CHAPTER 24

Cisco IPS ソフトウェアについて

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 を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、Cisco IPS ソフトウェアとその入手およびインストール方法について説明します。内容は次のとおりです。

注意 Cisco IPS センサーの BIOS は Cisco IPS センサーに固有のものです。シスコ Web サイトから入手できる BIOS ファイルを使用し、シスコの手順に基づいてアップグレードする必要があります。シスコ以外またはサードパーティの BIOS を Cisco IPS センサーにインストールする場合は、保証の対象外となります。

IPS 7.1(1)E4 のファイル リスト

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 を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。

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

Cisco IPS ソフトウェアの入手方法

メジャー アップデート、マイナー アップデート、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、システム ファイル、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 のソフトウェア ダウンロード サイトにあります。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、さらに頻繁にアップデートされます。サービス パックは必要に応じて Cisco.com に掲示されます。メジャー アップデートおよびマイナー アップデートも定期的に掲示されます。最新の IPS ソフトウェアがないかどうか、定期的に Cisco.com を確認してください。

ソフトウェアをダウンロードするには、暗号化アクセス用のアカウントが必要です。このアカウントは、ソフトウェア ダウンロード サイトから IPS ソフトウェアを初めてダウンロードする際にセットアップします。また、IPS Alert Bulletins にサインアップしてソフトウェア リリースの最新情報を入手することができます

（注） ソフトウェアをダウンロードするには、Cisco.com にログインする必要があります。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。シグニチャ アップデートを適用するにはセンサー ライセンスが必要です。

IPS ソフトウェアのダウンロード

Cisco.com のソフトウェアをダウンロードするには、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　[Support] ドロップダウン メニューから、[Download Software] を選択します。

ステップ 3　[Select a Software Product Category] で、[Security Software] を選択します。

ステップ 4　[Intrusion Prevention System (IPS)] を選択します。

ステップ 5　ユーザ名とパスワードを入力します。

ステップ 6　[Download Software] ウィンドウで、[IPS Appliances] > [Cisco Intrusion Prevention System] を選択し、ダウンロードするバージョンをクリックします。

（注）　ソフトウェアをダウンロードするには、IPS 登録サービス ライセンスが必要です。

ステップ 7　必要なソフトウェア ファイルのタイプをクリックします。利用可能なファイルがウィンドウの右側のリストに表示されます。これは、ファイル名、ファイル サイズ、メモリ、およびリリース日でソートすることができます。リリース ノートやその他の製品マニュアルにアクセスすることもできます。

ステップ 8　ダウンロードするファイルをクリックします。ファイルの詳細が表示されます。

ステップ 9　ファイルが正しいことを確認し、[Download] をクリックします。

ステップ 10　[Agree] をクリックして、ソフトウェア ダウンロード規約に同意します。Cisco.com から初めてファイルを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する必要があります。

- フォームに入力し、[Submit] をクリックします。

  Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy が表示されます。
- ポリシーを読み、[I Accept] をクリックします。

  [Encryption Software Export/Distribution] フォームが表示されます。

すでに [Encryption Software Export Distribution Authorization] フォームに記入し、Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy を読んで承諾した場合、これらのフォームは表示されません。[File Download] ダイアログボックスが表示されます。

ステップ 11　ファイルを開くか、コンピュータに保存します。

ステップ 12　Readme に記載されている説明に従ってアップデートをインストールします。

（注）　メジャー アップデート、マイナー アップデート、サービス パック、リカバリ ファイル、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。

詳細情報

- IPS メンテナンス契約の詳細については、「IPS 製品のサービス プログラム」（P.18-12）を参照してください。
- センサー ライセンスの詳細については、「ライセンスの設定」（P.18-10）を参照してください。

IPS ソフトウェアのバージョン管理

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）　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は、IME の [Device List] ペインにある [Sensor Information] タブに一覧表示されます。

メジャー アップデート

メジャー アップデートには、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、Cisco IPS 7.0 ベース バージョンでは、前回のメジャー リリース以降の内容（マイナー アップデートの機能、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）すべて（廃止予定の機能は除く）に加えて、新しい変更が組み込まれます。メジャー アップデート 7.0(1) には、5.1(6) 以降が必要です。各メジャー アップデートには、対応するシステム パッケージおよびリカバリ パッケージがあります。

（注） 7.0(1) メジャー アップデートは、5.1(6) 以降のセンサーを 7.0(1) にアップグレードする場合に使用します。7.0(1) がすでにインストールされているセンサーに 7.0(1) を再インストールする場合は、メジャー アップデートではなくシステム イメージまたはリカバリ手順を使用します。

マイナー アップデート

マイナー アップデートは、メジャー バージョンに対する差分です。マイナー アップデートは、サービス パックのベース バージョンでもあります。7.0 の最初のマイナー アップデートは、7.1(1) です。マイナー アップデートは、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 アップデートには、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（廃止予定の機能は除く）、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 アップデートを前回のメジャー バージョンまたはマイナー バージョンにインストールすることができます（通常、それよりも前のバージョンにもインストールすることができます）。最新のマイナー バージョン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、マイナー アップデートに付属している Readme に記載されています。各マイナー アップデートには、対応するシステム パッケージおよびリカバリ パッケージがあります。

サービス パック

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。最新のサービス パック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、サービス パックに付属している Readme に記載されています。サービス パックには、最新のエンジン アップデートも含まれています。たとえば、サービス パック 7.1(3) がリリースされるときに、最新のエンジン レベルが E4 の場合、サービス パックは 7.1(3)E4 としてリリースされます。

パッチ リリース

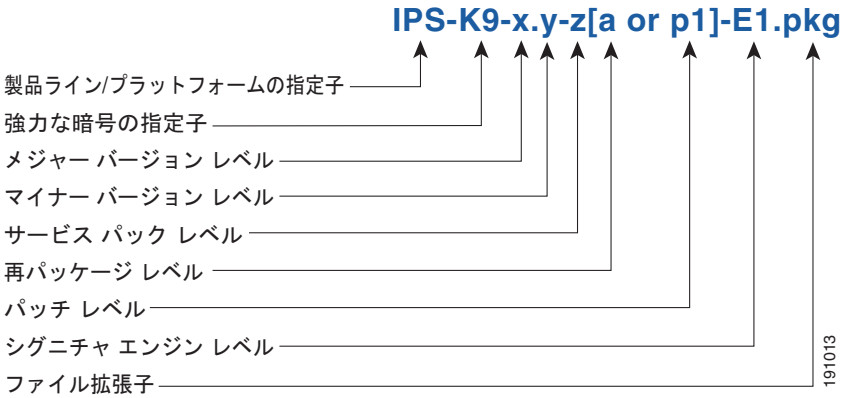
パッチ リリースは、ソフトウェアのリリース後にアップグレード バイナリで見つかった不具合をフィックスするために使用されます。次のメジャー アップデート、マイナー アップデート、またはサービス パックでこれらの不具合がフィックスされるまでの間に、パッチが公開されます。パッチには、関連するサービス パック レベルにある以前のパッチ リリースがすべて含まれます。各パッチは、次の公式のメジャー アップデート、マイナー アップデート、またはサービス パックで集約されます。

パッチ リリースをインストールする前に、最新のメジャー アップデート、マイナー アップデート、またはサービス パックをインストールしておく必要があります。たとえば、パッチ リリース 7.1(1p1) には、7.1(1) が必要です。

（注） 新しいパッチへのアップグレード時に、古いパッチをアンインストールする必要はありません。たとえば、7.1(1p1) を 7.1(1p2) にアップグレードする前に、7.1(1p1) をアンインストールする必要はありません。

図 24-1 は、メジャー アップデート、マイナー アップデート、サービス パック、およびパッチ リリースで、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 24-1　メジャー アップデート、マイナー アップデート、サービス パックおよびパッチ リリース用の IPS ソフトウェアのファイル名

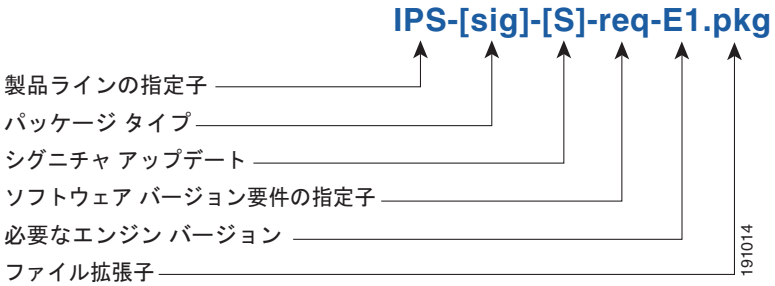


シグニチャ アップデート

シグニチャ アップデートは、悪意のあるネットワーク アクティビティを認識するように設計されたルール セットが含まれているパッケージ ファイルです。シグニチャ アップデートは、他のソフトウェア アップデートとは別個にリリースされます。メジャー アップデートまたはマイナー アップデートがリリースされるたびに、少なくとも 6 ヵ月間はシグニチャ アップデートを新しいバージョンおよび次に古いバージョンにインストールできます。シグニチャ アップデートは、必要なシグニチャ エンジンのバージョンによって決まります。このため、*req* 指示子で、特定のシグニチャ アップデートのサポートに必要なシグニチャ エンジンが示されています。

図 24-2 は、シグニチャ アップデートで、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 24-2　シグニチャ アップデート用の IPS ソフトウェアのファイル名

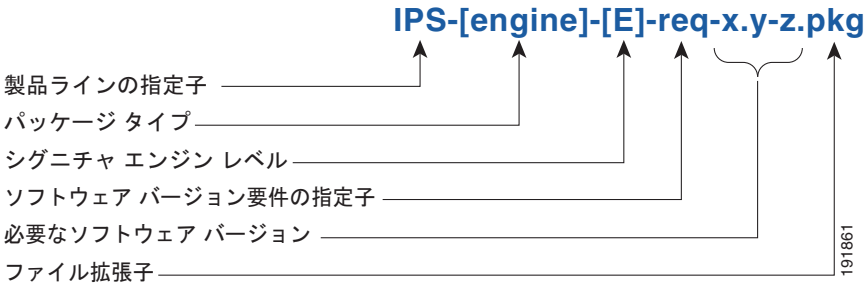


シグニチャ エンジンのアップデート

シグニチャ エンジンのアップデートは、新しいシグニチャ アップデートをサポートするためのバイナリ コードが含まれている実行可能ファイルです。シグニチャ エンジン ファイルには、特定のサービス パックが必要です。これは *req* 指示子でも識別できます。

図 24-3 は、シグニチャ エンジン アップデートで、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 24-3　シグニチャ エンジン アップデート用の IPS ソフトウェアのファイル名



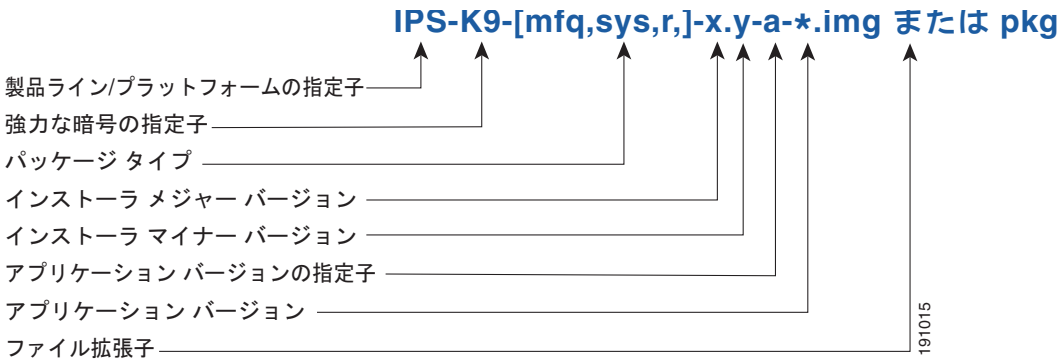
リカバリ イメージ ファイルおよびシステム イメージ ファイル

リカバリ イメージ ファイルおよびシステム イメージ ファイルには、インストーラのバージョンと基盤アプリケーションのバージョンが個別に含まれています。インストーラのバージョンには、メジャー バージョンのフィールドとマイナー バージョンのフィールドがあります。メジャー バージョンは、イメージ インストーラに大きな変更があるたびに増加されます。たとえば、.tar から .rpm への切り替えや、カーネルの変更などが挙げられます。マイナー バージョンは次のいずれかの場合に増加します。

- ユーザ プロンプトの追加など、インストーラに小さな変更があった場合。
- インストーラの不具合や問題をフィックスするためにイメージ ファイルを再パッケージングする必要がある場合。この場合、パッケージでは、インストーラのマイナー バージョンを 1 つ増加させる必要があります。

図 24-4 は、リカバリ イメージ ファイルおよびシステム イメージ ファイルで、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 24-4　リカバリ イメージ ファイルおよびシステム イメージ ファイルに対応する IPS ソフトウェアのファイル名



ソフトウェア リリースの例

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 を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。

表 24-1 に、プラットフォームに依存しない Cisco IPS 7.*x* ソフトウェア リリースの例を示します。

表 24-1　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	バージョンの例	ファイル名の例
シグニチャ アップデート[1]	週に 1 回	sig	S369	IPS-sig-S369-req-E4.pkg
シグニチャ エンジンのアップデート[2]	必要に応じて	engine	E4	IPS-engine-E4-req-7.1-1.pkg
サービス パック[3]	半年ごと または必要に応じて	—	7.1(3)	IPS-K9-7.1-3-E4.pkg
マイナー バージョン アップデート[4]	年に 1 回	—	7.2(1)	IPS-K9-7.2-1-E4.pkg （注）　IPS-AIM-K9-7.2-1-E4.pkg は、AIM-IPS のマイナー バージョン アップデートです。IPS-NME-K-9-7.2-1-E4.pkg は、NME-IPS のマイナー バージョン アップデートです。
メジャー バージョン アップデート[5]	年に 1 回	—	8.0(1)	IPS-K9-8.0-1-E4.pkg
パッチ リリース[6]	必要に応じて	patch	7.1(1p1)	IPS-K9-patch-7.1-1pl-E4.pkg
リカバリ パッケージ[7]	年に 1 回または必要に応じて	r	1.1-7.1(1)	IPS-K9-r-1.1-a-7.1-1-E4.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. シグニチャ エンジンのアップデートは、最新のシグニチャ アップデートの新しいシグニチャによって使用される新しいエンジンやエンジンのパラメータを追加します。
3. サービス パックには、障害のフィックスが含まれます。
4. マイナー バージョンには、マイナー バージョンの新しい特性や機能が含まれます。
5. メジャー バージョンには、メジャー バージョンの新しい機能やアーキテクチャが含まれます。
6. パッチ リリースは暫定的なフィックスです。
7. 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 7.1(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 24-2 に、プラットフォームに依存するソフトウェア リリースの例を示します。

表 24-2　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]	年に 1 回	sys	センサー プラットフォームごとに個別のファイル	IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
メンテナンス パーティション イメージ[2]	年に 1 回	mp	IDSM2	c6svc-mp.2-1-2.bin.gz
ブートローダ	必要に応じて	bl	AIM-IPS NME-IPS	pse_aim_x.y.z.bin pse_nm_x.y.z.bin （x、y、z はリリース番号）
ミニカーネル	必要に応じて	mini-kernel	AIM-IPS NME-IPS	pse_mini_kernel_1.1.10.64.bz2

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わ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、IDSM2 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。このファイルは、IDSM2 アプリケーション パーティションからインストールされますが、IDSM2 アプリケーション パーティションには影響はありません。

表 24-3 に、プラットフォーム固有の名前に使用するプラットフォーム識別子を示します。

表 24-3　プラットフォーム識別子

センサー ファミリ	識別子
IPS-4240 シリーズ	4240
IPS-4255 シリーズ	4255
IPS-4260 シリーズ	4260
IPS 4270-20 シリーズ	4270_20
Catalyst 6K の IDS モジュール	IDSM2
IPS ネットワーク モジュール	AIM NME
適応型セキュリティ アプライアンス モジュール	SSC_5 SSM_10 SSM_20 SSM_40

詳細情報

IPS ソフトウェア ファイルをインストールする方法の詳細については、第 25 章「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」を参照してください。

IPS のマニュアルへのアクセス

次の URL には、IPS のマニュアルが用意されています。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

また、Cisco.com から IPS のマニュアル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　[Support] をクリックします。

ステップ 3　[Support and Documentation] で、[Security] をクリックします。

ステップ 4　[Products] > [Security] > [Intrusion Prevention System (IPS)] > [IPS Appliances] > [Cisco IPS 4200 Series Sensors] の順にクリックします。[Cisco IPS 4200 Series Sensors] ウィンドウが表示されます。

ステップ 5　次のいずれかのカテゴリをクリックし、Cisco IPS のマニュアルにアクセスします。

- [Download Software]：ソフトウェア ダウンロード サイトに移動します。

（注） ソフトウェア ダウンロード サイト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。

- [Release and General Information]：マニュアルのロードマップおよびリリース ノートが表示されます。
- [Reference Guides]：コマンド リファレンスおよびテクニカル リファレンスが表示されます。
- [Design]：設計ガイドおよび設計テクニカル ノートが表示されます。
- [Install and Upgrade]：ハードウェアの設置と規制に関するガイドが表示されます。
- [Configure]：IPS CLI、IDM、および IME のコンフィギュレーション ガイドが表示されます。
- [Troubleshoot and Alerts]：TAC テクニカル ノートおよびフィールド ノーティスが表示されます。

Cisco Security Intelligence Operations

Cisco.com の Cisco Security Intelligence Operations サイトは、現在の脆弱性およびセキュリティ上の脅威に関するインテリジェンス レポートを提供します。また、組織のリスクを減らすために、ネットワークを保護し、セキュリティ システムを展開するのに役立つその他のセキュリティ項目に関するレポートも提供します。

最新のセキュリティ上の脅威を確認しておくことで、最も効果的にネットワークを保護、管理できます。Cisco Security Intelligence Operations には、日付、重大度、緊急性、および脅威に対処可能な新しいシグニチャがあるかどうかをトップ 10 形式で一覧表示するインテリジェンス レポートが含まれます。

Cisco Security Intelligence Operations には、該当するセキュリティ上の記事を一覧表示する Security News のセクションが含まれます。セキュリティ関連のツールやリンクもあります。

Cisco Security Intelligence Operations には、次の URL からアクセスできます。

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations はまた、シグニチャ ID、タイプ、構造、および説明を含む、個別のシグニチャ情報のリポジトリでもあります。

セキュリティ警告およびシグニチャは、次の URL で検索できます。

http://tools.cisco.com/security/center/search.x