CHAPTER 20

# IPS SSP システム イメージのインストール

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在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、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。次のような構成になっています。



## IPS 7.1(1)E4 のファイル

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585-X のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

次のファイルは、Cisco IPS 7.1(1)E4 の一部です。

- 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手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）を参照してください。

# サポートされる FTP および HTTP/HTTPS サーバ

次の FTP サーバで IPS ソフトウェアのアップデートがサポートされています。

- 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）

次の HTTP/HTTPS サーバで IPS ソフトウェアのアップデートがサポートされています。

- CSM - Apache サーバ（Tomcat）
- CSM - Apache サーバ（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 と呼ばれるプリブート CLI が含まれています。これにより、プライマリ デバイスのイメージが紛失、破損、またはその他の理由で通常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することができます。ROMMON は、リモートの適応型セキュリティ アプライアンスの復旧に特に役立ちます（シリアル コンソール ポートが利用可能な場合）。

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ています。

**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.20-3）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、起動します。TFTP は、遅延やエラー回復などのネットワークの問題は処理しません。TFTP は限定的なパケットの整合性チェックを実装するので、正しい整合性値を持つパケットが順番に到着し、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ので、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 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は、イメージを確実に伝送する必要があります。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 に制限されていることに注意してください。

# 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 接続を使用するターミナル 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 サーバで回線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 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方法や、センサーのブート時にリカバリ パーティションを選択する方法で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 のシステム イメージをインストールする方法について説明します。次のような構成になっています。

- 「hw-module コマンドを使用したシステム イメージのインストール」（P.20-4）
- 「ROMMON を使用したシステム イメージのインストール」（P.20-6）

## hw-module コマンドを使用したシステム 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 アプライアンスの 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て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 のソフトウェア 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 のリカバリ設定を行います。

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

**（注）**　リカバリ設定を誤った場合は、**hw-module module 1 recover stop** コマンドを使用してシステム イメージの再作成を停止すると、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://192.0.2.5/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

**ステップ 5**　IPS SSP のコマンドおよびコントロール 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]: 192.0.2.22
```

**ステップ 6**　VLAN ID を 0 のままにしておきます。

```
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]: 192.0.2.254
```

**ステップ 8**　リカバリを実行します。

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

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、再起動されます。

**ステップ 9**　リカバリが完了するまで、定期的に確認します。

**（注）**　ステータスは、リカバリ中は `Recovery` となり、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(1)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:       192.0.2.11
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       192.0.2.254
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）** このプロセス中に発生する可能性のあるエラーをデバッグするには、**debug module-boot** コマンドを使用して、ソフトウェア インストール プロセスのデバッグをイネーブルにします。

**ステップ 10**　IPS SSP に対してセッションを開始します。

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

**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 パーティションの復旧手順については、「アプリケーション パーティションの復旧」（P.20-10）を参照してください。
- IPS ソフトウェアの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）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 のシステム 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**　IPS SSP のシステム イメージ ファイル（IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img など）を、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、次のプロンプトで Break または Esc キーを押してブートを中断します。ブートをただちに開始するには、Space を押します。

**（注）**　Break または Esc キーは 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.
```

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。

**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 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 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 PortChannel0/0 です。これは IPS SSP の管理インターフェイスに相当します。

**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 に割り当てられているのと同じ 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、ゲートウェイの 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、ローカルのイーサネット 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** コマンドをすべて大文字で入力していることを確認してください。他の ROMMON コマンドは小文字または大文字で入力できますが、**IMAGE** コマンドは、特にすべて大文字で入力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）　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 ディレクトリにあるイメージには、IMAGE 指定のディレクトリ名もスラッシュも含まれていません。

Windows の例

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

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

（注）　**sync** コマンドを使用すると、これらの設定がブート後も保持されるように NVRAM に設定を保存できます。そうしない場合は、ROMMON からイメージをブートするたびにこの情報を入力する必要があります。

**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 イメージの破損を防ぐため、システム イメージのインストール中は IPS SSP の電源を切らないでください。

**（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 の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 パーティションの復旧手順については、「アプリケーション パーティションの復旧」（P.20-10）を参照してください。
- IPS ソフトウェアの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.19-2）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

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。これにより、センサー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場合の準備ができます。

**（注）**　リカバリ パーティション イメージはメジャーおよびマイナー アップデートのために生成されます。サービス パックまたはシグニチャ アップデートのために生成されるという状況はごくまれにしかありません。

センサーのリカバリ 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**　リカバリ パーティション イメージ ファイル（IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg など）を、センサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバに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付加されます。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ファイル名と一致する必要があります。一致しないと、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。

```
ips-ssp# 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。

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

ips-ssp(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。アップグレードの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。アプリケーション パーティションは、このアップグレードでは変更されません。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。次のような構成になっています。

- 「アプリケーション パーティションについて」（P.20-10）
- 「IPS SSP アプリケーション パーティション イメージの復旧」（P.20-11）

## 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は、復旧することができます。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、復旧の実行後、ネットワークにアクセスできます。

**recover application-partition** コマンドを使用してリカバリ パーティションをブートすると、センサー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 または SSH 接続によって実行できるので、リモートの場所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.20-9）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**　リカバリ パーティション イメージ ファイル（IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg など）を、センサーからアクセスできる FTP、HTTP、または HTTPS サーバに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。

```
ips-ssp# 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、センサーがすでに 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。

```
ips-ssp(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。

**recover** コマンドを実行すると、すぐにシャットダウンが開始されます。シャットダウンには少し時間がかかることがあり、この間にも CLI にアクセスできますが、アクセスは警告なしに終了されます。

アプリケーション パーティションのイメージは、リカバリ パーティションに保存されているイメージを使用して再作成されます。ここで、**setup** コマンドを使用してセンサー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、時間帯、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になっているので、センサーを初期化するまで Telnet は使用できません。

### 詳細情報

- **setup** コマンドを使用して IPS SSP を初期化する手順については、第 3 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.20-9）を参照してください。