本校におけるスパムメール対策

専門技術班　中原　勝俊

１．はじめに

現在スパムメール（以降スパムと省略）は世界的にも大きな問題になっており、佐世保高専にとって、というよりも管理者にとっては常に大きな悩みの種でした。スパムとは、受信側が望んでいないのに送られてくる、いわゆる迷惑メールのことで、特に 2005 年に入ってから日本語によるスパムが大量に届くようになりました。しかもその内容が教育的に問題であり、というよりもいわば法に触れるような内容のものばかりで、さらにはサブジェクトが日本語のため不快な文字列が否応なく目に入ってしまいます。そこで、とにかくこれらをなんとかしたいと思い、スパム対策に本格的に取り組むことにしました。

２．スパムの現状

迷惑メール相談センター（（財）日本データ通信協会内：http://www.dekyo.or.jp/soudan/top.htm）の調査による平成１６年度上半期の日本におけるスパム（迷惑メール）の現状について見てみると、約７割強が携帯電話向けのスパムであり、残りの３割弱が PC 向けのスパムという現状でした。しかし、最近の調査では、携帯電話各社の努力により携帯電話向けのスパムは大幅に減少しており、反して PC 向けのスパムは増加しています（http://www.dekyo.or.jp/soudan/anketo/sub1.htm 参照）。つまりインターネットに接続している各組織（サイト）において、メールを管理する部門がしっかりと対策できていなければ、そのサイトはスパマー（スパム送信者）にとって格好の標的になってしまうということになります。なにもこれはインターネットサービスプロバイダ（ISP）等のインターネット接続業者だけの話ではなく、佐世保高専もその中に入るのは言うまでもありません。メールの送受信おいて、送信者認証などの抜本的なしくみの改革が普及しなければ、これからもスパムは一向に減ることはなく、それぞれのサイトが自分達で対策するしかないのが現状なのです。

2.1 スパムの送信手段

現在のスパムの送信手段は、初期の頃に比べて巧妙化、悪質化しており、その方法は大まかに以下のようになっています。

- **送信者を偽った送信（知人を装った送信）**
- **架空アドレスに宛てた送信**
- **自動収集や収集業者より入手したアドレスへの送信**
- **複数の ISP 等を渡り歩いての送信**
- **外国のサーバを経由した送信**

スパマーは、そのほとんどが送信元を偽って送信しており、最近ではフィッシングや出会い系サイトへの誘導といった悪質なスパムが日本語で届くようになっているので注意が必要です（以前は英語のスパムがほとんどだったので、多くの人はメールを見ることもなく削除することも多かったと思われ

ます）。また、図１のようにウィルスを利用してセキュリティ的に脆弱な一般家庭などのたくさんの PC を感染させ、それら PC（**ゾンビ PC** という）を介して大量にスパムを送信するという手法が現在主流となっています。そのためスパムによる大量のトラフィックがインターネットを席巻しており、これもまた大きな問題となっています。いずれにしても今のスパムは、明らかに騙そうとする意図が感じられ、非常に悪質でやっかいになってきています。

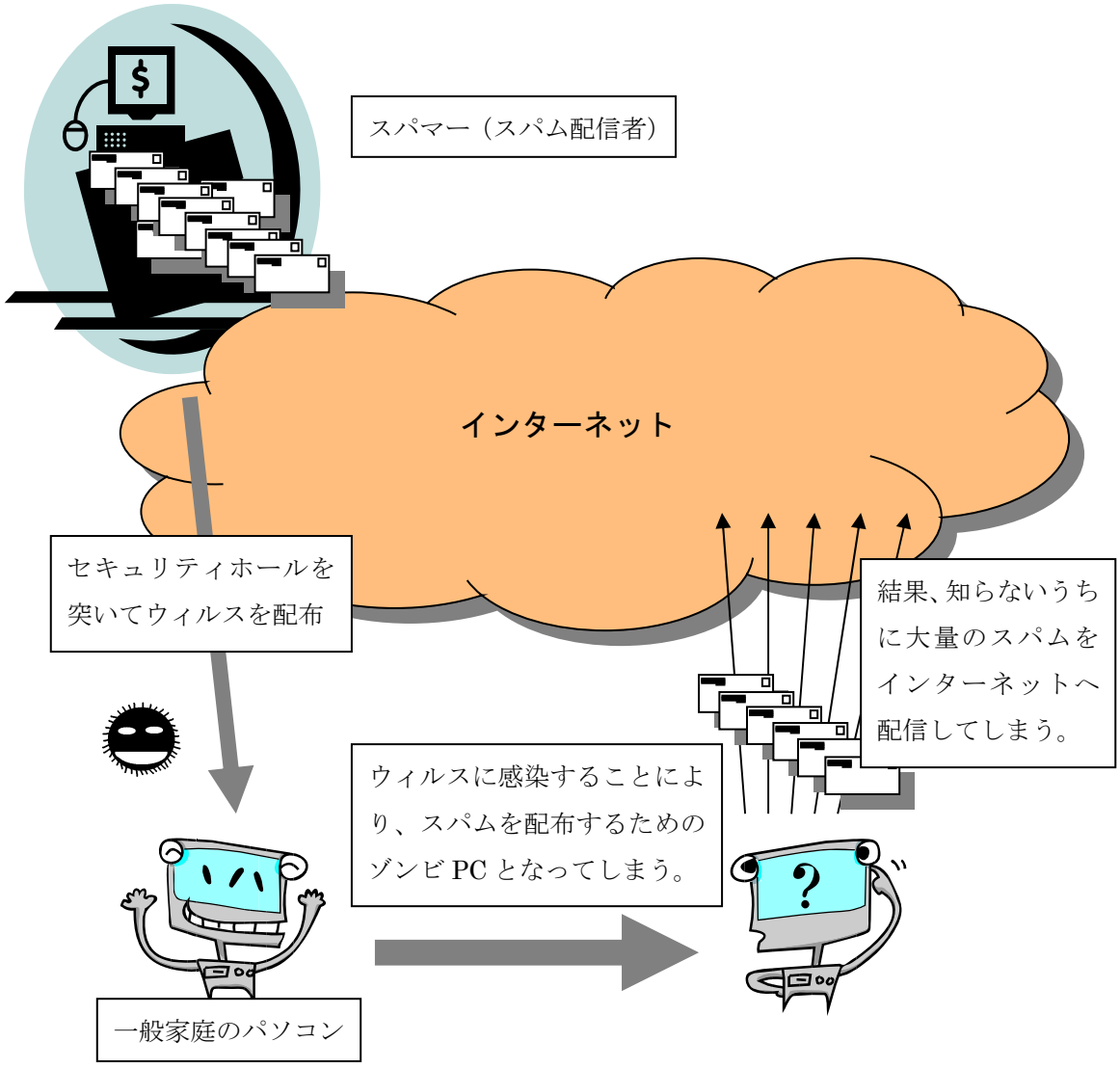

図１．ゾンビ PC によるスパムの配信

それでは本校において、これまで行ってきたスパム対策の経緯について述べていきます。

３．MUA（メールソフト）の変更

最初はサーバ側で検閲するのはためらわれたので、個人でできる対策を考えました。とりあえず普段利用するMUAを変更したり、POP3等でメールを受信する際にチェックするソフトウェア（POPFileやprocmailなど）を利用する方法を考えました。前者はMUAを変更するので抵抗があるのですが、後者はMUAを日頃使い慣れているものから変更しないでよいという利点があります。ただし、応答時間や使い勝手の点では劣ります。また、なれないと設定も難しいという点も問題となります。そこで、とりあえず簡単にできる前者の方法を選択しました。私の場合、具体的にはMUAをSylpheedからThunderbird（http://www.mozilla-japan.org/products/thunderbird/）に変更しました。もちろん通常のMUAならフィルタリング（メールの振り分け）機能は付属しているので、わざわざMUAを変更しなくてもよいような気もしますが、Thunderbirdを採用した理由は、「迷惑メールにお別れを、Thunderbird は、賢い迷惑メールフィルタ....」という点が大きく宣伝されていて、そこに興味を惹かれたためです。

3.1 Thunderbird

結論から言うとThunderbirdへの変更は正解でした。基本的にはMozillaと同じなのでNetscape Navigator付属のMUAと同じと思えばよく、特に問題なくSylpheedから移行することができました。また、Linux版とWindows版があり、IMAPと組み合わせることによって、どのような環境においても全く同じように利用できるという利点もあります。具体的には、仕事部屋からでも、情報処理センターからでも、さらには自宅からでも全く同じ状態でメールを見ることができて非常に便利です。また、問題のスパム対策ですが、これもまたボタンをワンクリックするだけでスパムを学習していくので、非常に簡単になっています。しかも使えば使うほど精度があがってくるので、日に日にスパムが正確にフィルタリングされていくのが最初は嬉しくてしょうがありませんでした。フィルタリングされるというのは、スパムと判断されたら自動的に［ゴミ箱］やその他のメールボックスに移動するという動作のことです。誤認識もあるので私の場合、一旦[SPAM]というフォルダに移動した後、確認してから削除することにしていました。

４．サーバ側でのスパム対策

Thunderbirdのおかげで個人的には変なメールをいきなり目にすることはなくなりましたが、いくら学習型といっても誤認識はあるので、一応SPAMフォルダを確認する作業は行わなければなりませんでした。いくつかの管理アドレスがエイリアスで私宛に届くようになっているため、受信メールの数は膨大で、これはいささか気の滅入る作業でした。しかし、このような対策をされていない人にとっては、おそらく気が狂わんばかりと言うと大げさかもしれませんが、大変なストレスになっていることはまず間違いありません。実際に「なんとかしてくれ！」という声をよく耳にしていました。そこで、いよいよサーバによるスパム対策に着手することを決心しました。サーバ側でスパム対策を行うことが妥当か妥当でないか議論が分かれるところですが、現状ではすでに多くの組織で同対策は実施されていることから、世の中の流れはサーバによるスパム対策は一般的になっているものと考え実施に着手しました。まずはスパム対策ソフトとして有名なSpamassassinを利用することにしました。

4.1 Spamassassin

Spamassassin（http://spamassassin.apache.org/）とは、Web サーバで有名な Apache の開発元で開発が進められているオープンソースのスパム対策ソフトウェアで、現在世界中で最も利用されていると思われるスパム対策ソフトウェアの一つです。Spamassassin は、「テキスト解析と複数ブラックリストを組み合わせてスパムを検知するメールフィルタ 」というもので、正規表現によるマッチングとベイジアンフィルタによる学習もできるフィルタリング方式のスパム対策です（しかし、残念なことにベイジアンフィルタは日本語に対応していません）。基本的には、サブジェクトや本文中に現れる文字列が、スパムの特徴として登録してあるデータベースのデータと照合し、一致すればポイントを加算していき、それがある設定値を越えた場合にスパムと判断するという仕組みです。また、スパムと判断されたメールは、 "X-Spam-Flag: YES"というヘッダが付加され、この情報を元にユーザーは、MUA の振り分け機能を使ってスパムを振り分けることができます。また、明らかにスパムであるのにスパムと判断されなかったり、まともなメールがスパムと判断された場合は、学習を繰り返していくことによって最終的に非常に高い精度でスパムを検出できるようになるということです。実際に運用を開始して私宛に届くメールにこのヘッダが付加されているのを見て、Spamassassin がちゃんと動作していることが確認できましたが、学習型ということもあって、最初はスパムの検出率はそれほど高くありませんでした。そこで、Spamassassin 用に書かれたブラックリストをインターネットより入手して、スパムの判断基準をいろいろと変更し、試行錯誤を繰り返しながら試験運用を行いました。結果として Spamassassin の場合、個人的に利用するような環境においては、MUA で行う場合と同様効果は大きいと思われますが、組織で運用するという環境においては、スパムの判定基準が難しく（一人一人の基準が違う）、スパムと誤ってはいけないような重要なメールを誤認識することがあります。そのような理由から、組織のサーバ側による運用には多少難があると感じられました。また、基本的にメールは配信されてしまいますので、例の不愉快なメールも見ることになってしまいます。さらに個人的にスパム対策されていた人の障害にもなっていたこともあり、実質一月程度で Spamassassin の運用は断念しました。

4.2 sendmail との決別

スパム対策には様々な方式があります。Spamassassin などは、図２のように「これはスパムと思います。目印を付けときましたので、後の処理はそちらで頼みます」という感じのフィルタリング方式のスパム対策ソフトです。確かに本来ならばこのように利用者にスパムかどうかの判断を委ねる方法が正しいと思いますし、トラブルも少ないと思います。しかし、スパムの数があまりにも多く、届いたスパムをいちいち削除することや、また、そのたびに不愉快なメールを目にすることに正直うんざりしていたので、できれば明らかにスパムと分かるメールはあらかじめブロックしたいというのが本音でした。また、利用者が多い Outlook Express のように、ヘッダによるメールの振り分け機能がない MUA には、この方式はあまり意味がありません。そこで次に取り組んだのは、ブロッキング方式のスパム対策でした。実はこの方式は、以前より sendmail の設定を利用して、私宛に届くスパムの From アドレスや IP アドレスを元にブラックリストに登録するという対策を地道に行っていました。しかし、これらの情報はまったく当てにならない上にその数は膨大で、いわばやっても意味がない作業と言ってもおかしくありませんでした。そこで、以前より注目していた「**浅見秀雄氏による Selective SMTP**

Rejection (S25R)方式：http://gabacho.reto.jp/anti-spam/）」という方式の採用を考えました。ただこの方式は、MTA に postfix の利用が前提とされていたため、これまで採用することができませんでした。私は、佐世保高専のサーバが UNIX となり、UUCP で細々とメールの送受信を行っていた頃から十数年間ずっと、MTA に sendamil を利用してメールサーバの管理・運用を行ってきました。もちろんこの S25R 方式は方法論ですので、sendmail を利用することもできます。しかし、sendmail の設定が自在にできるほどのスキルは持ち合わせていませんし、設定ツールには未だに WIDE の sendmail.cf Generation Package CF を利用していたくらいです。ずいぶん以前より設定ツールを sendmail 付属の cf へと移行しなければならないと思ってはいましたが、なかなか踏み出すことができずにずるずるとここまで来ていたのが現状でした。そういうことからも思い切って MTA を変更するにはよいタイミングではあったのですが、そのような中、本当に postfix に移行しなければならない事態となってしまいました。佐世保高専では、ウィルス対策用のサーバにトレンドマイクロの InterScan VirusWall という製品を利用していたのですが、それは 2005 年 9 月をもってサポートが終了される製品で、早急に代わりのサーバを導入しなければならず、そのサーバに同じトレンドマイクロの InterScan Messaging Security Suite(IMSS)という製品を利用することが決まっていました。そして、この IMSS で推奨している MTA が postfix だったのです。sendmail でも可能ということでしたが、postfix が強く推奨されていて、実質 postfix でやってくれという意味だと受け取りました。このような経緯から長年使い慣れた sendmail との決別を決心することになったのです。

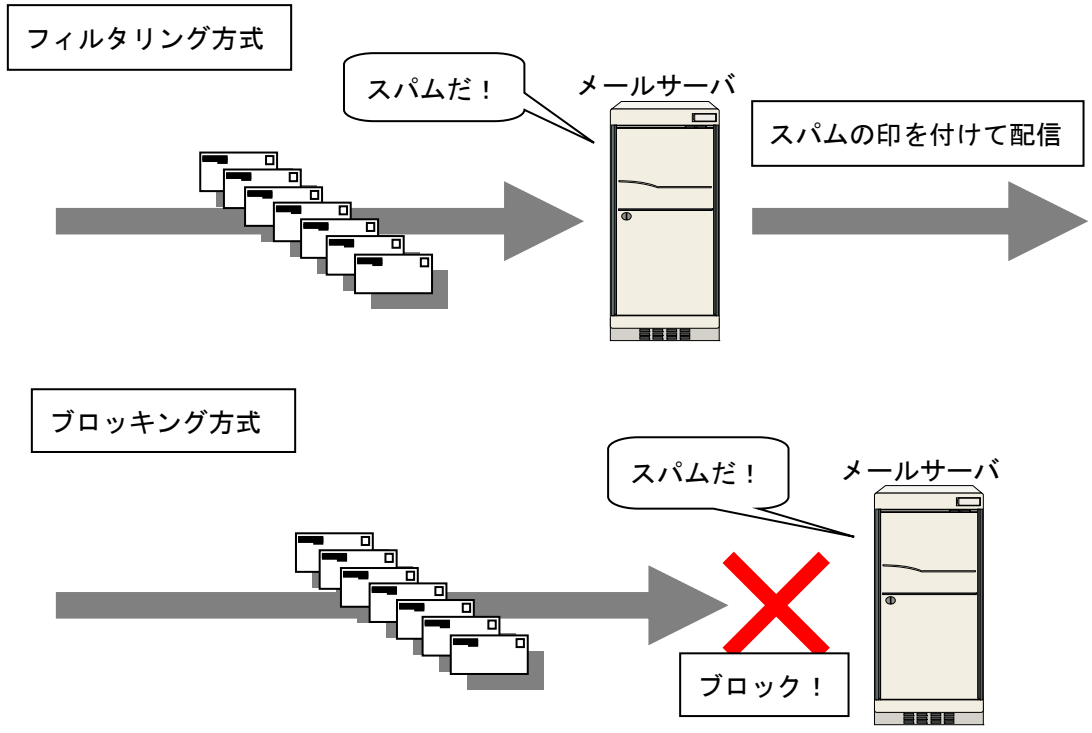

図２．フィルタリング方式とブロッキング方式

4.3 Selective SMTP Rejection (S25R)方式

*S25R*方式とは（浅見氏のWEBページより）、

「選択的SMTP拒絶方式」（Selective SMTP Rejection、略称：S25R）の要点

・逆引きできないクライアントを応答コード「450」（「後で再試行せよ」の意味）で拒否。

・逆引き名からメールサーバでないと推定されるクライアントを応答コード「450」で拒否。

・応答コード「450」による拒否に対して規則的に再試行する正当なメールサーバをホワイトリストで救済。

効果：スパムとウィルスメールの阻止率約99%。注意深く運用すれば正当なメールの受信失敗なし。

というもので、簡単に説明すれば「まともなメールは、まともなメールサーバからしか送信されない」ということを逆手にとった方式です。つまり、図３のようにゾンビ化してしまった一般家庭のPC等からのアクセスや、DNSでIPアドレスからホスト名を調べてもUnknownを返すサーバからのアクセスは拒否するという非常に単純なルールなのですが、それでいて高い効果を得ることができるというものです。とりあえずS25Rを導入する前にMTAをsendmail からpostfixに変更し、メールの送受信ができるように設定しなければなりませんでしたが、postfixは、５年電子制御の工学実験で学生にメールサーバを構築させる際に利用しているMTAでもあったので、sendmailからの移行には思ったほど手間はかかりませんでした。続いてS25R方式の設定を行いましたが、これも浅見氏のWebページに掲載されている通りに実行すれば問題なく設定することができました。最後にウィルス対策サーバのIMSSをインストールして、新しいメールサーバを利用した運用の準備はすべて整いました。

4.4 S25R方式による試験運用

最初は、試験的に週末だけこの方式で運用してみることにしました。週末の金曜日の帰宅前に設定を切り替え、週明けの月曜日出勤後に元に戻すという方法です。そして、試験運用の最初の週明けの月曜日、いつも通りにパソコンの電源を入れてメールを見ると、信じられない状況を目の当たりにしました。それまで私宛に届くメールは、土・日を挟むと百通を下らない数だったのが、それが数通しか届いておらず、最初は非常にまずい！と感じました。つまり、必要なメールまで拒否しているのではないかという思いが頭をよぎったからです。実際に事務部からも「メールが少なすぎる、何かするのなら事前に連絡をしてくれ」というクレームがありました。「スパムとウィルスメールの阻止率約99%」という謳い文句からすれば当前と言えば当前なのですが、まさか本当にここまで劇的に減少するとは予想していなかったのです。すぐに元の設定に戻そうとしましたが、よくよくメールを見ると、私宛に届いているメールで必要なものはすべて届いています。つまり、来なくなったのはあの訳の分からないメールだけでした。そこでまずログを見て、まともなメールサーバならば再送を繰り返すということでしたので、存在するユーザー宛に再送を繰り返しているSMTPサーバを早急にホワイトリストに登録しました。登録後それらのサーバからのメールを受け取ることが確認できたので、ログを監視しながらこのまましばらく試験運用を続けてみることにしました。

当初週末だけの試験運用のつもりで実施したS25R方式でしたが、運用し始めると結局元に戻ることができなくなってしまいました。というよりもはや戻る気がしなくなりました。つまり、それだけ高

い効果が得られたのです。ログを監視して ホワイトリストに正当と思われる SMTP サーバを登録するという作業を行わなければならなりませんでしたが、以前のように本当に正しいのか正しくないのかわからないような情報を登録していた頃の作業に比べると、それは遙かに実のある作業といえました。

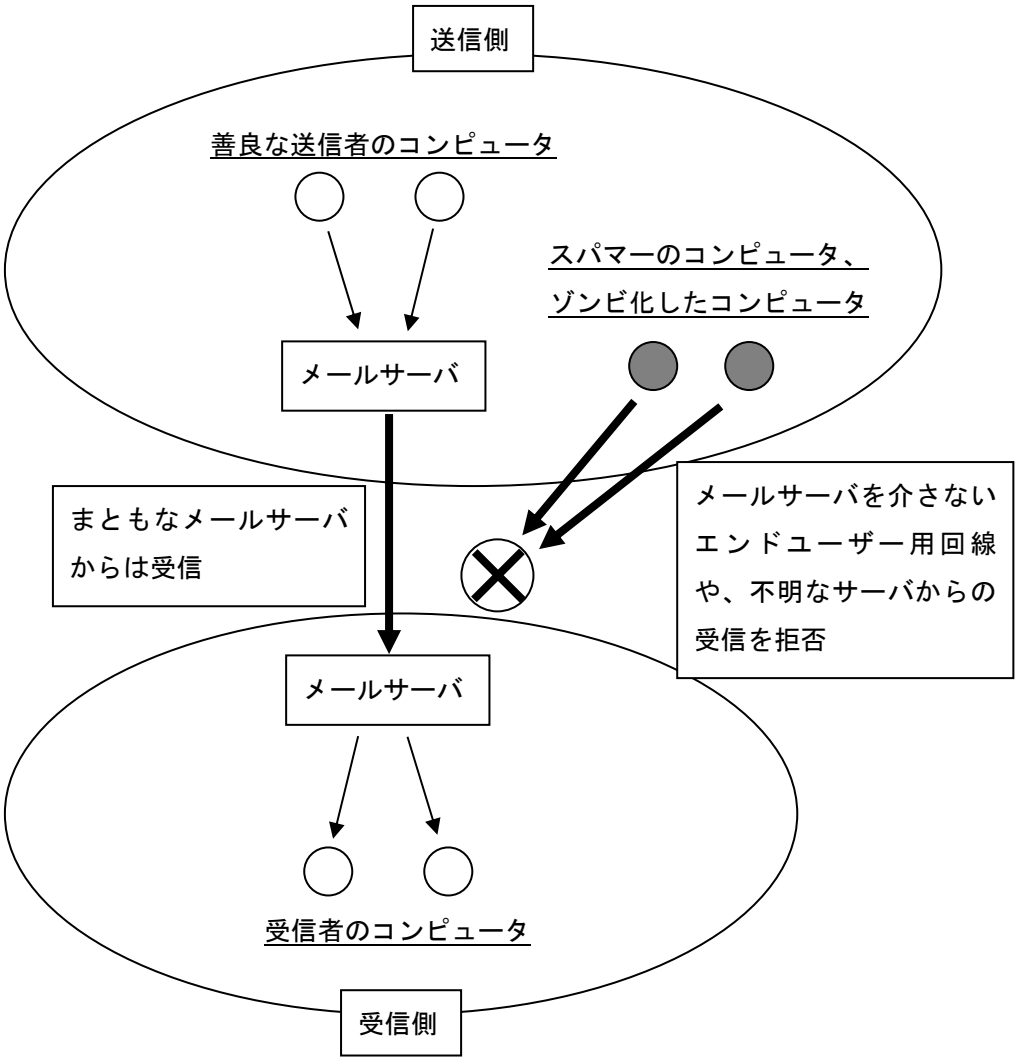

図３．S25R 方式（浅見氏 WEB ページより）

4.5 Greylisting 方式

S25R 方式による運用を始めてから一月もすると、ログを監視してまともな SMTP サーバをホワイトリストへ登録するという作業は、一回のログのチェックで一つあるかないかという程度まで減ってきていました。そのため作業自体は一週間に一度程度でもよかったのですが、そうすると最悪の場合、メールが届くのが一週間遅延するということもありえるため、ログの監視を止めるわけにはいきませんでした。また、ログを貯めれば貯めるほどチェック作業が大変になってしまうため、なるべく毎日チェックするように心がけていました。しかし、作業に対する慣れと、他業務に忙殺されたりするうちに、二日に一度、三日に一度というペースになることもしばしば起きてきたので、これではいけないと思い、スパム対策方式の一つである Greylisting（http://projects.puremagic.com/greylisting/）

という方式を併用する方法を取り入れてみることにしました。Greylisting 方式とは、簡単に言うと「一見さんお断り方式」、つまり、１回目の SMTP セッションに一時拒否エラーを返し、再送を行ったものだけを受信するという方式です。再送を受信する際の基準として、セッション中に得られる差出人、受取人、接続相手の IP アドレスの３種類を検査します。そして、それらの情報はデータベースに格納され、セッション中にポリシーに従って過去のデータと照合され受信可否の判断がなされるというものです。S25R がリストに登録されるまで再送を繰り返させるのに対し、Greylisting は、再送してきたことでデータベースに登録されます。さらに、その作業は自動で行われるので手作業による手間がかからないというのが最大の魅力です。これまで Greylisting 方式の採用に踏み切れなかった理由は、ログを監視するうちに分かったことなのですが、明らかに怪しいと思われるのに再送を繰り返す SMTP サーバの数がかなり多かったためです。Greylisting を採用すると、このようなサーバからもメールが届くようになり、結果的にスパムが増えることになってしまいます。そこで、ウィルス対策サーバの IMSS と組み合わせる方法を考えました。今回購入した IMSS は、スパム対策の機能も有していたため、前段で S25R+Greylisting、後段で IMSS でブロックすることにより、S25R 単独での運用に近い効果が期待できると考えました。

4.6 S25R+Greylisting+IMSS

postfix に Greylisting を実装方法に一つに、postgrey というパッケージを利用する方法があります。そして、この postgrey を S25R 方式に対応させるためには、**佐藤潔氏（http://k2net.hakuba.jp/）により作成された「Rgrey」**というパッチを利用することで実現できます。このパッチを佐藤氏の Web ページよりダウンロード・インストールし、さらに IMSS にスパム対策用の設定を追加して、**S25R+Greylisting+IMSS** による運用を開始しました。その結果、IMSS のログにはこれまでほとんど残ることがなかったウィルスやスパムのログが大量に残るようになりました。しかし、ログに表示されている情報は IMSS によってブロックされたスパムです。IMSS のスパム対策は、ウィルス対策と同様トレンドマイクロで常に更新されるスパムデータベースと照合してチェックが行われます。この設定により、現在全てという訳ではありませんが、私の手元にはスパムはほとんど来なくなりました。しかし、それでもすり抜けて来るものもあるので、それらについては最終的に Thunderbird でフィルタリングしています。

５．スパムのブロック率

2005/12 までの約一ヶ月間のログを解析し、この方式でどの程度までスパムがブロックされているか調べてみました。まず一次側の S25R+Greylisting 方式によるブロック率ですが、

S25R+Greylisting で遮断された件数　：154836 件
内部に転送されたメールの件数　　：29864 件
総数　　：184700 件

という結果となりました。これを見ると分かるように、ざっとこれだけでも約 83%のメールがブロックされています。さらに内部に転送されたメールは IMSS により検閲されますが、そこでスパムとしてブロックされた件数は、IMSS のログから 160 件という数でした。このログをもう少し詳しく解析すると、同一の差出人で複数の宛先は一つのログとしてまとめられており、実際の件数はこの倍近く多いこと

になります。つまり、内部に転送されるメールのうち、さらに 1%程度が IMSS によってブロックされていることが分かりました。また、この対策をもってしてもすり抜けるスパムも当然あって、その正確な数についてはログから判断することはできませんが、ログの解析結果に加えこれらを考慮すると、現在佐世保高専に届く全てのメールのうち、スパムとしてブロックされる割合は、85%以上ということになります。この割合を件数になおすと約 156995 件以上となり、一日あたり約 5233 件以上という数になります。つまり、スパム対策をしていなければこの数のスパムすべてを受け取ってしまうことになってしまうのです。

６．おわりに

我が国では、スパム問題に対応するために「**特定電子メールの送信の適正化等に関する法律（特定電子メール法）**」という法律が 2002 年に制定され、法的枠組みが整備されました。世界的に見ると、AOL や Yahoo!、Microsoft といった IT 業界のリーダーもスパム対策に乗り出しています。その他にも世界中で様々なスパム対策団体が発足しています。また、本校で導入しているトレンドマイクロの IMSS もそうですが、現在セキュリティベンダー等よるスパム対策用の商用ソフトウェアやハードウェア、さらには専用のアプライアンス（特定用途向けの専用装置）も販売されていることから、ウィルス対策と同様、スパム対策もビジネスとして成り立つほど問題は大きくなっているということが分かります。しかし、いくら法的に対策が強化されても、対策のための手段が講じられても、送信手法は年々巧妙化、悪質化し、今のところスパム自体は減っていないのが現状です。前述のスパム対策団体等により様々な対策や技術が提供されつつありますが、現在までのところスパムを根絶させるための抜本的な技術が一般に普及するためには、まだまだ時間がかかると思います。つまり、各組織が工夫して対策していくしかないという状況はまだしばらく続きそうです。

追記

S25R+Greylisting+IMSS 方式で運用を開始して数ヶ月、ほぼ順調に運用できていましたが、今年(2006 年）に入ったころからまたこの方式をすり抜けるスパムが目立ち始めました。そこで現在は、S25R 単独の方式に切り替えて運用しています。スパムにはまだ当分悩まされそうです。