CHAPTER 15

外部製品インターフェイスの設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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、外部製品インターフェイスの設定方法を説明します。次の事項について説明します。

外部製品インターフェイスについて

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 設定、アプリケーション設定、セキュリティ態勢）および悪意のあるネットワーク アクティビティを引き起こしていると識別されている IP アドレスを含みます。

（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。

CSA MC について

CSA MC は、ネットワーク ホストでセキュリティ 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。
- 管理コンソール（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別した 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 イベントの 2 種類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 識別名と呼ばれる）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 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一連の IP アドレス
- CSA ソフトウェアのバージョン
- CSA ポーリング ステータス
- CSA テスト モード ステータス
- NAC のポスチャ

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、応答の重大度は一般に小さくなります。シグニチャの攻撃関連性レーティングは、このホストに合わせて調整されます。

隔離ホスト 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
- 隔離理由
- ルール違反に関連付けられたプロトコル（TCP、UDP、または ICMP）
- ルールベースの違反が、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、これらのホストのいずれかを攻撃者としてリストしているシグニチャが起動された場合、非常に重大であると見なされます。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。増加の度合いは、ホストが隔離対象となった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、イベントの情報とホスト ポスチャおよび隔離された IP アドレスのリスク レーティング コンフィギュレーション設定に基づいて、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、仮想センサーには関連付けられませんが、グローバル情報として扱われます。

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 との 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 証明書を用意して認証を行います。センサーは、ユーザ名とパスワードによる認証を使用します。

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

注意　信頼できるホストとして CSA MC を追加し、センサーと通信できるようにする必要があります。CSA MC を信頼できるホストとして追加するには、[Configuration] > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add] を選択します。

詳細情報

信頼できるホストを追加する手順については、「信頼できるホストの追加」（P.12-10）を参照してください。

外部製品インターフェイスの問題

外部製品インターフェイスがホスト ポスチャ イベントおよび隔離イベントを受信すると、次の問題が発生する可能性があります。

- センサーでは、一定の数のホスト レコードだけを格納できます。
  - 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 の制限に達してから、9900 未満に下がると、新規レコードはドロップされなくなります。
- ホストは、たとえばワイヤレス ネットワークでの DHCP のリースの期限切れまたは移動のために、IP アドレスを変更するか、別のホストの IP アドレスを使用するように見せることができます。IP アドレスの競合の場合、センサーは、最近のホスト ポスチャ イベントが最も正確であると推定します。
- 1 つのネットワークでは、異なった VLAN で IP アドレス範囲が重複することは可能ですが、ホスト ポスチャには VLAN ID 情報は含まれません。指定したアドレス範囲を無視するようセンサーを設定できます。
- ホストはファイアウォールの背後にあるため、CSA MC からは到達不能な可能性があります。到達不能ホストは除外できます。
- CSA MC イベント サーバでは、デフォルトで最大 10 のサブスクリプションを開くことができます。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。これは、センサーによってグローバルに扱われます。
- ホスト ポスチャの OS と 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見なすことができます。
- 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。これは、信頼できるホストとして追加する必要があります。
- 最大 2 つの外部製品デバイスを設定できます。

詳細情報

- OS マップと ID の操作の詳細については、「設定した OS マップの追加、編集、削除、および移動」（P.9-30）および「OS ID の設定」（P.17-26）を参照してください。
- 信頼できるホストを追加するための手順については、「信頼できるホストの追加」（P.12-10）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 イベントおよび隔離された 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 CSA MC を設定するには、次の手順を実行します。

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、続いて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全体で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] を選択して、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] を選択して、新しい CSA MC 管理者アカウントを作成し、IPS から MC システムにアクセスできるようにします。

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ときに必要になるため、この管理者アカウントのユーザ名とパスワードを記録しておいてください。

ステップ 6　[Maintenance] > [Administrators] > [Access Control] を選択して、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、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て、CSA MC のセキュリティが維持されます。

外部製品インターフェイスの設定

ここでは、外部製品インターフェイスの設定方法について説明します。次の事項について説明します。

[External Product Interfaces] パネル

（注） 外部製品インターフェイスおよびポスチャ ACL を追加、編集、および削除するには、管理者でなければなりません。

センサーで CSA MC から情報を受信して処理できるように、CSA MC のインターフェイスを追加するには、[External Product Interfaces] パネルを使用します。

注意 信頼できるホストとして外部製品を追加し、センサーと通信できるようにする必要があります。信頼できるホストを追加するには、[Configuration] > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add] を選択します。

[External Product Interfaces] パネルのフィールド定義

[External Product Interfaces] パネルには、次のフィールドがあります。

- [IP Address]：外部製品の IP アドレス。
- [Enabled]：外部製品インターフェイスがイネーブルかどうかを示します。
- [Port]：通信に使用するポートを指定します。
- [TLS Used]：安全な通信が使用されているかどうかを示します。
- [Username]：CSA MC に接続するユーザ ログイン名を示します。
- [Host Posture Settings]：CSA MC から受信するホスト ポスチャの処理方法を示します。
  - [Enabled]：ホスト ポスチャの受信がイネーブルになっていることを示します。ディセーブルにした場合、CSA MC から受信したホスト ポスチャ情報は削除されます。
  - [Allow Unreachable]：CSA MC によって到達不能なホストのホスト ポスチャ情報の受信を許可または拒否します。

    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 から参照可能でないポスチャ、またはネットワーク全体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 から到達可能ではないホストが IPS からも到達可能ではない（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）ネットワーク トポロジで最も適切です。

  - [Posture ACLs]：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るネットワーク アドレス範囲を指定します。このオプションは、IPS で認識できない、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するメカニズムを提供します。
- [Watch List Settings]：CSA MC から受信するウォッチ リスト設定の処理方法を示します。
  - [Enabled]：ウォッチ リストの受信がイネーブルになっていることを示します。ディセーブルにした場合、CSA MC から受信したウォッチ リスト情報は削除されます。
  - [Manual RR Increase]：手動ウォッチ リストのリスク レーティングを高める必要のあるパーセンテージを示します。
  - [Session RR Increase]：セッションベースのウォッチ リストのリスク レーティングを高める必要のあるパーセンテージを示します。
  - [Packet RR Increase]：パケットベースのウォッチ リストのリスク レーティングを高める必要のあるパーセンテージを示します。
- [SDEE URL]：IPS が SDEE 通信を使用して情報を取得するために使用する CSA MC 上の URL を示します。IPS が通信している CSA MC のソフトウェア バージョンに基づいて、URL を次のように設定する必要があります。
  - CSA MC バージョン 5.0 の場合：/csamc50/sdee-server
  - CSA MC バージョン 5.1 の場合：/csamc51/sdee-server
  - CSA MC バージョン 5.2 以上の場合：/csamc/sdee-server（デフォルト値）

[Add External Product Interface]/[Edit External Product Interface] ダイアログボックスのフィールド定義

[Add External Product Interface]/[Edit External Product Interface] ダイアログボックスには、次のフィールドがあります。

- [External Product's IP Address]：外部製品の IP アドレス。
- [Enable receipt of information]：センサーで外部製品インターフェイスから情報を受信できるようにします。

（注） オフにした場合は、このデバイスからのすべてのホスト ポスチャ情報および隔離情報がセンサーから消去されます。

- [Communication Settings]：SDEE URL および TLS を参照でき、ポートを変更できます。
  - [SDEE URL]：IPS が SDEE 通信を使用して情報を取得するために使用する CSA MC 上の URL を示します。IPS が通信している CSA MC のソフトウェア バージョンに基づいて、URL を次のように設定する必要があります。CSA MC バージョン 5.0 の場合：/csamc50/sdee-server。CSA MC バージョン 5.1 の場合：/csamc51/sdee-server。CSA MC バージョン 5.2 以上の場合：/csamc/sdee-server（デフォルト値）。
  - [Port]：通信に使用するポートを指定します。
  - [Use TLS]：安全な通信が使用されていることを示します。

    この値は変更できません。
- [Login Settings]：CSA MC へのログインに必要な資格情報を指定できます。
  - [Username]：CSA MC へのログインに使用するユーザ名を入力できます。

  - [Password]：ユーザにパスワードを割り当てることができます。
  - [Confirm Password]：パスワードを確認できます。
- [Watch List Settings]：CSA MC から受信するウォッチ リスト設定の処理方法を設定できます。
  - [Enable receipt of watch list]：ウォッチ リスト情報の受信をイネーブルまたはディセーブルにすることができます。ディセーブルにした場合、CSA MC から受信したウォッチ リスト情報は削除されます。
  - [Manual Watch List RR Increase]：手動ウォッチ リストのリスク レーティングのパーセンテージを高めることができます。
  - [Session-based Watch List RR Increase]：セッションベースのウォッチ リストのリスク レーティングのパーセンテージを高めることができます。
  - [Packet-based Watch List RR Increase]：パケットベースのウォッチ リストのリスク レーティングのパーセンテージを高めることができます。
- [Host Posture Settings]：CSA MC から受信するホスト ポスチャの処理方法を示します。
  - [Enable receipt of host postures]：ホスト ポスチャ情報の受信をイネーブルまたはディセーブルにすることができます。ディセーブルにした場合、CSA MC から受信したホスト ポスチャ情報は削除されます。
  - [Allow unreachable hosts' postures]：CSA MC から到達不能なホストに関するホスト ポスチャ情報の受信を許可または拒否します。

    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 から参照可能でないポスチャ、またはネットワーク全体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 から到達可能ではないホストが IPS からも到達可能ではない（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）ネットワーク トポロジで最も適切です。
- [Permitted and Denied Host Posture Addresses]：許可または拒否されるホスト ポスチャ ACL を追加できます。
  - [Name]：ポスチャ ACL の名前。
  - [Active]：このポスチャ ACL がアクティブかどうかを示します。
  - [IP Address]：ポスチャ ACL の IP アドレス。
  - [Network Mask]：ポスチャ ACL のネットワーク マスク。
  - [Action]：ポスチャ ACL が行うアクション（拒否または許可）。

[Add Posture ACL]/[Edit Posture ACL] ダイアログボックスのフィールド定義

[Add Posture ACL]/[Edit Posture ACL] ダイアログボックスには、次のフィールドがあります。

- [Name]：ポスチャ ACL の名前。
- [Active]：このポスチャ ACL がアクティブかどうかを示します。
- [IP Address]：ポスチャ ACL の IP アドレス。
- [Network Mask]：ポスチャ ACL のネットワーク マスク。
- [Action]：ポスチャ ACL が行うアクション（拒否または許可）。

外部製品インターフェイスおよびポスチャ ACL の追加、編集、および削除

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 インターフェイスだけです。Cisco IPS では、2 つの CSA MC インターフェイスをサポートしています。

（注）　信頼できるホストとして外部製品を追加し、センサーと通信できることを確認してください。信頼できるホストを追加するには、[Configuration] > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add] を選択します。

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 IDM にログインします。

ステップ 2　[Configuration] > [Sensor Management] > [External Product Interfaces] を選択し、[Add] をクリックして外部製品インターフェイスを追加します。

ステップ 3　[External Product's IP Address] フィールドに、外部製品の IP アドレスを入力します。

ステップ 4　[Enable receipt of information] チェックボックスをオンにして、外部製品からセンサーに情報を渡せるようにします。

ステップ 5　[Port] フィールドで、必要に応じて、デフォルト ポートの 443 を変更します。

（注）　[Communication Settings] の下では、ポート値だけを変更できます。

ステップ 6　ログイン設定を行います。

a.　[Username] フィールドに、外部製品にログインできるユーザのユーザ名を入力します。

b.　[Password] フィールドに、ユーザが使用するパスワードを入力します。

c.　[Confirm Password] フィールドで、パスワードを再入力します。

（注）　ステップ 7 ～ 15 は任意です。ステップ 7 ～ 15 を実行しなかった場合は、デフォルト値を使用して、フィルタの適用なしにすべての CSA MC 情報が受信されます。

ステップ 7　（任意）ウォッチ リストを設定します。

a.　[Enable receipt of watch list] チェックボックスをオンにして、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。

（注）　[Enable receipt of watch list] チェックボックスをオフにした場合、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.　[Manual Watch List RR Increase] フィールドでは、パーセンテージをデフォルトの 25 から変更できます。有効な範囲は 0 ～ 35 です。

c.　[Session-based Watch List RR increase] フィールドでは、パーセンテージをデフォルトの 25 から変更できます。有効な範囲は 0 ～ 35 です。

d. [Packet-based Watch List RR Increase] フィールドでは、パーセンテージをデフォルトの 10 から変更できます。有効な範囲は 0 ～ 35 です。

ステップ 8　（任意）[Enable receipt of host postures] チェックボックスをオンにして、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。

（注）　[Enable receipt of host postures] チェックボックスをオフにした場合、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）[Allow unreachable hosts' postures] チェックボックスをオンにして、到達不能なホストからのホスト ポスチャ情報を外部製品からセンサーに渡せるようにします。

（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 から参照可能でないポスチャ、またはネットワーク全体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 から到達可能ではないホストが IPS からも到達可能ではない（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）ネットワーク トポロジで最も適切です。

ステップ 10　（任意）ポスチャ ACL を追加するには、[Add] をクリックします。

（注）　ポスチャ ACL とは、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る、ネットワーク アドレス範囲です。ポスチャ ACL を使用して、IPS で認識できない、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。

ステップ 11　（任意）[Name] フィールドに、ポスチャ ACL の名前を入力します。

ステップ 12　（任意）[Active] フィールドで、[Yes] オプション ボタンをクリックして、ポスチャ ACL をアクティブにします。

ステップ 13　（任意）[IP Address] フィールドに、ポスチャ ACL で使用する IP アドレスを入力します。

ステップ 14　（任意）[Network Mask] フィールドに、ポスチャ ACL で使用するネットワーク マスクを入力します。

ステップ 15　（任意）[Action] ドロップダウン リストで、ポスチャ ACL が実行するアクション（[Deny] または [Permit]）を選択します。

ヒント　変更を取り消して、[Add Posture ACL] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 16　（任意）[OK] をクリックします。新しいポスチャ ACL が、[Add External Product Interface] ダイアログボックスの [Host Posture Setting] リストに表示されます。[Move Up] ボタンおよび [Move Down] ボタンを使用して、作成したポスチャ ACL をリオーダーできます。

ステップ 17　既存のポスチャ ACL を編集するには、ACL を選択し、[Edit] をクリックします。

ステップ 18　[IP Address] フィールド、[Network Mask] フィールド、および [Action] フィールドを編集するか、[No] オプション ボタンをクリックしてアクティブ状態を非アクティブに変更します。

ヒント　変更を廃棄して、[Edit Posture ACL] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 19　[OK] をクリックします。編集したポスチャ ACL が、[Add External Product Interface] ダイアログボックスの [Host Posture Setting] リストに表示されます。

ステップ 20　ポスチャ ACL をリストから削除するには、キーを選択し、[Delete] をクリックします。新しいポスチャ ACL は、[Add External Product Interface] ダイアログボックスの [Host Posture Setting] リストに表示されなくなりました。

ステップ 21　[OK] をクリックします。これで、外部製品インターフェイスが [External Product Interfaces] パネルの [Management Center for Cisco Security Agents] リストに表示されるようになりました。

ヒント　変更を廃棄して、[Add External Product Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 22　外部製品インターフェイスを編集するには、そのインターフェイスを選択し、[Edit] をクリックします。

ステップ 23　ダイアログボックス内のフィールドに必要なすべての変更を加えます。

ヒント　変更を廃棄して、[Edit External Product Interface] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 24　[OK] をクリックします。編集した外部製品インターフェイスが [External Product Interfaces] パネルの [Management Center for Cisco Security Agents] リストに表示されます。

ステップ 25　外部製品インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] をクリックします。外部製品インターフェイスは [External Product Interfaces] パネルの [Management Center for Cisco Security Agents] リストに表示されなくなりました。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 26　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

外部製品インターフェイスのトラブルシューティング

外部製品インターフェイスをトラブルシューティングするには、次の点を確認してください。

- CLI で **show statistics external-product-interface** コマンドの出力を調べて、インターフェイスがアクティブであることを確認するか、IDM で [Monitoring] > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答で Interface state 行を確認します。
- CSA MC の IP アドレスを信頼できるホストに追加したことを確認します。追加することを忘れた場合は、追加して、数分待ってから、再度確認します。
- 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閉じることによって、サブスクリプションのログイン情報を確認します。
- CSA MC サブスクリプション エラーについては、イベント ストアを確認してください。

詳細情報

- 信頼できるホストを追加するための手順については、「信頼できるホストの追加」（P.12-10）を参照してください。

- イベントを表示するための手順については、「イベントのモニタリング」（P.17-2）を参照してください。