CHAPTER 14

AIP SSM コンフィギュレーション タスク

この章では、AIP SSM の設定に固有の手順について説明します。この章は、次の項で構成されています。

コンフィギュレーション シーケンス

AIP SSM を設定するには、次のタスクを実行します。

1. AIP SSM にログインします。

   手順については、P.2-9 の「AIP SSM へのログイン」を参照してください。

2. AIP SSM を初期化します。

   setup コマンドを実行して、AIP SSM を初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

3. AIP SSM 初期化を確認します。

   手順については、P.14-3 の「AIP SSM 初期化の確認」を参照してください。

4. IPS トラフィックを AIP SSM に送信するように ASA を設定します。

   手順については、P.14-4 の「AIP SSM へのトラフィックの送信」を参照してください。

5. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

6. 侵入防御を設定します。

   手順については、第 6 章「イベント アクション ルールの設定」、第 7 章「シグニチャの定義」、および第 10 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

7. 各種タスクを実行して、AIP SSM が円滑に動作し続けるようにします。

   手順については、第 13 章「センサーの管理タスク」を参照してください。

8. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

   詳細については、第 18 章「ソフトウェアの入手方法」を参照してください。

9. 必要に応じて、AIP SSM のイメージを再作成します。

   手順については、P.17-44 の「AIP SSM システム イメージのインストール」を参照してください。

AIP SSM 初期化の確認

show module *slot* **details** コマンドを使用すると、AIP SSM を初期化したことと、正しいソフトウェア バージョンを使用していることが確認できます。

初期化を確認するには、次の手順を実行します。

ステップ 1　ASA にログインします。

ステップ 2　AIP SSM の詳細を取得します。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.05)S179.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   false
asa#
```

ステップ 3　情報を確認します。修正が必要な場合は、P.14-2 の「コンフィギュレーション シーケンス」を参照してください。

AIP SSM へのトラフィックの送信

この項では、AIP SSM を設定して、ASA から IPS トラフィックを受信する方法（インライン モードまたは混合モード）について説明します。取り上げる事項は次のとおりです。

概要

ASA は、パケットが出力インターフェイスを出る直前（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 を設定すると、インライン モードまたは混合モード、およびフェールオープン モードまたはフェールオーバー モードでトラフィックが検査できます。

ASA で、AIP SSM に転送されて、AIP SSM によって検査されるトラフィックを識別するには、次の手順を実行します。

1. **class-map** コマンドを使用して、IPS トラフィック クラスを定義します。
2. **policy-map** コマンドを使用して、トラフィック クラスを 1 つまたは複数のアクションに関連付けることよって IPS ポリシー マップを作成します。
3. **service-policy** コマンドを使用して、ポリシー マップを 1 つまたは複数のインターフェイスに関連付けることによって IPS セキュリティ ポリシーを作成します。

   IPS トラフィック検査を設定するには、ASA CLI または ASDM が使用できます。

IPS トラフィックを AIP SSM に送信するための ASA の設定

（注）　このためのコマンドの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の第 18 章「Using Modular Policy Framework」を参照してください。

次のオプションが適用されます。

- **access-list** *word* : アクセス コントロール要素を設定します。*word* はアクセス リスト識別子です（最大 241 文字）。
- **access-group** *word* : access-list をインターフェイスにバインドしてトラフィックをフィルタリングします。*word* はアクセス リスト識別子です（最大 241 文字）。
- **class-map** *class_map_name* : IPS トラフィック クラスを定義します。
- **match** : トラフィック クラスに含まれるトラフィックを定義します。

  トラフィック クラス マップには、**match** コマンドが含まれます。パケットをクラス マップと照合してマッチングをとる場合、マッチング結果は一致または不一致です。

  - **access-list** : アクセス リストのマッチングをとります。
  - **any** : すべてのパケットのマッチングをとります。
- **policy-map** *policy_map_name* : トラフィック クラスを 1 つまたは複数のアクションに関連付けることよって IPS ポリシー マップを作成します。
- **ips [inline | promiscuous][fail-close | fail-open]** : トラフィックを AIP SSM に割り当てます。
  - **inline** : AIP SSM をトラフィック フローに直接置きます。

トラフィックは、まず AIP SSM を通過し、これによって検査されないと ASA を通過し続けることができません。このモードは、すべてのパケットが分析された後に通過を許可されるので、最も安全です。また AIP SSM は、パケットごとにブロッキング 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及ぼすことがあります。

- **promiscuous**：トラフィックの重複したストリームを AIP SSM に送信します。

  このモードは安全性は低くなりますが、トラフィックのスループットにはほとんど影響を及ぼしません。インライン モードとは異なり、AIP SSM がトラフィックをブロックできるのは、ASA にトラフィックをブロックするように指示した場合、または ASA 上の接続をリセットした場合だけです。さらに、AIP SSM がトラフィックを分析している間に、AIP SSM がブロックする前に少量のトラフィックが ASA を通過する場合があります。

- **fail-close**：AIP SSM が使用不能の場合は、すべてのトラフィックをブロックするように ASA を設定します。
- **fail-open**：AIP SSM が使用不能の場合は、検査しないで、すべてのトラフィックの通過を許可するように ASA を設定します。

- **service-policy** *service_policy_name* [**global** | **interface** *interface_name*]：ポリシー マップを 1 つまたは複数のインターフェイスに関連付けることによって IPS セキュリティ ポリシーを作成します。
  - **global**：ポリシー マップをすべてのインターフェイスに適用します。

    1 つのグローバル ポリシーのみが許可されます。インターフェイス上のグローバル 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無効にできます。各インターフェイスには 1 つのポリシー マップしか適用できません。
  - **interface**：1 つのインターフェイスにポリシーを適用します。

ASA から AIP SSM にトラフィックを送信して IPS が検査できるようにするには、次の手順を実行します。

ステップ 1　ASA にログインします。

ステップ 2　コンフィギュレーション モードに入ります。

```
asa# configure terminal
```

ステップ 3　IPS アクセス リストを作成します。

```
asa(config)# access-list IPS permit ip any any
```

ステップ 4　アクセス リストをインターフェイスおよびトラフィック方向に適用するには、アクセス グループを使用します。

```
asa(config)# access-group IPS [in|out] interface [DMZ|inside|mgmt|outside]
```

ステップ 5　IPS トラフィック クラスを定義します。

```
asa(config)# class-map class_map_name
asa(config-cmap)# match [access-list | any]
```

ステップ 6　IPS ポリシー マップを定義します。

```
asa(config-cmap)# policy-map policy_map_name
```

ステップ 7　アクションを割り当てる、ステップ 5 からのクラス マップを指定します。

```
asa(config-pmap)# class class_map_name
```

ステップ 8　トラフィックを AIP SSM に割り当てます。

```
asa(config-pmap-c)# ips [inline | promiscuous] [fail-close | fail-open]
```

ステップ 9　IPS サービス ポリシーを定義します。

```
asa(config-pmap-c)# service-policy policymap_name [global | interface interface_name]
```

ステップ 10　設定を確認します。

```
asa(config-pmap-c)# show running-config
!
class-map my_ips_class
class-map my-ips-class
 match access-list IPS
class-map all_traffic
 match access-list all_traffic
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map my-ids-policy
 class my-ips-class
  ips promiscuous fail-close
!
service-policy my-ids-policy global
```

ステップ 11　コンフィギュレーションを終了して保存します。

```
asa(config-pmap-c)# exit
asa(config-pmap)# exit
asa(config)# exit
asa#
```

次の例は、すべての IP トラフィックを混合モードで AIP SSM に転送し、何らかの理由で AIP SSM に障害が発生したらすべての IP トラフィックをブロックします。

```
hostname(config)# access-list IPS permit ip any any
asa(config)# access-group IPS in interface inside
asa(config)# access-group IPS in interface outside
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ids-policy global
```

AIP SSM のリロード、シャットダウン、リセット、および復旧

ASA から AIP SSM を直接、リロード、シャットダウン、リセット、および復旧するには、次のコマンドを使用します。

（注）　**hw-module** コマンドは、特権 EXEC モードまたはグローバル コンフィギュレーション モードで入力できます。このコマンドは、シングル ルーテッド モードおよびシングル透過モードで入力できます。マルチモード（ルーテッド マルチモードまたは透過マルチモード）で動作する適応型セキュリティ デバイスの場合は、**hw-module** コマンドは、（管理者コンテキストやユーザ コンテキストからではなく）システム コンテキストから実行できるだけです。

- **hw-module module 1 reload**

  このコマンドは、ハードウェアをリセットせずに、AIP SSM にソフトウェアをリロードします。AIP SSM が Up 状態の場合にのみ有効です。
- **hw-module module 1 shutdown**

  このコマンドは、AIP SSM 上のソフトウェアをシャットダウンします。AIP SSM が Up 状態の場合にのみ有効です。
- **hw-module module 1 reset**

  このコマンドは、AIP SSM のハードウェア リセットを実行します。カードが Up/Down/Unresponsive/Recover 状態の場合に適用できます。
- **hw-module module 1 recover** [**boot** | **stop** | **configure**]

  recover コマンドは、復旧パラメータの設定用または変更用の対話型オプション セットを表示します。パラメータを変更することも Enter キーを押して既存の設定を保持することもできます。

  AIP SSM の復旧の手順については、P.17-44 の「AIP SSM システム イメージのインストール」を参照してください。
  - **hw-module module 1 recover boot**

    このコマンドは、AIP SSM の復旧を開始します。AIP SSM が Up 状態の場合にのみ適用できます。
  - **hw-module module 1 recover stop**

    このコマンドは、AIP SSM の復旧を停止します。AIP SSM が Recover 状態の場合にのみ適用できます。

注意　AIP SSM 復旧を停止する必要がある場合は、**hw-module module 1 recover stop** コマンドを AIP SSM 復旧の開始後 30 ～ 45 秒以内に発行する必要があります。これ以上待つと、予期しない結果となる場合があります。たとえば、AIP SSM が Unresponsive 状態になることがあります。

  - **hw-module module 1 recover configure**

    このコマンドは、モジュール復旧のためのパラメータを設定する場合に使用します。不可欠なパラメータは、IP アドレスと復旧イメージ TFTP URL の場所です。