迷惑メール対策技術、DMARCの動向

今回の報告は、2014年3月31日から2015年3月29日までの52週分のデータを含めた迷惑メールの動向を、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、先日RFC化されたDMARCと、それを利用するための環境づくり、ドメインレピュテーションやフィードバックを含めたメールエコシステム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が関わる様々な迷惑メール対策活動について報告しています。今回は、迷惑メールの動向として、2014年度分を含めたIIR Vol.1からの迷惑メール割合の推移を示します。また、迷惑メールに起因する、セキュリティ的なトピックスについても報告します。

技術動向としては、DMARCのRFC化を契機に、DMARCが普及するための導入の利点について解説します。更にDMARCを含めた送信ドメイン認証技術が、メールシステムの中でどのような位置付けで利用できるのかについても述べます。これは、既にインターネット協会の迷惑メール対策カンファレンスなどでも構想として発表してきた内容になります。今後、迷惑メール対策関連のいくつかの組織で、実現に向けて具体的に検討していきたいと考えています。

昨年は、迷惑メール対策関連の活動が節目となるいくつかのイベントがありました。最後にそれらについても触れます。

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、迷惑メールの動向について考察します。迷惑メールの割合は、メールユーザの平日と休日でメール利用率が異なるため、1週間単位で集計しています。それでも、お盆の期間や年末年始など長期休暇を含む週は、通常のメール数が大幅に減少するため、相対的に迷惑メール割合が高くなる傾向があります。

2.2.1 2014年度は迷惑メール割合が一段と減少

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.23)からの1年間、2014年3月31日から2015年3月29日までの52週を含む、IIRの開始(Vol.1、2008年6月)時期からの356週分のデータです。このうち、昨年1年間(2014年度)の迷惑メール割合の平均値は、31.7%でした。一昨年度(2013年度)は47.4%でしたので、15.7%減少したことになります。2010年から迷惑メールの割合は急激に低下し、2011年度は48.1%、2012年度は44.3%としばらく40%台で推移していましたので、2014年度は一段と減少したことになります。

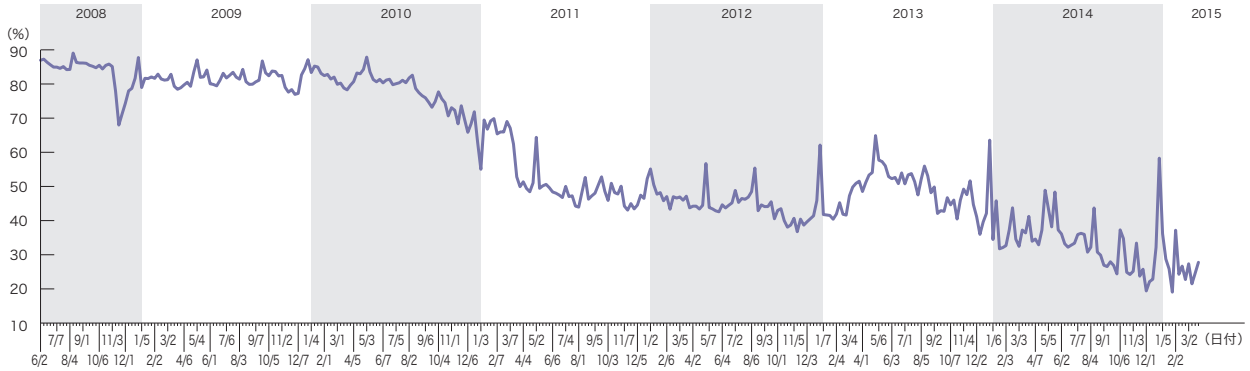

図-1 迷惑メール割合の推移

迷惑メールの割合を、もう少し長い期間で比較します。2009年度の平均値が78.6%でしたので、この5年間で格段に迷惑メールの割合、つまり迷惑メール量自体が減ったことになります。もう少し細かく説明すると、割合としては、46.7%減少したわけですが、迷惑メールではない通常のメールの受信数がこの5年間で一定だとすると、全体のメール受信量がおよそ3分の1程度まで減少したことになります。

2.2.2 量は減っても危険度は高まる

このように、迷惑メールの量自体は減少してきているわけですが、これまでも述べてきたとおり、迷惑メールに起因する危険性が減っているわけではなさそうです。警察庁が2015年2月12日に発表した資料[*1]によれば、平成26年(2014年)に発生した不正送金の件数は1,876件と前年から増加し、被害額は29億1,000万円と、前年の14億600万円からほぼ倍増しました。被害の種別としては、個人口座だけでなく、法人名義口座の被害が増えていると報告されています。不正送金の手法については、引き続き不正送金処理を自動で行うウイルスを利用した手口が巧妙化、と報告されていますので、いわゆるマルウェア[*2]を利用した手口が続いているものと思われます。

こうしたマルウェアがどのようにして個人、あるいは会社のPCに混入するのかを考えてみます。同じく警察庁などが2015年3月19日に発表した資料[*3]の不正アクセス行為の発生状況のデータでは、セキュリティホールを利用したいわゆる脆弱性を狙ったもの(資料ではセキュリティ・ホール攻撃型)の検挙件数は2件で、識別符号窃用型が336件と報告されています。もちろん、検挙されていない不正行為も相当数あると考えられますが、明らかになっているデータでは、不正行為の手口としては、外部から直接PCの脆弱性を利用したものは(まだ)少ないということが言えます。また、同資料の防御上の留意事項として以下が示されています。

1. パスワードの適切な設定・管理
2. フィッシングに対する注意
3. 不正プログラムに対する注意

フィッシングに対する注意としては、電子メールに注意するように述べられていることから、フィッシングサイトへの誘導元として、メールが利用されていることが考えられます。マルウェア(不正プログラム)についても同様で、メールの添付ファイルや信頼できないWebサイトからダウンロードしたファイルを開かない、などが示されています。つまり、これらの不正行為のトリガーとしてメールが利用され、メール内に示された不正なWebサイトへのアクセスがマルウェア感染の主要因であることが想像できます。

フィッシングについては、国内ではフィッシング対策協議会[*4]が実際のWebサイトを模倣したフィッシングサイトや、そこへ誘引するためのフィシングメールの文例などを情報提供していますので、怪しそうなメールが届いた場合には、既に登録されていないか確認することをお勧めします。また、グローバルでは、APWG[*5]が定期的にレポートを発行していますので、最近の動向など参考になると思います。

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動向について解説します。今回は、先日RFC化されたDMARCと、それを利用するための環境づくり、ドメインレピュテーションやフィードバックを含めたメールエコシステムについて解説します。

2.3.1 DMARCのRFC

DMARC(Domain-based Message Authentication, Reporting, and Conformance)については、これまでその

*1 平成26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について(https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf)。
*2 情報の搾取や迷惑メール送信、不正送金処理など悪意ある特定の目的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、悪意あるソフトウェア、マルウェア(malicious software、malware)と呼ぶ。
*3 不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況(https://www.npa.go.jp/cyber/statics/h26/pdf041.pdf)。
*4 フィッシング対策協議会(https://www.antiphishing.jp/)。
*5 APWG:Anti-Phishing Working Group(https://apwg.org)。

成り立ちやInternet-Draft(以後ID)段階から、その仕様をIIRで説明してきました。2015年3月に、そのDMARCの基本部分はRFC7489として公開[*6]されました。当初、DMARCのIDは、標準化を目指したStandard Trackとして公開され、検討されてきましたが、最終的にはInformational RFCとなりました。IETFのDMARC WrokingGroup(以後WG)の動きを逐次把握していなかったので、どのような理由でInformationalに変わったのかをきちんと把握していませんが、2014年の4月にIDがInformationalに変更されたようです。

これまでも指摘されてきたことですが、DMARCには通常利用できていたいくつかのケースで、認証が失敗する問題があります。こうした問題点が標準化に際して影響した可能性は高く、IETFのDMARC WGでも、引き続き取り組むべき課題として挙げられています。この問題は、DMARCと、DMARCの認証の基盤として利用しているSPF及びDKIMとで、それぞれが認証する送信ドメインが異なっていることが原因となっています。これについては、2012年8月に発行した本レポートVol.16[*7]で既に説明しています。

2.3.2 DMARCの課題とレポーティング

現在IETFのDMARC WGで取り組むべき課題としてチャーターにも挙げられている問題は、メールの再配送(indirect mail flow)です。事例として挙げられているケースは以下のような機能を利用した場合で、メールの便利な使い方としてこれまで広く使われてきたものです。

- メーリングリストサーバ
- 自動転送機能
- なんらかの理由でメッセージを改変するメールサーバ

いずれも、メールの最初の作成者と、そのメールを受け取る最終的な受信者からみた直近の送信者が異なったり、その間に介在する機能がメッセージを改変したりすることが根本的な原因となっています。実際、2014年4月に、米国Yahoo!がDMARCレコードのポリシーを"reject"に変更したため、Yahoo!を利用してメーリングリストに参加していた利用者のメールが、メーリングリストからの配送先でDMARCの認証に失敗し、DMARCレコードのポリシーに従ってreject(受信拒否)する事例が発生しました。一方で、DMARCレコードのポリシーを"reject"と宣言して以降、ドメインを詐称したメールに関連した問い合わせが激減してとても良かった、という米国大手銀行の担当者の話しも聞きました。

DMARCの目的は、こうした送信ドメインを詐称したメールを識別して、届かなくさせることですが、それを実現するためには、DMARCレコードのポリシーを"reject"に設定する必要があります。設定すると、前述の例のように大きな影響を及ぼすこともあります。しかしながら、DMARCにはポリシーを"reject"に設定するための移行的な位置づけとして、"none"や"quarantine"のようなポリシーも用意されています。ドメインの管理者は、こうした影響の少ないポリシーを設定しつつ、認証結果を送信側に報告するレポーティングの機能を活用することができます。ドメイン管理者は、このレポートを参照し、正規のメールが認証に失敗しているケースはないのか、"reject"とポリシーを変えた場合の影響はどの程度あるのか、詐称しているメールはどの程度流通しているのかなどを事前に確認することができます。こうしたレポーティングは、メールの受信側が受信したメールの送信ドメインを認証すると共に、認証が失敗したメールの情報をレポートとして送信ドメイン側へ通知することで実現されます。レポーティングは、受信側にとって新たな負荷となります。しかし、DMARCを普及させるためには、こうしたレポーティング機能を提供する、メール受信側が増えることが必要でしょう。

2.3.3 メール受信側のDMARCの利用

送信側からみれば、DMARCレコードを宣言することで、詐称されたメールが受信側に届かなくなるDMARCの利点は大きいと言えます。では、新たな認証機能の仕組みを追加し、更に認証が失敗した情報を送信側にレポーティングまでする受信側に、何かDMARCの利益があるのでしょうか。

これまで、SPFやDKIMなどの送信ドメイン認証技術は、送信者情報を認証(Authentication)する技術で、迷惑メールかどうかを判断するものではない、と何度か述べてきまし

*6　Domain-based Message Authentication, Reporting, and Conformance(DMARC)(https://datatracker.ietf.org/doc/rfc7489/)。
*7　本レポートのVol.16(http://www.iij.ad.jp/company/development/report/iir/016.html)の「メッセージングテクノロジー『送信ドメイン認証技術の普及と認証する識別子』」。

た。認証された送信ドメインは、詐称されていないことを示すだけですので、それが受け取るべきメールかどうかを判断するためには、認可(Authorization)の手続きが必要になります。メールの世界では、この認可の方法として、認証したドメインを元に、受け取るべきメールかどうかを評価するレピュテーションが必要になる、とずっと言われてきました。DMARCにより、SPF及びDKIMでそれぞれ認証したドメインと、最終的にDMARCとして認証するドメインの仕組みができましたので、ようやく統一した方法でドメインを取り出すことができるようになりました。つまり、いまこそ単一のドメインで、レピュテーションを利用して受け取るべきかどうかを判断する、認可の手続きができるようになった、と言えます。

メールの受信側がDMARCを導入する利点は、送信ドメイン認証によって送信元を明らかにし、その送信元(ドメイン)を評価することによって、評価の低い受け取るべきでない不要なメールの受信を減らせることです。メールの受信側は、不要なメールを受信しないことによって、通常行われる受信したメールに対するいくつかの処理、ウイルスチェックや迷惑メールフィルタの判定処理などを軽減できますし、メッセージスプールに保存しなくてもよいことになります。受信側のユーザにとっても、不要なメールを参照し削除するなどの手間を減らすことができますので、ユーザの満足度を上げることもできます。

2.3.4 ドメインレピュテーション

ドメインレピュテーションという言葉には、まだ明確な定義はありません。これまで受け取るべきでないドメインの集合を、ドメインブラックリストと表現する例はありましたし、その逆に受け取るべきドメインとしてホワイトリストと表現することもありました。一般的にドメインレピュテーションは、こうした悪と善の2値(いずれのドメインリストにも含まれていないものも考慮すれば3値)ではなく、その中間的な割合も含めて数値で示したもの、と考えられています。

例えば、これまで迷惑メールを送信したかどうかの明確な実績データのないドメインであっても、そのドメインが作成されてからの経過日数や、ドメインの管理元の素性などの情報から機械的に判断して、ある程度の傾向を数値の幅で表現することは可能でしょう。とはいえ、ドメインレピュテーションの精度を上げるためには、実際に受信したメールの認証結果と、受信者による迷惑メールかどうか(あるいは必要か不要か)の判断の情報がとても有益です。最近、DMARCレコードのレポーティングの宛先として、当該のドメイン名以外を指定しているレコードを見かけます。こうしたレポーティング先は、レポーティングメールを集約して、更に有益なレポートとしてまとめて提供する代わりに、DMARCの認証が失敗した事例を集めて、自社のドメインレピュテーションのデータとしても活用しているようです。このように、ドメインを管理する側とレポーティングを集約する事業者の間には、相互に有益な関係を構築することができますので、こうしたレポート分析とレピュテーションデータを提供する事業者が増えてくるかもしれません。

既に日本でも、受信者が受け取ったメールを迷惑メールとして申告するような仕組みの事例があります。例えば、一般財団法人日本データ通信協会の迷惑メール相談センターでは、メールの転送やWebからの入力によって、迷惑メールの情報を受け付けています。迷惑メール相談センターでは、こうした情報を元に違反行為があった場合に、総務省に報告するなどの処置を行っています。総務省では、集まった情報を元に送信者に対して警告を行ったり、行政措置を実施します[*8]。

迷惑メールとその明確な送信者情報(ドメイン)を、こうした仕組みで集めることができれば、よりドメインレピュテーションの精度を向上させることができます。これまで迷惑メールは、受信側に一方的に送りつけられ、受信側はそれらを個々の努力でなるべく排除しようとしてきました。しかし、DMARCが普及し、迷惑メールの送信者(ドメイン)の情報が広範囲に集約できて、ドメインレピュテーションがそのフィードバックとして提供できるようになれば、より積極的な形で不要な迷惑メールを排除することができるようになるかもしれません。

*8　総務省:迷惑メール対策(http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html)。

2.3.5 メールのエコシステム

図-2は、送信ドメイン認証を含めたDMARC認証、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、受け取ったメールを申告するフィードバックの関係を示した全体像（フレームワーク）です。これは、これまで述べてきた迷惑メール対策を含めた、より良いメールの利用環境を実現するために、それぞれの役割と持続可能な仕組みを含めたエコシステムとなっています。それぞの役割について簡単に述べます。

まず、メールの受信時には、SPF及びDKIM、DMARCでドメイン認証を行います。この時点で、例えばもろもろの問題点が技術的に解決できて、DMARCの認証が失敗し送信側のポリシーが"reject"であった場合は、受け取りを拒否できるかもしれません（あくまで技術的な観点として）。次に、受信して認証したドメインを、ドメインレピュテーションを利用して評価します。認証したドメインがあらかじめホワイトリストに登録されている場合には、状況によってはその後の迷惑メールフィルタを通さずに、メール受信者に届けることができるようになります。迷惑メールフィルタの難しさは、迷惑メールの判定を難しくするような巧妙な迷惑メールをいかに排除するかですが、その一方で、受け取るべき通常のメールを迷惑メールと判断する誤判定（false positive）が発生しないような工夫が求められます。こうしたメールの内容からだけでは判断が難しいメールも、認証したドメイン名がホワイトリストに含まれていれば、容易に受信者に届けることができるようになります。

また、認証したドメインが明らかに迷惑メールを送るドメインであることが分かれば、迷惑メールフィルタを経由するまでもなく、簡単に排除できるようになります。このように、事前に判断できるケースが増えれば、迷惑メールフィルタの設備コストも抑えることができるようになるかもしれません。

以前、メール送信時にSMTP認証するIDとパスワードが悪用されて、正規のメール送信サーバが踏み台にされているケースがあることを報告しました。つまり、正当なメール配信の経路を通っているわけですから、このフレームワークであっても、そのメールの送信側がホワイトリストに登録されていれば、迷惑メールであってもメールが届いてしまうことになってしまいます。こうした場合、受信側がドメインレピュテーションを管理している送信側に、誤判定メールとして申告（フィードバック）することができれば、送信サーバが踏み台にされていることが検知できるようになります。送信側の事業者は、メール送信時のSMTP認証時の記録を参照すれば、そのメールが実際にどこから送信されているのか、物理的な送信者は誰であるのかを調べることができます。例えば、そのPCがマルウェアに感染しているかもし

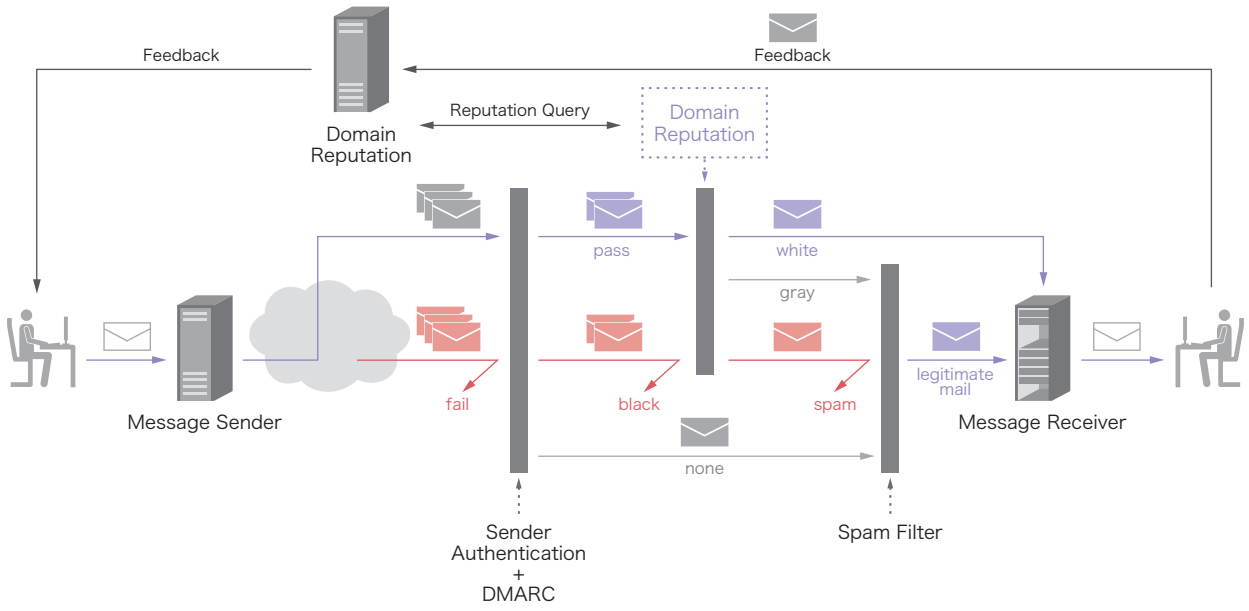

図-2 メールのエコシステム

れませんし、その契約者が明示的に迷惑メールを送信しているかもしれませんが、いずれにしてもメール送信元を確認することができますので、対応が取れるようになります。

2.4 おわりに

昨年、2014年10月に、LAP(London Action Plan[*9])の10回目となる会合、LAP 10 Tokyoが、東京の京王プラザホテルで開催されました。LAPは、迷惑メール対策に関わる各国の行政機関が集まる組織で、現在27ヵ国が参加しています。日本からは、総務省と消費者庁がメンバとして参加しています。私が参加しているM[3]AAWGとも関連が深く、これまでにも時々共同会合を開催してきたこともあり、ここ数年はメンバである総務省と一緒にLAPの単独会合にも参加してきました。これまでLAPの会合は、欧州と北米だけで開催されてきましたが、昨年10回目の会合では、初めてアジア地域である日本での開催となりました。そうした節目の会合を盛り上げるために、私が参加している迷惑メール対策推進協議会でも、LAP 10 Tokyo会合の準備組織としての委員会を結成し、併設した展示会場にパネル出展したり、インターネット協会の迷惑メール対策カンファレンスを同じ会場で開催して、一般の方にも足を運んでもらえるよう工夫をしました。私も、LAPの会議中にこれまでの日本の迷惑メール対策活動について、協議会を代表して発表させていただきました。関係者の様々な努力もあり、LAP 10 Tokyo会合は成功裏に終わり、参加者からも良い会合だったと評価していただきました。

更に、2004年に設立されたM[3]AAWGも、昨年は10年の節目の年でした。2014年10月に開催された32nd General Meetingは、私も参加した最初のFounding Meetingが開催された地、米国ボストンで開催されました。10周年記念会合として、オープニングでは当時のアジェンダが紹介されたり、私を含むこれまで最多の参加回数を誇る3名がスピーチを行いました。

10年前、こうした行政機関や民間組織が集まった頃は、迷惑メール対策活動が10年も続くとは思ってもいませんでした。日本でJEAG[*10]を立ち上げたのが2005年で、その前身となる組織を含めると10年経過したわけですが、これも発足当時は長く活動するつもりはありませんでした。迷惑メールに関わる問題が、ここまで長引くとは思わなかったのです。そのため、JEAGもきちんとした組織とはせずに、すべて関係者のボランティアとして活動してきたわけです。さすがにそうした組織形態を長く続けることはできずに、半ば自然消滅的に終息していったわけですが、活動の意義やそうした組織の重要性は10年経過した今も変わっていないようです。これは、電子メールというシステムが、一部の人だけが使う補助的なツールから、社会基盤の1つとして、より重要性を増してきたことが理由かもしれません。

本来、こうした迷惑メール対策活動が必要なくなる状況が望ましいと思っていますが、現実にはなかなか難しいかもしれません。せめて、もう少し安心してメールが使える環境に進化させていければと考えております。

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2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。一般財団法人インターネット協会 迷惑メール対策委員。

*9 London Action Plan(http://londonactionplan.org)。
*10 JEAG:Japan Email Anti-Abuse Group(http://jeag.jp)。