アジア地域を迷惑メール送信元にし続けないために、今すべきことは何か

今回は、2009年第27週〜第39週に検知した迷惑メールの割合の推移や送信元地域の分析とともに、迷惑メール対策のために行われている国際的な活動の状況と、送信ドメイン認証技術の普及度調査の結果を解説します。

2.1 はじめに

ここでは、迷惑メールの最新動向、迷惑メール対策に関連する技術情報、IIJが深く関わっているさまざまな活動などについてまとめています。迷惑メールの動向については、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機能から得た各種情報を元に、さまざまな視点で分析を行った結果を示します。ただし、メールの流量は、提供しているサービスの対象によって曜日ごとに変動します。このため、ここでは、よりよく傾向を把握できるようにするため、一週間単位でデータを集計し、その変化に着目して分析しています。今回の調査は、2009年第27週(2009年6月29日〜7月5日)から第39週(2009年9月21日〜9月27日)までの13週間、延べ91日間を対象にしています。また、前号(Vol.4)でIIR発行開始から1年が経過しましたので、これまでのデータを一部まとめて示します。

迷惑メール対策の動向としては、国際的な取り組みに関する話題を紹介します。IIJは、これまでもMAAWG(Messaging Anti-Abuse Working Group)を中心に、国際的な議論の場で活動してきました。今回は、これ以外の組織や取り組みについて、その概要を報告します。また、メールの技術動向としては、前号に続いて送信ドメイン認証技術を取り上げ、実際の普及がどの程度まで進んでいるのかを報告します。

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、迷惑メールフィルタによってIIJが検知した迷惑メールの割合の推移と、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。今回の調査対象である2009年第27週から第39週を含めた、過去1年間69週分での推移を図-1に示します。

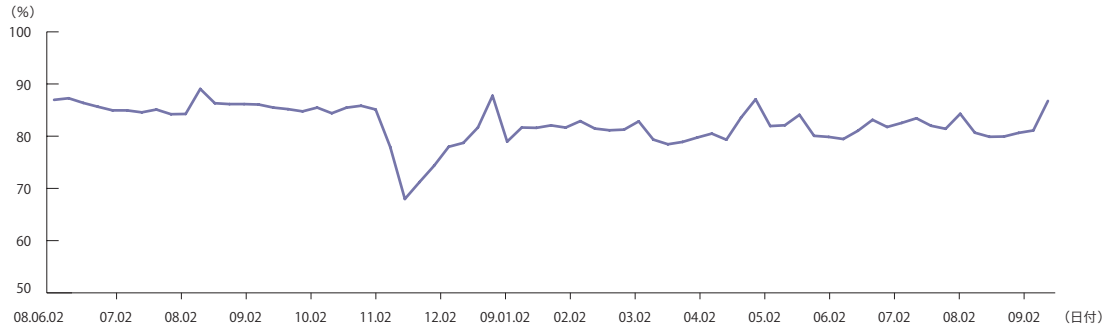

図-1 迷惑メールの割合の推移

2.2.1 迷惑メールの割合の推移

2009年第27週から第39週までの91日間で検出した迷惑メールの割合は、平均82.2%でした。前回(2009年第14～26週)の平均値が81.6%でしたので、0.6%微増したことになります。この期間もっとも検出割合が高かった週は、第39週(2009年9月21日～9月27日)で、その値は86.7%でした。第39週には、連休期間が含まれているため、通常のメール流量が減少したことによる影響が表れたものと考えます。ただし、これまでの経験上から、秋以降に迷惑メール量が増加する傾向があるため、今後も注意が必要だと考えています。

最近では、不正プログラムを添付ファイルとして送りつける迷惑メールがたびたび増加し、不正プログラムの亜種の更新頻度も高く、ウイルス検知ソフトウェアが対応できていないことがあります。このため、添付ファイルを不用意に解凍したり実行したりしない等の注意が必要です。

2.2.2 迷惑メールの送信元

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、前回と同様にブラジル(BR)で、全体の12.1%を占めていました。ブラジルは、前回に引き続いて1位であり、割合も0.3%増加しているため、迷惑メール送信が多い原因やその対策などの検討が必要と考えています。これ以外の上位地域には若干の変動がありました。これまで常に最上位にあった米国(US)が7.1%と前回から4.3%減少し、4位に順位を下げています。前回報告したように、FTC (米連邦取引委員会)など消費者行政に関する執行機関の対策活動が効果を上げているのかもしれません。

中国(CN)が9.8%、韓国(KR)が7.2%と、両国とも依然として大きな割合を占め、それぞれ2位と3位になっています。5.6%で6位のベトナム(VN)と合わせて、アジア地域の迷惑メール送信割合を押し上げる要因にもなっています。また、ベトナムは、前回の14位から急速に順位を上げているため今後注意が必要です。ベトナムやブラジルに限らず、経済発展が進むにつれてネットワークなどのインフラが整備されると、迷惑メールの送信元割合が増えるのは世界的な傾向です。6.0%で5位のインド(IN)も前回とほぼ同水準であり、同様のことが言えると推測しています。

今回、日本(JP)は3.1%で9位でした。前回からは、割合も順位も上がっています。割合が増えた原因はいくつか考えられますが、そのひとつとしていわゆるエラーメールの受信が目立ちました。迷惑メールと判定した日本発のメールの中に、主要ISPのメールサーバを送信元とするものが多くありました。ただし、配送上の送信元の情報(エンベロープFrom)や送信期間等から、その大部分が宛先不明メールに対するエラーメール、つまりバウンスメールであったと判断しています。

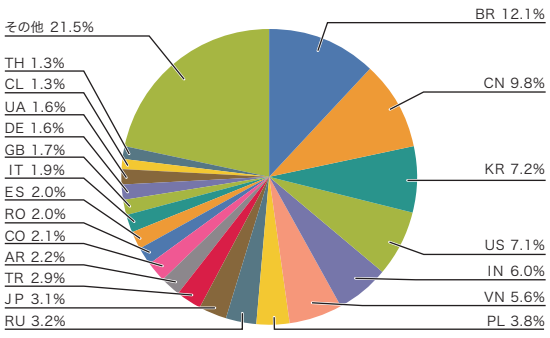

図-2　迷惑メール送信元地域

こういった事例は、IIJの顧客のドメイン名が、迷惑メールの送信元情報として悪用されたことによって発生します。一般的に、このような悪用をドメインの管理側で防ぐことは難しいです。ただし、これまでのIIRで紹介してきた送信ドメイン認証技術を送信側に導入することが、その対策手法の1つとなります。また、メール受信側でも、送信ドメイン認証を行うことで、送信者情報に示されているドメインが正しいメールの出口から送信されたものであるかどうかを判断することも必要になってきます。送信者情報として不正なドメイン名を利用しているメールに関しては、バウンスメールを返さない等の技術を導入することで、こういった事例は防ぐことができます。

図-3に上位6カ国(ブラジル、米国、中国, 韓国、ベトナム、インド)に日本を加えた 7カ国の迷惑メール送信元割合の推移を示します。

この期間の開始当初は、ベトナムは日本より迷惑メールの送信割合が低い国でしたが、その後急速に順位を上げ、8月以降は4位から5位に位置するなど迷惑メール送信元の上位国になっています。

これにより、全体としての順位も押し上げられ、今回の調査期間の全体でも 6位となりました。

このように図-3からは、それぞれの送信元からの迷惑メール量に、時期的な変動があることが読み取れます。しかし、その変動の内容についても同じような動きをしているわけではありません。

例えば韓国(KR)は、今回の調査期間中では第34週(2009年8月17日週)が送信元の割合が最も高く、10%を超えています。

この週での増加分は、同じ送信元(IP アドレス)から大量に送信している送信元が増えたことにより全体として、送信数が増えていました。

一方ブラジル(BR)は、それぞれの週で送信割合が多少変動していますが、ブラジルから送信された迷惑メールだけに着目すると、大量に送信している送信元の割合も、例えば1週間に1通だけしか送信しない少量の送信元の割合とも、あまり変動がありませんでした。

これらのことから、韓国から日本への迷惑メール送信は、大量に送信する特定の送信元の送信数が大きく影響していることがわかり、ブラジル等の地域は、大量に送信する送信元が少ないことから、不正プログラムに感染させられたボットからの送信が多いことが推測できます。

大量に送信する送信元に対しては、それぞれに対して法的措置によってある程度改善することが期待できますが、少量送信元が多数存在する場合には法的措置にも限界があります。

この様に、迷惑メール送信を抑制するには、それぞれの地域及び送信元の特性に応じた対応が必要になってきます。

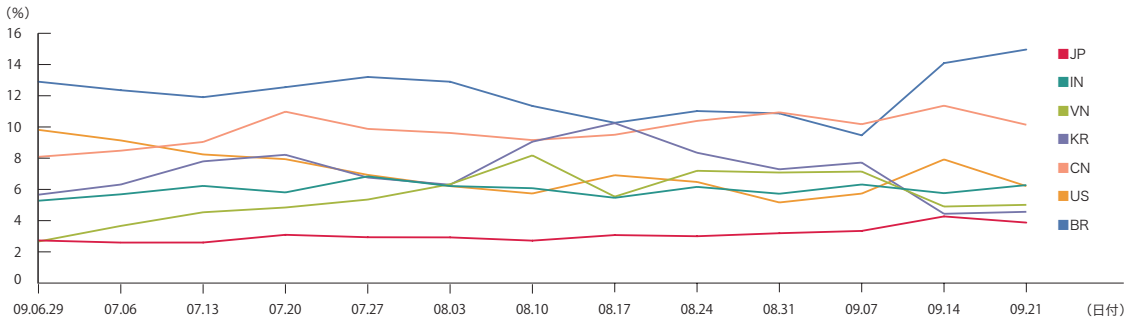

図-3　迷惑メール送信元の推移

2.2.3 国際的な迷惑メール対策活動

これまで示してきた迷惑メールの送信元の分析結果からも明らかなように、日本に向けた迷惑メールの大部分が海外から送信されたものです。特にアジア地域は、世界的にも迷惑メールの送信元地域として不名誉な結果がセキュリティベンダ等によって示されています[*1]。

アジア地域を対象とした、迷惑メール対策のための民間主体の組織に、APCAUCE (Asia Pacific Coalition Against Unsolicited Commercial Email)があります。APCAUCEは、北米を中心としたCAUCE (Coalition Against Unsolicited Commercial Email)のアジア地域版という位置づけで、筆者は2006年と2007年に会合に参加し、日本での取り組みを紹介してきました。しかし、残念ながら2007年のインドでの会合以降、2年間会合が開催されていません。このため、APを接頭語に持ついくつかのアジア地域組織の情報交換会合であるAP*Retreat[*2]会合が、APNIC 28ミーティングに合わせて北京で開催されました。ただし、このときも残念ながらAPCUACEからの参加はありませんでした。しかし、迷惑メール問題は重要なテーマであることから、AP*Retreatの共同議長らの協力により、対策の取り組み状況について日本と開催地の中国から発表が行われました。

こういったボランティアベースの組織は、モデレータの努力に大きく依存してしまう傾向にあり、会合の開催が不定期になることはある意味やむを得ないことかもしれません。しかし、アジア地域での迷惑メール対策は急務であり、日本の代表メンバである(財)インターネット協会などを中心に、まず来年の開催を目指して検討を進めています。

グローバルな民間組織には、前回(Vol.4)のインターネットトピックスで紹介したMAAWGがあります。現状は、参加者が欧米と筆者ら日本などの一部地域であり、アジア地域からの参加者があまり多くありません。MAAWGの会合は、開催地が北米や欧州であり地理的になかなか参加が難しい面もあるため、まずアジア地域での関係者による会合が必要ではないかと考えています。

行政府を中心とした組織としては、グローバルなものとしてLAP[*3]があります。LAPは、執行当局間の情報共有や連携、官民対話の促進等を目的として2004年に合意された行動計画を元に、毎年定期的に会合が開催されています。2007年には、MAAWG、CNSA(Contact Network of Spam Enforcement Authorities)との合同会合も開催されました。また、2009年10月7日から10月10日の3日間、ポルトガルのリスボンにおいて、CNSAとの5回目の合同会合も開催されています。日本からはメンバである総務省が参加し、筆者と(財)日本データ通信協会を含めて日本の取り組みを紹介しました[*4]。

LAPの会合では、各国の迷惑メールに関連する法律の紹介や執行状況、迷惑メールに対する取り組み等が報告されます。筆者も含め民間からも、ドイツのISPの団体であるecoやMAAWGから活動の紹介や今後検討していく法執行機関との協調に関する発表がありました。米国のFTCからは、前回紹介したPricewert社のネットワーク遮断の経緯についての紹介もありました。

＊1　例えばソフォス社によるスパム送信元の大陸別調査では、アジアが全体の約3分の1となっている(http://www.sophos.com/pressoffice/news/articles/2009/07/dirtydozenq209.html)
＊2　AP*Retreat会合の概要はWebサイトを参照(http://www.apstar.org/)
＊3　LAP: London Action Plan(http://www.londonactionplan.org/)
＊4　Workshop CNSA-LAP “Spam-Fighting” (http://www.anacom.pt/render.jsp?contentId=962326)

LAPには、アジアパシフィックからオーストラリアやニュージーランドなどが積極的に参加しています。また、今回、香港、台湾、マレーシアからの参加もあり、比較的アジアからの行政機関の参加は多いようです。同様に、アジアパシフィック地域の行政機関の集まりとして、ソウル-メルボルン スパム対策のための多国間MoU(Memorandum of Understanding)[*5]が2005年に合意され、関係国間で会合が開催されています。日本からは総務省が参加しており、2008年3月には東京で会合が開かれています。

行政府組織間では、こういった組織により定期的に情報交換が行われています。実際に効果を上げるためには、法執行を着実に行うこともちろん大切ですが、ボットネットなど高度化する迷惑メール送信手法に対抗するために、直接的な技術対策も重要です。迷惑メール対策を効果的に行うためには、民間と行政府が連携し、技術面と法執行面の両面が協調し対策を進めて行くことが必要になります。また、日本からの迷惑メール送信がOP25B (Outbound Port 25 Blocking)等の技術的な対策により難しくなり、海外、特にアジア地域に拠点を設けて迷惑メールを送信していると考えられています。こういった送信拠点を無くすためにも、アジア地域で行政府組織と協力して対応をしていくことが重要になっています。

2.3 メールの技術動向

2.3.1 送信ドメイン認証技術の普及状況

これまで送信ドメイン認証技術に関して、ネットワークベースのSPF/SenderIDや、電子署名技術を利用したDKIM技術を紹介してきました。また、普及状況については、WIDEプロジェクトの調査結果[*6]を示し、特にSPFの送信側導入が順調に進んでいることも紹介しました。

今回は、実際に流れているメールにおいて、送信ドメイン認証技術がどの程度普及しているかを調査した結果を紹介します。IIJでは、2005年から送信ドメイン認証技術を導入し[*7]、これまでにSPFに加えてDKIMも順次サービスに導入する等、積極的な取り組みを続けてきています。

IIJが提供するメールサービスの一部ですが、メール受信時の認証結果の割合を図-4に示します。

調査期間は2009年9月いっぱいです。受信したメールのうち、送信者情報に示されたドメイン名をSPF認証した結果、56.2%が“none”でした。これは、受信メールの43.8%のドメインがSPFレコードを宣言していたことを示しています。WIDEでの調査では、2009年10月

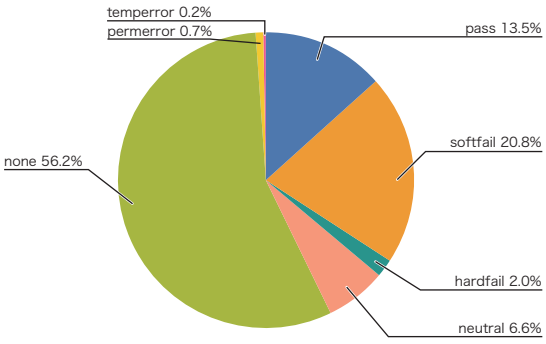

図-4　メール受信時の認証結果(SPF)

＊5　Seoul-Melbourne Multilateral Memorandum of Understanding on Cooperation in Countering Spam(http://www.sm-mou.org/)
＊6　WIDEが公表している送信ドメイン認証技術の普及率の調査結果(http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)
＊7　IIJ、送信ドメイン認証技術の導入を開始(http://www.iij.ad.jp/news/pressrelease/2005/0317.html)

時点での“jp”ドメインの宣言率は36.8%ですので、実際の流量ベースではそれより多いという結果になります。もちろん、受信メールの送信側ドメインには、“jp”以外にも“com”や“net”等、多様なTLD（Top Level Domain）を使っているわけですが、日本での受信メールの分析結果としては比較的SPFが使われていると言えると思います。

SPFの認証結果の割合で、“pass”が13.5%、“softfail”や“hardfail”といった認証に失敗した割合が29.4%となっています。このことから、正規のメールサーバから送信されたメールよりも、送信者情報を詐称したメールのほうが多かったと推測できます。迷惑メールの受信割合が80%を超えている状況では、ある程度納得できる割合です。SPFの場合、転送問題など誤判定の問題があるため、慎重な運用が必要になります。ただし、SPFの宣言率と利用率がこのように高い状況では、SPF認証結果によるある程度のふるい分けは、非常に効果がある手法の1つになると言えます。

次にDKIMの認証結果について図-5に示します。

調査期間は、SPFと同じく2009年9月いっぱいです。受信メール全体に対して、何らかのDKIMに対応した送信者からのメールは0.8%という結果でした。DKIMの場合、送信側の導入がSPFに比べてコスト高になる等の点から、あまり普及していないことが分かります。ただし、DKIMは、ネットワークベースのSPF/SenderIDに比べて比較的誤判定の問題が少ないため、今後より重要なメールに利用されていくと期待しています。受信側の認証コストは、SPFもDKIMも機能追加という点では同じであるため、DKIMに関しては受信側の普及をSPFの受信側認証と同じように進めて行くことが重要だと考えています。

2.4 おわりに

今回のメッセージングテクノロジーでは、迷惑メールの動向として、迷惑メールの判定割合の推移と送信元の分布について報告しました。さらに、迷惑メール対策として重要な国際協調に関して、民間や行政府組織間での会合情報や取り組みを、グローバルや日本が属するアジアパシフィック地域のそれぞれについて紹介しました。

IIJは、IIRに示すようなデータや技術を国際会議の場でも紹介し、それぞれの地域での取り組みや対策の促進を行っています。今後も、さまざまな場で積極的に迷惑メール対策に取り組んでいきます。

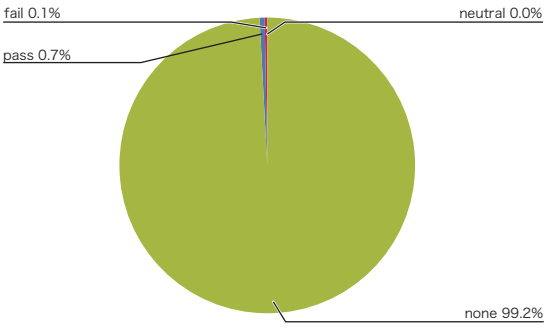

図-5　メール受信時の認証結果（DKIM）

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。（財）インターネット協会 迷惑メール対策委員。