送信ドメイン認証技術と迷惑メールの関係を考察

今回は、2010年第39 ～ 52週での迷惑メールの推移を報告します。迷惑メールの送信元地域は、前回に引き続いて米国が1位でした。今回は、迷惑メールと認証結果の関係についても考察します。

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。今回のレポートは、多くの企業の第3四半期にあたる2010年第39週（2010年9月27日～ 10月3日）から第52週（2010年12月27日～ 2011年1月2日）までの14週間分のデータを対象としています。

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。

2.2.1 2010年後半から迷惑メールの減少が続く

前回のIIR Vol.9では、9月以降迷惑メール割合の減少が続いていると報告しました。今回の調査範囲でも、この減少傾向が続いています。今回の調査範囲である2010年第39週から第52週までと、その前年同時期を含む1年3 ヶ月分（66週）の迷惑メール割合の推移を図-1に示します。

今回の調査期間での迷惑メール割合の平均は72.1%でした。前回（2010年第26 ～ 38週）から6.9%減少し、2009年同時期（2009年第40 ～ 53週）に比べても9.3%減少しています。今回の迷惑メールの割合の推移では、平均値が減少していることからも明らかなように、2009年の同時期に比べて大きく変化し、その傾向も減少しています。特に、2010年最終週である第52週は、63%まで減少しています。これは、IIR Vol.2で報告したMcColo社のネットワーク遮断による影響が見られた2008年第47週よりも低い割合です。今回の迷惑メールの減少に関しては、セキュリティベンダからのレポートや、その内容を引用したニュース記事でも、2010年後半からメール流量が減少していることが報告されています。原因は、迷惑メールの主要な送信手法であるボットネットの活動が低下しているためと推測されています。2008年にMcColo社のネットワーク遮断の詳細を報告し、ワシントンポスト紙の

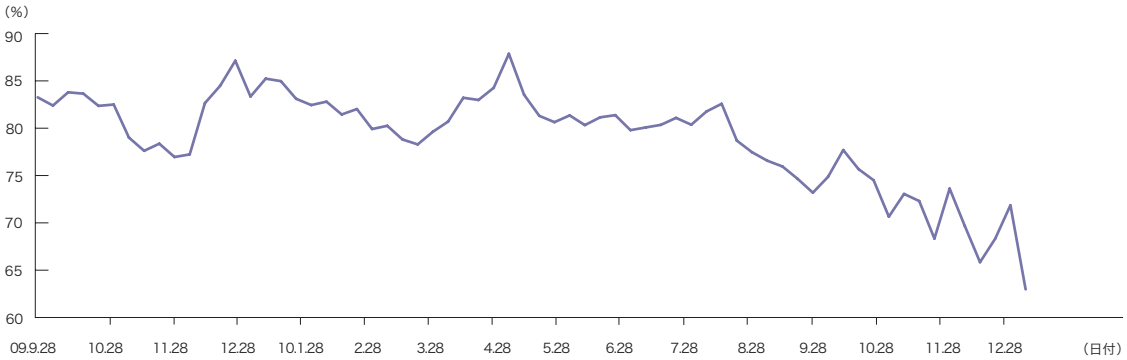

図-1　迷惑メール割合の推移

＊1　KrebsonSecurity (http://krebsonsecurity.com/2011/01/taking-stock-of-rustock/)

記者だったBrian Krebs氏のブログ[*1]でも、2010年8月からのスパム量の減少と、ボットネットのRustockとの関係性が報告されています。このように迷惑メールの割合が減っていくことは、メールサービスを運用する者にとっては望ましいことですが、残念ながらあまり長続きはしないようです。まだ速報値のレベルですが、2011年第2週あたりから迷惑メールの割合が再び上昇してきています。

2.2.2 送信元1位は米国、日本の割合も上昇

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、前回に引き続き米国（US）で、迷惑メール全体の10.3%を占めていました。ただし、前回からは1%減少していますし、迷惑メール全体の割合も減少していますので、実際に受信されたメール数も減少したことになります。2位は中国（CN）の10.2%で、前回の3位から上昇しています。3位はインド（IN）の6.2%で、前回2位であったときの割合（7.4%）から減少しています。4位はロシア（RU、5.4%）、5位は日本（JP、4.7%）です。日本は、前回の8位から上昇しました。以下、ブラジル（BR、4.6%）、ベトナム（VN、4.6%）、英国（GB、4.2%）が続いています。

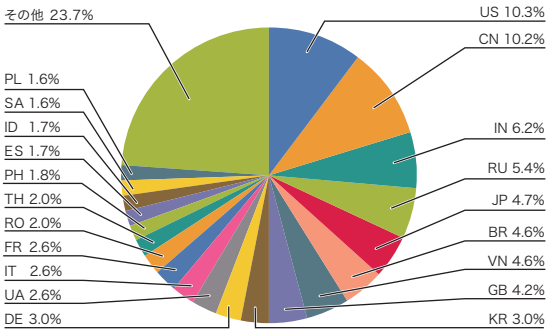

図-2　迷惑メール送信元地域の割合

2.2.3 ボットネットと送信元地域の関係

迷惑メール送信元地域で日本の順位が上がった原因は、日本発の迷惑メールがボットネットの活動の影響をあまり受けなかったためだと考えられます。ボットネットの活動が低下し全体の迷惑メール量が減少しました。しかし、日本発の迷惑メールは、ボットネットを利用した動的IPアドレスでなく、固定IPから送信されるものがほとんどです。このため、日本の順位が上がったものと思われます。中国の順位が上がった原因も同じ理由であると推測しています。以前IIR Vol.6で、日本や中国では特定の送信元からの迷惑メール量が多いという分析結果を示しました。この傾向は現在も続いています。このため、日本と同様にボットネットの活動の影響を受けなかったものと考えています。　図-3に、これら迷惑メール送信元の上位7地域（US、CN、IN、RU、JP、BR、VN）での割合の推移を示します。中国（CN）の割合が第44週（11月11日の週）に急上昇しています。これは、特定の送信元からの迷惑メール数が増加したことが原因です。これに対して第50週（12月13日の週）と第51週（12月20日の週）の割合が大きく減少しています。これらは、それまで続いていた特定の送信元からの迷惑メールが送信されなくなったことによるものです。第52週（12月27日の週）に中国（CN）の割合が再び急上昇し、米国（US）の割合が激減しています。図-1に示した全体の割合で、この週は迷惑メール量が極端に少なかった時期です。この原因が米国（US）からの送信量の減少であることが図-3から読み取れます。一方、中国（CN）やロシア（RU）の割合が上昇していますが、これは実際の送信数が増えたのではなく、全体の迷惑メール数が少なかった上に米国（US）の割合が極端に減ったことが影響しています。こうした傾向から、ボットネットの種類別に地域的な分布状況を分析できるかもしれません。

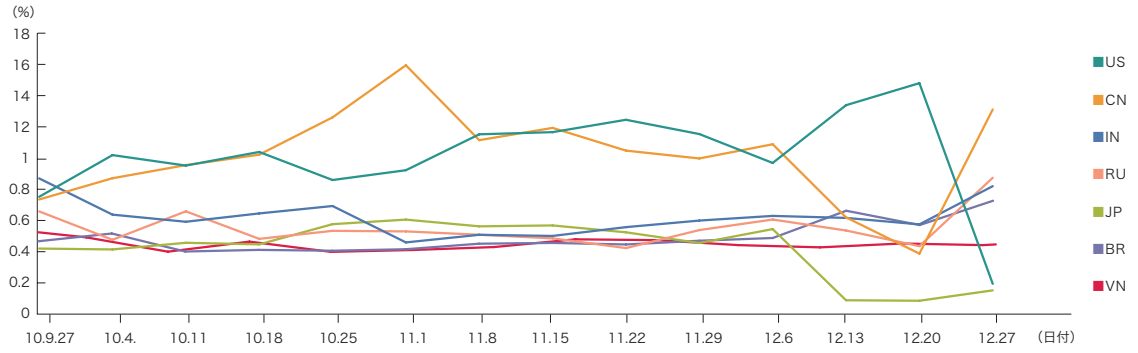

図-3　迷惑メール送信元のうち上位7地域の推移

2.3 メールの技術動向

IIJが提供するメールサービスでは、メールの受信時に送信ドメイン認証を標準で行っています。特に個人向けに提供しているIIJ4UとIIJmioブランドで提供しているメールサービスでは、SPF（Sender Policy Framework）とDKIM（Domain Keys Identified Mail）の2つの技術による認証を行っています。これまで、この認証結果を利用した送信ドメイン認証フィルタを提供してきましたが、2010年12月1日からはより簡単な設定で利用できる「なりすましメールフィルタ」の提供を開始しました[*2]。今回も送信ドメイン認証技術の普及状況について報告します。

2.3.1 流量ベースのSPFの導入が増加

今回の調査期間（2010年10月～12月）に受信したメールのSPFによる認証結果の割合を図-4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%でした。この結果は、前回IIR Vol.9で報告したものに比べて5.5%減少しています。したがって、送信側のSPFレコードの宣言率、すなわち送信側のSPFの導入割合が5.5%増えています。しかし、今回の調査期間では、迷惑メールの全体量も減少しているために、SPFの導入割合が見かけ上増加したのではないかと考えることもできます。これに対しては、認証結果“pass”の割合が23.6%と、前回から4.8%増加したことを挙げることができます。

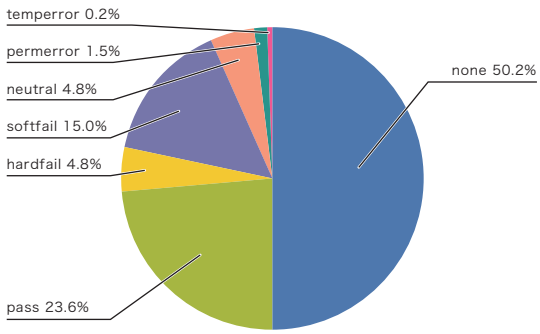

図-4　送信ドメイン認証結果の割合

2.3.2 認証結果と迷惑メールの関係

いまだに一部の人々の間で誤解されることが多いため、認証結果と迷惑メールの関係について改めて補足しておきます。認証結果が“pass”となった送信者情報のメールが迷惑メールでない、とは必ずしも言えません。同様に、“fail/hardfail”や“softfail”となったメールが必ずしも迷惑メールであるとも限りません。送信ドメイン認証技術が普及する以前は、多くの迷惑メールで、広く知られているドメイン名が送信者情報（配送プロトコルでの送信者情報や、メール本体のFrom:ヘッダに記述されているメールアドレス）に利用されていました。古くは、送信者情報を利用した受信ブロックを回避したり、実際の送信元を隠蔽したりするために、よく使われているドメインが嘘の情報として利用されました。また最近では、フィッシングなど、そのドメイン名を使っているWebサービスの偽サイトに誘導して個人情報などを搾取する目的で、受信者を騙すために送信者情報が利用されることがあります。このようなことから、送信者情報を詐称できないようにするために、送信ドメイン認証技術が開発され、普及されてきました。その一方で、認証結果だけを使うフィルタリングを回避するために、認証結果が“pass”となるドメインを送信者情報に利用する迷惑メールも増えてきました。母数が多いデータについての分析はまだ終えていませんが、個人で受け取っている迷惑メールについて調べてみると、最近の認証結果の半数以上が“pass”となっていました。この原因として、2つのことが考えられます。1つは、正規のメールサーバを踏み台にして、迷惑メールが送信されている可能性です。最近では、メールの送信時に送信者認証（SMTP-AUTH）を実施するメールサービスが増えました。しかし、この認証に利用するパスワードに、認証IDと同じ文字列が使われていたり、不正プログラム（マルウェア）によって搾取された認証IDが悪用されたりしているケースなどが考えられます。もう1つは、ドメイン名を

＊2　新しい送信ドメイン認証フィルタ「なりすましメール対策フィルタ」の提供及び従来の送信ドメイン認証フィルタの廃止について（https://www.iij4u.or.jp/info/iij/20101201-1.html）（https://www.iijmio.jp/info/iij/20101201-1.html）

詐称せず、堂々と独自のドメインを取得し、それに送信ドメイン認証技術を導入して送信しているケースです。前者の場合は、安易なパスワードを設定しないようにしたり、ウイルスチェックをこまめに実施したりするなどの啓発による対策が重要です。後者の場合については、元々送信ドメイン認証技術に関する議論の中で、こういった可能性があることが指摘されていました。ただし、このようなドメイン名は、自らが迷惑メール送信者だと名乗っているようなものなので、粛々とフィルタリング等を行えばよい、ということになります。つまり、認証結果だけで判断せずにドメイン名と合わせてフィルタリングするべき、ということです。確かに紛らわしいドメインが取得され、正規のドメインになりすましているようなケースもあります。しかし、このようなドメインは、ブラックリストなどで機械的に判断することができます。　このように認証結果が“pass”というだけでは、迷惑メールかどうかを判断することはできません。したがって、送信ドメイン認証技術が迷惑メール対策の1つであるとは、単純には言えません。認証されたドメイン名の情報と組み合わせることで対策が可能になる、いわば基盤のような技術であると言えます。また、きちんと管理されたドメインであれば、そのドメイン名と“pass”の認証結果を併せてホワイトリストとし、他のフィルタリング処理を省略してメールシステムの負荷を軽減させることも可能なはずです。このように、メールを受け取りやすくするためにも、メールの送信側で送信ドメイン認証技術を導入し、送信しているメールに迷惑メールが含まれないようにする、といった管理が必要になります。　また、正規のメールでの認証に失敗するケースについては、メールの再配送時に生じるなど、運用形態の一部で発生することが分かっています。このような問題は、技術的に解決可能であることをこれまでのIIRで解説してきていますので、参照にして頂ければと思います。

2.4　おわりに

前回、特電法（特定電子メールの送信の適正化等に関する法律）とその改訂に関する研究会のワーキンググループが開催されていることに触れました。報道機関による12月17日の発表によれば[*3]、この法律の違反容疑で東京の出会い系サイトの運営会社が逮捕されたそうです。報道内容から、今回の容疑は、送信者情報を偽って無差別に大量にメールを送信したことと、受信者の同意を得なかったこと（オプトイン規制）が要件となっているようです。いずれの容疑も、前回の法律改正時に強化された部分ですので、改正の意義があったと言えるでしょう。また、今回の迷惑メールの送信は、中国やフィリピンなどの海外から行われたと報道されています。もちろん、海外から送信されたとしても、日本に届く迷惑メールは日本の法律の対象になるため、逮捕することが可能です。海外から送信された理由は、これまでIIRで述べてきたとおり、OP25B（Outbound Port 25 Blocking）の導入などのISPの努力の結果、日本からは送信しにくくなったためだろうと考えています。前回の法律改正で、外国の執行機関に対して情報提供することも、一定の条件で可能になりました（第三十条）。ただし、外国の法律や執行制度には日本と異なる部分があるため、この法律改正だけで違法な業者の摘発が増えていくとは限りません。しかし、言うまでもなくインターネットは全世界をつなぐ基盤システムですので、今後もよりグローバルな視点で協力しあっていくことが重要だと考えています。その意味で、この部分の改正に関しても意義があったと考えています。　IIJは、今後も引続き、技術面や法的な側面を含め、よりグローバルな分野でよりよいインターネット環境実現のために貢献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 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。

＊3　迷惑メールを無差別に数百万通！出会い系を宣伝、容疑の7人逮捕（http://sankei.jp.msn.com/affairs/news/110117/crm11011720130102-n1.htm）