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。

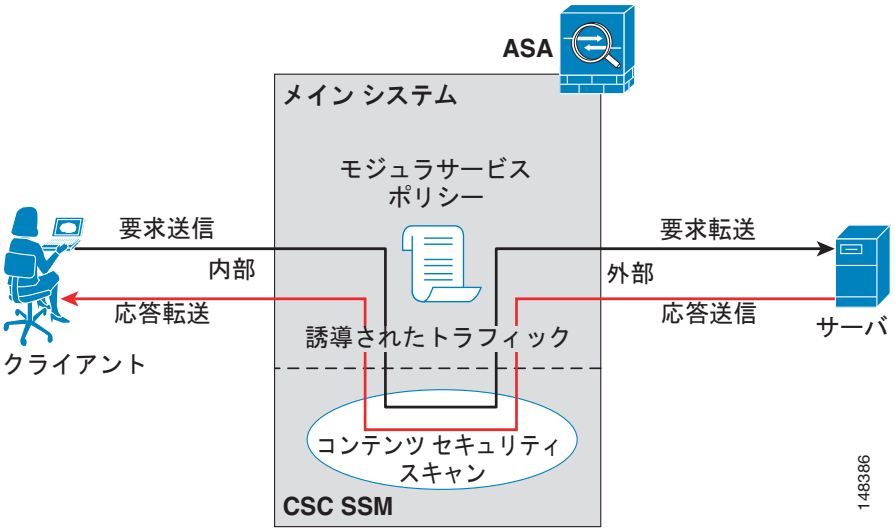
http://www.cisco.com/en/US/products/ps6823/index.html

図 31-1 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 31-1　　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。

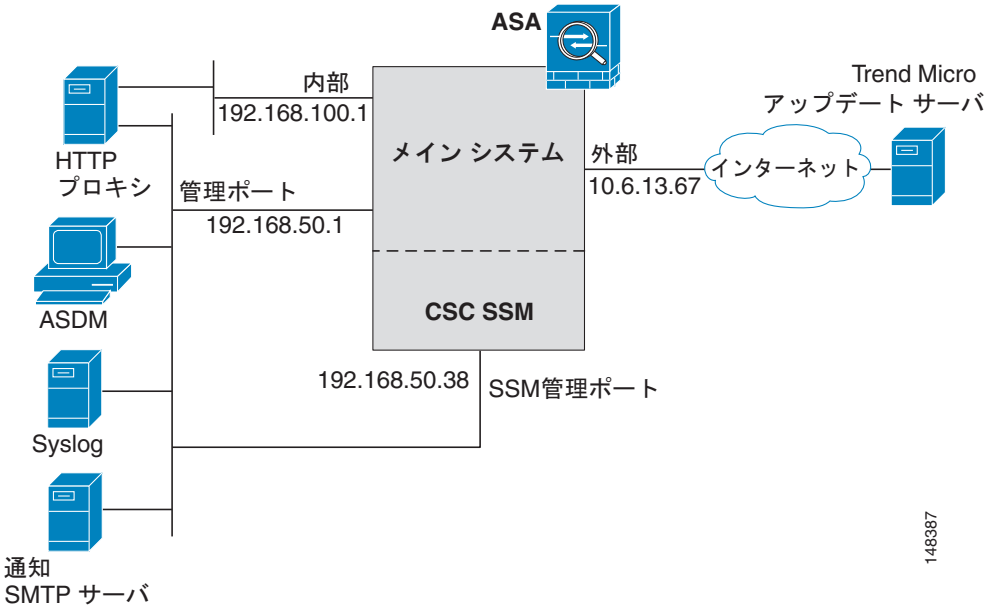
（注） ASDM と CSC SSM では、別個のパスワードが保持されます。それぞれのパスワードを同一にすることはできますが、これら 2 つのパスワードの 1 つを変更しても他のパスワードには影響を与えません。

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 31-2 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 31-2　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。

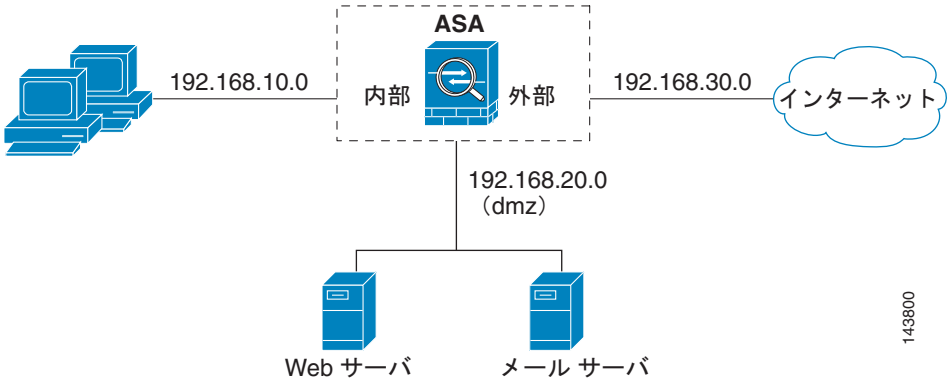
ASA と CSC SSM のパフォーマンスを最大化するには、CSC SSM でスキャンするトラフィックだけを CSC SSM に誘導します。信頼できる送信元と宛先間のトラフィックなど、スキャンしないトラフィックまで誘導すると、ネットワークのパフォーマンスに悪影響を与える可能性があります。

（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。詳細については、「CSC スキャンのためのサービス ポリシー ルール アクションの決定」（P.31-10）を参照してください。

図 31-3 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。

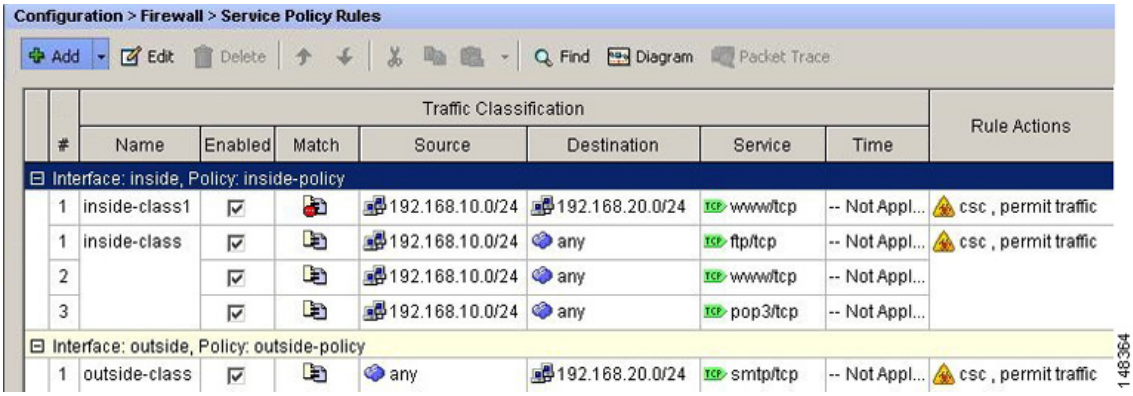
図 31-3　スキャンの一般的なネットワーク コンフィギュレーション



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 ACL を含める方法があります。

図 31-4 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 31-4　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 31-1 に、CSC SSM のデフォルト設定を示します。

表 31-1　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	イネーブル
購入したライセンスに含まれるすべての機能	イネーブル

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.31-7）
- 「CSC SSM への接続」（P.31-9）
- 「CSC スキャンのためのサービス ポリシー ルール アクションの決定」（P.31-10）

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、「その他の関連資料」（P.31-31）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、一般的な操作のコンフィギュレーション ガイドの “Configuring ASA Access for ASDM, Telnet, or SSH” section on page 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.31-9）を参照してください。

ステップ 8　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 9　CSC Setup Wizard を最後まで実行します。この中で、スキャン対象のトラフィックを CSC SSM に誘導するためのサービス ポリシーを設定します。

（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 10　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。手順については、「CSC スキャンのためのサービス ポリシー ルール アクションの決定」（P.31-10）を参照してください。

ステップ 11　（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.31-5）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.31-7）を参照してください。

次の作業

「CSC SSM への接続」（P.31-9）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

「CSC スキャンのためのサービス ポリシー ルール アクションの決定」（P.31-10）を参照してください。

CSC スキャンのためのサービス ポリシー ルール アクションの決定

CSC SSM は、HTTP/HTTPS、SMTP、POP3、および FTP トラフィックのみスキャンします。使用するサービス ポリシーに、これら 4 種類のプロトコル以外のプロトコルをサポートするトラフィックが含まれていると、他のプロトコルのパケットは、スキャンされることなく CSC SSM を通過します。HTTP/HTTPS、SMTP、POP3、または FTP のトラフィックのパケットだけを CSC SSM に送信するようにサービス ポリシー ルールを設定してください。

Add Service Policy Rule Wizard の [CSC Scan] タブを使用すると、現在のトラフィック クラスが示すトラフィックが CSC SSM によってスキャンされるかどうかを判定することができます。このタブは、ASA に CSC SSM が取り付けられていないと表示されません。

CSC スキャンのサービス ポリシー ルールを設定するには、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、[Configuration] > [Firewal]l > [Service Policy Rules] を選択します。

ステップ 2　ツールバーの [Add] をクリックします。

[Add Service Policy Rule Wizard] 画面が表示されます。

ステップ 3　[Global - applies to all interfaces] オプションをクリックして、[Next] をクリックします。

[Traffic Classification Criteria] 画面が表示されます。

ステップ 4　[Create a new traffic class] オプションをクリックして、隣のフィールドにトラフィック クラスの名前を入力し、[Any traffic] チェックボックスをオンにしてから、[Next] をクリックします。

[Rules Actions] 画面が表示されます。

ステップ 5　[CSC Scan] タブをクリックして、[Enable CSC scan for this traffic flow] チェックボックスをオンにします。

ステップ 6　[If CSC card fails, then] というラベルの付いた領域で適切な選択を行って、CSC SSM が使用不可の場合に、選択したトラフィックの通過を ASA で許可するか拒否するかを選択します。このチェックボックスをオンにすると、このタブの他のパラメータがアクティブになります。

ステップ 7　[If CSC card fails] 領域で、CSC SSM が動作不能になった場合のアクションを、次のいずれかから選択します。

- トラフィックを許可する場合は、[Permit traffic] チェックボックスをオンにします。
- トラフィックをブロックする場合は、[Close traffic] チェックボックスをオンにします。

ステップ 8　[Finish] をクリックします。

新しいサービス ポリシー ルールが [Service Policy Rules] ペインに表示されます。

ステップ 9　[Apply] をクリックします。

ASA は、購入したライセンスによってイネーブルになったコンテンツ セキュリティ スキャンを実行する CSC SSM へのトラフィックの誘導を開始します。

CSC SSM セットアップ ウィザード

[CSC Setup Wizard] では、CSC SSM の基本操作パラメータを設定できます。各画面でオプションを個別に設定する前に、このウィザードを少なくとも 1 回完了する必要があります。CSC Setup Wizard を完了した後は、このウィザードを再度使用しなくても各画面を個別に変更できます。

また、[CSC Setup Wizard] を完了するまでは、[Configuration] > [Trend Micro Content Security] > [CSC Setup or under Monitoring] > [Trend Micro Content Security] > [Content Security] の下にあるパネルにアクセスできません。このウィザードが完了する前にそれらのペインにアクセスしようとすると、ダイアログボックスが表示され、そこからウィザードに直接アクセスして設定を完了させることができます。

[CSC Setup Wizard] を開始するには、[Launch Setup Wizard] をクリックします。

この項では、次のトピックについて取り上げます。

Activation/License

[Activation/License] ペインでは、CSC SSM の基本ライセンスおよび Plus ライセンスのアクティベーション コードを確認または更新できます。

ASDM を使用して、2 つのライセンスにそれぞれ一度だけ CSC ライセンスを設定できます。ソフトウェアのアップデートをスケジュールしておくと、更新されたライセンス アクティベーション コードが自動的にダウンロードされます。ライセンス ステータス ペインと CSC UI ホーム ペインへのリンクがこのウィンドウの下部に表示されます。割り当てられたライセンスのシリアル番号が自動的に入力されます。

ライセンス ステータスを確認する、またはライセンスを更新するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Activation/License] を選択します。

ステップ 2　[Activation/License] ペインには、基本ライセンスおよび Plus ライセンスに関する次の情報が表示されますが、この情報は表示専用です。

- コンポーネントの名前。
- 対応する [Product] フィールドのアクティベーション コード。
- ライセンスのステータス。ライセンスが有効な場合、有効期限が表示されます。有効期限が過ぎている場合は、このフィールドにライセンスが失効している旨が表示されます。
- 基本ライセンスでサポートされているネットワーク デバイスの最大数。Plus ライセンスはサポートされているネットワーク デバイスの数に影響しません。したがって、[Plus License] 領域には [Nodes] フィールドが表示されません。基本ライセンスには、アンチウイルス、アンチスパイウェア、およびファイル ブロッキングが含まれます。Plus ライセンスには、アンチスパム、アンチフィッシング、コンテンツ フィルタリング、URL ブロッキングと URL フィルタリング、および Web レピュテーションが含まれます。

ステップ 3　ライセンス ステータスを確認する、またはライセンスを更新するには、表示されるリンクをクリックします。

ステップ 4　ASDM の CSC ホーム ペインに移動するには、表示されるリンクをクリックします。

次の作業

「IP 設定」（P.31-12）を参照してください。

IP 設定

[IP Configuration] ペインでは、CSC SSM の管理アクセス、使用する DNS サーバ、および CSC SSM ソフトウェアのアップデートを取得するためのプロキシ サーバを設定できます。

CSC SSM の管理アクセスおよびその他の関連詳細情報を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [IP Configuration] を選択します。

ステップ 2　CSC SSM に管理アクセスするための次のパラメータを設定します。

- CSC SSM への管理アクセスのための IP アドレスを入力します。
- CSC SSM の管理 IP アドレスが含まれるネットワークのネットマスクを入力します。
- CSC SSM の管理 IP アドレスが含まれるネットワークのゲートウェイ デバイスの IP アドレスを入力します。

ステップ 3　CSC SSM の管理 IP アドレスを含むネットワークの DNS サーバに関するパラメータを設定します。

- プライマリ DNS サーバの IP アドレスを入力します。
- （任意）セカンダリ DNS サーバの IP アドレス（設定されている場合）を入力します。

ステップ 4　（任意）CSC SSM が CSC SSM ソフトウェアのアップデート サーバに接続するために使用する HTTP プロキシ サーバのパラメータを入力します。ネットワーク コンフィギュレーションで、CSC SSM でプロキシ サーバの使用を必要としない場合、このグループのフィールドを空白のままにしてください。

- プロキシ サーバの IP アドレス（設定されている場合）を入力します。
- プロキシ サーバの受信ポート（設定されている場合）を入力します。

次の作業

「ホスト設定と通知設定」（P.31-12）を参照してください。

ホスト設定と通知設定

[Host/Notification Settings] ペインでは、ホスト名、ドメイン名、電子メール通知、および詳細なスキャンから除外する電子メールのドメイン名に関する詳細を設定できます。

ホストおよび通知設定を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Host/Notification Settings] を選択します。

ステップ 2　[Host and Domain Names] 領域で、CSC SSM のホスト名とドメイン名を設定します。

ステップ 3　[Incoming E-mail Domain Name] 領域で、SMTP ベースの電子メールに対する信頼できる着信電子メール ドメイン名を設定します。CSC SSM は、このドメインに送信された SMTP 電子メールをスキャンします。CSC SSM がスキャンする脅威のタイプは、購入した CSC SSM のライセンスと、CSC SSM ソフトウェアのコンフィギュレーションによって異なります。

（注）　CSC SSM では、着信電子メールド メインのリストを多数設定できます。ASDM は、最初のドメインだけをリストに表示します。着信電子メールのドメインを追加設定するには、CSC SSM インターフェイスにアクセスします。このインターフェイスにアクセスするには、[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Mail] を選択し、リンクのいずれかをクリックします。CSC SSM にログインしたら、[Mail (SMTP)] > [Configuration] を選択して [Incoming Mail] タブをクリックします。

ステップ 4　イベントの電子メール通知に、次の設定値を設定します。

- 電子メール通知の送信先となるアカウントの管理者の電子メール アドレス。
- SMTP サーバの IP アドレス。
- SMTP サーバがリッスンするポート。
- 通知電子メールを送信する必要がある製品ライセンス更新用の電子メール アドレス。複数の電子メール アドレスはセミコロンで区切ります。電子メール アドレスの長さは、最大で 1024 文字までです。指定した電子メール アドレスが有効であることを確認します。

次の作業

「管理アクセスホストとネットワーク」（P.31-13）を参照してください。

管理アクセスホストとネットワーク

[Management Access Host/Networks] ペインでは、CSC SSM への管理アクセスを許可するホストとネットワークを指定できます。許可するホストまたはネットワークを少なくとも 1 つ以上指定する必要があり、最大 8 つまでのホストまたはネットワークが許可されます。

CSC SSM への管理アクセスを許可するホストおよびネットワークを指定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Management Access Host/Networks] を選択します。

ステップ 2　[Selected Hosts/Network] リストに追加するホストまたはネットワークのアドレスを入力します。

ステップ 3　[IP Address] フィールドに指定したホストまたはネットワークのネットマスクを指定します。

（注）　すべてのホストとネットワークを許可するには、[IP Address] フィールドに **0.0.0.0** と入力し、[Mask] リストから 0.0.0.0 を選択します。

[Selected Hosts/Networks] リストに、CSC SSM への管理アクセスに信頼できるホストまたはネットワークが表示されます。

ステップ 4　[Selected Hosts/Networks] リストに、[IP Address] フィールドで指定したホストまたはネットワークを追加するには、[Add] をクリックします。

[Selected Hosts/Networks] テーブルには、追加した CSC SSM に接続可能なネットワークおよびホストの IP アドレスが表示されます。

ステップ 5　[Selected Hosts/Networks] リストからホストまたはネットワークを削除するには、リストからエントリを選択して、[Delete] をクリックします。

次の作業

「パスワード」（P.31-14）を参照してください。

パスワード

[Password] ペインでは、CSC SSM への管理アクセスに必要なパスワードを変更できます。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。それらに同じパスワードを設定できますが、CSC SSM のパスワードを変更しても ASDM のパスワードは変更されません。

ASDM が CSC SSM に接続されているときに CSC SSM パスワードを変更すると、CSC SSM への接続はドロップされます。その結果、ASDM には確認ダイアログボックスが表示されるので、パスワードを変更する前に応答する必要があります。

ヒント　CSC SSM への接続がドロップされた場合は、常にその接続を再確立できます。再確立するには、ステータス バーの [Connection to Device] アイコンをクリックして [Connection to Device] ダイアログボックスを表示し、[Reconnect] をクリックします。ASDM は、CSC SSM のパスワードを要求するプロンプトを表示します。このパスワードは、定義済みの新規パスワードです。

パスワードの長さは、5 ～ 32 文字で指定します。

パスワードを入力するとアスタリスクで表示されます。

（注）　デフォルトのパスワードは「cisco」です。

CSC SSM への管理アクセスに必要なパスワードを変更するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Password] を選択します。

ステップ 2　[Old Password] フィールドに、CSC SSM に管理アクセスするための現在のパスワードを入力します。

ステップ 3　[New Password] フィールドに、CSC SSM に管理アクセスするための新しいパスワードを入力します。

ステップ 4　[Confirm New Password] フィールドに、CSC SSM に管理アクセスするための新しいパスワードを再度入力します。

次の作業

必要に応じて、「デフォルト パスワードの復元」（P.31-15）を参照してください。

「ウィザードの設定」（P.31-15）を参照してください。

デフォルト パスワードの復元

ASDM を使用して CSC SSM のパスワードをリセットできます。このパスワードは、「cisco」（かぎカッコなし）というデフォルト値に戻すことができます。CSC パスワードリセット ポリシーが「Denied」に設定されていると、ASDM CLI を使用してパスワードをリセットできません。このポリシーを変更するには、ASA CLI から **session** コマンドを入力して CSC SSM にアクセスする必要があります。詳細については、『*Cisco Content Security and Control SSM Administrator Guide*』を参照してください。

（注）　SSM がインストールされていないと、このオプションはメニューに表示されません。

CSC SSM パスワードをデフォルト値にリセットするには、次の手順を実行します。

ステップ 1　[Tools] > [CSC Password Reset] を選択します。

[CSC Password Reset confirmation] ダイアログボックスが表示されます。

ステップ 2　[OK] をクリックして、CSC SSM パスワードをデフォルト値にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。パスワードがリセットされなかったときは、ASA でバージョン 8.0（2）のソフトウェアを使用していること、および CSC SSM で最新のバージョン 6.1.x ソフトウェアを使用していることを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

ステップ 4　パスワードをリセットしたら、一意のパスワードに変更する必要があります。

次の作業

「パスワード」（P.31-14）を参照してください。

ウィザードの設定

[Wizard Setup] 画面では、CSC Setup Wizard を起動できます。[CSC Setup Wizard] を開始するには、[Launch Setup Wizard] をクリックします。[Wizard Setup] 画面にアクセスするには、[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Wizard Setup] を選択します。

[CSC Setup] で他の画面に直接アクセスする前に、CSC Setup Wizard を完了する必要があります。このウィザードには、次の画面があります。

- 「CSC Setup Wizard アクティベーション コードの設定」（P.31-16）
- 「CSC Setup Wizard の IP コンフィギュレーション」（P.31-16）
- 「CSC Setup Wizard のホスト コンフィギュレーション」（P.31-16）
- 「CSC Setup Wizard の管理アクセス コンフィギュレーション」（P.31-17）
- 「CSC Setup Wizard のパスワード コンフィギュレーション」（P.31-17）
- 「CSC Setup Wizard の CSC スキャンのためのトラフィック選択」（P.31-18）
- 「CSC Setup Wizard の要約」（P.31-19）

CSC Setup Wizard を完了したら、CSC Setup Wizard を再度使用しなくても CSC SSM の関連画面で設定を変更できます。

CSC Setup Wizard アクティベーション コードの設定

CSC SSM の機能をイネーブルにするために入力したアクティベーション コードを表示するには、次の手順を実行します。

[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Activation/License] を選択します。

この画面には、入力したアクティベーション コード設定値が、所有するライセンスのタイプに応じて次のように表示されます。

- 基本ライセンスのアクティベーション コードが表示されます。基本ライセンスには、アンチウイルス、アンチスパイウェア、およびファイル ブロッキングが含まれます。
- Plus ライセンスのアクティベーション コードを入力した場合は、このアクティベーション コードが表示されます。入力していないときは、空白になります。Plus ライセンスには、アンチスパム、アンチフィッシング、コンテンツ フィルタリング、URL ブロッキングと URL フィルタリング、および Web レピュテーションが含まれます。

次の作業

「CSC Setup Wizard の IP コンフィギュレーション」（P.31-16）を参照してください。

CSC Setup Wizard の IP コンフィギュレーション

CSC SSM に入力した IP コンフィギュレーション設定を表示するには、次の手順を実行します。

[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [IP Configuration] を選択します。

CSC SSM に入力した IP コンフィギュレーション設定が表示され、これには次の情報が含まれます。

- CSC SSM の管理インターフェイスの IP アドレス。
- ドロップダウン リストから選択した CSC SSM の管理インターフェイスのネットワーク マスク。
- CSC SSM 管理インターフェイスが含まれるネットワークのゲートウェイ デバイスの IP アドレス。
- プライマリ DNS サーバの IP アドレス。
- セカンダリ DNS サーバの IP アドレス（設定している場合）。
- プロキシ サーバ（設定している場合）。
- プロキシ ポート（設定している場合）。

次の作業

「CSC Setup Wizard のホスト コンフィギュレーション」（P.31-16）を参照してください。

CSC Setup Wizard のホスト コンフィギュレーション

CSC SSM に入力したホスト コンフィギュレーション設定を表示するには、次の手順を実行します。

[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Host Configuration] を選択します。

CSC SSM に入力したホスト コンフィギュレーション設定が表示されます、この設定には次の情報が含まれます。

- CSC SSM のホスト名。

- CSC SSM が常駐するドメインの名前。
- 着信電子メールのドメイン名。
- ドメイン管理者の電子メール アドレス。
- SMTP サーバの IP アドレス。
- SMTP サーバがリッスンするポート。
- 製品ライセンス更新通知用の電子メール アドレス。

次の作業

「CSC Setup Wizard の管理アクセス コンフィギュレーション」（P.31-17）を参照してください。

CSC Setup Wizard の管理アクセス コンフィギュレーション

CSC SSM へのアクセス権を付与するために入力したサブネットおよびホスト設定を表示するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Management Access Configuration] を選択します。

CSC SSM に入力した管理アクセス コンフィギュレーション設定が表示されます、この設定には次の情報が含まれます。

- CSC SSM への接続が許可されているネットワークおよびホストの IP アドレス。
- ドロップダウン リストから選択した CSC SSM への接続が許可されているネットワークとホストのネットワーク マスク。

ステップ 2　CSC SSM への接続を許可するネットワークおよびホストの IP アドレスを追加する場合は、[Add] をクリックします。

ステップ 3　CSC SSM に接続する必要がなくなったネットワークまたはホストの IP アドレスを削除する場合は、[Delete] をクリックします。

[Selected Hosts/Networks] テーブルには、追加した CSC SSM に接続可能なネットワークおよびホストの IP アドレスが表示されます。

次の作業

「CSC Setup Wizard のパスワード コンフィギュレーション」（P.31-17）を参照してください。

CSC Setup Wizard のパスワード コンフィギュレーション

CSC SSM への管理アクセスに必要なパスワードを変更するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Password] を選択します。

ステップ 2　[Old Password] フィールドに、CSC SSM に管理アクセスするための現在のパスワードを入力します。

ステップ 3　[New Password] フィールドに、CSC SSM に管理アクセスするための新しいパスワードを入力します。

ステップ 4　[Confirm New Password] フィールドに、CSC SSM に管理アクセスするための新しいパスワードを再度入力します。

次の作業

「CSC Setup Wizard の CSC スキャンのためのトラフィック選択」（P.31-18）を参照してください。

CSC Setup Wizard の CSC スキャンのためのトラフィック選択

CSC スキャン対象のトラフィックを選択するために行った設定を表示するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Traffic Selection for CSC Scan] を選択します。

CSC SSM に入力した CSC スキャン対象のトラフィックを選択するためのコンフィギュレーション設定が表示され、この設定には次の情報が含まれます。

- ドロップダウン リストから選択した CSC SSM へのインターフェイス。
- CSC SSM がスキャンするネットワーク トラフィックの送信元。
- CSC SSM がスキャンするネットワーク トラフィックの宛先。
- CSC SSM がスキャンする送信元サービスまたは宛先サービス。

ステップ 2　次のいずれかを実行します。

- CSC スキャンに関する追加のトラフィック詳細を指定する場合は、[Add] をクリックします。詳細については、「CSC スキャン対象のトラフィック指定」（P.31-18）を参照してください。
- CSC スキャンに関する追加のトラフィック詳細を変更する場合は、[Edit] をクリックします。詳細については、「CSC スキャン対象のトラフィック指定」（P.31-18）を参照してください。
- CSC スキャンに関する追加のトラフィック詳細を削除する場合は、[Delete] をクリックします。

CSC スキャン対象のトラフィック指定

CSC スキャン対象のトラフィックを選択するための追加設定を定義、変更、または削除するには、次の手順を実行します。

ステップ 1　[Traffic Selection for CSC Scan] 画面で、[Specify traffic for CSC Scan] をクリックします。

[Specify traffic for CSC Scan] ダイアログボックスが表示されます。

ステップ 2　CSC SSM へのインターフェイスのタイプをドロップダウン リストから選択します。指定できる設定値は、global（すべてのインターフェイス）、inside、management、outside です。

ステップ 3　CSC SSM がスキャンするネットワーク トラフィックの送信元をドロップダウン リストから選択します。

ステップ 4　CSC SSM がスキャンするネットワーク トラフィックの宛先をドロップダウン リストから選択します。

ステップ 5　CSC SSM がスキャンするサービスのタイプをドロップダウン リストから選択します。

ステップ 6　CSC SSM がスキャンするように定義したネットワーク トラフィックの説明を入力します。

ステップ 7　CSC カードに障害が発生した場合に、CSC SSM にネットワーク トラフィックのスキャンを許可するかどうかを指定します。次のいずれかのオプションを選択します。

- スキャンされていないトラフィックの通過を許可するには、[Permit] をクリックします。
- スキャンされていないトラフィックが通過しないようにするには、[Close] をクリックします。

ステップ 8　[OK] をクリックして設定内容を保存します。

[CSC Setup Wizard Traffic selection for CSC Scan] 画面に、追加したトラフィック詳細が表示されます。

ステップ 9　これらの設定内容を破棄して [CSC Setup Wizard Traffic selection for CSC Scan] 画面に戻るには、[Cancel] をクリックします。[Cancel] をクリックすると、ASDM にはユーザの決定を確認するダイアログボックスが表示されます。

次の作業

「CSC Setup Wizard の要約」（P.31-19）を参照してください。

CSC Setup Wizard の要約

CSC Setup Wizard で行った設定内容を確認するには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Summary] を選択します。

[CSC Setup Wizard Summary] 画面に、次の設定内容が表示されますが、この設定内容は表示専用です。

- [Activation Codes Configuration] 画面で行った設定。基本ライセンスのアクティベーション コードおよび Plus ライセンスのアクティベーション コード（入力した場合）を含みます。入力していないときは、空白になります。
- [IP Configuration] 画面で行った設定。次の情報が含まれています。
  - CSC SSM の管理インターフェイスの IP アドレスとネットマスク。
  - CSC SSM 管理インターフェイスが含まれるネットワークのゲートウェイ デバイスの IP アドレス。
  - プライマリ DNS サーバの IP アドレス。
  - セカンダリ DNS サーバの IP アドレス（設定している場合）。
  - プロキシ サーバおよびポート（設定している場合）。
- [Host Configuration] 画面で行った設定。次の情報が含まれています。
  - CSC SSM のホスト名。
  - CSC SSM が含まれるドメインのドメイン名。
  - 着信電子メールのドメイン名。
  - 管理者の電子メール アドレス。
  - 電子メール サーバの IP アドレスとポート番号。
  - 製品ライセンス更新通知用の電子メール アドレス。
- [Management Access Configuration] 画面で行った設定。ドロップダウン リストには、CSC SSM が管理接続を許可するホストとネットワークが含まれています。
- [Password Configuration] 画面でパスワードを変更したかどうかを示します。

ステップ 2　（任意）CSC Setup Wizard の前の画面に戻って設定を変更するには、[Back] をクリックします。

（注）　[Next] ボタンはグレー表示されています。ただし、[Back] をクリックしてこのウィザードの前の画面のいずれかにアクセスした場合は、[Next] をクリックすると [Summary] 画面に戻ります。

ステップ 3　[Finish] をクリックして [CSC Setup Wizard] を終了し、指定したすべての設定を保存します。[Finish] をクリックした後は、CSC Setup Wizard を再度使用しなくても CSC SSM に関連するいずれの設定も変更できます。

デバイスに送信されたコマンドのステータスに関する要点が表示されます。

ステップ 4　[Close] をクリックしてこの画面を閉じ、[Next] をクリックします。

CSC SSM が起動し、使用状態になったことを示すメッセージが表示されます。

ステップ 5　（任意）[Cancel] をクリックすると、選択した設定内容を保存せずに CSC Setup Wizard を終了します。[Cancel] をクリックすると、ユーザの決定を確認するダイアログボックスが表示されます。

次の作業

「CSC SSM GUI の使用」（P.31-20）を参照してください。

CSC SSM GUI の使用

この項では、CSC SSM GUI を使用して機能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。

Web

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

Web 関連機能がイネーブルになっているかどうかを確認したり、これらの機能を設定するために CSC SSM GUI にアクセスするには、次の手順を実行します。

ステップ 1　[Configuration] > [Trend Micro Content Security] > [Web] を選択します。

[URL Blocking and Filtering] 領域は表示専用であり、CSC SSM で URL ブロッキングがイネーブルになっているかどうかを示します。

ステップ 2　[Configure URL Blocking] をクリックして、CSC SSM で URL ブロッキングを設定するための画面を開きます。

[URL Filtering] 領域は表示専用であり、CSC SSM で URL フィルタリングがイネーブルになっているかどうかを示します。

ステップ 3　[Configure URL Filtering] をクリックして、CSC SSM で URL フィルタリング ルールを設定するための画面を開きます。

[File Blocking] 領域は表示専用であり、CSC SSM で URL ファイル ブロッキングがイネーブルになっているかどうかを示します。

ステップ 4　[Configure File Blocking] をクリックして、CSC SSM でファイル ブロッキング設定を行うための画面を開きます。

[HTTP Scanning] 領域は表示専用であり、CSC SSM で HTTP スキャンがイネーブルになっているかどうかを示します。

ステップ 5　[Configure Web Scanning] をクリックして、CSC SSM で HTTP スキャンの設定を行うための画面を開きます。

[Web Reputation] 領域は表示専用であり、CSC SSM で Web レピュテーション サービスがイネーブルかどうかを示します。

ステップ 6　[Configure Web Reputation] をクリックして、CSC SSM で Web レピュテーション サービスの設定を行うための画面を開きます。

次の作業

「MAIL」（P.31-21）を参照してください。

MAIL

[Mail] ペインでは、電子メール関連の機能がイネーブルになっているかどうかを確認し、CSC SSM GUI にアクセスして電子メール関連機能を設定できます。電子メール関連機能を設定するには、[Configuration] > [Trend Micro Content Security] > [Mail] を選択します。

この項では、次のトピックについて取り上げます。

[SMTP] タブ

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

SMTP スキャンを設定するには、次の手順を実行します。

ステップ 1　[SMTP] タブをクリックします。

ステップ 2　[Incoming Scan] 領域は表示専用であり、CSC SSM で着信 SMTP スキャン機能がイネーブルになっているかどうかを示します。[Configure Incoming Scan] をクリックして、CSC SSM で着信 SMTP スキャン設定を行うための画面を開きます。

ステップ 3　[Outgoing Scan] 領域は表示専用であり、CSC SSM で発信 SMTP スキャン機能がイネーブルになっているかどうかを示します。[Configure Outgoing Scan] をクリックして、CSC SSM で発信 SMTP スキャン設定を行うための画面を開きます。

ステップ 4　[Incoming Filtering] 領域は表示専用であり、CSC SSM で着信 SMTP 電子メールのコンテンツ フィルタリングがイネーブルになっているかどうかを示します。[Configure Incoming Filtering] をクリックして、CSC SSM で着信 SMTP 電子メール コンテンツ フィルタリング設定を行うための画面を開きます。

ステップ 5　[Outgoing Filtering] 領域は表示専用であり、CSC SSM で発信 SMTP 電子メールのコンテンツ フィルタリングがイネーブルになっているかどうかを示します。[Configure Outgoing Filtering] をクリックして、CSC SSM で発信 SMTP 電子メール コンテンツ フィルタリング設定を行うための画面を開きます。

ステップ 6　[Anti-spam] 領域は表示専用であり、CSC SSM で SMTP アンチスパム機能がイネーブルになっているかどうかを示します。[Configure Anti-spam] をクリックして、CSC SSM で SMTP アンチスパム設定（Email レピュテーションを含む）を行うための画面を開きます。

ステップ 7　[Global Approved List] 領域は表示専用であり、CSC SSM で SMTP のグローバルな承認済みリスト機能がイネーブルになっているかどうかを示します。[Configure Global Approved List] をクリックして、CSC SSM で SMTP のグローバルな承認済みリスト設定値を設定するための画面を開きます。

[POP3] タブ

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

POP3 スキャンを設定するには、次の手順を実行します。

ステップ 1　[POP3] タブをクリックします。

ステップ 2　[Scanning] 領域は表示専用であり、CSC SSM で POP3 電子メール スキャンがイネーブルになっているかどうかを示します。[Configure Scanning] をクリックして、CSC SSM で POP3 電子メール スキャン設定を行うためのウィンドウを開きます。

ステップ 3　[Anti-spam] 領域は表示専用であり、CSC SSM で POP3 アンチスパム機能がイネーブルになっているかどうかを示します。[Configure Anti-spam] をクリックして、CSC SSM で POP3 アンチスパム機能設定を行うためのウィンドウを開きます。

ステップ 4　[Content Filtering] 領域は表示専用であり、CSC SSM で POP3 電子メール コンテンツ フィルタリングがイネーブルになっているかどうかを示します。[Configure Content Filtering] をクリックして、CSC SSM で POP3 電子メール コンテンツ フィルタリング設定を行うためのウィンドウを開きます。

ステップ 5　[Global Approved List] 領域は表示専用であり、CSC SSM で POP3 のグローバルな承認済みリスト機能がイネーブルになっているかどうかを示します。[Configure Global Approved List] をクリックして、CSC SSM で POP3 のグローバルな承認済みリスト設定値を設定するための画面を開きます。

次の作業

「File Transfer」（P.31-23）を参照してください。

File Transfer

[File Transfer] ペインでは、FTP 関連の機能がイネーブルになっているかどうかを確認し、CSC SSM にアクセスして FTP 関連機能を設定できます。

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

FTP 関連機能のステータスを表示する、またはを設定するには、次の手順を実行します。

ステップ 1　[File Transfer] タブをクリックします。

[File Scanning] 領域は表示専用であり、CSC SSM で FTP ファイル スキャンがイネーブルになっているかどうかを示します。

ステップ 2　[Configure File Scanning] をクリックして、CSC SSM で FTP ファイル スキャン設定を行うためのウィンドウを開きます。

[File Blocking] 領域は表示専用であり、CSC SSM で FTP ブロッキングがイネーブルになっているかどうかを示します。

ステップ 3　[Configure File Blocking] をクリックして、CSC SSM で FTP ファイル ブロッキング設定を行うためのウィンドウを開きます。

次の作業

「Updates」（P.31-23）を参照してください。

Updates

[Updates] ペインでは、アップデートのスケジュール設定がイネーブルになっているかどうかを確認し、CSC SSM にアクセスしてアップデートのスケジュールを設定できます。

（注）　CSC SSM にアクセスするには、CSC SSM パスワードを再入力する必要があります。非アクティブ状態が 10 分間続くと、CSC SSM ブラウザのセッションがタイムアウトになります。CSC SSM ブラウザを閉じて ASDM の他のリンクをクリックした場合は、1 つのセッションがすでに開いているため、CSC SSM パスワードの再入力は求められません。

アップデートのスケジュール設定のステータスを表示またはアップデートのスケジュールを設定するには、次の手順を実行します。

ステップ 1　[Updates] タブをクリックします。

[Scheduled Updates] 領域は表示専用であり、CSC SSM でアップデートのスケジュール設定がイネーブルになっているかどうかを示します。

[Scheduled Update Frequency] 領域には、アップデートを実行するスケジュールに関する情報（「Hourly at 10 minutes past the hour」など）が表示されます。

[Component] 領域には、アップデート可能な CSC SSM ソフトウェアのコンポーネントの名前が表示されます。

[Components] 領域の [Scheduled Updates] 領域は表示専用であり、対応するコンポーネントでアップデートのスケジュール設定がイネーブルになっているかどうかを示します。

ステップ 2　[Configure Updates] をクリックして、CSC SSM でアップデートのスケジュール設定を行うためのウィンドウを開きます。

（注） ASA を再起動しても、SSM は自動的に再起動しません。詳細については、CLI コンフィギュレーション ガイドの SSM および SSC の管理に関する項を参照してください。

次の作業

「CSC SSM のモニタリング」（P.31-24）を参照してください。

CSC SSM のモニタリング

ASDM では、CSC SSM の統計情報や CSC SSM 関連の機能を監視できます。

（注） [Configuration] > [Trend Micro Content Security] > [CSC Setup] で [CSC Setup Wizard] を完了していないと、[Monitoring] > [Trend Micro Content Security] のペインにアクセスできません。その代わりに、ダイアログボックスが表示され、[Monitoring] > [Trend Micro Content Security] から [CSC Setup Wizard] に直接アクセスできます。

この項では、次のトピックについて取り上げます。

Threats

CSC SSM によって検知されたさまざまなタイプの脅威に関する情報をグラフで表示するには、次の手順を実行します。

ステップ 1　[Monitoring] > [Trend Micro Content Security] > [Threats] を選択します。

[Available Graphs] 領域に、統計情報をグラフで表示できるコンポーネントが一覧表示されます。1 つのフレームに最大で 4 つのグラフを表示できます。グラフには、次に示すリアルタイム データが 12 秒間隔で表示されます。

- 検出されたウイルス
- フィルタリングされた URL、ブロックされた URL
- 検出されたスパム
- ブロックされたファイル
- ブロックされたスパイウェア
- ダメージ クリーンナップ サービス

ステップ 2　[Graph Window Title] には、モニタリング可能な統計情報のタイプが一覧表示されます。1 つのグラフ ウィンドウに表示する統計情報のタイプは 4 つまで選択できます。複数のグラフ ウィンドウを同時に開くことができます。グラフ ウィンドウにすでに含まれている統計情報が [Selected Graphs] リストに表示されます。

ステップ 3　[Available Graphs For] リストで選択した統計情報タイプを [Selected Graphs] リストに移動するには、[Add] をクリックします。

ステップ 4　選択した統計情報タイプを [Selected Graphs] リストから削除するには、[Remove] をクリックします。削除しようとしている項目が他のペインから追加されたものであり、[Available Graphs] ペインに戻されない場合、このボタン名は [Delete] に変わります。

ステップ 5　新しいウィンドウを表示してその [Graph] タブに選択した統計情報の最新のグラフを表示するには、[Show Graphs] をクリックします。同じ情報を表形式で表示するには、[Table] タブをクリックします。

ステップ 6　グラフまたは表形式の情報をローカル PC にファイルとして保存するには、[Graph] タブまたは [Table] タブで、メニューバーの [Export] をクリックするか、[File] > [Export] を選択します。

ステップ 7　ウィンドウに表示されている情報を印刷するには、[Graph] タブまたは [Table] タブで、メニューバーの [Print] をクリックするか、[File] > [Print] を選択します。

次の作業

「Live Security Events」（P.31-25）を参照してください。

Live Security Events

ライブかつリアルタイムのセキュリティ イベントを別のウィンドウに表示するには、次の手順を実行します。

ステップ 1　[Monitoring] > [Trend Micro Content Security] > [Live Security Events] を選択します。

[Buffer Limit] フィールドに、表示できるログ メッセージの最大数が表示されます。デフォルト値は 1000 です。

ステップ 2　[View] をクリックして、[Live Security Events Log] ダイアログボックスを表示します。着信メッセージを一時停止して、メッセージ ウィンドウをクリアし、イベント メッセージを保存できます。また、メッセージ内の特定のテキストを検索することもできます。

次の作業

「Live Security Events Log」（P.31-26）を参照してください。

Live Security Events Log

CSC SSM から受信した Live Security Events メッセージを表示するには、次の手順を実行します。

ステップ 1　セキュリティ イベント メッセージをフィルタリングするには、[Filter By] ドロップダウン リストで次のいずれかを選択します。

- [Filter by Text] を選択し、テキストを入力してから [Filter] をクリックします。
- [Show All] を選択すると、すべてのメッセージが表示されます。つまり、フィルタが解除されます。

ステップ 2　[Latest CSC Security Events] ペイン（すべてのカラムが*表示専用*）を使用するには、次のオプションのいずれかを選択します。

- イベントの発生時刻
- 脅威が検出された IP アドレスまたはホスト名
- 脅威のタイプ、イベント処理を決定するセキュリティ ポリシー、または URL フィルタリング イベントの場合にイベントをトリガーしたフィルタ。
- 脅威が含まれる電子メールの件名、脅威が含まれる FTP ファイルの名前、あるいはブロックまたはフィルタリングされた URL。
- 脅威が含まれる電子メールの受信者、脅威にさらされたノードの IP アドレスまたはホスト名、または脅威にさらされたクライアントの IP アドレス。
- 脅威が含まれるイベントのタイプ（Web、メール、FTP など）、HTTP または FTP イベントのユーザまたはグループの名前。
- 添付ファイルのクリーニングや削除など、メッセージの内容に対して実行するアクション
- メッセージを変更せずに配信、添付ファイルを削除してから配信、添付ファイルをクリーニングしてから配信など、メッセージに対して実行するアクション

ステップ 3　入力したテキストに基づいてセキュリティ イベント メッセージを検索するには、次のいずれかを選択します。

- [Text] フィールドに、セキュリティ イベント メッセージ ログ内で検索するテキストを入力してから、[Find Messages] をクリックします。
- このフィールドに入力したテキストに一致する次のエントリを見つけるには、[Find] をクリックします。

ステップ 4　[Latest CSC Security Events] ペインのスクロールを一時停止するには、[Pause] をクリックします。[Latest CSC Security Events] ペインのスクロールを再開するには、[Resume] をクリックします。

ステップ 5　ログを PC のファイルに保存するには、[Save] をクリックします。

ステップ 6　表示されているメッセージのリストを消去するには、[Clear Display] をクリックします。

ステップ 7　ペインを閉じて前の画面に戻るには、[Close] をクリックします。

次の作業

「Software Updates」（P.31-27）を参照してください。

Software Updates

CSC SSM ソフトウェア アップデートに関する情報を表示するには、[Monitoring] > [Trend Micro Content Security] > [Software Updates] の順に選択します。

[Software Updates] ペインに、次の情報が表示されます。このペインは約 12 秒間隔で自動的にリフレッシュされます。

- アップデート可能な CSC SSM ソフトウェアのコンポーネントの名前
- 対応するコンポーネントの現在のバージョン
- 対応するコンポーネントが最後にアップデートされた日付と時刻 CSC SSM ソフトウェアをインストールした後にコンポーネントをアップデートしたことがない場合は、このカラムに「None」と表示されます。
- CSC SSM ソフトウェアのアップデートに関する情報が ASDM によって最後に受信された日付と時刻

次の作業

「CSC CPU」（P.31-27）を参照してください。

Resource Graphs

ASA では、CSC SSM のステータス（CPU リソースとメモリの使用状況など）をモニタできます。この項では、次のトピックについて取り上げます。

CSC CPU

CSC SSM での CPU の使用状況に関する情報をグラフで表示するには、次の手順を実行します。

ステップ 1　[Monitoring] > [Trend Micro Content Security] > [Resource Graphs] > [CSC CPU] を選択します。

CSC CPU ペインに、CSC SSM での CPU の使用状況に関する統計情報など、グラフで統計情報を表示可能なコンポーネントが表示されます。

ステップ 2　以降の手順については、「Threats」（P.31-25）の手順 2 に進みます。

次の作業

「CSC Memory」（P.31-28）を参照してください。

CSC Memory

CSC SSM でのメモリの使用状況に関する情報をグラフで表示するには、次の手順を実行します。

ステップ 1　[Monitoring] > [Trend Micro Content Security] > [Resource Graphs] > [CSC Memory] を選択します。

[Available Graphs] 領域に、統計情報をグラフで表示できるコンポーネントが一覧表示されます。主なものは次のとおりです。

- 使用していないメモリの量
- 使用中のメモリの量

ステップ 2　以降の手順については、「Threats」（P.31-25）の手順 2 に進みます。

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。

（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。

新しいパスワードで ASDM に接続できない場合は、ASDM を再起動して再度ログインしてみます。新しいパスワードを定義したが、新しいパスワードと異なる既存のパスワードが ASDM にある場合は、[File] > [Clear ASDM Password Cache] を選択して、パスワード キャッシュを消去し、ASDM を再起動して再度ログインしてみます。

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

ステップ 1　ASDM のメニューバーの [Tools] > [CSC Password Reset] を選択します。

[Password Reset] 確認ダイアログ ボックスが開きます。

ステップ 2　デフォルトのパスワードをリセットするには、[OK] をクリックします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。

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。

その他の関連資料

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』*
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 31-2 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。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 31-2　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 セットアップ ウィザードでは、ASDM で CSC SSM を設定することができます。 次の画面が導入されました。[Configuration] > [Trend Micro Content Security] > [CSC Setup]。
CSC SSM	8.1(1) および 8.1(2)	この機能は、ASA 5580 ではサポートされていません。

表 31-2　CSC SSM の機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
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。送信元と宛先の IP 情報が ASDM ログのビューア GUI に追加されました。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。
CSC イベントのクリア	8.4(1)	[Latest CSC Security Events] ペインの CSC イベントをクリアする操作のサポートが追加されました。次の画面が変更されました。[Home] > [Content Security]。
CSC SSM	8.4(2)	次の機能のサポートが追加されました。 • HTTPS トラフィック リダイレクション : 受信 HTTPS 接続の URL フィルタリングと WRS クエリー。 • 受信および送信 SMTP、POP3 電子メールのグローバル認定のホワイト リスト。 • 製品ライセンス更新の電子メール通知。 次の画面が変更されました。 [Configuration] > [Trend Micro Content Security] > [Mail] > [SMTP]。 [Configuration] > [Trend Micro Content Security] > [Mail] > [POP3]。 [Configuration] > [Trend Micro Content Security] >[Host/Notification Settings]。 [Configuration] > [Trend Micro Content Security] > [CSC Setup] > [Host Configuration]。