COLUMN

インターネット生活向上委員会

07 メールサービスの利用

冨米野 孝徳（㈱ インターネットイニシアティブ）
taka@iij.ad.jp

◉はじめに◉

AntiAbuseという言葉をご存じだろうか？　主にスパム・メール，ウィルス付メール，ワーム付メールなど受信者にとって好ましくないメールなどに対する言葉だと思っていただければよいと思う．この連載の最初にはスパム・メールの対応の仕方について自主的に対応する方法を紹介したが，今回はスパム・メールだけでなくAntiAbuse全体を含めて，メールを安心して使えるようにするために，どのようにISPのサービスや自主対策を組み合わせていったらよいかを考えてみたい．

メールに関してウィルス，ワーム，スパムというような迷惑なメールの対策が最近重要になってきている．その背景としてはメール自身がビジネスツールとして利用されてきており，より安定し安全に利用できなければならないものとして位置づけられてきているからだと思われる．

参考としてスパム・メールの事例ではあるが米国における損失に関する調査結果の一部を紹介する．

［2005年］

Q1(1月～3月）に全世界に発信されるメールは2002年の149億通から350億通に増加，そのうち80%のメールがスパムメールと予測．

- 2003年に米国企業がスパム・メールに起因して損失した金額は2002年の89億ドルから100億ドルに増加．
- そのうちの40%がスパム・メールを受信したことによる従業員の生産性の低下に起因している．
- スパム・メールの識別／消去に費やす時間は：4.5秒／メール．
- 1メールボックスあたりにかかるスパム・メールに対する年間コスト：168ドル/2003年，257ドル/2007年．

といった結果が出ている．日本国内でも過去に携帯電話のメールアドレスにスパム・メールが大量に送られるため携帯電話の料金が高くなる，といった問題があり受信したメールをある一定量，無料にするというスパム・メール対策がなされた．これは料金的な面では対応したかたちになっているが，スパム・メールを対策した，という意味では不完全といえるかもしれない．上述のスパム・メールに関する報告を鵜呑みにはできないにしても，単に迷惑なメールというだけでなく損失として考えてもよい状況になってきている．

◉Anti-Virus◉

ウィルス／ワーム付メールの対策である．昨今，ほとんどのISPがウィルススキャン（ワームも含む）と呼ばれる機能を何らかのかたちで提供している．スパム・メールより被害が明確かつ大きいためすでにサービスとして提供されているであろう．

メールアカウントと一緒になっているのは個人向けにも利用されているが，DION（KDDI）ではこのようなサービスが提供されている．

http://www.dion.ne.jp/service/mail/virus/

また企業をターゲットにした場合，メールサーバ自身は企業内に置かれるケースがあるため，スキャンのみを提供するゲートウェイ的サービスが提供されている．OCN（NTT Communications）からはこのようなサービスが提供されている．

http://www.ocn.ne.jp/business/security/viruscheck-gw/?b

企業ユーザであれば，このようなサービスを何らかのかたちで利用しているケースが少なくないのではないかと思う．

◉Anti-SPAM◉

スパム・メールについてはウィルス／ワームより被害が明確でないため，サービス化という点においては若干遅れているように思う．実際，スパム・メールの対処方法としてはどのようなものがあるのか，少し詳しく見てみよう．

(1) ドメインレベルブラックリスト／ホワイトリストを利用する方法

スパム・メール送信者のメールアドレスを組織単位，ドメインレベルなどでブラックリストに追加，信頼できるメールアドレスをホワイトリストに追加する方法である．この手法は効果的なのであるが，ブラックリスト，ホワイトリストの作成に人手も時間もかかってしまう．またスパム・メール送信者は数百から数千の送信アドレスを利用したり，送信アドレスを偽るケースもあり安易にブラックリストに登録できない状況も存在する．

(2) 配付されているブラックリストを利用する方法

インターネットで配付されているブラックリストを利用する方法である．インターネット上でいくつかの組織

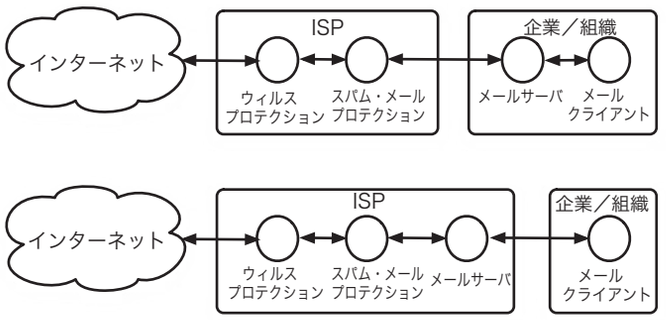

図-1　ISPによるサービス提供概要

がスパム・メールの送信アドレス，ドメイン名を収集しており，それを利用して駆除する方法である．具体的にはMAPS（Mail Abuse Prevention System，http://www.mail-abuse.com）がリストを公開している．

(3) ヒューリスティックエンジン（発見的エンジン）

この方法はメールごとにあるスコアを算出し，それを元に駆除する方法である．分かりやすく説明すると，"Get Rich"，"Free Viagra"などのスパム・メールに含まれる言葉をカウントして，メールごとにどのくらい入っているのかを計算して判断する方法である．カウントする方法として検出した単語，連語などにスパム・メールに含まれる可能性などを元にポイントをつけておりそれを元にスコアを計算する．

(4) 統計的手法

この方法は最近利用されいてるスパム・メールフィルタの手法である．連載の最初でご紹介したベイジアンフィルタがそれである．ヒューリスティックエンジンと似ている手法ではあるが，違いはスコアではなく単語，連語などの現出頻度をベースに検出している点である．

(5) DCC（Distributed Checksum Cleaninghouse）

この手法はウィルスチェックなどで利用されている手法である．メールのチェックサムやフィンガープリント（指紋）にあたるものを検出し，事前に持っているデータと比較して判断する方法である．

(6) Honey Pots

これはあらかじめスパム・メールを受けそうなメールアドレスを公開しておき，受信したスパム・メールをデータベースに記録しておき，判断する手法である．この手法は一度は受信しなければいけない上，送信者を偽られた場合有効ではない場合がある．

(7) Authenticated Mail

これはメールが実際の人から送られてきたかどうかを確認する，といった手法である．一般的な確認方法としてはメールを受信した際，送信者に簡単な質問メールを自動的に送り返すのである．質問の内容としては人間が見て答えられる質問であり，その質問にちゃんと答えられた場合のみ受信者に送信される，といった仕組みである．質問に対する答えがない場合，メールが配送されない，ということも起こり得る．

現在，このような手法が利用されている．これらの手法のうち，どの手法が一番良いのであろう？　いろんなケースのスパム・メールが存在するのでどれか1つの方法で十分ということはなく，実際は複数の手法を組み合わせるようなかたちになっている．組み合わせた場合でも100%スパム・メールの排除を保証できるわけではなく，現実的には限りなく100%を目指す，というアプローチになる．

具体的には外部，インターネットとの間にスパム・メールを駆除するためのメールリレーを入れて，そこでフィルタするやり方である（実際のISPはウィルスメールの駆除も含むかたちが多い）．

◉ISPによるサービス提供概要◉

メールアカウント自体をアウトソースしている場合とそうでない場合とで分かれるが，ISPのサービスを利用する場合，一般的にはこのような形態で利用する．ISPの提供するサービスとしては，迷惑なメールを排除するだけではなく，排除したメールの処理についてもただ単に消せばよい，といった処理だけでは誤ってスパム・メールと判断された必要なメールまで消してしまう可能性もあり，処理方法についても，いろいろと考慮されなければならない．

◉最後に◉

ウィルス対策，スパム・メール対策などがISPのサービスとして提供されるようになってきている．ウィルス対策については，ウィルスの感染経路がメール以外に組織内のファイルサーバ上のファイルを経由して広まったり，自宅に持ち帰ったPC経由で感染したり，最終的にPC本体にウィルス対策ソフトを入れなければならないことがあり，あまり効果的ではないのでは？という声もある．その一方で完璧ではないにしてもある程度ウィルス／ワームを駆除してくれるだけでも助かる，という声もある．それだけメールを通しての感染が起こっている，ということではあるのだが，サービスの利用という点については悩ましい話である．

スパム・メールはどうだろうか？　迷惑なメールなのだが，日に100通送られてくるものが，数通レベルにまでなればそれなりに効果的ではないだろうか．またスパム･メールは，迷惑なことこの上ないのだが，メールから直接感染して他人に迷惑をかける，ということは起こらず100%排除できなくてもウィルス／ワーム付メールのような被害がでることはない（もちろん，メールの中身に何か書いてあり，それにひっかかり被害を被る，というのもあるのだが..）．それぞれの人の考え方，というのもあるとは思うが，ある程度の規模の組織はISPのサービスを利用して，一定レベルの品質をしっかりと保つという方針がよいのではないかと思う．

（平成16年9月6日受付）