CHAPTER 12

ソフトウェアの入手方法

この章では、センサー用の Cisco IPS ソフトウェアの入手方法について説明します。この章は、次の項で構成されています。

Cisco IPS ソフトウェアの入手方法

メジャー バージョン アップデート、マイナー バージョン アップデート、シグニチャ アップデート、サービス パック アップデート、システム ファイルおよびリカバリ ファイル、ファームウェア アップグレード、および Readme は、Cisco.com の Downloads にあります。

（注）　Downloads にアクセスするには、Cisco.com にログインする必要があります。

シグニチャ アップデートは、約 1 週間ごとに Cisco.com に掲示されますが、必要な場合は、さらに頻繁に更新されます。サービス パックも、必要に応じて Cisco.com に用意されます。メジャー バージョン アップデートおよびマイナー バージョン アップデートも定期的に掲示されます。

アップデートのダウンロードには、有効な IPS メンテナンス契約と Cisco.com のパスワードが必要です。暗号化アクセス用の Cisco.com アカウントを入手する方法については、P.12-8 の「暗号化アクセスが可能な Cisco.com アカウントの申し込み」を参照してください。

最新の IPS ソフトウェア アップデートがないかどうか、定期的に Cisco.com を確認してください。

（注）　5.x からは、シグニチャ アップデートを適用するためのライセンスが必要になりました。詳細については、P.12-9 の「Cisco.com からのライセンス キーの取得」を参照してください。

Cisco.com の Downloads にアクセスするには、次の手順を実行します。

ステップ 1　Cisco.com に移動します。

ステップ 2　Cisco.com にログインします。

ステップ 3　**Technical Support > Downloads** をクリックします。

ステップ 4　Software Products & Downloads の下にある **Cisco Secure Software** をクリックします。

ステップ 5　Cisco Secure Software の下にある **Cisco Intrusion Detection System (IDS)** をクリックします。

ステップ 6　Downloads ページで対象のセンサーを特定し、Version 5.x の下で該当するソフトウェアのリンク（**Latest Service Pack**、**Minor**、**Major Updates** など）をクリックします。

BIOS のアップグレードの場合は、**Firmware** をクリックします。

ステップ 7　Download ページで必要なファイルをクリックします。

Filename、Release、Date、または Size で並べ替えるには、メニューでオプションを選択して **Go** をクリックします。

（注）　IPS ファイルのバージョン管理方式の説明については、P.12-4 の「IPS ソフトウェア イメージの命名規則」を参照してください。

ステップ 8　Cisco.com 用のユーザ名とパスワードを再入力する必要があります。

（注） Cisco.com からファイルを初めてダウンロードする場合は、先に Encryption Software Export Distribution Authorization フォームに必要事項を入力して **Submit** をクリックしない限り、ソフトウェアをダウンロードできません。

ステップ 9　ダウンロードするファイルをクリックします。

ステップ 10　Readme の説明に従って、更新をインストールします。

ソフトウェアのアップグレードが何らかの理由で失敗し、センサーが使用できない状態になった場合は、必要に応じてシステムを復旧します。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

（注） メジャー バージョン アップグレード、マイナー バージョン アップグレード、サービス パック、リカバリ ファイル、およびシグニチャ アップデートは、すべてのセンサーで同一です。システム イメージ ファイルは、プラットフォームごとに用意されます。

IPS ソフトウェアのバージョン管理

この項では、IPS ソフトウェアのバージョン管理について説明します。取り上げる事項は次のとおりです。

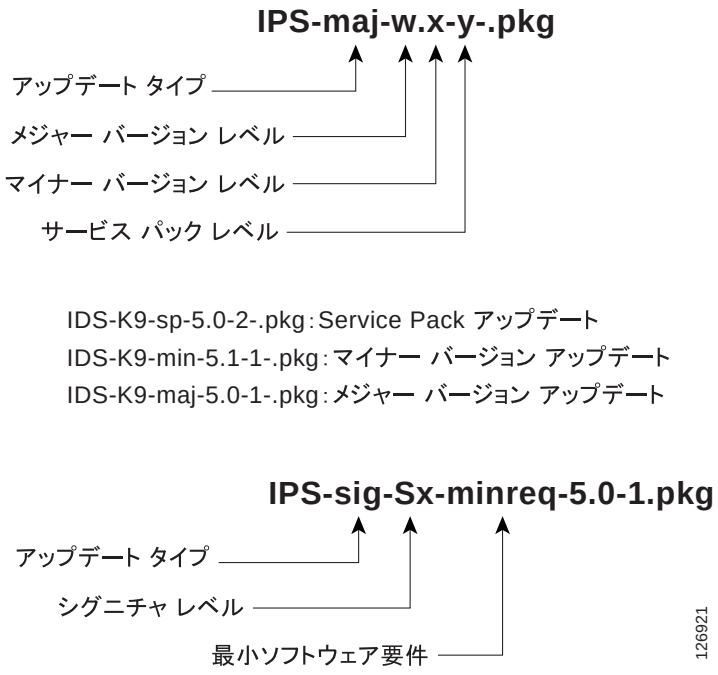
IPS ソフトウェア イメージの命名規則

Cisco.com から IPS ソフトウェア イメージをダウンロードするときは、そのバージョン管理方式を理解して、ファイルがそれぞれ、ベース ファイル、累積ファイル、あるいは差分ファイルのどれであるかを知っておく必要があります。

（注）　**show version** コマンドを使用すると、センサーにインストールされているソフトウェアのバージョンを特定できます。

図 12-1 は、IPS ソフトウェアのファイル名の各部分が何を表すかを示しています。

図 12-1　IPS ソフトウェアのファイル名



メジャー バージョン アップグレードには、製品の新しい機能やアーキテクチャの変更などが含まれます。たとえば、IPS 5.0 ベース バージョン リリースでは、前回のメジャー リリース以降の内容すべて（マイナー バージョンの機能、サービス パックのフィックス、およびシグニチャ アップデート）に加えて、新しい変更が組み込まれます。メジャー アップグレード 5.0(1) には、4.1 が必要です。

（注）　5.0(1) メジャー アップグレードは、4.1 センサーを 5.0(1) にアップグレードする場合にだけ使用します。5.0(1) がすでにインストールされているセンサーに 5.0(1) を再インストールする場合は、メジャー アップグレードではなくシステム イメージまたはリカバリ手順を使用します。

マイナー バージョン アップグレードは、メジャー バージョンに対する差分です。マイナー バージョン アップグレードは、サービス パックのベース バージョンでもあります。5.0 の最初のマイナー バージョン アップグレードは、5.1(1) です。マイナー バージョン アップグレードは、製品のマイナーな拡張を行うためにリリースされます。マイナー バージョン アップグレードには、前回のメジャー バージョン以降に発生したすべてのマイナー機能、サービス パックのフィックス、およびシグニチャ アップデートに加えて、新しいマイナー機能のリリースが組み込まれます。マイナー アップグレードには、メジャー バージョンが必要です。

サービス パックは、ベース バージョンのリリース（マイナーまたはメジャー）の後で、複数のプログラムが累積した形で提供されるものです。サービス パックは、障害フィックスのリリースとして使用され、新しい機能強化は行われません。サービス パックには、前回のベース バージョン（マイナーまたはメジャー）以降に発生したすべてのサービス パックのフィックスに加えて、新しい障害フィックスのリリースが組み込まれます。サービス パックを適用するには、マイナー バージョンが必要です。

シグニチャ アップデートは、新しいリリースにつき 1 つずつ（S145、S146、S147 など）発生する累積および差分です。シグニチャ アップデートには、最初のシグニチャ リリース（S1）以降に発生したすべてのシグニチャに加えて、新しいシグニチャのリリースが組み込まれます。シグニチャ アップデートには、ファイル名にリストされた最小バージョンが必要です。

最新のシグニチャ アップデートをインストールするには、最新のマイナー バージョンが必要です。サービス パックは最新のマイナー バージョンに依存しており、マイナー バージョンは最新のメジャー バージョンに依存しています。

（注）　ファイルのタイプ（ファイル名の例）と対応するソフトウェア リリースのリストについては、P.12-6 の「5.x ソフトウェア リリースの例」を参照してください。

この他に、IDS-4215、IPS-4240、IPS-4255、NM-CIDS、IDSM-2、AIP SSM 10、および AIP ASA 20 のシステム イメージ ファイル、すべてのセンサーのリカバリ パーティション ファイル、および IDSM-2 のメンテナンス パーティション ファイルなども存在します。

- システム イメージ ファイル（IDS-4215、IPS-4240、IPS-4255、NM-CIDS、IDSM-2、AIP ASA 10、および AIP ASA 20）：センサー全体のイメージの再作成に使用される IPS の完全なアプリケーションとリカバリのイメージです。
- リカバリ パーティション イメージ ファイル：リカバリ パーティション イメージ ファイルは、リカバリに使用される IPS の完全なアプリケーション イメージが組み込まれたセンサーのパーティションです。
- メンテナンス パーティション イメージ ファイル（IDSM-2 のみ）：IDSM-2 のメンテナンス パーティションのイメージを再作成するために使用されます。メンテナンス パーティション イメージ ファイルは、新しいバージョン（メジャーまたはマイナー）のメンテナンス パーティションと一緒にリリースされます。メンテナンス パーティション イメージ ファイルは、メンテナンス パーティションのサービス パックの際にはリリースされません。既存のメンテナンス パーティション イメージで特定された障害のフィックスのためにサービス パックがリリースされることはありますが、それ以降にリリースされるサービス パックのために新しいメンテナンス パーティション イメージが作成されることはありません。

（注）　メンテナンス パーティション イメージ ファイルにシグニチャ識別子は含まれていません。

5.x ソフトウェア リリースの例

表 12-1 に、プラットフォームに依存しない IDS 5.x ソフトウェア リリースの例を示します。ファイルの詳細なインストール手順については、ソフトウェア ファイルに添付されている Readme を参照してください。Cisco.com でこれらのファイルにアクセスする方法については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

表 12-1　プラットフォームに依存しないリリースの例

リリース	目標頻度	識別子	サポートされているプラットフォーム	ファイル名の例
シグニチャ　アップデート[1]	毎週	sig	すべて	IPS-sig-S70-minreq-5.0-1.pkg
サービス パック[2]	半年ごとまたは必要に応じて	sp	すべて	IPS-K9-sp-5.0-2.pkg
マイナー バージョン[3]	毎年	min	すべて	IPS-K9-min-5.1-1.pkg
メジャー バージョン[4]	毎年	maj	すべて	IPS-K9-maj-5.0-1.pkg
パッチ リリース[5]	必要に応じて	patch	すべて	IPS-K9-patch-5.0-1pl.pkg
リカバリ パッケージ[6]	毎年または必要に応じて	r	すべて	IPS-K9-r-1.1-a-5.0-1.pkg

1. シグニチャ アップデートには、最新の累積 IPS シグニチャが含まれます。
2. サービス パックには、障害のフィックスが含まれます。
3. マイナー バージョンには、新しい特性や機能（シグニチャ エンジンなど）が含まれます。
4. メジャー バージョンには、新しい機能やアーキテクチャが含まれます。
5. パッチ リリースは暫定的なフィックスです。
6. 同じ基盤アプリケーション イメージを含む新しいリカバリ パッケージをリリースする必要がある場合は、r 1.1 を r 1.2 に変更できます。たとえば、インストーラの障害フィックスがある場合、基盤アプリケーション バージョンがまだ 5.0(1) であっても、リカバリ パーティション イメージは r 1.2 になります。

表 12-2 に、プラットフォームに依存するリリースの例を示します。

表 12-2　プラットフォームに依存するリリースの例

リリース	目標頻度	識別子	サポートされているプラットフォーム	ファイル名の例
システム イメージ[1]	毎年	sys	すべて	IPS-4240-K9-sys-1.1-a-5.0-1.img
メンテナンス パーティション イメージ[2]	毎年	mp	IDSM-2 のみ	c6svc-mp.2-1-2.bin.gz
リカバリ / アップグレード CD	毎年または必要に応じて	cd	CD-ROM ドライブがあるすべてのアプライアンス	—

1. システム イメージには、センサー全体のイメージの再作成に使用される、リカバリとアプリケーションを組み合せたイメージが含まれます。
2. メンテナンス パーティション イメージには、メンテナンス パーティションの完全なイメージが含まれます。これはプラットフォーム固有のファイルです。IDSM-2 をメンテナンス パーティションから復旧する必要がある場合、復旧処理が完了した後で、適用可能な 5.0 バージョンがアプリケーション パーティションに反映されます。

Cisco IPS ソフトウェア 4.1 から 5.x へのアップグレード

（注）　IDSM（WS-X6381）を Cisco IDS 5.x にアップグレードすることはできません。IDSM（WS-X6381）は、Version 5.x をサポートしている IDSM-2（WS-SVC-IDSM2-K9）に置き換える必要があります。

5.1 にアップグレードするために最低限必要なバージョンは 5.0 です。5.0 にアップグレードするために最低限必要なバージョンは 4.1(1) です。Cisco 5.0 から 5.1 へのアップグレードおよび Cisco 4.1 から 5.0 へのアップグレードは、Cisco.com からのダウンロードで入手できます。Cisco.com の Downloads にアクセスする手順については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

5.1 アップグレード ファイルをダウンロードしたら、**upgrade** コマンドを使用して 5.1 アップグレード ファイルをインストールする手順について、添付の Readme を参照してください。または、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading the Sensor」を参照してください。

センサーに Auto Update を設定している場合は、センサーがアップデートの有無をポーリングするサーバ上のディレクトリに 5.1 アップグレード ファイルをコピーします。P.10-2 の「センサーの自動更新」を参照してください。

センサーにアップグレード ファイルをインストールし、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再作成する必要があります。また、Cisco IDS Version 4.1 より前のバージョンからセンサーをアップグレードするには、**recover** コマンドを使用するか、リカバリ / アップグレード CD を使用する必要があります。

センサーのイメージは、次の方法で再作成できます。

- CD-ROM ドライブがある IDS アプライアンスの場合、リカバリ / アップグレード CD を使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Using the Recovery/Upgrade CD」を参照してください。
- すべてのセンサー の場合、**recover** コマンドを使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Recovering the Application Partition」を参照してください。
- IDS-4215、IPS-4240、および IPS 4255 の場合、システム イメージの復元には ROMMON を使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the IDS-4215 System Image」および「Installing the IPS-4240 and IPS-4255 System Image」を参照してください。
- NM-CIDS の場合、ブート ローダーを使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the NM-CIDS System Image」を参照してください。
- IDSM-2 の場合、アプリケーション パーティションのイメージは、メンテナンス パーティションからイメージを再作成します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the IDSM-2 System Image」を参照してください。
- AIP SSM の場合、ASA からのイメージの再作成には、**hw-module module 1 recover configure/boot** コマンドを使用します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Installing the ASA-SSM System Image」を参照してください。

注意　センサーのシステム イメージをインストールすると、アカウントはすべて削除され、デフォルトのアカウントとパスワードが cisco にリセットされます。

暗号化アクセスが可能な Cisco.com アカウントの申し込み

ソフトウェア アップデートをダウンロードするには、暗号化アクセス用の Cisco.com アカウントが必要です。

暗号化アクセスを申し込むには、次の手順を実行します。

ステップ 1　Cisco.com アカウントを持っている場合はステップ 2 に進みます。Cisco.com アカウントを持っていない場合は、次の URL に移動してアカウントを登録します。
http://tools.cisco.com/RPF/register/register.do

ステップ 2　次の URL に移動します。http://www.cisco.com/pcgi-bin/Software/Crypto/crypto_main.pl

Enter Network Password ダイアログボックスが表示されます。

ステップ 3　Cisco.com アカウントでログインします。

Encryption Software Export Distribution Authorization Form ページが表示されます。

ステップ 4　リスト ボックスでソフトウェアを選択して **Submit** をクリックします。

Encryption Software Export Distribution Authorization Form が表示されます。

ステップ 5　Encryption Software Export Distribution Authorization Form を検討し、各項目に入力し、**Submit** をクリックします。

「`Cisco Encryption Software: Crypto Access Granted`」というメッセージが表示されます。

（注）　申し込みの処理には、約 4 時間かかります。受け付け処理が完了するまで、ソフトウェアのダウンロードはできません。完了通知は送信されません。

Cisco.com からのライセンス キーの取得

この項では、Cisco.com からのライセンス キーの取得方法と、CLI または IDM を使用したインストール方法を説明します。取り上げる事項は次のとおりです。

概要

センサーはライセンスなしでも動作しますが、シグニチャ アップデートを取得するには、ライセンスが必要です。ライセンスを入手するには、IPS に関するシスコのサービス契約が必要です。契約を購入するには、代理店、シスコのサービス担当者または営業担当者にお問い合せください。

（注）　ライセンスがない場合でも、5.x の最初のいくつかのシグニチャ アップデートをインストールできます。この作業により、センサーのライセンスを入手する時間ができます。契約内容が不明なためにセンサーのライセンスを入手できない場合は、ライセンスが必要なシグニチャ アップデートをサポートしている 60 日のトライアル ライセンスを入手してください。

IPS の登録ライセンス キーのステータスは、IDM の Licensing パネルで確認できます。Cisco.com のライセンシング サーバから取得したライセンス キーは、センサーに送信されます。または、ローカル ファイルに含まれているライセンス キーからセンサーのライセンス キーをアップデートすることもできます。

ライセンス キーの取得には、IPS デバイスのシリアル番号が必要です。IPS デバイスのシリアル番号は、**Configuration > Licensing** をクリックして IDM で確認することができます。また、CLI で **show version** コマンドを実行して確認することもできます。

IDM を起動するたびに、ダイアログボックスによってライセンスのステータスが表示されます。ライセンス キーのステータスは、trial、invalid、または expired のいずれかです。ライセンス キーがない場合や、無効な場合、または期限が切れている場合でも、IDM を継続して使用できますが、シグニチャ アップデートはダウンロードできません。

ライセンスがインストールされていない場合は、CLI に入ると次のメッセージが表示されます。

```
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a
license.
```

このメッセージは、ライセンスをインストールするまで毎回表示されます。ライセンスを申し込むには、http://www.cisco.com/go/license にアクセスして、IPS Signature Subscription Service をクリックします。

ライセンスのインストール

この項では、IDM または CLI を使用してライセンスをインストールする方法を説明します。取り上げる事項は次のとおりです。

IDM の使用方法

センサーのライセンス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　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Licensing** をクリックします。

Licensing パネルが表示されます。現在のライセンスのステータスに関する情報が表示されます。すでにライセンスがインストールされている場合は、必要に応じて **Download** をクリックしてライセンスを更新します。

ステップ 3　ライセンスを入手する方法を選択します。

a. Cisco.com からライセンスを取得するには、**Cisco Connection Online** を選択します。

IDM は、Cisco.com のライセンス サーバに接続し、サーバにシリアル番号を送信してライセンス キーを取得します。これがデフォルトの方法です。ステップ 4 に進みます。

b. ライセンス ファイルを使用するには、**License File** を選択します。

このオプションを使用するには、www.cisco.com/go/license で、ライセンスを申し込む必要があります。

ライセンスは、電子メールで送られてきます。送られてきたライセンスは、IDM がアクセスできるドライブに保存してください。このオプションは、Cisco.com にアクセスできないコンピュータを使用している場合に役立ちます。

ステップ 7 に進みます。

ステップ 4　**Update License** をクリックします。

Licensing ダイアログボックスが表示されます。

ステップ 5　**Yes** をクリックして続行します。

Status ダイアログボックスには、センサーが Cisco.com に接続しようとしていることが示されます。

Information ダイアログボックスによって、ライセンスがアップデートされたことが示されます。

ステップ 6　**OK** をクリックします。

ステップ 7　www.cisco.com/go/license にアクセスします。

ステップ 8　必須フィールドに入力します。

注意　IPS デバイスの正しいシリアル番号を用意しておく必要があります。これは、その番号のデバイスでだけライセンス キーが機能するからです。

シスコの IPS Signature Subscription Service のライセンス キーは、指定した電子メール アドレスに電子メールで送信されます。

ステップ 9　ライセンス ファイルは、IDM が動作中のクライアントでアクセス可能なハードディスク ドライブまたはネットワーク ドライブに保存します。

ステップ 10 IDM にログインします。

ステップ 11 **Configuration > Licensing** をクリックします。

ステップ 12 Update License で、**Update From: License File** を選択します。

ステップ 13 **Local File Path** フィールドに、ライセンス ファイルへのパスを指定するか、または **Browse Local** をクリックしてファイルを参照します。

Select License File Path ダイアログボックスが表示されます。

ステップ 14 ライセンス ファイルを参照して、**Open** をクリックします。

ステップ 15 **Update License** をクリックします。

CLI の使用方法

copy *source-url license_file_name* **license-key** コマンドを使用して、ライセンス ファイルをセンサーにコピーします。

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。URL またはキーワードです。
- *destination-url*：コピー先のファイルの場所。URL またはキーワードです。
- **license-key**：登録ライセンス ファイル。
- *license_file_name*：受け取るライセンス ファイルの名前。

（注） 新しいライセンス キーを上書きするように古いライセンス キーをインストールすることはできません。

コピー元およびコピー先の URL の正確な形式は、ファイルによって異なります。有効なタイプは次のとおりです。

- ftp:：FTP ネットワーク サーバのコピー元またはコピー先 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
- scp:：SCP ネットワーク サーバのコピー元またはコピー先 URL。このプレフィクスの構文は、次のとおりです。
  scp:[//[username@] location]/relativeDirectory]/filename
  scp:[//[username@] location]//absoluteDirectory]/filename
- http:：Web 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。
  http:[[/[username@]location]/directory]/filename
- https:：Web 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。
  https:[[/[username@]location]/directory]/filename

（注）　FTP または SCP を使用する場合は、パスワードの入力を求められます。

（注）　SCP を使用する場合は、リモート ホストが SSH の既知ホスト リストに含まれている必要があります。手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

（注）　HTTPS を使用する場合、リモート ホストは TLS の信頼できるホストである必要があります。手順については、P.2-17 の「信頼できるホストの追加」を参照してください。

ライセンス キー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　www.cisco.com/go/license で、ライセンス キーを申し込みます。

ステップ 2　必須フィールドに入力します。

（注）　IPS デバイスの正しいシリアル番号を用意しておく必要があります。これは、その番号のデバイスでだけライセンス キーが機能するからです。

シスコの IPS Signature Subscription Service のライセンス キーは、指定した電子メール アドレスに電子メールで送信されます。

ステップ 3　ライセンス キーを Web サーバ、FTP サーバ、または SCP サーバのあるシステムに保存します。

ステップ 4　管理者特権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 5　ライセンス キーをセンサーにコピーします。

```
sensor# copy scp://user@10.89.147.3://tftpboot/dev.lic license-key
Password: *******
```

ステップ 6　センサーのライセンスがあることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R0JS
Licensed, expires: 19-Dec-2005 UTC
Sensor up-time is 2 days.
Using 706699264 out of 3974291456 bytes of available memory (17% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.5M out of 166.8M bytes of available disk space (23%
usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_15_03.00   (QATest)    2005-02-15T12:59:35-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600


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#
```

ステップ 7　センサーからサーバにライセンス キーをコピーして、ライセンスのバックアップ コピーを保存します。

```
sensor# copy license-key scp://user@10.89.147.3://tftpboot/dev.lic
Password: *******
sensor#
```

Cisco Intrusion Prevention Alert Center

Cisco Intrusion Prevention Alert Center を使用すると、発生している脅威に関する情報を表示し、ネットワークを保護するために Cisco ネットワーク IPS シグニチャを使用できます。アクティブな脅威および詳細な情報のリンクのリストが用意されています。また、アクティブなアップデート通知を受信するように登録できます。アクティブなアップデート通知の詳細については、P.12-15 の「Cisco IPS のアクティブなアップデート通知」を参照してください。このサイトから、NSDB を検索することもできます。NSDB の詳細については、P.12-16 の「Network Security Database」を参照してください。

また、役に立つ関連ツールのリンクのリストには、Software Center、Cisco IPS ホームページ、IPS Technical Documentation、Cisco NetPro Forum、および TAC Case Open などが含まれています。

Cisco Intrusion Prevention Alert Center にアクセスするには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Technical Support > Tools and Resources** をクリックします。

ステップ 3　Alerts & RMAs で、**Cisco Intrusion Prevention Alert Center** をクリックします。

Cisco IPS のアクティブなアップデート通知

Cisco.com にある Active Update Notifications に加入すると、シグニチャ アップデートおよびサービス パック アップデートがあった場合に電子メールを受け取ることができます。

アップデートに関する通知を受信するには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Technical Support & Documentation > Tools and Resources** をクリックします。

ステップ 3　Alerts & RMAs で、**Cisco Intrusion Prevention Alert Center** をクリックします。

ステップ 4　Active Updates で、**Active Update Notifications** をクリックします。

ステップ 5　次のように必要な情報を入力します。

a. IPS Active Update Notifications を受信するかどうかを指定します。メニューから **Yes** または **No** を選択します。
b. **First Name** フィールドに名前を入力します。
c. **Middle Name/Initial** フィールドにミドル ネームまたはそのイニシャルを入力します。
d. **Last Name/Surname** フィールドに姓を入力します。
e. **Organization** フィールドに所属組織名を入力します。
f. メニューから国を選択します。
g. **E-mail** フィールドに電子メール アドレスを入力します。

ステップ 6　シスコの製品やオファリングについての詳細情報を電子メールで受け取ることを希望する場合は、チェックボックスをオンにします。

ステップ 7　メニューから希望する電子メール形式を選択します。

ステップ 8　必要に応じてその他の情報を入力します。

a. メニューから職種を選択します。
b. メニューから役職を選択します。
c. メニューから業種を選択します。
d. メニューから、所属組織の世界全体における従業員数を選択します。
e. メニューから、会社または組織のタイプを選択します。

ステップ 9　**Submit Form** をクリックします。

これで、アップデートが行われたとき、電子メールの通知とアップデート入手方法の説明が送られてくるようになります。

Network Security Database

NSDB は、ネットワークの脆弱性情報の辞書を HTML ベースで示したものです。

通常、NSDB のエントリには次の重要なセキュリティ情報が含まれています。

- Signature Name：シグニチャの名前。
- Signature ID：シグニチャの一意の ID。
- Default Alarm Severity：そのシグニチャのデフォルトのアラーム レベル。
- Release Version：この番号は、そのシグニチャが最初に掲載されたリリースを示します。
- Release Date：シグニチャがリリースされた日付。
- Description：シグニチャと検出する不正利用についての簡潔な説明。
- Benign Trigger(s) : 不正利用のように表示されるが、実際は通常のネットワーク アクティビティである任意の「false positives」についての簡潔な説明。
- Recommended Filters：そのシグニチャに推奨するフィルタのリスト。
- Related Threats：各シグニチャには、0 個以上の関連する脅威があります。それぞれの脅威情報のページでは、脅威の背景と利用可能な対抗策のリンクが提供されます。

NSDB にアクセスするには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　**Technical Support > Tools and Resources** をクリックします。

ステップ 3　Alerts & RMAs で、**Cisco Intrusion Prevention Alert Center** をクリックします。

ステップ 4　シグニチャ ID によって並べ替えたシグニチャのリストを表示するには、左側の TOC の **List Signatures by Signature ID** をクリックします。

シグニチャ ID 順のリストが表示されます。

ステップ 5　特定のリリースのシグニチャのリストを表示するには、左側の TOC の **List Signatures by Release** をクリックします。

シグニチャ リリースによってグループ化されたシグニチャのリストが表示されます。

ステップ 6　シグニチャのキーワード、シグニチャ ID、脅威のキーワード、CVE ID、および脅威の重大度で検索を行うには、検索対象のカテゴリを選択し、キーワード、ID、または重大度を入力して、**Go** をクリックします。

条件に一致するシグニチャのリストが表示されます。

IPS ドキュメントへのアクセス

次の URL には、IPS 5.1 のマニュアルが用意されています。

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids12/index.htm