主要ISP・通信事業者30社でJEAGを設立

ドメイン認証技術を導入したIIJが語るスパムメール対策の最新動向

スパムメールの数は増え続け、フィッシング詐欺などの犯罪にも利用され始めている。スパムメール対策技術への対応が急務とされている中、IIJは3月17日、自社に送信ドメイン認証技術を導入することを発表した。「Japan E-mail Anti-Abuse Group（JEAG）」の発起人でもあるIIJ（インターネットイニシアティブ）は、スパムメールの現状と将来をどのように捉えているのだろうか。

野本 幹彦
フリーライター

増加し続けるスパムメールは法規制では撲滅できない

シマンテックが2005年3月3日に公表したアンケート調査によると、55.2％のユーザーが1日1通以上スパムメールを受け取り、1日10通以上スパムメール受信しているユーザーが18.4％になるという（ISPなどの有料メールの場合）。無料メールの場合は、1日1通以上が60.0％、10通以上が19.7％とさらに比率が上昇し、スパムメールの処理にかかる時間は平均で1日7.78分、1日10分以上かかるユーザーが26.7％に上っている。さらに同社がモニター対象としている企業のスパムの増加量を見ると全メールトラフィックに占めるスパム量の多さが見て取れる（図1）。

このような電子メール量全体のうち、ほとんどをスパムメールが占める場合などはメールサーバーやシステムへの負荷も問題視されている。

国内のスパムメールに対する法規制としては、「特定電子メールの送信の適正化等に関する法律」（特定電子メール法）が2002年7月に施行されている。施行直後はスパムメールが一時的に減少したというデータもあるが、罰則規定である行政処分が困難であることなどから効果的な法運用が行えているとはいえず、迷惑（スパム）メールの数は年々増加する一方となっている。また、送信者側の手口も巧妙化し、送信者の偽装、なりすまし、メール送信の経路情報を正しく記録しないオープンリレーサーバーを使った中継（図2）など、受信側が送信者を特定できないような手法を使うケースが多い。そのため、総務省が違法送信者に警告メールを送信しても、送信者名やメールアドレスを変え、警告を無視して再びスパムメールを送り続けているのが現状だ。

スパムメールを減少させるためには、今や法規制だけでなく、ISPなどの電子通信事業者の自主規制やスパムメール対策技術の開発／導入が不可欠となってきている。総務省が2004年10月に発表した「スパムメールへの対応の在り方に関する研究会」の中間とりまとめでも、「措置命令など政府による法執行のみでスパムメールを撲滅することや、フィルタリングなどの技術的対策のみでスパムメールの受信を回避することは困難である」とし、「政府による効果的な法執行」「電気通信事業者による自主規制」「技術的解決策」「利用者啓発」「国際協調」の5つの柱で対策を行うべきとしている。

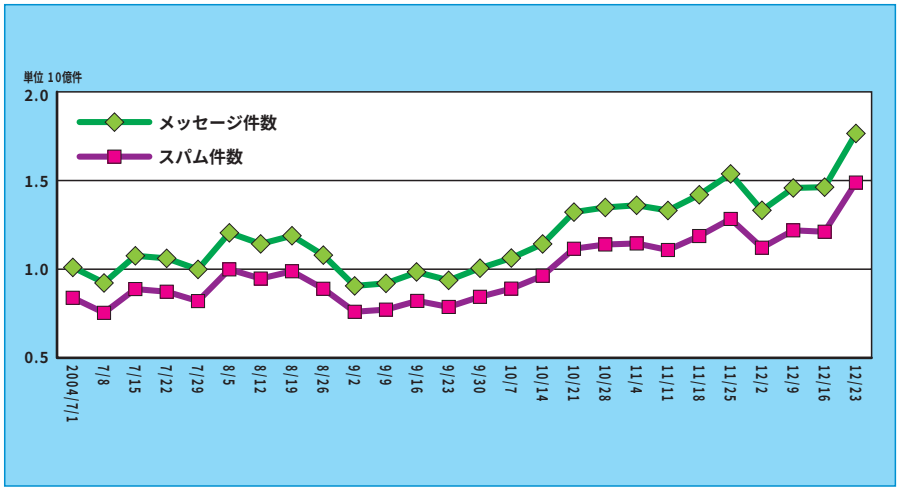

図1　シマンテックのモニター対象企業における2004年下期のスパム量の動向　出典：シマンテック

IIJが導入するSender ID/SPFとDomainKeys

IIJでは今回、IPアドレスベースで認証

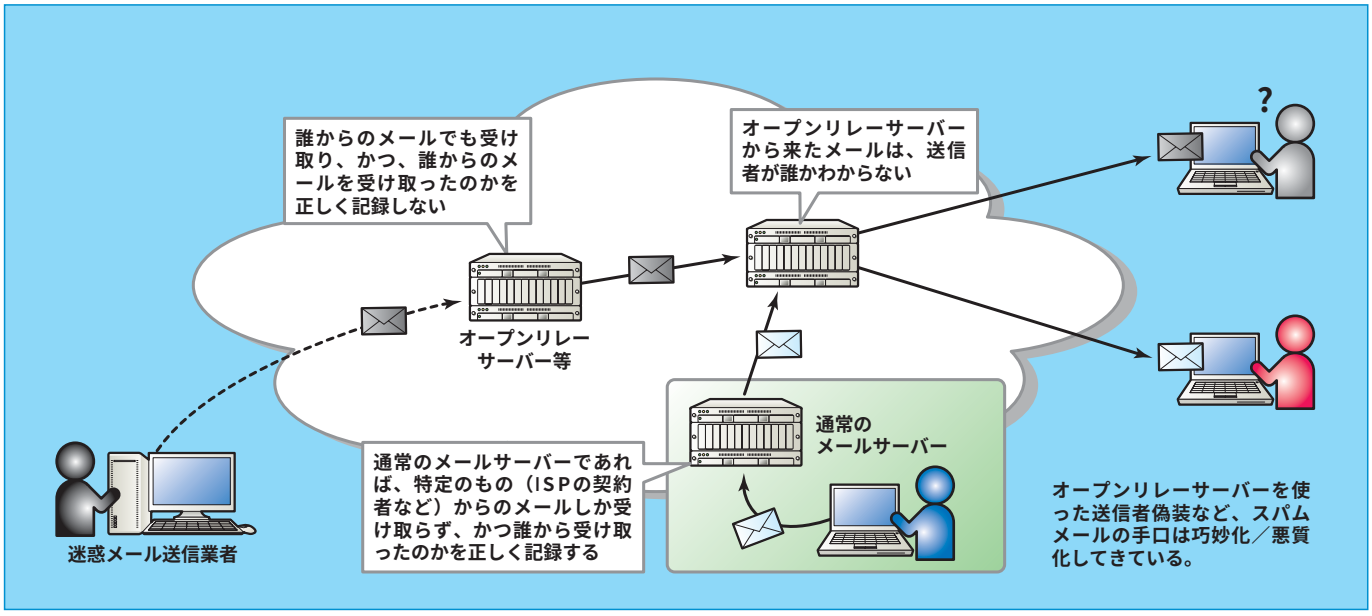

図2　オープンリレーサーバーの利用イメージ

を行うSender ID/SPFと、公開鍵暗号を使った電子署名で認証を行うDomainKeysの2つの送信ドメイン認証方式を自社に導入すると発表した。では、これらの送信ドメイン認証によって、スパムメールはどのように制御されるのだろうか。

Sender ID/SPFは、DNSのTXTレコードに記録されたIPアドレスを元に送信者のドメインを認証する方式だ（図3）。送信者が送信元を偽装して「xxx@impress.co.jp」というメールアドレスでスパムメールを送信しても、「impress.co.jp」の正しいIPアドレスが記録されていればDNSで確認が行われ、IPアドレスの異なるメールの受信を拒否できるようになる。また、DomainKeysでは、「impress.co.jp」用の電子署名をもちいることによって、送信者が「impress.co.jp」と偽装してメールを送ってきても、署名の有無で送信者を判定できるものだ。IIJでは、これら2つの認証方式のどちらか、または組み合わせによって、ドメイン名を詐称するスパムメール（特にフィッシングメールなどの詐欺目的の行為）への対策を効果的に行うことができるとしている。

メール送信業者のメリットを下げることが重要

しかし、これらの技術によって、スパムメールが完全にシャットアウトされるわけではない。Sender IDやSPFのニュースを探せば、スパムメール送信業者が積極的に自分のドメインを登録しているとか、IPアドレスベースで認証されたメールアドレスの多くがスパムメール送信業者のドメインであったという調査などの記事が目に付く。

「送信ドメイン認証はあくまで偽装を暴くものであって、スパムメールを判断するものではない」とプロダクト推進部プロダクトマネージャーの近藤学氏はいう。送信元の偽装を防ぐことによって、怪しいメールやフィッシングなどの不正行為を目的としたメールをトレースしやすくなり、特定電子メール法に基づいて指導を行ったり、犯罪として検挙できる確立も高くなってくる。「怪しいものをチェックしていく、何段階かの一番最初の所」と近藤氏が言うように、これらの技術を使い

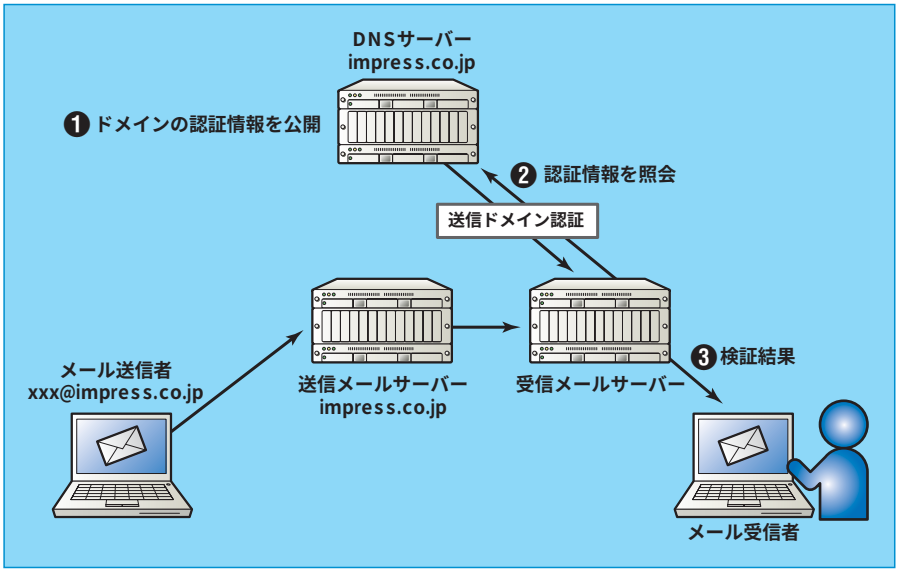

図3　送信ドメインを詐称したメールを受け取らないようにする送信ドメイン認証技術。

株式会社インターネットイニシアティブ
取締役
戦略企画部部長
三膳孝通氏

株式会社インターネットイニシアティブ
プロダクト推進部
プロダクトマネージャー
近藤学氏

続けていくことで信頼できない送信元を淘汰させていく効果は出てきそうだ。

また、取締役 戦略企画部部長の三膳孝通氏は「送信業者のリスクが高くなることで、投資効果が下がる効果がある」という。前述のシマンテックのアンケート調査でも、スパムメールに書かれてあるURLにアクセスすると答えたユーザーが13.8％存在し、米国の調査でもスパムメールで宣伝された製品やサービスを購入した人が4％という結果が出ている。低いコストやリスクで結果が出せるということがスパムメールが増加する原因の1つとされているが、送信元を曝さず、手間もかけずに数千通のメールを送った結果4％の購買につながれば、大きなメリットを得たといっても過言ではないだろう。しかし、送信ドメイン認証技術によってこのような業者が特定されていき、ユーザーの意識が啓蒙されていけば「スパムをばら撒いても誰も読んでくれない」という状況を作ることができるのだ。

送信ドメイン認証はメールシステムのリテラシーの1つ

欧米ではスパムメールの被害が深刻化しており、銀行やカード会社のサポート業務のほとんどがフィッシングの対応に追われているという話も聞く。そのため、「Sender IDやSPFをすでに導入している企業も多く、海外とやり取りする国内企業の中にはメールが届かなくなって困ったというケースもある」（近藤氏）というように、いち早く送信ドメイン認証技術が取り入れられている。Sender IDやSPFは標準化技術としての認定はされていないが、すでに多くの企業が取り入れるデファクトスタンダードと化しており、メールを確実に届ける「メールシステムのリテラシーの1つ」（近藤氏）と考えなければならない状況となっている。送信ドメイン認証技術を取り入れていないため、国内でも取引先とメール交換できないケースが生まれるという状況も近いのかもしれない。

前述のように送信ドメイン認証技術は、送信者の詐称を防ぐ技術であるため、実際のスパムメール対策は受信側の企業や個人が行う必要がある。そのため、送信ドメイン認証に登録されているドメインの信頼性を判断する仕組みが必要だ。

欧米の企業では、レピュテーション（reputation：世評、評判）とアクレディテーション（accreditation：基準を満たしていると認定されたもの、信頼できるもの）という考え方でこの仕組みが作られている。送信ドメイン認証に登録されているドメインの評判や信頼度を示すリストを作成し、これらのリストを元に企業などでセキュリティーポリシーを立て、信頼できるドメイン以外からはメールを受け取らないという動きとなっているのだ。その際の考え方も、「ブラックリストのメールを受け取らない」のではなく、「ホワイトリストの信頼できるメールを受け取る」というように変化してきている。「知らない人とメールをやり取りすることは考えにくく、ホワイトリストに入っていない相手でも、やり取りする中で信頼関係が生まれ、ホワイトリストに昇格していく」（近藤氏）といったメールに対する新たな考え方が今後は定着していくのだという。一方で、これらのリストを作成するビジネスもすでに登場し、アイアンポートシステムズなどの企業がサービスとして提供し始めている。ソフトウェアの認定プログラムのように、ある一定の基準を判定してもらい、判定料を支払うことによって評価を得られるようにするサービスもあるようだ。

スパムメールはウイルスなどとは異なり、その判断基準があいまいで難しい。仮に怪しいメールをすべてスパムメールと判定するような技術が導入されてしまえば「技術でガチガチに縛ってしまうことになり、間違いメールすら出せなくなってしまう」（三膳氏）というように、メールシステム自体が使い勝手の悪いものとなりかねない。三膳氏は、「送信ドメイン認証技術は信頼性を作るための技術で、ISPや企業などがその手段を提供していくというのが原則論。後は、受信側の依頼によってセキュリティーポリシーを決めて運用するため、ユーザーへの啓蒙活動が重要となる」と語る。

スパムメール対策の業界団体JEAG

スパムメール対策の技術的な見地を元にした対策を検討・実施するワーキング

グループJEAGは、IIJなどを発起人として2005年3月15日に創設されている。国内の主要ISP、通信事業者などをはじめとする30社以上が参加(表1)し、技術的な議論や共同作業をつうじて統一した方向で技術やポリシーを導入していくことを目標としている。また、ユーザーの啓蒙活動はもちろん、サービス提供事業者への啓蒙活動も対策の一部と考えている。

JEAGは、いきなり3月に創設されたのではなく、1～2年前から数社が集まってスパムメール対策について情報交換してきたのをベースに、必要に迫られて自然発生的に生まれたものだという。このため、「結果を出すことがすべてと考えており、いかにすばやく動けるかが重要。理事会などは作らず、各社が技術を持ち寄って、できるところからやっていく」(三膳氏)というように、フットワークの軽い団体として活動していくようだ。スパムメールの問題が深刻化していく中、特定電子メール法の改正も3月に国会に提出され、JEAGに総務省や警察庁がオブザーバーとして招かれるなど官民一体の動きも出てきている。「国際協調」の面でも、IIJはAOLやヤフー、アースリンク、オープンウェーブシステムズなどが2003年12月に創設した北米のスパムメール対策のワーキンググループMAAWG(Messaging Anti-Abuse Working Group)のメンバーでもあり、JEAGとMAAWGの間で密に連携を取り合う体制はできているという。

メールやネットワークの転換期を迎えて

インターネットが一般化してから10年になるが、三膳氏は「スパムメールなどが問題化してきたのは、インターネットがきちんとした社会基盤として成立し始めた証拠」だと言う。これまでとは異なり、誰でもが使うということを前提に、ネットワークを再設計しなければならない段階に来ているというのだ。

JEAGなどの活動を通して、ネットワーク全体やメールシステムを「信頼」という部分で作り直していくことをこれから行っていくため、「技術やサービスなどのさまざまな分野で積極的に先進的な役割を果たしていきたい」(三膳氏)と考えているようだ。国内ではまだ導入が遅れている送信ドメイン認証技術だが、「リテラシー」として必要になる日はもう目前に迫っている。今後のサービス事業者や政府などの動向に注目していきたい。

【発起人】
株式会社インターネットイニシアティブ(IIJ)
株式会社エヌ・ティ・ティ・ドコモ(NTTドコモ)
KDDI株式会社(KDDI)
パナソニック ネットワークサービシズ株式会社(hi-ho)
株式会社ぷららネットワークス(ぷらら)
ボーダフォン株式会社(Vodafone)
【設立メンバー】
株式会社IRIコミュニケーションズ
アイアンポート システムズ(IronPort)
アットネットホーム株式会社(@NetHome)
株式会社インターネットイニシアティブ(IIJ)
エヌ・ティ・ティ・コミュニケーションズ株式会社(NTT Com)
株式会社エヌ・ティ・ティ・ドコモ(NTTドコモ)
株式会社エヌ・ティ・ティ ピー・シー コミュニケーションズ(NTTPC)
株式会社大塚商会
KDDI株式会社(KDDI)
有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)
センドメール株式会社(SENDMAIL)
ソニーコミュニケーションネットワーク株式会社(So-net)
ソフトバンクBB株式会社
東芝ソリューション株式会社
ニフティ株式会社(@nifty)
日本アイ・ビー・エム株式会社(日本IBM)
日本インターネットエクスチェンジ株式会社(JPIX)
日本オープンウェーブシステムズ株式会社
日本テレコム株式会社(ODN)
日本電気株式会社(NEC)
日本ヒューレット・パッカード株式会社(日本HP)
パナソニック ネットワークサービシズ株式会社(hi-ho)
株式会社ぷららネットワークス(ぷらら)
フリービット株式会社(FreeBit)
ボーダフォン株式会社(Vodafone)
ミラポイント ジャパン株式会社(Mirapoint Japan)
ヤフー株式会社(Yahoo! JAPAN)
他

表1　JEAGのメンバー企業

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp