2 メールテクニカルレポート

2.1 はじめに

メールテクニカルレポートでは、主にIIJがサービス提供している迷惑メールフィルタ機能の判定結果や、送信ドメイン認証技術による判定結果等、実際にインターネット上で流通しているメールを対象に分析し結果をまとめています。対象としている迷惑メールには、望まなくても一方的に送られてくるいわゆる広告宣伝メールやウイルスメール等が含まれいます。通常のメールと迷惑メールの流通量については、それぞれ曜日による変動が発生するために、一週間単位で集計し、その変化に着目して分析しています。

今回の調査は、2008年の第36週(9/1～7)から第52週(12/22～28)までの17週、119日間を対象にしました。今後は四半期ごとの、およそ13週間ごとに調査及び分析をし、情報提供をする予定です。また、迷惑メール対策に関連した技術の解説や、関連するトピックス等についても随時取り上げていきます。

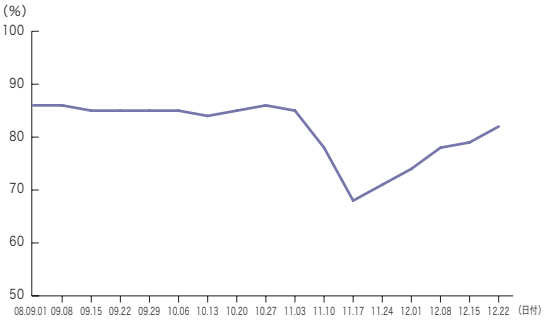

図-1　迷惑メールの割合

2.2 迷惑メールの動向

今回の調査では、迷惑メールの送信に大きく関わっていると言われていたMcColo社のネットワークが遮断されるという大きな出来事があり、その影響と考えられる大きな変動を観測しました。詳細については、後半で述べます。

2.2.1 迷惑メールの割合

第36週から第52週までの17週間について、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82.7%でした。割合が最も大きかったのは、第36週(9/1～7)の86.1%で、最も低かったのが第47週(11/17～23)の68.0%でした。この期間、迷惑メールの割合が最大で18.1%減少したことになりますが、メール受信数の実数値ではより大きく変化しています。全体のメール受信量が減っていても、通常のメール受信量もそれほど変化しない場合は、迷惑メールの受信量自体が18.1%減ったということにはなりません。この期間の迷惑メールの受信量は、第36週に比べて第47週は1/3近くまで大幅に減少しました。

McColo社のネットワークが遮断されたのが、米国時間の11月11日火曜日と言われています。我々の調査では、第46週(11/10～16)から割合が下がりはじめ、その次の週である第47週(11/17～23)が最も迷惑メールの割合が低くなったという結果になりました。時間的にもほぼ同期していることから、今回の迷惑メールの大幅な減少は、これが影響したものと考えられます。しかしながら、その次の第48週(11/24～30)から割合が増え始め、残念ながら2008年の末には81.7%まで上昇し、減少前の水準まで戻りつつあります。迷惑メール送信者は、既に別の送信手法を利用していると言えるでしょう。

迷惑メールの割合が、前回の2008年第23週から第35週(6/2～8/31)での調査の平均85.8%に比べ、約3.1%減少したのもこれが影響したものと考えられます。

2.2.2 迷惑メールの送信元

迷惑メールと判定されたメールの送信元について、同様の期間、調査・集計した結果を図-2に示します。

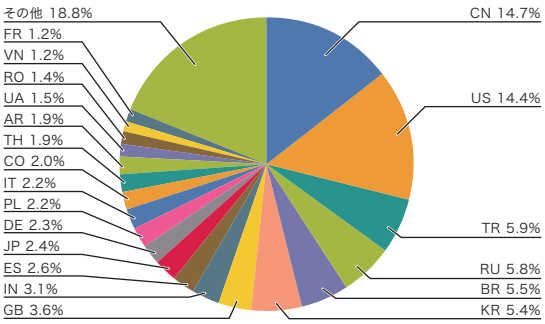

図-2　迷惑メールの送信元

日本に対する迷惑メールの送信元は、中国が1位で14.7%という結果になりました。前回12.9%で1位だった米国は、割合としては14.4%と増えましたが順位は2位となりました。3位以降は、トルコ(5.9%)、ロシア(5.8%)、ブラジル(5.5%)、韓国(5.4%)となり、それぞれ前回と同じ順位となりました。7位は英国(3.6%)、8位はインド(3.1%)となりましたが、これも前回と順位が入れ替わっただけですので、日本からみた迷惑メール送信主要国にそれほど変化はなかったと言えます。上位10カ国の割合の推移を図-3に示します。

図-3で特徴的な動きは、第46週(11/10〜16)から米国の割合が急激に下がり、中国が急激に増加している点です。米国以外にも、トルコやロシア等の上位国がこの時期に下がっていることから、これらの国ではマルウェアに感染したボットが多数存在している可能性があります。逆に、増加している中国や日本、変化が少ない韓国やブラジル等は、ボットの利用より、特定ホストから大量送信する従来的な方法を多用している可能性が考えられます。実際に過去の迷惑メール送信業者の検挙事例等からも、中国や韓国には日本の送信拠点が数多く存在するのではないかと言われています。また、2008年の最後(第52週)に中国に続いて2位となったブラジルにも今後は注意が必要です。

前回の調査と比べて大きく異なる点は、日本が前回の16位から大きく順位を上げ10位(2.4%)となったことです。割合としては2%台と変わりませんし、10位以降も2%〜1%の範囲ですので誤差の範囲と言えなくもありませんが、以下の要因が影響したと考えています。

■McColo社ネットワーク遮断の影響

前号でも触れたとおり、日本国内の主要ISPではOP25B[*1]が比較的普及していることから、ボット[*2]による迷惑メール送信が利用されにくいという特徴があります。そのため、日本発の迷惑メールの多くは、固定IPアドレスと思われる送信元が大部分となっています。

McColo社のネットワーク遮断によって影響を受けたのはボットネットだと言われています。第46週(11/10〜16)以降には、全体の迷惑メールの受信量が激減しましたが、送信国の割合としては日本の順位が上がってい

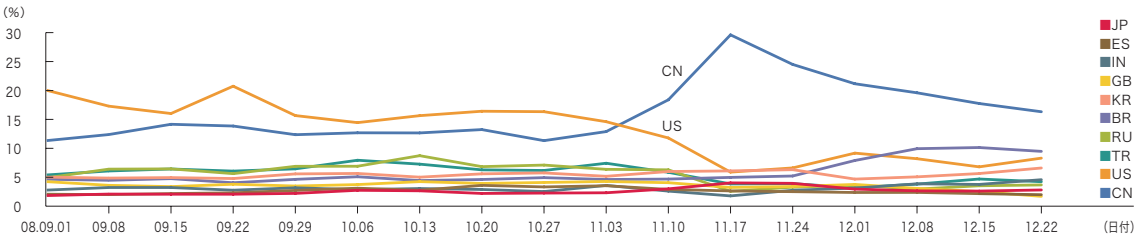

図-3　迷惑メール送信元の推移

＊1　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　不正なプログラム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)と呼ばれる。またその集合体をボットネット(Botnet)と呼ぶ。

ます。期間中、迷惑メールの割合が最も低かった第47週(11/17〜23)とその次の第48週(11/24〜30)には日本の順位が5位に上がっていますが、受信数自体は大きな変化はありませんでした。このことから、McColo社のネットワーク遮断によって影響を受けたのは明らかにボットネットからの迷惑メール送信であり、ボットネット経由の送信が少ない日本の順位が相対的に押し上げられたということが推測できます。

■バウンスメール(bounce mail)

日本発の迷惑メールと判断されたものを調べたところ、メールを正しく管理していると思われるドメインからの大量送信が何度か観測されました。調査した範囲では、その多くが宛先不明のメールに対するエラーメール、いわゆるバウンスメールと思われるものでした。つまり、送信者情報を詐称して送られたメールの多くが宛先不明で、それに対するエラーメールが送信者情報を詐称された側に返されているということになります。

バウンスメールを返している側は、宛先不明のものに対して規約どおりエラーとして返した結果、それが全く関係のない第三者側に迷惑をかけているということになります。元々の詐称されたメールの送信元は不明ですが、それが一旦、日本のメールサーバに届き、そこから送信されたバウンスメールが届いているため、受け取った側は、日本発の迷惑メールが大量に送られるように見えるという構造です。

2.2.3 迷惑メールの傾向

今回は、迷惑メールの動向にも大きな影響を与えたMcColo社のネットワーク切断について取り上げます。

ワシントンポスト紙のウェブ版[*3]によれば、ウェブホスティングのMcColo社のネットワークが2008年11月11日(米国時間)にオフラインになったと報じています。これは、McColo社にインターネット接続を提供している2社が接続を遮断したことによるものです。McColo社はカリフォルニア州サンノゼにあり、セキュリティ専門家に、数百万の不正なプログラムに感染させたPCであるボットをリモート管理し、メールを使った多くの違法な製品の販売に関与する国際的な組織として注目されていました。つまり、ボットネットの管理サーバ(Command & Controlサーバ)がMcColo社のホスティングサービス上に構築されていたということです。

運用していたボットネットの種類には、Mega-D、Srizbi、Rustock、Warezov等が挙げられています。McColo社のネットワークが遮断されたことにより、ボットを操るための指令が届かないためボットが活動できなくなり、迷惑メールの減少につながりました。

IIJの迷惑メールフィルタに関するパートナーであるMX Logic社[*4]によれば、Srizbiボットネットに関連するトラフィックは80%以上、Mega-Dボットネットにいたっては95%以上減少したと報告されています。

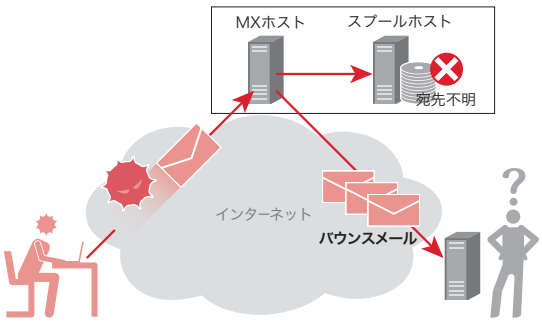

図-4　バウンスメール

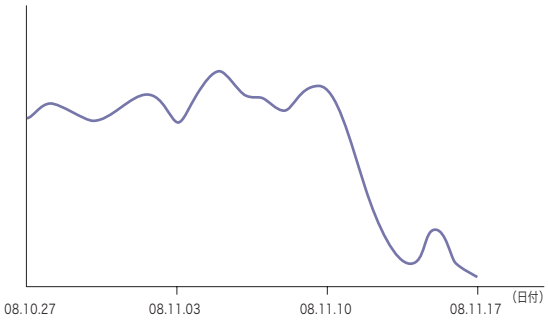

図-5　Srizbiボットネット関連トラフィックの推移

＊3　Host of Internet Spam Groups Is Cut Off(http://www.washingtonpost.com/wp-dyn/content/article/2008/11/12/AR2008111200658.html)。
＊4　MX Logic社のURL(http://www.mxlogic.com/)

同じような報告は、程度の差はありますが他のセキュリティベンダや迷惑メール対策団体等でも報告されており、IIJでも、迷惑メール量の急激な減少を確認しています。しかし、残念なことに、11月の下旬から迷惑メールの量は減少前の水準に戻りつつあり、多くのボットネットが既に別の管理サーバ(Command & Controlサーバ)に移っているとの情報もあります。

今回の遮断については、法的な観点やその効果の持続性について等、課題もいくつか残しましたが、有効な手段であれば効果が得られるという点、短い期間でもその効果を実感できたことの意義は非常に大きいと考えています。日本国内では普及したOP25Bが世界的に広がらないのは、その実施に対する諸々の困難さはありますが、それを導入することによって得られる効果が正しく理解されていないことも要因の一つです。

こういった事例を含め、何が有効な迷惑メール対策か、抜本的に迷惑メールを根絶させる方法について、IIJでは引き続き検討を行うと共に、MAAWG等の国際的な組織等で発信していきます。

2.3 メールの技術動向

2.3.1 送信ドメイン認証技術の動向

今回も、前回に引き続き送信ドメイン認証について解説します。WIDEプロジェクト[*5]とJPRSの共同研究による「jpドメイン」に対するSPFレコードの宣言率調査では、2009年1月時点で33.28%となり前回(2008年8月)に比べて8.84%上昇しました。

ドメインの種別として2番目に登録数の多い「co.jpドメイン」に関しては、37.7%と更に高い宣言率になっています。逆に言えば、それ以外のドメインが平均を下げており、全体の宣言率を向上させるには、企業以外の組織に対するSPFレコードの認知度の向上が必要と考えています。

前回は、メール受信側としてSPFの認証結果の推移を示しましたが、現在でも傾向はあまり変わっていません。実際のメール流量に対するSPFレコードを宣言したドメインからの受信量の割合は、WIDEプロジェクトの調査より低い結果になっています。迷惑メール送信者は、SPF宣言されていないドメインを送信者情報に使い、認証結果に基づくフィルタ処理を回避しているようです。

■ネットワークベースの送信ドメイン認証技術

送信ドメイン認証技術には、大きく分けて送信元のIPアドレスを元に判断するネットワークベースのものと、電子署名技術を用いるものがあります。前者のものとしては、SPF (Sender Policy Framework)と Sender IDがあり、IETF によってRFC 4408とRFC 4406として仕様が公開されています。今回は、これらの技術の違いと、共通するメール転送時の問題について解説します。

元々、Sender IDは、他の技術を取り込んだSPFの改良版として仕様が検討されていた技術であるため、主要部分はSPFとまったく同じ仕組みとなっています。類似した2つのRFC (Experimentalではありますが)が公開された背景には、知的所有権の問題が大きく影響しました。技術的な課題以外の要素によって、同じような技術規格が複数存在することになり、その普及にとっては大きなマイナスとなったと言えます。

ネットワークベースの送信ドメイン認証技術が利用する重要な要素に、認証の対象である送信者のドメイン名と、そのドメインが公開しているSPFレコードがあります。メール受信時の送信元IPアドレスが、SPFレコードのどの部分に含まれているかで認証結果は決まります。ドメインの管理者は、正しいメールの出口とそれ以外から出た場合の判断基準をSPFレコードに記述します。メール受信者は、受信したときの送信元のIPア

＊5　WIDEが公表しているSPF宣言率のデータ及び推移グラフ(http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)

ドレスが表明された正しい出口と合致しているかを確認(認証)します。(図-6参照)

この方式の注意点は、認証結果がメールの安全性を保証するものではないということです。認証が通ったということは、ただそのドメインから正しく送信されていることが確認できているだけであり、次に、ドメインの信頼性の判断が必要となってきます。最近では迷惑メール送信者が認証を通るようなSPFレコードを公開する例もありますので、こういった判断が重要になってきます。

■送信ドメイン

SPFとSender IDの違いのひとつに、送信者のドメインの取得方法があります。SPFでは主に配送上の送信者メールアドレス(Reverse-PathまたはMAIL FROM)のドメイン部分を利用します。Sender IDはSPFを含んでいますので、SPFと同じくMAIL FROMも利用できますが、PRA(Purported Responsible Address)も利用できます。PRAは、空でないメールのヘッダ情報の中から、「Resent-Sender」「Resent-From」「Sender」「From」の順番で探すことが決められています。

元々は、フィッシング対策等のために、メール受信者がMUA(いわゆるメーラ)で表示されるメールヘッダ上の情報を認証に利用することが望ましいという発想がありました。一方で、メールヘッダの情報を利用することは、メール配送のプロトコル(SMTP)の手順上、メール本文を受信するまで認証判断ができないという問題があります。SPFが利用するMAIL FROMは、メール本文より前に取得でき、一般にデータ量の多いメール本文を受信する前に認証できます。そのため、その後の処理継続について、より早い段階で判断できることになります。

■SPFレコード

SPFもSender IDもほぼ同じSPFレコードを利用します。SPFレコードは、SPF資源レコード(コード99)もしくはTXT(テキスト)資源レコード(コード16)上に情報を格納します。テキスト形式で、IPアドレスやホスト情報等を記述し、メールの出口を表明します。

Sender IDでは、先頭のバージョン番号部分が異なり、「v=spf1」部分が「spf2.0/pra」となります。「pra」部分は、「mfrom」または「pra,mfrom」と記述することもでき、送信者情報をPRAから取得するのかMAIL FROMなのか、その両方なのかをSPFレコード宣言側(メール送信側)が選択できます。

また、Sender IDはSPFのSPFレコードだけであっても、それを「spf2.0/mfrom,pra」と同等に解釈することになっています。つまり、メール送信側がどちらのSPFレコードを表明していても、メール受信側はSender IDとして認証できます。逆に、SPFだけで認証している場合には、Sender ID用のSPFレコードは解釈できません。現在のオープンソース*6のいくつかの実装では、SPFとSender ID両方の認証を同時に行うようになっています。

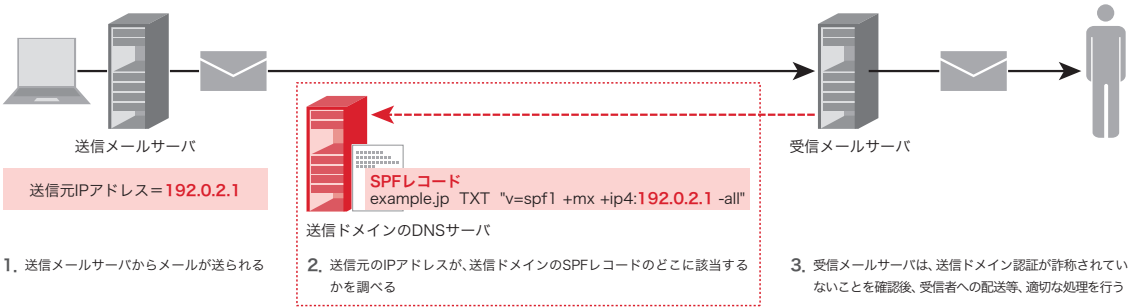

図-6　ネットワークベースの送信ドメイン認証技術

*6　IIJが無償公開しているENMA(http://www.iij.ad.jp/news/pressrelease/2008/0828.html)も、SPFとSenderIDの双方に対応している。

■転送問題

ネットワークベースの送信ドメイン認証技術には、メールの利用形態によっては正しく認証が行えない場合があります。これは、直近の送信元のIPアドレスでしか認証できないことによるものです。

例えば、複数のメールアドレスを保有していても、特定のメールボックスしか利用しないために、それ以外のメールをすべてそのメールボックスに転送するような場合です。外出先でメールを確認するために自身のメールを携帯電話に転送設定する場合でも、携帯電話側では正しく認証できない可能性が高いです。

認証が失敗してしまう原因には、メール転送時に元々の送り元のMAIL FROMをそのまま利用してしまう現在のMTAの実装があります。この場合、転送先でSPF認証をしようとしてもドメイン名は変わらず、送信元が変更されています。Sender IDのPRAの場合、転送時にPRAで参照されるヘッダに転送元のドメインを設定すれば良いですが、こういった転送処理を実施するMTAはあまり多くないようです。正しくヘッダを追加しなければ、転送先で、Sender IDのPRAの認証は失敗します。

しかし、こうした転送時の認証の不備のみを問題としても迷惑メール対策は進展しません。ネットワークベースの送信ドメイン認証技術には、導入の手軽さと普及率の高さという大きな利点があります。認証の結果だけで機械的に不正なメールかどうかを判断するのではなく、送信元を確認するツールの一つとして利用することが大事です。

転送問題に関しては、転送者と転送先のメール受信者は同じ人物である場合が多いので、運用の工夫で改善が可能だと考えています。重要な局面で認証技術が必要な場合は、電子署名技術を用いたDKIM（DomainKeys Identified Mail、RFC 4871）を利用するという方法もあります。詳細については、次回以降で解説します。

■バウンスメールの抑制

日本発の迷惑メール増加の原因の一つとして、バウンスメールの増加があることについては既に報告しました。元々、バウンスメールは、返すべき相手が正しい送信者であることを前提に設計されています。よって、送信ドメイン認証でパスしない送信者にまで、わざわざバウンスする必要はありません。

メール受信時に送信ドメイン認証を行い、それをバウンスメールの送信処理時に参照できれば、正しい送信者にだけバウンスメールを返すことが可能になります。認証に失敗した不正な送信者へのバウンスメールは破棄することができます。こういった処理が普及すれば、日本発の迷惑メールがより減少する可能性があります。

2.4 おわりに

今回のメールテクニカルレポートでは、迷惑メールの動向として迷惑メールの割合の変化とその要因となったボットネット封じ込めの動きについて解説しました。この大きな変化により、それぞれの地域での送信手法をある程度、把握することができました。

また、前回に引き続いて迷惑メール対策として重要な技術のひとつである送信ドメイン認証技術について、特に比較的導入が容易なネットワークベースのSPFとSender IDについて解説しました。また、普及の観点からこれまであまり触れてこなかった転送問題についても今回はとりあげ、その原因について解説しました。それぞれの利点をうまく活用し、引き続き普及していくことを期待しています。

今後も迷惑メール対策に有効な技術について、その利点とともに残されている課題についても取り上げ、解決に努力し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 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。メールシステムの企画及び調査に従事。特に快適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。迷惑メール対策推進協議会及び幹事会構成員。