送信元の地域特性に合わせた迷惑メール対策の必要性

今回は、2009年第40週〜第52週を加えた2009年一年間での迷惑メールの割合の推移とともに、同期間での送信元地域の分析結果を示します。
また、迷惑メールの主要な送信元地域での送信傾向を推測し、地域特性に合わせた対策の必要性を解説するとともに、送信ドメイン認証技術DKIMの関連技術を解説します。

2.1 はじめに

ここでは、迷惑メールの最新動向、迷惑メール対策に関連する技術、IIJ が深く関わっているさまざまな活動などについてまとめています。迷惑メールの動向については，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機能から得た各種情報を元に、さまざまな分析を行った結果を示します。ただし、メールの流量は、提供しているサービスの対象によって曜日ごとに変動します。このため、ここでは、よりよく傾向を把握できるようにするために、一週間単位でデータを集計し、その変化に着目して分析しています。今回の調査は、2009年第40週（2009年9月28日〜 10月4日）から第52週（2009年12月21日〜 12月27日）までの13週間を加えた、2009年一年間のデータを対象にしています。

迷惑メールの動向では、地域ごとの迷惑メールの送信傾向の違いについて取り上げます。日本発の迷惑メールは、OP25B[*1]により劇的に減少しましたが、こういった対策技術が有効に機能する地域と、個別に対処していくべき特定の地域の違いが明らかになりました。さらに、迷惑メール対策のための基礎となる技術、送信ドメイン認証技術の導入状況についても報告します。

メールの技術動向では、電子署名技術に用いる送信ドメイン認証技術DKIMに関して、その署名方針を表明する DKIM-ADSPを解説します。また、DKIM-ADSPを含めてDKIMの仕様が一部改訂されたため、その改訂ポイントも示します。

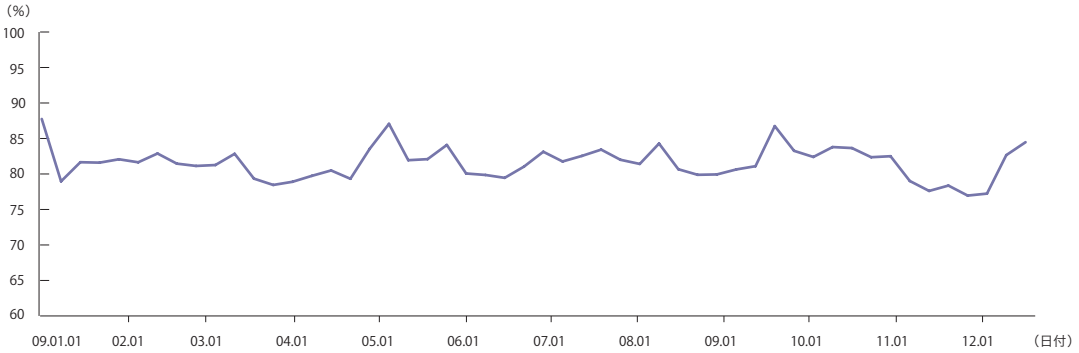

図-1　迷惑メールの割合の推移

＊1　OP25B (Outbound Port 25 Blocking)は、一般ネットワーク利用者に割り当てられた動的IPアドレスが、直接外部の受信メールサーバにメール送信することをブロックすることで、迷惑メール送信を抑制する技術です。

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、迷惑メールフィルタによってIIJが検知した迷惑メールの割合の推移と、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 迷惑メールの割合の推移

2009年第40週から第52週までの91日間に検出した迷惑メールの割合は、平均81.4%でした。前回（2009年第27 ～ 39週）での平均値が82.2%でしたので、0.8%減少したことになります。昨年の同時期での平均値が81.5%でしたので、ほぼ同じ傾向が続いていると考えられます。今回の調査期間を含めた2009年一年間での迷惑メールの割合の推移を図-1に示します。

迷惑メールの割合は、通常のメール流量と相対的な関係になります。このため、たとえば長期休暇やイベントなどの活動の有無によって一般的なメール流量に変化が生じると、その影響が迷惑メールの割合に現れます。また、迷惑メールの流量自体にも、時期的な変動が見られます。このため、一般的な迷惑メールの増減傾向を判断するには、長期的な視点での観測が必要です。このような点から、迷惑メールの流量は、昨年から引き続いて高い割合を維持し続けていると言えます。

今回の調査期間に見られる特徴として、11月から12月上旬にかけての迷惑メール割合の減少を挙げることができます。この期間には、迷惑メールの流量自体が減少しています。これは、通常メールとの相対的な関係で減少したものではありませんでした。ただし、その後12月後半から迷惑メールの流量が増加に転じましたので、この減少は一時的なものと考えられます。

2.2.2 迷惑メールの送信元

今回の調査期間での迷惑メールの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、迷惑メールの送信元地域の1位は、前回と同じくブラジル（BR）で、迷惑メール全体の12.5%を占めていました。ブラジルは、IIR Vol.3で報告した2009年第1四半期に1位となって以降、その位置を保ち続けています。2位から6位までの上位送信地域は、順に中国（CN）の10.4%、米国（US）の7.0%、インド（IN）の5.6%、ベトナム（VN）の5.2%となりました。順位自体は前回のものから変わっていますが、1位から6位までを占める地域は同じです。

これら6か国に日本（JP）を加えた迷惑メールの割合の推移について、これまでIIR Vol.1 ～ 6で報告してきたものを図-3にまとめてみました。このグラフから、米国（US）からの迷惑メールの割合が減少傾向であるのに対して、ブラジル（BR）、インド（IN）、ベトナム（VN）からのものが増加傾向にあることが分かります。また、中国（CN）や韓国（KR）については、時期によって変動しているため傾向を把握し難いですが、減少しているとは言えず、注意が必要です。

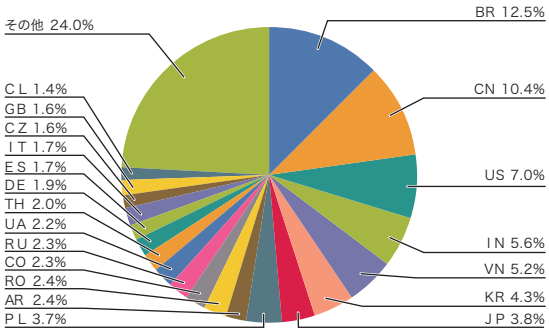

図-2　迷惑メール送信元地域

ここまでに示したように、ブラジルが日本に対する迷惑メールの主要送信元の1つであることから、日本データ通信協会とJPCERT/CCは、ブラジルと迷惑メールに関する情報交換を開始すると発表しました[*2]。この発表資料では、IIRで示してきたデータが引用されています。これまでにIIRで報告してきたとおり、迷惑メールの大部分が海外から送信されているという現状では、迷惑メールの受信量を減らすためにこういった地域の関係当局との連携が必要です。

IIJは、JEAG[*3]などによる活動と連携し、韓国や中国の関係組織と迷惑メール対策、特にOP25Bの導入について意見を交換しています。現在は、それぞれの地域固有の事情もあり、すぐに効果的な対策を実施するには至っていませんが、今後も国内外の関係組織と協力してグローバルな迷惑メール対策に取り組んでいきます。

2.2.3 迷惑メールの送信傾向

今回の調査期間では、先ほど図-2に示したように、日本(JP)は3.8%で迷惑メール送信地域の7位になっています。迷惑メールの送信割合は、前回に比べて0.7%とわずかに増加しています。また、図-3からも明らかなように、迷惑メールの割合は、IIR Vol.1で報告した時期(2008年6月～8月)から少しずつ増加しています。

日本発で迷惑メールと判定されるメールの傾向としては、これまでにも分析してきたとおり、固定IPアドレスを利用して大量送信を目的としたものが依然として多いです。これらの中には、データセンターやホスティング事業のホストと思われる送信元が含まれています。また、OP25Bが対応できていない動的IPアドレスも依然として送信元に含まれています。ただし、その割合は、他の地域に比べて圧倒的に低くなっています。

今回、特定の期間中に迷惑メールの送信元と判定された送信元のうち、迷惑メール数が1日あたり平均1通以下であったものの割合を、主要な迷惑メール送信国ごとに比較してみました。つまり、これは、迷惑メールと判定したメール送信数全体に対して、非常にわずかなメールしか送信していない送信元の割合を示すものになります。比較結果を図-4に示します。

図-4では、中国(CN)、米国(US)、韓国(KR)、日本(JP)がいずれも5%前後であるのに対して、ブラジル(BR)、インド(IN)、ベトナム(VN)が高い割合を示しています。これらの高い割合を示す地域は、いずれも図-3に示したグラフで迷惑メール送信の割合が増えている地域です。近年増加している迷惑メールの送信手法が不正プログラム(malware: malicious software)に感

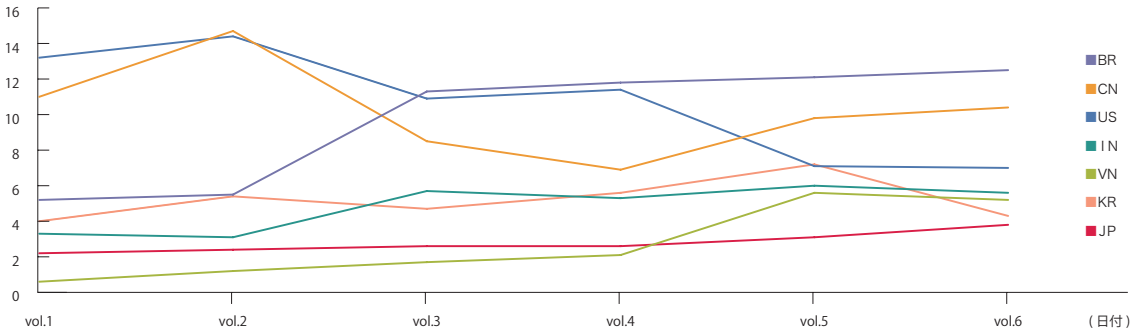

図-3　迷惑メール送信元の推移

＊2　報道資料: ブラジルとの迷惑メールに関する情報交換の開始について(http://www.dekyo.or.jp/soudan/image/n-image/PL_20100108.pdf)
＊3　JEAG (Japan Email Anti-Abuse Group)は、2005年3月に主要ISPや携帯電話事業者を中心に設立された、迷惑メール対策のためのワーキンググループ(http://www.iij.ad.jp/news/pressrelease/2005/0315.html

染させられたボット（bot）と考えられていることから、これらの増加している地域でボットが増えていると考えられます。

ボットに感染しやすいPCは、対策が不十分な個人利用のPCであり、その都度IPアドレスが変わる動的IPアドレスを主に利用します。今回の調査では、これらの地域で同一送信元（IPアドレス）からの迷惑メール送信数が少ないという結果になりました。この理由は、動的IPアドレスにあると考えられます。このような地域では、OP25Bなどのネットワークレベルで迷惑メールを直接送信できないようにする技術の導入が効果的です。

一方、1日にわずかな数の迷惑メールしか送信しない送信元の割合が低いにもかかわらず、迷惑メールの送信割合が高い地域は、特定の送信元が大量に迷惑メールを送信していると考えられます。日本は、OP25Bの導入によって動的IPアドレスからの迷惑メール送信がそれほど多くないため、図-4で示した割合が低いことが説明できます。中国や韓国の割合が低いことは意外かも知れません。これらの日本に近い地域では、特定の送信者が日本に向けて大量に迷惑メールを送信していると考えられます。実際に、2007年に逮捕された迷惑メール送信事業者は、中国国内にPCを設置して日本へ迷惑メールを送信していたと報道されています。こういった地域では、特定の大量迷惑メールの送信元を処分することで、迷惑メールの送信量の減少が期待できます。

このように、即効性のある迷惑メール対策としては、それぞれの地域の事情や特性に合わせた対策が肝要であると考えています。

2.2.4 送信ドメイン認証技術の導入状況

ネットワークベースの送信ドメイン認証技術の一つSPFについて、今回の調査期間（2009年10月～12月）での認証結果の割合を図-5に示します。この期間に受信したメールについて56.3%の認証結果が“none”でした。これは、受信メールの43.7%のドメインがSPFレコードを宣言したいたことを示しています。

この送信元のSPFの導入割合は、前回（vol.6）とほぼ横ばいですが、認証結果“pass”の割合が今回は15.9%となり、前回の13.5% から2.4%増加しました。迷惑メール量の若干の減少が影響しているかもしれません。もう一つの特徴として、認証結果“neutral”の割合が4.3%となり、前回から2.3%減少しました。これは、SPFレコードの末尾に宣言する“?all”部分に適合する割合が減ったことを意味しています。SPFの仕様では“?all”はテスト的な意味を持ちますので、テスト運用のドメインから本格運用に切り替えたドメインが増えていると考えられます。

今後も IIR では、送信ドメイン認証技術の導入状況について調査を継続し、適宜報告していきます。

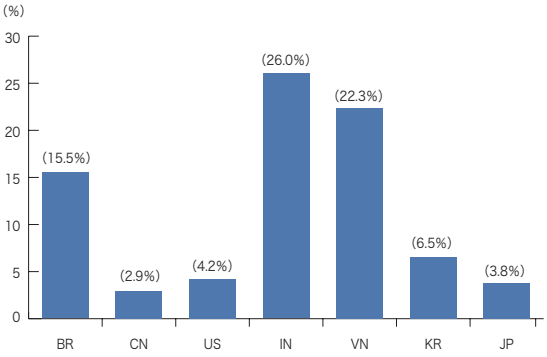

図-4　迷惑メールの送信頻度が低い送信元割合

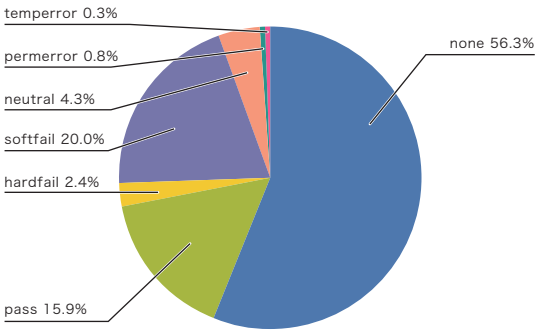

図-5　SPF の認証結果の割合

2.3 メールの技術動向

2.3.1 DKIM ADSP とその経緯

DKIM (DomainKeys Identified Mail) については、すでにIIR Vol.3でその技術を詳細に解説しています。DKIMでは、メールヘッダと本文から電子署名を作成し、それをDKIM-Signatureヘッダとしてメールに添付することで、メール受信者側で認証を行うことができます。また、DKIMには、電子署名を検証するために必要となる公開鍵を送信者側のドメインのDNS上で公開することで、特別な認証機関や配布手段を用意しなくても送信者側のシステムで完結できるという特徴があります。メールの受信者側は、受信したメールのDKIM-Signatureヘッダから署名情報を取得し、それを検証することで送信ドメインの認証を行います。この手順には、SPF/Sender IDなどネットワークベースの送信ドメイン認証技術との大きな違いがあります。

ネットワークベースの技術は、いずれのものも送信者情報として既存の情報 (SMTP上のreverse-pathやFromヘッダなどのPRA情報) を利用しているため、SPFレコードの取得場所が明確であり、SPFレコードの有無を確認することで送信ドメイン認証技術に対応している送信者であるかどうかが判断できます。これに対してDKIMでは、DKIM-Signatureヘッダが存在しているときにはそれを元に認証処理を実行すればよいのですが、ヘッダが存在していないときにはそれが元々DKIMに対応していない送信者によるものなのか、何らかの事情によってそのメールだけにDKIM-Signatureヘッダが付けられていないのかが判断できません。これは、電子署名に利用する公開鍵を取得するためには、DKIM-Signatureヘッダに指定されているセレクタ (selector) 情報が必要であり、送信側のドメイン名だけではDKIMに対応しているかどうかを判断できないためです。

また、ネットワークベースの技術では、SPFレコードの末尾に設定する“all”の前に記述した限定子 (qualifier) の種類によって、認証が失敗したときの強度をメール送信者側が指定できます。

これに対して、DKIM本体の仕様 (RFC4871) だけでは、DKIM-Signatureヘッダが存在しているときには認証の可否は判断できますが、認証が失敗したときに受信者側が振る舞うべき指針を送信者側が指定することはできません。このため、送信者側で署名方針を表明するための手段として、ADSP (Author Domain Signing Practices) がRFC5617として策定されました。

当初、DKIMの仕様検討段階には、こうした送信者側の意思を表明したり、現在のメール利用の流れに沿ったメールの配信者と実際のメール送信者 (作成者) を分離できるような仕組みが必要であることが指摘されていました。しかし、送信者が誰であるかという部分の議論がなかなかまとまらなかったこともあり、普及のためにDKIMの本体部分をまず仕様として出すべきとの判断から、RFC4871が公開されました。その後も、この送信者側の方針部分に関しては、継続して議論が行われましたが、結果としては核となる基本部分だけをADSPとしてまとめることになりました。このため、仕様の名称についても、議論を進める過程で次のように変化していきました。

表-1　DKIM-ADSP名称の変遷

仕様時期	略称	名称
2006年 1月 10日	SS	Sender Signing Policy
2007年 3月 3日	SS	Sender Signing Practices
2008年 8月 26日	ASP	Author Signing Practices
2009年 1月 3日	ADSP	Author Domain Signing Practices
2009年 8月	ADSP	RFC5617

2.3.2 DKIM ADPS の概要

DKIM ADSP (DomainKeys Identified Mail Author Domain Signing Practices) は、RFC5617としてその仕様が公開されています。ADSPの情報は、DNS上にADSPレコードとして公開することになっています。

具体的には、DNSのTXT資源レコードを利用します。この情報は、メールのFromヘッダ領域に示されているAuthorアドレスのドメイン名（Authorドメイン）を利用して、DNSに問い合わせることで取得します。このときドメインは、DKIM-Signatureヘッダの“d=”タグに示されているドメイン名と同じになります。たとえば、Authorドメイン名が“example.jp”であったときには、次のドメイン名に対してADSPレコード（TXT資源レコード）を問い合わせます。

_adsp._domainkey.example.jp

この例からも明らかなように、ドメイン名は、Authorドメインに“_adsp._domainkey”のサブドメインを付加したものになります。ADSPレコードの記述形式は、“tag=value”（タグ形式）ですが、現在のところ“dkim=”タグだけが定義されています。“dkim=”タグには、次の値（value）が指定できます。また、ここに示す以外の値が設定されていたときには、“unknown”として扱われます。

表-2　DKIM-ADSPの値

Value	意　味
unknown	送信ドメインはメールの全部、または一部に署名している
all	すべてのメールは署名されている
dicardable	すべてのメールは署名されている。署名が正しくないときには、受信者はメールを破棄してもかまわない

2.3.3 DKIM のアップデート

DKIMの仕様は、RFC4871として2007年5月に公開されました。その2年3か月後の2009年8月には、RFC5672として、それまであいまいであったDKIM-Signatureヘッダ上の2つの識別子“d=”と“i=”の部分が整理されました。しかし、DKIMの本質部分である電子署名の作成と検証については変更がなく、それまでもきちんと整理されてこなかった第三者署名に関する有益な変更も加えられませんでした。

2.4　おわりに

今回のメッセージングテクノロジーでは、迷惑メールの動向として、迷惑メール割合の推移と、それらの送信元に関する情報を報告しました。また、迷惑メールの主要送信国に関して、同一送信元からの迷惑メール送信数に着目してその違いをまとめ、考察しました。IIJでは、今後も実際に流通されているメールを元に迷惑メールの特徴や傾向を分析し、グローバル環境でそれぞれの特徴に応じた迷惑メール対策について貢献していきたいと考えています。さらに、メールの技術動向では、今後普及が期待される電子署名方式の送信ドメイン認証技術であるDKIMと、その周辺仕様であるADSPの概要について解説しました。IIJが提供するSecureMXサービスは、すでにDKIM ADSPに対応し、送信側に加えて、メール受信時にDKIM ADSPの情報をAuthentication-Resultsヘッダに記録するといった、送受信の両方での最新技術に対応しています。今後もIIJは、常に最新動向を把握し、いち早く有効な技術を提供できるよう努力していきます。

執筆者：
櫻庭 秀次（さくらば しゅうじ）
IIJ ネットワークサービス本部 メッセージングサービス部 サービス推進課シニアプログラムマネージャ。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。MAAWGメンバ及びJEAGボードメンバ。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。