※　総務省注釈
　推奨事項の１～３点目（２５番ポート閉鎖等、流量制限規制、コンピュータの特定・隔離等）については、電気通信事業法との関係を整理する必要がありますので、実施に当たっては、事前に総務省にご相談ください。

ネットワーク専門担当者 様

　我々は、世界中の政府機関から成る国際組織に代わって、スパマーが消費者のコンピュータに不正侵入し、「スパムゾンビ」として利用することを防止するための世界的な取組に、貴組織が参加されることを要請します。 我々は、法執行、技術的調査、消費者や事業者への教育、政策立案、官民連携を通じて、違法なスパムを撲滅することに責任を有しています。

　スパマーは、家庭のコンピュータを使用して、数百万単位の大量の電子メールを送信しています。セキュリティの脆弱性を利用して密かにソフトウェアをインストールし、消費者のコンピュータをメールサーバやプロキシサーバに変えてしまいます。彼らは、それらのスパムゾンビを経由させて大量の電子メールを送り、真の送信元を曖昧にするのです。

　インターネット・サービス・プロバイダ（ＩＳＰ）として、貴組織は電子メールシステムの高度化に興味があるかと思いますが、それは、スパムゾンビを通じて送信された大量のスパムによって脅かされています。さらに、受信者は、貴組織のシステム又は貴組織の契約者のシステムから送信されたように見えるスパムのために、貴組織を非難するかも知れません。そして、スパムは貴組織のネットワーク接続に不必要な負荷を与え、管理コストの増大を引き起こすかもしれません。

　我々は、以下の自主的な反ゾンビ対策を、まだ導入していない場合には、適用することを薦めます[1]。

- ２５番ポートを閉じる。ただし、契約者の通信のために設置されているメールサーバにおいて認証されたユーザが、外に対しＳMTＰで通信しようとする場合を除く。外向け（送信）メールサーバを運用しなければならない契約者のために５８７番ポートにおけるＳMTＰ認証の 適用を探究すること。

- 電子メール中継において流量制限規制を適用すること。

- 電子メールの大量送信を行ったコンピュータを特定し、そのコンピュータがスパムゾンビとして作用しているかどうか判断するためのステップを踏むこと。必要なときは、問題の原因が取り除かれるまで、問題のコンピュータを隔離すること。

[1]これらの推奨事項を適用する場合には、それらが、データ保護、プライバシー、情報セキュリティに関する法律、又はその他の法的要件や責務といった、域内の既存の法令に抵触しないことをご確認下さい。これらの推奨事項は、既にいくつかの地域で、義務化されているかもしれないことにご留意ください。

- パソコンをスパムゾンビに変えてしまうワームやトロイの木馬その他のマルウェアに感染することを防ぐ方法について、平易な言葉で利用者にアドバイスを与え、適切なツールや支援を提供すること。

- 契約者のコンピュータが感染していた場合、ゾンビコードを取り除くための使いやすいツールを提供又は指摘するとともに、適切な支援を提供すること。

最後に、スパマーがゾンビコンピュータを生み出すことを防ぐようＩＳＰを奨励することに加えて、我々は、世界中のスパムゾンビであると思われるコンピュータのIP番号と、そのＩＰ番号を管理していると思われるＩＳＰや他のインターネット接続提供者を特定する計画を進めています。この分析は、スパムデータベースやWHOＩＳデータベースのように、公的に蓄積された情報に基づいて実施される予定です。我々は、スパムゾンビだと想定されるコンピュータによって利用されているＩＰ番号に関連するインターネット接続提供者と連絡を取る予定です。この第二のレターでは、被害を受けたＩＳＰが、自社システムにおける明白なスパムゾンビ問題と戦う取組を加速させるよう要請する予定です。

このプロジェクトに関する追加情報やこの取組の参加機関リストを参照する場合には、www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htmをご覧下さい。

スパム撲滅へのご支援ありがとうございます。