CHAPTER 2

デバイス リストの設定

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

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

[Device List] ペインでデバイスを IME に追加し、各デバイスに関する重要な情報を表示できます。この章では、[Device List] ペインとデバイスの追加方法について説明します。内容は次のとおりです。

[Device List] ペイン

IME は、最大 10 台の Cisco IPS デバイスを管理します。[Device List] ペインの上半分には、各デバイスに関連する情報が表示されます。

ペインの右隅にある列ボタンをクリックして、[Choose Columns to Display] ダイアログボックスを表示し、表示する列や非表示にする列をカスタマイズできます。

このペインから、デバイス リストのセンサーを追加、編集、または削除できます。センサーに対するヘルスおよびイベント接続を開始および停止したり、センサーのステータスを表示したりすることができます。ping、trace route、whois、DNS ルックアップなどのツールを使用して、センサーに関する情報を取得することもできます。

[Device List] テーブルの [Add]、[Edit]、[Delete]、[Start]、[Stop]、[Status]、[Tools] ボタンを使用できます。テーブルでセンサーを選択して、右クリック メニューを使用することもできます。

[Device List] ペインの下半分には、IME ヘルス モニタリング センターにより、ペインの上半分で選択したセンサーに関する詳細が表示されます。ここに表示されるデータは、カスタマイズ可能なダッシュボード ガジェットの情報と一致します。

[Device Details] ペインには、選択されたセンサーに関する次の詳細が表示されます。

- [Sensor Health]：センサーおよびネットワーク セキュリティのヘルス情報がグラフ形式で表示されます。

  センサーのヘルスおよびネットワーク セキュリティのグラフの横にある [Details] をクリックすると、センサーよびネットワーク セキュリティのヘルス状態について固有の情報を取得できます。

  センサー ヘルス メトリックを変更する場合は、[Details] > [Configure Sensor Health Metrics] を選択します。[Configuration] > *sensor_name* > [Sensor Management] > [Sensor Health] へ移動し、ヘルス メトリックを再設定できます。

  脅威のしきい値を変更する場合は、[Details] > [Configure Thresholds] を選択します。[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Risk Category] へ移動し、脅威のしきい値を設定できます。

  ネットワーク セキュリティ ヘルスをリセットする場合は、[Details] > [Reset Health Status] を選択します。[Configuration] > *sensor_name* > [Sensor Monitoring] > [Properties] > [Reset Network Security Health] へ移動し、ネットワーク セキュリティ ヘルスのステータスと計算をリセットできます。

- [Sensor Information]：ホスト名、IPS バージョン、センサーがインライン バイパスを使用しているかどうか、検知インターフェイスの合計、最後の設定更新、センサーの IP アドレス、デバイス タイプ、合計メモリ、合計データ ストレージが表示されます。

  [Analysis Engine Status] には、分析エンジンが動作しているかどうか、またはその状態を表示できます。

- [CPU, Memory, and & Load]：CPU、メモリ、センサー負荷の使用量、がグラフ形式で表示されます。

  検査負荷グラフの横にある [Details] をクリックすると、検査負荷の判断方法の詳細な説明が表示されます。

- [Licensing]：関連するライセンス、シグニチャ バージョン、およびシグニチャ エンジンのバージョン情報のすべてが表示されます。

- [Interface Status]：インターフェイス名、リンク ステータス、イネーブルかどうか、速度、モード、受信および転送されたパケットが表示されます。

- [Global Correlation Health]：グローバル相関の設定ステータスとネットワーク参加が表示されます。

（注） AIP SSC-5 は、グローバル相関機能をサポートしていません。

詳細情報

- センサーおよびネットワーク セキュリティ ヘルスを設定する手順については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- 脅威のしきい値を変更する手順については、「リスク カテゴリの設定」（P.8-33）を参照してください。
- ネットワーク セキュリティ ヘルスを再設定する手順については、「ネットワーク セキュリティの稼動状態のリセット」（P.19-30）を参照してください。
- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。

[Device List] ペインのフィールド定義

[Device List] ペインには次のフィールドがあります。

- [Time]：ローカル システムと追加したセンサーの間に同期の問題がある場合、時刻フィールドにアイコンが表示されます。ローカル システムとセンサーが同期されている場合、フィールドは空白です。

  （注）　センサーとローカル システムの間で時刻が同期されていないと、正確なモニタリングとレポートが行われません。

- [Device Name]：センサーに付けた名前が表示されます。
- [IP Address]：センサーの IP アドレスが表示されます。
- [Device Type]：IPS モデル名が表示されます。
- [Event Status]：IME がイベントを受け取るためにセンサーに接続されていることを示します。
- [Sensor Health]：センサーのヘルスが正常か、注意が必要かどうかを示します。
- [Global Correlation Status]：センサーのグローバル相関ステータスを示します。

  （注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

- [Version]：インストールされている Cisco IPS ソフトウェア バージョンが表示されます。
- [License Expiration]：センサーのライセンスの有効期限が切れるまでの日数を示します。
- [Load]：負荷の割合が表示されます。
- [Memory]：メモリの使用率が表示されます。
- [CPU]：CPU の使用率が表示されます。
- [Signature Version]：現在のシグニチャのバージョンが表示されます。

詳細情報

- 時刻とセンサーについては、「時刻の設定」（P.6-8）を参照してください。
- センサー ヘルス メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。
- センサーのライセンシングの詳細については、「ライセンスの設定」（P.18-10）を参照してください。
- 最新の IPS ソフトウェアの入手手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

[Add Device List] および [Edit Device List] ダイアログボックスのフィールド定義

[Add Device List] および [Edit Device List] ダイアログボックスには次のフィールドがあります。

- [Sensor Name]：追加しているセンサーの名前。
- [Sensor IP Address]：追加しているセンサーの IP アドレス。
- [User Name]：このセンサーへのアクセスが許可されたユーザ アカウント名。
- [Password]：このセンサーへのアクセスが許可されたユーザ アカウントのパスワード。
- [Web Server Port]：Web サーバが使用する TCP ポート。HTTP または HTTPS の場合、デフォルトは 443 です。1 ～ 65535 以外の値を入力すると、エラー メッセージが表示されます。
- [Communication Protocol]：Web サーバで TLS と SSL をイネーブルにします。デフォルトは [Use encrypted connection (HTTPS)] です。暗号化された接続を使用することを強くお勧めします。
- [Event Start Time (UTC)]：最新のアラートを取得するか、取得するアラートの開始時刻を設定するかを選択できます。
- [Exclude alerts of the following severity level(s)]：取得する情報からセキュリティ レベルを除外するかどうかを選択できます。デフォルトでは、すべてのセキュリティ レベルが表示されます。

詳細情報

センサー パスワードの回復手順については、「パスワードの回復」（P.18-3）を参照してください。

デバイスの追加、編集、および削除

デバイスを追加、編集、および削除するには、次の手順を実行します。

ステップ 1　[Home] > [Devices] > [Device List] を選択し、[Add] をクリックします。

ステップ 2　[Add Device] ダイアログボックスの必須フィールドに入力します。

a. 追加しているセンサーのセンサー名とセンサーの IP アドレスを入力します。

b. このセンサーにアクセスできるユーザのユーザ名とパスワードを入力します。

c. デフォルトの Web サーバ ポートを変更するには、新しいポート番号を入力します。

d. 通信プロトコルを選択します。

（注）　暗号化された接続を使用することを強くお勧めします。

e. [Latest Alerts] チェックボックスをオンにするか、[Start Date] および [Start Time] フィールドに開始日時を入力して、イベントの開始時刻を選択します。

f. [Exclude alerts of the following severity level(s)] で、除外するレベルのチェックボックスをオンにします。デフォルトでは、すべてのレベルが表示されます。

g. [OK] をクリックして、IME システムにセンサーを追加します。

ステップ 3　[Yes] をクリックして、証明書を受け入れ、センサーとの HTTPS 接続を続行します。

（注）　[No] をクリックすると、証明書が拒否され、IME はセンサーにアクセスできません。

IME は、IME とセンサーの時刻設定をチェックし、正確であることを確認します。時刻が不正確で、センサーと IME システムの間に 5 分を超すずれがある場合、警告メッセージが表示されます。必ず、センサーとシステムを同期させてください。

注意　レポート、履歴イベント、およびトップ ガジェットの精度を維持するために、時刻が正確であることは非常に重要です。時刻の誤差が 5 分を超えている場合、[Device Lists] ペインでそのデバイスの横にアイコンが表示されます。

ステップ 4　デバイスを編集するには、リストでそのデバイスを選択し、[Edit] をクリックし、必要な変更を加えて [OK] をクリックします。

（注）　センサー名は IME データベースのキーなので、[Sensor Name] は変更できません。

ステップ 5　デバイスを削除するには、リストでそのデバイスを選択し、[Delete] をクリックします。[Device List] ペインにそのデバイスが表示されなくなります。

詳細情報

センサーの時刻を修正する方法については、「センサーの時刻の修正」（P.6-13）を参照してください。

デバイス、イベント、ヘルス、およびグローバル相関接続ステータスの開始、停止、および表示

[Start] > [Health Connection] を選択している限り、IME はセンサーに 10 秒おきにクエリーを実行して、ヘルス ステータス情報を取得します。[Start] > [Events Connection] を選択している限り、IME はセンサーからアラートを取得します。[Start] > [Global Correlation Connection] を選択している限り、IME はグローバル相関データを送受信します。

センサーでのイベントのポーリングを停止しなければならない場合があります。たとえば、別のセンサーのイベントを分析しているときに、リアルタイム イベントによる中断を避ける必要がある場合は、特定のセンサーからのイベントのポーリングを停止できます。ポーリングの完了後再開できます。また、10 秒単位の更新なしで、ステータスのスナップショットを表示する場合は、ヘルスとセキュリティのポーリングを停止できます。

イベント、ヘルス、およびグローバル相関の接続ステータスを開始、停止、および表示するには、次の手順を実行します。

ステップ 1　イベント、ヘルス、またはグローバル相関の接続ステータスを開始または停止するセンサーをデバイス リストで選択します。

ステップ 2　[Start] または [Stop] > [Health Connection] または [Events Connection] または [Global Correlation Connection] を選択します。列に [Connected] または [Not Connected] が表示されます。

ステップ 3　IME からセンサーへの接続ステータス、センサー バージョン、および統計情報を表示するには、リストでセンサーを選択し、[Status] をクリックします。[Device Status] ダイアログボックスに次の IPS コンポーネントの統計情報が表示されます。

- 分析エンジン
- 異常検出
- イベント ストア
- 外部製品インターフェイス
- グローバル相関
- Host
- Interface
- ネットワーク アクセス
- 通知
- OS 識別名
- SDEE サーバ
- トランザクション サーバ
- Virtual Sensor
- Web サーバ

ステップ 4　[Device Status] ダイアログボックスの内容を更新するには、[Refresh] をクリックします。

ステップ 5　センサーに関する詳細を表示するには、リストでそのセンサーを選択し、ペインの [Device Details] セクションに表示される情報を確認します。

[Device Details] ペインに表示するヘルス メトリックを変更するには、[Configuration] > *sensor_name* > [Sensor Management] > [Sensor Health] に進みます。[Device Details] ペインに表示するグローバル相関メトリックを変更するには、[Configuration] > *sensor_name* > [Sensor Management] > [Global Correlation] に進みます。

詳細情報

- センサー ヘルス メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。

デバイスでのツールの使用

デバイスにツールを使用するには、次の手順を実行します。

ステップ 1　[Home] > [Devices] を選択します。

ステップ 2　センサーの ping 統計情報を取得するには、デバイス リスト テーブルでそのセンサーを選択し、[Tools] > [ping] をクリックします。そのセンサーの ping 統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

ステップ 3　IP パケットのルートを調べるには、リストでそのセンサーを選択し、[Tools] > [Traceroute] をクリックします。そのセンサーのルート統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

ステップ 4　whois 情報を調べるには、リストでそのセンサーを選択し、[Tools] > [WhoIs] をクリックします。そのセンサーの WHOIS 統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

ステップ 5　DNS 情報を調べるには、リストでそのセンサーを選択し、[Tools] > [DNS] をクリックします。そのセンサーの DNS ルックアップ統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。