CHAPTER 4

マスメーリング ベースの脅威

ここでは、マスメーリング（大量メール送信）ベースの脅威の概念と、SCE を使用してそれらを防御する方法について説明します。

マスメーリング ベースの脅威

マスメーリング ベースの脅威検出モジュールは、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に基づいています。SCE プラットフォームのサブスクライバ認識機能を使用し、サブスクライバ認識モードまたは匿名サブスクライバ 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開始されたセッションのレートが過剰な場合、通常は、E メール送信に関わる悪質なアクティビティを示しています。このようなアクティビティには、メールベースのウイルス、またはスパムゾンビ アクティビティがあります。

マスメーリング検出の設定

マスメーリング検出は、定義済みの SMTP セッション クォータ（割当量）に違反したサブスクライバに基づきます。

この機能を動作させるには、システムをサブスクライバ認識モードまたは匿名サブスクライバ モードに設定する必要があります。これによって SCE プラットフォームは、サブスクライバごとに生成される 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。

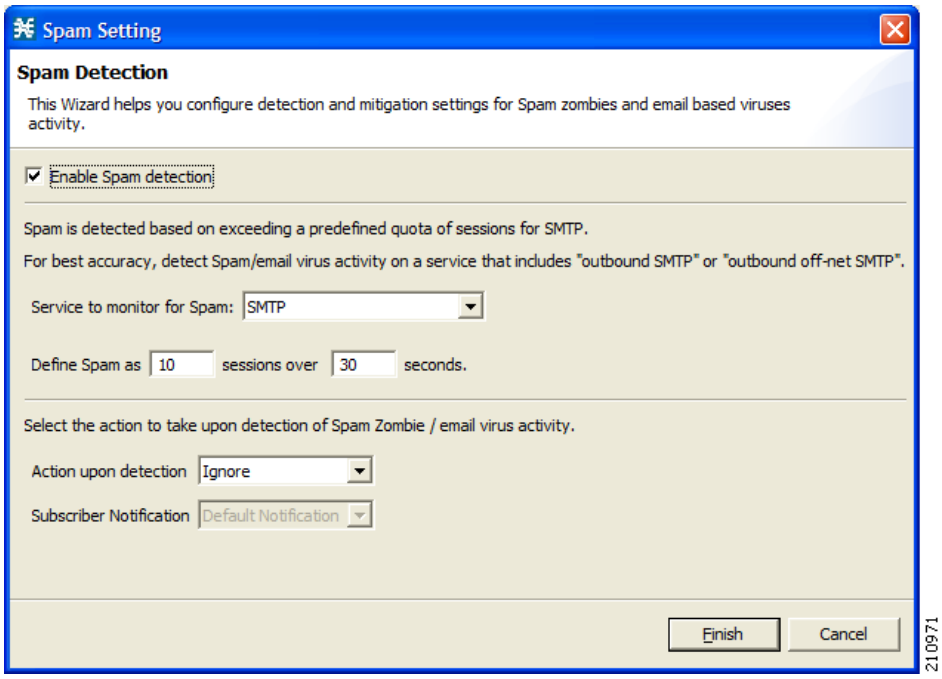
設定には、次の段階があります。

- 検出用サービスの設定 — 適切なサービスを設定します。サービスは、マスメーリング検出用に事前に作成されている必要があります。SMTP プロトコルだけを含むサービスを使用するのが一般的です。調整を加えて、検出範囲を絞り込んだり、可能な場合は検出しきい値を引き下げ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。SMTP では、サブスクライバが自分の宅内で SMTP サーバを稼働することは前提とされていないため、通常は着信プロトコルとは見なされません。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「発信」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 サーバを介して E メールを送信します。ホーム SMTP サーバは、その後、必要が生じたときに随時 E メールを中継します。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、つまり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配慮する必要がなくなります。1 つ注意すべき点は、Google や Yahoo! などの有名な ISP 以外の E メール プロバイダーが有料または無料で SMTP ベースのサービスの提供を開始したことです。そのため、オフネットは、「正規」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ために適した差別化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、「オンネット」サービス定義に SMTP サーバ リストを含め、それ以外の SMTP が「オフネット」になるように設定する必要があります。
  - 上記 2 つの組み合せ

- 異常な E メール アクティビティを見分け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はどちらも設定可能です。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、これらのフィールドの値を決定することを推奨します。「マスメーリング アクティビティのモニタリング」（p.4-3）を参照してください。
- マスメーリング アクティビティが検出されたときの対処方法を定義します。対処には、次の方法があります。
  - ブロック — クォータを超えると、検出が実行されている SMTP またはそれ以上にきめ細かいサービスはブロックされます。クォータ モニタリング期間が終了すると、ブロックは解除されます。たとえば、10 セッション / 60 秒の制限がある場合、クォータ期間（クォータ期間は任意の時点から開始される）内で 10 セッションが発生したあと、ブロックが適用され、そのクォータ期間が終了すると解除されます。
  - 通知 — 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送信します。これは、「サブスクライバ通知」を使用して実行されます。
  - 上記 2 つの組み合せ

図 4-1　Spam Setting ウィンドウ



マスメーリング アクティビティのモニタリング

マスメーリング アクティビティは、CM データベース内で処理され、格納されている情報に基づいてモニタできます。

サブスクライバがマスメーリング アクティビティを検出するために最適なレポートは、「セッション別上位サブスクライバ（top subscribers by sessions）」レポートです。このレポートは、サービスに関して生成され、大量 E メール検出（SMTP、または定義されている場合はよりきめ細かいサービス）に使用されます。レポートでは、マスメーリング アクティビティの被害に遭っている可能性の高いサブスクライバの ID が強調表示されます。

図 4-2　Top Subscribers レポート