CHAPTER 67

ASA CSC モジュールの設定

この章では、ASA で CSC SSM にインストールされる Content Security and Control（CSC）アプリケーションの設定を設定する方法について説明します。

この章の内容は、次のとおりです。

CSC SSM に関する情報

ASA の一部のモデルは、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、望ましくないトラフィックからの保護を提供します。これは、ASA が CSC SSM に送信するように設定した FTP、HTTP/HTTPS、POP3、および SMTP パケットをスキャンすることによって実現されます。

CSC SSM の詳細については、次の URL を参照してください。

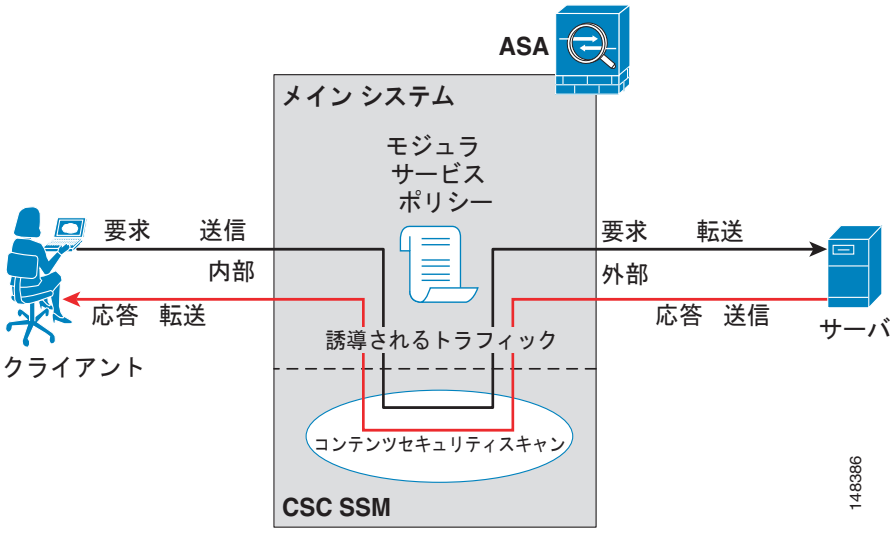
http://www.cisco.com/en/US/products/ps6823/index.html

図 67-1 は、次の条件を満たす ASA 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、設定されている。
- CSC 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、ASA 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、ASA を設定する必要がある点で異なります。

図 67-1　CSC SSM でスキャンされる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 は、別個の Web ブラウザ ウィンドウに表示されます。CSC SSM にアクセスするには、CSC SSM のパスワードを入力する必要があります。CSC SSM GUI を使用するには、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

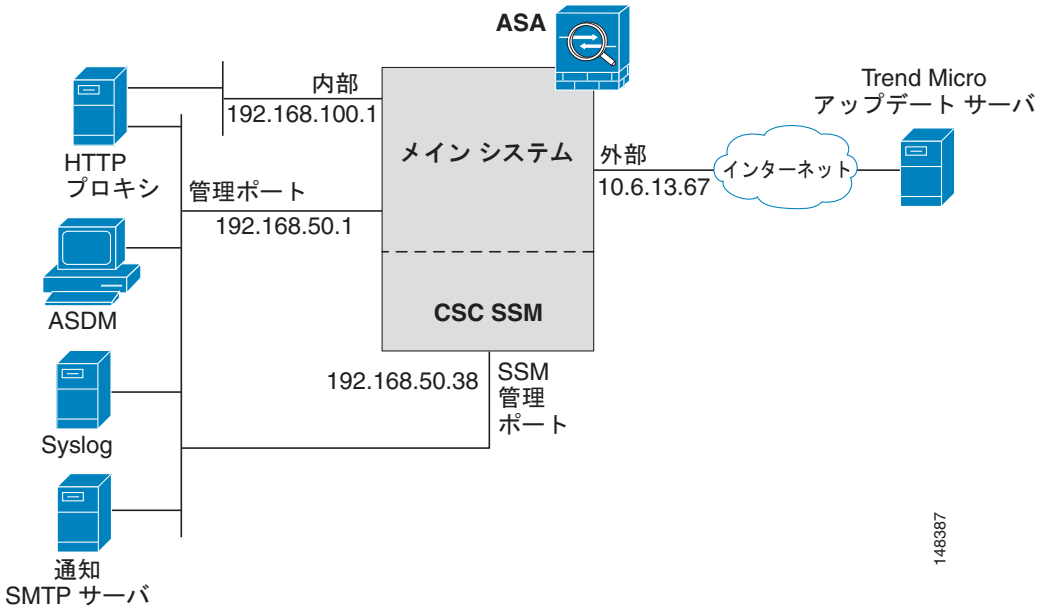
（注）　ASDM と CSC SSM では、別個のパスワードが保持されます。それぞれのパスワードを同一にすることはできますが、これら 2 つのパスワードの 1 つを変更しても他のパスワードには影響を与えません。

ASDM を実行しているホストと ASA の間の接続は、ASA 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、ASA 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 67-2 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 ASA 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。この設定では、次の項目が特に重要です。

- 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。この HTTP プロキシ サーバにより、CSC SSM から Trend Micro Systems アップデート サーバに接続できます。
- ASA の管理ポートが、管理ネットワークに接続されている。ASA 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 67-2　管理ネットワークを備えた CSC SSM 構成



スキャンするトラフィックの指定

CSC SSM が FTP、HTTP/HTTPS、POP3、および SMTP のトラフィックをスキャンできるのは、接続を要求しているパケットの宛先ポートが、指定されたプロトコルの well-known ポートであるときのみです。CSC SSM がスキャンできる接続は、次の接続に限られます。

- 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 443 に対してオープンされている HTTPS 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 ユーザが POP3 電子メールの受信を許可しない場合は、POP3 トラフィックを CSC SSM に誘導するように、ASA を設定しないでください。代わりに、このトラフィックをブロックします。

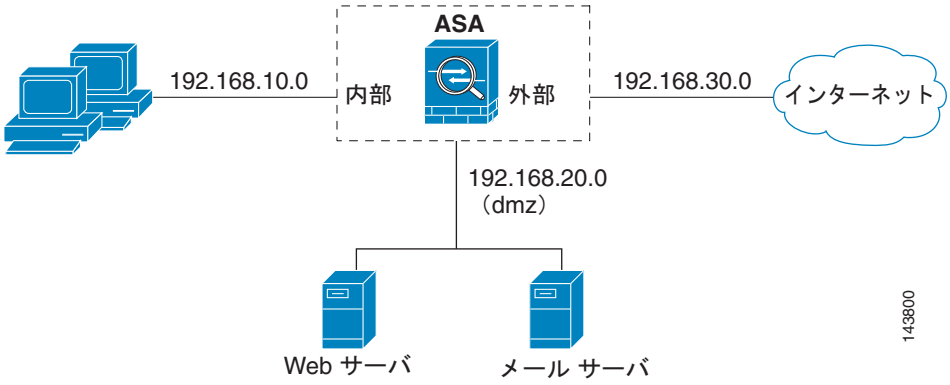
ASA と CSC SSM のパフォーマンスを最大化するには、CSC SSM でスキャンするトラフィックだけを CSC SSM に誘導します。信頼できる送信元と宛先間のトラフィックなど、スキャンしないトラフィックまで誘導すると、ネットワークのパフォーマンスに悪影響を与える可能性があります。

（注）　トラフィックが最初に CSC 検査用に分類されるときは、フローベースとなります。既存の接続の一部であるトラフィックは、その接続に設定されているサービス ポリシーに直接移動します。

CSC スキャンを含むサービス ポリシーはグローバルにも、特定のインターフェイスにも適用できるので、CSC スキャンをグローバルにイネーブルにするか、特定のインターフェイスに対してイネーブルにするかを選択できます。

図 67-3 で示されている設定を基にして、ASA を、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 接続だけを CSC SSM に誘導するように設定します。内部ネットワークから DMZ ネットワークの Web サーバへの HTTP 要求はスキャンしません。

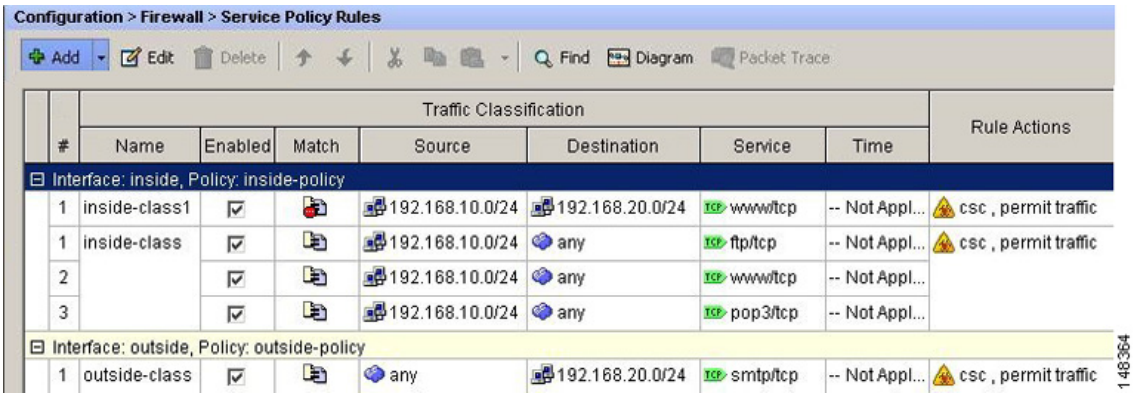
図 67-3　CSC SSM スキャンの一般的なネットワーク コンフィギュレーション



スキャンするトラフィックを識別するよう、ASA 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と外部インターフェイスにそれぞれ 1 つずつサービス 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を照合するアクセス リストを含める方法があります。

図 67-4 に、ASA でスキャンするトラフィックだけを選択するサービス ポリシー規則を示します。

図 67-4　CSC スキャン用に最適化されたトラフィックの選択



inside-policy の最初のクラスである inside-class1 では、ASA によって内部ネットワークと DMZ ネットワークの間の HTTP トラフィックがスキャンされないことが保証されています。[Match] カラムに表示された [Do not match] アイコンが、この設定を示しています。この設定は、ASA によって、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 へのトラフィック送信がブロックされることを意味するものではありません。この設定では、内部インターフェイスに適用されるサービス ポリシーによる照合からトラフィックを除外し、ASA によってトラフィックが CSC SSM に送信されないようにします。

inside-policy の 2 番目のクラスである inside-class では、内部ネットワークとすべての宛先との間の FTP、HTTP、および POP3 トラフィックが照合されます。DMZ ネットワークへの HTTP 接続は、inside-class1 の設定によって除外されます。前述のとおり、CSC スキャンを特定のインターフェイス

に適用するポリシーは、着信トラフィックと発信トラフィックの両方に影響しますが、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、inside-class1 では内部ネットワークのホストから開始された接続だけが照合されます。

outside-policy では、outside-class で外部送信元から DMZ ネットワークへの SMTP トラフィックが照合されます。この設定では、SMTP クライアントからサーバへの接続をスキャンせずに、SMTP サーバと、DMZ ネットワーク上の SMTP サーバから電子メールをダウンロードする内部ユーザが保護されます。

DMZ ネットワーク上の Web サーバで、HTTP によって外部ホストからアップロードされたファイルを受信した場合は、任意の送信元から DMZ ネットワークへの HTTP トラフィックを照合するルールを外部ポリシーに追加できます。ポリシーは外部インターフェイスに適用されるので、このルールでは、ASA 外部の HTTP クライアントからの接続だけが照合されます。

CSC SSM のライセンス要件

モデル	ライセンス要件
ASA 5510	• 基本ライセンス：SMTP ウイルス スキャン、POP3 ウイルス スキャンおよびコンテンツ 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 スキャンおよびファイル ブロッキング、ロギング、および自動アップデートをサポートします。2 個のコンテキストをサポートします。 *オプション ライセンス：5 コンテキスト。* • Security Plus ライセンス：基本ライセンスの機能に加えて、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 フィルタリングをサポートします。2 個のコンテキストをサポートします。 *オプション ライセンス：5 コンテキスト*
ASA 5520	基本ライセンス：すべての機能をサポートします。2 個のコンテキストをサポートします。 *オプション ライセンス：5、10、または 20 コンテキスト*
ASA 5540	基本ライセンス：すべての機能をサポートします。2 個のコンテキストをサポートします。 *オプション ライセンス：5、10、20、または 50 コンテキスト*
他のすべてのモデル	サポートしない

CSC SSM の前提条件

CSC SSM には次の前提条件があります。

- CSC SSM カードを ASA に装着する必要があります。
- CSC SSM の登録に使用する Product Authorization Key（PAK）。
- CSC SSM を登録した後に電子メールで受け取るアクティベーション キー。
- CSC SSM の管理ポートを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。
- CSC SSM 管理ポートの IP アドレスには、ASDM の実行に使用するホストからアクセスできる必要があります。

- CSC SSM の設定で使用する次の情報を入手する必要があります。
  - CSC 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。
  - DNS サーバの IP アドレス。
  - HTTP プロキシ サーバ IP アドレス（セキュリティ ポリシーで、HTTP を使用したインターネット アクセスでプロキシ サーバを使用する必要がある場合にのみ必要）。
  - CSC 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、およびポート番号。
  - 製品ライセンス更新通知用の電子メール アドレス。
  - 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 管理ポートと ASA 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。
  - CSC SSM 用のパスワード。

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

フェールオーバーのガイドライン

ステートフル フェールオーバーのセッションはサポートされません。CSC SSM は接続情報を保持しないため、必要な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ている ASA で障害が発生するとドロップされます。スタンバイの ASA 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。

IPv6 のガイドライン

IPv6 はサポートされません。

モデルのガイドライン

ASA 5510、ASA 5520、および ASA 5540 だけでサポートされます。ASA 5580 および ASA 5585-X ではサポートされていません。

その他のガイドライン

モジュールにインストールされるソフトウェアのタイプの変更はできません。CSC モジュールを購入した場合に、後で IPS ソフトウェアをインストールすることはできません。

デフォルト設定

表 67-1 に、CSC SSM のデフォルト設定を示します。

表 67-1　CSC SSM のデフォルト パラメータ

パラメータ	デフォルト
ASA での FTP 検査	Enabled
購入したライセンスに含まれるすべての機能	Enabled

CSC SSM の設定

この項では、CSC SSM を設定する方法について説明します。次の項目を取り上げます。

- 「CSC SSM を設定する前に」（P.67-7）
- 「CSC SSM への接続」（P.67-9）
- 「トラフィックの CSC SSM への転送」（P.67-10）

CSC SSM を設定する前に

ASA および CSC SSM を設定する前に、次の手順を実行します。

ステップ 1　CSC SSM が Cisco ASA 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 Quick Start 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 メッセージに管理ポートを使用します。

ステップ 2　CSC SSM には、製品認証キー（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 キーが届きます。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 で必要な次の情報を入手します。

- アクティベーション キー。
- CSC 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。
- DNS サーバの IP アドレス。
- HTTP プロキシ サーバ IP アドレス（セキュリティ ポリシーで、HTTP を使用したインターネット アクセスでプロキシ サーバを使用する必要がある場合にのみ必要）。
- CSC 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、およびポート番号。
- 製品ライセンス更新通知用の電子メール アドレス

- 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 がインストールされている ASA 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、「その他の参考資料」（P.67-18）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、Telnet、または SSH の ASA アクセスの設定」（P.43-1）を参照してください。

ステップ 5　ASA 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。次のいずれかを実行します。

- 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 を開きます。

ステップ 7　CSC SSM に接続し、ログインします。手順については、「CSC SSM への接続」（P.67-9）を参照してください。

ステップ 8　スキャンするトラフィックを CSC SSM に誘導するサービス ポリシーを設定します。手順については、「トラフィックの CSC SSM への転送」（P.67-10）を参照してください。

ステップ 9　CSC Setup Wizard を実行します。

- CSC Setup Wizard にアクセスするには、[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Wizard Setup] > [Launch Setup Wizard] を選択します。
- CSC Setup Wizard を再実行する場合は、前述と同じ手順を実行してください。

CSC Setup Wizard が表示されます。

ステップ 10　CSC Setup Wizard を完了させます。

（注）　CSC スキャン用のトラフィックを誘導するグローバル サービス ポリシーを作成すると、サポートされているプロトコルのすべてのトラフィック（着信および発信）がスキャンされます。ASA と CSC SSM のパフォーマンスを最大化するには、非信頼送信元からのトラフィックだけをスキャンします。

ステップ 11　CSC SSM に対する負荷を軽減するには、HTTP/HTTPS、SMTP、POP3、または FTP トラフィックのパケットのみを CSC SSM に送信するようにサービス ポリシー ルールを設定します。

ステップ 12　（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。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。機能を使用できるかどうかについては、「CSC SSM のライセンス要件」（P.67-5）を参照してください。デフォルト設定については、「デフォルト設定」（P.67-7）を参照してください。

次の作業

「CSC SSM への接続」（P.67-9）を参照してください。

CSC SSM への接続

ASDM で開始する各セッションでは、CSC SSM に関する機能にアクセスするたびに、管理 IP アドレスを指定して、CSC SSM のパスワードを入力する必要があります。CSC SSM に正常に接続した後は、管理 IP アドレスとパスワードの入力を求めるプロンプトは再表示されません。新しい ASDM セッションを開始すると、CSC SSM への接続がリセットされるので、IP アドレスと CSC SSM パスワードを再び指定する必要があります。ASA で時間帯を変更すると、CSC SSM への接続もリセットされます。

（注）　CSC SSM には、ASDM パスワードとは別に保持されるパスワードがあります。同じパスワードを 2 つ設定することもできますが、CSC SSM パスワードを変更しても ASDM パスワードには影響しません。

CSC SSM に接続するには、次の手順を実行します。

ステップ 1　ASDM のメイン アプリケーション ウィンドウで、[Content Security] タブをクリックします。

ステップ 2　[Connecting to CSC] ダイアログボックスで、次のいずれかのオプション ボタンをクリックします。

- SSM の管理ポートの IP アドレスに接続するには、[Management IP Address] をクリックします。ASDM によって ASA の SSM の IP アドレスが自動的に検出されます。この検出に失敗した場合は、手動で管理 IP アドレスを指定できます。
- SSM の代替 IP アドレスまたはホスト名に接続するには、[Other IP Address or Hostname] にクリックします。

ステップ 3　[Port] フィールドにポート番号を入力し、[Continue] をクリックします。

ステップ 4　[CSC Password] フィールドに CSC パスワードを入力し、[OK] をクリックします。

（注）　CSC Setup Wizard（[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Wizard Setup] を選択）をまだ完了していない場合は、CSC Setup Wizard での設定を完了してください。この中に、デフォルト パスワード「cisco」の変更が含まれています。

パスワード入力後の 10 分間は、CSC SSM GUI の他の部分にアクセスするために CSC SSM パスワードを再入力する必要はありません。

ステップ 5　CSC SSM GUI にアクセスするには、[Configuration] > [Trend Micro Content Security] を選択し、[Web]、[Mail]、[File Transfer]、または [Updates] のいずれかをクリックします。

次の作業

「トラフィックの CSC SSM への転送」（P.67-10）を参照してください。

トラフィックの CSC SSM への転送

ASA がトラフィックを CSC SSM に誘導するように設定するには、モジュラ ポリシー フレームワーク コマンドを使用します。

前提条件

トラフィックを CSC SSM に誘導するように ASA を設定する前に、第 36 章「モジュラ ポリシー フレームワークを使用したサービス ポリシーの設定」を参照してください。モジュラ ポリシー フレームワーク の概念と一般的なコマンドについて説明されています。

トラフィックを CSC SSM に誘導するように ASA を設定するには、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**access-list extended** **例：** `hostname(config)# access-list extended`	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。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/HTTPS、POP3、および SMTP のトラフィックを指定する場合、4 つの 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.67-3）を参照してください。
ステップ 2	**class-map** *class_map_name* **例：** `hostname(config)# class-map class_map_name`	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_name* 引数は、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	**match access-list** *acl-name* **例：** `hostname(config-cmap)# match access-list acl-name`	ステップ 1 で作成したアクセス リストとともに、スキャンするトラフィックを特定します。*acl-name* 引数は、アクセス リストの名前です。
ステップ 4	**policy-map** *policy_map_name* **例：** `hostname(config-cmap)# policy-map policy_map_name`	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。*policy_map_name* 引数は、ポリシー マップの名前です。**policy-map** コマンドを入力すると、CLI がポリシー 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 5	**class** *class_map_name* **例：** `hostname(config-pmap)# class class_map_name`	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_map_name* 引数は、ステップ 2 で作成したクラス マップの名前です。CLI がポリシー マップ クラス コンフィギュレーション モードに移行します。

	コマンド	目的
ステップ 6	**set connection per-client-max** *n* **例：** `hostname(config-pmap-c)# set connection per-client-max 5`	DoS 攻撃を阻止するための制限を設定できます。**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、ASA が CSC SSM に誘導する同時接続を、クライアントごとに制限できます。引数 *n* は、ASA がクライアントごとに許可される同時接続の最大数です。このコマンドは、CSC SSM や SSM によって保護されるサーバによるサービスを、1 つのクライアントが必要以上に大量に使用するのを防ぐものです。たとえば、CSC SSM によって保護される HTTP/HTTPS、FTP、POP3、または SMTP サーバに対する DoS 攻撃を阻止します。

	コマンド	目的
ステップ 7	**csc** {**fail-close** | **fail-open**} **例：** `hostname(config-pmap-c)# csc {fail-close | fail-open}`	CSC SSM でのトラフィック スキャンをイネーブルにし、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。サービス ポリシーの一部である必要があり、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ます。ASA 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、この設定により、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。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、このコマンドは双方向性を持つようになります。双方向性があるということは、ASA 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この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、ASA 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 に誘導すると、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ことになる可能性があります。そのため、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ため、次に一致するアクセス 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/HTTPS 接続 • ASA の内部のクライアントから ASA の外部のサーバへの FTP 接続。 • ASA の内部のクライアントから ASA 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。 **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、ASA 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、「注意事項と制限事項」（P.67-6）を参照してください。

	コマンド	目的
ステップ 8	**service-policy** *policy_map_name* [**global** | **interface** *interface_ID*] **例：** hostname(config-pmap-c)# service-policy *policy_map_name* [global | interface *interface_ID*]	ポリシー マップをグローバルに適用するか、特定のインターフェイスに適用します。*policy_map_name* 引数は、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は、**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のトラフィックに適用するには、**interface** *interface_ID* というキーワードと引数のペアを使用します。ここで *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。

次の作業

「CSC SSM のモニタリング」（P.67-13）を参照してください。

CSC SSM のモニタリング

モジュールのステータスを確認するには、次のいずれかのコマンドを入力します。

コマンド	目的
show module	ステータスを表示します。
show module 1 details	ステータスの追加情報を表示します。
show module 1 recover	イメージをモジュールに転送するためのネットワーク パラメータを表示します。

例

次に、CSC SSM がインストールされている ASA での **show module** コマンドの出力例を示します。

```
hostname# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            JMX1241L05S
  1 ASA 5500 Series Content Security Services Mo ASA-SSM-CSC-10     AF1234BQQL

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.2.1599.0
```

次に、**show module details** コマンドの出力例を示します。この出力の内容は、CSC SSM がインストールされている ASA に関する追加情報です。

```
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: JAF10333331
Firmware version: 1.0(10)0
Software version: Trend Micro InterScan Security Module Version 6.2
App.name: Trend Micro InterScan Security Module
App.version: Version 6.2
Data plane Status: Up
Status: Up
HTTP Service: Up
Mail Service: Up
FTP Service: Up
Activated: Yes
Mgmt IP addr: 209.165.200.225
Mgmt web port: 8443
```

次に、**show module recover** コマンドの出力例を示します。この出力には、CSC SSM がインストールされている ASA の回復の詳細が含まれます。

```
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: 209.165.200.230
Port Mask: 255.255.224.0
Gateway IP Address: 209.165.200.254
```

CSC モジュールのトラブルシューティング

この項では、モジュールの回復やトラブルシューティングに役立つ手順について説明します。次の項目を取り上げます。

- 「モジュールへのイメージのインストール」（P.67-14）
- 「パスワードのリセット」（P.67-15）
- 「モジュールのリロードまたはリセット」（P.67-16）
- 「モジュールのシャットダウン」（P.67-17）

（注） ここでは、ASA のすべてのモジュール タイプを網羅します。使用するモジュールに該当する手順を実行してください。

モジュールへのイメージのインストール

モジュールに障害が発生して、モジュール アプリケーション イメージを実行できない場合は、TFTP サーバからモジュール上に新しいイメージを再インストールできます。

（注） モジュール ソフトウェア内部では、イメージをインストールするために **upgrade** コマンドを使用しないでください。

前提条件

指定する TFTP サーバが、最大 60 MB のサイズのファイルを転送できることを確認してください。

（注）　ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

手順の詳細

	コマンド	目的

ステップ 1	**hw-module module 1 recover configure**
	
	例：
	`hostname# hw-module module 1 recover configure`
	`Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg`
	`Port IP Address [127.0.0.2]: 10.1.2.10`
	`Port Mask [255.255.255.254]: 255.255.255.0`
	`Gateway IP Address [1.1.2.10]: 10.1.2.254`
	`VLAN ID [0]: 100`
		新しいイメージの場所を指定します。このコマンドを実行すると、TFTP サーバの URL、管理インターフェイスの IP アドレスとネットマスク、ゲートウェイ アドレス、および VLAN ID（ASA 5505 のみ）の入力を求めるプロンプトが表示されます。これらのネットワーク パラメータは ROMMON で設定されます。モジュール アプリケーション コンフィギュレーションで設定したネットワーク パラメータは ROMMON には使用できないため、ここで別個に設定する必要があります。
		
		show module 1 recover コマンドを使用してリカバリ コンフィギュレーションを表示できます。
		
		マルチ コンテキスト モードでは、システム実行スペースでこのコマンドを入力します。

ステップ 2	**hw-module module 1 recover boot** **例：** `hostname# hw-module module 1 recover boot`	TFTP サーバからモジュールにイメージを転送し、モジュールを再起動します。
ステップ 3	**show module 1 details** **例：** `hostname# show module 1 details`	イメージ転送とモジュール再起動のプロセスの進捗を確認します。 出力の [Status] フィールドが、モジュールの動作ステータスを示します。モジュールの動作ステータスは、通常は「Up」と表示されます。ASA によってアプリケーション イメージがモジュールに転送されているときは、出力の [Status] フィールドには [Recover] と表示されます。ASA によるイメージの転送が完了してモジュールが再起動されると、新たに転送されたイメージが実行されます。

パスワードのリセット

モジュールのパスワードをデフォルトにリセットできます。デフォルトのパスワードは cisco です。パスワードをリセットした後は、モジュール アプリケーションを使用してパスワードを独自の値に変更する必要があります。

モジュールのパスワードをリセットすると、モジュールがリブートします。モジュールのリブート中は、サービスを使用できません。

モジュールのパスワードをデフォルトの「cisco」にリセットするには、次の手順を実行します。

手順の詳細

コマンド	目的
hw-module module 1 password-reset **例：** `hostname# hw-module module 1 password-reset`	モジュールのパスワードを cisco にリセットします。*1* は SSM ハードウェア モジュール上の指定したスロット番号です。CSC SSM で、このコマンドを入力すると、パスワードがリセットされた後でハードウェア モジュールの Web サービスがリセットされます。ASDM への接続が失われる、またはハードウェア モジュールからログ アウトされることがあります。CSC SSM では、最新バージョン 6.3（2010 年 1 月）および以降のバージョンでこのコマンドがサポートされています。 **（注）** SSM ハードウェア モジュールがアップ状態にあり、パスワードのリセットがサポートされていることを確認します。

モジュールのリロードまたはリセット

モジュールをリロードまたはリセットするには、ASA CLI で次のいずれかのコマンドを入力します。

手順の詳細

コマンド	目的
hw-module module 1 reload **例：** `hostname# hw-module module 1 reload`	モジュール ソフトウェアをリロードします。
hw-module module 1 reset **例：** `hostname# hw-module module 1 reset`	リセットを実行してから、モジュールをリロードします。

モジュールのシャットダウン

ASA を再起動したときに、モジュールは自動的には再起動されません。モジュールをシャットダウンするには、ASA CLI で次の手順を実行します。

手順の詳細

コマンド	目的
hw-module module 1 shutdown **例：** hostname# hw-module module 1 shutdown	モジュールをシャットダウンします。

CSC SSM の設定例

スキャンするトラフィックを特定するようにASAを設定する方法はさまざまです。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。次の例は図 67-3 に示したネットワークに基づいており、一般的な CSC SSM スキャン シナリオを使用する 2 つのサービス ポリシーの作成を示しています。

- 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。

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

hostname(config-pmap-c)# 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-cmap)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

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

次の例は、アクセス リストを使用してトラフィックをポリシー マップによる照合から免除し、ASA がトラフィックを CSC SSM に送信できないようにします。

```
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
```

次の例は、ACE を csc_out アクセス リストに追加して、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。

```
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 209.165.201.7
255.255.255.255 eq 80
```

次の例は、外部インターフェイスに適用されるサービス ポリシーでアクセス リストを使用します。

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

次の例は、ACE を csc_in アクセス リストに追加し、CSC SSM を使用して、外部ホストから HTTP 経由でアップロードされる感染したファイルから DMZ ネットワークの Web サーバを保護できます。

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

その他の参考資料

CSC SSM の実装に関するその他の情報については、次のマニュアルを参照してください。

関連項目	参照先
CSC SSM GUI の使用方法。 CSC SSM GUI で使用できる特定のウィンドウの追加ライセンス要件。 修正する前、または高度なコンフィギュレーション設定を入力する前の、CSC SSM GUI でのデフォルトのコンテンツ セキュリティ ポリシーの確認。	*『Cisco Content Security and Control SSM Administrator Guide』*
ASDM への初めてのアクセス、および Startup Wizard に関する説明。	*『Cisco ASA 5500 Series Quick Start Guide』*
SSM のハードウェアの設置に関する説明、および ASA への接続。	ハードウェア ガイド
ASDM への初めてのアクセス、および Startup Wizard に関する説明。	*『Cisco ASA 5500 Series Quick Start Guide』*

関連項目	参照先
CSC SSM GUI の使用方法。 CSC SSM GUI で使用できる特定のウィンドウの追加ライセンス要件。 修正する前、または高度なコンフィギュレーション設定を入力する前の、CSC SSM GUI でのデフォルトのコンテンツ セキュリティ ポリシーの確認。	『*Cisco Content Security and Control SSM Administrator Guide*』
技術マニュアル、マーケティング、およびサポートに関する情報。	次の URL を参照してください。 http://www.cisco.com/en/US/products/ps6823/index.html

CSC SSM の機能履歴

表 67-2 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。

表 67-2　CSC SSM の機能履歴

機能名	プラットフォーム リリース	機能情報
CSC SSM	7.0(1)	CSC SSM は Content Security and Control ソフトウェアを実行し、ウイルス、スパイウェア、スパム、など望ましくないトラフィックから保護します。 **csc {fail-close | fail-open}**、**hw-module module 1** [**recover** | **reload** | **reset** | **shutdown**]、**session**、**show module** [**all** | *slot* [**details** | **recover**]] の各コマンドが導入されました。
パスワードのリセット	7.2(2)	**hw-module module password-reset** コマンドが導入されました。
CSC SSM	8.1(1) および 8.1(2)	この機能は、ASA 5580 ではサポートされいません。
CSC syslog 形式	8.3(1)	CSC syslog 形式は、ASA syslog 形式に一致しています。syslog メッセージの説明は、『*Cisco Content Security and Control SSM Administrator Guide*』に追加されています。すべての syslog メッセージには事前定義の syslog プライオリティが含まれており、CSC SSM GUI を通じて設定することはできません。