メッセージングテクノロジー

1.1 はじめに

フィッシング対策協議会の報告[*1]によれば、協議会に寄せられたフィッシングの報告件数が急増しています。2020年4月には11,645件が報告されており、これは前月（2020年3月）から1,974件の増加であり、前年同月（2019年4月）から9,257件もの大幅増加となっています。内容としては、インターネットを活用する大手事業者をかたったものが大量配信されているようです。実際、私のところにも何通か届いていますが、表題（Subjectヘッダ）や送信者（Fromヘッダ）のディスプレイネームやローカルパートはそれらしい文字列となっていますが、送信者のドメイン名は全く異なっている場合が多いようです。また、行政機関になりすました詐欺的なメールが増えてくる可能性もありますので、なりすまされる可能性が高いドメインの所有者、メール受信側それぞれで対策を講じるべきです。

これまでも何度も報告してきたとおり、フィッシングメールなどのなりすましメールの対策としては、送信ドメイン認証技術が有効に機能します。しかしながら、フィッシングメールの送信者もこうした対策は把握しているようですので、有効活用するための正しい使い方が重要となります。また、こうしたメールが増えている背景としては、昨今の社会状況も反映しているのではと推測されますので、しばらくは続くかもしれません。

本報告では、なりすましメール対策に有効である送信ドメイン認証技術（SPF、DKIM、DMARC）の普及状況について報告します。また、送信ドメイン認証の結果を、現在流通しているフィッシングメールに対して活用する方法についても述べます。更に、昨年開催されたJPAAWG 2nd General Meetingの様子についても報告します。

1.2 送信ドメイン認証技術の普及状況

最初のSPF（Sender Policy Framework）の仕様であるRFC4408[*2]が2006年4月に発行されてから14年が経過しました。その後、電子署名を利用するDKIMが仕様として作られ、SPF、DKIMの認証結果を利用するDMARCも作られました。これらの送信ドメイン認証技術が、現在どの程度普及しているかについて報告します。

＊1　フィッシング対策協議会 | 月次報告書一覧（https://www.antiphishing.jp/report/monthly/）。
＊2　その後2014年4月に改定されてRFC7208となった。

1.2.1 受信メールに対する調査結果

送信ドメイン認証技術の普及率を調査する観点として、実用上の効果を考えれば、メール受信時の認証結果の割合が重要であると考えることができます。IIJが提供するメールサービスでは、メール受信時にSPF、DKIM、DMARCの送信ドメイン認証機能を提供しています。受信メールのうち、それぞれで認証ができなかった場合の結果はnoneとなります。つまり、受信メールに対しての認証結果noneを除いた割合が受信メールに対する普及率の割合と言えます。

最新の2020年4月に受信したメールに対しての、SPFの認証結果の割合を図-1に示します。認証結果noneの割合は12.1%、つまり普及率は87.9%であったと言えます。1年前のIIR Vol.43では普及率が85.7%でしたので、2.2%増加したことになります。SPFによる認証成功を示すpassの割合は、2019年4月の70.1%から2020年4月には79.1%に9%増加しています。つまり認証失敗（SPFの場合はhardfail、softfail、neutral）の割合も6.4%減っていますが、これはSPFとしてなりすまさないメールが増えたことを示しています。しかし、いわゆるなりすましメール自体が減少しているわけではないことは、フィッシングメール報告の増加からも推測できます。つまり、SPFとしてはなりすまさない、なりすましメールが増えている可能性があります。

2020年4月に受信したメールに対してのDKIMによる認証結果の割合を図-2に示します。認証結果noneの割合が51.7%となり（普及率48.3%）、1年前の62.2%から10.5%減少、普及率としては10.5%増加したと言えます。メール送信側としてDKIMを導入するためには、送信時のメールサーバなどで、DKIMの電子署名を追加する必要があり、送信側の導入には手間がかかります。現在の普及率が十分な割合とは言えませんが、それでもDKIMの最初の仕様であるRFC4871が公開されて13年が経過し、ようやく受信メールの半分程度まで普及してきたことになります（IIJの受信メールに対する割合としてです）。

2020年4月に受信したメールに対してのDMARCによる認証結果の割合を図-3に示します。認証結果noneの割合が75.4%なので、普及率は24.6%であると言えます。1年前からは1.5%

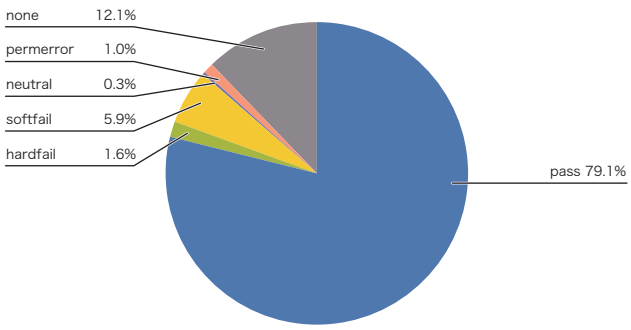

図-1 SPFによる認証結果割合

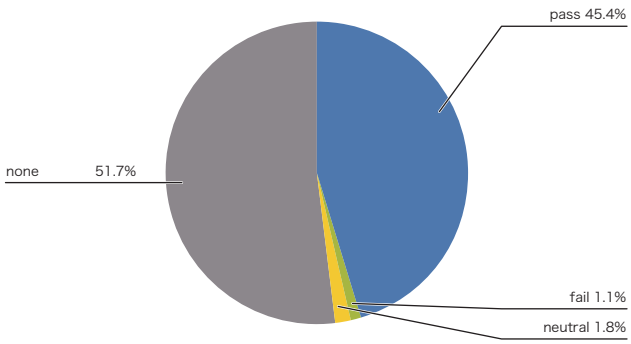

図-2 DKIMによる認証結果割合

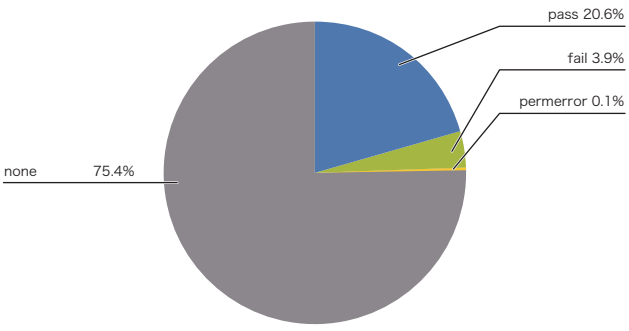

図-3 DMARCによる認証結果割合

増加しました。ほぼ実用上普及したと言えるSPFや一般的に導入にコストが伴うDKIMと比べると、非常に低い増加です。DMARC導入には、SPFあるいはDKIM、またはその両方の導入が必要ですが、それらを導入さえしていれば、SPFと同様にDNS上にDMARCレコード（テキスト資源レコード）を記述するだけでDMARCは導入できます。むしろ送信メールサーバの出口を調べなくても良いので、DMARCレコードの方が簡単に設定できるはずです。そうした背景がありながら、SPFやDKIMより割合としての増加値が少ないことの理由は、単に認知していないのか、DMARCレコードを記述する動機が不明と考えているのか、まだよく分かっていません。今後も普及のための活動を継続していきたいと考えています。

図-4に2016年1月からのDMARCの認証結果の割合の推移を示します。このグラフからも、2020年4月が時期的に極端に低かったということではなく、少しずつDMARCに対応した送信ドメインは増えてきているものの、その伸びが非常に緩やかであったことが分かります。

図-5に、DMARCがpassしたドメイン名のTLD（Top Level Domain）の割合を示します。これは、受信したメール量に対する割合ではなく、DMARCドメイン名別（ユニークなドメイン名）のTLDの数の割合です。最も割合が高いTLDは.comで53.2%でした。続いて2番目に割合が高いのが.netで9.5%、日本の.jpドメイン名が3番目で6.7%でした。SPFがpassしたドメイン名のTLDでも.comが最も多いTLDでしたので、順位的には大きな違いはありませんでした。

1.2.2 ドメイン名に対する調査結果

送信ドメイン認証技術の普及率に関するもう1つの観点は、登録されているドメイン名に対して、各送信ドメイン認証技術に関連するレコードがどの程度登録されているかを調べることです。そのためには、対象の範囲を決めてそこに属するすべてのドメイン名を得る必要があります。

IIR Vol.39でも報告したとおり、jpドメイン名に対する調査を、（株）日本レジストリサービス（JPRS）と協力して実施しており、

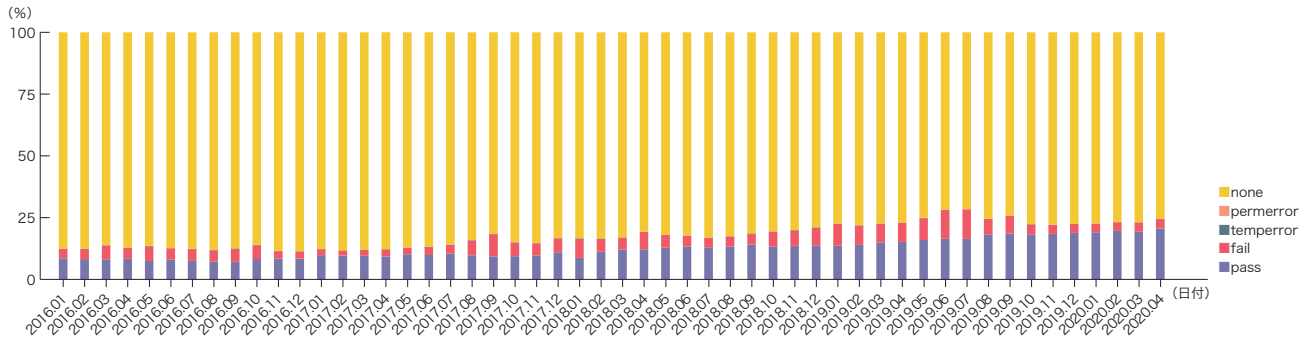

図-4 DMARCによる認証結果割合の推移

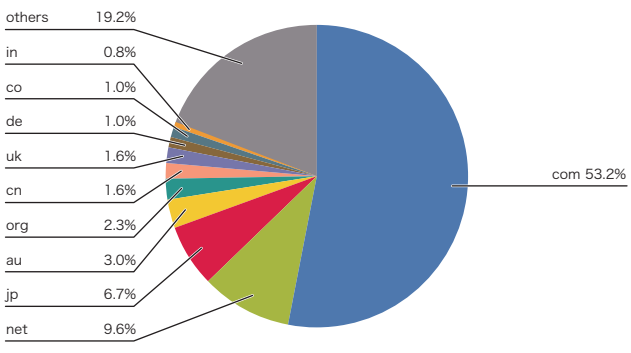

図-5 DMARCドメイン名のTLDの割合

現在は(一財)インターネット協会(IAjapan)との間で共同研究契約を結んでいます。筆者はIAjapanの立場で設定状況を調査しています。

DKIMは、電子署名のための情報(DKIMレコード)を取得するためにDKIMのセレクタ名が必要ですが、セレクタ名はメールのヘッダに指定されているため、ドメイン名からだけではDKIMレコードの場所を得ることができません。DKIMレコードが設定されているかを推測できる場合もありますが[*3]、必ずしも正確ではありません。そのため、DKIMの普及状況に関する調査結果は公開しておらず、SPFとDMARCのみが公開されています[*4]。いずれも、メールに利用されているドメイン名であることを確認するために、MX資源レコードが設定されているドメイン名に対しての割合となっています。もちろん、メールに利用しないドメイン名に対するSPFやDMARCレコードの設定方法(最近ではMX資源レコードについても)もありますが、これらの詳細はまた別の機会に報告したいと思います。

今回は、これらSPFとDMARCの最新の調査結果を含めて報告します。SPFは、調査開始当初の2018年3月にはjpドメイン名全体の平均で57.3%でした。最新の2020年5月の調査結果では65.1%となり、7.8%増加しています。

DMARCのjpドメイン名での普及率の推移を図-6に示します。2018年3月が0.57%で、2020年5月では1.19%となり、0.62%増加しました。割合は2年ほどで倍増はしましたが、そもそもの設定割合が低いのと、増加自体もSPFに比べても非常に低い値であり、いずれの数値も非常に低い結果となりました。属性別で現在最も設定割合が高いのはgo.jpドメイン名で、それでも5.4%です。go.jpのSPF設定割合は92.4%ですので、DMARCレコードの設定もSPFと同様の取り組みで、率先して設定を増やすことを期待しています。

1.2.3 なりすましメール対策としての送信ドメイン認証技術

現在の社会状況により、行政機関などによる様々な施策が行われており、その過程でメールによる連絡が増えてくることが予想されます。また、外出を避ける傾向からオンラインでの購入などが増えているようです。これらの状況を反映して、フィッシングメールやなりすましメールによる詐欺的行為が増えているかもしれません。

例えば、Amazon社になりすますメールがいくつかのパターンで頻繁に送信されていますが、Amazon社からのメールは、SPF、DKIM、DMARCいずれも対応しており、これらの送信ドメイン認証を行えば、なりすましメールかどうかを判断することができます。また、SPFの認証失敗時には、最も強い失敗failとなるようにSPFレコードの末尾が"-all"となっており、DMARCのポリシーも比較的強めの"p=quarantine"と設定されています。つまり、Amazon社では送信ドメイン認証技術を積極的に取り入れ、なりすましメール対策を強化していると言えます。Amazon社をなりすますメールで気をつけなければならないのは、認証したドメイン名が正しいかを確認する必要もあることです。日本でAmazon社が利用するドメイン名はamazon.co.jpですが、なりすましメールの多くは、全く関係のない別のドメイン名を用い、SPFやDMARCがpassするようなりすましメールを送信します。件名(Subjectヘッダ)や送信者(Fromヘッダ)の表示名(display name)にはAmazonの文字列が含まれています。そのため、きちんと認証されたドメイン名も含めて確認することがだまされないためには大事です。

＊3　ドメイン認証の普及率に対する測定方法(http://member.wide.ad.jp/wg/antispam/stats/measure.html.ja)。
＊4　迷惑メール対策|統計データ(https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei)。

図-6に示した属性別のjpドメイン名の中で、調査開始当初から継続してDMARCの導入割合が最も低いのは、地方公共団体などで利用されるlg.jpドメイン名です。地方公共団体がlg.jpだけを使っているわけではないと思いますが、示している導入割合はMXレコードを設定しているドメイン名に対するDMARCレコードの設定割合ですし、SPFレコードの導入割合はgo.jpに続く80.7%と高い普及率でした。これも同様に、なりすましメール対策するためには、まずDMARCレコードを設定することでヘッダ上の送信ドメインを守ること、更にどれだけ当該ドメイン名をなりすましたメールが送信されているのかを理解するために、DMARCレポートを受信する設定を行い、状況を随時把握できるようにしておくことが必要と考えています。

1.3 JPAAWG 2nd General Meeting

2019年11月14日と15日の2日間で、JPAAWG 2nd General Meeting（GM）をベルサール飯田橋ファーストで開催しました（図-7）。2018年と同様にIAjapan主催の迷惑メール対策カンファレンスとの併催です。IIJはプラチナスポンサーとして、1stに引き続きサポートしました。

2nd GMでは、1st GMの結果を踏まえ、以下のような新たな試みを行いました。

1. 2日間での開催
2. M^{3}AAWGメンバーなど海外からの多くの講演や参加
3. トレーニングセッション（有料）の開催
4. Open Round Tableによるディスカッション

特にOpen Round Table（ORT）は、M^{3}AAWG[*6]のGeneral Meetingでも毎回開催されている、テーマごとに興味を持つ参加者が集まって議論するセッションです。M^{3}AAWGでは、このORTから新しい技術仕様やBest Practicesなどの文書が作られる発端にもなる、いまや活動の原動力の1つです。今回JPAAWGでは、5つのテーマを用意し、JPAAWGメンバーらのモデレータが進行を務め、一方的ではない参加者相互による議論を行うことができました。JPAAWGでは、課題の共有や解決のための検討の場として、ORTのような取り組みを継続していきたいと考えています。

2020年度も、JPAAWG 3rd General Meetingを同様に開催したいと考えていました。しかしながら、現時点では多くの人が集まっての開催がなかなか難しい状況となっています。現在、どういった形式で開催できるのかを検討している段階ですので、決まり次第Webサイト[*7]などで告知します。

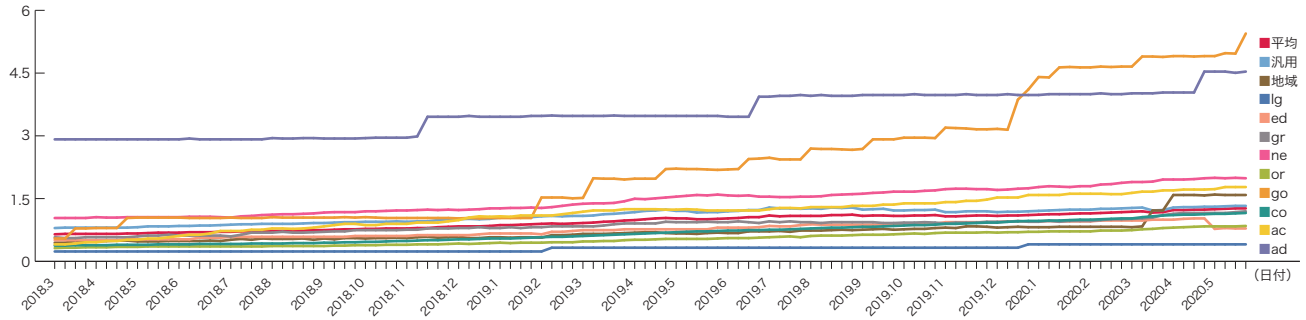

図-6 jpドメイン名[*5]のDMARC普及割合の推移

＊5　地域型（新規登録終了）には都道府県型を含む。
＊6　Messaging, Mobile and Malware Anti-Abuse Working Group（https://www.m3aawg.org）。
＊7　Japan Anti-Abuse Working Group（JPAAWG）（https://www.jpaawg.org/）。

1.4 おわりに

2020年1月22日から24日に札幌で開催されたJANOG45ミーティングに参加し、「フィッシングの現状とその対策」のセッションで発表を行いました。本稿でも述べたとおり、送信ドメイン認証技術、特にDMARCがあまり普及していない現状から、多くの関係者にまず理解してもらうべきと考え参加しました。また、2020年2月17日から20日に米国サンフランシスコで開催されたM^{3}AAWG 48th General Meetingでも、JPAAWGのBoF会合を引き続き開催すると共に、JPAAWGの活動内容を「State of Messaging Anti-Abuse in Japan」のセッションで他のJPAAWG/M^{3}AAWGメンバーと共に紹介してきました。

このように2020年は、国内と海外でそれぞれ講話をする機会が得られ、より積極的な情報発信を目指していましたが、ご承知のとおりその後の状況変化により、様々な会合が開催形態の見直しを余儀なくされています。しかしながら、我々はインターネット上の様々なツールが正しく使われていくことを目指す活動をしているのですから、こうした状況においてもコミュニケーションできるように、またそうしたツールが悪用されないような取り組みをしていくべきと考えています。

図-7 JPAAWG 2nd General Meetingの様子

執筆者:
櫻庭 秀次（さくらば しゅうじ）
IIJネットワーククラウド本部アプリケーションサービス部担当部長。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。Japan Anti-Abuse Working Group（JPAAWG）会長。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客員研究員、迷惑メール対策委員会委員長。一般財団法人日本情報経済社会推進協会（JIPDEC）客員研究員。