単純なウィルスメール拒否システムについて

井 関 文 一 *

1．はじめに

近年インターネットの発達に伴って、ウィルスプログラムによる被害が急増している。中でもe-メールを媒介にして広まるウィスルは短期間の内に爆発的に感染先を拡大させ、被害を長期化させる恐れがある。インターネットサービスプロバイダーや大きな組織では、ウィルスのプログラムコードに対してパターンマッチングを行ってウィルスメールを駆除する市販のウィルスチェックシステムを導入しているところも存在するが、このようなシステムは一般に非常に高価で、組織の小さな大学などでは導入に消極的にならざるを得ない。

今回の研究では簡単なシステムでできるだけ多くの効果を得ることを目標に、UNIX（Linux）上で最もポピュラーなメールサーバプログラムの一つとして知られているsendmailに簡単なパッチを当てて、ウィルスメールの疑いのあるメールの受信を拒否するシステムを作成した。単純なシステムにも関わらず、これにより当大学では該当ドメインでのメール添付型のウィルスの被害が完全に無くなった。

2．開発の背景

ウィルスプログラムが添付されているメールは短期間に感染先を拡大し、被害を長期化する恐れがある。ウィルス駆除ソフトの普及に伴って、パソコンなどのシステム自体への被害は減少しつつあるが、駆除そのものや事後対応（自分のパソコンが新たに撒き散らしたウィルスメールへの対応など）に多くの時間と労力を強いられるのが現状である。

しかしながら市販のウィルスメールのチェックシステムは非常に高価なものが多く、またウィルスのプログラムコードに対するパターンマッチングのため新しいウィルスへの対応がどうしても一歩遅れてしまうといった欠点がある。

そこで今回、なるべく簡単なシステムで大きな効果を上げるために、UNIX （Linux）システム上のメールサーバプログラムであるsendmailに簡単なパッチを当てて、ウィルスメールの疑いのあるメールの拒否システムを作成した。

*東京情報大学総合情報学部情報システム学科

2003年6月11日受理

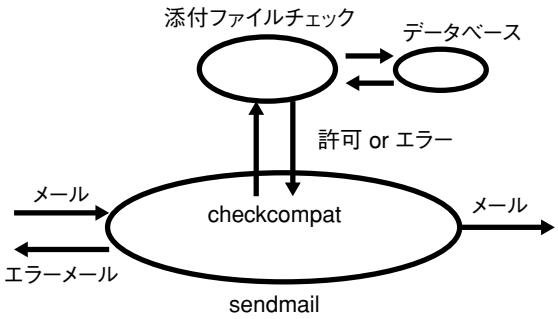

図1.　ウィルスメール拒否システムの概略

3．システムの概要

sendmailは非常にフレキシブルなメールサーバプログラムである。sendmailのソースプログラム中のconf.cにはcheckcompat関数[1)]が存在する。この関数はドメイン管理者がメール配信の制御をするためのものであり、この関数で特定のメールの送受信を制限することができる。

ウィルスメールでは、ウィルス本体は実行可能形式としてメールに添付されてくるのがほとんどである。今回のシステムではメールに添付されてくるファイルの名前を確認し、それをもとにメールの送受信の制御を行う（図1）。

システムの機能は以下の通りである。

1）添付ファイルの名称を見てデータベースにあるものと一致した場合、メールそのものを破棄する。
2）データベースを作成しない場合は、.DLL、.EXE、.COM、.BAT、SCR、PIF、.VBSなどの拡張子の付いたファイルを添付して来た場合、メールを破棄する。

1）の機能はウィルスメールの添付ファイルの名称を指定することによって、False Negative（ウィスルメールでないものをウィルスメールとして検知すること）をできるだけ小さくする機能である。しかしながらこの場合、データベースに登録していない種類のウィスルメールは検知できないので、新規（未知）のウィルスメールなどに対してはFalse Positive（ウィスルメールを検知しないこと）が発生する。一般に市販のウィルスメール駆除システムはこのタイプである。ただし、市販のシステムではパターンマッチィングの対象は添付ファイルの名称ではなく、ウィルスのプログラムコードである。

ウィルスメールに感染すると非常に大きな損害を受ける可能性がある。できれば新規（未知）のウィルスメールであっても拒否できることが望ましい。2）の機能はウィスルメールの疑いのあるメールを全て拒否する。すなわちFalse Positiveを 0 にする効果がある。従って、添付ファイルに .EXEなどの拡張子を持つファイルを添付できなくなる（False Negative）が、この場合はメールの差出人と受取人で、添付ファイルの拡張子を適当に変更することなどをお互いに合意していれば問題にはならない。また、第 3 者からの実行可能ファイルが添付されたメールを受け取ることはできなくなるが、むしろ見知らぬ相手にいきなり実行可能形式のファイルを添付して送りつけることの方が、ネットワーク上のエチケット（ネチケット）的にも非常識といえる。

1)、2）の場合とも、メールの差出人には該当ファイル名付きのエラーメールが返る。もし、ウ

ィルスがFrom（Reply）行を書き換えない種類のものであれば、ウィルスメールを発信している相手にメールが届くので、知らずにウィルスメールを出していることを相手に通知することができる。

4．結果

当大学では、平成14年の3月より研究（RSCH）ドメインで、9月より教育（EDU）ドメインでこのプログラムの運用を開始している（教育ドメインで運用が遅れたのは、筆者が教育ドメインの管理権限をもたないためである）。設定としては特にデータベースを作らず、特定の拡張子を持つ添付ファイルを拒否するようにしている。これはウィルスの中に添付ファイル名を自動的に変更するものが存在することと、データベースを更新するドメイン管理者の負担を軽減するためである。これにより該当ドメインでは、メールに実行可能形式のファイルを添付するタイプのものは、False Positive（ウィスルメールの検知ミス）0で検出可能である。

平成14年3月～平成15年4月までの研究（RSCH）ドメインでのメール総受信数は251,190件であり、そのうち1,256件（約0.500%）に対してウィスルメールとして受信の拒否を行った。また、平成14年9月～平成15年4月までの教育（EDU）ドメインでのメール総受信数は821,975件であり、そのうち1,511件（約0.184%）に対してウィスルメールとして受信の拒否を行った。両ドメイン合計のウィルスメール率は0.257%である。

図2のグラフに平成14年3月～平成15年4月までの研究（RSCH）ドメインでの全メールとウィルスメールの受信数を示す（全メールに関しては目盛りを100倍する）。全受信メールに対してほぼ一定の割合でウィルスメールが送られてきていることが分かる。

また図3のグラフに平成14年9月～平成15年4月までの教育（EDU）ドメインでの全メールとウィルスメールの受信数を示す（全メールに関しては同様に目盛りを100倍する）。教育ドメインではウィルスーメール率は低いが、1ヶ月に200～300件前後のウィルスメールが、ほぼコンスタントに送られてきているが、グラフの傾向から単調増加傾向に移る可能性もあるので注意が必要である。ただし、このデータは8ヶ月間のものでウィルスメールの傾向を調べるためには、今後最低でも一年間の統計をとりたいところである。

図4、5は、研究（RSCH）および教育（EDU）ドメインでのウィルスメールの種類を示している。やはりEXEファイルが一番多く、以下BATファイル、SCR（スクリプト）ファイル、PIF（ショートカット）ファイルの順で続き、COMファイルは非常に少ない。また、VBS（ビジュアルベーシックスクリプト）は現在1件もないが、最近VBSを使用したウィルスが出回り始めているので、今後は増加する可能性がある。図6に各ウィルスの割合を示す。

このウィルス拒否システムは簡単なシステムであるにもかかわらず、該当ドメインでは、運用を開始して以来、ウィルスメールによる被害は報告されていない（研究ドメインでは、システムの導入前は被害が頻発していた）。

実行形式のメールが送れないという苦情は、学生から1件だけ報告されただけにすぎない。学生からの苦情は、システムの変更を学生に徹底できなかったためで、システムの説明を行うことにより納得してもらった。また教員から、メールを出した覚えのないのにエラーメール（ウィルスメールの拒否報告）が返ってくるとの報告を受け、該当行員のパソコンがウィルスに感染していることを発見することができた。

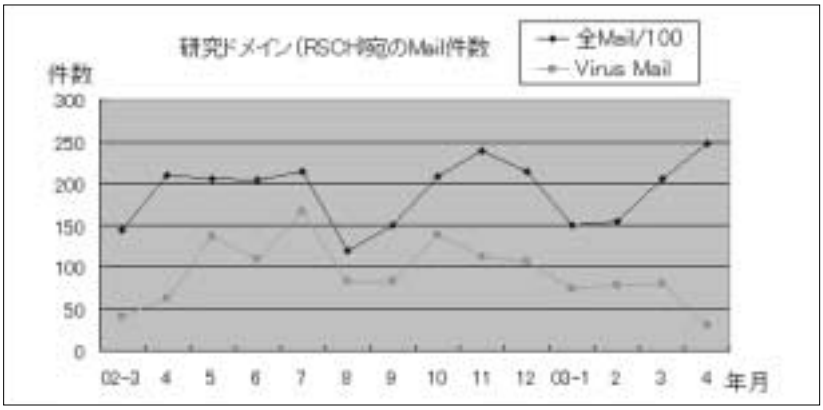

図2.　研究（RSCH）ドメインでのメール受信件数

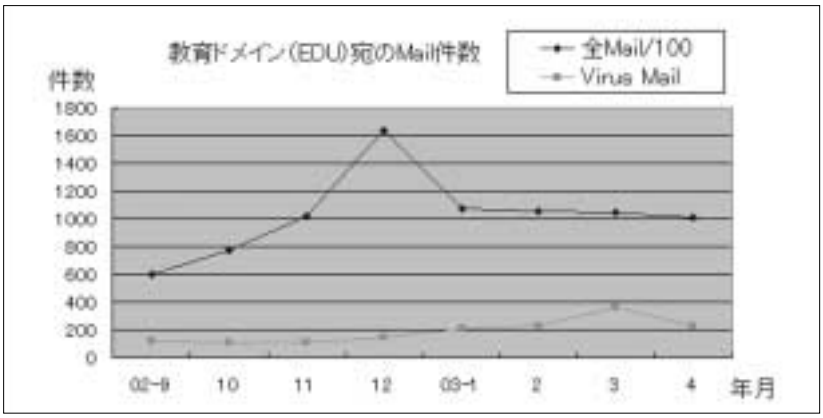

図3.　教育（EDU）ドメインでのメール受信件数

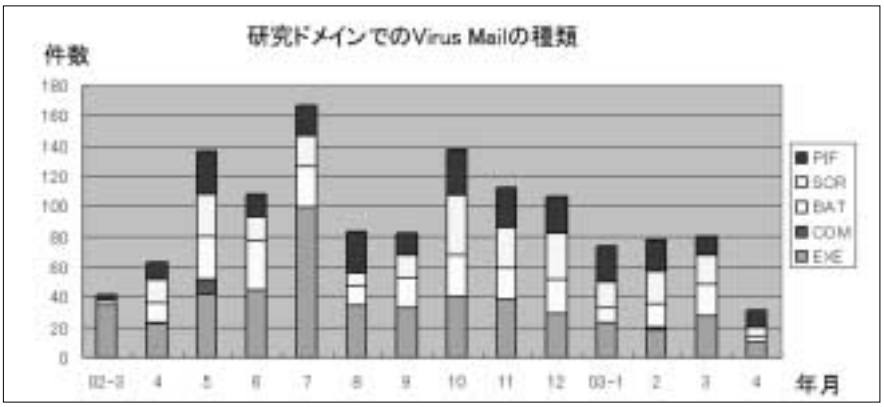

図4.　研究（RSCH）ドメインでのウィルスメールの種類

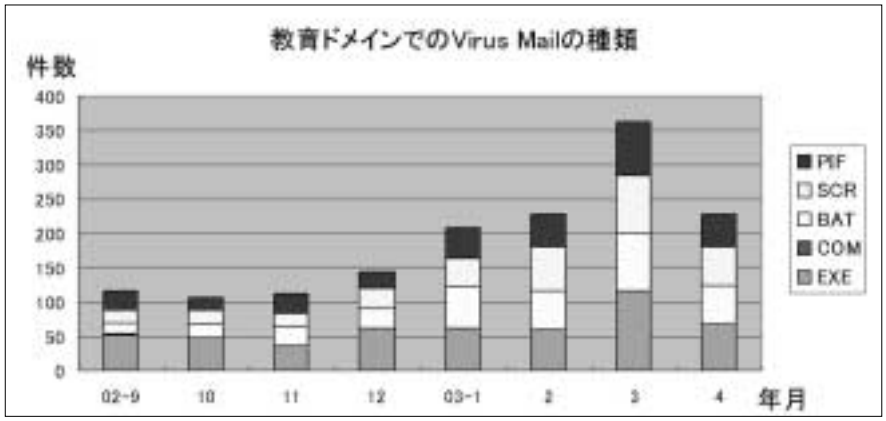

図5.　教育（EDU）ドメインでのウィルスメールの種類

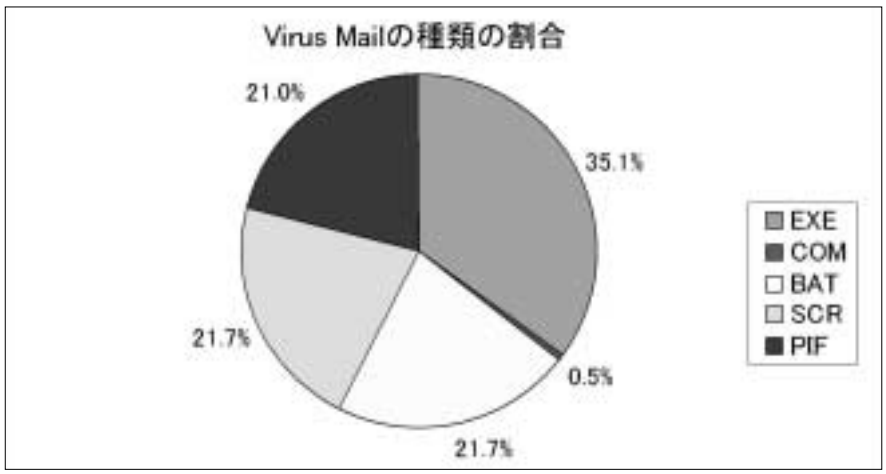

図6.　各ウィルスメールの割合

5．まとめ

このシステムでの問題点としては以下の点が挙げられる。

1）内部へのシステムの説明の徹底が必要。
2）外部の第 3 者へのシステムの説明が困難。
3）ウィスル以外のメールの受信拒否。
4）sendmail 以外のメールサーバには未対応。
5）マクロ形式のウィルスには未対応。
6）ウィルス部分のみを削除することができない。
7）Windows以外のウィルスには未対応

1）はシステムの運用前に必ず行わなければならず、内部の同意なしにシステムを作動させると混乱の元となる。

2）と3）の問題は、実行ファイルが添付されているメールを拒否していることを知らない第 3 者

が、メールを送って来た時に生じる問題であるが、先に述べたように、通常はメールの受取人が見知らぬ第３者が送って来た実行可能形式のファイルを実行させることはほとんどありえないし、送信者には、ウィルスメールの可能性があるためメールの受信を拒否した旨のエラーメールが返るようになっているので、この問題でのリスクは小さいと思われる。

4）では、sendmailのプログラム中に機能を埋め込んだことが原因であり、現在TCP Wrapperのようなラッパープログラムにより、この機能を実現するシステムの開発を行っている。この機能が実現すれば、sendmail以外でもSMTPを理解するメールサーバ全てに対応することが可能となる。また、ラッパープログラム（デーモン）であれば、機能を拡張することも容易にできる。例えば、送られて来たメールに対して、相手のメールサーバに該当アドレスが返信可能かどうかチェックすることにより、そのメールが匿名メールかどうかを知ることが可能である（図７）。

5）～7）の問題はシステムの機能の問題であるが、これらの機能を追加すると非常に大掛かりなシステムとなり、単純なシステムできるだけ多くの効果を得る最初の目的からは外れてしまう。この場合は市販のソフトウェアを利用した方が良いだろう。

今回作成したシステムにはさまざまな問題が存在するが、コストパフォーマンス的には非常に優れているシステムであり、Windowsを対象としたウィルスメールの対応には大きな効果があると言える。

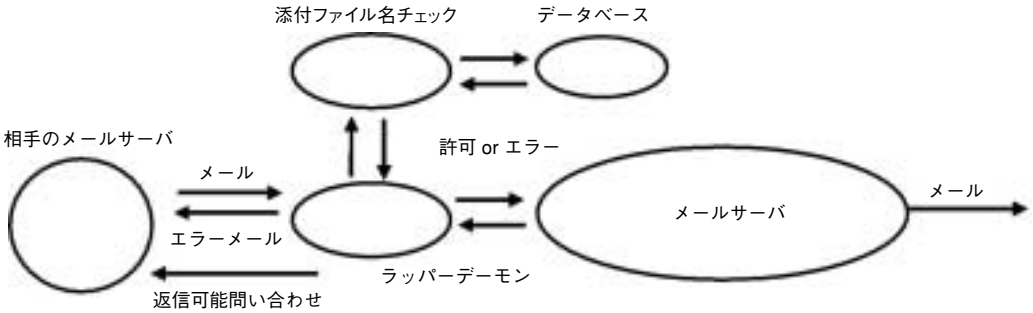

図7.　ラッパーデーモンを用いたウィルスメール拒否システムの概略

参考文献

1）B.Costales,E.Allman and N.Rickert,「sendmail 解説」,pp.230-339,Int.THOMSON Pub.Japan.,1994.

参照

http://www.solar-system.tuis.ac.jp/~iseki/sendmail/index.html