CHAPTER 5

Startup Wizard の使用

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

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

この章では、Startup Wizard、およびそれを使用してセンサーを設定する方法について説明します。内容は次のとおりです。

[Startup Wizard Introduction] ウィンドウ

（注） Startup Wizard でセンサーの基本的な設定を行うには、管理者である必要があります。

注意 IME は設定されていないセンサーと通信できないため、センサーの CLI にログインし、**setup** コマンドを実行して通信パラメータを設定する必要があります。例外的に、AIP SSC-5 の場合は、ASDM から初期化できます。

Startup Wizard を使用すると、センサーのセットアップや、すでに設定されているセンサーの変更ができます。新しい未設定のセンサーの初期化には使用できません。この場合は、**setup** コマンドを使用する必要があります。**setup** コマンドでセンサーを初期化するまで、IME はセンサーと接続できません。

Startup Wizard では、センサーが検査、応答、およびトラフィックのレポートを行うように、必要に応じて段階的な設定を行います。これを使用して、センサーの基本的な設定、インターフェイスの設定、仮想センサーの作成、ポリシーの作成、仮想センサーへのポリシーおよびインターフェイスの割り当て

ができます。また、センサーが Cisco.com からシグニチャ アップデートおよびシグニチャ エンジン アップデートを自動的にダウンロードするように設定したり、センサーに変更を保存することもできます。

Startup Wizard は、すべての IPS プラットフォームで使用できます。ある機能が特定のプラットフォームで使用できない場合でも、設定ウィンドウを確認する必要はありません

（注） Startup Wizard では、VLAN グループはサポートされていません。

IPS モジュールは、次の機能をサポートしていません。

- AIM IPS および NME IPS：インライン インターフェイス ペア、VLAN グループ、仮想化、または時刻設定。
- AIP SSM および IPS SSP：インライン VLAN ペア、インライン インターフェイス ペア、VLAN グループ、時刻設定、またはインターフェイス設定（適応型セキュリティ アプライアンスでインターフェイスを設定する必要があります）。
- AIP SSC-5：インライン VLAN ペア、インライン インターフェイス ペア、VLAN グループ、仮想化、時刻設定、またはインターフェイス設定（適応型セキュリティ アプライアンスでインターフェイスを設定する必要があります）。
- IDSM2：インライン インターフェイス ペアの VLAN グループまたは時刻設定。

（注） IPS モジュールは、設置されているルータ、スイッチ、または適応型セキュリティ アプライアンスから時刻設定を取得します。

注意 IME がスタンドアロン モードで動作しているときは、IME の Startup Wizard を使用して ASA トラフィックを AIP SSM および IPS SSP に割り当てることはできません。ASDM から IME に接続できる場合は、IME を使用して ASA トラフィックを割り当てることができます。

注意 IPS SSP には、4 種類のポートがあります（コンソール、管理、GigabitEthernet、および 10GE）。コンソールおよび管理ポート（IPS SSP の前面パネル右側）は、IPS ソフトウェアによって設定および管理されます。GigabitEthernet および 10GE ポート（IPS SSP の前面パネル左側）は、IPS ソフトウェアではなく ASA ソフトウェアによって設定および管理されます。しかし、IPS SSP をリセットまたはシャットダウンすると、GigabitEthernet および 10GE ポートもリンク ダウンします。リンク ダウンによるポートへの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンは、スケジュールされたメンテナンス時間中に行う必要があります。

詳細情報

- センサーの高度な設定を行うには、先にセンサーを初期化する必要があります。その後、IME で [Configuration] > *sensor_name* > [Sensor Setup] を選択します。**setup** コマンドを使用してセンサーを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。
- ASA ソフトウェアについての詳細は、『ASA User Documentation』を参照してください。

センサーのセットアップ

ここでは、センサーのセットアップ方法について説明します。内容は次のとおりです。

[Sensor Setup] ウィンドウ

（注） IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（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。

（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。

[Sensor Setup] ウィンドウでは、センサーの基本動作を設定できます。初期化の際にすでに値が割り当てられているので、ほとんどのフィールドにはすでにデータが入力されていますが、このウィンドウで必要に応じて変更することができます。

フィールド定義

[Sensor Setup] ウィンドウには、次のフィールドが表示されます。

- [Network Settings]：センサーのネットワーク設定を設定します。
  - [Host Name]：センサーの名前。ホスト名は 1 ～ 64 文字の文字列で、^[A-Za-z0-9_/-]+$ に一致するパターンです。デフォルトは sensor です。ホスト名にスペースが含まれているか、または英数字が 64 文字を超えていると、エラー メッセージが表示されます。
  - [IP Address]：センサーの IP アドレス。デフォルトは 192.168.1.2 です。
  - [Subnet Mask]：IP アドレスに対応するマスク。デフォルトは 255.255.255.0 です。
  - [Gateway]：デフォルト ゲートウェイ アドレス デフォルトは 192.168.1.1 です。
  - [HTTP Proxy Server]：HTTP プロキシ サーバの IP アドレスを入力します。カスタマー ネットワークでプロキシが使用されている場合は、グローバル相関のアップデートをダウンロードするためのプロキシ サーバが必要になる場合があります。
  - [HTTP Proxy Port]：HTTP プロキシ サーバのポート番号を入力します。
  - [DNS Primary]：プライマリ DNS サーバの IP アドレスを入力します。

注意 グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル相関のアップデート サーバにアクセスする場合にだけサポートされます。

- [Allowed hosts/networks that can access the sensor]：ACL を追加します。
  - [Network]：アクセス リストに追加するネットワークの IP アドレス。
  - [Mask]：アクセス リストに追加するネットワークのネットマスク。

  （注）　センサーの ACL エントリを変更すると、変更を適用する際に、IME によりセンサーへの接続が切断される場合があります。

- [Network Participation]：データ送信の際に SensorBase ネットワーク に参加するかどうか、および参加するレベルを選択します。
  - [Off]：どのデータも SensorBase ネットワークに提供されません。
  - [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
  - [Full]：すべてのデータが SensorBase ネットワーク に提供されます。
- [Current Sensor Date and Time]：NTP サーバが設定されていないアプライアンスの時刻と日付を設定します
  - [Date]：センサーのローカルな日付。時刻と日付をアップデートしたら、[Apply Date/Time to Sensor] をクリックして変更を有効にします。
  - [Apply Date/Time to Sensor]：センサー上の時刻と日付をただちにアップデートします。

  （注）　Startup Wizard をキャンセルしても、時刻と日付の変更は保持されます。

- [Time Zone]：時間帯の名前および UTC オフセットを設定します。
  - [Zone Name]：サマータイムが実施されていない場合のローカル時間帯。デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
  - [Offset]：ローカル時間帯のオフセット（分単位）。デフォルトは 0 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。

  （注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

- [NTP Server]：センサーが NTP サーバを時刻源として使用するように設定します。
  - [IP Address]：NTP サーバを使用してセンサー上の時刻を設定する場合の、NTP サーバの IP アドレス。
  - [Authenticated NTP]：認証された NTP を使用します。キーおよびキー ID が必要です。
  - [Key]：NTP MD5 キー タイプ。
  - [Key ID]：NTP サーバ上で認証に使用されるキーの ID（1 ～ 65535）。キー ID が範囲外の場合は、エラー メッセージが表示されます。

  （注）　センサーの時刻源として NTP サーバを使用する方法を推奨します。

- [Summertime]
  - [Enable Summertime]：このチェックボックスをオンにすると、サマータイム モードがイネーブルになります。デフォルトはディセーブルです。
  - [Configure Summertime]：サマータイム設定を設定する場合は、これをクリックします。

[Add ACL Entry]/[Edit ACL Entry] ダイアログボックス

センサーへのアクセスを許可するホストまたはネットワークのリストを設定することができます。アクセス リストには、次のホストのエントリが存在する必要があります。

- センサーに Telnet で接続する必要のあるホスト。
- センサーに対して SSH を使用する必要のあるホスト。
- Web ブラウザからセンサーにアクセスする必要のある、IDM や ASDM などのホスト。
- センサーにアクセスする必要のある、CSM などの管理ステーション。
- 該当のセンサーがマスター ブロッキング センサーの場合、リストにはブロッキング転送センサーの IP アドレスのエントリが必要です。

フィールド定義

[Add ACL Entry]/[Edit ACL Entry] ダイアログボックスには、次のフィールドが表示されます。

- [IP Address]：センサーへのアクセスを許可するホストまたはネットワークの IP アドレス。
- [Network Mask]：センサーへのアクセスを許可するホストまたはネットワークのネットワーク マスク。単一のホストのネットマスクは 32 です。

[Configure Summertime] ダイアログボックス

[Configure Summertime] ダイアログボックスには、次のフィールドが表示されます。

- [Summer Zone Name]：サマータイム時間帯の名前。デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
- [Offset]：サマータイム中に付加する時間数（分単位）。デフォルトは 60 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。

  （注） 時間帯のオフセットを変更するには、センサーをリブートする必要があります。

- [Start Time]：サマータイム開始時刻の設定。値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- [End Time]：サマータイム終了時刻の設定。値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- [Summertime Duration]：サマータイム期間が毎年実施されるか、1 回だけの日付かを設定します。
  - [Recurring]：サマータイム期間は recurring（毎年実施される）モードです。
  - [Date]：サマータイム期間は、nonrecurring（毎年実施されない）モードです。
  - [Start]：開始の週、日、月の設定。
  - [End]：終了の週、日、月の設定。

センサー設定の設定

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（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。

（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。

Startup Wizard でセンサー設定を設定するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] を選択し、[Next] をクリックします。

ステップ 3　[Host Name] フィールドにセンサー名を入力します。

ステップ 4　[IP Address] フィールドにセンサーの IP アドレスを入力します。

ステップ 5　[Subnet Mask] フィールドにネットワーク マスク アドレスを入力します。

ステップ 6　[Gateway] フィールドにデフォルト ゲートウェイ アドレスを入力します。

（注）　センサーのネットワーク設定を変更すると、変更を適用する際に IME および ASDM によりセンサーへの接続が切断されます。

ステップ 7　グローバル相関をサポートするために、HTTP プロキシ サーバまたは DNS サーバを設定するには、[HTTP Proxy Server] フィールドに HTTP プロキシ サーバの IP アドレスを入力して [HTTP Proxy Port] フィールドにポート番号を入力するか、または [DNS Primary] フィールドに DNS サーバの IP アドレスを入力します。

注意　グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル脅威の相関のアップデート サーバにアクセスする場合にだけサポートされます。

ステップ 8　センサーへのアクセスを許可するホストおよびネットワークを設定するには、[Add] をクリックします。

a.　[IP Address] フィールドに、センサーへのアクセスを許可するホストの IP アドレスを入力します。

b.　[Network Mask] フィールドに、センサーへのアクセスを許可するホストのネットワーク マスク アドレスを入力します。

c.　[OK] をクリックします。

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

ステップ 9　ネットワーク参加をイネーブルにするには、参加するネットワーク参加のレベルを選択します。

- [Off]：どのデータも SensorBase ネットワークに提供されません。
- [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- [Full]：すべてのデータが SensorBase ネットワーク に提供されます。

デフォルトはオフです。[Partial] または [Full] を選択した場合は、Network Participation Disclaimer に同意する必要があります。

ステップ 10　[Current Sensor Date and Time] で、ドロップダウン カレンダーから現在の日付と時刻を選択し、[OK] をクリックしてから、[Apply Date/Time to Sensor] をクリックします。ローカル ホスト上の日付と時刻が表示されます。

注意　誤った時刻を指定すると、保存されているイベントに誤ったタイムスタンプが設定されます。この場合は、イベントをクリアする必要があります。

（注）　Startup Wizard をキャンセルしても、時刻と日付の変更は保持されます。

（注）　IPS モジュール上では日付または時刻の変更はできません。また、NTP を設定している場合も日付または時刻の変更はできません。

ステップ 11　[Time Zone] で、時間帯およびオフセットを設定します。

a.　[Zone Name] フィールドのドロップダウン リストから時間帯を選択するか、または作成済みの時間帯を入力します。これは、サマータイム時間が実施されていない場合に表示される時間帯です。

b.　[Offset] フィールドに、UTC のオフセットを分単位で入力します。事前に定義された時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

（注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

ステップ 12　NTP 時刻同期を使用している場合は、[NTP Server] で次を入力します。

- [IP Address] フィールドに NTP サーバの IP アドレスを入力します。
- 認証された NTP を使用している場合は、[Authenticated NTP] チェックボックスをオンにしてから、[Key] フィールドに NTP サーバのキーを入力し、[Key ID] フィールドに NTP サーバのキー ID を入力します。

（注）　NTP サーバを定義すれば、センサーの時間はその NTP サーバによって設定されます。CLI で **clock set** コマンドを実行するとエラーが発生しますが、時間帯のパラメータおよびサマータイムのパラメータは有効です。

ステップ 13　サマータイムをイネーブルにするには、[Enable Summertime] チェックボックスをオンにし、[Configure Summertime] をクリックします。

ステップ 14　ドロップダウン リストから [Summer Zone Name] を選択するか、または作成済みのサマータイム名を入力します。これは、サマータイム時間が実施されている間に表示される時間帯名です。

ステップ 15　[Offset] フィールドに、サマータイム中に付加する時間数を分単位で入力します。事前に定義されたサマータイム時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

ステップ 16　[Start Time] フィールドに、サマータイム設定に適用する時刻を入力します。

ステップ 17　[End Time] フィールドに、サマータイム設定から削除する時刻を入力します。

ステップ 18　[Summertime Duration] で、サマータイム設定が毎年指定された日付に発生する（recurring）か、または指定された日付で開始および終了する（date）かを選択します。

a. [Recurring]：ドロップダウン リストから開始時刻と終了時刻を選択します。デフォルトは 3 月の第 2 日曜日と 11 月の第 1 日曜日です。

b. [Date]：ドロップダウン リストから開始時刻と終了時刻を選択します。開始および終了時刻のデフォルトは 1 月 1 日です。

ステップ 19　[OK] をクリックします。

ヒント　変更を破棄するには、[Cancel] をクリックします。

ステップ 20　Startup Wizard を続行するには、[Next] をクリックします。

（注）　ネットワーク設定を変更すると、センサーへの接続が中断し、新しいアドレスでの再接続が必要になることがあります。

インターフェイスの設定

（注）　Startup Wizard は、AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、または NME IPS のインターフェイスおよび仮想センサーの設定には使用できません。

ここでは、センサー インターフェイスの設定方法について説明します。内容は次のとおりです。

[Interface Summary] ウィンドウ

[Interface Summary] ウィンドウには、既存のインターフェイス コンフィギュレーションの設定が表示されます。仮想センサーにインターフェイスが割り当てられていない場合は、[Assigned Virtual Sensor] カラムに「Unassigned」と表示され、[Details] カラムには「Promiscuous」と表示されます。インターフェイスは、物理インターフェイスか論理インターフェイスのいずれかになります。物理インターフェイスは、論理インターフェイスの一部となる場合もあり、さらに細分化することもできます。

インターフェイス コンフィギュレーションは、次の 5 種類のいずれかに指定できます。

- 無差別
- 無差別 VLAN グループ（サブインターフェイス）
- インライン インターフェイス ペア
- インライン インターフェイス ペア VLAN グループ（サブインターフェイス）
- インライン VLAN ペア（サブインターフェイス）

（注） Startup Wizard では、VLAN グループはサポートされていません。

注意 無差別モード、インライン ペア モード、またはインライン VLAN ペア モードで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせてインターフェイスを設定することはできません。

（注） Startup Wizard セッションごとに 1 つの物理または論理インターフェイスを設定できます。複数のインターフェイスを設定するには、Startup Wizard を複数回実行します。

このウィンドウで [Finish] をクリックすると、Startup Wizard が終了し、変更をコミットできます。そうしない場合は、インターフェイスおよび仮想センサーの設定を続行できます。

フィールド定義

[Interface Summary] ウィンドウには、次のフィールドが表示されます。

- [Name] : インターフェイスの名前。値は、無差別インターフェイスの場合、FastEthernet または GigabitEthernet です。インライン インターフェイスの場合、この名前はペアに割り当てた名前になります。
- [Details] : インターフェイスが無差別またはインラインであるかどうかを示し、VLAN ペアの有無を示します。
- [Assigned Virtual Sensor] : インターフェイスまたはインターフェイス ペアが仮想センサーに割り当てられているかどうかを示します。
- [Enabled] : インターフェイスをイネーブルにするかどうかを指定します。
- [Description] : インターフェイスの説明。

[Restore Defaults to an Interface] ダイアログボックス

[Restore Default Interface] ダイアログボックスには、仮想センサーに設定された、または割り当てられたすべてのインターフェイスが表示されます。ここから復元を行うインターフェイスを選択します。選択したインターフェイスが仮想センサーに割り当てられている場合は、割り当てが取り消されます。インライン インターフェイス ペアを選択した場合は、両方の物理インターフェイスがデフォルトに復元され、論理インターフェイスは削除されます。インライン VLAN ペアまたは VLAN グループを選択してデフォルトに復元することはできません。

注意　デフォルトに復元できるのは、物理インターフェイスおよびインライン インターフェイス ペアだけです。

[Traffic Inspection Mode] ウィンドウ

[Traffic Inspection Mode] ウィンドウでは、センサー インターフェイスを、無差別、インライン インターフェイス、またはインライン VLAN ペア モードとして設定します。センサーに 1 つの物理インターフェイス（AIM-IPS など）だけがある場合、[Inline Interface Pair Mode] オプション ボタンはディセーブルになります。センサーがインライン VLAN ペア モードをサポートしていない場合も、オプション ボタンはディセーブルになります。

[Traffic Inspection Mode] ウィンドウには、次のオプション ボタンが表示されます。

- [Promiscuous Mode]：センサーは、検査されたパケットのデータ パス内にありません。センサーはパケットを変更またはドロップできません。
- [Inline Interface Pair Mode]：センサーは、検査されたパケットのデータ パス内にあります。センサーは検査されたパケットを変更またはドロップできます。インライン インターフェイス インスペクションを行うには、2 つの物理インターフェイスをペアにする必要があります。
- [Inline VLAN Pair Mode]：センサーは、検査されたパケットのデータ パス内にあります。センサーは検査されたパケットを変更またはドロップできます。インライン VLAN インスペクションを行うには、1 つの物理インターフェイスと偶数の VLAN が必要です。また、このインターフェイスはトランク ポートに接続される必要があります。

[Interface Selection] ウィンドウ

[Interface Selection] ウィンドウでは、設定するインターフェイスを選択できます。

（注）　Startup Wizard セッションごとに 1 つの物理または論理インターフェイスを設定できます。複数のインターフェイスを設定するには、Startup Wizard を複数回実行します。

[Inline Interface Pair] ウィンドウ

[Inline Interface Pair] ウィンドウでは、2 つの一意のインターフェイスにインターフェイス名を割り当てることができます。センサーがハードウェア バイパスをサポートしている場合は、そのことを示すアイコンが表示されます。ハードウェア バイパス インターフェイスとハードウェア バイパスをサポートしていないインターフェイスをペアにすると、ハードウェア バイパスが使用できないことを示す警告メッセージが表示されます。

（注）　停電が発生した場合でも、ハードウェア バイパス インターフェイスにより、パケット フローが続行されます。

フィールド定義

[Inline Interface Pair] ウィンドウには、次のフィールドが表示されます。

- [Inline Interface Name]：このインライン インターフェイス ペアに名前を割り当てます。
- [First Interface of Pair]：このペアの最初のインターフェイスを割り当てます。
- [Second Interface of Pair]：このペアの他のインターフェイスを割り当てます。

[Inline VLAN Pairs] ウィンドウ

[Interface Inspection Mode] ウィンドウで [Inline VLAN Pair Mode] オプション ボタンをオンにすると、[Inline VLAN Pairs] ウィンドウでインライン VLAN ペアを設定できます。設定済みの場合はインライン VLAN ペアがテーブルに表示され、編集または削除できます。

（注）　別のインターフェイスとペアになっているインターフェイスや無差別モードで仮想センサーに割り当てられているインターフェイスにはインライン VLAN ペアは作成できません。

無差別モードのインターフェイスにインライン VLAN ペアを作成するには、仮想センサーからインターフェイスを削除してからインライン VLAN ペアを作成する必要があります。ペアにできるのは使用可能なインターフェイスだけです。

（注）　使用しているセンサーが、インライン VLAN ペアをサポートしていない場合、[Inline VLAN Pairs] ウィンドウは表示されません。AIM IPS、AIP SSC-5、および NME IPS はインライン VLAN ペアをサポートしていません。

フィールド定義

[Inline VLAN Pairs] ウィンドウには、次のフィールドが表示されます。

- [Subinterface Number]：インライン VLAN ペアのサブインターフェイス番号。値は 1 ～ 255 です。
- [VLAN A]：最初の VLAN の VLAN 番号が表示されます。値は 1 ～ 4095 です。
- [VLAN B]：第 2 の VLAN の VLAN 番号が表示されます。値は 1 ～ 4095 です。
- [Interface]：インライン VLAN ペアの名前。
- [Virtual Sensor]：このインライン VLAN ペアの仮想センサーの名前。
- [Description]：インライン VLAN ペアの説明。

[Add Inline VLAN Pair Entry]/[Edit Inline VLAN Pair Entry] ダイアログボックス

（注）　VLAN をそれ自身とペアにすることはできません。

（注）　サブインターフェイス番号と VLAN 番号は、物理インターフェイスごとに一意である必要があります。

[Add Inline VLAN Pair Entry]/[Edit Inline VLAN Pair Entry] ダイアログボックスには、次のフィールドが表示されます。

- [Subinterface Number] : サブインターフェイス番号を割り当てることができます。1 ～ 255 の範囲の番号を割り当てることができます。
- [VLAN A] : このインライン VLAN ペアに最初の VLAN を割り当てることができます。1 ～ 4095 の任意の VLAN を割り当てることができます。
- [VLAN B] : このインライン VLAN ペアにもう一方の VLAN を割り当てることができます。1 ～ 4095 の任意の VLAN を割り当てることができます。
- [Description] : このインライン VLAN ペアの説明を追加できます。

インライン VLAN ペアの設定

Startup Wizard でインライン VLAN ペアを設定するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] を選択し、[Traffic Inspection Mode] ウィンドウが表示されるまで [Next] をクリックします。

ステップ 3　[Inline VLAN Pair Mode] オプション ボタンをクリックしたら、[Next] をクリックして [Add] をクリックします。

ステップ 4　[Subinterface Number] フィールドに、インライン VLAN ペアのサブインターフェイス番号（1 ～ 255）を入力します。

ステップ 5　[VLAN 1] フィールドで、このインライン VLAN ペアの最初の VLAN（1 ～ 4095）を指定します。

ステップ 6　[VLAN 2] フィールドで、このインライン VLAN ペアのもう一方の VLAN（1 ～ 4095）を指定します。

ステップ 7　必要に応じて、[Description] フィールドにインライン VLAN ペアの説明を入力します。

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

ステップ 8　[OK] をクリックします。新しいインライン VLAN ペアが、[Inline VLAN Pairs] ウィンドウのリストに表示されます。

ステップ 9　インライン VLAN ペアを編集するには、そのペアを選択し、[Edit] をクリックします。

ステップ 10　サブインターフェイス番号と VLAN 番号の変更、説明の編集を行えます。

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

ステップ 11　[OK] をクリックします。編集された VLAN ペアが [Inline VLAN Pairs] ウィンドウのリストに表示されます。

ステップ 12　VLAN ペアを削除するには、そのペアを選択して [Delete] をクリックします。その VLAN ペアは、[Inline VLAN Pairs] ウィンドウのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 13　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

仮想センサーの設定

ここでは、仮想センサーの設定方法について説明します。内容は次のとおりです。

[Virtual Sensors] ウィンドウ

インターフェイスを設定したら、Startup Wizard の [Virtual Sensors] ウィンドウで、インターフェイスを仮想センサーに割り当てます。デフォルトでは、インターフェイスは仮想センサー vs0 に割り当てられます。インターフェイスは既存の仮想センサーに割り当てることができます。また、新しい仮想センサーを作成することもできます。仮想センサーを作成するには、[Create a Virtual Sensor] をクリックします。[Add Virtual Sensor] ダイアログボックスが表示され、仮想センサーを設定できるようになります。

（注）　AIM IPS、AIP SSM、AIP SSC-5、IPS SSP、および NME IPS には設定可能なインターフェイスがないため、デフォルトの仮想センサーを使用する必要があります。

フィールド定義

[Virtual Sensors] ウィンドウには、次のフィールドが表示されます。

- [Interface(s)]：仮想センサーに割り当てる 1 つまたは複数のインターフェイスがリストされます。
- [Assign Interface to Virtual Sensor]：使用できる仮想センサーがリストされます。デフォルトのセンサーは vs0 です。
- [Create a Virtual Sensor]：[Add Virtual Sensor] ダイアログで、新しいシグニチャ、イベント アクション規則、および異常検出ポリシーを使用する仮想センサーを作成できます。また、デフォルト ポリシーを使用することもできます。
- [IPS Policy Summary Information]：割り当てられたインターフェイスが、割り当てられたポリシーとともに表示されます。
- [Default Block Policy]: 拒否イベント アクション オーバーライドで使用されるデフォルトのリスク カテゴリ。リスク レーティングが 90 ～ 100 のアラートはデフォルトで拒否されます。

  デフォルトのリスク カテゴリを使用しない場合は、[HIGHRISK] リスク カテゴリを編集するか、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Event Action Rules] > [rules0] > [Risk Category] を選択して新しいリスク カテゴリを作成できます。

[Add Virtual Sensor] ダイアログボックス

[Add Virtual Sensor] ダイアログボックスでは、新しいシグニチャ ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーを作成できますが、これらを設定することはできません。新しいポリシーを作成するには、デフォルトのポリシーをクローニングします。

新しいポリシーを設定するには、

- 新しいシグニチャ ポリシーの場合は、[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [NewSigPolicy] > [All Signatures] を選択します。
- 新しいイベント アクション規則ポリシーの場合は、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [NewRulesPolicy] を選択します。
- 新しい異常検出ポリシーの場合は、[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [NewADPolicy] を選択します。

フィールド定義

[Add Virtual Sensor] ダイアログボックスには、次のフィールドが表示されます。

- [Virtual Sensor Name]：仮想センサーに名前を割り当てます。
- [Description]：仮想センサーの説明を入力します。
- [Assign a Signature Policy]
  - [Assign an Existing Signature Policy]：すでに作成済みのシグニチャ ポリシーを割り当てます。
  - [Create a New Signature Policy]：新しいシグニチャ ポリシーを作成します。
- [Assign an Event Action Rules Policy]
  - [Assign an Existing Event Action Rules Policy]：すでに作成済みのイベント アクション規則ポリシーを割り当てます。
  - [Create a New Event Action Rules Policy]：新しいイベント アクション規則ポリシーを作成します。
- [Assign an Anomaly Detection Policy]
  - [Assign an Existing Anomaly Detection Policy]：すでに作成済みの異常検出ポリシーを割り当てます。
  - [Create a New Anomaly Detection Policy]：新しい異常検出ポリシーを作成します。

仮想センサーの追加

Startup Wizard を使用して仮想センサーを追加するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] を選択し、[Virtual Sensors] ウィンドウが表示されるまで [Next] をクリックします。

ステップ 3　[Create a Virtual Sensor] をクリックします。

ステップ 4　[Virtual Sensor Name] フィールドに仮想センサー名を入力します。

ステップ 5　[Description] フィールドに、この仮想センサーの識別に役立つ説明を入力します。

ステップ 6　次のいずれかの方法でシグニチャ ポリシーを割り当てます。

a. [Assign a Signature Policy] オプション ボタンをクリックし、ドロップダウン リストからシグニチャ ポリシーを選択します。

b. [Create a Signature Policy] オプション ボタンをクリックし、フィールドにシグニチャ ポリシーの名前を入力します。

（注）　新しいシグニチャ ポリシーを設定するには、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Signature Definitions] > [NewSigPolicy] > [All Signatures] を選択します。

ステップ 7　次のいずれかの方法でイベント アクション規則ポリシーを割り当てます。

a. [Assign an Event Action Rules Policy] オプション ボタンをクリックし、ドロップダウン リストからイベント アクション規則ポリシーを選択します。

b. [Create an Event Action Rules Policy] オプション ボタンをクリックし、フィールドにイベント アクション規則ポリシーの名前を入力します。

（注）　新しいイベント アクション規則ポリシーを設定するには、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [NewRulesPolicy] を選択します。

ステップ 8　次のいずれかの方法で異常検出ポリシーを割り当てます。

a. [Assign an Anomaly Detection Policy] オプション ボタンをクリックし、ドロップダウン リストから異常検出ポリシーを選択します。

b. [Create an Anomaly Detection Policy] オプション ボタンをクリックし、フィールドに異常検出ポリシーの名前を入力します。

（注）　新しい異常検出ポリシーを設定するには、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Anomaly Detections] > [NewADPolicy] を選択します。

ステップ 9　[Finish] をクリックし、[Confirm Configuration Changes] ダイアログボックスで [Yes] をクリックして変更を保存します。

自動アップデートの設定

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

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

フィールド定義

Startup Wizard の [Auto Update] ウィンドウには、次のフィールドが表示されます。

- [Enable Signature and Engine Updates from Cisco.com]：センサーが Cisco.com にアクセスし、シグニチャ アップデートおよびシグニチャ エンジン アップデートをダウンロードしてセンサー上にインストールするようにします。

（注）　[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにして、フィールドをイネーブルにする必要があります。

- [Cisco.com Access]：Cisco.com サーバのために次のオプションを指定します。
  - [Username]：Cisco.com 上のユーザ アカウントに対応するユーザ名を示します。
  - [Password]：Cisco.com 上のユーザ アカウントのパスワードを示します。
  - [Confirm Password]：Cisco.com のパスワードの再入力を強制することで、パスワードを確定します。
- [Schedule]：毎日の開始時刻を指定します。
  - [Start Time]：アップデート プロセスを開始する時刻を 24 時間制で示します。これは、センサーが Cisco.com にアクセスして新しいアップデートをダウンロードする時刻です。

自動アップデートの設定

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

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

ステップ 2　[Configuration] > *sensor_name* > [Sensor Setup] > [Startup Wizard] > [Auto Update] を選択します。

ステップ 3　Cisco.com からのシグニチャ アップデートとシグニチャ エンジン アップデートをイネーブルにするには、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。

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

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

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

d. [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は hh:mm:ss（24 時間制）です。アップデートは毎日実行されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

ステップ 4　[Finish] をクリックして変更を保存します。

詳細情報

- ソフトウェアおよび暗号化特権を持つアカウントの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- サポートされている FTP および HTTP サーバのリストについては、「サポートされる FTP および HTTP サーバ」（P.18-17）を参照してください。

- 自動アップデートをダウンロードするためにUNIX スタイルのディレクトリ リストを設定するには、「UNIX スタイルのディレクトリ リスト表示」（P.18-17）を参照してください。
- シグニチャ アップデートのインストールに要する時間の詳細については、「シグニチャのアップデートおよびインストール時間」（P.18-17）を参照してください。