CHAPTER 19

AIP SSM の設定

（注） すべての IPS プラットフォームで、許可される同時 CLI セッション数は 10 です。

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。次のような構成になっています。

AIP SSM の設定手順

適応型セキュリティ アプライアンスと IPS ソフトウェアの両方を AIP SSM で設定します。

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（セッションを確立）します。
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。
3. AIP SSM の初期化を確認します。
4. （任意）Cisco Adaptive Security Appliance Software 7.2.3 以降を使用している場合は、複数の仮想センサーを設定します。
5. IPS トラフィックを AIP SSM に送信するよう、適応型セキュリティ アプライアンスを設定します。
6. ユーザの追加、信頼されるホストの追加など、その他の初期タスクを実行します。
7. 侵入防御を設定します。
8. グローバル相関を設定します。
9. AIP SSM をスムーズに実行し続けるためのその他のタスクを実行します。

10. 新しいシグニチャ アップデートおよびサービス パックで IPS ソフトウェアをアップグレードします。
11. 必要であれば AIP SSM のイメージを再作成します。

詳細情報

- AIP SSM にログインする手順については、第 2 章「センサーへのログイン」を参照してください。
- **setup** コマンドを実行する手順については、「AIP SSM の高度な設定」（P.3-16）を参照してください。
- AIP SSM の初期化を確認する手順については、「AIP SSM の初期化の確認」（P.19-2）を参照してください。
- 仮想センサーを作成する手順については、「AIP SSM 用の仮想センサーの作成」（P.19-3）を参照してください。
- トラフィックを AIP SSM に送信するよう ASA を設定する手順については、「AIP SSM へのトラフィックの送信」（P.19-9）を参照してください。
- センサーを設定する手順については、第 4 章「センサーのセットアップ」を参照してください。
- 侵入防御を設定する手順については、第 7 章「イベント アクション規則の設定」、第 8 章「シグニチャの定義」、第 9 章「異常検出の設定」、および第 14 章「Attack Response Controller でのブロッキングとレート制限の設定」を参照してください。
- グローバル相関を設定する手順については、第 10 章「グローバル相関の設定」を参照してください。
- AIP SSM をスムーズに実行し続ける手順については、第 17 章「センサーの管理タスク」を参照してください。
- Cisco IPS ソフトウェアの入手方法の詳細については、第 22 章「ソフトウェアの入手」を参照してください。
- AIP SSM イメージを再作成する手順については、「AIP SSM システム イメージのインストール」（P.23-26）を参照してください。

AIP SSM の初期化の確認

show module *slot* **details** コマンドを使用して、AIP SSM の初期化が完了していること、および正しいソフトウェア バージョンを使用していることを確認できます。

初期化を確認するには、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　AIP SSM の詳細を入手します。

```
asa# show module 1 details
ASA 5500 Series Security Services Module-10
Model:              ASA-SSM-10
Hardware version:   1.0
Serial Number:      JAB09370212
Firmware version:   1.0(10)0
Software version:   7.0(4)E4
MAC Address Range:  0012.d948.fe73 to 0012.d948.fe73
App.name:           IPS
App.Status:         Up
App.Status Desc:
App.version:        6.2(1)E3
```

```
Data plane Status:  Up
Status:             Up
Mgmt IP addr: 171.69.36.171
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

ステップ 3　情報を確認します。

AIP SSM 用の仮想センサーの作成

注意　Cisco Adaptive Security Appliance Software 7.2.3 以降では、仮想化がサポートされています。

ここでは、AIP SSM 上に仮想センサーを作成する方法について説明します。内容は次のとおりです。

- 「AIM-SSM 仮想センサーの設定手順」（P.19-3）
- 「AIP SSM での仮想センサーの作成」（P.19-4）
- 「仮想センサーの適応型セキュリティ アプライアンス コンテキストへの割り当て」（P.19-6）

AIP SSM と仮想化

AIP SSM には 1 つのインターフェイス、GigabitEthernet0/1 があります。複数の仮想センサーを作成するときは、このインターフェイスを 1 つの仮想センサーだけに割り当てる必要があります。他の仮想センサーについては、インターフェイスを指定する必要はありません。

仮想センサーを作成後、**allocate-ips** コマンドを使用して、それらを適応型セキュリティ アプライアンスのセキュリティ コンテキストにマッピングする必要があります。複数のセキュリティ コンテキストを複数の仮想センサーにマッピングできます。

（注）　**allocate-ips** コマンドは、シングル モードには適用されません。このモードでは、**policy-map** コマンドで指定されたすべての仮想センサーを、セキュリティ アプライアンスが受け入れます。

allocate-ips コマンドは、新しいエントリをセキュリティ コンテキスト データベースに追加します。指定したセンサーが存在しない場合は警告が表示されますが、設定は可能です。設定は、service-policy コマンドが処理されるときに再びチェックされます。仮想センサーが有効でない場合は、**fail-open** ポリシーが実施されます。

AIM-SSM 仮想センサーの設定手順

この手順に従って AIP SSM 上に仮想センサーを作成し、それらを適応型セキュリティ デバイス コンテキストに割り当てます。

1. AIP SSM 上に最大 4 つの仮想センサーを設定します。
2. AIP SSM インターフェイス、GigabitEthernet0/1 を仮想センサーの 1 つに割り当てます。
3. 仮想センサーを、適応型セキュリティ デバイスのさまざまなコンテキストに割り当てます。

4. MPF を使用して、トラフィックをターゲットの仮想センサーに送信します。

AIP SSM での仮想センサーの作成

（注）　4 つの仮想センサーを作成できます。

AIP SSM 上に仮想センサーを作成するには、サービス分析エンジン サブモードで **virtual-sensor** *name* コマンドを使用します。仮想センサーにポリシー（異常検出、イベント アクション規則、およびシグニチャ定義）を割り当てます。デフォルトのポリシー、ad0、rules0、または sig0 を使用することも、新しいポリシーを作成することもできます。次に、インターフェイス GigabitEthernet0/1 を 1 つの仮想センサーに割り当てます。

次のオプションが適用されます。

- **anomaly-detection**：次のような異常検出パラメータを指定します。
  - **anomaly-detection-name** *name*：異常検出ポリシーの名前を指定します。
  - **operational-mode {inactive | learn | detect}**：異常検出モードを指定します。
- **description**：仮想センサーの説明。
- **event-action-rules**：イベント アクション規則ポリシーの名前を指定します。
- **signature-definition**：シグニチャ定義ポリシーの名前を指定します。
- **physical-interfaces**：物理インターフェイスの名前を指定します。
- **no**：エントリまたは選択項目を削除します。

AIP SSM 上に仮想センサーを作成するには、次の手順に従います。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　サービス分析モードを開始します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

ステップ 3　仮想センサーを追加します。

```
sensor(config-ana)# virtual-sensor vs1
sensor(config-ana-vir)#
```

ステップ 4　この仮想センサーの説明を追加します。

```
sensor(config-ana-vir)# description virtual sensor 1
```

ステップ 5　異常検出ポリシーと動作モードをこの仮想センサーに割り当てます。

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad1
sensor(config-ana-vir-ano)# operational-mode learn
```

ステップ 6　イベント アクション規則ポリシーをこの仮想センサーに割り当てます。

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules1
```

ステップ 7　シグニチャ定義ポリシーをこの仮想センサーに割り当てます。

```
sensor(config-ana-vir)# signature-definition sig1
```

ステップ 8　インターフェイスを 1 つの仮想センサーに割り当てます。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/1
```

ステップ 9　仮想センサーの設定を確認します。

```
sensor(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      description: virtual sensor 1 default:
      signature-definition: sig1 default: sig0
      event-action-rules: rules1 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad1 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 2)
      -----------------------------------------------
         name: GigabitEthernet0/1
         subinterface-number: 0 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana-vir)#
```

ステップ 10　分析エンジン モードを終了します。

```
sensor(config-ana-vir)# exit
sensor(config-ana)# exit
Apply Changes:?[yes]:
sensor(config)#
```

ステップ 11　Enter を押して変更を適用するか、**no** と入力して変更を破棄します。

詳細情報

- 異常検出ポリシーを作成および設定する手順については、「異常検出ポリシーの操作」（P.9-8）を参照してください。
- イベント アクション規則ポリシーを作成および設定する手順については、「イベント アクション規則ポリシーの使用」（P.7-7）を参照してください。
- シグニチャ定義を作成および設定する手順については、「シグニチャ定義ポリシーの操作」（P.8-1）を参照してください。

仮想センサーの適応型セキュリティ アプライアンス コンテキストへの割り当て

AIP SSM 上に仮想センサーを作成した後、それらを適応型セキュリティ アプライアンスのセキュリティ コンテキストに割り当てる必要があります。

次のオプションが適用されます。

- **[no] allocate-ips** *sensor_name* [*mapped_name*] [**default**]：仮想センサーをセキュリティ コンテキストに割り当てます。サポートされるモードは、マルチ モード、システム コンテキスト、およびコンテキスト サブモードです。

  （注）　同じ AIP SSM を 1 つのコンテキストの中で 2 回割り当てることはできません。

  - *sensor_name*：AIP SSM の名前。名前が無効な場合は、警告メッセージが表示されます。
  - *mapped_name*：セキュリティ コンテキストで AIP SSM が認識される名前。

    （注）　マッピング名は、AIP SSM の実際の名前をコンテキストから隠すために使用されます。通常、これはセキュリティ上の理由から、またはコンテキスト設定をより一般的にするために行われます。マッピング名が使用されない場合は、AIP SSM の実際の名前が使用されます。マッピング名をコンテキスト内で 2 つの異なる AIP SSM に再使用することはできません。

  - **no**：センサーを割り当て解除し、ポリシー マップの設定をすべて検索し、それを参照している IPS サブコマンドを削除します。
  - **default**：この AIP SSM をデフォルトとして指定します。仮想センサーが指定されていないすべてのレガシー IPS 設定は、この AIP SSM にマッピングされます。

注意　コンテキストごとに設定できる AIP SSM は 1 つのみです。別の AIP SSM をデフォルトとして指定するには、既存の AIP SSM のデフォルト フラグをオフにしておく必要があります。

  - **clear configure allocate-ips**：設定を削除します。
  - **allocate-ips?**：設定された AIP SSM のリストを表示します。

- **show ips [detail]**：使用可能なすべての仮想センサーを表示します。サポートされるモードは、EXEC モード、シングルまたはマルチ モード、システムまたはユーザ モードです。
  - **detail**：仮想センサーの ID 番号を追加します。

  （注）　このコマンドをシングル モードで実行すると、使用可能なすべての仮想センサーの名前が表示されます。このコマンドをマルチ モードのユーザ コンテキストで実行すると、このコンテキストに割り当てられたすべての仮想センサーのマッピング名が表示されます。このコマンドをマルチ モードのシステム コンテキストで実行すると、すべての仮想センサーの名前が表示され、detail キーワードを使用した場合は、センサーの ID 番号、割り当てられたコンテキスト、およびマッピング名も表示されます。

- **show context** [**detail**]：仮想センサーに関する情報を表示するように更新されました。ユーザ コンテキスト モードでは、このコンテキストに割り当てられたすべての仮想センサーのマッピング名を表示する新しい行が追加されました。システムでは、このコンテキストに割り当てられた仮想センサーの実際の名前とマッピング名を表示するために、新しい 2 行が追加されました。

次の手順では、マルチ モードで 3 つのセキュリティ コンテキストを追加する方法と、それらのセキュリティ コンテキストに仮想センサーを割り当てる方法を示します。

（注） 複数の仮想センサーを 1 つのコンテキストに割り当てることができます。複数のコンテキストで 1 つの仮想センサーを共有でき、共有する場合、各コンテキストで同じ仮想センサーに異なるマッピング名（エイリアス）を使用できます。

AIP SSM 仮想センサーをマルチ モードで適応型セキュリティ アプライアンスの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　適応型セキュリティ アプライアンスにログインします。

ステップ 2　使用可能な仮想センサーのリストを表示します。

```
asa# show ips detail
Sensor Name      Sensor ID
-----------      ---------
vs0              1
vs1              2
asa#
```

ステップ 3　コンフィギュレーション モードを開始します。

```
asa# configure terminal
asa(config)#
```

ステップ 4　マルチ モードを開始します。

```
asa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] yes
asa(config)#
```

ステップ 5　3 つのコンテキストをマルチ モードに追加します。

```
asa(config)# admin-context admin
Creating context 'admin'... Done. (13)
asa(config)# context admin
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.101
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.102
asa(config-ctx)#   allocate-interface Management0/0
asa(config-ctx)#   config-url disk0:/admin.cfg
Cryptochecksum (changed): 0c34dc67 f413ad74 e297464a db211681
INFO: Context admin was created with URL disk0:/admin.cfg
INFO: Admin context will take some time to come up .... please wait.
asa(config-ctx)#
asa(config-ctx)# context c2
Creating context 'c2'... Done. (14)
asa(config-ctx)#   allocate-interface GigabitEthernet0/0.103
asa(config-ctx)#   allocate-interface GigabitEthernet0/1.104
asa(config-ctx)#   config-url disk0:/c2.cfg

WARNING: Could not fetch the URL disk0:/c2.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

```
asa(config-ctx)# context c3
Creating context 'c3'... Done. (15)
asa(config-ctx)# all
asa(config-ctx)# allocate-in
asa(config-ctx)# allocate-interface g0/2
asa(config-ctx)# allocate-interface g0/3
asa(config-ctx)#   config-url disk0:/c3.cfg

WARNING: Could not fetch the URL disk0:/c3.cfg
INFO: Creating context with default config
asa(config-ctx)#
```

ステップ 6　仮想センサーをセキュリティ コンテキストに割り当てます。

```
asa(config)# context admin
asa(config-ctx)#   allocate-ips vs0 adminvs0
asa(config-ctx)# exit
asa(config)# context c2
asa(config-ctx)#   allocate-ips vs1 c2vs1
asa(config)# context c3
asa(config-ctx)# allocate-ips vs0 c3vs0
asa(config-ctx)# allocate-ips vs1 c3vs1
asa(config-ctx)#
```

ステップ 7　各コンテキストの MPF を設定します。

（注）　次に、コンテキスト 3（c3）の例を示します。

```
asa(config)# context c3
asa/c3(config)# class-map any
asa/c3(config-cmap)# match access-list any
asa/c3(config-cmap)# exit
asa/c3(config)# policy-map ips_out
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips promiscuous fail-close sensor c3vs1
asa/c3(config-pmap-c)# policy-map ips_in
asa/c3(config-pmap)# class any
asa/c3(config-pmap-c)# ips inline fail-open sensor c3vs0
asa/c3(config-pmap-c)# service-policy ips_out interface outside
asa/c3(config)# service-policy ips_in interface inside
asa/c3(config)#
```

ステップ 8　設定を確認します。

```
asa/c3(config)# exit
asa(config)# show ips detail
Sensor Name      Sensor ID        Allocated To     Mapped Name
-----------      ---------        ------------     -----------
vs0              1                admin            adminvs0
                                  c3               c3vs0
vs1              2                c2               c2vs1
                                  c3               c3vs1
asa(config)#
```

AIP SSM へのトラフィックの送信

ここでは、適応型セキュリティ アプライアンス（インラインまたは無差別モード）から IPS トラフィックを受信するよう AIP SSM を設定する方法について説明します。ここでは、次の項目について説明します。

適応型セキュリティ アプライアンスと AIP SSM

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 をインラインまたは無差別モードおよびフェール オープンまたはフェール オーバー モードでトラフィックを検査するように設定できます。

AIP SSM に転送して検査するトラフィックを識別するには、適応型セキュリティ アプライアンスで次の手順を実行します。

1. ACL を作成するか、既存のものを使用します。
2. **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。
3. **policy-map** コマンドを使用して、トラフィック クラスと 1 つ以上のアクションを関連付けることにより、IPS ポリシー マップを作成します。
4. **service-policy** コマンドを使用して、ポリシー マップと 1 つ以上のインターフェイスを関連付けることにより、IPS セキュリティ ポリシーを作成します。

   適応型セキュリティ アプライアンス の CLI または ASDM を使用して、IPS トラフィック検査を設定できます。

IPS トラフィックを AIP SSM に送信するための適応型セキュリティ アプライアンスの設定

適応型セキュリティ アプライアンスから AIP SSM にトラフィックを送信して検査するには、次の手順に従います。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
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　AIP SSM に送信するトラフィックを識別する IPS クラス マップを定義します。

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

例

```
asa(config)# class-map ips_class
```

（注）　複数のトラフィック クラス マップを作成して、複数のトラフィック クラスを AIP SSM に送信できます。

ステップ 5　クラス マップにトラフィックを指定します。

```
asa(config-cmap)# match parameter
```

例

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

ステップ 6　クラス マップ トラフィックで実行するアクションを設定する IPS ポリシー マップを追加します。

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

例

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

ステップ 7　ステップ 4 で作成したクラス マップを確認します。

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

例

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

ステップ 8　AIP SSM にトラフィックを割り当てます。

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

例

```
asa(config-pmap-c)# ips promiscuous fail-close
```

ステップ 9　（任意）IPS トラフィックに複数のクラスマップを作成した場合、別のクラスを指定できます。

```
asa(config-pmap)# class class_map_name_2
```

例

```
asa(config-pmap)# class ips_class_2
```

ステップ 10　（任意）AIP SSM に送信するトラフィックの 2 番目のクラスを指定します。

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

例

```
asa(config-pmap-c)# ips promiscuous fail-close
```

ステップ 11　1 つ以上のインターフェイスで IPS サービス ポリシー マップをアクティブにします。

```
asa(config)# service-policy policymap_name {global | interface interface_name}
```

例

```
asa(config)# service-policy tcp_bypass_policy outside
```

ステップ 12　設定を確認できます。

```
asa# show running-config
```

ステップ 13　設定を終了し、保存します。

詳細情報

バイパス モードの詳細については、「適応型セキュリティ アプライアンス、AIP SSM、およびバイパス モード」（P.19-11）を参照してください。

適応型セキュリティ アプライアンス、AIP SSM、およびバイパス モード

バイパス モードの設定、適応型セキュリティ アプライアンス、および AIP SSM には、次の条件が適用されます。

- AIP SSM がリセットまたはシャットダウン状態にある。

  適応型セキュリティ アプライアンスは、設定されたフェール オープンまたはフェール クローズ規則に従ってトラフィックを許可するかブロックします。

- AIP SSM がリセットまたはシャットダウン以外の状態にあり、SensorApp が停止している。
  - Bypass Auto

    適応型セキュリティ アプライアンスは、設定されたフェール オープンまたはフェール クローズ規則に関係なく、すべてのトラフィックを許可します。AIP SSM NIC ドライバがまだ機能しており、ハートビート パケットを渡しているためです。
  - Bypass Off

    適応型セキュリティ アプライアンスは、設定されたフェール オープンまたはフェール クローズ規則に関係なく、すべてのトラフィックを拒否します。
  - Bypass On

    適応型セキュリティ アプライアンスは、設定されたフェール オープンまたはフェール クローズ規則に関係なく、検査されたすべてのトラフィックを通過させます。

詳細情報

バイパス モードの詳細については、「インライン バイパス モードの設定」（P.6-38）を参照してください。

AIP SSM のリロード、シャットダウン、リセット、および回復

（注）　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 モードから、**hw-module** コマンドを入力できます。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 トラスペアレント モードで入力できます。マルチ モード（ルーテッドまたはトランスペアレント マルチ モード）で動作している適応型セキュリティ デバイスでは、（管理者またはユーザ コンテキストからでなく）システム コンテキストからのみ **hw-module** コマンドを実行できます。

パスワードのリロード、シャットダウン、リセット、回復、および適応型セキュリティ アプライアンスから直接、AIP SSM の回復を行うには、次のコマンドを使用します。

- **hw-module module** *slot_number* **reload**

  このコマンドは、ハードウェアのリセットを行わずに AIP SSM にソフトウェアをリロードします。これは、AIP SSM が Up 状態であるときにのみ有効です。

- **hw-module module** *slot_number* **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。これは、AIP SSM が Up 状態であるときにのみ有効です。

- **hw-module module** *slot_number* **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。これは、AIP SSM が Up/Down/Unresponsive/Recover 状態であるときに適用できます。

- **hw-module module** *slot_number* **password-reset**

  このコマンドは、AIP SSM 上の Cisco CLI アカウント パスワードをデフォルトの **cisco** に回復します。

- **hw-module module** *slot_number* **recover** {**boot** | **stop** | **configure**}

  recover コマンドでは、回復パラメータを設定または変更する一連の対話式オプションが表示されます。パラメータを変更するか、既存の設定値を保持するには、Enter を押します。

  - **hw-module module** *slot_number* **recover boot**

    このコマンドは、AIP SSM の回復を開始します。これは、AIP SSM が Up 状態であるときにのみ適用できます。

  - **hw-module module** *slot_number* **recover stop**

    このコマンドは、AIP SSM の回復を停止します。これは、AIP SSM が Recover 状態であるときにのみ適用できます。

注意　AIP SSM の回復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 の回復の開始後 30 秒から 45 秒以内に発行する必要があります。それ以上待っていると、予期しない結果が生じることがあります。たとえば、AIP SSM が Unresponsive 状態で起動する場合があります。

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

    このコマンドは AIP SSM の回復のパラメータを設定するために指定します。必要なパラメータは、IP アドレスと回復イメージの TFTP URL ロケーションです。

    例

```
AIP SSM# hardware-module module 1 recover configure
Image URL [tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-6.2-1.img]:
Port IP Address [10.89.149.226]:
VLAN ID [0]:
Gateway IP Address [10.89.149.254]:
```

詳細情報

AIP SSM システム イメージを回復する手順については、「AIP SSM システム イメージのインストール」（P.23-26）を参照してください。

新しいコマンドと変更されたコマンド

（注）　その他の Cisco ASA CLI コマンドについては、Cisco.com（http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html）の『*Cisco Security Appliance Command Reference*』を参照してください。

ここでは、AIP SSM をサポートし、AIP SSM を設定するために使用する Cisco ASA の新しいコマンドと変更されたコマンドについて説明します。構成するトピックは、次のとおりです。

allocate-ips

IPS 仮想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、AIP SSM がインストールされている場合には、コンテキスト コンフィギュレーション モードで **allocate-ips** コマンドを使用します。仮想センサーをコンテキストから削除するには、このコマンドの **no** 形式を使用します。

allocate-ips *sensor_name* [*mapped_name*] [**default**]

no allocate-ips *sensor_name* [*mapped_name*] [**default**]

構文の説明

default	（任意）コンテキストごとに 1 つのセンサーをデフォルト センサーとして設定します。コンテキスト コンフィギュレーションでセンサー名が指定されていない場合は、コンテキストでこのデフォルト 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 つのみです。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。

mapped_name	（任意）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るセンサー名のエイリアスとして、マッピング名を設定します。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」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 と sensor2 に「highsec」センサーと「lowsec」センサーをマッピングし、コンテキスト B の sensor1 と sensor2 に「medsec」センサーと「lowsec」センサーをマッピングできます。
sensor_name	AIP SSM に設定されているセンサー名を設定します。AIP SSM に設定されているセンサーを表示するには、**allocate-ips ?** と入力します。使用可能なすべてのセンサーが表示されます。**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表示されます。このコマンドをコンテキストで入力すると、そのコンテキストにすでに割り当てられているセンサーが表示されます。AIP SSM にまだ存在しないセンサー名を指定した場合は、エラーが表示されますが、**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が作成されるまで、コンテキストはそのセンサーがダウンしていると見なします。

デフォルト

なし

コマンド モード

次の表に、コマンドを入力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	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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。その後、**ips** コマンドを使用して AIP SSM にトラフィックを送信するように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。

例

次に、sensor1 と sensor2 をコンテキスト A に、sensor1 と sensor3 をコンテキスト B に割り当てる例を示します。両方のコンテキストで、センサー名を「ips1」と「ips2」にマッピングします。コンテキスト A では sensor1 をデフォルト センサーとして設定しますが、コンテキスト B ではデフォルトを設定しないため、AIP SSM に設定されているデフォルトが使用されます。

```
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
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
ips	トラフィックをインスペクションのために AIP SSM に転送します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show ips	AIP SSM に設定されている仮想センサーを表示します。