メール・Webアクセスを介した脅威へのセキュリティ対策

いまスパムメールは“迷惑広告”という域を超えて、PCをウイルスに感染させるための主要な手段となっている。また、検索サイトの出力結果などを経由して不正なプログラムが仕込まれたWebサイトにアクセスさせるなどの新たな攻撃も現れている。本稿では、これらの脅威へ対抗するためのセキュリティ対策について解説する。

ウイルス感染を狙うスパムメール

企業の情報セキュリティ対策として、コンピュータウイルスへの対策を講じていない企業はほとんどない状況となっているが、じつはウイルス付きメールはここ数年、大幅な減少傾向にある。逆に、急激に増加しているのがスパムメールである。シマンテック社のレポートによれば、スパムメールの割合は2007年は平均でほぼ65％を超えている（http://www.symantec.com/avcenter/reference/Symantec_Spam_Report_-_August_2007.pdf）。

スパムメールの目的は、元来は違法ドラッグの販売、出会い系サイト、ワンクリック詐欺といったサイトへの勧誘がおもなものであった。ところが最近では、メールに記されたURLにアクセスしただけでウイルスに感染してしまうケースが増えている。これはユーザーが利用しているアプリケーションのぜい弱性が悪用されて、ウイルスなど悪意のあるプログラムがダウンロードされてしまうためである。

スパムメールを遮断する

ウイルス付きメールに対しては「不審な添付ファイルを開かない」ことが対策として行われてきた。同様に、スパムメールに対しては「メール内の不審なURLをクリックしない」ことをユーザーに徹底させる必要がある。しかし、このような感染の危険を防ぐのに最も効果的な方法は、そもそもスパムメールをユーザーの手元に届けないことである。メールのウイルスチェックを行うゲートウェイ製品でもスパムメールを検出するものがあるが、旧来型の製品の場合は、ウイルス検知に特化してスパムメールを対象としていないものや、検出精度が低いものがあるので注意が必要である。

スパムメールに対しては、やはりスパムメール対策に特化した機能をもつ製品を導入することが望ましい。それらの製品には、ウイルス感染につながるようなスパムメールを隔離または削除し、また、当該メールがスパムメールであることをユーザーに知らせるために、メールのタイトルに特定の文字を挿入してから配送するといった機能がある。

なお、NRIセキュアテクノロジーズでも、米国Proofpoint（プルーフポイント）社のセキュリティ製品「Proofpoint」を利用した「スパム対策サービス」を提供している（http://

NRIセキュアテクノロジーズ
情報セキュリティ事業部
主任セキュリティエンジニア
田中貴志（たなかたかし）

専門はウイルス・スパムメール対策、情報漏洩対策など

proofpoint.nri.co.jp/)。

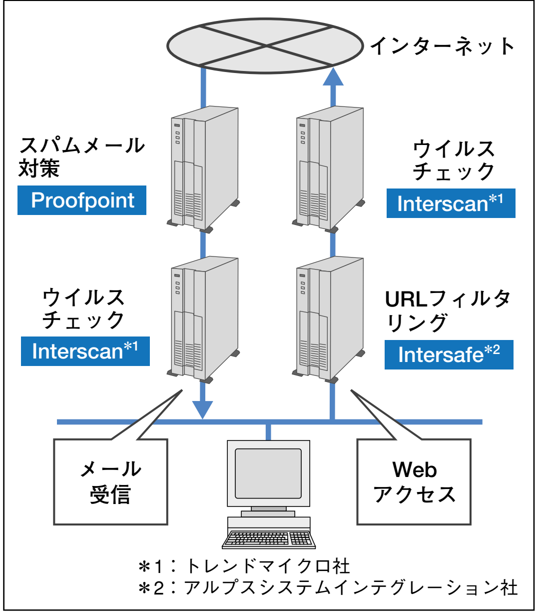
Webサイトを介した危険への対策

スパム対策の専用製品でも問題がないわけではない。検出率が100%というわけにはいかないため、一部のスパムメールがユーザーの手元に届いてしまう危険があるからである。そこで、不用意にURLをクリックしてしまった場合にも感染を防ぐ手段を講じておく必要がある。

そのひとつがWeb閲覧時のウイルスチェックである。以前はウイルスの感染経路はおもにメールであったため、ウイルスチェックというとメールを対象にしたものであった。しかしWebサイトへのアクセス時にもコンテンツのウイルスチェックは必要である。検索サイト大手のgoogle（グーグル）では、ユーザーが閲覧しただけでウイルスなどに感染してしまうサイトが全体の1割にも及ぶという調査結果を発表している。スパムメールを介さずとも、知りたいキーワードについて検索を行い、その検索結果のURLをクリックしただけでウイルスに感染してしまう危険があるのである（http://www.nri-secure.co.jp/security/topics/topics_070518.html）。したがって、Webアクセスについてウイルスチェックを行うことは非常に有用である。

Web閲覧時のウイルスチェックに加えて、そもそも危険なWebサイトにアクセスさせない対策も有効である。たとえばURLフィルタリングは、あらかじめ不適切なサイトのURLを登録したデータベース（随時、更新される）に基づいて、それらの危険なサイトへのアクセス自体をブロックする。フィッシング詐欺のようなケースでは、ウイルスなど悪意のあるプログラムをダウンロードさせる方式ではないためウイルスチェック機能は危険防止には役立たない。そのため、URLフィルタリングのような仕組みが必要になる（図1参照）。

図1　ウイルス感染などへの防御策の組み合わせ例



Webサイトを介したウイルス感染などの脅威への防御策としては、以上のようなツールやサービスが現時点でのベストエフォートであると考えられるが、未公開のぜい弱性を衝いた攻撃などを100%防ぐことはできないという点は留意すべきである。■