社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－ＤＳＭ－42／2006－ＱＡＩ－20（８）
2006／7／20

milter-greylist のための静的 whitelist 自動生成

松原 義継† 只木 進一†

† 佐賀大学 総合情報基盤センター
〒840-8502 佐賀県 佐賀市 本庄町 本庄 1 番地
E-mail: †{matubara,tadaki}@cc.saga-u.ac.jp

あらまし spam メール対策ソフトである milter-greylist には，特定の送信者メールアドレス，受信者メールアドレス，そして中継アドレスに対して greylisting を静的に無効にする設定がある．これを用いることで，信頼できる相手からのメールを milter-greylist による遅延を生じさせずにメールを受信できる．しかしながら，このリストの手動設定は人的コストが大きい．このリストを自動的に保守する手法について提案するとともに，登録実験について報告する．
キーワード spam メール, greylisting, 静的 whitelist

An automatic generator of static whitelists in the milter-greylist system

Yoshitsugu MATSUBARA† and Shin-i-chi TADAKI†

† Computer and Network Center, Saga University
1 Honjo Honjo-machi, Saga-shi, Saga-ken, 840-8502 Japan
E-mail: †{matubara,tadaki}@cc.saga-u.ac.jp

Abstract The milter-greylist, an anti-spam, system has a mechanism which allows mails to bypass the greylisting if their senders, recievers and relay hosts are listed in a static whitelist. This mechanism provides advantages of relaying without delay from reliable senders. Manual maintenance of this list, however, requires huge cost. We propose an automatic maintenance method of the static whitelist. We also report the experimental maintainance of the list.
Key words spam mail, greylisting, static whitelist

1. はじめに

電子メールが情報交換の重要な手段となる一方で，電子メールを介したコンピュータウィルスの蔓延や spam メールの増加が問題となっている．spam メールの対策として，各利用者のメールソフトウェアで行う方法とメール受信を行うサーバによる方法がある．後者の方法の一つとして miltergeylist がある．佐賀大学総合情報基盤センター (以下，当センター) でも，spam メール対策方法として milter-greylist [1] を採用している．

milter-greylist による spam 対策は，その性質上，いくつか問題がある．

- spam メールが再配送されると，受信してしまう．
- spam でないメールが，受信できない場合がある．

後者は，以下のような事情で発生する．

- 再配送の度にその中継ホストが変わるメール送信元が存在する．このようなメールは拒否され続ける．
- 再配送を全く行わないメール送信元が存在する．

spam メールの受信拒否が目的の milter-greylist によって，spam でないメールが受信できことは大きな問題である．そこで，milter-greylist には特定の送信者メールアドレス，受信者メールアドレス，もしくは中継ホストを常に拒否なしに受信させる設定が可能である．このように常に受信可と設定されたリストを，本稿では静的 whitelist と呼ぶことにする．このようなリストを作成することにより，信頼できる相手からのメールを遅延なく配送できる．

しかし，静的 whitelist への登録は spam 対策の効果を下げてしまう場合がある．例えば，中継ホストの許可範囲を広げることで，そこを経由する spam メールを受け取ってしまう場合があり得る．そのため，適切な静的 whitelist の調整が必要である．この調整を手動で行い，milter-greylist 以外にもブラックリスト及びコンテンツフィルタを組み合わせて対 spam メールシステムを運用する方法が報告されている [2]．静的 whitelist を手動で調整する場合，大きな組織の場合には，対応しなければならない送受信情報は膨大であり，調整には大きな人的コストが必要となる．そこで，本稿では，静的 whitelist の自動的保守の方法について提案する．

2. 設　　計

静的 whitelist に登録するのは，信用できる中継ホストである．このリストを自動的に保守するために，各エントリに成績を付け，その成績に応じた登録，削除を行うことで自動保守を行うことを考える．そのために，成績表を作成する．

始めに，信用できる可能性のあるドメインの登録について考える．これは成績の付け方を定義する設定表の作成である．この初期設定表成績表には，信用できる可能性のあるドメインを登録し，各ドメインに対する加点単位，減点単位，及び合格点を設定する．これは管理者が手動で行う．

次に中継ホストの登録について考える．ドメインの登録とは異なり，あらかじめ成績表に中継ホストの登録は行わない．定期的に whitelist を調査し，そこに登録されている中継ホストについて，対応するドメインを調査する．このドメインが設定表に登録されているドメインを含む場合には，成績表にこの中継ホストを登録する．すでに成績表に登録されている中継ホストの場合には，そのドメインに対応した加点単位を加算する．同時に，成績表に登録されている中継ホストが whitelist に登録されていない場合には，ドメインに対応した減点単位を減ずる．成績表の点数が 0 点以下となると，成績表からその中継ホストが削除される．成績表の点数が合格点を越えれば，静的 whitelist に その中継ホストが登録される．

milter-greylist の仕様上，静的 whitelist に登録されている中継ホストは whitelist に載らない．そのため，静的 whitelist の調査対象から外れることになるため，これ以後は成績の減点は行われない．

静的 whitelist の書き換えが行われると，そのリストが milter-greylist に導入され，管理者に変更内容がメールで通知される．

2.1 登 録 実 験

静的 whitelist の自動保守の状況を確認するために，milter-greylist への導入を行わずに登録実験を行った．milter-greylist を運用しているサーバは 2 台あり，これら 2 台で実験を行った．実験期間は，2006 年 2 月 7 日から 2006 年 5 月 31 日までである．実験環境は，OS が Solaris9 および Solaris10，milter-greylist のバージョンは 2.0，調査プログラムの開発言語は PHP5.1.4 である．

登録候補となるドメイン名と加点単位，減点単位，及び合格点を表 1 に示す．whitelist の調査は 1 日 1 回の頻度で行い，30 日間連続して登録されていれば最短で静的 whitelist が生成される．減点単位を 7 と設定したのは，whitelist の有効期間が 7 日間であり，登録されれば自動的に 7 点加点されることを相殺するためである．成績表の一部分を表 2 に示す．

静的 whitelist 候補数，つまり成績表に登録されている中継ホスト数と静的 whitelist 数の月日毎の変化をそれぞれ図 1 に示す．2 月 6 日に実験を開始し，翌日に候補数 1283 が登録された．その後，3 月 7 日に最初の静的 whitelist が生成された．現在も静的 whitelist 数は増加し続けている．

3. ま と め

spam メール対策の一つの方法である milter-greylist を導入した場合，信用できる中継サイトに対しても大幅な遅延や受信拒否を引き起こす場合がある．その対策として信用できる中継サイトを静的 whitelist に登録する方法がある．この静的 whitelist を自動保守する方法を提案し，実装実験を行った．

静的 whitelist の自動保守のため，whitelist への登録状況に基づいて成績表を作成し，その結果によって静的 whitelist を作成した．この方法に基づき実装実験を行い，静的 whitelist への自動登録が行われることを確認した．

この後は，この方法で生成された静的 whitelist を milter-greylist へ導入し，spam 対策としての有効性を検証したい．これと平行して，静的 whitelist の削除は milter-greylist の仕様上 手動であるので，この自動削除を検討したい．

文　　献

[1] E. Harris: “milter-greylist home page”. http://hcpnet.free.fr/milter-greylist/.

[2] 吉田：“メールゲートウェイにおける spam 対策について”，学術情報処理研究，9，pp. 37—43 (2005).

表 1　登録候補の設定

Table 1　Configuration of the entries

登録候補ドメイン名	加点	減点	合格点
ac.jp	1	7	30
go.jp	1	7	30
ad.jp	1	7	30
gr.jp	1	7	30
gmail.com	1	7	30

表 2　成績表の 1 部

Table 2　Part of the record

中継ホスト	ドメイン名	成績	加点	減点	合格点
130.153.8.30	ac.jp	26	1	7	30
130.153.8.31	ac.jp	26	1	7	30
130.158.105.49	ac.jp	7	1	7	30
130.158.118.46	ac.jp	26	1	7	30
130.34.136.2	ac.jp	3	1	7	30

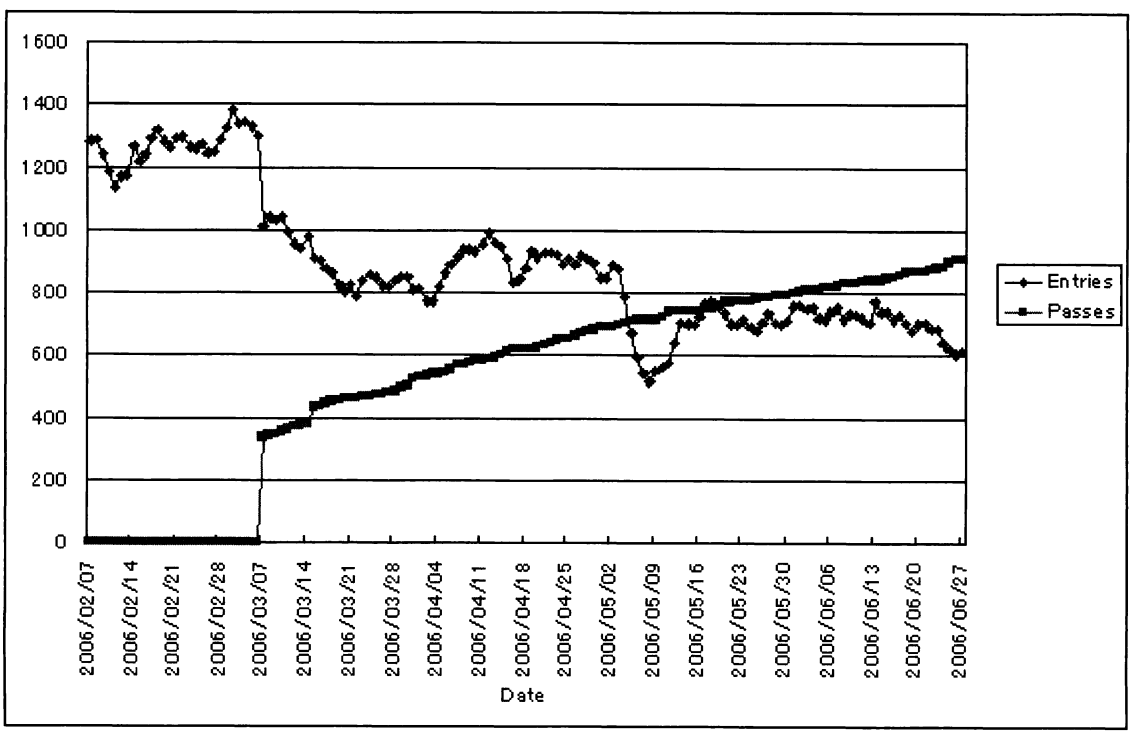

図 1　静的 whitelist 候補数および合格数の変化

Fig. 1　Num. of entries of static whitelist and num. of passes of it