CHAPTER 39

IPS の設定

この章では、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 を使用でき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。

この章には、次の項があります。

AIP SSM の概要

AIP SSM は、ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールできます。AIP SSM は高度な IPS ソフトウェアを実行して全機能を備えた予防型の侵入防護サービスを提供し、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をネットワークに影響を与える前に阻止します。ここでは、次の項目について説明します。

AIP SSM と適応型セキュリティ アプライアンスの連携動作

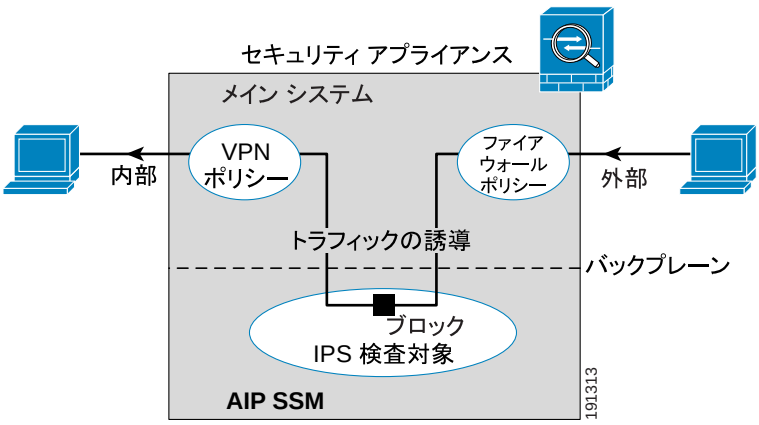
AIP SSM は、適応型セキュリティ アプライアンスとは別のアプリケーションを実行します。ただし、そのアプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されます。AIP SSM 自体には、管理インターフェイス以外に外部インターフェイスは含まれていません。適応型セキュリティ アプライアンスで IPS 検査対象のトラフィックを識別すると、トラフィック フローは適応型セキュリティ アプライアンスと AIP SSM を次のように通過します。

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. トラフィックは、バックプレーンを経由して AIP SSM に送信されます。

   トラフィックのコピーのみを AIP SSM に送信する方法の詳細については、P.39-3 の「動作モード」を参照してください。
4. AIP SSM は、セキュリティ ポリシーをトラフィックに適用し、該当するアクションを実行します。
5. 有効なトラフィックは、バックプレーン経由で再び適応型セキュリティ アプライアンスに送信されます。AIP SSM は、そのセキュリティ ポリシーに従って一部の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。
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 アプライアンスを出ます。

図 39-1 に、インライン モードで AIP SSM を実行するときのトラフィックを示します。この例では、AIP SSM は、攻撃と特定したトラフィックを自動的にブロックします。その他すべてのトラフィックは、セキュリティ アプライアンスを経由して転送されます。

図 39-1　AIP SSM 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：インライン モード

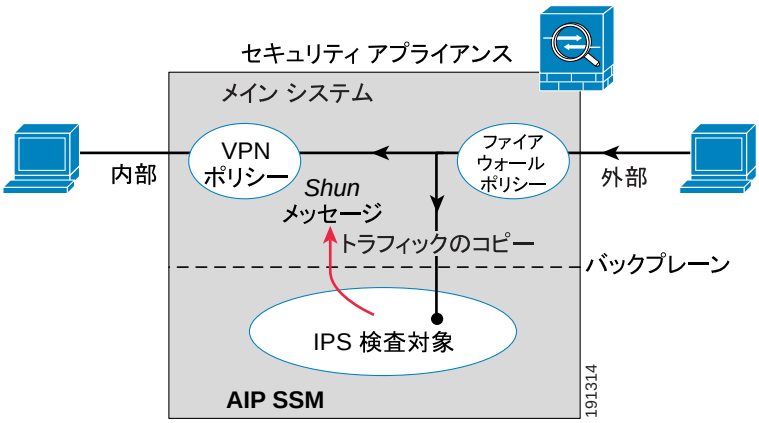


動作モード

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 がトラフィック フロー内に直接置かれます（図 39-1 を参照）。IPS 検査対象として識別されたトラフィックが、続けて適応型セキュリティ アプライアンスを通過するためには、まず、AIP SSM を通過して検査に合格する必要があります。検査対象として識別されたすべてのパケットは分析されてから通過を許可されるため、このモードはきわめてセキュアなモードです。また、AIP SSM は、パケット単位でブロッキング ポリシーを実装することもできます。ただし、このモードはスループットに影響を与える場合があります。
- 無差別モード：このモードでは、トラフィックのストリームを複製して AIP SSM に送信できます。このモードでは、セキュリティは低下しますが、トラフィック スループットには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、無差別モードの AIP SSM がトラフィックをブロックするためには、適応型セキュリティ アプライアンスにトラフィックを除外するように指示するか、適応型セキュリティ アプライアンス上の接続をリセットする必要があります。また、AIP SSM によるトラフィックの分析中、AIP SSM が除外できずに少量のトラフィックが適応型セキュリティ アプライアンスを通過してしまうことがあります。図 39-2 に無差別モードの AIP SSM を示します。この例では、AIP SSM が、脅威と特定したトラフィックについて、除外メッセージをセキュリティ アプライアンスに送信しています。

図 39-2　AIP SSM 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：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。これは、AIP SSM に複数のセキュリティ ポリシーを設定できるということです。各コンテンツまたはシングルモードのセキュリティ アプライアンスを 1 つ以上の仮想センサーに割り当てることができます。または、複数のセキュリティ コンテキストを同一仮想センサーに割り当てることができます。サポートされる最大センサー数を含む、仮想センサーの詳細については、IPS のマニュアルを参照してください。

図 39-3 に、仮想センサーとセキュリティ コンテキストの 1 対 1 の組み合せ（インライン モード）と、同一仮想センサーを共有する 2 つのセキュリティ コンテキストを示します。

図 39-3　セキュリティ コンテキストと仮想センサー

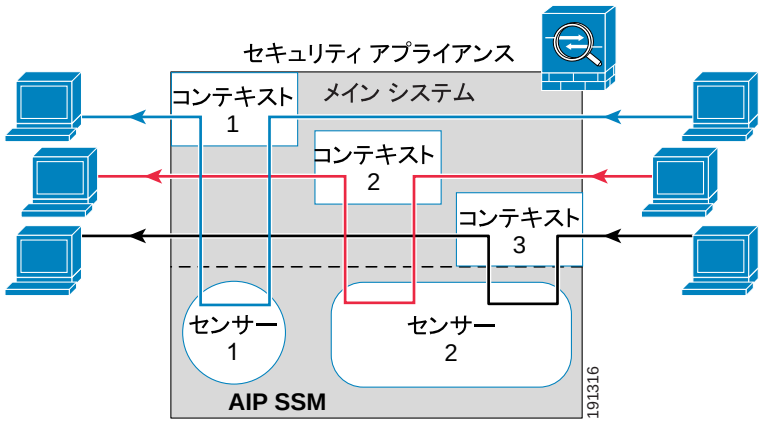
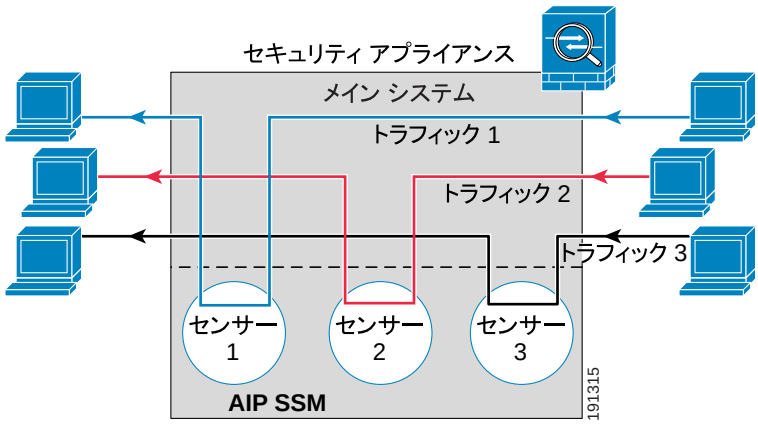


図 39-4 に、シングルモードのセキュリティ アプライアンスと複数の仮想センサーの組み合せ（インライン モード）を示します。定義されたトラフィック フローはそれぞれ別のセンサーに流れます。

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



AIP SSM の手順の概要

AIP SSM を設定するプロセスには、AIP SSM の設定と ASA 5500 シリーズ適応型セキュリティ アプライアンスの設定が含まれます。

1. ASDM から IDM を起動します。P.39-5 の「ASDM からの IDM へのアクセス」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、検査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。AIP SSM を複数センサー モードで実行する場合には、仮想センサーごとに検査および保護ポリシーを設定します。P.39-5 の「IDM での AIP SSM セキュリティ ポリシーの設定」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、コンテキストごとに使用できる IPS 仮想センサーを指定します（仮想センサーが設定されている場合）。P.39-6 の「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」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 に誘導するトラフィックを識別します。P.39-8 の「AIP SSM へのトラフィックの誘導」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 ソフトウェアがそれ以前のバージョンの場合、IDM は別のブラウザ ウィンドウで起動されます。

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場合、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、P.39-10 の「AIP SSM パスワードのリセット」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。IPS バージョン 6.0 以降で仮想センサーを設定している場合、センサーのいずれかをデフォルトとして指定します。ASA 5500 シリーズ適応型セキュリティ アプライアンスのコンフィギュレーションに仮想センサー名が指定されていない場合、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、このマニュアルの対象範囲ではないため、詳細な設定情報は IDM オンライン ヘルプを参照してください。IDM オンライン ヘルプには、ASDM に表示される IDM ペインからアクセスできます。また、次の Web サイトにアクセスし、Cisco.com で IDM と IPS のマニュアルを参照することもできます。

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

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

セキュリティ アプライアンスがマルチコンテキスト モードの場合、各コンテキストに 1 つ以上の IPS 仮想センサーを割り当てることができます。割り当てると、AIP SSM にトラフィックを送信するためのコンテキストを設定するときに、コンテキストに割り当てられているセンサーは指定でき、コンテキストに割り当てられていないセンサーは指定できません。コンテキストにセンサーを割り当てない場合、AIP SSM 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） 仮想センサーを使うためにマルチコンテキスト　モードである必要はありません。シングルモードで、複数のセンサーを複数のトラフィック フローに使用できます。

1 つ以上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、次の手順を実行します。

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** を選択します。

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、P.9-22 の「セキュリティ コンテキストの設定」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 に設定されている仮想センサー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。マッピングされる名を指定しない場合、コンテキスト内でセンサー名が使用されます。セキュリティ上の理由から、コンテキストが使用しているセンサーをコンテキスト管理者に知られたく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の汎用化が必要な場合もあります。たとえば、すべてのコンテキストに「sensor1」および「sensor2」というセンサーを使用する場合、コンテキスト A の sensor1 および sensor2 には「highsec」センサーおよび「lowsec」センサーをマッピングし、一方でコンテキスト B の sensor1 および sensor2 には、「medsec」センサーおよび「lowsec」センサーをマッピングすることができます。

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。1 つのコンテキストに設定できるデフォルト センサーは 1 つだけです。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 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　P.39-8 の「AIP SSM へのトラフィックの誘導」の説明に従って、各コンテキストに変更して IPS セキュリティ ポリシーを設定します。

AIP SSM へのトラフィックの誘導

適応型セキュリティ アプライアンスから AIP SSM に誘導するトラフィックを識別するには、次の手順を実行します。マルチコンテキスト モードの場合は、この手順を各コンテキスト実行スペースで実行します。

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 アドレス* > Contexts の下にあるコンテキスト名をクリックします。

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、P.23-5 の「通過トラフィックのサービス ポリシー ルールの追加」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、P.39-3 の「動作モード」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 オプションは、AIP SSM を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適応型セキュリティ アプライアンスを設定します。

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　（オプション）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、指定できるセンサーは、コンテキストに割り当てたものだけです（P.39-6 の「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」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 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 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 センサーを指定しない場合は、トラフィックは AIP SSM に設定されているデフォルト 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 フローで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、P.39-3 の「動作モード」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、パケットが IPS に転送されます。パケットは、IPS の働きにより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。元のパケットがドロップされることはありません。
- If IPS card fails：AIP SSM が動作不能に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：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、P.39-3 の「仮想センサーの使用」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、指定できるセンサーは、コンテキストに割り当てたものだけです（P.39-6 の「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」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 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 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 センサーを指定しない場合は、トラフィックは AIP SSM に設定されているデフォルト センサーを使用します。

モード

次の表に、この機能を使用できるモードを示します。

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することができます。デフォルトのパスワードは「cisco」（かぎカッコなし）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、P.39-5 の「ASDM からの IDM へのアクセス」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 confirmation 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。