研究論文

鳴門教育大学情報教育ジャーナル　1，49 － 54，2004

電子メールシステムの構築と運用

曽根　直人*

情報処理センターは鳴門教育大学ドメインのメールサーバを運用している。本稿では大学規模のメールを処理するシステムの構築について述べるとともに，メールサーバのトラフィックを分析し，ウィルス付きメールや spam メールの実態を明らかにする。

〔**キーワード**：ウィルスメール，spam メール，RBL，MTA，ウィルスゲートウェイ〕

Ⅰ．はじめに

電子メールはインターネットの黎明期から存在するアプリケーションであり，手軽な連絡手段として広く利用されている。従来は電子メールの利用にはインターネットに接続された端末が必要であったが，国内では携帯電話からもインターネットの電子メールが利用可能になり一気に日常的な通信手段として重要な位置を占めるようになった。

情報処理センターにおいても設立当初から電子メールのサービスを開始している。現在のシステムでは電子メールに関連するサービスとして

・SMTP によるメールの送受信
・POP3 によるメールの読み出し
・IMAP4 によるメールの読み出し

などを提供しており多くのユーザに利用されている。

本稿では情報処理センターで運用している電子メールシステムについての詳細を述べる。

Ⅱ．電子メールシステムの構築

1．メールシステム構成

本学におけるメールシステムの構成を図 1 に示す。このシステムにおけるメールの処理の流れは以下のようになる。

1．インターネットや学内 LAN からのメールを一旦 mail.naruto-u.ac.jp で受け付ける。
2．ウィルスゲートウェイに転送され，ウィルスを駆除する。
3．ウィルスチェックを受けたメールは受信メールサーバである sanuki.naruto-u.ac.jp に届けられる。
4．利用者は，pop や imap プロトコルを利用し，受信メールサーバからメールを読み出す。

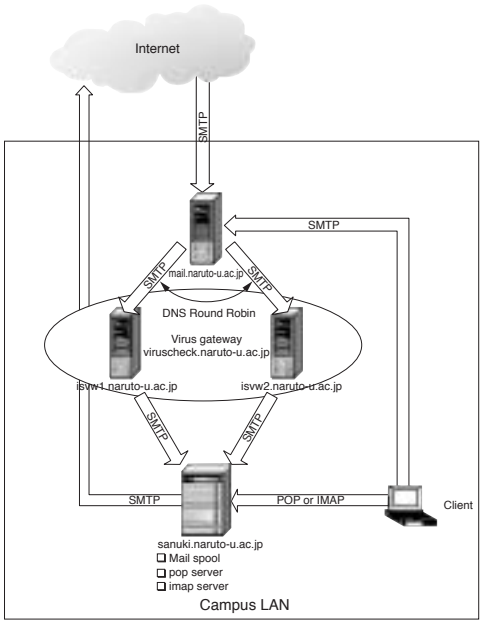

図 1　メールシステムの構成

2．MTA

MTA(Message Transfer Agent) はメールの配送を受け持つプログラムである。

図 1 では，mail.naruto-u.ac.jp と sanuki.naruto-u. ac.jp の 2 つのホストにおいて MTA が稼働している。

情報処理センターの電子メールシステムは Unix(Solaris) サーバ上に構築されており，従来は MTA として実績のある sendmail[1] を用いていた。sendmail は古くから開発されている MTA であり，多くの Unix システムにおいて標準的な MTA として採用されている。しかし sendmail は広く普及しているものの，基本的な設計が古いために次のような問題点が指摘されている。

・一つのプログラムがメールの受信から配送までを受け持つため，構造が複雑になっている。その複雑さに由来するセキュリティホール[1)] の発見も多い。
・設定ファイルが難解である。
・標準の設定では，第三者中継を許可している。

* 情報処理センター

最近の新しい sendmail ではこれらの問題点を多く解決しているが，まだセキュリティホールの存在を報告されることも多い。メールシステムの安全な運用を行うためには，管理者はセキュリティホールの発見のたびに sendmail のバージョンアップの必要性を確認する必要がある。したがって sendmail を安全に運用するには管理者に大きく負担がかかる。そこで管理・運用の負担を低減させるため，本センターでは sendmail に替わるより現代的な MTA の postfix[2] へ移行した。postfix は次のような特徴を持つ MTA であり, sendmail からのスムーズな移行が可能である。

・sendmail との互換性
・高性能
・設定ファイルの可読性が高い
・機能ごとに分割されたプログラムで構成

現代的な MTA では，sendmail と異なり，受信や配送といった役割に応じて単純化された複数のプログラムが協調し，動作するようになっている。プログラムを単機能かつ単純化することで，バグの発生が少なくなるとともに，万一バグが含まれていた場合でもその影響を最小限に留め，致命的なセキュリティホールとなり難い設計になっている。

sendmail を置換える新しい設計の MTA としては postfix 以外にも qmail[3] などが有名である。qmail も MTA として多くのサイトでの採用実績があるが sendmail との互換性が低く，移行時にはプログラムを入れ替えに加えてユーザのメール保存領域の形式の変更などの作業が必要になる。

3．ウィルスゲートウェイ

Sobig や MyDoom などのメールにより感染するコンピュータウィルスによる被害が年々拡大している。そこで本システムではウィルスゲートウェイ（トレンドマイクロ社 Interscan VirusWall 3.6 Linux 版）を導入し，メールに添付されているウィルスの除去を行っている。ウィルスゲートウェイは通常の MTA の動作と異なり，SMTP で送られるデータを一旦保存せず，透過的に指定したサーバの MTA に中継する。ただし，中継するデータにウィルスが含まれていた場合には，設定にしたがって添付ファイルの削除などの指定した動作を行う。

本システムではウィルスゲートウェイを２台用意している。これはウィルス検査の負荷を分散させるためであり，DNS のラウンドロビン機能を利用している。これは viruscheck.naruto-u.ac.jp というホスト名に対して２つの異なる IP アドレスを設定しておくことで実現できる。DNS を利用した負荷分散は簡単に実現できるが，分散を受け持つホストの故障や過大な負荷がかかっている場合などの状況によって負荷を振り分けることができないという欠点がある。しかし本システムのように SMTP 処理の分散を考えた場合は，万が一故障のために分散処理ができないホストが存在する場合も SMTP そのものがリトライ機能を持つため大きな問題にはならない。

MTA は DNS に登録されている MX(Mail eXchanger) 情報に従って電子メールを配送する。鳴門教育大学のドメイン“naruto-u.ac.jp”では MX として mail.naruto-u.ac.jp が指定されている。つまり学外の MTA が配信するメールは mail.naruto-u.ac.jp に届けられ，そこからウィルスゲートウェイに転送される。従って学外からのメールはほぼ完全にウィルスを駆除できる。一方学内のクライアントパソコンから発信されるメールの場合は，MX ではなく設定した送信メールサーバの指定に従う。そのため各クライアントにおいて送信メールサーバとして mail.naruto-u.ac.jp を指定しておけば，発信するメールは viruscheck.naruto-u.ac.jp によるウィルス検査が行われる。

4．受信メールサーバ

本システムでは，受信メールサーバとしてセンターのファイルサーバである sanuki.naruto-u.ac.jp を使用しており，imap.naruto-u.ac.jp, pop.naruto-u.ac.jp を別名として登録している。

センターではすでに以前のシステムからユーザの利便性を考え pop に加えて imap[4] によるメールの読み出しをサポートしてきた。さらに古くからあるコンソールから直接メールスプールを読み出す Mail や mnews コマンドの利用者もおり，全てのユーザの読み出しをサポートするために wu-imapd[5] を利用している。

Ⅲ．電子メールシステムの運用

従来電子メールシステムの運用では，設定ファイルの記述と MTA のセキュリティホールなどに注意すれば良かった。しかし昨今ではウィルスや spam といった迷惑メールが非常に多く，これらの迷惑メールに対抗するためにはシステムでの対応が重要になる。本節では，鳴門教育大学におけるこれら迷惑メールへの対策のための運用について述べる。

1．spam メール対策

一方的な電子ダイレクトメール UCE(unsolicited commercial email) は一般に spam メールと呼ばれており，メール利用者にとって非常に迷惑な存在である。さらに受信メールに占める spam の割合は年々増加しており, 米国ではメールに占める UCE の割合が 2003 年には 45%，2007 年には 70% を越えるという予測を発表している会社もある [6]。本学においても受信したメールに占める UCE の割合は増加傾向にあり，対策を講じる必要がある。

postfix では設定により spam への対策が可能である。セ

ンターのシステムでは spam 対策として，

・RBL による送信者のフィルタリング

・制限リストによるフィルタリング

・正規表現を利用したヘッダのフィルタリング

などを行っている。

図 2 に mail.naruto-u.ac.jp における MTA の配信状況（2003 年 11 月 9 日～2004 年 1 月 31 日）を示す。図 3 は，さらに MTA の配送状況を曜日毎に集計し，平均をとったものである。図 2, 図 3 において sent は正常に受け取ったメールを示しているが，それ以外の状況はサーバが拒否もしくはエラーになったメールを示している。この期間では 1 日平均で約 3887 通のメールを受け取り，約 1255 通のメールを拒否している。つまりサーバに届くメールのうち約 32% がフィルターによって拒否もしくはエラーになっている。図 3 からは，正常にサーバが受信するメールの数は週末には減少するが，拒否される spam メールは常に一定の数が受信されていることが判る。

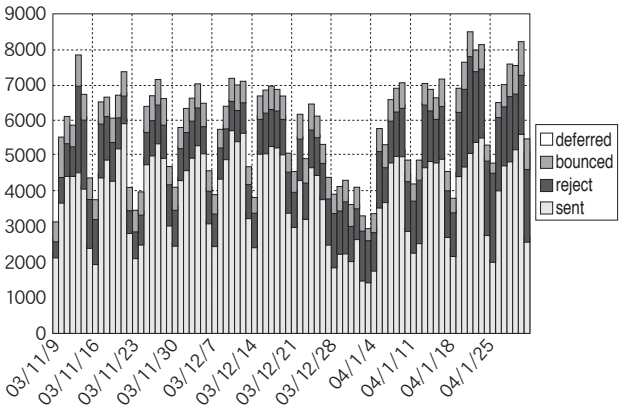

図 2　mail.naruto-u.ac.jp における MTA の配送ステータス

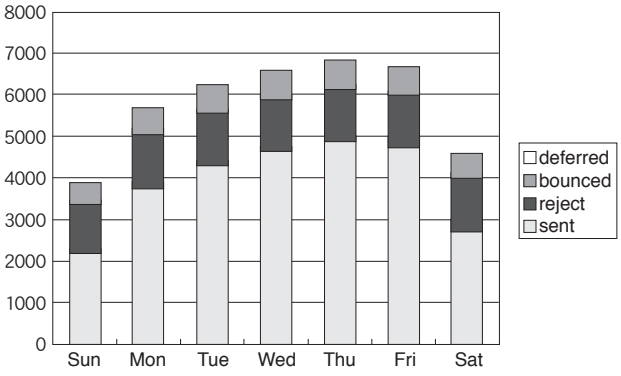

図 3　曜日別 MTA 配送ステータス

1．1．RBL によるフィルタリング

RBL（Realtime Black List）は spammer（spam 発信者）によって利用されている第三者中継サイトが登録されているリストである。このリストは DNS をつかって参照することができる。Postfix などの RBL に対応した MTA では，接続してきたメールサーバが RBL に登録されていないか確認し，登録されているメールサーバの場合は接続を切断する。本学のシステムでは RBL として

・list.dsbl.org

・sbl-xbl.spamhaus.org

・mail-abuse.blacklist.jippg.org ,
mail-abuse.blacklist.jippg.org

を利用している。（2004 年 2 月 5 日現在）

RBL によるフィルタリングでは当然ながらリストに掲載されているサーバからのメールは完全に遮断することができる。その反面，本来受け取りたいサーバがリストに掲載された場合はメールを受けとることができなくなるという問題がある。また ADSL のような高速回線の普及により，従来のように高速回線に接続された第三者中継サイトを経由しなくても spam を送信できるようになりつつあるため，リストに掲載されていないサーバからの spam も多くある。したがって RBL の利用だけでは完全に spam を防ぐことは難しい。

1．2．制限リスト

メールを本学に送信してきたサーバを本学で設定したリストに従って動作を決定することもできる。例えば RBL には掲載されていないが受信を拒否したいサイトや，RBL に掲載されているものの受信したいサイトをリストに登録し，破棄（REJECT）や許諾（ACCEPT）といった動作を設定できる。

表 1 に制限リストの一部を示す。2004 年 2 月 5 日の時点でコメントを除き 55 ほどのドメインおよび IP アドレスが制限リストに登録されている。これらは実際に spam メールを送ってきたサイトのアドレスや RBL によってブロックされたくないサイトを手動で編集している。

表 1　制限リストの一部

150.59.112.17	OK
61.49.138.219	REJECT
61.41.210.63	REJECT
61.49.229.77	REJECT
61.103.142.142	REJECT

1．3．ヘッダによるフィルタリング

表 2　正規表現による拒否ルールの一部

/^Subject: .*Make Money Fast/	REJECT
/^Subject:.*Penis/	REJECT
/^Subject:.*V[il1]agra/	REJECT
/^Subject:.*V.I.A.G.R.A/	REJECT
/^Subject:.*F¥.R¥.E¥.E/i	REJECT
/^Subject:.*F¥.U¥.C¥.K/	REJECT
/^Subject:.*Casino/	REJECT
/^Subject:.*ink*jet.*cartridges/	REJECT
/^Subject:.*ink.*save.*/	REJECT
/^Subject:.*sex life/	REJECT
/^Subject:.*fat.*muscle/	REJECT

postfix では正規表現を利用したメールのフィルタリングも可能である。ヘッダやボディなどに対して正規表現によるルールを設定することが可能であり，ルールにマッチした場合の動作を設定できる。spam には商品のキーワードなどが Subject ヘッダに含まれることが多く，また国内の spam メールは同報メールソフトが利用されることが多いため，これらにマッチする正規表現を記述し，マッチしたメールは破棄(REJECT)している。表２に実際の運用に用いている正規表現ルールの一部を示す。2004 年２月５日における正規表現ルールはコメントを除き 63 行ほどになっている。

１．４．ベイジアンフィルター

spam メール対策としてこれまではサーバ側での対策を述べた。しかしこれらの対策はリストやルールに登録して有効になる対策であり，日々大量に送られてくる spam の中にはこれらの対策を抜けてくるものがある。そこでセンターでは受信メールサーバ上にベイジアンフィルターを利用した学習型のフィルタリングソフトである bsfilter[7] をインストールしている。著者のメールアドレスに届くメールは bsfilter を用いて spam を判断しており，効果を上げている。図４は，2003 年９月 14 日から 2004 年２月４日の期間に著者宛に届いたメールのうち，bsfilter により spam と判断されたメールの推移を示す。期間中，一日平均約 156 通のメールを受け取りそのうち spam と判断されたメールは約 14% にあたる約 22 通となった。システム管理者である著者が受け取るメールは，一般ユーザよりも多いが，その中にはシステムが定期的に送信する（つまり spam ではない）メールも多く含まれる。したがって，一般ユーザでは受け取るメールに占める spam の割合は 14% よりもさらに大きいと考えられる。

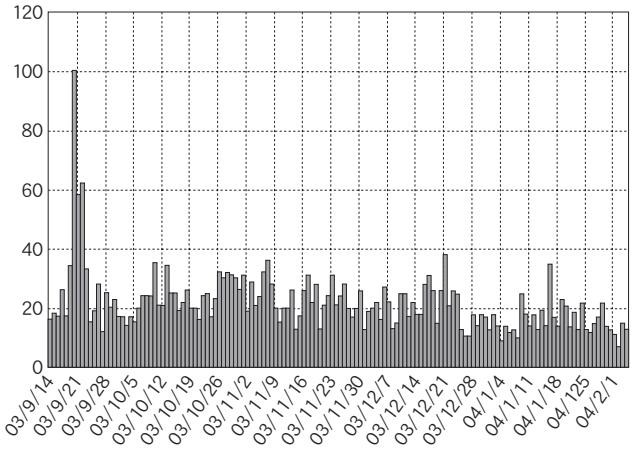

図４　bsfilter により spam と判断されたメール

bsfilter のような学習型のソフトではあらかじめ通常のメールおよび spam メールを学習させておく必要がある。また個人によって spam かそうでないかの判断は異なるため，現状ではシステム全体でのベイジアンフィルターの設定は行っていない。しかし，個々人による設定の手間と導入効果を考えればシステム側に組込むことも十分検討する必要がある。

またこのような学習型のフィルターを備えたクライアントソフトとして Mozilla Mail がある。Unix での設定に慣れてないユーザはこのようなクライアントを利用することで spam を制限できる。

２．ウィルス対策

メールを媒介として感染が拡がるタイプのウィルス対策にはウィルスゲートウェイの導入が効果的である。ウィルスゲートウェイはメールサーバと連携しながら組織に届くメールを集中的に監視し，ウィルスが含まれたメールであればサーバが受信する前にウィルスを駆除することができる。

２．１．ウィルスゲートウェイの導入

図１に示したように，本学においても既にウィルスゲートウェイを導入し，鳴門教育大学に届くメールからウィルスを駆除している。

ウィルスゲートウェイは，学内へ届くメールを全て検査できるため，ウィルスメールの駆除には大きな効果が期待できる。図 ５にウィルスゲートウェイにおけるウィルスの駆除件数(2001年６月５日～2004年２月３日)を示す。

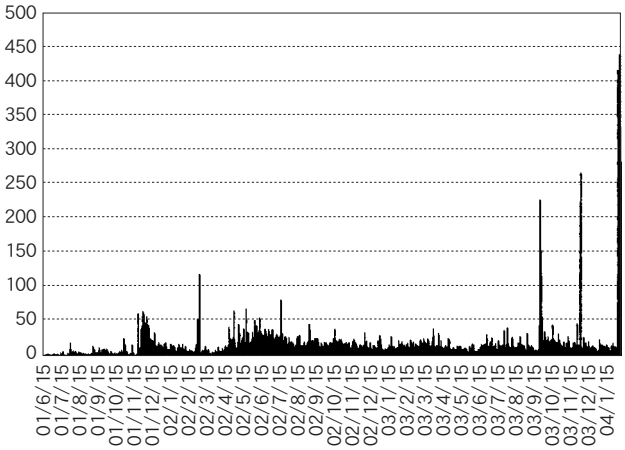

図５　ウィルスゲートウェイにおける駆除件数

図５を見るといくつか鋭いピークが発生していることが判る。これは強力な感染力を持つ新型のウィルスの発生と一致しており，そのウィルスの活動結果が反映されていると考えられる。しかし，ピークはすぐに終わることから，新種のウィルスが発生した場合には，その感染活動の影響により駆除数が一気に多くなるが数日で活動が減少していることが判る。しかし，ピークを過ぎても完全にメール感染型のウィルスがなくなるわけではなく，毎日ウィルスに感染したメールが届いている。平均すると一日あたり約 18 通のウィルス付きメールを処理している。サーバには１日平均で約 3887 通のメールを受信

していることから，約0.45%のメールがウィルスに感染していたことになる。また，ウィルスの活動が活発な時期（MyDoomウィルス，2004年1月28～2004年2月3日）に注目すると，この期間では受信メールのうち約9.94%がウィルスに感染したメールであった。このように電子メールを利用している以上，常にウィルス付のメールが送られてくる可能性がある。したがってノートパソコンなどを自宅に持ち帰り，大学以外のアカウントで電子メールを受信している場合は，感染しないように注意が必要である。

2．2．ウィルスゲートウェイの管理

ウィルスゲートウェイの仕組みは一般のウィルス対策ソフトと同様であり，パターンファイルに登録されたウィルス情報とSMTPで送られるデータを照合し，一致していればウィルスとして判断している。そのため，パターンファイルが更新されていなければ新種のウィルスを見逃してしまうことになる。

ウィルスゲートウェイにおけるパターンファイルの更新は手動はもちろんのこと，指定した頻度で自動的に行うこともできる。図5からメールを媒介とするウィルスの場合は，急速に感染が広まる傾向があることが判る。したがって，ウィルスに感染したメールを学内に侵入させないためにはパターンファイルの更新を頻繁に行うことが望ましい。現在はパターンファイルの更新は毎時行っているが，以前は1日毎に行っていた。しかし1月末に発生し，急速に感染が拡がったMyDoomウィルスに対しては1日毎の更新では遅すぎた。管理者が手動でパターンファイルをアップデートするまで学内にMyDoomウィルスの侵入を防ぐことができなかった。

3．受信メールサーバ

本システムの受信メールサーバに対するクライアントからのアクセス数を図6に示す。

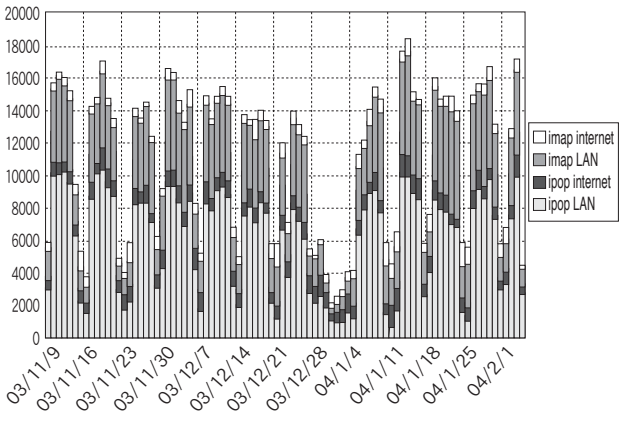

図6　受信サーバのアクセス数

imapは複数の端末からサーバ上のメールボックスへのアクセスができるなどpopと比べてユーザからの利便性が向上している。そのためユーザの利用もimapがpopを上回るのではないかと予想していた。しかし図6からはpopのアクセス数の方が多いことが判る。ただし図6はアクセス数のみをグラフにしたものであり，imapはpopと比べ比較的長時間接続が続く特徴を考慮する必要があり，単純に比較することはできない。また，imap，popともに学外からのアクセスもあることが判る。学内からのアクセス数は週末には落ち込むが，学外からのアクセス数は曜日にかかわらずほぼ一定になっている。

4．受信メールサイズ

2003年11月9日から2004年1月31日の期間に受信メールサーバが受け取ったメールのサイズ分布を表3に示す。受信したメールのうち，約70%は10KB以下の小さなメールであり，さらに大きさが100KB以下のメールは全体の約99%を占めることが判る。

適切なメールのサイズについては様々な意見があるが，あまり大きなサイズのメールは望ましくないとされている。これは電子メールの配送を考えた場合，巨大なメールはMTAのスプールを圧迫するなどの影響が考えられるためである。

添付ファイルの普及により，巨大なメールの交換が懸念されたが，実際はそれほど大きなメールの交換はないことがわかる。これはOutlook Expressなど多くのMUA（Mail User Agent）では設定した大きさ以上のメールを分割して送信する機能の活用や，巨大なデータはメール以外の手段（ftpやscp）を利用しているためではないかと思われる。

表3　メールのサイズ分布

受信サイズ	受信数	割　合
1KB以下	12380	2.74
10KB以下	311484	68.98
100KB以下	122672	27.17
1MB以下	4041	0.89
10MB以下	974	0.22
10MB以上	2	0.00

Ⅳ．ま　と　め

情報処理センターの電子メールシステムの構成および運用について述べた。現在のシステムは非常に安定して動作している。またウィルスゲートウェイの導入によりウィルスメールの効果的な駆除が行えている。しかしspamメールの増加に対する対策はまだ不十分である。MTAにおける対策で多くのspamメールの受け取りを拒否しているが，それでもなお個人のメールボックスに届くspamメールの数は多い。不要なメールはシステムの資源を無駄に使うだけでなく，受取人の時間をも無駄に使ってしまうため，効果的な対策の導入が不可欠である。

またブロックのためのポリシーやブロックルールをいかに利用者に公開するべきかも解決しておかなければならない問題である。

学外から受信メールサーバへのアクセスも多くの利用者がいるが，現状のプロトコルではアクセス時に認証情報が暗号化されず平文[2)]のまま流れている。インターネット経由で平文の認証情報を流すことは認証情報の漏洩につながるため，平文の認証情報を利用しない APOP や imap over TLS の導入, もしくは通信路そのものを暗号化する VPN 接続の導入を進める必要がある。さらに出張先などから手軽に大学のメールを読み出したいという要望には Web メールを導入することが考えられる。Web メールではブラウザでの閲覧になるため，学内で広く用いられている Outlook Express よりもウィルスの影響を受けにくいという利点もある。

既に電子メールは日常的に用いる重要な通信手段となっている。今後は安定した運用はもちろん安全にかつ利便性を損なわないシステムを目指してシステムの構築・運用を行っていく必要がある。

注　　釈

1）プログラム上の不具合であり，安全な運用に支障をきたすもの。
2）暗号化されてないデータ。クリアテキストとも呼ばれる。

参 考 文 献

[1] sendmail: http://www.sendmail.org/
[2] postfix: http://www.postfix.org/
[3] qmail: http://www.jp.qmail.org/
[4] imap: http://www.imap.org/
[5] wu-imapd: ftp://ftp.cac.washington.edu/mail/imap.tar.Z
[6] ニュースリリース :Radicati Group
http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20030214/16/
[7] bsfilter: NABEYA Kenichi,
http://www.h2.dion.ne.jp/~nabeken/bsfilter/