基調講演

# スパムの現状と対策

安東孝二
東京大学情報基盤センター
ando@itc.u-tokyo.ac.jp

概要：スパムという言葉に代表される、いわゆる迷惑メールは日本でも看過することは出来なくなっている。日本におけるスパムの状況の解説と、スパム対策の選択肢について述べる。

キーワード：スパム、迷惑メール対策、Junk Mail, Bulk Mail, UCE, UBE

## 1. スパムとは

スパムの語源に関する Monty Python の話はどこかで耳にされたことがあると思いますので省略します。日本では迷惑メールという表現が定着しつつありますが、Junk Mail, Bulk Mail なんていう呼び名も英語圏ではよく使われます。今までは日本語でスパムといえば缶詰以外ならスパムメールだったのですが、最近はメールとは違う分野にも使われ始めています。ブログの世界でスパムといえば、コメントスパムやトラックバックスパムです。そのほか検索エンジンスパム（SEO/SEM スパム）という言葉も出てきています。もちろん、メールに関して使われることが多い「スパム」ですが、一般に、受信者の意図を無視して送りつけられる大量の情報について使われる言葉になりました。いずれにせよ缶詰とは大違いで嫌われ者です。ここでは従来のスパムメールについて考えてみます。

## 2. スパムあれこれ

### 2.1 スパムが送られてくる技術的理由とその背景

スパムが大量に送られるのには技術的にも理由があります。電子メールはインターネットでも古くて重要なサービスの一つですが、かつての電子メールの世界は、現在のようにほぼ全てのメールサーバが TCP/IP で接続された均一なものではありませんでした。インターネットの中でも常時接続ではなく polling してメールを配送しているところも多かったですし、TCP/IP でなく UUCP で接続されているところもありました。接続状況が多彩な上に、そもそも BITNET など全く異なった世界のメールとの接続もありました。

また、インターネットが拡大するにつれ、メールサーバの数と種類・バージョンも加速度的に増加しました。インターネットはまずつながることで大きくなってきました。メールは最もインターネットらしいサービスの一つといえます。キーワードは性善説に基づいた相互接続性（Interoperability）です。相手のサーバの振る舞いがちょっとおかしくても、メールサーバは頑張ってメールを受け取ることが望まれます。非常に寛容な運用が求められてきたのです。

電子メールの決まりはいくつかありますが、送受信に関して重要な決まりが記述されているのが RFC2822 です。この RFC は 2001 年 4 月 24 日に発効したものですが、それまでは 1982 年 8 月 13 日に出た RFC822 が基準となっていました。言い方を変えると 19 年間放置されていた訳です。電子メールは何時でも何処へでも誰とでもやりとりが出来ます。ここは郵便や電話と同じです。一方、電子メールは分散したプライベートなシステムです。ここは郵便や電話と違っているところです。このインターネットらしい分散システムが古き良き時代の性善説の前提に立っていたため、「穴がいっぱいのお人好しの規格」であったことは否めません。

### 2.2 スパムの現状

スパムが劇的に増えてきた背景にはいくつかの理由があります。昨今のスパムの状況を振り返ってみましょう。

まず、スパムを分類すると悪戯を目的としたスパムがあります。ウイルスメールやチェーンメールが挙げられます。ウイルスメールはコンピュータウイルスの伝染経路としてメールを利用することから増加していますが、既知のウイルスメールは、技術的には比較的簡単に阻止できます。チェーンメールは電子

メールという媒体でなくとも流行していたものですが、特に若者の間で流行する傾向があります。日本データ通信協会では、チェーンメール対策専用のアドレスを用意してチェーンメールを停止するサービスを行っています。幸いなことにデマやチェーンメールは我々の電子メールのシステムを脅かすほど大量にはなっていません。

スパムのうちの大半を占めるのは、お金儲けに関連したものです。最も簡単なのはダイレクトな広告メールですが、近頃は詐欺的な要素を含んだ広告メールからフィッシングを目的としたメールまで多岐にわたります。ここでは詳しく触れませんが、ターゲットを絞って、つまり特定の個人を想定してフィッシングを行う例も出てきているようです。数打ちゃ当たる方式の大量のフィッシングメール送信でなく、このようなフィッシングメールを防ぐことは困難なので今後問題になるかもしれません。

収益を上げるビジネスモデルが確立してきたため、スパムを送信する側には強いモーティベーションが働きます。いくつかのレポートによると、既に世界のメールの 60 %以上がスパムだそうです。米国や韓国などのスパムに関して悪名高いいくつかの国では 80 %を超えており、スパムのために電子メールというメディア自体の存続が危ぶまれています。

また、スパムの送信方法も様変わりしてきています。従来はサードパーティーリレーと呼ばれる方法で多く送信されてきました。設定が不十分な他人のサーバを探し出し勝手に使う方法です。性善説で全てがうまくいった頃のインターネットでは他人のサーバを使ってメールを送ることも許容されていましたが、さすがにスパム業者に使われるのはまずいということで、このサードパーティーリレーに対する防御は進んできています。このため、スパム業者は自らのサーバから直接スパムを送信するようになりました。ブロードバンド化とサーバの高性能化により、インターネットにつながった自分のサーバから直接大量のメールを送信することが可能になったのです。ただ、接続業者（ISP）に嫌われて接続が禁止されることも多く、イタチごっこの状態が続いています。オンライン・サインアップなどで接続業者と契約し、大量のスパムを送りつけた後、直ぐに解約し、次の異なった接続業者へ渡り歩く「渡り」という手口が日本でも多く見られるようになっています。この手口への対策として、接続業者はＯＰ２５Ｂ（Outbound Port 25 Blocking）を推進しています。

この「渡り」による直接送信の他に、「ボット」によるスパム送信が台頭しています。テクニカルには非常に洗練されたやり方です。ウイルスもしくはスパイウェアに感染したPC、もしくは直接の攻撃によって侵入に成功したマシンを大量に自分のコントロール下に置き、グリッド技術を用いてインターネット上に巨大で仮想的なスパム送信マシンを作ってしまいます。これをボットネットと言います。このボットネットを駆使してスパムを送るやり方がどんどん増えてきています。スパム送信者も新しい技術を使ってきていることが分かります。

### 2.2　スパムビジネスの確立

「渡り」によるスパム送信はテクニカルにはあまり洗練されていない地道な方法で行われる一方で、ボットネットからの送信は、その規模にしても比較にならないほどです。オランダで発覚した事件の捜査では、犯人は 150 万台のボットを操作していた疑いがもたれています。

スパム送信に新しいビジネスモデルが形成されていると David H. Crocker 氏は言っています。彼は 1982 年に RFC822 を書いた人です。今のスパム送信は分業制です。メールアドレスを集める業者、ウイルスや侵入を通じてボットネットの候補になるマシンを探す業者、ボットネットを作りレンタルする業者、そして実際にスパムを送る業者。様々な人間が関わっているため全体像をつかむのがより難しくなります。おそらくこれも彼らのねらいでしょう。また、聞いたところによると 2005 年くらいから日本のスパム送信業者も世界のボットネットを用いる業者と接触を始めたと言われています。ボットネットは 1 時間 300 ドルくらいでレンタルできるとも言われています。

このようにスパムビジネスが確立してしまうと、経済的な理由で高度な技術者がスパム送信者に加担してしまうことも考えられます。困ったことですが、スパム送信者はだんだん

高度なテクニックを使い始めているようです。Telecom ISAC Japan によると、ウイルス対策を行っていない PC をインターネットに繋ぐと 4 分でウイルスに感染するそうです。また、日本国内の PC の 40 から 50 台に 1 台がボットになってしまっているそうです。

## 3. スパム対策

スパム対策には立場によっていくつかのアプローチが考えられます。

まず、世の中からスパムというものをなくすための方策があります。これは電子メールの世界を変えてしまうことにつながるので容易ではありません。Cisco や Yahoo が中心となって、現在、DKIM（DomainKeys Identified Mail）という規格を標準化しようとしています。これは偽造送信者アドレスを使えないようにしようというアプローチです。

二番目にスパムを送りにくくしようとする方策があります。いくつかあるのですが、有名かつ実効性があるものとして OP25B（Outbound Port 25 Blocking）が挙げられます。これは接続業者が、顧客が勝手に外部ネットワークへのメール送信をしないようにするために行われるものです。「渡り」のスパム送信を防止するための措置です。日本でも大手の接続業者が導入を始めていますが、善良なモバイルユーザが StartTLS を使えなくなるなどの副作用もあります。ユーザは接続業者が提供するメールサーバを使うか、サブミッションポートを使う必要があります。US では多くの接続業者が OP25B をしています。

三番目にスパムを受け取らなくする方策があります。Throttling, Filtering, Blocking の三つに分けて説明します。

Throttling は、特に大規模なサーバでメリットがある方策です。スパムを大量に送りつけてくるサーバからの通信自体を制限することで、サーバリソースの枯渇を防ぐと同時に、送信にかかる時間を待ちきれないスパム送信サーバが接続を切ってくれるのを待ちます。SMTP サーバの接続時の振る舞いやメールトラフィックから接続の制限をする方法もありますが、簡単にできるのは Sendmail にも実装されている Greet Pause だと思います。うまく設定することで大きな効果を上げている大分大学などの例があります。（http://www.cc.saga-u.ac.jp/ipc2005/jacn9/ipc04.pdf）

Filtering はサーバでもクライアントでも利用できる方策です。キーワードによるパターンマッチングなど単純なものから、ベイジアンフィルターを用いた複雑なものなど様々です。フリーの MUA である Thunderbird などにも実装されており利用は簡単ですが、スパム判定の間違いがゼロではないので悩ましいところです。また、スパム送信者もベイジアンフィルターを意識してメールを送り始めていますので、効果は万能ではありません。しかし、実際によく使われ、効果もある程度期待できます。

Blocking は主にサーバで利用される方策です。理想論をいうと、スパムメールは受け取ったら負け！なので、最も正しい方策です。サードパーティーリレーを防ぐために ORBL などの外部 DB を参照してメールをブロックする方法は有名ですが、そのほか有望な方法が Gray Listing と Reputation サービスによるブロックです。Gray Listing とは White List/Black List によるメールの仕分けを機械的に行おうという試みです。日本語では一見さんお断り方式などと言われているのを聞いたことがあります。最初の送信は必ずお断りして、きちんと再送されてきた二回目以降はちゃんと受け取ろうという方式です。スパム送信者はエラーを理解するプログラムなど利用していないし、再送処理もしないので多くのスパムをこれで防ぐことが出来ます。副作用として、世の中に意外に多いきちんと再送しないサーバからのメールが受け取れません。また、再送するたびに異なる MTA から送信されるなど、再送されたことが認識しづらいメールが届かなくなってしまいます。White List/Black List との併用が望ましい方法ですが、スパムメールを劇的に排除することが出来る方法です。

Reputation によるスパムの排除は非常に効果的です。多くのアンチスパム業者が様々な方法でスパム情報（発信源からその内容まで）を瞬時に解析してデータベースに保持しています。これを使ってスパム情報を排除する訳です。メールサーバ管理者が悩む必要がないので今後有望な方策です。Mirapoint 社が提供する Rapid Anti Spam 機能では、データベースへの問い合わせにも Comtouch 社が開発し

たRPD（Recurrent Pattern Detection）という技術を利用し特徴を持たせるなど、Reputationサービスも多様化を見せています。今後が楽しみです。

## 3. まとめ

スパム、ウイルスを含め電子メールに関わるコストは増大しています。フリーソフトでのスパム対策も限界に近づきつつありますが、まずはこつこつと出来る範囲でのスパム対策で経験を積んで、来たるべき日に備えておく必要があります。スパム送信者に負けないだけの勉強が必要です。