



## CHAPTER 23

# システム イメージのアップグレード、ダウングレード、およびインストール

この章では、システム イメージをアップグレード、ダウングレード、および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。

- 「アップグレード、ダウングレード、およびシステム イメージ」 (P.23-1)
- 「サポートされる FTP および HTTP/HTTPS サーバ」 (P.23-2)
- 「センサーのアップグレード」 (P.23-2)
- 「自動アップグレードの設定」 (P.23-6)
- 「センサーのダウングレード」 (P.23-12)
- 「アプリケーションパーティションの復旧」 (P.23-12)
- 「システム イメージのインストール」 (P.23-14)

## アップグレード、ダウングレード、およびシステム イメージ

センサーのソフトウェアをアップグレードおよびダウングレードできます。アップグレードでは、サービス パック、シグニチャ アップデート、シグニチャ エンジン アップデート、マイナー バージョン、メジャー バージョン、またはリカバリ パーティション ファイルが適用されます。ダウングレードでは、最後に適用されたサービス パックまたはシグニチャ アップデートがセンサーから削除されます。



注意

**downgrade** コマンドを使用して、以前のメジャーまたはマイナー バージョンに戻すことはできません (Cisco IPS 7.0 から 6.2 など)。**downgrade** コマンドでできることは、最新のシグニチャ アップデートまたはシグニチャ エンジン アップデートからのダウングレードだけです。6.2 に戻すには、センサーのイメージを再作成する必要があります。

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。**recover** コマンドを使用すると、ホストの設定を維持しながら、その他の設定を出荷時の初期状態に戻すことができます。

新しいシステム イメージをセンサーにインストールするには、プラットフォームに応じて、ROMMON、ブートローダ ファイル、またはメンテナンス パーティションを使用します。

新しいシステム イメージをセンサーにインストールすると、すべてのアカウントは削除され、デフォルトの **cisco** アカウントはデフォルト パスワード **cisco** を使用するようにリセットされます。システム イメージをインストールした後、センサーを再初期化する必要があります。

センサーのイメージを再作成し、初期化した後、センサーを最新のサービス パック、シグニチャアップデート、シグニチャ エンジン アップデート、マイナー アップデート、メジャー アップデート、およびリカバリ パーティション ファイルでアップグレードします。

#### 詳細情報

- センサーを初期化する手順については、「[センサーの基本的なセットアップ](#)」(P.3-4) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) 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

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。

- CMS - Apache Server (Tomcat)
- CMS - Apache Server (JRun)

#### 詳細情報

- Cisco.com から IPS ソフトウェア アップデート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.22-1) を参照してください。
- 自動アップデートを設定する手順については、「[自動アップグレードの設定](#)」(P.23-6) を参照してください。

## センサーのアップグレード

ここでは、**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について説明します。次の項目について説明します。

- 「[IPS 7.0\(4\)E4 アップグレード ファイル](#)」(P.23-3)
- 「[upgrade コマンドおよびオプション](#)」(P.23-3)
- 「[upgrade コマンドの使用法](#)」(P.23-4)
- 「[リカバリ パーティションのアップグレード](#)」(P.23-5)

## IPS 7.0(4)E4 アップグレード ファイル

次のファイルは、Cisco IPS 7.0(4)E4 の一部です。

- Readme
  - IPS-7.0-4-E4.readme.txt
- メジャー バージョン アップグレード ファイル
  - IPS-K9-7.0-4-E4.pkg
  - IPS-AIM-K9-7.0-4-E4.pkg
  - IPS-NME-K9-7.0-4-E4.pkg
- システム イメージ ファイル
  - IPS 4240-K9-sys-1.1-a-7.0-4-E4.img
  - IPS 4255-K9-sys-1.1-a-7.0-4-E4.img
  - IPS 4260-K9-sys-1.1-a-7.0-4-E4.img
  - IPS-4270\_20-K9-sys-1.1-a-7.0-4-E4.img
  - IPS-IDSM2-K9-sys-1.1-a-7.0-4-E4.bin.gz
  - IPS-SSM\_10-K9-sys-1.1-a-7.0-4-E4.img
  - IPS-SSM\_20-K9-sys-1.1-a-7.0-4-E4.img
  - IPS-SSM\_40-K9-sys-1.1-a-7.0-4-E4.img
  - IPS-AIM-K9-sys-1.1-a-7.0-4-E4.img
  - IPS-NME-K9-sys-1.1-a-7.0-4-E4.img
- リカバリ イメージ ファイル
  - IPS-K9-r-1.1-a-7.0-4-E4.pkg
  - IPS-AIM-K9-r-1.1-a-7.0-4-E4.pkg
  - IPS-NME-K9-r-1.1-a-7.0-4-E4.pkg

### 詳細情報

これらのファイルを Cisco.com で入手する手順については、「[Cisco IPS ソフトウェアの入手方法](#) (P.22-1) を参照してください。

## upgrade コマンドおよびオプション

**upgrade source-url** コマンドを使用して、サービス パック、シグニチャ アップデート、エンジン アップデート、マイナー バージョン、メジャー バージョン、またはリカバリ パーティション ファイル アップグレードを適用します。

次のオプションが適用されます。

- **source-url** : コピー元のファイルの場所。
  - **ftp** : FTP ネットワーク サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。  
ftp://[username@] location[/relativeDirectory]/filename  
ftp://[username@]location[/absoluteDirectory]/filename



(注) パスワードを入力するように求められます。

- scp: : SCP ネットワーク サーバのコピー元 URL。このプレフィックスの構文は、次のとおりです。

```
scp:[//[username@] location]/relativeDirectory]/filename
```

```
scp:[//[username@] location]//absoluteDirectory]/filename
```



(注) パスワードを入力するように求められます。

- http: : Web サーバのコピー元 URL。このプレフィックスの構文は、次のとおりです。

```
http:[//[username@] location]/directory] filename
```



(注) ディレクトリは、目的のファイルの絶対パスで指定する必要があります。

- https: : Web サーバのコピー元 URL。このプレフィックスの構文は、次のとおりです。

```
https:[//[username@] location]/directory] filename
```



(注) ディレクトリは、目的のファイルの絶対パスで指定する必要があります。

## upgrade コマンドの使用方法



### 注意

ソフトウェアをダウンロードするには、暗号化特権を持つアカウントを使用して、Cisco.com にログインする必要があります。初めて Cisco.com でソフトウェアをダウンロードするときに、暗号化特権を持つアカウントを設定する方法が表示されます。



### 注意

ファイル名は変更しないでください。センサーがアップデートを受け入れるには、元のファイル名が維持されている必要があります。



### 注意

手動アップグレードで AIM IPS または NME IPS をアップグレードするときは、アップグレードをインストールする前に、ルータのハートビートリセットをディセーブルにする必要があります。アップグレードが完了した後、ハートビートリセットを再度イネーブル化できます。ハートビートリセットをディセーブルにしないと、アップグレードが失敗して AIM IPS または NME IPS が不明な状態になることがあり、この場合、回復にはシステムのイメージの再作成が必要になります。

センサーをアップグレードするには、次の手順に従います。

- ステップ 1** センサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバに、該当するファイル (IPS-K9-7.0-4-E4.pkg など) 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
```

**ステップ 4** センサーをアップグレードします。

```
sensor(config)# upgrade url/IPS-K9-7.0-4-E4.pkg
```

URL は、アップデート ファイルがある場所を指します。たとえば、FTP を使用してアップデートを取得するには、次のように入力します。

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-K9-7.0-4-E4.pkg
```

**ステップ 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: *****
```

**ステップ 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 パックのインストールを完了するには、IPS プロセスの再起動、またはセンサーのリブートが必要になることがあります。



(注) オペレーティング システムのイメージが再作成され、サービス アカウントによってセンサーに作成されたすべてのファイルが削除されます。

### 詳細情報

- センサーをアップグレードする IDM の手順については、「[Manually Updating the Sensor](#)」を参照してください。IME の手順については、「[Manually Updating the Sensor](#)」を参照してください。
- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「[サポートされる FTP および HTTP/HTTPS サーバ](#)」(P.23-2) を参照してください。
- Cisco.com でソフトウェアを検索し、暗号化特権を持つアカウントを取得する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) を参照してください。
- AIM IPS でハートビート リセットをディセーブルにする手順については、「[Disabling and Enabling Heartbeat Reset](#)」を参照してください。NME IPS の場合は「[Disabling and Enabling Heartbeat Reset](#)」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



(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 アップデートの場合に生成され、サービス パックまたはシグニチャ アップデートでは、非常にまれなケースでのみ生成されます。



(注) AIM IPS および NME IPS には、リカバリ パーティションのアップグレードに使用する独自のリカバリ イメージがあります。

```
AIM IPS : IPS-AIM-K9-r-1.1-a-7.0-4-E4.pkg
```

```
NME IPS : IPS-NME-K9-r-1.1-a-7.0-4-E4.pkg
```

センサー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て、**upgrade** コマンドを使用して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しておきます。

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、次の手順に従います。

**ステップ 1** センサーからアクセスできる FTP、SCP、HTTP、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 (IPS-K9-r-1.1-a-7.0-1-E2.pkg) をダウンロードします。



#### 注意

ブラウザによっては、ファイル名に拡張子が追加されます。保存する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。一致しない場合、このファイルでリカバリパーティションをアップグレードできません。

**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-K9-r-1.1-a-7.0-1-E2.pkg
```

```
sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-7.0-1-E2.pkg
```

**ステップ 5** サーバの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の再作成だけが行われます。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で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。

#### 詳細情報

- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「サポートされる FTP および HTTP/HTTPS サーバ」(P.23-2) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」(P.22-1) を参照してください。
- recover** コマンドの使用手順については、「**recover** コマンドの使用法」(P.23-13) を参照してください。

## 自動アップグレードの設定

ここでは、アップグレードディレクトリで自動的にアップグレードを検索するように、センサーを設定する方法について説明します。次の項目について説明します。

- 「自動アップグレード」(P.23-7)
- 「auto-upgrade コマンドおよびオプション」(P.23-7)

- 「[auto-upgrade コマンドの使用法](#)」 (P.23-8)
- 「[自動アップグレードの例](#)」 (P.23-11)

## 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、複数のセンサーが同じリモート FTP サーバのディレクトリを異なるアップデートスケジュール (24 時間おき、月、水、金曜日の午後 11:00 など) で指すようにできます。

自動アップグレードをスケジュール設定するには、次の情報を指定します。

- サーバの 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のディレクトリパス
- ファイルコピーのプロトコル (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

あらかじめソフトウェアアップグレードを [Cisco.com](#) からダウンロードし、アップグレードディレクトリにコピーし、センサーが自動アップグレードの目的でポーリングできるようにしておく必要があります。

### 詳細情報

[Cisco.com](#) でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」 (P.22-1) を参照してください。

## auto-upgrade コマンドおよびオプション

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。

次のオプションが適用されます。

- **cisco-server** : [Cisco.com](#) からの自動シグニチャアップデートおよびエンジンアップデートをイネーブルにします。
- **cisco-url** : Cisco サーバロケータサービス。  
www.cisco.com の IP アドレスが変更されない限り、変更する必要はありません。
- **default** : システムのデフォルト設定に値を設定します。
- **directory** : ファイルサーバでアップグレードファイルがあるディレクトリ。  
絶対パスで指定する場合は、先頭に「/」を付けます。
- **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ときに使用す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、センサーがサーバと SSH で通信できるように、**ssh host-key** コマンドを使用してサーバを SSH 既知ホストリストに追加する必要があります。

- **ip-address** : ファイルサーバの IP アドレス。
- **password** : Cisco サーバ認証に使用するユーザパスワード。

- **schedule-option** : Cisco サーバで自動アップグレードを実行するスケジュール。カレンダー スケジュールでは、指定された曜日の指定された時刻にアップグレードが開始されます。定期スケジュールでは、指定された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を実行する曜日と時刻を設定します。
  - **days-of-week** : 自動アップグレードを実行する曜日。複数の曜日を選択できます。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を開始する時刻。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発生する時刻と、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（時間単位）です。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** : サーバ認証に使用するユーザ名。
- **user-server** : ユーザ定義のサーバからの自動アップグレードをイネーブルにします。

#### 詳細情報

SCP サーバを SSH 既知ホスト リストに追加する CLI の手順については、「SSH の既知ホスト リストへのホストの追加」(P.4-49) を参照してください。

## auto-upgrade コマンドの使用方法



(注)

自動アップデートの設定中に、認証不可というエラー メッセージが表示される場合は、センサーと Cisco.com との間にあるファイアウォールで正しいポートが開かれていることを確認してください。たとえば、www.cisco.com への自動アップデートの初期接続には 198.133.219.25 ポート 443 が必要です。選択したパッケージを Cisco ファイル サーバからダウンロードするには 198.133.219.243 ポート 80 が必要です。Cisco ファイル サーバの IP アドレスは変更される可能性があります。 **show statistics host** コマンドの出力の lastDownloadAttempt セクションで確認できます。



(注)

最後の自動アップデートのステータス、または次にスケジュールされている自動アップデートを確認するには、**show statistics host** コマンドを実行し、Auto Update Statistics セクションを確認します。

自動アップグレードをスケジューリングするには、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 CLI にログインします。

**ステップ 2** 自動アップグレード サブモードを開始します。

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

**ステップ 3** センサーが Cisco.com または独自のファイル サーバで新しいアップグレードを定期的に検索するように設定します。

a. Cisco.com の場合は、次のようにします。



```
sensor(config-hos-aut)# cisco-server enabled
```

ステップ 4 に進みます。

- b. 独自のサーバの場合は、次のようにします。

```
sensor(config-hos-aut)# user-server enabled
```

- c. ファイルサーバの IP アドレスを指定します。

```
sensor(config-hos-ena)# ip-address 10.1.1.1
```

- d. ファイルサーバでアップグレードファイルがあるディレクトリを指定します。

```
sensor(config-hos-ena)# directory /tftpboot/sensor_updates
```

- e. ファイルサーバのプロトコルを指定します。

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



(注) SCP を使用する場合は、センサーがサーバと SSH で通信できるように、**ssh host-key** コマンドを使用してサーバを SSH 既知ホストリストに追加する必要があります。

- ステップ 4** 認証用のユーザ名を指定します。

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

- ステップ 5** このユーザのパスワードを指定します。

```
sensor(config-hos-ena)# password  
Enter password[:] : *****  
Re-enter password: *****
```

- ステップ 6** スケジュールを指定します。

- a. カレンダー スケジュールの場合は、指定された曜日の指定された時刻にアップグレードが開始されます。

```
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
```

- b. 定期スケジュールの場合は、指定された間隔でアップグレードが開始されます。

```
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
```

- ステップ 7** 設定を確認できます。

```
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/6.1_dummy_updates
```

```
user-name: tester
password: <hidden>
file-copy-protocol: ftp default: scp
-----
sensor(config-hos-ena)#
```

**ステップ 8** 自動アップグレード サブモードを終了します。

```
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:[yes]:
```

**ステップ 9** Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

---

### 詳細情報

- センサーを自動的にアップグレードする IDM の手順については、「[Configuring Automatic Update](#)」を参照してください。IME の手順については、「[Configuring Automatic Update](#)」を参照してください。
- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「[サポートされる FTP および HTTP/HTTPS サーバ](#)」(P.23-2) を参照してください。
- SCP サーバを SSH 既知ホスト リストに追加する CLI の手順については、「[SSH の既知ホスト リストへのホストの追加](#)」(P.4-49) を参照してください。
- **show statistics host** コマンドの出力については、「[統計情報の表示](#)」(P.17-24) を参照してください。

## 自動アップグレードの例

表 23-1 に、自動アップグレードの例を示します。これらの例では、1:00 から 1 時間おきにアップグレードが実行されるように設定されています。たとえば、サイクル 1 は 1:00 に、サイクル 2 は 2:00 に、サイクル 3 は 3:00 に開始されます。

表 23-1 自動アップグレードの例

ケース / 現在のバージョン	リモート ディレクトリのファイル	自動アップデートのサイクル / 新しいバージョン
ケース 0 5.1(4) E0 S250	<ul style="list-style-type: none"> <li>IPS-sig-S260-minreq-5.0-6.pkg</li> <li>IPS-engine-E2-req-5.1-4.pkg</li> <li>IPS-sig-S262-req-E2.pkg</li> <li>IPS-sig-S263-req-E2.pkg</li> <li>IPS-engine-E3-req-5.1-4.pkg</li> <li>IPS-sig-S264-req-E3.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-engine-E3-req-5.1-4.pkg をインストール。 新しいバージョンは 5.1(4) E2 S250。</li> <li>サイクル 2 で IPS-sig-S264-req-E3.pkg をインストール。 新しいバージョンは 5.1(4) E2 S264。</li> </ul>
ケース 1 5.1(4) E0 S250	<ul style="list-style-type: none"> <li>IPS-K9-sp-5.1-5.pkg</li> <li>IPS-sig-S260-minreq-5.0-6.pkg</li> <li>IPS-K9-5.1-6-E1.pkg</li> <li>IPS-engine-E2-req-5.1-6.pkg</li> <li>IPS-sig-S262-req-E2.pkg</li> <li>IPS-sig-S263-req-E2.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-K9-5.1-6-E1.pkg をインストール。 新しいバージョンは 5.1(6) E1 S260。</li> <li>サイクル 2 で IPS-engine-E2-req-5.1-6.pkg をインストール。 新しいバージョンは 5.1(6) E2 S260。</li> <li>サイクル 3 で IPS-sig-S263-req-E2.pkg をインストール。 新しいバージョンは 5.1(6) E2 S263。</li> </ul>
ケース 2 5.1(6) E5 S300	<ul style="list-style-type: none"> <li>IPS-K9-6.0-1-E7.pkg</li> <li>IPS-K9-6.0-2-E9.pkg</li> <li>IPS-K9-6.0-3-E11.pkg</li> <li>IPS-engine-E10-req-6.0-2.pkg</li> <li>IPS-engine-E12-req-6.0-3.pkg</li> <li>IPS-sig-S305-req-E12.pkg</li> <li>IPS-sig-S307-req-E12.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-K9-6.0-3-E11.pkg をインストール。 新しいバージョンは 6.0(3) E11 S300。</li> <li>サイクル 2 で IPS-engine-E12-req-6.0-3.pkg をインストール。 新しいバージョンは 6.0(3) E12 S300。</li> <li>サイクル 3 で IPS-sig-S307-req-E12.pkg をインストール。 新しいバージョンは 6.0(3) E12 S307。</li> </ul>
ケース 3 5.1(6) E10 S300	<ul style="list-style-type: none"> <li>IPS-K9-6.0-1-E9.pkg</li> <li>IPS-engine-E11-req-6.0-1.pkg</li> <li>IPS-sig-S305-req-E11.pkg</li> <li>IPS-sig-S307-req-E11.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 では、E9 が E10 よりも低いいため、何もインストールされない。</li> </ul>
ケース 4 5.1(6) E10 S300	<ul style="list-style-type: none"> <li>IPS-engine-E11-req-5.1-6.pkg</li> <li>IPS-sig-S301-req-E10.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-engine-E11-req-5.1-6.pkg をインストール。 新しいバージョンは 5.1(6) E11 S300。</li> </ul>
ケース 5 5.1(6) E10 S300	<ul style="list-style-type: none"> <li>IPS-sig-S301-req-E10.pkg</li> <li>IPS-sig-S302-req-E11.pkg</li> <li>IPS-sig-S303-req-E12.pkg</li> <li>IPS-engine-E11-req-5.1-6.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-engine-E11-req-5.1-6.pkg をインストール。 新しいバージョンは 5.1(6) E11 S300。</li> <li>サイクル 2 で IPS-sig-S302-req-E11.pkg をインストール。 新しいバージョンは 5.1(6) E11 S302。</li> </ul>

表 23-1 自動アップグレードの例 (続き)

ケース/現在のバージョン	リモート ディレクトリのファイル	自動アップデートのサイクル/新しいバージョン
ケース 6 6.0(3)E1 S300 (IPS 4270-20)	<ul style="list-style-type: none"> <li>IPS-K9-6.0-4-E1.pkg</li> <li>IPS-4270_20-K9-6.0-4-E1.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-4270_20-K9-6.0-4-E1.pkg をインストール</li> <li>新しいバージョンは 6.0(4)E1 S310</li> </ul>
ケース 7 6.0(4)E3 S330 (AIM IPS)	<ul style="list-style-type: none"> <li>IPS-K9-6.0-5-E3.pkg</li> <li>IPS-AIM-K9-6.0-5-E3.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-AIM-K9-6.0-5-E3.pkg をインストール。</li> <li>新しいバージョンは 6.0(5)E3 S335。</li> </ul>
ケース 8 6.0(5)E5 S330 (AIM IPS)	<ul style="list-style-type: none"> <li>IPS-K9-7.0-1-E5.pkg</li> <li>IPS-AIM-K9-7.0-1-E5.pkg</li> </ul>	<ul style="list-style-type: none"> <li>サイクル 1 で IPS-K9-7.0-1-E5.pkg をインストール。</li> <li>新しいバージョンは 7.0(1)E5 S377</li> </ul>

## センサーのダウングレード



### 注意

**downgrade** コマンドを使用して、以前のメジャーまたはマイナー バージョンに戻すことはできません (Cisco IPS 7.0 から 6.2 など)。**downgrade** コマンドでできることは、最新のシグニチャ アップデートまたはシグニチャ エンジン アップデートからのダウングレードだけです。6.2 に戻すには、センサーのイメージを再作成する必要があります。

最後に適用されたシグニチャ アップグレードまたはシグニチャ エンジン アップグレードをセンサーから削除するには、**downgrade** コマンドを使用します。

最後に適用されたシグニチャ アップデートまたはシグニチャ エンジン アップデートをセンサーから削除するには、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次のようにセンサーにログインします。

**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** 最近適用されたサービス パックまたはシグニチャ アップデートがない場合、**downgrade** コマンドは使用できません。

```
sensor(config)# downgrade
No downgrade available.
sensor(config)#
```

## 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。内容は次のとおりです。

- 「アプリケーションパーティション」 (P.23-13)
- 「recover コマンドの使用法」 (P.23-13)

## アプリケーションパーティション

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は保持され、復旧の実行後に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でブートして、センサーのアプリケーションパーティションを自動的に復旧するには、**recover application-partition** コマンドを使用します。**recover application-partition** コマンドは Telnet または SSH 接続から実行できるため、離れた場所にインストールされているセンサーを復旧するときに、このコマンドを使用することを推奨します。



(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。



(注) リカバリ後にセンサーに再接続するときは、デフォルトユーザ名とパスワード **cisco** を使用して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.23-5) を参照してください。

## recover コマンドの使用方法

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、HTTP、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 (IPS-K9-r-1.1-a-7.0-4-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 IPS 7.0(1) が実行され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 6.2(1)E3. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

- ステップ 5** **yes** と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ります。その間も CLI にアクセスすることはできますが、警告なしにアクセスが終了します。

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、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となっているため、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

- TFTP サーバの詳細については、「[TFTP サーバ](#)」(P.23-15) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) を参照してください。
- **setup** コマンドを使用してセンサーを初期化する手順については、「[センサーの基本的なセットアップ](#)」(P.3-4) を参照してください。

## システムイメージのインストール

ここでは、システムイメージをアプライアンスおよびモジュールにインストールする手順について説明します。次の項目について説明します。

- 「[ROMMON について](#)」(P.23-15)
- 「[TFTP サーバ](#)」(P.23-15)
- 「[ターミナルサーバへのアプライアンスの接続](#)」(P.23-15)
- 「[IPS 4240 および IPS 4255 システムイメージのインストール](#)」(P.23-16)
- 「[IPS 4260 システムイメージのインストール](#)」(P.23-19)
- 「[IPS 4270-20 システムイメージのインストール](#)」(P.23-21)
- 「[AIM IPS システムイメージのインストール](#)」(P.23-24)
- 「[AIP SSM システムイメージのインストール](#)」(P.23-26)
- 「[IDSM2 システムイメージのインストール](#)」(P.23-29)
- 「[NME IPS システムイメージのインストール](#)」(P.23-41)



#### 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。

#### 詳細情報

**recover application-partition** コマンドの使用手順については、「[アプリケーションパーティションの復旧](#)」(P.23-12) を参照してください。

## ROMMON について

一部の Cisco センサーには ROMMON というプリブート CLI があり、プライマリ デバイスのイメージが欠落または破損していたり、通常のアプリケーションをブートできない場合に、センサーのイメージをブートできます。シリアル コンソール ポートを使用できれば、ROMMON は特にリモート センサーの復旧に役立ちます。

ROMMON へのアクセスは、シリアル コンソール ポート（センサー シャーシの RJ-45F コネクタで利用できる Cisco 標準非同期 RS-232C DTE）からのみ可能です。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、「[ターミナル サーバへのアプライアンスの接続](#)」(P.23-15) 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 リカバリなどネットワークの問題に対応していません。限定的なパケット整合性チェックは実装されているため、パケットの整合性値が正しく、順番に到着する場合は、エラーの可能性がほとんどありません。しかし、TFTP はパイプライン処理を提供しないため、転送時間の合計は、転送されるパケット数にネットワークの平均 RTT を掛けた値になります。このような制限があるため、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、信頼性の高いイメージの配送ができます。一部の TFTP サーバでは、転送可能な最大ファイル サイズが 32 MB までに制限されていることがあるため注意してください。

## ターミナル サーバへのアプライアンスの接続

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 4240 および IPS 4255 システムイメージのインストール

**(注)**

この手順は IPS 4240 用ですが、IPS 4255 にも適用されます。IPS 4255 システムイメージは、ファイル名に「4255」が含まれています。

アプライアンスで ROMMON を使用して、システムイメージをコンパクトフラッシュデバイスに TFTP でダウンロードすることにより、IPS 4240 および IPS 4255 システムイメージをインストールできます。

IPS 4240 および IPS 4255 システムイメージをインストールするには、次の手順に従います。

**ステップ 1** IPS 4240 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 4240 システムイメージファイル (IPS 4240-K9-sys-1.1-a-7.0-4-E4.img) をダウンロードします。



**(注)** IPS 4240 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 4240 をブートします。

```
Booting system, please wait...
```

```
CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90
```

```
Low Memory: 631 KB
High Memory: 2048 MB
PCI Device Table.
Bus Dev Func Vendid DevID Class          Irq
00 00 00 8086 2578 Host Bridge
00 01 00 8086 2579 PCI-to-PCI Bridge
00 03 00 8086 257B PCI-to-PCI Bridge
```



```

00 1C 00 8086 25AE PCI-to-PCI Bridge
00 1D 00 8086 25A9 Serial Bus 11
00 1D 01 8086 25AA Serial Bus 10
00 1D 04 8086 25AB System
00 1D 05 8086 25AC IRQ Controller
00 1D 07 8086 25AD Serial Bus 9
00 1E 00 8086 244E PCI-to-PCI Bridge
00 1F 00 8086 25A1 ISA Bridge
00 1F 02 8086 25A3 IDE Controller 11
00 1F 03 8086 25A4 Serial Bus 5
00 1F 05 8086 25A6 Audio 5
02 01 00 8086 1075 Ethernet 11
03 01 00 177D 0003 Encrypt/Decrypt 9
03 02 00 8086 1079 Ethernet 9
03 02 01 8086 1079 Ethernet 9
03 03 00 8086 1079 Ethernet 9
03 03 01 8086 1079 Ethernet 9
04 02 00 8086 1209 Ethernet 11
04 03 00 8086 1209 Ethernet 5

```

```

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

```

```
Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004
```

```

Platform IPS 4240-K9
Management0/0

```

```
MAC Address: 0000.c0ff.ee01
```

**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** を押して、ブートを中断します。スペースバーを押すと、すぐにブートが開始します。



**(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.

```

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> 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=

```

変数の定義は次のとおりです。

- Address : IPS 4240 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 4240 が使用するゲートウェイ IP アドレス
- Port : IPS 4240 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 (untagged のままにしておきます)
- Image : システムイメージのファイル名とパス名
- Config : このプラットフォームでは使用しません



(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。



(注) TFTP ダウンロードに使用されるデフォルト インターフェイスは Management0/0 です。これは、IPS 4240 の MGMT インターフェイスに対応します。

```
rommon> PORT=interface_name
```

**ステップ 6** 必要に応じて、IPS 4240 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 4240 に割り当てられているものと同じ IP アドレスを使用してください。

**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、すべて大文字で入力する必要があります。他の ROMMON コマンドは、小文字でも大文字でも入力できますが、**IMAGE** コマンドは特別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_4240-K9-sys-1.1-a-7.0-4-E4.img
```



(注) パスは、UNIX TFTP サーバのデフォルトの tftpboot ディレクトリからの相対パスです。イメージがデフォルトの tftpboot ディレクトリにある場合、IMAGE 指定でディレクトリ名またはスラッシュは付きません。

Windows の例

```
rommon> IMAGE=Ysystem_imagesYIPS 4240-K9-sys-1.1-a-7.0-4-E4.img
```

**ステップ 11** **set** と入力して Enter を押し、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、後からブート時に使用できます。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インストール中は IPS 4240 の電源を切らないでください。電源を切ると、システムイメージが破損する場合があります。



**(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 4240 にダウンロードし、ブートします。必ず IPS 4240 のイメージを使用してください。

### 詳細情報

- TFTP サーバの詳細については、「[TFTP サーバ](#)」(P.23-15) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) を参照してください。

## IPS 4260 システムイメージのインストール

アプライアンスで ROMMON を使用して、システムイメージをフラッシュ デバイスに TFTP でダウンロードすることにより、IPS 4260 システムイメージをインストールできます。

IPS 4260 システムイメージをインストールするには、次の手順に従います。

**ステップ 1** IPS 4260 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 4260 システムイメージファイル (IPS 4260-K9-sys-1.1-a-7.0-4-E4.img) をダウンロードします。

IPS 4260 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 4260 をブートします。

**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 Ctrl キーを押した状態で R キーを押します。

```
Evaluating Run Options...
```



**(注)** Ctrl+R は 5 秒以内に押してください。

```
Assuming IPS 4260-K9 Platform
 2 Ethernet Interfaces detected
```

```
Cisco Systems ROMMON Version (1.0(11)1c) #26: Mon Mar 13 18:05:54 CST 2006
```

```
Platform IPS 4260-K9
Management0/0
Link is UP
MAC Address: 0004.23cc.6047
```

```
Use ? for help.
rommon #0>
```

**ステップ 4** 必要に応じて、TFTP ダウンロードに使用するポートを変更します。

```
rommon #1> interface name
```

使用中のポートがプラットフォーム ID の直後に示されます。この例では、ポート Management0/0 が使用されています。



**(注)** TFTP ダウンロードに使用されるデフォルトポートは Management0/0 です。これは、IPS 4260 のコマンド/コントロール (MGMT) インターフェイスに対応します。



**(注)** ポート Management0/0 (MGMT) および GigabitEthernet0/1 (GE 0/1) は、シャーシの背面でラベルによって示されています。

**ステップ 5** IPS 4260 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 4260 に割り当てられているものと同じ IP アドレスを使用してください。

**ステップ 6** TFTP サーバの IP アドレスを指定します。

```
rommon> server ip_address
```

**ステップ 7** ゲートウェイの IP アドレスを指定します。

```
rommon> gateway ip_address
```

**ステップ 8** 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 9** 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指定します。

```
rommon> file path/filename
```

UNIX の例

```
rommon> file /system_images/IPS 4260-K9-sys-1.1-a-7.0-4-E4.img
```



(注) パスは、UNIX TFTP サーバのデフォルトの `tftpboot` ディレクトリからの相対パスです。イメージがデフォルトの `tftpboot` ディレクトリにある場合、ファイルの場所にディレクトリ名またはスラッシュは付きません。

Windows の例

```
rommon> file <tftpboot_directory>IPS 4260-K9-sys-1.1-a-7.0-4-E4.img
```

**ステップ 10** 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) イメージの再作成プロセスの途中で、IPS 4260 は 1 回リポートします。アップデートプロセスの間は IPS 4260 の電源を切らないでください。電源を切ると、アップグレードが破損する場合があります。

#### 詳細情報

- TFTP サーバの詳細については、「[TFTP サーバ](#)」(P.23-15) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) を参照してください。

## IPS 4270-20 システムイメージのインストール

アプライアンスで ROMMON を使用して、システムイメージをコンパクトフラッシュ デバイスに TFTP でダウンロードすることにより、IPS 4270-20 システムイメージをインストールできます。

IPS 4270-20 システムイメージをインストールするには、次の手順に従います。

**ステップ 1** IPS 4270-20 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 4270-20 システムイメージファイル (IPS-4270\_20-K9-sys-1.1-a-7.0-4-E4.img) をダウンロードします。



(注) IPS 4270-20 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 4270-20 をブートします。

```
Booting system, please wait...
Cisco Systems ROMMON Version (1.0(12)10) #7: Thu Jun 21 13:50:04 CDT 2007
```

```
ft_id_update: Invalid ID-PROM Controller Type (0x5df)
```

```
ft_id_update: Defaulting to Controller Type (0x5c2)
```



(注) コントローラ タイプのエラーは既知の問題です。無視してください。

- 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** を押して、ブートを中断します。スペースバーを押すと、すぐにブートが開始します。



**(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.
```

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> 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=2
  RETRY=20
```

変数の定義は次のとおりです。

- **Address** : IPS 4270-20 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 4270-20 が使用するゲートウェイ IP アドレス
- **Port** : IPS 4270-20 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 (untagged のままにしておきます)
- **Image** : システム イメージのファイル名とパス名
- **Config** : このプラットフォームでは使用しません



**(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、IPS 4270-20 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 4270-20 に割り当てられているものと同じ IP アドレスを使用してください。

- ステップ 6** 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 7** 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 8** 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 9** 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
```

UNIX の例

```
rommon> IMAGE=/system_images/IPS-4270_20-K9-sys-1.1-a-7.0-4-E4.img
```



- (注)** パスは、UNIX TFTP サーバのデフォルトの tftpboot ディレクトリからの相対パスです。イメージがデフォルトの tftpboot ディレクトリにある場合、IMAGE 指定でディレクトリ名またはスラッシュは付きません。

Windows の例

```
rommon> IMAGE=¥system_images¥IPS-4270_20-K9-sys-1.1-a-7.0-4-E4.img
```

- ステップ 10** set と入力して Enter を押し、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、後からブート時に使用できます。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 11** 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インストール中は IPS 4270-20 の電源を切らないでください。電源を切ると、システムイメージが破損する場合があります。



- (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 4270-20 にダウンロードし、ブートします。必ず IPS 4270-20 のイメージを使用してください。

**詳細情報**

- TFTP サーバの詳細については、「[TFTP サーバ](#)」(P.23-15) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) を参照してください。

## AIM IPS システム イメージのインストール

AIM IPS システム イメージをインストールするには、次の手順に従います。

- ステップ 1** AIM IPS システム イメージ ファイル (IPS-AIM-K9-sys-1.1-7.0-4-E4.img) をダウンロードし、TFTP サーバに tftp ルート ディレクトリからの相対パスで置きます。



**(注)** AIM IPS が TFTP サーバにアクセスできるように、ネットワークが設定されていることを確認します。

TFTP サーバを使用できない場合は、ルータを TFTP サーバとして動作するように設定します。

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-AIM-K9-sys-1.1-7.0-4-E4.img
router(config)# exit
router#
```

- ステップ 2** ハートビート リセットをディセーブルにします。

```
router# service-module IDS-Sensor 0/slot_number heartbeat-reset disable
```



**(注)** ハートビート リセットをディセーブルにすると、システム イメージのインストール中に (このプロセスに非常に長い時間がかかる場合)、ルータによるモジュールのリセットが防止されます。

- ステップ 3** AIM IPS にセッション接続します。

```
router# service-module IDS-Sensor 0/slot_number session
```



**(注)** AIM IPS スロット番号を判定するには、**show configuration | include interface IDS-Sensor** コマンドを使用します。

- ステップ 4** Shift キーと Ctrl キーを押した状態で 6 を押してから X キーを押して、セッションを一時停止します。

router# プロンプトが表示されます。このプロンプトが表示されない場合は、Ctrl キーを押した状態で 6 を押してから X キーを押してみてください。

- ステップ 5** AIM IPS をリセットします。

```
router# service-module IDS-Sensor 0/slot_number reset
```

**reset** コマンドを確認するように要求されます。

- ステップ 6** Enter キーを押して確認します。

- ステップ 7** Enter を押して、一時停止中のセッションを再開します。

ブートローダのバージョンが表示されてから、次のプロンプトが 15 秒間表示されます。

```
Please enter '***' to change boot configuration:
```

- ステップ 8** この 15 秒の間に \*\*\* と入力します。

ブートローダのプロンプトが表示されます。

- ステップ 9** Enter を押すと AIM IPS とのセッションに戻ります。



**ステップ 10** ブートローダを設定します。

```
ServicesEngine bootloader> config

IP Address [10.89.148.188]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

それぞれのプロンプトで、値を入力するか、Enter を押して、角括弧で囲まれた以前に入力して保存してある値をそのまま適用します。



(注) ゲートウェイ IP アドレスは、IDS センサーのスロット/ポートインターフェイスと一致する必要があります。



(注) **unnumbered** コマンドを使用してモジュール インターフェイスを設定する場合、ゲートウェイ IP アドレスは、**unnumbered** コマンドの一部として使用した他のルータ インターフェイスの IP アドレスにする必要があります。

**注意**

AIM IPS イメージのパス名はフルパスですが、tftp サーバのルート ディレクトリ（一般的には /tftpboot）からの相対的なものにします。

**ステップ 11** ブートローダを起動します。

```
ServicesEngine bootloader> upgrade
```

**ステップ 12** ブートローダの指示に従ってソフトウェアをインストールします（オプション 1 を選択して、ウィザードの指示に従います）。

(注) 次の例では、AIM IPS の IP アドレスが 10.1.9.201 です。イメージ作成プロセスは、IP アドレスが 10.1.9.1 のルータ TFTP サーバから AIM IPS イメージにアクセスします。

**例**

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
11 ***
ServicesEngine boot-loader Version : 1.1.0
ServicesEngine boot-loader > config

IP Address [10.1.9.201]>
Subnet mask [255.255.255.0]>
TFTP server [10.1.9.1]>
Gateway [10.1.9.1]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for AIM IPS
-----
Main menu
```



- 「AIP SSM のイメージの再作成」 (P.23-27)
- 「recover configure/boot コマンドを使用した AIP SSM のイメージの再作成」 (P.23-27)

## AIP SSM のイメージの再作成

AIP SSM のイメージの再作成は、次のいずれかの方法で実行できます。

- ASA から **hw-module module 1 recover configure/boot** コマンドを使用する。
- センサーの CLI から **recover application-partition** コマンドを使用して、アプリケーション イメージを回復する。
- センサーの CLI から **upgrade** コマンドを使用して、リカバリ イメージをアップグレードする。

### 詳細情報

- **hw-module module 1 recover configure/boot** コマンドの使用手順については、「**recover configure/boot コマンドを使用した AIP SSM のイメージの再作成**」 (P.23-27) を参照してください。
- アプリケーション パーティションを回復する手順については、「**アプリケーション パーティションの復旧**」 (P.23-12) を参照してください。
- リカバリ イメージを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.23-5) を参照してください。

## recover configure/boot コマンドを使用した AIP SSM のイメージの再作成

AIP SSM に障害が発生し、モジュール アプリケーション イメージを実行できない場合は、適応型セキュリティ アプライアンスの CLI を使用して、アプリケーション イメージを TFTP サーバからモジュールに転送できます。適応型セキュリティ アプライアンスはモジュール 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 分かかることがあります。

AIP SSM システム イメージをインストールするには、次の手順に従います。

**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** AIP SSM 用のリカバリ設定を行います。

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



(注) リカバリ設定に誤りがあった場合は、**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、設定を修正できます。

**ステップ 4** システムイメージの 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-SSM-K9-sys-1.1-a-7.0-4-E4.img
```

**ステップ 5** AIP SSM 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 AIP SSM 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 ID は 0 のままにします。

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

**ステップ 7** AIP SSM 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** リカバリを実行します。

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

これによって、TFTP サーバから AIP SSM に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、定期的を確認します。



**(注)** リカバリ中はステータスが Recovery で、イメージの再作成が完了すると Up になります。

```
asa# show module 1
```

Mod	Card Type	Model	Serial No.
0	ASA 5540 Adaptive Security Appliance	ASA5540	P2B00000019
1	ASA 5500 Series Security Services Module-20	ASA-SSM-20	P1D000004F4

Mod	MAC Address Range	Hw Version	Fw Version	Sw Version
0	000b.fcf8.7b1c to 000b.fcf8.7b20	0.2	1.0(7)2	7.0(0)82
1	000b.fcf8.011e to 000b.fcf8.011e	0.1	1.0(7)2	5.0(0.22)S129.0

```
Mod Status
```

```
-----
```

```
0 Up Sys
```

```
1 Up
```

```
asa#
```



(注) 出力の **Status** フィールドは AIP SSM の動作ステータスを示します。AIP SSM 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 アプライアンスはアプリケーションイメージを AIP SSM に転送しますが、出力の **Status** フィールドには **Recover** と表示されません。適応型セキュリティ アプライアンスがイメージの転送を完了し、AIP SSM 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) リカバリ プロセスで発生したエラーをデバッグするには、**debug module-boot** コマンドを使用して、システムのイメージの再作成プロセスに関するデバッグをイネーブルにします。

**ステップ 10** AIP SSM にセッション接続し、**setup** コマンドで初期化します。

#### 詳細情報

- TFTP サーバの詳細については、「[TFTP サーバ](#)」(P.23-15) を参照してください。
- AIP SSM を初期化する手順については、「[AIP SSM の高度な設定](#)」(P.3-16) を参照してください。

## IDS M2 システムイメージのインストール

ここでは、IDS M2 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。内容は次のとおりです。

- 「[IDS M2 システムイメージについて](#)」(P.23-29)
- 「[IDS M2 システムイメージのインストール \(Catalyst ソフトウェア\)](#)」(P.23-30)
- 「[IDS M2 システムイメージのインストール \(Cisco IOS ソフトウェア\)](#)」(P.23-31)
- 「[IDS M2 のメンテナンスパーティションの設定 \(Catalyst ソフトウェア\)](#)」(P.23-32)
- 「[IDS M2 のメンテナンスパーティションの設定 \(Cisco IOS ソフトウェア\)](#)」(P.23-36)
- 「[IDS M2 のメンテナンスパーティションのアップグレード \(Catalyst ソフトウェア\)](#)」(P.23-40)
- 「[IDS M2 のメンテナンスパーティションのアップグレード \(Cisco IOS ソフトウェア\)](#)」(P.23-40)

### IDS M2 システムイメージについて

IDS M2 のアプリケーションパーティションが使用できなくなった場合は、メンテナンスパーティションからイメージを再作成することができます。IDS M2 のアプリケーションパーティションのイメージを再作成したら、**setup** コマンドを使用して IDS M2 を初期化する必要があります。

新しいメンテナンスパーティションイメージファイルがある場合は、アプリケーションパーティションからメンテナンスパーティションのイメージを再作成できます。

## IDSМ2 システムイメージのインストール (Catalyst ソフトウェア)

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** IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリに、IDSM2 システムイメージファイル (IPS-IDSМ2-K9-sys-1.1-a-7.0-4-E4.bin.gz) をダウンロードします。

**ステップ 2** スイッチの CLI にログインします。

**ステップ 3** IDSM2 をメンテナンス パーティションでブートします。

```
console> (enable) reset module_number cf:1
```

**ステップ 4** メンテナンス パーティションの CLI にログインします。

```
login: guest
Password: cisco
```



**(注)** IDSM2 のメンテナンス パーティションを設定する必要があります。

**ステップ 5** システムイメージをインストールします。

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/IPS-IDSМ2-K9-sys-1.1-a-7.0-4-E4.bin.gz
```

**ステップ 6** FTP サーバのパスワードを指定します。アプリケーション パーティション ファイルのダウンロードが完了すると、次に進むかどうか尋ねられます。

```
Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing
it [y/n]:
```

**ステップ 7** **y** を入力して続行します。アプリケーション パーティション ファイルのインストールが完了すると、メンテナンス パーティションの CLI に戻ります。

**ステップ 8** メンテナンス パーティションの CLI を終了して、スイッチの CLI に戻ります。

**ステップ 9** IDSM2 をアプリケーション パーティションでリブートします。

```
console> (enable) reset module_number hdd:1
```

**ステップ 10** IDSM2 のリブートが完了したら、ソフトウェアのバージョンをチェックします。

**ステップ 11** アプリケーション パーティションの CLI にログインして、**setup** コマンドを使用して IDSM2 を初期化します。

### 詳細情報

- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「サポートされる FTP および HTTP/HTTPS サーバ」(P.23-2) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」(P.22-1) を参照してください。
- IDMS-2 でメンテナンス パーティションを設定する手順については、「IDSM2 のメンテナンス パーティションの設定 (Catalyst ソフトウェア)」(P.23-32) および「IDSM2 のメンテナンス パーティションの設定 (Cisco IOS ソフトウェア)」(P.23-36) を参照してください。
- setup** コマンドを使用して IDSM2 を初期化する手順については、「IDSM2 の高度な設定」(P.3-20) を参照してください。

## IDSM2 システムイメージのインストール (Cisco IOS ソフトウェア)

システムイメージをインストールするには、次の手順に従います。

**ステップ 1** IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリに、IDSM2 システムイメージファイル (IPS-IDSM2-K9-sys-1.1-a-7.0-4-E4.bin.gz) をダウンロードします。

**ステップ 2** スイッチの CLI にログインします。

**ステップ 3** IDSM2 をメンテナンス パーティションでブートします。

```
router# hw-module module module_number reset cf:1
```

**ステップ 4** メンテナンス パーティションの CLI にセッション接続します。

```
router# session slot slot_number processor 1
```

**ステップ 5** メンテナンス パーティションの CLI にログインします。

```
login: guest  
Password: cisco
```

**ステップ 6** メンテナンス パーティションのインターフェイス IP アドレスを設定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```



**(注)** スイッチの設定に基づいて、IDSM2 管理インターフェイスがある VLAN に適したアドレスを選択します。

**ステップ 7** メンテナンス パーティションのデフォルト ゲートウェイ アドレスを設定します。

```
guest@localhost.localdomain# ip gateway gateway_address
```

**ステップ 8** システムイメージをインストールします。

```
guest@hostname.localdomain# upgrade  
ftp://user@ftp_server_ip_address/directory_path/IPS-IDSM2-K9-sys-1.1-a-7.0-4-E4.bin.gz  
-install
```

**ステップ 9** FTP サーバのパスワードを指定します。アプリケーション パーティション ファイルのダウンロードが完了すると、次に進むかどうか尋ねられます。

```
Upgrading will wipe out the contents on the hard disk.  
Do you want to proceed installing it [y/n]:
```

**ステップ 10** **y** を入力して続行します。アプリケーション パーティション ファイルのインストールが完了すると、メンテナンス パーティションの CLI に戻ります。

**ステップ 11** メンテナンス パーティションの CLI を終了して、スイッチの CLI に戻ります。

**ステップ 12** IDSM2 をアプリケーション パーティションでリブートします。

```
router# hw-module module module_number reset hdd:1
```

**ステップ 13** IDSM2 がオンラインであり、ソフトウェアのバージョンが正しいことと、ステータスが ok であることを確認します。

```
router# show module module_number
```

**ステップ 14** IDSM2 アプリケーション パーティションの CLI にセッション接続します。

```
router# session slot slot_number processor 1
```

**ステップ 15** `setup` コマンドを使用して IDSM2 を初期化します。

#### 詳細情報

- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「サポートされる FTP および HTTP/HTTPS サーバ」(P.23-2) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」(P.22-1) 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を設定する手順については、「IDSM2 のメンテナンスパーティションの設定 (Catalyst ソフトウェア)」(P.23-32) および「IDSM2 のメンテナンスパーティションの設定 (Cisco IOS ソフトウェア)」(P.23-36) を参照してください。
- IDSM2 を初期化する手順については、「IDSM2 の高度な設定」(P.3-20) を参照してください。

## IDSM2 のメンテナンスパーティションの設定 (Catalyst ソフトウェア)

IDSM2 メンテナンスパーティションを設定するには、次の手順に従います。

**ステップ 1** スイッチの CLI にログインします。

**ステップ 2** 特権モードを開始します。

```
console# enable
console(enable)#
```

**ステップ 3** IDSM2 をリロードします。

```
console> (enable) reset module_number cf:1
```

**ステップ 4** IDSM2 にセッション接続します。

```
console# session 9
Trying IDS-9...
Connected to IDS-9.
Escape character is '^]'.
```

```
Cisco Maintenance image
```



**(注)** IDSM2 メンテナンスパーティションには、Telnet または SSH で接続できません。スイッチの CLI からセッション接続する必要があります。

**ステップ 5** ユーザ `guest`、パスワード `cisco` としてログインします。



**(注)** `guest` のパスワードは変更できますが、変更は推奨しません。メンテナンスパーティションのゲストパスワードを忘れ、何らかの理由で IDSM2 のアプリケーションパーティションにログインできなくなると、IDSM2 で RMA が必要になります。

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```



**ステップ 6** IDSM2 のメンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

**ステップ 7** IDSM2 のメンテナンス パーティションのホスト設定 (IP アドレス、ゲートウェイ、ホスト名) をクリアします。

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

**ステップ 8** メンテナンス パーティションのホスト設定を行います。

a. IP アドレスを指定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. デフォルト ゲートウェイを指定します。

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. ホスト名を指定します。

```
guest@localhost.localdomain# ip host hostname
```

**ステップ 9** メンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

**ステップ 10** アプリケーション パーティションにインストールされたイメージを確認します。

```
guest@idsm2.localdomain# show images
Device name      Partition#      Image name
-----
Hard disk(hdd)  1              6.1(1)
guest@idsm2.localdomain#
```

**ステップ 11** メンテナンス パーティションのバージョンを確認します (BIOS のバージョンも含む)。

```

guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM 8 MB, SDRAM 256 MB

guest@idsm2.localdomain#

```

### ステップ 12 アプリケーションパーティションをアップグレードします。

```

guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.2-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.1-1.190-E0.1.bin.gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.gz
(unknown size)
/tmp/upgrade.gz      [!]    28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.gz
is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:

```

### ステップ 13 y と入力し、アップグレードに進みます。

```

Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#

```

### ステップ 14 アップグレードログを表示します。

```

guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/WS-SVC-IDSM2-K9-sys-1.1-a-6.2-1-E3.bin.g
z
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXXXXXX

```

```

Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#

```

#### ステップ 15 アップグレード ログをクリアします。

```

guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully

```

#### ステップ 16 アップグレード ログを表示します。

```

guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#

```

#### ステップ 17 別のコンピュータに ping を実行します。

```

guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#

```

#### ステップ 18 IDSM2 をリセットします。



(注) メンテナンス パーティションから **reset** コマンドを発行するときに、パーティションは指定できません。IDSM2 は、ブート デバイス変数で指定されたパーティションでブートします。ブート デバイス変数がブランクの場合、IDSM2 はアプリケーション パーティションでブートします。

```

guest@idsm2.localdomain# reset
guest@idsm2.localdomain#

```

```
2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in progress. Do
not remove module until shutdown completes
```

```
Broadcast message from root Fri Mar 11 21:55:47 2005...
```

```
The system is going down for system halt NOW !!
console> (enable)#
```

### 詳細情報

サポートされる FTP および HTTP/HTTPS サーバのリストについては、「[サポートされる FTP および HTTP/HTTPS サーバ](#)」(P.23-2) を参照してください。

## IDSM2 のメンテナンス パーティションの設定 (Cisco IOS ソフトウェア)

IDSM2 メンテナンス パーティションを設定するには、次の手順に従います。

**ステップ 1** スイッチの CLI にログインします。

**ステップ 2** IDSM2 にセッション接続します。

```
router# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.111 ... Open
```

```
Cisco Maintenance image
```



**(注)** IDSM2 メンテナンス パーティションには、Telnet または SSH で接続できません。スイッチの CLI からセッション接続する必要があります。

**ステップ 3** ユーザ `guest`、パスワード `cisco` としてログインします。



**(注)** `guest` のパスワードは変更できますが、変更は推奨しません。メンテナンス パーティションのゲストパスワードを忘れ、何らかの理由で IDSM2 のアプリケーションパーティションにログインできなくなると、IDSM2 で RMA が必要になります。

```
login: guest
password: cisco
```

```
Maintenance image version: 2.1(2)
```

```
guest@idsm2.localdomain#
```

**ステップ 4** メンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip
```

```
IP address       : 10.89.149.74
Subnet Mask      : 255.255.255.128
IP Broadcast     : 10.255.255.255
DNS Name         : idsm2.localdomain
Default Gateway  : 10.89.149.126
Nameserver(s)   :
```

```
guest@idsm2.localdomain#
```

**ステップ 5** メンテナンスパーティションのホスト設定（IP アドレス、ゲートウェイ、ホスト名）をクリアします。

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address       : 0.0.0.0
Subnet Mask      : 0.0.0.0
IP Broadcast     : 0.0.0.0
DNS Name         : localhost.localdomain
Default Gateway  : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

**ステップ 6** メンテナンスパーティションのホスト設定を行います。

a. IP アドレスを指定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

b. デフォルトゲートウェイを指定します。

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c. ホスト名を指定します。

```
guest@localhost.localdomain# ip host hostname
```

**ステップ 7** メンテナンスパーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address       : 10.89.149.74
Subnet Mask      : 255.255.255.128
IP Broadcast     : 10.255.255.255
DNS Name         : idsm2.localdomain
Default Gateway  : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

**ステップ 8** アプリケーションパーティションにインストールされたイメージを確認します。

```
guest@idsm2.localdomain# show images
Device name      Partition#      Image name
-----
Hard disk(hdd)  1              6.1(1)
guest@idsm2.localdomain#
```

**ステップ 9** メンテナンスパーティションのバージョンを確認します（BIOS のバージョンも含む）。

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDS2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
```

```
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM 8 MB, SDRAM 256 MB
```

```
guest@idsm2.localdomain#
```

### ステップ 10 アプリケーションパーティションをアップグレードします。

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE IPS-IDSM2-K9-sys-1.1-a-6.2-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/6.1-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img
(unknown size)
/tmp/upgrade.gz          [[]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img is
downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

### ステップ 11 y と入力し、アップグレードに進みます。

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.
```

```
Creating IDS application image file...
```

```
Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

### ステップ 12 アップグレードログを表示します。

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/6.2-1/IPS-IDSM2-K9-sys-1.1-a-6.2-1-E3.img
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
```

```

Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#

```

### ステップ 13 アップグレード ログをクリアします。

```

guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully

```

### ステップ 14 アップグレード ログを表示します。

```

guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#

```

### ステップ 15 別のコンピュータに ping を実行します。

```

guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#

```

### ステップ 16 IDSM2 をリセットします。



**(注)** メンテナンス パーティションから **reset** コマンドを発行するときに、パーティションは指定できません。IDSM2 は、ブート デバイス変数で指定されたパーティションでブートします。ブート デバイス変数がブランクの場合、IDSM2 はアプリケーション パーティションでブートします。

```

guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
Broadcast message from root Fri Mar 11 22:04:53 2005...

The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]
router#

```

### 詳細情報

サポートされる FTP および HTTP/HTTPS サーバのリストについては、「サポートされる FTP および HTTP/HTTPS サーバ」(P.23-2) を参照してください。

## IDSМ2 のメンテナンス パーティションのアップグレード (Catalyst ソフトウェア)

メンテナンス パーティションをアップグレードするには、次の手順に従います。

- 
- ステップ 1** IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリに、IDSM2 のメンテナンス パーティション ファイル (c6svc-mp.2-1-2.bin.gz) をダウンロードします。
- ステップ 2** スイッチから IDSM2 にセッション接続します。  
`console>(enable) session slot_number`
- ステップ 3** IDSM2 の CLI にログインします。
- ステップ 4** コンフィギュレーション モードを開始します。  
`idsm2# configure terminal`
- ステップ 5** メンテナンス パーティションをアップグレードします。  
`idsm2(config)# upgrade`  
`ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz`
- 続行するかどうか尋ねられます。
- ステップ 6** FTP サーバのパスワードを入力します。
- ステップ 7** `y` を入力して続行します。  
 メンテナンス パーティション ファイルがアップグレードされます。
- 

### 詳細情報

- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「[サポートされる FTP および HTTP/HTTPS サーバ](#)」(P.23-2) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「[Cisco IPS ソフトウェアの入手方法](#)」(P.22-1) を参照してください。

## IDSМ2 のメンテナンス パーティションのアップグレード (Cisco IOS ソフトウェア)

メンテナンス パーティションをアップグレードするには、次の手順に従います。

- 
- ステップ 1** IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリに、IDSM2 のメンテナンス パーティション ファイル (c6svc-mp.2-1-2.bin.gz) をダウンロードします。
- ステップ 2** スイッチの CLI にログインします。
- ステップ 3** アプリケーションパーティションの CLI との間にセッションを確立します。  
`router# session slot slot_number processor 1`
- ステップ 4** IDSM2 にログインします。
- ステップ 5** コンフィギュレーション モードを開始します。  
`idsm2# configure terminal`
- ステップ 6** メンテナンス パーティションをアップグレードします。  
`idsm2(config)# upgrade`  
`ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz`



**ステップ 7** FTP サーバのパスワードを指定します。

```
Password: *****
```

続行するかどうか尋ねられます。

```
Continue with upgrade?:
```

**ステップ 8** **yes** と入力して続行します。

#### 詳細情報

- サポートされる FTP および HTTP/HTTPS サーバのリストについては、「サポートされる FTP および HTTP/HTTPS サーバ」(P.23-2) を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」(P.22-1) を参照してください。

## NME IPS システムイメージのインストール



(注)

NME IPS スロット番号を判定するには、**show configuration | include interface ids-sensor** コマンドを使用します。

NME IPS システムイメージをインストールするには、次の手順に従います。

**ステップ 1** NME IPS システムイメージファイル (IPS-NME-K9-sys-1.1-7.0-4-E4.img) をダウンロードし、TFTP サーバに tftp ルート ディレクトリからの相対パスで置きます。



(注) NME IPS が TFTP サーバにアクセスできるように、ネットワークが設定されていることを確認します。

TFTP サーバを使用できない場合は、ルータを TFTP サーバとして動作するように設定します。

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-NME-K9-sys-1.1-7.0-4-E4.img
router(config)# exit
router#
```

**ステップ 2** ハートビートリセットをディセーブルにします。

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```



(注) ハートビートリセットをディセーブルにすると、システムイメージのインストール中に (このプロセスに非常に長い時間がかかる場合)、ルータによるモジュールのリセットが防止されません。

**ステップ 3** NME IPS にセッション接続します。

```
router# service-module ids-sensor 1/0 session
```

**ステップ 4** Shift キーと Ctrl キーを押した状態で 6 を押してから X キーを押して、セッションを一時停止します。router# プロンプトが表示されます。このプロンプトが表示されない場合は、Ctrl キーを押した状態で 6 を押してから X キーを押してみてください。

**ステップ 5** NME IPS をリセットします。reset コマンドを確認するように要求されます。

```
router# service-module ids-sensor 1/0 reset
```

**ステップ 6** Enter キーを押して確認します。

**ステップ 7** Enter を押して、一時停止中のセッションを再開します。ブートローダのバージョンが表示されてから、次のプロンプトが 15 秒間表示されます。

```
Please enter '***' to change boot configuration:
```

**ステップ 8** この 15 秒の間に \*\*\* と入力します。ブートローダのプロンプトが表示されます。

**ステップ 9** Enter を押して NME IPS とのセッションに戻ります。

**ステップ 10** ブートローダを設定します。

```
ServicesEngine bootloader> config
```

```
IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

それぞれのプロンプトで、値を入力するか、Enter を押して、角括弧で囲まれた以前に入力して保存してある値をそのまま適用します。



#### 注意

NME IPS イメージのパス名はフルパスですが、tftp サーバのルートディレクトリ（一般的には /tftpboot）からの相対的なものにします。

**ステップ 11** ブートローダを起動します。

```
ServicesEngine bootloader> upgrade
```

**ステップ 12** ブートローダの指示に従ってソフトウェアをインストールします（オプション 1 を選択して、ウィザードの指示に従います）。

例

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
12 ***
ServicesEngine boot-loader Version : 1.2.0
ServicesEngine boot-loader > config
```

```
IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade
```

```
Cisco Systems, Inc.
Services engine upgrade utility for NM-IPS
-----
Main menu
```



