# DMARC.orgが推進する技術仕様DMARC

**今回は、2012年第1週から13週までの迷惑メールの推移を報告します。**
**迷惑メール送信元地域の第1位は前回と同様に中国でした。**
**また、2012年1月30日に公開された、15社からなるDMARC.org[*1]と、その組織が推進する技術仕様DMARC[*2]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が関わる様々な活動についてまとめています。今回は、日本の多くの企業の第4四半期にあたる2012年第1週(2012年1月2日～1月8日)から第13週(2012年3月26日～4月1日)までの13週間分のデータを調査対象にしています。

迷惑メールの割合については、この2年間ほど減少が続いてきましたが、最近ではこの割合の低下の度合いも小さくなってきました。いずれ下げ止まるだろうと予測してきましたので、それがどうなったか確認していただければと思います。

## 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。

### 2.2.1 2年ぶりに迷惑メール割合が増加

今回の調査期間と前年の同時期を含む、1年3ヵ月分(65週)の迷惑メールの割合の推移を図-1に示します。今回の調査期間での迷惑メールの割合の平均は47.2%でした。前回のレポート(Vol.14)と比べると、0.4%の微増となりました。

調査期間中の平均の値がその前を超えるのは、2010年第1四半期(Vol.7)以来となります。実に2年間もの間、迷惑メール割合は減少し続けていたことになります。しかし、増加したといってもわずかですので、今後急激に迷惑メール量が増えてくるというよりは、これまでの減少傾向が下げ止まった、と考えるべきでしょう。今後、新たな大量送信手法が広まるまでは、この現在のような水準の割合が続くものと思われます。

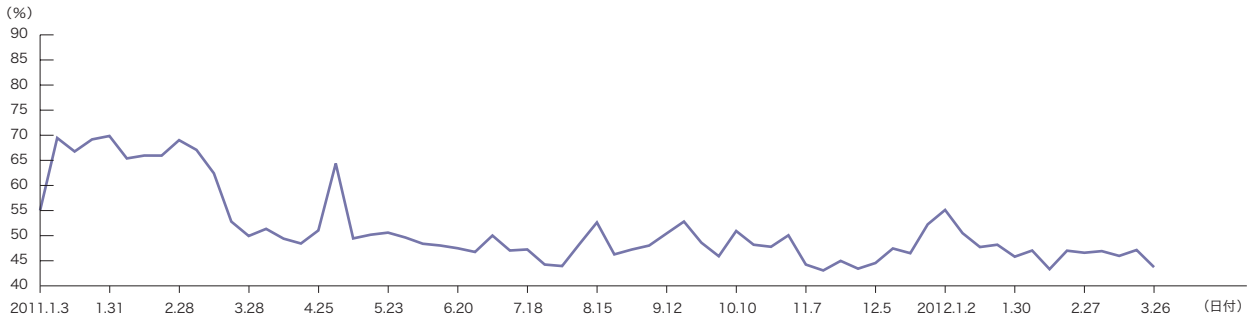


**図-1 迷惑メール割合の推移**

*1 DMARC.org(http://www.dmarc.org/)。
*2 DMARC:Domain-based Message Authentication, Reporting & Conformance。

### 2.2.2 主要送信元地域は変わらずフィリピンが上昇傾向

今回の調査期間での迷惑メール送信元地域の分析結果を図-2に示します。今回の調査では、迷惑メール送信元地域の1位は前回と同様に中国(CN)で、迷惑メール全体の23.7%を占めていました。前回から6.3%の減少です。2位は米国(US)で14.9%となり、前回から4.3%の増加です。これにより前回の3位から2位に上昇しました。3位は日本(JP)で14.0%と前回から1.5%の減少です。これら3地域で52.6%となり、前回と同様に全体の半分以上を占めています。4位はフィリピン(PH)で9.0%と前回から4.1%の大幅増加となっています。5位は香港(HK、4.2%)、6位はタイ(TH、3.4%)と前回から順位を上げています。

これら上位6地域について、今回の調査期間を含めて1年間(2011年4月4日～2012年4月1日)の割合の推移を図-3に示します。中国(CN)は、この1年を通じて常に首位でしたが、2012年2月後半から割合を下げはじめました。逆に香港(HK)が、同時期に急上昇しています。米国(US)は、この1年間に少しづつ割合を増加させていることがわかります。最近上位に位置するようになったフィリピン(PH)は、前回のレポートと合わせてみると、1年前の同時期にも割合が高かった時期があることが分かります。

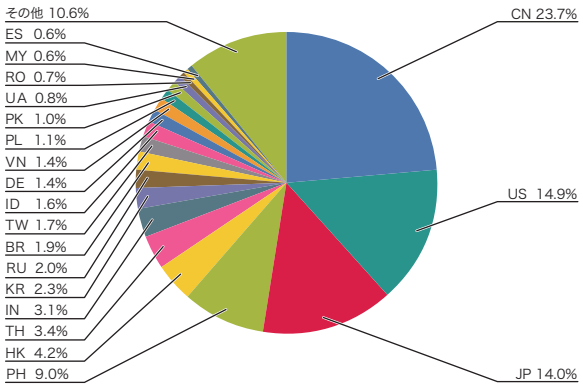


**図-2 迷惑メール送信元地域の割合**

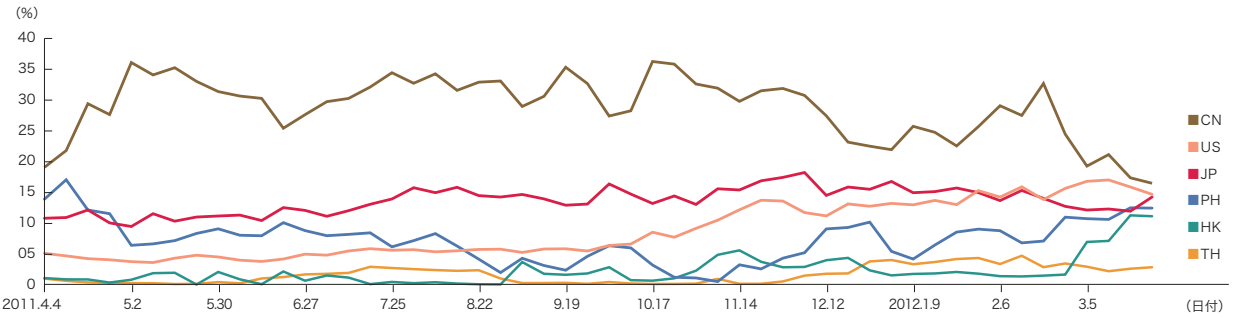


**図-3 主要迷惑メール送信元地域の割合の推移**

## 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的動向について解説します。

今回は、送信ドメイン認証技術の1つであるSPFについて、その普及状況をメールの受信側から調査した結果を報告します。

また、2012年1月30日に公開された、15社からなるDMARC.orgと、その組織が推進する技術仕様DMARCについて解説をします。DMARCについては、参加企業としてグーグル社やコムキャスト社などメールに関わる主要企業が参加していたことから、日本でも記事になるなど注目を集めましたが、残念ながら正しく内容を伝えているものはありませんでした。報告者は、DMARC検討の発端にもなったM$^3$AAWG[*3]に継続して参加している立場から、その目的や技術内容について詳しく解説します。

*3　M$^3$AAWG:従来のメッセージングより議論の対象を広げて、2012年2月14日よりMessaging, Malware and Mobile Anti-Abuse Working Groupとなった。

### 2.3.1 SPFの送信側の導入状況

今回の調査期間(2012年1月～3月)に受信したメールについて、SPFによる認証結果の割合を図-4に示します。メール送信側のドメインがSPFを導入していない(SPFレコードを宣言していない)ことを示す認証結果「none」の割合は36.5%でした。前回から2.7%の減少ですので、受信メール全体で送信側でのSPFの導入割合が2.7%増加したことを示しています。

### 2.3.2 DMARCの概要と背景

DMARCは、メールの送信側が既存の送信ドメイン認証技術を利用して、メールの受信側に詐称されたメールをどう扱うべきかの方針を示すための仕組みです。最終的には、詐称されたメールは当然受信拒否すべきですが、SPFやDKIMなど既存の送信ドメイン認証技術は、その設定方法や配送経路、実装などの違いによって、正規のメールが確実に認証をパスするとは限らないのが現状です。しかし、送信したメールが認証をパスしたかどうかは、メール受信側だけが判断でき、それを送信側が知る方法が標準では備わっていません。そのため、送信側で何か設定上問題があったとしても、それを発見して改善することが難しい仕組みとなっています。同様に受信側では、認証が失敗したメールが、単純に詐称されたメールなのか、それとも何らかの技術的な要因により認証失敗してしまったメールなのか、の判断がなかなかできません。そのため、せっかく送信ドメイン認証技術が普及しても、受信ポリシーによっては、有効に認証結果を活用できないことが起こりえます。

そこでDMARCでは、送信側で受信側の認証結果のフィードバックを受け取る窓口を公開できる仕様にしています。同時に、送信側で認証が失敗した場合の動作レベル(ポリシー)を段階的に示すことができます。

これにより、受信側での認証状況がわからない最初の段階では、ポリシーを「none」に指定し、フィードバックされた情報をもとに段階的に「quarantine(隔離)」や「reject(拒否)」に上げていく、といった設定が可能になります。認証が失敗したメールを受信拒否する、といった強い受信ポリシーを導入できるようになれば、送信者情報を騙るフィッシングなどの悪質な手法を排除できると期待しています。

つまり、DMARCは新しい認証方式や標準化を提案するものではなく、既に標準化されているSPFとDKIMを利用して、送信側が受信側に期待する、認証に失敗したメールの扱い方の指針を表明する仕組み、ということになります。メール受信側が、認証が失敗したメールを排除しやすくするために、ポリシーの移行過程でフィードバックが行いやすくするための情報を表明できるようにした、ということです。

### 2.3.3 DMARCポリシーの表明

SPFやDKIMと同様に、DMARCでもポリシーやフィードバックの宛先を示すDMARCレコードは、DNS上に設定します。具体的には、例えば "example.com"ドメインのDMARCレコードは、"_dmarc.example.com" の TXT レコードとして表明することになります。では、ドメインはどのように決まるのでしょうか。既に存在する送信者情報(reverse-path)を利用するSPFと違い、例えば署名情報がないDKIMでも同様の難しさがあります。DKIMでは、署名情報(DKIM-Signatureヘッダ)上に、署名ドメイン名と、署名の検証に必要な情報の存在場所であるサブドメイン名

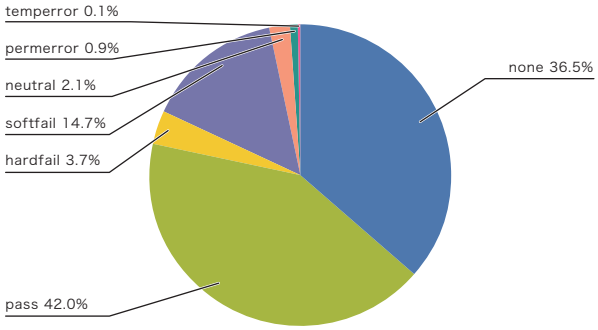


**図-4 SPFによる認証結果の割合**

| ポリシー | 認証失敗時に期待する動作 |
|---|---|
| none | 特に動作を指定しない |
| quarantine | 隔離するなど通常の配送経路と区別する |
| reject | 受信拒否する |

**表-1 DMARCのポリシー**

(セレクタ)が示されています。逆に言えば、署名情報がないメールは、それが送信者が意図して署名していないメールなのか、詐称されて送信されたメールかの判断ができないということになります。それを補完するための仕組みとして、DKIM ADSP[*4]が作られました。DKIM ADSPでは、ADSPレコードの場所として、メールヘッダのFrom:ヘッダにあるメールアドレス(Author Address, RFC5322.From)のドメインを利用します。DMARCでも同様に、DMARCレコードは、このRFC5322.Fromのドメイン上に設定されます。

現在提案されている、DMARCレコード上に設定可能なパラメータは表-2のとおりです。

"adkim"パラメータと"aspf"パラメータの値の意味は、s(strict)とr(relaxed)となります。strictの場合は、認証されたドメインが完全にRFC5322.Fromドメインと一致しなければならないことを意味しますが、relaxedの場合は、そのサブドメインであっても良いことになります。

| パラメータ | 意味 | 設定例 |
|---|---|---|
| v | バージョン | v=DMARC1 |
| pct | DMARCの適用すべき割合 | pct=100 |
| ruf | 認証失敗時のフィードバック先 | ruf=mailto:dmarc-authfail@example.com |
| rua | 集約されたレポートのフィードバック先 | rua=mailto:dmarc-aggrep@example.com |
| p | メール受信者がとるべきポリシー | p=quarantine |
| sp | サブドメインに対するポリシー | sp=reject |
| adkim | DKIMの署名ドメインとの関係 | adkim=s |
| aspf | SPFのドメインとの関係 | aspf=r |

**表-2 DMARCレコードのパラメータ**

```
_dmarc.example.com  IN  TXT  "v=DMARC1; p=reject; pct=100;
                        rua=mailto:dmarc-feedback@example.com"
```

DMARCレコードの設定は、上記のように送信側のドメイン(RFC5322.Fromのドメイン)のTXTレコード上に設定します。

## 2.4 おわりに

DMARCレコード及びDKIM ADSPレコードが、RFC5322.Fromのドメインを利用するのは、他に置き場がないための苦肉の策、というわけではありません。最終的なメール受信者がメールの送信者情報として参照するのは、やはりこのメールヘッダ上のRFC5322.Fromの情報なのです。このRFC5322.From上に詐称されたメールアドレス(ドメイン)が設定されていても、DKIMだけでは、全く無関係な別のドメインで署名したとしても認証が通ってしまいます。そして、多くのメール受信者は、その署名ドメインが何であるか、仮にそれが見かけ上の送信者(RFC5322.From)と何か密接な関係があったとしても、それを知るすべが提供されていないのです。メール受信者は、それでどうやって受信したメールが信頼に足りるものなのかを判断できるのでしょうか。

そのため、DKIM ADSPやSPFも含めた送信側のポリシーの表明先であるDMARCレコードは、メール受信者が参照できるRFC5322.Fromのドメインを利用するのです。もちろん、現在のメールの利用形態の多様性の中では、こうした仕組みと整合が取りにくい場合があるのも事実です。しかし、メールが組織内部へ簡単に侵入可能なツールであり、標的型攻撃をはじめ不正なメールの利用手法が広がっている現在では、メールの利用に関する技術的な仕様の見直しを含め、正しいメールがきちんと届く仕組みを考える時期にきているのかもしれません。

執筆者:
**桜庭 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 戦略的開発室 シニアエンジニア。メッセージング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、社外関連組織との協調した各種活動を行う。M$^3$AAWGメンバー及びJEAGボードメンバー。迷惑メール対策推進協議会及び幹事会構成員、送信ドメイン認証技術WG主査。(財)インターネット協会 迷惑メール対策委員。総務省 迷惑メールへの対応の在り方に関する検討WG構成員。

*4 DKIM ADSP:DomainKeys Identified Mail Author Domain Signing Practices, RFC5617。