送信ドメイン認証技術の普及と認証する識別子

今回は、2012年第14週〜第26週での迷惑メールの推移を報告します。
迷惑メールの割合は、前回のレポートから2.5%の微減となっていますが、
フィッシングによるネットバンキングの被害は増加しています。
こうした犯罪を防ぐため、送信ドメイン認証技術が認証する識別子について整理し解説します。

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1四半期にあたる2012年第14週(2012年4月2日〜4月8日)から第26週(2012年6月25日〜7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。

メールの技術動向では、送信ドメイン認証技術の普及状況について、IIJのメールサービスや他の調査結果をもとに解説します。更に、前回に引き続きDMARCの技術解説及び、今後の課題について整理します。

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。

2.2.1 迷惑メールの割合は低いが危険度は高まっている

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44.7%でした。前回のレポート(Vol.15)と比べると、2.5%の微減となりました。前年同時期(Vol.12)の平均からも5.5%減少しています。このように迷惑メールの量自体は、IIRが最初に発行された

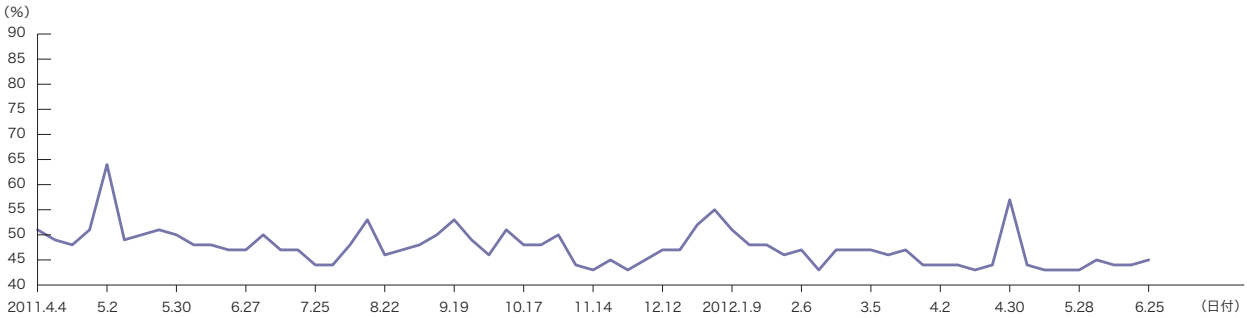

図-1 迷惑メール割合の推移

2008年当時に比べるとかなり少なくなりました。しかしながら、昨年警察庁から発表された情報[*1]によると、金融機関になりすましたメールを送信し、偽のインターネットバンクにIDとパスワードを入力させるいわゆるフィッシングによる被害が増加しているようです。その被害額は、昨年の3月末以降の約8ヵ月間で不正送金などにより約3億円発生したと報告されています。また、最近の報道機関によれば、今年の6月からネットバンキングの被害が再び増加している、との報道もありました。今回も、メールに記載した偽のサイトに誘導するフィシングの手法が使われたようです。被害を防ぐためには、メールを受け取ったらまず送信ドメイン認証技術の認証結果と認証されたドメイン名を確認し、信頼できるメールかどうかを確認することが必要です。

2.2.2 日本が再び送信元の2位に

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20.7%を占めていました。中国は、6四半期連続で日本にとっての最大の迷惑メール送信元となっています。2位は日本(JP)で13.2%でした。前回(Vol.15)では3位と一時後退しましたが、今回再び2位に戻りました。3位は米国(US)で11.5%で日本と順位を入れ替えています。4位がフィリピン(PH)で9%となり、前回からの高い割合を維持しています。これら4地域で54.4%となり、全体の半数以上を超える結果となりました。5位はインド(IN)4.5%、6位はベトナム(NV)3.3%、7位は、割合としては6位と同じ数値となっていますが、香港(HK)でした。

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について、IIJのメールサービス以外のデータも参照しながら普及状況を解説します。また、前回に引き続いて送信ドメイン認証技術のSPF[*2]及びDKIM[*3]を利用した、新しいメッセージ認証の仕組みであるDMARC[*4]について解説します。

2.3.1 IIJサービスでの送信ドメイン認証技術の普及状況

今回の調査期間(2012年4月～6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-3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33.8%でした。前回から2.7%の減少しましたので、認証可能だったメールの割合が逆にその分増加したことになります。つまり、受信しているメールの送信側でのSPFの普及率は、今回の調査期間で約66.2%まで増えたことになります。

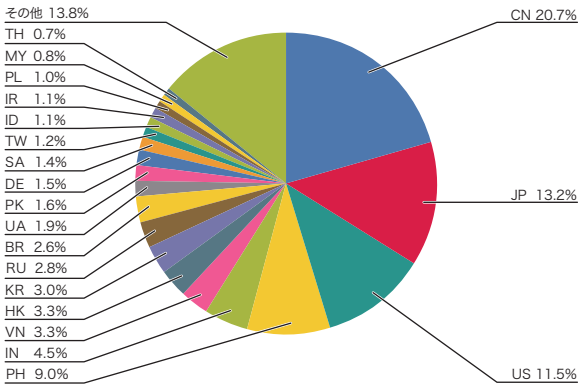

図-2 迷惑メール送信元地域の割合

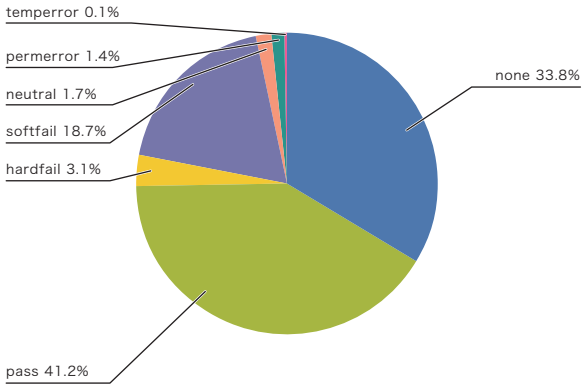

図-3 SPFによる認証結果の割合

＊1　インターネットバンキングに係る不正アクセス禁止法違反等事件の発生状況等について(http://www.npa.go.jp/cyber/warning/h23/111215_1.pdf)。
＊2　SPF:Sender Policy Framework, RFC4408。
＊3　DKIM:DomainKeys Identified Mail(DKIM)Signatures, RFC6376。
＊4　DMARC:Domain-based Message Authentication, Reporting & Conformance。

この普及率について、2009年8月から2012年6月までの35ヵ月間の推移を図-4に示します。多少の増減はありますが、ほぼ右肩あがりに増加しており、順調に普及が進んでいることが分かります。最新の2012年6月では、69.6%となっており、調査開始の2009年8月から約27%増加しています。

2.3.2 WIDEプロジェクトによる送信ドメイン認証技術の普及状況

WIDEプロジェクト[*5]では、JPRS[*6]と共同研究契約を結び、2005年4月から送信ドメイン認証技術の普及率を測定しています。調査は、2011年5月までは毎月行われ、それ以降は半年ごとに測定しています。この測定結果について、ドメインの登録型ごとの推移を図-5に示します。最新の2012年5月時点でのSPFの導入率の平均は、43.9%という結果になっています。

IIJのメールサービスでの66.2%との違いは、WIDEプロジェクトでは、JPRSが管理している「jp」ドメインのみを対象にしていることと、登録されているドメインに対するSPFの導入率（正確にはSPFレコードを宣言しているドメイン数）を調査していることにあります。つまり、静的な測定と、実際のメール流量に対する動的な測定の違い、と考えると分かりやすいと思います。

図-5で更に特徴的なのは、政府機関が利用する「go.jp」ドメインでの導入率が急増していることです。最新の測定値では、約114%となっています。測定値がおかしいように感じるかもしれませんが、間違っているわけではありません。これは、メールに利用するドメインを母数にSPFレコードを宣言しているドメイン数の割合を測定しているためです。「go.jp」ドメインでは、メールに利用しないドメイン

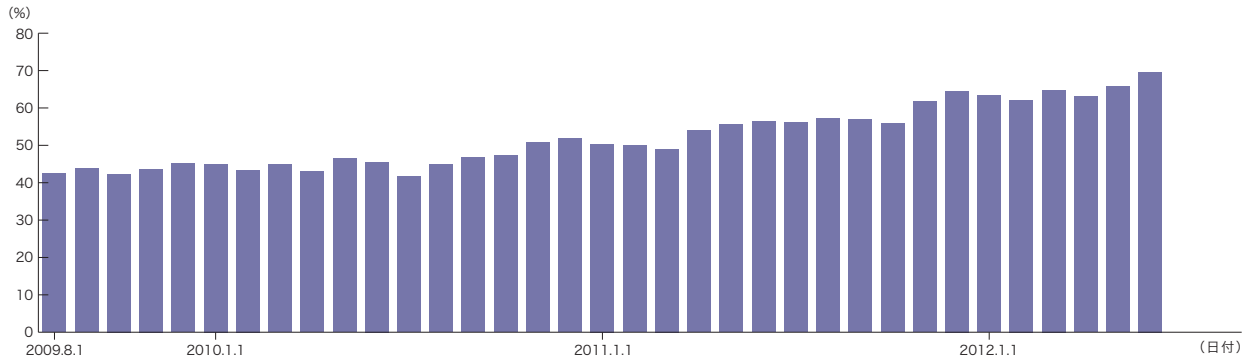

図-4 SPFの導入率の推移

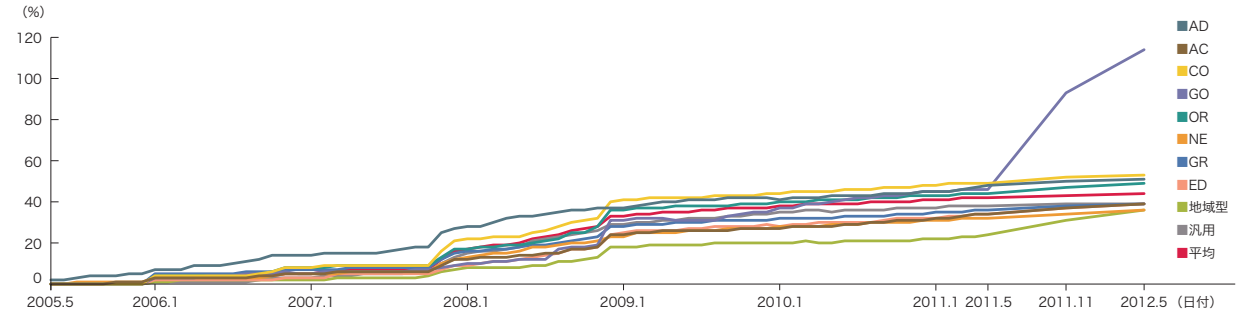

図-5 JPドメインの登録型ごとのSPF普及率の推移

*5 WIDE：Widely Integrated Distributed Environment（http://www.wide.ad.jp/）。
*6 JPRS：Japan Registry Services（http://jprs.jp/）。

についても、メール詐称に悪用されないように、以下のようなSPFレコードを宣言しているのです。

```
example.jp  TXT  "v=spf1 -all"
```

このSPFレコードは、正規のメールサーバの情報を指定していないので、すべて「-all」の部分に適合することになります。適合したときのqualifierが「-」ですので、必ず認証結果がfail ／ hardfailになります。つまり、このドメイン名を利用すると必ず認証が失敗するSPFレコード、ということになります。これにより、第三者が勝手に送信者情報として当該ドメインを利用したとしても、不正なものとして受信側が検知することができます。

2.4 DMARCと認証識別子の関係

前回は、DMARCの目的とその仕組みの概要について解説しました。今回は、既存の送信ドメイン認証技術を含め、認証の対象となっている識別子について整理し、解説します。DMARCで対象にしている送信ドメイン認証技術は、SPFとDKIMです。SPFが認証する識別子は、メール配送[*7]上の送信者情報であるreverse-path（RFC5321.MailFrom）のドメインです。これは、受信メールサーバがメール本体を受け取る前に通知される送信者情報で、通常はメールの受け取り手に提示されません。そのため、SPFで認証されたメールでも、MUA（メールソフト）や携帯電話などで表示される送信者の情報が信頼できないものである可能性があります。そのため、認証結果を示すヘッダ[*8]に記載されたドメインを確認する必要があります。DKIMが認証するのは、署名者を示したSDID（Signing Domain Identifier）です。署名情報を示す「DKIM-Signature」ヘッダの「d=」パラメータで示される識別子です。つまり、DKIMでは厳密にはメールの送信者ではなく、署名情報を作成した署名者を認証する技術、ということになります。そのため、送信するメールの署名方針、メール受信側に希望する認証ができなかった場合の取り扱い方法を示すDKIM ADSP[*9]が作られました。DKIM ADSPの詳細については、IIR Vol.6[*10]で解説しています。これに、DMARCを加えたそれぞれの認証識別子を以下の表-1で示します。ここで示したものだけでも、4種類の認証技術と3種類の異なった識別子をメール認証に利用していることが分かります。

2.4.1 DMARCのIdentifier Alignment

DMARCが利用する識別子は、Identifier Alignmentです。基本的にはSPFあるいはDKIMで認証された識別子であって、それが更にメールヘッダ上の送信者情報であるRFC5322.Fromと同じもの、あるいは密接に関連したドメインです。そのため、DMARCを利用するためには、まずSPFあるいはDKIMで認証した識別子の存在が前提となり、いずれの認証も失敗、あるいは認証できなかった場合には、DMARCの仕組みとしても失敗したことになります。次に、SPFあるいはDKIMで認証された識別子とRFC5322.Fromの識別子との関係です。いずれも同じドメインであれば何の問題もありません。しかし、組織が大きくてサブドメインを多用している場合や、サブドメインでメール送信の用途を使い分けている場合などには、サブドメインごとにDKIMの署名の仕組みや、DMARCレコードを用意するのが難しいため、代表的なドメインで集約できると便利なことがあります。DMARCレコードでは、Identifier Alignmentかどうかを決める仕組みとして、SPFとDKIMそれぞれで、認証した識別子に対して、strictかrelaxedを指定することができます。strictの場合には、認証した識別子のドメインとRFC5322.Fromのドメインが完全に一致しなければなりません。relaxedを指定した場合には、認証した識別子のOrganizational Domainが一致すれば良いことになります。Organizational Domainは、概念的には上位ドメインや親ドメイン、ということに

認証技術	認証識別子
SPF	reverse-path（envelope from, RFC5321.MailFrom）
DKIM	SDID（d=）
DKIM ADSP	Author Domain（RFC5322.From）
DMARC	Identifier Alignment（RFC5322.From）

表-1 認証技術と認証識別子の関係

＊7　メール配送の仕組みは、SMTP（Simple Mail Transfer Protocol、RFC5321）で定義されている。
＊8　Message Header Field for Indicating Message Authentication Status、RFC5451。
＊9　DomainKeys Identified Mail（DKIM）Author Domain Signing Practices（ADSP）、RFC5617。
＊10　IIR Vol.6「2.3 メールの技術動向」（http://www.iij.ad.jp/company/development/report/iir/pdf/iir_vol06.pdf）。

なります。ドメイン名は、「.com」や「.org」のようなTLD（Top Level Domain）を利用する場合と、日本（.jp）などのようにccTLDの下に属性型があるものなどいくつかのパターンがあります。そのため、Organizational Domainの厳密な定義は難しいので、今後の検討課題ということになっています。表-2に、Organizational Domainの例を挙げます。

2.5 DMARCの課題

DMARCでは、Alignmentのモードを設定できることにより、認証ドメインをある程度柔軟に集約できるようになりました。これにより、ドメインの委譲関係を、サブドメインを利用するなどうまく整理すれば、メール配信を委託する場合やホスティングサービスを利用する場合でも、DMARCの仕組みを利用できます。また、SPFとDKIMいずれかで認証が成功すれば、それを識別子として利用できます。そのため、メール転送のように、SPFで認証が失敗してもDKIMでは認証できるような場合にも有効に機能します。

しかし、現在多く使われているメール利用の形態の1つ、メーリングリストとDMARCの相性が良くありません。

認証ドメイン	Organizational Domain
foo.example.com	example.com
foo.bar.example.co.jp	example.co.jp

表-2 Organizational Domainの例

認証技術	認証結果	認証識別子
SPF	pass	メーリングリスト管理ドメイン
DKIM（再署名なし）	fail ＊11	メール作成者
DKIM（再署名あり）	pass	メーリングリスト管理ドメイン
DMARC	fail	メール作成者

表-3 メーリングリストでの認証識別子と認証結果の関係

メーリングリストでのそれぞれの認証識別子と認証結果の関係について、一般的な例を表-3に示します。

メーリングリストでSPFとDKIMの認証が成功するケースとしては、いずれもメーリングリスト管理アドレスのドメインを認証している場合となります。しかし、メーリングリストでは、RFC5322.Fromのドメインが、最初にメールを作成した投稿者のドメインがそのまま利用されることが一般的なので、DMARCのIdentifier Alignmentが取り出せず、失敗してしまいます。この課題については、DMARC.orgを中心として議論が行われていますが、残念ながらまだ明確な解決策は見えていません。

2.6 おわりに

メールに関わる技術者の多くは、メールの配送過程で受け取ったメールを、なるべく変更せずに次に渡したい、と考える傾向があります。これまでのメールヘッダについても、「Received」ヘッダは配送過程で追加はしても、既存のものを削除することは通常行われません。DKIMなど新しい技術についても、「DKIM-Signature」という新しいヘッダを追加することにより、機能拡張してきています。そのため、メールヘッダ部分がだんだん大きくなり、一方でMUAでは必要最小限の情報しか表示せず、メールヘッダ全体を参照する操作が難しくなっています。メールヘッダは、比較的柔軟な構造となっているので、こうした機能追加には利用しやすいわけですが、その反面、既存のヘッダをきちんと解析して変更するといったことが若干難しい側面もありました。しかし、メール配送システム側で、結局は参照されない情報を大事に保存する方法を延々と考えるよりも、これまでのようにうまくバランスを取りながら、どこかで思い切って整理することも必要かもしれません。

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。

＊11 電子署名に利用するヘッダや本文を改変しない場合には、認証が通るケースもある。