

2. メールテクニカルレポート

2.1 はじめに

インターネットの普及と共に、電子メールはその利便性から急速に利用者を増やし、利用形態も単なるテキストの送受信だけでなく、MIME (Multipurpose Internet Mail Extensions) の拡張から各種データを配送するためのプラットフォームとしても使われるようになりました。特に日本では、早い段階から携帯電話の標準機能として電子メールが利用できるようになったこともあり、その普及と共に利用者層が急速に増加し、いまや電子メールはコミュニケーションのための重要な社会基盤となっています。その一方で、実際の送信者が誰であるかを詐称できたり、受信側が送信者をあらかじめ選択できない等の機能的不備により、ウイルスや広告宣伝等のいわゆる「迷惑メール」が年々増加し大きな社会問題となっています。

IJ では、2001年からウイルス対策機能を法人及び個人向けに標準提供し、2004年には迷惑メールフィルタ機能をいち早く導入する等、より良いメールの利用環境の提供を目指してきました。

また、2004年に国際的な迷惑メール対策ワーキンググループである MAAWG (Messaging Anti-Abuse Working Group) の設立に参加し、2005年には日本国内でも JEAG (Japan Email Anti-Abuse Group) を発起人として立ち上げる等、国内外で迷惑メール対策について主導的な役割を果たしてきました。

迷惑メール対策の検討・推進には、関係機関や多くのネットワーク運用者との共通の問題認識の醸成が必須となります。そのため、本レポートは、これまでの IJ の活動を元に現在の迷惑メールの状況、特に日本国内における迷惑メールに関して信頼できるデータを広く提供することを目指しています。また、IJ では2005年からいち早く送信ドメイン認証技術を導入しており、こういったメールシステムに対する有益な拡張的機能を推進する立場から、これらの利用状況等についても随時情報を提供していく予定です。

2.2 迷惑メールの動向

望まないのに勝手に送られてくるメールに対して、日本では「迷惑メール」という言い方がほぼ定着していますが、欧米では英国のコメディ番組が起源と言われている「スパム (spam*)」が一般的に使われています。ここでの迷惑メールは、ウイルス付きメールや未承諾の広告メール等、受信者が望まないメール全般を対象とします。

2.2.1 迷惑メールの割合

2008年6月2日(23週)から8月31日(35週)までの週ごとの迷惑メールの割合を集計したものを図-1に示します。この期間の受信メール全体に対する迷惑メールの割合の平均は約85.8%でした。多少の変動はあるものの、一環して85%前後で推移しており、お盆の時期を含む33週目(8/11-8/17)が89%と最も高い割合となりました。これは、多くの企業が休日のため業務としてのメール利用が少ない時期にあたるものの、迷惑メールの数自体があまり変化していないことにより、相対的に割合が高くなったものと推測しています。

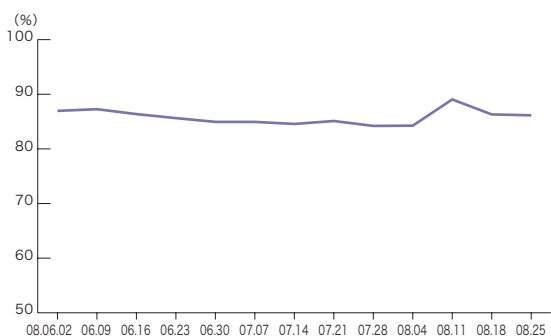


図-1 迷惑メールの割合

*1 ランチョンミート「SPAM」を販売している Hormel Foods 社は、メールのスパムに対しては小文字で記述することを推奨している (<http://www.spam.com/legal/spam/>)。

この期間の平均を 2007 年と比較したものを、図-2 に示します。

2007 年での平均は約 73.1% であり、1 年で迷惑メールの割合が約 12.7% 増加したことが分かります。迷惑メールははまだ増加傾向にあり、引き続き対策が必要です。

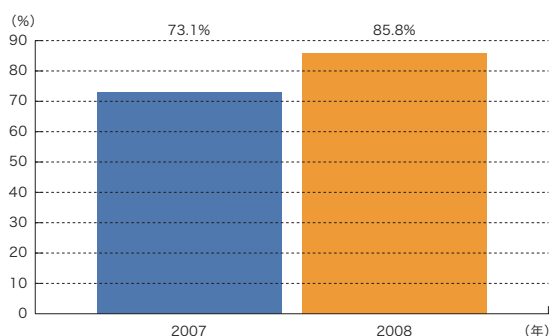


図-2 迷惑メール割合の前年との比較

2.2.2 迷惑メールの送信元

初めての迷惑メール (spam) は、今から 30 年前に ARPANET^{*2} にある製品の宣伝を流したことだと言われています。その時代のメールは利用者が限られていたため、誰が送信したのか、どこから送信されてきたものなのかが明確でした。ところが、迷惑メールの送信手法は日々進化しており、実際に誰が送信したのか判断が非常に難しくなってきました。それでもインターネットの普及によって、ほとんどのメールが SMTP^{*3} によって直接送られてくるようになり、どこから送信されたものかについては、把握しやすい環境にあります。

迷惑メールの送信元がどこで、それがどのような傾向にあるのかを分析することで、対策の検討が可能になります。ここでは迷惑メールと判定された送信元の IP アドレスについて、その送信元の地理的傾向と送信数に着目して集計をしました。

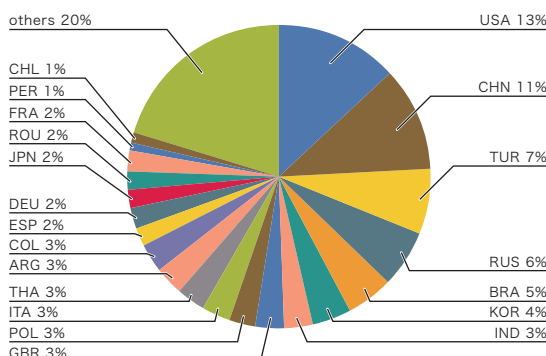


図-3 迷惑メールの送信元

図-3 は、2008 年 6 月 2 日 (23 週) から 8 月 31 日 (35 週) までの 3 か月間に迷惑メールと判断されたメールの送信元の国別^{*4}の割合を示しています。この期間に最も多かったのが米国で、全体の約 13% を占めていました。次いで中国 (11%)、トルコ (7%)、ロシア (6%)、ブラジル (5%)、韓国 (4%) の順となり、これまで迷惑メールの送信が多いと言われていた国がいずれも上位にあります。日本は 2% で 16 位という結果でした。日本ではブロードバンドを比較的に安価に利用できますが、その割に迷惑メールの送信量が少ないのは、大手 ISP を中心として OP25B^{*5} の導入が進んでいることが挙げられます。個人向け ISP を接続回線としてオンライン

*2 ARPANET は 1967 年に米国防総省によって構築されたネットワークで、その後インターネットへと発展していった。

*3 SMTP (Simple Mail Transfer Protocol) の詳細は、RFC2821 によって規定されている。

*4 Maxmind 社の「GeoLite Country (<http://www.maxmind.com/app/geolitecountry>)」から取得。

*5 OP25B (Outbound Port 25 Blocking) は一般ユーザが接続回線に利用する動的 IP アドレスから、外部ネットワークのメールサーバ間で利用する 25 番ポートへのアクセスを制限する技術で、迷惑メール送信の抑制に効果があると言われている。

で契約し、そこから迷惑メールを大量に送信したり、ボットネット*6 を利用するような送信手法に対しては、このOP25B は有効に機能します。

これまで、迷惑メール対策といえばメール受信側でのブロックまたはフィルタが主流でしたが、ネットワークを管理する送信側で抑制するOP25Bは、ある意味、画期的な手法でした。特定の範囲であったとしてもインターネットの利用を制限するOP25Bは、当初は批判的な意見が多くなかなか導入が進みませんでした。現在でもこれほど広範囲に行われている地域は、日本しかありません。これには、IIJが中心となって創設したJEAGが大きな役割を果たしました。この経緯については、また機会があればレポートしたいと考えています。

この期間（13週間）の各迷惑メールの送信元（IPアドレス）は、平均すると1IPアドレスあたり約37.7通を送信しています。

平均して1日に1通も送信しないということは、大半の送信元が日常的にメールのやりとりをするような一般的なメールサーバではないことが推測できます。迷惑メールを一度に大量に送信するような送信元（メールサーバ）がまだ存在することを考えると、この平均送信数はより小さな値になるはずで

す。各送信国の割合をみても、突出した国がなく、それぞれの国の規模やネットワークの整備状況に準じて順位づけられているように見えます。このように、迷惑メールの送信元はほぼ全世界に分散しており、多数の送信元から少しずつ送信しているというのが現在の傾向となっています。これもボットネットを利用した迷惑メール送信の特徴とされています。

2.2.3 迷惑メールの傾向

迷惑メール送信の目的は様々ですが、同じようなパターンのものが大量に発生するケースがあります。パターン適合によるウイルス検知が主流だった時代には、新たなパターンが作成されるまで次々と増幅し、結果として大量に発生することがありました。また、金融機関を装ったフィッシングでは、迷惑メールフィルタに検知される前に偽のサイトにアクセスさせようと、瞬間的に大量送信されることがあります。

今回は、8月に大量送信されたニュースサイトを騙った迷惑メールの状況について解説します。

2008年8月5日2時頃(日本時間)から表題(メールヘッダのSubject:行)に「CNN.com Daily Top 10」と書かれたメール(図-4)が大量に届くようになりました。IIJのあるサービスでは、8月5日に受信したメール全体の2.6%に、8月6日には全体の3.3%にも達しました。IIJが迷惑メールフィルタで提携しているMX Logic社*7では、1時間あたり500万通受信したと報告されています。

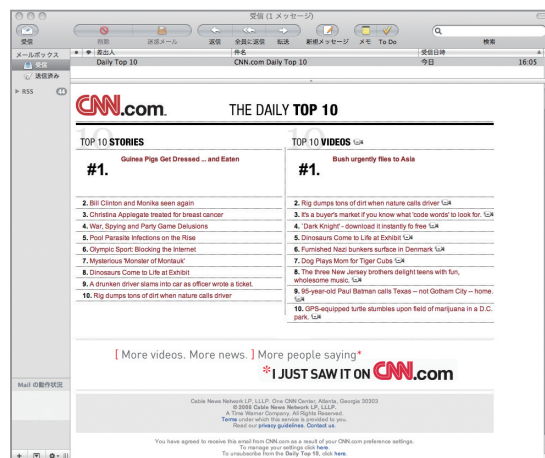


図-4 「CNN.com Daily Top 10」のサンプル

*6 マルウェアに感染したパソコンが外部からロボットのように操られていることからボット(Bot/Bot PC)と呼ばれ、その集合をボットネット(Botnet)と呼ぶ。ゾンビPC(Zombie PC)と呼ばれることもある。

*7 MX Logic社のURLは、「http://www.mxlogic.com/」。

2.3 メールの技術動向

この CNN を騙った迷惑メールは、通常のテキスト文字によるメッセージと HTML 形式によるものそれぞれが MIME 形式で含まれていました。HTML のリンク先は、CNN を模した無関係等メイン上に誘導され、フラッシュプレイヤーのバージョンアップをポップアップで促されます。このポップアップをクリック（どこをクリックしても挙動は同じ）するとマルウェアがダウンロードされる、という仕組みになっていました。

この「CNN.com Daily Top 10」メールは、その後「CNN Alerts: My Custom Alert」を表題とする類似の迷惑メールとなり、さらに「msnbc.com - BREAKING NEWS:」からはじまる複数の表題パターンへと変化し、8月中旬まで続きました。いずれもウェブサイトに誘導し、マルウェアに感染させようとする同様のパターンです。

これらのメールは、いずれも実在するメールに巧妙に似せていること、HTML 部分のリンク先や送信元を示すメールアドレスに多数のパターンが存在し、それらの特定が難しいことから、検知自体も難しいという特徴がありました。フィルタ側の対応が遅れて、受信者に届いたメールから不用意にマルウェアに感染した場合、新たなボットとして迷惑メール送信やマルウェア配布のための Web サイトとして悪用されてしまいます。

このように、迷惑メールは、フィルタをかいくぐり、受信者を欺く巧妙なものが増加しており、絶えず状況を把握し、迅速に対応することが必要です。

2.3.1 送信ドメイン認証技術

この3ヵ月（13週）の間に受信した迷惑メールの割合は85%を超え、かつてないほどの高水準状態が依然として続いています。迷惑メールが多い原因として、それにより利益が得られるという動機の面と、簡単に送信ができてしまうメールシステムの仕組み、双方の問題が挙げられます。ここでは、メールシステムの問題を改善するための幾つかの試みに焦点をあて、最新動向のレポートと解説を行っていきます。

今回は送信ドメイン認証技術^{*8}のひとつ SPF (Sender Policy Framework) の動向について解説します。SPF の仕様は、2006年4月に RFC4408 として公開されました。仕様策定の経緯や仕様の概要については、また別の機会にレポートしたいと考えています。今回は、メール受信側からみた送信者の対応状況について報告します。

多くのメールシステムの拡張がそうであるように、SPF もメールの送信側と受信側との双方が導入することにより効果が得られます。SPF の場合、送信側の導入は比較的容易ですが受信側で認証を行うには、メールサーバに対する新たな機能追加が必要になります。IJJ では 2005 年から送信側としての対応を順次行い、2006 年には業界に先駆けて、受信時の認証機能の導入及びその認証結果によるフィルタリングサービスを提供しました。

これらの実績を元に、現在の SPF の対応状況について分析します。

WIDE^{*9} と JPRS^{*10} の共同研究によれば、8月時点での JP ドメインの SPF 宣言率は 24.44% と報告^{*11} され

*8 送信ドメイン認証に対応する英語名称は「Sender Authentication」。直訳すると送信者認証だが、実際にはドメイン部分の認証が主体であることとメール投稿者を認証する SMTP-AUTH と区別するために日本語では「ドメイン」をつけて分かりやすくしている。

*9 1988年にスタートした産官学が連携した研究組織。WIDE (Widely Integrated Distributed Environment) プロジェクト。

*10 JPドメイン名の登録管理とDNSの管理をする組織 (<http://jprs.jp/>)。Japan Registry Services の略称。

*11 WIDE の「ドメイン認証の普及率に対する測定結果 (<http://member.wide.ad.jp/wg/antispam/stats/index.html.ja>)」から取得。

ています。また、Sendmail Consortium の調査では、Fortune 1000社の各ドメインで SPF を宣言している割合は25.6%となっています*12。今や主要ドメインの概ね4分の1は SPF に対応していると言っているでしょう。

IIJのあるサービスでのメール受信時のSPFの認証結果の推移を図-5に示します。

受信メールのうち、送信側が SPF に対応している数自体は概ね増加傾向にありますが、受信メール全体の SPF 対応の割合については2007年6月の約30%から徐々に減少傾向にあり、最新の2008年8月では26.4%でした。別のIIJのサービスでは、6月から8月までの間ではあまり変化がなく、平均すると約21.4%となり、いずれも20%台という結果になりました。

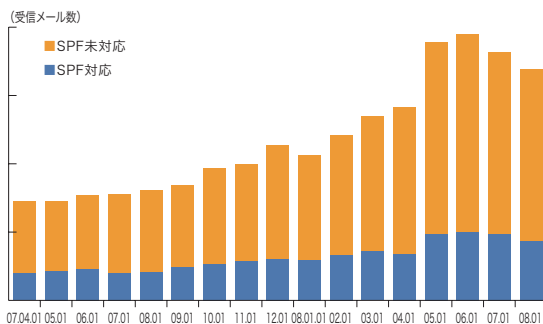


図-5 SPFの認証結果の推移

日本のISPや携帯電話事業者等、よくメールに利用される主要なドメインがほとんど SPF を宣言していることと、静的な調査結果の宣言率を考えると、実際の流量ベースではもっと SPF の宣言率が高くて良いはずですが、そうはならない原因は、85%を超える迷惑メールにあると考えています。

執筆者：

櫻庭 秀次 (さくらば しゅうじ)

IIJ ネットワークサービス本部 メッセージングサービス部 サービス推進課 シニアプログラムマネージャ。IIJのメールシステムの設計及び実装に従事。現在は安全なメッセージング環境実現のため、研究開発や、社外関連組織と協調した各種活動を行う。MAAWG メンバ及び JEAG ボードメンバ。2008年6月、日本発の迷惑メールの大幅な減少に寄与した JEAGの活動が総務大臣表彰を受賞。

*12 Sendmail Consortium の「Fortune 1000 DKIM Survey (<http://www.sendmail.org/dkim/surveyFortune1000/>)」から取得。

これまで迷惑メールの送信者メールアドレスには、受信者に怪しまれないように実在するドメイン名、特にフリーメールや大手ISP等ユーザ数の多いドメイン名を使う傾向がありました。SPFが標準化され、メール事業者を中心として SPF の宣言率が高まるにつれて、認証チェックをすればこれら詐称したドメインでは逆にすぐに認証できない怪しいメールであることが判明してしまいます。

こうした状況を反映して迷惑メール送信側は SPF の認証結果が得られない SPF の宣言されていないドメイン名、場合によっては迷惑メール送信者自身が取得した適当なドメイン名の利用に移行していると推測されます。SPF の宣言率が増加傾向にある現状で、もしそれが正しいとすれば、もはや SPF を宣言していないドメイン名自体を怪しいメールと判断しても良い時期にさしかかっているのかもしれない。自分のメールが迷惑メールと誤判定されないためには、まず自分が使っているドメインで SPF レコードの宣言をする、または SPF 宣言されているメールサービスを正しく利用することをお勧めいたします。

2.4 おわりに

このメール技術ニカルレポートでは、IIJが提供しているメールサービスを元に、迷惑メールの動向と SPF の認証結果を利用した幾つかの統計情報とそれについての解説をまとめました。最初に述べたとおり、増加し続ける迷惑メールに対処していくためには、実際の利用環境に近い範囲での的確な情報を、ある程度の長さの期間で俯瞰し分析していくことが重要です。今後信頼できるメール環境の実現を目指し、継続した分析とデータの提供を行って参ります。