本学迷惑メール防止装置の運用実績と効果について

三　谷　和　史

はじめに

本学におけるメール利用環境の変遷を，電子メールの歴史と共に概観し，更には前回システム更新時より本学に導入された迷惑メール防止装置の運用実績と効果について一個人としての立場で大雑把に検証を試みる。さらには装置運用に関しての問題点やトラブルについて考察を行う。

電子メールの歴史と本学におけるメール利用環境の変遷

電子メールの歴史

電子メールの歴史は大きく3つに分けられる。1台のホスト上で他のユーザとメッセージ交換ができた時代，同一機種間でネットワークを経由してメッセージ交換ができた時代，そして異機種間で初期にはFTPのコマンドを使い，その後はSMTPを使ってメッセージ交換ができる時代となろう。

1960年代のコンピュータはTSS（Time Sharing System）によって複数のユーザが同時に1台の計算機を共用していた時代であった。そこで同じ計算機を利用している他のユーザに対してメッセージを計算機上のファイルとして置いておき，後に相手がそのファイルを見ることによってメッセージのやり取りを行うという原始的な方法が発展していったものが，電子メールとなってゆく。

コンピュータ上のメールやメッセージはおそらく何度も独立して発明されており，いつ誰が最初に発明したかは定かではない。

TSSの例としては，MIT Project MACのCTSS（Compatible Time-Sharing System）が1961年から使用されていた。The First Network Email by Ray Tomlinson[1]によれば，1965年以前には電子メールは存在しなかった模様である。1964年の12月もしくは1965年の1月にメッセージを他のユーザに送るコマンドが計画された模様だが実装はされていなかった。それを，1965年の夏にNoel MorrisとTom Van Vleckが実装したMAILコマンドが一つの始まりとなる。メールはTSS上の他のユーザ所有のファイルに書き込むため，特権が必要なプログラムとなる。

史上最初のspamと言われる1978年のDEC Spam[2]以前の1971年には，既に長文の反戦spamをCTSSの全ユーザに送りつける事例が起きていた。複数人に対して同時にメールを送ることができるようになれば，当然このようなことが起こり得るであろうという証左と言えよう。

他のOSでも，一つのシステム内でメールを送るためのコマンドが作成されてきた。

次に，コンピュータネットワークの発達に伴って電子メールがどのように進化したかを辿ってみる。

先の資料や［1］，［2］，ワシントンポスト紙2012年3月20日付けのA history of e-mail：Collaboration, innovation and the birth of a system by David Crocker[3]そして，The History of Electronic Mail by Tom Van Vleck[4]によると，ARPANETの計画段階からJ.C.R.Licklideはコンピュータ間のメールにも言及していた。

1971年7月20日付けのRFC196［3］に“Mail Box Protocol”とあるが，実際にデプロイはしなかった。

1）https://openmap.bbn.com/~tomlinso/ray/firstemailframe.html
2）http://www.templetons.com/brad/spamreact.html
3）https://goo.gl/eMbFeB（長いため短縮形を利用）
4）http://www.multicians.org/thvv/mail-history.html

ネットワークを介した電子メールは，BBN[5]のRay Tomlinsonの手によるものが最初である[6]。彼は1971年末にARPANETで接続されたDEC PDP-10のTENEX間でNCPを使ってファイルを転送するためのプログラムCPYNETを作成した。

続いて彼は，１台のPDP-10のTENEX上でのユーザ間の文書送信のためのSNDMSGプログラムを作成した。その後RFC196を読んだ彼は，SNDMSGとCPYNETを組み合わせると，別のTENEXのメールボックスにメッセージを追加できることを思いついた。そして，SNDMSGを拡張してメッセージを読むためのプログラムのREADMAILを実装し，ARPANET上の他のTENEXとの間でメールが使えるようにした。SNDMSGはリモートホストのメールを送る相手のメールボックスの位置を送信者が知っている必要があった。また，彼はSNDMSGのメールアドレスに@を使うことを定めた。1973年３月のTENEXのリリースにSNDMSG，READMAILが組み込まれた。READMAILは使いにくかったので，後にLawrence G. RobertsがTECOのマクロを使用したユーザ用のRDコマンドを作成しそれが広まった。

1971年の10月にはMULTICSがARPANETに接続している。そして1972年の初めには，Mike Padlipsky率いるProject MAC networking groupの手によって他のMULTICSシステムとの間でメールが使えるようになっていた。宛先には-atを用いていたが，これは@が端末のline kill文字として使われていたためであった。また，他のユーザのファイルに書き込むための特権の必要性もMULTICSでは問題となった。

当時は，同じOS間でメールがやり取りできるようになった時期であり，その方法もOS固有であった。

次に，異なるOS間でもメールのやり取りがしたいという要求に応えて，MITのAbhay Bhushan等が開発していたFTPの拡張による実現が検討されて

5）現在のBBN Technologies（www.bbn.com）
6）http://history-computer.com/Internet/Maturing/Tomlinson.html

いた。

1972年7月のRFC354［4］でFTPにAPPENDコマンドを追加してメールを実現するとしていたが，1972年8月18日付けのRFC385［5］では，FTPに対してMLFL（Mail File）とMAILコマンドの追加が提案された。TENEXのSNDMSGは1972年秋にBBNのRobert ClementsによってMLFLに対応した。CTSSもこれに対応し，最初の異機種間のメールはCTSSとTENEXの間で行われた。

また，MULTICSにもFTPに対応したNETMLが実装され，異機種間でのメール転送が拡大していった。その後，1973年2月の会合でメールのアドレスに@を用いることと，FTPにTOコマンドを追加することで合意が得られ，RFC469［6］で現在のuser@hostの形式が定まった。

TomlinsonはBhushanと共にメール・ヘッダの標準化に取り組み，RFC561［7］を1973年9月に発表した。ここでは，FROM，SUBJECT，DATEの情報を最初に記述することとし，まだTOフィールドがなかった。

TENEXのRDはその後複数の人々によって書き直され，NRD（Barry D. Wessler），WRD/BANANARD（Marty Yonke），MSG（John Vittal）と進化し，1975年頃から現在でいうメーラーの機能をもつようになっていった。CCやBCCもこの頃 John Vittal によって考案された。

A Personal view：Impact of Email Work at The Rand Corporation in the mid-1970's by D. Crocker[7]は当時の様子が判る小文である。

Wikipediaによれば，1973年にはARPANETの75％のトラフィックがメールであったという。

さらに多くのホストがARPANETに接続されてくると，別のメールの考え方が生まれてきた。Mail Transfer Agent（MTA）というものがメールを他のMTAへ転送してゆき，受信者のホストがネットワークに接続した時点でメールを配送するモデルである。

7）http://bbiw.net/articles/rand-email.pdf

このモデルに基づいて，1980年９月にRFC772［8］によるMTPの提案から２度の改訂を経て，1982年８月にSMTP（RFC821［9］，RFC2821［10］，現在RFC5321［11］）が作られ，現在のインターネットにおけるメールの転送プロトコルの標準となっている。

1970年代後半から1980年代に入ると，ARPANET以外にもコンピュータネットワークが形成され，そこでもメールが使用されていた。

UUCPはUNIXの本家であるAT＆Tが1976年に作成し，1977年から配布された。これは，電話線とモデムを使って，間歇的に接続相手にデータと実行すべきコマンドを送って，それを相手に実行してもらうものである。この仕組みを使ってSteve Bellovin, Tom Truscott, Jim Ellisが1979年にUSENET[8)]を始めた。そこでは，バケツリレー方式でメールとNetNEWSが送られた。メールのアドレスは経由するUUCPのホスト名を“！”で繋ぐ，BANG形式が基本であった。

CSNETは1981年からアメリカ国立科学財団の資金を得て設立され，ARPANETに接続できない学術研究組織によって使用された。CSNETではMMDF（the Multichannel Memorandum Distribution Facility）がメールシステムとなった。回線は初期には56Kbpsで，X.25が使われていた。

IBM系のメインフレームを使ったBITNETも1981年から運用が開始され，E. Alan CrosswellによるMAILER MTAが多く使われていた。これは，専用線を介したIBMのRSCSプロトコルを使用したもので，バケツリレー型のものであった。1989年にはCSNETとBITNETは統合されてCRENとなった。

また，DEC独自のDECNETではMAIL-11が使用され，アドレスの形式が“host::user”というものであった。

1980年代中頃から，これらのネットワークの間で中継ホストを経由することでメールが相互に送受信できるようになってきた。

8）https://en.wikipedia.org/wiki/Usenet

sendmail

sendmailはEric Allman（当時UCB）がARPANETのメール接続用にBSD UNIX上で作成したdelivermailを元に1980年代初頭に作成したMTAである。delivermailはTCP/IP以前のARPANETのNCPをネットワークプロトコルとして使用し，FTPプロトコルを使ったMTAであり，1979年に4.0及び4.1BSDで配布された。TCP/IPネットワーク上でSMTPを使いDNSをホスト名の解決に使うsendmailは1983年に4.1cBSDで配布された。

当時は様々な電子メールプロトコルとその実装システムがあり，sendmailは各種プロトコルの相互変換が可能なMTAとして作られているため，設定ファイルはオートマトンとなっておりかなり難解なものであった。また，セキュリティホールも多数見つかった。特に1988年11月2日にsendmail等の既知の脆弱性を使って起こされたMorris wormは，全世界の約6000台のUNIXマシンが影響を受けた。このworm本体はBSD4.xが動作するVAXとSun-3がターゲットであった。当時のインターネットに接続していたコンピュータの10％程度が被害を被った。

1996年の調査ではMTAの80％であったsendmailの比率が，2015年8月には24％，2017年3月には5.06％となっている[9)]。

Allmanは1998年3月にSendmail社を立ち上げ，2003年2月には日本法人も設立された。Open Source版のsendmailの他に，商用版としてsendmailが組込まれたアプライアンスのSentrionが販売され，本学でも前回のメールシステム更新時に導入している。

しかしながら，2013年10月にSendmail社は米セキュリティ会社のProofpointに買収された。現在のOpen Source版のsendmailは8.15.2（2015/7/3）である。

9）https://goo.gl/9gMPzu

JUNETから始まる日本のインターネットの歴史

USENETと同様の仕組は，日本では1984年８月に慶應大学から東京工業大学に異動した村井純が，同年９月に300bpsのモデムで慶應大学と東京工業大学を接続したのが始めといわれる。その後10月には東京大学の石田晴久先生の所とも接続を行い，後にJUNETと呼ばれるネットワークが動き出した［12］。

そこからJUNETが広がってゆく過程は，人同士の繋がりによる所が大きかった。また，そこで使われているOSがUNIXであることから，1983年６月に設立された日本UNIXユーザ会（jus[10)]）の役割も大きかった。

さらには，国内に広くJUNETによる接続が可能であったのは，NTTの通信研究所がハブとなって，遠隔地域の拠点に対してUUCPのpollingを行ってくれた点も大きい。当時の遠距離電話料金は高額であり，研究所から発呼する接続に対しては社内的に課金を行わないので，遠隔拠点組織は外線電話の基本料金だけでハブとの接続が行えた[11)]。

JUNETは当初.JUNETというドメイン名を用いていた。その後1989年４月に.JPへの移行が行われた。メールアドレスは，UUCPで経由するホスト名を！で連ねて記述するBANG形式ではなく，最初からドメイン形式のメールアドレスを使っていた。そのため，UUCP接続で上流下流の概念があり，UUCPホストは自分の下流にあるドメインについて全て把握してsendmailの設定ファイルに記述し，そのドメイン宛のメールをUUCPで送信する。また，それ以外の宛先へのメールは自分の上流に送信することでメールの配送を行っていた。そのため，国内全部のドメインの情報を持ったドメインマスタが最上位に必要であった。東工大のtittcaと東大のccutがドメインマスタとして機能していたが，1991年３月でtittcaが廃止，７月にccutもDNSへ移行し，この後DNSを使った

10）http://www.jus.or.jp

11）当時は武蔵野通研のnttlabというマシンが国内接続のハブとなり，後藤滋樹氏や野島久雄氏等が切り盛りしていた。野島氏は研究所を退職した後，成城大学で2005年より認知科学を教授していたが，惜しくも2011年に逝去した。

名前解決によるメール配送となった。

80年代の終わりから90年代の初めにかけて，研究系のIPネットワーク（WIDE, JAIN, TISN, HEPnet-J, JOIN, SINET）や，地域系のネットワーク（TRAIN, KARRN, NORTH, TiA, RIC-Tsukuba, ORIONS, WINC, CSI, TRENDY, TOPIC, NCA5）が誕生し，それらに参加できない組織がJUNET協会（1992年10月設立1994年10月解散）としてUUCPで繋がる形で日本のネットワークは拡大していった。1992年から93年にかけてはAT&T JensやIIJ，東京インターネットといった民間プロバイダが誕生して，更にユーザ数が加速した。

一部のUUCP接続組織等が海外にメールを出すためには，当時KDDの研究所が行っていたInetClubに加入して通信費を支払っていた。これは1987年5月から1994年12月まで存在し，その後はISPに引き継がれていった。

国内のネットワークとしては，所謂パソコン通信と呼ばれたサービスも存在した。PC-VANとASCII-NETは1986年から，NIFTY-Serveは1987年からサービスを開始しており，メールもサービスされていた。

これらパソコン通信とインターネットのメールの接続も実験的に開始された。WIDEは1992年9月からPC-VAN, NIFTY-Serve, ASCII-NETと接続実験を開始し［13］，接続範囲を徐々に広げて1993年2月にはJAINの一部まで，1993年5月にはjpとメールの相互接続が可能となった。また，SINETでは1993年5月よりPC-VAN, NIFTY-Serveとメールの交換を開始した。

これら日本でのインターネット及びその前史については，ある程度の情報が流布している。吉村氏による記事[12)]や渡邊氏によるJUNETとfjの記念碑[13)]が判りやすい。

12）https://portal.graphy.co.jp/?p=264
13）http://katsu.watanabe.name/doc/monument-junetfj.html

本道，本学におけるネットワークの歴史

本道や本学におけるコンピュータネットワークの歴史についてはあまり情報がないのが現状である。

道内では，1985年に慶應義塾大学工学部管理工学科より北海道大学文学部行動科学科へ異動してこられた安西祐一郎助教授が，最初にJUNETへの接続を行った。安西先生が村井純と知り合いであったため接続が実現した。使用したのは，戸田正直教授のNENEプロジェクトで使用していたVAX11/750で，telebit社のモデムであるトレイルブレイザーを使って，4.2BSDがOSとして稼働していたのではないかと推測される。また，北大のドメイン名としてhokudai.junetを決めたのは安西先生で，hubs.hokudai.junetがホスト名であったと記憶する。その後，junetドメインからac.jpドメインへの変更時，ドメイン名を変えることができたが，そのままhokudai.ac.jpとしたのは筆者である。

その後VAXが壊れ，直す資金もなかったため接続は途絶えていた。安西先生はその後1988年に慶應義塾大学理工学部電気工学科に異動し，後に慶應義塾大学の塾長となり，現在は日本学術振興会理事長等の役職を務めている。

その後，接続が途絶えていたJUNETを，当時北大工学部情報工学専攻に所属していた筆者が引き継ぎ，全道に広めていくこととなった。1987年９月に情報処理学会第35回全国大会が北大で開催され，その折にJUNETのBoF[14)]を開催するので場所を用意するように，という指令が村井純から筆者に下ったのが出会いであった。当時北大工学部に情報工学科ができたばかりで，学科の計算機室に設置された富士通の汎用機M340Rの上で稼働していた米国アムダール社製のUTSというSystemV系のUNIXを使ってのJUNET接続であった。clark.huie.hokudai.junetがホスト名であった。このOSによる接続については，当時九州大学情報処理教育センターの藤村直美先生の御助力を頂いた。また，この

14）Birds of a Feather。元はBirds of a feather flock together（類は友を呼ぶ）より。通常なんらかの会合の合間等に非公式かつ臨時的に関係者が集まって情報交換や議論をすること。インターネット関係で使われる。

ために筆者の属していた講座で外線電話を新たに1本引くことを事務方と折衝して認めてもらい，JUNET用にtelebit社のモデム，トレイルブレイザーも購入した。当時はJUNET特別価格で30万円であった。しかし，M340Rではこのモデムが使えず，最初は富士通製の1200bpsのモデム，次に2400bpsのモデムで接続していた。その後，Apollo社のアポロドメインDN3000を接続マシンに使用するようになって，トレイルブレイザーが利用できるようになった。wsclark.huie.hokudai.ac.jpがホスト名であった。ホスト名のclarkはクラーク博士から取り，wsはワークステーションになったので追加してみると，William Smith Clarkと丁度かさなり語呂がよかったため採用し，その後マシンが変わってもこの名前を使い続けている。これら，道内におけるネットワークの歴史については稿を改めて述べる予定である。

本学も北大と接続した組織のひとつである。当時，情報処理センター長で管理科学科の若林伸夫先生（故人）が接続の担当であり，必要な設定をOSのファイルに書き込むために，電話でviエディタのコマンドを筆者が口伝しながら打ち込ませたがうまく行かず，当時北大情報工学専攻の大学院生であった南弘征君を何度かアルバイトに出して接続に成功した。これが，1989年の12月22日で，本学のマシンはSUN3で，使用したモデムはtelebit社のトレイルブレイザーTB2000で，ホスト名はsnotaru.otaru-uc.ac.jpであった。

その後，北大はJAIN[15]によってインターネットへのIP接続を果たしたが，速度的にはX.25の48kbps，後に64kbpksであった。X.25接続のためのネットワークスタックはWIDEプロジェクトが作成したものを使用していた。北大大型計算機センターのcyntia.cc.hokudai.ac.jpがその任を負って，当時同センターにおられた山本強助教授と筆者が運用に当たっていた。山本先生はこのプロトコルスタックに潜むmbuf絡みの致命的なバグを炙り出して直された。

15）Japan Academic Inter-university Network. 科研費プロジェクト。（総合研究A：高度学術インターネットワークの構築と高度応用技術の研究，代表：野口正一東北大学教授）

当時の本学の学内ネットワークの様子は，若林先生の論文［14］で伺うことができる。それによると，本学では1989年１月に計算センターが情報処理センターに改組され，10MbpsのEthernetによる学内ネットワークが構築された。JUNETに接続したのが同年の秋から冬にかけてであり，学外と電子メールが通じるようになった。1990年秋にはNetNewsが学内にも導入され，北大からNetNewsの配送が開始された。1991年にはインターネットへの接続の検討を始め，７月には150.83.0.0/16のIPアドレスを取得し，11月からJAINへの参加という形でX.25でのIP接続が開始された。北大との間は64KbpsのX.25であったが，ソフトウェアとモデムの制限で実質9.6Kbps程度の速度であった。JAINの終了に伴い，1993年３月末にSINETへの接続に移行した。1992年６月まで学内で運用していたNetNewsは廃止している。

また，1991年度のWIDEプロジェクトの報告書［15］によれば，計算機関連学科の学部学生のInternet accessに関する調査に，本学は「no Global mail, no news責任を伴う。卒業後のaccessについての諸問題（security）など考慮。」と回答しており，学生が自由に利用できる環境ではなかったことが伺える。

その後，南氏は1994年４月に本学に採用され，2000年に北大へ異動して，現在は北大情報基盤センターのサイバーセキュリティ研究部門で活躍している。本学から出て行くメールのドメインをotaru-uc.ac.jpに限定した設定をsendmail.cfに導入したのは同氏であった。

尚，本学でユーザがメールを読み書きするためのMUA（Message User Agent），所謂メールクライアントとして標準的に使われてきたのは，1992, 3年頃からJR総研と本学中村隆志先生（現名誉教授）の共同開発によるアルメール，次に1995年頃からAL-Mail[16]，その後2003年頃からMozillaのThunderbird[17]を標準とし，学生はActive! Mailに移行した。2003年以前はPOP3で，2003年から

16）http://www.almail.com/
17）https://www.mozilla.org/ja/thunderbird/

はPOP3に加えてIMAP4でもサービスを行ったので，対応するメールクライアントであれば使用することができた。

迷惑メール防止装置の導入

本学では，現システムの4代前より，ウィルス付きのメールをチェックして排除するための装置が導入され，学内にメール経由で既存のウィルスが侵入することを防いできた。これは現在でも変わりなく行われている。

ウィルス付きのメールを排除しても，所謂スパムと呼ばれる不要なメールは教職員や学生のメールボックスに届き，その処理に無駄な時間と資源が費やされていた。そこで，前回2010年の情報処理センターのシステム更新時に，迷惑メール防止装置を導入してはどうかと進言して，認められることとなった。

前回のシステム更新時に本学に導入されたのは，sendmail社のSentrion MP4/8が2台構成で，スパムフィルタリングには，米国Cloudmark社の製品を搭載していた。これは，当時米国や日本の大手のISP等でも多く採用されていたフィルタリングサービスであり，sendmailで良く利用されるコンテンツマッチング規則に基づいたスパムフィルタリングプログラムであるSpamAssassinのプラグインとして動作する。Cloudmark社はSpamAssassinの初期開発メンバーの一人であるVipul Prakash氏等によって2001年に設立され，2009年には日本支社も置かれた。当時の小島國照支社長は前職がsendmailの日本支社長で，両社の関係が深いことがわかる。また，Sentrion上でMcAfee社製Anti-Virusモジュールを用いてウィルスチェックも行っていた。同時に，本学の構成員がメールを送信する際のsubmissionサーバとしての役割もSentrionが果たしており，その際にユーザの認証とコンテンツのチェックを行いウィルスやスパムの排除を行なった。

このフィルタは，独自のフィンガープリント技術に基づき，間違いが少なく処理速度が非常に速いのが特徴である。また，スパムと認識するためにスパムメールをCloudmark社に添付ファイルとして送ることで，素早いフィルタの更

新が行われる。通常45秒毎に新しいスパム情報が送られてくる。また，誤判定に対しては，スパムではない旨をCloudmark社に添付ファイルとして送ることでスパムからの解除を求めることができる。本学では，情報処理センター関係者（含む筆者）がこの作業を行っていた。

この２台の装置は，DNSのメール配送用のMXの数値を異なる値として，一方をプライマリ，他方をセカンダリとして運用した。理由は定かではないが，スパム送信者はMX値の大きなセカンダリからメールを送り込む傾向も見られた。また，送られてきたメールをスプーリングして教職員にPOP3やIMAP4を介して提供するためのサーバとして，Sentrionとは別にpopという名前のサーバがあり，Sentrionからpopに対してメールを送りpopがスプールする体制を取った。更に，本学はSINET以外に北電のHOTnetとも接続しており，学外から本学にメールを送るときに参照されるIPアドレスはradware社のマルチホーミング製品であるLinkProofを使ってHOTnet側も使えるようにしてあった。

後に露呈したこの構成の問題点は，popサーバに対してSentrionからメールを配送する際，DNSを参照して名前解決を行っていた点である。これに関しては後で述べる。

Sentrionの効果

mstore@caspi.otaru-uc.ac.jpから毎日Quarantine mailbox summary notifica-tionという件名で隔離ボックスの状況が送られてきた。そこから情報を取り出すこととする。筆者宛の情報から，

```
egrep -a ', you have |additional' | egrep 'message|As'
```

によって，日付と隔離ボックス中の迷惑メールの数，新規の迷惑メールの数の行を集め，

```
tr -d '\r' |  sed -e 'N;s/\n/,/g;' | sed -e 's/As of ..., //' \
-e 's/ ..:..:.. +0900//' -e 's/ you have //' \
-e 's/messages in your quarantine mailbox. //' \
-e 's/ additional//'
```

によって，25 Mar 2010,850,134というような日付，隔離ボックス中の迷惑メールの数，新規の迷惑メールの数というcsv形式のファイルに変換する。これを用いてグラフを作成するとおかしな点が見られたので，日付の重複がないか

```
sed 's/,.*$//'  |uniq -c|sort|awk '{if ($1>1) {print $0}}'
```

このようなコマンドで調べると，

```
2 29 Jul 2015
2 29 Oct 2010
```

２件の重複が見られた。全職員用のメーリングリストのアドレスに迷惑メールが来た旨を全職員に向けて知らせたもので，この迷惑メールは誤検知であった。この２件を除いたデータから日付毎の隔離ボックス中の迷惑メールの数と，新規の迷惑メールの数のグラフを作成したのが図１及び図２である。隔離ボックスには２週間迷惑メールが留まり，ユーザが誤検知を発見して救出を行わなければ消去されていく。

迷惑メール防止装置は，2010年の３月25日から稼働し2016年の３月１日に現装置と交換されて停止している。

図２によれば，2014年の７月より数が顕著に減少しているが，それ以前は一日に150通程度の迷惑メールを受信し，図１によれば，隔離ボックスには一日に1000通を超える迷惑メールが置かれていたことがわかる。正確には，2014年７月４日までと５日からの２つに分けると，４日までは１日平均144通で分散51，隔離ボックスのメール総数は平均1023通で分散が313程度であり，５日以降は１日平均が12通で分散11，隔離ボックスのメール総数は平均89通で分散が66程度となっている。

この激減の理由は，カナダのアンチスパム法であるCASL[18)]が2014年７月１日に施行されたことが大きいと見られる。それ以前の迷惑メール数の増減については，サイバー犯罪者が悪意あるプログラムを使用して乗っ取った多数のコンピュータによって構成される巨大なbotnetの発現とその検挙によるものであろうと推察されるが，はっきりとしたことは一個人宛の迷惑メール数だけでは判断し得ない。

迷惑メール防止装置の効果があったと見るべきかどうかを判定するために，装置の導入前から筆者が受信していたメールの数を月毎に調べたものが図３である。このグラフは，2007年の６月から2016年の12月までの月毎の筆者の受信メール数で，迷惑メール防止装置が稼働したあたりから急激にその数が減少しているのが判る。おおまかに，月4500通程度迷惑メールが隔離ボックスに隔離されて筆者の手元に来ずに済んだ。

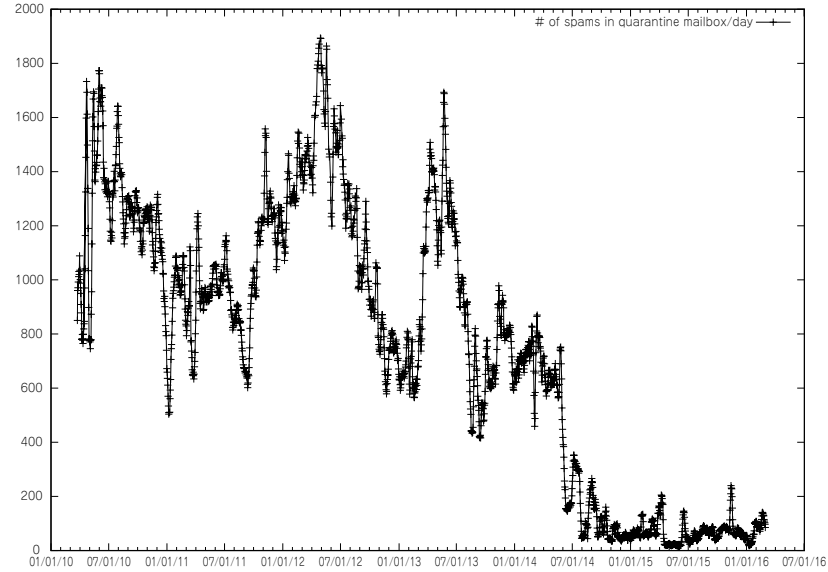

図１：隔離ボックス中の迷惑メールの総数

18）http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html

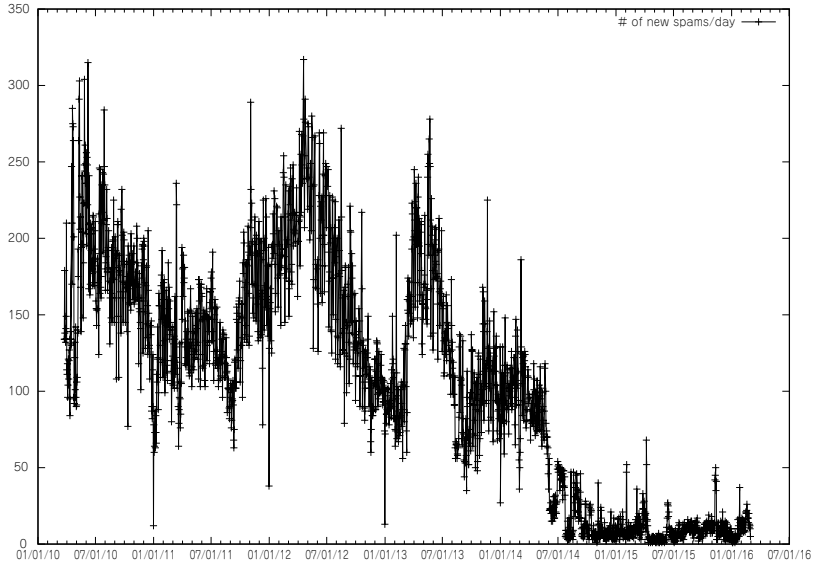

図2：新規迷惑メールの数

尚，図3の迷惑メール防止装置稼働以前のメールもその多くがスパムであった。筆者は前職のメールを本学に転送しており，［16］で述べたように，外部へのメールを透過型ウィルスチェッカに通すために発生した問題を回避しつつ，筆者の手元のホストにTCP 26番ポート経由でfilterというメールアドレス宛に送り，それを本学の筆者のアドレスにaliasesで送りつけてウィルスチェックを行った後取り込むという形で受け取っていた。2008年11月あたりから筆者の前職のドメインも外部からのメールを横取りしてチェッカに通す設定となったため，迷惑メールの数は減少したことが読みとれる。実際，2008年10月では前職経由のメールが8725通に対して11月には3418通と大幅に減少している。

さて，迷惑メール以外にウィルスが添付されたメールはどれくらい排除されたかという点も当然重要である。そこでvirusadmin@office.otaru-uc.ac.jpから送られてくる「ウィルスを検知しました」という件名のメールが何通筆者へ送信されているかをグラフにしたのが図4である。これは年毎のグラフであり，

多い年でも54通，2014と2015年は５通で2016年は１月２月のみではあるが０通である。ウィルスが添付されたメールは当然排除しなくてはならないが，やってくる頻度は迷惑メールに比べると微々たるものであった。

正しく迷惑メールが迷惑メールとして隔離され，本来自分に届くべき正常なメールを誤って迷惑メールと誤検知しないということがどの程度達成されているかも重要な点である。これはほぼ満足がいく結果である。

隔離されないものは，実は筆者のメール受信用のホストを直接指定して配送されたものであって，迷惑メール防止装置を経由していないものである。

誤検知されたものはダイジェストモードのメーリングリストである。筆者が入っているのはfreebsd-questions@freebsd.orgとfreebsd-stable@freebsd.orgであるが，これは一日にメーリングリストに投稿されたメールをまとめて１本のメールとして送る方式で，多数のメールが飛び交う状況を一々見たくはないが情報は欲しいという場合には便利な方法である。

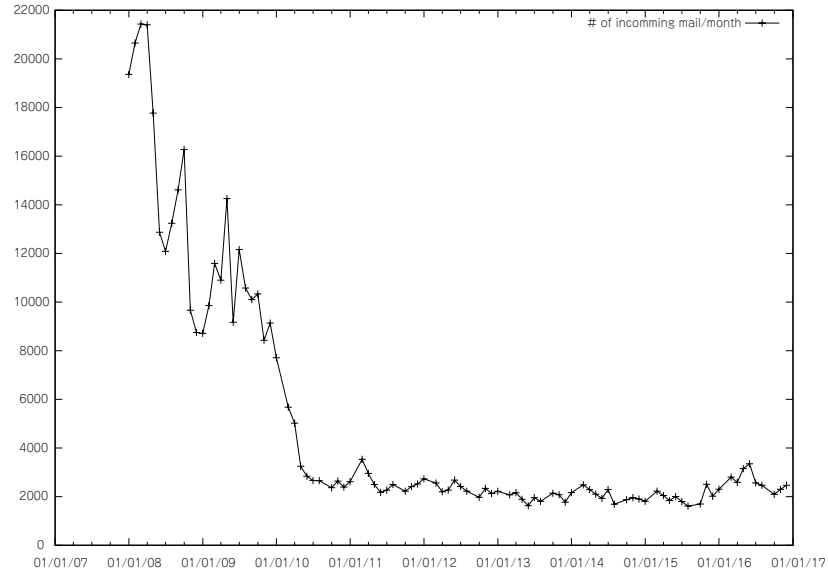

図３：月毎の受信メールの数

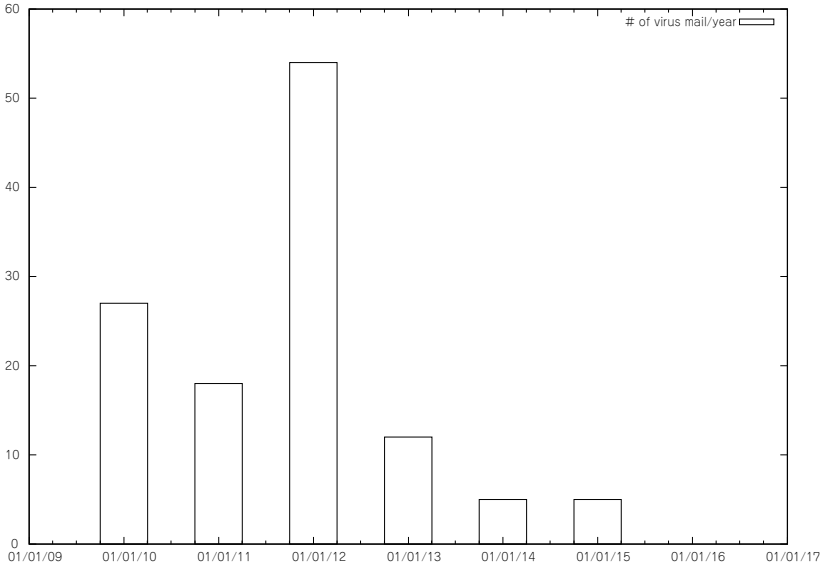

図 4 ：年毎のウィルスメールの数

ダイジェスト系メーリングリストに関しては，その一部にスパムが混入している場合もあるが，大抵の場合は引用が多く含まれる事でスパムの判定を受けると推察される。メールへの返信を行う場合，元のメールを引用する事が多いので，行頭が引用符と判断される行の割合での判断かもしれないが詳細は不明である。これは，OSの管理者向けの日々の状況報告を行うdaily reportのメールが，設定の変更等の変化の多い場合に，前日との相違点を教えるためにdiff形式で情報が送られたためにスパムと判定された例からも伺える。そのため，筆者はWhite Listとしてアドレスを登録し，スパムと判定されても隔離せずに通常通り送ってもらっていた。

それ以外にも，筆者が属しているWIDEプロジェクトからのメールが隔離される事態が短時間ではあるが発生した。2011年 3 月13日の夕方から14日にかけてで，理由は不明である。スパムではない旨のメールをCloudmarkに送り解除された。それ以外にも引用が多すぎるようなメールも隔離される傾向があった

ので，WIDE関係のメールもWhite Listに登録した。

これらは，メーリングリストがナンバリングされており，Subjectに番号が付加されているため，番号が飛んでいることで気がついたものである。

また，先に述べた教職員全体に当てたメールが誤判定されたのは，Subjectが全角で29文字だと落ちるという訳の判らない例で，世界中から送られるスパムメールの例から学習して作り出されるルールに何があるのかはユーザは全く判らないので対処のしようがなかった。その時のメールは

```
From:    総務課職員係 <shokuin@office.otaru-uc.ac.jp>
Subject: [QUAR] 【総務課職員係】高病原性インフルエンザに関する注意
について
Date:    Thu, 28 Oct 2010 15:52:27 +0900
```

及び

```
From:    小樽商科大学会計課契約係 <keiyaku@office.otaru-uc.ac.jp>
Subject: [QUAR] 【会計課契約係】返納物品の引取募集について（8月7日
17:00締切）
Date:    Tue, 28 Jul 2015 17:17:41 +0900
```

となっていた。

以上まとめると，本装置の導入は少なくとも筆者にとっては十分な効果があったものである。

現在の本学のメール用アプライアンスであるQualitia社のMailSuiteもCloudmarkのフィルターを使用している。また，submissionサーバとメールスプールも兼ねており，迷惑メールの隔離とウィルスチェックを行っている。

筆者は本学ではres.otaru-uc.ac.jpとmit-s.otaru-uc.ac.jpのドメイン名でメールがやってくる。最終的にはどちらも筆者の研究室のメールホストに届く。現在のシステムでは，運用の都合上筆者のように研究室単位のドメインを運用している部分は（筆者ではmit-s.otaru-uc.ac.jp）隔離ボックスではなくメールへのマーキングだけとなってしまったため，筆者の手元まで届くメールの数は増えている。しかし，Thunderbirdのメッセージフィルタを使ってローカルな隔

離フォルダへの排除はできている。図3で2016年3月以降のメールの数が増加しているのはそのためである。それに加えて，関係するプロジェクトのオペレータ宛のメールが本年1月からcisco社のIronPortを通過しなくなったためにスパムが増加した面もある。IronPortを通っていた2015年には1万通を超えるメールを受信して，534通を通過させ残りをスパムとして落としていたそうである。

運用上の問題点とまとめ

Sentrionの運用及び本学のメールシステムの運用に関して幾つかの問題点があったので，ここに記しておく。

まずSentrionの導入時であるが，メールシステムは送受信時刻等をメールヘッダに書き込んだり送受信記録をログとして時刻と共に残すため，できるだけ正確な時刻で運用される必要がある。そのために，通常ntpを使って時刻合わせを行うのであるが，本システムはstrutum 1のntpサーバとは接続しない仕様となっていた。そのため，筆者のホストで動作していたntpに同期させるということで設定をして稼働できた。

また，本システムはメールの送受信以外に，迷惑メールのパターンをアップデートするために外部と通信を行うため，セットアップ時に本学のfirewallで必要なポートの開放等を行って動作することを確認した。しかし，その後何故か開放してあったポートが閉じられて外部からのパターンのアップデートができない状態で2010年5月初旬までの暫くの間運用されていた。これは，スパムをCloudmarkに何度か報告しても一向に隔離されず，おかしいのではないかと気がつき判明した。複数の業者が関係しての情報システムのセットアップは，現場での意思疎通が難しい面があるため，必要な情報を事前に書き出して貰って，関係する全ての業者間で共有しておく必要がある。

次に，本製品はメールアドレス単位の課金となっており，教職員と学生の数で必要なライセンスを毎年購入する必要があるが，個人ではなくアドレス単位なので，学内のメーリングリストに対してもライセンスが必要となる点が悩ま

しかった。また，ライセンスの更新が年度単位でなかった点も面倒があった。

そのメーリングリストの管理についても，本学情報処理センターの非常勤職員が，前職から引き継がれたマニュアルを見ながら，管理者権限でエディタを使ってファイルを更新していくという手法で行われている。この職員はUNIX等に関しては素人であって，rootの権限が何であるか，自分がマニュアル通りにやっている作業がどういうことであるかを真に理解している訳ではない。例えば，今年２月28日に発生した米Amazon.comのクラウド事業AWSのAmazon S3で発生した大規模障害も，素人の管理者が管理権限を持って数台のサーバ停止の作業を行う際に，誤ってコマンドを入力したのが原因であった。素人の管理者が行う作業にはできるだけ特権を与えずに作業できる環境を整えるべきである。

また，Sentrionの内部で動作しているシステムのアップデートに関しても，販売元から技術者が来て行われるような大規模なものを除けば，パッチと作業手順書が送られてきて，センターの非常勤職員が実際の作業を行っているのが実情であった。しかし，本来UNIXやそのシステム管理を知らない素人であるため，作業手順書をよく理解せずに作業を行って必要なパッチが当てられない事態になったこともあり，その時は丁度筆者が情報処理センターへ出向いていたので，筆者の手によって正しくパッチを当てて事なきを得た。

最後に，先に述べた本学のメール環境での問題点に関して詳しく述べる。当時のシステム構成では２台のSentrionがプライマリとセカンダリのMTAとしてメールを受信して必要な処理を行った後，popサーバに転送してメールをスプーリングし，教職員は各自が自分のメールクライアントを使ってpopサーバからPOP3またはIMAP4プロトコルでメールを読み出していた。学生についてはActive! Mailを使ってWEB経由でメールを読み出すという体制をとっていた。独自ドメインで運用している筆者のような所は，そのドメインのメール受信用のマシンに送る設定となっていた。

通常の運用状態では何ら問題のない環境に思われるが，落とし穴が一点存在することが見つかった。それはSentrionからpopへのメール配送をDNSを参照して行っていた点である。そのため，DNSが参照できなくなると困った事態

となる。このような事態が発生し得るのは，停電の後のシステム起動時である。通常は停電後のシステム起動は，順序を考えて手動で行うか，自動化できればそうするわけであるが，先に上がっている筈のDNSをサービスする当時の本学の仮想ホストが，停電後にサーバの不調で全て立ち上がっていない状態でSentrionが稼働してしまい，外部からのメールを受け付け出したという場面であった。SentrionはDNSによる名前解決は自身では行わずに学内のDNSサーバに頼っており，それが参照不能であるためにpopに対してメールを送り出すことができず，エラーメールを引き起こした事象が発生した。DNSを参照せずにIPアドレスを決め打ちした形でpopへの配送を行っていれば防げたのであろうが，アプライアンスの設定の自由度がそこまであったかは不明である。この後，対応策として本学のSentrion上でbindを動作させて自身でもアドレス解決ができるような設定を追加した模様である。

また，ソフトウェアであるから不具合が起こることもあるが，それらは本学に納入した日本の代理店経由で対応をお願いし，プログラムを修正してもらうことができた。例えば，2010年10月に発覚した問題としては，メールアドレスに”の対応が取れていないアドレスを書かれると迷惑メールとして隔離できず，そのまま正常なメールとして送るのではなく，処理途中で処理ができなくなってアボートしたメールを送ってくるといったものがあった。2011年からはほぼ大きな不具合もなく運用されてきた。また，

- Content-Typeにmultipart/alternativeとあるのに本文にmultipartの構造がないケース
- Fromに生のUTF-8（キリル文字）がある場合にヘッダが壊れるケース

に関しては，筆者の指摘を2011年10月にSendmail社のCTOであるGreg Shapiroに直接持って行って貰い解決を加速した。

最後に以上をまとめると，前回のシステム更新時に当時業界で実績のある迷惑メール防止装置を導入したことにより，運用上のエラーが多少あったにせよ，迷惑メールを十分排除して教職員の作業効率の向上に貢献し得たと言えよう。

参 考 文 献

［1］ Tom Van Vleck. Electronic Mail and Text Messaging in CTSS, 1965–1973. *IEEE Annals of the History of Computing,* Vol. 29, No. 1, pp. 3–29, 2005.

［2］ Craig Partridge. The technical development of internet email. *IEEE Annals of the History of Computing,* Vol. 30, No. 2, pp. 3–29, 2008.

［3］ R.W. Watson. Mail Box Protocol. RFC196, July 1971. Obsoleted by RFC 221.

［4］ A.K. Bhushan. File Transfer Protocol. RFC 354, July 1972. Obsoleted by RFC 542, updated by RFCs 385, 454, 683.

［5］ A.K. Bhushan. Comments on the File Transfer Protocol. RFC 385, August 1972. Updated by RFC 414.

［6］ M.D. Kudlick. Network mail meeting summary. RFC 469, March 1973.

［7］ A.K. Bhushan, K.T. Pogran, R.S. Tomlinson, and J.E. White. Standardizing Network Mail Headers. RFC 561, September 1973. Updated by RFC 680.

［8］ S. Sluizer and J. Postel. Mail Transfer Protocol. RFC 772, September 1980. Obsoleted by RFC 780.

［9］ J. Postel. Simple Mail Transfer Protocol. RFC 821 (Internet Standard), August 1982. Obsoleted by RFC 2821.

［10］ J. Klensin. Simple Mail Transfer Protocol. RFC 2821 (Proposed Standard), April 2001. Obsoleted by RFC 5321, updated by RFC 5336.

［11］ J. Klensin. Simple Mail Transfer Protocol. RFC 5321 (Draft Standard), October 2008. Updated by RFC 7504.

［12］ 砂原秀樹．インターネット　歴史の一幕：JUNETの誕生．ニュースレター，JPNIC, May 2005. https://www.nic.ad.jp/ja/newsletter/No29/060.html.

［13］ 吉村伸，森下泰宏．第5部パソコン通信との相互接続実験．1992年度研究報告書，WIDEプロジェクト，July1992.
http://www.wide.ad.jp/project/document/reports/pdf1992/part5.pdf.

［14］ 若林伸夫．インターネットを利用したOR計算環境の改善：Oberonシステムの移入．商学討究，Vol. 44, No. 1/2, pp. 35–56, 1993.

［15］ 吉村伸，徳川義崇，鈴木茂哉．第3部 ネットワークに関する社会科学的検討．1991年度研究報告書，WIDEプロジェクト，July 1991.
http://www.wide.ad.jp/project/document/reports/pdf1991/part3.pdf.

［16］ 三谷和史．透過型電子メールチェッカの導入に係る諸問題．商学討究，Vol. 60, No. 1, pp. 71–87, 2009.