2 メールテクニカルレポート

2.1 はじめに

メールテクニカルレポートでは、迷惑メールの最新動向や迷惑メール対策に関連する技術等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られる各種情報を元に様々な分析を行い、結果を公表しています。なお、メールの流量は曜日ごとの変動があるため、より傾向を把握しやすいよう暦週*1を基準とした1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年の第1週（2008/12/29〜2009/1/4）から第13週（2009/3/23〜2009/3/29）までの13週、91日間を対象にしました。

迷惑メール対策技術については、前回に引き続き「送信ドメイン認証技術」を取り上げます。今回は、電子署名技術を利用したDKIM（DomainKeys Identified Mail）の概要について解説します。

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が提供する迷惑メールフィルタ機能によって検知され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情報を中心に報告します。迷惑メールの送信元については、2008年11月のMcColo社のネットワーク遮断（参考：Internet Infrastructure Review Vol.2）以降大きな変動がありました。前回に引き続き、その推移と変動について分析します。

2.2.1 迷惑メールの割合

2009年第1週から第13週までの91日間について、週ごとの迷惑メールの割合の推移を図-1に示します。

この期間の受信メール全体に対する迷惑メールの割合は、平均して81.5%でした。割合が最も大きかったのは、第1週（2008/12/29〜2009/1/4）の87.8%です。この期間は年末年始の休暇にあたり、業務用のメールが少なかったため、相対的に迷惑メールの割合が大きくなりました。前回（2008/9/1〜2008/12/28）の平均値は82.7%でしたので約1.2ポイント減少したことになります。迷惑メールの割合は、依然として高いレベルにあり、引き続き対策の強化が必要と考えています。

2.2.2 迷惑メールの送信元

IIJが迷惑メールと判定したメールについて、それらがどこから送信されたのか、国別に分類した結果を図-2に示します。

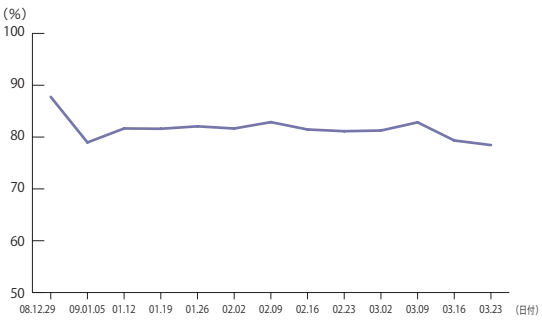

図-1　迷惑メールの割合

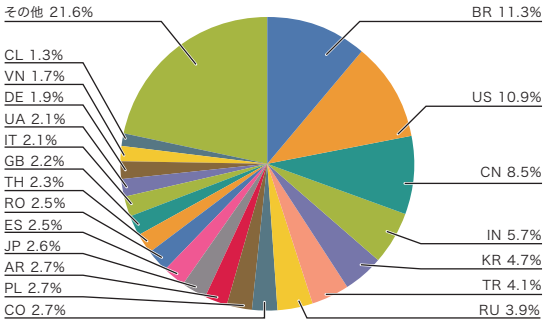

図-2　迷惑メールの送信元

＊1　暦週は、JIS X0301「情報交換のためのデータ要素及び交換形式-日付及び時刻の表記」を基準としているため、2008年の期間が一部含まれる。

今回の調査では、迷惑メールの送信元はブラジル(BR)が11.3%で1位となりました。ブラジルは前回の調査で5.5%の5位でしたので、急上昇したことになります。前回の迷惑メール送信元の推移調査では、2008年最終週(第52週)で2位となり今後の増加が懸念されていました。

2位は前回と同様に米国(US、10.9%)で、3位は前回1位だった中国(CN、8.5%)となりました。4位はインド(IN、5.7%)で前回の8位から急上昇しています。5位は韓国(KR)、6位はトルコ(TR)、7位はロシア(RU)でいずれも前回から引き続き上位にランクしています。日本(JP)は2.6%で11位です。今回の調査結果では、ブラジル、米国、中国で約3割、上位7カ国で約半分を占める結果となりました。日本が受信する迷惑メールの量を減らすためには、これら上位国によるOP25B[*2]の導入等、送信側の対策が必要と考えています。

これら7カ国に日本を加えた週単位での割合の推移を図-3に示します。昨年11月にMcColo社のネットワークが遮断されてから順位を下げてきた米国が第5週(1/26～2/1)から急激に上昇し、その後上位に位置しています。このことから前回McColo社のネットワーク遮断によって活動に影響を受けたボットネットが、新たな管理サーバ(Command & Controlサーバ)を得る等によって復活していることが推測できます。また、昨年11月以降に順位が上がったブラジルも、そのまま上位で推移したことから今回の調査期間全体では1位となりました。

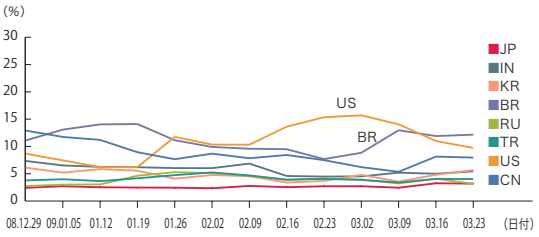

図-3　迷惑メール送信元の推移

前回1位となった中国はやや減少傾向がみられましたが、第12週から第13週(3/16～3/29)にかけて再び上昇しており、今後も注意が必要です。

図-3のグラフから日本と他の上位国の間では、迷惑メールの送信割合の推移に違いが読み取れます。日本の割合が約2.5%前後で横ばいに推移しているのに対し、他の上位国の送信割合は大きく変化しています。この違いは興味深いため、割合の変化の背景にある送信者の動向や各国の事情の違いについて、引き続き調査を進めていきます。

2.2.3 日本発の迷惑メール

これまで述べてきたとおり、日本では多くのISPがOP25Bを導入していることにより、日本発の迷惑メール対策が比較的うまくいっていると言えます。本レポートの調査結果からも、97%以上の迷惑メールが日本以外から送信されていることが分かります。また迷惑メール(スパム)の上位送信国ランキングを定期的に発表しているソフォス社[*3]のレポートでも同様の結果が示されています。

総務省がとりまとめた平成20年「通信利用動向調査」の結果[*4]に、日本のインターネット利用者数は9,091万人で、世帯におけるブロードバンド回線(FTTH、xDSL、CATV等)の割合が73.4%と非常に高速な接続回線が普及していることが示されています。こういった状況だけをみれば、日本は迷惑メールを短時間に大量にばらまくことが可能な環境と言えますが、実際の迷惑メール送信量は他国に比べて低い結果になっています。この理由はOP25Bを導入しているISP数の多さとその規模[*5]によるものと考えられます。

このような努力によって、日本発の迷惑メールの量は非常に少なくなりましたが、それでもなかなかゼロにはならないという現実があります。例えば、メール全体数に占める迷惑メールのうち日本発の割合は、100通の

＊2　OP25B (Outbound Port 25 Blocking)は一般ユーザが接続回線に利用する動的IPアドレスから、外部ネットワークのメールサーバ間で利用する25番ポートへのアクセスを制限する技術で、迷惑メールの送信抑制に非常に効果があると言われている。
＊3　ソフォス社のURLは、http://www.sophos.co.jp/。2008年のスパム送信国順位で日本は32位。
＊4　総務省の調査結果(http://www.soumu.go.jp/menu_news/s-news/02tsushin02_000001.html)。
＊5　財団法人日本データ通信協会の迷惑メール相談センターの調査によれば、49社のISPがOP25Bを実施している(http://www.dekyo.or.jp/soudan/taisaku/i2.html)。

メールを受信したうちの約2通であるということが分かります。この数値はIIJが提供している法人向けメールサービスの場合ですので、携帯電話等では割合が更に高くなる可能性があります。

こういった日本発の迷惑メールはどこから送信されているのでしょうか。ひとつは、固定IPアドレスを取得している場合があります。勿論、固定IPアドレスだから迷惑メールを送信しても良いというわけはなく、多くの場合、迷惑メールの送信は不正利用とみなされ、ISPまたは利用しているインターネット接続サービスの契約解除の対象になります。しかし、送信側の管理元では迷惑メールを送信しているか否かを把握することは大変難しく、迷惑メール受信者の申告等によって発覚することになります。また、その申告者が正しい情報を提供しているのか、対象となっている契約者が本当に迷惑メールを送信しているのかといった証拠を明確にする必要があり、対処まで時間を必要とします。

もうひとつは、残念ながらOP25Bの実施が不十分なケースです。迷惑メール送信者はこうした穴を確実に狙い、大量に迷惑メールの送信を続けていることがわかっています。さらに最近増えてきたケースに、モバイルのデータ通信端末を利用した迷惑メールの送信があります。モバイルデータ通信は、利用場所を選ばない便利なサービスです。利用者数も急速に増えてきましたが、その一方で悪用も目立ってきています。OP25Bの導入も予定されているようですが、すでにOP25Bの有効性は明らかになっており、早期の導入が望まれます。

日本発の迷惑メールをなくすには、こうした送信側の不備を是正していくことが必要になります。また、日本の例からも分かるとおり、世界的な規模で迷惑メールの送信を減らすためには、各国でOP25Bを導入することが重要であると考えています。IIJでは様々な国際会議の場や機会を利用して、常にOP25Bの効果を説明していますが、これからも積極的な情報発信をしていきます。

2.3 メールの技術動向

2.3.1 送信ドメイン認証技術の動向

前号までに、送信ドメイン認証技術には、ネットワークベースのものと電子署名技術を利用するものとの2つの技術が存在することを紹介しました。そのうち、ネットワークベースのSPF/Sender ID技術についてこれまで連続して取り上げましたが、今回はもう一つの方式である電子署名技術を利用するDKIM（DomainKeys Identified Mail）の概要について解説します。

WIDEプロジェクトの調査[*6]によれば、2009年4月の「jp」ドメインのSPFレコードの宣言率は34.56%となり、前号の発行時点（2009年1月）から1.28%上昇しました。前回の伸び率（8.84%）に比べると微増でしたが、ドメイン数自体も増えていることを考えれば、着実にSPFを導入するドメインが増えていると言えます。また、企業ドメインに使われる「co.jp」ドメインについては、前回から更に増加し、41.65%と高い宣言率になりました。前回述べたバウンスメールの弊害などの問題もあり、企業ブランドとしてのドメイン名を守る意識が高まってきていることを示しているのではないでしょうか。

一方DKIM関連のレコードの宣言率は、全体で0.37%と導入が非常に遅れていることが分かります。これは、送信側の導入コストに大きな違いがあるためと言われています。

2.3.2 電子署名技術を用いた送信ドメイン認証技術

送信ドメイン認証技術の目的は、受信したメールが正しい送信者情報を名乗っているかを判定できるようにすることです。逆に言えば、送信者情報に示される送信者の管理元（ドメイン）が許可している送信元から送られているかを認証する技術です。

ネットワークベースのSPF/Sender IDでは、送信者の管理元が送信元のネットワーク情報をDNS上のSPFレコードに表明します。DKIMでは、秘密鍵を管理している送信元でなければ付けることができない電子署名

＊6　WIDEが公表している送信ドメイン認証技術の普及率の調査結果（http://member.wide.ad.jp/wg/antispam/stats/index.html.ja）。

をメールヘッダに付加します。メール送信側の秘密鍵が漏れないようきちんと管理されていれば、それを知らない第三者が電子署名を作成することは一般に困難です。この性質を利用して、送信者を特定できるようにしています。

DKIMを送信側で導入するには、これまでのメール配送の手順に加え、送信されるメール本体を利用して電子署名を作成し、それをメールヘッダに追加する作業が新たに必要になります。これらの作業は通常、送信メールサーバ上で行われるため、一般のメール送信者には影響はありませんが、送信メールサーバには新たな機能追加が必要です。この機能追加が、DNS上にレコードを一度だけ書けば良いSPF/Sender IDとの導入コストの大きな差となり、普及率の大きな違いとなっています。

2.4 DKIM認証の流れ

DKIMの仕様は、IETFからRFC4871として公開されています。図-4に、DKIMの認証の流れを説明します。

2.4.1 送信側の手順

DKIMの署名情報は、メールのDKIM-Signatureヘッダとして記述されます。DKIM-Signatureヘッダには、署名そのもの以外に署名対象範囲やハッシュ、暗号化のアルゴリズム、公開鍵の入手情報、署名の有効期限等の情報がパラメータとして一緒に記述されています。

```
DKIM-Signature: a=rsa-sha256; d=example.net; s=brisbane;
      c=simple; q=dns/txt; i=@eng.example.net;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      z=From:foo@eng.example.net|To:joe@example.com|
      Subject:demo=20run|Date:July=205,=202005=203:44:08=20PM=20-0700;
      bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
      VoG4ZHRNiYzR
```

図-5　DKIM-Signatureの例

まず、メール本文とメールヘッダそれぞれでハッシュ値を計算します。ハッシュ計算の前にはメール配送上に発生するメッセージの変換処理*7を考慮して、正規化処理が行われます。メール本文のハッシュ値は、BASE64で変換された後にDKIM-Signatureヘッダ上に「bh=」タグ(パラメータ)として保管されます。ヘッダのハッシュ値は、DKIM-Signatureヘッダを必ず含んだ上で計算されます。他にどのメールヘッダをハッシュ計算に含めるか(すなわち署名対象に含めるか)を決め、選択したヘッダ名をDKIM-Signatureヘッダ上に「h=」タグとして指定します。この時点では、最終的な署名情報はもちろん分かりませんので、ヘッダのハッシュ値の計算には、DKIM-

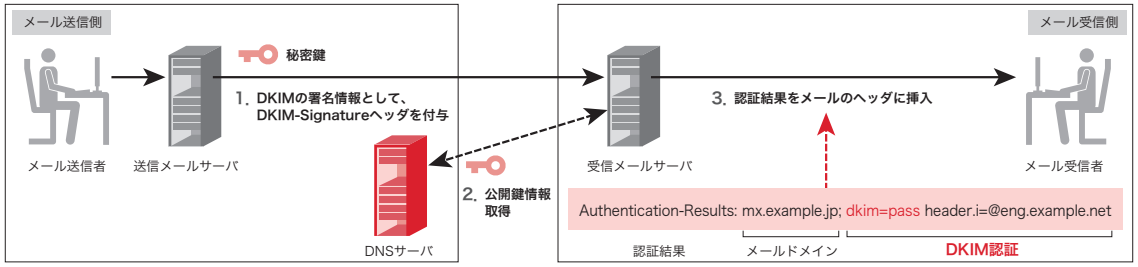

図-4　DKIM 認証の流れ

*7　例えば、配送されるメールやヘッダの一行の長さはメールフォーマットを決めているRFC5322によって推奨値(98文字以下)と最大値(998文字以下)が決められているため、メールサーバ上で折り返し処理が自動的に施される場合がある。

Signatureヘッダの署名情報が示される「b=」タグは含まれません[*8]。ヘッダのハッシュ値の計算には、メール本文のハッシュ情報が含まれているので、メール本文も署名の対象に含まれることになります。

署名情報は、このヘッダのハッシュ値から公開鍵暗号技術を使って作成します。

2.4.2 受信側の手順

DKIMの署名情報が付加されたメールを受信したサーバは、まず受信時に公開鍵を取り出します。取得方法は、DKIM-Signatureヘッダの「q=」タグに指定されますが、デフォルトではDNSを利用します。取り出す先のドメイン名は、DKIM-Signatureヘッダの「d=」タグに指定されたドメイン名と「s=」タグに指定されたセレクタから構成します。例えば、図-5のヘッダの例ではドメイン名が「example.net」でセレクタが「brisbane」ですから、参照先は図-6になります。

```
brisbane._domainkey.example.net
```

図-6　公開鍵の参照先の例

署名元の「example.net」ドメインに続くサブドメイン「_domainkey」は、その配下に DKIM の鍵情報等が格納される固定名となります。

この様に公開鍵の参照先は、実際のメールを受信してそのDKIM-Signatureヘッダをみるまで判断ができません。このことが、DKIMの導入調査を難しくしています。一方、セレクタを導入することの利点もあります。DNSはキャッシュの仕組みがあるため、レコードを書き換えたとしても、すぐにメール受信側に反映されるとは限りませんし、そのタイミングにも差があります。そこで、別のセレクタを使ったドメインに新しい公開鍵を前もって設定しておき、そのペアとなる秘密鍵を変更するタイミングでセレクタ名も変更すれば、メール受信側は混乱なく署名に対応する公開鍵を取得できます。また、サブドメインを分けることにより、鍵の管理を委譲することもできます。これは、ホスティングサービス等に、メールの運用をアウトソースする場合などにも便利です。公開鍵を取り出したあとは、送信時と同様にメール本文を正規化します。その後ハッシュ値を計算し、その値と「bh=」タグの値とを比較します。次に、取り出した公開鍵を利用し「a=」タグで示されたアルゴリズムを使って署名を検証します。

2.5 おわりに

今回の調査結果でも、依然として迷惑メールの量はメール全体の80%を超える高いレベルを維持しています。迷惑メールの送信元が激しく動いていることからも、昨年11月のMcColo社のネットワーク遮断の後に送信方法を模索している動きが感じられますので、今後さらに悪化する可能性も当然あると考えています。IIJは、引き続きOP25Bの導入等、日本の迷惑メール対策の成功事例を世界に対してアピールすることにより、迷惑メール自体の削減に今後も協力していきたいと考えています。また、まだ日本発の迷惑メールが一定数あることから、残されている送信の穴をふさぐための対策も引き続き重要です。今回は、電子署名技術を利用した送信ドメイン認証技術DKIMの概要とその導入動向について解説しました。DKIMでは、正しいメール送信か否かの判定以外にも、メール内容の改ざんが行われたかどうかの判定もできる等の特徴があり、コミュニケーションツールとしての重要性が増し続けているメールの信頼性の確保に活用できます。IIJでは今後も安全なメール接続の実現のため、こうした技術の普及に努め、積極的な情報発信を継続していきます。

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。メールシステムの企画及び調査に従事。特に快適なメッセージング環境実現のため、研究開発や社外関連組織と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。

＊8　パラメータ名を示す「b=」文字列は含むが、「=」の後の値は空にして計算することになっている。