Cisco Service Control ソリューション ガイド

Cisco Service Control サービス セキュリティ：発信スパムの低減ソリューション ガイド リリース 3.6.x

Cisco Service Control Service Security: Outgoing Spam Mitigation Solution Guide, Release 3.6.x

OL-21077-01-J

1 概要および範囲

インターネットを介したさまざまな攻撃や悪意のあるトラフィックに対する保護の必要性が注目されています。Denial of Service（DoS; サービス妨害）攻撃と Distributed DoS（DDoS; 分散 DoS）攻撃、ワーム、ウイルス、悪意のある HTTP コンテンツ、および多種多様な侵入が頻繁に発生しています。

Deep Packet Inspection（DPI; ディープ パケット インスペクション）プラットフォーム（特に、Cisco Service Control Engine（SCE））は、インライン展開が可能な、ステートフルでプログラマブルなプラットフォームです。このような特徴から SCE プラットフォームは、サービス プロバイダーや彼らの顧客に対する悪意のあるトラフィックの影響を特定して軽減するために使用されます。

Service Control Application for Broadband（SCA BB）には、異常検出、スパムと大量メール送信の検出、およびシグニチャ検出からなるサービス セキュリティ機能が組み込まれています。これらの検出機能により、SCE プラットフォームでは、現行ネットワークに潜む脅威に対処することができます。

SCA BB ソリューションは、オペレータ ネットワーク内での悪質なアクティビティを見抜き、ネットワーク全体のパフォーマンスやユーザ エクスペリエンスを低下させる可能性がある悪質なアクティビティを広範囲にわたって抑えることができます。

このマニュアルでは、発信スパムと大量メール送信に伴う脅威を検出し、低減するための具体的な方法について説明します。サービス セキュリティ機能および関連の管理モジュールの詳細については、SCA BB のユーザ ガイドを参照してください。

2 機能の概要

Cisco SCE プラットフォームは、大量メール送信アクティビティ検出アプローチを使用して、発信スパムを検出し、低減します。

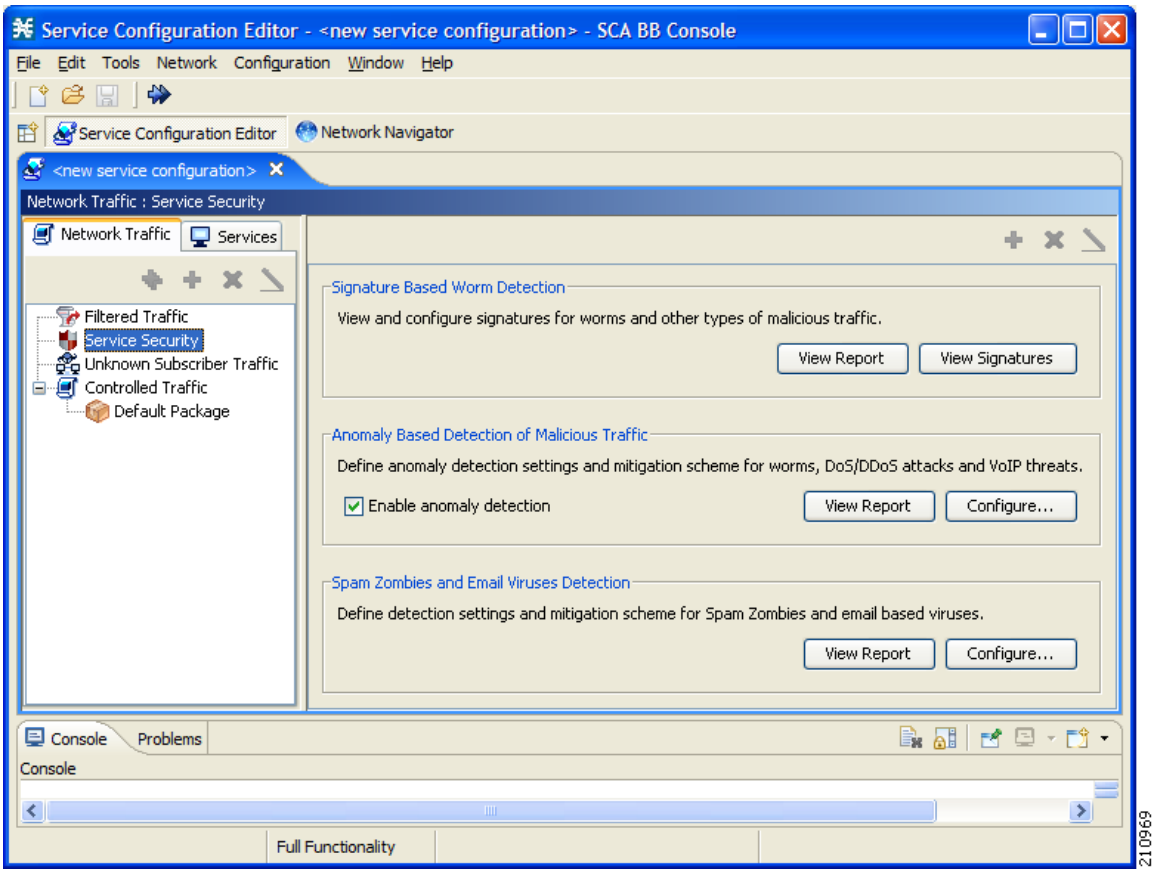
*Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）*は、E メールの送信に使用されるプロトコルです。個々のサブスクライバから発信された SMTP セッションのレートが異常に高いということは、多くの場合、E メールの送信に関連する悪質なアクティビティ（E メールベースのウイルスまたはスパムゾンビ アクティビティ）が存在していることを示しています。このメカニズムは、個々のサブスクライバの SMTP セッション レートのモニタリングをベースとしています。また、このメカニズムは、SCE プラットフォームのサブスクライバ アウェアネス機能を使用し、サブスクライバアウェア モードまたはアノニマス サブスクライバ モードで動作できます。

この検出アプローチでは、オペレータが、ビジネス ニーズに基づいて、実装すべきアクションの実現可能な方向性を選択できます。

- モニタ：この方法で検出された悪質なアクティビティが存在するかどうかについて、ネットワークを調べます。この作業は、検出された悪質なアクティビティに関して収集された情報に基づくレポートを使用して実施できます。
- ブロック：SCE プラットフォームによって検出された悪質なアクティビティを自動的にブロックし、ネットワークに対する脅威の伝播や悪影響を阻止します。
- 通知：Web セッションをキャプティブ ポータルにリダイレクトすることによって、悪質なアクティビティへの関与が検出されたことをサブスクライバに通知します。

オペレータは、検出方法や特定のニーズに基づいて実施するアクションを柔軟にカスタマイズすることができます。SCA BB セキュリティ ダッシュボードの GUI アプリケーション（図 1 を参照）は、セキュリティ機能の設定およびモニタリングを行うためのフロント エンドとして機能します。

図 1　　SCA BB セキュリティ ダッシュボード



大量メール送信の検出プロセス

設定が完了したら、次に、大量メール送信の検出プロセスの概要について説明します。

大量メール送信の検出プロセスは、セッション クォータに基づいています。クォータは、一定期間のセッション数を表します。

1. 期間は、最初のセッションが送信されたときに開始します。
2. まだ最初の期間内であるにもかかわらず、次のセッションが送信された場合は、最初の期間内のセッションとしてカウントされます。最初の期間を経過した場合、その時点で 2 番めの期間が開始します。
3. サブスクライバが送信したセッション数が期間内に割り当てられているセッション数よりも多い場合、そのサブスクライバは、クォータを超過したことにより、スパム送信者としてマークされます。スパム送信者としてマークされた場合、それ以降は、そのサブスクライバから送信されるすべてのトラフィックがスパムとして処理され、定義済みのアクション（Raw Data Record（RDR; 未加工データ レコード）の送信、ブロック、通知、またはミラーリング）が適用されます。

（注） このアクションは、サブスクライバがスパム送信者としてマークされたときのセッション以降に対してのみ適用されます。これよりも前から継続しているセッションには適用されません。

4. このサブスクライバは、設定されているクォータを超えるセッション数を送信せずに期間が経過するまで、スパム送信者としてマークされます。
5. クォータは、10 秒間に 6 セッションなどのように定義されます。この 10 秒のカウントは、最初のセッションが送信されたときに開始されます。10 秒以内にさらに 5 つのセッションが送信されると、それ以降、そのサブスクライバはスパム送信者としてマークされ、定義済みのアクション（RDR、ブロック、通知、またはミラーリング）が適用されます。

（注） サブスクライバがスパム送信者としてマークされたときに開いていたセッションに対しては、このアクションは適用されません。

たとえば、12 秒後に次のセッションが送信された場合、期間は再度 0 から開始され、セッション数が再度カウントされます。サブスクライバが 10 秒の間に送信したセッション数が 6 よりも少ない場合、そのサブスクライバはスパム送信者とは見なされなくなり、指定されているアクションが適用されなくなります。また、サブスクライバがスパム送信者でなくなったことを示す RDR が Collection Manager に送信されます。

関連トピック

- 「発信スパム検出の設定」（P.6）

3 大量メール送信に伴う脅威

このモジュールは、個々のサブスクライバの SMTP セッション レートのモニタリングをベースとしています。また、このモジュールは、SCE プラットフォームのサブスクライバ アウェアネス機能を使用し、サブスクライバアウェア モードまたはアノニマス サブスクライバ モードで動作できます。

SMTP は、E メールの送信に使用されるプロトコルです。個々のサブスクライバから発信された SMTP セッションのレートが異常に高いということは、多くの場合、E メールの送信に関連する悪質なアクティビティ（E メールベースのウイルスまたはスパムゾンビ アクティビティ）が存在していることを示しています。

大量メール送信検出の設定

大量メール送信の検出は、定義済みの SMTP セッション クォータに違反しているサブスクライバに基づいて行われます。

この機能を正しく動作させるためには、システムをサブスクライバアウェア モードまたはアノニマス サブスクライバ モードに設定する必要があります。SCE プラットフォームは、この設定を行うことで、各サブスクライバによって生成された SMTP セッションの数を正確にカウントできるようになります。

設定は、次に示す各段階に基づいて行います。

- 検出対象のサービスの設定：大量メール送信を検出する該当のサービス（この段階ですでに作成されている必要があります）を設定します。通常、SMTP プロトコルのみを含むサービスを使用します。調整を行って、検出範囲を絞り込んだり、可能な場合は検出しきい値を小さくしたりすることができます。
  - 「発信 SMTP」：サブスクライバによって生成された SMTP セッションのみを対象とします。サブスクライバ自身の構内で SMTP サーバを運用する必要はないため、SMTP が着信プロトコルと見なされることは通常ありません。着信 SMTP 接続は、他の種類の悪質なアクティビティを示している場合があります。このようなサービスを作成するには、サービス定義に「サブスクライバ側」属性を含める必要があります。
  - 「オフネット SMTP」：サブスクライバの「ホーム SMTP サーバ」をターゲットとしていない SMTP。通常の E メール クライアントは、ホーム SMTP サーバ経由で E メールを送信します。ホーム SMTP サーバは、必要に応じて、後で E メールをリレーします。サービスをオフネットに制限することで、「正規」のセッション（サブスクライバが自身の ISP の SMTP サーバとやり取りしているセッション）を考慮する必要がなくなります。1 つ注意すべき点は、著名な非 ISP E メール プロバイダーが有料または無料で SMTP ベースのサービスを提供していることです。そのため、オフネットは、「正規」のアクティビティと「正規以外」のアクティビティを区別するのに適した要因ではなくなりました。このようなサービスを作成するには、IP ゾーンの範囲を定義し、そのゾーンと SMTP プロトコルを関連付けるサービスを定義する必要があります。
  - 上記 2 つの組み合わせ。
- 異常な E メール アクティビティを識別するために使用するクォータを定義します。クォータは、一定期間のセッション数として定義されます（セッション数と期間のいずれも設定可能）。これらのフィールドの値は、ある程度のサブスクライバ アクティビティのベースライン モニタリングに基づいて決定することを推奨します。
- 大量メール送信アクティビティを検出した場合のアクションを定義します。定義可能なアクションは次のとおりです。
  - [Send RDR]：1 つの未加工データ レコード（RDR）が SCE から Collection Manager に送信されます。スパム送信者としてのサブスクライバのステータスが削除されると、第 2 の RDR が送信されます。Collection Manager は、ロギング目的でこれらの RDR を Comma Separated Value（CSV; カンマ区切り形式）ファイルに収集します。または、独自の RDR コレクタを実装して、これらの RDR を受信し、リアルタイムで応答できます。
  - [Block]：スパム SMTP トラフィックをブロックします。
  - [Notify]：サブスクライバのブラウジング セッションをキャプティブ ポータルにリダイレクトし、オペレータからのメッセージを示します。このアクションは、*サブスクライバ通知*を使用して実行されます。
  - [Mirror]：スパム SMTP トラフィックをインライン スパム検出サービスに迂回させます。

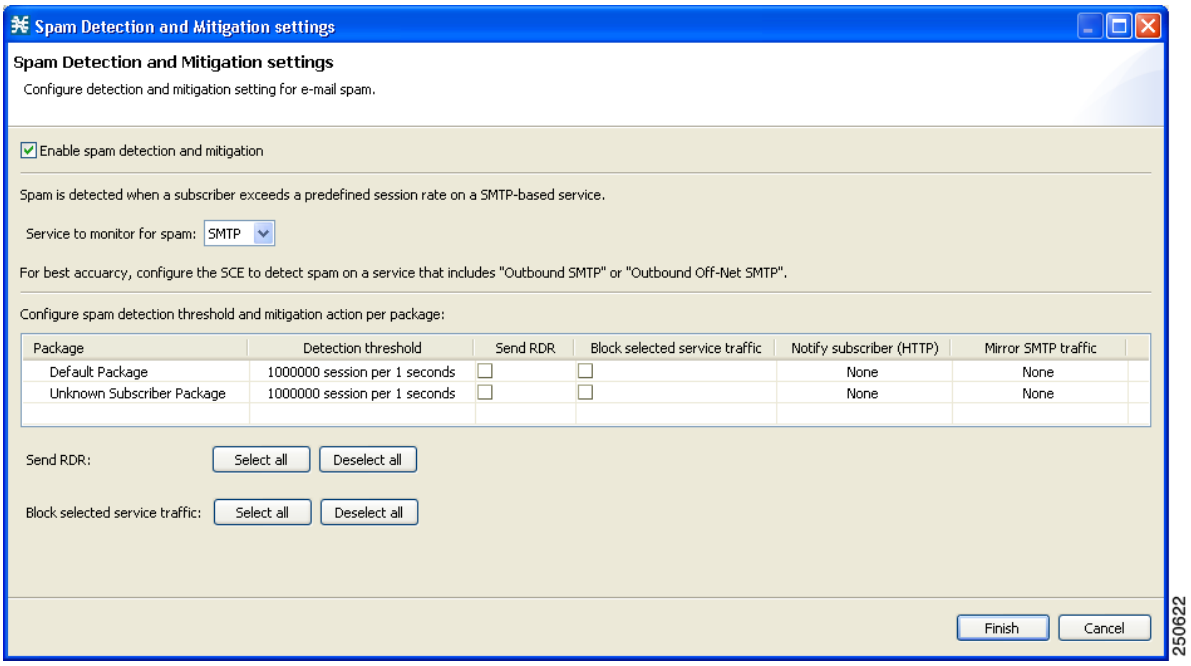
（注） [Send RDR] アクションでは、サブスクライバがスパム送信者としてマークされると 1 つの RDR が SCE から送信され、サブスクライバがスパム送信者と見なされなくなると第 2 の RDR が送信されます。しかし、ブロック、通知、およびミラーリングの各処理を使用する場合、サブスクライバがスパム送信者として示されると処理が開始され、サブスクライバがスパム送信者と見なされなくなるまで続行されます。

発信スパム検出の設定

ステップ 1 サービス セキュリティ ダッシュボードの [Spam Zombies and e-mail Viruses Detection] ペインで、[Configure] をクリックします。

[Spam Detection and Mitigation Settings] ウィンドウが表示されます （図 2 を参照）。

図 2　　[Spam Detection and Mitigation Settings] ウィンドウ



ステップ 2 [Service to monitor for spam] ドロップダウン リストからサービスを選択します。

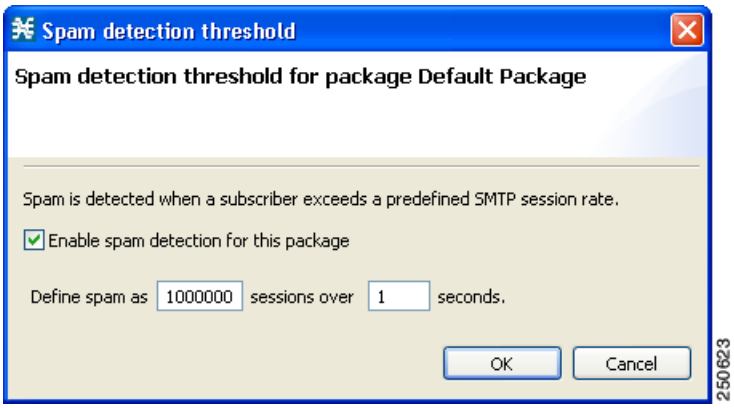
（注） 発信 SMTP やオフネット SMTP などのさらに具体的なサービスを定義している場合を除いて、モニタリング対象のサービス（SMTP）のデフォルト値を変更しないでください。

ステップ 3 各パッケージについて次の処理を実行します。

a. 異常な E メール アクティビティを識別するために使用するクォータを定義します。クォータは、一定期間のセッション数として定義されます（セッション数と期間のいずれも設定可能）。これらのフィールドの値は、ある程度のサブスクライバ アクティビティのベースライン モニタリングに基づいて決定することを推奨します。

- [Detection Threshold] カラムをクリックします。[More]（ ）ボタンが表示されます。
- [More] ボタンをクリックします。[Spam Detection Threshold] ウィンドウが表示されます （図 3 を参照）。

図 3　　[Spam Detection Threshold] ウィンドウ



- 異常動作の E メール セッション レートのしきい値を定義します。
- [OK] をクリックします。

b. 大量メール送信アクティビティを検出した場合のアクションを 1 つ以上定義します。次のアクションから選択できます。

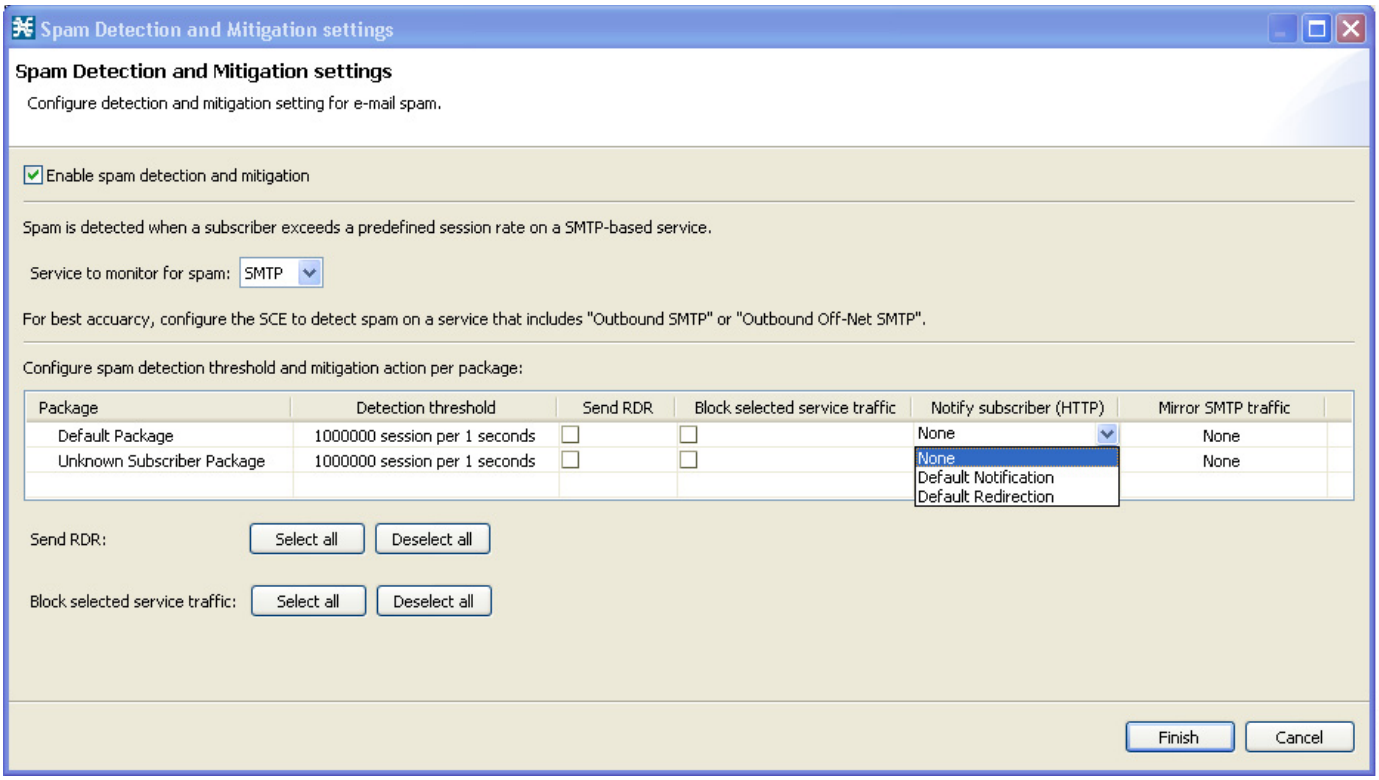
- [Send RDR]：1 つの未加工データ レコード（RDR）が SCE から Collection Manager に送信されます。スパム送信者としてのサブスクライバのステータスが削除されると、第 2 の RDR が送信されます。Collection Manager は、ロギング目的でこれらの RDR を CSV ファイルに収集します。または、独自の RDR コレクタを実装して、これらの RDR を受信し、リアルタイムで応答できます。
- [Block SMTP Traffic]：スパム SMTP トラフィックをブロックします。
- [Notify Subscriber (HTTP)]：サブスクライバのブラウジング セッションをキャプティブ ポータルにリダイレクトし、オペレータからのメッセージを示します。このアクションは、サブスクライバ通知を使用して実行されます。
- [Mirror SMTP traffic]：スパム SMTP トラフィックをインライン スパム検出サービスに迂回させます。

（注） [Send RDR] アクションでは、サブスクライバがスパム送信者としてマークされると 1 つの RDR が SCE から送信され、サブスクライバがスパム送信者と見なされなくなると第 2 の RDR が送信されます。しかし、ブロック、通知、およびミラーリングの各処理を使用する場合、サブスクライバがスパム送信者として示されると処理が開始され、サブスクライバがスパム送信者と見なされなくなるまで続行されます。

（注） [Block SMTP Traffic] と [Mirror SMTP traffic] の両方を選択できません。一方を選択すると、他方がディセーブルになります。

[Notify Subscriber (HTTP)] アクションを実行するには、通知対象のサブスクライバを選択するか入力します （図 4 を参照）。

図 4　[Spam Detection and Mitigation Settings] ウィンドウ（通知対象のサブスクライバ）



[Mirror SMTP traffic] アクションを実行するには、[Server Group] を選択します。

ステップ 4　[Finish] をクリックします。

ステップ 5　サービス コンフィギュレーションを SCE プラットフォームに適用します。

a. ツールバーの  ([Apply Service Configuration to SCE Devices]）をクリックします。

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

b. SCE を管理するためのユーザ名とパスワードを入力し、[Apply] をクリックします。

サービス コンフィギュレーションが SCE プラットフォームに適用されます。

関連トピック

- 「大量メール送信アクティビティのモニタリング」（P.9）

発信スパム検出のディセーブル化

ステップ 1　サービス セキュリティ ダッシュボードの [Spam Zombies and e-mail Viruses Detection] ペインで、[Configure] をクリックします。

[Spam Detection and Mitigation settings] ダイアログボックスが表示されます。

ステップ 2　[Enable Spam detection and mitigation] チェックボックスをオフにします。その他すべてのフィールドもディセーブルになります。

ステップ 3　[Finish] をクリックします。

発信スパム検出のディセーブル化（パッケージ単位）

ステップ 1 サービス セキュリティ ダッシュボードの [Spam Zombies and e-mail Viruses Detection] ペインで、[Configure] をクリックします。[Spam Detection and Mitigation settings] ダイアログボックスが表示されます。

ステップ 2 発信スパム検出をディセーブルにするパッケージの行で、[Detection Threshold] カラム内をクリックします。[More] ボタン（ ）が表示されます。

ステップ 3 [More] ボタンをクリックします。[Spam detection threshold] ダイアログボックスが表示されます。

ステップ 4 [Enable Spam detection for this package] チェックボックスをオフにします。すべてのフィールドがディセーブルになります。

ステップ 5 [OK] をクリックします。

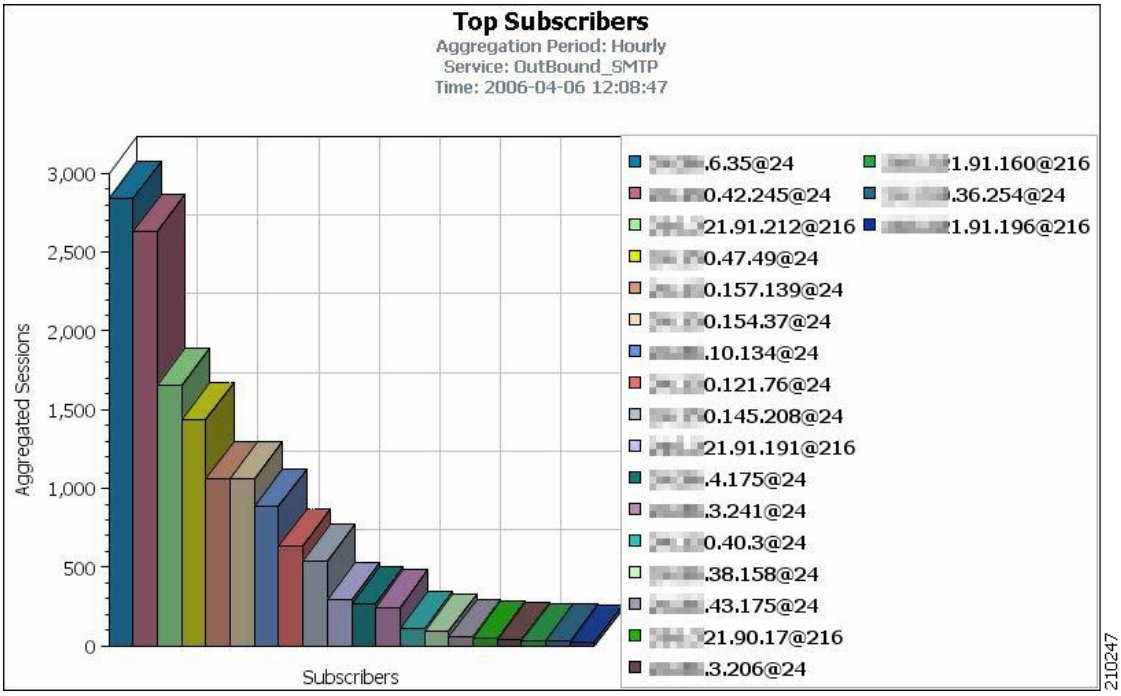
大量メール送信アクティビティのモニタリング

大量メール送信アクティビティは、Collection Manager データベース内で処理され、格納された情報に基づいてモニタすることができます。

サブスクライバが大量メール送信アクティビティを検出するのに最適なレポートは、*Top Subscribers* レポートです（図 5 を参照）。このレポートは、メトリック =Aggregated Sessions で Top Subscribers レポートを実行することにより生成されます。

Top Subscribers レポートは、大量メール送信の検出用に使用されているサービス（SMTP、またはよりきめ細かいサービス（定義されている場合））に対して生成されます。このレポートを利用すると、大量メール送信アクティビティの被害に遭っている可能性が最も高いサブスクライバの ID を特定できます。

図 5　　Top Subscribers レポート



次に、通常使用されるレポートの例を 2 つ示します。

- Global Daily Usage Sessions per Service レポート：システムで定義されている各種のサービス使用カウンタ間の、日ごとにグループ化されたセッションの分布が表示されます （図 6 を参照）。
- Global Hourly Usage Sessions per Service レポート：システムで定義されている各種のサービス使用カウンタ間の、時間ごとにグループ化されたセッションの分布が表示されます （図 7 を参照）。

図 6　　Global Daily Usage Sessions per Service レポート

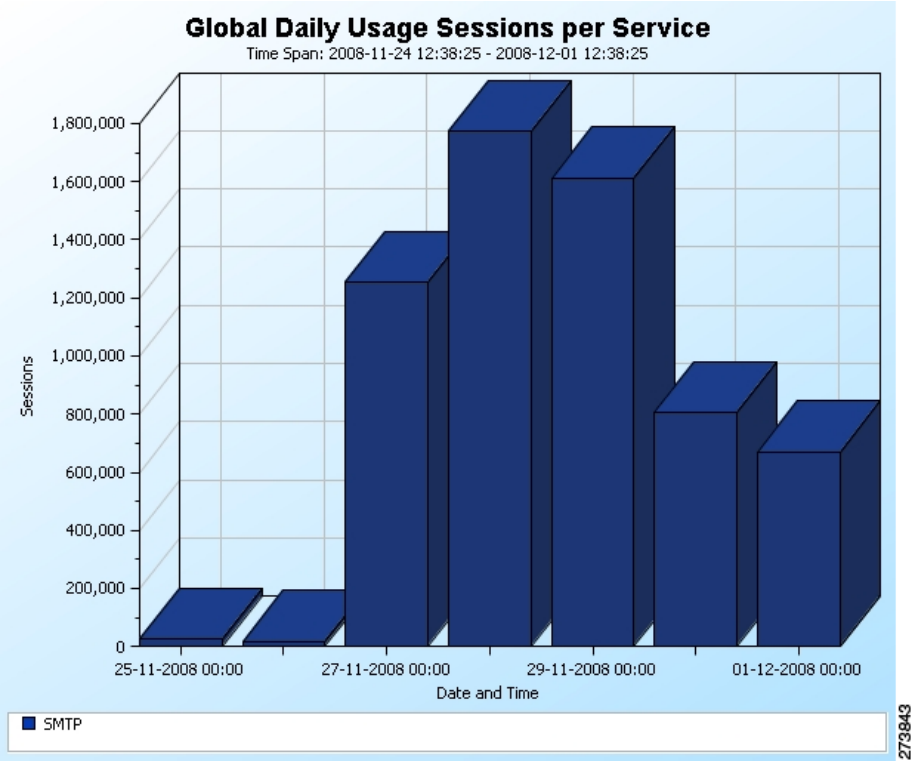
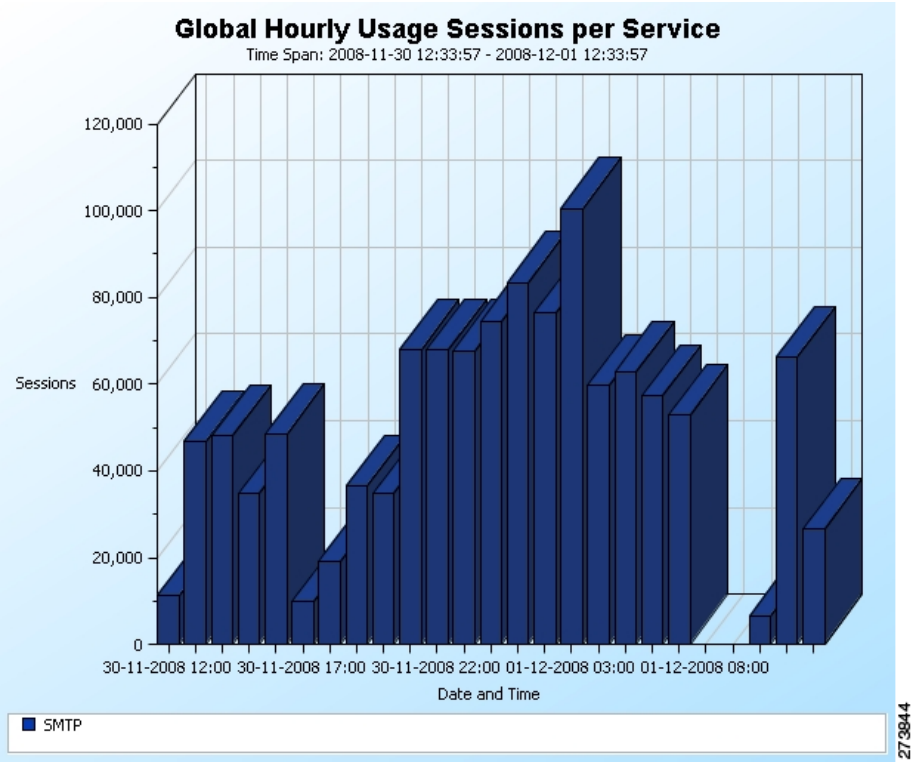


図 7　　Global Hourly Usage Sessions per Service レポート



サービス セキュリティの大量メール送信レポートの表示

ステップ 1 サービス セキュリティ ダッシュボードの [Spam Zombies and e-mail Viruses Detection] ペインで、[View Report] をクリックします。

[Choose a report] ダイアログボックスが表示され、関連レポートのツリーが表示されます。

ステップ 2 レポートのツリーからレポートを選択します。

ステップ 3 [OK] をクリックします。[Choose a report] ダイアログボックスが閉じます。

Reporter ツールが Console で開き、要求したレポートが表示されます。

ステップ 4 レポートの操作方法および保存方法については、『*Cisco Service Control Application Reporter User Guide*』の「Getting Started」の章を参照してください。

4 マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS 含む）
電話受付時間：平日 10:00 ～ 12:00、13:00 ～ 17:00
http://www.cisco.com/jp/go/contactcenter/

OL-21077-01-J