6R-7

忘却を考慮したブラックリスト自動管理を用いたspam拒否システム

森崎 智博　　渥美 清隆
鈴鹿工業高等専門学校

1　はじめに

現在、インターネットにおいてspamが社会問題となっており、spamを拒否するために多くの研究[1, 2, 3]がなされている. spamを拒否する方法にフィルタリングと通信セッションを検査する方法がある.

代表的なフィルタリングの手法に、ベイジアンフィルタ[4]とSpamAssassin[5]がある. ベイジアンフィルタはspamメールとhamメールを学習させ、単語ごとにspamである確率を求め、それを用いてspamと判断する. SpamAssassinはテキスト解析と複数のブラックリストを組み合わせて、メールのspamらしさを点数化しspamかどうか判断する.

通信セッションを検査する手段として、RBL[6]のようなブラックリストを用いる方法と、greylisting[7]がある.

ブラックリストは第三者中継が可能であるサーバ、spamメールを送ったことがあるサーバなどのドメイン名(IPアドレス)を集めたものである. メールを受け取る時に、相手をブラックリストと照合し、存在していればメールを拒否する.

greylistingは、spam送信者は効率を求めるために、メールを再送してこないだろうという推測からsmtpセッションを張ってきた相手に一時的エラーを返すというものである. 再送してきたメールは受け取る.

本論文では、ブラックリストとフィルタリングを組み合わせた、より効果的なspam拒否システムを提案する.

2　ブラックリストとフィルタリングの統合

第三者中継が可能なサーバを集めたブラックリストは誰もが納得できる条件で集められているので一意的だが、spam送信IPを集めたブラックリストでは会社や自宅など、場所によって受信するメールが異なるために、場所によっては必要なメールが届かないことが起こり得る. どの場所でも通用するグローバルなブラックリストは存在しない. それぞれの場所でローカルなブラックリストを作成することでその問題は解消できる.

そこで、ブラックリストとフィルタリングを統合して使うことを考える. サーバに送られてくるメールをフィルタリングによってspam判定し、その結果によりそのサーバ独自のブラックリストを作成する. 本システムではベイジアンフィルタを用いるが、ユーザごとの学習が容易に設定できるという利点と、処理が遅いという欠点がある. ここでのブラックリストはフィルタリングの処理の遅さを助け、さらに、ユーザに柔軟に対応することができる.

ブラックリストに掲載された送信者から送られるメールは通信セッションレベルで拒否することになるので、フィルタリングのみを用いるよりも効率的になる. また、ユーザが必要とするメールを受け取れないという問題もブラックリストに追加する条件を調整することで避けられる.

3　システムの構築

インターネット空間、メールサーバの間にブリッジとしてPCを設置し、図1のようなspam拒否システムを構築する.

グレイリストはIPアドレス、spamが連続で送られてきた回数、spamが最後に送られてきた日付のリストで、ブラックリストはIPアドレスとspamが最後に送られてきた日付のリストである.

メールを送ってきた送信IPをブラックリストと照合し、存在していれば受信拒否をする. 存在していなければ、送られてきたメールがspam拒否システム内のベイジアンフィルタによりspamかどうか判定される. ここでspamと判定されると、送信IPがグレイリストに追加される. グレイリストにすでにその送信IPが存在していれば、spamが送られてきた回数を増やす. このときメールヘッダにspamと判定されたこ

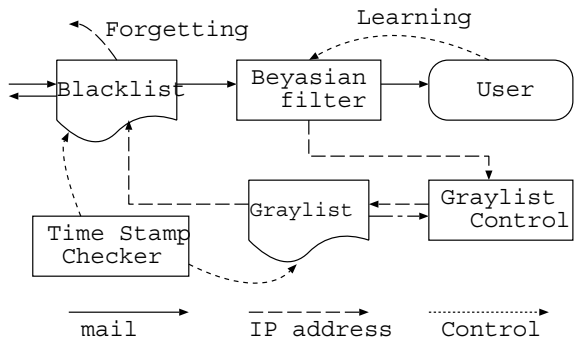

図 1: システムの構築

とが分かるようにフラグを加えておく. spam と判定されなかった場合は、グレイリストにその送信 IP があるかどうか調べ、存在していれば削除する.

この動作を続けていくことで spam のみ送信する送信 IP かどうかが分かるため、ある程度連続で spam が送られてくればその送信 IP をブラックリストに追加する. ブラックリストに存在し、メールを送信してこなくなった送信 IP はある程度の期間が経った後に、ブラックリストから削除される.

4 実験

2 回連続で spam と判定された場合にブラックリストに追加するという条件の元、本システムの運用を短期間行った.

表 1: メールの内訳

受信したメール	79
ham	55
spam	24
拒否したメール	3
合計	82

表 2: リストの動き

グレイリストに追加	24
グレイリストから削除	4
ブラックリストに追加	3

受信拒否するのはブラックリストに掲載されている送信 IP だけなので、受信したメールの中にはベイジアンフィルタで spam と判定されたメールも含まれている.

グレイリストに追加というのは、ベイジアンフィルタで spam と判定されたメールと置き換えることができる. グレイリストからの削除は、同一の送信 IP が spam を送った後で、必要なメールを送った場合に行われるが、ベイジアンフィルタの誤判定が含まれる可能性もある. 実際に、グレイリストから削除されたメールはベイジアンフィルタの誤判定であった.

5 まとめ

運用期間が短く、メールが少ないために有効な実験結果が取れていないが、システムの動作は確認できている. 今後の課題としては、フィルタが誤判定したときに再学習やリストの更新が必要になるので、ユーザがどのように管理者に知らせるかなど、システムの長期的な運用を考えた対策を考えている.

参考文献

[1] 渥美: "アクセス制御と SPAM フィルタを組み合わせた動的 SPAM 拒否システム", 情報処理学会分散システム／インターネット運用研究会, 情報処理学会研究報告 2004-DSM-35(2004)

[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 No.9(2005)

[3] 広瀬, 大駒: "SPAM 門前払い・SMTP レベルでの受信拒否方策の検証", 平成 15 年度第 2 回 情報処理学会東北支部研究会 資料番号 14(2003)

[4] Kenichi Nabeya: "ベイジアン スパム フィルタ", http: // bsfilter.org /

[5] Apache Spamassassin Project: "Spamassasin", http: // www.spamassassin.apache.org

[6] RBL.JP プロジェクト: "RBL.JP", http: // www.rbl.jp / index-j.php

[7] 吉田: "greylisting による spam メールの抑制について", 情報処理学会分散システム／インターネット運用研究会, 情報処理学会研究報告 2004-DSM-35(2004)