DMARCのインターネットドラフトについて

今回は、2013年第1週から第13週までの迷惑メールの推移を報告します。
日本の近隣地域やアジア圏からの迷惑メール割合が、全体の64.8%と大部分を占めています。
引き続き、近隣諸国からの迷惑メール送信に対する取り組みが重要です。
また、2013年3月31日付けでIETFに提出されたDMARCのインターネットドラフトについて解説します。

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4四半期にあたる2013年第1週(2012年12月31日～2013年1月6日)から第13週(2013年3月25日～3月31日)までの13週間分のデータを調査対象として分析結果を報告します。

迷惑メールの動向については、迷惑メール割合の推移と送信元地域の割合の分析について報告します。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報告します。また、これまで何度か解説してきた送信ドメイン認証技術を使った新しい技術的な枠組みであるDMARCのインターネットドラフトについて解説します。

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 迷惑メール割合が増加傾向

今回の調査期間(2012年12月31日～2013年3月31日)での迷惑メール割合の平均値は、45.5%でした。前回のレポート(Vol.18)から5.0%の増加となりました。前年同時期のレポート(Vol.15)と比べると1.7%の減少ですので、前回での減少傾向から以前の水準に戻りつつあります。前年の同時期(Vol.15)から今回の調査期間での迷惑メールの割合の推移を図-1に示します。

この期間、最も割合が高かったのが、2013年の第1週で、62.1%でした。この期間は、年末年始の休暇期間にあたり通常のメール量が少なかったため、相対的に迷惑メールの割合が増えました。その後割合は、元の水準に戻りましたが、2013年3月から迷惑メールの割合が増えてきています。実際に迷惑メール量も増えていますので、今後注意が必要です。

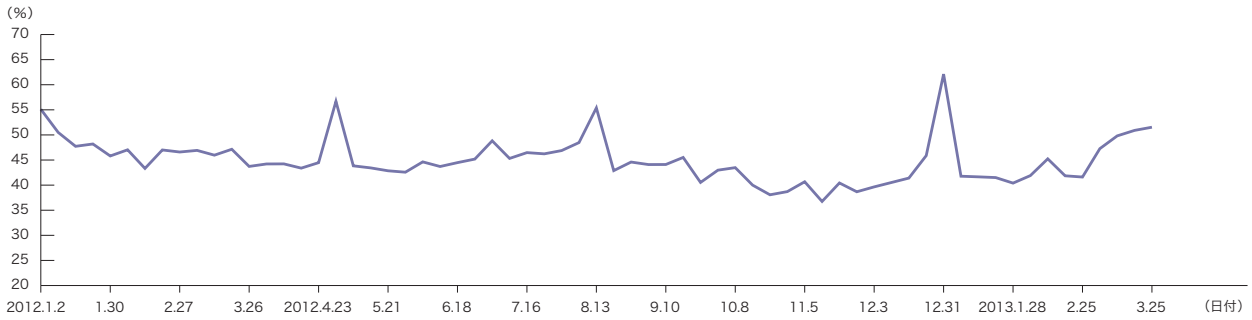

図-1 迷惑メール割合の推移

2.2.2 迷惑メール送信元の動向

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、前回に引き続き中国が1位となり、迷惑メール全体の21.7%を占めていました。前回の割合と比較すると4.9%減少しました。2位も前回と同様に日本(JP)で15.4%と、こちらも前回から3.2%減少しています。3位は韓国(KR、8.7%)で、前回の4位から順位も割合も上昇しました。4位は香港(HK、8.5%)、5位はバングラディッシュ(BD、6.7%)、6位がロシア(RU、3.8%)という結果でした。

5位のバングラディッシュは、前回の6位からの上昇で、割合も3.5%増加とほぼ倍増しています。前回、増加傾向にあることを危惧していましたが、今回の調査結果でも引き続き増加していることが分りました。今後、国際的な協力で対策を後押しするなど、何らかの対策が必要な地域と言えます。一方で、これまで主要送信元であった米国(US)が、今回は7位、3.6%と大幅に減少しました。これまで米国では、ボットネットの撲滅活動や、大手通信事業者によるポート25ブロッキングの導入などの取り組みが行われているとの情報がありましたが、それらの効果が現れてきているのかもしれません。

一方で、上位6地域がいずれも日本の近隣地域となっており、ロシアを含めたアジア圏の迷惑メール対策は不十分といえます。この上位6地域の割合を合計すると64.8%となり、日本が受信する迷惑メール送信元の大部分は、近隣地域から送信されていることが分かります。これら、上位6地域(CN、JP、KR、HK、BD、RU)の1年間(2012年4月2日～2013年3月31日)の割合の推移を図-3に示します。

これまでしばらく首位だった中国(CN)が、2013年の第9週から第10週(2013年2月25日～3月10日)の間は2位に後退し、首位が日本(JP)に入れ替わりました。その他、香港(HK)が2013年の第5週に2位になるなど、今回の調査期間中、いくつかの変動がありました。

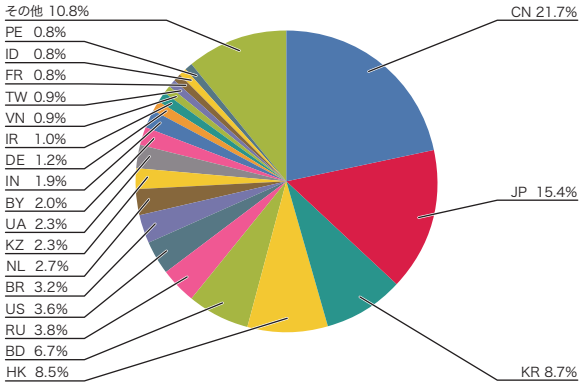

図-2 迷惑メール送信元地域の割合

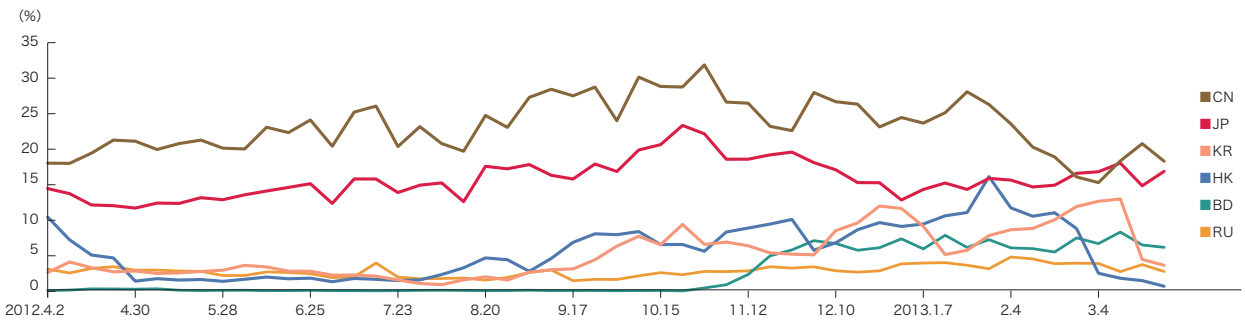

図-3 主要迷惑メール送信元地域の割合の推移

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、メール受信側からみた送信ドメイン認証技術の普及状況と、IETF[*1]に提出されたDMARC[*2]のインターネットドラフトの状況について解説します。

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(2013年1月～3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25.8%でした。前回(Vol.18)の調査期間から2.2%減少し、認証可能だったメールの割合は、逆に2.2%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74.2%まで増えたことになります。

更に、前年の同時期(2012年、Vol.15の期間)と比較すると、送信側でのSPFの導入率は10.7%増加しており、一昨年の同時期(2011年、Vol.11の期間)からは24.4%増加しています。メールの送信側でのSPFの普及率は、順調に伸びているといえます。

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88.5%でした。前回(Vol.18)の調査期間から0.1%増加しましたが、前々回(Vol.17)からは1.8%減少しています。つまり、今回の調査期間では、DKIMで認証可能だったメールの割合は11.5%であり、前回から1%の減少、前々回から1.8%増加したことになります。DKIMも同様に年単位での導入率を比較すると、前年の同時期(2012年、Vol.15の期間)からは3.3%の増加、一昨年(2011年、Vol.11の期間)からは8.6%の増加にとどまっています。DKIMは、送信側の導入にコストがかかることもあり、なかなか普及率が伸びません。しかも以前(Vol.17)分析した通り、DKIMを導入している送信元は、特定のドメインが流量の大部分を占めていますので、メールの利用者全体からみれば、普及があまり進んでいないといえます。DKIMにはSPFに比べて利点となる部分も多いので、技術について正しく理解してもらい、重要なメールにはDKIM署名が必ず付いているような状況を目指す普及活動が今後も重要と考えています。

2.3.2 DMARCのインターネットドラフト

これまでVol.15及びVol.16でDMARCについて解説してきました。DMARCは、既にGmailやYahoo!(yahoo.com)などで利用されていますが、その仕様はdmarc.orgのウェブサイトで公開されているだけでした。こういった方針は、仕様の検討に時間を費やすよりも、実際に運用することによって問題点などを検討し、仕様を考えていこう、というdmarc.orgの方針に基づくものでした。今回ようやく

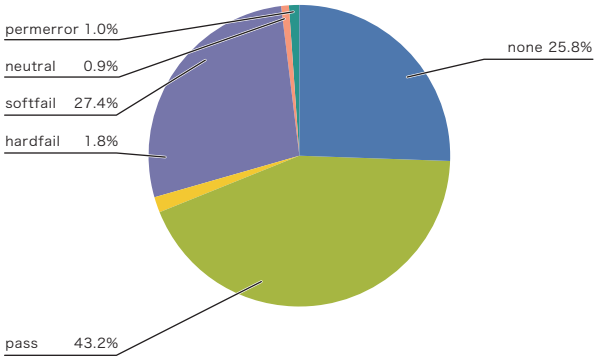

図-4 SPFによる認証結果の割合

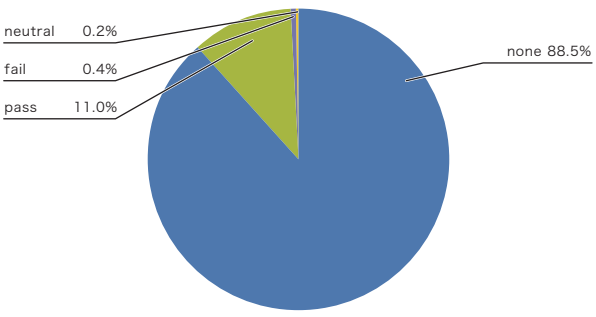

図-5 DKIMによる認証結果の割合

*1 IETF:The Internet Engineering Task Force。
*2 DMARC:Domain-based Message Authentication, Reporting and Conformance。

DMARCの仕様が、インターネットドラフト[*3]として2013年3月31日付けで、IETFに提出されました。これにより、今後はIETFで仕様が検討されていくものと思います。

インターネットドラフトになったことによる変更点は、それほど大きなものはありませんが、DMARCレコードに新しいパラメータ「fo」が追加されています。このパラメータは、認証が失敗したときのレポート生成に関わる条件を指定します。このパラメータで指定する値は以下の意味を持ちます。デフォルトは、値「0」となっています。

"fo="の値	意 味
0	すべての認証機構が失敗した場合
1	いずれかの認証機構が失敗した場合
d	DKIM の認証が失敗した場合
s	SPF の認証が失敗した場合

もともとDMARCのレポーティングには、送信ドメイン認証技術(DKIMやSPF)が予期せず認証に失敗した場合の原因分析の意味がありました。今回追加されたパラメータは、その分析をより行いやすくするための意味があると思われます。

2.4 おわりに

日本でも報道されましたが、2013年3月にスパム対策組織のSpamhausがDDoS攻撃を受け、インターネットの一部の地域で遅延などの障害が発生したとの報道がありました[*4]。報道にもある通り、Spamhausがスパムを送信していることにより、オランダの会社をブラックリストに登録したことに対しての報復だったようです。こうしたことはこれまでも起きていたことですが、今回大きく報道されたのは、攻撃の規模がピーク時に300Gbpsにまで達したことです。これは、SpamhausがCloudFlare社と協力し、Anycastの技術を使って広域分散処理によって対抗したことによって、攻撃がエスカレートした結果のようです。このDDoSの攻撃者(オランダ人)は、4月25日にスペインのバルセロナで当局によって逮捕されたようです[*5]。

インターネット上で行われるこうした攻撃は、その影響が目に見える形で現れない限り、なかなか実感することができません。特に最近、セキュリティ上のインシデントは、なるべく目立たないよう密かに行われる傾向があるため、被害が目に見える形で現れるまでなかなか発覚しませんし、発覚したときの被害規模の推定も難しいケースがあります。

最近、日本でもISPなどのメールサーバを踏み台にして迷惑メールを送信するケースが増えてきています。その多くは、送信者認証(SMTP AUTH)をきちんとした上で送信しているため、認証のためのIDやパスワードが不正プログラム(マルウェア)などにより搾取されている可能性があります。マルウェアが、IDやパスワードを搾取しているということは、操作しているPC上やアクセスしている他のサーバ上の重要な情報も危険な状態にある可能性があります。最近それほど注目もされなくなりつつある迷惑メールですが、こうした動向を注意深くみることにより、より大きなセキュリティ上の危険性について気がつくことがあるかもしれません。

執筆者:

櫻庭 秀次(さくらば しゅうじ)
IIJ プロダクト本部 戦略的開発部 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、社外関連組織と協調した各種活動を行う。M3AAWG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。

＊3 draft-kucherawy-dmarc-base-00(http://www.ietf.org/id/draft-kucherawy-dmarc-base-00.txt)。
＊4 "Firm Is Accused of Sending Spam, and Fight Jams Internet"(http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html)。
＊5 OPENBAAR MINISTERIE、"Nederlander aangehouden in Spanje vanwege cyberaanvallen op Spamhaus"(http://www.om.nl/actueel/nieuws-persberichten/@160856/nederlander/)。