メールシステムの現状と課題
Status and assignment of the mail system

車古正樹 ＊1,　　松平拓也*2,　　中野三智子＊3
SHAKO Masaki　MATSUHIRA Takuya　NAKANO Sachiko
井町智彦＊4,　　西川直樹＊5
IMACHI Tomohiko　NISHIKAWA Naoki

〒920-1192　金沢市角間町
金沢大学総合メディア基盤センター
Information media center of Kanazawa University
TEL：076-234-6912

＊1　shako@office0.ipc.kanazawa-u.ac.jp
＊2　takusng@kenroku.kanazawa-u.ac.jp
＊3　nakano@kenroku.kanazawa-u.ac.jp
＊4　imachi@office0.ipc.kanazawa-u.ac.jp
＊5　nisikawa@office0.ipc.kanazawa-u.ac.jp

概要

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一つとなっている。しかし，最近では UCE，UBE と呼ばれる迷惑メール（Spam メール[以下 Spam と呼ぶ]）の数が急増しており，その数は無視できないほどになっている。また，コンピュータウイルスには自己増殖の為に大量のメールを無作為に発信する（以下マスメーリング型と呼ぶ）ものも多い。これらがメールサーバを含むネットワークに与える影響は非常に大きく，対策を講じたメールシステムの構築が必要となっている。そこで，本稿では金沢大学における Spam 対策，ウイルスメール対策の現状と今後の課題について報告する。

キーワード

Spam 対策，ウイルス対策，コンテンツフィルタ

1. はじめに

近年，インターネットの普及により，学内において電子メールの利用が一般化している。しかし，最近では Spam が急増しており，ウイルスは NETSKY や BAGLE に代表される，マスメーリング型が大部分を占めている。金沢大学では Spam 対策として，昨年 11 月よりトレンドマイクロ社製 InterScan Messaging Security Suite（以下 IMSS と呼ぶ）を利用し，Spam のフィルタリング及びウイルスメールの検出・駆除を行っており，マスメーリング型についてはメール自体を削除している。最近のウイルスは新種（亜種）の登場までの期間が短く，パターンファイルが更新され

るまでの間に多くのウイルスメールが内部に侵入する場合がしばしば見受けられる。その為，本学では疑わしいメールが学内に侵入する前に，コンテンツフィルタを利用し，ファイル名の拡張子でフィルタリングを行い，新種の侵入を防いでいる。本稿では，現在のメールシステムの構成，金沢大学における Spam 及びウイルスメール対策（コンテンツフィルタ）について説明する。

2. システム構成

金沢大学のメール受信経路を図１に示す。外部から来たメールは学外用 FireWall を通過し，送受信サーバに送られる。送受信サーバのリレー先に IMSS サーバを指定し，ここでウイルスチェック，Spam チェックを行う。そして学内用 FireWall を通過し，学内配信サーバに送られ，そこから各部局のメールサーバに配送される。学内に存在しないユーザ宛のメールは学内配送サーバにエラーが返り，そこから送受信サーバにエラーメールが返される。また，内部からのメールに関しては学内送信用サーバに IMSS を導入しており，ウイルスチェックを行っている。その為学内すべてのユーザにこの送信用サーバを利用するよう呼びかけている。

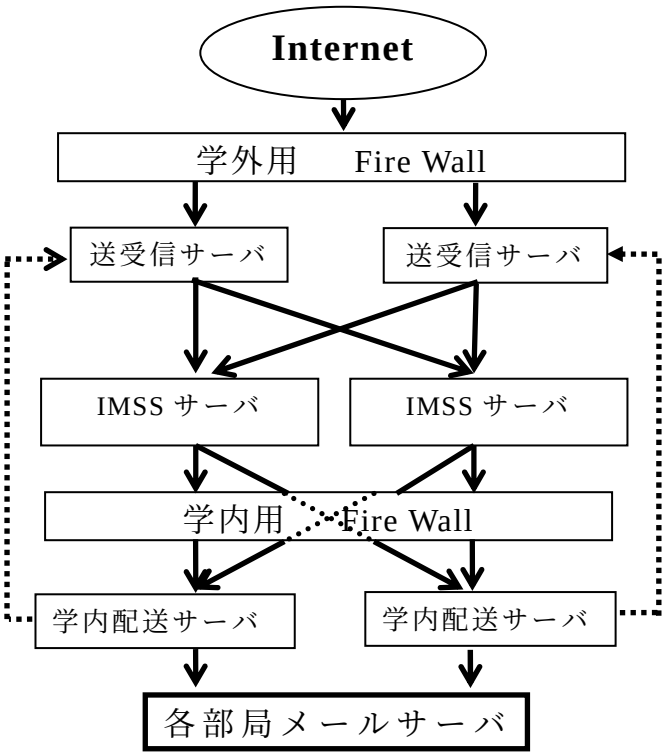

図 1　金沢大学のメール受信経路

3.Spam メール対策

前節のシステム構成で述べたとおり，金沢大学では学外からのすべてのメールを IMSS の Spam フィルタでチェックしている。金沢大学では，Spam と判断されたメールは原則配信していない。Spam と判断したメールの Subject に[SPAM]などの文字を追加し，削除するかどうかを受信者に委ねる方法も考えられるが，導入当初は MIME エンコードの仕様により，UNIX では Subject が文字化けするという不具合が起きてしまった。また，Spam フィルタの定義ファイルはトレンドマイクロ社から提供されているが，本学ではそれを用いず独自に Spam フィルタを定義している。その理由として，提供されているフィルタを使用した場合，IMSS が正規のメールも Spam と判断してしまう場合があることと，定義ファイルがブラックボックスとなっており，こちら側で変更することができないことが挙げられる。

3-1.データ収集方法

Spam フィルタを定義するためには，多数の Spam メールを解析し，特徴・傾向などの情報を得る必要がある。本学では，すでに名称を変更しているホスト宛のメール，学内に存在しないユーザ宛のメールで，from が詐称されているため返送できずに送受信サーバに溜まっているメールから Spam メール特徴・傾向を調べ，Spam フィルタに定義している。

3-2.Spam フィルタの定義

表 1 は Spam メールから抽出した特徴・傾向から作成した，Spam フィルタの定義のパターン例を表しており，表の上から順に適用される設定になっている。Spam フィルタの定義には柔軟性を持たせるため，正規表現を使用している。(定義文中の.REG.は正規表現利用の宣言を示す。.AND.は[かつ]を示す。.OCCUR.は繰り返しを示す。)。

表 1　Spam フィルタの定義

分類	パターン例	除去割合	備考
大量メール(題名)	PHOTOSHOP .AND. XP PRO .AND. NORTON .AND. .REG. ¥$[0-9][0-9]	21.6%	1 日 100 件以上受信
大量メール(本文)	.REG. Casino.* .AND. .(. internet .OR. Online .OR. .REG. .*bonus .OR. money .OR. today .OR. wins .OR. Cash .).	8.7%	1 日 100 件以上受信
題名（擬似語）	.*0nline.*,p[^a-z]rice.?	1.9%	綴りを変える
題名（語句）	Supersavings on .OR. .(. medications .OR. drugs .OR. pharmaceuticals .OR. meds .OR. Ambien .).	6.9%	
強制配信	.REG. .*news-master@mail[0-9]+¥.rakuten¥.co¥.jp	5.9%	Spam フィルタを通過させる
大量メール(タグ)	.OCCUR. .REG. .*<[a-z]+[0-9]+¥w{4,10}>.*	4.4%	1 日 100 件以上受信
本文（擬似語）	.(. Y0ur .OR. t0day .OR. .REG. d0ct.. .OR. 0rder .). .AND. .REG. .*http:/.*	11.4%	本文に綴りを変えた文字列が存在
本文（語句）	.(. 100 .AND. % .AND. money back guarantee .OR. always 100% money back guarantee .). .AND. .REG. .*http:/.*	11.4%	
未承諾	.REG. .*未承諾広告.* .AND. .(. .REG. .*配信者.* .OR. .REG. .*発信元.* .). .AND. .REG. .*http://.*	0.1%	
本文（タグ）	.REG. .*font-size:[1-3]px"">.* .OR. .REG. .*font-size: [1-3]px"">.* .OR. .REG. .*font-size: 0px; .OR. .REG. style=font-size:[1-3]px.* .OR. #ff6600 1px .OR. .REG. .*font-size:0px.*	6.2%	
サイトの一部	.REG. .*¥.us/f99/.*,.REG. .*¥&winner¥&_m01.*	4.5%	本文中に記載されている URL でフィルタ
サイト（com 以外）	.REG. .*http://notinuse¥.biz/.*	10.0%	
サイト（com）	.REG. .*http:/.*¥.promoaudit¥.com/.*	4.4%	
偽装サーバ	.REG. .*@e-mail¥.ru .OR. .REG. .*@emails¥.ru .OR. .REG. .*@e-mails¥.ru	0.6%	
ロングユーザ名	.REG. .*.....@aa¥.kanazawa-u¥.ac¥.jp	0.9%	9 文字以上のユーザ名
要確認	money back .AND. .REG. guarante.*your loan .OR. Mortgage .OR. Homeowner .OR. bad-credit .OR. Refinance .OR. Re-finance	1.1%	正式メールの可能性あり

フィルタ定義に際しては，コンピュータに負荷をかけないために，題名でのフィルタを優先し，正規表現や演算子を極力使わずに，シンプルに書くよう配慮している。

3-3.全体に対する Spam メール除去の割合

図 2 は外部から配送されてくるメールに対して，表 1 のように定義した Spam フィルタを適用した結果を図示したものである。集計は一月ごとに行い，図の横軸が年月を示す。図の縦軸はメールの数と Spam の割合を示し，ヒストグラムが全メール数と Spam 数，折れ線が全メール数に対する Spam の割合を示している。集計結果から，2003 年 1 月から 2004 年 6 月までは，約 40%のメールが Spam と判定されていることがわかる。また 2004 年 7 月は約 53%のメールを Spam と判定している。この原因として，7 月以降は Spam フィルタの定義の更新間隔をこれまで以上に短くしており，それが検出率向上につながっているものと考えられる。しかしながら Spam フィルタを

かいくぐるメールの数もいまだ多く，このことを加味すると，検出できていないものも含めた実際の Spam は 60%～70%にのぼる可能性が高いと考えている。

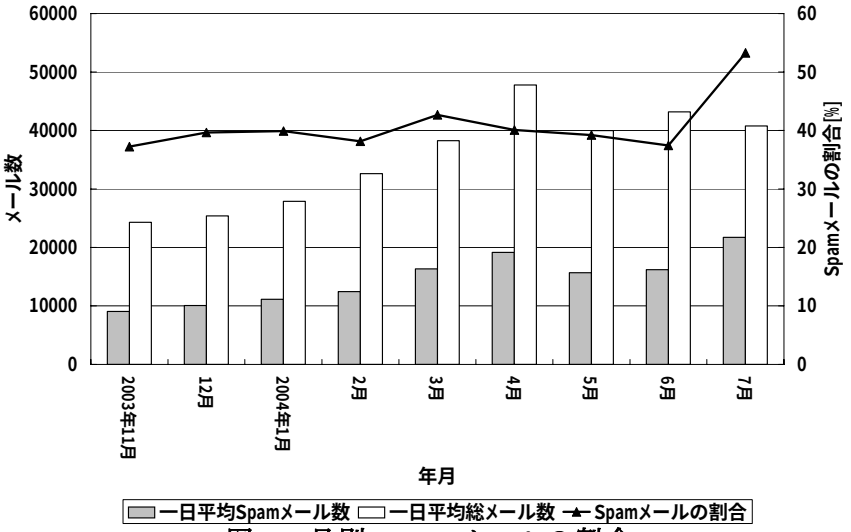

図 2　月別 Spam メールの割合

3-4.サイト用メールアドレスの Spam メール除去率

最近の Spam 送信者は Web からメールアドレスを収集するケースが多く，実際，金沢大学では Web ページに記載されているサイト用メールアドレスに多くの Spam が送られてきている。図 3 は，このようなメールアドレス宛にくる Spam 除去率の結果を図示したものである。図の横軸は月日を示す。縦軸はメールの数と Spam除去率を示し，積み上げ縦棒の灰色部分がフィルタによって隔離されたメール数，白色部分が隔離されずに通過したメール数，折れ線が Spam 除去率を示している。その結果，サイト用メールアドレスについては，Spam の 7～8 割が除去されていることがわかった。

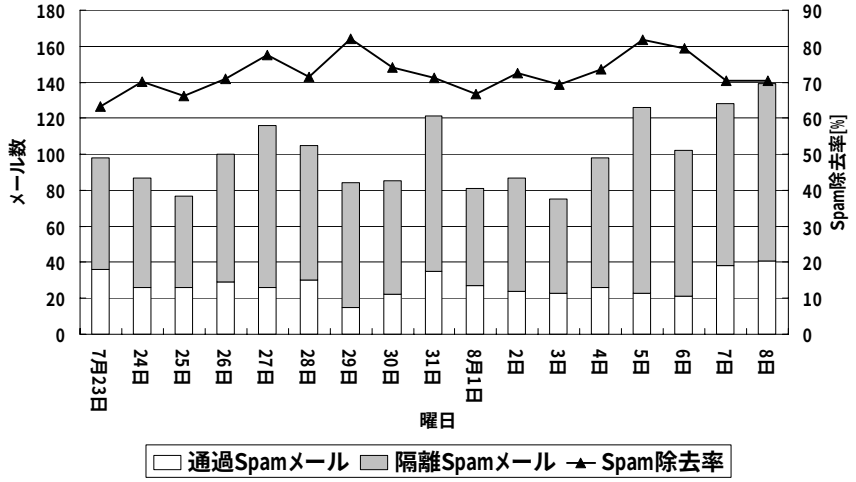

図 3　Web サイト記載メールアドレスにおける Spam 除去率の例

4.ウイルスメール対策

冒頭で述べたとおり，最近のウイルスの動向から，パターンファイルが更新されるまでの間に新種が学内に侵入する危険性が考えられる。そこで，金沢大学ではこの状況に対応するため，IMSS のコンテンツフィルタ機能を用い，新種の学内への侵入を防いでいる。

ウイルスメールには，必ずといっていいほどファイルが添付されてくる。ウイルスメールの添付ファイルには，下記のような拡張子がつけられている場合が多い。

*.pif, *.com, *.lnk, *.scr, *.hta, *.vbs, *.exe（*は任意の文字列を表す）

このような拡張子を持つファイルを対象にフィルタリングしている。これらのファイルは，正常なメールに添付されることは極めて稀で，ウイルスの可能性が非常に高いと考えられる。その為，これらのメールはユーザに配信せずに隔離しておき，受信者に対し From，To，Subject の情報を

通知して，正規メールかを確認してもらい，正規メールの場合は配送希望を提出してもらった上で，配送を行っている。

次に，実際に学内でコンテンツフィルタが有効だった事例を３点報告する。

事例１）６月１４日（PE_ZAFI.B）

9:31　コンテンツフィルタに最初のウイルスと疑われるメールが届く。

10:05　外部から同様のメールが大量に送られてくるようになるが，コンテンツフィルタで隔離。

11:31　亜種または新種のウイルスの疑いがある為，メーカにウイルスを送り調査を依頼。

18:28　メーカから PE_ZAFI.B であるという報告と共に最新のパターンファイルが送付され，これを適用。これまでに計 276 通のウイルスメールを隔離し，学内への侵入を阻止。コンテンツフィルタで隔離できたのは，添付ファイルがすべて pif ファイルだったためである。

事例 2）７月５日(WORM_BAGLE.AD)

コンテンツフィルタが最初に隔離してからパターンファイルが更新されるまでの約 2 時間半で，323 件をコンテンツフィルタで隔離できた。隔離できたのは WORM_BAGLE.AD の添付ファイルの拡張子に.com, .exe, .hta, .scr, .vbs が含まれていたからである。

事例 3）8 月 10 日(WORM_BAGLE.AC)

WORM_BAGLE.AC は添付ファイルの拡張子が Zip 形式で，上記の拡張子と一致していなかったが，解凍した中身の HTML 文書に含まれるパターンが Spam フィルタのパターンと一致していた。その為，ウイルスパターンファイルが更新されるまでの約 3 時間半の間，計 53 通のメールが Spam として隔離された。このように，ウイルス用のフィルタにかからなくても，Spam フィルタに引っかかり隔離できるケースも存在する。

5.今後の課題

現在のところ，Spam フィルタの定義は手動で行っており，非常に手間がかかってしまうのが現状である。そのため，現在 Spam の傾向・特徴ごとに Spam メールを分類し，Spam フィルタの定義の自動化の可能性について検討している。また，Spam と誤認識したメールがないかどうかのチェックについても現在は目視で検索していて，これも非常に手間がかかっている。そこで 1 日に一度，隔離した Spam と疑われるメールの一覧（Subject，From，To）をユーザごとに作成し，それをユーザに送信し，ユーザに Spam かどうかの判断を任せる方法を考案中である。この方法のメリットとしては，もちろん管理者の負担が減ることが上げられるが，その他に，ユーザには多数の Spam と思われるメールの情報が一通で届くため，大事なメールを見落とす可能性を減らすことができると考えている。

またウイルス対策に関しては，現在はコンテンツフィルタの導入により，外部からのウイルスメールの大部分から防御することに成功している。しかしながら，学内のユーザが ISP などの外部 POP サーバからメールを受信し，その中にウイルスメールが含まれていて感染した場合，学内にウイルスを蔓延させてしまう危険性がある。IMSS は POP3 に対応しているため，それを防ぐために，IMSS を経由して外部メールサーバからメールを受信するように，ユーザに指導している。ただし，このシステムは POP3 にしか対応していないため，POP3 以外のプロトコルを使用しているユーザには，できるだけ学内のメールアドレスに転送をかけて，受信するよう指導している。