CHAPTER 11

外部製品インターフェイスの設定

この章では、外部製品インターフェイスを設定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。

外部製品インターフェイスについて

（注） Cisco IPS では、CSA MC だけにインターフェイスを追加できます。

外部製品インターフェイスは、外部セキュリティおよび管理製品から情報を受信して処理するように設計されています。これらの外部セキュリティおよび管理製品は、センサー設定情報を自動的に拡張するために使用できる情報を収集します。たとえば、外部製品から受信できる情報のタイプには、ホスト プロファイル（ホスト OS コンフィギュレーション、アプリケーション設定、およびセキュリティ ポスチャ）、および悪意のあるネットワーク アクティビティの原因であると識別された IP アドレスが含まれます。

CSA MC について

CSA MC は、ネットワーク ホストにセキュリティ ポリシーを適用します これには 2 つのコンポーネントがあります。

- ネットワーク ホスト上に存在し、そのホストを保護するエージェント。
- Management Console（MC）：エージェントを管理するアプリケーション。セキュリティ ポリシーの更新をエージェントにダウンロードし、エージェントから操作情報をアップロードします。

CSA MC は、管理している CSA エージェントからホストのポスチャ情報を受信します。また、ネットワークから隔離する必要があると判断された IP アドレスのウォッチ リストを維持します。CSA MC は、ホスト ポスチャ イベントと隔離された IP アドレス イベントという、2 つのタイプのイベントをセンサーに送信します。

ホスト ポスチャ イベント（IPS ではインポートされた OS ID と呼ばれる）には、次の情報が含まれます。

- CSA MC によって割り当てられた一意のホスト ID
- CSA エージェントのステータス
- ホストシステムのホスト名
- ホスト上でイネーブルになっている IP アドレスのセット
- CSA ソフトウェアのバージョン
- CSA のポーリング ステータス
- CSA のテスト モード ステータス
- NAC ポスチャ

たとえば、OS 固有のシグニチャが起動し、ターゲットがその OS を実行している場合、攻撃の関連性は高く、応答の重大度は大きくなります。ターゲットの OS が異なる場合、攻撃の関連性は低く、応答の重大度が小さくなる場合があります。シグニチャの攻撃関連性レーティングは、このホストに対して調整されます。

隔離されたホスト イベント（IPS ではウォッチ リストと呼ばれる）には、次の情報が含まれます。

- IP アドレス
- 隔離の理由
- 規則違反に関連付けられたプロトコル（TCP、UDP、または ICMP）
- 規則ベースの違反が、確立したセッションまたは UDP パケットのどちらに関連付けられているかを示すインジケータ

たとえば、これらいずれかのホストを攻撃者として表示するシグニチャが起動する場合、非常に深刻であると考えることができます。このホストに対するリスク レーティングは高くなります。高める度合いは、ホストが隔離される原因によって異なります。

センサーは、これらのイベントからの情報を使用して、イベント内の情報とホスト ポスチャおよび隔離される IP アドレスのリスク レーティング設定に基づいたリスク レーティングの増加を決定します。

（注） ホスト ポスチャとウォッチ リスト IP アドレス情報は仮想センサーに関連付けられていませんが、グローバル情報として処理されます。

CSA MC と IPS センサー間の安全な通信は、SSL/TLS によって維持されます。センサーは、CSA MC を使用して SSL/TLS 通信を開始します。この通信は相互に認証されます。CSA MC は、X.509 証明書を提供して認証を行います。センサーは、ユーザ名およびパスワード認証を使用します。

（注） イネーブルにできるのは、2 つの CSA MC インターフェイスだけです。

注意 CSA MC を信頼できるホストとして追加し、センサーと通信できるようにする必要があります。

詳細情報

信頼できるホストを追加する手順については、「TLS の信頼できるホストの追加」（P.4-54）を参照してください。

外部製品インターフェイスの問題

外部製品のインターフェイスがホストのポスチャおよび検疫イベントを受信したときに、次の問題が発生する可能性があります。

- センサーが保存できるホストのレコード数には限りがあります。
  - レコード数が 10,000 を超えると、後続のレコードはドロップされます。
  - 10,000 の制限に達した後、9900 未満まで下がると、新しいレコードはドロップされなくなります。
- DHCP のリース期限切れや、無線ネットワーク内での移動などにより、ホストの IP アドレスが変更されたように見えたり、別のホスト IP アドレスが使用されているように見えたりすることがあります。

  IP アドレスの衝突が発生した場合、センサーは、最新のホストのポスチャ イベントが最も正確であると見なします。
- ネットワークには VLAN が異なる IP アドレス範囲の重複が含まれることがありますが、ホストのポスチャには VLAN ID 情報が含まれません。

  指定したアドレス範囲を無視するように、センサーを設定できます。
- ファイアウォールの背後にあるために、CSA MC からホストに到達できないことがあります。

  到達できないホストは除外できます。
- CSA MC イベント サーバで同時に開くことができるサブスクリプションは、デフォルトで最大 10 です。この値は変更できます。

  サブスクリプションを開くには、管理者アカウントとパスワードが必要です。
- CSA データは仮想化されません。センサーでグローバルに扱われます。
- ホストのポスチャの OS および IP アドレスは、パッシブ OS フィンガープリント ストレージに統合されます。これらは、インポートされた OS プロファイルとして表示できます。
- 隔離されたホストは表示できません。
- センサーは、各 CSA MC ホストの X.509 証明書を認識する必要があります。これらを信頼できるホストに追加してください。
- 設定できる外部製品デバイスは、2 台までです。

詳細情報

- OS マップおよび ID の操作の詳細については、「設定済みの OS マップの追加、編集、削除、および移動」（P.7-28）および「OS ID の表示とクリア」（P.7-32）を参照してください。
- 信頼できるホストを追加する手順については、「TLS の信頼できるホストの追加」（P.4-54）を参照してください。

IPS インターフェイスをサポートする CSA MC の設定

（注）　ホスト ポスチャ イベントと隔離された IP アドレス イベントの詳細については、『*Using Management Center for Cisco Security Agents 5.1*』を参照してください。

ホスト ポスチャ イベントと隔離された IP アドレス イベントをセンサーに送信するように、CSA MC を設定する必要があります。

IPS インターフェイスをサポートするように CSA MC を設定するには、次の手順に従います。

ステップ 1　[Events] > [Status Summary] を選択します。

ステップ 2　[Network Status] セクションで、[Host history collection enabled] の横にある [No] をクリックし、次にポップアップ ウィンドウで [Enable] をクリックします。

（注）　ホスト履歴の収集がシステムでグローバルにイネーブルになります。この機能をオンにすると MC ログ ファイルがすぐにいっぱいになる可能性があるので、デフォルトではディセーブルになっています。

ステップ 3　[Systems] > [Groups] を選択し、次に作成する管理者アカウントと併せて使用する新しいグループ（ホストなし）を作成します。

ステップ 4　[Maintenance] > [Administrators] > [Account Management] を選択し、新しい CSA MC 管理者アカウントを作成して MC システムに対する IPS アクセスを提供します。

ステップ 5　**モニタ**のロールを持つ新しい管理者アカウントを作成します。

この新しいアカウントには設定特権が許可されていないので、新しいアカウントを作成すると、MC のセキュリティを維持できます。

センサーに外部製品インターフェイスを設定する場合に必要となるため、管理者アカウントのユーザ名とパスワードを記憶しておいてください。

ステップ 6　[Maintenance] > [Administrators] > [Access Control] を選択し、この管理者アカウントに制限を追加します。

ステップ 7　[Access Control] ウィンドウで、作成した管理者とグループを選択します。

（注）　この設定を保存すると、CSA MC のセキュリティを維持する目的で、この新しい管理者アカウントの MC アクセスがさらに制限されます。

外部製品インターフェイスおよびポスチャ ACL の追加

注意　Cisco IPS では、追加できる外部製品インターフェイスは CSA MC インターフェイスのみです。Cisco IPS は、2 つの CSA MC インターフェイスをサポートします。

CSA MC を外部製品インターフェイスとして追加するには、サービス外部製品インターフェイス サブモードで **cisco-security-agents-mc-settings** *ip-address* コマンドを使用します。

次のオプションが適用されます。

- **enabled {yes | no}**：CSA MC からの情報の受信をイネーブルまたはディセーブルにします。
- **host-posture-settings**：CSA MC から受信したホスト ポスチャの処理方法を指定します。
  - **allow-unreachable-postures {yes | no}**：CSA MC から到達不能なホストのポスチャを許可します。

    CSA MC がホストのポスチャのどの IP アドレス上のホストにも接続を確立できない場合、ホストは到達不能です。このオプションは、IP アドレスが IPS から認識できないポスチャ、またはネットワーク上で重複している可能性のあるポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC から到達不能なホストが IPS からも到達できないようなネットワーク トポロジに最も適しています。たとえば、IPS と CSA MC が同じネットワーク セグメント上にある場合などです。
  - **enabled** {**yes** | **no**}：CSA MC からのホスト ポスチャの受信をイネーブルまたはディセーブルにします。
  - **posture-acls** {**edit** | **insert** | **move**} **name1 {begin | end | inactive | before | after}**：許可または拒否されたポスチャ アドレスのリスト。

    このコマンドは、IP アドレスが IPS から認識できない可能性のあるポスチャ、またはネットワーク上で重複している可能性のあるポスチャのフィルタリングのメカニズムを提供します。
  - **action {permit | deny}**：指定されたネットワーク アドレスに一致するポスチャを許可または拒否します。
  - **network-address** *address*：許可または拒否するポスチャのネットワーク アドレス（x.x.x.x/nn の形式）。
- **password**：CSA MC へのログインに使用するパスワード。
- **port**：CSA MC に接続するための TCP ポート。有効な範囲は 1 ～ 65535 です。デフォルトは 443 です。
- **username**：CSA MC へのログインに使用するユーザ名。
- **watchlist-address-settings**：CSA MC から受信したウォッチ リスト アドレスの処理方法を指定します。
  - **enabled {yes | no}**：CSA MC からのウォッチ リスト アドレスの受信をイネーブルまたはディセーブルにします。
  - **manual-rr-increase**：CSA MC によって攻撃者が手動でウォッチ リストに記載されたために、イベント リスク レーティングに追加される数。有効な範囲は 0 ～ 35 です。デフォルトは 25 です。
  - **packet-rr-increase**：セッションレス パケットベースのポリシー違反が原因で、CSA MC によって攻撃者が手動でウォッチ リストに記載されたために、イベント リスク レーティングに追加される数。有効な範囲は 0 ～ 35 です。デフォルトは 10 です。
  - **session-rr-increase**：セッションベースのポリシー違反が原因で、CSA MC によって攻撃者が手動でウォッチ リストに記載されたために、イベント リスク レーティングに追加される数。有効な範囲は 0 ～ 35 です。デフォルトは 25 です。

（注） CSA MC を信頼できるホストとして追加し、センサーと通信できることを確認します。

外部製品インターフェイスを追加するには、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　外部製品インターフェイス サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service external-product-interface
```

ステップ 3　CSA MC インターフェイスを追加します。

```
sensor(config-ext)# cisco-security-agents-mc-settings 10.89.146.25
sensor(config-ext-cis)#
```

ステップ 4　CSA MC からの情報の受信をイネーブルにします。

```
sensor(config-ext-cis)# enabled yes
```

ステップ 5　デフォルトのポート設定を変更します。

```
sensor(config-ext-cis)# port 80
```

ステップ 6　ログイン設定を設定します。

a. ユーザ名を入力します。

```
sensor(config-ext-cis)# username jsmith
```

b. パスワードを入力して確認します

```
sensor(config-ext-cis)# password
Enter password[]: *******
Re-enter password: *******
sensor(config-ext-cis)#
```

（注）　ステップ 7 ～ 10 は任意です。ステップ 7 ～ 10 を実行しなかった場合は、すべての CSA MC 情報の受信にデフォルト値が使用され、フィルタは適用されません。

ステップ 7　（任意）ウォッチ リスト設定を行います。

a. 外部製品からセンサーにウォッチ リスト情報を渡せるようにします。

```
sensor(config-ext-cis-wat)# enabled yes
```

（注）　ウォッチ リストをイネーブルにしなかった場合、CSA MC から受信したウォッチ リスト情報は削除されます。

b. 手動のウォッチ リスト リスク レーティングの割合を、デフォルトの 25 から変更します。

```
sensor(config-ext-cis-wat)# manual-rr-increase 30
```

c. セッションベースのウォッチ リスト リスク レーティングの割合をデフォルトの 25 から変更します。

```
sensor(config-ext-cis-wat)# session-rr-increase 30
```

d. パケットベースのウォッチ リスト リスク レーティングの割合をデフォルトの 10 から変更します。

```
sensor(config-ext-cis-wat)# packet-rr-increase 20
```

ステップ 8　（任意）外部製品からセンサーにホスト ポスチャ情報を渡せるようにします。

```
sensor(config-ext-cis)# host-posture-settings
sensor(config-ext-cis-hos)# enabled yes
```

（注）　ホスト ポスチャ情報をイネーブルにしなかった場合、CSA MC から受信したホスト ポスチャ情報は削除されます。

ステップ 9　（任意）外部製品から、センサーに到達不能ホストからのホスト ポスチャ情報を渡せるようにします。

```
sensor(config-ext-cis-hos)# allow-unreachable-postures yes
```

（注）　CSA MC がホストのポスチャのどの IP アドレス上のホストにも接続を確立できない場合、ホストは到達不能です。このオプションは、IP アドレスが IPS から認識できないポスチャ、またはネットワーク上で重複している可能性のあるポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC から到達不能なホストが IPS からも到達できないようなネットワーク トポロジに最も適しています。たとえば、IPS と CSA MC が同じネットワーク セグメント上にある場合などです。

ステップ 10　ポスチャ ACL を設定します。

a.　ポスチャ ACL を ACL リストに追加します。

```
sensor(config-ext-cis-hos)# posture-acls insert name1 begin
sensor(config-ext-cis-hos-pos)#
```

（注）　ポスチャ ACL とは、ネットワーク アドレス範囲です。その範囲に対してホスト ポスチャが許可または拒否されます。ポスチャ ACL を使用して、IPS で認識できないか、またはネットワーク全体で重複している可能性がある IP アドレスを持つポスチャをフィルタリングします。

b.　ポスチャ ACL が使用するネットワーク アドレスを入力します。

```
sensor(config-ext-cis-hos-pos)# network-address 171.171.171.0/24
```

c.　ポスチャ ACL が実行するアクション（拒否または許可）を選択します。

```
sensor(config-ext-cis-hos-pos)# action permit
```

ステップ 11　設定を確認できます。

```
sensor(config-ext-cis-hos-pos)# exit
sensor(config-ext-cis-hos)# exit
sensor(config-ext-cis)# exit
sensor(config-ext)# show settings
   cisco-security-agents-mc-settings (min: 0, max: 2, current: 1)
   -----------------------------------------------
      ip-address: 10.89.146.25
      -----------------------------------------------
         interface-type: extended-sdee <protected>
         enabled: yes default: yes
         url: /csamc50/sdee-server <protected>
         port: 80 default: 443
         use-ssl
         -----------------------------------------------
            always-yes: yes <protected>
         -----------------------------------------------
         username: jsmith
         password: <hidden>
         host-posture-settings
```

```
            ---------------------------------------------
               enabled: yes default: yes
               allow-unreachable-postures: yes default: yes
               posture-acls (ordered min: 0, max: 10, current: 1 - 1 active, 0 inactive)
               ---------------------------------------------
               ACTIVE list-contents
               ---------------------------------------------
                  NAME: name1
                  ---------------------------------------------
                     network-address: 171.171.171.0/24
                     action: permit
                  ---------------------------------------------
                  ---------------------------------------------
               ---------------------------------------------
            ---------------------------------------------
            watchlist-address-settings
            ---------------------------------------------
               enabled: yes default: yes
               manual-rr-increase: 30 default: 25
               session-rr-increase: 30 default: 25
               packet-rr-increase: 20 default: 10
            ---------------------------------------------
         ---------------------------------------------
      ---------------------------------------------
sensor(config-ext)#
```

ステップ 12　外部製品インターフェイス サブモードを終了します。

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

ステップ 13　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

信頼できるホストを追加する手順については、「TLS の信頼できるホストの追加」（P.4-54）を参照してください。

外部製品のインターフェイスのトラブルシューティング

外部製品のインターフェイスのトラブルシューティングを行うには、次の点をチェックします。

- インターフェイスがアクティブであることを確認します。そのためには、CLI の **show statistics external-product-interface** コマンドの出力をチェックするか、IDM で [Monitoring] > [Sensor Monitoring] > [Support Information] > [Statistics] を選択し、応答に含まれるインターフェイス状態の行をチェックするか、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択し、応答に含まれるインターフェイス状態の行をチェックします。
- CSA MC IP アドレスが信頼できるホストに追加されていることを確認します。追加していない場合は追加し、数分経ってから再度チェックします。
- ブラウザを使用して、CSA MC でサブスクリプションを開いてから閉じ、サブスクリプション ログイン情報を確認します。
- イベント ストアで CSA MC サブスクリプション エラーをチェックします。

詳細情報

- 信頼できるホストを追加する手順については、「TLS の信頼できるホストの追加」（P.4-54）を参照してください。
- イベントを表示する手順については「イベント ストアのイベントのクリア」（P.7-43）を参照してください。