CHAPTER 13

AIP SSM の設定

オプションの AIP SSM は、インライン モードまたは混合モードで追加のセキュリティ検査を提供する高度な IPS ソフトウェアを実行します。適応型セキュリティ アプライアンスは、パケットが出力インターフェイスから送信される直前（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）、および他のファイアウォール ポリシーが適用された後に、パケットを AIP SSM に転送します。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 を購入された場合は、この章で示す手順を使用して次の作業を実行します。

- AIP SSM に転送するトラフィックを指定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
- AIP SSM へのセッションを確立し、セットアップを実行する

（注） AIP SSM は、Cisco ASA 5500 シリーズ ソフトウェア バージョン 7.0（1）以降でサポートされています。

AIP SSM を ASA 5500 シリーズ適応型セキュリティ アプライアンスに取り付けられます。AIP SSM は、ワームやネットワーク ウイルスなど悪意があるトラフィックをネットワークに影響を与える前に止めるため、予防的な、フル機能を備えた侵入防御システムを提供する高度な IPS ソフトウェアを実行します。この章は、次の項で構成されています。

AIP SSM について

この項は、次の内容で構成されています。

適応型セキュリティ アプライアンスとの AIP SSM の動作

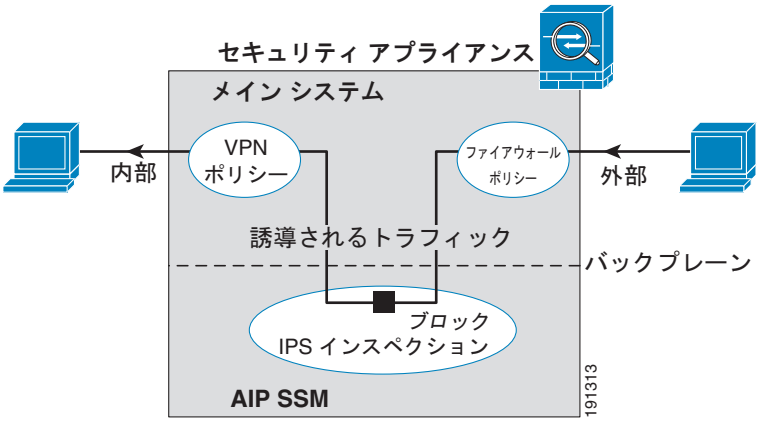
AIP SSM は、適応型セキュリティ アプライアンスから別のアプリケーションを実行します。ただし、そのアプリケーションは適応型セキュリティ アプライアンスのトラフィック フローに統合されます。AIP SSM 自体には、管理インターフェイスを除き、外部インターフェイスは入っていません。IPS 検査のため適応型セキュリティ アプライアンスでトラフィックを指定する場合、トラフィックは適応型セキュリティ アプライアンスと AIP SSM を通して次のように流れます。

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.13-3）を参照してください。
4. AIP SSM はそのセキュリティ ポリシーをトラフィックに適用して、適切な処理を行います。
5. 有効なトラフィックはバックプレーンを通って適応型セキュリティ アプライアンスに返信されます。AIP SSM がそのセキュリティ ポリシーに従ってあるトラフィックをブロックする場合、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 アプライアンスから出ます。

図 13-1 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。その他のトラフィックはすべて適応型セキュリティ アプライアンスを経由して転送されています。

図 13-1　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

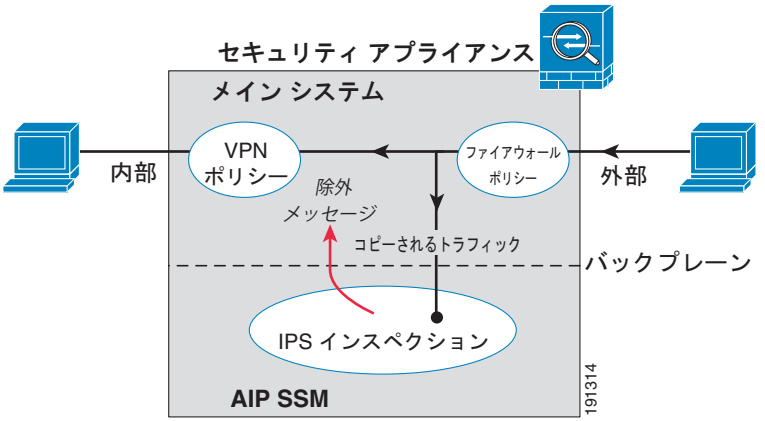


動作モード

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 13-1 を参照）。IPS 検査に指定したトラフィックが適応型セキュリティ 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。検査に指定するあらゆるパケットが通過を許可される前に分析されるため、このモードが最も安全です。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可能性があります。
- 混合モード：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は劣りますが、トラフィックの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、混合モードでは、AIP SSM 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回避するか、適応型セキュリティ 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適応型セキュリティ アプライアンスを通過する場合があります。図 13-2 は混合モードの 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適応型セキュリティ アプライアンスに回避メッセージを送信します。

図 13-2　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: 混合モード



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。1 つまたは複数の仮想センサーに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られます。サポートされている最大センサー数など、仮想センサーの詳細については、IPS マニュアルを参照してください。

図 13-3 は、（インライン モードの）仮想センサー 1 つが 1 つのセキュリティ コンテキストとペアになり、同時に 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るところを示しています。

図 13-3　セキュリティ コンテキストと仮想センサー

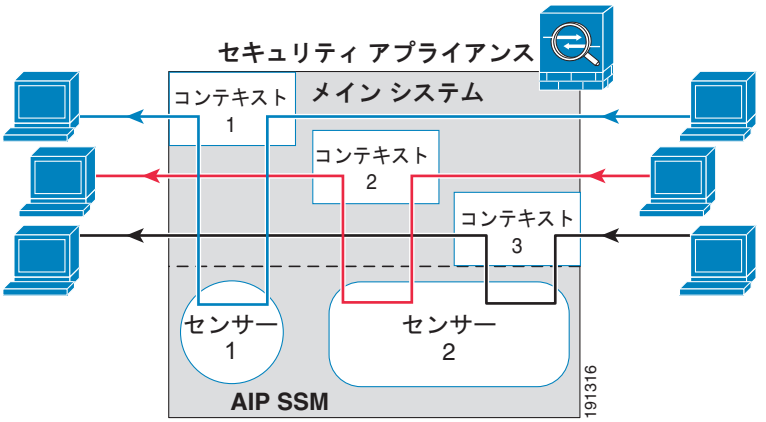
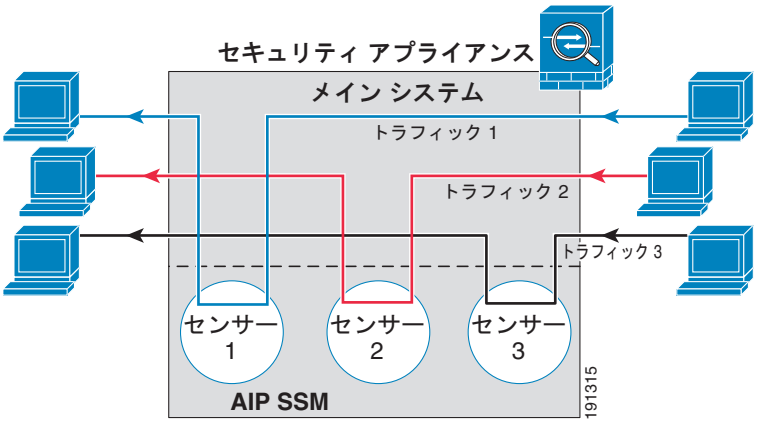


図 13-4 は、（インライン モードの）複数の仮想センサーがシングル モードの適応型セキュリティ アプライアンスとペアになり、定義されたトラフィック フローがそれぞれ異なるセンサーに流れているところを示しています。

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

この項は、次の内容で構成されています。

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. 適応型セキュリティ アプライアンスから AIP SSM にセッションを確立します。「AIP SSM へのセッション確立」（P.13-7）を参照してください。
2. 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浸入が検出されたときに行う作業が決まります。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。「AIP SSM でのセキュリティ ポリシーの設定」（P.13-8）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、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.13-9）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、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.13-12）を参照してください。

AIP SSM へのセッション確立

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 へセッションを確立します（SSH または Telnet を使用して AIP SSM 管理インターフェイスに直接接続することもできます）。

適応型セキュリティ アプライアンスから AIP SSM にセッションを確立するには、次の手順に従います。

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 にセッションを確立するには、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）　AIP SSM に初めてログインしたとき、デフォルトのパスワードを変更するよう求められます。パスワードは、8 文字以上で、意味を持たない言葉である必要があります。

```
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） （一部のソフトウェア バージョンだけに表示される）前回のライセンス通知が表示された場合、AIP SSM のシグニチャ ファイルのアップグレードが必要になるまでメッセージを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が検出されたときに行う作業を決定する検査および保護ポリシーを設定するには、次の手順に従います。適応型セキュリティ アプライアンスから AIP SSM へセッションを確立するには、「AIP SSM へのセッション確立」（P.13-7）を参照してください。

AIP SSM でのセキュリティ ポリシーを設定するには、次の手順に従います。

ステップ 1　AIP SSM の初期設定用のセットアップ 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、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 シリーズ適応型セキュリティ アプライアンスが設定中に仮想センサー名を指定していない場合は、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 にセッションを確立した場合、適応型セキュリティ アプライアンスプロンプトに戻ります。

仮想センサーのセキュリティ コンテンツへの割り当て

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、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られます。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。センサーをコンテキストに割り当てない場合、AIP SSM で設定されたデフォルト 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のにマルチ コンテキスト モードである必要はありません。シングル モードでも、異なるトラフィック フロー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　コンテキスト設定モードに入るには、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　仮想センサーをコンテキストに割り当てるには、次のコマンドを入力します。

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

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 AIP SSM で設定されたセンサー名です。AIP SSM で設定されたセンサーを表示するには、**allocate-ips ?** コマンドを入力します。利用可能なすべてのセンサーがリストされます。**show ips** コマンドを入力することもできます。**show ips** コマンドは、システム実行スペースにすべての利用可能なセンサーをリストします。コンテキストでそのコマンドを入力すると、コンテキストにすでに割り当てられたセンサーが表示されます。まだ AIP SSM に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。AIP SSM にその名前のセンサーを作成するまで、コンテキストによりセンサーがダウンしていると見なされます。

コンテキスト内で使用できるセンサー名のエイリアスとして、実際のセンサー名ではなく *mapped_name* 引数を使用します。マップ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。セキュリティを考慮すると、どのセンサーがコンテキストで使用されているかをコンテキスト アドミニストレータに知られたくない場合があります。または、コンテキスト設定の一般名を使用する場合があります。たとえば、すべてのコンテキストで「sensor1」と「sensor2」というセンサーを使用したい場合、コンテキスト A で「highsec」センサーと「lowsec」センサーを sensor1 と sensor2 にマップし、コンテキスト B では「medsec」センサーと「lowsec」センサーを sensor1 と sensor2 にマップできます。

default キーワードを指定すると、コンテキストごとに 1 つのセンサーがデフォルト センサーとして設定されます。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 1 つにつき、1 つのデフォルト センサーしか設定できません。デフォルト センサーを変更する場合、**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。センサーをデフォルトとして指定していないためコンテキスト設定にセンサー名が含まれていない場合、トラフィックは AIP SSM でデフォルト センサーを使用します。

ステップ 3　コンテキストごとにステップ 1 とステップ 2 を繰り返します。

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移ります。

```
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。「トラフィックの AIP SSM への転送」（P.13-12）に記載されているように、各コンテキストに移り、IPS セキュリティ ポリシーを設定します。

次の例では、sensor1 と sensor2 がコンテキスト A に、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もセンサー名を「ips1」と「ips2」にマップしています。コンテキスト A では、sensor1 はデフォルト 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 AIP SSM で設定されているデフォルトが使用されるよう、デフォルトは設定されていません。

```
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
...
```

トラフィックの AIP SSM への転送

適応型セキュリティ 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、各コンテキスト実行スペースでこれらの手順を行います。

ステップ 1　AIP SSM で検査するトラフィックを指定するには、**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、次のコマンドを使用してすべてのトラフィックを一致させることができます。

```
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ため、アクセス リストを一致させることができます。

```
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 にトラフィックを転送するよう処理を設定するポリシー マップを追加したり、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 からのクラス 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　AIP SSM にトラフィックを転送するには、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}]
```

ここで **inline** キーワードと **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、「動作モード」（P.13-3）を参照してください。

fail-close キーワードを指定すると、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するように設定されます。

fail-open キーワードを指定すると、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の通過を検査なしで許可するように設定されます。

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。利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。利用可能なセンサーがリストされます。**show ips** コマンドを使用することもできます。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、コンテキストに割り当てたセンサーだけ指定できます（「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.13-9）を参照）。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い場合、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、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、トラフィックは AIP SSM で設定されているデフォルト センサーを使用します。まだ AIP SSM にない名前を入力するとエラーになり、コマンドは拒否されます。

ステップ 4　（オプション）別のクラスのトラフィックを AIP SSM に転送し、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 検査を実行する別のクラス 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。

トラフィックは、同じ処理タイプについて複数のクラス マップを一致させることはできません。したがって、ネットワーク A を sensorA に送信し、他のすべてのトラフィックを sensorB に送信する場合は、ネットワーク A に **class** コマンドを入力してから、すべてのトラフィックに **class** コマンドを入力する必要があります。そうしないと、（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** コマンドと一致し、sensorB に送信されます。

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 マップを有効にするには、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 で設定されたポリシー マップです。このポリシー マップをすべてのインターフェイスのトラフィックに適用するには、**global** キーワードを使用します。ポリシー マップを特定のインターフェイスのトラフィックに適用するには、**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られた名前です。

使用できるグローバル ポリシーは、1 つに限られます。インターフェイスのグローバル ポリシーを無効にするには、そのインターフェイスにサービス ポリシーを適用します。各インターフェイスに適用できるポリシー マップは、1 つだけです。

次の例では、すべての IP トラフィックは AIP SSM に混合モードで転送され、何らかの原因で AIP SSM カードに障害が発生した場合、IP トラフィックはすべてブロックされます。

```
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 ネットワークに宛てられたすべての IP トラフィックはインライン モードで AIP SSM に転送され、何らかの原因で AIP SSM カードに障害が発生した場合、すべてのトラフィックが通過できます。my-ips-class トラフィックの場合 sensor1 が使用され、my-ips-class2 トラフィックの場合 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
```

次の作業

これで、適応型セキュリティ アプライアンスに侵入防御を設定する準備ができました。次のマニュアルを使用して、各実装内容に応じた適応型セキュリティ アプライアンスの設定を続けます。

実行内容	参照先
IPS センサーの設定	『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』
より効率的なサービス ポリシーを作成することによる AIP SSM と CSC SSM のパフォーマンスの最適化	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』

IPS センサーと AIP SSM ソフトウェアを設定したら、次の追加の手順を実行することもできます。

実行内容	参照先
詳細な設定およびオプション機能と拡張機能の設定	『*Cisco ASA 5500 Series Configuration Guide using the CLI*』
日常的な運用について	『*Cisco ASA 5500 Series Command Reference*』 『*Cisco ASA 5500 Series 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*』

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できます。次の項では、適応型セキュリティ アプライアンスの他の一般的なアプリケーションの設定手順について説明します。

実行内容	参照先
DMZ Web サーバの保護設定	第 8 章「シナリオ：DMZ 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 設定」
ソフトウェア クライアントのリモートアクセス SSL 接続設定	第 10 章「シナリオ：Cisco AnyConnect VPN クライアント用接続の設定」
ブラウザベースのリモートアクセス SSL 接続設定	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 設定」