メール処理システム
- spam メール及びコンピュータウイルス対策への取り組み -

松原義継*

1 はじめに

本センターがインターネットに接続されてから 15 年以上が経過しているが，その当初からインターネットにおけるコミュニケーション手段として電子メール (以下，“ メール ” で表記) が使われている．1994 年にインターネットが一般に開放されたのに伴い，メールも一般に普及し，携帯電話がメール機能を持ったことで その普及は留まるところを知らない．

本大学においても，一部の関係者だけで利用されていたメールが，今では全学の教職員及び学生に対して，その研究，教育，そして業務において，当然のように利用されるようになっている．極端な話，メールなしには何も出来ない状況になりつつある．

その一方で，メールの普及は新たな問題を生ずる事となった．メールは 低コストで世界中のどことでもやり取りできること，基本的に文章及び添付ファイルだけのコミュニケーションであり 相手の顔が見えないこと，そしてメールの配送規約が 25 年前から基本的に変わっておらず [1, 2]，現在から見れば不備があることから，それらを悪用したメールも普及するばかりである．当初はメールの書き方が原因で相手とトラブルになることが主たる問題だったが，やがてコンピュータウイルス (以下，“ ウイルス ” で表記) 付きのメールが世界中から配送されることで自分のパソコンがそれに感染する問題がクローズアップされてきた．そして，ドラッグの販売やアダルトサイトへの勧誘，金融機関を装ってクレジット番号や口座の暗証番号を盗むフィッシングメール等の spam メールと総称されるメールが世界中から配送されることで，それらが原因の刑事事件がマスコミで報道されるようになっている．

本センターでは，このような問題に対応するため，対ウイルス及び対 spam メールのサーバ群を導入している．当初は単にメールを送受信するだけだったメール処理システムが，それらサーバ群の導入により 全体としては かなり大規模化している．それに伴い，このシステムを維持するための資源的コスト及び人的コストが膨らむばかりであり，「メールは 24 時間使えて当然」という状況下で，その対応に苦慮しているのが実態である．

一般ユーザが そのシステムの全体像を知る機会が少ないため，「自分がメールを相手から受け取ったり，逆に自分が配送したメールが相手に届くまでに何が起きているのか？」を知っている方々は少ない．そこで，その全体像を広く知って頂き，本センターのウイルス及び spam メールに対する取り組みをご理解頂きたく，今回それを紹介する．

2 歴史的経緯

本センターでは，元々は研究用メールサーバ及び教育用メールサーバの 2 台によるメールシステムを運用していた．

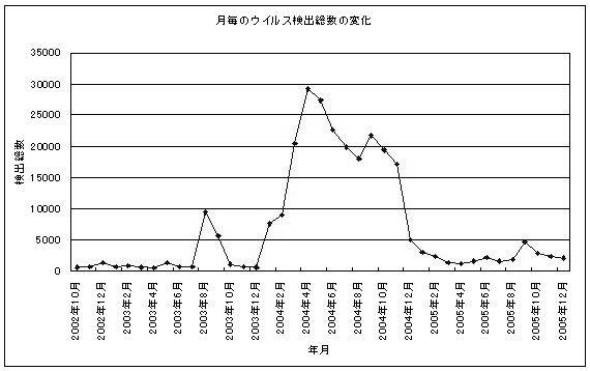
2002 年になった頃から，添付ファイルの付いた身に覚えのないメールが目に付くようになり，次第にその量が増えていった．その添付ファイルは実行形式のファイルであり，これがウイルスである．パソコン用の対ウイルスソフトが市販されてはいたが，学内に設置されている全パソコンにそれをインストールさせ，ウイルス定義の定期更新を行わせる

* E-mail: matubara@cc.saga-u.ac.jp

のは現実問題として難しかった．そこで，対ウイルス用の専用機を導入して，メールサーバに配送される前段階でメールをフィルタリングすることにした．同時に，本センターだけウイルス対策を行っても，他学部学科のメールサーバ宛のメールが素通しでは全学レベルでのウイルス対策として不完全である．そこで，他学部学科にお願いして，このサーバを経由してメールを配送させるように配送経路を変更して頂いた．

しかしながら，ウイルス付きメールの量の増大に専用機の処理能力が追いつかず，なおかつ，配送先メールアドレス及び送信元メールアドレス共に不明でどこにも配送できないメールがこのサーバの中で溜まり続け，メールサービスに支障が出てきた．そこで，対ウイルス用サーバを 2 台に増設し，なおかつ，メール配送を中継するサーバを 2 台用意して，対ウイルス用サーバは純粋にウイルス付きメールをフィルタリングするだけにした．そして，各メールサーバへの配送 及び どこにも配送できないメールの溜まり場確保として，この中継用サーバを運用している．

このサーバを導入してから今日までのウイルス検出状況を図 2 に示す．



2004 年に入ったら，今度はドラッグの販売メールやアダルトサイトの勧誘メールが目に付くようになってきた．これが今で言う spam メールである．spam メール自身は 10 年程前から存在していたようである [3]．だが，今まで目に付くようなことはなかった．

spam メールの量は増える一方であり，著者の場合，1 日に受け取るメールの約 4 割は spam メールであった．そこで，対 spam メール用サーバの導入を決定し，2004 年 11 月末に そのためのサーバ 2 台を導入した．

それと併せて，学内からウイルス付きメールが配送される可能性を考慮し，学内から学内外へ配送されるメールに対しても対ウイルス用サーバ 1 台と中継用サーバ 1 台を運用して今日に至っている．

3 全体像

2006 年 1 月時点におけるメール処理システムの全体図を図 1 に示す．

大きく以下のように分けられる．

- 学外から学内へ配送されるメールの処理
- 学内から学内外へ配送されるメールの処理
- 配送記録

3.1 学外から学内へ配送されるメールの処理

この場合, 処理の手順は, spam メールフィルタリング → ウイルスフィルタリング → 各メールサーバへ中継，となる．

3.1.1 spam メールフィルタリング

学外から学内に配送される場合，最初に対 spam メール用サーバによる spam メールフィルタリングが行われる．学内からのメールの一部が これらサーバに配送されるが，その場合は spam メールフィルタリングを行わずに，素通しで対ウイルス用サーバに配送させている．従って，spam メールフィルタリングは，学外から学内宛のメールのみに対して行われている．

サーバ台数は 2 台あり，負荷分散のために どちらか 1 台にランダムに配送される．

現在，行っている spam メールフィルタリング方式は「greylisting」と呼ばれるものである．spam メールの性質の 1 つに, その配送に対して一旦「待った」をかけると，再配送してこないことが多いというものがある．普通は，配送する側のサーバが しばらく待った後に再配送してくる．再配送された場合は，一定期間配送を素通しする．本センターの場

合，この素通しの期間は 1 週間である．1 週間経てば，再び「待った」がかけられる．もし，何かしらの理由で再配送ができなければ，配送した本人に そのメールが差し戻される．spam メールはインターネットにおけるダイレクトメールのようなものであり，それは不特定多数の人たちに送り付けられる．この性質上，「待った」のかかったメールを再配送するよりかは，次の相手にメールを送ったほうが，その目的を達成できる．これを逆手にとり，意図的に「待った」をかけて spam メールの配送を抑止するのが，greylisting である．

本センターで導入している greylisting のソフトウェアは メール配送ソフトとして古くから存在する Sendmail[4] 用の milter-greylist[5] である．サーバの構成は，ハードウェアが 米 Sun Microsystems 社 [6] の Sun Fire V120，OS は 同社の Solaris9 及び Solaris10 である．

運用経験上，処理したメール全体で学内に配送されるのは 4 割程である．残り 6 割程は，「待った」に対して配送元からの再配送が行われていない．まれに，普通のメールが この「待った」によって配送が止まってしまう事例が報告されている．この原因は，「待った」がかかった側のサーバが，その運用方針により再配送を早々に止めてしまう場合があるからである．このような場合，メールの送信者もしくは組織を信用して そこからのメールを素通しするか，spam メールを受けるのを覚悟で受信者宛のメールを素通しさせることを行っている．前者の場合，spam メールが身元を偽ることもあり， メインセンターでは 原則として 後者で お願いしている．

時々，spam メールが「待った」に対して再配送される事例も確認しているが，この付近は新たな spam メール対策を追加する等の今後の課題である．

3.1.2 ウイルスフィルタリング

対 spam メールサーバを通過したメールは，今度は対ウイルスサーバによるウイルスの添付が確認される．もし，ウイルスが添付されていれば，ここでそれを除去する．

サーバの構成は，米 McAfee 社 [7] の専用機 Webshield Appliance E500 である．これを 2 台用意して，負荷分散運用を行っている．ウイルス定義ファイルの更新は 1 時間毎に行い，新種のウイルスがここをすり抜けないように可能な限り務めている．

3.1.3 各メールサーバへの中継

ここでは，各メールサーバへの中継及び，何かしらの原因で中継が止まった場合のメールの保留が行われる．

サーバの構成は，ハードウェアが 米 Sun Microsystems 社 [6] の Sun Fire V120，OS は 同社の Solaris9 である．これを 2 台用意して，負荷分散運用を行っている．

中継先のメールサーバに障害が起きて配送ができない場合は，ここで配送が保留され障害の回復を待つ．メールの中には，送信者メールアドレス及び受信者メールアドレス共に存在しないという，メールの利用上 不適切なものがある．卒業生のように，かつて存在していたユーザ宛に配送されるだけならば，送信者メールアドレスへ差し戻されるだけなので あまり問題とはしない．問題は，送信者メールアドレスが存在しない場合であり，単に入力ミスなのか あるいは悪意を持った詐称の可能性がある．悪意を持った送信者メールアドレスの詐称は，身元の特定を困難にすることが意図されており，メールの健全な利用にとって深刻な問題である．保留メール数が多すぎると，メール配送がここで詰まってしまい，場合によっては管理者が手動で強制削除等を行う．今のところ，その送信者メールアドレスが本当に存在することを配送前に確認する方法がないので，今後の技術の進歩に期待したい．

3.2 学内から学内外へ配送されるメールの処理

学内から配送されたメールは，対ウイルス用サーバによるウイルスフィルタリングが行われる．ウイルスに感染したファイルをディスクもしくはパソコンで持ち込んだ場合，学内からウイルスが広がることになり，先のメール処理では効力を発揮しない．この場合，本大学が学外から加害者扱いされる可能性もあり，学術機関としての信用問題になる．そこで，学内から配送されるメールもウイルスフィルタリングが行われる．

サーバの構成は，先の場合と同じ米 McAfee 社の専用機 Webshield Appliance E500 であり，1 台で運用している．ウイルス定義ファイルの更新は先と同じく 1 時間毎である．学内宛のメールはここから直接配送されるか中継用サーバに配送される．学外宛のメールは，全て中継用サーバに配送される．

中継用サーバの構成は，ハードウェアが 米 Sun Microsystems 社の Sun Fire V120，OS は 同社の Solaris9 であり，1 台で運用している．宛先のメールサーバに何かしらの障害が発生して配送できない場合は，ここで保留され，障害の回復を待つ．

3.3 配送記録

対 spam メール用サーバ群，そして中継用メールサーバ群におけるメール配送記録及び対ウイルス用サーバ群におけるウイルス検出記録は，配送記録用サーバに記録される．マシンの構成は，ハードウェアが 米 Dell 社の 1UPC サーバで，OS は FreeBSD 5.2.1 である．

メール配送記録の内容は，各サーバ群におけるローカルな記録先である syslog の内容そのままである．

対ウイルス用サーバがウイルスを検出した場合の記録内容は，検出日及びウイルス名である．月一回管理者は これを集計することで，先に示した図 2 を作成する．

4 メールの処理量

本システムで処理されるメールの量は，配送記録を見る限りだと 月平均 100 万通程である．本センターに登録されているユーザ数は約 1 万であるので，月平均 100 万通程を単純に一人月平均で割ると 3, 4 通になる．一人単位で見ると，配送量は決して多くないと思われるが，ユーザ全体のメールを処理するため，本システムは常に高負荷状態である．「よく持ち堪えているなあ」というのが管理に携わる立場としての率直な感想である．

この数字には本センターのメールサーバ内だけのローカルなメール配送が含まれなし，他学部学科内部だけのメール配送も含まれないので，大学全体としてはこれ以上の量のメールが処理されていることになる．

spam メール及びウイルス付メールは今も途絶えることなく配送されており，本センターはこれらの配送を止めるために日々努力している．これらの対策のために皆様にご迷惑をおかけすることもあるが，何卒ご理解頂きたいと思う．

参考文献

[1] J. Postel. Simple Mail Transfer Protocol. RFC821, August 1982.

[2] D. Crocker. Standard for the format of ARPA Internet text messages. RFC822, August 1982.

[3] 山本和彦. spam からメールを守れ（ユーザ編） — 第 1 回：spam の歴史と分類 —. http://www.rbbtoday.com/column/spam/20041201/.

[4] Sendmail.org. Sendmail home page. http://www.sendmail.org/.

[5] Milter-greylist.org. Milter-greylist home page. http://hcpnet.free.fr/milter-greylist/.

[6] Sun Microsystems, Inc. Sun microsystems home page. http://www.sun.com/.

[7] McAfee Co., Ltd. Mcafee home page. http://www.mcafee.com/.

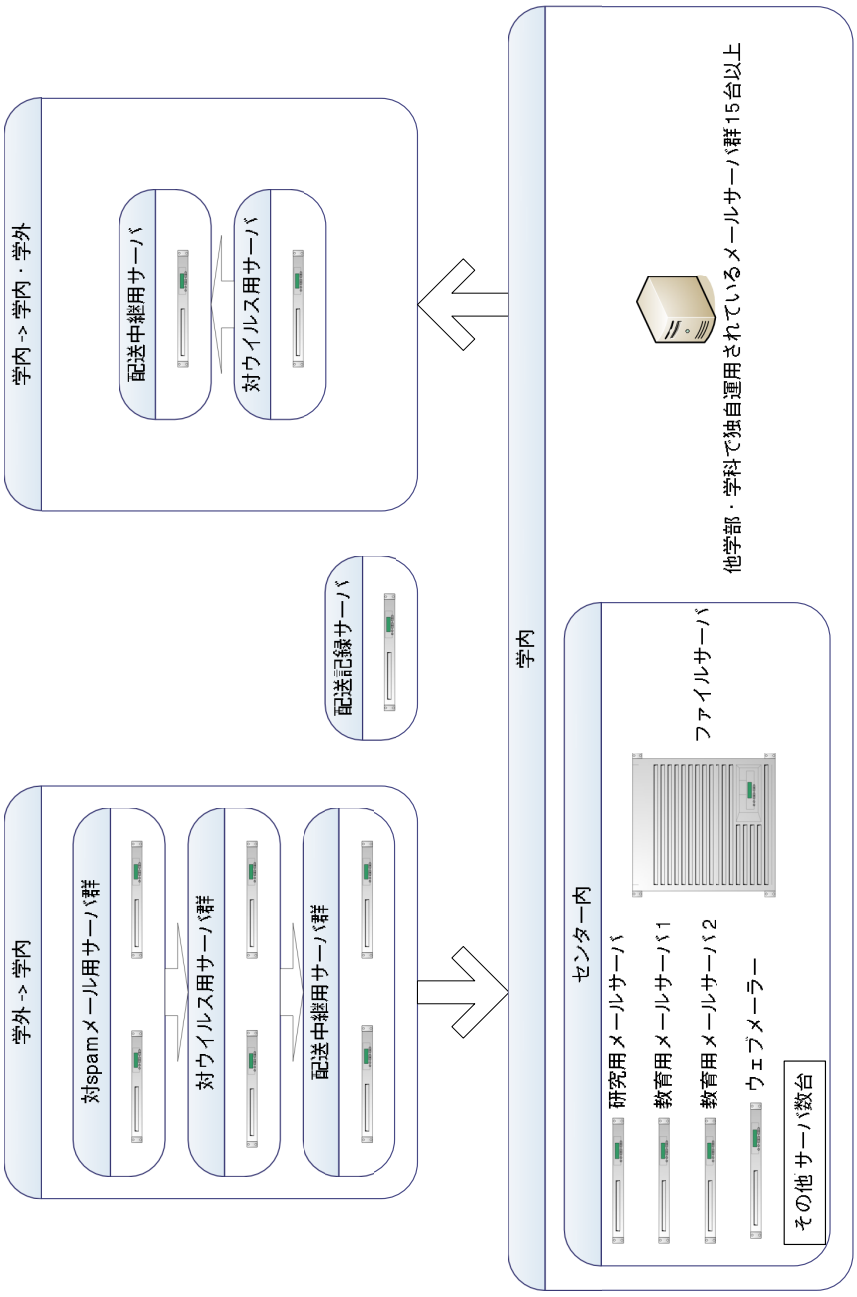

学外 -> 学内
対spamメール用サーバ群
対ウイルス用サーバ群
配送中継用サーバ群
配送記録サーバ
学内 -> 学内・学外
配送中継用サーバ
対ウイルス用サーバ
学内
センター内
研究用メールサーバ
教育用メールサーバ1
教育用メールサーバ2
ウェブメーラー
その他 サーバ数台
ファイルサーバ
他学部・学科で独自運用されているメールサーバ群15台以上

図1　システム概要図