CHAPTER 22

AIP SSM および CSC SSM の管理

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、さまざまな SSM をサポートします。この章では、AIP SSM または CSC SSM をサポートするように適応型セキュリティ アプライアンスを設定する方法を説明します。これには、これらの SSM にトラフィックを送信する方法も含まれます。

ASA 5000 シリーズ適応型セキュリティ アプライアンス用 4GE SSM の詳細については、第 5 章「イーサネット設定およびサブインターフェイスの設定」を参照してください。

（注） Cisco PIX 500 シリーズ セキュリティ アプライアンスは、SSM をサポートできません。

この章は、次の項で構成されています。

AIP SSM の管理

ここでは、次の内容について説明します。

AIP SSM について

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、追加のセキュリティ検査機能を備えた高度な IPS ソフトウェアを実行する AIP SSM をサポートします。適応型セキュリティ アプライアンスは、パケットが出力インターフェイスから送信される直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）、および他のファイアウォール ポリシーが適用された後に、パケットを AIP SSM に誘導します。たとえば、アクセス リストによってブロックされたパケットは、AIP SSM に転送されません。

AIP SSM は 2 種類のモードのいずれかで次のように動作します。

- **インライン モード**：トラフィック フローに直接 AIP SSM を配置します。まず AIP SSM を通過して検査を受けないと、トラフィックは適応型セキュリティ アプライアンスを通過し続けられません。すべてのパケットが分析されてから通過を許可されるため、このモードが最も安全です。また、AIP SSM では、パケットごとにブロッキング ポリシーを実装できます。ただし、このモードは、スループットに影響を与えることがあります。このモードを指定するには、**ips** コマンドで **inline** キーワードを使用します。
- **無差別モード**：トラフィックの重複ストリームを AIP SSM に送信します。このモードは安全性では劣りますが、トラフィックのスループットにほとんど影響を与えません。インライン モードの動作とは異なり、無差別モードの動作では、SSM は適応型セキュリティ アプライアンスにトラフィックを**回避**するよう指示するか、適応型セキュリティ アプライアンスへの接続をリセットすることで、トラフィックをブロックすることだけができます。また、AIP SSM がトラフィックを分析している間、AIP SSM がトラフィックをブロックする前に少量のトラフィックが適応型セキュリティ アプライアンスを通過する場合があります。このモードを指定するには、**ips** コマンドで **inline** キーワードを使用します。

ハードウェア障害やその他の原因で AIP SSM が使用不可能である場合の、適応型セキュリティ アプライアンスのトラフィック処理方法を指定できます。**ips** コマンドの 2 個のキーワードがこの動作を制御します。**fail-close** キーワードを指定すると、AIP SSM が使用できない場合、適応型セキュリティ アプライアンスはすべてのトラフィックをブロックするように設定されます。**fail-open** キーワードを指定すると、AIP SSM が使用できない場合、適応型セキュリティ アプライアンスはすべてのトラフィックの通過を検査なしで許可するように設定されます。

AIP SSM の動作モードを設定する方法、および AIP SSM に障害発生時の適応型セキュリティ アプライアンスによるトラフィック処理方法の詳細については、「トラフィックの AIP SSM への転送」（P.22-2）を参照してください。

AIP SSM の準備

AIP SSM の設定は、まず ASA 5500 シリーズ適応型セキュリティ アプライアンスを設定した後で、AIP SSM を設定する 2 段階のプロセスです。

1. ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、AIP SSM に誘導するトラフィックを特定します（「トラフィックの AIP SSM への転送」（P.22-2）を参照）。
2. AIP SSM で、検査および保護ポリシーを設定します。これにより、トラフィックの検査方法と侵入が検出されたときに行う作業が決まります。AIP SSM で実行される IPS ソフトウェアは非常に堅牢であり、このマニュアルではそれらの機能について説明していないため、詳細な設定情報については次の別のマニュアルを参照してください。
   - *『Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface』*
   - *『Cisco Intrusion Prevention System Command Reference』*

トラフィックの AIP SSM への転送

適応型セキュリティ アプライアンスがトラフィックを AIP SSM に誘導するように設定するには、MPF コマンドを使用します。適応型セキュリティ アプライアンスをこのように設定する前に、MPF の概念と一般的なコマンドについて説明されている第 21 章「モジュラ ポリシー フレームワークの使用」を参照してください。

適応型セキュリティ アプライアンスから AIP SSM に誘導するトラフィックを特定するには、次の手順を実行します。

ステップ 1　すべてのトラフィックと照合するアクセス リストを作成します。

```
hostname(config)# access-list acl-name permit ip any any
```

ステップ 2　AIP SSM に誘導する必要があるトラフィックを特定するためのクラス マップを作成します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI がクラス マップ コンフィギュレーション モードに移行します。

ステップ 3　ステップ 1 で作成したアクセス リストとともに、**match access-list** コマンドを使用してスキャンするトラフィックを特定します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　AIP SSM にトラフィックの送信に使用するポリシー マップを作成するか、既存のポリシー マップを修正します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 5　ステップ 2 で作成した、スキャンするトラフィックを特定するクラス マップを指定します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　クラス マップで特定されたトラフィックを AIP SSM に送信されるトラフィックとして割り当てます。**ips** コマンドを次のように使用します。

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close | fail-open}
```

ここで **inline** キーワードと **promiscuous** キーワードは AIP SSM の動作モードを制御します。**fail-close** キーワードと **fail-open** キーワードは、AIP SSM が使用できない場合に、適応型セキュリティ アプライアンスがトラフィックを処理する方法を制御します。動作モードと障害時の動作の詳細については、「AIP SSM について」（P.22-1）を参照してください。

ステップ 7　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 4 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** キーワードを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、**interface** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

適応型セキュリティ アプライアンスが、指定したとおりにトラフィックを AIP SSM に誘導しはじめます。

次に、無差別モードですべての IP トラフィックを AIP SSM に誘導し、何らかの理由で AIP SSM カード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
```

適応型セキュリティ アプライアンスから AIP SSM へのネットワーク トラフィック誘導の完全な例については、例 16：ネットワーク トラフィックの誘導を参照してください。

AIP SSM へのセッション確立とセットアップの実行

AIP SSM にトラフィックを誘導するように ASA 5500 シリーズ適応型セキュリティ アプライアンスの設定を完了した後で、AIP SSM へのセッションを確立して初期設定用のセットアップ ユーティリティを実行します。

（注） 適応型セキュリティ アプライアンスから SSM へのセッションを確立するか（**session 1** コマンドを使用）、または管理インターフェイスで SSH または Telnet を使用して直接 SSM に接続できます。または、ASDM を使用する方法もあります。

セキュリティ アプライアンスから AIP SSM にセッションを確立するには、次の手順に従います。

ステップ 1　**session 1** コマンドを入力して、ASA 5500 シリーズ適応型セキュリティ アプライアンスから AIP SSM にセッションを確立します。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ステップ 2　ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードはどちらも **cisco** です。

（注） AIP SSM への初回ログインでは、デフォルト パスワードの変更を求められます。パスワードは 8 文字以上の長さで、辞書に載っていない単語にする必要があります。

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use. Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption. Importers, exporters, distributors and
users are responsible for compliance with U.S. and local country laws. By using
this product you agree to comply with applicable laws and regulations. If you
are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

（注）　（一部のソフトウェア バージョンだけに表示される）前回のライセンス通知が表示された場合、AIP SSM のシグニチャ ファイルのアップグレードが必要になるまでメッセージを無視してかまいません。有効なライセンス キーがインストールされるまで、AIP SSM は現在のシグニチャ レベルで動作します。ライセンス キーは後でインストールできます。ライセンス キーは AIP SSM の現在の機能に影響を与えません。

ステップ 3　**setup** コマンドを入力して、AIP SSM の初期設定用のセットアップ ユーティリティを実行します。

```
AIP SSM# setup
```

これで、AIP SSM に侵入防御を設定する準備ができました。AIP SSM 設定情報については、次の 2 種類のガイドを参照してください。

- *『Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface』*
- *『Cisco Intrusion Prevention System Command Reference』*

CSC SSM の管理

ここでは、次の内容について説明します。

CSC SSM について

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、Content Security and Control ソフトウェアを実行する CSC SSM をサポートしています。CSC SSM は、ウイルス、スパイウェア、スパムなどの好ましくないトラフィックを予防します。これは、FTP、HTTP、POP3、および SMTP トラフィックをスキャンすることで実現されます。そのためには、これらのトラフィックを CSC SSM に送信するように適応型セキュリティ アプライアンスを設定しておきます。

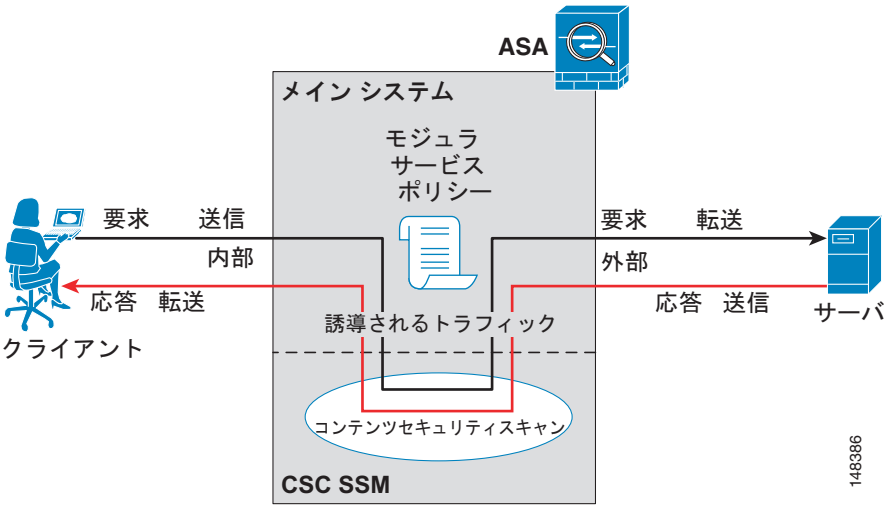
図 22-1 は、次の条件を満たす適応型セキュリティ アプライアンスを通過するトラフィック フローを示しています。

- CSC SSM がインストールされてセットアップされている。
- SSM に誘導しスキャンするトラフィックを決定するサービス ポリシーがある。

この例では、クライアントは、Web サイトにアクセスするネットワーク ユーザ、FTP サーバからファイルをダウンロードするネットワーク ユーザ、または POP3 サーバからメールを取得するネットワーク ユーザです。SMTP スキャンは、適応型セキュリティ アプライアンスによって保護されている SMTP サーバに外部から送信されるトラフィックをスキャンするために、適応型セキュリティ アプライアンスを設定する必要がある点で異なります。

（注）　CSC SSM は、適応型セキュリティ アプライアンスで FTP 検査がイネーブルになっている場合にだけ FTP ファイル転送をスキャンできます。FTP 検査はデフォルトでイネーブルになっています。

図 22-1　CSC SSM でスキャンされたトラフィックのフロー



CSC SSM のシステム セットアップとモニタリングには、ASDM を使用します。CSC SSM ソフトウェアのコンテンツ セキュリティ ポリシーの高度な設定を行うには、ASDM 内のリンクをクリックして、CSC SSM の Web ベースの GUI にアクセスします。CSC SSM GUI の使用方法は、『*Trend Micro InterScan for Cisco CSC SSM Administrator Guide*』で説明されています。

（注）　ASDM と CSC SSM では、別個のパスワードが保持されます。それぞれのパスワードを同一にすることはできますが、これら 2 つのパスワードの 1 つを変更しても他のパスワードには影響を与えません。

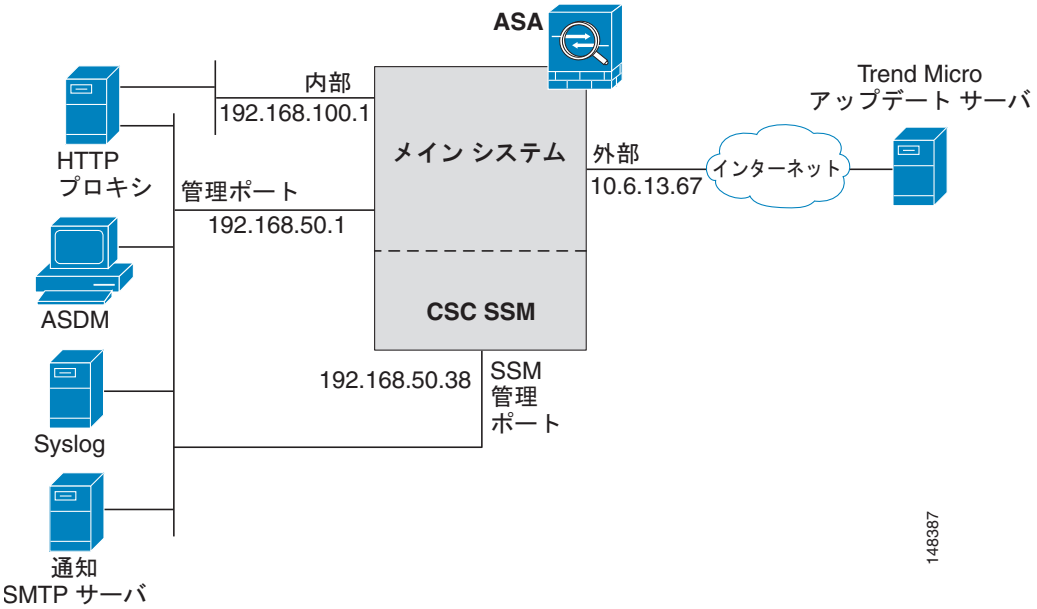
ASDM を実行しているホストと適応型セキュリティ アプライアンスの間の接続は、適応型セキュリティ アプライアンスの管理ポートを通じて確立されます。CSC SSM GUI への接続は、SSM 管理ポートを通じて確立されます。これら 2 つの接続は、CSC SSM の管理に必要であるため、ASDM を実行しているホストは、適応型セキュリティ アプライアンスの管理ポートと SSM の管理ポートの両方の IP アドレスにアクセスできる必要があります。

図 22-2 は、専用の管理ネットワークに接続されている CSC SSM がある適応型セキュリティ アプライアンスを示しています。専用の管理ネットワークの使用は必須ではありませんが、使用することをお勧めします。図 22-2 で特に重要な点は次のとおりです。

- HTTP プロキシ サーバが内部ネットワークと管理ネットワークに接続されている。これにより、CSC SSM から Trend Micro アップデート サーバに接続できます。
- 適応型セキュリティ アプライアンスの管理ポートが、管理ネットワークに接続されている。適応型セキュリティ アプライアンス と CSC SSM の管理を許可するには、ASDM を実行しているホストが管理ネットワークと接続している必要があります。

- 管理ネットワークに、CSC SSM への電子メール通知に使用される SMTP サーバ、および CSC SSM が syslog メッセージを送信できる syslog サーバが含まれている。

図 22-2　管理ネットワークを備えた CSC SSM 構成



CSC SSM は、ステートフル フェールオーバーをサポートできません。これは、CSC SSM は接続情報を保持しないため、ステートフル フェールオーバーで必要とされる情報をフェールオーバー装置に提供できないからです。CSC SSM がスキャンしている接続は、CSC SSM がインストールされたセキュリティ アプライアンスの失敗時にドロップされます。スタンバイの適応型セキュリティ アプライアンスがアクティブになると、スキャンされるトラフィックは CSC SSM に転送され、接続がリセットされます。

CSC SSM の準備

CSC SSM のセキュリティ上の利点を得るには、SSM の単純なハードウェア インストールだけではなく、他にもいくつかの手順を実行する必要があります。ここでは、それらの手順の概要を示します。

適応型セキュリティ アプライアンスと CSC SSM を設定するには、次の手順を実行します。

ステップ 1　CSC SSM が Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスに事前インストールされていない場合は、インストールして、ネットワーク ケーブルを SSM の管理ポートに接続します。SSM のインストールおよび接続については、『*Cisco ASA 5500 Series Hardware Installation Guide*』を参照してください。

CSC SSM の管理ポートは、お使いのネットワークに接続して、CSC SSM ソフトウェアの管理と自動アップデートを可能にする必要があります。また、CSC SSM は、電子メール通知と syslog 処理用に管理ポートを使用します。

ステップ 2　CSC SSM には、Product Authorization Key（PAK）が付属しています。PAK を使用して、次の URL で CSC SSM を登録します。

http://www.cisco.com/go/license

登録後、電子メールでアクティベーション キーを受信します。ステップ 6 を完了するには、アクティベーション キーが必要です。

ステップ 3　ステップ 6 で使用するために必要な次の情報を収集します。

- ステップ 2 を完了した後に受信したアクティベーション キー。
- SSM 管理ポートの IP アドレス、ネットマスク、およびゲートウェイ IP アドレス。

（注） SSM 管理ポートの IP アドレスは、ASDM の実行で使用されるホストによりアクセスできなければなりません。SSM 管理ポートと適応型セキュリティ アプライアンス管理インターフェイスの IP アドレスは、異なるサブネットに属していてもかまいません。

- DNS サーバの IP アドレス。
- HTTP プロキシ サーバの IP アドレス（セキュリティ ポリシーで、インターネットへの HTTP アクセスにプロキシ サーバの使用が求められている場合に限り必要）。
- SSM のドメイン名とホスト名。
- 電子メール通知に使用する電子メール アドレス、SMTP サーバの IP アドレスとポート番号。
- CSC SSM の管理を許可されたホストまたはネットワークの IP アドレス。
- CSC SSM 用のパスワード。

ステップ 4　Web ブラウザで、CSC SSM がある適応型セキュリティ アプライアンスの ASDM にアクセスします。

（注） ASDM に初めてアクセスする場合は、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』の Startup Wizard の説明を参照してください。

ASDM アクセスをイネーブルにする方法の詳細については、「ASDM での HTTPS アクセスの許可」（P.40-4）を参照してください。

ステップ 5　適応型セキュリティ アプライアンスの時刻設定を確認します。時刻設定が正確であることは、セキュリティ イベントのロギング、および CSC SSM ソフトウェアの自動アップデートにとって重要です。

- 時刻設定を手動で制御する場合は、時間帯を含む、クロック設定を確認します。[Configuration] > [Properties] > [Device Administration] > [Clock] を選択します。
- NTP を使用している場合は、NTP コンフィギュレーションを確認します。[Configuration] > [Properties] > [Device Administration] > [NTP] を選択します。

ステップ 6　ASDM で、Content Security セットアップ ウィザードを実行します。これには、サポートされている Web ブラウザで ASDM GUI にアクセスし、[Home] ページの [Content Security] タブをクリックします。Content Security セットアップ ウィザードが起動します。Content Security セットアップ ウィザードについては、[Help] ボタンをクリックしてください。

（注） ASDM に初めてアクセスする場合は、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』の Startup Wizard の説明を参照してください。

ステップ 7　ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、CSC SSM に誘導するトラフィックを特定します（「トラフィックの CSC SSM への転送」（P.22-12）を参照）。

ステップ 8　（任意）CSC SSM GUI でデフォルトのコンテンツ セキュリティ ポリシーを確認します。デフォルトのコンテンツ セキュリティ ポリシーは、ほとんどの実装に適しています。これらの修正は高度な設定であるため、必ず『*Trend Micro InterScan for Cisco CSC SSM Administrator Guide*』を読んでから実行してください。

コンテンツ セキュリティ ポリシーを確認するには、CSC SSM GUI でイネーブルになっている機能を表示します。使用できる機能は、購入したライセンス レベルによって異なります。デフォルトでは、購入したライセンスに含まれているすべての機能がイネーブルになっています。

基本ライセンスの場合、デフォルトでイネーブルになっている機能は、SMTP ウイルス スキャン、POP3 ウイルス スキャン、コンテンツ フィルタリング、Web メール ウイルス スキャン、HTTP ファイル ブロッキング、FTP ウイルス スキャンとファイル ブロッキング、ロギング、および自動アップデートです。

Plus ライセンスの場合、デフォルトでイネーブルになっている追加機能は、SMTP アンチスパム、SMTP コンテンツ フィルタリング、POP3 アンチスパム、URL ブロッキング、および URL フィルタリングです。

CSC SSM GUI にアクセスするには、ASDM で、[Configuration] > [Trend Micro Content Security] を選択し、次に [Web]、[Mail]、[File Transfer]、または [Updates] のいずれかを選択します。これらのペインにある、単語「Configure」で始まる青いリンクをクリックすると、CSC SSM GUI が開きます。

スキャンするトラフィックの指定

CSC SSM は、FTP、HTTP、POP3、および SMTP トラフィックをスキャンできます。接続を要求しているパケットの宛先ポートが、これらのプロトコルにとって既知のポートである場合にのみ、これらのプロトコルがサポートされます。つまり、CSC SSM は、次の接続のみをスキャンできます。

- TCP ポート 21 に対してオープンされている FTP 接続。
- TCP ポート 80 に対してオープンされている HTTP 接続。
- TCP ポート 110 に対してオープンされている POP3 接続。
- TCP ポート 25 に対してオープンされている SMTP 接続。

これらすべてのプロトコルのトラフィックをスキャンすることも、任意のプロトコルの組み合わせをスキャンすることもできます。たとえば、ネットワーク ユーザの POP3 電子メールの受信を許可しないときに、POP3 トラフィックを CSC SSM に誘導するように適応型セキュリティ アプライアンスを設定しない場合（代わりにこれをブロックする場合）があります。

適応型セキュリティ アプライアンスと CSC SSM のパフォーマンスを最大化するには、CSC SSM でスキャンするトラフィックだけを CSC SSM に誘導します。信頼できる送信元と宛先間のトラフィックなど、スキャンする必要がないトラフィックまで誘導すると、ネットワークのパフォーマンスに悪影響を与える可能性があります。

CSC SSM によるトラフィック スキャンの処理は、サービス ポリシーの一部の必要がある **csc** コマンドでイネーブルにできます。サービス ポリシーはグローバルに適用することも、特定のインターフェイスに適用することもできるため、**csc** コマンドは、グローバルにイネーブルにすることも、特定のインターフェイスに対してイネーブルにすることも選択できます。

csc コマンドをグローバル ポリシーに追加すると、適応型セキュリティ アプライアンスを通過する暗号化されていないすべての接続は CSC SSM によって確実にスキャンされます。ただし、これにより、信頼できる送信元からのトラフィックが不必要にスキャンされることになる場合もあります。

csc コマンドをインターフェイス固有のサービス ポリシーでイネーブルにすると、双方向性を持つようになります。これは、適応型セキュリティ アプライアンスが新しい接続を開くとき、その接続の着信インターフェイスまたは発信インターフェイスのいずれかで **csc** コマンドがアクティブであり、ポリシーのクラス マップでスキャン対象のトラフィックが特定されていれば、適応型セキュリティ アプライアンスはこのトラフィックを CSC SSM に誘導することを意味します。

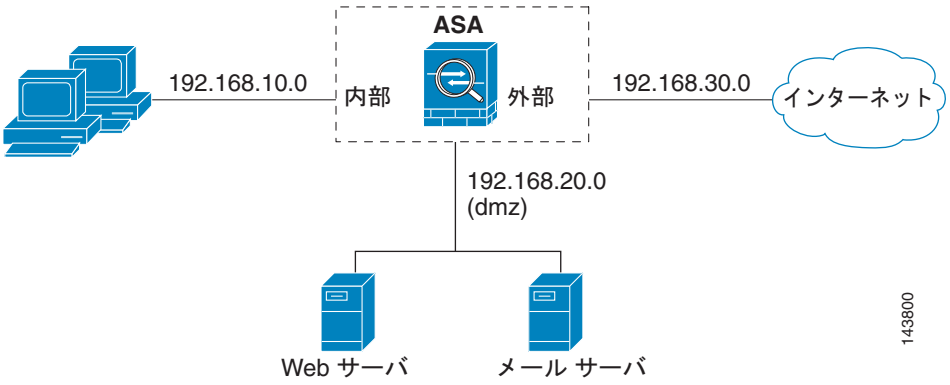
ただし、双方向性があるということは、特定のインターフェイスを通過するサポート対象のトラフィック タイプのいずれかを CSC SSM に誘導する場合、CSC SSM は信頼できる内部ネットワークからのトラフィックに対して不必要なスキャンを実行する可能性があります。たとえば、DMZ ネットワークの Web サーバから要求された URL とファイルは、内部ネットワークのホストに対してコンテンツ セキュリティ リスクをもたらす可能性は低いため、適応型セキュリティ アプライアンスでこのようなトラフィックを CSC SSM に誘導する必要はほとんどありません。

そのため、アクセス リストを使用して、CSC SSM サービス ポリシーのクラス マップで選択されたトラフィックをさらに制限することを強くお勧めします。特に、次の条件を満たすアクセス リストを使用することをお勧めします。

- 外部ネットワークへの HTTP 接続
- 適応型セキュリティ アプライアンスの内部のクライアントから、適応型セキュリティ アプライアンスの外部のサーバへの FTP 接続
- セキュリティ アプライアンスの内部のクライアントから適応型セキュリティ アプライアンスの外部のサーバへの POP3 接続
- 内部メール サーバ宛ての着信 SMTP 接続。

図 22-3 では、適応型セキュリティ アプライアンスが、内部ネットワークのクライアントから外部ネットワークへの HTTP、FTP、および POP3 接続要求、および外部ホストから DMZ ネットワーク上のメール サーバへの着信 SMTP 接続のトラフィックを CSC SSM に誘導するように設定されています。内部ネットワークから DMZ ネットワーク上の Web サーバへの HTTP 要求は、スキャンされません。

図 22-3　CSC SSM スキャンの一般的なネットワーク コンフィギュレーション



スキャンするトラフィックを特定するために適応型セキュリティ アプライアンスを設定するには、さまざまな方法があります。そのうちの 1 つに、内部インターフェイスに 1 つ、外部インターフェイスに 1 つというように、2 つのサービス ポリシーを定義して、それぞれにスキャンするトラフィックと一致するアクセス リストを含める方法があります。次のアクセス リストは、内部インターフェイスに適用するポリシーで使用できます。

```
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110
```

前述のとおり、**csc** コマンドを特定のインターフェイスに適用するポリシーは、入力トラフィックと出力トラフィックの両方で有効ですが、csc_out アクセス リストの送信元ネットワークとして 192.168.10.0 を指定することにより、内部インターフェイスに適用されたポリシーは、内部ネットワークのホストによって開始された接続だけと一致するようになります。アクセス リストの 2 番目の ACE

では、**deny** キーワードが使用されます。この ACE は、192.168.10.0 ネットワークから 192.168.20.0 ネットワークの TCP ポート 80 に送信されたトラフィックを適応型セキュリティ アプライアンスがブロックするということを意味するものでは**ありません**。ポリシー マップによる照合からトラフィックを単に除外するため、適応型セキュリティ アプライアンスが CSC SSM にこれを送信することを防ぎます。

deny ステートメントをアクセス リスト内で使用すると、信頼できる外部ホストとの接続をスキャンから除外できます。たとえば、CSC SSM の負荷を軽減するために、既知の信頼できるサイトへの HTTP トラフィックを除外できます。このようなサイトの Web サーバの IP アドレスが 209.165.201.7 である場合、次の ACE を csc_out アクセス リストに追加すると、信頼できる外部 Web サーバと内部ホスト間の HTTP 接続を、CSC SSM によるスキャンから除外できます。

```
access-list csc_out deny tcp 192.168.10.0 255.255.255.0 209.165.201.7 255.255.255.255 eq 80
```

この例の 2 番目のポリシー（外部インターフェイスに適用される）は、次のアクセス リストを使用します。

```
access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
```

このアクセス リストは、任意の外部ホストから DMZ ネットワークの任意のホストへの着信 SMTP 接続を照合します。したがって、外部インターフェイスに適用されるポリシーにより、着信 SMTP 電子メールは、確実に CSC SSM に誘導され、スキャンされます。内部ネットワークのホストから DMZ ネットワークのメール サーバへの SMTP 接続は照合しません。これは、SMTP 接続は外部インターフェイスを一切使用しないためです。

DMZ ネットワークの Web サーバが、外部ホストから HTTP 経由でアップロードされたファイルを受信する場合、次の ACE を csc_in アクセス リストに追加すると、CSC SSM を使用して Web サーバを感染したファイルから保護できます。

```
access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80
```

この項のアクセス リストを使用するサービス ポリシーのコンフィギュレーションの完全な例については、例 22-1 を参照してください。

CSC SSM を通過する接続の制限

適応型セキュリティ アプライアンスは、CSC SSM および CSC SSM がスキャンする接続の宛先が、必要以上の接続要求を受け入れないようにする、または必要以上の接続要求を受信しないようにすることができます。これは、初期接続または完全に確立された接続に対して行うことができます。class-map 制限と per-client 制限に含まれるすべてのクライアントに対する制限を指定することもできます。**set connection** コマンドを使用すると、初期接続または完全に確立された接続に対する制限を設定できます。

class-map 制限と per-client 制限に含まれるすべてのクライアントに対する制限を指定することもできます。**per-client-embryonic-max** パラメータと **per-client-max** パラメータは、個々のクライアントが開くことができる接続の最大数を制限します。クライアントが必要以上のネットワーク リソースを同時に使用している場合、これらのパラメータを使用して、適応型セキュリティ アプライアンスが各クライアントに許可する接続の数を制限できます。

DoS 攻撃の目的は、接続や接続要求を行い、主要ホストの容量を圧迫することでネットワークを中断することです。**set connection** コマンドを使用して、DoS 攻撃を阻止できます。攻撃対象となる可能性があるホストがサポートできる per-client の最大値を設定すると、悪意のあるクライアントは保護されたネットワークのホストを圧迫できなくなります。

set connection コマンドを使用して、CSC SSM およびそれがスキャンする接続の宛先を保護する方法については、「トラフィックの CSC SSM への転送」（P.22-12）を参照してください。

トラフィックの CSC SSM への転送

適応型セキュリティ アプライアンスがトラフィックを CSC SSM に誘導するように設定するには、MPF コマンドを使用します。適応型セキュリティ アプライアンスをこのように設定する前に、MPF の概念と一般的なコマンドについて説明されている第 21 章「モジュラ ポリシー フレームワークの使用」を参照してください。

適応型セキュリティ アプライアンスから CSC SSM に誘導するトラフィックを特定するには、次の手順を実行します。

ステップ 1　CSC SSM でスキャンするトラフィックと一致するアクセス リストを作成します。これを行うには、**access-list extended** コマンドを使用します。すべてのトラフィックと一致させるのに必要な数の ACE を作成します。たとえば、FTP、HTTP、POP3、および SMTP トラフィックを指定する場合は、4 個の ACE が必要です。スキャンするトラフィックを特定する方法については、「スキャンするトラフィックの指定」（P.22-9）を参照してください。

ステップ 2　CSC SSM に誘導する必要があるトラフィックを特定するためのクラス マップを作成します。**class-map** コマンドを次のように使用します。

```
hostname(config)# class-map class_map_name
hostname(config-cmap)#
```

class_map_name は、トラフィック クラスの名前です。**class-map** コマンドを入力すると、CLI がクラス マップ コンフィギュレーション モードに移行します。

ステップ 3　ステップ 1 で作成したアクセス リストとともに、**match access-list** コマンドを使用してスキャンするトラフィックを特定します。

```
hostname(config-cmap)# match access-list acl-name
```

ステップ 4　CSC SSM にトラフィックの送信に使用するポリシー マップを作成するか、既存のポリシー マップを修正します。そのためには、**policy-map** コマンドを次のように使用します。

```
hostname(config-cmap)# policy-map policy_map_name
hostname(config-pmap)#
```

policy_map_name は、ポリシー マップの名前です。CLI はポリシー マップ コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 5　ステップ 2 で作成した、スキャンするトラフィックを特定するクラス マップを指定します。**class** コマンドを次のように使用します。

```
hostname(config-pmap)# class class_map_name
hostname(config-pmap-c)#
```

class_map_name は、ステップ 2 で作成したクラス マップの名前です。CLI はポリシー マップ クラス コンフィギュレーション モードを開始し、プロンプトがそれに応じて変わります。

ステップ 6　適応型セキュリティ アプライアンスが CSC SSM に誘導する同時接続の per-client 制限を適用する場合は、**set connection** コマンドを次のように使用します。

```
hostname(config-pmap-c)# set connection per-client-max n
```

n は、適応型セキュリティ アプライアンス が許可するクライアントごとの最大同時接続数です。これは、1 台のクライアントが CSC SSM のサービスや SSM で保護されたサーバを必要以上に使用しないようにします。また、CSC SSM が保護する HTTP、FTP、POP3、または SMTP サーバに対する DoS 攻撃の試みも阻止します。

ステップ 7　クラス マップで特定されたトラフィックを CSC SSM に送信されるトラフィックとして割り当てます。**csc** コマンドを次のように使用します。

```
hostname(config-pmap-c)# csc {fail-close | fail-open}
```

fail-close キーワードと **fail-open** キーワードは、CSC SSM が使用できない場合に、適応型セキュリティ アプライアンスがトラフィックを処理する方法を制御します。動作モードと障害時の動作の詳細については、「CSC SSM について」（P.22-5）を参照してください。

ステップ 8　ポリシー マップをグローバルに、または特定のインターフェイスに適用するには、**service-policy** コマンドを次のように使用します。

```
hostname(config-pmap-c)# service-policy policy_map_name [global | interface interface_ID]
hostname(config)#
```

policy_map_name は、ステップ 4 で設定したポリシー マップです。ポリシー マップをすべてのインターフェイス上のトラフィックに適用する場合、**global** キーワードを使用します。ポリシー マップを特定のインターフェイス上のトラフィックに適用する場合、**interface** *interface_ID* オプションを使用します。*interface_ID* は、**nameif** コマンドでインターフェイスに割り当てられた名前です。

グローバル ポリシーは 1 つしか適用できません。インターフェイスのグローバル ポリシーは、そのインターフェイスにサービス ポリシーを適用することで上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

適応型セキュリティ アプライアンスが、指定したとおりにトラフィックを CSC SSM に誘導しはじめます。

例 22-1 は図 22-3 に示したネットワークに基づいています。これは 2 つのサービス ポリシーを作成します。最初のポリシー csc_out_policy は、内部インターフェイスに適用され、csc_out アクセス リストを使用して、FTP および POP3 に対するすべての発信要求が確実にスキャンされるようにします。csc_out アクセス リストにより、内部から外部インターフェイスのネットワークへの HTTP 接続が確実にスキャンされることにもなりますが、このアクセス リストには、内部から DMZ ネットワーク上のサーバへの HTTP 接続を除外する deny ACE が含まれています。

2 番めのポリシー csc_in_policy は、外部インターフェイスに適用されます。このポリシーは csc_in アクセス リストを使用して、外部インターフェイスで発信され、DMZ ネットワークを宛先とする SMTP 要求と HTTP 要求が CSC SSM で確実にスキャンされるようにします。HTTP 要求をスキャンすることで、Web サーバは HTTP ファイルのアップロードから保護されます。

例 22-1　一般的な CSC SSM スキャン シナリオのサービス ポリシー

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
```

```
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside
```

（注）　FTP により転送されたファイルを CSC SSM がスキャンするには、FTP インスペクションがイネーブルである必要があります。FTP インスペクションは、デフォルトでイネーブルになっています。

SSM ステータスのチェック

SSM のステータスをチェックするには、**show module** コマンドを使用します。

次の出力は、CSC SSM がインストールされている適応型セキュリティ アプライアンスの例です。[Status] フィールドに SSM の動作ステータスが示されます。正常に動作している SSM は、**show module** コマンドの出力で、ステータスが「UP」と表示されます。適応型セキュリティ アプライアンスがアプリケーション イメージを SSM に転送する間は、出力の [Status] フィールドには「Recover」と表示されます。可能なステータスの詳細については、『*Cisco Security Appliance Command Reference*』の **show module** コマンドの項目を参照してください。

```
hostname# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
0 000b.fcf8.c30d to 000b.fcf8.c311  1.0      1.0(10)0     7.1(0)1
1 000b.fcf8.012c to 000b.fcf8.012c  1.0      1.0(10)0     Trend Micro InterScan Security Module Version 5.0

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 Trend Micro InterScan Security Version 5.0

Mod Status             Data Plane Status     Compatability
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

コマンドの末尾の引数 **1** は、SSM 専用のスロット番号です。スロット番号がわからない場合、省略すると、スロット 0（ゼロ）を占有すると見なされている適応型セキュリティ アプライアンスを含む、すべてのモジュールの情報が表示されます。

SSM の追加情報を表示するには、details キーワードを使用します。

次の出力は、CSC SSM がインストールされている適応型セキュリティ アプライアンスの例です。

```
hostname# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   1.0
Serial Number:      0
Firmware version:   1.0(10)0
Software version:   Trend Micro InterScan Security Module Version 5.0
App. name:          Trend Micro InterScan Security Module
App. version:       Version 5.0
Data plane Status:  Up
Status:             Up
```

```
HTTP Service:       Up
Mail Service:       Up
FTP  Service:       Up
Activated:          Yes
Mgmt IP addr:       10.23.62.92
Mgmt web port:      8443
```

SSM へのイメージの転送

AIP SSM や CSC SSM などのインテリジェント SSM の場合、アプリケーション イメージを TFTP サーバから SSM に転送できます。このプロセスでは、アップグレード イメージのとメンテナンス イメージがサポートされています。

（注） SSM のアプリケーションをアップグレードする場合、SSM アプリケーションによってそのコンフィギュレーションのバックアップがサポートされる場合があります。SSM アプリケーションのコンフィギュレーションをバックアップしないと、イメージを SSM に転送したときに失われます。SSM によるバックアップのサポートの詳細については、SSM のマニュアルを参照してください。

イメージをインテリジェント SSM に転送するには、次の手順を実行します。

ステップ 1　SSM のリカバリ コンフィギュレーションを作成または修正します。そのためには、次の手順を実行します。

a. SSM のリカバリ コンフィギュレーションが存在するかどうかを確認します。これを行うには、**recover** キーワードを指定した **show module** コマンドを次のように使用します。

```
hostname# show module slot recover
```

slot は、SSM 専用のスロット番号です。

recover キーワードが有効でない場合、リカバリ コンフィギュレーションは存在しません。**show module** コマンドの **recover** キーワードは、SSM のリカバリ コンフィギュレーションが存在する場合にだけ使用できます。

（注） 適応型セキュリティ アプライアンスがマルチ コンテキスト モードで動作している場合、**configure** キーワードは、システム コンテキストだけで使用できます。

SSM のリカバリ コンフィギュレーションが存在する場合は、適応型セキュリティ アプライアンスに表示されます。リカバリ コンフィギュレーションを丹念に調べて（特に [Image URL] フィールド）、正しいことを確認します。次に、スロット 1 の SSM のリカバリ コンフィギュレーションの例を示します。

```
hostname# show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

b. リカバリ コンフィギュレーションを作成または変更する必要がある場合、次のように、**configure** キーワードを使用して **hw-module module recover** コマンドを使用します。

```
hostname# hw-module module slot recover configure
```

slot は、SSM 専用のスロット番号です。

必要に応じて、プロンプトへの応答を完了します。コンフィギュレーションを修正する場合は、**Enter** キーを押して、以前の設定値を保持することができます。プロンプトの例を次に示します。これらの詳細については、『*Cisco Security Appliance Command Reference*』の **hw-module module recover** コマンドの項目を参照してください。

```
Image URL [tftp://0.0.0.0/]:
Port IP Address [0.0.0.0]:
VLAN ID [0]:
Gateway IP Address [0.0.0.0]:
```

（注） 指定する TFTP サーバが、最大 60 MB ファイルを転送できることを確認してください。TFTP サーバが、SSM の管理ポートとして指定した IP アドレスに接続できることも確認してください。

プロンプトが完了すると、適応型セキュリティ アプライアンスは、指定した URL にあるイメージを SSM に転送できます。

ステップ 2　TFTP サーバから SSM にイメージを転送し、SSM を再起動します。これを行うには、**boot** キーワードを指定した **hw-module module recover** コマンドを次のように使用します。

```
hostname# hw-module module slot recover boot
```

slot は、SSM 専用のスロット番号です。

ステップ 3　イメージ転送の進捗と SSM の再起動プロセスを確認します。これを行うには、**show module** コマンドを使用します。詳細については、「SSM ステータスのチェック」（P.22-14）を参照してください。

適応型セキュリティ アプライアンスによるイメージ転送および SSM の再起動が完了すると、SSM では新たに転送されたイメージが実行されています。

（注） SSM がコンフィギュレーションのバックアップをサポートしていて、SSM で実行しているアプリケーションのコンフィギュレーションを復元する場合の詳細については、SSM のマニュアルを参照してください。