CHAPTER 3

Startup Wizard の使用

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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 およびウィザードを使用したセンサーの設定方法について説明します。次の事項について説明します。

IPS SSP セットアップについて

注意 IPS SSP には、4 種類のポート（コンソール、管理、GigabitEthernet、10GE）があります。IPS SSP の右前面パネルにあるコンソール ポートと管理ポートは、IPS ソフトウェアを使用して設定および制御します。IPS SSP の左前面パネルにある GigabitEthernet ポートと 10GE ポートは、IPS ソフトウェアではなく、ASA ソフトウェアを使用して設定および制御します。ただし、IPS SSP をリセットまたはシャットダウンした場合は、GigabitEthernet ポートと 10GE ポートもリンク ダウンします。スケジュールされたメンテナンスの時間帯は IPS SSP をリセットまたはシャットダウンして、これらのポートがリンク ダウンする影響を最小化する必要があります。

ネットワークに設置した IPS SSP に、ネットワークを介して通信できるようにするには、**setup** コマンドを使用して初期設定する必要があります。**setup** コマンドを使用して IPS SSP を初期設定するまで、IDM を設定できません。**setup** コマンドを使用してセンサーを初期設定するまで、IME を設定できません。

setup コマンドを使用して、ホスト名、IP アドレス、アクセス コントロール リスト、グローバル相関サーバ、時間帯、サマータイム設定といった基本的なセンサー設定、および SensorBase Network に参加するかを設定します。CLI で詳細設定を継続すれば、Telnet をイネーブルにして Web サーバを設定すること、仮想センサーとインターフェイスを割り当ててイネーブルにすること、脅威に対するデフォルトの防御設定を変更することが可能です。

（注）　IPS SSP は、インストール先の適応型セキュリティ アプライアンスから時刻の設定を取得します。

詳細情報

- IPS SSP の初期設定手順については、第 18 章「IPS SSP の初期化」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 11 章「グローバル相関の設定」を参照してください。
- ASA ソフトウェアの詳細については、次の URL を参照してください。
  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

[Startup Wizard Introduction] ウィンドウ

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

IDM は未設定のセンサーと通信できないため、センサー 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。通信パラメータは、すべて **setup** コマンドを使用して設定できます。すでに設定されているセンサーを Startup Wizard を使用して編集することは可能ですが、未設定の新規センサーに Startup Wizard を使用することはできません。この場合、**setup** コマンドを使用する必要があります。**setup** コマンドを使用してセンサーを初期化するまで、IDM はセンサーに接続できないからです。

注意　IDM がスタンドアロン モードで実行されている場合、IDM Startup Wizard を使用して ASA トラフィックを IPS SSP に割り当てることはできません。ASDM から IDM に接続できる場合は、IDM を使用して ASA トラフィックを割り当て可能です。

詳細情報

setup コマンドを使用した IPS SSP の初期設定手順については、第 18 章「IPS SSP の初期化」を参照してください。

センサーのセットアップ

このセクションでは、センサーのセットアップ方法について説明します。次の項目を取り上げます。

[Sensor Setup] ウィンドウ

[Sensor Setup] ウィンドウでは、基本動作用にセンサーを設定できます。初期化時に値を割り当ててあるので、ほとんどのフィールドには値がすでに読み込まれています。必要な場合は変更も可能です。

フィールド定義

[Sensor Setup] ウィンドウには、次のようなフィールドがあります。

- [Network Settings] : センサーのネットワークを設定できます。
  - [Host Name] : センサーの名前。ホスト名は、^[A-Za-z0-9_/-]+$ のパターンと一致する 1 ～ 64 文字のストリングにすることができます。デフォルトは sensor です。名前にスペースが含まれる場合、または名前が 64 文字を超える英数字の場合は、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 アドレスを入力できます。お客様のネットワークでプロキシが使用されている場合、グローバル相関更新のダウンロードにプロキシ サーバが必要なことがあります。
  - [HTTP Proxy Port] : HTTP プロキシ サーバのポート番号を入力できます。
  - [DNS Primary] : プライマリ DNS サーバの IP アドレスを入力できます。

  （注） グローバル相関が機能するには、DNS サーバと 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） DNS 解決は、グローバル相関更新サーバへのアクセスについてだけサポートされています。

- [Allowed hosts/networks that can access the sensor] : ACL（アクセス コントロール リスト）を追加できます。
  - [Network] : アクセス リストを追加するネットワークの IP アドレス。
  - [Mask] : アクセス リストを追加するネットワークのネットマスク。

  （注） センサー ACL エントリを変更する場合、変更が適用されるときに IDM がセンサーとの通信を失う可能性があります。

- [Network Participation] : SensorBase ネットワークへのデータ送信に参加するか、および参加するレベルを選択できます。
  - [Off] : いずれのデータも 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るため送信されません。
  - [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に日付と時刻を設定します。
  - [Date]：センサーの現地日付。日付と時刻を更新するときは、[Apply Date/Time to Sensor] をクリックして設定を有効にします。
  - [Apply Date/Time to Sensor]：センサーの日付と時刻をただちに更新します。

  （注）　Startup Wizard をキャンセルしても、日付と時刻の変更はそのまま残ります。

- [Time Zone]：時間帯名と UTC オフセットを設定します。
  - [Zone Name]：サマータイムが有効でないときの現地時間帯。デフォルトは UTC です。事前定義済みの 37 セットの時間帯から選択するか、^[A-Za-z0-9()+:,_/-]+$ というパターンと一致する一意の名前（24 文字）を作成することができます。
  - [Offset]：現地時間帯のオフセット（分単位）。デフォルトは 0 です。事前定義済みの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設定されます。

  （注）　時間帯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]：時刻源として NTP サーバを使用するようにセンサーを設定できます。
  - [IP Address]：NTP サーバの IP アドレス（NTP サーバを使用してセンサーの時刻を設定する場合）。
  - [Authenticated NTP]：キーおよびキー ID の必要な認証付きの NTP を使用できます。
  - [Key]：NTP MD5 キー タイプ。
  - [Key ID]：NTP サーバでの認証に使用するキーの ID（1 ～ 65535）。範囲外のキー ID を指定すると、エラー メッセージが表示されます。

  （注）　センサー時刻源として NTP サーバを使用することを推奨します。

- Summertime
  - [Enable Summertime]：サマータイム モードをイネーブルにします。デフォルトではディセーブルです。
  - [Configure Summertime]：クリックしてサマータイムを設定します。

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

センサーへアクセスさせるホストやネットワークのリストを設定できます。

次のホストは、アクセス リストにエントリが必要です。

- センサーへの Telnet が必要なホスト。
- センサーとの間で SSH の使用が必要なホスト。
- IDM や ASDM など、Web ブラウザからセンサーにアクセスする必要があるホスト。
- CSM など、センサーにアクセスする必要がある管理ステーション。
- センサーがマスター ブロッキング センサーの場合、ブロッキング転送センサーの IP アドレスがリストのエントリに含まれている必要があります。

フィールド定義

[Add ACL Entry]/[Edit ACL Entry] ダイアログボックスには、次のフィールドがあります。

- [IP Address] : センサーにアクセスさせるホストやネットワークの IP アドレス。
- [Network Mask] : センサーにアクセスさせるホストや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、次のフィールドがあります。

- [Summer Zone Name] : サマータイム ゾーン名。デフォルトは UTC です。事前定義済みの 37 セットの時間帯から選択するか、^[A-Za-z0-9()+:,_/-]+$ というパターンと一致する一意の名前（24 文字）を作成することができます。
- [Offset] : サマータイム中に加える分数。デフォルトは 60 です。事前定義済みの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設定されます。

  （注）　時間帯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] : サマータイムの開始時刻設定。値は、hh:mm です。範囲外の時間または分を指定すると、エラー メッセージが表示されます。
- [End Time] : サマータイムの終了時刻設定。値は、hh:mm です。範囲外の時間または分を指定すると、エラー メッセージが表示されます。
- [Summertime Duration] : 期間を定期にするか、単一の日付にするかを設定できます。
  - [Recurring] : 期間は定期モードです。
  - [Date] : 期間は非定期モードです。
  - [Start] : 開始する週、曜日、月の設定。
  - [End] : 終了する週、曜日、月の設定。

センサーの設定

Startup Wizard でセンサーの設定を行うには、次の手順に従います。

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

ステップ 2　[Configuration] > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] と選択し、[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 ネットワーク設定を変更すると、変更が適用されたときに IDM はセンサーとの接続を失います。

ステップ 7　グローバル相関のサポートのために HTTP プロキシ サーバまたは DNS サーバのいずれかを設定する場合、[HTTP Proxy Server] フィールドに HTTP プロキシ サーバの IP アドレス、[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。

DNS サーバを使用する場合、グローバル相関の更新が成功するには、DNS サーバを 1 台以上設定する必要があり、このサーバに到達できる必要があります。

注意　グローバル相関が機能するには、DNS サーバと 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更新サーバへのアクセスについてだけサポートされています。

ステップ 8　センサーへのアクセスが許可されたホストと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　変更を廃棄して [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、希望するネットワーク参加のレベルを選択します。

- [Off] : いずれのデータも 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るため送信されません。
- [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、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て [OK] をクリックしてから、[Apply Date/Time to Sensor] をクリックします。

ステップ 11　[Time Zone] で時間帯とオフセットを設定します。

a. [Zone Name] フィールドで、ドロップダウン リストから時間帯名を選択するか、自分で作成したものを入力します。これは、サマータイムの時間が有効でないときに表示される時間帯です。

b. [Offset] フィールドに、UTC からのオフセットを分単位で入力します。事前定義済みの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設定されます。

（注）　時間帯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 同期を使用する場合は、[NTP Server] の下で次の内容を入力します。

- NTP サーバの IP アドレス（[IP Address] フィールド）。

- 認証付き NTP を使用する場合は、[Authenticated NTP] チェックボックスをオンにして、NTP サーバのキーを [Key] フィールドに入力し、NTP サーバのキー ID を [Key ID] フィールドに入力します。

（注）　NTP サーバを定義すると、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 の **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てから、[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、作成した名前を入力します。これは、サマータイムが有効な場合に表示される名前です。

ステップ 15　サマータイム期間中に時計を進める時間幅（分数）を、[Offset] フィールドに入力します。事前定義済みの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設定されます。

ステップ 16　サマータイム設定の適用を開始する時刻を、[Start Time] フィールドに入力します。

ステップ 17　サマータイム設定を解除する時刻を、[End Time] フィールドに入力します。

ステップ 18　[Summertime Duration] の下で、サマータイム設定を毎年特定の期間有効にするのか（recurring）、特定の日付で開始および終了するのか（date）を選択します。

a. [Recurring]：ドロップダウン リストから開始時間と終了時間を選択します。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。デフォルトは、開始時刻、終了時刻とも 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　[Next] をクリックすると Startup Wizard を継続します。

（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。

Auto Update の設定

シグニチャとシグニチャ エンジンのアップデートを自動的に Cisco.com からダウンロードするようセンサーを設定できます。自動アップデートをイネーブルにした場合、センサーは Cisco.com にログインし、シグニチャ アップデートおよびシグニチャ エンジン アップデートをチェックします。アップデートが提供されている場合、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 IPS 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 Cisco.com からダウンロードするには、暗号化権限を持つ Cisco.com ユーザ アカウントが必要です。シスコのソフトウェアを初めてダウンロードするときに、暗号化権限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 サーバを介した Cisco.com との通信をサポートしていません。

サポートされるユーザ ロール

次のユーザ ロールがサポートされています。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）

自動アップデートを設定するには、管理者である必要があります。

フィールド定義

Startup Wizard の [Auto Update] ウィンドウには、次のようなフィールドがあります。

- [Enable Signature and Engine Updates from Cisco.com] : 自動的に Cisco.com からシグニチャとエンジン アップデートをダウンロードしてインストールするようセンサーを設定します。

  （注）　このフィールド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する必要があります。

- [Cisco.com Access] : 次のような Cisco.com サーバ アクセス オプションを指定できます。
  - [Username] : Cisco.com のユーザ アカウントに対応するユーザ名を指定します。
  - [Password] : Cisco.com のユーザ アカウントのパスワードを指定します。
  - [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認します。
- [Schedule] : 毎日の開始時刻を指定できます。
  - [Start Time] : アップデート プロセスの開始時刻を 24 時間制で指定します。この時刻に、センサーは Cisco.com に接続し、新しいアップデートがあればダウンロードします。

Auto Update の設定

Cisco.com からの自動アップデートを設定するには、次の手順に従います。

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

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

ステップ 3　Cisco.com からのシグニチャおよびエンジンの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 用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. [Confirm Password] フィールドに、確認のために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、24 時間制の hh:mm:ss 形式です。アップデートは毎日発生します。

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 4　[Finish] をクリックして変更を保存します。

詳細情報

- 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 サーバおよび HTTP サーバ」（P.16-12）を参照してください。
- UNIX スタイルのディレクトリ一覧の詳細については、「UNIX スタイルのディレクトリ リスト」（P.16-12）を参照してください。
- シグニチャ アップデートとインストール時刻の詳細については、「シグニチャ アップデートおよびインストール時間」（P.16-12）を参照してください。
- IPS ソフトウェアを入手する手順については、「Cisco IPS ソフトウェアの入手」（P.20-2）を参照してください。
- IPS ソフトウェアのバージョン管理の詳細については、「IPS ソフトウェアのバージョン管理」（P.20-3）を参照してください。