金沢大学における spam・ウイルスメール対策

金沢大学情報部情報基盤整備課（総合メディア基盤センター） 松平 拓也

今日，インターネットにおける電子メールの利用は重要な要素の 1 つとなっており，
コミュニケーション手段として世界中で利用されています．
しかしながら，最近ではその利便性を逆手に取った
spam メールやウイルスメールの急増が大きな問題となっています．

増加，悪質化する「spam メール」

spam メールとは，商品の広告や出会い系など営利を目的に不特定多数に大量送信されるメールです．現在，全世界を流通しているメールの 7~8 割が spam メールであるとも言われています．また，最近ではフィッシング (Phishing*) メールと呼ばれる，金融機関などを装い暗証番号やクレジット番号の搾取を目的としたメールの増加や，メール本文のリンク先をクリックすると，ユーザの個人情報の搾取を目的とするスパイウェア (Spyware) を埋め込まれる事例の増加が問題となっています．特にフィッシングメールは，送信元メールアドレスやメール本文に記載されている URL を巧妙に詐称している為，正規のメールかどうかの判断が非常に困難です．このように spam メールはどんどん悪質化してきており，犯罪性をおびた目的で送られてくるケースが増えてきています．

またウイルスメールにおいても，最近では自己増殖のために大量のメールを無作為に発信するマスメーリング型と呼ばれるものが増加しています．

spam メール，ウィルスメールの数による被害

このようなメールを各ユーザが全て受け取った場合どうなるでしょうか？ユーザは必要なメールと spam 及びウイルスメールを分類しなければなりません．この作業には時間がかかる上，その過程で重要なメールを見落としてしまう危険性が考えられます．また，大量のメールがネットワーク上を流れると，ネットワークにかかる負担が非常に大きくなってしまいます．

全メールの約 7 割が spam メール！！

では，実際に金沢大学にはどれだけこれらのメールが送られてきているかを見ていきます．図 1 は金沢大学に配信されてくる 1 日あたりの総メール数とそのうちの spam メールと判断されたメール数を示したものです．全到来メールのうち約 7 割が spam メールと判定されていることが分かります．しかしながら，spam メールと判断できない巧妙なメールも到来している可能性があるため，実際は全体の 7 割を超えるメールが spam メールであると想定されます．また，図 2 は金沢大学に配信されてくる 1 日あたりのウイルスメール数のグラフになります．1 日あたり千通以上が到来していることが分かります．このように金沢大学にも大量の spam 及びウイルスメールが送られてきていることが分かります．

金沢大学ではこの問題を深刻に受け止め，spam 及びウイルスメールから学内ユーザ及びネットワークを守るため，独自に spam・ウイルスメール対策システムを構築し，対応を行っています．

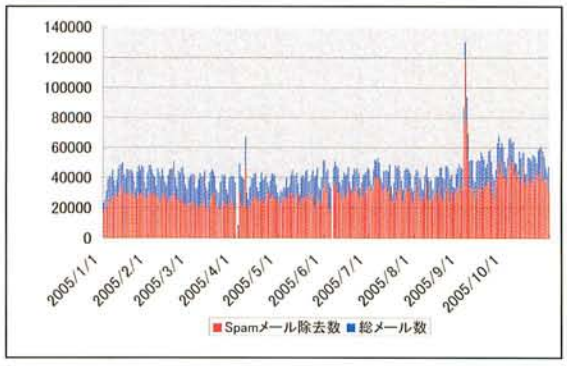

図 1 1 日毎の全メール数と spam メール数

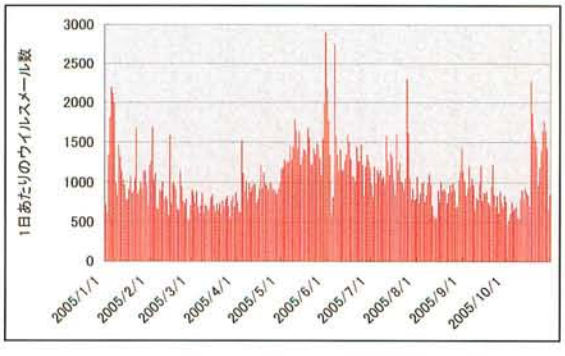

図 2 1 日毎のウィルスメール数

*) Phishing: Fishing と sophisicated からなる造語

学内のメール配送経路及び対策システム概要

メール配送経路とチェック機構

図３に本学のメール配送経路及び対策システム概念図を示します．学外から送られてきた全てのメールは対学外 Firewall を通過し，対学外メール中継サーバに送られます．この中継サーバのリレー先に spam 及びウイルスをチェックするサーバを指定し，チェックを行います．ウイルスチェックにはベンダ提供のパターンファイルを用いており，既にウイルスと特定可能なメールはここで削除されます．但し，まだパターンファイルが対応していない新種・亜種のウイルスの可能性のあるメールは管理サーバに隔離し，学内へ侵入し蔓延する事態を未然に防ぐようにしています．ウイルスの可能性のあるメールとは，拡張子が .exe，.com，.pif など，ウイルスメールによく添付されてくるファイルが添付されているメールです．また，spam の疑いのあるメールも同様に管理サーバに隔離します．

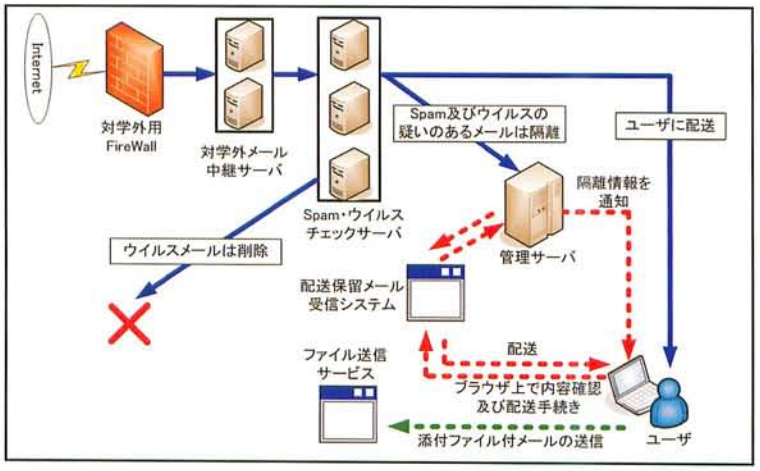

図３ 金沢大学のメール配送経路及び対策システム概念図

spam，ウィルスメールの削除と隔離

このようにチェックサーバをパスしたメールのみユーザに配送し，spam 及びウイルスの疑いのあるメールは隔離することで，ユーザに届く spam 及びウイルスメールの数を減らすようにしています．メールを隔離する際には細心の注意を払って行っています．そして万一，普通のメールが spam またはウイルスメールと判断された場合にメール不達のトラブルが発生しないように，隔離を行った際には必ずメールの送信先に隔離を行った旨を通知します．隔離情報を受け取ったユーザはその情報をもとに，Web ブラウザ上で「配送保留メール受信システム」にアクセスすることで隔離されたメールを簡単に確認し，取り出せるようにしています．また，ファイルが添付されているメールがウイルスメールと判断されて隔離されないように「ファイル送信サービス」を構築し，提供しています．

配送保留メール受信システム

メールの隔離とその通知

チェックサーバで spam 及びウイルスの疑いがあると判断されたメールは管理サーバに隔離され，隔離されたことを送信先ユーザに通知します．ウイルスメールの疑いが濃いと判断された場合は，隔離されるとすぐに隔離情報をメールで通知します．送信されるメールの内容を図４に示します．

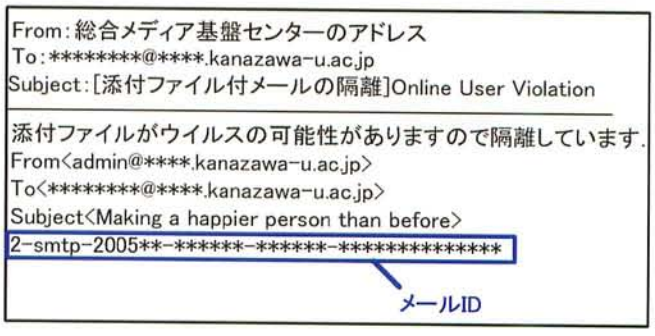

図４ ウイルスの可能性による隔離通知メール

一方，spam メールの疑いのあるメールはウイルスメールの疑いのあるメールよりも数が非常に多いため，spam メールと判断された場合は隔離されてもすぐには隔離情報を通知せず，図５に示すように隔離したメールの件名，送信元アドレスなどを含むリストを１日に１度，送信先ユーザに配送するようにしています．

１日に１度，リストとして隔離

情報を通知することで，ユーザは1日分のspamメール情報を1通で受け取ることができます．それにより，ユーザはspamメールにまぎれて重要なメールを見落とすといった危険性を減らすことができます．

また，spam及びウイルスの疑いで隔離されたメールの隔離期間は3ヶ月間と十分な期間を設け，都合により長期間メールが取得できないユーザのことを考慮して設計されています．

```
From：総合メディア基盤センターのアドレス
To：********@****.kanazawa-u.ac.jp
Subject：[配送保留メール確認リスト一覧](2005/05/10日分)

#No. 1
2005 May 10 01:39
From<Clare4@madferit.co.uk>
To<********@****.kanazawa-u.ac.jp>
Subject<Making a happier person than before>
2-smtp-2005**-******-******-**************
                                    メールID
#No. 2
2005 May 10 02:00
From<fefagggbger@fefghfcf.com>
To<********@****.kanazawa-u.ac.jp>
Subject<サイドビジネスにいかがですか？>
1-smtp-4020**-******-******-**************

#No. 3
2005 May 10 03:30
From<info@etesrfifdef.com>
To<********@****.kanazawa-u.ac.jp>
Subject<お久しぶりです>
1-smtp-4032**-******-******-**************
                    .
                    .
                    .
```

図5 spamの可能性による隔離通知メール

隔離されたメールの再配送

隔離した全てのメールには，メールを一意に特定するためにメールIDをつけています．ユーザは，もしリストの中に再配信してもらいたいメールが存在した場合は，図6に示す配送保留メール受信システムにWeb上からアクセスします．メールIDは他人に推測されないように複雑に設計されています．

ユーザはフォームに再配信を希望するメールのメールIDを入力し，確認ボタンをクリックします．確認ボタンをクリックすることで図7に示す隔離メール内容確認画面に移動し，該当メールの本文を一部表示するようにしています．すぐに該当メールを配送しない理由は，メールの送信元は詐称されていることがよくあり，メールの内容を一部表示することで本当に必要なメールかどうかをユーザが判断できるようにするためです．メールの内容を確認した上で配信を望む場合は「受信する」を選択することで自動的に再配信されます．

このようにWeb上でいつでも簡単にメールを再配信できるようにすることで，ユーザにできるだけ不便さを感じさせないようにしています．

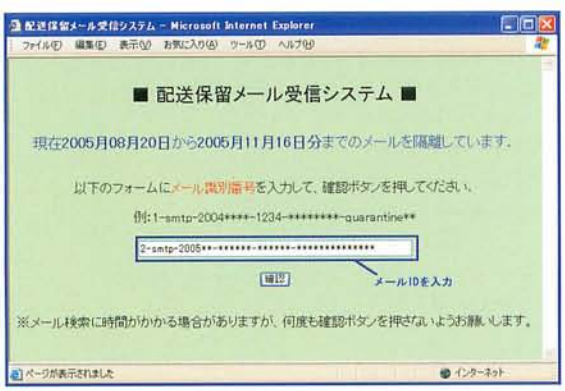

図6 配送保留メール受信システム

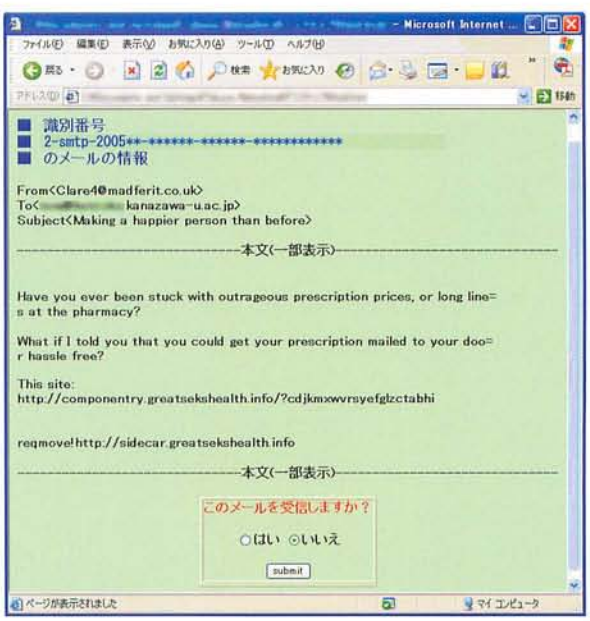

図7 隔離メール内容確認画面

ファイル送信サービス

ウィルスチェッカも万全ではない？！

学外から送られてくるメールは全てウイルスチェックを行い，また最近では市販のウイルス駆除ソフトを導入している人が多くなってきているため，届くメールはすべて安全だと思う人も多くいるかと思います．しかしながら，新種・亜種ウイルスが送られてきた場合に，パターンファイルが対応していなかった場合はウイルスチェッカをすり抜けてユーザに配送されてしまいます．そしてユーザのウイルス駆除ソフトも未対応だった場合，メールを開いてしまうとウイルスに感染してしまいます．

先ほども少し触れましたが，一般的にウイルスメールにはファイルが添付されています．添付ファイルの多くは .exe，.com，.pif などの拡張子を持つ実行形式のファイルがほとんどですが，一般的にこのようなファイルを添付することは稀なため，金沢大学では隔離を行い，新種・亜種ウイルスの学内への進入を未然に防いでいます．

図８ ファイル送信サービス

この仕組みを導入して以来，新種・亜種ウイルスが学内に蔓延することがほとんどなくなりました．しかしながらこのことがメールの利便性を欠くという側面も併せ持つことは否定できません．

安全にファイルを送信するために

これを解決するため，センターでは図８に示すファイル送信サービスを構築し，ユーザに利用を推奨しています．

ファイル送信サービスの仕組みについて簡単に説明します．メールの送信者は添付ファイルを一時的にサーバにアップロードしておき，その情報を受信者に通知します．受信者はその情報をもとにサーバにアクセスしてファイルをダウンロードすることができるシステムです．

最大５メールアドレス同時に送信でき，最大 50Mbyte まで添付することができます．ウイルスの疑いによる隔離を避ける場合だけではなく，サイズの大きいファイルを添付したいユーザも利用することを強く推奨します．

ファイル送信サービス URL：http://www2.imc.kanazawa-u.ac.jp/sendfile/

個人でできる spam・ウイルスメール対策

一人一人の防衛意識が大切

金沢大学では spam 及びウイルスメールの対策を行い，できるだけユーザが快適にメールを利用できるよう努めています．しかしながら，ユーザがこのことに安心して何も考えなくてもよいわけではありません．ユーザの努力で spam 及びウイルスメールから身を守ることが可能です．

ユーザは特に以下のことに注意してください．

Web 上で，むやみにメールアドレスを公開しない

spam 送信者は Web 上で公開されているメールアドレスを自動収集しています．できるだけメールアドレスは Web 上で公開しないようにすべきです．

怪しいメールの本文に書かれているリンクはクリックしない

spam メール等怪しいメールの本文に張ってあるリンクをクリックしてしまった結果，リンク先が自動的にスパイウェアをダウンロードさせ，個人情報を搾取するものであったり，不当な金額を要求されるいわゆる「ワンクリック料金請求」のサイトであったりする可能性があります．

安易に添付ファイルを実行しない

最近のウイルスメールは送信元アドレスを詐称したり，内容が重要な通知であるようにみせたりするケースが増えてきています．そのため，たとえ送信元や内容が信頼できると思われる場合でも，安易に添付ファイルを実行せず，まず送信元に問い合わせ安全なものか確認するようにすべきです．

メールをいきなりHTML 形式で表示しない

最近，見栄えがよい等の理由から，HTML 形式のメールが増えてきています．しかし，ウィルスメールの中には HTML 形式で表示するだけで感染を引き起こすものも存在します．メールを表示する時には，まずはテキスト形式で表示させ，必要かつ安全なもののみ HTML 形式で表示させるようにしましょう．