

迷惑メールフィルタリングシステム実現方式

黒柳大造 佐野恵理 伊勢勝 別司啓次 斉藤典明 高見一正

NTT 情報流通プラットフォーム研究所

あらまし

現在、迷惑メール問題は深刻な社会問題となっている。一般に提供されている迷惑メールフィルタリングシステムはユーザの設定する固定的フィルタ条件に基づいてフィルタリングを実施する方式が主流である。しかし、現実的には迷惑メールの傾向（ヘッダ情報設定、本文の書き方等）は短い周期で頻繁に変化していくため、固定的なフィルタ条件の寿命は非常に短い等の課題がある。本稿ではフィルタを実際に流通する迷惑メールから作成し更新を実施することにより、迷惑メールの傾向の変化に柔軟に対応可能な迷惑メールフィルタリングシステムを提案する。また、そのシステムを試作し、基本動作の検証及び性能測定の結果を評価して、今後の迷惑メールフィルタリングシステムの課題について考察した。

A Junk Mail Filtering System

Daizo KUROYANAGI Eri SANO Masaru ISE Keiji BESSI
Noriaki SAITO Kazumasa TAKAMI

NTT Information Sharing Platform Laboratories

Abstract:

Recently, "junk mail" causes serious social problems. Junk mail filtering systems on sale check E-mail with filters that filter-users decide each check- words and any other check-parameter. Therefore, it is difficult for them to preserve their validity for a long time because of frequent changes of style on "junk mail". Our junk mail filtering system can make their filters renew by themselves frequently, because they create their filters with circulated "junk mail" in public IP network. This paper presents our junk mail filtering system and its performance on trial-system.

1. 背景

現在、迷惑メール問題は深刻な社会問題となっている[1][2]。本稿では迷惑メール問題の現状について日本国内の規制動向、欧米での規制動向も視野に入れて検討し、受信者のプライバシー保護を目的に含めた迷惑メールフィルタリングシステムの実現方式を提案する。また、システムの試作による性能評価の結果、及び課題に対する考察を示す。

迷惑メールが世界各国で社会問題として認識されるのは、

- ・通信キャリアの業務及び設備運営の保護
- ・商業行為における受信者(消費者)保護
- ・受信者のプライバシー保護

等の観点による。ここで「プライバシーの侵害」は受信者の意思に反して迷惑メールを送信されることを示す[3][4]。

この問題に対して既に欧米では法律やその他の公的規則に基づいて迷惑メールの規制システムの整備が進んでいる[5][6]。日本国内においても通信キャリアの多くが規制を実施または実施予定としているほか、総務

省研究調査会にて対策が検討されている[7]。また、同時に、商業広告に係る電子メール通信の適正化に関する法律[8]、特定商取引法[9]、東京都消費生活条例[10]等、法律や自治体条例に基づく規制の準備が進んでいる。

日本国内の迷惑メールの定義と規制の動向を図1に示す。

(A)は平成13年から国内の通信キャリアにより規制が実施されている対象の迷惑メールである。この場合の「迷惑メール」の定義は通信キャリアの観点からの認識である。

(B)は政府による今後の公的な規制の対象として認識された迷惑メールである。これは受信者の観点から認識する「迷惑メール」の定義であり、この点で(A)とは大きく異なる。

(C)については政府研究調査会で迷惑メールとの認定は受けたものの政府の公的規制の対象からは外れているメールである。なお、受信者の観点から認識する「迷惑メール」の定義である点では(B)と同じである。

欧米では(C)の定義による迷惑メール対策

が実施されていることから、今後、日本国内でも(C)の定義による迷惑メール規制実施が要求されることが予想される。これより本稿の検討では(B)(C)の迷惑メールに対する規制実施を目標とする。問題内容の具体例としては一方的な商業広告、出会い系サイト勧誘、ウィルス添付、脅迫、ねずみ講勧誘、誹謗中傷等が挙げられる。

2. 迷惑メール問題への取組みの方向性

迷惑メール問題への取組みの方向性として総務省研究調査会は以下の5つの案を提示している[7]。

- (1) 既存の対応(アドレス指定受信許容/拒否等の固定的フィルタ条件)の継続的実施
- (2) 受信者側での多様な条件による選択を可能とする技術開発
- (3) 受信者へのヘッダ情報の受信前照会
- (4) ランダムな送信への対応方策の検討
- (5) 発信者側の通信キャリアの契約約款に基づく措置等

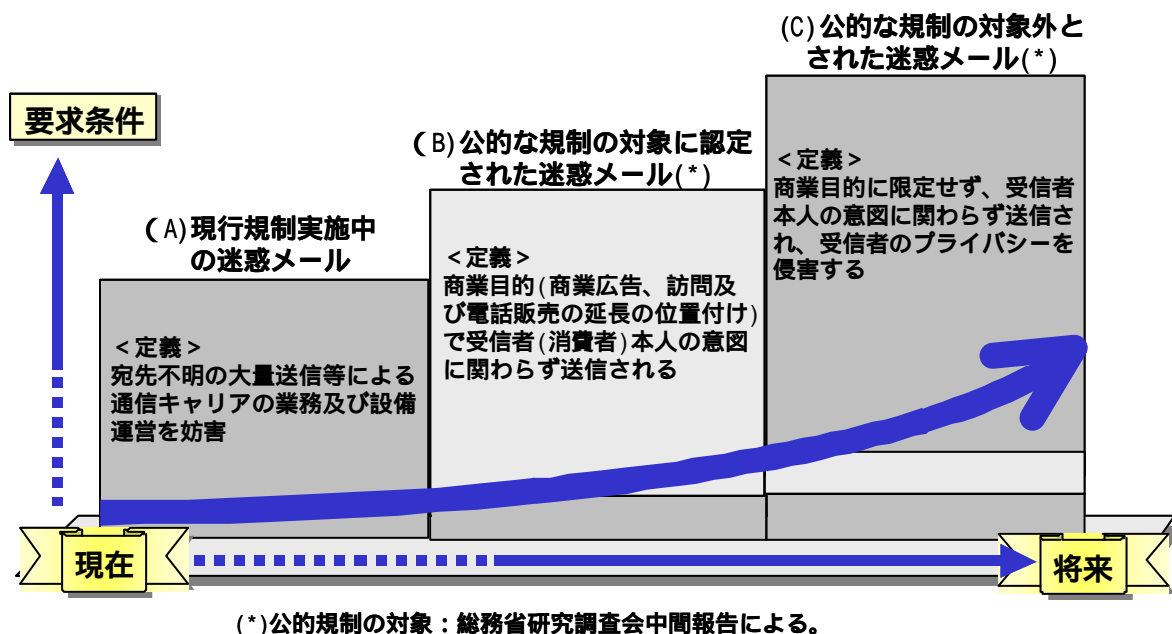


図1：迷惑メールの定義と規制の動向

(1)～(5)について通信キャリアの観点から評価する。通信キャリアが(2)の機能を提供した場合、受信者が迷惑メールの傾向の変化に合わせて随時選択を実施するため、規制効果の中長期的な維持が期待できる。これより本稿では(2)に着目し、この方向性に従って検討を進める。(2)に対応するための迷惑メールフィルタリングシステムへの要求条件について、受信者側、通信キャリア側それぞれの観点から整理した結果を表1に示す。

表1：要求条件一覧

	要求条件
受信者側からの要求条件	迷惑メールの受信拒否 迷惑メール受信に伴う課金の回避 操作の容易性確保 フィルタ条件の有効性確保 通常通信性能の確保 通信の秘密の保護
通信キャリア側からの要求条件	多量の無効メールからの設備保護 自社の企業イメージの保護 通信の秘密の保護

3．システム試作

3-1. 実現方式

本稿では、受信者端末へ着信前にフィルタリングサーバがメールのフィルタリングを実施し、迷惑メール受信に伴う受信者の操作、及び受信者の被害を最小化する実現方式を提案する[11]。そして、その実現方式に基づいて試作したシステムの概要を図2に示す。

システムは

- ・フィルタリングサーバ
- ・メールサーバ
- ・発信者端末
- ・受信者端末

から構成される。ここでフィルタリングサーバは() ()2段階のフィルタが搭載される。

() 固定フィルタ部：

本システムのユーザ(以下、ユーザ)が固定的に設定したフィルタ条件で通常のメールと迷惑メールに区分

() 柔軟フィルタ部：

メールのヘッダ情報や本文の書き方からユーザ共通のフィルタで通常のメールと迷惑メールに区分

システムでは、明らかに受信が必要なメールの自動受信及び明らかな迷惑メールの自動

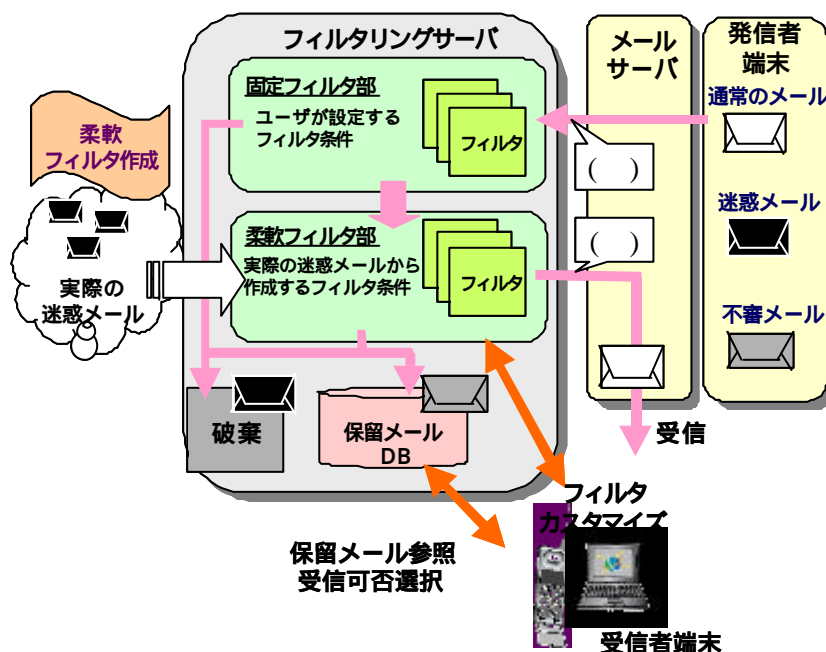


図2：システム概要

破棄または自動保留を固定フィルタ部で実施する。そして上記に含まれないメールのみ、最新の迷惑メールの傾向を反映した自動判定機能を具備する柔軟フィルタ部で、判定を実施する。

3-2 . ハード構成

図2に示すシステムの試作に使用したサーバの性能を表2に示す。

表2 使用したサーバの性能

用途	性能値
フィルタリングサーバ	OS/Linux, CPU/ 2GHz メモリ/1GB 1 CPU 構成
メールサーバ	OS/Linux CPU/ 2GHz メモリ/1GB 1 CPU 構成

3-3 . 固定フィルタ部

固定フィルタ部はユーザが設定する固定的フィルタ条件を用いて受信するメールをフィルタリングする機能である。メールのヘッダ情報や本文情報とフィルタに登録された情報とのマッチングを調べることによりメールのフィルタリングを実施する。システムが具備する固定的フィルタ条件を表3に記す。

表3 固定的フィルタ条件一覧

	フィルタ条件	処理	最大設定数
(a)	受信許容発信者アドレス/ドメイン (ユーザが設定)	受信	10(*1)
(b)	受信許容同報宛先アドレス	受信	10
(c)	受信拒否発信者アドレス/ドメイン	破棄 / 蓄積	10
(d)	受信拒否キーワード	破棄 / 蓄積	10

(*1) 表3(a)の受信許容発信者アドレスフィル

タについてはユーザが受信者端末 (PC 端末, 携帯電話端末等) を操作することにより設定する。これとは別に、ユーザが送信したメールの宛先アドレス (送信履歴) を自動的にフィルタ条件に反映させることにより設定される受信許容アドレスフィルタ (最大設定数 10) があり、これは柔軟フィルタ部に属する。

3-4 . 柔軟フィルタ部

柔軟フィルタ部のフィルタはインターネット上に実際に流通している迷惑メールから抽出したキーワードから構成される。ここではそのフィルタを用いてメールのヘッダ情報や本文情報とフィルタ条件として登録された情報との合致有無を調べる。そしてフィルタ条件を適切なタイミングで情報更新することにより、迷惑メールの傾向に柔軟に対応可能なフィルタリングが実現される。

システムでは、サンプルとなる迷惑メールを形態素解析した後に個々のキーワードに重み付けを実施したものをフィルタとして使用する。そしてシステムはフィルタにヒットしたキーワードの重みの合計値を評価することで迷惑メール判定を実施している。抽出された迷惑メールはユーザの選択により破棄、またはフィルタリングサーバ内に保留される。

なお、フィルタの作成には市販の言語解析システムをカスタマイズして使用している。

また、ユーザの受信者端末からのメール送信履歴による受信許容アドレスの自動設定 (最大設定数 10) 機能も具備している。

4 . 評価と考察

4-1 . 基本動作について

表1の要求条件に対する本システムの評価結果を表4に示す。

はフィルタリングサーバにおける迷惑メールの破棄、及びそれに伴う課金回避の基本動作の実現により要求条件を満たした。

はフィルタリングサーバでのユーザによる設定に従った自動判定及び自動処理の基本動作確認により、要求条件の一部を満たすことが出来た。しかし、同時に要求される

自動判定の精度及びフィルタの有効性維持において、試作したシステムでは人間の判断と自動判定の結果が異なる例が多数発生すること、及び有効性維持のためのフィルタ条件の自動更新機能が具備されていないことから、要求条件の実現には課題が残る。後者についてはにもあてはまる。は試作したシステムに設計の最適化の余地が残るため今後の課題である。は、希望するユーザのみに個別契約にもとづいてフィルタリングを実施することで要求条件を満たすことが可能である。は図1の(A)に対する迷惑メール対策にて対処は完了している。

表4：要求条件と作成したフィルタリングシステム機能の対応

要求条件	評価結果	評価内容
		・サーバでの受信前フィルタリング機能で対応可
		・サーバでの受信前フィルタリング機能で対応可
		・サーバでの受信前フィルタリング機能で対応可 ・自動判定の精度が不十分 ・柔軟フィルタ部フィルタの自動更新機能の必要有
		・自動判定の精度が不十分 ・柔軟フィルタ部フィルタの自動更新機能の必要有
		・設計最適化の余地有
		・契約者のみへの機能提供で対応可
		・サーバでの受信前フィルタリング機能で対応可
		・契約者のみへの機能提供で対応可

：要求条件を満たしている。

：要求条件を一部満たしているが残課題有。

-：本システム以外による対処で対応実施済。

フィルタリングの柔軟性及び中長期的な有効性の確保を目的とする柔軟フィルタ部

は、短期間に頻繁に変化する迷惑メールの傾向に追随するために、適切なタイミングでのフィルタ条件の更新が必要である。ここでは、

()フィルタ条件の自動更新

()フィルタの精度向上

の観点からフィルタ条件の有効性確保について検討を進める。

()について、自動更新用フィルタ条件の材料となる迷惑メールは実際にシステムが迷惑と判定したメールを用いることが考えられる。但し、フィルタ更新の方法であるが、

(a1)全ユーザ共通の情報更新実施

(a2)ユーザ毎の情報更新実施

の2つが存在する。(a1)ではユーザ全体への一律適用であることからユーザ個々への柔軟な対応が困難である。しかし材料となる迷惑メールが多量になることによる精度向上が期待できる。(a2)はフィルタ条件の材料となるメールは全てそのユーザ宛てであるためユーザ個々への柔軟な対応が可能である。しかし材料となる迷惑メール数が(a1)と比較して少ないことによる精度の限界が予想される。

今後は上記以外の観点による評価の実施も含めて、最適なフィルタ条件の自動更新方法を検討する。

()については、柔軟フィルタで通常のメールについても迷惑メールと判定する誤判断が発生している。これはフィルタ作成において迷惑メール内の非迷惑メール要素もフィルタ条件に登録されるためである。これより、柔軟フィルタ部での精度向上のため、下記の2つの方法が考えられる。

(b1)通常メールフィルタの作成

(b2)迷惑メールフィルタの編集

(b1)については通常のメールについては通常メールフィルタにて抽出可能である。しかし、同時に迷惑メールフィルタ内の非迷惑メール要素も残るためフィルタリング実施順序等の設計により精度に影響がでる。(b2)については、編集にあたって多大な作業量が予想されること、また編集の指針を何らかの方法で明確化する必要があることから、実現性の検討が必要である。

今後は、(b1)(b2)各々の方法についての詳細検討、及び両方法の併用を含めた方法の検討を進めていく必要があると考えられる。

4-2. 性能測定について

フィルタリングサーバでの迷惑メール処理速度(図2()~()間)の測定を実施した。性能測定を実施した結果を表5に示す。

表5：測定結果

測定項目	測定結果
収容ユーザ数	13万ユーザ/台
メール受信数	86万通/日
メール送信数	518万通/日

これを2002年2月のiモードメールのトラヒックモデル[12]を適用して評価する。ここでは、13万ユーザのシステムに期待されるiモードメールシステムの処理メール数は、受信メール数が73万通/日、送信メール数が51万通/日となる。このとき、本システムの処理能力は、メール送信数、メール受信数ともにiモードメールシステムに要求される処理能力を上回る。これより本システムは、実用化時に要求されることが予想される性能条件を満たすことが証明された。

但し、収容ユーザ数に対するメール受信数及びメール送信数、及びメール受信数とメール送信数の比についてiモードメールでの実績と乖離があることから、解析アルゴリズム及びリソース設計に適正化の余地が残っていることが考えられる。さらに、性能測定の精度向上の観点から、送信処理と受信処理が並存したケースの測定等、測定条件を適正化することにより、実用化のための評価に耐え得る測定値の取得が必要となる。またフィルタカスタマイズ及び保留メール参照実施のためのDBへのアクセスについても測定条件に加える必要があると考えられる。

また、収容ユーザ数に関しても、iモードメールユーザの半数(約1500万ユーザ)が本システムを利用すると仮定した場合、設置サーバ数が約120台と多数にのぼることから、収容機能と処理機能間の設計適正化に加え

て、システム全体の効率化の検討を進める必要がある。

5. まとめ

試作したシステムの評価により、迷惑メールフィルタリングシステムの基本的動作と性能の検証が完了した。

今後は4項で示した評価の厳密化、性能向上、機能拡張について検討を進め、また制度的な環境変化を、随時、仕様に反映させながら本システムの機能向上を実現する。

参考文献：

- [1] 浜屋・碓井 監修「インターネットビジネス白書 2002」ソフトバンクパブリッシング,2001.
- [2] <http://www.kantei.go.jp/jp/nippon-now/2001/0806/3men.pdf>
- [3] 新保「プライバシー権利の生成と展開」成文堂,2000
- [4] 堀部「プライバシーと高度情報化社会」岩波書店,1988.
- [5] 土谷・河野・Mestecky「インターネットをめぐる米国判例・法律100選」JETRO,2001.
- [6] 益田,舟井,Eifert & Mitchell 法律事務所「米国インターネット法」JETRO,2002.
- [7] http://www.soumu.go.jp/joho_tsusin/joho_tsusin.html
- [8] <http://www.sangiin.go.jp/japanese/frame/joho5.htm>
- [9] <http://www.meti.go.jp/kohosys/press/0002285/>
- [10] http://www.shouhiseikatu.metro.tokyo.jp/s_hogo/singi/singi5.html
- [11] 黒柳,佐野,斉藤,高見,“迷惑メール対策フィルタ実現方式”情報処理学会インタラクシオン2002論文集, p31-32,2002.
- [12] http://www.nttdocomo.co.jp/p_s/imode/