CHAPTER 13

AIP SSM の設定

オプションの AIP SSM は、インライン モードまたは無差別モードでセキュリティ検査を強化する、高度な IPS ソフトウェアを実行します。適応型セキュリティ アプライアンスが AIP SSM にパケットを転送するのは、パケットが出力インターフェイスを通過する直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）と、他のファイアウォール ポリシーが適用された後です。たとえば、アクセスリストによってブロックされたパケットは、AIP SSM に転送されません。

AIP SSM を購入した場合は、この章の手順に従って、次の操作を行います。

- AIP SSM に誘導するトラフィックを特定するための適応型セキュリティ アプライアンスの設定
- AIP SSM へのセッションの接続とセットアップの実行

（注） AIP SSM は、バージョン 7.0(1) 以降の ASA ソフトウェアでサポートされます。

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、事前対応型で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及ぼす前に、これらを阻止します。この章は、次の項で構成されています。

AIP SSM について

この項では、次のトピックについて取り上げます。

AIP SSM と適応型セキュリティ アプライアンスの連携のしくみ

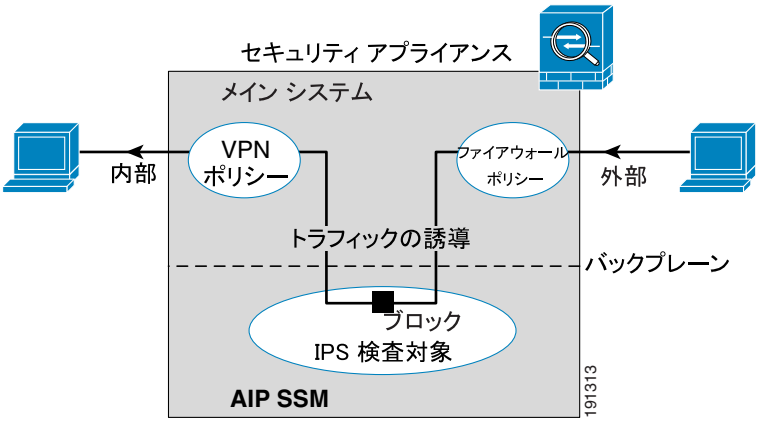
AIP SSM は、適応型セキュリティ アプライアンスとは異なるアプリケーションを実行します。しかし、適応型セキュリティ アプライアンスのトラフィック フローに統合されています。AIP SSM 自体には、管理インターフェイス以外に外部インターフェイスは含まれていません。適応型セキュリティ アプライアンス上で IPS 検査対象のトラフィックが確認されると、トラフィックは、次のように適応型セキュリティ アプライアンスと AIP SSM を流れます。

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. トラフィックはバックプレーン経由で AIP SSM に送信されます。

   トラフィックのコピーだけを AIP SSM に送信する場合の詳細については、P.13-3 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、適切な処理を行います。
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 アプライアンスに戻されます。AIP SSM 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し、そのようなトラフィックは戻されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックは適応型セキュリティ アプライアンスから出ます。

図 13-1 は、AIP SSM がインライン モードで実行されている場合のトラフィック フローを示しています。この例では、AIP SSM 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ています。それ以外のトラフィックは、適応型セキュリティ アプライアンスを通って転送されます。

図 13-1　AIP SSM 適応型セキュリティ アプライアンスにおけるトラフィック フロー：インライン モード



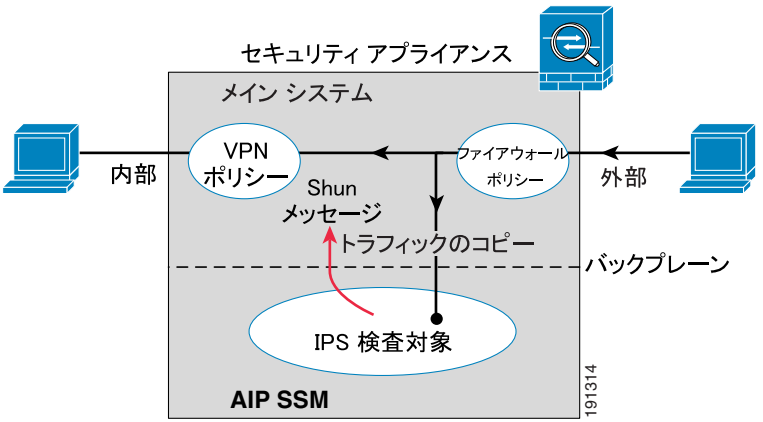
動作モード

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 は直接トラフィック フローに配置されます（図 13-1 を参照してください）。IPS 検査対象と認識されたトラフィックは、まず AIP SSM に渡されて検査を受けないと、適応型セキュリティ アプライアンスを通過することはできません。検査対象と認識されたすべてのパケットが分析されてから通過を許可されるため、このモードは最もセキュアです。また、AIP SSM はパケット別にブロッキング ポリシーを実行できます。ただし、このモードはスループットに影響を及ぼす可能性があります。

- 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 AIP SSM に送信されます。このモードは、安全性は劣りますが、トラフィック スループットへの影響も小さくなります。インライン モードとは異なり、無差別モードでは、AIP SSM がトラフィックをブロックできるのは、適応型セキュリティ アプライアンスに対してトラフィックの shun を指示するか、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した場合だけです。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 shun する前に一部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することが可能です。図 13-2 は、無差別モードの AIP SSM を示しています。この例では、AIP SSM が脅威と見なしたトラフィックについての shun メッセージを適応型セキュリティ アプライアンスに送信しています。

図 13-2　AIP SSM 適応型セキュリティ アプライアンスにおけるトラフィック 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 では、複数の仮想センサーを実行できます。つまり、複数のセキュリティ ポリシーを AIP SSM に設定できます。各コンテキストまたはシングル モードの適応型セキュリティ 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たり、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たりできます。仮想センサーの詳細（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 13-3 では、1 つのセキュリティ コンテキストが 1 つの仮想センサー（インライン モード）と対になり、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 13-3　セキュリティ コンテキストと仮想センサー

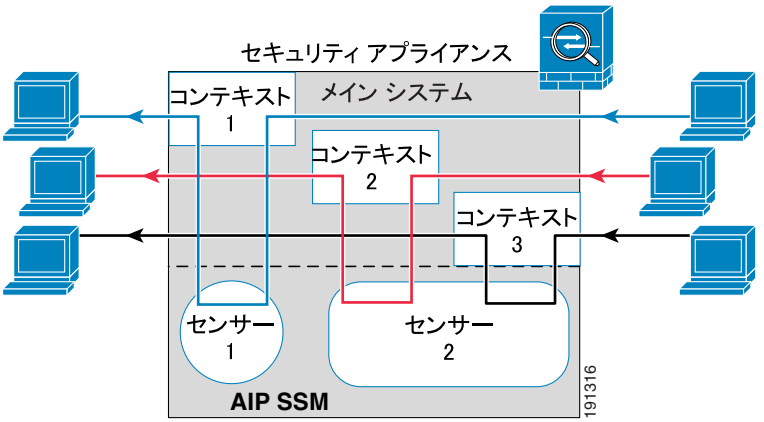
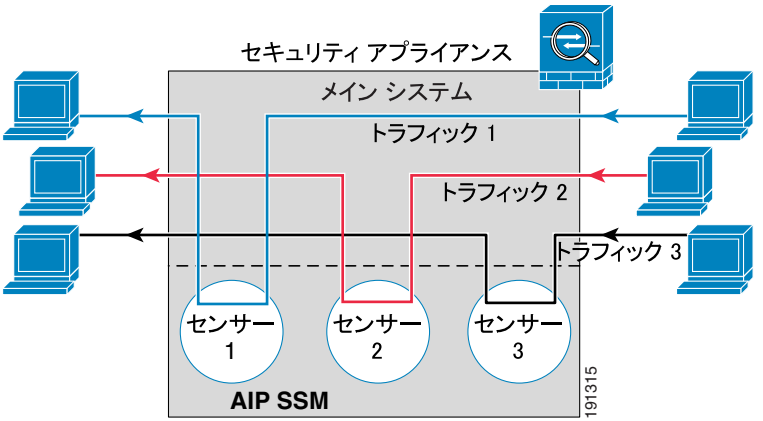


図 13-4 では、シングル モードの適応型セキュリティ アプライアンスが複数の仮想センサー（インライン モード）と対になっています。定義されている各トラフィック フローは、異なるセンサーを進みます。

図 13-4　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 の設定

この項では、次のトピックについて取り上げます。

AIP SSM の手順の概要

AIP SSM の設定は、次に示すように、まず AIP SSM を設定し、次に 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からなります。

1. 適応型セキュリティ アプライアンスから AIP SSM へのセッションを接続します。P.13-8 の「AIP SSM へのセッション接続」を参照してください。
2. AIP SSM では、検査と保護ポリシーを設定することにより、トラフィックの検査方法と侵入検出時の対処を決定します。AIP SSM をマルチ センサー モードで実行する場合は、仮想センサーごとに検査と保護ポリシーを設定します。P.13-10 の「AIP SSM でのセキュリティ 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 モードの ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、各コンテキストに対してどの IPS 仮想センサーが使用可能かを指定します（仮想センサーを設定している場合）。P.13-11 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 アプライアンスでは、AIP SSM に誘導するトラフィックを特定します。P.13-14 の「AIP SSM へのトラフィックの誘導」を参照してください。

AIP SSM へのセッション接続

AIP SSM の設定を開始するには、適応型セキュリティ アプライアンスから AIP SSM にセッションを接続します（あるいは、SSH または Telnet を使用して、直接 AIP SSM 管理インターフェイスに接続します）。

適応型セキュリティ アプライアンスから AIP SSM へのセッションを接続するには、次の手順を実行します。

ステップ 1　ASA 5500 シリーズ適応型セキュリティ アプライアンスから AIP SSM へのセッションを接続するには、次のコマンドを入力します。

```
hostname# session 1

Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 2　ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードは「cisco」です。

（注）　初めて AIP SSM にログインしたときに、デフォルト 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。

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United
States
and local country laws governing import, export, transfer and use.
Delivery
of Cisco cryptographic products does not imply third-party authority
to import,
export, distribute or use encryption. Importers, exporters,
distributors and
users are responsible for compliance with U.S. and local country laws.
By using
this product you agree to comply with applicable laws and regulations.
If you
are unable to comply with U.S. and local laws, return this product
immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

（注） 上記のライセンスの注意が表示された場合（一部のソフトウェア バージョンでのみ表示されます）、AIP SSM でシグニチャ ファイルをアップグレードする必要がなければ、無視してかまいません。有効なライセンス キーがインストールされるまで、AIP SSM は現在のシグニチャ レベルで動作し続けます。ライセンス キーは後でインストールできます。ライセンス キーは、AIP SSM の現在の機能には影響を与えません。

AIP SSM でのセキュリティ ポリシーの設定

AIP SSM で、トラフィックの検査方法と侵入検出時の対処を決定する、検査と保護ポリシーを設定するには、次の手順を実行します。適応型セキュリティ アプライアンスから AIP SSM へのセッションを接続するには、P.13-8 の「AIP SSM へのセッション接続」を参照してください。

ステップ 1　AIP SSM の初期設定のセットアップ ユーティリティを実行するには、次のコマンドを入力します。

```
sensor# setup
```

ステップ 2　IPS セキュリティ ポリシーを設定します。IPS バージョン 6.0 以降で仮想センサーを設定する場合は、センサーのうちの 1 つ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 アプライアンスの設定時に仮想センサー名を指定しなかった場合、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ではないため、詳細な設定情報については、次のマニュアルを参照してください。

- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
- *Command Reference for Cisco Intrusion Prevention System*

ステップ 3　AIP SSM 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
```

適応型セキュリティ アプライアンスから AIP SSM へセッションを接続した場合は、適応型セキュリティ アプライアンスのプロンプトに戻ります。

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

適応型セキュリティ アプライアンスがマルチ コンテキスト モードの場合は、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。この方法を行うと、トラフィックを AIP SSM 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。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かった場合、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。複数のコンテキストに同じセンサーを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 モードにする必要はありません。シングル モードでも、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、次の手順を実行します。

ステップ 1　コンテキスト コンフィギュレーション モードに入るには、システム実行スペースで次のコマンドを入力します。

```
hostname(config)# context name
hostname(config-ctx)#
```

ステップ 2　コンテキストに仮想センサーを割り当てるには、次のコマンドを入力します。

```
hostname(config-ctx)# allocate-ips sensor_name [mapped_name] [default]
```

このコマンドは、コンテキストに割り当てる仮想センサーごとに入力します。

sensor _name 引数は、AIP SSM に設定されているセンサー名です。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** を入力します。使用可能なすべてのセンサーが一覧表示されます。また、**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一覧表示されます。コンテキストでこのコマンドを入力すると、コンテキストに割り当て済みのセンサーが表示されます。まだ AIP SSM に存在しないセンサー名を指定した場合、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。指定した名前のセンサーを AIP SSM に作成するまで、コンテキストはそのセンサーはダウンしていると見なします。

mapped_name 引数は、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。mapped name を指定しなかった場合、センサー名がコンテキストで使用されます。セキュリティのためには、コンテキストでどのセンサーが使用されているかをコンテキスト管理者に知らせない方がいいでしょう。あるいは、コンテキスト設定をジェネリクス化します。たとえば、すべてのコンテキストで「sensor1」および「sensor2」という名前のセンサーを使用する場合、コンテキスト A では「highsec」および「lowsec」センサーを sensor1 および sensor2 にそれぞれマッピングし、コンテキスト B では「medsec」および「lowsec」センサーを sensor1 および sensor2 にそれぞれマッピングします。

default キーワードは、コンテキストごとに 1 つのセンサーを設定するものです。コンテキスト設定でセンサー名が指定されていない場合、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 つだけです。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、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 センサーを指定せず、コンテキスト設定にセンサー名が含まれていない場合、トラフィックでは AIP SSM のデフォルト センサーが使用されます。

ステップ 3　ステップ 1 および ステップ 2 をコンテキストごとに繰り返します。

ステップ 4　コンテキスト IPS ポリシーを設定するには、次のコマンドを使用して、コンテキスト実行スペースに切り替えます。

```
hostname(config-ctx)# changeto context context_name
```

ここで、*context_name* 引数は、設定するコンテキストの名前です。IPS セキュリティ ポリシーを設定するように各コンテキストを変更します（P.13-14 の「AIP SSM へのトラフィックの誘導」を参照してください）。

次の例では、sensor1 と sensor2 がコンテキスト A に割り当てられ、sensor1 と sensor3 がコンテキスト B に割り当てられています。どちらのコンテキストでも、これらのセンサー名を「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 センサーに設定されていますが、コンテキスト B では、デフォルト センサーが設定されていないため、AIP SSM でデフォルトに設定されているセンサーが使用されます。

```
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
...
```

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特定するには、次の手順を実行します。マルチ コンテキスト モードで、各コンテキスト実行スペースで次の手順を実行します。

ステップ 1　AIP SSM で検査を行うトラフィックを特定するには、**class-map** コマンドを使用して 1 つまたは複数のクラス マップを追加します。

たとえば、すべてのトラフィックを一致させるには、次のコマンドを使用します。

```
hostname(config)# class-map IPS
hostname(config-cmap)# match any
```

特定のトラフィックを一致させるには、アクセスリストを一致させます。

```
hostname(config)# access list IPS extended permit ip any 10.1.1.1
255.255.255.255
hostname(config)# class-map IPS
hostname(config-cmap)# match access-list IPS
```

ステップ 2　AIP SSM にトラフィックを誘導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するには、次のコマンドを入力します。

```
hostname(config)# policy-map name
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

ここで、*class_map_name* はステップ 1 のクラス マップです。

次の例を参考にしてください。

```
hostname(config)# policy-map IPS
hostname(config-pmap)# class IPS
```

ステップ 3　トラフィックを AIP SSM に誘導するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor {sensor_name | mapped_name}]
```

inline キーワードおよび ***promiscuous*** キーワードは、AIP SSM の動作モードを制御します。詳細については、P.13-3 の「動作モード」を参照してください。

fail-close キーワードは、AIP SSM が使用不能の場合に、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。

fail-open キーワードは、AIP SSM が使用不能の場合に、すべてのトラフィックが検査なしで通過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。

AIP SSM で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 ... sensor ?** コマンドを入力します。使用可能なセンサーが一覧表示されます。また、**show ips** コマンドも使用できます。適応型セキュリティ 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られているセンサーだけです（P.13-11 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）。コンテキストで設定されている場合は、*mapped_name* を使用します。センサー名を指定しなかった場合、トラフィックではデフォルト センサーが使用されます。マルチ コンテキスト モードでは、デフォルト センサーをコンテキストに指定できます。マルチ モードでデフォルト センサーを指定しなかった場合またはシングル モードの場合は、AIP SSM で設定されているデフォルト センサーがトラフィックで使用されます。まだ AIP SSM に存在しない名前を入力した場合、エラーになり、コマンドは拒否されます。

ステップ 4　（オプション）他のクラスのトラフィックを AIP SSM に誘導し、IPS ポリシーを設定するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# class class_map_name2
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close |
fail-open} [sensor sensor_name]
```

ここで、*class_map_name2* 引数は、IPS 検査を行う別のクラス マップの名前です。コマンド オプションの詳細については、ステップ 3 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 に誘導し、それ以外のすべてのトラフィックは sensorB に誘導する場合、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** コマンドを入力します。この方法をとらないと、すべてのトラフィック（ネットワーク A を含む）が最初の **class** コマンドに一致し、sensorB には送信されません。

ステップ 5　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するには、次のコマンドを入力します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global |
interface interface_ID]
hostname
```

ここで、*policy_map_name* は、ステップ 2 で設定したポリシーマップです。すべてのインターフェイスのトラフィックにポリシーマップを適用するには、**global** キーワードを使用します。特定のインターフェイスのトラフィックにポリシーマップを適用するには、***interface*** *interface_ID* オプションを使用します。ここで、*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てた名前です。

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。

次の例では、すべての IP トラフィックが AIP SSM に無差別モードで誘導され、何らかの理由で AIP SSM 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 ネットワークおよび 10.2.1.0 ネットワーク宛のすべての 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 カード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 sensor1 が使用され、my-ips-class2 トラフィックには sensor2 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
```

次の手順

これで、侵入防止のために適応型セキュリティ アプライアンスを設定する準備ができました。次のマニュアルを参照して、実装に合せて適応型セキュリティ アプライアンスを設定します。

作業内容	参照先
IPS センサーの設定	*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface* *Cisco Intrusion Prevention System Command Reference*
より効率的なサービス ポリシーの作成によるパフォーマンスの最適化	『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」

IPS センサーおよび AIP SSM ソフトウェアを設定した後、次の追加の手順について、実行する必要があるかどうかを検討してください。

作業内容	参照先
設定の調整およびオプション機能と高度な機能の設定	*Cisco Security Appliance Command Line Configuration Guide*
日常のオペレーションの学習	*Cisco Security Appliance Command Reference* *Cisco Security Appliance Logging Configuration and System Log Messages*
ハードウェア メンテナンスおよびトラブルシューティング情報の確認	*Cisco ASA 5500 Series Hardware Installation Guide*

適応型セキュリティ アプライアンスは、複数のアプリケーション用に設定できます。次の項で、その他の一般的なアプリケーション用に適応型セキュリティ アプライアンスを設定する手順を説明します。

作業内容	参照先
DMZ Web サーバの保護の設定	第 8 章「シナリオ：DMZ の設定」
リモートアクセス VPN の設定	第 9 章「シナリオ：IPSec リモートアクセス VPN の設定」
ソフトウェア クライアント用のリモートアクセス SSL 接続の設定	第 10 章「シナリオ：Cisco AnyConnect VPN Client 用の接続の設定」
ブラウザベースのリモートアクセス用の SSL 接続の設定	第 11 章「シナリオ：SSL VPN クライアントレス接続」
サイトツーサイト VPN の設定	第 12 章「シナリオ：サイトツーサイト VPN の設定」

次の手順