CHAPTER 17

管理タスク

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在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、センサーの管理面で役立つ手順について説明します。次のような構成になっています。

IPS SSP パスワードの回復

ここでは、IPS SSP のパスワードを回復する方法について説明します。次のような構成になっています。

IPS SSP パスワードの回復

（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。

CLI または ASDM を使用して IPS SSP のデフォルト（**cisco**）にパスワードをリセットできます。パスワードをリセットすると、IPS SSP がリブートします。リブート中は、IPS サービスを使用できません。

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の **cisco** にリセットします。ASA 5500 シリーズ適応型セキュリティ アプライアンスは、ROMMON confreg ビットを 0x7 に設定してから、IPS SSP をリブートします。この ROMMON ビットにより、GRUB メニューがデフォルトでオプション 2（**パスワードのリセット**）になります。

指定したスロット内の IPS SSP に搭載されている IPS のバージョンがパスワード回復をサポートしていない場合、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 バーから、[Tools] > [IPS Password Reset] を選択します。

（注）　このオプションは、IPS モジュールがインストールされていなければ表示されません。

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。リセットに失敗した場合は、適応型セキュリティ アプライアンスに正しい ASA ソフトウェアが搭載されていること、および IPS SSP に IPS 7.1 以降が搭載されている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。IPS SSP がリブートします。

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化されたセンサーでパスワードを回復しようとすると、プロセスはエラーや警告なしに進行しますが、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ず、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。CLI、IDM、または IME を使用してパスワード回復をディセーブルにできます。

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。

```
ips-ssp# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
ips-ssp(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。

```
ips-ssp(config-hos)# password-recovery disallowed
```

IDM または 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、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、パスワード回復がイネーブルかどうかを確認します。

パスワード回復がイネーブル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。

```
ips-ssp# configure terminal
ips-ssp (config)# service host
ips-ssp (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタリングされた出力で設定を表示することにより、パスワード回復の状態を確認します。

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

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ときは、次の点に注意します。

- ROMMON プロンプト、GRUB メニュー、スイッチ CLI、またはルータ CLI からは、センサー設定内でパスワード回復がディセーブルになっているかどうかを判別できません。パスワード回復を試みると、常に成功しているように見えます。ディセーブルになっていた場合、パスワードは **cisco** にリセットされません。この場合、センサーのイメージを再作成するしか方法はありません。
- パスワード回復は、ホスト設定でディセーブルにできます。外部メカニズムを使用するプラットフォームの場合、コマンドを実行してパスワードをクリアすることができますが、IPS でパスワード回復がディセーブルになっていると、IPS は、パスワード回復が許可されていないことを検出し、外部からの要求を拒否します。
- パスワード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。

センサー データベースのクリア

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

注意　TAC の指示に基づく場合、あるいは蓄積した状態情報をクリアしてクリーンなデータベースで起動する必要がある条件のテストの場合を除き、このコマンドの使用を推奨しません。

オプション

次のオプションが適用されます。

- *virtual-sensor*：センサー上に設定された仮想センサーの名前を指定します。
- **all**：すべてのノード、インスペクタ、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 アラートが破棄されます。

- **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 リストを含む、パケット データベースの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 カウント構造を含む、アラート データベースをクリアします。
- **inspectors**：ノードのインスペクタ リストをクリアします。インスペクタ リストは、センサーが実行している間に収集されたパケットの動作と監視結果を示します。

センサー データベースのクリア

センサー データベースのクリアには、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　センサー データベース全体をクリアします。

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

ステップ 3　**yes** を入力してセンサー上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。

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

ステップ 5　**yes** を入力してパケット 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上のアラート データベースをクリアします。

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

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

ステップ 8　センサー上のインスペクタ リストをクリアします。

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

ステップ 9　**yes** を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 カテゴリは赤色と緑色で評価され、赤色が重大であることを示します。

オプション

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全体的なセンサーのヘルス レーティングに適用するかどうか選択できます。
- **bypass-policy {enable | disable} {true | false} status {green | yellow | red}**：バイパス モードがアクティブかどうかを確認して、それを全体的なセンサーのヘルス レーティングに適用するかどうか選択できます。

（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 で実行されるアクティビティのタイプに応じて、フェールオープン、フェールクローズ、フェールオーバーのいずれかを実行します。

- **enable-monitoring {true | false}**：センサーのヘルスとセキュリティをモニタするかどうか選択できます。
- **event-retrieval-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*：いつ最後のイベントを取得したか、しきい値を設定して、それを全体的なセンサーのヘルス レーティングに適用できます。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 など外部のモニタリング 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刻を記録します。外部のイベント モニタリングを実行しない場合は、event retrieval policy をディセーブルにします。

- **global-correlation-policy {enable | disable} {true | false}**：このメトリックを全体的なセンサーのヘルス レーティングに適用できます。
- **heartbeat-events {enable | disable}** *seconds*：指定した秒単位の間隔でハートビート イベントを送信できるようにして、それを全体的なセンサーのヘルス レーティングに適用できます。間隔の範囲は、15 ～ 86400 秒です。
- **inspection-load-policy {enable | disable} {true | false} red-threshold yellow-threshold** *seconds*：インスペクション ロードのしきい値を設定できます。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インターフェイスが 1 つ以上ダウンしているかどうかを確認して、それを全体的なセンサーのヘルス レーティングに適用するかどうか選択できます。
- **license-expiration-policy {enable | disable} {true | false} red-threshold yellow-threshold**：ライセンスが期限切れになる時点にしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。しきい値の範囲は 0 ～ 4294967295 秒です。
- **memory-usage-policy {enable | disable} {true | false} red-threshold yellow-threshold**：メモリ使用状況のパーセンテージしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。範囲は 0 ～ 100 です。
- **missed-packet-policy {enable | disable} {true | false} red-threshold yellow-threshold**：欠落パケットのパーセンテージしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。
- **network-participation-policy {enable | disable} {true | false}**：このメトリックを全体的なセンサーのヘルス レーティングに適用できます。
- **persist-security-status**：セキュリティ ステータスを下げる最新のイベントの発生後に、低セキュリティが続く期間を分単位で設定できます。
- **signature-update-policy {enable | disable} {true | false} red-threshold yellow-threshold**：最後にシグニチャがアップデートされてから経過した日数のしきい値を設定して、このメトリックを全体的なセンサーのヘルス レーティングに適用するかどうか設定できます。しきい値の範囲は 0 ～ 4294967295 秒です。

ヘルス統計情報の設定

センサーにヘルス統計情報を設定するには、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 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。

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

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

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

ステップ 4　バイパス ポリシーに対してメトリックをイネーブルにします。

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

ステップ 5　IPS-SSP ヘルスおよびセキュリティ モニタリングに対してメトリックをイネーブルにします。

```
ips-ssp(config-hea)# enable-monitoring true
ips-ssp(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のしきい値を設定します。

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

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

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

ステップ 8　指定した秒単位の間隔で送信されるハートビート イベントに対してメトリックをイネーブルにします。

```
ips-ssp(config-hea)# heartbeat-events enable 20000
ips-ssp(config-hea)#
```

ステップ 9　インスペクション ロードのしきい値を設定します。

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

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

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

ステップ 12　メモリ使用状況のしきい値を設定します。

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

ステップ 13　欠落パケットのしきい値を設定します。

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

ステップ 14　セキュリティ ステータスを下げる最新のイベントの発生後に、低セキュリティが続く期間を分単位で設定します。

```
ips-ssp(config-hea)# persist-security-status 10
ips-ssp(config-hea)#
```

ステップ 15　最後にシグニチャがアップデートされてからの日数を設定します。

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

ステップ 16　設定値を確認します。

```
ips-ssp(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
   ------------------------------------------------
ips-ssp(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。

```
ips-ssp(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** を入力して変更を破棄します。

センサーの全体的なヘルス ステータスの表示

特権 EXEC モードで **show health** コマンドを使用して、センサーの全体的なヘルス ステータス情報を表示します。ヘルス ステータス カテゴリは赤色と緑色で評価され、赤色が重大であることを示します。

注意　センサーを初めて起動するときは、センサーが完全に起動して動作するまで、特定のヘルス メトリック ステータスが赤色になりますが、これは正常な状態です。

（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 で実行されるアクティビティのタイプに応じて、フェールオープン、フェールクローズ、フェールオーバーのいずれかを実行します。

センサーの全体的なヘルス ステータスを表示するには、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　センサーのヘルスおよびセキュリティ ステータスを表示します。

```
ips-ssp# 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
ips-ssp#
```

バナー ログインの作成

banner login コマンドを使用して、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。

```
ips-ssp# configure terminal
```

ステップ 3　バナー ログインを作成します。

```
ips-ssp(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
ips-ssp(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？ キーを押すか、Ctrl キーを押した状態で V キーと Enter を押します。これらは ^M と表現されます。

例

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

ステップ 5　バナー ログインを削除します。ログイン時にバナーが表示されなくなります。

```
ips-ssp(config)# no banner login
```

CLI セッションの終了

clear line *cli_id* [**message**] コマンドを使用して、別の CLI セッションを終了します。**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。

オプション

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 番号を指定します。**show users** コマンドを使用して、CLI ID 番号を確認します。
- **message**：受信ユーザに送信するメッセージを指定します。

注意　**clear line** コマンドでは、CLI ログイン セッションのクリアしかできません。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。

最大セッション数に達した場合に、管理者がログインしようとすると、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]
```

最大セッション数が開かれている場合に、オペレータまたはビューアがログインしようとすると、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 セッションの終了

CLI セッションを終了するには、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。

（注）　オペレータおよびビューアは、現在のログインと同じユーザ名のある行しかクリアできません。

ステップ 2　ログイン セッションに関連付けられた CLI ID 番号を確認します。

```
ips-ssp# 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。

```
ips-ssp# clear line cli_id message
Message[]:
```

例

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

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

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

ターミナル プロパティの変更

terminal [length] *screen _length* コマンドを使用して、ログイン セッションのターミナル プロパティを変更します。*screen_ length* オプションによって、--more-- プロンプトが表示される前に、画面上に表示される行数を設定できます。値をゼロにすると、出力は一時停止しなくなります。デフォルト値は 24 行です。

（注）　ターミナル セッションの一部のタイプは画面長を指定する必要がありません。これは、一部のリモート ホストで、指定した画面長を取得できるためです。

ターミナル プロパティを変更するには、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　複数画面の出力間で一時停止しないようにするには、screen length の値に 0 を使用します。

```
ips-ssp# terminal length 0
```

（注）　screen length の値は、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 を一時停止して、--more-- プロンプトを表示するには、*screen length* の値に 10 を使用します。

```
ips-ssp# terminal length 10
```

イベントの設定

ここでは、イベント ストアからイベントを表示したりクリアしたりする方法について説明します。次のような構成になっています。

- 「イベントの表示」（P.17-13）
- 「イベント ストアからのイベントのクリア」（P.17-16）

イベントの表示

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*] コマンドを使用して、イベント ストアのイベントを表示します。

開始時刻に開始されているイベントが表示されます。開始時刻を指定しない場合、現時点で開始されているイベントが表示されます。イベント タイプを指定しないと、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。

オプション

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。シグニチャがネットワーク アクティブによってトリガーされると常に、分析エンジンによってアラート イベントが生成されます。レベルが選択されていない場合（informational、low、medium、または high）、すべてのアラート イベントが表示されます。
- **include-traits**：指定された特徴を持つアラートを表示します。
- **exclude-traits**：指定された特徴を持つアラートを表示しません。
- **traits**：特徴ビット位置を 10 進数で指定します（0 ～ 15）。
- **min-threat-rating**：脅威レーティングがこの値以上である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である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。エラーの条件が検出されると、サービスによってエラー イベントが生成されます。レベルが選択されていない場合（warning、error、または fatal）、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。この名前の変更は、Cisco IPS 7.1 の IDM、IME、および CLI に完全には実装されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定した過去の時、分、および秒から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、分、秒。

（注）　**show events** コマンドは、指定したイベントが使用可能になるまで、イベントを表示し続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベントの表示

イベント ストアのイベントを表示するには、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　現在開始しているイベントをすべて表示します。

```
ips-ssp# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2011/01/07 04:41:45 2011/01/07 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: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

Ctrl キーを押した状態で C キーを押すまで、フィードはすべてのイベントを表示し続けます。

ステップ 3　2011 年 2 月 9 日 10:00 a.m に開始されたブロック要求を表示します。

```
ips-ssp# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 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
ips-ssp#
```

ステップ 4　2011 年 2 月 9 日 10:00 a.m. に開始された警告レベルのエラーを表示します。

```
ips-ssp# show events error warning 10:00:00 Feb 9 2011
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2011/01/07 04:49:25 2011/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
ips-ssp# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2011/03/02 14:15:59 2011/03/02 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　30 秒前に開始されたイベントを表示します。

```
ips-ssp# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 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: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベント ストアからのイベントのクリア

clear events コマンドを使用して、イベント ストアをクリアします。

イベント ストアからイベントをクリアするには、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　イベント ストアをクリアします。

```
ips-ssp# 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** を入力して、イベントをクリアします。

システム クロックの表示

show clock [**detail**] コマンドを使用して、システム クロックを表示します。**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、時刻が信頼できる（正確であると信じられる）かどうかを示す信頼性フラグを保持しています。システム クロックがタイミング ソース（NTP など）によって設定されている場合は、このフラグが設定されます。

表 17-1 に、システム クロック フラグを示します。

表 17-1　システム クロック フラグ

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

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　システム クロックを表示します。

```
ips-ssp# show clock
22:57:43 UTC Fri Aug 13 2010
```

ステップ 3　システム クロックを詳細表示します。これは、センサーが時刻を適応型セキュリティ アプライアンスから取得していることを示します。

```
ips-ssp# show clock detail
22:58:08 UTC Fri Aug 13 2010
Time source is chassis
Summer time starts 03:00:00 UTC Sun Mar 14 2010
Summer time stops 01:00:00 UTC Sun Nov 07 2010
```

ステップ 4　システム クロックを詳細表示します。これは、時刻源が設定されていないことを示しています。

```
ips-ssp# show clock detail
*20:09:43 UTC Thu Apr 03 2010
No time source
Summer time starts 03:00:00 UTC Sun Mar 09 2010
Summer time stops 01:00:00 UTC Sun Nov 02 2010
```

拒否攻撃者リストのクリア

show statistics denied-attackers コマンドを使用して、拒否攻撃者リストを表示します。**clear denied-attackers** [*virtual_sensor*] [**ip-address** *ip_address*] コマンドを使用して、拒否攻撃者リストを削除し、仮想センサー統計情報をクリアします。

センサーがインライン モードで動作するよう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シグニチャを設定できます。この結果、センサーが単一のパケット、接続、および特定の攻撃者を検出した場合に、これらは拒否されます（つまり、送信されません）。

シグニチャが起動されると、攻撃者は拒否され、リストに追加されます。センサー管理の一部として、リストの削除、またはリスト内の統計情報のクリアが必要な場合があります。

オプション

次のオプションが適用されます。

- *virtual_sensor*：（任意）拒否攻撃者リストをクリアする必要がある仮想センサーを指定します。
- *ip_address*：（任意）クリアする IP アドレスを指定します。

拒否攻撃者リストの表示、削除、およびクリア

拒否攻撃者リストの表示、リストの削除、統計情報のクリアを行うには、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　拒否された IP アドレスのリストを表示します。統計情報は、この時点で 2 つの IP アドレスが拒否されていることを示します。

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

ステップ 3　拒否攻撃者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** を入力して、リストをクリアします。

ステップ 5　特定の仮想センサーの拒否攻撃者リストを削除します。

```
ips-ssp# 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** を入力して、リストをクリアします。

ステップ 7　特定の仮想センサーの拒否攻撃者リストから、特定の IP アドレスを削除します。

```
ips-ssp# clear denied-attackers vs0 ip-address 192.0.2.1
Warning: Executing this command will delete ip address 192.0.2.1 from the list of
attackers being denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 8　**yes** を入力して、リストをクリアします。

ステップ 9　リストをクリアしたことを確認します。**show statistics denied-attackers** または **show statistics virtual-sensor** コマンドを使用できます。

```
ips-ssp# 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.
ips-ssp#

ips-ssp# 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　統計情報のみをクリアします。

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

ステップ 11　統計情報をクリアしたことを確認します。Number of Active Denied Attackers および Number of exec Clear commands during uptime カテゴリ以外の統計情報がすべてクリアされました。リストがクリアされたかどうかを認識することが重要です。

```
ips-ssp# 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
```

ポリシー リストの表示

EXEC モードで **list {anomaly-detection-configurations | event-action-rules-configurations | signature-definition-configurations}** を使用して、これらのコンポーネントのポリシーのリストを表示します。ファイル サイズはバイト単位です。N/A の状態の仮想センサーは、ポリシーが仮想センサーに割り当てられていないことを示します。

センサー上のポリシーのリストを表示するには、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　異常検出のポリシーのリストを表示します。

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

ステップ 3　イベント アクション規則のポリシーのリストを表示します。

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

ステップ 4　シグニチャ定義のポリシーのリストを表示します。

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

統計情報の表示

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]** コマンドを使用して、各センサー アプリケーションの統計情報を表示します。

show statistics {**anomaly-detection** | **denied-attackers** | **os-identification** | **virtual-sensor**} [***name*** | **clear]** を使用して、すべての仮想センサーについてこれらのコンポーネントの統計情報を表示します。仮想センサー名を指定すると、その仮想センサーの統計情報のみが表示されます。

（注）　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 識別アプリケーションには、**clear** オプションを使用できません。

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　分析エンジンの統計情報を表示します。

```
ips-ssp# 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
ips-ssp#
```

ステップ 3　異常検出の統計情報を表示します。

```
ips-ssp# 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 2011
   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 2011
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
ips-ssp#
```

ステップ 4　認証の統計情報を表示します。

```
ips-ssp# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
ips-ssp#
```

ステップ 5　システムの拒否攻撃者の統計情報を表示します。

```
ips-ssp# 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.


ips-ssp#
```

ステップ 6　イベント サーバの統計情報を表示します。

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

ステップ 7　イベント ストアの統計情報を表示します。

```
ips-ssp# 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
ips-ssp#
```

ステップ 8　グローバル相関の統計情報を表示します。

```
ips-ssp# 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.
ips-ssp#
```

ステップ 9　ホストの統計情報を表示します。

```
ips-ssp# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2011
   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 2011
    =   Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
    =   Success
   lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2011
    =   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 2011

ips-ssp#
```

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。

```
ips-ssp# 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
ips-ssp#
```

ステップ 11　ARC の統計情報を表示します。

```
ips-ssp# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 192.0.2.1
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.3
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 192.0.2.4
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 192.0.2.5
      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 = 192.0.2.6
      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 = 192.0.2.7
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 192.0.2.8
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 192.0.2.9
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 192.0.2.10
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 192.0.2.11
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 203.0.113.1
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 203.0.113.24
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 209.165.201.30
         Mask = 255.255.255.224
         BlockMinutes =
ips-ssp#
```

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。

```
ips-ssp# 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
ips-ssp#
```

ステップ 13　OS 識別の統計情報を表示します。

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

ステップ 14　SDEE サーバの統計情報を表示します。

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

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。

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

ステップ 16　仮想センサーの統計情報を表示します。

```
ips-ssp# 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。

```
ips-ssp# 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
ips-ssp#
```

ステップ 18　ロギング アプリケーションなどのアプリケーションの統計情報をクリアします。統計情報が取得され、クリアされます。

```
ips-ssp# 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
```

ステップ 19　統計情報がクリアされたことを確認します。これによって統計情報はすべて 0 から始まります。

```
ips-ssp# 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
ips-ssp#
```

技術サポート情報の表示

show tech-support [**page**] [**destination-url** *destination_url*] コマンドを使用して、画面にシステム情報を表示するか、その情報を特定の URL に送信します。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。

オプション

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。

  Enter を押して出力の次の行を表示するか、Space を使用して次のページの情報を表示します。
- **destination-url**：HTML としてフォーマットし、このコマンドに続く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すると、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いと、画面に情報が表示されます。

技術サポート情報の表示

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。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 Space 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。

```
ips-ssp# show tech-support page
```

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、次の手順を実行します。

a. 次のコマンドを入力し、その後に有効な宛先を指定します。`password:` プロンプトが表示されます。

```
ips-ssp# 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。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。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` に送信するには、

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

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。

```
ips-ssp# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          ABC1234DEFG
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

ips-ssp#
#
```

（注） --MORE-- というプロンプトが表示された場合、Space を押して詳細な情報を表示するか、Ctrl キーを押した状態で C キーを押して出力をキャンセルし、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。

```
ips-ssp# more current-config
! ------------------------------
! Current configuration last modified Thu Aug 12 18:52:21 2010
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S503.0   2010-07-22
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
general
global-overrides-status Enabled
exit
risk-categories
yellow-threat-threshold 70
exit
exit
! ------------------------------
service host
network-settings
host-ip 192.0.2.0/24,255.255.255.0
host-name ips-ssp
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server disabled
dns-secondary-server disabled
dns-tertiary-server disabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option recurring
summertime-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
```

```
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
sig-description
sig-comment asdf
exit
status
enabled false
exit
exit
signatures 1004 0
sig-description
sig-comment asdf
exit
exit
signatures 1006 0
status
enabled false
exit
exit
signatures 19639 0
status
enabled false
exit
exit
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
network-participation partial
exit
! ------------------------------
service analysis-engine
virtual-sensor vs1
exit
exit
ips-ssp#
```

ネットワークの接続性の診断

ping *ip_address* [**count**] コマンドを使用して、基本的なネットワークの接続性を診断します。

注意　このコマンドには、コマンド割り込みは使用できません。完了まで実行する必要があります。

基本的なネットワークの接続性を診断するには、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　目的のアドレスを ping します。count は、送信するエコー要求の数です。数を指定しない場合、4 回の要求が送信されます。範囲は 1 ～ 10,000 です。

```
ips-ssp# ping ip_address count
```

正常な ping の例

```
ips-ssp# ping 192.0.2.1 6
PING 192.0.2.1 (192.0.2.1): 56 data bytes
64 bytes from 192.0.2.1: icmp_seq=0 ttl=61 time=0.3 ms
64 bytes from 192.0.2.1: icmp_seq=1 ttl=61 time=0.1 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=61 time=0.1 ms
64 bytes from 192.0.2.1: icmp_seq=3 ttl=61 time=0.2 ms
64 bytes from 192.0.2.1: icmp_seq=4 ttl=61 time=0.2 ms
64 bytes from 192.0.2.1: icmp_seq=5 ttl=61 time=0.2 ms

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

失敗した ping の例

```
ips-ssp# ping 172.16.0.0 3
PING 172.16.0.0 (172.16.0.0): 56 data bytes

--- 172.16.0.0 ping statistics ---
3 packets transmitted, 0 packets received, 100% packet loss
ips-ssp#
```

コマンド履歴の表示

show history コマンドを使用して、現在のメニューで入力したコマンドのリストを取得します。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　EXEC モードで使用したコマンドの履歴を表示します。

```
ips-ssp# 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。

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

IP パケットのルートのトレース

trace *ip_address count* コマンドを使用して、IP パケットが宛先まで送られるルートを表示します。*ip_address* オプションはルートをトレースする先のシステムのアドレスです。*count* オプションで、実行するホ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。

注意　このコマンドに対して使用できる、コマンド割り込みはありません。完了まで実行する必要があります。

IP パケットのルートをトレースするには、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　目的の IP パケットのルートを表示します。

```
ips-ssp# trace 10.0.0.1
traceroute to 10.0.0.1 (10.0.0.1), 4 hops max, 40 byte packets
 1  192.0.2.2 (192.0.2.2)  0.267 ms  0.262 ms  0.236 ms
 2  192.0.2.12 (192.0.2.12)  0.24 ms *  0.399 ms
 3  * 192.0.2.12 (192.0.2.12)  0.424 ms *
 4  192.0.2.12 (192.0.2.12)  0.408 ms *  0.406 ms
ips-ssp#
```

ステップ 3　デフォルトの 4 より多くのホップを実行するルートを設定します。*count* オプションを使用します。

```
ips-ssp# trace 10.0.0.1 8
traceroute to 10.0.0.1 (10.0.0.1), 8 hops max, 40 byte packets
 1  192.0.2.2 (192.0.2.2)  0.35 ms  0.261 ms  0.238 ms
 2  192.0.2.12 (192.0.2.12)  0.36 ms *  0.344 ms
 3  * 192.0.2.12 (192.0.2.12)  0.465 ms *
 4  192.0.2.12 (192.0.2.12)  0.319 ms *  0.442 ms
 5  * 192.0.2.12 (192.0.2.12)  0.304 ms *
 6  192.0.2.12 (192.0.2.12)  0.527 ms *  0.402 ms
 7  * 192.0.2.12 (192.0.2.12)  0.39 ms *
 8  192.0.2.12 (192.0.2.12)  0.37 ms *  0.486 ms
ips-ssp#
```

サブモード設定の表示

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

サブモードの現在の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　ARC サブモードの現在の設定を表示します。

```
ips-ssp# configure terminal
ips-ssp (config)# service network-access
ips-ssp (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
      ---------------------------------------------
   ---------------------------------------------
ips-ssp (config-net)#
```

ステップ 3　簡単なモードで ARC 設定を表示します。

```
ips-ssp(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
   ------------------------------------------------
ips-ssp(config-net)#
```

ステップ 4　**include** キーワードを使用して、フィルタ処理された出力に設定を表示できます。たとえば、ARC 設定のプロファイル名と IP アドレスだけを表示できます。

```
ips-ssp(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
ips-ssp(config-net)#
```