1 世界の電子メールを spam 制御へ

Brandenburg InternetWorking
David Crocker dcrocker@bbiw.net
東京大学
翻訳：安東 孝二 chutzpah@ecc.u-tokyo.ac.jp

インターネットが教えてくれたことの 1 つに“スケーリング”についての教訓がある．インターネットにはおそらく十億人のユーザと数百万台のマシンと数万から数十万人のサービスオペレータがいて，世界中のあらゆる国で，あるいは国と国の間で仮想的に動いている．インターネットは，個人のためにも，組織のためにも，政府のためにも利用される．それゆえに，それぞれ文化や，意思伝達の様式，統治の方法が異なっても齟齬をきたしてはならない．インターネットを統治する中心はどこにもないし，運用上なにか決められた予定があるわけでもない．インターネットは一度変更すべき点が皆で合意されたら，緩やかに自発的に変わっていかないといけないのである．

1990 年代初めにインターネットは小さな研究上のコミュニティから世界的な巨大マーケットへ変貌した．まるで小さな町が大都市に変わってしまったかのようだ．大都市では大抵の場合よその地域から来た人が多く，価値観や行動様式はそれぞればらばらである．なので，そこの住民は以前よりお互いを警戒して暮らさないといけない．元々の町の運営は問題ではない．必要なものの変化が問題なのである．

誰でも spam は問題だと思っている．おそらく spam の説明には“unsolicited bulk email”（UBE：望まない大量のメール）[16] が最もよく使われる言葉だろうが，皆が納得する定義を見つけるのは難しい．spam の多くはインターネットにおける技術標準を守っている．彼らが守っていないのは我々の社会における取り決めである．そのため，spam に対する技術的対抗策は，社会の spam に対する姿勢をリードするどころか後追いしているのである．

spam 以外の社会問題と同じように，もし仮に spam を根絶できないとしても，制御することはおそらく可能である．spam は我々の社会風景の一部になってしまった．局所的に有効な対策技術はあるが，それらはほんの一時的なものである．このことは，我々が新しい spam 対策の提案に期待する際には慎重にならないといけないことを意味している．spam を制御するには互いに補完しあう一連の技術が必要だし，spammer（spam メールの発信者）は独自の手法を工夫し続けるのだから，それに対応する絶え間ない努力も必要になるだろう．世界的な社会基盤に変更を加えるには長い時間と多くのコストがかかるものだ．いくつかの提案は，運用中での実質的な管理作業を必要とし，また，いくつかの提案は複雑なテクノロジーを必要とする．それゆえに，我々が装備する spam 対策の仕組みには相当長い期間，恩恵を得られることを保証しないといけない．また，開発コストも妥当でないといけないし，必要とする運用中での管理作業も限定的でないといけないし，十分に使いやすくないといけない．うまくいきそうな簡単な方法は，たとえ仮に spam が問題視されなかったとしても，人々に望まれるような仕組みを探すことである．この仕組みが見つかれば，我々はコアとなる戦略的にも重要な利益を得られるのだ．

インターネットは我々すべてによりよいアクセスを提供する．コラボレーションにも，専門のコミュニティを作り上げるにも，個人的なやりとりをするにしても，インターネットはすばらしいものだ．一方，プライバシーの侵害やオンラインセキュリティの脅威の点では問題を抱えている．不幸なことにこれらの利害は表裏一体である．だからこそ，spam を制御しようとする取り組みは，今までの利益を損なわないように慎重に行う必要がある．悪くても，我々の取り組みは，まだ見ぬ「将来の」革新的な利益に対する悪い影響を抑えなければならない．

spam の送信者がメッセージ 1 通を余計に送る際に増分するコストはほとんどない．すべてのメッセージに直接課金することによって電子メールを単に郵便や電話のようにしてしまおうと考えるのは簡単なことだ．この課

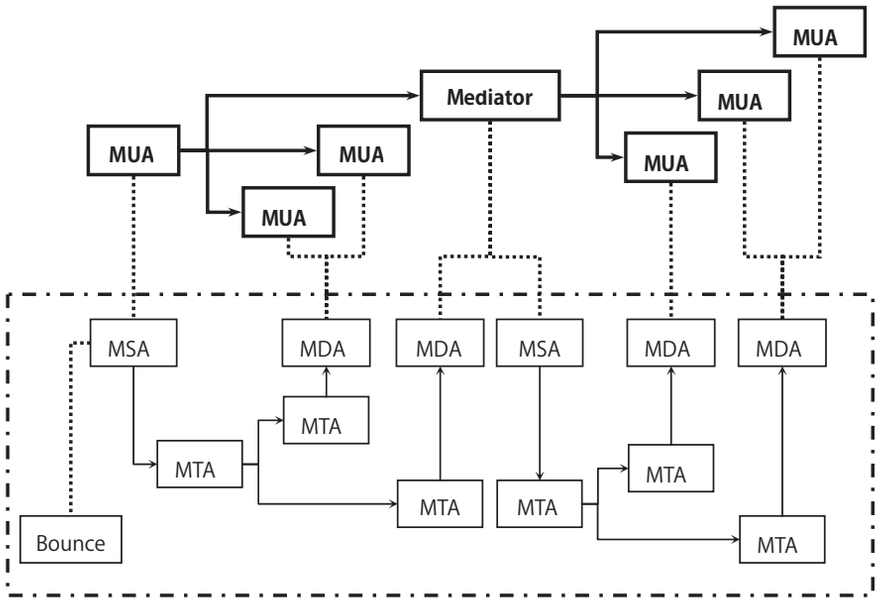

図-1　現在の電子メールの仕組み

金によって不正な利用や大量の利用に対する障壁を作ることができる．しかし実際には，電子メールは郵便や電話とは別種のサービスであり，それ自身も長い歴史があり，これらとは異なった方法を選択することもあり得る．電話や郵便は高度に中央集権化された公的な現業機関を持ち，利用に際しての課金で直接実際の支出をまかなっている．対照的に，電子メールは公的機関による介在は必要なく，利用者の私的なシステムが互いにやりとりをする，高度に分散化されたサービスである．もし，余分に課金するならば，そのお金もまた実際のサービスに使わないといけない．恣意的な“税金”はそれ自身が単に問題を生み出すだけである．

■ 電子メールのアーキテクチャ

インターネットの電子メールサービスのコアは簡単なモデルだ．このモデルではユーザの世界は伝送の世界から分けられている．ユーザは Mail User Agents（MUA）に対応する．伝送とは，複数の Mail Transfer Agents（MTA）が構成する Mail Handling Service（MHS）である．MHS は Simple Message Transfer Protocol（SMTP）[8), 10)] を使って，発信者から受信者まで電子メールを送る．誰でも誰へでもメッセージを送ることができる．基本的なサービスには誰の認証も必要ない（これが電話や郵便と同じであることは注目に値する）．ユーザにとって自分の電子メールクライアント，つまり MUA こそが直接感じとれる電子メールのすべてである．ネットワーク管理者にとっては，MHS のソフトウェアが主な関心事である．

電子メールのメッセージオブジェクトのコアも単純である．ヘッダと呼ばれる構造化されたテキストで書かれたメタインフォメーションで始まり，ボディとよばれる自由な形式の ASCII テキストが続く．ヘッダはアドレスや送信日時，ユニークなメッセージ ID と短い内容の説明が含まれる [9), 11)]．

図-1 に示すように，現在のアーキテクチャは見て分かるようにずっと手が込んでいる．さらに機能を分けて厳密に役割を割り当て，任意の言語で表現された複合的なマルチメディアコンテンツを送ることが可能になっている [1)]．

これらの設計上あるいは規格上の拡張により以下のものが当初のモデルより分離・独立した．

- Message Submission Agent（MSA）を経由した電子メールの送信 [14)]
- Message Delivery Agent（MDA）を経由した電子メールの配送．これによりユーザ特有の配送の振る舞いも可能 [5), 7)]
- メーリングリスト（Mediator）のようなユーザレベルの再送 [12)]

種類	指定場所	意味
MTA の IP アドレス	IP ネットワーク	SMTP クライアント
EHLO ドメイン名	SMTP コマンド	SMTP クライアント
プロバイダの IP アドレス	IP ネットワーク	SMTP クライアントのサイト
Mail-From メールアドレス	SMTP コマンド	バウンスアドレス
From メールアドレス	RFC2822 メッセージヘッダ	作者
Sender メールアドレス	RFC2822 メッセージヘッダ	投函エージェント
Received ドメイン名	RFC2822 メッセージヘッダ	中継 MTA サイト

表 -1　電子メールに関連する各種アドレス

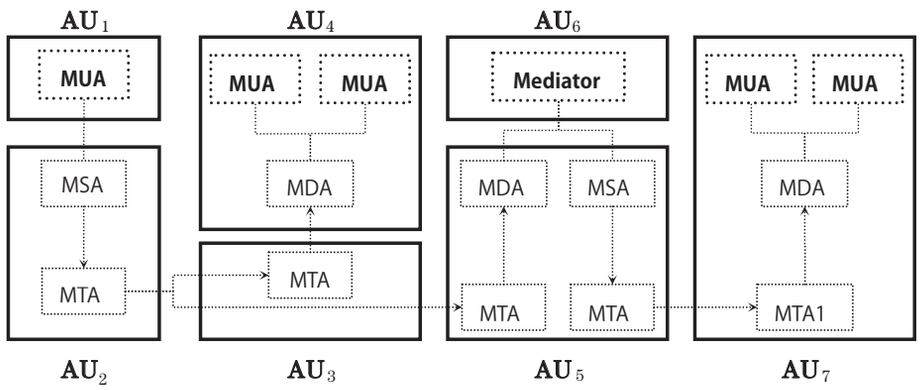

図 -2　AU の例

- 送信が失敗した際の通知（Bounce）など，伝送に関するレポートを扱うエージェントの分離 [3)]
- 階層構造を持ったコンテンツの添付（MIME），代替文字セットによるコンテンツも利用可能 [6)]

spam を制御することで説明責任の問題が浮上する．誰が責任のあるエージェントなのか？　あいにく，spam の生成や伝送には表 -1 のように多くの個人がかかわっている．

SMTP クライアントは前ホップの事業者のエージェントである．電子メール事業者は IP ネットワークの事業者とは違ってもよいので，ここでまた異なる個人が出てくることになりかねない．このことで，表 -1 の興味深い点が浮き彫りにされる．表のエントリーのほとんどが“Sender”と呼べるため，結果として“Sender”は spam 対策の議論ではほとんど意味がなくなってしまっているのである．

インターネットの電子メールでは，独立した運用主体の間で運用上の境界線を明らかにしておくことが求められる．この管理単位（Administrative Units，AU）は信頼できる境界を規定するものだ．図 -2 に示すようにこれらには技術上あるいは運用上の面でいろいろ異なる種類があることが文献 15）で議論されている．

インターネットへのさらに多様化する接続は，我々が“abuse”と呼んでいる行動がずっと増えていることを意味している．これは，AU 間の信頼の本質と，その信頼を強化する方法を変えないといけないことを明らかにしている．

spam 送信のアーキテクチャ

残念なことだが spam 送信の世界でもスケーラビリティのある高度な開発が進んでいる．かつての spam 送信では 1 人の送信者が 1 つのマシンを使っていた．そのパフォーマンスはマシンの能力とインターネット接続のバンド幅により限界があった．しかし，今や spammer は図 -3 にあるように“ゾンビ”と呼ばれる不正侵入されたシステムで構成された巨大な軍隊を統制し

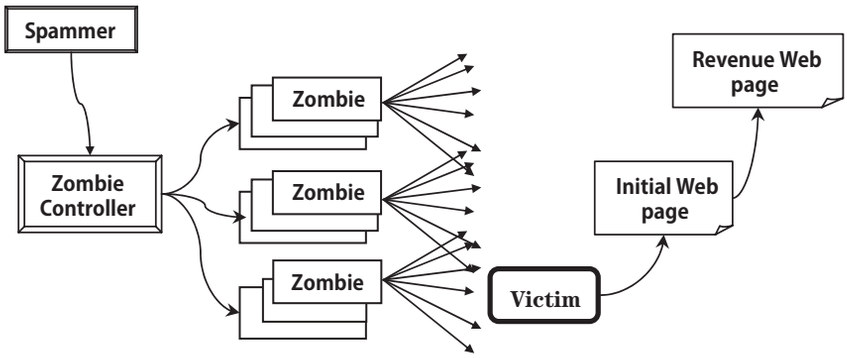

図-3　現在の spam の仕組み

ている．

spammer のコミュニティは異常なほど高度に組織化されており，すでに巨大な地下経済を形成している．コミュニティには spam がフィルタを通り抜ける方法を開発している者もいれば，マシンを乗っ取りゾンビにしてしまう者もいるし，そのマシンの利用権を spam 送信の期間だけ切り売りする者もいる．ゾンビシステムの数は数千万台にのぼると見られている．spam の受信者はしばしばリンクをクリックして取引用の Web ページに辿り着く．この Web ホスティングは，サーバ側の処理を分かりにくくして責任を回避するために，多重構造になっている．

何人かの spammer は形式上では制限できないという理由で現在のところ合法的なビジネスに精を出している．将来，法律と契約の両方に基づく法的な制限で彼らを押さえ込むことはできるだろう．対照的に，責任を逃れようとしたり，spam 通信に対する障害を突破しようとしたり，他人の所有するマシンを知らないうちに意に反して利用しようとしたりする spammer もいる．後者のグループを分析するために使うべき最もよい社会モデルが犯罪のモデルである．彼らの活動は特定の法律には違反しないこともしばしばあるが，最も大事なのは spammer の行動が犯罪者の行動と同じであるということだ．

概して spammer は商品を売るという典型的な目標を持っているが，spammer は同時に政治的もしくは宗教的な動機を持つこともある．場合によっては恐喝などの露骨な犯罪行為を意図していることさえある．きわめて大量のメッセージを送る能力を持った spammer は DoS（denial of service）攻撃でターゲットのネットワークをトラフィックで溢れさせる脅威を与えることができるのだ．

これまでの，spammer および spam 送信をコントロールするための取り組みは世界中の spam の数を減らすまでには至っていない．よくても局所的かつ短い期間でのメリットが得られているにすぎない．

技術的な制限手法の選択

spam の問題は解決するのは簡単だと信じたくはなるが，歴史は我々に用心深くなるべきだと教えてくれる．http://craphound.com/spamsolutions.txt という Web ページでは，安直な spam 制限手法の提案に対してありがちな問題点のチェックリストをあらかじめ用意しておくという不遜な姿勢をとっているが，その手の提案を手早くふるい落とすには驚くほど有効である．

電子メールはユーザや事業者の数が非常に多いので，広範囲かつ急速な変化は見込めない．その上，spam の技術的な特徴はまたすべてある種の正当な電子メールの特徴でもある．このことは，メッセージの内容を評価するとか，メッセージの総流量を評価するとかのツールは一時的には使えるかもしれないが，効果的で長期間使えるツールではあり得ないことを物語っている．コンテンツやトラフィックをリアルタイムに評価するどんな試みも 2 つの点で問題がある．第 1 は正当なメールが spam と判断されてしまう“false positives”の問題だ．第 2 は互いに技術を改良し続けなければならない spammer と anti-spammer の間での“軍拡競争”という本質にある．spam 制御で一般的なのは，条件によってメールを振り分けるフィルタである．一般的に AU の境界線にある MTA や MDA などの電子メールを受け取る場所に設置される [13]．しかし，フィルタは，経路のどこに設置してもよく，送出側 AU の MTA はもちろん，特に MSA

に設置してもよい．受け取る側のフィルタは spam のトラフィックを減少させることはできないが，送出側ならトラフィックを減少させることができる．フィルタの設置に際しては，疑わしいメッセージの取り扱いについていくつかの選択肢がある．

- メッセージに特別な注釈をつける
- メッセージを特別な場所へ振り分ける
- バウンスアドレスへ送り返すかクライアントからの SMTP セッション中に受け取りを拒否する．
- 単純に消してしまう
- SMTP の伝送レートを制御するため，トラフィックシェーピング技術を用いてゆっくり受け取る

フィルタの基準をどうするのかという難しい問題がある．これに対しては，基準はたくさんあるという解答になってしまう．このため，フィルタのエンジンは，実際には汎用かつ拡張性のある spam 制御のためのプラットフォームになっている．基準にはそれぞれ複雑ではあるが，2 つの種類がある．

- ベイズ統計で語彙を追跡するようなコンテンツ解析
- 発信者の身元により，ホワイトリストで許可をしたりブラックリストで拒否をしたりする評価

コンテンツ解析はいつも部分的にはうまくいく（そして部分的にはうまくいかない）．判断基準の確立はデータベースに登録する学習メッセージに依存している．一方で，spammer は最新のフィルタ技術をすり抜けるための技法を常に開発している．

身元調査は問題となる電子メールに責任がある者を捕まえようとするものだが，その実体には 2 つの大きな分類がある．

- **コンテントエージェント**：個々のメッセージに責任を持つ，作者（From）と投函者（Sender）のこと．もし，コンテントエージェントが，あるメッセージに関して正当であれば，そのメッセージの中身はおそらく彼らの意図に沿っている．つまり，他の誰かがメッセージの中身を改竄したとはあまり考えられない．バウンスアドレス（MailFrom）は SMTP プロトコルの中に現れるのだが，投函者と関係があるため，しばしば解析に有効であると思われている．しかし，残念ながら，そのアドレスは多くの場合，From フィールドの作者，もしくは Sender フィールドの投函者との間に明白な関係はない．ただし，spammer は配送に失敗した大量のエラーメールをどこかほかのところに差し向けるため，よく嘘のバウンスアドレスを指定するので，結果として MailFrom アドレスの正当性を確認するのに役立つ．
- **オペレーションズエージェント**：MTA を動かしたり，ネットワークを維持したりする人々のこと．大量のトラフィックに対して責任を問われることがある．コンテンツを作っていないにもかかわらず，顧客に厳しいルールを課し，それに対するいくつかのパターンの違反を検知することが可能だが，実際に事業者には，なんらかのコンセンサスを得るように行動を開始することを勧めたい[4]．

身元調査は事前にでも事後でも行える．本質的には送信者側でも受信者側でも可能であるということだ．

- “Accreditation”とは送信者による登録所への登録作業である．そのためには送信者は，送信者の身元保証を信頼して行える登録所と提携する．
- “Reputation”とは送信者の過去の送信記録を評価することを指す．そのためには独立した第三者が送信者の記録を評価する．

データベースには，身元が明確に記載されるので，記載されていないものが多くても，“false positive”をほとんどゼロにすることができる．しかしまだ，身元調査をベースにしたフィルタリングを使うのは大きな課題が残されている．

- どの身元情報を利用するべきか？　また，将来起こり得る spam 送信とどのように関連づけられるか？　前述の表はかなり多くの選択肢が挙げられていることに注意してほしい．さらに，作者がよくないコンテンツを作ることはできるが，そのコンテンツの From フィールドに挙げられた身元情報は実際の作者のものではないかもしれない．メール送信ネットワークの事業者はコンテンツの作成とはまったく関係ないが，総トラフィック量の問題を引き起こした者を把握するのは当然である．
- 身元の確認（認証）はどうするのか？　誰が確認するのか？　確認されている個体との関連づけは？　な

ぜ信用できるのか？　確認のメカニズム自身にはごまかしがないか？

- どうやって spammer かどうかを判断するのか？　どの部分で送信者の質を保証するのか？　そして，それはなぜ信用できるのか？

現在の身元調査の枠組みでは，サーバに対して直接メールを送りつけてくるクライアントの IP アドレスを使い，サーバでフィルタリングする．IP アドレスは根底となるネットワークによって与えられるため，今までは偽装されることは少なかった．しかし，spammer は IP アドレス空間を盗むことに熟達してきている！

ホストがインターネットへの接続を変えればその IP アドレスも変わる．そして，その IP アドレスをつけるのはメールの作者ではなく事業者である．ホストの参照をもっと安定して行えるように，IP アドレスの代わりにドメイン名を使う新しい方法が模索されている [2]．

時が経てばインターネットの電子メールが論理的に 2 つのサブセットに進化していく見込みはある．1 つは，信頼できかつ責任を持った参加者だけのメール．もう 1 つはそれ以外のメールだ．信頼できる参加者はこれから先も，より緩いチェックやフィルタリングの制限ですむかもしれない．もっと大事なのは，もし問題が発生しても，信頼できる通信路で届くメールは自動的には受信拒否されるのではなく，送信者チェックを行いつつ相変わらず配送される可能性が高いということだ．

サポートメカニズム

spam との戦いは協調作業である．情報交換や連携を支援するツールや標準規格が役に立つ．この目的には，spam 送信事例を報告したり，個々の spam の特徴を表したり，spam を制御するデータを送信したりする標準的な方法があれば助かる．spam と spam 対策のグローバルな性質を考えれば，協調作業には互いに言葉の通じないネットワーク管理者間の交流を促すサービスも必要だ．ホワイトリストとブラックリストのためのシンタックスとセマンティクスの標準が出てくることもありそうだ．

参考文献

1）Crocker, D.: Internet Mail Architecture, Internet Draft draft-crocker-email-arch-04(Mar. 2005).
2）Mockapetris, P.: Domain Names - Concepts and Facilities, STD 13, RFC 1034(Nov. 1987).
3）Moore, K.: Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs), RFC 3461(Jan. 2003).
4）Hutzler, C., Crocker, D., Resnick, P. and Sanders, R.: Email Submission Between Independent Networks, Internet-Draft draft-hutzler-spamops-04(May 2005) .
5）Crispin, M.: Internet Message Access Protocol - Version 4rev1, RFC 3501(Mar. 2003).
6）Freed, N. and Borenstein, N.: Multipurpose Internet Mail Extensions (MIME)Part One: Format of Internet Message Bodies, RFC 2045(Nov. 1996).
7）Myers, J. and Rose, M.: Post Office Protocol - Version 3, STD 53, RFC 1939(May 1996).
8）Postel, J. B. : Simple Mail Transfer Protocol, STD 10, RFC 821(Aug.1982).
9）Crocker, D. H. :Standard for the Format of ARPA Internet Text Messages, STD 11, RFC 822(Aug. 1982).
10）Klensin, J. : Simple Mail Transfer Protocol, RFC 2821(Apr. 2001).
11）Resnick, P. : Internet Message Format, RFC 2822(Apr. 2001).
12）Chandhok, R. and Wenger, G.:List-Id: A Structured Field and Namespace for the Identification of Mailing Lists, RFC 2919(Mar. 2001).
13）Showalter, T.: Sieve: A Mail Filtering Language, RFC 3028(Jan. 2001).
14）Gellens, R. and Klensin, J.: Message Submission, RFC 2476(Dec. 1998).
15）Clark, D., Wroclawski, J., Sollins, K. and Braden, R.:Tussle in Cyberspace: Defining Tomorrow's Internet, ACM SIGCOMM(2002).
16）Hoffman, P. and Crocker, D.: Unsolicited Bulk Email: Mechanisms for Control, Internet Mail Consortium, UBE-SOL IMCR-008, http://www.imc.org/ube-sol.html, revised May 4, 1998.

（平成 17 年 6 月 15 日受付）