CHAPTER 6

仮想センサーの設定

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585 のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585 は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、分析エンジンの機能、および仮想センサーの作成、編集、削除方法について説明します。また、インターフェイスを仮想センサーに割り当てる方法についても説明します。この章は、次の内容で構成されています。

- 「分析エンジンについて」（P.6-1）
- 「仮想センサーについて」（P.6-2）
- 「仮想化の利点および制約事項」（P.6-2）
- 「IPS SSP 上での仮想センサーの追加、編集、および削除」（P.6-3）
- 「グローバル変数の設定」（P.6-11）

分析エンジンについて

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。

分析エンジンでは、仮想センサーを作成します。各仮想センサーには、一意の名前が割り当てられ、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 グループのリストが関連付けられます。定義順序による問題の発生を避けるため、割り当てに競合や重複が存在してはなりません。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 グループは、複数の仮想センサーによって処理されるパケットが発生しないように、特定の仮想センサーに割り当てます。各仮想センサーは、固有の名前を持つシグニチャ定義、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廃棄されます。

（注） Cisco IPS では仮想センサーが 4 つまでサポートされます。デフォルトの仮想センサー vs0 は削除できません。

仮想センサーについて

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。また、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、一連の設定ポリシーで定義されるデータの集合です。仮想センサーは、インターフェイス コンポーネントで定義される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することができ、単一の物理センサー内では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。分析時には、モニタ対象セグメントごとに異なるポリシーをセットアップできます。また、同じポリシー インスタンス（sig0、rules0、ad0 など）を複数の仮想センサーに適用することもできます。仮想センサーには、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に対して変更可能な設定機能は、インターフェイス リスト、異常検出動作モード、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、異常検出ポリシーは変更できません。

仮想化の利点および制約事項

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。

IPS SSP 上での仮想センサーの追加、編集、および削除

ここでは、IPS SSP 上で仮想センサーを作成する方法について説明します。次のような構成になっています。

- 「IPS SSP と仮想化」（P.6-3）
- 「IPS SSP 仮想センサーの設定手順」（P.6-3）
- 「仮想センサーの作成」（P.6-4）
- 「適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て」（P.6-6）
- 「仮想センサーの編集と削除」（P.6-9）

IPS SSP と仮想化

IPS SSP には、センシング インターフェイスが 1 つ（PortChannel0/0）存在します。複数の仮想センサーを作成する場合は、このインターフェイスを 1 つの仮想センサーにだけ割り当てる必要があります。残りの仮想センサーには、インターフェイスを指定する必要はありません。

注意　IPS SSP は、4 種類のポート（コンソール、管理、GigabitEthernet、および 10GE）を備えています。コンソール ポートと管理ポート（IPS SSP の右前面パネル上にある）は、IPS ソフトウェアによって設定および制御を行います。GigabitEthernet ポートと 10GE ポート（IPS SSP の左前面パネル上にある）は、IPS ソフトウェアではなく、ASA ソフトウェアによって設定および制御を行います。ただし、IPS SSP をリセットまたはシャットダウンするときは、GigabitEthernet ポートと 10GE ポートもリンクダウンします。これらのポートに対するリンク ダウンの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンはスケジュールされたメンテナンス期間中に行う必要があります。

仮想センサーを作成した後、**allocate-ips** コマンドを使用して、それらを適応型セキュリティ アプライアンス上のセキュリティ 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** コマンドで名前が指定されているすべての仮想センサーが適応型セキュリティ アプライアンスで受け入れられます。

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。指定した仮想センサーが存在しないと、警告が出力されます。ただし、設定は受け入れられます。**service-policy** コマンドが処理されるとき、設定が再びチェックされます。仮想センサーが有効でなければ、**fail-open** ポリシーが適用されます。

IPS SSP 仮想センサーの設定手順

次の手順に従って、IPS SSP 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 アプライアンスのコンテキストに割り当てます。

1. IPS SSP 上で最大 4 つの仮想センサーを設定します。
2. IPS SSP センシング インターフェイス（PortChannel0/0）を仮想センサーの 1 つに割り当てます。

3. （任意）仮想センサーを適応型セキュリティ アプライアンス上の異なる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誘導します。

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。

サービス分析エンジン サブモードで **virtual-sensor** *name* コマンドを使用して、IPS SSP 上の仮想センサーを作成します。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である ad0、rules0、または sig0 を使用できます。あるいは、新しいポリシーを作成することもできます。その後、IPS SSP のセンシング インターフェイス PortChannel0/0 を 1 つの仮想センサーに割り当てます。

オプション

次のオプションが適用されます。

- **anomaly-detection**：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**：異常検出モード（**inactive**、**learn**、**detect**）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-interface**：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を削除します。

仮想センサーの作成

IPS SSP 上で仮想センサーを作成するには、次の手順を実行します。

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。

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

ステップ 3　仮想センサーを追加します。

```
ips-ssp(config-ana)# virtual-sensor vs1
ips-ssp(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。

```
ips-ssp(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。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# anomaly-detection-name ad1
ips-ssp(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。

```
ips-ssp(config-ana-vir-ano)# exit
ips-ssp(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。

```
ips-ssp(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。

```
ips-ssp(config-ana-vir)# physical-interface PortChannel0/0
```

ステップ 9　仮想センサー設定を確認します。

```
ips-ssp(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: PortChannel0/0
         subinterface-number: 0 <defaulted>
         -----------------------------------------------
      -----------------------------------------------
      logical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ana-vir)#
```

ステップ 10　分析エンジン モードを終了します。

```
ips-ssp(config-ana-vir)# exit
ips-ssp(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** を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および設定の手順については、「異常検出ポリシーの使用」（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および設定の手順については、「イベント アクション ルール ポリシーの使用」（P.8-7）を参照してください。
- シグニチャ定義の作成および設定の手順については、「シグニチャ定義ポリシーの操作」（P.7-1）を参照してください。

適応型セキュリティ アプライアンスのコンテキストへの仮想センサーの割り当て

シングルコンテキスト モードの場合、仮想センサーをコンテキストに割り当てる必要はありません。マルチコンテキスト モードの場合、IPS SSP 上に仮想センサーを作成した後、それらの仮想センサーを適応型セキュリティ アプライアンス上のセキュリティ コンテキストに割り当てる必要があります。

オプション

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。サポートされているモードは、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）　同じ仮想センサーを 1 つのコンテキストに 2 回割り当てることはできません。

  - *sensor_name*：IPS SSP 上に設定された仮想センサーの名前を指定します。名前が有効でない場合、警告メッセージが表示されます。
  - *mapped_name*：セキュリティ コンテキストが仮想センサーを認識するための名前を指定します。

    （注）　マッピングされた名前は、仮想センサーの本当の名前をコンテキストから隠すために使用され、一般にセキュリティ上または便宜上の理由から、コンテキスト設定をより一般化するために使用されます。マッピングされた名前を使用しなければ、実際の仮想センサー名が使用されます。コンテキスト内の 2 つの異なる仮想センサーに同じマッピングされた名前を使用することはできません。

  - **no**：センサーの割り当てを解除し、ポリシー マップ設定を検索し、そのセンサーを参照しているすべての IPS サブコマンドを削除します。
  - **default**：この仮想センサーをデフォルトに指定します。仮想センサーを指定しないすべてのレガシー IPS 設定は、この仮想センサー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デフォルト仮想センサーは 1 つのみです。別の仮想センサーをデフォルトに指定する場合は、その前に既存のデフォルト仮想センサーのデフォルト フラグをオフにする必要があります。

  - **clear configure allocate-ips**：設定を削除します。
  - **allocate-ips?**：設定済みの仮想センサーのリストを表示します。

- **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す。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ているすべての仮想センサーのマッピングされた名前を表示するために、新しい行が 1 つ追加されます。システム モードでは、このコンテキストに割り当てられた仮想センサーの本当の名前とマッピングされた名前を表示するために、新しい行が 2 つ追加されます。

適応型セキュリティ アプライアンスのコンテキストへの IPS SSP 仮想センサーの割り当て

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。1 つの仮想センサーは複数のコンテキストで共有することができます。共有した場合、それらのコンテキストは、同じ仮想センサーに対してそれぞれ異なるマッピングされた名前（エイリアス）を使用できます。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。

マルチ モードで IPS SSP の仮想センサーを、適応型セキュリティ アプライアンス 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　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 モードをマルチ 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　各コンテキストに 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)# changeto system
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)#
```

設定例

次に、インライン モードですべての IP トラフィックを IPS SSP に迂回させ、何らかの理由で IPS SSP で障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
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-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips inline fail-close
hostname(config-pmap-c)# service-policy my-ids-policy global
```

次に、無差別モードですべての IP トラフィックを IPS SSP に迂回させ、何らかの理由で IPS SSP で障害が発生した場合にはすべての IP トラフィックをブロックする例を示します。

```
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
```

仮想センサーの編集と削除

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
- 説明
- 物理インターフェイス

仮想センサーを編集または削除するには、次の手順を実行します。

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　分析エンジン モードを開始します。

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

ステップ 3　仮想センサー vs1 を編集します。

```
ips-ssp(config-ana)# virtual-sensor vs1
ips-ssp(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。

```
ips-ssp(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。

```
ips-ssp(config-ana-vir)# anomaly-detection
ips-ssp(config-ana-vir-ano)# anomaly-detection-name ad0
ips-ssp(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。

```
ips-ssp(config-ana-vir-ano)# exit
ips-ssp(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。

```
ips-ssp(config-ana-vir)# signature-definition sig0
```

ステップ 8　編集された仮想センサー設定を確認します。

```
ips-ssp(config-ana-vir)# show settings
   name: vs1
   -----------------------------------------------
      description: virtual sensor A default:
      signature-definition: sig0 default: sig0
      event-action-rules: rules0 default: rules0
      anomaly-detection
      -----------------------------------------------
         anomaly-detection-name: ad0 default: ad0
         operational-mode: learn default: detect
      -----------------------------------------------
      physical-interface (min: 0, max: 999999999, current: 0)
      -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ana-vir)##
```

ステップ 9　仮想センサーを削除します。

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

ステップ 10　削除された仮想センサーを確認します。デフォルトの仮想センサー vs0 だけが存在します。

```
ips-ssp(config-ana)# show settings
   global-parameters
   -----------------------------------------------
      ip-logging
      -----------------------------------------------
         max-open-iplog-files: 20 <defaulted>
      -----------------------------------------------
   -----------------------------------------------
   virtual-sensor (min: 1, max: 255, current: 1)
   -----------------------------------------------
      <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)
         -----------------------------------------------
         -----------------------------------------------
      -----------------------------------------------
   -----------------------------------------------
ips-ssp(config-ana)##
```

ステップ 11　分析エンジン モードを終了します。

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

ステップ 12　Enter を押して変更を適用するか、**no** を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および設定の詳細については、「異常検出ポリシーの使用」（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および設定の詳細については、「イベント アクション ルール ポリシーの使用」（P.8-7）を参照してください。
- シグニチャ定義ポリシーの作成および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.7-1）を参照してください。

グローバル変数の設定

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

（注）　Cisco IPS で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のみです。

オプション

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 パラメータを指定します。
  - **max-open-iplog-files**：同時に開くログ ファイルの最大数を指定します。範囲は 20 ～ 100 です。デフォルトは 20 です。

グローバル変数の作成

グローバル変数を作成するには、次の手順を実行します。

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。

```
ips-ssp# configure terminal
ips-ssp(config)# service analysis-engine
ips-ssp(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。

```
ips-ssp(config-ana)# global-parameters
ips-ssp(config-ana-glo)# ip-logging
ips-ssp(config-ana-glo-ip)# max-open-iplog-files 50
```

ステップ 4　グローバル変数設定を確認します。

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

ステップ 5　分析エンジン モードを終了します。

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

ステップ 6　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。