L-013

グレイリスティングとベイジアンフィルタの組合せによるスパムメールフィルタリング

Spam Mail Filtering Using Greylisting and Bayesian Filter

小池　隆司†　　佐藤　直‡
Takashi Koike　　Naoshi Sato

1. まえがき

迷惑メール（スパムメール）は，インターネットのトラヒックを占有しつつあり，円滑なコミュニケーションを阻害している．スパム対策として，特電メール法[1]が施行され法的な規制の枠組みが設けられた他，JEAG [2]が技術的な対策を継続検討している．しかし，これらの対策はまだ十分に機能していないように見られる．本稿では，このようなスパムメール対策の現状を背景に，広く適用されている二つのスパムメールフィルタリング方式；Greylisting[3]と Bayesian Filter[4]を組み合わせた対策手法を検討する．

以下，最初に，スパムメール対策への要件と現状を整理する．次に，提案方法の概要を述べ，システム構成を示す．更に，実環境下での実験結果を示し，提案方法の有効性を考察する．

2. スパムメール対策への要件と現状

スパムメール対策への要件として，以下の A～F が考えられる．

A. スパムメール削減効果が大きい．
B. 電気通信事業法（検閲の禁止，秘密の保護）に抵触しない．
C. ネットワークトラヒックを増加しない．
D. 受信ユーザの負担が小さい．
E. スパム／非スパムメールの誤判定が少ない．
F. メール転送遅延が増えない．

これまで，メールの内容を検査してスパムメールかどうかを判定する方法，メール送信者がスパムメール源であるかどうかを判定する方法，メールに対して強制的に一定のコストを課す方法，が種々提案されているが，従来技術はこれらの要件について，一長一短があり，全ての要件を満足するものは単体では見受けられないのが現状である．

3. Greylisting と Bayesian Filter の組み合わせによるスパムメールフィルタリングの概要

本稿では，従来技術を組合せることによって，より望ましいスパムメール対策システムを検討する．一例として，前述の要件 A に優れている Greylisting，及び要件 C に優れている Bayesian Filter の組み合わせを検討する．具体的には，到来したメールに対して，最初に ISP が Greylisting の機能を実施する．次に，Greylisting を通過し転送されたメールについてユーザが Bayesian Filter の機能を実施する．更に，ユーザでのフィルタリング結果を ISP にフィードバックする．このように両者を組み合わせることで，フィルタリング性能の相乗的向上が期待される．なお，提案システムでは ISP メール内容をチェックせず，ユーザが行うため，要件 B が遵守される．同じ理由で要件 E が満たされる．また，Greylisting によりユーザが検査するスパムメール数が減少することから，要件 D の点でも望ましい．ただし，要件 F について，Greylisting 実施に伴う遅延増加は避けられない．

4．システム構成

提案システムの構成を図 1 に示す．提案システムは，SMTP を制御し Greylisting を実行する SMTP 接続制御部，Greylisting を構成している各種リストを制御するリスト制御部，及び Greylisting を通過したメール内容を基に Bayesian Filter でフィルタリングするスパムフィルタ部から構成される．同図においてユーザと記した以外は全て ISP に設置される．なお，一般に，グレイリスト状態では

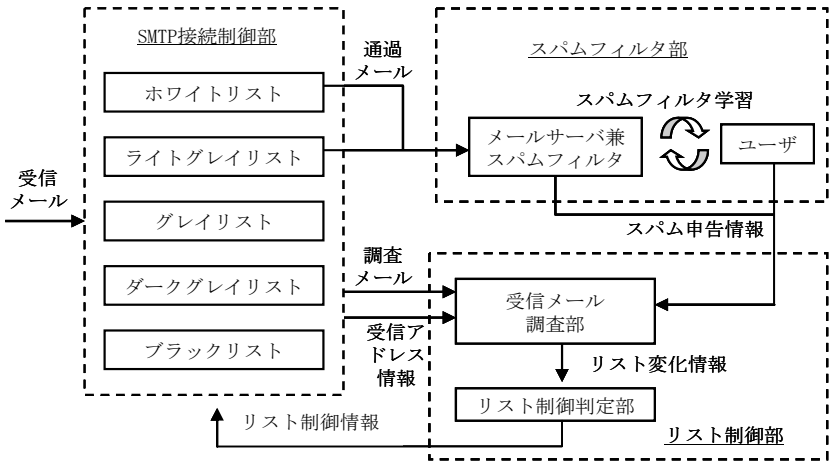

図１　システム構成

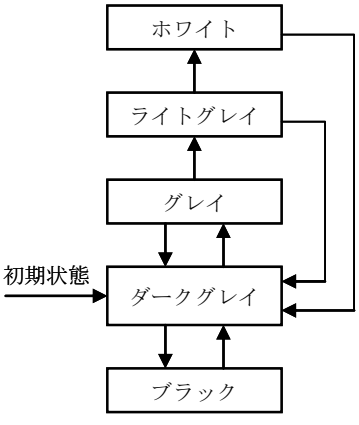

図２　状態遷移

† ヤフー株式会社　‡ 情報セキュリティ大学院大学

複数の処理が行われる．このため，本稿では，グレイリストにおける処理を区別し，ホワイトリストとグレイリストの中間，及びグレイリストとブラックリストの中間に，それぞれライトグレイリスト，ダークグレイリストを定義する．受信アドレス情報はこれら 5 つのいずれかの状態に分類され，リスト制御部からのリスト制御情報に応じて遷移する．この状態遷移を図 2 に示す．リストに対応する判定状態と Greylisting における処理を表 1 に示す．なお，図 2 におけるリスト間の遷移条件は従来の Greylisting の実施例を参考に設定する．

表１　リストに対応する判定状態と処理

リスト	判定状態	処理
ホワイトリスト	スパム源ではないと判定	通過
ライトグレイリスト	スパム源かも知れないが一旦受信	通過
グレイリスト	スパム源か否かを調査中	調査
ダークグレイリスト	初期状態	遮断
ブラックリスト	スパム源と判定	遮断

5. 実験と考察

前章で示したシステム構成を実装し，実環境で実験を行った．以下，実験の概要を示し結果を考察する．

実験では，ランダムな文字列の受信メールアドレスを使用した．また，スパムメール内に記されているアドレスに故意にアクセスし，到来するスパムメール数を増やして実験した．実験は 2 週間ほど行い，7 日目まではスパムフィルタ学習のみとした．8 日目より Greylisting 機能を加えてフィルタリングを実施した．また，比較のため，従来の Greylisting 方式単体（リストはブラック，グレイ，ホワイトのみ）によるフィルタリングも実施した．

実験結果を図 3 から図 5 に示す．図 3 において，Greylisting 開始後のスパムフィルタにおけるスパム判定メール数が激減している．これは Greylisting により，相当数のスパムメールが遮断されたことを示している．また，同図から，Greylisting の運用に伴って，ホワイトリストとブラックリストが増えていくことが分る．図 4 は Greylisting で遮断したメールと通過したメールの数の変化を表している．Greylisting 開始直後は，各送信元の状態が殆どダークグレイ，グレイ，ライトグレイなため，遮断数と通過数がともに直線的に増えているが，数日後には，ホワイトあるいはブラックに遷移する割合が増え，両者の変化が小さくなることが分かる．図 5 において，提案方式の遮断メール数は従来の Greylisting 方式単体に比べ概ね 2 割～3 割程度増えており，Bayesian Filter を組み合わせた効果が現れている．なお，最終的なスパム判別率は 96%であり，比較的良好な結果を得た．

6. むすび

Greylisting と Bayesian Filter を組み合わせたスパムメール対策システムを提案し，実環境下で実験を行った．

本検討により，提案方法がスパムメール対策として有効であるという見通しを得た．今後，残された課題（メール転送遅延の評価，ユーザ及び ISP の負荷軽減効果の定量化，更なるフィルタリング性能の向上）を検討し，具体的な適用を図る．

文　献

[1]総務省：特定電子メールの送信の適正化等に関する法律，2002 年 4 月．
[2] 迷惑メール対策グループ JEAG：http://jeag.jp/（2007.7）．
[3]Evan Harris：The Next Step in the Spam Control War:Greylisting,http://projects.puremagic.com/greylisting/whitepaper.html（2007.7）．
[4]Bayesian spamfilter:http://bsfilter.org/(2007.7).

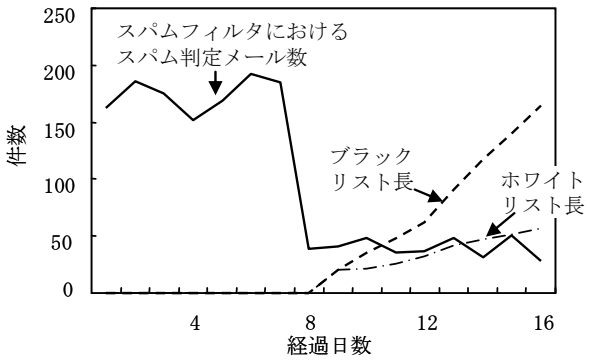

図３　スパムフィルタにおけるスパム判定メール数とホワイトリスト長・ブラックリスト長

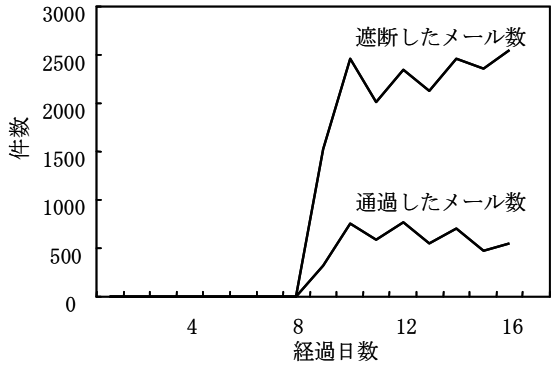

図４　遮断したメール数と通過したメール数

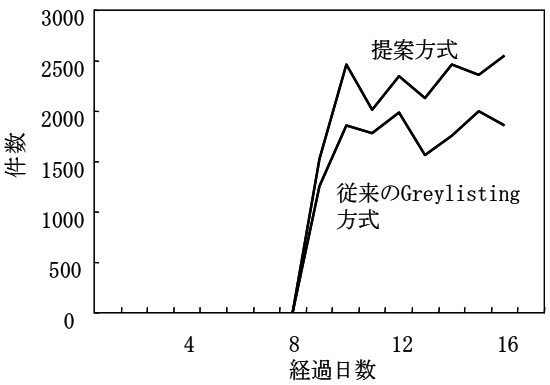

図５　提案方式と従来のGreylisting方式の遮断メール数