メールアドレスの国際化アプローチに対する考察

今回は、2010年第1週〜第12週での迷惑メールの割合の推移とともに、前年同期との比較結果を示します。また、迷惑メールの主要な送信元地域の傾向の変化、送信ドメイン認証技術の導入状況に加えて、メールアドレスの国際化に対するアプローチの問題点を考察します。

3.1 はじめに

本稿では、迷惑メールの最新動向や、メールに関する技術解説、IIJが関わるさまざまな活動についてまとめています。

今回のレポートでは、2010年第1週(2010年1月4日〜1月10日)から第12週(2010年3月22日〜3月28日)までの12週間分と、2009年一年間分のデータを対象としています。迷惑メールの流量は、時期や迷惑メールの流行のタイミングなど複数の要因で変化しますので、迷惑メールの割合の推移を前年同期と合わせて示すことで、時期的な要因を勘案した比較が可能です。

今回の2.2迷惑メールの動向では、迷惑メールの送信元の分布や、そこからの推測される送信手法などについても分析しました。さらに、迷惑メール対策のための基礎技術である、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。

2.3メールの技術動向では、現在IETFで議論されているメールアドレスの国際化と関連する技術動向についてレポートするとともに、EAI(Email Address Internationalization)の問題点を考察します。

3.2 迷惑メールの動向

ここでは、迷惑メールの動向として、IIJセキュアMXサービス等で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。

3.2.1 2010年第1週から第12週までの迷惑メールは微増

2010年第1週から第12週までの84日間に検出した迷惑メールの割合は、平均82.1%でした。前回(2009年第40週〜52週)の平均が81.4%、2009年同期(第1週〜第13週)が81.5%でしたので、いずれに対しても微増という結果になります。今回の調査期間を含めた2009年からの迷惑メールの割合の推移を図-1に示します。

今回の調査期間には、長期休暇が含まれているため、これまでの調査結果と同様にその時期に迷惑メールの割合が高くなっています。しかし、これまでは長期休暇の期間が終わると迷惑メールの割合が下がる傾向がありましたが、今回は80%を超える比較的高い期間がしばらく続いています。今回の微増は、この継続の延長が原因で

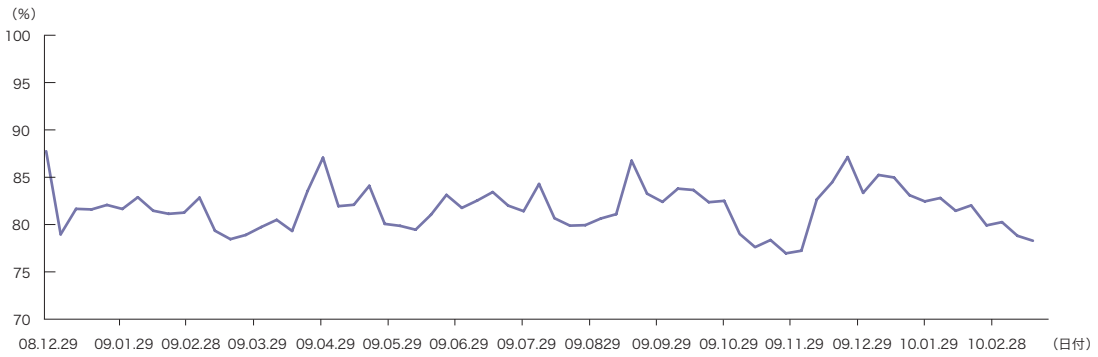

図-1 迷惑メールの割合

あると考えられます。迷惑メールの送信傾向には、時期による要因も影響しますが、送信手法の変化、例えば新たなマルウェア（不正プログラム）の流行に伴うボットネットの増加によって急激に増えることもあります。

近年は、ハードウェアの高性能化やネットワーク帯域の利用増加などもあり、新たな手法が作り出されると、急激に迷惑メールが増える傾向にあります。ISPなどの常に大量のメールを受信する事業者にとって、こうした急激なメールの増加は、安定した運用を阻害する要因になります。ISPのメールサービスで提供されるウイルス対策や迷惑メール判定機能は、主に専門のベンダ企業によるもので、こうした急激な変化への対応が難しくなっています。今後、ISPに対しては、こうした迷惑メール送信手法の動向を把握し、メールシステム全体として素早く対応できる体制が求められます。

3.2.2 迷惑メール送信元1位の地域は、ブラジルから新たに米国に

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位は米国（US）で、迷惑メール全体の9.6%を占めていました。2位は中国（CN）の7.6%、3位はインド（IN）の6.1%でした。これまで連続して首位であったブラジル（BR）は、今回の調査で5.8%となり4位に後退しました。同様に、前回5位だったベトナム（VN）も、今回の調査は3.2%で10位に後退しました。これら2つの国が大きく順位を下げていますが、これは2つの国からの迷惑メールの受信数自体が極端に減少したのではなく、他の上位国からのものが増加したことによる相対的な順位の低下です。図-2のグラフからも、これまでの調査結果と比較して、送信割合が極端に大きい地域が減少していることが分かります。日本の順位は、前回と同様の7位で3.9%、前回より0.1%微増という結果でした。前回の調査でも微増していましたが、その原因は通常のメールサーバと思われる送信元からの迷惑メールが増加していることにあります。

通常のメールサーバから迷惑メールが送信されるケースには、メールサーバが迷惑メール送信の踏み台にされているケースと、転送設定などによって迷惑メールも含めたすべてのメールが転送されているケースが考えられます。このうち踏み台にされているケースでは、外部組織などによるブラックリストに送信メールサーバが登録される可能性が高く、いったん登録されるとそれらを参照している受信メールサーバで受け取りが拒否されてしまいます。日本では、OP25B[*1]の導入時にメール投稿サーバでのSMTP-AUTH[*2]の導入が推奨されているため、簡単にはメールを送信できない仕組みになっています。しかし最近では、迷惑メール送信に利用されるボットPC上の不正プログラムがSMTP-AUTHに対応して迷惑メールを送信しているとの情報もあり、送信時の認証機構だけでは不十分かもしれません。メール投稿時にSMTP-AUTHを利用することに加えて、送信者ごとにメール送信数の上限を設定して大量の送信を防止する、メールログに送信者情報を記録して迷惑メールが送信されてしまった後でも追跡可能にするなどの対応が必要になります。

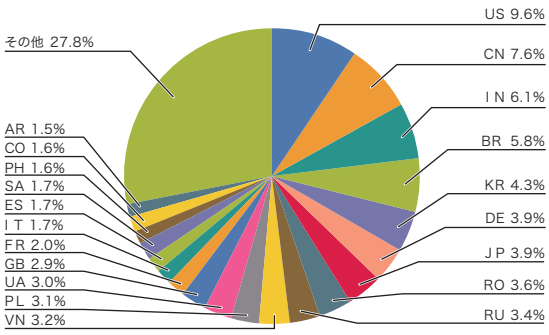

図-2　迷惑メール送信元

＊1　OP25B（Outbound Port 25 Blocking）は、一般のネットワーク利用者に割り当てられる動的IPアドレスに対して、直接外部の受信メールサーバへのメール送信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　SMTP-AUTHは、メール送信時にSASL（Simple Authentication and Security Layer, RFC4422）の機構を利用して送信者の認証を行います。多くの場合、送信者を特定するAuthentication IDとパスワードによって認証されます。SMTP-AUTHはSMTPの拡張としてRFC4954で仕様が定められています。

3.2.3 送信ドメイン認証技術の導入により、迅速なメール受信を

迷惑メール対策には、迷惑メールを判定する迷惑メールフィルタの導入やアンチウイルス機能の導入など、迷惑メールを排除するための機能と合わせて、正しいメールを遅滞なく受信するための仕組みも重要です。近年の迷惑メールの巧妙化やウイルスメールの多様化、ボットネットなどを利用した新種や亜種の瞬間的な流行に対応するため、迷惑メールを判定するための機能に高度な判定処理が導入される傾向にあります。しかし、判定処理自体に時間がかかり、大量にメールを受信したときに配送遅延などが生じる懸念もあります。例えば、ビジネス上の取引先など、すでにメールの送信元が明らかであるときには、こうした迷惑メールの判定処理の一部分を省略して、迅速にメールを受け取りたいと考えるかもしれません。

これまでは、正しい送信元を判断する基準や方法がありませんでした。しかし現在は、送信ドメイン認証技術を導入することで、この要望に対応できます。これまでのIIRで解説してきたとおり、広く普及しているネットワークベースの送信ドメイン認証技術には、転送などメールの再配送時に送信者を正しく特定できない、という問題点が指摘されています。この問題の解決方法についても、普及するまでに時間が必要です。

ただし、この問題が未解決でも、送信ドメイン認証技術による認証結果を利用できます。メールの再配送での認証の誤判定は、受信メール全体の量に対してそれほど大きな割合ではありません。認証できたドメインからのメールを優先して受け取るバイパス的な配送処理の仕組みが受信側にあれば、より迅速に必要なメールを受け取ることが可能になります。送信ドメイン認証技術の認証結果と、特定の送信者をホワイトリストで取り扱うことにより、信頼のある両者間でより効率的なメールの送受信が可能になります。このような状況を促進するためにも、引き続き送信ドメイン認証技術の普及を訴えていきたいと考えています。

3.2.4 送信ドメイン認証技術の導入は微増、効率の良いメール配送を目指す

ネットワークベースの送信ドメイン認証技術のひとつであるSPFの調査結果として、今回の調査期間(2010年1月〜3月)での特定のメールサービスの認証結果の割合を図-3に示します。この期間に受信したメールの認証結果は、全体の55.6%が“none”でした。これは、受信メールの44.4%のドメインでSPFレコードが宣言されていたことを表します。この結果は、前回の調査に比べて0.7%の微増となります。

また、認証結果が“pass”であった受信メールの割合も16.3%で、0.4%の微増という結果になりました。これは、受信メールの約6分の1の割合ですが、これらをすべてホワイトリストに設定すれば、これらのメールに対してより効率のよい配送が可能になります。ただし、最近は、迷惑メールの送信側でもSPFをパスするようなドメインを利用しているため、ホワイトリストの導入時には、認証結果だけでなく、対象とするドメイン名と合わせて処理するように設定することが必要です。

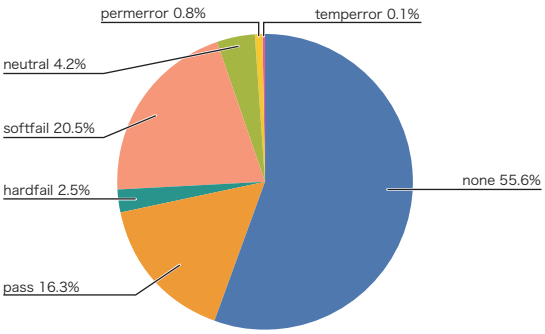

図-3　メールサービスの認証結果の割合

3.3 メールの技術動向

3.3.1 メールアドレス国際化

taro@example.jpといった、インターネットで利用されているメールアドレスは、アットマーク（@）の左右でその役割が分かれています。アットマーク（@）の右側がドメイン名、左側が個々のメール受信者を示すローカルパートです。このような形式のメールアドレスで利用できる文字コードは、基本的にASCII文字列です。アットマーク（@）の右側に置かれるドメイン名の国際化は、すでにIDN（Internationalized Domain Name）という仕組みにより利用可能になっています。IDNの仕組みは、（株）日本レジストリサービス（JPRS）が提供するJPRSトピック&コラムの『No.7 国際化ドメイン名を実現する3つの技術』[*3]に詳しく説明されています。ここでは、その概要を説明します。

ドメイン名の国際化対応は、Unicodeによる文字列を使用可能にしたことで実現されています。Unicodeを採用することで、“日本語.jp”などのASCII文字以外を母語の文字とする言語がそのまま使えるようになります。しかし、Unicodeをそのまま利用することは、既存のプロトコル、特にDNSの仕組みへ大きく影響することが懸念されました。そのため、punycodeと呼ばれる変換方式を導入してUnicodeを符号化し、IDNであることを示すACE prefixを付けることで、これまでどおりの英数字とハイフン（-）だけの組合せとなるようにしています。この符号化の仕組みによって、例えばWebブラウザに入力するURLに日本語のドメイン名が含まれていても、Webページを参照するために必要なIPアドレスをWebブラウザがDNSから取得する際に、punycodeによって符号化されたドメイン名で問い合わせることができます。図-4に、punycodeを利用した“日本語.jp”のIDN表記の例を示します。

符号化例:

“日本語.jp”

↓

“xn--wgv71a119e.jp”

図-4　punycodeによる符号化例

ドメイン名の国際化に関しては、さまざまな議論が交わされた結果、既存の仕組みに影響が少ない手法が選ばれました。今後の普及については、実際にどの程度の需要があるかというマーケット面での要因に左右されるでしょう。

Webブラウザと同様にメールでも、メールアドレスに国際化ドメインが使われたときにMUA（Mail User Agent）がWebブラウザと同様に符号化を実施すれば、既存のメールサーバに影響しないため問題はほとんど生じません。しかし、メールアドレスの国際化の現状は、ドメイン名に加えてアットマーク（@）の左側部分のローカルパートも国際化する動きがあります。しかも、Unicodeを符号化せずにそのまま扱おうとしているため、問題をより複雑なものにしています。

現在提唱されているメールアドレスの国際化（EAI: Email Address Internationalization）について、JPRSトピック&コラム『No.11 電子メールアドレスの国際化 ～ Email Address Internationalization（EAI）の概要～』[*4]で詳しく述べられています。IETFからは、EAI全体の枠組みについてはExperimentalとしてRFC4952、メール配送の仕組みであるSMTP（Simple Mail Transfer Protocol, RFC5321）の拡張仕様についてもExperimentalとしてRFC5336がそれぞれ定義されています。

3.3.2 メール関連プロトコルとEAIは深刻な問題を抱えている

SMTPでのEAIの利用では、これまでのSMTPの拡張機能と同様に、SMTPセッションの開始時のコマンド（EHLO）に対する応答により、受信側メールサーバのEAI対応が判断されます。実際には、EHLOコマンドへの応答に“UTF8SMTP”が含まれていれば、受信側のメールサーバがEAIに対応していることになります。EAIに対応していれば、メールの送信者を示すMAILコマンドの引数reverse-pathや宛先を示すRCPTコマンドにUnicodeを含めることができます。同様に、メール本体のヘッダ部分のFrom:ヘッダやTo:ヘッダにも、そのままUnicodeが利用できます。メール配送の開始時

＊3　http://jpinfo.jp/topics-column/007.pdf
＊4　http://jpinfo.jp/topics-column/011.pdf

に利用可能な機能をお互いにネゴシエーションした上で拡張機能を利用するため、ここまでの処理に大きな問題はありません。

EAIで問題になる部分は、メールの受信側がEAIに対応していなかったときの処理です。例えば、EAIに対応したメールの投稿サーバ（MSA: Mail Submission Agent）がMUAからEAIをそのまま受け取ったが、受信側のメールサーバが対応していなかったとします。いったん受け取ったメールを配送できない場合、通常はエラーメールとして送信者にバウンスされます。このような処理は、EAIの段階的な導入時期にメールシステム全体の可用性を下げるかもしれませんが、それほど深刻な問題ではありません。

より深刻な問題は、下位互換性を維持するためにダウングレーディングという変換方法がEAIに用意されていることです。これは、EAIに対応していない受信側のメールサーバにメールを送信するために、エラーとしてバウンスするのでなく、ダウングレードによりできるかぎり配送しようとするものです。細かな部分ではSMTPに関してもいくつかの疑問点がありますが、もっとも深刻な問題はメールヘッダの変換に関するものです。受信側のメールサーバがEAIに対応していない場合、EAIで記述された元のヘッダ情報が“Downgreaded-”で始まるヘッダに書き換えられ、ダウングレードされたメールアドレスによって既存のFrom:ヘッダやTo:ヘッダが書き換えます。この処理での問題は、送信ドメイン認証技術のひとつであるDKIMが、これらの主要なメールヘッダを署名の対象として参照していることです。署名の対象となるヘッダが書き換えられた場合、当然、署名が不正なものと見なされ、認証が失敗することになります。

これまでメールに関連したプロトコルの拡張は、SPF、Sender ID、DKIMなどの送信ドメイン認証技術や、いわゆる添付ファイルに使われるMIME（Multipurpose Internet Mail Extension, RFC2045）などのように、既存のプロトコルにできるかぎり影響を与えず下位互換となるように慎重に行われてきました。こうした努力をまったく無視するように仕様を拡張しているEAI、特にそのダウングレーディングの仕様は、あまりにも乱暴だと言えます。今後、EAIは、国際標準とすべき仕様を目指して検討が行われる予定のようですが、拡張の仕組みやその手順に関しては、より慎重に議論されることを望みます。

3.4 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、これまでと同様に迷惑メールの割合の推移、送信元地域に関する分析結果、送信ドメイン認証技術のひとつであるSPFの普及状況について報告しました。迷惑メールの割合は、引き続き高い状況が続いており、急増する可能性もあるため、継続した注意が必要です。

メールの技術動向は、これまでの送信ドメイン認証技術に代わり、EAIについて取り上げました。EAIは、送信ドメイン認証技術とまったく無関係なものではなく、むしろその仕様の拡張によって大きな影響を及ぼす可能性がある手法であると考え、今回取り上げました。今回は、EAIの問題点に注目しましたが、本来の目的であるメールの利用者層を広げること自体には賛成です。メール利用者層の広がりを目指して、常日頃ASCII文字を使うことがない地域や民族の人々が、より簡単に電子メールを利用できるようにするための仕組みを模索したり検討したりすることは、むしろ積極的に行うべきです。しかしながら、それを実現する手法が、これまでのプロトコル拡張の積み重ねを無視するような強引なものであるときには、メールの利用環境自体を分断する可能性があります。新たな仕様の導入については、これまでと同様に、より慎重に検討すべきです。あるいは、よく多くの地域や民族の人々が利用するに適したメッセージ伝達のための新たな枠組みが必要になってきているのかもしれません。

執筆者：
櫻庭 秀次（さくらば しゅうじ）
IIJ サービス本部 アプリケーションサービス部 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。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。