イメージとシグニチャ IDS 4.1 から IPS 5.0 以降（AIP-SSM、NM-IDS、IDSM-2）へのアップグレードの構成例

内容

はじめに

このドキュメントでは、Cisco Intrusion Detection Sensor(IDS)ソフトウェアのイメージとシグニチャをバージョン4.1からCisco Intrusion Prevention System(IPS)5.0以降にアップグレードする方法について説明します。

注：ソフトウェアバージョン5.x以降では、Cisco IPSがCisco IDSに置き換わります。これはバージョン4.1まで適用できます。

注：センサーは、Cisco.comからソフトウェアアップデートをダウンロードできません。Cisco.comからFTPサーバにソフトウェアアップデートをダウンロードし、FTPサーバからダウンロードするようにセンサーを設定する必要があります。

手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「AIP-SSMシステムイメージのインストール」セクションを参照してください。

Cisco Secure IDS（旧NetRanger）アプライアンスおよびバージョン3.xと4.xのモジュールを回復する方法についての詳細は、『Cisco IDS Sensor and IDS Services Modules (IDSM-1, IDSM-2)(Cisco IDSセンサーおよびIDSサービスモジュール(IDSM-1、IDSM-2)のパスワード回復手順』を参照してください。

注：アップグレード中は、ASA - AIP-SSMのinlineおよびfail-open設定のユーザトラフィックは影響を受けません。

注：IPS 5.1をバージョン6.xにアップグレードする手順についての詳細は、『コマンドラインインターフェイス6.0を使用したCisco Intrusion Prevention System Sensorの設定』の「Cisco IPSソフトウェアの5.1から6.xへのアップグレード」セクションを参照してください。

注：センサーは、自動更新のプロキシサーバをサポートしていません。プロキシ設定は、グローバルコリレーション機能に対してのみ使用できます。

前提条件

要件

5.0へのアップグレードに必要な最低限のソフトウェアバージョンは4.1(1)です。

使用するコンポーネント

このドキュメントの情報は、ソフトウェアバージョン4.1（バージョン5.0へのアップグレード予定）が稼働するCisco 4200シリーズIDSハードウェアに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

Cisco 4.1から5.0へのアップグレードは、Cisco.comからダウンロードできます。Cisco.comのIPSソフトウェアのダウンロードにアクセスする手順については、『Cisco IPSソフトウェアの入手』を参照してください。

アップグレードを実行するには、次に示すいずれかの方法を使用できます。

- 5.0アップグレードファイルをダウンロードした後、upgradeコマンドを使用して5.0アップグレードファイルをインストールする方法の手順について、『Readme』を参照してください。詳細は、このドキュメントの「upgradeコマンドの使用」セクションを参照してください。

- センサーの自動更新を設定した場合は、センサーが更新をポーリングするサーバ上のディレクトリに5.0アップグレードファイルをコピーします。詳細は、このドキュメントの「auto-upgradeコマンドの使用」セクションを参照してください。
- センサーにアップグレードをインストールし、リブート後にセンサーが使用できない場合は、センサーのイメージを変更する必要があります。4.1よりも前のCisco IDSバージョンからセンサーをアップグレードする場合は、recoverコマンドまたはrecovery/upgrade CDを使用する必要もあります。詳細は、このドキュメントの「センサーのイメージの変更」セクションを参照してください。

センサーのアップグレード

次のセクションでは、upgradeコマンドを使用してセンサーのソフトウェアをアップグレードする方法を説明しています。

概要

次のファイルを使用してセンサーをアップグレードできます。これらのファイルはすべて拡張子.pkgが付いています。

- シグニチャアップデート（IPS-sig-S150-minreq-5.0-1.pkgなど）
- シグニチャエンジンのアップデート（IPS-engine-E2-req-6.0-1.pkgなど）
- メジャーアップデート（IPS-K9-maj-6.0-1-pkgなど）
- マイナーアップデート（IPS-K9-min-5.1-1.pkgなど）
- サービスパックのアップデート（IPS-K9-sp-5.0-2.pkgなど）
- リカバリパーティションのアップデート（IPS-K9-r-1.1-a-5.0-1.pkgなど）
- パッチリリース（IPS-K9-patch-6.0-1p1-E1.pkgなど）
- リカバリパーティションのアップデート（IPS-K9-r-1.1-a-6.0-1.pkgなど）

センサーをアップグレードすると、センサーのソフトウェアバージョンが変更されます。

アップグレードコマンドとオプション

自動アップグレードを設定するには、サービスホストサブモードでauto-upgrade-option enabledコマンドを使用します。

これらのオプションによって、次の設定が割り当てられます。

- default：値をシステムのデフォルト設定に戻します。
- directory：アップグレードファイルが存在するファイルサーバ上のディレクトリ。
- file-copy-protocol：ファイルサーバからファイルをダウンロードするために使用されるファイルコピープロトコル。有効な値はftpまたはscpです。

  注：SCPを使用する場合は、ssh host-keyコマンドを使用してサーバをSSHの既知のホストリストに追加し、センサーがSSH経由でサーバと通信できるようにする必要があります。手順については、『既知のホストリストへのホストの追加』を参照してください。
- ip-address：ファイルサーバのIPアドレス。
- password：ファイルサーバでの認証用のユーザパスワード。
- schedule-option：自動アップグレードが行われるタイミングをスケジュールします。カレンダーのスケジュール設定では、特定の日の特定の時刻にアップグレードが開始されます。定期的なスケジュールでは、特定の定期的な間隔でアップグレードが開始されます。
  - calendar-schedule：自動アップグレードが実行される曜日と時刻を設定します。
    - days-of-week：自動アップグレードが実行される曜日。複数の日を選択できます。有効な値はSundayからSaturdayです。
    - no：エントリまたは選択設定を削除します。
    - times-of-day：自動アップグレードが開始される時刻。複数の時刻を選択できます。有効な値はhh:mm[:ss]です。
  - periodic-schedule：最初の自動アップグレードが実行される時刻、および自動アップグレードの間隔を設定します。
    - interval：自動アップグレードの間隔を時間数で指定します。有効な値は0 ~ 8760です。
    - start-time：最初の自動アップグレードを開始する時刻。有効な値はhh:mm[:ss]です。
- user-name：ファイルサーバでの認証用のユーザ名。

センサーをアップグレードするIDMの手順については、『Updating the Sensor』を参照してください。

upgradeコマンドの使用

IPS 6.0にアップグレードする前に、read-only-communityパラメータとread-write-communityパラメータが設定されていない場合は、SNMPエラーが発生します。SNMP setやgetの機能を使用している場合は、IPS 6.0にアップグレードする前に、read-only-communityとread-write-

communityのパラメータを設定する必要があります。IPS 5.xでは、read-only-communityはデフォルトでpublicに設定され、read-write-communityはデフォルトでprivateに設定されました。IPS 6.0では、これら2つのオプションにデフォルト値はありません。IPS 5.xでSNMP getおよびsetを使用しなかった場合（enable-set-getがfalseに設定された場合など）、IPS 6.0にアップグレードしても問題はありません。IPS 5.xでSNMPのgetおよびsetを使用した場合、たとえば、enable-set-getがtrueに設定されている場合、read-only-communityおよびread-write-communityパラメータを特定の値に設定する必要があります。そうしないと、IPS 6.0のアップグレードは失敗します。

次のエラー メッセージが表示されます。

```
Error: execUpgradeSoftware : Notification Application "enable-set-get" value set to true,
but "read-only-community" and/or "read-write-community" are set to null. Upgrade may not
continue with null values in these fields.
```

注：IPS 6.0はデフォルトで高リスクのイベントを拒否します。これはIPS 5.xからの変更です。デフォルトを変更するには、deny packet inlineアクションのイベントアクションオーバーライドを作成し、無効に設定します。管理者がread write（RW；読み取りと書き込み）コミュニティを認識していない場合、このエラーメッセージを削除するには、アップグレードを試行する前にSNMPを完全に無効にする必要があります。

センサーをアップグレードするには、次の手順を実行します。

1. メジャーアップデートファイル(IPS-K9-maj-5.0-1-S149.rpm.pkg)を、センサーからアクセス可能なFTP、SCP、HTTP、またはHTTPSサーバにダウンロードします。

   Cisco.comにあるソフトウェアの入手方法については、『Cisco IPSソフトウェアの入手』を参照してください。

   注：ファイルをダウンロードするには、暗号化権限を持つアカウントでCisco.comにログインする必要があります。ファイル名は変更しないでください。センサーが更新を受け入れるには、元のファイル名を保存する必要があります。

   注：ファイル名は変更しないでください。センサーが更新を受け入れるには、元のファイル名を保存する必要があります。

2. 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。

3. 次の設定モードを入力します。

   <#root>

   ```
   sensor#
   ```

   configure terminal

4. センサーをアップグレードします。

<#root>

sensor(config)#

upgrade scp://

@

//upgrade/

以下に例を挙げます。

注：このコマンドは、スペースの関係上2行で表記されています。

<#root>

sensor(config)#

upgrade scp://tester@10.1.1.1//upgrade/
IPS-K9-maj-5.0-1-S149.rpm.pkg

注：サポートされているFTPおよびHTTP/HTTPSサーバのリストについては、『サポートされているFTPおよびHTTP/HTTPSサーバ』を参照してください。SCPサーバをSSHの既知のホストリストに追加する方法については、『SSHの既知のホストリストへのホストの追加』を参照してください。

5. プロンプトが表示されたら、パスワードを入力します。

```
Enter password: ********
Re-enter password: ********
```

6. yesと入力して、アップグレードを完了します。

注：メジャーアップデート、マイナーアップデート、およびサービスパックによって、IPSプロセスの再起動が必要になったり、センサーの再起動を強制してインストールを完了させたりする場合があります。そのため、サービスが少なくとも2分間中断されます。ただし、シグニチャのアップデートでは、アップデートの実行後にリブートする必要はありません。最新のアップデートについては、『シグニチャアップデートのダウンロード』(登録ユーザ専用)を参照してください。

7. 新しいセンサーのバージョンを確認します。

```
<#root>

sensor#

show version

Application Partition:

Cisco Intrusion Prevention System,

Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys

Platform: ASA-SSM-20

Serial Number: 021

No license present

Sensor up-time is 5 days.

Using 490110976 out of 1984704512 bytes of available memory (24% usage)

system is using 17.3M out of 29.0M bytes of available disk space (59% usage)

application-data is using 37.7M out of 166.6M bytes of
available disk space (24 usage)

boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)

MainApp          2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running
```

```
AnalysisEngine  2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600  Running

CLI             2005_Mar_04_14.23 (Release)  2005-03-04T14:35:11-0600


Upgrade History:


  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004


Recovery Partition Version 1.1 - 5.0(1)S149


sensor#
```

注：IPS 5.xでは、「アップグレードのタイプが不明です」というメッセージが表示されます。このメッセージは無視してかまいません。

注：オペレーティングシステムが再イメージ化され、サービスアカウントを介してセンサーに配置されたすべてのファイルが削除されます。

センサーのアップグレードに関するIDMの手順についての詳細は、『Updating the Sensor』を参照してください。

自動アップグレードの設定

自動アップグレード

アップグレードディレクトリで新しいアップグレードファイルを自動的に検索するようにセンサーを設定できます。たとえば、複数のセンサーが、異なる更新スケジュールを持つ同じリモートFTPサーバディレクトリを指している場合があります。たとえば、24時間ごと、月曜日、水曜日、金曜日の午後11時などです。

自動アップグレードをスケジュールするには、次の情報を指定します。

- サーバ IP アドレス
- センサーがアップグレードファイルを確認するファイルサーバー上のディレクトリのパス
- ファイルコピープロトコル（SCPまたはFTP）
- ユーザ名とパスワード
- アップグレードスケジュール

センサーが自動アップグレードをポーリングできるようにするには、Cisco.comからソフトウェアアップグレードをダウンロードして、アップグレードディレクトリにコピーする必要があります。

注：AIM-IPSおよび他のIPSアプライアンスまたはモジュールで自動アップグレードを使用する場合、6.0(1)アップグレードファイルのIPS-K9-6.0-1-E1.pkgとAIM-IPSアップグレードファイルのIPS-AIM-K9-6.0-4-E1.pkgの両方を自動アップデートサーバに配置して、AIM-IPSが自動的にダウンロードしてインストールする必要ファイルを正検出できるようにします。6.0(1)アップグレードファイルIPS-K9-6.0-1-E1.pkgのみを自動更新サーバに配置した場合、AIM-IPSはダウンロードして、それをインストールしようとします。これは、AIM-IPSでは不適切なファイルです。

センサーの自動アップグレードに関するIDMの手順についての詳細は、『センサーの自動更新』を参照してください。

auto-upgradeコマンドの使用

auto-updateコマンドについては、このドキュメントの「upgradeコマンドとオプション」のセクションを参照してください。

自動アップグレードをスケジュールするには、次の手順を実行します。

1. 管理者権限を持つアカウントで CLI にログインします。
2. アップグレードディレクトリで新しいアップグレードを自動的に検索するようにセンサーを設定します。

```
<#root>

sensor#

configure terminal

sensor(config)#

service host

sensor(config-hos)#

auto-upgrade-option enabled
```

3. スケジューリングを指定します。
   - カレンダーのスケジュール設定では、特定の日の特定の時刻にアップグレードを開始します。

```
<#root>

sensor(config-hos-ena)#

schedule-option calendar-schedule

sensor(config-hos-ena-cal#

days-of-week sunday

sensor(config-hos-ena-cal#
```

```
times-of-day 12:00:00
```

- 定期的なスケジュールでは、特定の定期的な間隔でアップグレードが開始されます。

```
<#root>
sensor(config-hos-ena)#
schedule-option periodic-schedule
sensor(config-hos-ena-per)#
interval 24
sensor(config-hos-ena-per)#
start-time 13:00:00
```

4. ファイルサーバのIPアドレスを指定します。

```
<#root>
sensor(config-hos-ena-per)#
exit
sensor(config-hos-ena)#
ip-address 10.1.1.1
```

5. アップグレードファイルが存在するファイルサーバ上のディレクトリを指定します。

```
<#root>
sensor(config-hos-ena)#
directory /tftpboot/update/5.0_dummy_updates
```

6. ファイルサーバで認証するユーザ名を指定します。

```
<#root>
sensor(config-hos-ena)#
user-name tester
```

7. ユーザのパスワードを指定します。

```
<#root>
sensor(config-hos-ena)#
password

Enter password[]:
******
Re-enter password:
 ******
```

8. ファイルサーバプロトコルを指定します。

```
<#root>
sensor(config-hos-ena)#
file-copy-protocol ftp
```

注：SCPを使用する場合は、センサーがSSH経由でサーバと通信できるように、ssh host-keyコマンドを使用してサーバをSSHの既知のホストリストに追加する必要があります。手順については、『既知のホストリストへのホストの追加』を参照してください。

9. 設定を確認します。

```
<#root>
sensor(config-hos-ena)#
show settings

   enabled
   ----------------------------------------------
      schedule-option
      ----------------------------------------------
         periodic-schedule
         ----------------------------------------------
            start-time: 13:00:00
            interval: 24 hours
```

```
        ----------------------------------------------

      ----------------------------------------------

      ip-address: 10.1.1.1

      directory: /tftpboot/update/5.0_dummy_updates

      user-name: tester

      password: <hidden>

      file-copy-protocol: ftp default: scp

   ----------------------------------------------

sensor(config-hos-ena)#
```

10. 自動アップグレードサブモードを終了します。

```
<#root>

sensor(config-hos-ena)#

exit

sensor(config-hos)#

exit


Apply Changes:?

[yes]:
```

11. 変更を適用するにはEnterキーを押し、変更を破棄するにはnoと入力します。

センサーの再イメージング

センサーの再イメージ化は、次の方法で実行できます。

- CD-ROMドライブを備えたIDSアプライアンスの場合は、recovery/upgrade CDを使用します。

  手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「リカバリ/アップグレードCDの使用」セクションを参照してください。

- すべてのセンサーで、recoverコマンドを使用します。

  手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「アプリケーションパーティションの回復」セクションを参照してください。

- IDS-4215、IPS-4240、およびIPS 4255の場合は、ROMMONを使用してシステムイメージを復元します。

  手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「IDS-4215システムイメージのインストール」および「IPS-4240およびIPS-4255システムイメージのインストール」のセクションを参照してください。

- NM-CIDSの場合は、ブートローダを使用します。

  手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「NM-CIDSシステムイメージのインストール」セクションを参照してください。

- IDSM-2で、メンテナンスパーティションからアプリケーションパーティションのイメージを変更します。

  手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「IDSM-2システムイメージのインストール」セクションを参照してください。

- AIP-SSMの場合は、hw-module module 1 recover [configure | boot]コマンドを発行します。

  手順については、『システムイメージのアップグレード、ダウンロード、およびインストール』の「AIP-SSMシステムイメージのインストール」セクションを参照してください。

関連情報

- Cisco 侵入防御システムに関するサポート ページ
- IPS 6.0システムイメージのアップグレード、ダウンロード、およびインストール
- Cisco Catalyst 6500シリーズ侵入検知システム(IDSM-2)モジュールに関するサポートページ
- Cisco IDS SensorおよびIDSサービスモジュールのパスワード回復手順1、IDSM-2)
- 自動シグニチャアップデートのトラブルシューティング
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。