日本を発信元とする迷惑メールの実態

今回は、2011年第40週から第52週までの迷惑メールの推移を報告します。
前回から引き続き、迷惑メールの割合は低下していますが、日本発の迷惑メールの実数にはそれほど変化がありません。
また、送信ドメイン認証が成功した「pass」の割合が42.1%となり、初めて「none」の割合を上回りました。

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3四半期にあたる2011年第40週(2011年10月3日～10月9日)から第52週(2011年12月26日～2012年1月1日)までの13週間分のデータを調査対象にしています。迷惑メールの送信元は、ボットネットの活動低下により、特定の地域に集中する傾向が続いています。今回は、日本発の迷惑メールの送信元についてより詳しく分析した結果を報告します。

メールの技術動向では、送信ドメイン認証技術の普及割合について報告します。また、なりすまし防止対策としての送信ドメイン認証の結果利用についても解説します。

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。

2.2.1 迷惑メール割合の低下とセキュリティ脅威

今回の調査期間と前年の同時期を含む、1年3ヵ月分(65週)の迷惑メールの割合の推移を図-1に示します。今回の調査期間での迷惑メールの割合の平均は46.8%でした。前年の同時期と比べると25.2%の大幅減少ですが、前回のレポート(Vol.13)と比べると1.4%の減少で、前回での下げ幅よりも縮小しており、暫くはこの水準が続くと考えられます。

しかしながら、外部ネットワークから組織内部に入り込むことが可能な電子メールを悪用した標的型攻撃等の脅威は高まっています。通常のメールであるように偽装して特定のWebサイトに誘導したり、細工された添付ファイルを実行することにより、不正プログラム(マルウェア)が組織内部に入り込んでしまうことがあります。怪しい送信元からのメールや、送信元が確かであっても普段と様子が異なったメールには注意が必要です。

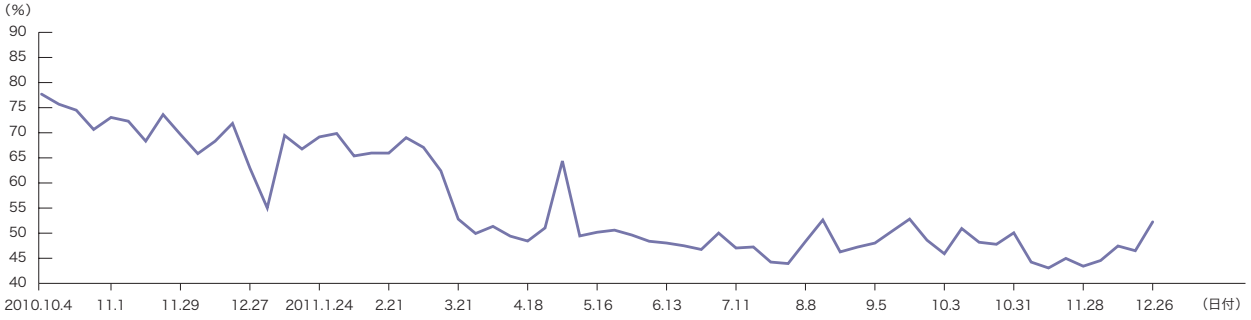

図-1 迷惑メール割合の推移

2.2.2 日本発の割合が増加

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位は引き続き中国(CN)で、迷惑メール全体の30.0%を占めていました。前回から2.2%の減少です。2位は日本(JP)で15.5%となり、前回から1.7%増加しました。3位は米国(US)で10.6%と前回から5%増加し、順位も前回の4位から上昇しました。これら上位3ヵ国で56.1%となり、迷惑メール全体の半分以上を占めています。4位はフィリピン(PH 4.9%)、5位はインド(IN 3.7%)、6位は韓国(KR 3.3%)と、これら上位地域は前回と同じ顔ぶれでした。

2011年全体について、迷惑メールの送信元上位6地域の割合の推移を図-3に示します。2011年当初、突出した迷惑メールの送信元はあまりありませんでしたが、3月以降から少しづつ整理され、5月以降、中国が突出して割合が高く、続いて日本という状態が続くようになりました。直近では、これら2地域に米国とフィリピンを加えた4地域の割合が高くなっていることが分かります。

2.2.3 日本発の送信元の詳細

IIJが提供する迷惑メールフィルタが検知した日本発信の迷惑メールの割合は、IIRの最初の号(Vol.1 2008年6月〜8月)では2%で16位でした。それが今号(Vol.14 2011年10月〜12月)では15.5%で2位と大幅に増加しました。これは迷惑メールの送信元であるボットネットの活動が低下しているために全体の迷惑メール量は減少しているものの、日本から発信される迷惑メールにはこのボットネットが元々あまり使われていないために迷惑メールの実数には影響が少なく、相対的に割合が増えていることが原因です。今回は、送信元をより詳細に調べることにより、これまでの主張を検証してみます。

図-4は、日本発の迷惑メールについて、その主要送信元をWHOISデータベースのネットワーク名や管理組織を元に分類し、送信数の割合を上位10位までまとめたものです。これを見ると、上位6組織だけで、全体の半分を占めていることが分かります。また、いずれの組織も、ボットネットの温床となっている一般ユーザを顧客とするISPではあ

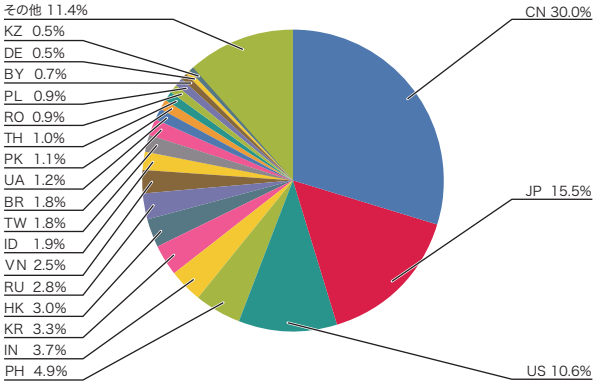

図-2 迷惑メール送信元地域の割合

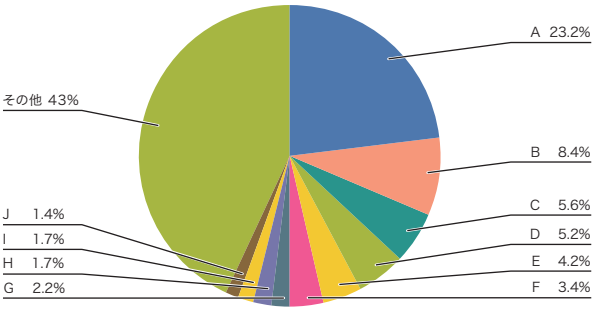

図-4 日本発の迷惑メールの送信元割合

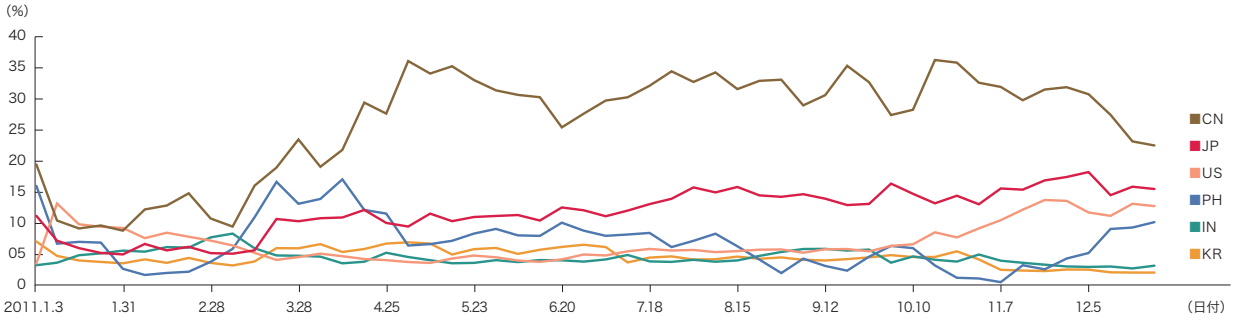

図-3 主要迷惑メール送信元地域の割合の推移

りませんでした。これらのことから、日本発の迷惑メールの大部分は、ボットネットを介さずに、特定の組織から意識的に送信されていると言えます。これら上位組織の中には、APNICからIPアドレスを割り当てられていても、住所は存在せず、電話番号も国番号の81以外全部0といった信用のおけない情報が登録されていました。

WHOISデータベースは、迷惑メール送信等、インターネット上の不正行為を調査するための重要なツールであるのに対し、APNIC等ではそれが正しく管理されていない、との指摘があります。私がメンバーとなっているMAAWG[*1]からも、以前にコメントを提出したことがありました。今後の改善を期待したいところです。

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な動向について解説します。今回は送信ドメイン認証技術の普及状況について、複数の調査結果を紹介します。

2.3.1 SPFの送信側の導入状況

今回の調査期間(2011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-5に示します。メール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39.2%で、前回から4%減少しました。これは、メールの送信側の導入率が、メールの流量ベースで4%増加したことを示します。送信ドメイン認証が成功した「pass」の割合は42.1%となりました。IIRのこれまでの調査で、初めて「pass」の割合が「none」を上回りました。

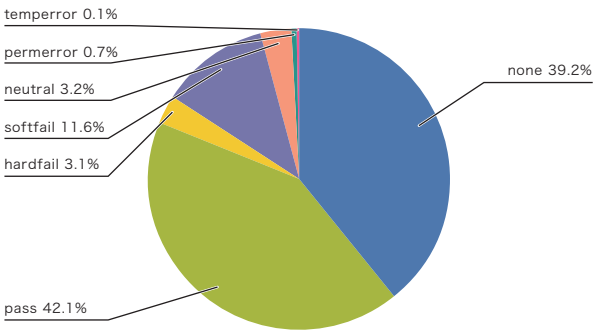

図-5 SPFによる認証結果の割合

認証結果が「pass」であっても送信者情報のドメインを詐称していないというだけで、迷惑メールでない、ということではありません。しかし「pass」した送信ドメインは、詐称していないことが明らかなのですから、ドメインをフィルタすることで必要なメールと不要なメールを区別しメールの疎通の向上に役立てることができます。今後も、送信ドメイン認証技術の導入を推進していきたいと考えています。

2.4 おわりに

WIDEプロジェクトでは、JPRSと共同研究により、日本での送信ドメイン認証技術(SPF及びDKIM)の普及率を2005年から調査しています。2011年5月の調査から暫く間が空きましたが、2011年11月の調査結果が公表されました[*2]。今後は、年に2回、5月と11月に調査結果を公表するとのことです。2011年11月の調査結果によれば、JPドメインのSPFの普及率は43.48%と順調に増加しています。特にgo.jpドメインの普及率は、93%という結果であり、政府の取り組みの本気度が示されています。送信ドメイン認証技術は、標的型攻撃でよく用いられるなりすましメールに対して有効に機能します。政府等、信用度が高い機関が送信するメールは、特になりすまされないように、このような取り組みを是非推進してほしいと思います。

執筆者:
桜庭 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。

＊1　MAAWG:Messaging Anti-Abuse Working Group, (http://www.maawg.org/)。
＊2　ドメイン認証の普及率に対する測定結果(http://member.wide.ad.jp/wg/antispam/stats/index.html.ja)。