送信ドメイン技術の導入状況と標準化の動向

今回の報告は、2013年第14週から2014年第13週までの52週分のデータを含めた分析結果を
IIR Vol.1からのデータを参照しながら報告します。
また、メールの技術解説では、送信ドメイン認証技術の一つであるSPFの変更点について報告解説します。

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が関わる様々な迷惑メール対策活動について報告しています。これまで、IIRのVol.1からVol.19までレポートを継続して掲載してきましたが、今後は不定期の報告、およそ1年に1回のレポートを予定しています。今回の報告では、日本の2013年度の第4四半期にあたる、2014年第1週(2013年12月30日～ 2014年1月5日)から第13週(2014年3月24日～ 3月30日)のデータを中心に、前回(Vol.19)からの1年間、2013年第14週(2013年4月1日～ 4月7日)から2014年第13週までのおよそ1年間、52週分のデータも含めた分析結果を報告します。また、IIR Vol.1からの6年近い304週分のデータについても適宜参照します。メールの技術解説では、これまで解説してきた送信ドメイン認証技術の導入状況や現在標準化作業が行われている、送信ドメイン認証技術の一つであるSPFの変更点について、報告解説します。

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。今回は、迷惑メール割合の長期的な変化を分析するために、IIR Vol.1 (2008年6月2日)からの割合の推移を図-1に示します。

2.2.1 2010年中頃から割合が減少

2008年及び2009年の迷惑メール割合は、年間の平均割合がそれぞれ82.3%と81.8%であり、受信したメールの大部分が迷惑メールという状況でした。こうした状況が変化したのは、2010年の第2四半期(2010年6月28日～ 10月3日)からで、この時期から少しずつ割合が減少してきました。2010年の平均割合は79.4%でしたが、2010年の第1四半期まで80%を超えていた割合が2010年の第2四半期では78.7%と調査開始以来初めて80%を下回りました。その後も減少を続け、2011年第2四半期以降、40%台が続いています。

迷惑メールの割合や量自体が減少した理由は、既にIIRでも何度か報告してきたとおり、迷惑メールの送信元であるボットネットの活動低下によるものと推測されています。

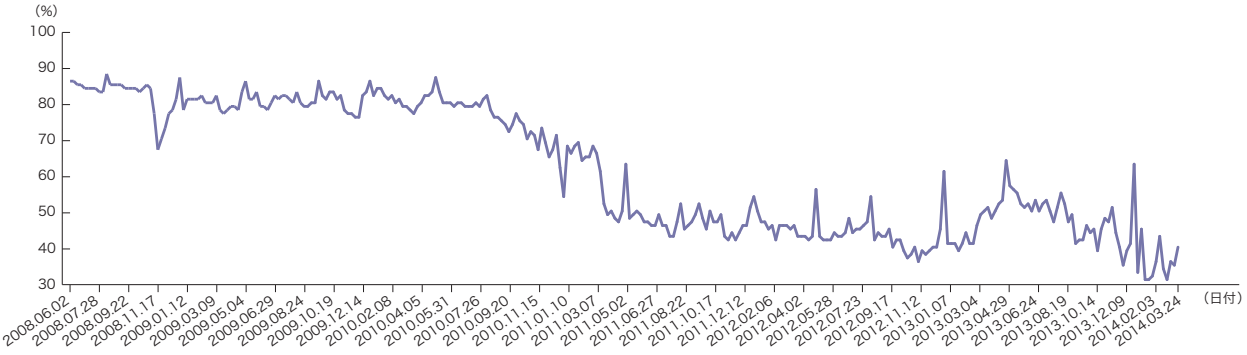

図-1 迷惑メール割合の推移

不正なソフトウェア[*1]に感染させられ、外部から制御された状態のPCをボット(bot)と呼びます。これらのボットの集合をボットネットと呼び、ボットを制御するサーバをC&Cサーバ[*2]と呼びます。ボットネットの活動を止める効果的な方法は、このC&Cサーバを止めてボットネットへの指示を出せないようにすることです。各国の行政機関が、こうしたC&Cサーバを法的な手段などによって停止に追い込むことによって、ボットネットの活動を押さえ込んだことが迷惑メール量の減少に繋がったといわれています。また、特定のC&Cサーバを持たない、P2P(Peer-to-Peer)型のボットネットに進化しているとの情報もありますので、引き続き警戒が必要です。

2.2.2 直近の迷惑メール割合は減少

2013年度の第4四半期にあたる2014年第1週(2013年12月30日～2014年1月5日)から第13週(2014年3月24日～3月30日)までの迷惑メール割合の平均は38.5%でした。前年同時期(2012年度第4四半期)の平均は45.5%だったので、7%減少したことになります。この期間、最も迷惑メールの割合が高かったのは、2014年の第1週の63.5%でした。この期間の迷惑メール量もそれなりに多かったのですが、年末年始の休暇期間であったことから、通常のメール量が少なかったことで相対的に割合が高くなったのが理由です。それ以外で週平均40%を超えたのは、第3週、第8週、第13週の4週間だけでした。

2.2.3 メールをトリガにした危険度は高まる

一時期に比べて迷惑メールは、受信メール全体に対する割合と迷惑メール量共に、大幅に減少しました。しかし、迷惑メールに起因する危険性の度合いについては増しているようです。従来は主に何らかの製品(非合法も含めて)の広告宣伝の道具としてメールが利用されるケースが多かったのに対し、最近は、組織内部にあるPCへの侵入の経路として、メールが使われているのでは、と思われるケースが増えています。

例えば、2014年1月30日に警察庁が発表した資料[*3]によれば、平成25年中に発生した不正送金が1,315件、約14億600万円と過去最大の被害と報告されています。更に、メールによってフィッシングサイトへ誘導されるケースが増えていることが報告されています。つまり、迷惑メールが単に削除をするのが面倒なもの、迷惑なもの、という範疇から、金銭的な犯罪被害のトリガになる、危険なものに変化している、ということが言えます。更に、こうしたオンラインバンキングの犯罪が発生している現状を考えれば、同様の手口で様々なIDとパスワードが搾取されている可能性も高いと考えられます。このような搾取された情報の中には、メール送信のためのIDやパスワードも含まれ、正規のメールサーバを踏み台にした、迷惑メール送信に利用される事例も多く発生しています。

2.2.4 迷惑メール送信元の動向

2013年度の第4四半期での、迷惑メールの送信元地域の分析結果を図-2に示します。この分析に利用したデータは、IIJが提供するメールサービス全般を対象にしたものではないため、図-1で示した迷惑メールのすべての送信元を対象にしたデータとはなっていません。そのため、多少の偏りがあるかもしれないことを補足しておきます。

今回の調査期間での、迷惑メールの送信元の1位は中国(CN)で、迷惑メール全体の19.1%を占めていました。中国は、IIR Vol.11 (2010年度第4四半期)から迷惑メール送信

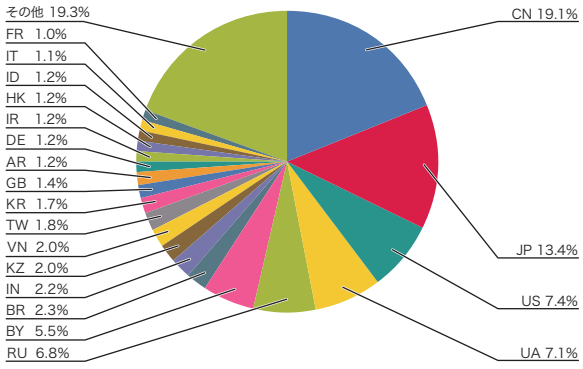

図-2 迷惑メール送信元地域の割合

*1 迷惑メール送信など悪意ある特定の目的のために作成されたソフトウェアを、より一般的な用語であるウイルスと区別して、悪意のあるソフトウェア(malicious software、malware)と呼ぶことがあります。
*2 C&Cサーバ(Command & Control Server)。
*3 平成25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発生状況等について(http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf)。

が最も多い状態が続いています。2位は日本(JP)で13.4%でした。日本もIIR Vol.16（2012年度第1四半期)から継続して2位という状態が続いており、その1年程度前から上位に位置するようになりました。これらの地域は、2010年の中頃に受信メール全体に対する迷惑メールの割合が減少して以来(図-1参照)、ほぼ固定的に上位となっていることから、ボットネットの活動低下にあまり影響しない、固定的な送信元である可能性が高いと言えるでしょう。

3位は米国(US、7.4%)、4位はウクライナ(UA、7.1%)、5位はロシア(RU、6.8%)、ベラルーシ(BY、5.5%)という結果になりました。これまでは、アジアが迷惑メールの主要な送信元地域という結果でしたが、今回の結果から、東ヨーロッパや中央アジア(9位にカザフスタン、KZ)の地域も増えていることが分りました。

これら上位6地域(CN、JP、US、UA、RU、BY)について、今回の調査期間に加えその前の1年間、65週分の割合の推移を図-3に示します。このグラフから、上位2地域(CN、JP)がほぼ一貫して高い割合を維持していることが分ります。また、直近(2013年度第4四半期)では、中国(CN)と日本(JP)の割合の変化が連動しているようにも見えます。過去には2007年の「タクミ通信」逮捕の事例もあり、中国発の迷惑メール送信には、日本が関係していたこともありますので、その関係が深まっているのかもしれません。

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動向について解説します。今回は、迷惑メール対策として期待されている送信ドメイン認証技術の導入状況について報告します。また、これらの技術は標準化され、同じ技術が広く使われることによって効果を上げます。その標準化の動向についても補足します。

2.3.1 送信ドメイン認証技術の普及状況

送信ドメイン認証技術は、既存のメール配送の仕組みであるSMTP[*4]に直接影響を与えることなく、導入ができるように作られました。メールを認証するのは、メールの受信側ですが、メールの送信側が送信ドメイン認証技術を導入しているメールのみが認証できます。つまり、メールの送信側と受信側それぞれの判断とタイミングで送信ドメイン認証技術を導入することはできますが、送受信の両方が導入して初めて認証結果を得ることができます。

送信ドメイン認証技術には、メールの送信元のIPアドレスを元に認証するSPF[*5]と、メールの本文から電子署名を作成し、それを検証することによって認証するDKIM[*6]があります。それぞれの技術について、送信側の導入状況を図-4、図-5に示します。これは、IIJの主要なメールサービスで、2014年1月～3月の間に受信したメール数に対する受信認証結果の割合を調査したものです。

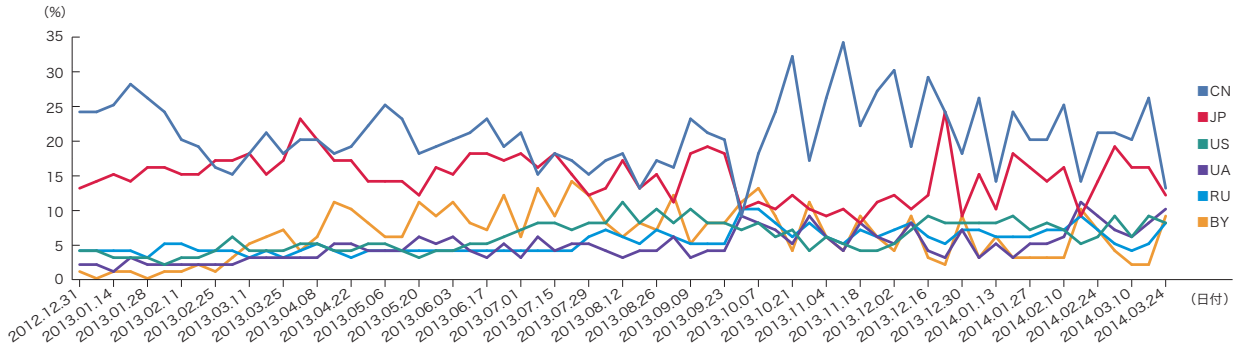

図-3 主要迷惑メール送信元地域の割合の推移

＊4　SMTP(Simple Mail Transfer Protocol)、何度か改訂され、最新版はRFC5321として公開されている。
＊5　SPF(Sender Policy Framework)、Experimentalというカテゴリの RFC4408として公開された後、RFC7208(Standards Track)として改訂された。
＊6　DKIM(DomainKeys Identified Mail)、RFC6376として公開後、STD76としてインターネット標準となった。

メールの送信側としてSPFを導入するには、メールに利用する(あるいは利用しない)ドメインのDNS TXT資源レコードにSPFレコードを宣言(設定)します。一度SPFレコードを設定すれば、そのドメイン名を利用するメールサーバのIPアドレスに変更がなければ、何もしなくて良いのがSPFの大きな利点です。

この利点もあり、SPFの導入率は、図-4をみても分かるとおり、非常に高い割合になっています。送信側でSPFを導入している割合は、認証結果が「none」(認証できなかった)以外の割合となり、今回の調査期間では73.2%でした。認証結果「pass」(47.7%)は、正しく認証されたメールの割合を示します。「hardfail」(2.2%)と「softfail」(21.0%)は、認証が失敗した割合となり、これらはドメインが詐称されたか、メールが転送などにより配送経路が変わって認証できなかったことを示します。

一方DKIMは、送信するメールそれぞれに、メールの本文などから電子署名情報を作成し、それをメールのヘッダに挿入する追加処理が必要になります。そのため、送信用のメールサーバへの新たな機能追加が必要となり、署名を作成するための処理が新たに追加されることで、負荷が高くなる傾向もあるようです。つまり、SPFに比べて送信側での導入が簡単には行えない要因があり、そのため受信側も含めて導入があまり進まない傾向にあると考えられています。しかし、SPFの認証結果で触れたメールの配送経路の変更による認証失敗がほとんど発生しない、という大きな利点があります。また、メール本文の内容から電子署名が作成されるため、途中経路でのメール本文の改ざんも検知できるなど、SPFに比べてより堅牢な送信ドメイン認証技術と言われています。

今回の調査期間で、DKIMの認証結果から見た送信側の導入割合は、11.6%でした。この割合をもっと増やす施策が必要と考えます。

2.3.2 送信ドメイン認証技術の普及の推移

SPFの認証結果の割合の推移を図-6に、DKIMの認証結果の割合の推移を図-7に示します。

SPFは、調査開始(2009年8月)以降、順調に導入割合を伸ばしています。2013年以降はあまり導入割合が伸びていませんが、それでも70%以上と高い導入率を維持しています。この期間、最大で約32.7%導入率が伸びました。DKIMの導入割合はSPFほど急速に増えていませんが、それでも割合は少しずつ増えてはいます。この期間で導入割合は約11.1%増加しました。

Gmailを提供しているGoogle社が、2013年12月に発表したデータ[*7]によれば、Gmailが受け取ったspam(迷惑メール)でないメールの91.4%がSPFあるいはDKIMで認証可能であった、と報告しています。本レポートで示している送信ドメイン認証の結果割合は、受信できたメール全体を対象にしているので(迷惑メールも含んでいる)、Google

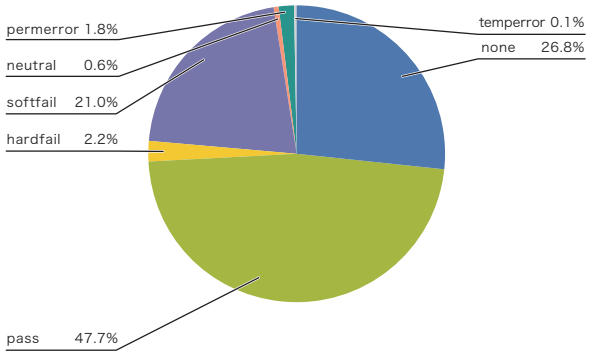

図-4 SPFによる認証結果の割合

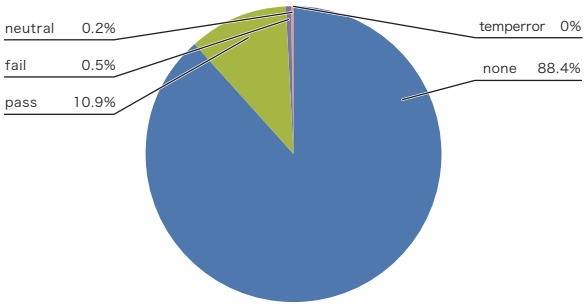

図-5 DKIMによる認証結果の割合

*7 Internet-wide efforts to fight email phishing are working (http://http://googleonlinesecurity.blogspot.sg/2013/12/internet-wide-efforts-to-fight-email.html)。

社の報告とは、元になったデータの性質が異なっているので、単純には比較できませんが、かなり高い割合でした。

Google社の報告をより詳しく紹介すると、SPFの認証可能だったメールの割合は、89.1%で、DKIMでは76.9%でした。SPFとDKIMの両方が認証できた割合は74.7%ですが、SPFだけ、またはDKIMだけ、というドメインも存在するので、双方の和をとると、全体で91.4%になる、ということのようです。

Google社は、SPFとDKIMの両方の認証結果を利用する、DMARCを推進する企業の一つなので、このような高い導入割合を示し、既に世の中のメールは、DMARCの導入準備が整っている、ということを示していると考えられます。本文中でも、既に8万ドメインが、認証できなかったメールを拒否するポリシーをDMARCで表明しており、このポリシーに従い、毎週数億通のメールを拒否していると報告しています。

DMARCでは、現在利用されているメーリングリストの配送方法と相性の悪い部分が仕様として残っているので、DMARCのポリシーとして受信拒否(reject)を宣言するには難しいケースもありますので、注意が必要です。

2.3.2 SPFの標準化動向

SPFは、実験的(Experimental)RFCとして標準化された技術です。現在、このSPFの改訂作業が行われています。そもそもSPFは、同時期(2006年4月)に同じくExperimental RFCとして公開されたSender ID[*8]との統合を目指して、IETFのMARID WGで検討が重ねられていた技術です。Sender IDの特徴であるPRA (Purported Responsible Address)について、提案元の会社が知的所有権を主張したことなどから統合の議論が不調に終わってしまった、という経緯がありました。

しかし、既にデータを示してきたとおり、SPFが送信ドメイン認証技術として、広く普及していることから、標準化

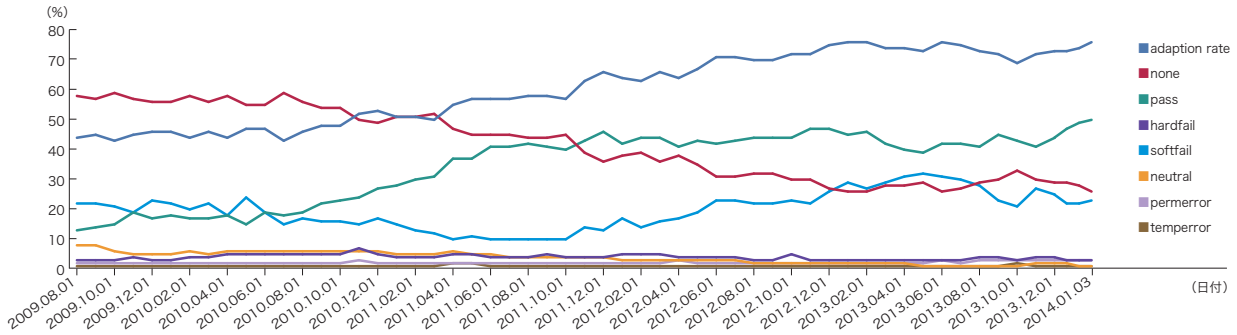

図-6 SPFによる認証結果割合の推移

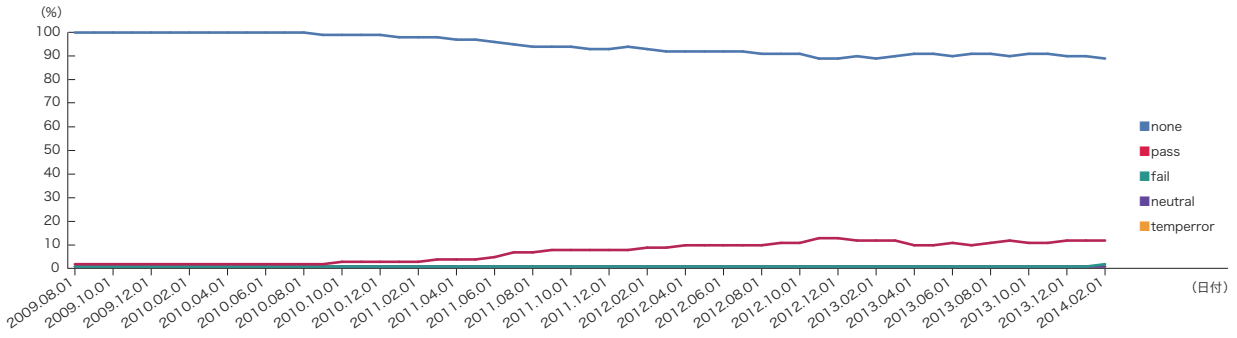

図-7 DKIMによる認証結果割合の推移

*8 Sender ID: RFC4406, RFC4407

を目指してこれまでの経験も踏まえてまとめよう、ということでIETF spfbis WGが2011年11月から議論を重ねて来ました。SPFは、2014年4月にRFC7208として、標準化への提唱(Standard Track)として公開されました。今回は、このRFC7208と従来のRFC4408との違いについて解説します。

まず、議論の前提として、以下のような見解を示しています。

・SPFは成功したがSender-IDはそうではない(なのでSender IDの取り込みはしない)
・SPFの仕様改訂のポイントは、間違いの訂正、利用していない機能の削除、既に広く使われている拡張の追加など
・SPF自体の拡張や使われている機能の削除はしない

よって、spfbis WGによるIDでは、それほど大きな変更が加えられませんでした。現在のIDで示されている主な変更点は以下です。

1. SPFレコードは、DNS上のSPF RR type (99)ではなくTXT RR(16)を利用
2. 認証結果を保存するメールヘッダは、"Received-SPF"と"Authentication-Results"を併用

これ以外については、細かな間違いの修正などです。結局、認証失敗時のメールの取り扱いについてRFCでは指針を示すことはせず、受信側で方針を決めて判断することになりました。比較的複雑な書式を記述できるSPFのマクロ機能は、それほど積極的に使っているドメインは少ないと思いますが、仕様として残すことになりました。

SPFの課題である、メールの転送についても、明確に対処方法は示さず、転送時にRFC5321.From (エンベロープFrom)を書き換えたり、転送先で受け取るようホワイトリスト的な設定をすることなどが示されただけでした。SPFのInternet-Draftは、21版まで改訂されており、実際に変更されたポイントの割にはかなりの時間を要しました。SPFは、送信側の導入が用意であることから普及率も高く、この標準化作業によって、SPFの認証結果の活用が進むことを期待します。

2.4 おわりに

今回は、1年ぶりのメッセージングテクノロジーでしたので、少し詳しく迷惑メールの動向や送信ドメイン認証技術について解説しました。本文中でも述べたとおり、迷惑メールの量自体は減少傾向にありますが、(迷惑)メールに起因する危険度は高まっています。

例えば先日、大手銀行によるフィッシングメールの注意喚起のCMがテレビで放送されているのを見ました。テレビのような媒体で、一般の方々に注意を促さなければならないほど、被害が増えている、ということだと思います。そのCMでも、手口が巧妙になっていると述べられていました。インターネット上のセキュリティ的な脅威が高まるにつれて、企業などの組織や個人も含めて様々な対策をするようになってきました。しかしながら、現在のメールシステムは、様々な情報を受信者に直接届けることができる数少ないアプリケーションの一つです。そこを狙った攻撃がこうして続いている現在では、メール受信者個々の判断力に依存した形での脅威の回避方法には限界があるでしょう。メールシステムに関わる者としては、こうした危険性の高いものを判別し、メール利用者に届けることのない仕組みの提供を早く実現したい、と日々取り組んでいます。

執筆者:

櫻庭 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 サービス開発課 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。M^{3}AAWG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、送信ドメイン認証技術WG 主査、LAP 10 Tokyo 委員会 委員長。一般財団法人インターネット協会 迷惑メール対策委員。