CHAPTER 18

センサーの管理

(注) IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

(注) IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、パスワードの設定、ライセンス キーの取得とインストール、IP ロギング変数の設定、最新ソフトウェアによるセンサーのアップデート、センサー デフォルトの復元、センサーのリブート、センサーのシャットダウンなど、センサーの管理方法について説明します。この章は、次の内容で構成されています。

パスワードの設定

ここでは、センサーのユーザのパスワードを設定する方法について説明します。内容は次のとおりです。

[Passwords] ペイン

センサーの管理者は、[Passwords] ペインでパスワードの作成方法を設定できます。ユーザが作成するパスワードはすべて、[Passwords] ペインで設定されたポリシーに従う必要があります。

注意　パスワード ポリシーに、大文字や数字などの文字セットの最小文字数を含める場合、必須文字セットの最小文字数の合計は最小パスワード サイズを超えることはできません。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。

[Passwords] ペインのフィールド定義

[Passwords] ペインには次のフィールドがあります。

- [Attempt Limit]：ユーザがある回数ログインに失敗したら、それ以上続けられないようにアカウントをロックできます。デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。
- [Size Range]：パスワードに許容される最小サイズと最大サイズに指定する範囲。有効な範囲は 6 ～ 64 文字です。
- [Minimum Digit Characters]：ユーザが指定するパスワードには、この数以上の数字が含まれている必要があります。
- [Minimum Upper Case Characters]：ユーザが指定するパスワードに含むことができる大文字のアルファベットの数の上限です。
- [Minimum Lower Case Characters]：ユーザが指定するパスワードには、この数以上の小文字のアルファベット文字が含まれている必要があります。
- [Minimum Other Characters]：ユーザが指定するパスワードには、この数以上のアルファベット以外の印刷可能文字が含まれている必要があります。
- [Number of Historical Passwords]：アカウントごとにセンサーで記憶させる履歴パスワードの数。新しいパスワードが記憶されているいずれかのパスワードと一致した場合は、アカウントのパスワードの変更試行に失敗します。この値が 0 の場合、以前のパスワードは記憶されません。

詳細情報

さまざまなセンサーでパスワードを回復する手順については、「パスワードの回復」（P.18-3）を参照してください。

パスワード要件の設定

パスワード要件を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Passwords] を選択します。

ステップ 3　[Attempt Limit] フィールドに、ユーザが正しいパスワードを入力するまで試行できる回数を入力します。デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。

ステップ 4　[Size Range] フィールドに、パスワードに許容される長さを入力します。有効な範囲は 6 ～ 64 です。

ステップ 5　[Minimum Digit Characters] フィールドに、パスワードに入力できる数字の数の最小値を入力します。

ステップ 6　[Minimum Upper Case Characters] フィールドに、パスワードに入力できる大文字の数の最小値を入力します。

ステップ 7　[Minimum Lower Case Characters] フィールドに、パスワードに入力できる小文字の数の最小値を入力します。

注意　パスワード ポリシーに、大文字や数字などの文字セットの最小文字数を含める場合、必須文字セットの最小文字数の合計は最小パスワード サイズを超えることはできません。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。

ステップ 8　[Minimum Other Characters] フィールドに、パスワードに入力できるその他の文字数の最小値を入力します。

ステップ 9　[Number of Historical Passwords] フィールドに、アカウントごとにセンサーで記憶させる履歴パスワードの数を入力します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 10　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

パスワードの回復

ほとんどの IPS プラットフォームでは、サービス アカウントを使用したり、センサーのイメージを再作成したりせずに、センサー上でパスワードを回復できるようになりました。ここでは、さまざまなプラットフォームでパスワードを回復する方法について説明します。内容は次のとおりです。

パスワードの回復について

パスワード回復の実装は、IPS プラットフォームの要件によって異なります。パスワードの回復は、cisco 管理者アカウントに対してのみ実装され、デフォルトでイネーブルになっています。IPS 管理者は、その後 CLI を使用して他のアカウントのユーザ パスワードを回復できます。シスコのユーザ パスワードは **cisco** に戻るため、次回ログイン後に変更する必要があります。

（注）　管理者は、セキュリティ上の理由から、パスワードの回復機能をディセーブルにしなければならない場合があります。

表 18-1 に、プラットフォーム別のパスワード回復方法を示します。

表 18-1　プラットフォーム別のパスワード回復方法

プラットフォーム	説明	回復方法
4200 シリーズ センサー	スタンドアロン IPS アプライアンス	GRUB プロンプトまたは ROMMON
AIM IPS NME IPS	ルータ IPS モジュール	ブートローダ コマンド
AIP SSM AIP SSC-5 IPS SSP	ASA 5500 シリーズ適応型セキュリティ アプライアンス モジュール	適応型セキュリティ アプライアンス の CLI コマンド
IDSM2	スイッチ IPS モジュール	メンテナンス パーティションからイメージをダウンロード

詳細情報

パスワード回復をディセーブルにする手順については、「パスワード回復のディセーブル化」（P.18-9）を参照してください。

アプライアンスのパスワードの回復

アプライアンスのパスワードを回復するには、GRUB メニューを使用する方法と ROMMON を使用する方法があります。ここでは、アプライアンスでパスワードを回復する方法について説明します。内容は次のとおりです。

- 「GRUB メニューの使用」（P.18-4）
- 「ROMMON の使用」（P.18-5）

GRUB メニューの使用

4200 シリーズのアプライアンスでは、パスワードの回復には、ブートアップ中に表示される GRUB メニューを使用します。GRUB メニューが表示されたら、任意のキーを押してブート プロセスを停止します。

（注）　GRUB メニューを使用してパスワードを回復するには、ターミナル サーバを使用するか、アプライアンスとの直接シリアル接続が必要です。

アプライアンスでパスワードを回復するには、次の手順を実行します。

ステップ 1　アプライアンスをリブートして、GRUB メニューを表示します。

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
------------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
```

```
2: Cisco IPS Clear Password (cisco)
-----------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

ステップ 2　任意のキーを押して、ブート プロセスを停止します。

ステップ 3　[2: Cisco IPS Clear Password (cisco)] を選択します。

パスワードが **cisco** にリセットされます。次に CLI にログインするときにパスワードを変更できます。

詳細情報

アプライアンスをターミナル サーバに接続する手順については、「ターミナル サーバへの接続」（P.C-23）を参照してください。

ROMMON の使用

IPS 4240 と IPS 4255 については、ROMMON を使用してパスワードを回復できます。ROMMON CLI にアクセスするには、ターミナル サーバまたは直接接続からセンサーをリブートして、ブート プロセスを中断します。

ROMMON CLI を使用してパスワードを回復するには、次の手順を実行します。

ステップ 1　アプライアンスをリブートします。

ステップ 2　ブート プロセスを中断するには、**ESC** または **Control-R**（ターミナル サーバ）を押すか、**BREAK** コマンドを送信します（直接接続）。

ブート コードによって 10 秒間停止するか、次のようなメッセージが表示されます。

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

ステップ 3　次のコマンドを入力してパスワードをリセットします。

```
confreg 0x7
boot
```

サンプル ROMMON セッション：

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
```

```
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

詳細情報

アプライアンスをターミナル サーバに接続する手順については、「ターミナル サーバへの接続」（P.C-23）を参照してください。

AIM IPS パスワードの回復

AIM IPS のパスワードを回復するには、**clear password** コマンドを使用します。AIM IPS へのコンソール アクセスとルータへの管理者アクセス権が必要です。

AIM IPS のパスワードを回復するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

ステップ 4　AIM IPS との間にセッションを確立します。

```
router# service-module ids-sensor slot/port session
```

例

```
router# service-module ids-sensor 0/0 session
```

ステップ 5　**Control-shift-6** のあとで **x** を押して、ルータ CLI に移動します。

ステップ 6　ルータ コンソールから AIM-IPS をリセットします。

```
router# service-module ids-sensor 0/0 reset
```

ステップ 7　**Enter** を押して、ルータ コンソールに戻ります。

ステップ 8　ブート オプションのプロンプトが表示されたら、素早く ******* を入力します。ブートローダが起動されます。

ステップ 9　パスワードをクリアします。

```
ServicesEngine boot-loader# clear password
```

AIM IPS がリブートします。パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

ASA モジュールのパスワードの回復

CLI または ASDM を使用して AIP SSM、AIP SSC-5、および IPS SSP のパスワードをデフォルト（**cisco**）にリセットできます。パスワードをリセットすると、ASA モジュールはリブートされます。リブート中、IPS サービスは利用できません。

（注） AIP SSM のパスワードをリセットするには、ASA 7.2.(2) 以降が必要です。AIP SSC-5 のパスワードをリセットするには、ASA 8.2.(1) 以降が必要です。IPS SSP のパスワードをリセットするには、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降が必要です。ASA 8.3(*x*) ではサポートされていません。

hw-module module *slot_number* **password-reset** コマンドを使用して、パスワードをデフォルトの **cisco** にリセットします。ASA 5500 シリーズの適応型セキュリティ アプライアンスは、ROMMON の confreg ビットを 0x7 に設定し、モジュールをリブートします。ROMMON ビットによって、GRUB メニューのデフォルトがオプション 2（[reset password]）に設定されます。

指定されたスロットのモジュールにパスワードの回復をサポートしない IPS バージョンがある場合、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーで、[Tools] > [IPS Password Reset] を選択します。

（注） IPS モジュールがインストールされていない場合、このオプションはメニューに表示されません。

ステップ 2　[IPS Password Reset] 確認ダイアログボックスで [OK] をクリックして、パスワードをデフォルト（**cisco**）にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。リセットが失敗した場合は、ソフトウェア バージョンが正しいことを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。ASA モジュールがリブートされます。

IDSM2 パスワードの回復

IDSM2 のパスワードを回復するには、特別なパスワード回復イメージ ファイルをインストールする必要があります。このインストールでは、パスワードだけがリセットされ、他のすべての情報は影響を受けません。パスワード回復イメージはバージョンに依存し、Cisco Download Software サイトから入手できます。IPS 6.*x* の場合は、WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz をダウンロードします。IPS 7.*x* の場合は、WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz をダウンロードします。

イメージのインストールにサポートされているプロトコルは FTP だけなので、必ずスイッチがアクセスできる FTP サーバにパスワード回復イメージを置いてください。IDSM2 でパスワードを回復するには、Cisco 6500 シリーズ スイッチへの管理者アクセス権が必要です。

パスワード回復イメージのインストール中に次のメッセージが表示されます。

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

このメッセージはエラーです。パスワード回復イメージをインストールしても設定は削除されません。ログイン アカウントがリセットされるだけです。

パスワード回復イメージ ファイルをダウンロードしたら、システム イメージ ファイルのインストール手順を実行します。ただし、システム イメージ ファイルの代わりにパスワード回復イメージ ファイルを使用します。イメージ回復ファイルのインストール後、IDSM2 はプライマリ パーティションにリブートされます。そのようにリブートされない場合は、スイッチから次のコマンドを入力します。

```
hw-module module module_number reset hdd:1
```

（注）　パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

詳細情報

システム イメージ ファイルのインストール手順を使用して IDSM2 パスワード回復ファイルをインストールする手順については、「IDSM2 システム イメージのインストール」（P.25-29）を参照してください。

NME IPS パスワードの回復

NME IPS のパスワードを回復するには、**clear password** コマンドを使用します。NME IPS へのコンソール アクセスとルータへの管理者アクセス権が必要です。

NME IPS のパスワードを回復するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

ステップ 4　NME IPS との間にセッションを確立します。

```
router# service-module ids-sensor slot/port session
```

例

```
router# service-module ids-sensor 1/0 session
```

ステップ 5　**Control-shift-6** のあとで **x** を押して、ルータ CLI に移動します。

ステップ 6　ルータ コンソールから NME IPS をリセットします。

```
router# service-module ids-sensor 1/0 reset
```

ステップ 7　**Enter** を押して、ルータ コンソールに戻ります。

ステップ 8　ブート オプションのプロンプトが表示されたら、素早く ******* を入力します。ブートローダが起動されます。

ステップ 9　パスワードをクリアします。

```
ServicesEngine boot-loader# clear password
```

NME IPS がリブートします。パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

パスワード回復のディセーブル化

注意　パスワード回復がディセーブルになっているセンサーでパスワードを回復しようとすると、エラーや警告が表示されずにプロセスは進みますが、パスワードはリセットされません。パスワードを忘れたためにセンサーにログインできないときに、パスワード回復がディセーブルに設定されている場合は、センサーのイメージを再作成する必要があります。

パスワードの回復は、デフォルトでイネーブルです。パスワード回復は、CLI または MIE からディセーブルにすることができます。

CLI でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　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。

```
sensor# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
sensor(config)# service host
```

ステップ 4　パスワード回復をディセーブルにします。

```
sensor(config-hos)# password-recovery disallowed
```

IME でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Network] を選択します。

ステップ 3　パスワード回復をディセーブルにするには、[Allow Password Recovery] チェックボックスをオフにします。

パスワード回復のトラブルシューティング

パスワード回復のトラブルシューティングを行う場合は、次の点に注意してください。

- ROMMON プロンプト、GRUB メニュー、スイッチの CLI、ルータの CLI からは、パスワード回復がセンサーの設定でディセーブルになっているかどうかを確認できません。パスワード回復を試みると、常に成功したように見えます。ディセーブルになっている場合、パスワードは **cisco** にリセットされません。唯一のオプションはセンサーのイメージの再作成です。
- パスワード回復は、ホストの設定でディセーブルにすることができます。AIM IPS や NME IPS ブートローダ、ROMMON、IDSM2 のメンテナンス パーティションなどの外部メカニズムを使用しているプラットフォームの場合、パスワードをクリアするコマンドを実行できますが、IPS でパスワード回復がディセーブルになっている場合、IPS はパスワード回復が許可されていないことを検出し、外部要求を拒否します。
- パスワード回復の状態をチェックするには、**show settings | include password** コマンドを使用します。
- IDSM2 でパスワード回復を実行すると、「`Upgrading will wipe out the contents on the storage media.`」というメッセージが表示されます。このメッセージは無視できます。指定されたパスワード回復イメージを使用すると、パスワードだけがリセットされます。

パスワード回復の状態の確認

パスワード回復がイネーブルになっているかどうかを確認するには、**show settings | include password** コマンドを使用します。

パスワード回復がイネーブルになっているかどうかを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　サービス ホスト サブモードを開始します。

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタ処理された出力で設定を表示し、パスワード回復の状態を確認します。

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

ライセンスの設定

ここでは、ライセンス キーの取得およびインストール方法について説明します。内容は次のとおりです。

[Licensing] ペイン

（注）　[Licensing] ペインにライセンス情報を表示し、センサーのライセンス キーをインストールするには、管理者である必要があります。

[Licensing] ペインで、センサーのライセンス キーを取得し、インストールできます。[Licensing] ペインには、現在のライセンスのステータスが表示されます。

ライセンスについて

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

ライセンス キーがなくてもセンサーは機能しますが、シグニチャのアップデートを取得する場合とグローバル相関機能を使用する場合はライセンス キーが必要です。ライセンス キーを取得するには、次のものが必要です。

- Cisco Service for IPS サービス契約：代理店、シスコ サービスまたは製品のセールスにお問い合わせの上、契約を購入してください。
- IPS デバイスのシリアル番号：IME で IPS デバイスのシリアル番号を確認するには、[Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。または、CLI で **show version** コマンドを使用します。
- 有効な Cisco.com ユーザ名およびパスワード

トライアル ライセンス キーも使用できます。契約上の問題によってセンサーのライセンスを取得できない場合は、ライセンスが必要なシグニチャのアップデートをサポートする 60 日間のトライアル ライセンスを取得できます。

Cisco.com ライセンス サーバからライセンス キーを取得できます。キーはその後センサーに配信されます。または、ローカル ファイルで提供されたライセンス キーからライセンス キーを更新できます。http://www.cisco.com/go/license にアクセスし、[IPS Signature Subscription Service] をクリックして、ライセンス キーを申し込みます。

次の場所で、ライセンス キーのステータスを表示できます。

- IME ホームページの [Licensing] タブの [Device Details] セクション
- CLI ログインのライセンスのお知らせ

IME または CLI を起動すると、トライアル、無効、有効期限切れなど、ライセンス キーのステータスが通知されます。ライセンス キーがない場合、ライセンス キーが無効または有効期限切れの場合、IME および CLI は引き続き使用できますが、シグニチャのアップデートをダウンロードすることはできません。

センサーに有効なライセンスがある場合は、[License] ペインの [Download] をクリックして、IME が動作しているコンピュータにライセンス キーのコピーをダウンロードして、ローカル ファイルに保存できます。その後、紛失したライセンスまたは破損したライセンスを置き換えるか、センサーのイメージの再作成後にライセンスを再インストールできます。

IPS 製品のサービス プログラム

ライセンス キーをダウンロードし、最新の IPS シグニチャのアップデートを取得するには、IPS 製品の Cisco Services for IPS サービス契約が必要です。シスコと直接取引がある場合は、アカウント マネージャまたはサービス アカウント マネージャにお問い合わせのうえ、Cisco Services for IPS サービス契約を購入してください。シスコと直接取引がない場合は、第 1 層または第 2 層パートナーからサービス アカウントを購入できます。

次の IPS 製品を購入する場合は、Cisco Services for IPS サービス契約も購入する必要があります。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

IPS を搭載していない ASA 5500 シリーズの適応型セキュリティ アプライアンス製品を購入する場合は、SMARTnet 契約を購入する必要があります。

（注） SMARTnet は、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、サイトでのハードウェア交換 NBD を提供します。

AIP SSM、IPS SSP、または AIP SSC-5 がインストールされた ASA 5500 シリーズの適応型セキュリティ アプライアンス製品を購入した場合、または ASA 5500 シリーズの適応型セキュリティ アプライアンス製品に追加するようにこれらを購入した場合、Cisco Services for IPS サービス契約を購入する必要があります。

（注） Cisco Services for IPS は、IPS シグニチャのアップデート、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、サイトでのハードウェア交換 NBD を提供します。

たとえば、ASA 5585-X を購入し、その後 IPS が必要となり ASA-IPS10-K9 を購入した場合、Cisco Services for IPS サービス契約を購入する必要があります。Cisco Services for IPS サービス契約の購入後、ライセンス キーを申請するための製品シリアル番号も必要になります。

注意 製品を RMA のために送付した場合、シリアル番号が変わります。そのときは、新しいシリアル番号用に新しいライセンス キーを取得する必要があります。

[Licensing] ペインのフィールド定義

[Licensing] ペインには次のフィールドがあります。

- [Current License]：現在のライセンスのステータスを提供します。
  - [License Status]：センサーの現在のライセンス ステータス。

  - [Expiration Date]：ライセンス キーの有効期限が切れる（または切れた）日付。キーが無効の場合、日付は表示されません。
  - [Serial Number]：センサーのシリアル番号。
  - [Product ID]：センサーの製品 ID。
- [Update License]：新しいライセンス キーの入手先を指定します。
  - [Cisco.com]：Cisco.com のライセンス サーバにライセンス キーを問い合わせます。
  - [License File]：ライセンス ファイルを使用するように指定します。
  - [Local File Path]：ライセンス キーを含むローカル ファイルの場所を示します。

ライセンス キーの取得とインストール

（注） 有効な Cisco.com ユーザ名とパスワードのほかに、ライセンス キーを申請するには、その前に Cisco Services for IPS サービス契約を購入する必要があります。

ライセンス キーを取得およびインストールするには、次の手順に従ってください。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。[Licensing] ペインには、現在のライセンスのステータスが表示されます。ライセンスをすでにインストールした場合は、必要に応じて、[Download] をクリックして保存できます。

ステップ 3　次のいずれかの方法でライセンス キーを取得します。

- [Cisco.com] オプション ボタンをクリックして、Cisco.com からライセンスを取得します。IME が Cisco.com のライセンス サーバにアクセスし、サーバにシリアル番号を送信して、ライセンス キーを取得します。これがデフォルトの方法です。ステップ 4 に進みます。
- [License File] オプション ボタンをクリックして、ライセンス ファイルを使用します。このオプションを使用するには、URL www.cisco.com/go/license にアクセスして、ライセンス キーを申請する必要があります。ライセンス キーが電子メールで送信されます。そのメールを IME がアクセスできるドライブに保存します。このオプションは、コンピュータから Cisco.com にアクセスできない場合に便利です。ステップ 7 に進みます。

ステップ 4　[Update License] をクリックし、[Licensing] ダイアログボックスで [Yes] をクリックして、続行します。[Status] ダイアログボックスに、センサーが Cisco.com に接続しようとしていることを伝えるメッセージが表示されます。情報ダイアログボックスにライセンス キーが更新されたことを伝えるメッセージが表示されます。

ステップ 5　[OK] をクリックします。

ステップ 6　www.cisco.com/go/license にアクセスします。

ステップ 7　必須フィールドに入力します。ライセンス キーが、指定された電子メール アドレスに送信されます。

注意　ライセンス キーは指定されたシリアル番号のデバイスでのみ機能するので、IPS デバイスの正しいシリアル番号が必要です。

ステップ 8　ライセンス キーを、ハードディスク ドライブまたは IME を実行するクライアントがアクセスできるネットワーク ドライブに保存します。

ステップ 9　IME にログインします。

ステップ 10　[Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。

ステップ 11　[Update License] で [License File] オプション ボタンをクリックします。

ステップ 12　[Local File Path] フィールドでライセンス ファイルへのパスを指定するか、[Browse Local] をクリックして、ファイルを検索します。

ステップ 13　ライセンス ファイルを検索し、[Open] をクリックします。

ステップ 14　[Update License] をクリックします。

センサーのヘルスの設定

ここでは、センサーのヘルスのメトリックの設定方法について説明します。内容は次のとおりです。

[Sensor Health] ペイン

（注）　センサーのヘルスのメトリックを設定するには、管理者である必要があります。

[Sensor Health] ペインで、IPS のヘルスとネットワーク セキュリティのステータスを判断するために使用されるメトリックを設定できます。さまざまなガジェットの [Home] ペインに結果が表示されます。

チェックボックスをオンにせずにメトリックを選択しない場合、ヘルスとネットワーク セキュリティ ステータスの結果に表示されません。デフォルト設定を受け入れるか、値を編集できます。

全体的なヘルスは、メトリックの中で最も重大な設定値に設定されます。たとえば、選択されたすメトリックで、赤いメトリックが 1 つある以外はすべて緑の場合、全体的なヘルスは赤になります。IPS は、IPS の全体的なヘルス ステータスが変化すると、ヘルスおよびセキュリティ ステータス イベントを生成します。

センサーのセキュリティ ステータスは、仮想センサーによって検出されたイベントの脅威レーティングを使用して、仮想センサーごとに決定されます。仮想センサーのセキュリティ ステータスは、仮想センサーがそのセンサーのしきい値を超える脅威レーティングのイベントを検出すると発生します。しきい値を超えると、セキュリティ ステータスは、設定された時間内に、それ以上のイベントが高いレベルで検出されなくなるまで、重大レベルのままです。

[Sensor Health] ペインのフィールド定義

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

[Sensor Health] ペインには次のフィールドがあります。

- [Inspection Load]：検査負荷のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [Missed Packet]：失われたパケットのしきい値のパーセントと、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [Memory Usage]：メモリ使用量のしきい値のパーセントと、このメトリックがセンサーの全体的なヘルス レーティングに適用されるかどうかを設定できます。
- [Signature Update]：最後のシグニチャのアップデートが適用された時間のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [License Expiration]：ライセンスの有効期限のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [Event Retrieval]：最後にイベントが取得された時間のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。

（注） イベント取得メトリックでは、IME などの外部モニタリング アプリケーションによって最後のイベントが取得された時間が記録されます。外部イベント モニタリングを行っていない場合は、[Event Retrieval] をディセーブルにしてください。

- [Network Participation]：ネットワーク参加ヘルス メトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [Global Correlation]：グローバル相関ヘルス メトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [Application Failure]：アプリケーション障害をセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [IPS in Bypass Mode]：バイパス モードがアクティブかどうかを認識し、それをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。

（注） IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

- [One or More Active Interfaces Down]：1 つ以上のインターフェイスがダウンしているかどうかを認識し、それをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [Yellow Threshold]：黄色の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。
- [Red Threshold]：赤の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。

詳細情報

- IME ガジェットの詳細については、「IME ガジェット」（P.3-2）を参照してください。
- IME の [Home] ペインの説明については、「IME の [Home] ペイン」（P.1-3）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」を参照してください。

IP ロギング変数の設定

（注）　IP ロギング変数を設定するには、管理者である必要があります。

IP ロギング変数の Maximum Open IP Log Files を設定できます。これは、センサーの一般的な操作に適用されます。

フィールド定義

[Global Variables] ペインには、次のフィールドがあります。

- [Maximum Open IP Log Files] : 同時に開いている IP ログ ファイルの最大数。有効な範囲は 20 ～ 100 です。デフォルトは 20 です。

自動アップデートの設定

ここでは、ソフトウェアの自動アップデートを行うようにセンサーを設定する方法について説明します。内容は次のとおりです。

[Auto/Cisco.com Update] ペイン

（注）　[Auto Update] ペインを表示して、自動アップデートを設定するには、管理者である必要があります。

注意　自動アップデートは、DOS スタイルのパスで設定された Windows FTP サーバでは動作しません。サーバが DOS スタイルのパスではなく、UNIX スタイルのパス オプションで設定されていることを確認してください。

Cisco.com およびローカル サーバからシグニチャのアップデートとシグニチャ エンジンのアップデートを自動的にダウンロードするようにセンサーを設定できます。自動アップデートをイネーブルにすると、センサーは Cisco.com にログインし、シグニチャ アップデートとシグニチャ エンジン アップデートをチェックします。アップデートが入手可能な場合、センサーはアップデートをダウンロードして、インストールします。Cisco.com から Cisco IPS シグニチャのアップデートおよびシグニチャ エンジンのアップデートをダウンロードするには、暗号化特権を持つ Cisco.com ユーザ アカウントが必要です。初めてシスコ ソフトウェアをダウンロードするときに、暗号化特権を持つアカウントを設定します。

注意　センサーは、非透過プロキシ サーバからの Cisco.com との通信をサポートしていません。

詳細情報

ソフトウェアおよび暗号化特権を持つアカウントの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

サポートされる FTP および HTTP サーバ

IPS ソフトウェアのアップデートについてサポートされている FTP サーバは次のとおりです。

- WU-FTPD 2.6.2（Linux）
- Solaris 2.8
- Sambar 6.0（Windows 2000）
- Serv-U 5.0（Windows 2000）
- MS IIS 5.0（Windows 2000）

IPS ソフトウェアのアップデートについてサポートされている HTTP/HTTPS サーバは次のとおりです。

- CSM - Apache Server（Tomcat）
- CSM - Apache Server（JRun）

UNIX スタイルのディレクトリ リスト表示

FTP サーバを使用して自動アップデートを設定するには、FTP サーバは UNIX スタイルのディレクトリ リスト表示応答を提供する必要があります。MS-DOS スタイルのディレクトリ リスト表示は、センサーの自動アップデート機能ではサポートされていません。

（注） サーバが MS-DOS スタイルのディレクトリ リスト表示を提供している場合、センサーはディレクトリ リスト表示を解析できず、入手可能な新しいアップデートがあるかどうかを判断できません。

Microsoft IIS で UNIX スタイルのディレクトリ リスト表示を使用するには、次の手順を使用します。

ステップ 1　[Start] > [Program Files] > [Administrative Tools] を選択します。

ステップ 2　[Home Directory] タブをクリックします。

ステップ 3　[UNIX directory listings style] オプション ボタンをクリックします。

シグニチャのアップデートおよびインストール時間

シグニチャのアップデートの実行中、短時間トラフィックが検査されない時間があります。ただし、バイパスをイネーブルにしている場合、トラフィックは引き続き通過します。

シグニチャのアップデートによって正規表現を含むシグニチャが追加または変更される場合、SensorApp で使用される正規表現キャッシュ テーブルを再コンパイルする必要があります。再コンパイル時間はプラットフォーム、変更または追加されたシグニチャの数、および変更または追加されたシグニチャのタイプによって異なります。

シグニチャのアップデートで、IPS 4255 や IPS 4260 などのハイエンド プラットフォームで 1 つまたは 2 つの新しいシグニチャが追加されただけの場合、再コンパイルはほんの数秒で終了します。

次の条件では、再コンパイルに数分、最大で 30 分かかります。

- 大量のシグニチャを追加する場合。たとえば、シグニチャのアップデートで、S240 の上に S258 をインストールするなど、複数のシグニチャ レベルをスキップして新しいシグニチャをインストールする場合。
- 大量のシグニチャを変更する場合。たとえば、シグニチャのアップデートで、大量の古いシグニチャをディセーブルまたは非アクティブにする場合。

再コンパイル中、SensorApp はパケットのモニタリングを停止します。パケット バッファが SensorApp への途中で蓄積し始めると、インターフェイス ドライバはそれを検出し、SensorApp からのパケットの受信を停止します。センサーがインライン モードで、バイパス オプションが [Auto] に設定されている場合、ドライバはバイパスをオンにします。バイパスが [Off] に設定されている場合、ドライバはインターフェイス リンクを切断します。

（注）　バイパス設定が動作し始める前に、一部のパケットがドロップされる可能性があります。SensorApp は、正規表現キャッシュ ファイルの再コンパイルを完了すると、ドライバと再接続し、モニタリングを再開します。ドライバは解析のために SensorApp にパケットの受け渡しを開始し、必要に応じて、インターフェイス リンクをアップさせます。

詳細情報

バイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

[Auto/Cisco.com Update] ペインのフィールド定義

[Auto/Cisco.com Update] ペインには次のフィールドがあります。

- [Enable Auto Update From a Remote Server]：センサーはリモート サーバに格納されたアップデートをインストールできます。

  （注）　[Enable Auto Update From a Remote Server] がオフの場合、すべてのフィールドはディセーブルとなり、クリアされます。このオンとオフを切り替えると、他のすべての設定が失われます。

- [Remote Server Settings]：リモート サーバ用に次のオプションを指定できます。
  - [IP Address]：リモート サーバの IP アドレスを示します。
  - [File Copy Protocol]：FTP または SCP のどちらを使用するかを指定します。
  - [Directory]：リモート サーバ上のアップデートへのパスを示します。
  - [Username]：リモート サーバのユーザ アカウントに対応するユーザ名を示します。
  - [Password]：リモート サーバのユーザ アカウントのパスワードを示します。
  - [Confirm Password]：リモート サーバのパスワードの再入力を強制することで、パスワードを確定します。
- [Enable Signature and Engine Updates from Cisco.com]：センサーが Cisco.com にアクセスして、シグニチャのアップデートとエンジンのアップデートをダウンロードできるようにします。
- [Cisco.com Server Settings]：Cisco.com サーバ用の次のオプションを指定できます。

  - [Username]：Cisco.com 上のユーザ アカウントに対応するユーザ名を示します。
  - [Cisco.com URL]：[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにした場合、正しい URL が自動的に入力されます。
  - [Password]：Cisco.com 上のユーザ アカウントのパスワードを示します。
  - [Confirm Password]：Cisco.com のパスワードの再入力を強制することで、パスワードを確定します。
- [Schedule]：次のスケジュール オプションを指定できます。
  - [Start Time]：アップデート プロセスの開始時間を示します。これは、センサーがリモート サーバにアクセスし、使用可能なアップデートを検索する時間です。
  - [Frequency]：時間または週単位のどちらでアップデートを実行するかを指定します。

    [Hourly]：n 時間ごとにアップデートをチェックするように指定します。

    [Daily]：アップデートを実行する曜日を指定します。

Auto Update の設定

リモート サーバまたは Cisco.com から自動アップデートを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Auto/Cisco.com Update] を選択します。

ステップ 3　リモート サーバからの自動アップデートをイネーブルにするには、[Enable Auto Update from a Remote Server] チェックボックスをオンにします。

a. [IP Address] フィールドに、アップデートをダウンロードして格納したリモート サーバの IP アドレスを入力します。

b. リモート サーバへの接続に使用するプロトコルを指定するには、[File Copy Protocol] ドロップダウン リストから FTP または SCP を選択します。

c. [Directory] フィールドに、アップデートが置かれるリモート サーバ上のディレクトリへのパスを入力します。パスの有効な値は、1 ～ 128 文字です。

d. [Username] フィールドに、リモート サーバにログインする際に使用するユーザ名を入力します。ユーザ名の有効な値は、1 ～ 2047 文字です。

e. [Password] フィールドに、リモート サーバのユーザ名のパスワードを入力します。パスワードの有効な値は、1 ～ 2047 文字です。

f. 確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

g. 時間単位のアップデートの場合は、[Hourly] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Every_hours] フィールドに、各アップデートが行われる時間間隔を入力します。有効な値は 1 ～ 8760 です。

  たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新があれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーはインストール可能な最新のアップデートを特定し、そのファイルをインストールします。

h. 週単位のアップデートの場合は、[Daily] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Days] フィールドで、センサーが使用可能なアップデートをチェックしてダウンロードする曜日をオンにします。

ステップ 4　Cisco.com からのシグニチャ アップデートとシグニチャ エンジン アップデートをイネーブルにするには、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。

a. [Username] フィールドに、Cisco.com にログインするときに使用するユーザ名を入力します。ユーザ名の有効な値は、1 ～ 2047 文字です。

b. [Password] フィールドに、Cisco.com のユーザ名パスワードを入力します。パスワードの有効な値は、1 ～ 2047 文字です。

c. 確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

d. 時間単位のアップデートの場合は、[Hourly] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Every_hours] フィールドに、各アップデートが行われる時間間隔を入力します。有効な値は 1 ～ 8760 です。

  たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新があれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーはインストール可能な最新のアップデートを特定し、そのファイルをインストールします。

e. 週単位のアップデートの場合は、[Daily] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Days] フィールドで、センサーが使用可能なアップデートをチェックしてダウンロードする曜日をオンにします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 5　[Apply] をクリックして変更内容を保存します。

センサーの手動アップデート

ここでは、センサーの手動アップデート方法について説明します。内容は次のとおりです。

- 「[Update Sensor] ペイン」（P.18-21）
- 「[Update Sensor] ペインのフィールド定義」（P.18-21）
- 「センサーのアップデート」（P.18-21）

[Update Sensor] ペイン

（注）　[Update Sensor] ペインを表示して、サービス パックとシグニチャのアップデートでセンサーを更新するには、管理者である必要があります。

[Update Sensor] ペインでは、サービス パックとシグニチャのアップデートを即座に適用できます。センサーを手動で更新するには、サービス パックとシグニチャのアップデートを Cisco.com から FTP サーバにダウンロードし、それらを FTP サーバからセンサーにダウンロードするように設定する必要があります。

詳細情報

- シグニチャのアップデートおよびそれらのインストールに要する時間については、「シグニチャのアップデートおよびインストール時間」（P.18-17）を参照してください。
- Cisco.com でソフトウェア ファイルを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

[Update Sensor] ペインのフィールド定義

[Update Sensor] ペインには次のフィールドがあります。

- [Update is located on a remote server and is accessible by the sensor]：次のオプションを指定できます。
  - [URL]：アップデートが置かれているサーバのタイプを示します。FTP、HTTP、HTTPS、または SCP のどれを使用するかを指定します。
  - [://]：リモート サーバ上のアップデートへのパスを示します。
  - [Username]：リモート サーバのユーザ アカウントに対応するユーザ名を示します。
  - [Password]：リモート サーバのユーザ アカウントのパスワードを示します。
- [Update is located on this client]：次のオプションを指定できます。
  - [Local File Path]：このローカル クライアントでのアップデート ファイルへのパスを示します。
  - [Browse Local]：このローカル クライアントのファイル システムの [Browse] ダイアログボックスを開きます。このダイアログボックスから、アップデート ファイルに移動できます。

センサーのアップデート

（注）　センサーを手動で更新するには、サービス パックとシグニチャのアップデートを Cisco.com から FTP サーバにダウンロードし、それらを FTP サーバからセンサーにダウンロードするように設定する必要があります。

サービス パックとシグニチャのアップデートをすぐに適用するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Update Sensor] を選択します。

ステップ 3　リモート サーバからアップデートを取得して、センサーにインストールするには、次の手順を実行します。

a. [Update is located on a remote server and is accessible by the sensor] チェックボックスをオンにします。

b. [URL] フィールドには、アップデートのある URL を入力します。

次の URL タイプがサポートされています。

- [FTP:] : FTP ネットワーク サーバのソース URL。
  このプレフィクスの構文は次のとおりです。
  `ftp://location/relative_directory/filename`

  または
  `ftp://location//absolute_directory/filename`

- [HTTPS:] : ウェブ サーバのソース URL。
  このプレフィクスの構文は次のとおりです。
  `https://location/directory/filename`

  （注） HTTPS プロトコルを使用し始める前に、TLS の信頼できるホストを設定します。

- [SCP:] : SCP ネットワーク サーバのソース URL。
  このプレフィクスの構文は次のとおりです。
  `scp://location/relative_directory/filename`

  または
  `scp://location/absolute_directory/filename`

- [HTTP:] : Web サーバのソース URL です。
  このプレフィクスの構文は次のとおりです。
  `http://location/directory/filename`

  次の例は、FTP プロトコルを示しています。
  `ftp://user@ip_address/UPDATES/file_name.rpm.pkg`

  （注） アップデートをあらかじめ Cisco.com からダウンロードし、FTP サーバに保存しておく必要があります。

c. [Username] フィールドに、リモート サーバのアカウントのユーザ名を入力します。

d. [Password] フィールドに、リモート サーバのこのアカウントに関連付けられているパスワードを入力します。

ステップ 4　ローカル クライアントからプッシュして、センサーにインストールするには、次の手順を実行します。

a. [Update is located on this client] チェックボックスをオンにします。

b. ローカル クライアントのアップデート ファイルへのパスを指定するか、[Browse Local] をクリックして、ローカル クライアントのファイルを検索します。

ステップ 5　[Update Sensor] をクリックします。[Update Sensor] ダイアログボックスに、更新すると、センサーとの接続が失われ、再ログインが必要になることを伝えるメッセージが表示されます。

ステップ 6　[OK] をクリックして、センサーを更新します。

（注）　サービス パック、マイナー、メジャー、およびエンジニアリング パッチのアップデート中は、IME および CLI 接続が失われます。これらのアップデートの 1 つを適用している場合、インストーラにより IPS アプリケーションが再起動されます。センサーをリブートできます。シグニチャのアップデートの場合、接続は失われないので、システムをリブートする必要はありません。

ヒント　変更を破棄してダイアログボックスを閉じるには、[Cancel] をクリックします。

詳細情報

Cisco.com でソフトウェア ファイルを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

デフォルトの復元

（注）　[Restore Defaults] ペインを表示して、センサーのデフォルトを復元するには、管理者である必要があります。

[Restore Defaults] ペインでは、センサーにいつでもデフォルトの設定を復元できます。

警告　**デフォルトを復元すると、現在のアプリケーションの設定が削除され、デフォルト設定が復元されます。ネットワーク設定もデフォルトに戻り、センサーとの接続もただちに失われます。**

デフォルトの設定を復元するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Restore Defaults] を選択します。

ステップ 3　デフォルト設定を復元するには、[Restore Defaults] をクリックします。

ステップ 4　[Restore Defaults] ダイアログボックスで [OK] をクリックします。

（注）　デフォルトを復元すると、IP アドレス、ネットマスク、デフォルト ゲートウェイ、およびアクセス リストがリセットされます。パスワードと時間はリセットされません。手動および自動ブロックも有効なままになります。手動でセンサーをリブートする必要があります。

センサーのリブート

（注）　[Reboot Sensor] ペインを表示して、センサーをリブートするには、管理者である必要があります。

[Reboot Sensor] ペインからセンサーのシャットダウンと再起動を行うことができます。

センサーをリブートするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Reboot Sensor] を選択し、[Reboot Sensor] をクリックします。

ステップ 3　センサーをシャットダウンして再起動するには、[OK] をクリックします。センサー アプリケーションがシャットダウンされ、センサーがリブートされます。リブート後に、再ログインする必要があります。

（注）　CLI にログインしているユーザに対して、センサー アプリケーションがシャットダウンされることを伝えるメッセージが表示されてから、30 秒後にシャットダウンされます。

センサーのシャットダウン

（注）　[Shut Down Sensor] ペインを表示し、センサーをシャットダウンするには、管理者である必要があります。

センサーは、IPS アプリケーションをシャットダウンしたあとに安全に電源を切断できる状態になります。

センサーをシャットダウンするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Management] > [Shut Down Sensor] を選択し、[Shut Down Sensor] をクリックします。

ステップ 3　[Shut Down Sensor] ダイアログボックスで [OK] をクリックします。センサー アプリケーションがシャットダウンされ、センサーに開かれている接続が閉じます。

（注）　CLI にログインしているユーザに対して、センサー アプリケーションがシャットダウンされることを伝えるメッセージが表示されてから、30 秒後にシャットダウンされます。