

迷惑メールの現状とその対応方法

総合情報基盤センター 技術職員 山田 純一

1. はじめに

迷惑メールは近年急激に増加している。英語ではスパム (spam) メールと呼ばれているが、この解説では迷惑メールと呼ぶことにする。この迷惑メールだが、総合情報基盤センターの問い合わせメールアドレスである info@itc.u-toyama.ac.jp にも1晩で約400通の迷惑メールを受信しており、中には図1のように送信元を少しずつ変えながら送信している迷惑メールも存在する。

✉	2006/09/02 22:02	2006/09/05 08:33	info@vjsuey.com
✉	2006/09/02 22:01	2006/09/05 08:33	info@vhdue.com
✉	2006/09/02 21:58	2006/09/05 08:33	info@vbfget.com
✉	2006/09/02 21:56	2006/09/05 08:32	info@vhuste.com
✉	2006/09/02 21:55	2006/09/05 08:33	info@vgdter.com
✉	2006/09/02 21:55	2006/09/05 08:32	info@vfgbhy.com
✉	2006/09/02 21:54	2006/09/05 08:32	info@vghnj.com

図1 送信元が少しずつ異なる迷惑メール

現在、インターネット上で見られる迷惑メールの種類は大きく以下の5種類程度に分類できると考えられる。

- 出会い系メール
- 広告・宣伝メール
- ワンクリック詐欺・架空請求メール
- フィッシングメール
- コンピュータウィルスを添付したメール

それぞれの迷惑メールがどんなものであるかは省略する。

2. 迷惑メールの経路

迷惑メール送信者のメールアドレスの収集には様々な方法がある。一般的な方法としては、図2のようになる。

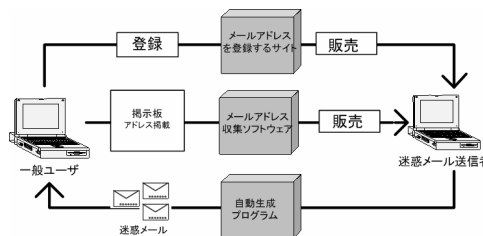


図2 メールアドレスの収集方法

メールアドレスを入手する一番簡単で早い方法はメールアドレスを登録させるサイト (アダルトサイト等) にお金を支払って入手することである。

別の方法としてはメールアドレス収集ソフトウェアを用いて、掲示板等のメールアドレスが記載されているWebサイトを自動巡回してメールアドレスを収集する。実際、インターネットを検索するとメールアドレス収集ソフトウェアが販売されている。

それと、自動生成プログラムがある。これは一定の法則で自動生成したユーザアカウントを任意のドメイン (メールアドレスの@の後半部分) とセットにしてメールを送信するものである。例えばjで始まるアドレスを条件として指定するとそれに合うアドレスを自動的に生成してメールを送信する。もしエラーが戻って来なかったアドレスは、実際に使用していると判断してリストを作成する。

それにメールマガジンを一方的に送りつけ、受信者が何かの間違いと思い、例えば誘導されたWebサイトの図3の画面で登録解除を行えば、たちまちメールアドレスが収集されてしまう手口も存在する。



図3 メールマガジンの解除

他には Web ビーコン (Web バグ) がある。Web ビーコンとは目には見えない小さな画像を Web ページや HTML 形式の電子メールに埋め込むことで閲覧したという情報を収集する。HTML 形式の電子メールの場合は、個人ごとに異なる画像ファイルの URL を埋め込むことができるため、誰が電子メールを読んだかを特定しながら、メールアドレスを収集する。

また、パソコンがコンピュータウィルスに感染し、パソコンの中のアドレス帳、メールアドレスが外部に流出することによって、迷惑メール送信者がメールアドレスを収集する。

このように、メールアドレスの収集方法は高度化しており、送信された迷惑メールの対策は今のメール環境にとって必須であるが、社団法人日本インターネットプロバイダ協会を始め、いくつかのサイトでは「**いわゆる迷惑メールが来ることをやめさせる為の決定的な措置はありません。**」との記載があった。

迷惑メールに対しての決定的な措置がない理由としては迷惑メールの送信者を特定するのが非常に難しいからであると考えられる。まず、迷惑メールの送信には契約したプロバイダではなく、自分のパソコンをメールの送信サーバにして、プロバイダの迷惑メールフィルタを通り抜ける技術を用いている。

さらに高度な技術になると、ボットネットワーク及びオープンリレーサーバを悪用し、身元を隠しながら大量の迷惑メールを送信する。ボットネットワークのボットとは遠隔から操作するために、パソコンに仕込むコンピュータウィルス的一种で、名前の由来はロボット=攻撃者の命令のままに動くマシンからきている。迷惑メールの送信者はこのボットをパソコンに感染させ、感染したパソコン同士をネットワーク化する。これらのボットに感染したパソコンはゾンビ PC と呼ばれる。

迷惑メール送信者は IRC と呼ばれるチャットのシステムを用いてボットネットワークに命令を出し、図 4 のようにそれぞれのゾンビ PC から大量の迷惑メールを送信するため、発信者が詐称される。

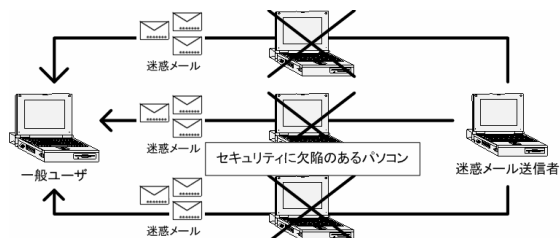


図 4 ボットネットワーク

次にオープンリレーサーバは誰もがメール転送に使用できるサーバのことである。大学ならば大学に所属している学生、教職員のみが利用できるよう、送信元のアカウントや送信を受け付ける IP アドレスを限定するのが通常だが、オープンリレーサーバは誰からもメールを受け付け、配送する。この原因の多くがサーバの設定ミスである。迷惑メール送信者は図 5 のようにオープンリレーサーバを用いて発信元を詐称し、迷惑メールを送信する。

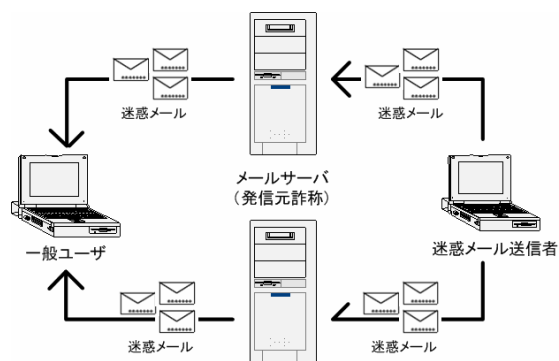


図 5 オープンリレーサーバ送信

3. 迷惑メールの対策

現在迷惑メールの大半が、前述したボットネットワーク及びオープンリレーサーバによって発信元が詐称されており、送信者を特定するのは非常に困難となっている。

迷惑メールの送信者を特定するのが非常に

難しいことから完全な対策というのは今のところなく、迷惑メールを防ぐには迷惑メールの送信者にメールアドレスを知られないようにするしかない。そのための対策をインターネット及び書籍等で調査した結果、以下の7つが考えられる。

- 迷惑メールには返信しない。
- メールアドレスはインターネットに公開しない。公開しなければならない場合は工夫する。
- HTML メールは使用しない。
- 添付ファイルやメールの本文中にあるURLは信用できるもの以外開かない。
- Windows Update (セキュリティのアップデート) 及びウイルス対策を怠らない。
- メールフィルタリング機能を活用する。
- 迷惑メールばかりの方は思い切ってメールアドレスを変更するのも1つの方法である。

基本は迷惑メールには絶対に返信しないことである。同様にプライバシーポリシーを公開していない懸賞サイト等ではアドレスを登録しないことが重要である。また、掲示板やホームページ等で不用意にメールアドレスを公開しないことも大事である。しかし、連絡先等で公開しなければならない事態も考えられる。その際は図6のようにメールアドレスを画像にしたり、全角にしたり、HTMLのmailtoタグをハイパーリンクにしない等の方法がある。



Email address: please change  to toyama
yama@cns.-u.ac.jp

図6 メールアドレス公開の工夫

最後にメールフィルタリングについて記載する。通常のメールと迷惑メールを区別するソフトウェアの機能をフィルタ、フィルタを

使用した分類作業はフィルタリングと呼ばれる。フィルタが採用する方法には大きく分けて2種類ある。ルール型と学習型である。まず、ルール型とはユーザが決めたルールに従ってメールを分類する方法である。例えば未承諾広告等の文字列が、件名や本文に含まれるメールを受信ボックス以外の場所に移動することが当てはまる。

もう1つは学習型である。過去の迷惑メールの内容を分析し、その傾向を基準にしてメールを自動で分類する。学習型フィルタではベイジアンフィルタが主流になってきている。ベイジアンフィルタとは18世紀の数学者Thomas Bayesが提唱した確率理論=ベイズ理論を応用したフィルタである。ベイジアンフィルタではユーザが受信したメールを迷惑メールと通常のメールに分類するたびに統計を蓄積し、単語や単語グループなどの辞書の作成と更新を行い、識別精度を徐々に高め、迷惑メールの出現率を計算する。その後、受信したメールはこれを基準に、受信するメールが迷惑メールかそうでないかを自動判断する。

以上のようなフィルタリングを搭載したメールソフトウェアを使用するのも対策の1つである。ただし、メールフィルタリングは間違っていてフィルタリングすることがあること、どの方式でも万能ではないことに注意しなければならない。

富山大学でも迷惑メールの数は年々増加している。五福キャンパスでは現在、迷惑メールのほとんどは旧富山大学のアドレス(***@***.toyama-u.ac.jp)に届いているが、旧メールアドレスから新メールアドレス(***@***.u-toyama.ac.jp)への自動転送サービスを実施しているため、迷惑メールも全て新メールアドレスに転送されている(ただし、自動転送サービスの停止を希望された方は除

く)。

旧メールアドレスから新メールアドレスへの自動転送サービスは2007年3月31日に停止するが、旧メールアドレスに送付される多量の迷惑メールに困っている方は、自動転送サービスの停止をご検討ください。

五福キャンパスで自動転送サービスの停止を希望される方は、「旧メールアドレスから新メールアドレスへの自動転送サービス停止申請書」を総合情報基盤センターまで提出してください。自動転送サービスを停止されたユーザの方々からは、迷惑メールが来なくなったとの報告を受けている。

4. まとめ

繰り返すが、迷惑メールが来ないための完全な対応策はない。ただし、迷惑メールを防ぐ7つの方法を行うことにより、迷惑メールが来る確率は変わる。また、メールを使用しているユーザ1人1人の対策に加えて、学内

全体で今後の対策を議論していく必要があるかと思われる。例えば自動生成プログラムにより生成されたメールアドレスに対して、サーバ側でユーザが存在するかしないかの受け答えをするのか、大学全体で迷惑メール対策の機器を導入することになった際、大事なメールが届かないことがあるが、その時はどうするかなど、課題はたくさんある。

5. 参考

- 1) 日経パソコン、2005年4月号
- 2) 月刊アスキー、2005年3月号
- 3) 月刊アスキー、2005年4月号
- 4) 社団法人日本インターネットプロバイダー協会：
<http://www.jaipa.or.jp/UCE/stop.html>
- 5) 月刊 NETWORK MAGAZINE、2006年6月号