSH の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、拡張機能はサポートしていません。

Secure Shell（SSH; セキュア シェル）プロトコルを使用して、Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスと通信できます。このプロトコルにより、セキュアでないチャネルでも強固な認証と安全な通信を確保できます。Security Manager は、SSH バージョン 1.5 と 2 の両方をサポートしています。デバイスに接続されると、Security Manager はどのバージョンを使用するかを決定し、そのバージョンを使用して通信を行います。

ここでは、サポートされているデバイスで SSH を設定する方法について説明します。

SSH の重要な行末端ルール

システム障害を防止するため、SSH では次の行末端ルールに従う必要があります。

- バナーメッセージの行を「#」、「#」、「>」、または「>」で終了しないでください。システムで、バナーメッセージの最後に「#」記号または「>」記号が必要となる場合は、必ずその後に 2 つのスペースを入れてください。

- 「Username:」または「Password:」だけを含むバナーメッセージ行を使用しないでください。
- 「>」または「#」で終わるようにデバイスユーザEXECモードプロンプトをカスタマイズしないてください。

認証のテスト

SSHを設定する前に、SSHなしで認証をテストして、デバイスを認証できることを確認する必要があります。ローカルのユーザ名とパスワードを使用して認証することも、TACACS+ またはRADIUS を実行している認証、許可、アカウンティング（AAA）サーバを使用して認証することもできます。

ここでは、ローカルまたはAAA サーバのユーザ名とパスワードを使用して、SSH なしで認証をテストする方法について説明します。

ステップ1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ2 AAA ステートメントがない場合はローカルのユーザ名とパスワードを使用するように指定します。Cisco IOS ルータで、VTY 行で **aaa new-model** コマンドの代わりに **login local** コマンドを使用できます。

例：

```
hostname(config)#aaa new-model
```

ステップ3 （任意）デバイスのローカル データベース内にユーザ アカウントを設定します。

例：

```
hostname(config)# username
 name
 password 0
 password
```

ステップ4 コンフィギュレーション モードを終了し、EXEC モードに戻ります。

例：

```
hostname(config)# exit
```

ステップ5 設定の変更を保存します。

例：

```
hostname(config)# write memory
```

Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSMおよび IPS をサポートしますが、拡張機能はサポートしません。

ここでは、Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定に必要なタスクについて説明します。

ヒント Security Manager は SSH 接続を使用して SSL 展開中にインタラクティブ コマンド展開を処理するため、Cisco IOS ルータで SSH を設定する必要があります。

関連項目

- SSH の重要な行末端ルール （7 ページ）
- 認証のテスト （8 ページ）
- 非 SSH 接続の禁止（任意） （10 ページ）

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ 2 デバイスが新規の場合は、ホスト名とドメイン名を設定します。

例：

```
router(config)# hostname
 name

hostname(config)# ip domain-name
 your_domain
```

ステップ 3 SSH セッションの RSA キーペアを生成します。デバイスにより係数のサイズの入力を要求されたら、1024 を入力することを推奨します。

例：

```
hostname(config)# crypto key generate rsa
```

ステップ 4 （任意）タイムアウト間隔（分）と再試行回数を設定します。

例：

```
hostname(config)# ip ssh timeout
 time
hostname(config)# ip ssh authentication-retries
 n
```

ステップ 5 コンフィギュレーション モードを終了し、EXEC モードに戻ります。

例：

```
hostname(config)# exit
```

ステップ 6 設定の変更を保存します。

例：

```
hostname# write memory
```

非 SSH 接続の禁止（任意）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、IOS デバイス、および IPS をサポートしますが、拡張機能はサポートしません。

SSH の設定後は、SSH 接続だけを使用するように Cisco IOS ルータ、Catalyst スイッチ、およびCatalyst 6500/7600 デバイスを設定できます。

関連項目

- SSH の重要な行末端ルール （7 ページ）
- 認証のテスト （8 ページ）
- Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定（9 ページ）

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ 2 Telnet アクセス用のルータを設定します。使用できる最初と最後の行番号を指定します（数字の範囲は 0 ～ 1180 で、最後の番号の方が最初の番号よりも大きくなっている必要があります）。

例：

```
hostname(config)# line vty
 first_line last_line
```

ステップ 3 非 SSH 接続（Telnet など）を禁止します。

例：

```
hostname(config-line)# transport input ssh
```

ステップ 4 コンフィギュレーション モードを終了します。

例：

```
hostname(config-line)# end
```

ステップ 5 設定の変更を保存します。

例：

```
hostname# write memory
```

AUS または Configuration Engine の設定

多くのデバイスでは、中間トランスポート サーバを使用して、設定の更新をデバイスにステージングできます。また、このトランスポート サーバを使用すると、静的 IP アドレスではなく、（DHCP サーバを使用して）動的に割り当てられた IP アドレスを使用するデバイスを管理することもできます。トランスポート サーバを使用して設定を展開すると、Security Manager が設定をサーバに展開し、デバイスがサーバから設定を取得します。AUS プロトコルを実行する Auto Update Server を使用することも、CNS プロトコルを実行する Cisco Configuration Engine を使用することもできます。

ここでは、デバイスで AUS または CNS を設定する方法について説明します。

• PIX ファイアウォールおよび ASA デバイスでの AUS の設定 （11 ページ）

PIX ファイアウォールおよび ASA デバイスでの AUS の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

設定およびイメージの更新のために AUS プロトコルを使用して Auto Update Server または CNS Configuration Engine に接続するように、PIX ファイアウォールおよび ASA デバイスを設定できます。Configuration Engine を使用する場合、デバイスは Auto Update Server と同じ AUS プロトコルを使用するため、設定は同じです。AUS/CE 展開の処理に関するエンドツーエンドの説明については、Auto Update Server または CNS Configuration Engine を使用した設定の展開を参照してください。

設定の更新のために AUS/CE サーバに接続する必要があることをデバイスが認識できるように、最初に AUS 設定を行う必要があります。最初の展開後は、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] ポリシーを使用して、これらの設定を変更できます。

ここでは、PIX ファイアウォールおよび ASA デバイスでデバイス管理用のトランスポート プロトコルとして AUS または CNS を使用する前に実行する必要のあるタスクについて説明します。

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ 2 AUS に接続します。Security Manager にログインできるユーザ名とパスワードを指定します。通常、ポート番号は 443 です。

例：

```
hostname(config)# auto-update server https://
username:password@AUSserver_IP_address:port
 /autoupdate/AutoUpdateServlet
```

ステップ 3 AUS のポーリング期間を指定します。

例：

```
hostname(config)# auto-update poll-period
 poll_period
 [retry_count
 ] [retry_period
 ]
```

ここで、

- *poll_period*：2 つの更新の間のポーリング間隔。デフォルトは 720 分（12 時間）です。
- *retry_count*：（任意）サーバー接続試行が失敗した場合に再試行する回数。デフォルトは 0 です。

ステップ 4 指定した固有のデバイス ID を使用して自身を識別するようにデバイスを設定します。

例：

```
hostname(config)# auto-update device-id
 [ hardware-serial | hostname |
ipaddress
 [if_name
 ] |  mac-address
 [if_name
 ] | string
 text
 ]
```

ここで、

- *if_name*：デバイスインターフェイス名（デフォルトは **inside**）。
- *text*：固有の文字列名。

ステップ 5 設定の変更を保存します。

例：

```
hostname# write memory
```

Cisco ASA デバイスでのライセンスの設定

Cisco ASA ソフトウェアを実行するデバイスには、機能のライセンスごとに製品アクティベーション キーが必要です。ボットネット トラフィック フィルタなど、一部のライセンスはオプションであり、使用期間があります。あるモデルでは標準でも、他のモデルではオプションになる機能もあります。たとえば、フェールオーバーのライセンスは、5505 モデルおよび 5510 モデルではオプションになりますが、その他すべてのモデルでは標準です。

Security Manager を使用して ASA ライセンスをインストールおよびアクティブ化できません。代わりに、Adaptive Security Device Manager（ASDM）を使用します。[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [アクティベーション キー（Activation Key）] を選択してアクティベーションキーを入力し、このページのオンライン ヘルプの説明に従います。[Activation Key] ページには、すべての機能のライセンスのステータスも表示されます。ASDM オンライン ヘルプには、ASA ライセンスに関する広範な情報が含まれます。

Security Manager から設定を展開する場合、デバイスには、設定に含まれるすべての機能に対してアクティブなライセンスが必要です。そうでない場合は、展開エラーが表示されます。ほとんどの場合、デバイス上にあるアクティブなライセンスに基づいた、ユーザによる機能の設定を Security Manager が妨げることはありません。たとえば、デバイスのボットネット ライセンスがディセーブルである場合でも、そのデバイスのボットネット トラフィック フィルタリングを設定することはできます。

例外は、5505 モデルおよび 5510 モデル上のフェールオーバー ライセンスです。デバイス上にアクティブなフェールオーバー ライセンスがあるかどうかを示すように設定が可能なデバイス プロパティがあります。ライセンスはフェールオーバーをサポートします。（デバイス ビューで）デバイスをダブルクリックして [Device Properties] ページを開き、このプロパティを設定できます。このオプションは [General] タブ（[デバイスのプロパティ（Device Properties）]：[全般（General）]ページを参照）にあります。デバイス上のポリシーを検出する場合、たとえば、[Add Device From Network] オプションまたは [Add Device from File]（設定ファイルではなくインベントリ ファイルから）オプションを使用してデバイスをインベントリに追加するときなど、Security Manager は、フェールオーバー ライセンスのステータスを判断し、プロパティを適切に設定します。プロパティが正しく維持されていることを確認する必要があります。プロパティが選択されても、デバイスに非アクティブのフェールオーバー ライセンスがある場合は、展開に失敗します。

ヒント [New Device] オプションまたは [Configuration File] オプションを使用してデバイスを追加する場合は、License Supports Failover プロパティは、デバイス プロパティに設定されるのを待つ代わりに、デバイスの追加時に設定できます。

Cisco IOS デバイスでのライセンスの設定

Cisco IOS ソフトウェアを実行するデバイスには、さまざまな機能（セキュリティ機能など）のライセンス ファイルが必要です。これらのライセンス（securityk9 パッケージなど）がデバイスにインストールされていない場合、Security Manager は、特定のライセンス レベルを必要とするコマンドを設定できません。この場合、ライセンスされていないデバイスにポリシーを展開しようとすると、展開が失敗します。

Security Manager を使用して、IPS ライセンスを展開および管理できますが、それ以外のタイプのライセンスは展開および管理できません。コマンドライン インターフェイスを使用して、デバイスで直接これらのライセンスを設定するか、Cisco License Manager を使用します。次に、ライセンスを設定するための一般的なプロセスを示します。ライセンスの設定方法の詳細については、Cisco.com の『Cisco IOS Software Activation Command Guide』および『Cisco IOS Software Activation Command Reference』を参照してください。

1. 使用する機能に必要なライセンスを取得します。または、一部のデバイスに付属の評価版ライセンスを使用できます。**show license all** コマンドを使用すると、使用可能なライセンスが表示されます。
2. 購入したライセンスをデバイス上のフラッシュ ストレージにコピーするか、TFTP サーバに配置します。たとえば、ライセンスを TFTP サーバーに配置し、**copy tftp flash0:** コマンドを使用してファイルを flash0 ストレージエリアにコピーします。
3. **license install** コマンドを使用して、購入した各ライセンスをインストールします。次に例を示します。

license install flash0:uc-base-CISCO2951-FHH1216P06Z.xml

一部のライセンスでは、ライセンス契約書を読んで合意するように要求されます。

評価ライセンスを使用する場合は、**license boot** コマンドを使用してライセンスを有効にしてから、デバイスをリロードします。エンドユーザ ライセンス契約書に合意しないと、Security Manager はデバイスに設定を展開できません。

- **show version**、**show license feature**、および **show license all** コマンドを使用して、インストールされたライセンスを確認できます。

IPS デバイスの初期化

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

IPS デバイスを初期化するには、次の設定を行う必要があります。次の設定はネットワーク設定であり、IPS デバイスの管理者権限を持つユーザだけが設定できます。

- センサー名
- IP アドレス
- ネットマスク
- デフォルト ルート（Default route）
- TLS/SSL の有効化（デバイスで Web サーバの TLS/SSL をイネーブルにするため）
- Web サーバのポート
- デフォルト ポートの使用

これらの設定は、IPS デバイスで使用されているプラットフォームに応じて、Intrusion Prevention System Device Manager（IDM）またはコマンドラインセッションで **setup** コマンドを使用して設定します。サポートされている IPS プラットフォームのリストについては、次の URL で、サポートされているデバイスおよびソフトウェアバージョンの情報を参照してください：
http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html

これらの設定の詳細については、IPS デバイスの技術マニュアルを参照してください。

（注） IOS IPS デバイスの使用準備に関する詳細については、Cisco IOS IPS ルータでの最初の準備を参照してください。

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。