

送信ドメイン認証技術の送信側導入状況はやや停滞

今回は、2010年第26～38週での迷惑メールの推移を報告します。迷惑メールの送信元地域は、中国に代わって米国が1位になりました。また、今回は、送信ドメイン認証技術の導入状況とボットネット対策についても考察します。

3.1 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する技術解説など、IJ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年の第2四半期にあたる第26週(2010年6月28日～7月4日)から第38週(2010年9月20日～9月26日)までの13週間分のデータを対象としています。

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、IJ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出した割合の推移と、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。

3.2.1 前年までとは異なり、9月以降も迷惑メールは増えず
2010年第26週から第38週までの91日間に検出した迷惑メールの割合は、平均79.0%でした。前回(2010年第13～25週)の平均が81.3%、2009年同期(第27～39週)が82.2%でしたので、いずれも若干の減少という結果になります。今回の調査期間を含めた2009年第27週からの迷惑メールの割合の推移を図-1に示します。

これまでの調査では、日本の連休期間に重なる第32週(8月9日～15日)に、通常のメール流量が減少することで迷惑メールの割合が高くなり、その後に減少するものの9月以降に再び高くなるという傾向が続いていました。今回も8月までは同じような割合で推移し、第32週がこの期間でもっとも高い割合である82.6%を示

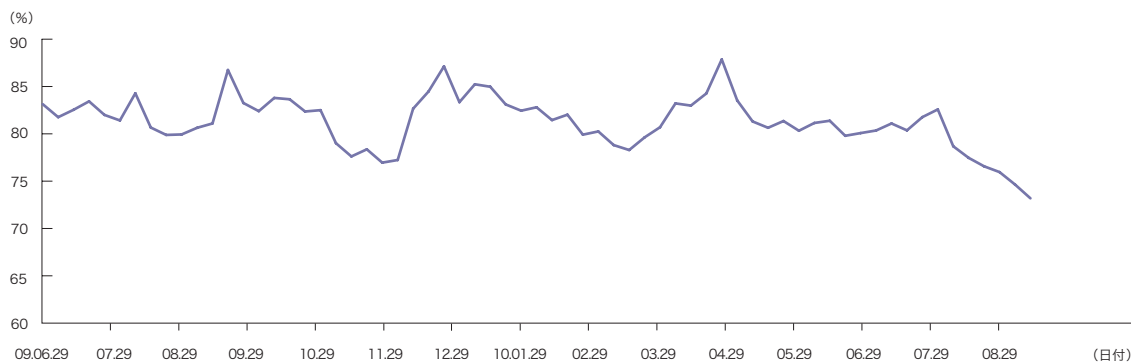


図-1 迷惑メール割合の推移

しました。しかし、9月以降になっても低い割合が続いたため、この期間全体の迷惑メールの平均値が低くなっています。この減少が一時的なものなのか、何かの理由によって今後も迷惑メール量が減少していくのかは不明です。今後の分析とともに調査していきたいと考えています。

3.2.2 中国に代わって米国が迷惑メール送信元1位に

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11.3%を占めていました。前回の2位から順位を上げ、再び首位に戻りました。2位はインド (IN) の7.4%で、前回の3位から上昇しています。3位は前回首位だった中国 (CN) で7.1%でした。また、前回上昇傾向を示していた欧州の英国 (GB) とドイツ (DE) は、それぞれ5

位 (5.0%) と7位 (4%) となり、引き続き高めの傾向にあります。その他は、ブラジル (BR) が4位 (5.2%)、ベトナム (VN) が6位 (4.8%) と、これまでも割合が高かった地域が引き続き上位を占めています。日本は、割合が0.1%微減して順位を8位 (3.8%) に後退しています。

図-3に、これらの迷惑メール送信元の上位6地域 (US、IN、CN、BR、GB、VN) での割合の推移を示します。前回1位だった中国 (CN) は、7月に低下していますが、8月以降は上昇傾向にあり、今後再び上位送信地域になる可能性があります。今回1位であった米国 (US) は、調査期間中を通してほぼ1位であったため、全体でも首位になりました。これら以外の上位4地域 (IN、BR、GB、VN) は、大きな変動はありません。ただし、今回2位であったインド (IN) は、時期によって1位や2位になっているため、引き続き注意が必要と考えています。

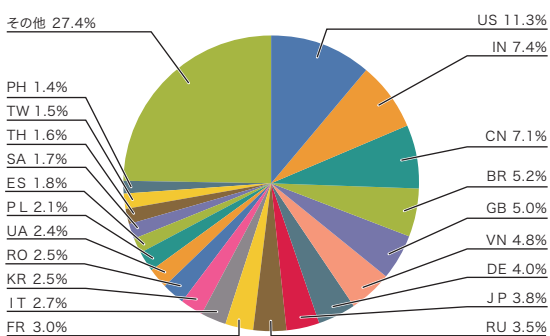


図-2 迷惑メール送信元地域の割合

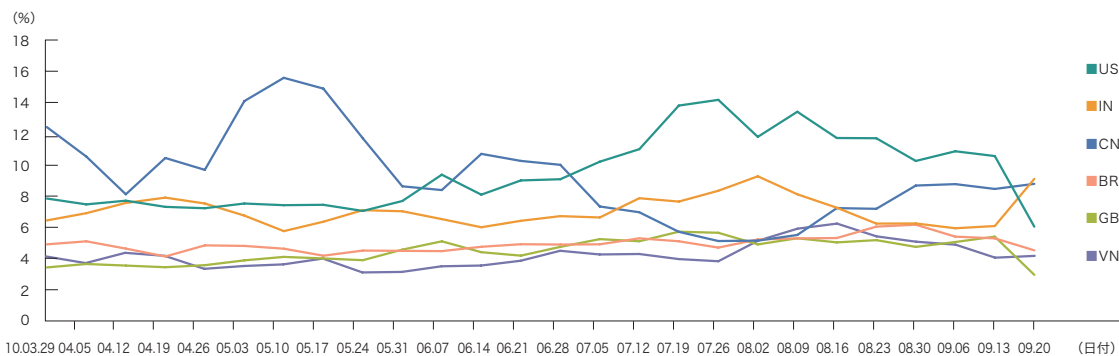


図-3 迷惑メール送信元のうち上位6地域の推移

3.3 メールの技術動向

前回到引き続いて今回も、広く普及している送信ドメイン認証技術の一つである SPF (Sender Policy Framework) の導入状況について報告します。また、今回は、迷惑メール送信の主な原因であるボットネットを根絶させるための活動事例についても報告します。

3.3.1 送信ドメイン認証技術

IJが提供しているメールサービスでは、メール受信時の送信ドメイン認証をほぼ標準で行っています。図-4に、今回の調査期間(2010年7～9月)での認証結果の割合を示します。この期間に受信したメールの認証結果は、全体の55.7%が“none”でした。これは、受信メールの約44.3%のドメインでSPFレコードが宣言されていたことを表しています。この結果は、前回の調査結果に比べて0.8%の微減になります。また、JPドメインだけを調査しても減少していました(図-5)。WIDEプロジェクトの調査^{*1}でも、以前に比べて横ばい傾向にあるため、導入ドメイン数があまり伸びていないことが予想できます。

総務省では、IJを含めた電気通信事業者6社でのSPFの認証結果の割合の推移を、2009年8月から統計データとして公表しています^{*2}。最新データの2010年8月では、認証結果のうち“none”が約18%でしたので、受信メールの約82%のドメインがSPFレコードを宣言していることになります。

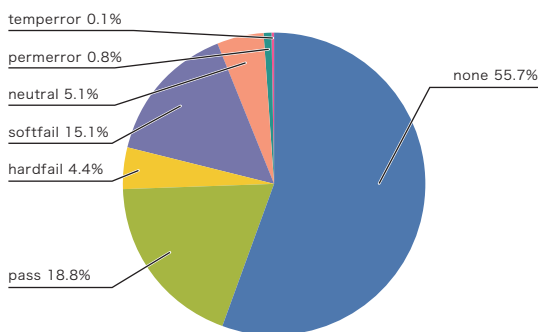


図-4 送信ドメイン認証結果の割合

この結果は、本レポートでの結果と大きく異なっています。これは、メールサービスの利用者層や集計ポイントの違いによるものと考えられます。例えば、携帯電話では、受信メールの多くが携帯電話から送信されたものです。携帯電話事業者のほとんどのドメインがSPFレコードを宣言しているため、高い認証結果になることが予想できます。このことから、送信ドメイン認証技術の導入傾向を把握するためには、それぞれのデータの絶対値を比較するのではなく、それぞれの割合の時間的な推移で判断したほうがよいと思えます。

データの集計開始時点での導入割合が元々高かったこともあり、いずれの結果でも、最近の傾向として導入が進んでいるとは言い難い状況が続いていることがわかります。

3.3.2 ボットネット対策

今回報告した迷惑メールの送信元地域で7位のドイツ(DE)では、迷惑メールの主な送信手法であるボットネットを根絶するために、The German Anti-Botnet Initiative^{*3}を今年9月に立ち上げました。これは、ドイツのインターネット産業協会であるecoと連邦政府組織であるBSI(The Federal Office for Information Security)の協力の元に運営されるプロジェクトで、不正プログラムに感染した一般ユーザに警告を発し、正常に戻るまでインターネットへのアクセス制限なども行う対策です。このプロジェクトでは、不正プログラムを駆除するツールを提供したり、電話サポートを行ったりすることで、ユーザのPCをクリーンにしようと計画してい

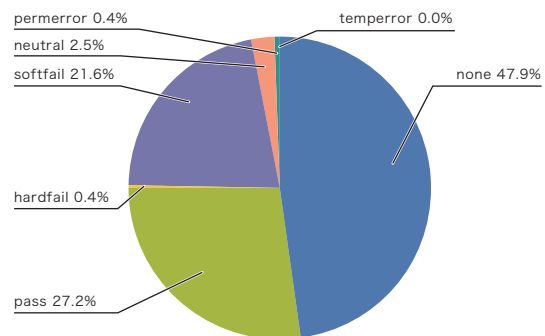


図-5 送信ドメイン認証結果の割合 (JPドメインのみ)

*1 2010年8月現在でのJPドメインにおけるドメイン認証技術のおおよその普及率 (<http://member.wide.ad.jp/wg/antispam/stats/index.html>)

*2 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei

*3 <http://www.oecd.org/dataoecd/42/50/45509383.pdf>

ます。日本のCCC (Cyber Clean Center)^{*4}での取り組みに非常によく似ていると思われるかもしれません。実際に、このプロジェクトに関わっているecoのメンバーがCCCの関係者にヒアリング等を行っていますので、かなりの部分を参考にしたのではないかと思います。また、今年の6月に開催されたMAAWGのGeneral Meetingでも、CCCの活動が報告されました。

迷惑メールの送信を止めるだけであれば、日本で広く導入されている、動的IPアドレスからの直接メール送信を止めるOP25B (Outbound Port 25Blocking) が非常に効果的な方法になります。ポットネットは、迷惑メールの送信だけでなく、不正プログラムの配布元やDDoS攻撃の発信元になったり、不正プログラムによってPC内の個人情報を搾取したりすることに使われるなど、より深刻な被害の原因になります。このため、ポット化されるときは主な原因である、不正プログラムが添付された迷惑メールの流通を抑えるために、まず通信事業者がOP25Bを導入することが必要です。そして、そこでブロックした情報や、不正プログラムが指令を受けるために使用したDNSの問い合わせ情報などから、感染したPCを特定します。また、おとりホストを運用し、不正アクセスの送信元を検知することもできます。さらに、CCCやThe German Anti-Botnet Initiativeでの活動のように、駆除ツールを配布し、ポット化の原因である不正プログラムを除去します。

このように、ポットネットを根絶するための手順は、ある程度確立されつつあります。しかし、不正プログラム駆除のためには、それ相当のコストがかかります。日本やドイツのプロジェクトでは、主に政府が費用を負担していますが(ドイツは初年度)、最終的にはそれぞれの国の国民がこのコストを負担していることとなります。こうした負担を軽減するためにも、個々の利用者がポット化されないように日頃からの注意が重要です。

執筆者:

櫻庭 秀次 (さくらば しゅうじ)

IJ 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JEAAG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。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 <http://www.ccc.go.jp/>

*5 http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html

3.4 おわりに

日本における迷惑メール対策法ともいえる「特定電子メールの送信の適正化等に関する法律(特電法)」には、施行3年後の見直し規定が盛り込まれています。平成14年に公布された特電法は、平成17年と平成20年にそれぞれ改正され、今回も特電法の施行の状況等を踏まえつつ、今後の迷惑メール対策として必要な措置を検討するための会合が今年の9月から開催されました。今回は、「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」の下に「迷惑メールへの対応の在り方に関する検討WG」が設置され、このWGの会合で検討が行われています^{*5}。IJでは、この特電法の見直しのための検討に継続して参加しており、今回は本レポートの報告者が構成員として参加しています。

前回の改正では、特定電子メール(いわゆる広告宣伝メール)を送信するためには事前の同意が必要なオプトイン規制が導入されるという、大きな変更がありました。しかし、個人的に受信するメールをみても、オプトインした覚えの無い、様々な勧誘を行う広告宣伝メール的な迷惑メールが相変わらず届く状況が続いています。こうした状況が続く背景には、様々な要因があるわけですが、そもそもメールの送信者を明確に特定することができないことが大きな原因の一つと考えています。

送信ドメイン認証技術を普及させることによって、こうした問題のある程度改善していけるのではと考えています。IJでは、技術的な問題解決だけでなく、こうした法的な側面を含め、今後も迷惑メール対策に積極的に関わっていく予定です。