



第7章 ホストベース IDS および IPS デバイスの設定

ホストベースの侵入検知および侵入防御デバイスは、ネットワークレベルではなく、ホストレベルで認識される攻撃の詳細を MARS に提供します。また、ホストのオペレーティングシステムや攻撃防御の成功に関する情報も表示します。どちらの情報も、フォールス ポジティブ分析に特化したデータを提供します。

この章では、次に示すホストベース IDS および IPS デバイスをブートストラップして、MARS に追加する方法を示します。

- ・ Intercept Intercept 2.5 および 4.0
- ・ Cisco Security Agent 4.x デバイス

Intercept Intercept 2.5 および 4.0

Intercept 側の設定

Intercept エージェント情報の CSV ファイルへの抽出 (Intercept バージョン 2.5 の場合)



注 Intercept エージェント情報は、Intercept コンソールのデータベース ファイルに保存されます。

Intercept エージェントを追加するように MARS を設定すると、エージェントごとにマッピングを入力しなくても、Intercept コンソールでデータベース ファイルからエージェントを抽出できます。

バージョン 2.5 の Intercept エージェント用の CSV ファイルを作成する手順

ステップ 1 ディレクトリ Program Files\Cisco IDS\Console\Database に移動して、ファイル CoreShield.mdb を別のディレクトリ (C:\temp など) にコピーします。

ステップ 2 コピーされた CoreShield.mdb を Microsoft Access で開いて、「Agents」テーブルに移動します。

ステップ 3 テーブルをファイル Agents.txt にエクスポートして、このファイルのフォーマットとして CSV を選択します。

ステップ 4 Agents.txt を、MARS ボックスによるロードが可能な特定のディレクトリにコピーします。

サンプルの agents.txt ファイルは次のようになります。

```
1,3,"entercept1",6,1,1,1,438,1,"127.0.0.1",0,,1051055867,2086
```

フィールドは次のとおりです。AgentID、AgentTypeID、ComputerName、ComputerType、

NewFlag、StatusID、OperatingModeID、VersionID、VersionModelID、IP、License、Note、NoConnection、および UpTime。

SNMP トラップの宛先の定義

ステップ 1 Entercept コンソールにログインします。

ステップ 2 **Configuration** をクリックします。

ステップ 3 **Address Book** タブをクリックします。

ステップ 4 All Contacts ツリーで、**SNMP Trap** をクリックします。

ステップ 5 プラス(+) ボタンをクリックします。

ステップ 6 New SNMP Trap ページで、次の処理を実行します。

- a. MARS アプライアンスの **Alias** を入力します。
 - b. **Privilege** レベルを Global に設定します。
 - c. **Status** を Enabled に設定します。
 - d. DNS サーバが名前を解決できる場合は、MARS アプライアンスの名前を入力します。それ以外の場合は、IP アドレスを使用します。
 - e. **Community** フィールドにコミュニティ スtring の名前を入力します。
 - f. **Port** 番号を入力します。
 - g. **Protocol** を選択します。
-

MARS に送信される SNMP トラップの定義

ステップ 1 **Notifications** タブをクリックします。

ステップ 2 プラス(+) ボタンをクリックします。

ステップ 3 General タブの名前フィールドに、通知名を入力します。

ステップ 4 **Agent Groups** タブをクリックして、**All Agents** オプション ボタンを選択します。

ステップ 5 **Security Events** タブをクリックして、**Events by Severity Levels** オプション ボタンを選択します。目的のイベント (**High**、**Medium**、**Low**、および **Information**) を選択します。

ステップ 6 **System Events** タブをクリックして、**Events by Severity Levels** オプション ボタンを選択します。目的のイベント (**Error**、**Warning**、および **Information**) を選択します。

ステップ 7 **Address Book** タブをクリックして、Available Destinations フィールド内の宛先をクリックします。Down 矢印をクリックして、Selected Destinations フィールドに宛先を移動します。

ステップ 8 **OK** をクリックして、プログラムを終了します。

MARS 側の設定

Entercept デバイスを追加するには、2 つの手順を実行します。まず、コンソール自体の設定情報を追加します。次に、エージェントを追加します。

コンソールの設定情報の追加

ステップ 1 Admin > Security and Monitor Devices > Add の順にクリックします。

ステップ 2 Device Type リストで、Add SW Security apps on a new host または Add SW security apps on existing host を選択します。

ステップ 3 新しいホストを追加する場合は、Device Name にデバイス名、IP addresses に IP アドレスを入力します。

ステップ 4 Apply をクリックします。

ステップ 5 Reporting Applications タブをクリックします。

ステップ 6 Select Application リストで、Entercept 2.5 or 4.0 を選択します。

ステップ 7 Add をクリックします。

ステップ 8 Console Name を入力します。

ステップ 9 センサであるかどうかを確認するための「Is Sensor」チェックボックスをオンにします。

ステップ 10 Agent Name にセンサのエージェント名を入力します。コンソールがエージェントである場合は、この値がエージェント名となります。

Management Console

→ *Console Name:

→ Is Sensor

*Agent Name:

Cancel

Submit

143220

ステップ 11 Submit をクリックします。

これでエージェントを追加することができます。

Entercept エージェントを手動で追加する手順

ステップ 1 Add Agent をクリックします。

ステップ 2 エージェントをすでに稼働しているデバイスを選択するか、または Add New を選択します。

ステップ 3 新しいデバイスを追加するには、Device Name、Agent Name、および Reporting IP アドレスを入力します。

・ 最初のインターフェイスには、IP アドレスおよびマスクを入力します。

- ・ インターフェイスが複数ある場合は、**Add Interface** をクリックして、新しいインターフェイスの IP アドレスおよびマスクを追加します。

ステップ 4 Submit をクリックします。

シードファイルによる Entercept エージェントの追加

ステップ 1 Load From CSV をクリックします。

ステップ 2 FTP サーバ情報および CSV (カンマ区切り値) ファイルの場所を入力します。

- ・ Entercept Agent CSV ファイルを生成する必要がある場合は、「Entercept 側の設定」を参照してください。

ステップ 3 Submit をクリックします。

Cisco Security Agent 4.x デバイス

Cisco Security Agent (CSA) を MARS のレポート デバイスとしてイネーブルにするには、CSA Management Console (CSA MC) をレポート デバイスとして特定する必要があります。CSA MC はモニタ対象の CSA エージェントからアラートを受信して、これらのアラートを SNMP (簡易ネットワーク管理プロトコル) 通知として MARS に転送します。

MARS が SNMP 通知を受信した場合、通知内の送信元 IP アドレスは、転送した CSA MC でなく、イベントのトリガー元である CSA エージェントの IP アドレスになります。したがって、MARS は、イベントをトリガーする可能性のある CSA エージェントごとに、ホストを定義する必要があります。これらの定義は、CSA MC のデバイス定義のサブコンポーネントとして追加されます。

リリース 4.1.1 以降の MARS アプライアンスは、アラートを生成するときに CSA エージェントを検出するので、手動で CSA エージェントを定義する必要はありません。MARS はアラートを解析して、CSA エージェントのホスト名を識別したり、ホスト OS (オペレーティング システム) を検出したりします。MARS はこの情報を使用して、定義されていないエージェントを CSA MC の子として追加します。CSA MC は Generic Windows (すべての Windows) または Generic (Unix または Linux) オペレーティング システム値を持つホストとなります。CSA MC の定義は引き続き必要ですが、各エージェントの定義は必要ありません。検出された CSA エージェントのデフォルトのトポロジー表現は、クラウドです。



注 未知の CSA エージェントから送信された最初の SNMP 通知は、CSA MC から送信されているように認識されます。MARS はこの通知を解析して、検出済みの設定を使用し、CSA MC の子エージェントを定義します。エージェントが定義されると、以降のすべてのメッセージは CSA エージェントから送信されているように認識されます。

4.1.1 より前のリリースでは、手動、またはエクスポートされたホスト ファイル (「ファイルへの CSA エージェント情報のエクスポート」で定義) を使用して、エージェントを個別に追加する必要がありました。



注 4.1.1 より前のリリースでは、CSA はデバイス タイプ *Cisco CSA 4.0* で識別されていました。アップグレードを実行するときに、すべての Cisco CSA 4.0 デバイスの名前は *Cisco CSA 4.x* に変更されました。この新しい名前には、Cisco CSA 4.0 および 4.5 のサポートが含まれています。

ここで説明する内容は、次のとおりです。

- ・ 必要なデータを生成するための CSA Management Center の設定
- ・ MARS での CSA MC デバイスの追加および設定
- ・ CSA エージェントのインストールに関するトラブルシューティング

必要なデータを生成するための CSA Management Center の設定

CSA をブートストラップするには、SNMP 通知を MARS アプライアンスに転送するように CSA MC を設定します。MARS でのインポートが可能なフォーマットで CSA エージェントリストをエクスポートすることもできます。ただし、MARS が情報を生成するときにエージェントが検出されるため、このエクスポート処理は必須ではありません。

ここで説明する内容は、次のとおりです。

- ・ SNMP 通知を MARS に転送するための CSA MC の設定
- ・ CSA エージェント情報のファイルへのエクスポート

SNMP 通知を MARS に転送するための CSA MC の設定

唯一必要な設定は、CSA MC が受信した SNMP 通知をエージェントから MARS に転送するように設定することです。これらの通知から、MARS はエージェントおよび関連する設定を検出できます。MARS がネットワークで発生しているホストレベル アクティビティの情報を取得するのも、これらのイベントからです。

MARS アプライアンスにすべての通知を転送するための手順は、次のとおりです。

ステップ 1 CiscoWorks Server デスクトップにログインします。

ステップ 2 ナビゲーション ツリーで、**VPN/Security Management Solution > Management Center > Security Agents** の順に選択します。

ステップ 3 Management Center 画面で、**Alerts** リンクをクリックします。

ステップ 4 **New** をクリックします。

ステップ 5 Name and Description フィールドに、SNMP 通知の名前および説明を入力します。

ステップ 6 下にスクロールして、**SNMP** チェックボックスをオンにします。

ステップ 7 Community name フィールドに、SNMP 通知のコミュニティ名を入力します。

ステップ 8 Manager IP address フィールドに、MARS の IP アドレスを入力します。

ステップ 9 **Save** をクリックして、プログラムを終了します。

CSA エージェント情報のファイルへのエクスポート

MARS 4.1.1 のリリースでは、デバイスが SNMP 通知を CSA MC に送信するときに Cisco CSA エージェントが検出されるため、エージェントを個別に定義する必要はありません。



注 次の説明は、Microsoft Internet Explorer を使用して CSA MC Web インターフェイスにアクセスする場合に、Cisco CSA 4.x に適用されます。

すべてのホスト レポートをタブ区切りファイルとしてエクスポートする手順は、次のとおりです。

ステップ 1 URL 内で完全修飾ドメイン名を使用してコンソールにアクセスし、CSA MC にログインします。

CSA MC にアクセスする場合は、URL 内で完全修飾ドメイン名を使用する必要があります。CiscoWorks Desktop を使用して CSA MC を起動した場合は、ActiveX レポートが表示されません。

ステップ 2 **Reports > Host Details** の順にクリックします。

ステップ 3 **New** をクリックします。

ステップ 4 **Groups** で <All Hosts>を、**Viewer Type** で **ActiveX (IE only)** を選択します。

ステップ 5 **View report** をクリックします。

ホストの詳細を示すウィンドウが表示されます。

ステップ 6 **Export** をクリックし、**Excel 5.0 Document** タイプへのエクスポートを選択します。

ステップ 7 **Name** ボックスで、エクスポートするファイルの名前を識別します (csahosts.xls など)。

ステップ 8 エクスポートされたファイルを Excel で開いて、**[ファイル] > [名前を付けて保存...]** の順にクリックします。

ステップ 9 **[ファイルの種類]** ボックスで、**[テキスト (タブ区切り) (*.txt)]** をクリックします。

ステップ 10 **[ファイル名]** ボックスに、このファイルの名前を入力し (csahosts.txt など)、**[保存]** をクリックします。

ステップ 11 生成されたファイルを、MARS アプライアンスによるアクセスが可能な FTP (ファイル転送プロトコル) サーバにアップロードします。

MARS HTML インターフェイスに CSA デバイスを追加する場合は、このファイルに戻ります (「MARS での CSA MC デバイスの追加および設定」を参照)。

MARS での CSA MC デバイスの追加および設定

エージェントを識別する前に、MARS に CSA MC を追加する必要があります。すべての CSA エージェントは通知を CSA MC に転送し、CSA MC は SNMP 通知を MARS に転送します。CSA MC を定義したら、デバイスをアクティブにします。MARS はその CSA MC で管理されるエージェントを検出できます。ただし、これらのエージェントは手動で選択することも可能です。

MARS に CSA MC を追加する手順は、次のとおりです。

ステップ 1 **Admin > Security and Monitor Devices > Add** の順にクリックします。

ステップ 2 **Device Type** リストで、**Add SW security apps on a new host** または **Add SW security apps on existing host** を選択します。

ステップ 3 新しいホストを追加する場合は、**Device Name** にデバイス名、**IP addresses** に IP アドレスを入力します。

ステップ 4 **Apply** をクリックします。

ステップ 5 **Reporting Applications** タブをクリックします。

ステップ 6 **Select Application** リストで、**Cisco CSA 4.x** を選択します。

ステップ 7 **Add** をクリックします。

ステップ 8 Management Console ページが表示されます。

Management Console

Add or edit agents for this csa management console.

Add Agent

Edit Agent

Delete Agent

Load From File

Cancel

Submit

143194

ステップ9 Submit をクリックしてから、Done をクリックします。

ステップ10 次のいずれかの操作を実行します。

- ・ 変更を保存して、CSA エージェントの自動検出を許可する場合は、**Submit** をクリックしてから、**Done** をクリックします。
- ・ エクスポートされたホスト レポートを使用してエージェントを追加する場合は、「ファイルからの CSA エージェントの追加」に進んでください。
- ・ 単一のエージェントを手動で追加する場合は、「手動による CSA エージェントの追加」に進んでください。

手動による CSA エージェントの追加

CSA エージェントを CSA MC の子として手動で追加することができます。この機能を使用すると、通知を生成しなかったエージェントを含めて、すべてのエージェントを表すことができます。

CSA エージェントを手動で追加する手順は、次のとおりです。

ステップ1 Admin > Security and Monitoring Devices の順にクリックします。

ステップ2 デバイス リストで、Cisco CSA Management Center で稼働するホストを選択し、**Edit** をクリックします。

ステップ3 Reporting Applications タブをクリックし、Device Type リストで **Cisco CSA Management Center** を選択し、**Edit** をクリックします。

ステップ4 Add Agent をクリックします。

ステップ5 次のいずれかの操作を実行します。

- ・ 既存デバイスを選択して、**Edit Existing** をクリックし、ステップ8に進みます。
ホスト名、レポート IP アドレス、および 1 つ以上のインターフェイスに値が読み込まれた状態で、ページが表示されます。
- ・ **Add New** をクリックして、ステップ6に進みます。

→ A CSA agent will be added to this device.

→ *Device Name:

→ Reporting IP: ...

Add Interface
Remove Interface

Name:	IP Address:	Network Mask:
<input type="checkbox"/> ether0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Cancel
Submit

143192

ステップ6 Device Name フィールドに、CSA エージェントが常駐するホストの名前を入力します。

このデバイスの DNS エントリを反映した値を入力します。

ステップ7 Reporting IP フィールドに、CSA MC にログを送信するためにエージェントが使用する IP アドレスを入力します。

ステップ8 インターフェイス名、IP アドレス、およびネットワーク マスクを指定して、このホストに設定する各インターフェイスを定義します。新しいインターフェイスを追加するには、**Add Interface** をクリックします。

インターフェイスの設定は、攻撃パスの計算に使用されます。各インターフェイスを定義して、デュアルホーミング ホストを識別することが、非常に重要です。

ステップ 9 **Submit** をクリックしてから、**Done** をクリックします。

ステップ 10 このデバイスをアクティブにするには、**Activate** をクリックします。

ファイルからの CSA エージェントの追加

CSA エージェントがインストールされたホストの完全なリストを追加するには、CSA MS からすべてのホスト レポートをエクスポートして、MARS にそのファイルをインポートします。エクスポート ファイルを使用してエージェントを追加する唯一の利点は、エージェントから送信されて受信した最初の通知が、CSA MS の影響を受けないことです。

CSA エージェントをファイルから追加する手順は、次のとおりです。

ステップ 1 **Admin > Security and Monitoring Devices** の順にクリックします。

ステップ 2 デバイス リストで、Cisco CSA Management Center で稼働するホストを選択し、**Edit** をクリックします。

ステップ 3 **Reporting Applications** タブをクリックし、Device Type リストで **Cisco CSA Management Center** を選択し、**Edit** をクリックします。

ステップ 4 **Load From File** をクリックします。

Remote File Location:

→ *IP Address:	<input type="text"/>
→ *User Name:	<input type="text"/>
→ *Password:	<input type="text"/>
→ *Path:	<input type="text"/>
→ *File Name:	<input type="text"/>

143193



注意 ファイルはタブ区切りファイルとしてフォーマットする必要があります。CSV ファイルは使用できません。CSA MC で管理される CSA エージェントのタブ区切りファイルを生成するには、「CSA エージェント情報のファイルへのエクスポート」を参照してください。

ステップ 5 IP Address フィールドに、エクスポートされたホスト ファイルを格納した FTP サーバのアドレスを入力します（「CSA エージェント情報のファイルへのエクスポート」を参照）。

ステップ 6 User Name フィールドに、FTP サーバとの認証に使用するアカウントの名前を入力します。

ステップ 7 Password フィールドに、ステップ 6 で指定されたアカウントに対応するパスワードを入力します。

ステップ 8 Path フィールドに、ファイルが格納されたフォルダのパスを入力します。このファイルがルート フォルダに格納されている場合は、このフィールドにバックslash (\) を指定する必要があります。この値のフォーマットは、\

ステップ 9 File Name フィールドに、タブ区切りファイルの名前を入力します。

ステップ 10 **Submit** をクリックします。

次のメッセージが表示され、ホストが CSA MC のエージェントとして追加されます。

Success:
Status:OK

ステップ 11 Done をクリックします。

CSA エージェントのインストールに関するトラブルシューティング

CSA エージェントをファイルからインポートすると、次のメッセージが表示されることがあります。

表 7-1 CSA エージェントをファイルからインポートする場合のエラーおよびステータス メッセージ

メッセージ	説明/問題
Status:NumberFormatException occurred parsing the file at line X	タブ区切りファイルでなく CSV ファイルをインポートした場合に発生します。行番号が変わります。
Error Occurred: Status:DbDevice occurred parsing the file at line -1	重複したファイルをインポートした場合に発生します。これは、すべてのエージェントおよび CSA MC を削除した場合でも同様です。
Success: Status:OK	タブ区切りファイルを使用して、CSA エージェントが正常にインポートされています。
Error Occurred: Status:FileNotFoundException	ファイルが指定したパスに存在しません。パスが FTP サーバのルートにある場合は、パス値として \ を追加したかどうかを確認してください。
Error Occurred: Status:NoRouteToHostException	識別された FTP サーバに MARS アプライアンスが到達できません。その他のルートを定義するか、トラフィック フローをイネーブルにして接続を許可する必要があります。

