# 迷惑メール最新動向

## 2.1 はじめに

IIRのメッセージングテクノロジーでは、迷惑メールを中心としたメールの動向と、迷惑メール対策に関わる技術動向について報告します。

迷惑メールの量自体は、本報告の開始当時(2008年)に比べれば大幅に減少しましたが、様々なメディアでも報道されているとおり、セキュリティ的な脅威は益々高まっています。現在のメールシステムは、単なる迷惑を取り除くという視点から、セキュリティ的な脅威をいかにして軽減させるか、という課題に直面していると言えます。攻撃者からみれば、メールは各種防御で守られた組織内部に情報を届けることができる、数少ない経路の1つであることから、今後も様々な試みに悪用されることが予想されます。

今回は、1年分の迷惑メール割合の推移と、この間に発生した迷惑メールに関わるトピックスを報告します。また、迷惑メール対策としても有効なDMARCとその関連技術の動向、日本での普及状況について報告します。

## 2.2 迷惑メールの動向

ここでは、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。

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.31)から1年以上の調査結果を含む、2015年から2年以上となる122週間のデータです。具体的には、2015年の第1週(2014年12月29日からの1週間)から2017年の第17週(2017年4月24日の週)までの期間です。これより前のデータについては、IIR Vol.31及びVol.27を参照してください。

2016年度の迷惑メールの平均割合は38.5%でした。2015年度が24.2%でしたので、昨年度は前年度から14.3%増加したことになります。ここ数年は減少傾向が続いていたのですが、昨年度から増加傾向に転じたようです。図-1のグラフをみても、2016年度は変動の幅は大きいのですが、全体として増えていることが分かります。

図-1のグラフでは、2016年12月中旬から2017年3月まで、急激に迷惑メールが減少しています。Sophos社の記事[*1]でも同様の傾向が示されており、その理由としてNecursというボットネットが活動を低下させているようだ、との報告がありました。その後2017年3月以降、迷惑メールの割合が増加に転じていますので、ボットネットの活動低下は一時的なものだったようです。

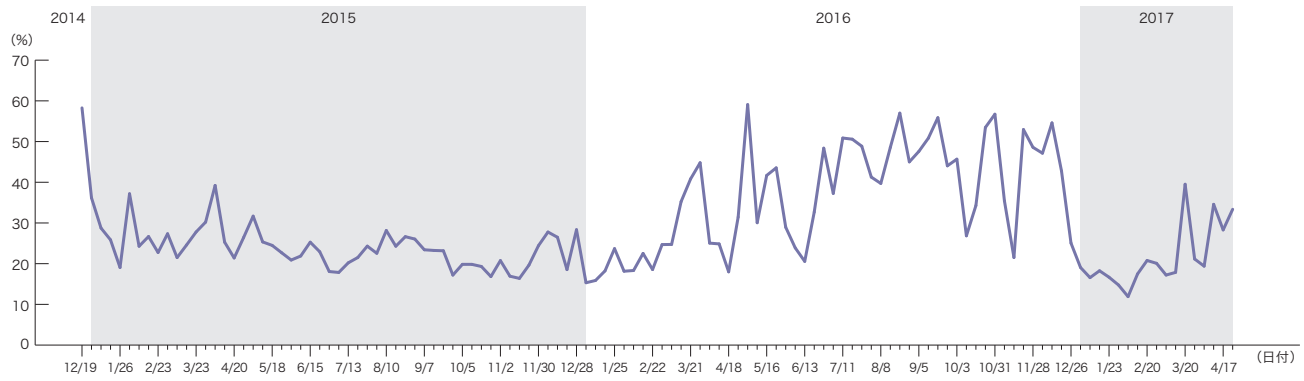


**図-1 迷惑メール割合の推移**

*1　世界的に半数以下に激減するスパムメール(http://sophos-insight.jp/blog/20170315)。

### 2.2.1 送信ドメインの不正利用

迷惑メールの中で悪質なものの1つにフィッシングがあります。これは、迷惑メールの中に示されたURLなどにアクセスしてしまうことで、実在のサイトを模倣した偽のサイトに騙され、IDやパスワードなどの重要な情報を入力させ搾取する手口の1つです。最近では、日本のユーザ向けに日本語で記述されたフィッシングメールや偽のサイトなど、巧妙に作られたものも多く、警察庁のレポート[*2]でも引き続き金銭的な被害が発生していることが報告されています。

こうしたフィッシングメールを受け取らない対策や受け取ったときに騙されないことは重要ですが、こうしたメールの送信者情報に悪用されないための対策も忘れてはいけません。

フィッシング対策協議会のWebサイト[*3]やマイクロソフト社[*4]でも度々注意喚起が行われましたが、2017年1月から3月にかけて、マイクロソフトを騙るフィッシングメールの大量送信が何度か発生しました。いずれも表題(Subject: ヘッダ)は日本語で記述されており、筆者に直接届いたメールだけでも表-1のものがありました。

これらのメールは、当初は送信者情報として以下のドメインを利用しており、メールのHTML部分のリンク先のURLにも同じドメインを利用していました。

| 日付 | Subject |
|---|---|
| 01/12 | ご注意！！OFFICEのプロダクトキーが不正コピーされています。 |
| 01/30 | ご注意！！OFFICEのプロダクトキーが不正コピーされています。 |
| 03/17 | 警告！！マイクロソフトのプロダクトキーが不正コピーされている恐れがあります。 |
| 03/31 | [大切]マイクロソフトのプロダクトキーが不正コピーされた警告です！ |

表-1 マイクロソフトを騙るメールの表題

```
microsoft-securityprotection-support.com
support-securityprotection-microsoft.com
```

これが3月に送られたメールでは、いずれの送信者情報[*5]もメールごとに別のドメインが用いられていましたが、メールのリンク先はほぼ固定のURLが利用されていました。

注目すべき点は、これらの送信ドメインは、送信ドメイン認証技術(SPF、DKIM、DMARCいずれも)の認証結果がすべて'none'だったことです。直接届いたメール以外も簡単に分析してみましたが、ほぼSPFの認証結果は'none'でした。総務省の統計データ[*6]では、最新の調査結果では'none'の割合は9.26%ですので、3月に大量送信されたメールは、意図的にSPFに対応していないドメインを選んで利用したことが考えられます。

更に、手元に届いたメールの実際の送信元は、大半が海外から送信されていましたが、利用されたドメインの約8割のTLDが'jp'でした。日本語で記述されたメールですので、意図して'jp'ドメインを利用した可能性はありますが、SPFに対応していない 'jp'ドメインがこれ程実在していることも今後の課題だと考えています。

例えメールに利用していないドメインであっても、SPFの設定は必要です。迷惑メール対策推進協議会が発行した「送信ドメ

＊2　平成28年中におけるサイバー空間をめぐる脅威の情勢などについて(http://www.npa.go.jp/kanbou/cybersecurity/H28cyber_jousei.pdf)。
＊3　マイクロソフトをかたるフィッシング(https://www.antiphishing.jp/news/alert/microsoft_20170331.html)。
＊4　マイクロソフトを装った不審メールの配信について(https://www.microsoft.com/ja-jp/office/2016/attention5.aspx)。
＊5　送信者情報には、MUA(メーラ)などで表示されるヘッダFrom (RFC5322.From)とメール配送上で利用されるエンヴェロープFrom (RFC5321.From)がありますが、今回両方とも同じドメインが利用されていました。
＊6　送信ドメイン認証結果の集計(SPF)(2016年12月時点)(http://www.soumu.go.jp/main_content/000468608.pdf)。

イン認証技術導入マニュアル第２版」[*7]では、メールを送信しないドメインの記述例を下記のとおり載せています。この設定例では、必ずSPFが'fail'の結果となります。

Sample 6: メールを送信しないドメイン

管理しているドメインがまったくメール送 信しない場合は、
"-all" を利用して、その旨を公開できます。

```
example.org. IN TXT "v=spf1 -all"
```

こうした設定例は、2006年2月に発行した「JEAG Recommendation ～送信ドメイン認証について～」でもRecommendation 2.として前述の内容を提言しています。また最近では、SPFの設定例も含めて新たにメールに利用しない"Null MX"レコードの設定方法を示したRFC7505[*8]が発行されました。

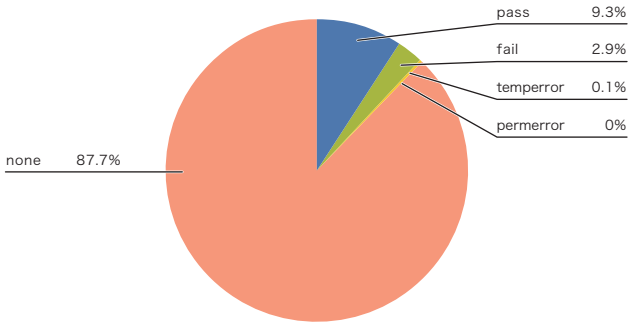


図-2 DMARCの認証結果割合（2017年4月）

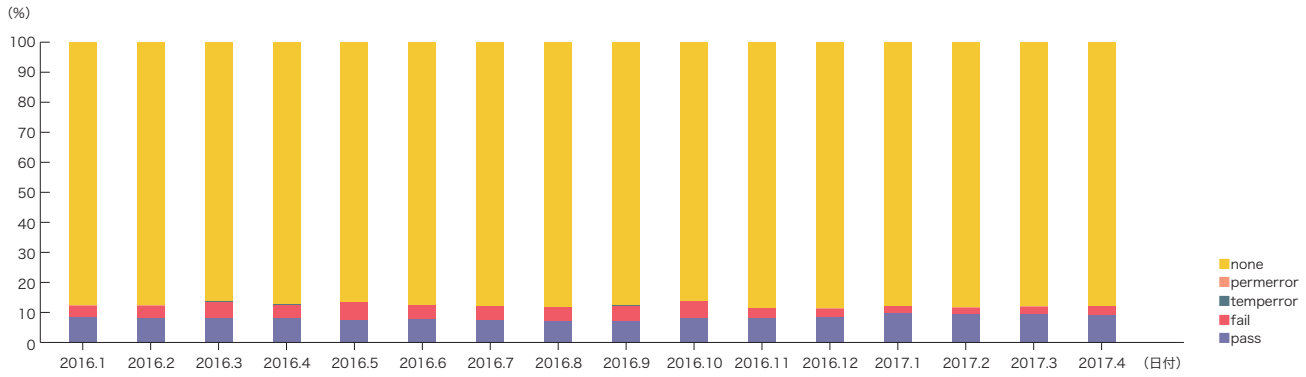


図-3 DMARCの認証結果割合の推移

送信側のドメインとして、メールを受け取ってもらうための送信ドメイン認証技術の導入も必要ですが、迷惑メール送信に悪用されないための、ドメインを守るための設定も忘れずに必要になると考えています。

## 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[*9]の普及状況や技術動向について報告します。

DMARCは送信ドメイン認証技術のSPFとDKIMを基盤に、送信側から受信ポリシーを示したり、受信側での認証結果をレポートで受け取れることで、より正当なメールが送受信しやすくなるための技術です。そうした状況を作り出すためにも、DMARCが今後普及していくことが望まれます。

### 2.3.1 DMARCの普及状況

IIJのメールサービスでは、受信したメールについてDMARC認証を行っています。図-2に示したグラフは、直近の2017年4月に受信したメールのDMARCの認証結果の割合を示したものです。認証結果"none"は、受信したメールの送信ドメインが、DMARCを導入していなかったことを示す認証結果です。"none"が87.7%ですので、9割近い受信メールがまだDMARCに対応していないこと示しています。

＊7　送信ドメイン認証技術導入マニュアル第２版（http://www.dekyo.or.jp/soudan/anti_spam/report.html#dam）。
＊8　RFC7505: A "Null MX" No Service Resource Record for　Domains That Accept No Mail（https://www.ietf.org/rfc/rfc7505.txt）。
＊9　Domain-based Message Authentication, Reporting, and Conformance（DMARC）, RFC7489（https://www.ietf.org/rfc/rfc7489.txt）。

次に、2016年1月からの認証結果割合の推移を図-3に示します。残念ながら"none"の割合が87%前後で推移しており、ほとんど変化のない結果となりました。既にSPFやDKIMを導入していれば、DMARCレコードを記述するだけで送信側のDMARCは導入できたことになりますので、こうした認証率の低さは、DMARCが国内であまり認知されていないことを示しているものと考えています。

### 2.3.2 DMARC普及に向けて

DMARCの認知率の低さを確認するために、受信したメールをSPFとDKIMとDMARCについて、それぞれの認証結果の組み合わせを調べてみました(図-4)。対象は、図-1と同じく2017年4月です。

いずれかの認証結果が"pass"だったものは、そのまま示しています。例えば"DMARC+SPF+DKIM"のデータ項目は、DMARCとSPFとDKIMのすべての認証結果が"pass"だったことを示しています(グラフでは6.7%の割合)。逆に"! ()"で括られたデータは、いずれの認証結果でも"pass"だったものはなく、逆に"fail"などの認証が失敗した認証技術の組み合わせを示しています。例えば、"!(SPF)"のデータ項目は12.5%ありますが、これはDKIMとDMARCでは認証できなかった(認証結果としては"none")が、SPFだけの認証結果が失敗なもの、つまり"hardfail"、"softfail"、"neutral"のいずれかの認証結果だったことを示しています。

このグラフでは、DMARCでは認証できていないが、SPFあるいはDKIM、あるいはその両方で認証できた割合が56.5%もあります。つまり、受信したメールの半分以上が、本来DMARCレコードを記述するだけで、DMARCとして認証できる状態、潜在的にDMARC普及率を向上できる送信元であったと言えます。もちろん、第三者署名の課題など、単純にDMARC認証できないケースに該当することでDMARCレコードを記述できていない可能性は考えられますが、そうした場合でも、DMARCポリシーを強い設定にしなければ、現状悪影響はあまりありませんので、やはり普及率の低さは認知度に影響していると考えています。

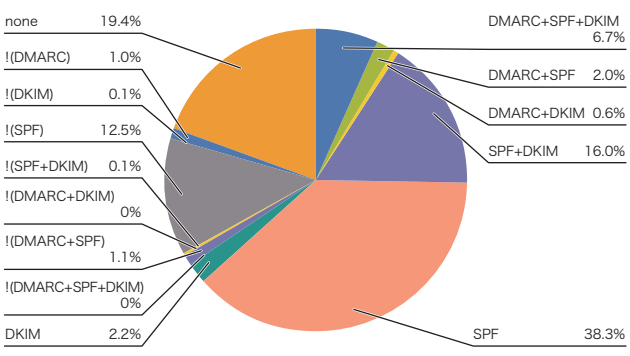


図-4 送信ドメイン認証結果の組み合わせ(2017年4月)

送信側でDMARCを導入することは簡単です。例えば、"iij.ad.jp"ドメインにDMARCレコードを設定するには、"_dmarc"サブドメインを作成し、そのTXT資源レコードにまず以下の設定をしてみてください。

```
_dmarc.iij.ad.jp IN TXT "v=DMARC1; p=none"
```

SPFかDKIMを導入しているのであれば、最初の設定としては、これで十分です。パラメータ"p="の意味は、認証が失敗した場合に送信側から受信側に求める処理のポリシーを示す値で、表-2の値が設定できます。"none"は隔離や受信拒否などを求めない値となりますので、仮にSPFやDKIM、DMARCで認証失敗したとしても、正しくDMARCの仕様に沿った処理をする受信側に対しては、悪影響はありません。このように、送信側メールサーバのIPアドレスなどを調べる必要もありませんので、SPFレコードより簡単に設定することができます。

更に、"rua="や"ruf="のパラメータを正しく設定すれば、機能に対応しているメール受信側から、認証結果のレポートを受信できるようになります。これらのレポートを参照することで、これまで確認することができなかった、SPFやDKIMが正しく認証できていなかったメール送信経路を明らかにできたり、自組織を詐称したメールがどこからどの程度送信されているか、を知ることができるようになります。これにより、正しいメー

| policy | 意味 |
|---|---|
| none | 特別な処理を要求しない |
| quarantine | 不審なメールとしての取り扱い(隔離やタグ付けなど)を求める |
| reject | 受信拒否(SMTP上での)を求める |

表-2 DMARCレコードのポリシー

ルの配送経路を正しく認証できるように修正したり、詐称メールがメール受信者に届かないように、より強い"reject"などのDMARCポリシーを設定することができるようになります。

ただし、"rua="を指定することで受け取れるようになる集約レポート（aggregate report）は、XML形式のデータで、更に圧縮されたMIME形式のメールで届きますので、実際にデータを参照するためには、ある程度の準備が必要となります。最近では、こうしたレポートを代わりに受信し、視覚的にデータとして提示するサービスもありますので、それらを利用する、という方法もあります。

### 2.3.3 DMARCレポートの委譲

DMARCレポートを自ドメイン宛て以外に送信する場合、つまりレポートの受信を委譲するためには設定が必要になります。これは、勝手に第三者をレポート先に指定し、詐称メールを大量に送信することで無用なレポートが無関係の第三者に送信されてしまうことを防ぐためです。DMARCレポートを委譲する側と委譲される側の間で、双方の関係が見えるような設定が必要になります。具体的には、DMARCレコードのレポート先に示されたURIがそのレコードのドメインと無関係である場合、図-5のように委譲先でのDNS設定が必要になります。

図-5は、"example.jp"のレポートの委譲先に"example.com"を指定した場合です。この場合、"example.com"側では、"example.jp"のDMARCレポートを受け取ることを示すために、"example.jp._report._dmarc.example.com"にTXT資源レコードに"v=DMARC1"を設定します。レポートを送信するメール受信側は、送信時にDNSを参照することで委譲関係を確認します。

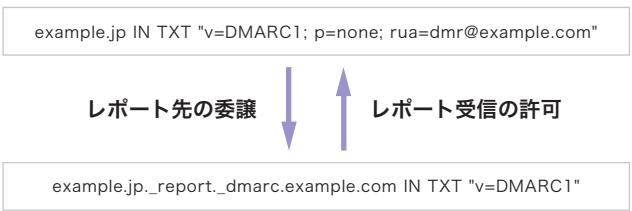


図-5 DMARCレポート委譲時の設定

### 2.3.4 DMARCポリシー

DMARCの普及あるいは送信ドメイン認証技術全体がどの程度普及しているかを示す指標の1つとして、DMARCレコードで設定しているポリシーを確認する方法が考えられます。つまり、より強いポリシーを設定しているドメインの割合が高ければ、正規のメールが認証失敗する可能性がほとんどない状態と判断して設定していると考えられます。ドメインごとのDMARCポリシーの宣言内容の割合を図-6に示します。

"none"の割合が76.4%と高い結果となりましたが、それでも"reject"の割合が11.0%ありました。1割以上のドメインが、最も強いポリシーを設定しているということは、送信ドメイン認証技術が徐々に普及してきている、認証結果を利用して不要なメールを受け取って欲しくない、と考えるドメイン管理者がある程度存在している、ということを示しています。DMARC認証できるメール割合の増加と共に、より強いDMARCポリシーの割合についても今後注目していきたいと考えています。

なお、"error"については、DMARC認証したメール受信時と、調査のためDMARCレコードを参照したときとの時間差があるため、その後ドメインが参照できなくなったなどのDNSエラーを示しています。6.1%と比較的高い割合ですが、とりあえず受け取ってもらうためにドメイン名あるいはそのDMARCレコードを立ち上げた、という場合が少なからずあるのかもしれません。

### 2.3.5 DNS側の対応

DMARCレコードを設定する場合、DNSサービスを提供する側の対応が必要になる場合もあります。これまで述べてきたとおり、DMARCレコードは"_dmarc"というサブドメインが必要になり

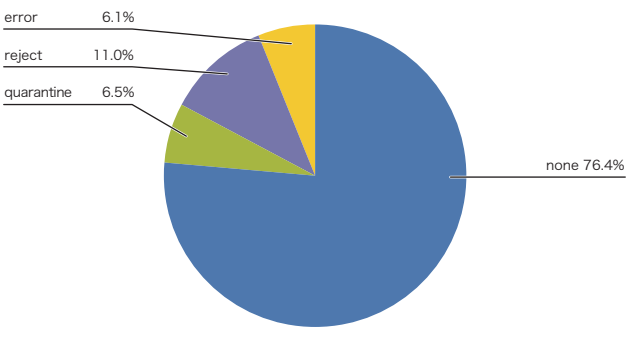


図-6 DMARCポリシーの割合（2017年4月）

ます。また、DMARCレポートの委譲にも"_report"というサブドメインが必要ですし、DKIMを導入する場合にも"_domainkeys"が必要になります。ところが、DNSを提供する側でこの"_"(アンダースコア)文字を使えない場合があるようです。そのため、DKIM、DMARCを導入する場合は、自ドメインで利用しているDNSサービス側の仕様を確認しておく必要があります。

更に、最近ではメールシステムを他社が提供するクラウドサービス上で利用することが多くなりました。こうしたサービスでDKIMを導入する場合、電子署名の第三者署名となるのが一般的ですが、第三者署名ではDMARCの認証が失敗します。これは、ヘッダ上の送信者ドメインと署名を作成するクラウドサービス側のドメインが異なるためです。双方のドメインを管理していれば、DKIMの鍵の設定や更新などの鍵管理が比較的簡単にできますが、それぞれの管理が異なっている場合には何らかの連携作業が必要になります。これを解決するため、DNSのCNAMEレコードを利用する方法がマイクロソフト社によって示されています[*10]。ところが、利用しているDNSサービスによっては、このCNAMEレコードがそもそも利用できなかったり、CNAMEレコードが指し示すレコードとしてTXT 資源レコードが設定できなかったりする場合もあるようです。これについても、利用しているクラウド型のメールサービスやDNSサービスを事前に確認しておく必要があります。

## 2.4 おわりに

これまでも何度か報告してきたとおり、迷惑メールの問題は明らかに量から質へ変化してきており、質の面ではより危険性が高まってきています。最近でも、感染することでPC内部のファイルを暗号化し、解読キーを入手するために金銭を要求するランサムウェアが全世界的に問題となりました。また、PC内部の情報を搾取することで情報漏えいを引き起こす不正プログラム(マルウェア)に感染したと思われる事例が引き続き発生しています。こうしたインシデントを発生させないためには、ランサムウェアやマルウェアに感染させない対策が必要なことは言うまでもありませんが、感染経路の特定も含め、その対策は簡単ではありません。

こうした状況の中で、電子メールシステムはこれまでの仕組みをなるべく維持しながら、様々な対策のための技術を開発し提案してきました。特になりすましメール対策としての送信ドメイン認証技術は、DMARCによってある程度の完成形に近づいたのではないかと考えています。もちろん、メールの再配送時の課題やDKIMの第三者署名問題などの課題はありますが、それぞれある程度の技術的な運用やARC(Authentication Results Chain)などで補完できる方法が示されています。また日本では、こうした技術的な対策の導入については、法的な課題も少なくありません。こうした課題に対して過去には、OP25B(Outbound Port 25 Blocking)や送信ドメイン認証技術SPFやDKIMの導入に際しての留意点などが整理されてきました。DMARCについても、DMARCのポリシー適用やDMARCレポートの送信について同様の課題があります。こうした課題については、迷惑メール対策推進協議会を中心に検討が進められている状況です。

本レポートでも報告したとおり、DMARCの普及状況はまだこれからといった状況であり、その原因の多くはDMARC自体の認知度の少なさが原因と考えています。本レポートが、そうした認知度の向上に寄与し、DMARCが普及していくことをメールセキュリティの観点からも強く希望しています。

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 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。
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。Email Security Conference プログラム委員。

*10 DKIMを使用して、Office 365のカスタム ドメインから送信される送信電子メールを検証する(https://technet.microsoft.com/ja-jp/library/mt695945(v=exchg.150).aspx)。