CHAPTER 5

仮想センサーの設定

（注） AIM IPS および NME IPS は、仮想化をサポートしません。

この章では、分析エンジンの機能と、仮想センサーの作成、編集、および削除の方法について説明します。また、仮想センサーにインターフェイスを割り当てる方法についても説明します。次のような構成になっています。

分析エンジンについて

（注） Cisco IPS では、5 つ以上の仮想センサーはサポートされません。デフォルトの仮想センサー vs0 は削除できません。

分析エンジンは、パケット分析とアラート検出を実行します。指定したインターフェイスを流れるトラフィックをモニタします。仮想センサーは、分析エンジンで作成します。各仮想センサーは、固有の名前と、それに関連付けられているインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループのリストを持っています。定義の順序の問題を防止するため、割り当てで競合や重複は許可されません。パケットが複数の仮想センサーによって処理されないよう、インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを特定の仮想センサーに割り当てます。また、各仮想センサーは、明示的に指定されたシグニチャ定義、イベント アクション規則、および異常検出設定にも関連付けられます。どの仮想センサーにも割り当てられていないインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループからのパケットは、インライン バイパス設定に従って破棄されます。

仮想センサーについて

（注）　AIM IPS および NME IPS は、仮想化をサポートしません。

センサーは 1 つまたは多数のモニタ対象データ ストリームからのデータ入力を受信できます。これらのモニタ対象データ ストリームは、物理インターフェイス ポートまたは仮想インターフェイス ポートのどちらでも構いません。たとえば、単一のセンサーでファイアウォールの前からのトラフィック、ファイアウォールの後ろからのトラフィック、またはファイアウォールの前後からのトラフィックを同時にモニタできます。単一のセンサーで 1 つ以上のデータ ストリームをモニタできます。この場合、単一のセンサー ポリシーまたは設定がすべてのモニタ対象データストリームに適用されます。

仮想センサーは、設定ポリシーのセットによって定義されたデータの集合です。仮想センサーは、インターフェイス コンポーネントによって定義されたとおりに、一連のパケットに適用されます。1 つの仮想センサーで複数のセグメントをモニタでき、単一の物理センサー内で、仮想センサーごとに異なるポリシーまたは設定を適用できます。分析するモニタ対象のセグメントごとに、異なるポリシーを設定できます。また、異なる仮想センサーに同じポリシー インスタンス（たとえば、sig0、rules0、または ad0）を適用することもできます。

仮想センサーに、インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを割り当てることができます。

（注）　デフォルトの仮想センサーは vs0 です。デフォルトの仮想センサーは削除できません。デフォルトの仮想センサーで変更できる設定機能は、インターフェイス リスト、異常検出の動作モード、インライン TCP セッション トラッキング モード、および仮想センサーの説明だけです。シグニチャ定義、イベント アクション規則、または異常検出ポリシーを変更することはできません。

仮想化の利点および制約事項

（注）　AIM IPS および NME IPS は、仮想化をサポートしません。

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。
- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。
  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パス スイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。
- 固定ストアが制限されます。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

次のセンサーで仮想化がサポートされます。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIP SSM

IDSM2 では、インライン インターフェイス ペアでの VLAN グループを例外として、仮想化がサポートされます。

Inline TCP Session Tracking Mode

インラインでのパケット変更を選択している場合、ノーマライザ エンジンでは、ストリームからのパケットを 2 回認識すると、ストリームの状態を適切に追跡できません。このような場合は、ストリームが頻繁にドロップされます。この状況は、ストリームが、IPS によってモニタされている複数の VLAN またはインターフェイスを介してルーティングされている場合に、最もよく発生します。また、いずれかの方向のトラフィックがそれぞれ異なる VLAN またはインターフェイスから受信された場合に、ストリームを適切に追跡するために非対称トラフィックをマージできるようにする必要があり、これにより、状況がより複雑化します。

この状況を処理するために、ストリームが別々のインターフェイスや LAN（または VLAN ペアのサブインターフェイス）で受信された場合には、これらを一意のストリームとして認識するように、モードを設定できます。

次のインライン TCP セッション トラッキング モードが適用されます。

- インターフェイスおよび VLAN：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。
- VLAN だけ：同じ VLAN（またはインライン VLAN ペア）内で同じセッション キー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。
- 仮想センサー：仮想センサー内で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。これがデフォルトであり、ほとんどの場合、最良のオプションです。

詳細情報

- Modify Packet Inline イベント アクションの詳細については、「イベント アクション」（P.7-4）を参照してください。
- Normalizer エンジンの詳細については、「Normalizer エンジン」（P.B-36）を参照してください。

仮想センサーの追加、編集、および削除

ここでは、仮想センサーの追加、編集、および削除の方法について説明します。内容は次のとおりです。

仮想センサーの追加

注意　AIM IPS および NME IPS ではセンサーの仮想化はサポートされず、したがって、複数のポリシーはサポートされません。

（注）　4 つの仮想センサーを作成できます。

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。次に、仮想センサーにインターフェイス（無差別、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループ）を割り当てます。インライン インターフェイス ペアおよび VLAN ペアを設定してからでないと、それらを仮想センサーに割り当てることができません。

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。
  - **operational-mode {inactive | learn | detect}**：異常検出モード。
- **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。
- **inline-TCP-evasion-protection-mode**：トラフィック検査に必要な次のノーマライザ モードのタイプを選択できます。
  - **asymmetric**：双方向トラフィック フローのいずれかの方向だけを参照できます。[Asymmetric Mode Protection] を指定すると、TCP レイヤでの回避防止が緩和されます。

    （注）　Asymmetric モードの場合、センサーは状態をフローと同期し、双方向を必要としないエンジンの検査を継続します。完全な保護には双方向のトラフィックを確認する必要があるため、Asymmetric モードではセキュリティが低下します。

  - **strict**：何らかの理由でパケットが失われた場合、失われたパケット以降のすべてのパケットが処理されなくなります。[Strict Evasion Protection] を指定すると、TCP ステートとシーケンスのトラッキングの完全な施行が提供されます。

（注）　パケットの順序が正しくないか、またはパケットが失われていると、ノーマライザ エンジンのシグニチャ 1300 または 1330 が起動する場合があります。この処理によって状況の修正が試行されますが、結果として接続が拒否されることがあります。

- **inline-TCP-session-tracking-mode**：インライン トラフィック内の重複する TCP セッションを識別する高度な方式。デフォルトは virtual sensor で、ほとんどの場合これが最適です。
  - **virtual-sensor**：仮想センサー内で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属します。
  - **interface-and-vlan**：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属します。同じキーを持ち、VLAN またはインターフェイスが異なるパケットは、独立して追跡されます。
  - **vlan-only**：同じ VLAN（またはインライン VLAN ペア）内で同じセッション キー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属します。同じキーを持ち、VLAN が異なるパケットは、独立して追跡されます。
- **signature-definition**：シグニチャ定義ポリシの名前。
- **logical-interfaces**：論理インターフェイス（インライン インターフェイス ペア）の名前。
- **physical-interfaces**：物理インターフェイス（無差別、インライン VLAN ペア、および VLAN グループ）の名前：
  - **subinterface-number**：物理サブインターフェイス番号。subinterface-type が none の場合、値 0 はインターフェイス全体が無差別モードで割り当てられることを示します。
- **no**：エントリまたは選択項目を削除します。

仮想センサーを追加するには、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　インライン TCP セッション トラッキング モードを割り当てます。

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode virtual-sensor
```

デフォルトは仮想センサー モードで、ほとんどの場合これが最適です。

ステップ 9　インライン TCP 回避保護モードを割り当てます。

```
sensor(config-ana-vir)# inline-TCP-evasion-protection-mode strict
```

デフォルトは strict モードで、ほとんどの場合これが最適です。

ステップ 10　使用可能なインターフェイスのリストを表示します。

```
sensor(config-ana-vir)# physical-interface ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet2/0     GigabitEthernet0/2 physical interface.
GigabitEthernet2/1     GigabitEthernet0/3 physical interface.
sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?
<none available>
```

ステップ 11　この仮想センサーに追加する無差別モード インターフェイスを割り当てます。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/3
```

この仮想センサーに割り当てるすべての無差別インターフェイスについて、ステップ 10 を繰り返します。

ステップ 12　この仮想センサーに追加するインライン インターフェイス ペアを割り当てます。

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

すでにインターフェイスのペアの作成が済んでいる必要があります。

ステップ 13　この仮想センサーに追加するインライン VLAN ペアまたはグループのサブインターフェイスを割り当てます。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

すでにインターフェイスの VLAN ペアまたはグループへの分割が済んでいる必要があります。

ステップ 14　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: GigabitEthernet0/3
         subinterface-number: 0 <defaulted>
      -----------------------------------------------
      inline-TCP-session-tracking-mode: virtual-sensor default: virtual-sensor
      -----------------------------------------------
```

```
        logical-interface (min: 0, max: 999999999, current: 0)
        ----------------------------------------------
        ----------------------------------------------
    ------------------------------------------------
sensor(config-ana-vir)#
```

ステップ 15　分析エンジン モードを終了します。

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

ステップ 16　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

- AIP SSM に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。
- 異常検出ポリシーの作成と設定の詳細については、「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の作成と設定の詳細については、「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。
- シグニチャ定義ポリシーの作成と設定の詳細については、「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。
- インライン インターフェイスのペアを作成する手順については、「インライン インターフェイス ペアの設定」（P.6-20）を参照してください。この仮想センサーに割り当てるすべてのインライン インターフェイスについて、ステップ 11 を繰り返します。
- インライン VLAN のペアとグループを作成する手順については、「インライン VLAN ペアの設定」（P.6-24）および「VLAN グループの設定」（P.6-32）を参照してください。この仮想センサーに割り当てるすべてのインライン VLAN ペアまたは VLAN グループについて、ステップ 12 を繰り返します。

仮想センサーの編集と削除

注意　AIM IPS および NME IPS ではセンサーの仮想化はサポートされず、したがって、複数のポリシーはサポートされません。

仮想センサーの次のパラメータを編集できます。

- シグニチャ定義ポリシー
- イベント アクション規則ポリシー
- 異常検出ポリシー
- 異常検出動作モード
- インライン TCP セッション トラッキング モード
- 説明
- インターフェイスの割り当て

仮想センサーを編集または削除するには、次の手順に従ってください。

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　分析エンジン 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 vs1 を編集します。

```
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編集します。

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

ステップ 5　この仮想センサーに割り当てられている異常検出ポリシーと動作モードを変更します。

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# anomaly-detection-name ad0
sensor(config-ana-vir-ano)# operational-mode learn
```

ステップ 6　この仮想センサーに割り当てられているイベント アクション規則ポリシーを変更します。

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# event-action-rules rules0
```

ステップ 7　この仮想センサーに割り当てられているシグニチャ定義ポリシーを変更します。

```
sensor(config-ana-vir)# signature-definition sig0
```

ステップ 8　インライン TCP セッション トラッキング モードを変更します。

```
sensor(config-ana-vir)# inline-TCP-session-tracking-mode interface-and-vlan
```

デフォルトは仮想センサー モードで、ほとんどの場合これが最適です。

ステップ 9　使用可能なインターフェイスのリストを表示します。

```
sensor(config-ana-vir)# physical-interface ?
GigabitEthernet0/0     GigabitEthernet0/0 physical interface.
GigabitEthernet0/1     GigabitEthernet0/1 physical interface.
GigabitEthernet2/0     GigabitEthernet0/2 physical interface.
GigabitEthernet2/1     GigabitEthernet0/3 physical interface.
sensor(config-ana-vir)# physical-interface

sensor(config-ana-vir)# logical-interface ?
<none available>
```

ステップ 10　この仮想センサーに割り当てられている無差別モード インターフェイスを変更します。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet0/2
```

ステップ 11　この仮想センサーに割り当てられているインライン インターフェイス ペアを変更します。

```
sensor(config-ana-vir)# logical-interface inline_interface_pair_name
```

すでにインターフェイスのペアの作成が済んでいる必要があります。

ステップ 12　この仮想センサーに割り当てられているインライン VLAN ペアまたはグループを使用するサブインターフェイスを変更します。

```
sensor(config-ana-vir)# physical-interface GigabitEthernet2/0 subinterface-number
subinterface_number
```

すでにインターフェイスの VLAN ペアまたはグループへの分割が済んでいる必要があります。

ステップ 13　編集した仮想センサーの設定を確認します。

```
ssensor(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: GigabitEthernet0/3
         subinterface-number: 0 <defaulted>
      -----------------------------------------------
      inline-TCP-session-tracking-mode: interface-and-vlan default: virtual-sensor
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
sensor(config-ana-vir)#
```

ステップ 14　仮想センサーを削除するには、次のようにします。

```
sensor(config-ana-vir)# exit
sensor(config-ana)# no virtual-sensor vs1
```

ステップ 15　削除した仮想センサーを確認します。

```
sensor(config-ana)# show settings
   global-parameters
   -----------------------------------------------
      ip-logging
      -----------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      -----------------------------------------------
   -----------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 2)
   -----------------------------------------------
      <protected entry>
      name: vs0 <defaulted>
      -----------------------------------------------
         description: default virtual sensor <defaulted>
         signature-definition: sig0 <protected>
         event-action-rules: rules0 <protected>
         anomaly-detection
         -----------------------------------------------
            anomaly-detection-name: ad0 <protected>
            operational-mode: detect <defaulted>
         -----------------------------------------------
         physical-interface (min: 0, max: 999999999, current: 0)
         -----------------------------------------------
         -----------------------------------------------
         logical-interface (min: 0, max: 999999999, current: 0)
         -----------------------------------------------
         -----------------------------------------------
sensor(config-ana)#
```

デフォルトの仮想センサー vs0 のみが存在します。

ステップ 16　分析エンジン モードを終了します。

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

ステップ 17　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

- 異常検出ポリシーの作成と設定の詳細については、「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の作成と設定の詳細については、「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。
- シグニチャ定義ポリシーの作成と設定の詳細については、「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。
- インライン インターフェイスのペアを作成する手順については、「インライン インターフェイス ペアの設定」（P.6-20）を参照してください。この仮想センサーに割り当てるすべてのインライン インターフェイスについて、ステップ 11 を繰り返します。
- インライン VLAN のペアとグループを作成する手順については、「インライン VLAN ペアの設定」（P.6-24）および「VLAN グループの設定」（P.6-32）を参照してください。この仮想センサーに割り当てるすべてのインライン VLAN ペアまたは VLAN グループについて、ステップ 12 を繰り返します。

グローバル変数の設定

（注）　Cisco IPS で唯一のグローバル変数は、開く IP ログ ファイルの最大数の設定です。

グローバル変数を作成するには、サービス分析エンジン サブモードで **global-parameters** コマンドを使用します。

次のオプションが適用されます。

- **ip-logging**：グローバル IP ロギング パラメータ。
  - **max-open-iplog-files**：同時に開けるログ ファイルの最大数。範囲は 20 ～ 100 です。デフォルトは 20 です。

グローバル変数を作成するには、次の手順に従ってください。

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　開く IP ログの最大数を表す変数を作成します。

```
sensor(config-ana)# global-parameters
```

```
sensor(config-ana-glo)# ip-logging
sensor(config-ana-glo-ip)# max-open-iplog-files 50
```

ステップ 4　グローバル変数の設定値を確認します。

```
sensor(config-ana-glo-ip)# show settings
   ip-logging
   -----------------------------------------------
      max-open-iplog-files: 50 default: 20
   -----------------------------------------------
sensor(config-ana-glo-ip)#
```

ステップ 5　分析エンジン モードを終了します。

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

ステップ 6　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。