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

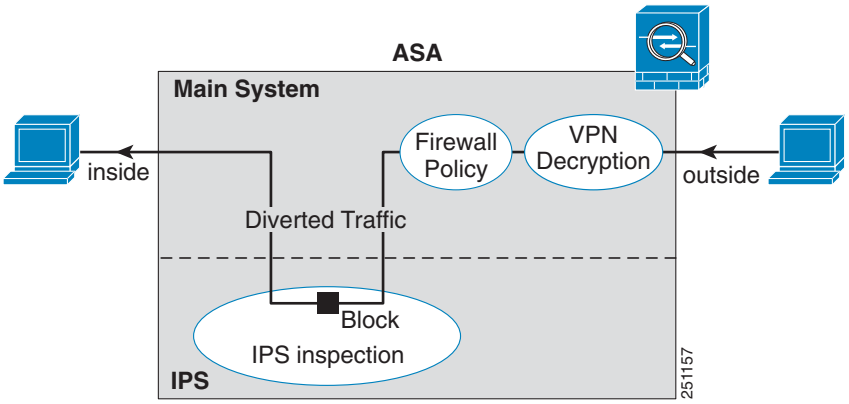
ASA IPS モジュールは、ASA とは別のアプリケーションを実行します。ASA IPS モジュールに外部管理インターフェイスが搭載されている場合は、ASA IPS モジュールに直接接続することができます。管理インターフェイスが搭載されていない場合は、ASA インターフェイスを介して ASA IPS モジュールに接続できます。ASA 5585-X 上の ASA IPS SSP にはデータ インターフェイスが含まれます。このインターフェイスによって、ASA のポート密度が増加します。ただし、ASA の全体的なスループットは増加しません。

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.20-2）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 20-1 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 20-1　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



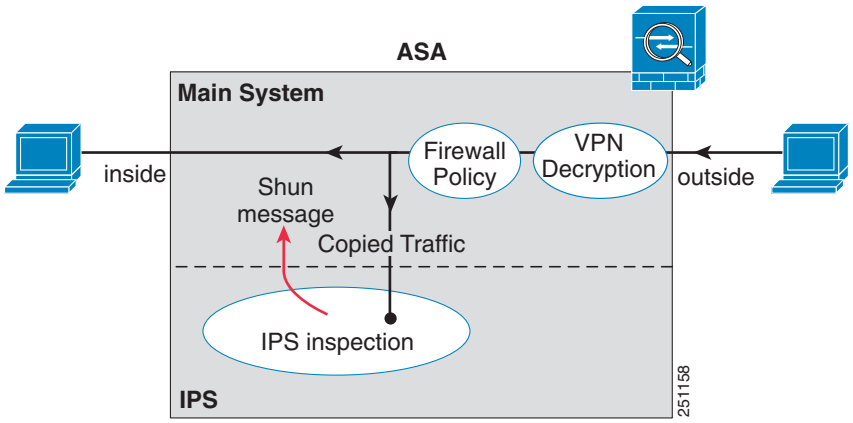
動作モード

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 20-1 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 20-2 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 20-2　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 20-3 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 20-3　　セキュリティ コンテキストと仮想センサー

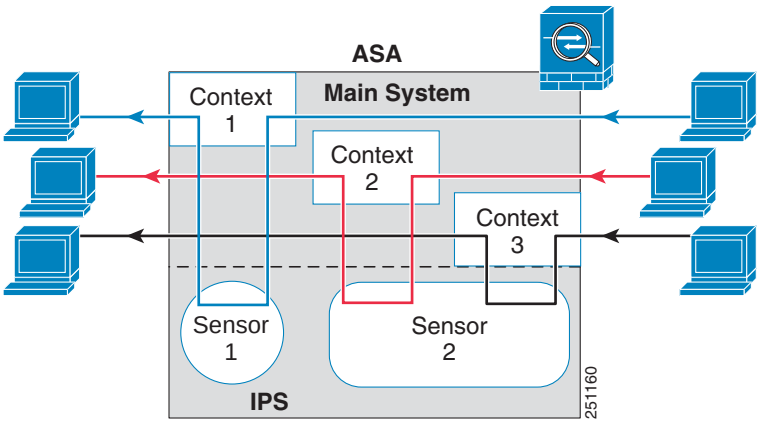
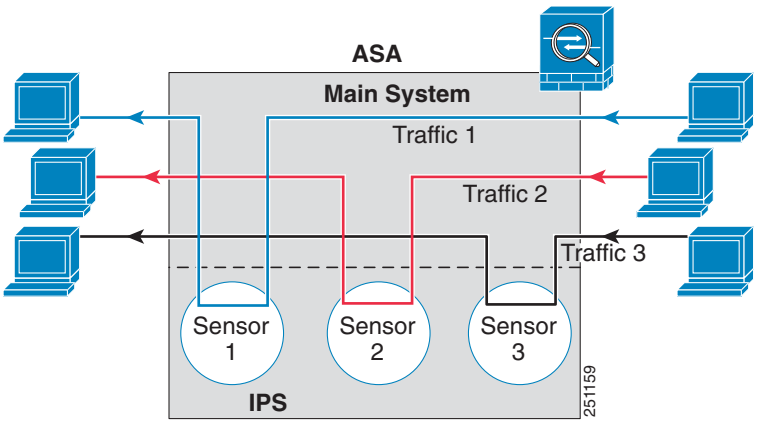


図 20-4 では、シングル モードの ASA が複数の仮想センサー（インライン モード）とペアになっています。定義されている各トラフィック フローは異なるセンサーに進みます。

図 20-4　　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（必要な場合がある）」（P.20-10）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 20-1 に、ASA IPS モジュールのデフォルト設定値を示します。

表 20-1　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.20-7）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。ASDM ユーザの場合は、IPS ソフトウェアを実行していない場合、モジュールへのセッションを開始して IPS ソフトウェアを起動する必要がある場合があります。「ASA からモジュールへのセッションの開始（必要な場合がある）」（P.20-10）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.20-11）を参照してください。

ステップ 4　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.20-13）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.20-14）を参照してください。

ステップ 6　（オプション）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.20-16）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.20-17）を参照してください。

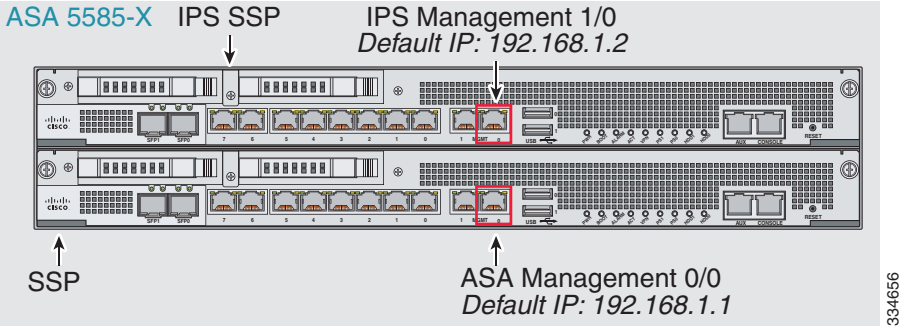
ASA IPS 管理インターフェイスの接続

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）」（P.20-8）
- 「ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）」（P.20-9）

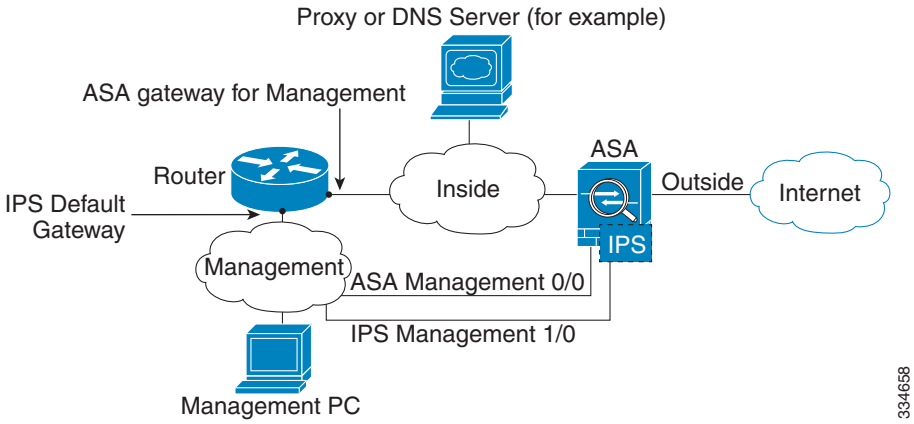
ASA 5585-X（ハードウェア モジュール）

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。



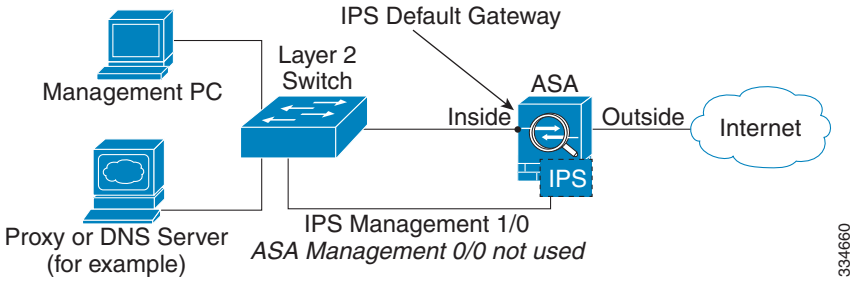
内部ルータがある場合

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。



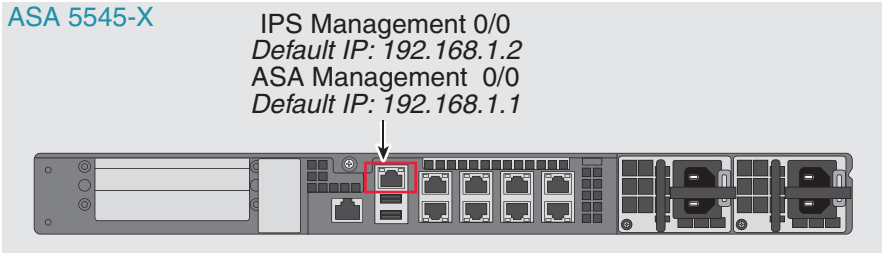
内部ルータがない場合

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。



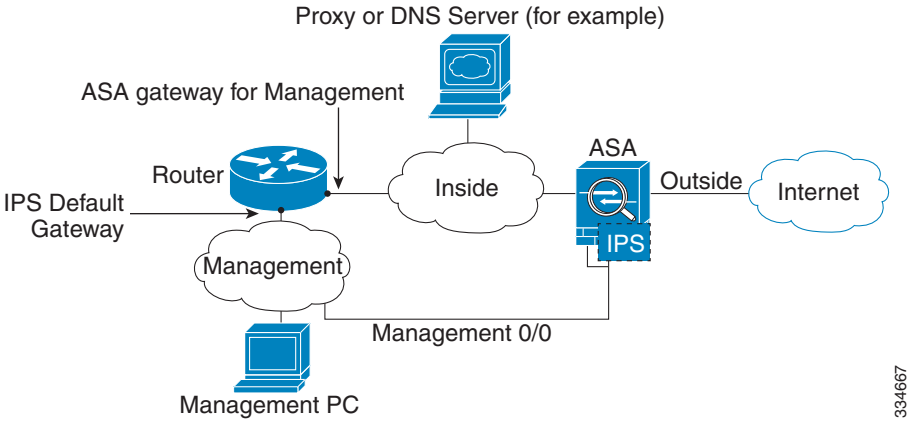
ASA 5512-X ～ ASA 5555-X（ソフトウェア モジュール）

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。



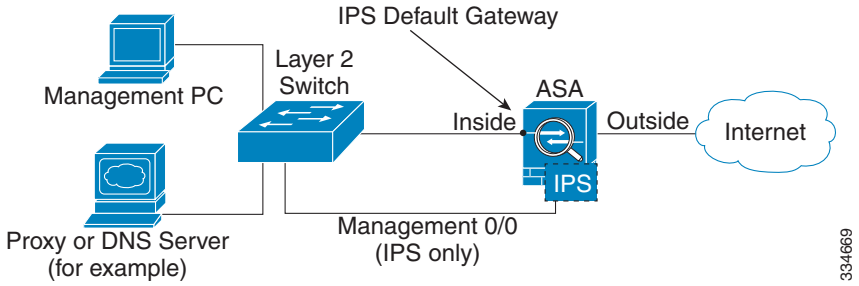
内部ルータがある場合

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行います。「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）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（必要な場合がある）

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。

マルチ コンテキスト モードを使用している場合は、CLI にアクセスする必要があり、CLI を使用している場合、またはトラブルシューティングには基本的なネットワーク設定を設定する必要があります。

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であるか不明な場合は、起動ウィザードの実行時に [IPS Basic Configuration] 画面が表示されません（「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）を参照）。

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、[Tools] > [File Management] を選択します。

  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 からコンピュータ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

  [Tools] > [File Management] を選択し、[File Transfer] > [Between Local PC and Flash] を選択して、新しいイメージを disk0 にアップロードします。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。

ステップ 2　[Tools] > [Command Line Interface] を選択します。

ステップ 3　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、[Send] をクリックします。

```
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。

```
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 4　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、[Send] をクリックします。

```
sw-module module ips recover boot
```

ステップ 5　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、[Send] をクリックします。

```
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

シングル コンテキスト モードでは、ASDM で起動ウィザードを使用して、基本的な IPS ネットワーク設定を行うことができます。これらの設定は、ASA コンフィギュレーションではなく、IPS コンフィギュレーションに保存されます。

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）[IPS Basic Configuration] 画面がウィザードに表示されない場合は、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.20-11）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：シングル モード

ステップ 1　[Wizards] > [Startup Wizard] を選択します。

ステップ 2　[IPS CX Basic Configuration] 画面が表示されるまで、[Next] をクリックして、初期画面から進みます。

ステップ 3　[Network Settings] 領域で、次の設定を行います。

- [IP Address]：管理 IP アドレス。デフォルトのアドレスは 192.168.1.2 です。
- [Subnet Mask]：管理 IP アドレスのサブネット マスク。
- [Gateway]：アップストリーム ルータの IP アドレス。ネクスト ホップ ルータの IP アドレス。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.20-7）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。
- [HTTP Proxy Server]：（オプション）HTTP プロキシ サーバのアドレス。インターネット経由でダウンロードする代わりに、グローバル相関の更新やその他の情報をダウンロードするためにプロキシ サーバを使用できます。
- [HTTP Proxy Port]：（オプション）HTTP プロキシ サーバのポート。
- [DNS Primary]：（オプション）プライマリ DNS サーバのアドレス。DNS サーバを使用している場合は、グローバル相関更新に正常に到達できる DNS サーバを少なくとも 1 つ設定する必要があります。

  グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。DNS 解決は、グローバル相関更新サーバへのアクセスについてのみサポートされます。

ステップ 4　[Management Access List] 領域に、IPS 管理インターフェイスへのアクセスを許可するホストの IP アドレスとサブネット マスクを入力し、[Add] をクリックします。複数の IP アドレスを追加できます。

ステップ 5　[Cisco Account Password] 領域に、ユーザ名 **cisco** に対するパスワードを設定し、確認のためにもう一度入力します。ユーザ名 **cisco** とこのパスワードは、管理アクセス リストで指定されたホストからの Telnet セッションと ASDM（[Configuration] > [IPS]）から IPS モジュールへのアクセス時に使用されます。デフォルトのパスワードは、**cisco** です。

ステップ 6　IPS モジュールを SensorBase データ共有に参加させるために使用する [Network Participation] 領域で、[Full]、[Partial]、または [Off] をクリックします。

手順の詳細：CLI を使用するマルチ モード

	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（必要な場合がある）」（P.20-10）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	**setup** **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.20-7）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。

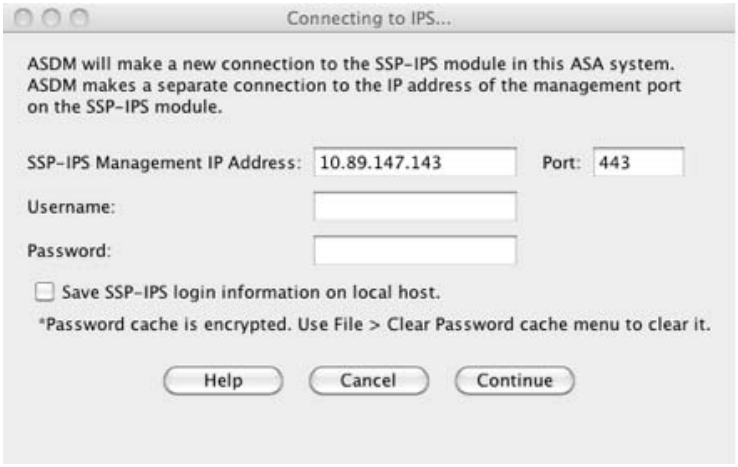
ASA IPS モジュールでのセキュリティ ポリシーの設定

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　*ASA* の管理 IP アドレスを使用して、ASDM に接続します。

ステップ 2　ASDM から IPS Device Manager（IDM）にアクセスするには、[Configuration] > [IPS] をクリックします。



ステップ 3　「IPS モジュールの基本的なネットワーク設定値の設定」（P.20-13）で設定した IP アドレス、ユーザ名、およびパスワードを、ポートとともに入力します。デフォルトの IP アドレスとポートは 192.168.1.2:443 です。デフォルトのユーザ名およびパスワードは、**cisco** と **cisco**.です。

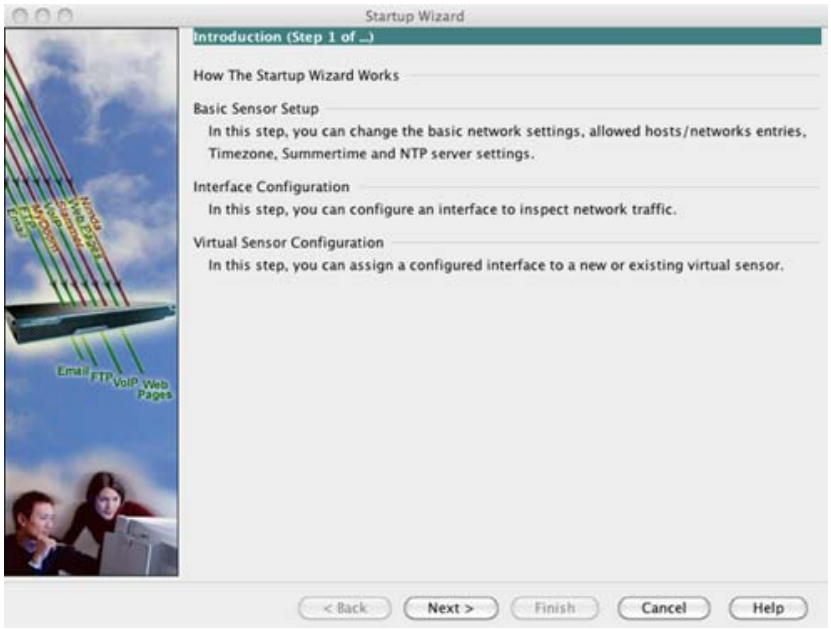
IDM にアクセスするためのパスワードがわからない場合は、ASDM を使用してパスワードをリセットできます。詳細については、「パスワードのリセット」（P.20-22）を参照してください。

ステップ 4　お使いのローカル PC にログイン情報を保存するには、[Save IPS login information on local host] チェックボックスをオンにします。

ステップ 5　[Continue] をクリックします。

[Startup Wizard] ペインが表示されます。

ステップ 6　[Launch Startup Wizard] をクリックします プロンプトに従って画面を完了します。詳細については、IDM オンライン ヘルプを参照してください。



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 シリーズが、そのコンフィギュレーションで仮想センサー名を指定しない場合は、デフォルト センサーが使用されます。

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.20-16）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.20-17）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

ステップ 1　[ASDM Device List] ペインで、アクティブなデバイスの IP アドレスの下にある [System] をダブルクリックします。

ステップ 2　[Context Management] > [Security Contexts] ペインで、設定するコンテキストを選択し、[Edit] をクリックします。

[Edit Context] ダイアログボックスが表示されます。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。

ステップ 3　[IPS Sensor Allocation] 領域で、[Add] をクリックします。

[IPS Sensor Selection] ダイアログボックスが表示されます。

ステップ 4　[Sensor Name] ドロップダウン リストで、ASA IPS モジュールに設定されているものの中からセンサー名を選択します。

ステップ 5　（オプション）センサーにマッピング名を割り当てるには、[Mapped Sensor Name] フィールドに値を入力します。

このセンサー名は、コンテキスト内で実際のセンサー名の代わりに使用できます。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。

ステップ 6　[OK] をクリックして [Edit Context] ダイアログボックスに戻ります。

ステップ 7　（オプション）1 つのセンサーをこのコンテキストのデフォルト センサーとして設定するには、[Default Sensor] ドロップダウン リストからセンサー名を選択します。

コンテキスト コンフィギュレーション内に IPS を設定するときにセンサー名を指定しない場合、コンテキストはデフォルト センサーを使用します。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。デフォルトとしてセンサーを指定せず、コンテキスト コンフィギュレーションにセンサー名が含まれていない場合、トラフィックは ASA IPS モジュールでデフォルト センサーを使用します。

ステップ 8　この手順をセキュリティ コンテキストごとに繰り返します。

ステップ 9　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.20-17）で説明されています）。

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.20-17）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

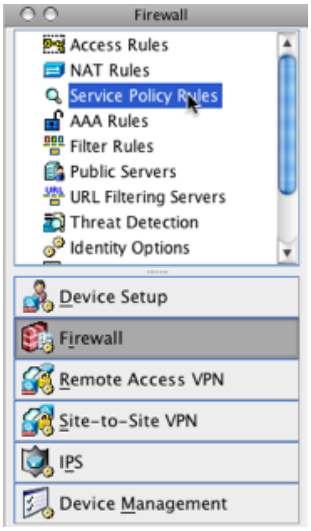
この項では、ASA から ASA IPS モジュールに誘導するトラフィックを指定します。

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、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順の詳細

ステップ 1　[Configuration] > [Firewall] > [Service Policy Rules] の順に選択します。



ステップ 2　[Add] > [Add Service Policy Rule] を選択します。[Add Service Policy Rule Wizard - Service Policy] ダイアログボックスが表示されます。

ステップ 3　必要に応じて [Service Policy] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 4　[Next] をクリックします。[Add Service Policy Rule Wizard - Traffic Classification Criteria] ダイアログボックスが表示されます。

ステップ 5　必要に応じて [Traffic Classification Criteria] ダイアログボックスに入力します。これらの画面の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 6　[Next] をクリックして [Add Service Policy Rule Wizard - Rule Actions] ダイアログボックスを表示します。

ステップ 7　[Intrusion Prevention] タブをクリックします。

ステップ 8　[Enable IPS for this traffic flow] チェックボックスをオンにします。

ステップ 9　[Mode] 領域で、[Inline Mode] または [Promiscuous Mode] をクリックします。詳細については、「動作モード」（P.20-2）を参照してください。

ステップ 10　[If IPS Card Fails] 領域で、[Permit traffic] または [Close traffic] をクリックします。[Close traffic] オプションを選択すると、ASA は ASA IPS モジュールが使用不可の場合にすべてのトラフィックをブロックします。[Permit traffic] オプションを選択すると、ASA は ASA IPS モジュールが使用不可の場合に、すべてのトラフィックの通過を検査なしで許可します。[IPS Sensor Selection] 領域の詳細については、ASDM オンライン ヘルプを参照してください。

ステップ 11　（ASA 5512-X 以降）[IPS Sensor to use] ドロップダウン リストから、仮想センサー名を選択します。

仮想センサーを使用する場合は、このオプションを使用してセンサー名を指定できます。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.20-16）を参照）。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。

ステップ 12　[OK]、続いて [Apply] をクリックします。

ステップ 13　この手順を繰り返して、追加のトラフィック フローを必要に応じて設定します。

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

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。

新しいパスワードで ASDM に接続できない場合は、ASDM を再起動して再度ログインしてみます。新しいパスワードを定義したが、新しいパスワードと異なる既存のパスワードが ASDM にある場合は、[File] > [Clear ASDM Password Cache] を選択して、パスワード キャッシュを消去し、ASDM を再起動して再度ログインしてみます。

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

ステップ 1　ASDM メニューバーの [Tools] > [module Password Reset] を選択します。

[Password Reset] 確認ダイアログ ボックスが開きます。

ステップ 2　パスワードをデフォルトにリセットするには、[OK] をクリックします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

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。

コマンド	目的
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

『一般的な操作のコンフィギュレーション ガイド』の [Intrusion Prevention] タブを参照してください。

ASA IPS モジュールの機能履歴

表 20-2 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 20-2　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。 次の画面が導入されました。[Configuration] > [Firewall] > [Service Policy Rules] > [Add/Edit Service Policy Rule] > [Intrusion Prevention]。
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。 次の画面が変更されました。[Context Management] > [Security Contexts] > [Edit Context]。
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。 次の画面が導入されました。[Configuration] > [Device Setup] > [SSC Setup]。

表 20-2　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
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。
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 つの 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。 変更された画面はありません。
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。 変更された画面はありません。