2007－DSM－47 (10)
2007／9／21

適用時間限定型greylistingとthrottlingによる迷惑メール対策の評価

石島 悌†, 平松 初珠†, 林 治尚‡,
池添 竜也*, 恩地 拓己*, 三瓶明希夫*

† 大阪府立産業技術総合研究所 情報電子部
‡ 兵庫県立大学 学術総合情報センター
* 京都工芸繊維大学大学院 工芸科学研究科

あらまし 迷惑メール対策において大切なことは，単に迷惑メールの排除を図ることだけではなく，見落としてはならないメールを確実に配送することである．また，さほど大きくない組織においては，その対策にかける人的・時間的コストを下げることも非常に重要である．大阪府立産業技術総合研究所では，業務時間外にのみgreylistingを適用し，throttlingを併用することによって，迷惑メールの排除を試みるとともに，対策のメンテナンスフリー化を実現した．本稿では，配送ログの解析とメール利用者に対するアンケート調査から得られた，本対策手法の有用性を報告する．さらに，大学の研究室に配置されたメールサーバにおける本対策手法の効果を報告する．

キーワード 迷惑メール対策，greylisting，throttling，メンテナンスフリー

Evaluation of Anti-Spam Method with Time Schedule Controlled Greylisting and Throttling

Dai ISHIJIMA†, Hatsumi HIRAMATSU†, Haruhisa HAYASHI‡,
Ryuya IKEZOE*, Takumi ONCHI*, and Akio SANPEI*

† Information and Electronics Department, Technology Research Institute of Osaka Prefecture
‡ Library and Academic Information Center, University of Hyogo
* Graduate School of Science and Technology, Kyoto Institute of Technology

Abstract In controlling spam mails, it is important not only to reduce spam mails, but also to deliver non-spam mails. It is also important to lower the cost in small and medium enterprises. The anti-spam method using greylisting only after working hours and throttling was implemented at Technology Research Institute of Osaka Prefecture. And we tried to reduce spam mails without maintenance of white list and database. In this paper, we describe the usefullness of this method from questionnaire survey and mail log analysis. After that, we report the result that we tried to reduce spam mails in the university laboratory with this method.

Keywords Anti-Spam method, Greylisting, Throttling, Maintenance-Free

1. はじめに

電子メールは，インターネット利用者にとってもっとも身近で，かつ，手軽なコミュニケーション手段の一つとして定着している．また，メールは，業種や規模を問わず多くの企業や事業所，そして教育研究機関などで広く利用され，我々の生活や社会活動になくてはならない存在となった．

このようにメールが有効に活用される一方で，迷惑メールの存在が大きな問題となっている．迷惑メールは，ネットワークの帯域やメールサーバの資源を浪費するだけでなく，それを受け取ってしまったメール利用者にとっても大きな負担となっている．

このような状況においては，必要なメッセージを確実に受信者に配送するとともに，不要なメールをできるだけ排除し，利用者の負担を軽減する

ことが，ネットワークやメールを運用するシステム管理者に求められている．

大阪府立産業技術総合研究所（以下，大阪府産技研）においても，近年，多数の迷惑メールが届くようになり，利用者から何らかの対策を求める声が寄せられるようになった．そこで，業務時間内はメールをそのまま通過させるgreylistingとthrottlingを併用した迷惑メール対策を導入した[1]．

本稿では，まず，この適用時間限定型greylistingとthrottlingを用いた迷惑メール対策手法の仕組みを説明する．そして，MTAのログ解析とメール利用者へのアンケート調査から，この対策の有用性を評価した結果を報告する．さらに，大学の研究室に設置されたメールサーバにおける本対策手法の効果を調べ，異なる環境においてもこの対策が有効であることを報告する．

2. 本迷惑メール対策手法の仕組み

迷惑メール対策にはいくつかの手法があるが，そのうち，greylisting[2]とthrottling[3]は，メールの中身を見ないので，比較的MTAにかかる負担が少なく，かつ効果の高い手法であるという評価を得ている．

これらの手法は，いずれも迷惑メールを送信してくるMTAの特徴的な挙動を逆手にとったものである．すなわち，あるメールが迷惑メールであるかどうかを判断するのではなく，送信MTAが迷惑メール送信用のMTAかどうかという点に着目して，迷惑メールの受信を減らそうとする手法である[4]．

greylistingは，迷惑メールを送信するMTAの多くが再送を行わないことを利用している．このため，あるMTAが過去に送信を行ったかどうかを記録しておくデータベースを必要としている．また，データベースに登録されていないMTAからのメールでは遅配が生じたり，迷惑メールの送信元ではないMTAでも再送を行わないことがあるため，特定のMTAをgreylistingの対象から外すためのホワイトリスト[5]をメンテナンスする必要がある．

大阪府産技研では，受信者に遅配を意識させないために，業務時間内とその前後の時間帯はgreylistingの学習のみを行い，メールをそのまま通過させるという対策を導入した．さらに，この対策により，greylistingで用いるデータベースやホワイトリストのメンテナンスフリー化を実現した[1]．

しかし，この方法では，業務時間内に送られてくる迷惑メールに対する抑止効果が期待できない．このため，クライアントに対してゆっくりと応答するthrottlingを併用している．

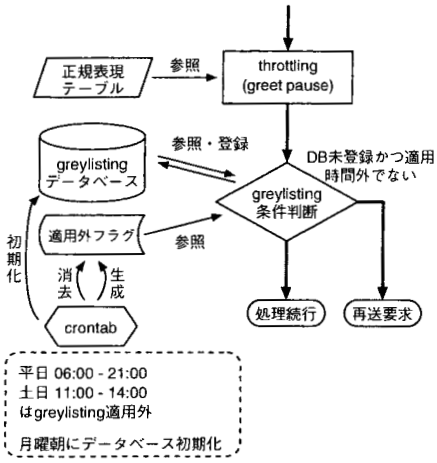

図1　本迷惑メール対策の仕組み

throttlingは，迷惑メールを送信するMTAはSMTPの確認応答手順を無視したり，タイムアウトが短いことを利用している．TCPセッションが確立してから応答を返すまでに，数秒から数十秒程度の遅延をかけることによって，迷惑メールを送信するMTAが配送に失敗することを期待するという手法である．

throttlingでは，TCPセッションを保持しまたま遅延をかけるので，プロセス数やTCPセッション数が増え，受信側MTAに負担がかかる恐れがある[4]．また，迷惑メールの送信元ではないMTAを無駄に待たせる可能性がある．

そこで，このような好ましくない状況を避けるため，正規表現テーブルを用いて，迷惑メールを送ってくる可能性が高いと思われるMTAには長い待ち時間を，そうでないMTAには短い待ち時間を設定している．

図1に，大阪府産技研での現在の適応時間限定型greylistingとthrottlingによる迷惑メール対策の仕組みを示す．

本対策を導入した当初は，greylistingで用いるポリシーサーバ（greylist.pl）に，greylistingの適用を除外する時間をそのままハードコーディングしていたが，これでは柔軟性に欠けるため，crontabからgreylistingの適用時間を制御するように変更した．

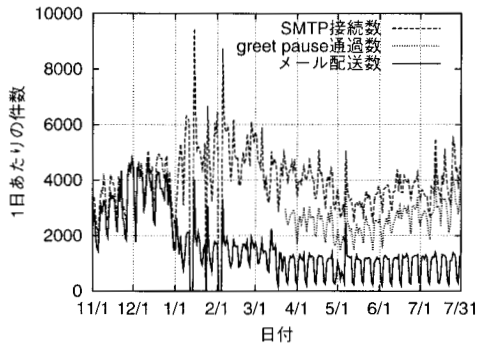

図2　SMTP接続数，配送数の変化

そして，平日は6時から21時まで，週休日である土曜日と日曜日は11時から14時までをgreylistingの適用対象外とした．

3. 本迷惑メール対策の評価

2007年1月より導入した本迷惑メール対策の効果と，この対策によって必要なメールが配送されなくなるなどの不具合が発生していないことを確認するために，MTAのログ解析とメール利用者へのアンケート調査を行った．

3.1 メールゲートウェイのログ解析

図2に，対策実施前後である2006年11月から2007年7月までの，大阪府産技研の対外プライマリメールゲートウェイにおける，SMTP接続数・メール配送数・throttling（greet pause）通過数の変化を示す．ただし，greet pause通過数については，記録を取りはじめたのは3月22日からである．

この図から，対策実施前の2006年12月末までは，SMTP接続数（破線）とメール配送数（実線）は，ほぼ等しいことがわかる．一方，対策実施後の2007年1月以降は，SMTP接続数に比較してメール配送数は大きく減少し，この差が本対策によって排除できた迷惑メールの件数であると考えられる．

対策実施直後の1月から3月中旬までと，それ以降で，メール配送数の傾向に違いが見られるが，これは，3月中旬までは，迷惑メール対策にさまざまな調整を行っていたことに起因する．週休日のgreylisting適用対象外時間を短く変更したのは3月の中旬である．受け取ってしまった迷惑メールの送信元などを調べ，throttlingの待ち時間の調整を行っていたのも3月中旬までである．それ以降は，本対策についてのパラメータ調整は行っておらず，対策に関するメンテナンスは行っていない．

SMTP接続数とメール配送数に7日周期の減少がみられるが，これは，週休日にはメールが減少することによると考えられる．この特徴は，週休日のgreylisting適用対象外時間を短くした3月中旬以降のメール配送数において，特に顕著である．

1月中旬と2月上旬に，SMTP接続数とメール配送数が0となった日があり，直後に大きな値をとっているが，これは電気設備の法定点検にともない，ネットワークをすべて停止させたためである．また，5月初旬に一時的にSMTP接続数とメール配送数が減少している期間は連休中である．その後大きな値となっているのは，連休明けに一時的にメールが増えたからであろう．

時期によって変動はあるが，4月以降のSMTP接続数は，平均すると1日あたり3700回程度である．一方，メール配送数は930通程度であり，およそ2800通の迷惑メールを排除できていることになる．また，greet pause通過数（点線）は1日あたり2500回であり，throttlingによって，1日あたり1200回程度，迷惑メールを送信してくるMTAが配送に失敗したと考えられる．

3.2 アンケートによる評価

迷惑メール対策の効果に関する利用者アンケート調査を2007年6月に行った．アンケートは，その案内を所内グループウェアの掲示板に掲載し，ウェブブラウザで回答してもらう形で回収した．アンケート項目は，以下のとおりである．

- 採用年度
- 対策前の迷惑メール受信数
- 対策による迷惑メール減少の程度
- 対策後の迷惑メール受信数
- 不具合の有無

回答は，メール利用者のほぼ1/3である41名より得られた．アンケートは，所属部署を通して利用者全員に回答を依頼したわけではないので，迷惑メール対策について関心のある利用者から十分な数の回答が得られたと考えている．

迷惑メールの受信数については，「毎日100通以上・毎日10通以上・毎日1通以上・毎週1通以上・毎月1通以上・受信なし」を選択肢とした．回収結果では，毎日100通以上迷惑メールを受信していたと回答した利用者はいなかった．

表1　採用年度と対策前の迷惑メール受信数

迷惑メール数	採用年 96以前	97	98	99	00	01	02	03	04	05	06	07	計
1日10通以上	8	4	3	0	1	1	0	0	0	0	0	0	17
1日1通以上	4	3	1	0	0	1	1	0	0	0	0	0	10
週1通以上	1	1	0	0	0	0	0	0	0	0	0	0	2
月1通以上	1	0	0	0	0	1	1	0	0	0	0	0	3
なし	0	0	0	0	0	0	0	0	1	3	1	4	9
合計人数	14	8	4	0	1	3	2	0	1	3	1	4	41

表1に，採用年度別の，迷惑メール受信数の各選択肢を選んだ利用者数を示す．この表から，多くの迷惑メールを受信しているのは，メールの利用期間が長い利用者に多いことがわかる．また，2004年以降に採用された職員からは，迷惑メールを受け取っていないという回答を得た．

同じメールアドレスを長期間使い続けていると，何らかの理由でそのアドレスが迷惑メール配送元に流出してしまう可能性が高くなることは容易に推測できる．逆に，同じメールアドレスを使い続けている期間が短ければ，流出の可能性は低くなるだろう．表1の結果は，このことを反映したものであるといえる．

最近では，ウェブページの開設にあたって，自身のメールアドレスをそのまま掲載しないように所内のガイドラインを定めている．この数年のうちに採用された職員に迷惑メールが届いていないのはこのことがうまく作用しているためと思われる．逆に，大阪府産技研がインターネットを利用しはじめた1996年当時は，むしろ積極的にメールアドレスを掲載する職員が多かった．ウェブページに掲載したままにしておいたメールアドレスが自動収集されたことも，多くの迷惑メールが届くようになった要因の一つであると推測できる．

迷惑メール対策の効果については，「1/10以下に減少した・1/3以下に減少した・少し減少した・変化なし・増えた」を選択肢とした．これに関する調査結果を表2に示す．なお，増えたという回答を選んだ利用者はいなかった．

表2から，多くの迷惑メールを受信していた利用者ほど，その効果を感じていることがわかる．逆に，受信していた迷惑メールの数が元々少なければ，その効果を感じることも少ないだろう．

表2　迷惑メール対策の効果

対策前の迷惑メール受信数	迷惑メールの減少 1/10	1/3	少し	不変	計
1日10通以上	3	7	5	2	17
1日1通以上	2	3	3	2	10
週1通以上	0	0	1	1	2
月1通以上	0	0	1	2	3
なし	0	0	0	9	9
合計人数	5	10	10	16	41

迷惑メールが減少していないと回答している利用者は16人いるが，そのうち9人はそもそも迷惑メールを受信しておらず，実質的に効果がないと答えているのは7人である．つまり，本対策の効果を実感しているのは，迷惑メールを受信していた32人中25人のおよそ8割である．1/10以下，1/3以下に減少したと回答している利用者は15人であり，利用者の約半数は，本対策でそれなりの効果が出ていると評価している．

その一方で，効果がないと回答した利用者のうち，4人は1日10通あるいは1日1通以上と，比較的多くの迷惑メールを受信していたと答えている．このように多くの迷惑メールを受信していた利用者の負担を軽減するためには，利用者の要望によりコンテンツフィルタリングなどを併用するなど，追加の対策を検討すべきかもしれない．

次に，現在受信している迷惑メールの数についての調査結果を表3に示す．

1日10通以上メールを受け取っていた利用者は，17人から6人へと大きく減少している．1日1通以上，週1通以上と回答している利用者は，それぞれ10人から12人，2人から8人へと増えているが，

表 3　対策前後での迷惑メール受信数の変化

対策後の迷惑	対策前の受信数					
メール受信数	(1)	(2)	(3)	(4)	(5)	計
(1) 1日10通以上	6	0	0	0	0	6
(2) 1日1通以上	10	2	0	0	0	12
(3) 週1通以上	1	6	1	0	0	8
(4) 月1通以上	0	0	1	2	0	3
(5) なし	0	2	1	1	9	12
合計人数	17	10	2	3	9	41

これは，対策前に1日10通以上，1日1通以上と回答していた利用者の迷惑メールが減少したためである．

この表からは，対策によって，受信している迷惑メール数が1日10通以上から1通以上に減少している利用者は10人，同じく週1通以上になった利用者は1人であることがわかる．1日1通以上から週1通以上に減少したのは6人で，受信なしになったのは2人である．あわせると，利用者のうち19人で比較的大きな効果が得られたことがわかる．

不具合の有無については，

- メーリングリストなどの到着順が入れ替わる
- メールマガジンなどが届かなくなった
- 特定のアドレスからのメールが届かなくなった
- 業務時間内にメールがすぐに届かない
- 業務時間外にメールがすぐに届かない
- その他（自由記述）

についてたずねたが，不具合があると答えた利用者は皆無であった．

greylistingによって，メールの遅配や，再送を行わないMTAにより，メールが配送されなくなることが懸念されたが，そのような不具合がないことがわかった．これは，業務時間とその前後にメールをそのまま通過させていることが有効に働いているからであると考えられる．大阪府産技研にメールを送ってくる相手も，深夜など，業務時間外にメールを送信することが少ないのであろう．

4. 大学の研究室への導入

本対策の有効性をさらに検証するため，ネットワーク構成や利用者のメール使用状況が大阪府産技研と異なる，京都工芸繊維大学大学院 電子システム工学専攻 プラズマ基礎工学分野の研究室のサーバへ，本対策を2007年8月4日に導入した．

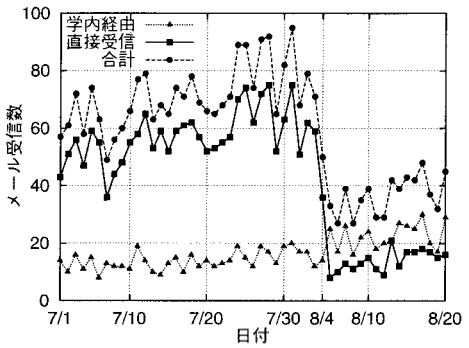

図 3　対策前後のメール受信数の変化

大学の研究室，特に理系の研究室では，夜間や土曜日にも教員や学生が活動を行っていることが多い．そこで，この研究室に本対策を導入する際には，教員と大学院生にヒアリングを行い，greylistingを適用する時間は，曜日にかかわらず24時から翌朝6時までとした．

本対策の効果を検証するため，まず，著者（石島）宛に届くメールの変化を調べた．その結果を図3に示す．

この図から，受信メール数（破線）は，1日あたり約70通から約40通へと，およそ半分になったことがわかる．これは，大阪府産技研での効果[1]である約1/4より小さい．

この違いを調べるために，研究室のサーバが直接受信するメール数（実線）と学内のサーバを経由して配送されるメール数（点線）を比較した．研究室のサーバが直接受信するメール数は約60通から15通へと減少する一方で，学内のサーバを経由するメールは20通前後であまり変化がない．このことが，対策の効果の違いに影響を与えている要因であると考えられる．

なお，学内のサーバはgreylistingとthrottlingの対象から外している．これは，学内のサーバを経由してくるメールによって，これらのサーバに負担がかかるのを避けるためである．

次に，時間帯別のメール受信数を比較した．この結果を図4に示す．

対策の導入によって，すべての時間帯でメール受信数が減少していることがわかる．しかし，greylistingを導入している夜間の減少の度合が，昼

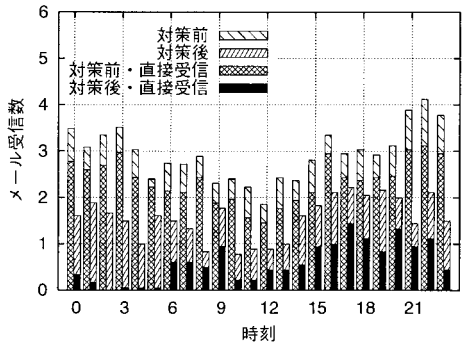

図 4　時間帯別のメール受信数

間とさほど変わらない．これも，学内のサーバを経由して配送されるメールによる影響を受けていることが原因の一つと考え，研究室のサーバが直接受信するメール数を重ねてプロットした．その結果，greylistingが有効である0時台から5時台においては，研究室のサーバが直接受信したメールの数がほぼ0であり，本対策の効果が表れていることがわかった．

さらに，この研究室においても，本対策の効果と不具合の有無などを調べるために，メールを利用する機会が多く，同じメールアドレスを使い続けている期間の長い博士後期課程の大学院生に，大阪府産技研で行ったものと同様のアンケート調査を行った．

本対策の効果については，元々受信している迷惑メールの件数が毎日数通程度，あるいは受信なしとのことで，迷惑メールは減少したが大きな効果は実感していないとの回答を得た．これは，大阪府産技研でのアンケート調査の傾向と一致する．

不具合についても，大阪府産技研同様に，ないという回答を得た．これは，greylistingを適用している時間が深夜に限定されていることや，研究室のサーバが再送を促した場合に，送信側MTAが学内のメールサーバへの再送を行い，メールの遅配などが生じないからであると考えられる．

5. おわりに

本稿では，適用時間限定型greylistingとthrottlingによる迷惑メール対策の効果を，大阪府産技研のメールゲートウェイのログ解析と利用者へのアンケート調査によって検証した．

ログ解析からは，1日あたり約1200回，throttlingにより，迷惑メールを送信してくるMTAが配送に失敗し，greylistingとあわせて，約2800通の迷惑メールを排除できていることがわかった．

アンケート調査からは，迷惑メールを受信している利用者の約8割が，本対策の効果を認識していることがわかった．また，本対策により，遅配などの不具合が皆無であることも確認できた．

大学の研究室にも本対策を導入し，その効果を検証した．ネットワーク構成や利用環境が異なるため，その効果に違いはあるものの，本対策はやはり有効であり，不具合もないことがわかった．

また，以上の検証結果から，greylistingとthrottlingが迷惑メール対策として有用であることがあらためて確認できた．

本対策も，他の迷惑メール対策手法と同様に，単独で用いているだけでは，迷惑メールを完全に排除することはできない．今後，利用者の希望に応じてコンテンツフィルタリングを併用するなど，メール利用者の負担をさらに減らすことを検討している．

本対策は，メールの遅配などの不具合が発生せず，導入後の調整を終えればメンテナンスは不要である．この特長を活かし，大阪府産技研の主たる支援先である中小事業者への普及を図りたい．

参考文献

[1] 石島 悌, 平松 初珠, 林 治尚, “メンテナンスフリーを目指した適用時間限定型greylistingによる迷惑メール対策とその効果”, 情報処理学会研究報告, Vol. 2007, No. 38, pp. 89—94, May 2007.

[2] 吉田 和幸, “greylistingによるspamメールの抑制について”, 情報処理学会研究報告, Vol. 2004, No. 96, pp. 19—24, Sep. 2004.

[3] 吉田 和幸, “throttlingによるspamメールの抑制について”, 情報処理学会研究報告, Vol. 2005, No. 39, pp. 69—74, May 2005.

[4] 三原 槙仁, 吉田 和幸, “Trottlingによるspam対策のためのメールサーバの分別について”, 情報処理学会研究報告, Vol. 2007, No. 72, pp. 43—48, Jul. 2007.

[5] 松原 義継, 只木 進一, “milter-greylistのための静的whitelist自動生成”, 情報処理学会研究報告, Vol. 2006, No. 80, pp. 43—46, Jul. 2006.