CHAPTER 16

センサーの管理

（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、センサーの管理方法、たとえば、パスワードの設定方法、ライセンス キーの入手方法およびインストール方法、IP ロギング変数の設定方法、最新ソフトウェアによるセンサーのアップデート方法、センサーをデフォルトに戻す方法、センサーのリブート方法、センサーのシャットダウン方法などについて説明します。次の事項について説明します。

パスワードの設定

ここでは、センサーのユーザのパスワードを設定する方法について説明します。次の事項について説明します。

[Password] ペイン

センサー管理者として、[Passwords] ペインでパスワードの作成方法を設定できます。すべてのユーザ作成パスワードは、[Passwords] ペインで設定したポリシーに準拠する必要があります。

[Passwords] ペインのフィールドの定義

[Passwords] ペインには次のフィールドが表示されます。

- [Attempt Limit]：アカウントをロックできます。これにより、ユーザは、ログイン試行を特定の回数失敗した後、ログイン試行を継続できなくなります。デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。
- [Size Range]：パスワードの最小許容サイズおよび最大許容サイズを表す範囲を指定します。有効な範囲は 6 ～ 64 文字です。
- [Minimum Digit Characters]：パスワードに含める必要のある数字の最小数を指定します。
- [Minimum Upper Case Characters]：パスワードに含める必要のある英大文字の最大数を指定します。
- [Minimum Lower Case Characters]：パスワードに含める必要のある英小文字の最小数を指定します。
- [Minimum Other Characters]：パスワードに含める必要のある英数字以外の印刷可能文字の最小数を指定します。
- [Number of Historical Passwords]：アカウントごとにセンサーで記憶する過去のパスワードの数。新しいパスワードが記憶されているいずれかのパスワードと一致した場合は、アカウントのパスワードの変更試行に失敗します。この値が 0 の場合、以前のパスワードは記憶されません。

パスワード要件の設定

パスワード要件を設定するには、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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Passwords] を選択します。

ステップ 3　[Attempt Limit] フィールドに、ユーザが正しいパスワードの入力を試行できる回数を入力します。

（注）　デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。

ステップ 4　[Size Range] フィールドに、パスワードの有効な長さを入力します。有効な範囲は 6 ～ 64 です。

ステップ 5　[Minimum Digit Characters] フィールドに、パスワードに含めることができる数字の最小数を入力します。

ステップ 6　[Minimum Upper Case Characters] フィールドに、パスワードに含めることができる英大文字の最小数を入力します。

ステップ 7　[Minimum Lower Case Characters] フィールドに、パスワードに含めることができる英小文字の最小数を入力します。

注意　パスワード ポリシーに、大文字や数字などの文字セットの最小数を含める場合、必要な文字セットの最小数の合計が、最小パスワード サイズを超えないようにする必要があります。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。

ステップ 8　[Minimum Other Characters] フィールドに、パスワードに含めることができるその他の文字の最小数を入力します。

ステップ 9　[Number of Historical Passwords] フィールドに、アカウントごとにセンサーで記憶する過去のパスワードの数を入力します。

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 10　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

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。

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

パスワードをデフォルトの **cisco** にリセットするには、**hw-module module** *slot_number* **password-reset** コマンドを使用します。ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、ROMMON confreg ビットに 0x7 を設定してからセンサーをリブートします。ROMMON ビットにより、GRUB メニューがデフォルトのオプション 2（**reset password**）に設定されます。

指定したスロットのモジュールに搭載されている IPS がパスワード回復をサポートしていないバージョンの場合は、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

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

（注）　IPS モジュールがインストールされていないと、このオプションはメニューに表示されません。

ステップ 2　[IPS Password Reset] の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。リセットが失敗した場合、IPS SSP の 適応型セキュリティ アプライアンス および IPS 7.1 以降に正しい ASA ソフトウェアがあることを確認します。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。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にされているセンサーでパスワードを回復しようとした場合、処理はエラーも警告も出さないで進められますが、パスワードはリセットされません。パスワードを忘れて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 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。パスワード回復は、CLI または IDM から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。

```
sensor# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
sensor(config)# service host
```

ステップ 4　パスワードの回復をディセーブルにします。

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

IDM 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 IDM にログインします。

ステップ 2　[Configuration] > [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。

パスワード回復のトラブルシューティング

パスワード回復をトラブルシューティングするときは、次の事項に注意してください。

- センサー設定でパスワード回復がディセーブルかどうかは、ROMMON プロンプト、GRUB メニュー、スイッチ CLI、ルータ CLI からは判別できません。パスワード回復を試行すると、常に成功したと表示されます。ディセーブルにされている場合、パスワードは **cisco** にリセットされません。センサーのイメージを再作成することだけ選択できます。
- パスワード回復はホスト コンフィギュレーションでディセーブルにすることができます。ROMMON などの外部メカニズムを使用するプラットフォームの場合、パスワードをクリアするコマンドは実行できますが、IPS でパスワード回復がディセーブルにされている場合、IPS はパスワード回復が許可されないことを検出して外部要求を拒否します。
- 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。

パスワード回復の状態の確認

パスワード回復がイネーブルかどうかを確認するには、**show settings | include password** コマンドを使用します。

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。

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

ステップ 3　フィルタリングした出力に設定を表示する **include** キーワードを使用して、パスワード回復の状態を確認します。

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

ライセンスの設定

ここでは、ライセンス キーの入手方法およびインストール方法について説明します。次の事項について説明します。

- 「[Licensing] ペイン」（P.16-6）
- 「ライセンスについて」（P.16-6）
- 「IPS 製品のサービス プログラム」（P.16-7）

[Licensing] ペイン

（注）　[Licensing] ペインでライセンス情報を表示したり、センサーのライセンス キーをインストールしたりするには、管理者である必要があります。

[Licensing] ペインで、センサーのライセンス キーを入手およびインストールできます。[Licensing] ペインに現在のライセンスの状態が表示されます。

ライセンスについて

センサーはライセンス キーなしでも動作しますが、シグニチャ アップデートの入手およびグローバル相関機能の使用には、ライセンス キーが必要です。ライセンス キーを入手するには、次の情報が必要です。

- Cisco Services for IPS サービス契約：リセラー、シスコのサービスまたは製品の営業担当者に問い合わせて、サービス契約をご購入ください。
- IPS デバイスのシリアル番号：IPS デバイスのシリアル番号を確認するには、IDM で [Configuration] > [Sensor Management] > [Licensing] を選択するか、CLI で **show version** コマンドを使用します。
- 有効な Cisco.com ユーザ名およびパスワード

トライアル ライセンス キーも使用可能です。契約に関係する問題が原因でセンサーのライセンスを受けられない場合は、ライセンスを必要とするシグニチャ アップデートをサポートしている 60 日間のトライアル ライセンスを入手できます。

ライセンス キーは、Cisco.com のライセンス サーバから入手できます。次に、このライセンス キーはセンサーに配信されます。または、ローカル ファイルに格納されているライセンス キーでライセンス キーをアップデートすることもできます。http://www.cisco.com/go/license にアクセスし、[IPS Signature Subscription Service] をクリックしてライセンス キーを申し込みます。

ライセンス キーのステータスは、次の場所に表示されます。

- [IDM Home] ウィンドウの [Health] タブの [Licensing] セクション
- [IDM Licensing] ペイン（[Configuration] > [Licensing]）
- CLI ログイン時のライセンス通知

IDM または CLI を起動すると、ライセンスの状態、つまり、ライセンス キーがトライアル、無効、または期限切れかどうかが常に通知されます。ライセンス キーなし、無効なライセンス キー、または期限切れライセンス キーでも IDM および CLI を引き続き使用できますが、シグニチャ アップデートはダウンロードできません。

すでに有効なライセンスがセンサーにインストールされている場合は、[License] ペインの [Download] をクリックして IDM を実行しているコンピュータにライセンス キーのコピーをダウンロードし、ローカル ファイルに保存できます。その後、紛失または破損したライセンスを置き換えることや、センサーのイメージを再作成してからライセンスを再インストールすることができます。

IPS 製品のサービス プログラム

ライセンス キーをダウンロードするときや、最新の IPS シグニチャ アップデートを入手するときは、任意の IPS 製品の Cisco Services for IPS サービス契約が必要です。シスコと直接的な関係を結んでいる場合は、担当のアカウント マネージャまたはサービス アカウント マネージャに連絡して、Cisco Services for IPS サービス契約を購入してください。シスコと直接的な関係を結んでいない場合は、サービス アカウントをティア 1 またはティア 2 のパートナーから購入できます。

次の IPS 製品を購入する場合は、Cisco Services for IPS サービス契約も購入する必要があります。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

IPS が含まれていない ASA 5500 シリーズ適応型セキュリティ アプライアンス製品を購入する場合は、SMARTnet 契約を購入する必要があります。

（注） SMARTnet では、オペレーティング システム アップデート、Cisco.com へのアクセス、TAC へのアクセス、および現場での翌営業日までのハードウェア交換サービスを利用できます。

IPS SSP がインストールされている状態で出荷される ASA 5500 シリーズ適応型セキュリティ アプライアンス製品を購入する場合、またはそれを購入して ASA 5500 シリーズ適応型セキュリティ アプライアンス製品に追加する場合、Cisco Services for IPS サービス契約を購入する必要があります。

（注） Cisco Services for IPS では、IPS シグニチャ アップデート、オペレーティング システム アップデート、Cisco.com へのアクセス、TAC へのアクセス、および現場での翌営業日までのハードウェア交換サービスを利用できます。

たとえば、ASA 5585-X を購入した後で IPS を追加する必要が生じ、ASA-IPS10-K9 を購入する場合は、その時点で Cisco Services for IPS サービス契約を購入する必要があります。Cisco Services for IPS サービス契約を結んだ後、ライセンス キーを申し込むには製品シリアル番号も必要です。

注意 RMA として製品を送った場合、シリアル番号は変わっています。この場合は、新しいシリアル番号に対応する新しいライセンス キーを取得する必要があります。

[Licensing] ペインのフィールド定義

[Licensing] ペインには、次のフィールドがあります。

- [Current License]：現在のライセンスの状態が表示されます。
  - [License Status]：センサーの現在のライセンスの状態が表示されます。
  - [Expiration Date]：ライセンス キーの有効期限が切れる日付（または切れた日付）。キーが無効な場合、日付は表示されません。

  - [Serial Number]：センサーのシリアル番号。
  - [Product ID]：センサーの製品 ID。
- [Update License]：新しいライセンス キーの入手先を指定します。
  - [Cisco.com]：ライセンス キーを取得するために Cisco.com のライセンス サーバに接続します。
  - [License File]：ライセンス ファイルを使用することを指定します。
  - [Local File Path]：ライセンス キーを格納しているローカル ファイルの場所を示します。

ライセンス キーの入手とインストール

（注） ライセンス キーを適用するには、有効な Cisco.com ユーザ名およびパスワードに加えて、事前に Cisco Services for IPS サービス契約が必要です。

ライセンス キーを入手してインストールするには、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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Licensing] を選択します。[Licensing] ペインに現在のライセンスの状態が表示されます。ライセンスをすでにインストールしてある場合は、[Download] をクリックして必要に応じて保存できます。

ステップ 3　次のいずれかを実行してライセンス キーを入手します。

- Cisco.com からライセンスを入手するには、[Cisco.com] オプション ボタンをクリックします。IDM は Cisco.com のライセンス サーバに接続し、シリアル番号をサーバに送信してライセンス キーを入手します。これがデフォルトの方式です。ステップ 4 に進みます。
- ライセンス ファイルを使用する場合は、[License File] オプション ボタンをクリックします。このオプションを使用するには、次の URL www.cisco.com/go/license からライセンス キーを申し込む必要があります。電子メールで送信されるライセンス キーを、IDM がアクセスできるドライブに保存してください。このオプションは、Cisco.com にアクセスできないコンピュータを使用している場合に有用です。ステップ 7 に進みます。

ステップ 4　[Update License] をクリックし、[Licensing] ダイアログボックスで [Yes] をクリックして続行します。[Status] ダイアログボックスにより、センサーが Cisco.com への接続を試行していることが通知されます。ライセンス キーが更新されたことを [Information] ダイアログボックスで確認できます。

ステップ 5　[OK] をクリックします。

ステップ 6　www.cisco.com/go/license にアクセスします。

ステップ 7　必須フィールドに入力します。ライセンス キーは、指定した電子メール アドレスに送信されます。

注意　ライセンス キーは、正しい IPS デバイス シリアル番号を持つデバイスでのみ有効であるため、正しい IPS デバイス シリアル番号が必要です。

ステップ 8　ハード ディスク ドライブまたは IDM を実行しているクライアントからアクセスできるネットワーク ドライブに、ライセンス キーを保存します。

ステップ 9　IDM にログインします。

ステップ 10　[Configuration] > [Sensor Management] > [Licensing] を選択します。

ステップ 11　[Update License] の下の [License File] オプション ボタンをクリックします。

ステップ 12　[Local File Path] フィールドにライセンス ファイルのパスを指定するか、[Browse Local] をクリックしてファイルを参照します。

ステップ 13　ライセンス ファイルを参照し、[Open] をクリックします。

ステップ 14　[Update License] をクリックします。

センサー ヘルスの設定

ここでは、センサー ヘルス メトリック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。

- 「[Sensor Health] ペイン」（P.16-9）
- 「[Sensor Health] ペインのフィールドの定義」（P.16-9）

[Sensor Health] ペイン

（注）　センサー ヘルス メトリックを設定するには、管理者である必要があります。

[Sensor Health] ペインで、IPS のヘルスおよびネットワーク セキュリティの状態を特定するために使用するメトリックを設定できます。結果は、各種ガジェットの [Home] ペインに表示されます。

チェックボックスをオンにしてメトリックを選択しない場合、そのメトリックは、ヘルスおよびネットワーク セキュリティの状態の結果には表示されません。デフォルトの設定をそのまま使用することもできますし、値を編集することもできます。

全体のヘルスは、すべてのメトリックの最も重要な設定に設定されます。たとえば、選択したメトリックの 1 つが赤で、残りのすべてが緑の場合、全体のヘルスは赤になります。IPS は、IPS の全体ヘルス状態が変化したとき、ヘルスおよびセキュリティ状態イベントを生成します。

センサーのセキュリティ状態は、仮想センサーが検出するイベントの脅威レーティングを使用して、仮想センサーごとに特定されます。仮想センサーが、その仮想センサーのしきい値を超過する脅威レーティングを持つイベントを検出すると、仮想センサーのセキュリティ状態は上昇します。しきい値を超過した後、設定済みの時間が経過するまで、セキュリティ状態は critical レベルのままです（その間、より高いレベルのイベントが検出されなかった場合）。

[Sensor Health] ペインのフィールドの定義

[Sensor Health] ペインには次のフィールドが表示されます。

- [Inspection Load]：検査ロードのしきい値を設定すること、およびこのメトリックをセンサーの全体的ヘルス評価に適用するかどうかを設定することができます。
- [Missed Packet]：損失パケットのしきい値パーセンテージを設定すること、およびこのメトリックをセンサーの全体的ヘルス評価に適用するかどうかを設定することができます。
- [Memory Usage]：メモリ使用量のしきい値パーセンテージを設定すること、およびこのメトリックをセンサーの全体的ヘルス評価に適用するかどうかを設定することができます。

- [Signature Update]：最後のシグニチャ アップデートが適用された時点に関するしきい値を設定すること、およびこのメトリックをセンサーの全体的ヘルス評価に適用するかどうかを設定することができます。
- [License Expiration]：ライセンスが有効期限切れになる時点に関するしきい値を設定すること、およびこのメトリックをセンサーの全体的ヘルス評価に適用するかどうかを設定することができます。
- [Event Retrieval]：最後のイベントが取得された時点に関するしきい値を設定すること、およびこのメトリックをセンサーの全体的ヘルス評価に適用するかどうかを設定することができます。

（注）　イベント取得メトリックでは、IME などの外部モニタリング アプリケーションが最後のイベントをいつ取得したかが追跡されます。外部イベント モニタリングを実行しない場合、[Event Retrieval] はディセーブルにします。

- ネットワーク参加：ネットワーク参加ヘルス メトリックをセンサーの全体的ヘルス評価に適用するかどうかを選択できます。
- グローバル相関：グローバル相関ヘルス メトリックをセンサーの全体的ヘルス評価に適用するかどうかを選択できます。
- [Application Failure]：アプリケーション障害をセンサーの全体的ヘルス評価に適用するかどうかを選択できます。
- [IPS in Bypass Mode]：バイパス モードがアクティブかどうか認識することを選択でき、それをセンサーの全体的ヘルス評価に適用できます。

（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 アプライアンスのコンフィギュレーションおよび IPS SSP で実行中の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、またはフェールオーバーのいずれかになります。

- [One or More Active Interfaces Down]：1 つ以上のイネーブル インターフェイスがダウンしているかどうか認識することを選択でき、それをセンサーの全体的ヘルス評価に適用できます。
- [Yellow Threshold]：黄色の最低しきい値をパーセンテージ、日、秒、または障害単位で設定できます。
- [Red Threshold]：赤色の最低しきい値をパーセンテージ、日、秒、または障害単位で設定できます。

IP ロギング変数の設定

（注）　IP ロギング変数を設定するには、管理者である必要があります。

IP ロギング変数の Maximum Open IP Log Files を設定できます。これは、センサーの一般動作に適用されます。

フィールド定義

[IP Logging Variables] ペインには、次のフィールドが表示されます。

- [Maximum Open IP Log Files]：同時に開くことができる IP ログ ファイルの最大数。有効な範囲は 20 ～ 100 です。デフォルトは 20 です。

自動アップデートの設定

ここでは、センサーに対し自動ソフトウェア アップデートを設定する方法について説明します。次の事項について説明します。

- 「[Auto/Cisco.com Update] ペイン」（P.16-11）
- 「サポートされる FTP サーバおよび HTTP サーバ」（P.16-12）
- 「UNIX スタイルのディレクトリ リスト」（P.16-12）
- 「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）
- 「[Auto/Cisco.com Update] ペインのフィールドの定義」（P.16-13）
- 「Auto Update の設定」（P.16-14）

[Auto/Cisco.com Update] ペイン

（注）　[Auto/Cisco.com Update] ペインを表示するには、および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。

注意　自動アップデートは、DOS スタイルのパスを使用して設定された Windows FTP サーバでは動作しません。サーバ設定で、DOS スタイルのパスではなく、UNIX スタイルのパス オプションがイネーブルになっていることを確認します。

Cisco.com から、およびローカル サーバからシグニチャ 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 FTP サーバおよび HTTP サーバ

IPS ソフトウェア アップデートでサポートされている FTP サーバは次のとおりです。

- WU-FTPD 2.6.2（Linux）
- Solaris 2.8
- Sambar 6.0（Windows 2000）
- Serv-U 5.0（Windows 2000）
- MS IIS 5.0（Windows 2000）

IPS ソフトウェア アップデートでサポートされている HTTP/HTTPS サーバは次のとおりです。

- CSM - Apache Server（Tomcat）
- CSM - Apache Server（JRun）

UNIX スタイルのディレクトリ リスト

FTP サーバを使用した自動アップデートを設定するには、FTP サーバで UNIX スタイルのディレクトリ リストを提供する必要があります。MS-DOS スタイルのディレクトリ リストは、センサーの自動アップデート機能ではサポートされていません。

（注）　サーバで MS-DOS スタイルのディレクトリ リストを提供すると、センサーはディレクトリ リストを解析できず、入手可能な新しいアップデートがあることを認識できません。

UNIX スタイルのディレクトリ リストを使用するように Microsoft IIS を変更するには、次の手順を実行します。

ステップ 1　[Start] > [Program Files] > [Administrative Tools] を選択します。

ステップ 2　[Home Directory] タブをクリックします。

ステップ 3　[UNIX directory listings style] オプション ボタンをクリックします。

シグニチャ アップデートおよびインストール時間

シグニチャ アップデートの実行中、トラフィックが検査されない短い期間があります。ただし、バイパスがイネーブルになっている場合、トラフィック フローは続行されます。

シグニチャ アップデートにより、正規表現を含むシグニチャが追加または変更される場合、SensorApp が使用する正規表現キャッシュ テーブルを再コンパイルする必要があります。再コンパイル時間は、プラットフォーム、変更、追加されるシグニチャの数、および変更、追加されるシグニチャのタイプにより異なります。

シグニチャ アップデートにより、ハイエンド プラットフォーム（たとえば、IPS 4255 や IPS 4260）に新しいシグニチャが 1 つまたは 2 つのみ追加される場合、再コンパイルは数分でただちに完了します。

次の条件下では、再コンパイルは数分から 30 分ほどかかります。

- シグニチャ アップデートにより、多数のシグニチャが追加される場合（たとえば、S240 の上に S258 をインストールする場合など、複数のシグニチャ レベルをスキップして新しいシグニチャをインストールする場合）。
- シグニチャ アップデートにより、多数のシグニチャが変更される場合（たとえば、多数の古いシグニチャがディセーブルにされ、廃棄される場合。またはこの一方が行われる場合）。

再コンパイル中、SensorApp はパケットのモニタリングを停止します。SensorApp への経路上にあるパケット バッファの空き容量が少なくなり始めると、インターフェイス ドライバはこれを検出し、SensorApp からのパケットの受信を停止します。センサーがインライン モードの場合、バイパス オプションが Auto に設定されている場合にはドライバはバイパスをオンにし、バイパス オプションが Off に設定されている場合にはドライバはインターフェイス リンクをダウン状態にします。

（注） バイパス設定が有効になる前に、一部のパケットがドロップされる場合があります。SensorApp は、正規表現キャッシュ ファイルの再コンパイルを完了すると、ドライバに再接続し、モニタリングを再開し、ドライバは、分析のために SensorApp へのパケットの受け渡しを開始し、必要に応じて、インターフェイス リンクをアップ状態に戻します。

[Auto/Cisco.com Update] ペインのフィールドの定義

[Auto/Cisco.com Update] ペインには、次のフィールドが表示されます。

- [Enable Auto Update From a Remote Server] : センサーでリモート サーバに格納されているアップデートをインストールできるようにします。

  （注） [Enable Auto Update From a Remote Server] がオフの場合、すべてのフィールドがディセーブルになり、クリアされます。これのオンとオフを切り替えると、他のすべての設定が失われます。

- [Remote Server Settings] : リモート サーバに関する次のオプションを指定できます。
  - [IP Address] : リモート サーバの IP アドレスを指定します。
  - [File Copy Protocol] : FTP と SCP のどちらを使用するかを指定します。
  - [Directory] : リモート サーバ上のアップデートへのパスを指定します。
  - [Username] : リモート サーバのユーザ アカウントに対応するユーザ名を指定します。
  - [Password] : リモート サーバのユーザ アカウントのパスワードを指定します。
  - [Confirm Password] : リモート サーバ 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。
- [Enable Signature and Engine Updates from Cisco.com] : センサーが Cisco.com にアクセスして、シグネチャ アップデートおよびエンジン アップデートをダウンロードできるようにします。
- [Cisco.com Server Settings] : Cisco.com サーバに関する次の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。
  - [Cisco.com URL] : [Enable Signature and Engine Updates from Cisco.com] チェックボックスがオンの場合、正しい URL が自動的に入力されます。

  - [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]：次のスケジュール オプションを指定できます。
  - [Start Time]：アップデート プロセスの開始時刻を指定します。これは、センサーがリモート サーバに接続し、入手可能なアップデートを検索する時刻です。
  - [Frequency]：アップデートを時間単位と週単位のどちらで実行するかを指定します。
  - [Hourly]：n 時間ごとにアップデートをチェックすることを指定します。
  - [Daily]：アップデートを実行する曜日を指定します。
- [Auto Update Info]：自動アップデート試行に関する情報を表示します。
  - [Last Directory Read Attempt]：センサーが新しいアップデートをチェックするために自動アップデート ディレクトリにアクセスした最終時刻を表示します。
  - [Last Download Attempt]：センサーがアップデートのダウンロードを試行した最終時刻を表示します。
  - [Last Install Attempt]：センサーがアップデートのインストールを試行した最終時刻を表示します。
  - [Next Attempt]：センサーがアップデートのダウンロードを試行する次の時刻を表示します。

Auto Update の設定

リモート サーバまたは Cisco.com からの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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Auto/Cisco.com Update] を選択します。

ステップ 3　リモート サーバからの自動アップデートをイネーブルにするには、[Enable Auto Update from a Remote Server] チェックボックスをオンにします。

a. [IP Address] フィールドに、アップデートをダウンロードし、保存した先のリモート サーバの IP アドレスを入力します。

b. リモート サーバに接続するために使用するプロトコルを指定するには、[File Copy Protocol] ドロップダウン リストから [FTP] または [SCP] を選択します。

c. [Directory] フィールドに、アップデートがあるリモート サーバのディレクトリへのパスを入力します。パスの有効な値は 1 ～ 128 までの文字です。

d. [Username] フィールドに、リモート サーバへ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。

e. [Password] フィールドに、リモート サーバのユーザ名の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。

f. [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。

g. アップデートを時間単位で指定するには、[Hourly] チェックボックスをオンにし、次の手順を実行します。

- [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 です。

- [Every_hours] フィールドに、時間間隔を入力します。この時間間隔で、すべてのアップデートが実行されます。有効な値は 1 ～ 8760 です。

  たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新があれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーは、インストールできる最新のアップデートを判別し、そのファイルをインストールします。

h. アップデートを週単位で指定するには、[Daily] チェックボックスをオンにし、次の手順を実行します。

- [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 です。
- [Days] フィールドにおいて、センサーで入手可能なアップデートをチェックし、ダウンロードする曜日をオンにします。

ステップ 4　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. アップデートを時間単位で指定するには、[Hourly] チェックボックスをオンにし、次の手順を実行します。

- [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 です。
- [Every_hours] フィールドに、時間間隔を入力します。この時間間隔で、すべてのアップデートが実行されます。有効な値は 1 ～ 8760 です。

  たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新があれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーは、インストールできる最新のアップデートを判別し、そのファイルをインストールします。

e. アップデートを週単位で指定するには、[Daily] チェックボックスをオンにし、次の手順を実行します。

- [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 です。
- [Days] フィールドにおいて、センサーで入手可能なアップデートをチェックし、ダウンロードする曜日をオンにします。

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 5　[Apply] をクリックして変更を保存します。

センサーの手動アップデート

ここでは、センサーを手動でアップデートする方法について説明します。次の事項について説明します。

[Update Sensor] ペイン

（注）　[Update Sensor] ペインを表示するには、およびサービス パックおよびシグニチャ アップデートを使用してセンサーをアップデートするには、管理者である必要があります。

[Update Sensor] ペインで、サービス パックおよびシグニチャ アップデートをただちに適用できます。センサーを手動でアップデートするには、サービス パックおよびシグニチャ アップデートを Cisco.com から FTP サーバにダウンロードし、その後、その FTP サーバからそれらをダウンロードするようにセンサーを設定します。

[Update Sensor] ペインのフィールドの定義

[Update Sensor] ペインには次のフィールドが表示されます。

- [Update is located on a remote server and is accessible by the sensor]：次のオプションを指定できます。
  - [URL]：アップデートがあるサーバのタイプを指定します。FTP、HTTP、HTTPS、または SCP を使用することを指定します。
  - [://]：リモート サーバにあるアップデートのパスを指定します。
  - [Username]：リモート サーバのユーザ アカウントに対応するユーザ名を指定します。
  - [Password]：リモート サーバのユーザ アカウントのパスワードを指定します。
- [Update is located on this client]：次のオプションを指定できます。
  - [Local File Path]：このローカル クライアントにあるアップデート ファイルのパスを指定します。
  - [Browse Local]：このローカル クライアントのファイル システム用の [Browse] ダイアログ ボックスを開きます。このダイアログボックスから、アップデート ファイルを参照できます。

センサーのアップデート

サービス パックとシグニチャのアップデートをすぐに適用するには、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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Update Sensor] を選択します。

ステップ 3　リモート サーバからアップデートを取得し、それをセンサーにインストールするには、次の手順を実行します。

a. [Update is located on a remote server and is accessible by the sensor] チェックボックスをオンにします。

b. [URL] フィールドには、アップデートのある URL を入力します。

（注） アップデートをあらかじめ Cisco.com からダウンロードし、FTP サーバに保存しておく必要があります。

次の URL タイプがサポートされています。

- FTP：：FTP ネットワーク サーバのソース URL です。

  このプレフィクスの構文は、次のとおりです。

  `ftp://location/relative_directory/filename`

  または

  `ftp://location//absolute_directory/filename`

- HTTPS:：Web サーバのソース URL です。

  （注） HTTPS プロトコルを使用する前に、TLS 信頼ホストを設定します。

  このプレフィクスの構文は、次のとおりです。

  `https://location/directory/filename`

- SCP:：SCP ネットワーク サーバのソース URL です。

  このプレフィクスの構文は、次のとおりです。

  `scp://location/relative_directory/filename`

  または

  `scp://location/absolute_directory/filename`

- HTTP:：Web サーバのソース URL です。

  このプレフィクスの構文は、次のとおりです。

  `http://location/directory/filename`

  次の例は、FTP プロトコルを示しています。

  `ftp://user@ip_address/UPDATES/file_name.rpm.pkg`

c. [Username] フィールドに、リモート サーバのアカウントのユーザ名を入力します。

d. [Password] フィールドに、リモート サーバのこのアカウントに関連付けられているパスワードを入力します。

ステップ 4　ローカル クライアントからアップデートを取得し、それをセンサーにインストールするには、次の手順を実行します。

a. [Update is located on this client] チェックボックスをオンにします。

b. ローカル クライアントにあるアップデート ファイルのパスを指定し、[Browse Local] をクリックして、ローカル クライアントにあるファイルを参照します。

ステップ 5　[Update Sensor] をクリックします。[Update Sensor] ダイアログボックスにより、アップデートする場合は、センサーへの接続が切断され、再ログインする必要があることが通知されます。

ステップ 6　[OK] をクリックして、センサーをアップデートします。

（注）　サービス パック、マイナー パッチ、メジャー パッチ、およびエンジニアリング パッチを使用したアップデート中、IDM および CLI の接続は切断されます。これらのアップデートのいずれかを適用する場合、インストーラにより IPS アプリケーションが再起動されます。センサーがリブートされる場合もあります。シグネチャ アップデートを適用する場合、接続は切断されず、したがって、システムをリブートする必要はありません。

ヒント　変更を廃棄してダイアログボックスを閉じるには、[Cancel] をクリックします。

デフォルトの復元

（注）　[Restore Defaults] ペインを表示するには、およびセンサーをデフォルト設定に戻すには、管理者である必要があります。

[Restore Defaults] ペインで、いつでもセンサーをデフォルト設定に戻すことができます。

警告　**デフォルト設定に戻すと、現在のアプリケーション設定が削除され、デフォルト設定が復元されます。ネットワーク設定もデフォルト設定に戻るため、センサーへの接続がただちに切断されます。**

デフォルトの設定を復元するには、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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Restore Defaults] を選択します。

ステップ 3　デフォルト設定に戻すには、[Restore Defaults] をクリックします。

ステップ 4　[Restore Defaults] ダイアログボックスで、[OK] をクリックします。

（注）　デフォルト設定に戻すと、IP アドレス、ネットマスク、デフォルト ゲートウェイ、およびアクセス リストがリセットされます。パスワードおよび時刻はリセットされません。手動および自動ブロックも有効なままになります。センサーを手動でリブートする必要があります。

センサーのリブート

（注）　[Reboot Sensor] ペインを表示するには、およびセンサーをリブートするには、管理者である必要があります。

[Reboot Sensor] ペインからセンサーをシャットダウンし、再起動できます。

センサーをリブートするには、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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Reboot Sensor] を選択し、[Reboot Sensor] をクリックします。

ステップ 3　センサーをシャットダウンし、再起動するには、[OK] をクリックします。センサー アプリケーションがシャットダウンし、その後リブートします。リブート後、再ログインする必要があります。

（注）　CLI にログインしているユーザに対して、センサー アプリケーションがシャットダウンするという通知が表示され、その 30 秒後にシャットダウンされます。

センサーのシャットダウン

（注）　[Shut Down Sensor] ペインを表示するには、およびセンサーをシャットダウンするには、管理者である必要があります。

IPS アプリケーションをシャットダウンした後、センサーの電源を安全に切ることができます。

センサーをシャットダウンするには、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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [Shut Down Sensor] を選択し、その後、[Shut Down Sensor] をクリックします。

ステップ 3　[Shut Down Sensor] ダイアログボックスで、[OK] をクリックします。

センサー アプリケーションがシャットダウンし、センサーへの接続が切断されます。

（注）　CLI にログインしているユーザに対して、センサー アプリケーションがシャットダウンするという通知が表示され、その 30 秒後にシャットダウンされます。