

Cisco IPS AIM

全般

Q. Cisco Intrusion Prevention System (IPS; 侵入防御システム) Advanced Integration Module (AIM) とは何ですか。

A. Cisco ISR 1841、Cisco ISR 2800 および Cisco ISR 3800 サービス統合型ルータ シリーズ用の Cisco IPS AIM は、Cisco IPS センサー製品の 1 つです。Cisco IPS AIM は専用の CPU とメモリを搭載しており、インライン モードおよびプロミスキャス モードでの侵入防御処理における負荷を軽減します。また、Cisco IPS AIM 上で Cisco IPS 6.0 センサーのイメージを動作させることにより、Cisco IPS 4200 シリーズ センサーおよび Cisco ASA 5500 シリーズ 適応型セキュリティ アプライアンスと同等の機能を提供します。

Q. 本社側ですでに侵入防御機能を実装しているにもかかわらず、ブランチでも Cisco IPS AIM を実装する必要があるのはなぜですか。

A. 企業用 WAN において、多対多のコミュニケーション トポロジへの移行が進んでいる現在、ブランチ間通信のすべてのトラフィックがデータセンターを通過しているとは限りません。また、ブランチ オフィスはワームやウイルスの侵入に対して脆弱です。ブランチ オフィスで IPS を実装すると、企業全体に攻撃が広がる前にネットワーク エッジでそれらを識別して問題を解決できます。コア IPS に到達する前に内部ネットワークに広がるワームの場合、コア IPS のサーバーへの DoS 攻撃が発生する可能性があります。

Q. Cisco IOS® IPS はどのような場合に導入したらよいですか。また、Cisco IPS AIM はどのような場合に使用すべきですか。両方を同時に使用することはできますか。

A. Cisco IOS IPS と Cisco IPS AIM を同時に使用することはできません。Cisco IPS AIM を導入する場合、Cisco IOS IPS を無効にする必要があります。Cisco IOS IPS は、ルータを経由するトラフィックを検査する機能を提供する IPS アプリケーションであり、Cisco IOS Advanced Security フィーチャ セットに付属しています。Cisco IOS IPS は、検査を実行する際にルータの CPU および共有メモリ プールを使用します。このとき Cisco IOS IPS が用いるのは、IPS シグニチャのサブセットです。Cisco IPS AIM は専用の CPU とメモリを使用して動作するため、ルータの CPU における IPS シグニチャ処理の負荷を軽減できます。また、フルセットのシグニチャ セットをロードすることにより、Cisco IOS IPS では不可能な高度な IPS 機能を提供することもできます。

Q. Cisco IPS AIM の最も一般的な展開シナリオは何ですか。

A. WAN リンク、企業オフィス、およびリモート サイトのサーバーの保護のために導入するのが最も一般的な展開シナリオです。プライベート接続かパブリック接続かに関係なく、WAN リンクはブランチ オフィスで発生する脅威に対して脆弱です。ブランチで IPS を実装すれば、攻撃がネットワークの他の部分に広がる前にそれらを WAN エッジ上で軽減できます。同様に、多くの場合、リモート サイトのサーバーには企業のデータセンターで処理されるデータに匹敵する重要なデータが格納されています。このようなデータを保護するには、これらのサーバーが攻撃を受ける前に脅威を隔離することが重要です。中堅・中小規模企業あるいは小規模ブランチ オフィスのインターネット ルータに Cisco IPS AIM を搭載すれば、最終的にメインのネットワークの保護に役立ちます。

Q. IPS の利用に最も適しているのは、どのようなブランチ オフィスですか。

A. 事実上すべてのブランチ オフィスで IPS を活用できます。最も危険なブランチは、IT スタッフを配置していない企業のブランチです。このようなブランチでは、ブランチまたは店舗の管理者が IT ポリシーの適用ではなく経営に重点を置いているためです。

Q. Cisco IPS AIM の製品番号を教えてください。

A. Cisco IPS AIM の製品番号は AIM-IPS-K9 です。

Q. Cisco IPS AIM をサポートしているプラットフォームを教えてください。

A. Cisco IPS AIM は、Cisco ISR 1841、Cisco ISR 2800 および Cisco ISR 3800 シリーズでサポートされています。ただし、Cisco 2600 および 3700 シリーズ マルチサービス アクセス ルータなどの以前のプラットフォームでは、AIM スロットを搭載している場合でも Cisco IPS AIM をサポートしていません。これらのプラットフォームに Cisco IPS AIM を搭載した場合、カードおよびプラットフォームに回復不能な損傷が発生する可能性があります。

Q. Cisco IPS AIM をサポートしているフィーチャ セットを教えてください。

A. Cisco IPS AIM は、Cisco IOS Advanced IP Services フィーチャ セットや Advanced Enterprise Services フィーチャ セットなど、Cisco IOS Advanced Security フィーチャ セット以上でサポートされています。

Q. 製品番号にある K9 とはどのような意味ですか。

A. K9 は、Triple Digital Encryption Standard (3DES)、Advanced Encryption Standard (AES) などの強固な暗号化方式が利用可能であることを意味します。Cisco IPS AIM は IPBASE イメージなどでもサポートされていますが、カードは K9 製品としての指定を受けています。これは、カード自体に Secure Shell (SSH) プロトコルの強固な暗号化方式が含まれているためです。シスコでは、K9 指定の暗号化対応デバイスおよびソフトウェアの出荷管理を行っており、このようなデバイスの輸出に関する米商務省の規定に準拠しています。

Q. Cisco IPS AIM をサポートする Cisco IOS ソフトウェア リリースを教えてください。

A. Cisco IPS AIM は、Cisco IOS ソフトウェア リリース 12.4(15) BU Special および 12.5(1st)T でサポートされています。

Q. Cisco IPS AIM は IPv6 をサポートしていますか。

A. いいえ。現在、Cisco IPS AIM およびネットワーク モジュールでは IPv6 をサポートしていません。

Q. Cisco IPS AIM でマルチキャストトラフィックを監視できますか。

A. いいえ。Cisco IPS AIM では、マルチキャストトラフィックを監視できません。

Q. Cisco IPS AIM と Cisco IOS IPS の違いは何ですか。

A. Cisco IPS AIM と Cisco IOS IPS の主な違いは次のとおりです。

- Cisco IPS AIM には IPS 処理の負荷を軽減するための専用の CPU と DRAM が搭載されていますが、Cisco IOS IPS はルータのリソースを共有し、それらを使用することで処理を実行します。
- Cisco IPS AIM はインライン モードとプロミスキャス モードの両方をサポートしますが、Cisco IOS IPS はインライン モードのみをサポートします。
- Cisco IPS AIM はフルセットの IPS シグニチャ セットをサポートしますが、Cisco IOS IPS はサブセットのみをサポートします。
- Cisco IPS AIM は Linux ベースの Cisco IPS 6.0 センサー イメージで動作しますが、Cisco IOS IPS は Cisco IOS ソフトウェア ベースの IPS コードで動作します。

Q. Cisco IPS AIM と Cisco Intrusion Detection System (IDS; 侵入検知システム) ネットワーク モジュールの違いは何ですか。

A. Cisco IPS AIM と Cisco IDS ネットワーク モジュールの主な違いは次のとおりです。

- Cisco IPS AIM はインライン モードとプロミスキャス モードの両方をサポートしますが、Cisco IDS ネットワーク モジュールはプロミスキャス モードのみをサポートします。
- Cisco IPS AIM はルータ ポートによって内部的に管理されますが、Cisco IDS ネットワーク モジュールはカードの外部管理ポートによって管理されます。
- Cisco IPS AIM には 256 MB の eUSB フラッシュ メモリが搭載されていますが、Cisco IDS ネットワーク モジュールには 40 GB のハード ディスクが搭載されています。

インストールおよび設定

Q. Cisco IPS AIM のコンソールにアクセスする方法を教えてください。

A. Cisco IPS AIM にアクセスするには、`service-module ids-sensor 0/0 session` コマンドを使用します。これにより、リバース Telnet セッションが開始され、AIM のコンソール プロンプトが表示されます。この時点から、Cisco IOS ソフトウェアではなく Cisco IDS アプリケーションに対する設定が行われます。AIM から抜けて Cisco IOS ソフトウェアの設定に戻るには、Ctrl キーと Alt キーを押しながら ^ キーを押します。これによりリバース Telnet セッションが終了し、Cisco IOS コマンド プロンプトが表示されます。

Q. Cisco IPS AIM ではどのような番号付けが行われていますか。

A. Cisco IOS IDS-Sensor インターフェイスでは、スロットまたはポートに番号が付けられています。Cisco IPS AIM の場合、スロット番号は常に 0 で、ポート番号は AIM スロットの番号です。AIM スロット 0 の IPS AIM は IDS-Sensor 0/0、AIM スロット 1 の IPS AIM は IDS-Sensor 0/1 です。

Q. ブート ローダおよびミニカーネルとは何ですか。

A. ブート ローダは、該当するオペレーティング システムを検索およびロードしたうえで処理を受け渡すソフトウェアです。Cisco IPS AIM には ランタイム ブート ローダおよびフェールセーフ ブート ローダの 2 つのブート ローダがあります。ランタイム ブート ローダは、通常の操作で実行されます。ランタイム ブート ローダの起動に失敗すると、カードはフェールセーフ ブート ローダにフォールバックします。ランタイム ブート ローダはアップグレードできますが、フェールセーフ ブート ローダではできません。

ミニカーネルは、ブート ローダ設定ファイルが示す IPS センサー イメージを USB フラッシュ デバイスから読み取り、指定されたパラメータに従ってイメージを実行する場合に使用します。カードが通常モードになるように設定されている場合、ミニカーネルはランタイム ブート ローダによって自動的に呼び出されます。

Q. Cisco IPS AIM の最新の IPS センサー イメージはどこで入手できますか。

A. IPS ソフトウェア イメージの入手については、以下の URL にアクセスしてください。

<http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/index.shtml>

Q. IPS センサー イメージをアップグレードする方法を教えてください。

A. アプリケーションのアップグレード方法については、以下の URL (英語) にアクセスしてください。

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

Q. IPS センサーをバイパス モードに設定する方法を教えてください。

A. IPS センサーをバイパス モードに設定するには、次の手順を実行します。

- センサーとのセッションを開始します。
- センサーのプロンプトで、**configure terminal** コマンドを入力します。
- センサーの config プロンプトで、**service interface** コマンドを入力します。
- センサーの config-int プロンプトで、**bypass off|on|auto** コマンドを入力します。off オプションを使用すると、インライン バイパスがオフになります。パケットのインスペクションはインライン データ トラフィック上で実行されます。ただし、IPS 分析エンジンが停止すると、インライン データのトラフィックは中断します。on オプションを使用すると、インライン バイパスがオンになります。トラフィックのパケット インスペクションは実行されません。分析エンジンが停止した場合も、インライン トラフィックは引き続き送信されます。auto オプションを使用すると、分析エンジンがパケット処理を停止した場合、インラインでのパケット インスペクションが自動的にバイパスされます。このオプションでは、インライン インターフェイスでのデータの中断はありません。

Q. 何らかの理由で Cisco IPS AIM がパケット インスペクションを実行できない場合、トラフィックは通過しますか、それとも廃棄されますか。

A. Cisco IPS AIM が特定のパケットまたはすべてのパケット インスペクションを実行できない場合、ユーザはパケットを廃棄するか、検査なしで通過させるかを選択できます。この選択は、Cisco IOS IDS-Sensor インターフェイスで **service module fail-close** コマンドまたは **service-module fail-open** コンフィギュレーション コマンドを使用して行います。

```
atg2851-21#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
atg2851-21(config)#interface IDS-Sensor 0/0
atg2851-21(config-if)#service-module ?
    fail-close Blocks traffic if Service Module fails
    fail-open  Permits traffic if Service Module fails
```

fail-open を指定すると、検査できないトラフィックはそのまま送信されます。fail-close を指定すると、検査できないトラフィックは廃棄されます。デフォルトは fail-open です。

Q. IPS センサー イメージと Cisco IOS ソフトウェア イメージは個別にアップグレードできますか。

A. はい。

Q. Cisco IPS AIM と Cisco IDS ネットワーク モジュールは同じイメージを使用しますか。

A. いいえ。別の IPS センサー イメージを使用します。

Q. レイヤ 2 の Cisco EtherSwitch[®] インターフェイスでは ids-service-module monitoring コマンドを設定できませんが、それはなぜですか。

A. ids-service-module monitoring コマンドは、レイヤ 2 インターフェイスでは使用できません。レイヤ 2 インターフェイスを VLAN に割り当て、VLAN 上で monitoring コマンドを設定してください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日10:00～12:00、13:00～17:00

お問い合わせ先