メール トラフィック（SMTP および POP3）の設定

インストール後に ASA が SSM にトラフィックを送信するよう設定した場合、SMTP トラフィックおよび POP3 トラフィックに、ウイルスや、ワームやトロイの木馬といったその他のマルウェアがないかどうか、スキャンが行われます。この章では、スパイウェアなどのセキュリティ リスクの検出に必要な追加設定、および着信メッセージと発信メッセージへの組織としての免責条項の追加に必要な追加設定について説明します。この章は次の項で構成されています。

デフォルトのメール スキャン設定

表 3-1 に、メール コンフィギュレーション設定、およびインストール後に動作するデフォルト値の要約を示します。

表 3-1　デフォルトのメール スキャン設定

機能	デフォルト設定
着信メールおよび発信メールのメール（SMTP）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
メール（POP3）スキャン	デフォルトのスキャン方式として All Scannable Files の使用がイネーブルになっています
メール（SMTP）およびメール（POP3）のスキャン メッセージ フィルタ（指定したサイズより大きいメッセージを拒否します）	20 MB より大きいメッセージを拒否するようにイネーブルになっています
メール（SMTP）メッセージ拒否（指定した数よりも多くの受信者があるメッセージを拒否します）	100 人以上の受信者宛のメッセージを拒否するようにイネーブルになっています
着信メールおよび発信メールに対するメール（SMTP）圧縮ファイル処理、および メール（POP3）圧縮ファイル処理	次の場合は圧縮ファイルのスキャンを省略するように設定されています • 圧縮解除されるファイル数が 200 よりも多い場合 • 圧縮解除されるファイル サイズが 20 MB を超える場合 • 圧縮レイヤ数が 3 を超える場合 • 圧縮解除/圧縮ファイルのサイズ比率が 100/1 を超える場合
メール（SMTP）の着信と発信、およびマルウェアが検出されたメッセージのメール（POP3）アクション	マルウェアが検出されたメッセージまたは添付ファイル（あるいはその両方）を修復します メッセージまたは添付ファイル（あるいはその両方）を修復できない場合は、削除します
メール（SMTP）の着信と発信、およびスパイウェア / グレーウェアが検出されたメッセージのメール（POP3）アクション	ファイルの配信を許可します
メール（SMTP）の着信と発信、およびマルウェアが検出された場合のメール（POP3）通知	マルウェアが検出されたメッセージには、%VIRUSNAME% was detected in the file (%FILENAME%). The following action has been taken: %ACTION% というインライン通知が挿入されます。
パスワードで保護された電子メール メッセージ（SMTP および POP3）	スキャンを行わずにファイルの配信を許可します
指定したスキャンの基準を超えるためスキャンされない、SMTP および POP3 経由で送信された圧縮ファイル	ファイルの配信を許可します

これらのデフォルト設定では、Trend Micro InterScan for Cisco CSC SSM をインストールした後に、電子メール トラフィックにある程度の保護が適用されます。これらの設定は変更できます。変更する前に、これらの選択の詳細についてオンライン ヘルプで慎重に検討してください。

インストール後にアップデートすることで、電子メール トラフィックを最大限に保護する追加のコンフィギュレーション設定があります。これらの追加設定については、この章の残りのページで説明します。

アンチスパムおよびコンテンツ フィルタリング機能を使用できる Plus ライセンスを購入した場合は、これらの機能を設定する必要があります。デフォルトでは動作しません。

着信 / 発信 SMTP メールの定義

1 つの電子メール メッセージが複数の受信者宛で、受信者の 1 人または複数人へは着信メッセージ（同じドメイン名を持つ同じ組織内のだれか宛）で、受信者の 1 人へは発信メッセージ（異なるドメイン名を持つ異なる組織のだれか宛）である場合、着信規則が適用されます。たとえば、psmith@example.com からのメッセージが jdoe@example.com および gwood@example.net 宛になっています。

着信 SMTP メッセージが「scan all」オプションでスキャンされるのに対し、発信 SMTP メッセージは IntelliScan でスキャンされるとします。また、スパイウェア / グレーウェア検出が着信メッセージに対してのみイネーブルになっているとします。

たとえ gwood が「発信」受信者であっても、psmith から jdoe および gwood へのメッセージは両方の受信者宛の着信メッセージとして扱われます。

SMTP および POP3 スパイウェア / グレーウェア検出のイネーブル化

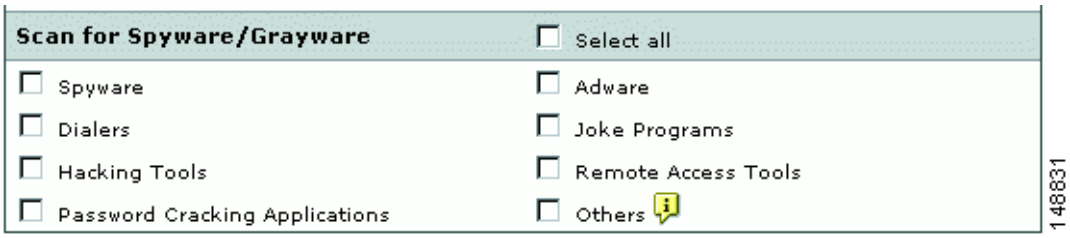
グレーウェアは、正当か、好ましくないか、または悪意があるかが不明確なソフトウェアのカテゴリです。ウイルス、ワーム、トロイの木馬などの脅威とは異なり、グレーウェアは、データが感染したり、データの複製または破壊を行ったりすることはありませんが、プライバシーが侵害される可能性があります。グレーウェアの例としては、スパイウェア、アドウェア、リモート アクセス ツールがあります。

スパイウェア / グレーウェア検出は、デフォルトではイネーブルになっていません。電子メール トラフィックでスパイウェアおよびその他の形態のグレーウェアの検出を開始するには、次のウィンドウでこの機能を設定します。

- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Incoming Scan リンクをクリックすると、**SMTP Incoming Message Scan/Target** ウィンドウが表示されます
- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Outgoing Scan リンクをクリックすると、**SMTP Outgoing Message Scan/Target** ウィンドウが表示されます
- CSC SSM コンソールで **Mail (POP3) > Scanning > POP3 Scanning/Target** をクリックすると、**POP3 Scanning/Target** ウィンドウが表示されます

これらのウィンドウの **Scan for Spyware/Grayware** セクションで（図 3-1 を参照）、Trend Micro InterScan for Cisco CSC SSM で検出するグレーウェアのタイプを選択します（チェックボックスをオンにします）。

図 3-1　スパイウェア / グレーウェアのスキャンの設定



これらのタイプのグレーウェアの説明については、上記のウィンドウの固有のオンライン ヘルプを参照してください。検出するグレーウェアのタイプを指定した後、必ず **Save** をクリックして新しい設定をイネーブルにしてください。

SMTP 通知および POP3 通知の検討

デフォルトの通知設定で十分な場合、それ以上の設定は必要ありません。しかし、通知オプションを検討して、デフォルトを変更するかどうかを決定することができます。次の例を参考にしてください。

- 電子メール メッセージにセキュリティ リスクが検出された場合、管理者に通知を送信することができます（SMTP では、送信者と受信者の両方、またはいずれか一方に通知することもできます）
- 所属組織により適するように、通知メッセージのデフォルトのテキストを変更することができます

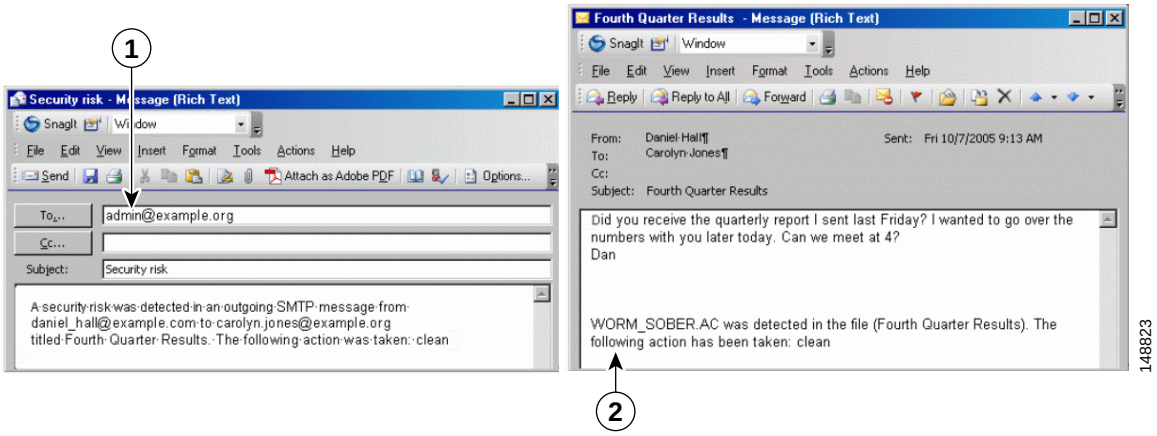
電子メール メッセージを検討し、場合によって書き換えるには、CSC SSM コンソールで次のウィンドウに進みます。

- **Mail (SMTP) > Scanning > Incoming > SMTP Incoming Message Scan/Notification**
- **Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification**
- **Mail (POP3) > Scanning > POP3 Scanning/Notification**

通知のタイプ

図 3-2 に示すように、電子メール トラフィックでは、電子メール通知とインライン通知の 2 つのタイプの通知を使用することができます。

図 3-2　通知の例



1	電子メール通知	2	インライン通知

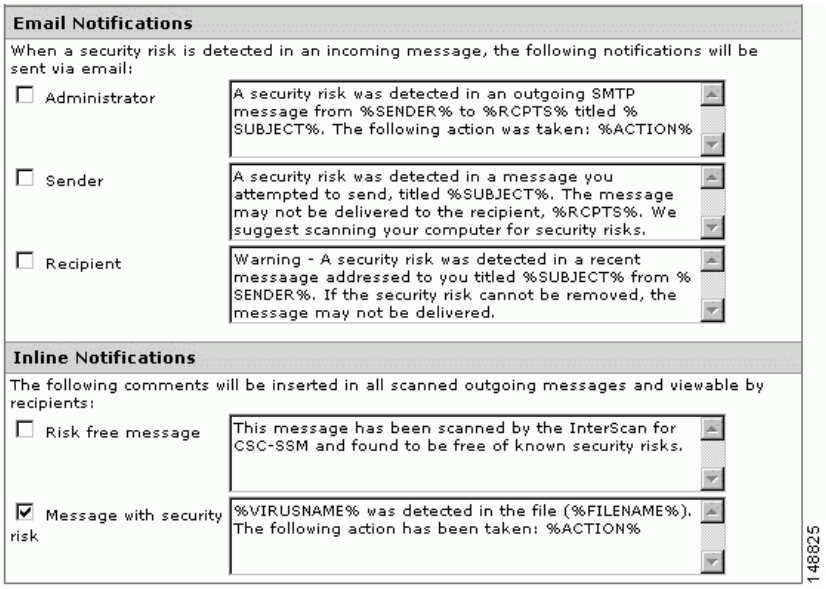
トークンと呼ばれる変数を使用して、通知をさらに有益なものとする情報を提供します。たとえば、%VIRUSNAME% と呼ばれるトークンは、右側のインライン通知の例のテキストでは WORM_SOBER.AC に置き換えられています。

トークンの詳細については、オンライン ヘルプのトピック「Using Tokens in Notifications」を参照してください。

通知の変更

追加の受信者に通知を送信する場合、またはトリガー イベントの発生時に送信される通知メッセージのデフォルトのテキストを変更する場合は、アップデートするメッセージ スキャン通知ウィンドウに進みます。例として、図 3-3 に、**Mail (SMTP) > Scanning > Outgoing > SMTP Outgoing Message Scan/Notification** ウィンドウの通知フィールドを示します。

図 3-3　発信 SMTP の通知の設定



デフォルトでは、通知は、メッセージ受信者に送られるインライン通知のみです。これは、送信者も発信元組織の管理者もセキュリティ上の脅威が検出され、無害化されたことを認識していないことを意味します。変更するには、次の手順を実行します。

- ウィンドウの **Email Notifications** セクションで、電子メールによる通知を受けとる追加の受信者をクリックします。
- ウィンドウの **Inline Notifications** セクションで、「risk-free」インライン通知のみ、デフォルトの「risk detected and action taken」メッセージのみ、どちらも指定しない、または両方とも指定する、のいずれかを選択します。
- いずれかの通知のテキストを変更するには、既存のテキストを強調表示し、独自のメッセージをテキストボックスに入力します。入力が終了したら必ず **Save** をクリックしてください。

SMTP メッセージ フィルタ、免責条項、および着信メール ドメインの設定

（注）　これらの設定は、SMTP プロトコルだけに適用されます。

Mail (SMTP) > Configuration > SMTP Configuration から可能なコンフィギュレーション設定を検討します。**SMTP Configuration** ウィンドウには次の 4 つのタブがあります。

- Message Filter
- Disclaimer
- Incoming Mail Domain
- Advanced Settings

これらを設定するには、次の手順を実行します。

ステップ 1　**SMTP Configuration** ウィンドウの **Message Filter** タブで、Trend Micro InterScan for Cisco CSC SSM は、20 MB より大きいメッセージ、および 100 人を超える受信者宛のメッセージを拒否するように、すでに設定されています。これらの設定は、電子メール サーバが数百人の受信者宛の膨大な偽のメッセージを処理しようとして CPU 時間を消費するネットワーク上の攻撃からの保護に役立ちます。デフォルト設定を推奨します。デフォルト設定を使用し続ける場合、このウィンドウでの処置は不要です。

ステップ 2　SMTP Configuration ウィンドウの **Message Filter** タブで、SMTP メッセージの最初または最後に表示される組織としての免責条項を追加できます。**Add this disclaimer...** チェックボックスをオンにすると、この機能がイネーブルになります。または、この機能を使用しない場合は、現状のままでこのページを終了します。免責条項のテキストをカスタマイズするには、デフォルトのメッセージを強調表示しておいて、上書きします。

ステップ 3　SMTP Configuration ウィンドウの **Incoming Mail** タブでは、次の目的で追加の着信メール ドメインを定義することができます。

- ウイルスおよびその他の脅威のスキャン
- アンチスパム
- コンテンツ フィルタリング

Incoming mail domains フィールドには、インストール時に（Host Configuration インストール ウィンドウで）入力した着信電子メール ドメイン名がすでに表示されています。ドメインを追加する場合は、トップ レベル ドメイン（tld）名のみを入力します。たとえば、example1.com や example2.com などの下位ドメインは入力せずに、example.com のみを入力します。他の着信ドメインがない場合は、このウィンドウでの処置は不要です。

ステップ 4　SMTP Configuration ウィンドウの **Advanced Settings** タブには次の設定ができるフィールドがあります。

- 攻撃者からのものと思われるメッセージに対してより積極的な（または緩やかな）タイムアウトを設定する
- メッセージが攻撃という形の動作をした場合、SMTP トラフィックの移動をより困難にする設定をイネーブルにする

詳細については、オンライン ヘルプを参照してください。

ステップ 5　変更を加えた場合は、**Save** をクリックして、アップデートした SMTP 設定をアクティブにします。

SMTP および POP3 スパム フィルタリングのイネーブル化

（注） この機能には Plus ライセンスが必要です。

SMTP および POP3 アンチスパム機能はデフォルトではディセーブルになっており、設定する必要があります。

ヒント Base ライセンスと Plus ライセンスを同時に購入した場合も、後で Plus ライセンスを追加した場合も、アンチスパムはデフォルトでディセーブルになっています。使用を開始するには、アンチスパム機能をイネーブルにして設定する必要があります。

アンチスパム機能を設定するには、次の手順を実行します。

- **ASDM の Configuration > Trend Micro Content Security > Mail** で Configure Anti-spam リンクをクリックすると、**SMTP Incoming Anti-spam** ウィンドウが表示されます
- CSC SSM コンソールで **Mail (POP3) > Anti-spam > POP3 Anti-spam** をクリックすると、**POP3 Anti-spam** ウィンドウが表示されます

アンチスパムをイネーブルにするには、次の手順を実行します。

ステップ 1　上記のウィンドウの **Target** ビューで **Enable** をクリックします。

ステップ 2　デフォルト値の **Low** を使用しない場合は、アンチスパムしきい値を **Medium** または **High** に再設定します。

ヒント 組織でスパムをブロックする経験を積んでから、後でこの設定を調整することもできます。しきい値が低すぎる場合は、スパムの発生率が高くなります。しきい値が高すぎる場合は、誤検出（スパムと識別された正当なメッセージ）の発生率が高くなります。

ステップ 3　**SMTP Incoming Anti-spam** ウィンドウおよび **POP3 Anti-spam/Target** ウィンドウの **Approved Senders** セクションで、承認された送信者を追加します。承認された送信者からのメールは、スパムと判断されることなく常に受信されます。

（注） 承認された送信者は、一方のウィンドウで追加および保存されると、もう一方のウィンドウにも表示されます。たとえば、**POP3 Anti-spam** ウィンドウの **Approved Senders** リストに robert_li@example.com を追加したとします。ここで、**SMTP Incoming Anti-spam** ウィンドウを開きます。robert_li@example.com のアドレスは、**SMTP Incoming Anti-spam** ウィンドウの **Approved Senders** のリストにもすでに追加されています。

Blocked Senders リストも同様に、一方のウィンドウで作成されたブロックされる送信者は、両方のウィンドウに表示されます。

ステップ 4　**SMTP Incoming Anti-spam** ウィンドウおよび **POP3 Anti-spam/Target** ウィンドウの **Blocked Senders** セクションで、ブロックされる送信者を追加します。ブロックされる送信者からのメールは常に拒否されます。ブロックされる送信者は、一方のウィンドウで追加および保存されると、もう一方のウィンドウにも表示されます。

ステップ 5　**SMTP Incoming Anti-spam** ウィンドウおよび **POP3 Anti-spam/Action** ウィンドウで、スパムと識別されたメッセージに対する処置を設定します。選択できる処置は、次のとおりです。

- メッセージに「Spam:」などのスパム識別子のマークを付けて送信します（スパム識別子は、たとえば、「Spam:Designer luggage at a fraction of the cost!」などメッセージ件名のプレフィックスの役割を果たします）
- メッセージを削除する

ステップ 6　**Save** をクリックして、設定ごとにアンチスパムをアクティブにします。

SMTP および POP3 コンテンツ フィルタリングのイネーブル化

（注）　この機能には Plus ライセンスが必要です。

SMTP および POP3 コンテンツ フィルタリング機能はデフォルトではディセーブルになっており、設定する必要があります。コンテンツ フィルタリング機能を設定するには、次のウィンドウに進みます。

- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Incoming Filtering リンクをクリックすると、SMTP Incoming Content Filtering/Target ウィンドウが表示されます
- ASDM の **Configuration > Trend Micro Content Security > Mail** で Configure Outgoing Filtering リンクをクリックすると、SMTP Outgoing Content Filtering/Target ウィンドウが表示されます
- CSC SSM コンソールで **Mail (POP3) > Content Filtering > POP3 Content Filtering/Target** をクリックすると、POP3 Content Filtering/Target ウィンドウが表示されます。

コンテンツ フィルタリングをイネーブルにするには、次の手順を実行します。

ステップ 1　上記のウィンドウの **Target** ビューで **Enable** をクリックします。

ステップ 2　メッセージ サイズ フィルタリング基準を使用するかどうかを決定し、使用する場合は、**Message size is** フィールドにパラメータを設定します。たとえば、5 MB を超えるメッセージおよび添付ファイルのメッセージ フィルタリングを指定した場合、5 MB より小さい添付ファイルがあるメッセージはフィルタリングされません。メッセージのサイズを指定しない場合、サイズにかかわらずすべてのメッセージがフィルタリングされます。

ステップ 3　ウィンドウの **Message Subject and Body** セクションで、メッセージの件名または本文（あるいは両方）に存在した場合に、コンテンツ フィルタリング アクションをトリガーする言葉を指定します。

ステップ 4　ウィンドウの **Message Attachment** セクションで、添付ファイル名の中に存在した場合に、コンテンツ フィルタリング アクションをトリガーする文字または言葉を指定します。ウィンドウのこのセクションで、ファイル タイプによってコンテンツ フィルタリングを選択することもできます。たとえば、フィルタリングに Microsoft Office のファイル タイプを選択した場合、Microsoft Office ツールを使用して作成された添付ファイルは、コンテンツのためにフィルタリングされます。

ステップ 5　上記のウィンドウの **Action** タブをクリックして、コンテンツ フィルタリングがトリガーされたときのアクションを指定します。電子メール メッセージでは、選択できるアクションは次のとおりです。

- コンテンツ フィルタリング ポリシーのいずれかに違反するメッセージを削除する
- メッセージを送信する

添付ファイルでは、選択できるアクションは次のとおりです。

- 違反する添付ファイルの通過を許可する（この場合、ウィンドウの **For messages that match the attachment criteria** セクションで変更を加えないでください）
- 添付ファイルを削除し、メッセージ本文にインライン通知を挿入する

ステップ 6　上記のウィンドウの **Notification** タブをクリックして、コンテンツ フィルタリング違反の通知を管理者に送信するかどうかを指定します（SMTP では、送信者または受信者（あるいは両方）に通知することもできます）。デフォルトのメッセージを強調表示して上書きすることで、通知メッセージボックスのデフォルトのテキストを変更します。

ステップ 7　**Save** をクリックして、設定ごとにコンテンツ フィルタリングをアクティブにします。