CHAPTER 39

IPS の設定

この章では、適応型セキュリティ アプライアンスにインストールされている AIP SSM をサポートするように適応型セキュリティ アプライアンスを設定する方法について説明します。

（注） Cisco PIX 500 シリーズ セキュリティ アプライアンスは、SSM をサポートしていません。

この章は、次の項で構成されています。

AIP SSM の概要

ASA 5500 シリーズ適応型セキュリティ アプライアンスに AIP SSM をインストールできます。AIP SSM は、予防的なフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行し、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。この項では、次のトピックについて取り上げます。

適応型セキュリティ アプライアンスとの AIP SSM の動作

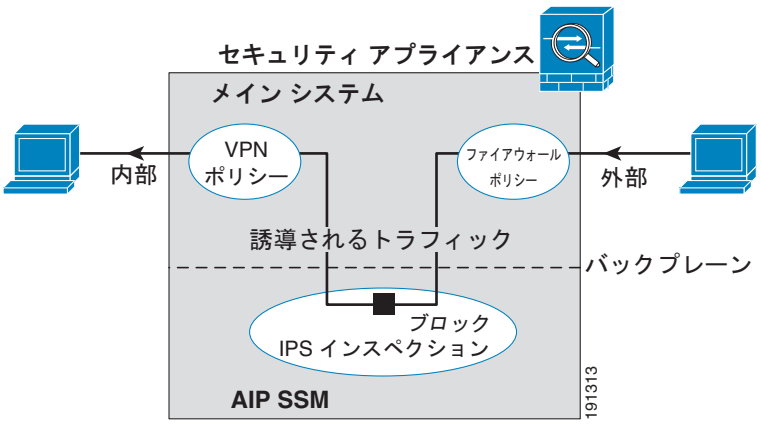
AIP SSM は、適応型セキュリティ アプライアンスとは別のアプリケーションを実行します。ただし、アプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されています。AIP SSM には、管理インターフェイス以外に外部インターフェイス自体は含まれていません。IPS 検査のため適応型セキュリティ アプライアンスでトラフィックを指定する場合、トラフィックは適応型セキュリティ アプライアンスと AIP SSM を通して次のように流れます。

1. トラフィックが適応型セキュリティ アプライアンスに入ります。
2. ファイアウォール ポリシーが適用されます。
3. バックプレーンからトラフィックが AIP SSM に送信されます。

   トラフィックのコピーの AIP SSM への送信だけについては、「動作モード」（P.39-2）を参照してください。
4. AIP SSM が、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。
5. 有効なトラフィックがバックプレーン経由で適応型セキュリティ アプライアンスに返送されます。AIP SSM が、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、そのトラフィックは渡されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが適応型セキュリティ アプライアンスを終了します。

図 39-1 は、AIP SSM をインライン モードで動作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、AIP SSM は攻撃と見なしたトラフィックを自動的にブロックしています。それ以外のトラフィックは、セキュリティ アプライアンスを通って転送されます。

図 39-1　適応型セキュリティ アプライアンスの AIP SSM トラフィック フロー：インライン モード



動作モード

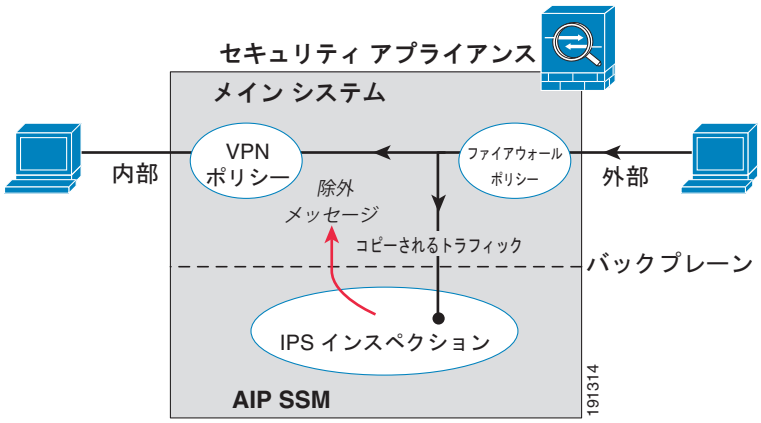
次のいずれかのモードを使用して、トラフィックを AIP SSM に送信できます。

- インライン モード：このモードでは、AIP SSM はトラフィック フローに直接配置されます（図 39-1 を参照）。IPS 検査に指定したトラフィックがセキュリティ アプライアンスを経由するには、まず AIP SSM を通り、その検査を受ける必要があります。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、AIP SSM では、パケットごとにブロッキング 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、トラフィックの重複したストリームが AIP SSM 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、AIP SSM はセキュリティ アプライアンスにトラフィックを回避するか、セキュリティ アプライアンスへの接続をリセットするよう指示することでだけ、トラフィックをブロックできます。また、AIP SSM がトラフィックを分析している間、AIP SSM がトラフィックを回避する前に少量のトラフィックがセキュリティ アプライアンスを通過する場合があります。図 39-2 は無差別モードの AIP SSM を示しています。この例では、AIP SSM は脅威として指定されたトラフィックに対してセキュリティ アプライアンスに回避メッセージを送信します。

図 39-2　適応型セキュリティ アプライアンスの AIP SSM 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 バージョン 6.0 以降を実行している AIP SSM は複数の仮想センサーを実行できます。つまり、AIP SSM で複数のセキュリティ ポリシーを設定できます。各コンテキストまたはシングル モードセキュリティ アプライアンスを 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 39-3 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 39-3　セキュリティ コンテキストと仮想センサー

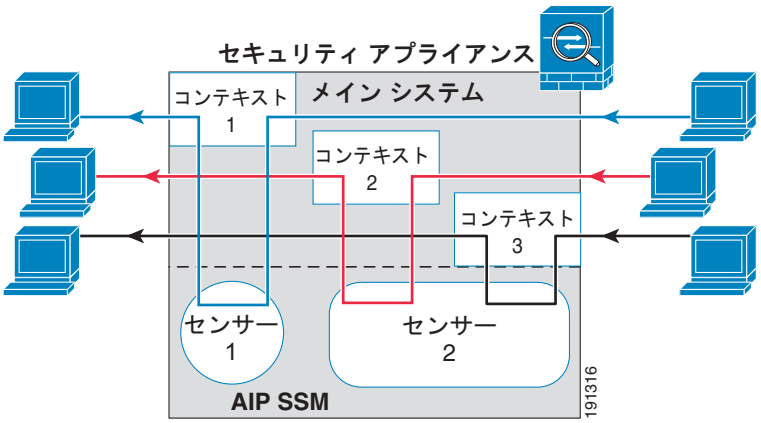
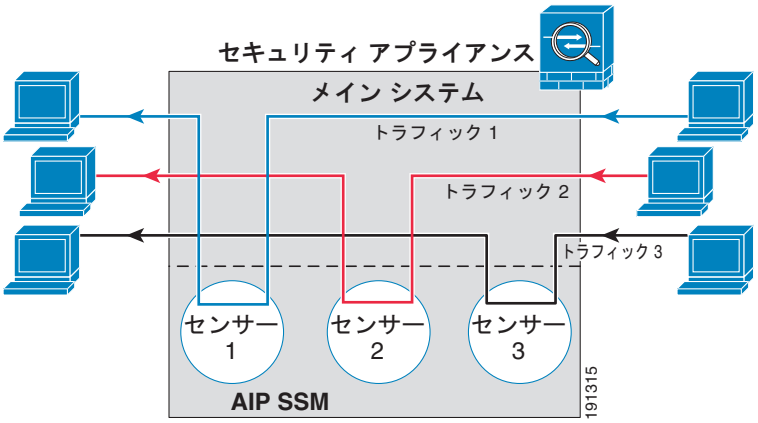


図 39-4 では、シングル モードのセキュリティ アプライアンスが複数の仮想センサー（インライン モード）とペアになっています。定義されている各トラフィック フローは異なるセンサーに進みます。

図 39-4　複数の仮想センサーがあるシングルモードのセキュリティ アプライアンス



AIP SSM 手順の概要

AIP SSM の設定は、AIP SSM を設定してから ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定するプロセスです。

1. ASDM から IDM を起動します。「ASDM からの IDM へのアクセス」（P.39-4）を参照してください。ASDM では、IDM を使用して AIP SSM を設定します。
2. IDM で、インスペクションおよび保護ポリシーを設定します。このポリシーにより、トラフィックの検査方法と侵入が検出された場合の処理が決まります。マルチ センサー モードで AIP SSM を実行する場合は、各仮想センサーに対して検査および保護ポリシーを設定します。「IDM での AIP SSM セキュリティ ポリシーの設定」（P.39-5）を参照してください。
3. マルチ コンテキスト モードで ASA 5500 シリーズ適応型セキュリティ アプライアンスの ASDM を使用して、各コンテキストに使用できる IPS 仮想センサーを指定します（仮想センサーを設定した場合）。「仮想センサーのセキュリティ コンテンツへの割り当て」（P.39-5）を参照してください。

4. ASA 5500 シリーズ適応型セキュリティ アプライアンスの ASDM を使用して、AIP SSM に転送するトラフィックを指定します。「トラフィックの AIP SSM への転送」（P.39-6）を参照してください。

ASDM からの IDM へのアクセス

ASDM では、IDM を使用して AIP SSM を設定します。AIP SSM で IPS バージョン 6.0 以降を実行している場合、ASDM は AIP SSM から IDM を取得して、IDM を ASDM インターフェイスの一部として表示します。IPS ソフトウェアの以前のバージョンでは、IDM は別のブラウザ ウィンドウで起動します。

ASDM から IDM にアクセスするには、[Configuration] > [IPS] をクリックします。

AIP SSM の IP アドレスまたはホスト名の入力を要求されます。

- AIP SSM で IPS バージョン 6.0 以降を実行している場合、ASDM は AIP SSM から IDM を取得して、IDM を ASDM インターフェイスの一部として表示します。AIP SSM のパスワードを入力して [OK] をクリックします。

  ASDM ウィンドウに [IDM] ペインが表示されます。

- AIP SSM が以前のバージョンの IPS ソフトウェアを実行していると、ASDM に IDM へのリンクが表示されます。リンクをクリックして、新しいブラウザ ウィンドウで IDM を起動します。IDM にアクセスするには、ユーザ名とパスワードを入力する必要があります。

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、「AIP SSM パスワードのリセット」（P.39-8）を参照してください。

IDM での AIP SSM セキュリティ ポリシーの設定

AIP SSM で、検査および保護ポリシーを設定します。これにより、トラフィックの検査方法と侵入が検出されたときに行う作業が決まります。IPS バージョン 6.0 以降で仮想センサーを設定する場合、いずれかのセンサーをデフォルトとして指定します。ASA 5500 シリーズセキュリティ アプライアンス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。

AIP SSM で実行される IPS ソフトウェアは、このマニュアルではそれらの機能について説明していないため、詳細な設定情報については IDM オンライン ヘルプを参照してください。IDM オンライン ヘルプは、ASDM に表示される [IDM] ペインで使用できます。また、次の URL にある Cisco.com で IDM および IPS のマニュアルを参照することができます。

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

仮想センサーのセキュリティ コンテンツへの割り当て

セキュリティ アプライアンスがマルチ 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。次に、トラフィックを AIP SSM に送信するようコンテキストを設定する場合、コンテキストに割り当てられるセンサーを指定できます。コンテキストに割り当てなかったセンサーは指定できません。コンテキストにセンサーが割り当てられていない場合は、AIP SSM に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。

1 つまたは複数のセンサーをセキュリティ コンテキストに割り当てるには、次の手順に従います。

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、「セキュリティ コンテキストの設定」（P.9-20）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、AIP SSM に設定されているセンサーの中からセンサー名を選択します。

ステップ 5　（任意）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　（任意）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。センサーをデフォルトとして指定せず、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 AIP SSM のデフォルト 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（「トラフィックの AIP SSM への転送」（P.39-6）で説明されています）。

トラフィックの AIP SSM への転送

セキュリティ アプライアンスから AIP SSM へトラフィックを転送するよう指定するには、次の手順に従います。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。

この機能は、サービス ポリシー ルールを使用してイネーブルにします。サービス ポリシー作成の詳細については、第 23 章「サービス ポリシー ルールの設定」を参照してください。

ステップ 1　[ASDM Device List] ペインで、アクティブなデバイスの [IP address] > [Contexts] の下にあるコンテキスト名をダブルクリックします。

ステップ 2　[Configuration] > [Firewall] > [Service Policy Rules] をクリックします。

ステップ 3　既存のルールを編集する、または新しいルールを作成するには、次の手順を実行します。

- 既存のルールの場合、ルールを選択して [Edit] をクリックします。

  [Edit Service Policy Rule] ダイアログボックスが表示されます。
- 新しいルールの場合、[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。[Service Policy] ダイアログボックスおよび [Traffic Classification Criteria] ダイアログボックスで設定を完了します。詳細については、「通過トラフィックのサービス ポリシー ルールの追加」（P.23-4）を参照してください。[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 4　[Intrusion Prevention] タブをクリックします。

他のタブを使用し、この同じトラフィックに対して他の機能アクションを設定することもできます。

ステップ 5　[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 6　[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.39-2）を参照してください。

ステップ 7　[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、AIP SSM が使用できない場合、適応型セキュリティ アプライアンスはすべてのトラフィックをブロックします。

[Permit traffic] オプションは、AIP SSM が使用できない場合は検査を行わずにすべてのトラフィックの通過を許可するように適応型セキュリティ アプライアンスを設定します。

ステップ 8　（任意）[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。

AIP SSM で仮想センサーを使用する場合、このオプションを使用してセンサー名を指定できます。セキュリティ アプライアンスでマルチ 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（「仮想センサーのセキュリティ コンテンツへの割り当て」（P.39-5）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、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。

ステップ 9　[OK] をクリックします。

[Intrusion Prevention] タブのフィールドの説明

フィールド

- [Enable IPS for this traffic flow]：このトラフィック フローの侵入防御をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このウィンドウの他のパラメータがアクティブになります。
- [Mode]：侵入防御の動作モードを設定します。詳細については、「動作モード」（P.39-2）を参照してください。
  - [Inline Mode]：インライン モードを選択します。このモードでは、パケットを IPS に向けて送ります。パケットは、IPS が動作した結果、ドロップされる場合があります。

  - [Promiscuous Mode]：無差別モードを選択します。このモードでは、元のパケットの複製パケットに対して IPS が作動します。元のパケットはドロップできません。
- [If IPS card fails]：AIP SSM が動作しなくなった場合に実行するアクションを設定します。
  - [Permit traffic]：AIP SSM の障害発生時にトラフィックを許可します。
  - [Close traffic]：AIP SSM の障害発生時にトラフィックをブロックします。
- [IPS Sensor Selection]：このトラフィック フローに使用する仮想センサーを選択します。詳細については、「仮想センサーの使用」（P.39-3）を参照してください。
  - [IPS Sensor to Use]：仮想センサー名を設定します。AIP SSM で仮想センサーを使用する場合、このオプションを使用してセンサー名を指定できます。セキュリティ アプライアンスでマルチ 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（「仮想センサーのセキュリティ コンテンツへの割り当て」（P.39-5）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、またはマルチ モードでデフォルトのセンサーを指定しない場合、トラフィックは AIP SSM に設定されているデフォルトのセンサーを使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

AIP SSM パスワードのリセット

AIP SSM で IPS バージョン 6.0 以降を実行している場合、ASDM を使用して AIP SSM パスワードをデフォルト設定にリセットできます。デフォルトのパスワードは「cisco」（かぎカッコは除く）です。パスワードをリセットしたら、IDM で一意のパスワードに変更する必要があります。ASDM から IDM にアクセスする方法については、「ASDM からの IDM へのアクセス」（P.39-4）を参照してください。

AIP SSM パスワードをリセットすると、AIP SSM が再起動します。AIP SSM の再起動中、IPS サービスは使用できません。

AIP SSM パスワードをデフォルト設定にリセットするには、次の手順を実行します。

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

（注）　SSM がインストールされていないと、このオプションはメニューに表示されません。CSC SSM がインストールされている場合、このオプションは [CSC Password Reset] と表示されます。

[IPS Password Reset] 確認ダイアログボックスが表示されます。

ステップ 2　[OK] をクリックして、AIP SSM パスワードをデフォルト設定にリセットします。

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。パスワードがリセットされなかったときは、適応型セキュリティ アプライアンスでバージョン 7.2(2) 以降のプラットフォーム ソフトウェアを使用していること、および AIP SSM で IPS バージョン 6.0 以降を使用していることを確認してください。

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。