ASA IPS モジュール

この章では、ASA IPS モジュールを設定する方法について説明します。ASA IPS モジュールは、ご使用の ASA モデルに応じて、ハードウェア モジュールである場合とソフトウェア モジュールである場合があります。ASA モデルごとにサポートされている ASA IPS モジュールのリストについては、次の URL にある『*Cisco ASA Compatibility Matrix*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

ASA IPS モジュールに関する情報

ASA IPS モジュールは、高度な IPS ソフトウェアを実行します。このソフトウェアによる、予防的なフル機能の侵入防御サービスは、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前に、これらを阻止します。

ASA IPS モジュールがどのように ASA と連携するか

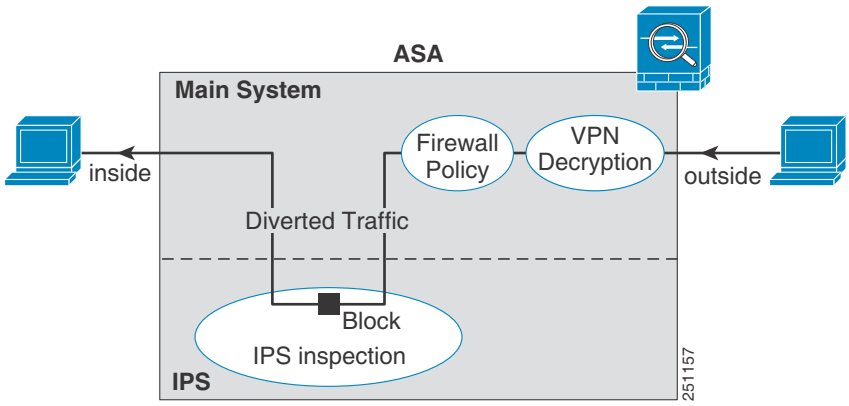
ASA IPS モジュールは、ASA とは別のアプリケーションを実行します。ASA IPS モジュールに外部管理インターフェイスが搭載されている場合は、ASA IPS モジュールに直接接続することができます。管理インターフェイスが搭載されていない場合は、ASA インターフェイスを介して ASA IPS モジュールに接続できます。ASA 5585-X 上の ASA IPS SSP にはデータ インターフェイスが含まれます。このインターフェイスによって、ASA のポート密度が増加します。ただし、ASA の全体的なスループットは増加しません。

トラフィックは、ファイアウォール検査を通過してから ASA IPS モジュールへ転送されます。ASA で IPS インスペクション対象として指定されたトラフィックは、次に示すように ASA および ASA IPS モジュールを通過します。**注**：この例は「インライン モード」の場合です。ASA がトラフィックのコピーを ASA IPS モジュールに送信するだけである「無差別モード」については、「動作モード」（P.19-3）を参照してください。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. トラフィックが ASA IPS モジュールに送信されます。
5. ASA IPS モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックが ASA に返送されます。ASA IPS モジュールは、セキュリティ ポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

図 19-1 は、ASA IPS モジュールをインライン モードで実行している場合のトラフィック フローを示します。この例では、ASA IPS モジュールが攻撃と見なしたトラフィックは自動的にブロックされます。それ以外のトラフィックは、ASA を通って転送されます。

図 19-1　ASA での ASA IPS モジュールのトラフィック フロー：インライン モード

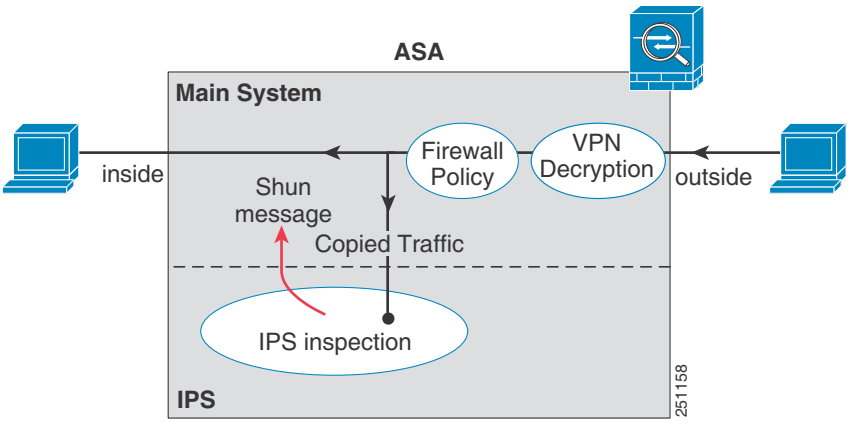


動作モード

次のいずれかのモードを使用して、トラフィックを ASA IPS モジュールに送信できます。

- インライン モード：このモードでは、ASA IPS モジュールはトラフィック フローの中に直接配置されます（図 19-1 を参照）。IPS インスペクション対象として指定されたトラフィックは、ASA IPS モジュールに渡されて検査を受けてからでなければ、ASA を通過することはできません。インスペクション対象と識別されたすべてのパケットは通過する前に分析されるため、このモードは最もセキュアです。また、ASA IPS モジュールはパケット単位でブロッキング ポリシーを実装できます。ただし、このモードは、スループットに影響を与えることがあります。
- 無差別モード：このモードでは、トラフィックの複製ストリームが ASA IPS モジュールに送信されます。このモードは安全性では劣りますが、トラフィックのスループットにほとんど影響を与えません。インライン モードとは異なり、無差別モードでは、ASA IPS モジュールがトラフィックをブロックできるのは、ASA にトラフィックの排除を指示するか、ASA 上の接続をリセットした場合だけです。また、ASA IPS モジュールがトラフィックを分析している間は、ASA IPS モジュールがそのトラフィックを排除できるようになる前に、少量のトラフィックが ASA を通過することがあります。図 19-2 は、無差別モードでの ASA IPS モジュールを示します。この例では、ASA IPS モジュールは脅威と見なしたトラフィックについての排除メッセージを ASA に送信します。

図 19-2　ASA での ASA IPS モジュールのトラフィック フロー：無差別モード



仮想センサーの使用

IPS ソフトウェアのバージョン 6.0 以降を実行している ASA IPS モジュールでは、複数の仮想センサーを実行できます。つまり、ASA IPS モジュールで複数のセキュリティ ポリシーを設定することができます。各 ASA セキュリティ コンテキストまたはシングル モードの ASA を 1 つまたは複数の仮想センサーに割り当てる、または複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。仮想センターの詳細（サポートされている最大センサー数など）については、IPS のマニュアルを参照してください。

図 19-3 では、1 つのセキュリティ コンテキストと 1 つの仮想センター（インライン モード）がペアになり、2 つのセキュリティ コンテキストが同じ仮想センサーを共有しています。

図 19-3　セキュリティ コンテキストと仮想センサー

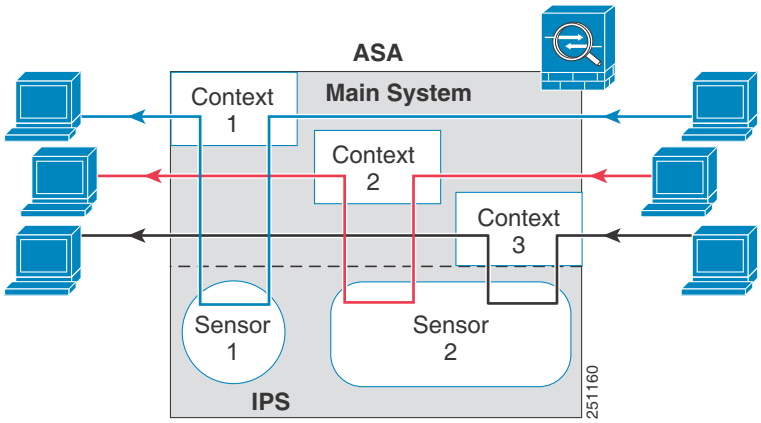
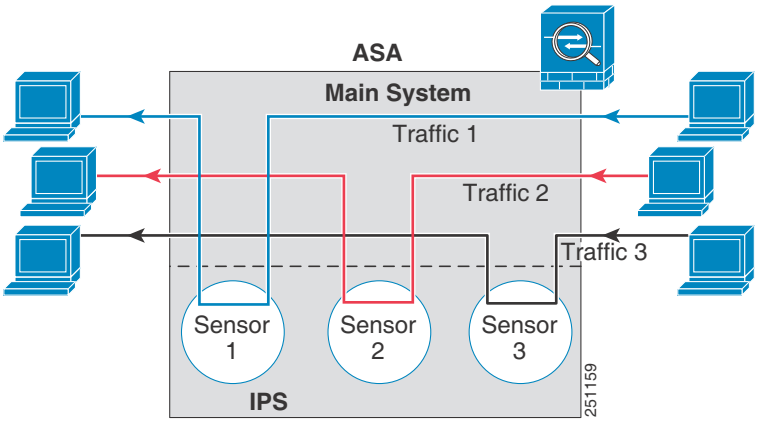


図 19-4 では、シングル モードの ASA が複数の仮想センサー（インライン モード）とペアになっています。定義されている各トラフィック フローは異なるセンサーに進みます。

図 19-4　複数の仮想センサーがあるシングル モードの ASA



管理アクセスに関する情報

次の方法を使用して、IPS アプリケーションを管理できます。

- ASA からモジュールへのセッション接続：ASA に CLI アクセスが可能な場合は、モジュールにセッション接続し、そのモジュール CLI にアクセスできます。「ASA からモジュールへのセッションの開始」（P.19-10）を参照してください。
- ASDM または SSH を使用して IPS 管理インターフェイスに接続する：ASDM を ASA から起動すると、IPS アプリケーションを設定するために管理ステーションがモジュール管理インターフェイスに接続します。SSH の場合、モジュール管理インターフェイスでモジュール CLI に直接アクセスできます（Telnet アクセスでは、モジュール アプリケーションで追加の設定が必要になります）。モジュール管理インターフェイスは、syslog メッセージの送信や、シグニチャ データベースの更新などのモジュール アプリケーションの更新に使用できます。

管理インターフェイスについては、次の情報を参照してください。

- ASA 5585-X：IPS 管理インターフェイスは、独立した外部ギガビット イーサネット インターフェイスです。
- ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X：これらのモデルは、ASA IPS モジュールをソフトウェア モジュールとして実行します。IPS 管理インターフェイスは、Management 0/0 インターフェイスを ASA と共有します。ASA と ASA IPS モジュールのそれぞれに別の MAC アドレスと IP アドレスがサポートされます。IPS IP アドレスの設定は、IPS オペレーティング システム内で（CLI または ASDM を使用して）実行する必要があります。ただし、物理特性（インターフェイスのイネーブル化など）は、ASA 上で設定されます。ASA インターフェイス コンフィギュレーションを削除して（特にインターフェイス名）、このインターフェイスを IPS 専用インターフェイスとすることができます。このインターフェイスは管理専用です。

ASA IPS モジュールのライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
ASA 5512-X、 ASA 5515-X、 ASA 5525-X、 ASA 5545-X、 ASA 5555-X	IPS モジュールのライセンス **（注）** IPS モジュール ライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。別の IPS シグニチャ サブスクリプションを購入する必要があります。フェールオーバー用に、各ユニットのサブスクリプションを購入します。IPS シグニチャのサポートを受けるには、IPS が事前インストールされた ASA を購入する必要があります（製品番号に「IPS」が含まれている必要があります）。結合されたフェールオーバー クラスタ ライセンスでは、非 IPS ユニットと IPS ユニットをペアにすることはできません。たとえば ASA 5515-X の IPS 版（製品番号 ASA5515-IPS-K9）を購入し、非 IPS 版（製品番号 ASA5515-K9）を使用してフェールオーバー ペアを作成しようとしている場合は、他のユニットから IPS モジュール ライセンスを継承した場合であっても、ASA5515-K9 ユニットの IPS シグニチャ アップデートを取得できません。
ASA 5585-X	基本ライセンス
他のすべてのモデル	サポートしない

ガイドラインと制限事項

この項では、この機能のガイドラインと制限事項について説明します。

モデルのガイドライン

- どのモデルがどのモジュールをサポートするかの詳細については、次の URL にある『*Cisco ASA Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

その他のガイドライン

- ASA と IPS モジュールの総スループットは、ASA 単独のスループットよりも低くなります。
  - ASA 5512-X ～ ASA 5555-X：http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-700608.html を参照
  - ASA 5585-X：http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/qa_c67-617018.html を参照
- モジュールにインストールされているソフトウェアのタイプの変更はできません。つまり、購入した ASA IPS モジュールに、後で別のソフトウェアをインストールすることはできません。

デフォルト設定

表 19-1 に、ASA IPS モジュールのデフォルト設定値を示します。

表 19-1　デフォルトのネットワーク パラメータ

パラメータ	デフォルト
管理 IP アドレス	192.168.1.2/24
ゲートウェイ	192.168.1.1/24（デフォルトの ASA 管理 IP アドレス）
ユーザ名	cisco
パスワード	cisco

（注）　ASA のデフォルトの管理 IP アドレスは 192.168.1.1/24 です。

ASA IPS モジュールの設定

この項では、ASA IPS モジュールを設定する方法について説明します。

ASA IPS モジュールのタスク フロー

ASA IPS モジュールの設定プロセスでは、IPS セキュリティ ポリシーを ASA IPS モジュール上で設定してから、トラフィックを ASA IPS モジュールに送信するように ASA を設定します。ASA IPS モジュールを設定するには、次の手順に従います。

ステップ 1　ASA IPS 管理インターフェイスにケーブル接続します。「ASA IPS 管理インターフェイスの接続」（P.19-7）を参照してください。

ステップ 2　モジュールへのセッションを開始します。バックプレーンを介して IPS CLI にアクセスします。「ASA からモジュールへのセッションの開始」（P.19-10）を参照してください。

ステップ 3　（ASA 5512-X ～ ASA 5555-X、必須の可能性があります）ソフトウェア モジュールをインストールします。「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.19-11）を参照してください。

ステップ 4　ASA は、IPS モジュールの基本的なネットワーク設定を設定します。「IPS モジュールの基本的なネットワーク設定値の設定」（P.19-13）を参照してください。

ステップ 5　モジュール上で、インスペクションと保護のポリシーを設定します。このポリシーによって、トラフィックの検査方法と侵入検出時の処理が決まります。「ASA IPS モジュールでのセキュリティ ポリシーの設定」（P.19-13）を参照してください。

ステップ 6　（任意）マルチ コンテキスト モードの ASA で、各コンテキストで使用可能な IPS 仮想センサーを指定します（仮想センサーが設定されている場合）。「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）を参照してください。

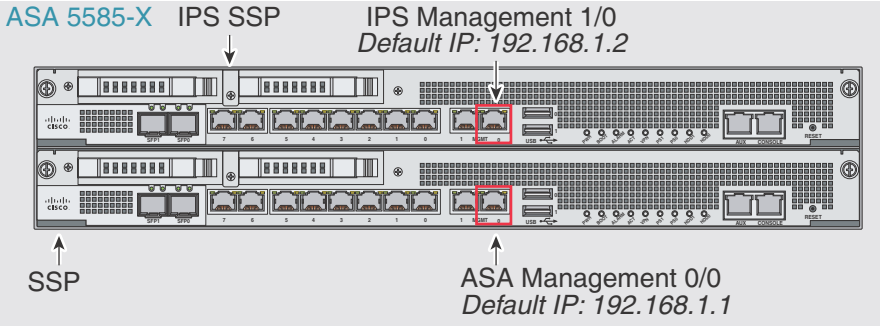
ステップ 7　ASA で、ASA IPS モジュールに誘導するトラフィックを指定します。「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）を参照してください。

ASA IPS 管理インターフェイスの接続

IPS モジュールへの管理アクセスを提供する以外に、IPS 管理インターフェイスは、HTTP プロキシ サーバまたは DNS サーバおよびインターネットへのアクセスを必要とします。グローバル相関、シグニチャ アップデートおよびライセンス要求をダウンロードできるようにするためです。この項では、推奨されるネットワーク コンフィギュレーションを示します。実際のネットワークでは、異なる可能性があります。

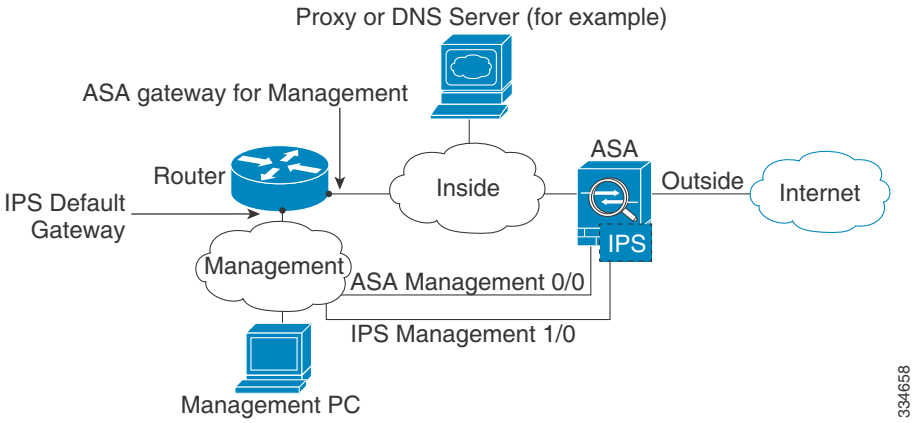
ASA 5585-X（ハードウェア モジュール）

IPS モジュールには、ASA とは別の管理インターフェイスが含まれます。



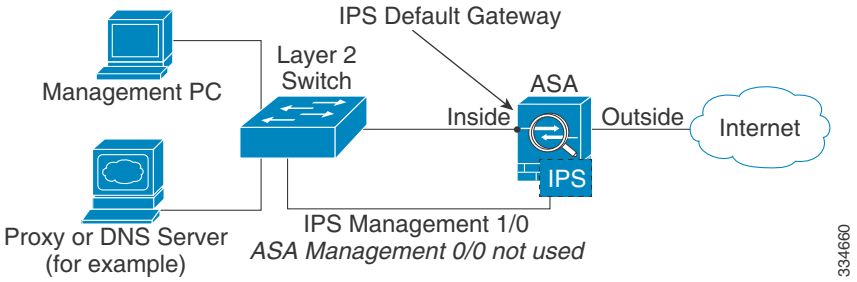
内部ルータがある場合

内部ルータがある場合は、管理ネットワーク（これには ASA Management 0/0 インターフェイスおよび IPS Management 1/0 インターフェイスの両方を含めることができます）と ASA 内部ネットワークとの間でルーティングできます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



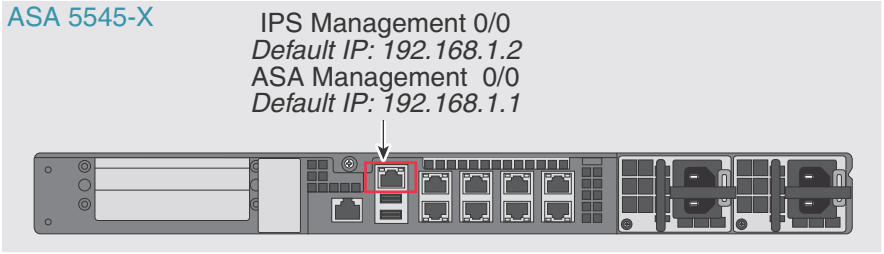
内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません（仮に持つとすれば、内部ルータがネットワーク間のルーティングを行う必要があります）。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。IPS モジュールは ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に IPS Management 1/0 アドレスを設定できます。



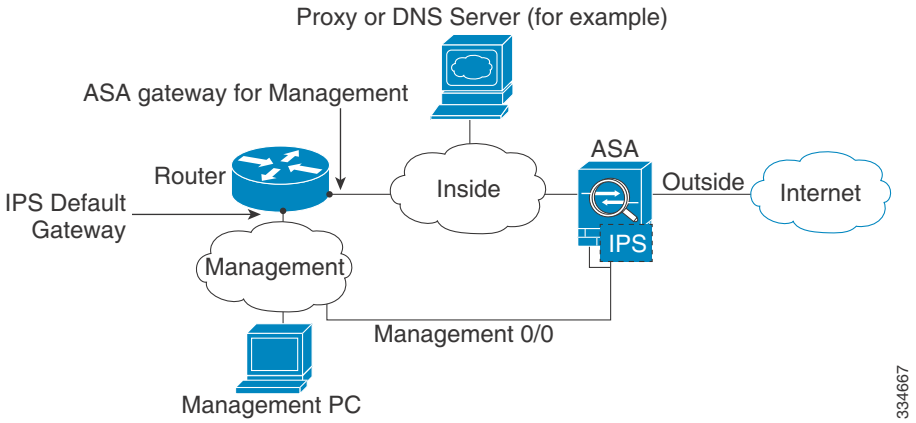
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

これらのモデルは、IPS モジュールをソフトウェア モジュールとして実行し、IPS 管理インターフェイスは Management 0/0 インターフェイスを ASA と共有します。



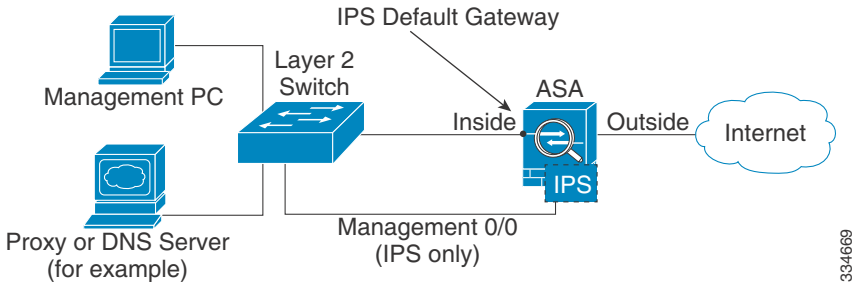
内部ルータがある場合

内部ルータがある場合は、Management 0/0 ネットワーク（これには ASA および IPS の両方の管理 IP アドレスとが含まれます）と内部ネットワークとの間でルーティングできます。必ず、内部ルータを介して管理ネットワークに到達するためのルートを ASA に追加してください。



内部ルータがない場合

内部ネットワークが 1 つだけの場合は、別の管理ネットワークも持つことはできません。この場合は、Management 0/0 インターフェイスの代わりに内部インターフェイスから ASA を管理できます。ASA で設定された名前を Management 0/0 インターフェイスから削除した場合も、そのインターフェイスの IPS IP アドレスを設定できます。IPS モジュールは実質的に ASA とは別のデバイスであるため、内部インターフェイスと同じネットワーク上に IPS 管理アドレスを設定できます。



（注）　Management 0/0 に対して ASA で設定された名前を削除する必要があります。この名前が ASA 上で設定されている場合は、IPS のアドレスは ASA と同じネットワーク上にあることが必要になり、その結果、他の ASA インターフェイス上ですでに設定されたネットワークが除外されます。名前が設定されていない場合は、IPS のアドレスが存在するのはどのネットワークでも、たとえば、ASA 内部ネットワークでもかまいません。

次の作業

- 基本的なネットワーク設定を設定します。「IPS モジュールの基本的なネットワーク設定値の設定」（P.19-13）を参照してください。

ASA からモジュールへのセッションの開始

IPS モジュール CLI に ASA からアクセスするには、ASA からセッションを開始します。ソフトウェア モジュールの場合は、モジュールへのセッションを開始することも（Telnet を使用）、仮想コンソール セッションを作成することもできます。コンソール セッションは、コントロール プレーンがダウンし、Telnet セッションを確立できない場合に便利です。

手順の詳細

コマンド	目的

Telnet セッション。
ハードウェア モジュール（例：ASA 5585-X）の場合：
session 1
ソフトウェア モジュール（例：ASA 5545-X）の場合：
session ips
 	
例：
`hostname# session 1`
 	
`Opening command session with slot 1.`
`Connected to slot 1.Escape character sequence is 'CTRL-^X'.`
 	
`sensor login: cisco`
`Password: cisco`
	Telnet を使用してモジュールにアクセスします。ユーザ名とパスワードの入力を求められます。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。
	（注） 初めてモジュールにログインしたときに、デフォルトのパスワードの変更を要求するプロンプトが表示されます。パスワードは 8 文字以上で、辞書に載っていない単語にする必要があります。

コンソール セッション（ソフトウェア モジュールのみ）。
session ips console
 	
例：
`hostname# session ips console`
 	
`Establishing console session with slot 1`
`Opening console session with module ips.`
`Connected to module ips.Escape character sequence is 'CTRL-SHIFT-6 then x'.`
 	
`sensor login: cisco`
`Password: cisco`
	モジュール コンソールにアクセスします。ユーザ名とパスワードの入力を求められます。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。
	（注） このコマンドは、Ctrl+Shift+6、x がターミナル サーバのプロンプトに戻るエスケープ シーケンスであるターミナル サーバとともに使用しないでください。Ctrl+Shift+6、x は、IPS コンソールをエスケープし ASA プロンプトに戻るシーケンスでもあります。したがって、この状況で IPS を終了しようとすると、代わりにターミナル サーバ プロンプトに戻ります。ASA にターミナル サーバを再接続すると、IPS コンソール セッションがまだアクティブなままであり、ASA プロンプトに戻ることができません。ASA プロンプトにコンソールを戻すには、直接シリアル接続を使用する必要があります。
	
	代わりに **session ips** コマンドを使用します。

（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動

ASA には一般的に、IPS モジュール ソフトウェアが付属しており、Disk0 に収録されています。このモジュールが実行されていない場合や、IPS モジュールを既存の ASA に追加する場合は、モジュール ソフトウェアを起動する必要があります。モジュールが実行中か不明な場合は、セッションを開始できません。

手順の詳細

ステップ 1　次のどちらかを実行します。

- プリインストール済みの IPS を搭載する新しい ASA : フラッシュ メモリで IPS モジュール ソフトウェアのファイル名を表示するには、次のコマンドを入力します。

  ```
  hostname# dir disk0:
  ```

  たとえば、IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip のようなファイル名を検索します。ファイル名をメモしておきます。このファイル名は、この手順で後ほど必要になります。

- 既存の ASA に新しい IPS をインストールする場合 : IPS ソフトウェアを Cisco.com から TFTP サーバ にダウンロードします。Cisco.com のログインをお持ちの場合は、次の Web サイトからソフトウェアを入手できます。

  http://www.cisco.com/cisco/software/navigator.html?mdfid=282164240

  ASA にソフトウェアをコピーします。

  ```
  hostname# copy tftp://server/file_path disk0:/file_path
  ```

  他のダウンロード サーバ タイプの場合は、一般的な操作のコンフィギュレーション ガイドを参照してください。

  ファイル名をメモしておきます。このファイル名は、この手順で後ほど必要になります。

ステップ 2　disk0 の IPS モジュール ソフトウェアの場所を設定するには、次のコマンドを入力します。

```
hostname# sw-module module ips recover configure image disk0:file_path
```

たとえば、この例のステップ 1 のファイル名を使用するには、次のとおりに入力します。

```
hostname# sw-module module ips recover configure image
disk0:IPS-SSP_5512-K9-sys-1.1-a-7.1-4-E4.aip
```

ステップ 3　IPS モジュール ソフトウェアをインストールし、ロードするには、次のコマンドを入力します。

```
hostname# sw-module module ips recover boot
```

ステップ 4　イメージ転送とモジュール再起動プロセスの進行状況を確認するには、次のコマンドを入力します。

```
hostname# show module ips details
```

出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

IPS モジュールの基本的なネットワーク設定値の設定

マルチ コンテキスト モードでは、ASA からモジュールへのセッションを開始し、**setup** コマンドを使用して基本設定を行います。

（注） （ASA 5512-X ～ ASA 5555-X）モジュールへのセッションを開始できない場合は、IPS モジュールが動作していません。「（ASA 5512-X ～ ASA 5555-X）ソフトウェア モジュールの起動」（P.19-11）を参照し、モジュールをインストールした後でこの手順をもう一度実行してください。

手順の詳細

	コマンド	目的
ステップ 1	「ASA からモジュールへのセッションの開始」（P.19-10）に従って、IPS モジュールへのセッションを開始します。	
ステップ 2	セットアップ **例：** `sensor# setup`	ASA IPS モジュールの初期設定用のセットアップ ユーティリティを実行します。基本設定を求めるプロンプトが表示されます。デフォルト ゲートウェイについては、アップストリーム ルータの IP アドレスを指定します。ネットワークの要件については、「ASA IPS 管理インターフェイスの接続」（P.19-7）を参照してください。ASA の管理 IP アドレスのデフォルト設定は機能しません。

ASA IPS モジュールでのセキュリティ ポリシーの設定

この項では、ASA IPS モジュール アプリケーションを設定する方法について説明します。

手順の詳細

ステップ 1　次のいずれかの方法を使用して ASA IPS モジュール CLI にアクセスします。

- ASA から ASA IPS モジュールへのセッションを開始します。「ASA からモジュールへのセッションの開始」（P.19-10）を参照してください。
- SSH を使用して IPS 管理インターフェイスに接続します。変更していなければ、デフォルトの管理 IP アドレスは 192.168.1.2 です。デフォルトのユーザ名は **cisco**、デフォルトのパスワードは **cisco** です。管理インターフェイスの詳細については、「管理アクセスに関する情報」（P.19-4）を参照してください。

ステップ 2　IPS のマニュアルに従って IPS セキュリティ ポリシーを設定します。

IPS に関連するすべてのドキュメントを利用するには、http://www.cisco.com/c/en/us/support/security/ips-4200-series-sensors/products-documentation-roadmaps-list.html にアクセスします。

ステップ 3　仮想センサーを設定する場合は、センサーの 1 つをデフォルトとして指定します。ASA のコンフィギュレーションで仮想センサー名が指定されていない場合は、デフォルト センサーが使用されます。

ステップ 4　ASA IPS モジュールの設定が完了したら、次のコマンドを入力して IPS ソフトウェアを終了します。

```
sensor# exit
```

ASA IPS モジュールへのセッションを ASA から開始した場合は、ASA のプロンプトに戻ります。

次の作業

- マルチ コンテキスト モードの ASA の場合は、「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）を参照してください。
- シングル コンテキスト モードの ASA の場合は、「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）を参照してください。

セキュリティ コンテキストへの仮想センサーの割り当て

ASA がマルチ コンテキスト モードにある場合、1 つまたは複数の IPS 仮想センサーを各コンテキストに割り当てることができます。このようにすると、トラフィックを ASA IPS モジュールに送信するようにコンテキストを設定するときに、そのコンテキストに割り当てられているセンサーを指定できます。そのコンテキストに割り当てられていないセンサーを指定することはできません。コンテキストにセンサーを割り当てない場合は、ASA IPS モジュール上で設定されているデフォルト センサーが使用されます。同じセンサーを複数のコンテキストに割り当てることができます。

（注）　仮想センサーを使用するためにマルチ コンテキスト モードを開始する必要はありません。シングル モードでトラフィック フローごとに異なるセンサーを使用できます。

前提条件

コンテキストの設定の詳細については、一般的な操作のコンフィギュレーション ガイドを参照してください。

手順の詳細

	コマンド	目的
ステップ1	**context** *name* **例：** hostname(config)# context admin hostname(config-ctx)#	設定するコンテキストを識別します。システム実行スペースにこのコマンドを入力します。
ステップ2	**allocate-ips** *sensor_name* [*mapped_name*] [**default**] **例：** hostname(config-ctx)# allocate-ips sensor1 highsec	コンテキストに割り当てるセンサーごとに、このコマンドを入力します。 *sensor _name* 引数は、ASA IPS モジュール上で設定されているセンサー名です。ASA IPS モジュール上で設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**show ips** コマンドを入力することもできます。システム実行スペースで **show ips** コマンドを入力すると、使用可能なすべてのセンサーが表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。ASA IPS モジュールにまだ存在しないセンサー名を指定すると、エラーになりますが、**allocate-ips** コマンドはそのまま入力されます。その名前のセンサーが ASA IPS モジュール上で作成されるまで、コンテキストはセンサーがダウンしていると見なします。 *mapped_name* 引数を、実際のセンサー名の代わりにコンテキストで使用可能なセンサー名のエイリアスとして使用します。マッピング名を指定しない場合、センサー名がコンテキスト内で使用されます。セキュリティのために、コンテキストで使用されているセンサーをコンテキスト管理者に知らせない場合があります。または、コンテキスト コンフィギュレーションを一般化する場合もあります。たとえば、すべてのコンテキストで「sensor1」と「sensor2」という名前のセンサーが使用されるようにする場合に、コンテキスト A ではセンサー「highsec」と「lowsec」を sensor1 と sensor2 にマッピングし、コンテキスト B ではセンサー「medsec」と「lowsec」を sensor1 と sensor2 にマッピングします。 **default** キーワードは、コンテキストごとに 1 つのセンサーをデフォルトのセンサーとして設定します。コンテキスト コンフィギュレーションでセンサー名を指定しない場合、コンテキストではこのデフォルト センサーが使用されます。コンテキストごとに設定できるデフォルト センサーは 1 つのみです。デフォルト センサーを変更する場合は、**no allocate-ips** *sensor_name* コマンドを入力して現在のデフォルト センサーを削除してから、新しいデフォルト センサーを割り当てます。デフォルトとして指定されたセンサーがなく、コンテキスト コンフィギュレーションにもセンサー名が含まれていない場合は、ASA IPS モジュールで指定されたデフォルト センサーがトラフィックに使用されます。
ステップ3	**changeto context** *context_name* **例：** hostname# changeto context customer1 hostname/customer1#	「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）での説明に従って、IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。両方のコンテキストで、センサー名を「ips1」と「ips2」にマッピングしています。コンテキスト A では、sensor1 がデフォルト センサーとして設定されていますが、コンテキスト B ではデフォルトは設定されていないため、ASA IPS モジュールで設定されているデフォルトが使用されます。

```
hostname(config-ctx)# context A
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1 default
hostname(config-ctx)# allocate-ips sensor2 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# allocate-ips sensor1 ips1
hostname(config-ctx)# allocate-ips sensor3 ips2
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver

hostname(config-ctx)# changeto context A
...
```

次の作業

IPS セキュリティ ポリシーを設定するには各コンテキストに切り替えます（「ASA IPS モジュールへのトラフィックの誘導」（P.19-16）で説明されています）。

ASA IPS モジュールへのトラフィックの誘導

この項では、ASA から ASA IPS モジュールに誘導するトラフィックを指定します。

前提条件

マルチ コンテキスト モードでは、各コンテキスト実行スペースでこれらの手順を実行します。コンテキストに変更するには、**changeto context** *context_name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	**class-map** *name* **例：** `hostname(config)# class-map ips_class`	ASA IPS モジュールに送信するトラフィックを指定するためのクラス マップを作成します。 ASA IPS モジュールに複数のトラフィック クラスを送信する場合は、セキュリティ ポリシーで使用するための複数のクラス マップを作成できます。
ステップ 2	**match** *parameter* **例：** `hostname(config-cmap)# match access-list ips_traffic`	クラス マップのトラフィックを指定します。詳細については、「トラフィックの特定（レイヤ 3/4 クラス マップ）」（P.1-14）を参照してください。
ステップ 3	**policy-map** *name* **例：** `hostname(config)# policy-map ips_policy`	クラス マップ トラフィックで実行するアクションを設定するポリシー マップを追加または編集します。
ステップ 4	**class** *name* **例：** `hostname(config-pmap)# class ips_class`	ステップ 1 で作成したクラス マップを識別します。

	コマンド	目的
ステップ 5	**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **例：** `hostname(config-pmap-c)# ips promiscuous fail-close`	トラフィックが ASA IPS モジュールに送信されるように指定します。 **inline** キーワードと **promiscuous** キーワードは、ASA IPS モジュールの動作モードを制御します。詳細については、「動作モード」（P.19-3）を参照してください。 **fail-close** キーワードを指定すると、ASA IPS モジュールが使用できない場合はすべてのトラフィックをブロックするように ASA が設定されます。 **fail-open** キーワードを指定すると、ASA IPS モジュールが使用できない場合はすべてのトラフィックを検査なしで通過させるように ASA が設定されます。 仮想センサーを使用する場合、**sensor** *sensor_name* 引数を使用してセンサー名を指定できます。使用可能なセンサー名を表示するには、**ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} **sensor ?**コマンドを使用します。使用可能なセンサーの一覧が表示されます。また、**show ips** コマンドを使用することもできます。ASA でマルチ コンテキスト モードを使用する場合、コンテキストに割り当てたセンサーだけを指定できます（「セキュリティ コンテキストへの仮想センサーの割り当て」（P.19-14）を参照）。コンテキストで設定する場合は、*mapped_name* を使用します。センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングル モードの場合や、マルチ モードでデフォルト センサーが指定されていない場合は、ASA IPS モジュールで設定されているデフォルト センサーがトラフィックに使用されます。入力した名前がまだ ASA IPS モジュール上に存在しない場合は、エラーとなり、コマンドは拒否されます。
ステップ 6	（任意） **class** *name2* **例：** `hostname(config-pmap)# class ips_class2`	IPS トラフィックに複数のクラス マップを作成した場合、ポリシーに対して別のクラスを指定できます。 ポリシー マップ内でのクラスの順番が重要であることの詳細については、「サービス ポリシー内の機能照合」（P.1-5）を参照してください。トラフィックを同じアクション タイプの複数のクラス マップに一致させることはできません。そのため、ネットワーク A を sensorA に進ませ、それ以外のすべてのトラフィックを sensorB に進ませる場合、まずネットワーク A に対して **class** コマンドを入力してから、すべてのトラフィックに対して **class** コマンドを入力する必要があります。このようにしないと、ネットワーク A を含むすべてのトラフィックが最初の **class** コマンドに一致して、sensorB に送信されます。

	コマンド	目的
ステップ 7	（任意） **ips** {**inline** | **promiscuous**} {**fail-close** | **fail-open**} [**sensor** {*sensor_name* | *mapped_name*}] **例：** hostname(config-pmap-c)# ips promiscuous fail-close	トラフィックの 2 番目のクラスが ASA IPS モジュールに送信されるように指定します。 これらのステップを繰り返して、必要な数のクラスを追加します。
ステップ 8	**service-policy** *policymap_name* {**global** | **interface** *interface_name*} **例：** hostname(config)# service-policy tcp_bypass_policy outside	1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。**global** はポリシー マップをすべてのインターフェイスに適用し、**interface** は 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

ASA IPS モジュールの管理

この項には、モジュールのリカバリやトラブルシューティングに役立つ手順が含まれます。

- 「モジュール上でのイメージのインストールおよび起動」（P.19-19）
- 「モジュールのシャットダウン」（P.19-21）
- 「ソフトウェア モジュール イメージのアンインストール」（P.19-21）
- 「パスワードのリセット」（P.19-22）
- 「モジュールのリロードまたはリセット」（P.19-22）

モジュール上でのイメージのインストールおよび起動

モジュールに障害が発生して、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、TFTP サーバから（ハードウェア モジュールの場合）、またはローカル ディスク（ソフトウェア モジュールの場合）から、モジュール上に新しいイメージを再インストールできます。

（注） モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。

前提条件

- ハードウェア モジュール：指定する TFTP サーバが、最大 60 MB のファイルを転送できることを確認してください。

（注） ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

- ソフトウェア モジュール：この手順を実行する前に、イメージを ASA 内部フラッシュ（disk0）にコピーします。

（注）　IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリの最低 50% が空いていることを確認します。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

手順の詳細

	コマンド	目的

ステップ 1	ハードウェア モジュール（例：ASA 5585-X）の場合：
	hw-module module 1 recover configure
	ソフトウェア モジュール（例：ASA 5545-X）の場合：
	sw-module module ips recover configure image disk0:*file_path*
	例：
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		新しいイメージの場所を指定します。
		ハードウェア モジュールの場合：このコマンドを実行すると、TFTP サーバの URL、管理インターフェイスの IP アドレスとネットマスク、ゲートウェイ アドレスの入力を求めるプロンプトが表示されます。これらのネットワーク パラメータは ROMMON で設定されます。モジュール アプリケーション コンフィギュレーションで設定したネットワーク パラメータは ROMMON には使用できないため、ここで別個に設定する必要があります。
		ソフトウェア モジュールの場合：ローカル ディスク上のイメージの場所を指定します。
		リカバリ コンフィギュレーションを表示するには、**show module {1 | ips} recover** コマンドを使用します。
		マルチ コンテキスト モードでは、システム実行スペースでこのコマンドを入力します。

ステップ 2	ハードウェア モジュールの場合： **hw-module module 1 recover boot** ソフトウェア モジュールの場合： **sw-module module ips recover boot** **例：** `hostname# hw-module module 1 recover boot`	IPS モジュール ソフトウェアをインストールして起動します。
ステップ 3	ハードウェア モジュールの場合： **show module 1 details** ソフトウェア モジュールの場合： **show module ips details** **例：** `hostname# show module 1 details`	イメージ転送とモジュール再起動のプロセスの進捗を確認します。 出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

モジュールのシャットダウン

モジュール ソフトウェアをシャットダウンするのは、コンフィギュレーション データを失うことなく安全にモジュールの電源をオフにできるように準備するためです。**注**：ASA をリロードする場合は、モジュールは自動的にはシャットダウンされないので、ASA のリロード前にモジュールをシャットダウンすることを推奨します。モジュールをグレースフル シャットダウンするには、ASA CLI で次の手順を実行します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 shutdown** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips shutdown** **例：** `hostname# hw-module module 1 shutdown`	モジュールをシャットダウンします。

ソフトウェア モジュール イメージのアンインストール

ソフトウェア モジュール イメージおよび関連するコンフィギュレーションをアンインストールするには、次の手順を実行します。

手順の詳細

	コマンド	目的

ステップ 1	**sw-module module ips uninstall**
	
	例：
	`hostname# sw-module module ips uninstall`
	`Module ips will be uninstalled.This will completely remove the`
	`disk image associated with the sw-module including any configuration`
	`that existed within it.`
	
	`Uninstall module <id>?[confirm]`
		ソフトウェア モジュール イメージおよび関連するコンフィギュレーションを永続的にアンインストールします。

ステップ 2	**reload** **例：** `hostname# reload`	ASA をリロードします。新しいモジュール タイプをインストールする前に、ASA をリロードする必要があります。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。ユーザ **cisco** のデフォルトのパスワードは **cisco** です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュールのパスワードをデフォルトの「cisco」にリセットするには、次の手順を実行します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 password-reset** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips password-reset** **例：** `hostname# hw-module module 1 password-reset`	ユーザ **cisco** のモジュール パスワードを **cisco** にリセットします。

モジュールのリロードまたはリセット

モジュールをリロードまたはリセットするには、ASA CLI で次のいずれかのコマンドを入力します。

手順の詳細

コマンド	目的
ハードウェア モジュール（例：ASA 5585-X）の場合： **hw-module module 1 reload** ソフトウェア モジュール（例：ASA 5545-X）の場合： **sw-module module ips reload** **例：** `hostname# hw-module module 1 reload`	モジュール ソフトウェアをリロードします。
ハードウェア モジュールの場合： **hw-module module 1 reset** ソフトウェア モジュールの場合： **sw-module module ips reset** **例：** `hostname# hw-module module 1 reset`	リセットを実行してから、モジュールをリロードします。

ASA IPS モジュールのモニタリング

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

コマンド	目的
show module	ステータスを表示します。
show module {**1** | **ips**} **details**	ステータスの追加情報を表示します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **ips** を指定します。
show module {**1** | **ips**} **recover**	イメージをモジュールに転送するためのネットワーク パラメータを表示します。ハードウェア モジュールの場合は **1**、ソフトウェア モジュールの場合は **ips** を指定します。

例

次に、**show module details** コマンドの出力例を示します。この出力の内容は、SSC がインストールされている ASA に関する追加情報です。

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Card-5
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App.Name: IPS
App.Status: Up
App.Status Desc: Not Applicable
App.Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
                  209.165.202.158/32
                  209.165.200.254/24
Mgmt Vlan: 20
```

ASA 5525-X に IPS SSP ソフトウェア モジュールがインストールされている場合の **show module ips** コマンドの出力例を次に示します。

```
hostname# show module ips
Mod Card Type                                    Model           Serial No.
--- -------------------------------------------- --------------------------
ips IPS 5525 Intrusion Protection System         IPS5525         FCH1504V03P

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
ips 503d.e59c.6f89 to 503d.e59c.6f89  N/A          N/A          7.1(1.160)E4

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------------------------------------
ips IPS                            Up               7.1(1.160)E4

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
ips Up                 Up
```

```
Mod License Name      License Status  Time Remaining
--- ----------------- --------------- ---------------
ips IPS Module        Enabled         7 days
```

ASA IPS モジュールの設定例

次の例では、すべての IP トラフィックが ASA IPS モジュールに無差別モードで誘導され、何らかの理由で ASA IPS モジュール カードに障害が発生した場合はすべての IP トラフィックがブロックされます。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが AIP SSM にインライン モードで誘導され、何らかの理由で AIP SSM に障害が発生した場合は、すべてのトラフィックの通過が許可されます。my-ips-class トラフィックにはセンサー 1 が使用され、my-ips-class2 トラフィックにはセンサー 2 が使用されます。

```
hostname(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
hostname(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list my-ips-acl
hostname(config)# class-map my-ips-class2
hostname(config-cmap)# match access-list my-ips-acl2
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-open sensor sensor1
hostname(config-pmap)# class my-ips-class2
hostname(config-pmap-c)# ips inline fail-open sensor sensor2
hostname(config-pmap-c)# service-policy my-ips-policy interface outside
```

ASA IPS モジュールの機能履歴

表 19-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 19-2　ASA IPS モジュールの機能履歴

機能名	プラットフォーム リリース	機能情報
AIP SSM	7.0(1)	ASA 5510、5520、および 5540 対応の AIP SSM のサポートが導入されました。 **ips** コマンドが導入されました。
仮想センサー（ASA 5510 以降）	8.0(2)	仮想センサーのサポートが導入されました。仮想センサーを使用すると ASA IPS モジュール上で複数のセキュリティ ポリシーを設定できます。 **allocate-ips** コマンドが導入されました。
ASA 5505 用 AIP SSC	8.2(1)	ASA 5505 対応の AIP SSC のサポートが導入されました。 **allow-ssc-mgmt**、**hw-module module ip**、および **hw-module module allow-ip** コマンドが導入されました。
ASA 5585-X 対応の ASA IPS SSP-10、-20、-40、および -60 のサポート	8.2(5)/ 8.4(2)	ASA 5585-X 対応の ASA IPS SSP-10、-20、-40、および -60 のサポートが導入されました。ASA IPS SSP をインストールできるのは、SSP のレベルが一致する場合だけです（たとえば、SSP-10 と ASA IPS SSP-10）。 **（注）** ASA 5585-X はバージョン 8.3 ではサポートされていません。

表 19-2　ASA IPS モジュールの機能履歴（続き）

機能名	プラットフォームリリース	機能情報
SSP-40 および SSP-60 対応のデュアル SSP のサポート	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。 **（注）** 2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。 **show module**、**show inventory**、**show environment** の各コマンドが変更されました。
ASA 5512-X ～ ASA 5555-X に対する ASA IPS SSP のサポート	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X に対する ASA IPS SSP ソフトウェア モジュールのサポートが導入されました。 **session**、**show module**、**sw-module** の各コマンドが導入または変更されました。