

## 迷惑メールの最新動向

樋口 貴章 株式会社オープンテクノロジーズ 主管調査役 戦略企画担当

### 迷惑メールはボットネットによって配信されるケースが増加傾向 先進的な日本の対策をベースに国際的な協力関係の広がりが望まれる

迷惑メールは、不特定多数を相手に大量に送信されるため、さまざまな弊害が生じている。メールの受信者にとっては、単に不要なメールであるのみならず、フィッシングやコンピューターウイルスの被害を受けることもありうる。メールサーバーを運用する側にとっては、メールサーバーの負荷増大や、極端な迷惑メール対策技術の導入によるメール送信障害などの問題がある。技術的な対策だけでなく、法的対策や国際協力を通じ、迷惑メール送信を削減するさまざまな努力が行われている。

携帯電話のメールでは、迷惑メールを受信する際にパケット課金が生じるため、受信ユーザーは金銭的な被害も被る可能性がある。近年では携帯電話通信事業者の規制により、携帯電話から送信される迷惑メールの数は減少しているが、インターネット経由のメールは相変わらず続いている。対策としては、推定しにくいメールアドレスの使用の推奨や、インターネット経由のメールを受信しないオプションや、登録ドメインのみ受信するオプションなどが行われている。

#### 迷惑メールは7割超で横ばい

国内の全メールに占める迷惑メールの割合は7割を越える程度でほぼ横ばい状態である(資料6-2-11)。

迷惑メールは、人間が手動で送信するケースや、サーバーでプログラムによって大量送信するケースがあるが、近年では、コンピューターウイルス感染によって形成されるボットネットを通じて分散配信されるケースが増えている。ブラジルやインドなどを送信国とする迷惑メールが増加傾向にあるが、これらの多くは、ボット

ネット経由と考えられている。

本文の内容については、英文メールでは通販広告が多いが、日本語メールでは出会い系が多数を占めている。迷惑メール送信者と、広告主であるサイト運営者が異なるケースも多い。サイト運営者は、迷惑メール送信者に料金を支払っており、それに見合う金銭的利益を得ていると推定される。迷惑メールを受信したユーザーが安易に金銭を支払わないように注意することも重要である。

#### 大きく3つの対策を実施

迷惑メール対策技術は大きく「送信させない対策」「受信しない対策」「受信後の対策」の3つに分けられる。

送信させない対策としては、OP25B (Outbound Port 25 Blocking) がある。ISPに接続する動的IPアドレスのユーザーから外部への直接メール送信を遮断するものであり、ボットネット対策としては効果的である。国内ISPではすでに採用が浸透しており、日本国内から送信される迷惑メールの削減に大きな効果があった。

次に、受信しない対策技術をみてみよう。迷惑メール送信IPアドレスを登録したブラックリストを用いる方法は古くから使われているが、誤登録や解除コストの問題が副作用として存在している。また、グレイリストイングと呼ばれる、初めて接続するサーバーには再送を要求する方法もあるが、メールの遅配が起きる可能性もある。このように副作用が考えられる技術は、ISPレベルでの積極的な採用には至っていない。一方、ユーザー企業などのレベルでは迷惑メール対策アライアンスなどの普及に伴って、採用も増えているのが実状である。

ISPが電気通信事業法の規制によって極力通信を遮断しないように努力しているのに対し、ユーザー企業などのレベルでは技術対策の導入自由度は高いが、メールサーバー管理者のレベルで副作用を明確に認識した上で採用するかどうかを判断するべきである。

近年、普及しつつある送信ドメイン認証技術は、メール送信者のメールアドレスを詐称させない技術である。IPアドレスをベースにメールサーバーを認証する「SPF(Sender Policy Framework)/Sender ID」と、電子署名によって送信者を特定する「DKIM」(DomainKeys Identified Mail)の2種類がある。両者は併用可能であるため、併用が望ましい。SPFは、DNSサーバーに設定するだけなので採用しているサイトも増えており、JPドメインのほぼ7割に達している。DKIMは、メール送信サーバーで電子署名を処理する必要があるため設定が複雑と思われるせいか、現時点ではそれほど普及していないが、IETFでは活発に議論が行われており、国際的に今後普及が期待される技術である。国内においてはSPF/DKIM双方の普及推進に努めている。送信ドメイン認証技術が普及すれば、受信側メールサーバーで、詐称メールに対する受信拒否を効果的に実現できる可能性が高まる。

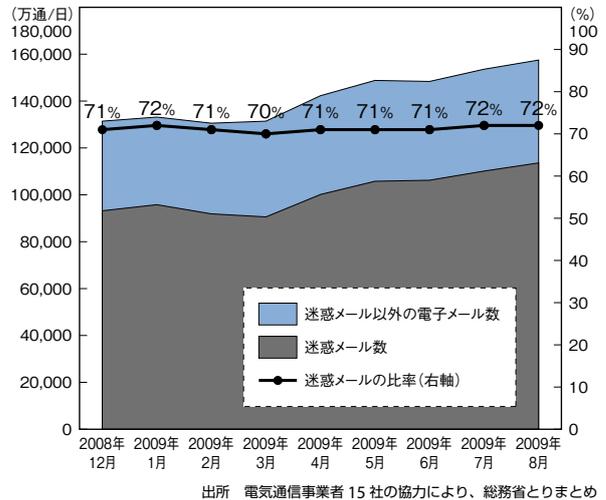
受信後の対策としては、受信側メールサーバーにおけるフィルタリング処理と、受信ユーザー側におけるフィルタリング処理が普及している。最終的なメール利用者の目に直接触れる数を減らすという意味では、フィルタリングの作業効率を上げることが求められるが、誤判定によって必要なメールが埋没する可能性には注意が必要である。前述したように、送信ドメイン認証技術が普及すれば、受信後のフィルタリング処理も可能となるため、フィルタリングの精度を上げられると期待される。

### 迷惑メールの法的対策

国内における法的対策としては、迷惑メール送信者を対象とする総務省・消費者庁共管の「特定電子メールの送信の適正化等に関する法律」(特電法)と、サイト運営者を対象とする経済産業省・消費者庁共管の「特定商取引に関する法律」(特商法)の2つがある。

これらの法律は3年ごとの改正で強化されてきている。当初は、送信者やサイト運営者の摘発は少なかったが、2008年の法改正によって、広告宣伝メールは受信

資料6-2-11 国内ISPにおける迷惑メール数・割合の推移



者からの請求や承諾が無い場合には送ってはいけないことになり(オプトイン規制)、罰則が強化され、措置命令の数は改正前よりは増加しつつある。

### 国際的な迷惑メール対策

日本国内における迷惑メール対策は、技術的対策と法的対策の両面で、国際的には先進的状况にある。結果として、国内を送信元とする迷惑メールは減っている一方、海外から国内へ送信される迷惑メールは増加傾向にある。その原因の1つは、前述したボットネットの増加によるものと推定される。よって、国際的な迷惑メール対策協力が必要となっている。日本はOECD(経済協力開発機構)やロンドンアクションプラン(スパム対策施策)などの国際的な活動にも参加している。また、中国・香港・台湾・ブラジルなどと二国間協力活動を行っており、民間レベルでも技術交流や情報交換が行われている。それらの活動を通じて、日本国内の対策の成果を伝達し、同様の対策を諸国で採用するよう働きかけている。

### 今後の迷惑メール対策の展望

国内の技術対策の中では、送信ドメイン認証技術(SPF/DKIM)のさらなる普及が望まれる。また、2011年の法改正を控えて、法制度の強化に関する議論も必要であろう。これらの国内での先進的な活動成果をベースに、国際的な協力関係を国家レベルならびに民間レベルでさらに広げる必要がある。



## [インターネット白書 ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<http://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ [iwp-info@impress.co.jp](mailto:iwp-info@impress.co.jp)