greylisting の運用について

吉田　和幸

大分大学　総合情報処理センター
〒870-1192 大分市旦野原
Tel. 097-554-7874　Fax. 097-554-7990
yoshida@csis.oita-u.ac.jp

概要

大分大学では統合メール管理システムを 2003 年 2 月から導入し、メールの DoS(Denial of Service)攻撃等で送られてくる宛先不明なメールを入り口のメールゲートウェイで拒否している。しかし、実在のメールアドレス宛ての spam メールに対しては、この方法では拒否することができないので、別の方法と組み合わせることが必要である。本学では、spamassassin と greylisting とを用いて、このような spam メールを拒否している。本稿では、greylisting の運用方針、運用経験について述べる。

キーワード

電子メール、spam メール対策、コンピュータウィルス、メールゲートウェイ

1　はじめに

近年、spam メールの増大が問題になっている。大分大学では、ウィルスを検出・除去するメールゲートウェイを導入し、学内 LAN とインターネットとの間を行き来するメールについてウィルスの有無を検査している。 spam メール対策として、そのメールゲートウェイで、学内各メールサーバのアカウントの有無を検査できる統合メール管理システムを導入し、運用している[1,2]。これにより、宛先が、実在しない spam メールを受け取らなくなり、メールの DoS(Denial of Service)攻撃に対して、効果があった。

一般に、宛先が実在するメールについては、宛先まで配送し、spam メールかどうかの判断は、受信者が行なうことになる。しかし、一旦受信してしまうと、送信者からみると、メールの配送が成功したことになる。spam 送信者にとってみれば、きちんと送信できたので、また spam メールを送ってくるかもしれない。このように spam メールは、受け取ってしまったら負けとなる。

本学では、2003 年 11 月から spamassassin[3]を、2004 年 4 月から greylisting[4]を、メールゲートウェイに導入し、spam メールの受信を拒否している。(spamassassin では、実際には、受信拒否をしたように見せかけている[5]。) 本稿では、greylisting の運用方針、運用経験について述べる。

2　Greylisting 方式

spam メールを送信するメールサーバは、特定の個人に確実にメールを送りたいというよりは、大量のメールを短時間に送信したいので、送信先のメールサーバの一時エラーに対しては、たぶん、再送処理を行なわない[6,7]。Greylisting は、このことを利用して、内容を見ないで、spam メールと通常のメールを分ける方法の一種である。

Greylisting 方式では、メールを受信すると、まず、メールサーバの IP アドレス、送信者、受信者のメールアドレス、を記憶して、(本文を受け取る前に)一時エラーを返して、再送を要求する。すぐに、再送されるメールは、spam の可能性が高いので、さらに、受信拒否をする。通常は、15 分から 1 時間後に、再送されるので、先ほど記憶していた IP アドレス、送受信者のメールアドレスと照合して、再送メールであれば、受信する。このように、一旦受信すれば、信用できるメールサーバとして、しばらくは、無条件で受信する。この時間関係を図 1 に示す。現在は、再送受付開始を 7 分 55 秒、greylist 状態時間切れ、autowhite 状態時間切れをともに 4 日としている。適当に流量があるメーリングリストは、常に autowhite 状態を維持し、遅れ無しに受信することができる。

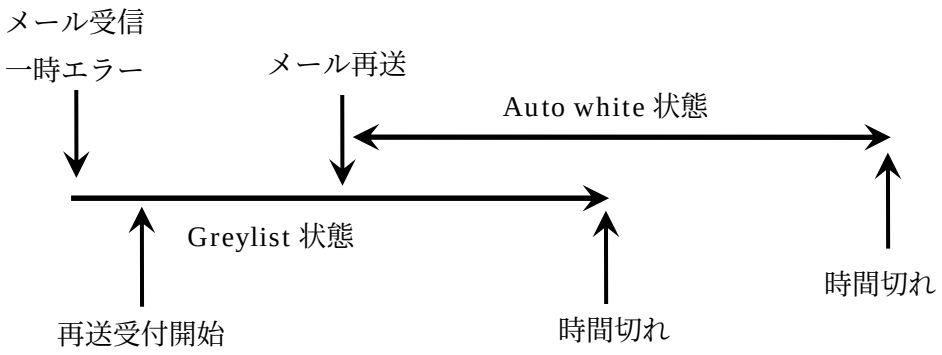

図１．Greylisting の時間パラメータ

3　想定外の動作をするメールサーバと Whitelist の作成

すべてのメールに上の greylisting を適用すると、再送が必要になり、メールの受信までに時間がかかることになる。spam の可能性があるメールは、なるべくゆっくり受信し、spam ではないと確信がもてるメールは、遅れ無しにすぐに、受信したい。そのため、信用できるメールサーバの IP アドレスを列挙し、その信用できるメールサーバから来るメールに関しては、greylisting 処理を skip するようにし、大部分のメールを、ほとんど遅れ無しに受信することができるようにした。

メールサーバの中には、greylisting 方式の想定外の以下のような動作をするメールサーバがある。

(1) 再送処理を行なわない。

ウィルス検査のためのメールゲートウェイと sendmail のような MTA との組み合わせ方によっては、再送処理をしなくなる。マニュアルにそのような設定例が載っている。

(2) 大手 ISP の中には、大量のメールを処理するため、複数のメールサーバを持ち、再送の度に、異なったサーバから送ってくる ISP がある。

数回再送されるうちに、偶然、最初のメールサーバと同じサーバから再送されると受信できるが、それまでに相当時間がかかる。

(3) spam メール対策であろうと思われるが、再送のたびに送信者のメールアドレスを変える ISP がある。

この場合、このままでは、まったく受信できない。

これらの問題を回避するためにも、信用できるメールサーバの whitelist の作成は、重要である。現在、500 件ほど、whitelist に登録している。/24, /16 のネットワークを丸々登録している場合もあるので、信用するメールサーバ数は、IP アドレス 500 個よりは、相当多くの IP アドレスをカバーしている。

4 運用

4.1 構成

メールゲートウェイの構成を図 2 に示す。メールゲートウェイは 3 台の PC で構成している。1 台は、Frontend となる sendmail，ウィルス検出削除システムの InterscanVirusWall，spamassassin へのインターフェースとなる milter-spamc，および milter-graylist を実行

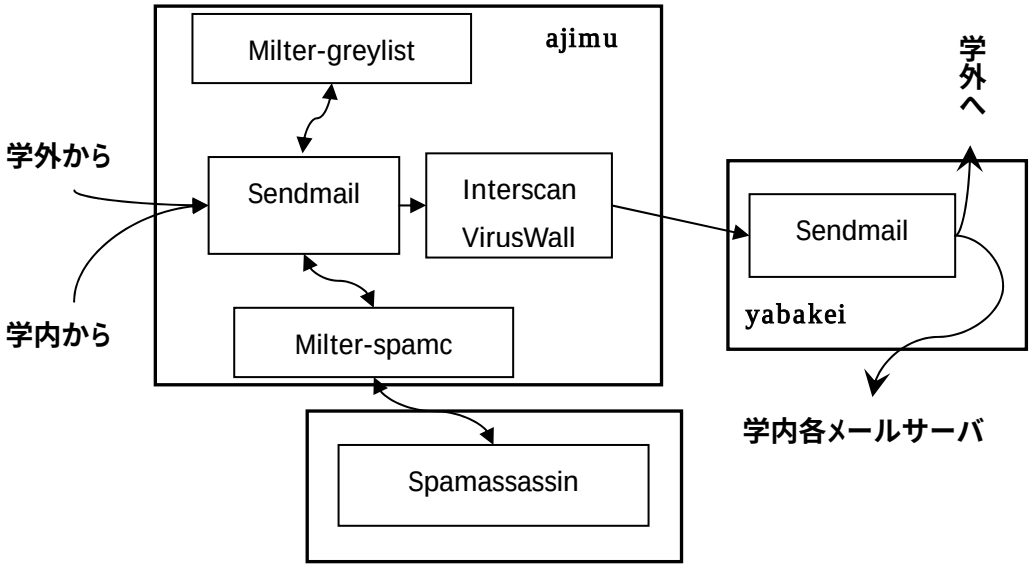

図 2. メールゲートウェイの構成

している。他の 1 台は、ウィルス検査後、学内、学外へメールを配送するための sendmail を動かしている。 3 台目は、spamassassin のみを動かしている。

4.2 運用状況

図 3 に greylist を通過した週ごとのメール数を示す。このグラフは積み上げグラフである。5 月いっぱい、各パラメータの調整、whitelist に登録するメールサーバの IP アドレスの選定等を行なった。6 月以降、安定して運用できている。Whitelist により greylist 処理を skip し、遅れ無しで受信するメールが約 70%、以前来たメールと同じサーバ、送受信者のため greylist が信用してすぐに受信するメールが約 15%，一時エラーを返した後、送信側の再送を待って受信したメールが約 15%となっているのがわかる。

図 4 には、greylist が結果的に受信拒否したメール数を示す。Greylist 方式では、直接、受信拒否をするわけではなく、一時エラーを返して、再送してこなかったメールが、結果的に受信拒否したことになる。4 月、5 月は、パラメーラを変更していたので、対応付けができす、一時エラーを返したメール数からの受信拒否したメール数を推定した。毎週、2 万通あるいはそれ以上のメールが、再送して来ずに、結果的に受信拒否したことになっている。

図 5 に、greylist による再送による遅れの分布を示す。8 月 8 日から 1 週間のうちに来たメールについて調べたものである。大部分のメールは 30 分以内に再送されてくることがわかる。26 分のところに特異的なピークがある。60 分のところにも、小さなピ

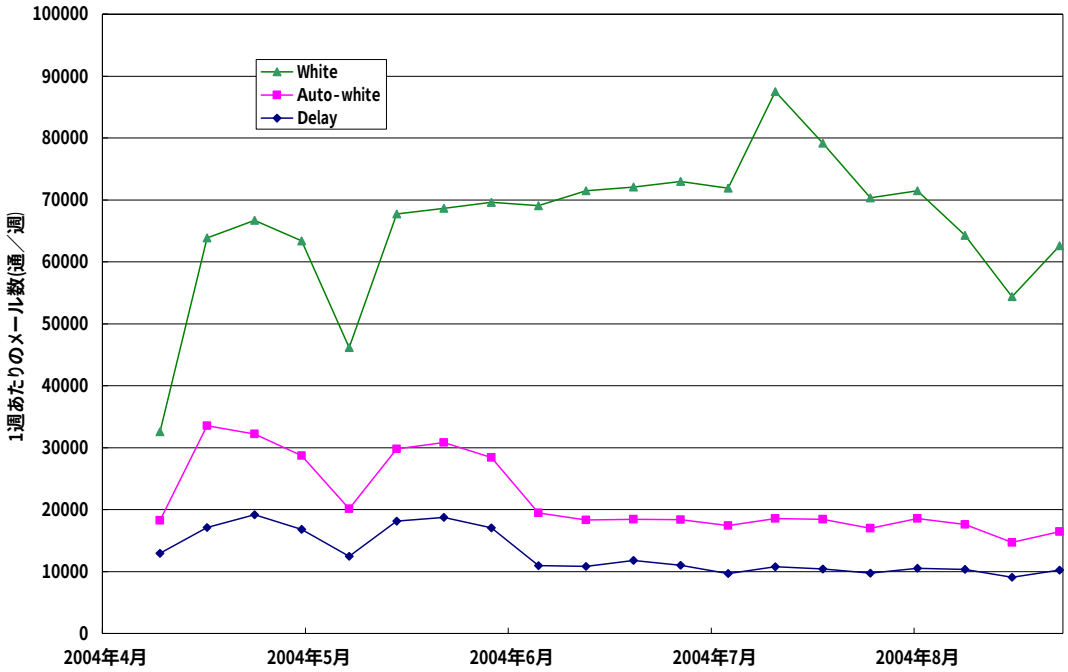

図 3 greylist を通過したメール数

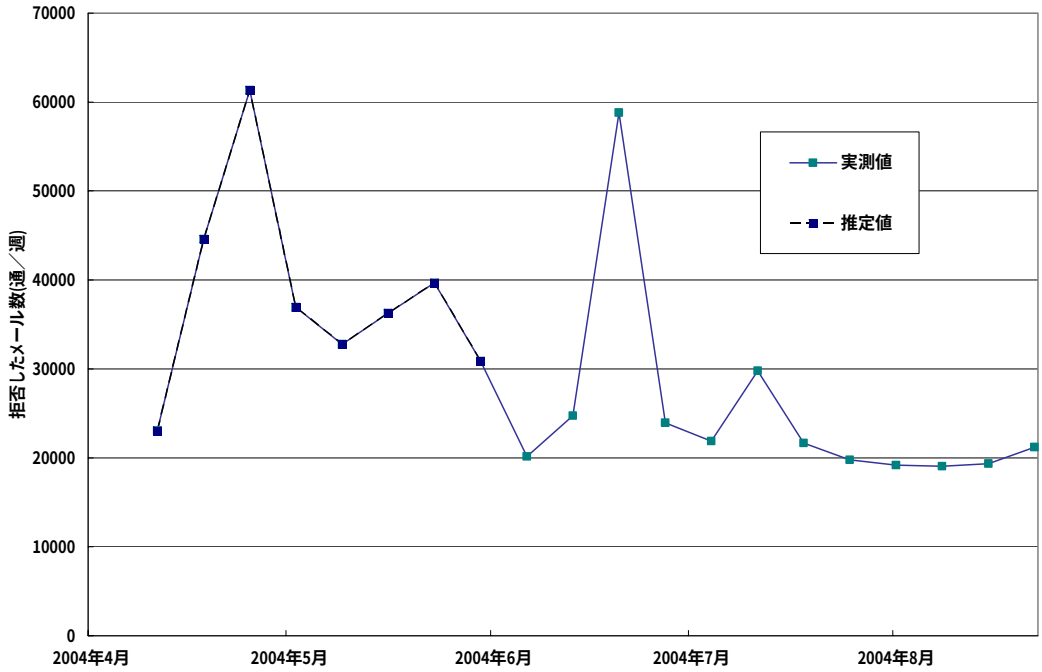

図 4. greylist が、受信拒否したメール数

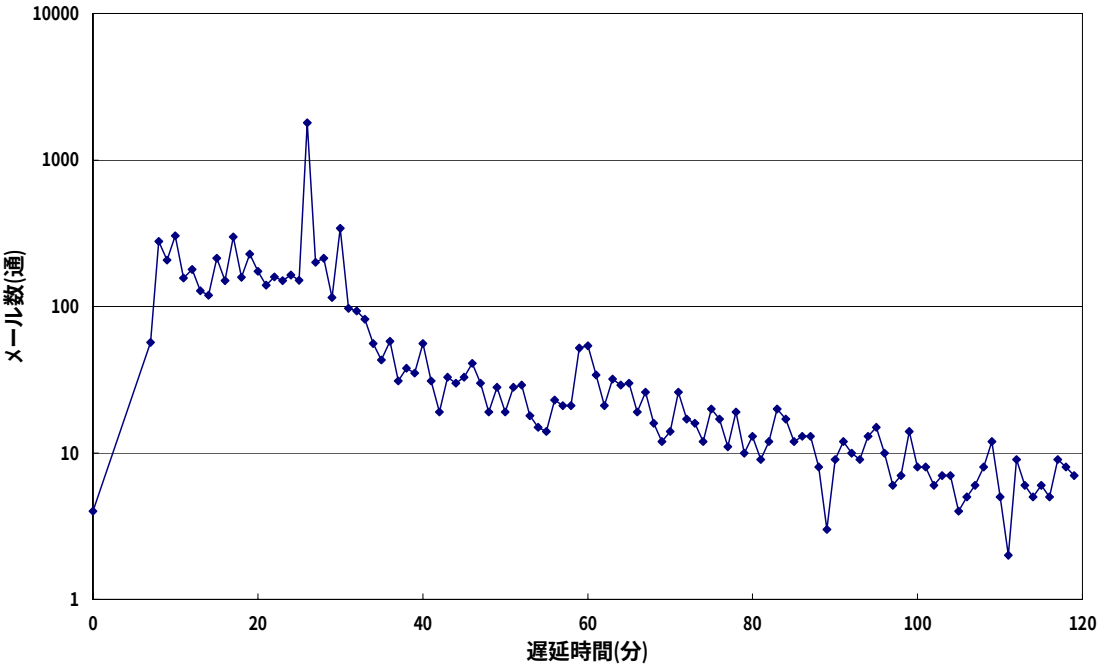

図 5. greylist による遅延時間の分布

ークがある。遅れ時間が長くなるとともに指数関数的に減少していくことがわかる。しかしながら、期限の 96 時間近くなって再送してくる例も少数ながらあった。

5　まとめ

spam メール対策としての greylisting について、その方式について述べ、4 月から 4 ヶ月ほどの運用状況について述べた。現時点では、greylisting 方式による spam メールの抑制は、大きな効果がる。さらに、コンピュータウィルスが自分自身を添付したメールを大量に撒き散らすとき、spam メール送信サーバと同じく再送処理を行なわない。このため、ウィルスの感染の広がり方が早く、検査削除システムのパターンファイルが間に合わないとき、100%ではないが、ウィルスの侵入をある程度抑えることができる。

spam メールにしろ、ウィルスメールにしろ、中継サーバを経由すると、greylisting 方式は、無力である。中継サーバは、中継を誰にでも許可している open relay なサーバばかりでなく、メーリングリストサーバ、利用者が行なう.forward による転送等も含まれる。この場合、それぞれのメールサーバの管理者の spam メール対策に期待するほかない。

参考文献

[1] 吉田、矢田、伊藤：spam メール対策と統合メール管理システムについて、情報処理学会分散システム／インターネット運用技術シンポジウム 2004 論文集,pp.37-42,2004.

[2] 吉田：LDAP を用いた統合メール管理システムについて、学術情報処理研究 No.7,pp.55-59,2003.

[3] http://www.spamassassin.org

[4] http://hcpnet.free.fr/milter-greylist/

[5] 吉田：メールゲートウェイにおける spam メールの検出について、情報処理学会 DICOMO2004 シンポジウム論文集、pp.493-496,2004.

[6] http://projects.puremagic.com/greylisting/whitepaper.html

[7] http://moin.qmail.jp