4 メッセージングテクノロジー

本レポートはこれまで「メールテクニカルレポート」として発行していたものです。今号より名称を「メッセージングテクノロジー」と変更いたします。

4.1 はじめに

メッセージングテクノロジーでは、迷惑メールの最新動向や迷惑メール対策に関連する技術等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られる各種情報を元に様々な分析を行い、結果を公表しています。メールの流量は平日と休日の違いなど、曜日ごとの変動があるため、より傾向を把握しやすいように1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年の第14週(2009/03/30〜2009/04/05)から第26週(2009/06/22〜2009/06/28)までの13週、91日間を対象にしました。

メールの技術動向としては、送信ドメイン認証技術の受信側の導入状況とDKIMの利用方法の例を解説しています。

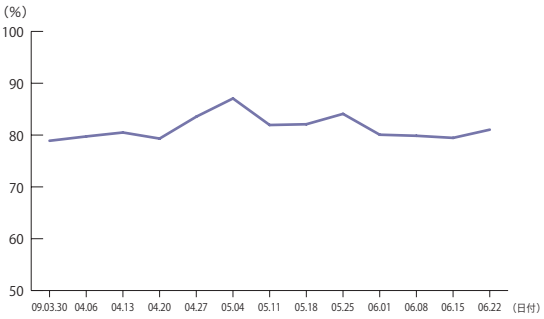

図-1　迷惑メールの割合

4.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJが提供する迷惑メールフィルタ機能によって検知され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。

4.2.1 迷惑メールの割合

2009年第14週から第26週までの91日間について週ごとの迷惑メールの割合の推移を図-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は、平均して81.6%でした。平均値としては前回(81.5%)とほぼ同水準でしたが、この期間の割合の推移には幾つか特徴的な変動がみられました。最も割合が高かったのは、第19週(2009/05/04〜2009/05/10)の87.1%でした。

これまでの傾向と同様に、この期間は5月の連休を含んでいたため、業務としての一般的なメール量が少なくなり、これにより相対的に迷惑メールの割合が高くなりました。しかし、この時期から迷惑メールの受信量そのものも急激に増加しています。特に、第18週(2009/04/27週)から第22週(2009/05/25週)にかけて迷惑メール量が増え、割合としても80%を超える高いレベルで推移しました。

その後、第23週(2009/06/01週)から迷惑メール量が若干減少傾向になりました。この時期の2009年6月4日に米連邦取引委員会(FTC)から発表された内容によれば[*1]、スパイウェアやフィッシング、児童ポルノなどの温床になっていると言われている、ISPのPricewert社のネットワークを遮断したと報告されています。Pricewert社は、3FNやAPS Telecomといった名義でのISP事業も行っており、昨年11月に遮断されたMcColo社[*2]と同様に、ボットネットの管理サーバ(Command & Control サーバ)も置かれていたと言われています。Pricewert社のネットワークが遮断されたことにより、ボットネットの活動が弱まり、迷惑メール量も減少したものと考えられます。しかし、今回はMcColo社のケースのような劇的な減少[*3]は見られな

＊1　http://www.ftc.gov/opa/2009/06/3fn.shtm
＊2　IIR vol.2（http://www.iij.ad.jp/development/iir/pdf/iir_vol02_mail.pdf）で解説
＊3　2008年第47週(11/17〜23)に迷惑メールの割合が68.0%まで減少

かったことから、対象となるボットネットの規模が小さかったか、送信者が事前に状況を察知してすでにネットワーク遮断に対する何らかの対策を講じた可能性が考えられます。

4.2.2 迷惑メールの送信元

この期間の迷惑メール送付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1位は、前回と同様にブラジル（BR）で、全体の11.8%を占めていました。前回（vol.3）が11.3%でしたので、微増したことになります。2位は米国（US）の11.4%で、前回（vol.3、10.9%）、前々回（vol.2、14.4%）と同じ順位でした。

今回の調査結果では、上位2カ国と3位以降に若干の開きがありました。3位は中国（CN、6.9%）で、4位は韓国（KR、5.6%）、5位はトルコ（TR、5.4%）、6位はインド（IN、5.3%）となりました。前回の調査結果と比べると、それぞれ若干の順位の入れ替えはありましたが、いずれも6位以内にすべて残ったままという結果になりました。日本（JP、2.6%）は前回と同様に11位でした。

これら6カ国に日本を加えた7カ国について、週単位での割合の推移を図-3に示します。ブラジルはいずれの週も高い割合で推移していますが、米国は5月中旬以降に割合を下げていることがわかります。中国は前々回（vol.2）で1位になって以降、割合が若干下がっていましたが、6月以降から高いレベルに戻りつつあり、再度注意が必要です。

日本に送られてくる迷惑メールの大部分が海外から送信されていることから、引き続き迷惑メール対策の国際連携が重要であると考えています。

4.2.3 迷惑メール対策の国際的な動向

これまで示してきたデータからもわかるように、迷惑メールの送信量は依然として高いレベルで推移しています。これは日本だけではなく世界的にも同様の傾向となっています。その送信元の多くは、一般ユーザのPCをマルウェアに感染させ、ネットワークの外部から操作する、ボットであると言われています。

日本では、一般ユーザが利用する動的IPアドレスから、外部ネットワークへの直接のメール送信を制限するOP25B[*4]を普及させたことにより、こういったボットを利用した、迷惑メール送信ができない環境を構築してきました。元々 OP25Bは、日本が最初に導入した技術ではなく、大手を含む米国のISP数社が導入していた技術です。国際的な迷惑メールの対策団体であるMAAWG[*5]が発足後に、迷惑メール送信側の対策として、有効な技術の一つと注目されました。日本の

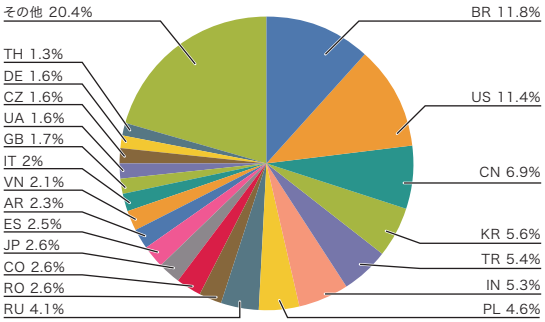

図-2　迷惑メールの送信元

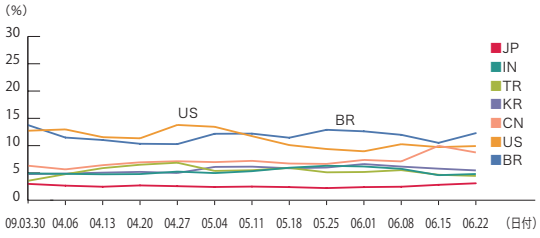

図-3　迷惑メール送信元の推移

＊4　Outbound Port 25 Blocking
＊5　MAAWG（Messaging Anti-Abuse Working Group）についてはインターネットトピックスを参照

JEAG[*6]で議論を重ねた結果、リコメンデーション（提言書）を発表[*7]し、これにより日本国内で急速に浸透しました。

OP25Bをより広範囲な地域に広めることによって、日本が受信する海外からの迷惑メールを減らすことができるはずです。そのため、IIJではMAAWGなどの国際会議の場や、政府と協調した活動を通して他国に対して、その有効性と技術概要を説き、導入を促す努力を継続してきました。その結果、一部の地域では導入が進みましたが、多くの地域では幾つかの理由により、導入がなかなか進んでいません。その詳細については、別の機会に解説したいと考えていますが、引き続きOP25Bの導入を促していきたいと考えています。

送信側の迷惑メール対策の動向としては、2008年11月のMcColo社、2009年6月のPricewert社のネットワーク遮断と続いたように、米国ではボットネットの管理元と思われるネットワークを遮断する動きが続いています。確かに、個別のボットにそれぞれ対処していくよりは、ボットに対して指令を送っている、管理元からの通信を遮断する手法の方が、一時的には大きな効果が得られます。しかしながら、今回のPricewert社の効果が限定的であったように、迷惑メールの送信側であるボットネットの管理者は、対応策を施し、既に新たな技術を導入している可能性があります。実際に、特定の管理元を持たずに、Peer-To-Peer技術を使って指令を伝播させていく、新たなボットネットの存在については以前から報告されていました[*8]。迷惑メール送信が、ビジネスとして成り立っている間は、こういった送信手法の高度化は続いていくものと考えられます。

送信側の対策として、最近ではWalled Garden[*9]という手法を導入する通信事業者も出てきています。Walled Gardenは、迷惑メール送信などを行っていると考えられるユーザの通信を、直接インターネットへ流さずに、特定の場所に囲い込む手法です。これにより、ボットの挙動を解析したり、マルウェア感染等により、意図せず不正な通信を行っている一般ユーザへ、注意喚起を行うことによって、セキュリティ対策を実施してもらうことができます。例えば、全てのウェブアクセス（HTTP/HTTPS）を特定のページに誘導させ、そのページでウィンドウズアップデートの実施を促したり、アンチウイルスソフトェアの実行を可能にして、PCがクリーンになるまでインターネットへ接続できないようにします。しかしWalled Gardenの手法には、怪しい挙動をしている通信元の特定や、Walled Gardenに誘導した利用者からの、問い合わせに対応する体制の整備等、課題も多くあります。

OP25Bは、迷惑メール送信については抑制できますが、例えば、ボットを利用したDDoS攻撃には対応できません。最近、米国や韓国の政府系ウェブサイトが閲覧できなくなるという事象が発生しましたが、この攻撃元にボットネットが使われているとの報道もあります。そのため、OP25Bの導入で安心することなく、Walled Gardenの手法も組み合わせることにより、クリーンなネットワーク環境を維持する努力も必要と考えています。

＊6　JEAG（Japan Email Anti-Abuse Group）は、2005年3月に主要ISPや携帯電話事業者を中心に創設された、迷惑メール対策のためのワーキンググループ（http://www.iij.ad.jp/news/pressrelease/2005/0315.html）
＊7　迷惑メール対策グループJEAGにおけるリコメンデーションの策定について（http://www.iij.ad.jp/news/pressrelease/2006/0223.html）
＊8　HotBots'07（http://www.usenix.org/events/hotbots07/tech/）
＊9　MAAWGではWalled Gardenに関するベストプラクティスを発表しています（http://www.maawg.org/about/whitepapers/MAAWG_Walled_Garden_BP_2007-09.pdf）

4.3 メールの技術動向

4.3.1 送信ドメイン認証技術の動向

日本のドメイン("jp"ドメイン)での送信ドメイン認証技術の、送信側での導入状況については、これまでも何度か引用してきたWIDEプロジェクトの調査結果[*10]があります。これにより、送信側の導入率、特にSPFレコードの宣言率の高さ(2009年5月時点で34.77%)を確認することができます。一方、メール受信側での、送信ドメイン認証技術の導入状況はどの程度進んでいるのでしょうか。

財団法人日本データ通信協会では、ISPや携帯電話事業者等、メールサービスを広く一般ユーザに提供している事業者を対象に、送信ドメイン認証技術の導入状況について調査を行い、結果を公表しています[*11]。調査結果によれば、2009年7月2日時点で、調査対象41社のうち、SPF(Sender Policy Framework)あるいはSenderIDの、受信側の認証を行っている事業者は13社となりました。割合としては約31.7%になりますが、対象をISPに限定すると約22.6%で、より低い普及率となります。DKIMの受信側の導入状況は、さらに低く約14.6%となっています。

今回の調査対象となっていない事業者は数多くあり、それぞれ調査対象でもメールの流量やアカウント数等の状況も異なるため、単純に受信側の送信ドメイン認証技術の普及率を示すことにはなりません。しかし、調査対象が通信事業者であることを考えると、「意外に少ない」というのが率直な感想です。受信側の認証を行うためには、新たな機能追加が必要になりますので、単純に比較はできませんが、送信側の普及率の高さと比較すると明らかに見劣りします。受信側の導入を促進させるためには、導入による効果や利点をより明確に示す必要があると考えています。

なお、今回の調査では個人系のメールサービスを対象としており、IIJではIIJ4U、IIJmioが対象のサービスとなります。そのため、DKIMの受信側の認証が未対応という結果になっていますが、IIJではSecureMXサービスで標準機能として DKIMの受信側認証を提供しており、これまで長い間、運用実績を持っています。現在この機能を個人系のサービスにも提供する準備を進めていることを補足しておきます。

4.3.2 DKIMの利用について

前回は、DKIMの認証の仕組みと送信側、受信側それぞれでの処理の概要について説明しました。今回は、DKIMの利点やその応用面について解説します。

DKIMは、秘密鍵を持っている送信者でなければ、作り出すことができない電子署名をメールに添付することにより、メールの送り手を認証します。電子署名は、メールの本文及びヘッダから作成されますので、これらの元になる情報が変更されない限り、署名を検証する公開鍵が入手可能ならば、いつでも検証することができます。そのため、ネットワークベースのSPF/SenderIDと違い、メールが転送されることによって認証が失敗する、ということがありません。この点はDKIMの大きな長所となっています。

逆にDKIMの認証が失敗するケースとして、メーリングリストなどで"Subject" ヘッダに、メーリングリスト名や番号などを付加する場合があります。こういった文字列の追加は、メールの改変にあたるため電子署名が一致しないことになり、認証が失敗します。このことは、しばしばDKIMの短所として取り上げられるポイントになっています。

しかし現在のメーリングリストの多くは、こういった"Subject"ヘッダへの情報の追加や、送信者情報の変更を既に行っており、もはや単なるメールの転送処理では無く、メーリングリストメンバへの再配送を行っているシステムといえます。つまり、メーリングリストのシステムが、配送されるメールの送信元にとなってお

＊10 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)
＊11 送信ドメイン認証実装状況(http://www.dekyo.or.jp/soudan/auth/)

り、DKIMの観点でみれば、本来はメーリングリストシステム側の署名を添付すべきと考えています。よって、DKIMのメーリングリストによる認証の失敗という問題については、配送時に電子署名を作成することによる回避を推奨しています。

メールの本文だけでDKIMの電子署名を認証できる利点は他にもあります。例えば、メールマガジンの購読を中止したり、改善を申し立てたりする際、そういった苦情を受ける送信側の立場では、申告者が本当に、送ったメールの受信者であるかどうかを確認したいはずです。ここで、メールの送信側が予め配信時にDKIMの電子署名を添付しておき、苦情を申告する側が、元々送られてきたメールを添付すれば、その添付されたメールを再認証することで、本当に送信されたメールか否かを確認することができます。また、こういった申告に利用可能な形式としても利用できるARF（Abuse Reporting Format）がIETFのInternet Draftとして公開され、標準化の議論が行われています。（図-4）

2.4 おわりに

今回のメッセージングテクノロジーでは、送信側の迷惑メール対策の最近の動きとして、ボットネットの管理元の対策の動きや、OP25B以外の送信側の対策手法として広がりつつある、Walled Gardenの手法を紹介しました。迷惑メールの送信は、送信している側はビジネスとして行っているために、日々技術革新を行い、迷惑メールが届くための工夫をしています。今後もネットワークの管理の在り方や、メールの送信側、受信側それぞれで総合的な対策が必要になってきます。本レポートでは、今後もこういった対策技術の紹介を継続していきます。

SPFレコードを一度記述して公開すれば良いSPF/Sender IDに比べて、DKIMの導入はなかなか進んでいないという現実があります。この背景には、費用対効果の関係もあると考えられますので、DKIMの長所や利用方法を紹介していくことにより、今後も普及を促進していきたいと考えています。

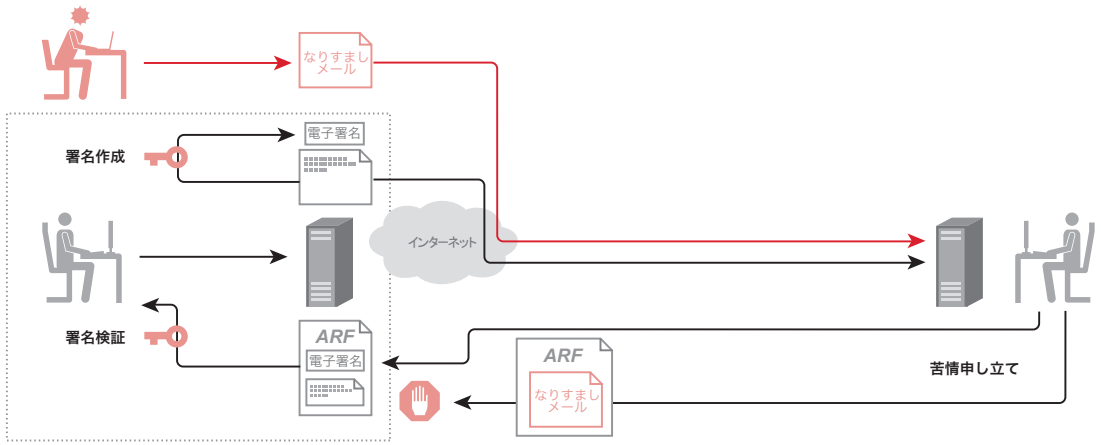

図-4　DKIMのARFでの利用例

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。