迷惑メール最新動向

2.1 はじめに

1年ぶりとなった、IIRのメッセージングテクノロジーでは、迷惑メールの動向や迷惑メール対策を含めた、メールに関する技術情報について報告します。迷惑メール量は、ここ数年は減少傾向が続いてきましたが、直近の2016年3月に一時的に増加しました。本レポートでは、増加の要因となった送信元地域の調査結果を報告します。メールの技術動向では、今後普及が望まれるDMARCを中心とする送信ドメイン認証技術の普及状況について調査結果を報告します。

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迷惑メール量の割合の推移を元に、迷惑メールの変化の動向について報告します。これまでと同様に迷惑メールの割合は、一週間単位で集計し全体の受信メール量に対して、迷惑メールと判断された受信メールの割合の推移をグラフなどで示します。ここしばらく迷惑メールの量及び割合は、IIRの発行当初の2008年に比べて大幅に減少してきましたが、2016年3月に一時的に増加しています。

図-1に示す迷惑メール割合の推移のグラフは、前回のIIR (Vol.27) からの1年間、2015年3月30日から2016年4月3日までの53週間を含む、3年分のデータです。これより以前の推移については、IIR Vol.27を参照してください。迷惑メールの割合は、グラフを見て分かるとおり、年末年始の長期休暇期間などを除き、概ね減少傾向が続いてきましたが、2015年あたりから下げ幅が縮小してきました。2015年度の平均割合は、24.2%でした。2014年度が31.7%でしたので、7.5%程度減少したことになります。2013年度から2014年度の減少幅は15.7%でした。しかし、2016年3月には再び増加傾向となり、2016年3月28日の週は、44.8%まで上昇しました。その後、速報値では再び20%前後に戻りましたので、一時的な増加と考えています。この時期に増えた迷惑メールの傾向については、後ほど分析します。

2.2.1 引き続き危険度は高い状況

警察庁が平成28年3月17日に発表した資料[*1]によれば、平成27年中のインターネットバンキングに係る不正送金事犯の被害額が、過去最高の昨年を更に上回り約30億7,300万円であったことが報告されています。標的型メール攻撃も、連携事業者などからの報告が、3,823件と過去最多となっており、引き続きメールに起因する危険度は高い状態が続いていると言えます。更に、標的型メールの送信元アドレスの多くが偽装されていると考えられるものが77%であったと報告されており、やはり送信者情報の詐称を防ぐ、送信ドメイン認証技術の普及及び導入が急務であると言えます。

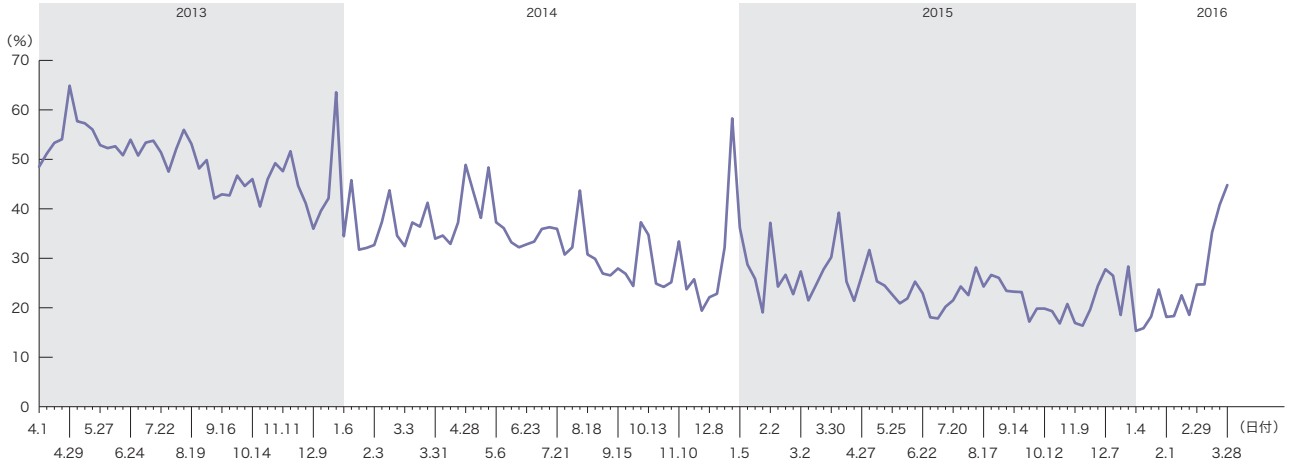

図-1 迷惑メール割合の推移

＊1　平成27年におけるサイバー空間をめぐる脅威の情勢について（http://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf）。

2.2.2 迷惑メール送信元の割合

2015年度の第4四半期にあたる、直近の2016年1月から3月までの迷惑メールの送信元を地域別に示したグラフを図-2に示します。

この時期、最も迷惑メールを送信した地域は米国(US)で、16.8%でした。これまで発表してきた調査の中では、IIR Vol.10(2010年第3四半期)以来の1位でした。2位は中国(CN)で6.4%、これまで1位だったのですが今回は2位となりました。3位はブラジル(BR)で割合としては同じ数値となっていますが6.4%でした。4位も同じ割合ですが日本(JP)の6.4%でした。以後、インド(IN、6.3%)、ベトナム(VN、6.1%)、メキシコ(MX、5.4%)、香港(HK、3.1%)、アルゼンチン(AR、2.5%)、スペイン(ES、2.5%)と続きます。日本に近い、香港やベトナム以外は、国土が広くて人口の多い地域が上位となっていることが分ります。これら、上位10ヵ国の迷惑メール送信量の推移を図-3に示します。今回は、2016年3月の迷惑メール量の増加を分析するため、迷惑メール割合の推移ではなく、迷惑メール量の推移としています。そのため、縦軸の数値は示していませんが、それぞれの地域間での比較が具体的に分かるようになっています。

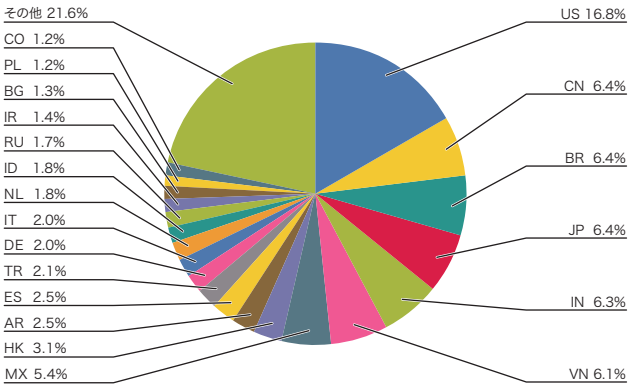

図-2 迷惑メール送信元地域の割合

2.2.3 主要送信元地域の推移

図-3を見て分かるとおり、上位地域の中で、米国(US)、中国(CN)、日本(JP)、香港(HK)はもともとが送信量の多い地域ですが、2016年3月の増加時期でもそれ程大きな増加はありませんでした。この期間、最小送信数と最大送信数の差は2倍から3倍程度の違いでした。一方で、それ以外の上位地域、インド(IN)、ベトナム(VN)、メキシコ(MX)、ブラジル(BR)、アルゼンチン(AR)、スペイン(ES)の最小と最大の差は、いずれも10倍以上、特にアルゼンチン(AR)は、85倍の差がありました。いずれも迷惑メール割合の高かった2016年3月に増加している地域であることから、この時期の増加の要因であることが分ります。これらの地域が増加した原因の可能性としては、地域的にも分散していることから、ボットネットが活発に迷惑メールを送信していたのではないか、と推測しています。今後も、国際的な連携を元に、こうしたボットネットの対策をしていくことが必要と考えています。

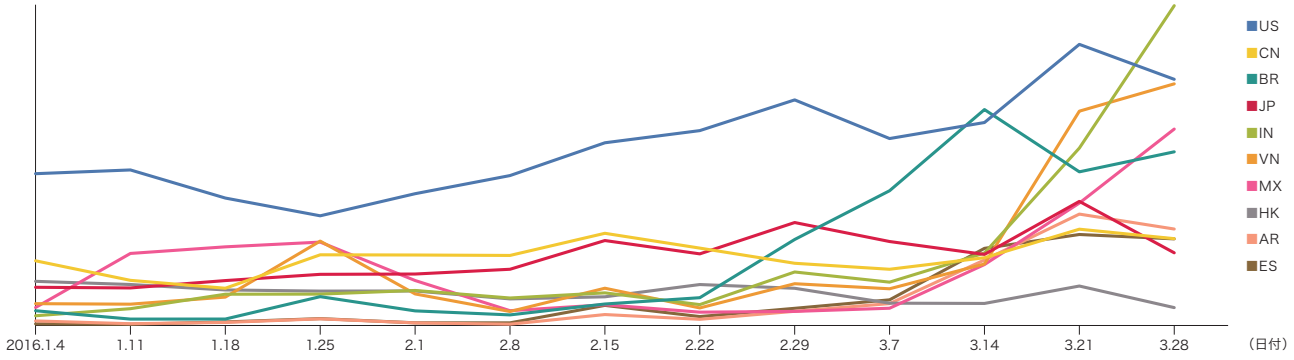

図-3 迷惑メール送信元上位10地域の推移

2.3 メールの技術動向

ここでは、迷惑メール対策にも有効な送信ドメイン認証技術、特にDMARC[*2]の普及状況や技術動向について報告します。

送信ドメイン認証技術は、これまでSPF[*3]とDKIM[*4]それぞれについて、技術詳細や普及の動向を述べてきましたが、今後は、それら2つの技術を基盤として利用するDMARCが主体になると考えています。

2.3.1 DMARCの概要

DMARCについては、既にIIR Vol.15から度々取り上げてきましたが、ここで改めてその特徴についてまとめておきます。DMARCも送信ドメイン認証技術の1つで、送信者情報から利用しているドメインが正しい送信者であるかを認証する技術です。主な特徴を以下に示します。

- SPFまたはDKIMで認証したドメインとメールヘッダ上のFrom (RFC5322.From)の一致(あるいは同じ組織であること)が前提
- 送信側(ドメインの管理側)が認証失敗時の受信側の振る舞いをポリシーとして表明可能
- 送信側が、認証失敗時のレポート先を指定可能
- これらの情報は、DNS上のTXT資源レコードで表明

つまりDMARCは、既に普及している、あるいは進みつつあるSPFとDKIMの認証結果を利用するもので、DMARC認証が「pass」したということは、メール受信者が参照可能なヘッダ上の送信者情報(RFC5322.From)とも一致していることを示す技術、ということになります。送信側では、認証が失敗した場合の情報をレポートとして受け取れることにより、メールが正しい経路で送信されているかを確認できます。これまで、SPFやDKIMで認証してきたドメインは、必ずしも最終的なメール受信者が確認しやすい送信者情報とは言えませんでした。DMARCで認証することにより、ある意味では、認証するドメインを統一することができ、受信者にも分かりやすい形になりました。

2.3.2 DMARCの普及状況

IIJのメールサービスでは、2014年よりDMARCに対応しており、受信するメールをDMARCで認証しています。ここでは、2016年1月から3月までの3ヵ月間で、DMARCでの認証結果の割合を図-4に示します。DMARC認証の前提となる、同期間でのSPFとDKIMの認証結果割合を図-5と図-6にそれぞれ示します。

まず、図-5のSPFの認証結果の割合ですが、今回SPFで認証できなかった「none」以外の割合、すなわち送信側でSPFを導入している割合は77.4%でした。前回調査結果を示したのは、2014年のIIR Vol.23で、このときから4.2%増加しました。送信側で

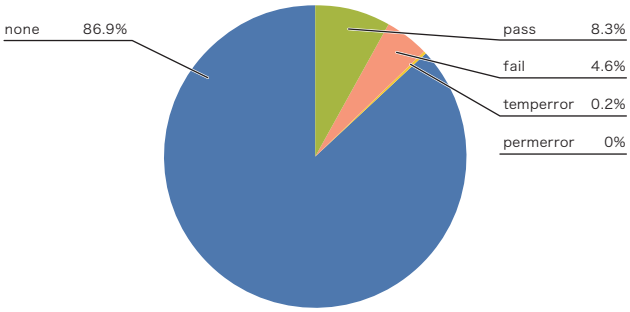

図-4 受信メールのDMARCでの認証結果割合

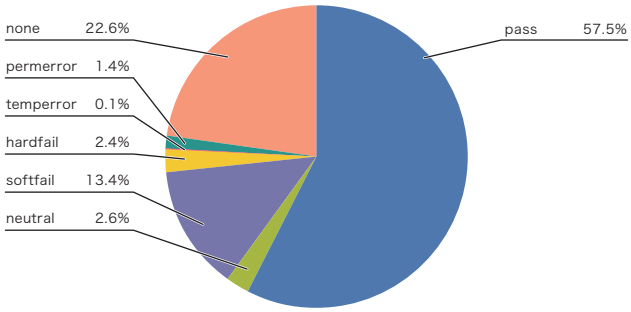

図-5 受信メールのSPFでの認証結果割合

*2 Domain-based Message Authentication, Reporting, and Conformance(DMARC), RFC7489(https://rfc-editor.org/rfc/rfc7489.txt)。
*3 Sender Policy Framework(SPF)for Authorizing Use of Domains in Email, Version 1, RFC7208(https://www.rfc-editor.org/rfc/rfc7208.txt)。
*4 DomainKeys Identified Mail(DKIM)Signatures, STD76, RFC6376(https://www.rfc-editor.org/rfc/rfc6376.txt)。

のSPFの導入は、比較的容易であることから、これまでもSPFの導入率は高い傾向がありましたが、今回の調査でも少しずつですが伸びていることが分ります。

図-6のDKIMの認証割合では、「none」以外の導入割合は20.1%でした。同様に前回からは8.5%伸びており、もともと送信側の導入にコストがかかるDKIMの導入率は低かったわけですが、それでもこちらも少しずつ導入割合が伸びていることが分かります。これらSPFあるいはDKIMを導入していることが、DMARC導入の前提となるのすが、図-4に示したとおり、DMARCでの認証ができなかった「none」以外の割合、すなわちDMARCの導入割合は、13.1%です。DMARCは、SPFあるいはDKIMを導入していれば、"_dmarc"サブドメインのTXT資源レコードにDMARCレコードを記述するだけで導入できますので、SPF及びDKIMより導入割合が低かったということは、まだDMARCに対する認知度が低いと考えられます。今後も、DMARCの利点及び導入方法について働きかけを行う必要があると考えます。

もう1つ、図-4のDMARCの認証割合で特徴的なのが、認証結果「fail」の割合が4.6%と高いことです。メールの転送時に認証が失敗しやすいSPFでは、予めそうした事象が想定される場合に「softfail」とやや弱めの失敗結果となるようにSPFレコードを宣言する傾向があります。そのため、SPFで「softfail」となる割合が13.4%と多いことは想定可能です。しかしながら、SPFでより強い認証の失敗結果である「hardfail」の2.4%、DKIMの「fail」の0.7%と比べると、DMARCの認証失敗だった4.6%はとても高い割合と言えます。この要因については、次節で分析します。

2.3.3 DMARC認証成功と失敗の要因

DMARCでは、SPFあるいはDKIMのどちらかの認証が成功した場合に、メールの「From:」ヘッダ上のドメインがDMARCレコードを宣言していた場合に、DMARC認証が評価されます。つまりDMARCの認証結果が「pass」であった、ということは、そのドメイン(RFC5322.From)とSPFあるいはDKIMで認証したドメインが一致あるいは関連のあるドメインで、SPFあるいはDKIMの認証結果のどちらかが「pass」であった、ということになります。そこで、DMARC認証が「pass」であった場合の、その要因について分析してみました。結果を図-7に示します。

DMARCが「pass」のときに最も多いSPFとDKIMの認証結果のパターンは、両方とも「pass」だった場合で、その割合は69.8%でした。つまり、DMARCレコードを宣言していて、正しくDMARC認証が「pass」するドメインの多くは、SPFとDKIMを共に導入しているドメイン、ということが分かりました。SPFとDKIMのどちらか一方の認証が失敗している、あるいは導入していない場合で、そのもう一方が「pass」だったためにDMARCとして

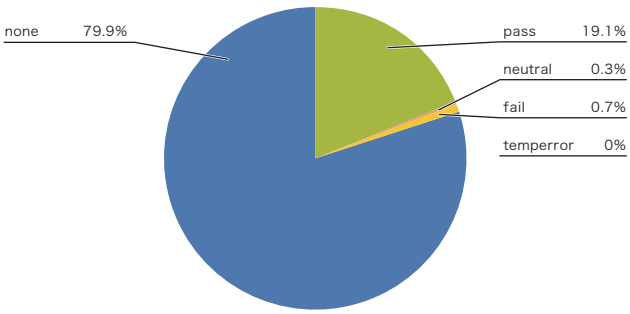

図-6 受信メールのDKIMでの認証結果割合

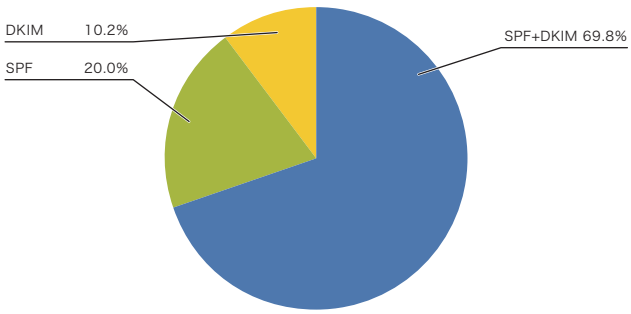

図-7 DMARCが「pass」の要因

は「pass」だった場合は、SPFが「pass」だった割合の方が多く、20.0%でした。DKIMだけが「pass」だった割合はそのおよそ半分で10.2%でした。SPFの普及率の高さが、そのままDMARC認証の「pass」の結果に結びついた、と考えられます。

今度は、DMARCが「fail」したときに最も多いSPFとDKIMの認証結果のパターンを図-8に示します。

DMARCが「fail」したときに、最も多いSPFとDKIMの認証結果のパターンは、SPFだけで認証し（DKIMは「none」）そのSPFの認証結果が「fail」だった場合です。逆に、DKIMだけの認証結果を利用した際、DKIMの認証結果が「fail」だったためにDMARCも「fail」となってしまった場合は、0.6%と非常に低い割合となりました。これもSPFとDKIMの普及率の違いと、DKIM認証の堅牢さを示した結果と考えられます。SPFとDKIMの両方が「fail」するパターンは、0.7%と低い数値でした。これらのことから、DMARCの認証失敗を防ぐためには、DKIMを導入することが有効である、ということが分かりました。

DMARC認証失敗要因の割合の中で、「DMARC」と示された10.6%は、SPFあるいはDKIMで認証したドメインとDMARCで認証するRFC5322.Fromのドメインが一致しないことにより、DMARCとして認証が「fail」してしまった割合です。これが、SPFやDKIMでの送信者情報を詐称してRFC5322.Fromだけを詐称元のドメインとしている場合であれば、正しく詐称が見破られた好例となります。しかし、もしこれが正規の正しいメールが「fail」しているとすれば、せっかくSPFあるいはDKIMを導入し、DMARCレコードを宣言しておきながら、認証するドメインが異なるために「fail」してしまう残念なケースと言えます。こうしたケースの中には、メール配送を他の事業者に委託しており、SPFあるいはDKIMの認証ドメインが、それら委託先のドメインで認証されることによるドメインの不一致が原因としてあるようです。私が受信したメールの中でも、大手銀行などから送られるメールマガジンなどが、このケースでDMARC認証が失敗しているものがありました。メールの送信者情報は、メールの送信元を示すものなので、SPFやDKIMで利用するドメインも、正しく送信者のドメインとして分かりやすいように利用すべきではないでしょうか。

図-8で示される「none」の割合の意味は、SPFとDKIMの両方の認証結果が「none」であるにも関わらず、DMARCとして認証結果が「fail」となったパターンです。これも、DMARCとして詐称が判断できたのであれば良いのですが、そうではないパターンもあるようです。詳しく調べると、DMARCの特徴である、RFC5322.Fromのドメインは、その上位ドメインも同じ組織のドメインとして扱うという「Organizational Domain」という仕組みも起因しているようです。つまり、送信しているメールがSPFとDKIMの両方に対応していないが、ヘッダ上のRFC5322.Fromドメインの上位ドメインがDMARCレコードを宣言していることで、DMARCとして認証しようとして、その結果「fail」

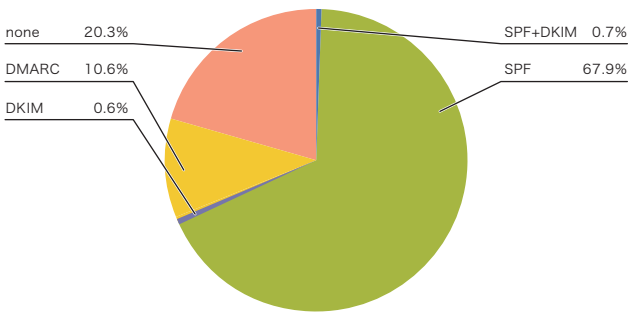

図-8 DMARCが「fail」の要因

となってしまう、ということです。ドメインの管理者としては、DMARCレコードを宣言する場合には、そのサブドメインも含めてSPFあるいはDKIMの設定もすることをお勧めします。

2.3.4 DMARCの関連技術動向

これまでIIRでは、メーリングリストやメール転送など、メールの再配送時に正しいメールであってもDMARCの認証が失敗してしまうケースがあることを紹介しました。DMARCの仕様を検討している組織でも、この問題は認識しており、今回この課題を補うための仕様の1つとして、ARC(Authenticated Received Chain)[*5]が提案されました。この技術は、その名前のとおりメールの再配送時などに、既に認証した情報をつないでいくことで、認証の連鎖を実現しようとするものです。ARCの仕様がある程度明確になった段階で、またその仕組みについて紹介したいと考えています。

2.4 おわりに

迷惑メールの割合は、2010年以降少しづつ減少してきましたが、本レポートで報告したとおり、一時的に増加した時期がありました。これまで減少してきた理由は、迷惑メールの主要な送信手法であるボットネットが活動できないような対策を継続してきたことで効果をあげてきたと言われています。今回の増加が一時的なものであれば良いのですが、こうした大量送信できる能力が依然として存在できるという状況は、やはり脅威であると考えています。

また、迷惑メールの質的な問題についても、引き続き注意が必要です。日本でも、迷惑メールが起因していると考えられる、金銭的な被害や情報漏えいなどの事象が引き続き高いレベルで発生しています。こうした被害の要因には、悪質なマルウェアが関係していると言われています。メールとして直接送信される場合もあるでしょうし、マルウェアに感染させるためのトリガとしてメールが利用される場合もあります。メールをコミュニケーション手段の基盤として引き続き維持していくためには、もう一段強い対策としての枠組みが必要なのかもしれません。

そうした対策の枠組みの1つの例として、前回のIIR(Vol.27)では、DMARCを中心とする送信ドメイン認証技術と、認証したドメインを評価するドメインレピュテーション、レピュテーションの精度を高めるためのフィードバックループの組み合わせについて解説しました。これらの機能要素は、それぞれが関連し合うことで機能を高める側面があります。なので、全体としてそれぞれが普及していくことが望ましいのですが、まずは送信側の導入が容易であり、既に標準化もされグローバル環境でも普及しつつあるDMARCが、もう少し日本で普及していても良いのではと考えています。まずは、現在の普及状況を知るために、今回のレポートではDMARCの認証結果の割合について調査し、報告しました。今後も引き続き、様々な調査を行い、対策に有効な技術の普及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 ネットワーク本部 アプリケーションサービス部 シニアエンジニア。
コミュニケーション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の設立時からのメンバー。迷惑メール対策推進協議会 座長代理、幹事会 構成員、技術WG 主査。
一般財団法人インターネット協会 迷惑メール対策委員会 委員長。

*5 Authenticated Received Chain(ARC)、draft-andersen-arc-04(https://www.ietf.org/id/draft-andersen-arc-04.txt)。