# SPAMメールの傾向と対策
## ── SPAMメールが激減した方策について ──

山　口　由紀子

## Ⅰ．はじめに

インターネットの普及とともにSPAMメール（迷惑メール）の数が増大し，受信したメールを振り分けるといった余分な作業が必要になってきた。このような状況は利用者個人個人のメール利用の所要時間を増大させる他，全学的なレベルでもメール配送に負荷がかかるという問題を引き起こしてきた。このような状況から情報連携基盤センターではSPAMメールの学内への流入を防ぐための対策を取ってきている。まず2004年11月にネームサーバによるホスト認証を設定したところ，SPAMメールの数は半減した。しかしその一方で，予想外に多くのサイトでネームサーバの設定が不十分であり，特に中国，韓国ではほとんど設定されていないため，電子メールが受信できなくなるという弊害が発生した。そこでホスト認証に代わる対策として2005年６月にグレイリスト方式を導入した。本稿では，これまでのSPAM対策の経緯について報告する。

## Ⅱ．全学メール受信システム

名古屋大学では，学外から受信する電子メールのウィルスを検出・除去するため，全学の受信メールを集中して受信している。図１に構成を示す。メール受信サーバ，ウィルス検出サーバ，配送サーバの３段構成となっており，それぞれ主系，副系の２系統で運用している。図２に１ヶ月当たりのウィルス検出数を示す（主系のサーバのみ）。ウィルスは次々と新種や亜種が作り出されており，また昨今はブロードバンド接続された家庭のパソコンの数が増えてきたためかウィルス検出数があまり減少しない。

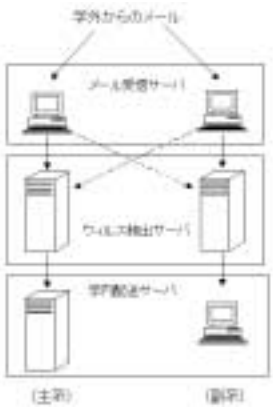


**図１　全学電子メール受信システム**

本稿で説明するSPAM対策は学外からのメールを集中して受信している受信サーバで設定するものであるため，結果として全学のメール受信状況に影響することとなる。

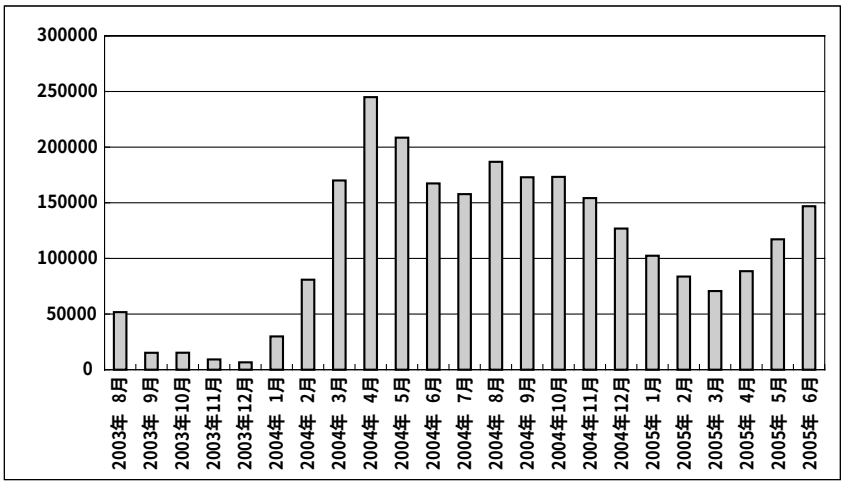


**図２　１ヶ月あたりの電子メールのウィルス検出数（全学）**

## Ⅲ．SPAMメールの動向

筆者は，基盤センターのメールサーバnuccにおいて，数年前までは利用していたがここ数年間メールの送受信に全く利用していないアドレスについて，SPAMメール観測用としてメール受信を継続している。図３に観測用のアドレスで受信した2003年８月からの１ヶ月当たりのSPAMメール数を示す。

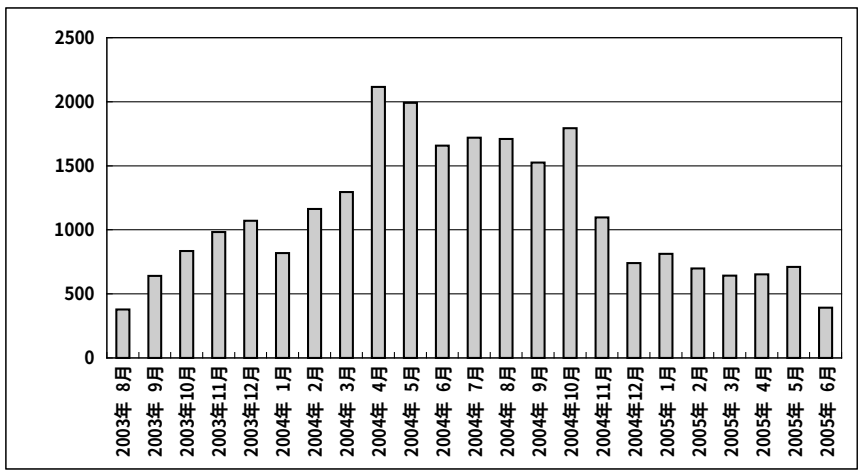


**図３　１ヶ月当たりのSPAMメール数（観測用アドレスで受信したもの）**

図３からわかるように，2003年８月から12月にかけてSPAMメールの数が顕著に増大している。

この傾向は全学的なものであるため，2004年１月から３月にかけて日常的にメール配送に遅延が発生したり，全学のメール受信サーバが過負荷でダウンするなどの障害が発生した。４月にシステムチューニングを行い，さらに８月にメール受信サーバ（主系のみ）を更新することにより，全学のメールが安定して受信できるようになった。その結果として大量のSPAMメールをも安定して受信することとなり，観測用アドレスでも2004年６月から10月にかけては連日50通から70通のSPAMメールを受信していた。

一般に，SPAMメールはSPAM送信ツールをインストールされたパソコンなどから送信されていることが多い。通常パソコンはネームサーバに登録されていない。そこで，2004年11月にネームサーバによるホスト認証を設定した。この効果によって１日当たりのSPAMメール受信数は約半分になったが，その一方で多くのサイトからメールが受信できなくなるという弊害が発生した。2005年１月に全学メール受信サーバ（副系）の更新が完了したことから，ホスト認証に代わるSPAM対策としてグレイリスト方式を導入し，SPAMメールの受信数を削減することができた。以下にその詳細を述べる。

## Ⅳ．ホスト認証によるセキュリティ強化

電子メールはサーバ間でsmtpと呼ばれるプロトコルを通じて送受信する。通常メールを送信するサーバはメールの受信も行うので，メールサーバのホスト名，IPアドレスはネームサーバに登録されている。一方，SPAMメールはSPAM送信プログラムを仕込まれたパソコンなどから送信される場合が多く，このようなパソコンはネームサーバに登録されていない場合が多い。ネームサーバによるホスト認証は，このような特徴を利用して，メール受信の際に送信してきたサーバのIPアドレスからホスト名を逆引きし，さらにそのホスト名を正引きしてその整合性がとれた場合にのみメールを受信するというものである。

2004年11月に全学メール受信サーバにおいてホスト認証を設定した。図４に前後３ヶ月の１日当たりのSPAMメール受信数を示す。ホスト認証設定後，SPAMメール数が約半数になり，効果が確認できた。

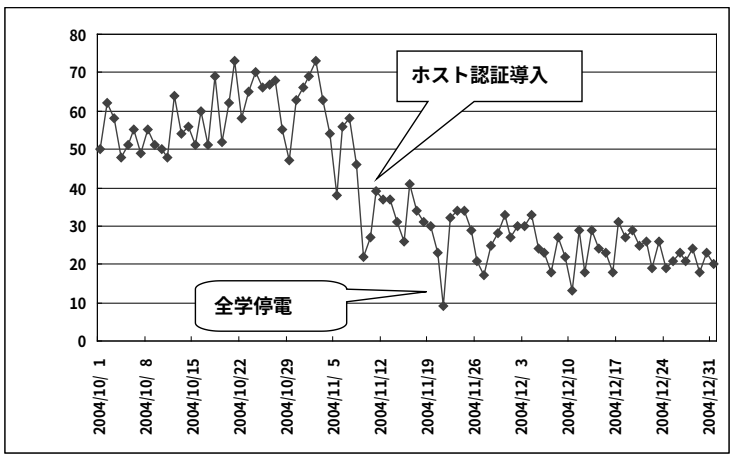


**図４　１日当たりのSPAMメール数（観測用メールアドレスで受信したもの）**

しかし，その一方でメールが受信できなくなるという弊害が多発した。予想外に多くの組織においてメールサーバが逆引きネームサーバに登録されておらず，内閣府や特許庁などの重要なサイトからのメールが受信できなくなってしまった。これらのサイトについては，各組織の管理者にネームサーバへの登録を依頼し，その後メールが受信できるようになった。また，学内の利用者からメールが受信できないという連絡を受けたサイトについては，ホスト認証することなくメールが受信できるホワイトリストに登録するなどの対処を取ってきた。

しかしながら，中国，韓国では逆引きネームサーバが設定されている組織の方が稀で，逆引きサーバの設定を依頼したとしても一組織の管理者で対処できる状態でないことがあきらかとなった。ホワイトリストで対応するにしても限界があるため，ホスト認証の運用を継続するのが難しい状況となった。

## Ⅴ．グレイリスト方式によるセキュリティ強化

メール受信において，ホワイトリストは無条件でメールを受信するサーバのリスト，ブラックリストは無条件でメール受信を拒否するサーバのリストとして利用する。グレイリストはその中間に位置するもので，ホワイトかブラックか判断を保留するサーバのリストである。

グレイリスト方式とは，メール受信の際に送信元のメールサーバをグレイリストに登録して一旦受信を保留し，同じサーバから再度送信されてきた際に受信するというものである。これは，SPAM送信プログラムは通常メールを再送しない，という特徴を利用している。グレイリストを導入することによって正当なメールの１回目の受信は遅延することになってしまうが，SPAMメールの受信が減少することが期待される。

図５に2005年６月１日から７月13日までの１日当たりのSPAMメール受信数を示す。グレイリスト方式を導入した2005年６月27日の昼過ぎ以降，SPAMメール数が激減した。筆者自身が受信するSPAMメールもかなり減少した。６月27日以降もSPAMメールは届いているが，以前は雑多なアドレス宛のSPAMメールが大量にあったが，現在は国際会議の参加者リストに載せたアドレス宛のものだけとなった。

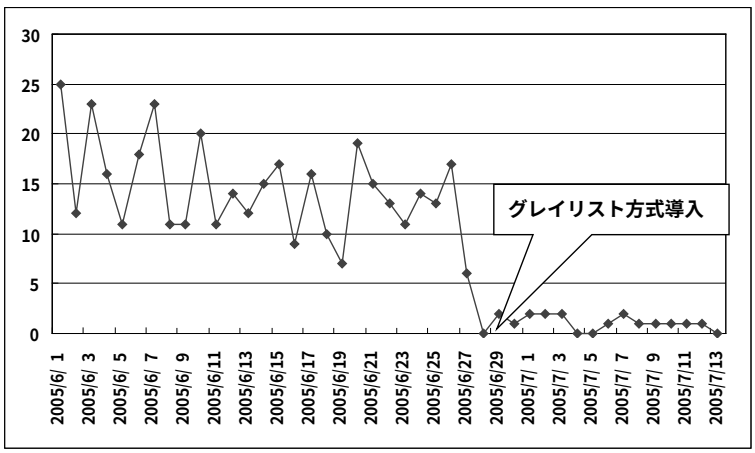


**図５　１日当たりのSPAMメール数（観測用メールアドレスで受信したもの）**

SPAMメールのほか，ウィルス検出数や，学内に配送される宛先不明となるメールの数も減少した。図６に図１のウィルス検出サーバでの１日当たりのウィルス検出数を示す。ウィルス感染したパソコンが発信するウィルス付きの電子メールは，SPAM送信プログラムと同じようなプログラムが使われているためか，６月27日以降のウィルス検出数が減少した。

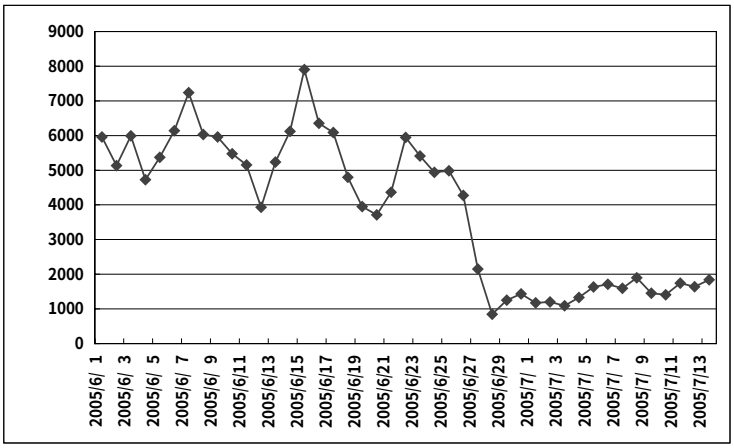


**図６　１日当たりの電子メールのウィルス検出数（全学）**

情報連携基盤センターの全国共同利用システムのメールサーバnuccで宛先不明となるメールの数は，６月第一週の１週間で宛先不明となったメールが41684通あったのに対し，７月第一週では8711通となり，５分の１ほどに減少した。宛先不明となるメールの学内への流入が阻止できていることが確認できた。これにより，全学の各メールサーバにおいて宛先不明となるゴミメールの処理にかかる負荷が軽減できた。

## Ⅵ．おわりに

ここ２年間のSPAMメールの動向とこれまで行った対策について述べた。６月27日から運用しているグレイリスト方式は今のところ効果が絶大であるが，今後も継続して動向を調査する必要がある。また，稀に再送しないメールサーバがありメールが受信できない場合があるという報告があることから，日常的な監視も必要である。

（やまぐち　ゆきこ：名古屋大学情報連携基盤センター情報基盤ネットワーク研究部門）