ボットネット対策が迷惑メールの割合に与えてきた影響と成果

今回は、2012年第27週から第39週までの迷惑メールの推移を報告します。
迷惑メールの割合は、前回のレポートから1.4%の微増、前年の同時期からは2.1%の微減となり、
変化が少ない状態で落ち着いてきています。
また、日本向けの迷惑メールの分析と、送信ドメイン認証技術の普及状況について報告します。

2.1 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が関わる様々な活動についてまとめています。今回は、日本の多くの企業の第2四半期にあたる2012年第27週(2012年7月2日～7月8日)から第39週(2012年9月24日～9月30日)までの13週間分のデータを調査対象にしています。

「2.2 迷惑メールの動向」では、最近増加してきている日本向けの迷惑メールの傾向について分析しています。「2.3 メールの技術動向」では、送信ドメイン認証技術の普及状況について、メール受信数だけでなくドメイン数の観点からの比較についても報告します。

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、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。また、これまでの分析結果の蓄積から得られる迷惑メールの送信手法の変化や、最近の迷惑メールの傾向についての分析結果についても解説します。

2.2.1 これまでのボットネット対策とその効果

今回の調査期間(2012年7月～9月)での迷惑メール割合の平均値は、46.1%でした。前回のレポート(Vol.16)から1.4%の微増、前年の同時期(Vol.13)からは2.1%の微減となりました。迷惑メールの割合は、ここ暫く変化が少ない状態で落ち着いてきていると言えます。一時期に比べて迷惑メールの量が激減した理由には、大規模なボットネットが活動できないように、制御サーバ(C&Cサーバ*1)を停止させてきたことが挙げられます。こうした対策が、迷惑メールの割合に与えてきた影響を確認できるように、これまで本レポートで報告してきた2008年6月2日から2012年9月30日までの迷惑メール割合の推移を図-1に示します。

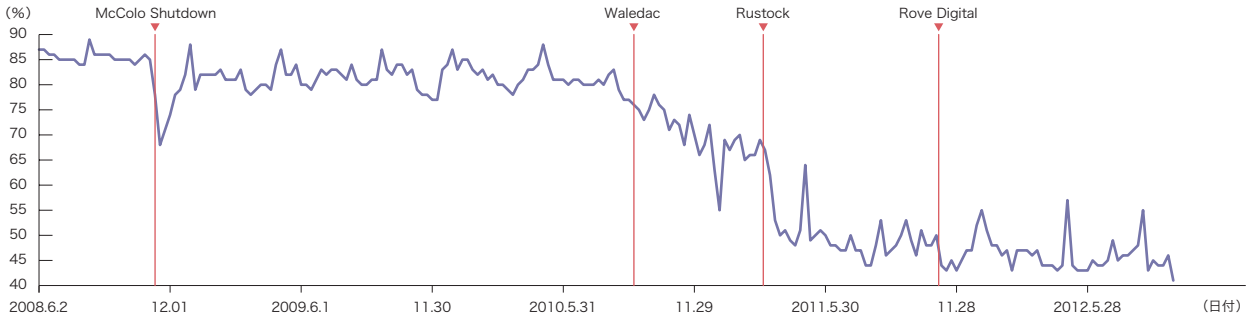

図-1 迷惑メール割合の推移

*1 Command and Controlサーバ。

2008年11月には、C&Cサーバをホスティングしていたの ISPのネットワークが上位ISPから遮断(McColo Shutdown)されたことにより、一時的に迷惑メール割合が激減しましたが、すぐに元のレベルまで持ち直しています。その後、Microsoft社が中心となり、2010年9月にWaledacと呼ばれる大規模なボットネットを、続いて2011年3月にRustockボットネットを活動停止に追い込みました。図-1では、迷惑メールの割合が、これらの時期から段階的に減少してきたことが分かります。いずれも、迷惑メール対策として、ボットネットの制御サーバを停止させることが効果的であったということが示された結果となりました。

2.2.2 迷惑メール送信元の変化

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、迷惑メール送信元地域の1位は前回(Vol.16)に引き続いて中国(CN)となり、迷惑メール全体の24.0%を占めていました。割合は前回から3.3%増加しています。2位も前回と同様で日本(JP)となり、15.6%でした。3位は、これまであまり上位には登場してこなかったサウジアラビア(SA)で11.1%でした。前回は1.4%でしたので、9.7%と大幅に増加したことになります。4位はインド(IN)で7.5%となり、前回から順位も割合も増加しています。5位は米国(US)で5.4%、6位は香港(HK)で3.3%でした。前回4位だったフィリピン(PH)は、今回は21位と大幅に順位を下げています。

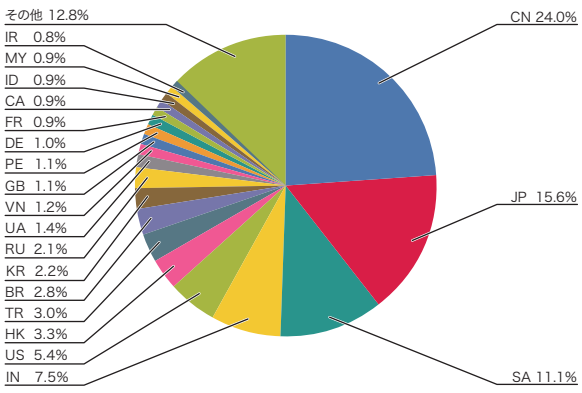

図-2 迷惑メール送信元地域の割合

これら、上位6地域(CN、JP、SA、IN、US、HK)と、前回4位だったフィリピン(PH)を加えた7地域のおよそ1年間(2011年11月3日～2012年9月30日)における迷惑メールの割合の推移を図-3に示します。この1年間で、中国(CN)は常に送信元地域で1位だったことが分かります。今回割合が急上昇したサウジアラビア(SA)は、2012年6月以降に急激に割合が増えました。しかし、2012年9月以降では、急激に割合が減ったため、この傾向が続くとすれば、次回以降は順位を下げることが予想されます。サウジアラビアが割合を増やしたこの期間、これまで上位にあったフィリピン(PH)の割合が下がっていることが分かります。これら2地域については、それぞれの迷惑メールの内容を確認することは難しいため、この割合の変動についての関連性までは判断できません。しかし、フィリピンで最も割合が高かった時期では、送信元(IPアドレス)あたりの迷惑メール数の平均が約500通だったのに対し、サウジアラビアでは約12通という結果でした。このことから、フィリピンでは特定の送信元が大量に日本に向けて迷惑メールを送信していたのに対し、サウジアラビアではボットネットを利用して迷惑メールを送信していることが推測でき、少なくとも迷惑メールの送信手法については関連性がなかったと言えると思います。

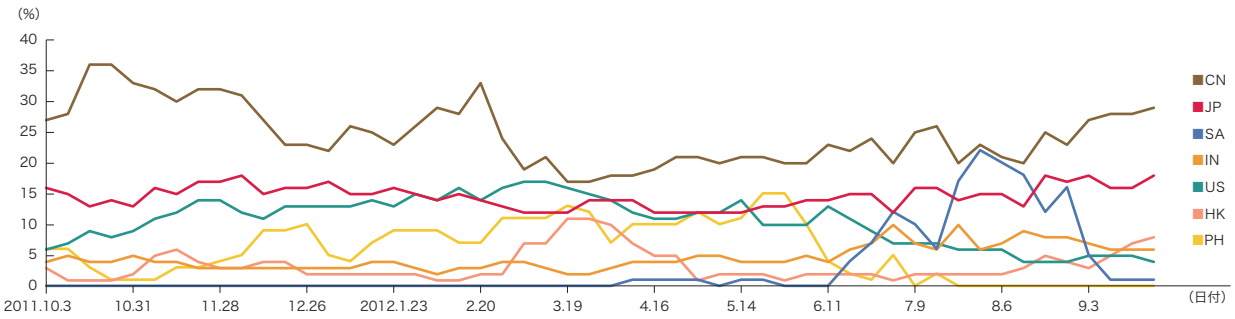

図-3 主要迷惑メール送信元地域の割合の推移

2.2.3 日本向けの迷惑メールの分析

これまで日本で受信する迷惑メールは、大部分が薬系の宣伝的なものや、最近では大手SNSからメッセージを騙ったものなど、英文で書かれたものが主流でした。しかし、図-1でも示したように、ボットネットの活動低下に伴い、グローバルで広く送信されてきた、こうした英文の迷惑メールの数が減少してきました。その一方で、日本語で書かれた日本向けの迷惑メールが増えてきているようにも感じられます。今回は、9月頃から大量に送信されている有料放送が解除できるというカードの宣伝を大量に送信している迷惑メールについて報告します。いくつかの内容のパターンがあるようですが、概ね以下のような宣伝内容になっています。

```
Subject: 約90チャンネル以上が半永久的に0円で見放題！
From: 噂のB-CAS<support@*****.com>
To: <*****@example.jp>

――――――――――――――――――――――――――――――――

【限】【定】【販】【売】▼噂のB-CAS▼数量限定販売

希少価値の高い商品です！お早めに御購入ください！

――――――――――――――――――――――――――――――――

豊富な約90チャンネル以上が半永久的に0円で見放題！
もうDVDを借りに行かなくても、お家でのんびり映画・ドラマ三昧！
...
```

文面をみて分かるとおり、きちんとした日本語で記述されており、注意をひく装飾も施されています。一見すると、メールマガジンのようにも見えますが、もちろん購読申請（オプトイン）をしたものではありません。メールの内容についても様々なパターンがあり、利用する文字コードを変えたりと、パターンマッチングを回避するようにしています。これらの迷惑メールのサンプルについて、送信元について調べてみたところ、およそ100の様々な地域から送信されていました。その中でも最も多かったのは、サンプル中40%を占めた中国（CN）でした。送信元が地理的に分散していることや、動的IPアドレスと思われる逆引きを持っていることから、ボットを利用している可能性が高いのですが、日本国内から送信されたものも多いので（10位）、複合的な送信手法を用いている可能性があります。メールの内容は、明らかに違法な製品の広告宣伝なので、あまり実害はないかもしれませんが、本文に記述されているURL先のWebサイトが有害なものになる可能性もありますので、安易にアクセスしない方が良いでしょう。

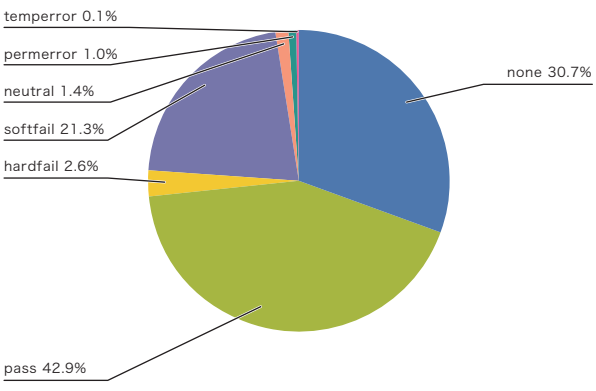

図-4 SPFによる認証結果の割合

これまで日本語で記述された日本向けの迷惑メールは、国内や近郊の地域の特定送信元から送られるものが主流だと考えられてきました。しかし、今回の例のように、日本向けであっても、様々な地域の送信元から複数の送信手法を用いて送られてくることが増えてくるかもしれません。今後も注意し、対策を強化することが必要です。

2.3 メールの技術動向

ここでは、メールに関わる様々な技術的動向について解説します。今回は、送信ドメイン認証技術であるSPF[*2]とDKIM[*3]の普及状況について報告します。

2.3.1 IIJサービスでの送信ドメイン認証技術の普及状況

今回の調査期間（2012年7月～9月）に受信したメールについて、SPFによる認証結果の割合を図-4に示します。メール送信側のドメインがSPFを導入していない（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30.7%でした。前回から3.1%減少しましたので、認証可能だったメールの割合は、3.1%増加したことになります。つまり、受信しているメールの送信側でのSPFの普及率は、今回の調査期間で約69.3%まで増えたことになります。

＊2　SPF：Sender Policy Framework、RFC4408。
＊3　DKIM：DomainKeys Identified Mail（DKIM）Signatures、RFC6376。

次に、DKIMによる認証結果の割合を図-5に示します。受信したメールのうち、「DKIM-Signature」ヘッダがなく、DKIM認証ができなかった「none」の割合は90.3%でした。前回の調査期間の割合が90.6%でしたので、DKIMでの認証可能だったメールの割合が0.3%増加したことになります。

2.3.2 認証可能なドメイン数の分析

図-4と図-5に示したとおり、SPFとDKIMとでそれぞれで認証可能だった送信元からのメールの量にはまだ大きな開きがあり、SPFの方が約7倍程度多いという結果となっています。これを、認証可能だったドメイン数で比較すると、その差はもう少し開きます。2012年9月に受信したメールを対象に調べると、ドメイン数ではSPFの方が約45倍程度多いという結果になりました。これは、DKIMの場合、電子署名をしている特定の送信元が、大量のメールを送信していることを表しています。更にSPFの場合、受信したメール数に対して、認証できたメール数の割合は約70%ありましたが、これがドメイン数で比較すると、約27%となってしまいます。これも、SPFに対応した送信元がより多くのメールを送信していることに起因していることになります。いずれもよく利用するメールが、SPFあるいはDKIMといった送信ドメイン認証技術を導入している、という結果となったことは、良い方向性だと思います。更に送信ドメイン認証技術を普及させるには、より多くのドメインが導入し、裾野を広げることが必要だと言えます。

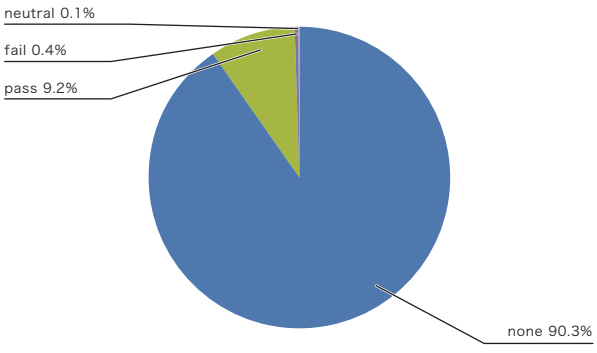

図-5 DKIMによる認証結果の割合

2.4 おわりに

前回のレポートでは、迷惑メール量自体は減ったが、金銭的な被害や情報漏えいなどが増えており、脅威は高まってきていると触れました。今回も、不正プログラム（マルウェア）がPC内部に常駐し、外部からの指令を受けて、外部の掲示板への書き込みやメール送信を行ったと考えられる事件の報道がありました。しかもこれらは、実際に書き込みをしたと考えられる実行犯ではなく、意図せずマルウェアを存在させてしまったPCの所有者が、一時犯人とされてしまいました。こういった手口は、迷惑メール送信に使われるボットネットの手法と同様です。そのため、一度マルウェアが存在してしまうと、様々な犯罪の温床となり得て、それら不正行為が明るみに出ると、そのPCの所有者が実行犯と判断されてしまう、ということになります。こうした不正行為に関わらないためにも、今回のように素性の怪しいソフトウェアをダウンロードしないような注意は必要ですし、送信元の怪しいメールの添付ファイルを開いたり、記述されたWebサイトにむやみにアクセスしたりしないといった行為も気をつけなければなりません。現在は、インターネットやPCあるいはスマートフォンといった道具が進化してより便利になってきていますが、その反面でこうした巧妙で複雑な手法を使った不正行為も増えてきていることに気をつける必要があります。

執筆者：

桜庭 秀次（さくらば しゅうじ）
IIJ プロダクト本部 アプリケーション開発部 戦略的開発室 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。M^3AAWGメンバー及びJEAGボードメンバー。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。