日本が迷惑メール送信元地域の第3位になった理由

今回は、2011年第1〜13週での迷惑メールの推移を報告します。
迷惑メール送信元地域の第1位は中国でした。また、日本の順位が大幅に上昇して第3位になりました。
今回は、この理由とともに、迷惑メール対策とIPv6アドレスとの現状の関係について解説します。

2.1 はじめに

このレポートでは、迷惑メールの最新動向やメールに関連する技術解説、IIJが関わるさまざまな活動についてまとめています。今回は、多くの企業の第4四半期にあたる2011年第1週（2011年1月3日〜 1月9日）から第13週（2011年3月28日 〜 4月3日）までの13週間分のデータを調査対象にしています。また、送信ドメイン認証技術の一つであるSPF（Sender Policy Framework）の普及状況を把握する目的で、認証結果の割合の推移について報告します。さらに、IPv4アドレスの枯渇によって増加が予想されるIPv6アドレスの利用と迷惑メール対策の留意点についても触れます。

2.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJのメールサービスで提供している迷惑メールフィルタが検知した割合の推移と、迷惑メールの送信元に関する分析結果を中心に報告します。前回のレポートでは、昨年後半から迷惑メールの割合が減少傾向にあったものの、年明けから再び増加する兆しも見られていると報告しました。ここでは、その後の経過についても報告します。

2.2.1 Rustockの活動停止により大幅減少に

迷惑メールの割合は、昨年末に急激に低下しましたが、年が明けて2011年からは以前の水準に戻りつつありました。しかし、3月中旬から再び急激に割合が低下しました。今回の調査期間と、前年の同時期を含む1年3ヵ月分（65週）の迷惑メールの割合の推移を図-1に示します。

今回の調査期間での迷惑メールの割合の平均は65.4%でした。前回のレポートから6.7%減少しており、前年の同時期に比べると16.7%と大幅な減少となっています。

前回のレポートでも報告したとおり、昨年後半からの迷惑メール量の減少には、迷惑メールの主要な送信元であるボットネットの活動低下が影響していると考えられています。特に、迷惑メール送信の大部分を占めるボットネットRustockの活動停止が主要な要因であるようです。The Wall Street Journal誌オンライン版[*1]の3月号では、マイクロソフト社と米国連邦司法当局がRustockの制御元[*2]になっているホストコンピュータ

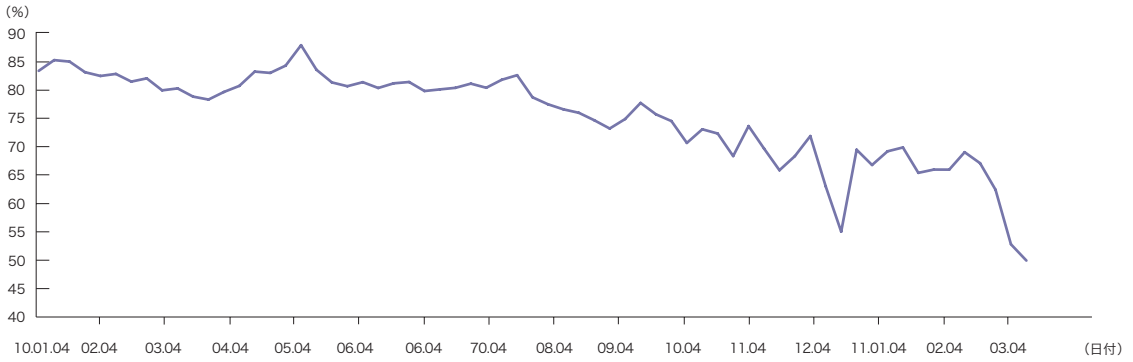

図-1 迷惑メール割合の推移

を押収したことで、その活動がほぼ完全に止まったと報じています。同様に、マイクロソフト社の公式ブログ[*3]でも概要が報告されています。

ユーザ各自が使用するPCがボット化されないようにすることや、ボット化された可能性があるときには速やかにクリーンにすることも大事です。しかし、2008年にあったMcColo社によるネットワーク遮断も同様ですが、ボットネットの活動を止める有効な方法は、ボットPCの制御元（Herder）を何らかの方法で処置することです。少なくとも、迷惑メールに関しては劇的な効果をもたらすことが、今回の事例からも明らかになりました。

2.2.2 日本が迷惑メール送信元の第3位に

今回の調査期間での迷惑メール送信元地域の分析結果を図-2に示します。今回の調査では、迷惑メールの送信元地域の1位は中国（CN）で、迷惑メール全体の12.4%を占めていました。中国は、2010年第1四半期以来の1位です。2位は、これまで1位だった米国（US）で8.0%でした。3位は日本（JP）で6.4%とこれまでで最も高い割合と順位になりました。4位はフィリピン（PH、6.1%）、5位はインド（IN、5.8%）、6位はロシア（RU、5.1%）という結果でした。

今回の上位8地域に関する週ごとの割合の変化を図-3に示します。この期間、中国（CN）がほぼ一貫して高い割合を維持していることからも、全体で1位となったことが分かります。2位の米国（US）は、1月中旬以降に割合を低下させています。割合の推移からはその特徴が見えにくいですが、Rustockの活動が低下した3月中旬以降は実数としても大きく低下しています。同様の傾向は、インド（IN）やブラジル（BR）にも見ることができます。その一方で、フィリピン（PH）が2月後半以降に大幅に割合を増加しています。また、中国（CN）も3月以降急激に増加しています。

2.2.3 Rustock活動停止から分かる迷惑メール送信の地域性

日本（JP）は、前回の5位（4.7%）から順位も割合も上昇しました。しかし、前回のレポートや前年の同時期と比較してみると、迷惑メール送信量の実数はそれほど増加していません。日本の割合の増加には、Rustock等

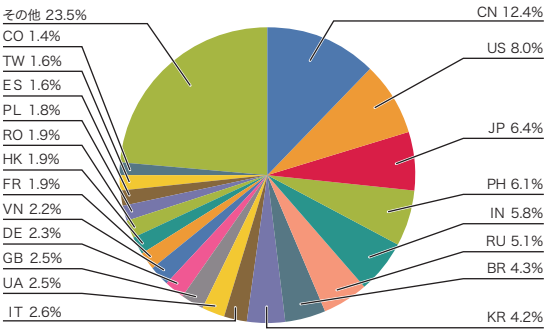

図-2　迷惑メール送信元地域の割合

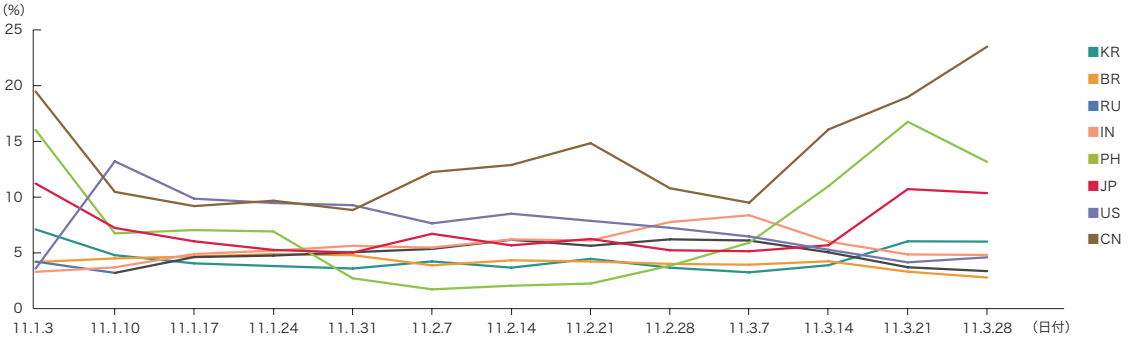

図-3　主要迷惑メール送信地域の割合の推移

＊1　The Wall Street Journal（http://online.wsj.com/public/page/news-tech-technology.html）。
＊2　ボットネットは不正プログラムに感染させられ、外部ホストからの制御により迷惑メール送信等の活動を行う。
＊3　The Official Microsoft Blog（http://blogs.technet.com/b/microsoft_blog/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx）。

のボットネットの活動低下が影響していると考えられます。そこで、上位8地域について、前年の同時期（2010年第1〜13週）からどのくらいの割合で変化したかを図-4に示します。

この図から、中国（CN）、日本（JP）、ロシア（RU）は、前年同時期の8割前後で、それほど迷惑メール送信量が低下していないことが分かります。これに対して、米国（US）、インド（IN）、ブラジル（BR）は5割以下に低下しているため、これらの地域にRustockボットネットが存在していたのではないかと考えられます。

ボットネットと迷惑メール送信数の関係については、日本のインターネット環境を考えることでも裏付けできます。これまで何度か述べてきたとおり、日本ではOP25B[*4]の広範囲な導入によって、元々ボットからの迷惑メール送信が少ないという状況でした。つまり、今回のRustockの活動停止については、日本はあまり影響を受けなかったため、前年同時期と比べて約8割という結果になり、実際にそれほど減少しなかったことになります。同様に、それほど低下しなかった中国（CN）、大幅に送信数を増加させたフィリピン（PH）については、少なくとも日本向けに送信されている迷惑メールが、Rustockボットネット経由ではなく別の手段を使っていると考えられます。前回のレポートでも触れたとおり、日本の迷惑メール送信事業者が、これらの地域を送信拠点としていることが何度か報道されています。地理的に離れているロシアについては、Rustockではない別のボットネットが広がっている可能性が高いのではないかと、現時点では考えています。

2.3 メールの技術動向

ここでは、メールに関わるさまざまな技術的な動向について解説します。今回も送信ドメイン認証技術の受信側の認証結果の動向について解説します。また、迷惑メール対策とIPv6アドレスの関係についても現状を整理します。

2.3.1 流量ベースのSPF認証結果割合

今回の調査期間（2011年1〜3月）に受信したメールのSPFによる認証結果の割合を図-5に示します。送信側のドメインがSPFレコードを宣言していないことを示す認証結果「none」の割合は、今回50.2%で、前回と同じ結果でした。認証結果が「pass」であった割合は28.6%で、前回から5%の増加となりました。逆に認証失敗を示す、「hardfail」、「softfail」、「neutral」の割合の合計が前回よりも4.7%減少しました。SPFの認証成功の増加は、迷惑メールの割合が減り、SPFを導入している正しい送信元からのメールの割合が増えたことによるものと考えられます。その一方で、全体の導入割合が増えていない理由は、SPFを導入しているドメイン名を送信者情報に使っている迷惑メールと、SPFを導入していない迷惑メールの両方が、同程度の割合であることが考えられます。つまり、少なくとも減少した分の迷惑メールについても、元々半分程度のドメインがSPFを導入していたことが分かります。認証失敗の割合が減少していることから、正規のドメイン名を詐称して利用していたことも考えられますが、迷惑メールの割合の低下を考えると、迷惑メールも堂々とSPFを導入し、認証をパスしているものが相当数あったと考えられます。

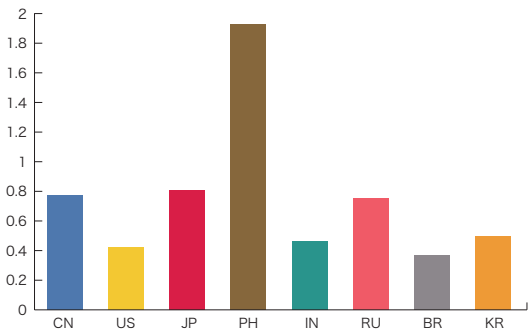

図-4　主要迷惑メール送信元地域の前年との比較

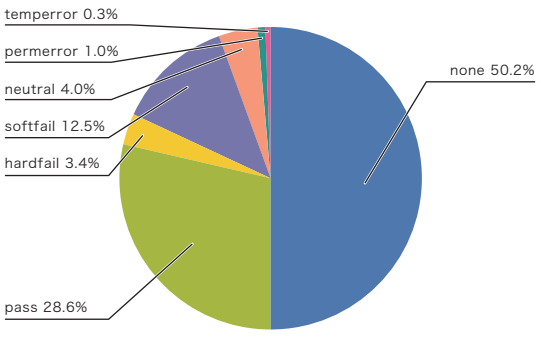

図-5　SPFによる認証結果の割合

＊4　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。

2.3.2 迷惑メール対策とIPv6

このレポートの執筆中であった4月15日に、通常申請で割り当てられるIPv4アドレスのAPNICとJPNICでの在庫が枯渇したとの発表[*5]がJPNICからありました。これにより、今後、IPv6アドレスの利用が増えることが予想されます。このため、ここでは迷惑メール対策とIPv6アドレスの関係を整理しておきます。

まず、送信ドメイン認証技術とIPv6アドレスの関係について整理しておきます。DKIM (DomainKeys Identified Mail) は、電子署名を利用して認証が行われ、送信元のIPアドレスには依存しないため、IPv6アドレスを利用したメールの送受信が行われても特に影響は受けません。SPFとSenderIDが利用するSPFレコードには、IPv6アドレスに対応した記述方法が既に仕様として含まれています。送信元のIPアドレスとしてIPv6を利用するときには、SPFレコードに機構 (mechanism) として「ip6」を付け、IPv6でのIPアドレスかネットワークアドレスを追加すれば問題ありません。

次に、迷惑メール対策として一般的に使われている手法についても、IPv6との関係を整理しておきます。迷惑メール対策として一般的に使われる機能に、メール内容の特徴によって迷惑メールを判定するコンテンツベースのものがあります。これらはメールの内容から迷惑メールを判定するため、IPv6の影響はほとんど受けません。

もう1つの迷惑メール対策手法として、メールの送信元のIPアドレスから迷惑メールを判定する方法があります。該当するIPアドレスをブラックリストを元に判断したり、警戒対象であることが判断できない送信元のIPアドレスからのメールに対しては送信の再試行を期待するグレーリスティング等の手法が、これにあたります。これらの手法は、IPv6アドレスに対応したデータベースを用意することで利用できそうに見えます。しかし、これには運用上の大きな問題点が潜んでいます。それは、IPv6でのアドレス空間がIPv4のものに比べてあまりにも広大すぎるという点です。技術的には、迷惑メール1通ごとに送信元のIPv6アドレスを変更して送信したとしても、十分に大量の迷惑メールを送信できてしまいます。IPアドレス個別に警戒対象かどうかを判断している従来のDNSBL等の手法では、迷惑メールの送信元をきちんと管理できない可能性が高いと思われます。したがって、ブラックリスト管理側でIPv6アドレスを個別に管理するのではなく、ある程度まとまったネットワークアドレス単位で管理することが望ましいと思います。しかし、あまり広い範囲でまとめてしまうと、その中に正規のメールサーバが含まれてしまう可能性があるので、注意が必要です。逆にIPv6アドレス全体を警戒対象として捉え、迷惑メール送信等をきちんと管理している正規のメールサーバのみを安全なものとして管理する、ホワイトリストによる運営方法も考えられます。しかし、インターネット上に正規のメールサーバがどれほどの数で存在しているかも未知数ですので、有為なIPアドレスが得られるまでには相当の試行錯誤が続く可能性があります。

IIJが提供するメールサービスの多くは、すでにIPv6アドレスを送信元とするメールの受信が可能になっています。今後は、これらのメールサービスの状況とともに、IPv6とメールの関係についても報告していきたいと考えています。

2.4 おわりに

このたびの東日本大震災で被害を受けられた皆様に謹んでお見舞い申し上げます。被災地の一日も早い復興を心よりお祈り申し上げます。災害時の情報伝達は、非常に重要になります。言うまでもなく、メールは、携帯電話の普及とともに、その即時性と蓄積型メッセージ交換という非同期性の両面を備えた有用な情報伝達手段の1つになっています。今回のような災害が発生した場合でも、情報伝達を担うインターネット、その上で広く使われているアプリケーションとしてのメールを、できるかぎり継続して利用できるよう、今後も携わっていきたいと考えています。

執筆者:
櫻庭 秀次 (さくらば しゅうじ)
IIJ サービス本部 アプリケーションサービス部 シニアエンジニア。メッセージングシステムに関する研究開発に従事。特に快適なメッセージング環境実現のため、社外関連組織との協調した各種活動を行う。MAAWGメンバ及びJEAGボードメンバ。迷惑メール対策推進協議会及び幹事会構成員、送信ドメイン認証技術WG主査。(財)インターネット協会 迷惑メール対策委員。総務省 迷惑メールへの対応の在り方に関する検討WG 構成員。

＊5　IPv4アドレスの在庫枯渇に関して (http://www.nic.ad.jp/ja/ip/ipv4pool/)。