CHAPTER 17

センサーの管理タスク

この章では、センサーの管理に役立つ手順を示します。次のような構成になっています。

- 「パスワードの回復」（P.17-2）
- 「センサー データベースのクリア」（P.17-9）
- 「ヘルス ステータス情報の設定」（P.17-10）
- 「センサーのヘルス ステータス全体の表示」（P.17-14）
- 「バナー ログインの作成」（P.17-14）
- 「CLI セッションの終了」（P.17-15）
- 「ターミナル プロパティの変更」（P.17-16）
- 「イベントの設定」（P.17-17）
- 「システム クロックの設定」（P.17-20）
- 「拒否された攻撃者のリストのクリア」（P.17-21）
- 「ポリシー リストの表示」（P.17-23）
- 「統計情報の表示」（P.17-24）
- 「技術サポート情報の表示」（P.17-34）
- 「バージョン情報の表示」（P.17-35）
- 「ネットワーク接続の診断」（P.17-37）
- 「アプライアンスのリセット」（P.17-38）
- 「コマンド履歴の表示」（P.17-39）
- 「ハードウェア コンポーネントの表示」（P.17-39）
- 「IP パケットのルートのトレース」（P.17-40）
- 「サブモード設定の表示」（P.17-41）

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 アカウントを使用するか、またはセンサーのイメージを再作成しなくても、センサー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 IPS 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。次の項目について説明します。

- 「パスワードの回復について」（P.17-2）
- 「アプライアンスのパスワードの回復」（P.17-3）
- 「AIM IPS パスワードの回復」（P.17-4）
- 「AIP SSM パスワードの回復」（P.17-5）
- 「IDSM2 パスワードの回復」（P.17-6）
- 「NME IPS パスワードの回復」（P.17-6）
- 「パスワード回復のディセーブル化」（P.17-7）
- 「パスワード回復の状態の確認」（P.17-8）
- 「パスワードの回復のトラブルシューティング」（P.17-8）

パスワードの回復について

パスワードの回復の実装は、IPS プラットフォーム要件によって異なります。パスワードの回復は、cisco 管理アカウントだけに対して実装され、デフォルトでイネーブルになっています。IPS 管理者は、CLI を使用して、その他のアカウントのユーザ パスワードを回復できます。cisco ユーザのパスワードは、**cisco** に戻り、次のログイン後に変更する必要があります。

（注）　セキュリティ上の理由から、管理者がパスワード回復機能をディセーブルにする必要が生じることがあります。

表 17-1 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 17-1　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	ルータの IPS モジュール	ブートローダ コマンド
AIP SSM	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	Switch IPS モジュール	パスワード回復イメージ ファイル

アプライアンスのパスワードの回復

ここでは、アプライアンスのパスワードを回復する 2 つの方法について説明します。次の項目について説明します。

- 「GRUB メニューの使用」（P.17-3）
- 「ROMMON の使用方法」（P.17-3）

GRUB メニューの使用

（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、またはアプライアンスへの直接シリアル接続が必要です。

4200 シリーズ アプライアンスでは、パスワード回復はブート中に表示される GRUB メニューにあります。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。

アプライアンスでパスワードを回復するには、次の手順に従います。

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。

ROMMON の使用方法

IPS 4240 と IPS 4255 では、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、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、次の手順に従います。

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 を押すか、Ctrl キーを押した状態で R キーを押すか（ターミナル サーバ）、または **BREAK** コマンドを送信します（直接接続）。

ブート コードが 10 秒間停止するか、または次のいずれかのような内容が表示されます。

- 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
```

ROMMON セッションのサンプル：

```
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
```

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、ルータへの管理アクセスが必要です。

AIM IPS のパスワードを回復するには、次の手順に従います。

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　Ctrl キーと Shift キーを押した状態で 6 を押してから x キーを押して、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 を押すと、ルータ コンソールに戻ります。

ステップ 8　ブート オプションの入力を要求されたら、すぐに ******* と入力します。

ブートローダが表示されます。

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 に再度ログインします。その後、パスワードを変更できます。

AIP SSM パスワードの回復

（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。

CLI または ASDM を使用して、AIP SSM 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、AIP SSM はリブートされます。リブート中に IPS サービスは使用できません。

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（**cisco**）にリセットします。ASA 5500 シーズ適応型セキュリティ アプライアンスでは、ROMMON confreg ビットが 0x7 に設定され、センサーがリブートされます。ROMMON ビットによって、GRUB メニューはデフォルトのオプション 2（**パスワードのリセット**）になります。

指定したスロットのモジュールの IPS バージョンがパスワードの回復をサポートしていない場合は、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、次の手順に従います。

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

（注）　モジュールが取り付けられていない場合、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 confirmation] 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の（**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、適応型セキュリティ アプライアンスに ASA 7.2(2) 以降、AIP SSM に IPS 6.0 以降が導入されていることを確認します。

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。AIP SSM 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、特殊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。これをインストールするとパスワードだけがリセットされ、その他の設定はすべて変更されません。パスワード回復イメージはバージョンによって異なり、Cisco Download Software サイトにあります。IPS 6.*x* では、WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz をダウンロードします。IPS 7.*x* では、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用にサポートされているプロトコルは FTP だけです。したがって、スイッチにアクセスできる FTP サーバにパスワード回復イメージ ファイルを置いてください。IDSM2 でパスワードを回復するには、Cisco 6500 シリーズ スイッチへの管理アクセスが必要です。

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]:
```

このメッセージは誤りです。パスワード回復イメージのインストールによって、設定が削除されることはありません。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に関する指示に従いますが、システム イメージ ファイルをパスワード回復イメージ ファイルと読み替えてください。回復イメージ ファイルのインストール後に、IDSM2 はプライマリ パーティションでリブートされるはずです。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 に再度ログインします。その後、パスワードを変更できます。

詳細情報

- IDSM2 でのシステム イメージのインストール手順については、「IDSM2 システム イメージのインストール」（P.23-29）を参照してください。
- Cisco IPS ソフトウェアのダウンロードの詳細については、「Cisco IPS ソフトウェアの入手方法」（P.22-1）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、ルータへの管理アクセスが必要です。

NME IPS のパスワードを回復するには、次の手順に従います。

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　Ctrl キーと Shift キーを押した状態で 6 を押してから x キーを押して、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 を押すと、ルータ コンソールに戻ります。

ステップ 8　ブート オプションの入力を要求されたら、すぐに ******* と入力します。

ブートローダが表示されます。

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 に再度ログインします。その後、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　パスワードの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しても、プロセスはエラーまたは警告なしで継続されますが、パスワードはリセットされません。パスワードを忘れ、パスワードの回復がディセーブルに設定されているためにセンサーにログインできない場合は、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。CLI、IDM、または IME を使用して、パスワードの回復をディセーブルにできます。

CLI でパスワードの回復をディセーブルにするには、次の手順に従います。

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　パスワードの回復をディセーブルにします。

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

IDM または IME でパスワードの回復をディセーブルにするには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して、IDM または 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　パスワードの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。

パスワード回復の状態の確認

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

パスワードの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、次の手順に従います。

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、フィルタリングした出力で設定を表示することにより、パスワードの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)#
```

パスワードの回復のトラブルシューティング

パスワードの回復をトラブルシューティングする場合は、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 CLI、またはルータ CLI から、センサー設定でパスワードの回復がディセーブルになっているかどうかを判断することはできません。パスワードを回復しようとすると、常に成功したように見えます。パスワードの回復が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。唯一の方法は、センサーのイメージ再作成です。
- ホスト設定で、パスワードの回復をディセーブルにできます。AIM IPS および NME IPS ブートローダ、ROMMON、および 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では、パスワードをクリアするコマンドを実行できます。ただし、パスワードの回復が IPS でディセーブルになっている場合、IPS によってパスワードの回復が許可されないことが検出され、その外部要求は拒否されます。

  パスワードの回復の状態を確認するには、**show settings** | **include password** コマンドを使用します。
- IDSM2 でパスワードの回復を実行した場合、メッセージ「`Upgrading will wipe out the contents on the storage media`」が表示されます。このメッセージは無視してください。指定したパスワード回復イメージを使用した場合は、パスワードだけがリセットされます。

センサー データベースのクリア

注意　累積された状態情報をクリアし、クリーンなデータベースで開始する必要があるときに、TAC の指示に基づいて、または一部のテスト状況で行う場合を除き、このコマンドを使用することは推奨しません。

センサー データベースの特定の部分をクリアするには、特権 EXEC モードで、**clear database** [*virtual-sensor*] **all | nodes | alerts | inspectors** コマンドを使用します。**clear database** コマンドは、トラブルシューティングとテストに役立ちます。

次のオプションが適用されます。

- *virtual-sensor*：センサーで設定する仮想センサーの名前。
- **all**：すべてのノード、インスペクタ、およびアラート データベースをクリアします。

注意　このコマンドによって、サマリー アラートは廃棄されます。

- **nodes**：パケット ノード、TCP セッション情報、およびインスペクタ リストを含め、パケット データベース要素全体をクリアします。
- **alerts**：アラート ノード、メタ インスペクタ情報、サマリー状態、およびイベント カウント構造を含め、アラート データベースをクリアします。
- **inspectors**：ノード内のインスペクタ リストをクリアします。

  インスペクタ リストには、センサーの実行時間中に収集されたパケットの動作と状況が示されます。

センサー データベースをクリアするには、次の手順に従います。

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　センサー データベース全体をクリアします。

```
sensor# clear database all
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 3　**yes** と入力して、センサーのすべてのデータベースをクリアします。

ステップ 4　パケット ノードをクリアします。

```
sensor# clear database nodes
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 5　**yes** と入力して、パケット ノード データベースをクリアします。

ステップ 6　特定の仮想センサーのアラート データベースをクリアします。

```
sensor# clear database vs0 alerts
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 7　**yes** と入力して、アラート データベースをクリアします。

ステップ 8　センサーのインスペクタ リストをクリアします。

```
sensor# clear database inspectors
```

```
Warning: Executing this command will delete database on all virtual sensors
Continue? [yes]:
```

ステップ 9　**yes** と入力して、インスペクタ データベースをクリアします。

ヘルス ステータス情報の設定

センサーのヘルス統計情報を設定するには、サービス サブモードで、**health-monitor** コマンドを使用します。**health-monitor** コマンドの結果を表示するには、**show health** コマンドを使用します。ヘルス ステータス カテゴリは赤と緑によってレーティングされ、赤は重大なステータスを示します。

次のオプションが適用されます。

- **application-failure-policy {enable | disable} {true | false} status {green | yellow | red}**：アプリケーション障害をセンサー ヘルス レーティング全体に適用できます。
- **bypass-policy {enable | disable} {true | false} status {green | yellow | red}**：バイパス モードがアクティブであるかどうかを確認し、これをセンサー ヘルス レーティング全体に適用できます。
- **enable-monitoring {true | false}**：センサー ヘルスおよびセキュリティをモニタできます。
- **event-retrieval-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*：最後のイベントが取得された時期に対してしきい値を設定し、これをセンサー ヘルス レーティング全体に適用できます。このしきい値に達すると、ヘルス ステータスは赤または黄色に低下します。しきい値の範囲は 0 ～ 4294967295 秒です。

  （注）　イベント取得メトリックは、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期を追跡します。外部イベントのモニタリングを実行していない場合は、event retrieval policy をディセーブルにします。

- **global-correlation-policy {enable | disable} {true | false}**：センサー ヘルス レーティング全体に、このメトリックを適用できます。
- **heartbeat-events {enable | disable}** *seconds*：指定した間隔（秒単位）でのハートビート イベントの発行をイネーブルにし、これをセンサー ヘルス レーティング全体に適用できます。間隔の範囲は 15 秒から 86400 秒です。
- **inspection-load-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*：検査負荷に対してしきい値を設定できます。このしきい値に達すると、ヘルス ステータスは赤または黄色に低下します。範囲は 0 ～ 100 です。
- **interface-down-policy {enable | disable} {true | false} status {green | yellow | red}**：イネーブルになっている 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確認し、これをセンサー ヘルス レーティング全体に適用できます。
- **license-expiration-policy {enable | disable} {true | false} red-threshold yellow-threshold**：ライセンスの期限が切れる時期に対するしきい値と、このメトリックをセンサー ヘルス レーティング全体に適用するかどうかを設定できます。しきい値の範囲は 0 ～ 4294967295 秒です。
- **memory-usage-policy {enable | disable} {true | false} red-threshold yellow-threshold**：メモリ使用率に対するしきい値と、このメトリックをセンサー ヘルス レーティング全体に適用するかどうかを設定できます。範囲は 0 ～ 100 です。
- **missed-packet-policy {enable | disable} {true | false} red-threshold yellow-threshold**：損失パケットの比率に対するしきい値と、このメトリックをセンサー ヘルス レーティング全体に適用するかどうかを設定できます。

- **network-participation-policy {enable | disable} {true | false}**：このメトリックをセンサー ヘルス レーティング全体に適用できます。
- **persist-security-status**：セキュリティ ステータスを低下させるまでに、最後のイベントの発生後、比較的低いセキュリティが持続する時間（分）を設定できます。
- **signature-update-policy {enable | disable} {true | false} red-threshold yellow-threshold**：最後のシグニチャの更新から経過した日数に対するしきい値と、このメトリックをセンサー ヘルス レーティング全体に適用するかどうかを設定できます。しきい値の範囲は 0 ～ 4294967295 秒です。

センサーのヘルス統計情報を設定するには、次の手順に従います。

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　サービス ヘルス モニタ サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service health-monitor
sensor(config-hea)#
```

ステップ 3　アプリケーション障害ステータスに対するメトリックをイネーブルにします。

```
sensor(config-hea)# application-failure-policy
sensor(config-hea-app)# enable true
sensor(config-hea-app)# status red
sensor(config-hea-app)# exit
sensor(config-hea)#
```

ステップ 4　バイパス ポリシーに対するメトリックをイネーブルにします。

```
sensor(config-hea)# bypass-policy
sensor(config-hea-byp)# enable true
sensor(config-hea-byp)# status yellow
sensor(config-hea-byp)# exit
sensor(config-hea)#
```

ステップ 5　センサー ヘルスとセキュリティ モニタリングに対するメトリックをイネーブルにします。

```
sensor(config-hea)# enable-monitoring true
sensor(config-hea)#
```

ステップ 6　イベント取得メトリックに対して、イベント取得しきい値を設定します。

```
sensor(config-hea)# event-retrieval-policy
sensor(config-hea-eve)# enable true
sensor(config-hea-eve)# red-threshold 100000
sensor(config-hea-eve)# yellow-threshold 100
sensor(config-hea-eve)# exit
sensor(config-hea)#
```

ステップ 7　グローバル相関に対するヘルス メトリックをイネーブルにします。

```
sensor(config-hea)# global-correlation-policy
sensor(config-hea-glo)# enable true
sensor(config-hea-glo)# exit
sensor(config-hea)#
```

ステップ 8　指定した間隔（秒単位）で発行されるハートビート イベントに対するメトリックをイネーブルにします。

```
sensor(config-hea)# heartbeat-events enable 20000
sensor(config-hea)#
```

ステップ 9　検査負荷しきい値を設定します。

```
sensor(config-hea)# inspection-load-policy
sensor(config-hea-ins)# enable true
sensor(config-hea-ins)# red-threshold 100
sensor(config-hea-ins)# yellow-threshold 50
sensor(config-hea-ins)# exit
sensor(config-hea)#
```

ステップ 10　インターフェイス ダウン ポリシーをイネーブルにします。

```
sensor(config-hea)# interface-down-policy
sensor(config-hea-int)# enable true
sensor(config-hea-int)# status yellow
sensor(config-hea-int)# exit
sensor(config-hea)#
```

ステップ 11　ライセンスの期限が切れるまでの日数を設定します。

```
sensor(config-hea)# license-expiration-policy
sensor(config-hea-lic)# enable true
sensor(config-hea-lic)# red-threshold 400000
sensor(config-hea-lic)# yellow-threshold 200000
sensor(config-hea-lic)# exit
sensor(config-hea)#
```

ステップ 12　メモリ使用率に対するしきい値を設定します。

```
sensor(config-hea)# memory-usage-policy
sensor(config-hea-mem)# enable true
sensor(config-hea-mem)# red-threshold 100
sensor(config-hea-mem)# yellow-threshold 50
sensor(config-hea-mem)# exit
sensor(config-hea)#
```

ステップ 13　損失パケットに対するしきい値を設定します。

```
sensor(config-hea)# missed-packet-policy
sensor(config-hea-mis)# enable true
sensor(config-hea-mis)# red-threshold 50
sensor(config-hea-mis)# yellow-threshold 20
sensor(config-hea-mis)# exit
sensor(config-hea)#
```

ステップ 14　セキュリティ ステータスを低下させるまでに、最後のイベントの発生後、比較的低いセキュリティが持続する時間（分）を設定します。

```
sensor(config-hea)# persist-security-status 10
sensor(config-hea)#
```

ステップ 15　最後のシグニチャの更新からの日数を設定します。

```
sensor(config-hea)# signature-update-policy
sensor(config-hea-sig)# enable true
sensor(config-hea-sig)# red-threshold 30000
sensor(config-hea-sig)# yellow-threshold 10000
sensor(config-hea-sig)# exit
sensor(config-hea)#
```

ステップ 16　設定を確認します。

```
sensor(config-hea)# show settings
   enable-monitoring: true default: true
   persist-security-status: 10 minutes default: 5
   heartbeat-events
   -----------------------------------------------
```

```
   enable: 20000 seconds default: 300
-----------------------------------------------
application-failure-policy
-----------------------------------------------
   enable: true default: true
   status: red default: red
-----------------------------------------------
bypass-policy
-----------------------------------------------
   enable: true default: true
   status: yellow default: red
-----------------------------------------------
interface-down-policy
-----------------------------------------------
   enable: true default: true
   status: yellow default: red
-----------------------------------------------
inspection-load-policy
-----------------------------------------------
   enable: true default: true
   yellow-threshold: 50 percent default: 80
   red-threshold: 100 percent default: 91
-----------------------------------------------
missed-packet-policy
-----------------------------------------------
   enable: true default: true
   yellow-threshold: 20 percent default: 1
   red-threshold: 50 percent default: 6
-----------------------------------------------
memory-usage-policy
-----------------------------------------------
   enable: true default: false
   yellow-threshold: 50 percent default: 80
   red-threshold: 100 percent default: 91
-----------------------------------------------
signature-update-policy
-----------------------------------------------
   enable: true default: true
   yellow-threshold: 10000 days default: 30
   red-threshold: 30000 days default: 60
-----------------------------------------------
license-expiration-policy
-----------------------------------------------
   enable: true default: true
   yellow-threshold: 200000 days default: 30
   red-threshold: 400000 days default: 0
-----------------------------------------------
event-retrieval-policy
-----------------------------------------------
   enable: true <defaulted>
   yellow-threshold: 100000 seconds default: 300
   red-threshold: 100 seconds default: 600
-----------------------------------------------
sensor(config-hea)#
```

ステップ 17　ヘルス モニタリング サブモードを終了します。

```
sensor(config-hea)# exit
Apply Changes:?[yes]:
```

ステップ 18　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

センサーのヘルス ステータス全体の表示

センサーのヘルス ステータス情報全体を表示するには、特権 EXEC モードで、**show health** コマンドを使用します。ヘルス ステータス カテゴリは赤と緑によってレーティングされ、赤は重大なステータスを示します。

注意　センサーを最初に起動する場合は、センサーが完全に起動し、動作するまで、特定のヘルス メトリック ステータスが赤になることは正常です。

センサーのヘルス ステータス全体を表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　センサーのヘルス ステータスとセキュリティ ステータスを表示します。

```
sensor# show health
Overall Health Status                                 Red
Health Status for Failed Applications                 Green
Health Status for Signature Updates                   Green
Health Status for License Key Expiration              Red
Health Status for Running in Bypass Mode              Green
Health Status for Interfaces Being Down               Red
Health Status for the Inspection Load                 Green
Health Status for the Time Since Last Event Retrieval Green
Health Status for the Number of Missed Packets        Green
Health Status for the Memory Usage                    Not Enabled
Health Status for Global Correlation                  Red
Health Status for Network Participation               Not Enabled

Security Status for Virtual Sensor vs0                Green
sensor#
```

バナー ログインの作成

ユーザおよびパスワードのログイン プロンプトの前に表示されるバナー ログインを作成するには、**banner login** コマンドを使用します。メッセージの最大長は 2500 文字です。バナーを削除するには、**no banner login** コマンドを使用します。

バナー ログインを作成するには、次の手順に従います。

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　バナー ログインを作成します。

```
sensor(config)# banner login
Banner[]:
```

ステップ 4　メッセージを入力します。

```
Banner[]: This message will be displayed on banner login. ^M Thank you
```

```
sensor(config)#
```

（注）　メッセージ内で？または復帰を使用するには、Ctrl キーを押した状態で V キーと ？ を押すか、Ctrl キーを押した状態で V キーと Enter を押します。これらの文字は、^M と表示されます。

例

```
This message will be displayed on login.
Thank you
login: cisco
Password:****
```

ステップ 5　バナー ログインを削除するには、次のコマンドを実行します。

```
sensor(config)# no banner login
```

ログイン時にバナーは表示されなくなります。

CLI セッションの終了

注意　CLI ログイン セッションをクリアできるのは、**clear line** コマンドだけです。このコマンドではサービス ログインをクリアできません。

別の CLI セッションを終了するには、**clear line** *cli_id* [**message**] コマンドを使用します。**message** キーワードを使用すると、受信ユーザに対して終了要求とともにメッセージを送信できます。メッセージの最大長は 2500 文字です。

次のオプションが適用されます。

- *cli_id*：ログイン セッションに関連付けられた CLI ID 番号。CLI ID 番号を調べるには、**show users** コマンドを使用します。
- **message**：受信ユーザに送信するメッセージ。

セッションの最大数に達しているときに、管理者がログインしようとした場合は、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, would you like to terminate
one of the open sessions? [no]
```

セッションの最大数が開かれているときに、オペレータまたはビューアがログインしようとした場合は、次のメッセージが表示されます。

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

CLI セッションを終了するには、次の手順に従います。

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。

（注）　オペレータとビューアは、現在のログインと同じユーザ名の行だけをクリアできます。

ステップ 2　ログイン セッションに関連付けられた CLI ID 番号を調べます。

```
sensor# show users
    CLI ID   User    Privilege
*   13533    jtaylor administrator
    15689    jsmith  operator
    20098    viewer  viewer
```

ステップ 3　jsmith の CLI セッションを終了します。

```
sensor# clear line cli_id message
Message[]:
```

例

```
sensor# clear line 15689 message
Message{}: Sorry! I need to terminate your session.
sensor#
```

ユーザ jsmith は、管理者 jtaylor から次のメッセージを受信します。

```
sensor#
***
***
*** Termination request from jtaylor
***
Sorry! I need to terminate your session.
```

ターミナル プロパティの変更

（注）　一部の種類のターミナル セッションでは、画面の長さを指定する必要はありません。これは、一部のリモート ホストは、指定した画面の長さを認識できるためです。

ログイン セッションのターミナル プロパティを変更するには、**terminal [length]** *screen _length* コマンドを使用します。*screen_ length* オプションでは、--more-- プロンプトの上に画面に表示される行数を設定できます。値 0 を設定すると、出力が停止されなくなります。デフォルト値は 24 行です。

ターミナル プロパティを変更するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　複数画面分の出力中に停止しないようにするには、screen length 値に 0 を使用します。

```
sensor# terminal length 0
```

（注）　screen length 値は、ログイン セッション間で保存されません。

ステップ 3　10 行ごとに CLI を停止し、--more-- プロンプトを表示するには、*screen length* 値に 10 を使用します。

```
sensor# terminal length 10
```

イベントの設定

ここでは、イベント ストアのイベントを表示およびクリアする方法について説明します。内容は次のとおりです。

- 「イベントの表示」（P.17-17）
- 「イベント ストアのイベントのクリア」（P.17-20）

イベントの表示

イベント ストアのイベントを表示するには、**show events** [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用します。

イベントは、開始時刻から表示されます。開始時刻を指定しなかった場合、イベントは現在の時刻から表示されます。イベント タイプを指定しない場合は、すべてのイベントが表示されます。

（注）　イベントは、ライブ フィードとして表示されます。要求をキャンセルするには、Ctrl キーを押した状態で C キーを押します。

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であるか試みられたことを示す可能性がある、ある種の疑わしいアクティビティを通知します。アラート イベントは、シグニチャがネットワーク アクティビティによってトリガーされるたびに、分析エンジンによって生成されます。

  レベル（informational、low、medium、または high）を選択しなかった場合は、すべてのアラート イベントが表示されます。
- **include-traits**：指定した特性があるアラートを表示します。
- **exclude-traits**：指定した特性があるアラートを表示しません。
- **traits**：10 進数での特性ビット位置（0 ～ 15）。
- **min-threat-rating**：脅威レーティングがこの値以上のイベントを表示します。デフォルトは 0 です。有効な範囲は 0 ～ 100 です。
- **max-threat-rating**：脅威レーティングがこの値以下のイベントを表示します。デフォルトは 100 です。有効な範囲は 0 ～ 100 です。
- **error**：エラー イベントを表示します。エラー イベントは、エラー条件が生じた場合に、サービスによって生成されます。

  レベル（warning、error、または fatal）を選択しなかった場合は、すべてのエラー イベントが表示されます。
- **NAC**：ARC（ブロック）要求を表示します。

  （注）　ARC は、以前は NAC と呼ばれていました。この名前変更は、IDM、IME、および CLI for Cisco IPS 7.0 全体に完全には適用されていません。
- **status**：ステータス イベントを表示します。
- **past**：指定した時間、分、および秒で、過去に開始されたイベントを表示します。

- *hh:mm:ss*：表示を開始する過去の時間、分、および秒。

（注）　**show events** コマンドを実行すると、指定したイベントが見つかるまで、イベントが表示され続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベント ストアからイベントを表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　現在から始まるすべてのイベントを表示します。

```
sensor#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exception:
handshake incomplete.
```

Ctrl キーを押した状態で C キーを押すまで、すべてのイベントが表示され続けます。

ステップ 3　2008 年 2 月 9 日、午前 10:00 以降のブロック要求を表示します。

```
sensor# show events NAC 10:00:00 Feb 9 2008
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2008/02/09 10:33:31 2008/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

ステップ 4　2008 年 2 月 9 日、午前 10:00 以降の warning レベルのエラーを表示します。

```
sensor# show events error warning 10:00:00 Feb 9 2008
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2008/01/07 04:49:25 2008/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　過去 45 秒間のアラートを表示します。

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2008/03/02 14:15:59 2008/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　過去 30 秒間に開始されたイベントを表示します。

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベント ストアのイベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアのイベントをクリアするには、次の手順に従います。

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　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** と入力して、イベントをクリアします。

システム クロックの設定

ここでは、システム クロックを表示し、手動で設定する方法について説明します。次の項目について説明します。

- 「システム クロックの表示」（P.17-20）
- 「システム クロックの手動設定」（P.17-21）

システム クロックの表示

システム クロックを表示するには、**show clock** [**detail**] コマンドを使用します。**detail** オプションを使用すると、クロック ソース（NTP またはシステム）と現在のサマータイム設定（設定されている場合）を表示できます。システム クロックは、信頼性がある（正確であると信じられる）かどうかを示す authoritative フラグを維持します。システム クロックが NTP などのタイミング ソースによって設定されている場合は、フラグを設定します。

表 17-2 にはシステム クロックのフラグを示します。

表 17-2　システム クロックのフラグ

記号	説明
*	時刻は信頼できません。
（ブランク）	時刻は信頼できます。
.	時刻は信頼できますが、NTP が同期していません。

システム クロックを表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　システム クロックを表示します。

```
sensor# show clock
*19:04:52 UTC Thu Apr 03 2008
```

ステップ 3　システム クロックと詳細情報を表示します。

```
sensor# show clock detail
20:09:43 UTC Thu Apr 03 2008
Time source is NTP
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

これは、センサーが時刻を NTP から取得し、設定および同期されていることを示しています。

```
sensor# show clock detail
*20:09:43 UTC Thu Apr 03 2008
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2008
Summer time stops 01:00:00 UTC Sun Nov 02 2008
```

これは、時刻源が設定されていないことを示しています。

システム クロックの手動設定

（注）　センサーが NTP クロック ソースなどの有効な外部のタイミング メカニズムによって同期されている場合、システム クロックを設定する必要はありません。

アプライアンスでクロックを手動で設定するには、**clock set** *hh:mm [:ss] month day year* コマンドを使用します。他の時刻源を使用できない場合は、次のコマンドを使用してください。

clock set コマンドは、次のプラットフォームには適用されません。

- AIM IPS
- AIP SSM
- IDSM2
- NME IPS

アプライアンスでクロックを手動で設定するには、次の手順に従います。

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　クロックを手動で設定します。

```
sensor# clock set 13:21 Mar 29 2008
```

（注）　時刻は 24 時間形式です。

拒否された攻撃者のリストのクリア

拒否された攻撃者のリストを表示するには、**show statistics denied-attackers** コマンドを使用します。拒否された攻撃者のリストを削除し、仮想センサー統計情報をクリアするには、**clear denied-attackers** [*virtual_sensor*] [**ip-address** *ip_address*] コマンドを使用します。

センサーがインライン モードで動作するように設定されている場合、トラフィックはセンサーを通過します。インライン モードでは、パケット、接続、および攻撃者を拒否するように、シグニチャを設定できます。つまり、センサーが 1 つのパケット、接続、および特定の攻撃者を検出した場合、これらは拒否されます（伝送されません）。

シグニチャが起動された場合、攻撃者は拒否され、リストに記載されます。センサー管理の一環として、リストを削除するか、リスト内の統計情報をクリアすることができます。

次のオプションが適用されます。

- *virtual_sensor*：（任意）拒否された攻撃者リストをクリアする必要がある仮想センサー。
- *ip_address*：（任意）クリアする IP アドレス。

拒否された攻撃者のリストを表示し、リストを削除し、統計情報をクリアするには、次の手順に従います。

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　拒否された IP アドレスのリストを表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

ここでは、拒否されている 2 つの IP アドレスがあることが統計情報に示されます。

ステップ 3　拒否された攻撃者のリストを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** と入力して、リストをクリアします。

ステップ 5　特定の仮想センサーに対して、拒否された攻撃者のリストを削除します。

```
sensor# clear denied-attackers vs0
Warning: Executing this command will delete all addresses from the list of attackers being
denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 6　**yes** と入力して、リストをクリアします。

ステップ 7　特定の仮想センサーに対する拒否された攻撃者のリストから特定の IP アドレスを削除します。

```
sensor# clear denied-attackers vs0 ip-address 10.1.1.1
Warning: Executing this command will delete ip address 10.1.1.1 from the list of attackers
being denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 8　**yes** と入力して、リストをクリアします。

ステップ 9　リストがクリアされたことを確認します。

show statistics denied-attackers コマンドまたは **show statistics virtual-sensor** コマンドを使用できます。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.
```

```
   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.
sensor#
```

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

ステップ 10　統計情報だけをクリアします。

```
sensor# show statistics virtual-sensor clear
```

ステップ 11　統計情報がクリアされたことを確認します。

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

`Number of Active Denied Attackers` と `Number of exec Clear commands during uptime` のカテゴリを除き、統計情報はすべてクリアされます。リストがクリアされたかどうかを確認することが重要です。

ポリシー リストの表示

各コンポーネントのポリシーのリストを表示するには、EXEC モードで、**list {anomaly-detection-configurations | event-action-rules-configurations | signature-definition-configurations}** を使用します。ファイル サイズは、バイト単位です。N/A と表示されている仮想センサーは、ポリシーがその仮想センサーに割り当てられていないことを示しています。

センサーのポリシーのリストを表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　異常検出に対するポリシーのリストを表示します。

```
sensor# list anomaly-detection-configurations
Anomaly Detection
   Instance   Size   Virtual Sensor
   ad0        255    vs0
   temp       707    N/A
   MyAD       255    N/A
   ad1        141    vs1
sensor#
```

ステップ 3　イベント アクション規則に対するポリシーのリストを表示します。

```
sensor# list event-action-rules-configurations
Event Action Rules
   Instance   Size   Virtual Sensor
   rules0     112    vs0
   rules1     141    vs1
sensor#
```

ステップ 4　シグニチャ定義に対するポリシーのリストを表示します。

```
sensor# list signature-definition-configurations
Signature Definition
   Instance   Size   Virtual Sensor
   sig0       336    vs0
   sig1       141    vs1
   sig2       141    N/A
sensor#
```

統計情報の表示

すべての仮想センサーに対して各コンポーネントの統計情報を表示するには、**show statistics [analysis-engine** | **anomaly-detection** | **authentication** | **denied-attackers** | **event-server** | **event-store** | **external-product-interface** | **global-correlation** | **host** | **logger** | **network-access** | **notification** | **os-identification** | **sdee-server** | **transaction-server** | **virtual-sensor** | **web-server**] [**clear**] コマンドを使用します。

すべての仮想センサーに対して各コンポーネントの統計情報を表示するには、**show statistics** {**anomaly-detection** | **denied-attackers** | **os-identification** | **virtual-sensor**} [***name*** | **clear**] を使用します。仮想センサー名を指定した場合は、その仮想センサーの統計情報だけが表示されます。

（注）　**clear** オプションは、分析エンジン、異常検出、ホスト、ネットワーク アクセス、または OS ID アプリケーションでは使用できません。

センサーの統計情報を表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　分析エンジンの統計情報を表示します。

```
sensor# show statistics analysis-engine
```

```
Analysis Engine Statistics
   Number of seconds since service started = 1421127
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 0
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 0
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 0
sensor#
```

ステップ 3　異常検出の統計情報を表示します。

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
```

```
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor-4240#
```

ステップ 4　認証の統計情報を表示します。

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
sensor#
```

ステップ 5　システムで拒否された攻撃者の統計情報を表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


sensor#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
sensor# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
```

```
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
sensor#
```

ステップ 8　グローバル相関の統計情報を表示します。

```
sensor# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
sensor#
```

ステップ 9　ホストの統計情報を表示します。

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2008
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185 Bcast:10.89.149.255 Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 Mib) TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
```

```
Auto Update Statistics
   lastDirectoryReadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
    =   Success
   lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Download: http://bmarquardt@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/IPS-
sig-S338-req-E1.pkg
    =   Error: httpResponse status returned:  Unauthorized
   lastInstallAttempt = N/A
   nextAttempt = 16:26:30 CDT Tue Jun 17 2008

sensor#
```

ステップ 10　ロギング アプリケーションの統計情報を表示します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
sensor#
```

ステップ 11　ARC の統計情報を表示します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
```

```
            InterfaceName = ethernet0/1
            InterfaceDirection = out
            InterfacePostBlock = Post_Acl_Test
         BlockInterface
            InterfaceName = ethernet0/1
            InterfaceDirection = in
            InterfacePreBlock = Pre_Acl_Test
            InterfacePostBlock = Post_Acl_Test
      NetDevice
         Type = CAT6000_VACL
         IP = 10.89.150.138
         NATAddr = 0.0.0.0
         Communications = telnet
         BlockInterface
            InterfaceName = 502
            InterfacePreBlock = Pre_Acl_Test
         BlockInterface
            InterfaceName = 507
            InterfacePostBlock = Post_Acl_Test
   State
      BlockEnable = true
      NetDevice
         IP = 10.89.150.171
         AclSupport = Does not use ACLs
         Version = 6.3
         State = Active
         Firewall-type = PIX
      NetDevice
         IP = 10.89.150.219
         AclSupport = Does not use ACLs
         Version = 7.0
         State = Active
         Firewall-type = ASA
      NetDevice
         IP = 10.89.150.250
         AclSupport = Does not use ACLs
         Version = 2.2
         State = Active
         Firewall-type = FWSM
      NetDevice
         IP = 10.89.150.158
         AclSupport = uses Named ACLs
         Version = 12.2
         State = Active
      NetDevice
         IP = 10.89.150.138
         AclSupport = Uses VACLs
         Version = 8.4
         State = Active
      BlockedAddr
         Host
            IP = 22.33.4.5
            Vlan =
            ActualIp =
            BlockMinutes =
         Host
            IP = 21.21.12.12
            Vlan =
            ActualIp =
            BlockMinutes =
         Host
            IP = 122.122.33.4
            Vlan =
            ActualIp =
```

```
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

ステップ 12　通知アプリケーションの統計情報を表示します。

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

ステップ 13　OS ID の統計情報を表示します。

```
sensor# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
sensor#
```

ステップ 14　SDEE サーバの統計情報を表示します。

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

ステップ 15　トランザクション サーバの統計情報を表示します。

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

ステップ 16　仮想センサーの統計情報を表示します。

```
sensor# show statistics virtual-sensor vs0
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1421711
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset =
         Total ARP packets processed since reset = 0
```

```
      Total ISL encapsulated packets processed since reset = 0
      Total 802.1q encapsulated packets processed since reset = 0
      Total packets with bad IP checksums processed since reset = 0
      Total packets with bad layer 4 checksums processed since reset = 0
      Total number of bytes processed since reset = 0
      The rate of packets per second since reset = 0
      The rate of bytes per second since reset = 0
      The average bytes per packet since reset = 0
   Denied Address Information
      Number of Active Denied Attackers = 0
      Number of Denied Attackers Inserted = 0
      Number of Denied Attacker Victim Pairs Inserted = 0
      Number of Denied Attacker Service Pairs Inserted = 0
      Number of Denied Attackers Total Hits = 0
      Number of times max-denied-attackers limited creation of new entry = 0
      Number of exec Clear commands during uptime = 0
   Denied Attackers and hit count for each.
   Denied Attackers with percent denied and hit count for each.


   The Signature Database Statistics.
      The Number of each type of node active in the system (can not be reset
         Total nodes active = 0
         TCP nodes keyed on both IP addresses and both ports = 0
         UDP nodes keyed on both IP addresses and both ports = 0
         IP nodes keyed on both IP addresses = 0
      The number of each type of node inserted since reset
         Total nodes inserted = 0
         TCP nodes keyed on both IP addresses and both ports = 0
         UDP nodes keyed on both IP addresses and both ports = 0
         IP nodes keyed on both IP addresses = 0
      The rate of nodes per second for each time since reset
         Nodes per second = 0
         TCP nodes keyed on both IP addresses and both ports per second = 0
         UDP nodes keyed on both IP addresses and both ports per second = 0
         IP nodes keyed on both IP addresses per second = 0
      The number of root nodes forced to expire because of memory constraint
         TCP nodes keyed on both IP addresses and both ports = 0
      Packets dropped because they would exceed Database insertion rate limit
s = 0
   Fragment Reassembly Unit Statistics for this Virtual Sensor
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
      Number of fragments received since reset = 0
      Number of fragments forwarded since reset = 0
      Number of fragments dropped since last reset = 0
      Number of fragments modified since last reset = 0
      Number of complete datagrams reassembled since last reset = 0
      Fragments hitting too many fragments condition since last reset = 0
      Number of overlapping fragments since last reset = 0
      Number of Datagrams too big since last reset = 0
      Number of overwriting fragments since last reset = 0
      Number of Initial fragment missing since last reset = 0
      Fragments hitting the max partial dgrams limit since last reset = 0
      Fragments too small since last reset = 0
      Too many fragments per dgram limit since last reset = 0
      Number of datagram reassembly timeout since last reset = 0
      Too many fragments claiming to be the last since last reset = 0
      Fragments with bad fragment flags since last reset = 0
   TCP Normalizer stage statistics
      Packets Input = 0
      Packets Modified = 0
      Dropped packets from queue = 0
      Dropped packets due to deny-connection = 0
```

```
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
   Current Streams Denied = 0
Statistics for the TCP Stream Reassembly Unit
   Current Statistics for the TCP Stream Reassembly Unit
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   Cumulative Statistics for the TCP Stream Reassembly Unit since reset
      TCP streams that have been tracked since last reset = 0
      TCP streams that had a gap in the sequence jumped = 0
      TCP streams that was abandoned due to a gap in the sequence = 0
      TCP packets that arrived out of sequence order for their stream = 0
      TCP packets that arrived out of state order for their stream = 0
      The rate of TCP connections tracked per second since reset = 0
SigEvent Preliminary Stage Statistics
   Number of Alerts received = 0
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 0
   Number of FireOnce Intermediate Alerts = 0
   Number of Summary First Alerts = 0
   Number of Summary Intermediate Alerts = 0
   Number of Regular Summary Final Alerts = 0
   Number of Global Summary Final Alerts = 0
   Number of Active SigEventDataNodes = 0
   Number of Alerts Output for further processing = 0
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
      request-rate-limit = 0
SigEvent Action Filter Stage Statistics
   Number of Alerts received to Action Filter Processor = 0
   Number of Alerts where an action was filtered = 0
   Number of Filter Line matches = 0
   Number of Filter Line matches causing decreased DenyPercentage = 0
   Actions Filtered
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
```

```
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
                request-block-connection = 0
                request-block-host = 0
                request-snmp-trap = 0
                reset-tcp-connection = 0
                request-rate-limit = 0
          SigEvent Action Handling Stage Statistics.
             Number of Alerts received to Action Handling Processor = 0
             Number of Alerts where produceAlert was forced = 0
             Number of Alerts where produceAlert was off = 0
             Actions Performed
                deny-attacker-inline = 0
                deny-attacker-victim-pair-inline = 0
                deny-attacker-service-pair-inline = 0
                deny-connection-inline = 0
                deny-packet-inline = 0
                modify-packet-inline = 0
                log-attacker-packets = 0
                log-pair-packets = 0
                log-victim-packets = 0
                produce-alert = 0
                produce-verbose-alert = 0
--MORE--
```

ステップ 17　Web サーバの統計情報を表示します。

```
sensor# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#
```

ステップ 18　ロギング アプリケーションなど、アプリケーションの統計情報をクリアします。

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

統計情報は取得され、クリアされました。

ステップ 19　統計情報がクリアされたことを確認します。

```
sensor# show statistics logger
```

```
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
sensor#
```

統計情報はすべて 0 から始まります。

技術サポート情報の表示

画面にシステム情報を表示するか、特定の URL にシステム情報を送信するには、**show tech-support** [**page**] [**destination-url** *destination_url*] コマンドを使用します。この情報は、TAC とのトラブルシューティング ツールとして使用できます。

次のパラメータはオプションです。

- **page**：一度に 1 ページの情報として出力を表示します。

  出力の次の行を表示するには、Enter を押します。次のページの情報を表示するには、スペースバーを押します。

- **destination-url**：HTML としてフォーマットし、このコマンドの次に指定する宛先に送信する必要がある情報を示します。このキーワードを使用した場合、出力は画面に表示されません。
- *destination_url*：HTML としてフォーマットする必要がある情報を示します。URL は、情報を送信する宛先を示します。このキーワードを使用しなかった場合、情報は画面に表示されます。

技術サポート情報を表示するには、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　画面上に出力を表示します。

```
sensor# show tech-support page
```

システム情報が画面上に一度に 1 ページずつ表示されます。次のページを表示するにはスペースバーを押します。プロンプトに戻るには、Ctrl キーを押した状態で C キーを押します。

ステップ 3　出力（HTML フォーマット）をファイルに送信するには、次の手順に従います。

a. 次のコマンドを入力してから、有効な宛先を指定します。

```
sensor# show tech-support destination-url destination_url
```

次に示す種類の宛先を指定できます。

- **ftp:**：FTP ネットワーク サーバの宛先 URL です。このプレフィクスの構文は、`ftp:[[//username@location]/relativeDirectory]/filename` または `ftp:[[//username@location]//absoluteDirectory]/filename` です。

- **scp:**：SCP ネットワーク サーバの宛先 URL です。このプレフィクスの構文は、scp:[[//username@]location]/relativeDirectory]/filename または scp:[[//username@]location]//absoluteDirectory]/filename です。

たとえば、技術サポート出力をファイル /absolute/reports/sensor1Report.html に送信します。

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

password: プロンプトが表示されます。

b. このユーザ アカウントのパスワードを入力します。

Generating report: メッセージが表示されます。

バージョン情報の表示

インストールされているすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで実行中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体の設定を表示するには、**more current-config** コマンドを使用します。

バージョンおよび設定を表示するには、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　バージョン情報を表示します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.0(4)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S383.0                  2009-02-20
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS 4240-K9
Serial Number:          JMX1013K020
No license present
Sensor up-time is 23:01.
Using 1421856768 out of 1984552960 bytes of available memory (71% usage)
system is using 16.5M out of 38.5M bytes of available disk space (43% usage)
application-data is using 43.5M out of 166.8M bytes of available disk space (27%
 usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)
application-log is using 123.5M out of 513.0M bytes of available disk space (24%
 usage)


MainApp            B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
AnalysisEngine     B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CollaborationApp   B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CLI                B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500
```

```
Upgrade History:

  IPS-K9-7.0-4-E4   21:41:28 UTC Mon Feb 22 2010

Recovery Partition Version 1.1 - 7.0(4)E4

Host Certificate Valid from: 08-Apr-2009 to 09-Apr-2011
sensor#
```

（注） --MORE-- というプロンプトが表示された場合、スペースバーを押すと詳細な情報が表示され、**Ctrl を押した状態で C** を押すと出力がキャンセルされ CLI プロンプトに戻ります。

ステップ 3　設定情報を表示します。

（注） **more current-config** または **show configuration** コマンドを使用できます。

```
sensor# more current-config
! ------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2009
! ------------------------------
! Version 7.0(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S383.0   2009-02-20
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.24/25,10.89.147.126
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
```

```
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

ネットワーク接続の診断

注意　このコマンドを中断することはできません。完了するまで実行する必要があります。

基本的なネットワーク接続を診断するには、**ping** *ip_address* [**count**] コマンドを使用します。

基本的なネットワーク接続を診断するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　診断するアドレスに対して ping を実行します。

```
sensor# ping ip_address count
```

count は、送信するエコー要求の数です。数を指定しなかった場合は、4 回の要求が送信されます。範囲は 1 ～ 10,000 です。

成功した ping の例

```
sensor# ping 10.89.146.110 6
PING 10.89.146.110 (10.89.146.110): 56 data bytes
64 bytes from 10.89.146.110: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 10.89.146.110: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 10.89.146.110: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 10.89.146.110: icmp_seq=5 ttl=61 time=0.2 ms

--- 10.89.146.110 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.3 ms
```

成功しなかった ping の例

```
sensor# ping 172.21.172.1 3
```

```
PING 172.21.172.1 (172.21.172.1): 56 data bytes

--- 172.21.172.1 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

アプライアンスのリセット

アプライアンスで実行されているアプリケーションをシャットダウンし、アプライアンスをリブートするには、**reset [powerdown]** コマンドを使用します。可能な場合は **powerdown** オプションを使用して、アプライアンスの電源をオフにするか、電源をオフにできるようなアプライアンスの状態を維持することができます。

シャットダウン（アプリケーションの停止）は、コマンドが実行されるとただちに開始されます。シャットダウンにはしばらく時間がかかり、その間も CLI コマンドは使用できますが、セッションは警告なしで終了されます。

アプライアンスをリセットするには、次の手順に従います。

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　すべてのアプリケーションを停止し、アプライアンスをリブートするには、手順 2 および 3 を実行します。それ以外の場合に、アプライアンスの電源をオフにするには、手順 4 および 5 を実行します。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 3　**yes** と入力してリセットを続行します。

```
sensor# yes
Request Succeeded.
sensor#
```

ステップ 4　すべてのアプリケーションを停止し、アプライアンスの電源をオフにします。

```
sensor# reset powerdown
Warning: Executing this command will stop all applications and power off the node if
possible. If the node can not be powered off it will be left in a state that is safe to
manually power down.
Continue with reset? []:
```

ステップ 5　**yes** と入力し、リセットと電源オフを続行します。

```
sensor# yes
Request Succeeded.
sensor#
```

詳細情報

モジュールをリセットするには、次の各手順を参照してください。

- 「AIM IPS のリブート、リセット、およびシャットダウン」（P.18-18）
- 「AIP SSM のリロード、シャットダウン、リセット、および回復」（P.19-11）

- 「IDSM2 のリセット」（P.20-41）
- 「NME IPS のリブート、リセット、およびシャットダウン」（P.21-12）

コマンド履歴の表示

現在のメニューで入力したコマンドのリストを取得するには、**show history** コマンドを使用します。リスト内のコマンドの最大数は 50 です。

最近使用したコマンドのリストを取得するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　EXEC モードで使用したコマンドの履歴を表示します。

```
sensor# show history
clear line
configure terminal
show history
```

ステップ 3　ネットワーク アクセス モードで使用したコマンドの履歴を表示します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor (config-net)# show history
show settings
show settings terse
show settings | include profile-name|ip-address
exit
show history
sensor (config-net)#
```

ハードウェア コンポーネントの表示

（注）　**show inventory** コマンドは、AIM IPS、AIP SSM、IDSM2、または NME IPS などの IPS モジュールには適用されません。

PEP 情報を表示するには、**show inventory** コマンドを使用します。このコマンドによって、センサーの PID、VID、および SN から構成される UDI 情報が表示されます。PEP 情報は、CLI を通じてハードウェアのバージョンとシリアル番号を取得するための簡単な方法を提供します。

PEP 情報を表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　PEP 情報を表示します。

```
sensor# show inventory

Name: "Chassis", DESCR: "IPS 4255 Intrusion Prevention Sensor"
PID: IPS 4255-K9, VID: V01 , SN: JAB0815R017

Name: "Power Supply", DESCR: ""
```

```
PID: ASA-180W-PWR-AC, VID: V01 , SN: 123456789AB
sensor#

sensor# show inventory

Name: "Module", DESCR: "ASA 5500 Series Security Services Module-20"
PID: ASA-SSM-20, VID: V01 , SN: JAB0815R036
sensor#

sensor-4240# show inventory

Name: "Chassis", DESCR: "IPS 4240 Appliance Sensor"
PID: IPS 4240-K9, VID: V01 , SN: P3000000653
sensor-4240#
```

TAC に連絡を取るときに、この情報を使用できます。

IP パケットのルートのトレース

注意　このコマンドを中断することはできません。完了するまで実行する必要があります。

宛先までの IP パケットのルートを表示するには、**trace** *ip_address count* コマンドを使用します。*ip_address* オプションは、ルートをトレースするシステムのアドレスです。*count* オプションでは、取得するポップ数を定義できます。デフォルトは 4 です。有効な値は 1 ～ 256 です。

IP パケットのルートをトレースするには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　トレースする IP パケットのルートを表示します。

```
sensor# trace 10.1.1.1
traceroute to 10.1.1.1 (10.1.1.1), 4 hops max, 40 byte packets
 1  10.89.130.1 (10.89.130.1)  0.267 ms  0.262 ms  0.236 ms
 2  10.89.128.17 (10.89.128.17)  0.24 ms *  0.399 ms
 3  * 10.89.128.17 (10.89.128.17)  0.424 ms *
 4  10.89.128.17 (10.89.128.17)  0.408 ms *  0.406 ms
sensor#
```

ステップ 3　デフォルトの 4 を超えるホップを取得するようにルートを設定するには、*count* オプションを使用します。

```
sensor# trace 10.1.1.1 8
traceroute to 10.1.1.1 (10.1.1.1), 8 hops max, 40 byte packets
 1  10.89.130.1 (10.89.130.1)  0.35 ms  0.261 ms  0.238 ms
 2  10.89.128.17 (10.89.128.17)  0.36 ms *  0.344 ms
 3  * 10.89.128.17 (10.89.128.17)  0.465 ms *
 4  10.89.128.17 (10.89.128.17)  0.319 ms *  0.442 ms
 5  * 10.89.128.17 (10.89.128.17)  0.304 ms *
 6  10.89.128.17 (10.89.128.17)  0.527 ms *  0.402 ms
 7  * 10.89.128.17 (10.89.128.17)  0.39 ms *
 8  10.89.128.17 (10.89.128.17)  0.37 ms *  0.486 ms
sensor#
```

サブモード設定の表示

現在の設定の内容を表示するには、任意のサブモードで、**show settings** [**terse**] コマンドを使用します。

サブモードに対する現在の設定を表示するには、次の手順に従います。

ステップ 1　CLI にログインします。

ステップ 2　ARC サブモードに対する現在の設定を表示します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor (config-net)# show settings
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ------------------------------------------------
      profile-name: 2admin
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: pix default:
      ------------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
      profile-name: insidePix
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username:  <defaulted>
      ------------------------------------------------
      profile-name: qatest
      ------------------------------------------------
         enable-password: <hidden>
```

```
      password: <hidden>
      username:  <defaulted>
   ------------------------------------------------
   profile-name: fwsm
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: outsidePix
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: cat
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username:  <defaulted>
   ------------------------------------------------
   profile-name: rcat
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ------------------------------------------------
   profile-name: nopass
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username:  <defaulted>
   ------------------------------------------------
   profile-name: test
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: pix default:
   ------------------------------------------------
   profile-name: sshswitch
   ------------------------------------------------
      enable-password: <hidden>
      password: <hidden>
      username: cisco default:
   ------------------------------------------------
------------------------------------------------
cat6k-devices (min: 0, max: 250, current: 1)
------------------------------------------------
   ip-address: 10.89.147.61
   ------------------------------------------------
      communication: telnet default: ssh-3des
      nat-address: 0.0.0.0 <defaulted>
      profile-name: cat
      block-vlans (min: 0, max: 100, current: 1)
      ------------------------------------------------
         vlan: 1
         ------------------------------------------------
            pre-vacl-name:  <defaulted>
            post-vacl-name:  <defaulted>
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
------------------------------------------------
router-devices (min: 0, max: 250, current: 1)
```

```
   ------------------------------------------------
      ip-address: 10.89.147.54
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ------------------------------------------------
            interface-name: fa0/0
            direction: in
            ------------------------------------------------
               pre-acl-name:  <defaulted>
               post-acl-name:  <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ------------------------------------------------
      ip-address: 10.89.147.10
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: insidePix
      ------------------------------------------------
      ip-address: 10.89.147.82
      ------------------------------------------------
         communication: ssh-3des <defaulted>
         nat-address: 0.0.0.0 <defaulted>
         profile-name: f1
      ------------------------------------------------
   ------------------------------------------------
sensor (config-net)#
```

ステップ 3　terse モードで ARC 設定を表示します。

```
sensor(config-net)# show settings terse
   general
   ------------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 default: 250
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ------------------------------------------------
   user-profiles (min: 0, max: 250, current: 11)
   ------------------------------------------------
```

```
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
   ------------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.61
   ------------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ------------------------------------------------
      ip-address: 10.89.147.54
   ------------------------------------------------
   firewall-devices (min: 0, max: 250, current: 2)
   ------------------------------------------------
      ip-address: 10.89.147.10
      ip-address: 10.89.147.82
   ------------------------------------------------
sensor(config-net)#
```

ステップ 4　**include** キーワードを使用すると、出力にフィルタをかけて設定を表示できます。たとえば、ARC 構成のプロファイル名と IP アドレスだけを表示します。

```
sensor(config-net)# show settings | include profile-name|ip-address
      profile-name: 2admin
      profile-name: r7200
      profile-name: insidePix
      profile-name: qatest
      profile-name: fwsm
      profile-name: outsidePix
      profile-name: cat
      profile-name: rcat
      profile-name: nopass
      profile-name: test
      profile-name: sshswitch
      ip-address: 10.89.147.61
         profile-name: cat
      ip-address: 10.89.147.54
         profile-name: r7200
      ip-address: 10.89.147.10
         profile-name: insidePix
      ip-address: 10.89.147.82
         profile-name: test
sensor(config-net)#
```