CHAPTER 21

IPS SSP のシステム イメージのインストール

（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、IPS SSP システム イメージをインストール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 7.1(1)E4 のファイル

（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。

次のファイルは、Cisco IPS 7.1(1)E4 に付属しています。

- Readme
  - IPS-7-1-1-E4.readme.txt
- システム イメージ ファイル
  - IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_40-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_60-K9-sys-1.1-a-7.1-1-E4.img
- リカバリ イメージ ファイル
  - IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_20-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_40-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_60-K9-r-1.1-a-7.1-1-E4.pkg

詳細情報

Cisco.com から IPS ソフトウェア ファイルをダウンロードするための手順については、「Cisco IPS ソフトウェアの入手」（P.20-2）を参照してください。

サポートされる FTP サーバおよび HTTP/HTTPS 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）

ROMMON について

適応型セキュリティ アプライアンス には、ROMMON というプリブート CLI が含まれています。これにより、プライマリ デバイス上のイメージが欠落または破損しているか、このいずれでもない一方で標準のアプリケーションをブートできない場合に、適応型セキュリティ アプライアンス上のイメージをブートできます。ROMMON は、シリアル コンソール ポートが利用可能であれば、リモート適応型セキュリティ アプライアンスの復旧に特に有用です。

ROMMON へのアクセスは、適応型セキュリティ アプライアンス シャーシの RJ-45F コネクタで利用可能なシスコ標準の非同期 RS-232C DTE であるシリアル コンソール ポートを介してのみ可能です。シリアル ポートは、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、フロー制御なしに設定されます。

詳細情報

ターミナル サーバを使用する手順については、「シリアル ポートへの接続」（P.21-3）を参照してください。

TFTP サーバ

ROMMON は TFTP を使用して、イメージをダウンロードして起動します。TFTP は、遅延やエラーリカバリなどのネットワークの問題は処理しません。TFTP では限定的なパケットの整合性チェックを実装するため、正しい整合性値を持つパケットは順番に到着し、エラーが発生する可能性はきわめて低くなります。ただし、TFTP はパイプラインを提供しないため、転送の合計時間は、転送するパケットの数にネットワークの平均値、RTT を掛けた値と等しくなります。この制限があるため、TFTP サーバはセンサーと同じ LAN セグメントに配置することを推奨します。RTT が 100 ミリ秒未満のネットワークであれば、イメージ配信の信頼性は高くなります。一部の TFTP サーバでは、転送可能な最大ファイル サイズが約 32 MB に制限されています。

シリアル ポートへの接続

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続のターミナル サーバの場合、180 ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで、ラインおよびポートを設定します。イネーブル モードでは、次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。

ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

IPS SSP のシステム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定は失われます。システム イメージをインストールしてセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、センサーの起動時にリカバリ パーティションを選択して復旧を試みてください。

ここでは、**hw-module** コマンドまたは ROMMON を使用して IPS SSP システム イメージをインストール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。

- 「hw-module コマンドの使用によるシステム イメージのインストール」（P.21-4）
- 「ROMMON を使用したシステム イメージのインストール」（P.21-6）

hw-module コマンドの使用によるシステム イメージのインストール

システム イメージをインストールするには、適応型セキュリティ アプライアンス CLI を使用して、TFTP サーバから IPS SSP にソフトウェア イメージを転送します。適応型セキュリティ アプライアンスは IPS SSP の ROMMON アプリケーションと通信し、イメージを転送できます。

（注）　指定する TFTP サーバが、最大 60 MB のサイズのファイルを転送できることを確認してください。

（注）　ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

IPS SSP ソフトウェア イメージを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　適応型セキュリティ アプライアンスにログインします。

ステップ 2　イネーブル モードを開始します。

```
asa# enable
```

ステップ 3　IPS SSP の復旧設定を行います。

```
asa (enable)# hw-module module 1 recover configure
```

（注）　誤った復旧設定を行った場合は、**hw-module module 1 recover stop** コマンドを使用して、システムのイメージの再作成を停止してから設定を修正できます。

ステップ 4　ソフトウェア イメージの TFTP URL を指定します。

```
Image URL [tftp://0.0.0.0/]:
```

例

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

ステップ 5　IPS SSP のコマンド/コントロール インターフェイスを指定します。

（注）　ポート IP アドレスは、IPS SSP の管理 IP アドレスです。

```
Port IP Address [0.0.0.0]:
```

例

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

ステップ 6　VLAN を ID は 0 のままにします。

```
VLAN ID [0]:
```

ステップ 7　IPS SSP のデフォルト ゲートウェイを指定します。

```
Gateway IP Address [0.0.0.0]:
```

例

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

ステップ 8　復旧を実行します。これにより、TFTP サーバから IPS SSP にソフトウェア イメージが転送されて、センサーが再起動されます。

```
asa# hw-module module 1 recover boot
```

ステップ 9　リカバリが完了するまで定期的にチェックします。

（注）　リカバリ中はステータスに [Recovery] と表示され、インストールが完了すると [Up] になります。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS10
Hardware version:   1.0
Serial Number:      ABC1234DEFG
Firmware version:   2.0(1)3
Software version:   7.1(0.326)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.148.11
```

```
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       10.89.148.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa
```

（注） 出力の [Status] フィールドは IPS SSP の動作ステータスを示します。IPS SSP の動作ステータスは、通常は「Up」と表示されます。適応型セキュリティ アプライアンスはソフトウェア イメージを IPS SSP に転送しますが、出力の [Status] フィールドには [Recover] と表示されます。適応型セキュリティ アプライアンスがソフトウェア イメージの転送を完了し、IPS SSP を再起動すると、新たに転送されたイメージが実行されます。

（注） この処理の間に発生した何らかのエラーをデバッグする場合は、**debug module-boot** コマンドを使用して、ソフトウェア インストール処理のデバッグをイネーブルにします。

ステップ 10　IPS SSP へのセッションを確立します。

ステップ 11　**cisco** を 3 回と新しいパスワードを 2 回入力します。

ステップ 12　**setup** コマンドを使用して、IPS SSP を初期化します。

詳細情報

- IPS SSP アプリケーション パーティションを復旧するための手順については、「アプリケーション パーティションの復旧」（P.21-10）を参照してください。
- Cisco.com から IPS ソフトウェア ファイルをダウンロードするための手順については、「Cisco IPS ソフトウェアの入手」（P.20-2）を参照してください。

ROMMON を使用したシステム イメージのインストール

適応型セキュリティ アプライアンスで ROMMON を使用して、システム イメージを IPS SSP に TFTP でダウンロードすることにより、IPS SSP のシステム イメージをインストールできます。

IPS SSP システム イメージを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　適応型セキュリティ アプライアンス からアクセスできる、TFTP サーバの tftp ルート ディレクトリに IPS SSP システム イメージ ファイル（例：IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img）をダウンロードします。

（注） 適応型セキュリティ アプライアンスのイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IPS SSP をブートします。

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 0.0(2)10 11:16:38 04/15/10
```

```
Com KbdBuf SMM UsbHid Msg0 Prompt Pmrt Cache1 LowM ExtM HugeM Cache2 Flg Siz0 Amrt PMM
PnpDsp Smbios Lpt0 Npx1 Apm Lp1 Acpi Typ Dbg Enb Mp MemReduce MemSync1 CallRoms MemSync2
DriveInit


Total memory : 12 GB
Total number of CPU cores : 8
Com Lp1 Admgr2 Brd10 Plx2 OEM0=7EFF5C74
Cisco Systems ROMMON Version (1.0(12)10) #0: Thu Apr 8 00:12:33 CDT 2010

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is UP
MAC Address: 5475.d029.7fa9
```

ステップ 3　システムのブート中に、次のプロンプトに対して Break または Esc を押し、ブートを中断します。ブートをすぐに開始するには、Space バーを押します。システムが ROMMON モードに入ります。rommon> プロンプトが表示されます。

（注）　Break または Esc は 10 秒以内に押してください。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

ステップ 4　現在のネットワーク設定を確認します。

```
rommon #0> set
ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

変数の定義は次のとおりです。

- Address：IPS SSP のローカル IP アドレス
- Server：アプリケーション イメージが格納されている TFTP サーバの IP アドレス
- Gateway：IPS SSP が使用するゲートウェイの IP アドレス
- Port：IPS SSP の管理に使用されるイーサネット インターフェイス
- VLAN：VLAN ID 番号（タグなしのままにしておきます）
- Image：システム イメージのファイル / パス名
- Config：これらのプラットフォームでは未使用

（注）　ネットワーク接続を確立するために、すべての値が必要なわけではありません。address、server、gateway、および image の値は必要です。ローカル環境を設定するために必要な設定がわからない場合は、システム管理者に連絡してください。

ステップ 5　必要に応じて、TFTP ダウンロードに使用するインターフェイスを変更します。

```
rommon> PORT=interface_name
```

（注）　TFTP ダウンロードに使用するデフォルト インターフェイスは、PortChannel 0/0 です。これは、IPS SSP の管理インターフェイスに対応しています。

ステップ 6　必要に応じて、IPS SSP 上のローカル ポートの IP アドレスを割り当てます。

```
rommon> ADDRESS=ip_address
```

（注）　IPS SSP に割り当てたものと同じ IP アドレスを使用します。

ステップ 7　必要に応じて、TFTP サーバの IP アドレスを割り当てます。

```
rommon> SERVER=ip_address
```

ステップ 8　必要に応じて、ゲートウェイ IP アドレスを割り当てます。

```
rommon> GATEWAY=ip_address
```

ステップ 9　次のいずれかのコマンドを使用して、ローカル イーサネット ポートから ping を実行することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 10　必要に応じて、イメージのダウンロード元である TFTP ファイル サーバ上のパスとファイル名を定義します。

```
rommon> IMAGE=path/file_name
```

注意　**IMAGE** コマンドは、必ず、すべて大文字で入力します。他の ROMMON コマンドは大文字と小文字のいずれでも入力できますが、**IMAGE** コマンドに限ってはすべて大文字にする必要があります。

UNIX の例

```
rommon> IMAGE=/system_images/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

（注）　このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリからの相対パスです。デフォルト tftpboot ディレクトリに配置されているイメージの場合は、IMAGE の指定でディレクトリ名もスラッシュも付きません。

ステップ 11　**set** と入力し、Enter を押してネットワーク設定を確認します。

（注）　**sync** コマンドを使用すると、これらの設定を NVRAM に保存して、複数ブート間で維持できます。保存しない場合は、ROMMON からイメージをブートするときは毎回この情報を入力しなければなりません。

ステップ 12　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

注意　システム イメージの破損を避けるために、システム イメージのインストール中は、IPS SSP から電源を取り出さないでください。

（注）　ネットワーク設定が正しければ、システムは指定されたイメージを IPS SSP にダウンロードし、ブートします。必ず IPS SSP イメージを使用してください。

詳細情報

- IPS SSP アプリケーション パーティションを復旧するための手順については、「アプリケーション パーティションの復旧」（P.21-10）を参照してください。
- Cisco.com から IPS ソフトウェア ファイルをダウンロードするための手順については、「Cisco IPS ソフトウェアの入手」（P.20-2）を参照してください。

リカバリ パーティションのアップグレード

IPS SSP 上のアプリケーション パーティションを復旧する必要があるときに備えるために、リカバリ パーティションを最新バージョンでアップグレードするには、**upgrade** コマンドを使用します。

（注）　リカバリ パーティション イメージはメジャー アップデートおよびマイナー アップデート用に生成されますが、まれにサービス パックまたはシグニチャ アップデート用に生成されます。

IPS SSP 上のリカバリ パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　センサーからアクセスできる、FTP サーバ、SCP サーバ、HTTP サーバ、または HTTPS サーバにリカバリ パーティション イメージ ファイル（例：IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg）をダウンロードします。

注意　一部のブラウザでは、ファイル名に拡張子が追加されます。保存されたファイルのファイル名は、ダウンロードページに表示されているものと一致している必要があります。一致していない場合、そのファイルは、リカバリ パーティションのアップグレードに使用できません。

ステップ 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。

ステップ 3　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 4　リカバリ パーティションをアップグレードします。

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
```

ステップ 5　サーバ パスワードを入力します。アップグレード プロセスが開始されます。

（注）　この手順では、リカバリ パーティションのイメージだけが再作成されます。このアップグレードでは、アプリケーションパーティションは変更されません。リカバリ パーティションの後にアプリケーション パーティションのイメージを再作成するには、**recover application-partition** コマンドを使用します。

アプリケーション パーティションの復旧

ここでは、アプリケーション パーティションの復旧方法について説明します。次の事項について説明します。

アプリケーション パーティションについて

センサーのアプリケーション パーティション イメージが使用できなくなった場合に、これを復旧できます。この方法を使用すると一部のネットワーク設定情報が保持されるので、復旧を実行した後もネットワークにアクセスできます。

リカバリ パーティションをブートするには、**recover application-partition** コマンドを使用します。これにより、センサー上のアプリケーションパーティションが自動的に復旧されます。

（注）　アプリケーション パーティション イメージを復旧する前にリカバリ パーティションを最新のバージョンにアップグレードしてある場合は、その最新のソフトウェア イメージをインストールできます。

recover application-partition コマンドは Telnet 接続または SSH 接続を介して実行できるため、リモート ロケーションに設置されているセンサーを復旧するにはこのコマンドを使用することを推奨します。

（注）　復旧後にセンサーに再接続するときは、デフォルトのユーザ名とパスワードの **cisco** でログインする必要があります。

詳細情報

リカバリ パーティションを最新バージョンにアップグレードするための手順については、「リカバリ パーティションのアップグレード」（P.21-9）を参照してください。

IPS SSP アプリケーション パーティション イメージの復旧

アプリケーション パーティション イメージを復旧するには、次の手順を実行します。

ステップ 1　センサーからアクセスできる、FTP サーバ、HTTP サーバ、または HTTPS サーバにリカバリ パーティション イメージ ファイル（例：IPS-SSP_20-K9-r-1.1-a-7.1-1-E4.pkg）をダウンロードします。

ステップ 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。

ステップ 3　コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

（注）　リカバリ パーティションをアップグレードするには、センサーですでに IPS 7.1(1) を実行している必要があります。

ステップ 4　アプリケーション パーティション イメージを復旧します。

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 7.1(1)E4. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

ステップ 5　**yes** を入力して続行します。

シャットダウンは、**recover** コマンドの実行直後に開始されます。シャットダウンは、少し時間がかることがあり、その間はまだ CLI にアクセスできますが、アクセスは警告なしで終了されます。

リカバリ パーティションに格納されているイメージを使用して、アプリケーション パーティションのイメージが再作成されます。次に、**setup** コマンドによってアプライアンスを初期化する必要があります。IP アドレス、ネットマスク、アクセス リスト、タイムゾーン、およびオフセットが保存され、イメージが再作成されたアプリケーション パーティションに適用されます。**recover application-partition** コマンドをリモートで実行した場合は、デフォルトのユーザ名とパスワード（**cisco**/**cisco**）を使用してセンサーに SSH で接続して、**setup** コマンドによって再度センサーを初期化します。Telnet はデフォルトでディセーブルなので、センサーを初期設定するまでは、Telnet を使用できません。

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。
- リカバリ パーティションを最新バージョンにアップグレードするための手順については、「リカバリ パーティションのアップグレード」（P.21-9）を参照してください。