1 ISPにおける対策

松下電器産業（株）eネット事業本部
ネットワークサービスエンジニアリングセンター
加藤 佳実　kato.y@jp.panasonic.com

spam（迷惑メール）の現状

ユーザに対して勝手に送り付けられる有害無益なメール群を総称して，spamメール，もしくは，迷惑メールと呼ぶ．

spamメールの数は，最近，増加の一途をたどっており，「メールトラフィックの60%はspamメールである」という数字も出ている[1)]．

ISPにとっては，

- 電子メールの大幅な遅延
- spamメールを受信したユーザからの苦情の増加
- 本来なら不要なはずの設備の増強

など，経営を圧迫しかねないほどの脅威となってきている．

さらに，phishing☆1に代表される，メールを使った詐欺が増加するにつれ，メール自体が信頼できない意思伝達手段になりさがる危険性を秘めている．

「振り込め詐欺」や「ワンクリック詐欺」☆2などにおいて，spamメールが重要な役割を担っていることは周知の事実であり，各ISPはspamメールを撲滅すべく多大な労力をかけている．

しかし，spamメール送信者もその対処を研究しており，現時点においては，spamメール対策はいたちごっこの様相を呈しており，決定的な防止手段がない状態である．

一方，ISPは，電気通信事業者として「通信の秘密」「役務提供の義務」ならびに「個人情報保護」などを遵守すべき立場にあり，このことがspamメール対策を進めるにあたって非常に微妙な問題をはらんでいることも，対策を難しくしている．

以下，ISPとして，spamメールに対する運用面からの対策と，対策を進める上での問題点について述べる☆3．

spamメールの送信手法

spamメールの送信に使われる主な手法としては，

- 契約しているISPのメール送信用サーバを使用して，大量のメールを送りつける
- 自前でメール送信用サーバを立ち上げ，大量のメールを送りつける

が以前の主流であったが，昨今は，

- ゾンビPC群（後述）を使って，spamメールを送りつける

が主流となった感がある．また，

- メールアドレスを収集する目的で，大量のメールを，サーバに対し送りつける

も相変わらず行われている（図-1）．

上記の手法は，いずれもspamメールを受信するサーバの負荷を増大させ，メールサービスに支障をきたすとともに，膨大なサポート工数を発生させるため（現状，サポート業務の半分以上はspam対応というISPもあるとのこと）ISPにとって問題となっている．

また，メールアドレス収集目的のメール送信については，存在しないアドレス宛てのエラーメールが，送信先アドレスとして騙られたユーザに大量に届くことによる被害も多発しており，誰もがspamメールの被害者になり得る．

このようなspamメールの送信行為に対し，各ISPはいろいろな取り組みを行い，ユーザへ迷惑をかけないように努力している（表-1）．

しかし，どの手段も「迷惑メール」が「迷惑な」状態

☆1 phishing：正規のサイトを装って，クレジットカード番号などを騙し取る詐欺行為．
☆2 ワンクリック詐欺：サイトのボタンを1度押すだけであたかも物やサービスを購入したように見せかけて，料金を騙し取る詐欺．
☆3 記述において定量的な部分が少ないかもしれないが，定量的な数字を公にすることが難しいISPの現状をご理解いただきたい．

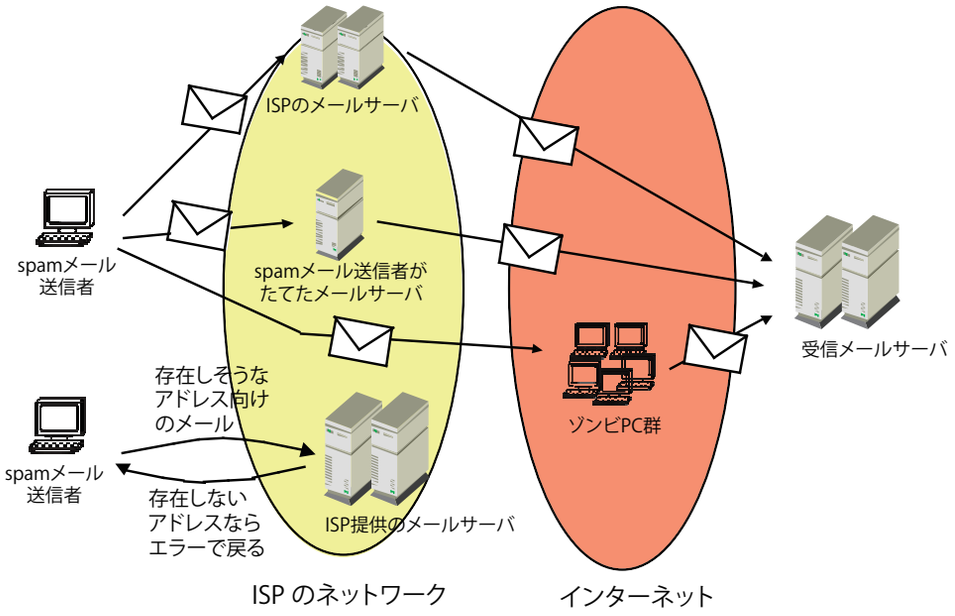

図 -1　spam メール送信の手法

ISP のメールサーバを使って，メールを出す場合	• 一定以上の流量に対して，以降の送信効率を下げる • サーバ負荷が一定になると，以降のメールを受け取らない，もしくは，受け取るスピードを下げる • ユーザの存在確認ができるまでは，メール総数を抑制する • 同一 IP アドレスからの同時送信数を抑制する • 存在しないドメインを送信者アドレスとしたメールを拒否する
自前で送信サーバを立ち上げ，メールを出す場合	• 同一 IP アドレスからの同時送信数を抑制する • 存在しないドメインを送信者アドレスとしたメールを拒否する • 苦情の多いメールを送ったユーザに対して警告を行い，従わない場合は規約に基づき一時的に通信できない状態とする
メールアドレス収集を目的としたメールを送りつける場合	• 1 回のメール送信手順において，大量の宛先を受け付けないようにする • 一定数以上の宛先不明の発生したトラフィックは，以降の受付をしない • すべてのメールを受け付け，メール送信時点におけるアドレスの生死は分からないようにする

表 -1　spam メール送信に対する対処方法の例

になって初めて，検知・対処する方法であり，それまでに送信されてしまう spam メールに対しては無力である．

■ ユーザ向け対策

企業など，ポリシーを一元的に強制できる事業体においては，spam メールの判定基準を一律として，その基準でメールを選別することは可能であると思われる．

しかし，さまざまな考え方を持つユーザにサービスを提供している ISP としては，あくまで最終的なメールの選別はユーザにお願いせざるを得ない．

明らかに spam メールであると思われるメールについても，その選別の是非はユーザ側にあり，ISP が勝手にメールを選別することはできない．

そのため，各 ISP はユーザの判断を助ける手段を提供することで，ユーザに対して spam メール対策を提供し

ているのが現状である.

ISP の提供している spam メール対策は,

- ユーザの PC にフィルタリングソフトを導入していただくもの
- ISP 側のサーバで spam メールとしたメールに識別情報をつける／別領域に移動するもの

に大別できる.

• ユーザの PC にフィルタリングソフトを導入していただくもの

最近のアンチウイルスベンダのウイルス対策ソフトは, spam メール対策機能を装備しているものが多い.

ISP としては, spam メール対策をウイルス対策と同時に行えるメリットがあるため, このようなソフトをユーザに購入してもらうサービスを行っているところもある.

この方式の難点は, 判定精度が今ひとつのものが多く, spam メール対策としては価格が高いことなどが挙げられる.

また, POPFile[2] など, spam メール排除に特化したオープンソースプログラムをユーザに導入していただくことを検討している ISP もあるが, サポートに限界があるため, なかなか踏み切れないのが実情である.

• ISP 側のサーバで判定を行うもの

受信したメールに対して条件をあてはめ, 合致するかどうかを判定し, spam メールと判定されたメールをユーザが区別できるようにする.

どの ISP もほぼ同じ機能を提供しており,

- 「未承諾広告※」など, 特定語句が入っているメールを無条件で認定する
- お客様が指定した文字列にマッチするメールを無条件で認定する
- spam メール送信者のデータベース（会社組織が提供するもの, ボランティアで運営されているもの, など） と比較して, 認定する
- ベイジアンフィルタなどを使って学習させ, その条件で認定する

などによって spam メールを特定し, その該当メールに対して

- 標題に [spam] とつける
- X-spam などのヘッダを追加する
- 別領域に移動する

などの方法により spam メールを選別しやすくする.

しかし, 各種設定をユーザ自らが行わないといけないものが多く, spam メールを不快に思いながらも, 設定の手間を嫌って設定をしないユーザも多い.

ISP としては, どのような手段をとれば, サービスをお使いいただけるかに知恵を絞っているが, 地道な啓蒙活動以外に有効な手段が見つからないのが現状である.

最近は, 各種雑誌などで spam メールの特集が増えており, このようなメディアとのコラボレーションによって, 一般のユーザの理解が進む方向にあることは喜ばしいことである.

【ゾンビ PC 対応】

ADSL/FTTH などの高速回線の普及とともに, 自宅や会社において簡単に無停止の公開用 PC を立ち上げることができるようになってきた.

しかし, セキュリティ設定の甘いものが多く, ウイルス感染やクラッキングなどの手段により, 持ち主が認知しない間にプログラムを埋め込まれ, spam メール送信や DDoS 送信の手先となってしまう PC が大量に発生している.

このような PC をゾンビ PC, bot などと呼び, その PC 群をゾンビクラスター, botnet と呼ぶが, 昨今, この PC 群から spam メールを送る手法が増えており, 海外では一般的になりつつある.

このようなサーバは, 持ち主にはまったく悪意がないにもかかわらず, spam メールを送信していることがほとんどであり, ISP のカスタマーサポートからの電話で初めて気付くお客様も多い.

PC が bot 化してしまうと発見が困難な場合が多く, ISP としても, お客様に悪意がないために, 事実の指摘や PC の修復などについて, 非常に神経を使う問題となっている.

PC をきちんと管理する技量のないユーザが, セキュリティの意識なしに安易に公開を行っている現実については, ISP としても, その危険性についてさらに啓蒙していく必要を感じている.

【カスタマーサポートにおける対応】

spam メールを受信したユーザが苦情を申告する場合, 一般的に自分が契約している ISP のカスタマーサポート（以下, CS）へ電話やメールをする場合が多い.

この場合, ユーザから入手したメールのヘッダ情報により, spam メールの送信者が自社のユーザであると特定できた場合は, 規約に照らして違反を確認後, 当該ユーザに対し送信行為を中止するよう警告を行う.

何度かの警告に無反応であれば一時的にメールを送信

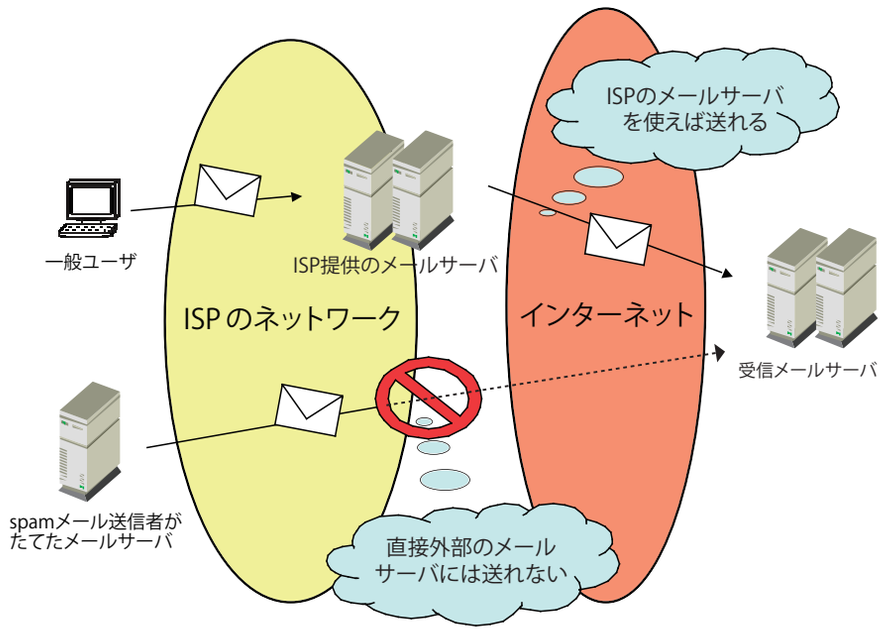

図-2 Outbound Port 25 Blocking

できない状態にし，当該ユーザからの申告を待つ．このような場合，spamメール送信者からの申告はほぼ皆無であり，そのまま規定の期日を過ぎて退会となるケースが多い．

一方，spamメール送信者が他社ISPのユーザの場合は，当該ISPと連絡を取り，対応をお願いする．そのため，メールヘッダ情報が改竄されていると，連絡を取るためのISPを特定できず，spamメール送信者を追いつめる手段がなくなってしまう．

公開のリレーサーバ，前述のbotnetなど，spamメール送信者にとって都合の良い環境がまだまだ多く，ISPとして，その撲滅を切に願うものである．

なお，spamメール送信者本人に関する情報をISP間で共有することは法的に難しいため，現状では，ある特定のspamメールの送信という一事象について各ISPで作業を分担している状況であり，spamメール送信者本人に対する有効な手立てがない状況である．

【Outbound Port 25 Blocking[3)]】

アメリカのある大手ISPは，自社が動的に振り出しているIPアドレス（以下，動的IPアドレス）のレンジを開示し，他ISPについても同じような対応を求めている．

これは，動的IPアドレスから送信されるspamメールが，spamメールの大多数を占めていることから，動的IPアドレスを発信元とするメールを特定するために行っている施策と考えられる．

先般，動的IPアドレスから送信されるメールについて，必ず自社サーバに向けて送信するようにし，他社のメールサーバに対して直接メール送信ができないようにする「Outbound Port 25 Blocking」（以下，OP25B）という手法をとるプロバイダが，特にアメリカで多くなり，日本においても採用するISP[4), 5)]が出てきている．

OP25Bを適用した際の状況は図-2のようになる．ISPのメールサーバを使ってメールを送信することは問題ないが，ISPのメールサーバを使わずに，ユーザが受信メールサーバに対して直接メールを送ることを制限する方法である．

OP25Bは，効果が期待できる反面，導入時に副作用が大きいことが分かっている（表-2）．

特に，（ISP側ではなく）ユーザ側に対して影響が大きいため，OP25B採用にあたっては，自社のユーザに対するサポートが必須になる．そのため，現時点において，先行したISPの状況を見ながら，少しずつ導入が進むものと思われる．

一方，携帯事業者向けに限ったOP25B[4)]は，spamメールのトラフィックによって正常なメールのトラフィックが阻害されている状況がなくなり，携帯宛てメールの遅延解消，および．遅延により寄せられる苦情の減少などISP側にもメリットがあるため，比較的導入しやすいと考えられる．

【送信ドメイン認証】

アメリカにおいて，大手ISPやホスティング業者が送

メリット	デメリット
• 自社 ISP 網から発信される spam メールを劇的に減少させることができる • 自社サーバを使って送られる spam メールを自社でコントロールできるようになるため，適正なメール流量を扱うことが可能になる • カスタマーサポートへの苦情がかなり減る	• 会社のメールサーバが使用できなくなる可能性がある • 他社の ASP 利用者が，ASP のメールサーバを使用できなくなる可能性がある • DynamicDNS などを使用し，動的 IP 上でメールサーバをたてることがやりにくくなってしまう可能性がある

表 -2　OP25B 導入によるメリット，デメリット

信ドメイン認証技術を積極的に導入してきているが，日本においても導入する旨を宣言する ISP が少しずつ増えてきている．

現時点において，ドメイン認証に違反したメールを拒否するかたちの運用はすぐにはなされないと思われるが，徐々に，なんらかのペナルティを課した後，受信する状況になっていくと考えられる．

そのため，各 ISP/ASP/ 企業などが，その対応を迫られつつある状況にあると考える．

■ spam メール対策における課題

各 ISP は spam メールに対するいろいろな施策・サービスを行っており，少しずつ成果があがってきている．

しかし，いまだに spam メールがなくならない原因として，特に問題であると考える事柄について述べる．

【ISP 渡り歩き問題】

NTT が提供しているフレッツ網は，その特性から，ADSL/FTTH の現行設備をそのままにして契約 ISP を変更することができる．

そのため，spam メール送信を理由として，ある ISP からメール送信ができなくなると，すぐに別の ISP と契約をすることで，高速な回線を維持したまま，spam メールを送ることができてしまう．

現状，ISP 側ではユーザのフレッツ網の情報までは入手できないため，入会を希望してきたユーザが，spam メールを送信する可能性の高い人かどうかの判別がつかない．

spam メールを送信されて初めて，そのユーザの対処を行うが，その時点ではすでに相当数の spam メールを送信された後になってしまう（俗に言う「打ち逃げ」をされてしまう）．

この問題については，現時点でもいろいろな議論があり，すぐに対処できない状況である．

【リンク先 Web サイトの問題】

spam メールは送られてきたメールで完結することはほとんどなく，関係する Web サイトへのリンクが必ず存在している．spam メールの送信は，この Web サイトへの誘導が目的であると言っても過言ではない．

逆にこのような Web サイトを作らせない，もしくは，すぐに閉鎖させられるようになれば，spam メールそのものを減らすことが期待できる．

しかし，「ユーザからの申告を拠り所として当該 Web サイトを閉鎖する」ことの是非については，法的な問題を含め微妙な判断が絡んでくるため，一般的には ISP にとって非常に難しい問題となっている．

また，spam 送信に加担している Web サイト（spam 送信のアルバイト募集や spam 送信ソフトの販売など）についても，正当な商行為との線引きが微妙なため，法的な見解が定まらない現状においては，問題であると感じつつも放置せざるを得ず，ISP を悩ませている．

■ これからの対策

spam メールは，誘導先の Web を見て行動（購入，通知など）を起こす人間がいることで，その存在意義が成り立っているものである．

逆に，ユーザがこのような行動をしなくなれば，必然的になくなっていくものである．

したがって，前述した技術的な対策はもちろんであるが，ユーザへの啓蒙活動も非常に重要な課題であると考えている．

spam メール対策を，ISP やベンダまかせにせず，自らの問題として考え，実践するユーザが増えることを切に願うものである．

参考文献
1）Gartner：メールトラフィックの 60% 以上は spam，http://www4.gartner.com/5_about/press_releases/pr29sept2003a.jsp
2）POPFile：http://popfile.sourceforge.net/
3）Outbound Port 25 Blocking：http://arena.nikkeibp.co.jp/qa/internet/20050329/111837/
4）ぷ ら ら：http://www.plala.or.jp/access/living/releases/nr05_jan/0050127.html
5）WAKWAK：http://www.wakwak.com/info/spec/port25/index.html

（平成 17 年 6 月 16 日受付）