情報処理学会論文誌 Vol. 50 No. 3 940–949 (Mar. 2009)

SMTP セッションの強制切断による spam メール対策

山井成良[†1] 岡山聖彦[†1] 中村素典[†2]
清家巧[†3] 漣一平[†4]
河野圭太[†1] 宮下卓也[†5]

spam メールへの対策方法として，一時的なエラーを発生することにより再送処理を行わない MTA からの電子メールを排除する tempfailing が広い範囲で利用されている．しかし，従来の tempfailing では，再送しない MTA から送信されたメールが受信者に配送されなかったり，異なる MTA から再送するような一部のドメインについては管理者が MTA を手作業で登録する必要があったりするなどの問題があった．そこで本論文では，受信側 MTA がヘッダや本文を受信後に強制切断する方式を提案する．これにより従来の tempfailing と同様に再送処理を行わない MTA からの電子メールを排除する効果を得ながら，メッセージのヘッダや本文を取得することが可能になる．また，取得したヘッダや本文を活用して管理コストの低減や再送されないメールの回復を図ることも可能になる．提案方式に基づく試作システムを試験運用した結果，異なる MTA から再送するドメインからのメールも正常に受信でき，提案方式の有効性を確認できた．

An Anti-spam Method with SMTP Session Abort

Nariyoshi Yamai,[†1] Kiyohiko Okayama,[†1]
Motonori Nakamura,[†2] Takumi Seike,[†3]
Ippei Sazanami,[†4] Keita Kawano[†1]
and Takuya Miyashita[†5]

Tempfailing, which temporarily refuses the first delivery attempt of a message from an untrusted Mail Transfer Agent (MTA), is one of typical anti-spam technologies commonly used in many organizations. This method can refuse spam mails considerably. However, it also may refuse legitimate mails sent from domains resending the temporarily failed message with a different MTA or those without resending function. In such a case, an administrator of the receiver MTA has to register those domains by hand. In this paper, in order to reduce these drawbacks, we propose an anti-spam method introducing SMTP session abort function. This method performs the same effect as existing tempfailing methods by means of SMTP session abort during the first delivery attempt. In addition, this method can obtain the header or the whole message even if it would not be resent and can use the header for second delivery checking and can use the whole message of unresent messages in case of false positives. According to the operation tests of the prototype systems, we confirmed that the proposed method received messages from domains using a different MTA for retry.

1. はじめに

電子メールは WWW と並んでインターネットにおいて最も普及しているサービスの 1 つであり，社会的な活動を支える通信手段としてもはや必要不可欠な存在となっている．一方，電子メールはセキュリティ上最も問題の多いサービスの 1 つである．特に，広告や phishing 詐欺などを目的に不特定多数の利用者に一方的に送信される spam メールの蔓延は大きな社会問題にまでなっており，その対策は重要である．

spam メールを受信側で排除する手段として，これまで多くの方式が提案されてきた．これらはブロッキング，フィルタリング，スロットリングの 3 種類に大別できる．このうちブロッキングは，SMTP セッション開始時あるいはセッション中の本文を受信する前に，送信 IP アドレスや差出人メールアドレスなどに基づいて spam メールの受信を拒否する手法で，一般的に判定に要するコスト（CPU 負荷，ネットワーク負荷など）が比較的小さいことから多くのドメインで採用されている．以下，本論文ではブロッキングに絞って議論する．

代表的なブロッキング手法としてブラックリストや tempfailing が知られている．

ブラックリストは，spam メールの送信 MTA（Mail Transfer Agent）や第三者中継を許す MTA などの IP アドレスを登録しておき，受信側 MTA では SMTP セッション確立

†1 岡山大学総合情報基盤センター
Information Technology Center, Okayama University
†2 国立情報学研究所
National Institute of Informatics
†3 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
†4 株式会社日立製作所
Hitachi Ltd.
†5 津山工業高等専門学校
Tsuyama National College of Technology

時にブラックリストを参照し，登録されている IP アドレスから SMTP セッション確立要求があればこれを拒否する方式である．インターネット上で公開されている多くのブラックリストは DNS（Domain Name System）を用いて提供されており，Spamhaus ZEN [1]，SCBL [2]，SORBS [3] などがよく知られている．しかし，一般にブラックリストは見逃し（false negative）や誤検出（false positive）が多く [4]，文献 5) では実在するあるブラックリストの有効性が低いことが示されている．特に，転送などにより同一の MTA から spam メールとそうでないメール（以下，正常メール）が混在して配送される場合には，当該 MTA がブラックリストに登録され正常メールまで受信を拒否される事例も存在する．

一方，tempfailing は，信頼できない MTA からの電子メール配送を一時的に拒否することにより，再送処理を行わない MTA からの電子メールを排除する手法である．spam メールの送信 MTA の多くは再送を行わないことから，この手法は spam メールの効果的な排除が期待でき，実際に有効に機能することが知られている [6),7)]．同手法に基づく代表的な方式として，greylisting [6]，5-way handshake [8] などがある．しかし，これらの方式には，送信 MTA が再送しない場合，あるいは再送を異なる MTA から行う場合は，正常メールであってもこれが受信者に配送されず，またこれに対処するには管理者による MTA の登録が必要になるなどの問題があることが知られている [7]．

そこで，本論文では，tempfailing 方式において上記のような問題を軽減するための spam 対策方式を提案する．本方式では SMTP セッションを受信側 MTA で途中で強制切断することにより送信側 MTA の再送処理を促す．これにより tempfailing と同様の効果を得ながら，電子メールのヘッダや本文を取得することが可能になる．また，取得したヘッダや本文を活用して管理コストの低減や再送されないメールの回復を図ることも可能になる．

以下，2 章では，従来の tempfailing の問題点について議論し，3 章では提案方式の詳細について述べる．4 章では提案方式に基づいて試作したシステムの実装方法と同システムの評価について述べる．

2. 従来の tempfailing 手法とその問題点

RFC2821 [9] によると，SMTP セッション中に受信 MTA から一時的なエラーを表す 400 番台の応答を受け取った場合，あるいは受信 MTA の障害などの理由により通信を完了できなかった場合，送信 MTA は一定の期間待った後に再送処理を行ったり，複数の MX が指定されている場合には次の順位の受信 MTA への配送を試みたりしなければならない．ところが，spam メールの発信に用いられる MTA（spam 発信 MTA）は一般に spam メール配送の確実性よりもスループットを重視するため，受信 MTA が一時的なエラーを返しても再送処理[⋆1]を行わないものが多い．

tempfailing では，このような挙動の違いを利用して spam 発信 MTA の判定を行い，spam メールの受信を拒否する．具体的には，送信 MTA が受信 MTA に対してメール配送を試みると，受信 MTA はこれが 1 回目の配送であるか 2 回目以降の配送（再送）であるかを判別する．もし，1 回目の配送であれば，受信 MTA はあえて受信を拒否することで再送を促し，逆に 2 回目以降の配送であれば通常どおりの受信処理を行うようにする．

tempfailing には，配送拒否の時期や再送判定基準などの違いによりいくつかの実装が存在する．本章では tempfailing に分類される従来の実装とその問題点について述べる．

2.1 greylisting

greylisting では SMTP セッション中に（送信 MTA の IP アドレス，エンベロープ From アドレス，エンベロープ To アドレス）の 3 つ組を取得し，これを再送判定に用いる．1 回目の配送では 3 つ組を短期間（文献 6) での推奨値は 4 時間）登録し，RCPT コマンドに対する応答として一時的エラーを送信 MTA に返す．この登録期間中に同一の 3 つ組の配送があればこれを再送と見なして受信処理を行う．ただし，登録後一定期間内（同 1 時間）の再送は再送と見なさず再び一時的エラー応答を返す．再送が確認された 3 つ組は長期間（同 36 日間）登録され，この期間中に同じ 3 つ組の配送があれば一時的エラー応答を返さず，ただちに受信処理を行うようにする．

同様の方式に「お馴染みさん方式」[10] がある．この方法では 3 つ組の代わりに送信 MTA の IP アドレスのみを用いる点が greylisting と異なる．

greylisting の問題点としては，通常メールの配送遅延があげられる．すなわち，RFC2821 では再送間隔は 30 分以上とすることが推奨されているため，ホワイトリスト（無条件で受信を行う MTA の IP アドレスを登録したもの）に登録されていない MTA からの配送はたとえ上記の再送と見なさない期間を短縮したとしても 30 分以上の遅延が生じることが予想される．

また，再送が初回配送時とは異なる MTA から行われる場合には，さらに以下のような問題が生じる．大規模なドメインでは，負荷分散のために複数の MTA を用意し，前回とは異なる MTA を用いて再送を試みることがある．このような場合では再送のたびに異なる MTA が用いられるため，受信 MTA では毎回再送でないと判定され，そのつど一時的なエ

⋆1 複数 MX 指定時における次順位 MTA への配送も含む．

ラーが返されることになる．これに対処するには，このような挙動をする送信 MTA を管理者が手作業でホワイトリストに登録する必要があり，管理コストの増大につながる．

さらに，greylisting では誤検出が発生した場合に利用者や管理者がこれを回復できない点が問題となる．もし初回時に送られた正常メールを受信拒否し，その後送信 MTA が再送をしなかった場合，この正常メールは宛先に配送されず，誤検出が発生したことになる．これに対処するためには再送しない送信 MTA をホワイトリストに登録する必要があるが，利用者や管理者が得られる情報は（送信 MTA の IP アドレス，エンベロープ From アドレス，エンベロープ To アドレス）の 3 つ組だけでヘッダや本文は記録されないため，送信 MTA をホワイトリストに登録すべきかどうかの判定が困難である．再送を行わない MTA は本来であれば RFC2821 に違反しており，誤検出の責任も送信 MTA 側が負うべきであるが，残念ながら現実にはこのような MTA も存在するため[11]，greylisting 導入における問題となりうる．

2.2　5-way handshake

5-way handshake ではプライマリ MTA およびセカンダリ MTA の 2 台の MTA を用意し，プライマリ MTA への配送を拒否することによりセカンダリ MTA への配送を促す．その際，プライマリ MTA への SMTP セッション確立時に送られる SYN フラグ付きパケット（以下，SYN パケット）に対して受信 MTA は RST フラグ付きパケット（以下，RST パケット）の送出によりセッション確立を拒否する．これにより多くの正常な MTA に対して短時間での再送を促し，greylisting で問題となっていた通常メールの配送遅延を大幅に軽減することが可能となる．

再送判定は，送信 MTA とセカンダリ MTA との間での SMTP セッション確立の直前における，同一送信 MTA からプライマリ MTA への SYN パケット送信の有無に基づいて行われる．SYN パケット送信の有無を必要とするのは，MX レコードの優先度を無視して直接セカンダリ MTA への配送を行うような spam 送信 MTA を排除するためである．

しかし，この方式では，再送が初回配送時とは異なる MTA から行われる場合には再送判定が正しく行われず通常メールを受信できないという問題点は解決されていない．また，RST パケット受信後にセカンダリ MTA への配送を試みない MTA の存在が確認されており[8]，ホワイトリストに登録しない限りそのような MTA から配送される正常メールが宛先に配送されない状態になる問題も依然として存在する．このほかにも，新たな問題点として，一部の MTA は正常に配送を完了した受信 MTA をしばらく記憶し，次回の配送にも同じ受信 MTA に配送を試みるため，1 度セカンダリ MTA への配送が成功すると次回の配送では直接セカンダリ MTA に配送しようとして再送判定が正しく行われない危険性がある．さらに，日本では一部の中小企業などで見られるように 1 つのグローバル IP アドレスしか利用できないドメインも多く[12]，そのようなドメインではこの実装をそのまま採用できない点も問題となりうる．

3.　SMTP セッションの強制切断による spam メール対策方式

前章で述べたように，従来の tempfailing は通常メールの配送遅延が大きい，再送を正しく判定できない危険性がある，誤検出が発生した場合に利用者がこれを認識できないなど，いずれも運用上あるいは性能上の問題があった．そこで本章では tempfailing において SMTP セッションの強制切断機能を導入することにより，従来の tempfailing 手法が持つ問題点を軽減する方式を提案する．

3.1　システム構成と提案方式の概要

本方式では，通常の MTA に SMTP セッション強制切断機能を導入する構成も可能であるが，既存の MTA をそのまま用いながら同機能を持つメールゲートウェイを新たに導入する構成も可能である．説明を容易にするため，以下ではメールゲートウェイを新規導入する構成を想定する．この場合のシステム構成図を**図 1** に示す．メールゲートウェイは便宜上プライマリメールゲートウェイ（PMG: Primary Mail Gateway）とセカンダリメールゲートウェイ（SMG: Secondary Mail Gateway）の 2 台で構成されており，それぞれ同図における各末端 MTA（図中右端の Server）のプライマリ MX，セカンダリ MX として指定されるように DNS が設定されているものとする．なお，後述するように PMG と SMG は同じ動作を行うため，1 台のメールゲートウェイが PMG と SMG を兼ねることも可能である．

これらのメールゲートウェイは RST パケット送出による SMTP セッションの強制切断機能を持ち，PMG への初回配送時にはヘッダあるいは本文を受信した時点で強制切断を行うように動作する．これにより，従来の tempfailing と同様に再送しない送信 MTA からの

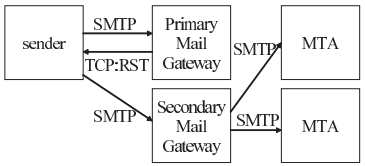

図 1　提案手法のシステム構成例
Fig. 1　A system layout of the proposed method.

メール配送を排除する効果を有しながら，従来の tempfailing とは一時エラーを発生させる時期が異なり，初回配送時にヘッダや本文を取得できるため，これらの情報を再送判定や誤検出発生時の回復に用いることが可能になる．また，5-way handshake と同様に複数の MX を設定しているため，強制切断により初回配送に失敗すると，多くの送信 MTA は次の優先度を持つ SMG へただちに配送を試み，SMG ではこれを受理する．これにより greylisting における配送遅延を軽減することが可能となる．

3.2　再送判定処理の改善

従来の tempfailing では，再送判定において電子メールのヘッダや本文をまったく利用せず，送信 MTA の IP アドレスやエンベロープ From，エンベロープ To のような SMTP セッションの情報のみに基づいて行っていたため，再送のたびに異なる MTA を用いて配送が試みられる場合に正しく判定できなかった．これに対して，提案方式ではヘッダあるいは本文を受信した後に SMTP セッションを強制的に切断するため，従来の送信 MTA の IP アドレスの代わりにヘッダあるいは本文に含まれる情報を用い，さらにエンベロープ From，エンベロープ To を組み合わせて再送判定を行う．これにより，従来のように異なった MTA からの再送に対しても正しく再送判定を行うことが可能になり，管理コストの減少が可能になる．

IP アドレスの代わりに再送判定に用いる情報は，メッセージの同一性を判定できるものであればヘッダあるいは本文に含まれる任意のものが利用できる．その候補としては，たとえばヘッダ中の Message-ID，Date，Received などのフィールド，あるいは本文のハッシュ値などがあげられる．ただし，ヘッダ受信後に強制切断する場合には，本文に含まれる情報を再送判定に用いることができないという点に注意する．

なお，Message-ID，Date あるいは本文のハッシュ値など，複数の宛先に配送されるメッセージに共通の情報だけを用いて再送判定を行うと，再送でないメッセージを誤って受信する危険性があることに注意する．すなわち，複数の宛先に同一内容のメッセージが個別の SMTP セッションで配送されると，2 通目以降が初回配送時に 1 通目と同じメッセージの再送と誤認識されて受信される．これを防ぐためには，少なくともエンベロープ To との組合せで再送判定を行う必要がある．

3.3　強制切断の時期

3.1 節で述べたように，本方式では PMG が初回配送時にヘッダあるいは本文を受信した時点で強制切断を行う．強制切断をどの時点で行うかは通信量や配送遅延時間，あるいは誤検出後の回復に影響を与える．すなわち，強制切断を本文受信後に行う場合，すべてのメールについて 1 回分の通信に要する通信量が増加し，これにともなって遅延時間も 1 回分の通信に要する時間だけ増加するが，誤検出が発生した場合にメッセージ全体を回復することが可能である．通信量や配送遅延時間の増加は，特に大きいサイズのメッセージを受信する場合に顕著になる．これに対して，強制切断をヘッダ受信後に行う場合には，ヘッダ部分の通信に要する通信量だけが増加するため，通信量や配送遅延時間の増加はメッセージサイズにかかわらず比較的小さく抑えられるが，誤検出が発生した場合に差出人アドレスや件名などヘッダ中に含まれる情報のみ回復可能で，メッセージ全体を回復することができない．

このような理由により，本方式では利用者自身が強制切断の時期を自由に設定できるような機能（以下，切断時期設定機能）を導入する．設定可能な動作は accept（最初のセッションで受信する），header（ヘッダ受信後に強制切断する），body（全文受信後に強制切断する）の 3 通りである．

このような機能を導入すると，複数のエンベロープ To が指定されたときにどのような動作を行うかが問題となる．これに対しては，**表 1** に示すように，宛先に対する動作の組合せによって実際に選択される動作を変更するようにする．宛先操作については，初回受信（accept）の宛先と再送時受信（header および body）の宛先が混在する際に必要で，初回受信時には初回受信の宛先のみ残し，逆に再送時には再送時受信の宛先のみ残すようにする．たとえば，3 番の行は初回受信（accept）の宛先とヘッダ受信後切断（header）の宛先が混在し，全文受信後切断（body）の宛先が含まれない場合に対応し，切断時期は全文受信後（body）とするが，PMG 自身はメッセージを受理し，初回受信の宛先のみを残して末端 MTA に配送する．

なお，初回受信と再送時受信の宛先が混在する際には，初回受信時に取得したメッセージ

表 1　複数の宛先が指定されている場合の動作
Table 1　Action with multiple recipients.

#	強制切断設定			動　作		
	accept	header	body	切断時期	初回配送	宛先操作
1	○			accept	あり	なし
2		○		header	なし	なし
3	○	○		body	あり	あり
4			○	body	なし	なし
5	○		○	body	あり	あり
6		○	○	body	なし	なし
7	○	○	○	body	あり	あり

の処理が初回受信の宛先と再送時受信の宛先で異なる点に注意する．すなわち，まず初回受信の宛先については，送信 MTA がメール送信を完了していないにもかかわらず受信側ではメール配送が行われる．これは RFC1047 [13] で示されるように強制切断をともなわない通常のメール配送においても起こりうる状況であり，特に問題にならない．一方，再送時受信の宛先については，同じメッセージを取得するが配送は行わない．メッセージの取得は誤検出発生の確認を行うためのものであり，誤検出されたメッセージを後に回復したとしても，これがただちに正常なメール配送を意味するものではない．

3.4　全体の処理手順

これまでに述べた方法をまとめた，システム全体の典型的な処理手順の例を以下に示す．この例では，（エンベロープ From アドレス，エンベロープ To アドレス，Message-ID）の 3 つ組を用いて再送判定を行うものとする．

なお，以下の手順においては PMG と SMG を区別せずに扱っているが，これは通常の MTA の中にも MX の優先度の指定に従わないものが存在するためである．

(1)　送信 MTA は，PMG/SMG との間で SMTP セッションを開始する．

(2)　送信 MTA は PMG/SMG に対して MAIL FROM コマンドおよび RCPT TO コマンドを発行し，差出人アドレスおよび宛先アドレスを指定する．PMG/SMG は末端 MTA 宛の配送であればこれらのコマンドに対して肯定応答（250 OK）を返し，これらのアドレスを後の再送判定で用いるために記録しておく．また，PMG/SMG は指定された宛先に対応する強制切断設定を参照し，表 1 のどの行の動作を行うかを決定する．

(3)　切断時期が accept の場合（表 1 の 1 番）には，PMG/SMG は通常どおり受信し，末端 MTA に中継して終了する．

(4)　そうでなければ切断時期が accept 以外の場合（表 1 の 2〜7 番）に該当する．この場合，送信 MTA は引き続いて DATA コマンドを発行する．PMG/SMG は同コマンドを受け付けた後，ヘッダの内容を受信する．

(5)　PMG/SMG はヘッダ中の Message-ID フィールドを抜き出し，（エンベロープ From アドレス，エンベロープ To アドレス，Message-ID）の 3 つ組に基づいて再送判定を行う．判定の結果，初回配送と判定された場合には (6) に進み，再送と判定された場合には (10) に進む．

(6)　PMG/SMG は（エンベロープ From アドレス，エンベロープ To アドレス，Message-ID）の 3 つ組を記録する．

(7)　切断時期が header の場合（表 1 の 2 番）には，PMG/SMG は RST パケットをただちに送信 MTA に送出して SMTP セッションを強制切断し，送信 MTA に再送を促す．また，受信したヘッダを誤検出時に備えて保存し，終了する．

(8)　そうでなければ，切断時期が body の場合（表 1 の 3〜7 番）に該当する．この場合，PMG/SMG は全文を受信後に RST パケットを送信 MTA に送出して SMTP セッションを強制切断し，送信 MTA に再送を促す．また，受信したヘッダおよび本文を誤検出時に備えて保存する．

(9)　初回配送がありの場合（表 1 の 3，5，7 番）には，PMG/SMG は宛先アドレスのうち初回受信（accept）の宛先のみを残し，その宛先に受信したメッセージを中継して終了する．そうでなければ（表 1 の 4，6 番の場合），初回受信する宛先がないため単に終了する．

(10)　PMG/SMG は再送されたメッセージを通常どおり受信し，宛先アドレスのうち初回受信（accept）の宛先を削除して残りの宛先に受信したメッセージを中継する．また，誤検出時に備えて保存していたヘッダおよび本文を削除して終了する．

3.5　メールゲートウェイの統合

2.2 節で述べたように，一部のドメインではグローバル IP アドレスを 1 つしか利用できないため，図 1 のように複数のメールゲートウェイを必要とするシステム構成は採用できない．

これに対して，提案方式では 1 台のメールゲートウェイが PMG，SMG の両方を兼用する構成が適用可能である．この場合，**図 2** に示すように右辺の異なる MX レコードを複数用意し，これらが同一の IP アドレスを持つように設定する必要がある．この構成により，利用する IP アドレスは 1 つに抑えつつ，複数のメールゲートウェイを導入する構成とほぼ同様に配送遅延時間の短縮効果を期待できる．また，PMG，SMG 間での再送判定情報の共

```
$ORIGIN example.com.
@       IN    MX    10 pmg
        IN    MX    20 smg
pmg     IN    A     192.0.2.123
smg     IN    A     192.0.2.123
```

図 2　メールゲートウェイ統合時の DNS 設定
Fig. 2　A sample DNS setting for a single mail gateway.

有が不要になり，実装が容易になるという利点も生ずる．ただし，耐故障性の面では，図 1 の構成の場合は 2 台のメールゲートウェイのうち 1 台が故障しても遅延時間は大きくなるものの配送は可能であるのに対して，1 台のメールゲートウェイしかない構成の場合はこれが故障すると配送が不可能になることから，図 1 の構成のほうが優れている．

4. 試作システムの実装と評価

前章で述べたシステム構成および動作手順に基づき，我々は spam メール対策システムの試作を行った．試作システムは切断時期設定機能を実装していない初期のシステムと，同機能を実装した後期のシステムの 2 種類作成した，以下では，それぞれの試作システムの実装と評価について述べる．

4.1 初期の試作システム

初期の試作システムでは 2 台のメールゲートウェイを用い，MTA プログラムとして sendmail を稼動させた．本システムでは管理者の設定により初回配送時のヘッダ受信後あるいは本文受信後に SMTP セッションの強制切断を行うようにした．SMTP セッションの強制切断には外部プログラムを導入して SMTP セッションを監視し，初回配送時のヘッダ受信後あるいは本文受信後に RST パケットを生成して送信 MTA，メールゲートウェイの両方に送るようにした．再送判定方法としては，3.4 節で述べた 3 つ組を用いるようにした．

試作システムの動作試験として，まず外部ネットワークから隔離された実験ネットワークにおいて，試作システムの基本動作を調査した．その結果，SMTP セッション強制切断機能，再送判定機能のいずれもが正しく動作することが確認された．

次に，動作試験の一環として試作システムを外部のネットワークにつなぎ，実際に外部から送られてくる spam メールの処理を行った．この試験運用では，近々廃止される予定の岡山大学内のあるドメイン宛の電子メールを試作システムがいったん受け取るように MX レコードを書き換え，その後試作システムが本来の末端 MTA に受け取った電子メールを配送するようにした．このドメイン宛に送信される電子メールの大半は宛先不明メールで，また，その多くが spam メールであると思われるが，その確認には受信者の同意が必要となるため行うことができず，実際の spam メールの割合は不明である．この試験運用では，このような環境において，2006 年 1 月 29 日から 2 月 5 日までの 7 日間連続して試作システムを運用した．

試験運用では，提案方式のブロッキング機能の有効性を確認するため，試作システムのログを解析し，動作試験の期間中に試作システムで処理したメールのうち，初回の配送に失敗した後に再送されたメールと再送されなかったメールの数を算出した．その結果を**表 2** に示す．

表 2　初期の試作システムの運用結果
Table 2　Operation result of the first prototype system.

	再送数	未再送数	受信数
PMG	5,340	34,415	39,755
SMG	5,076	9,888	14,964
total	10,416	44,303	54,719

この表から，試作システムが処理した全メール 54,719 通のうち，81%にあたる 44,303 通のメールを試作システムにおいてブロックできたことが分かる．これは我々の経験における従来の greylisting と同等の性能であり，これより提案方式の SMTP セッション強制切断機能がブロッキング機能として十分に動作するといえる．

4.2 後期の試作システム

後期の試作システムではメールゲートウェイは 1 台とし，MTA プログラムとして sendmail を一部改造したものを用いた．改造の内容はヘッダ終了に関する milter（mail filter）の実行時期に関するもので，本来であれば本文受信後に実行されるが，これをヘッダ受信直後に実行されるようにした．強制切断の方法は，ヘッダ受信後あるいは本文受信後に呼び出された milter が外部プログラムに通知して送信側，受信側の双方に RST パケットを送るようにした．ただし，表 1 における 2，4，6 番の処理を行う場合には送信側，受信側の双方に同時に RST パケットを送るのに対し，3，5，7 番の処理を行う場合には，外部プログラムは送信側に先に RST パケットを送りながら，受信側から肯定応答が送られるのを待ち，これを受信すると受信側にも RST パケットを送るように動作する．また，宛先操作には milter を用いた．再送判定方法としては，原則として 3.4 節で述べた 3 つ組を用いるようにしたが，後述するように Message-ID フィールドの代わりに Date フィールドを用いる場合もあった．

試作システムの動作試験として，後期の試作システムで新たに導入した，切断時期設定機能が正しく動作するかどうかを確認した．その結果，表 1 に示すすべての組合せについて正しく動作することが確認された．

次に，試作システムの評価を行った．初期の試作システムでは，提案方法と従来方法との比較を行えなかったため，後期の試作システムではいくつかの無料のメールサービス，匿名メールサービス，メーリングリスト（ML），メールマガジンおよび個人のメールアドレスを用いてメールを送信し，強制切断後の再送の有無，再送に用いる MTA，再送までの最小

表 3　後期の試作システムの運用結果
Table 3　Operation result of the second prototype system.

ドメイン名（サービス）	MTA ソフトウェア	再送	再送 MTA	最小配送遅延
cc.okayama-u.ac.jp（大学）	sendmail	○	同一	0 （sec）
nifty.com（ISP）	sendmail	○	同一	1
listbox.com（spf-discuss ML）	postfix	○	同一	1
yahoo.com（無料メール）	?	○	同一	10
gmail.com（無料メール）	?	○	別個	385
aol.com（無料メール）	?	○	同一	6
hotmail.com（無料メール）	SMTPSVC	○	同一	6
yahoogroups.jp（無料 ML）	?	○	同一	1
freeml.com（無料 ML）	qmail	○	同一	399
mag2.com（メールマガジン）	qmail	○	同一	3,264
trashmail.net（匿名メール）	postfix	○	同一	6

時間を測定した．ただし，初期のシステムの試験運用で使用したドメインはすでに廃止されていたため，本評価では新たなドメインを用意した．このドメインでは一般のメールは送受されておらず，見逃し率や誤検出率は意味を持たないため，評価していない．

代表的なドメイン（サービス）における測定結果を**表 3** に示す．

この表に示されているように，調査した範囲ではすべての送信者が再送機能を持っていた．異なる MTA を用いて再送を行うドメインはいくつか存在し，gmail.com もその 1 つであった．このようなドメインからのメールは従来の greylisting および 5-way handshake では再送を受け付けず管理者がホワイトリストに登録する必要があったが，提案方式ではこのようなメールでもホワイトリストへの登録を必要とせずに受信できることが確認できた．

再送時間については，多くのドメインが 10 秒以内で再送を行っており，greylisting と比較すると提案方式が再送時間の短縮に一定の効果を有することが確認された．しかし，特に qmail を使用しているドメインや gmail.com については再送に 6 分以上かかり，なかには 1 時間近くかかるものもあった．一方，5-way handshake では qmail からの再送は 1 秒以内に行われる[8]．この再送時間の違いは，qmail については 5-way handshake で行われたようにプライマリ MX とのセッションの確立に失敗した場合にはただちにセカンダリ MX とのセッション確立を試みるが，提案方式で行われたように 1 度プライマリ MX とのセッション確立に成功した場合には，その後配送が一時的に失敗しても同一のプライマリ MX に対して再送を試みるためである．gmail.com についても異なる MTA から再送する点を除いて同様の理由で再送時間の違いが現れたと思われる．

4.3　誤検出に関する考察

後期の試作システムの試験運用では誤検出の例は確認されなかったが，実際の運用では様々な理由により誤検出の発生が考えられる．そこで，本節では起こりうる誤検出の発生原因とその対策について議論する．

4.3.1　Message-ID を持たないメッセージの配送

RFC2822[14] によれば，Message-ID フィールドはオプションであって必須ではない．そのため，（エンベロープ From，エンベロープ To，Message-ID）の 3 つ組に基づく再送判定は失敗する可能性がある．実際に yahoo.com や yahoogroups.jp からのメールについては Message-ID フィールドがないものもあった．

この問題への対策としては，Message-ID の代わりに本文のハッシュ値か，必須である Date フィールドを用いる方法が考えられる．前者は再送判定を確実に行える（見逃しが少ない）が，本文を最後まで受信する必要が生じる．一方，後者は同じ時刻（1 秒以内）に同じ送信アドレスから同じ宛先アドレスに 2 通以上のメールが配送された場合には 2 通目以降を再送なしで受け取ってしまう可能性があるが，ヘッダ受信後にただちに SMTP セッションを切断して通信量を削減することが可能である．

4.2 節で述べたように，後期の試作システムでは Message-ID フィールドが含まれないメッセージについては代わりに Date フィールドを用いる再送判定機能を実装し，その結果，たとえば yahoogroups.jp からの一部のメッセージのように Message-ID がないメッセージもすべて受信できることを確認した．

4.3.2　再送を行わない MTA

後期の試作システムの試験運用では確認されなかったが，2.1 節でも述べたように，正常メールを配送するにもかかわらず再送を行わない送信 MTA も一部存在する．その場合，従来の tempfailing 手法ではそこから送られるメッセージが宛先に配送されないことになる．ホワイトリストへの登録によりこのような MTA からのメッセージを受信することは可能であるが，2 章で述べたように，ユーザや管理者が知ることが可能なのは送信 MTA の IP アドレス，エンベロープ From，エンベロープ To の 3 つだけであるため，送信 MTA をホワイトリストに登録すべきかどうかの判定が一般には困難である．

提案方式でもホワイトリストに登録しない限りこのような MTA からのメールを正常に受信することができない．しかし，提案方式において本文を受信した後に強制切断する技法を用いると，再送されなかったメッセージをすべて一時的に保存できるため，たとえば保存したメッセージの送信者アドレスとサブジェクトを提示し，必要があれば後でそれを回復す

ることが可能になる．その結果，もしそれが正常なメッセージであれば，そのメッセージを送信した MTA をホワイトリストに登録すればよい．

なお，自組織内から提案方式を導入した MTA を用いてメール発信を行う場合，MUA（Mail User Agent）の多くが再送を行わない点が問題となりうる．これについては，このような MTA の代わりに MSA（Message Submission Agent）を用いて発信するようにすれば問題ない．

4.3.3　再送時におけるエンベロープ From アドレスの変化

後期の試作システムの試験運用では確認されなかったが，初回時と再送時でエンベロープ From が異なるような正常な送信 MTA も存在する．たとえば，送信 MTA がメッセージの配送を試みるたびにエンベロープ From に配送時刻を埋め込むのであれば，このような現象が起こる．このような例として，文献 11) では BATV [15] があげられている．その場合，従来の tempfailing 手法ではそこから送られるメッセージが宛先に配送されないことになる．

この問題は提案方式でも発生するが，その対策として再送判定からエンベロープ From を除外し，（エンベロープ To，Message-ID）の 2 つ組を用いるようにする方法が考えられる．これは一般に Message-ID が同一のメッセージは同じ送信者から送信したと考えられるためである．しかし，この場合でもエンベロープ From だけでなく Message-ID も再送のたびに変化するような場合，あるいは Message-ID がない場合には再送を正しく判定できず，ホワイトリストへの登録を行うしかない．

4.4　管理・運用コストに関する考察

これまでに述べたように，提案方式では異なった MTA からの再送に対してもホワイトリストへの登録を行わずに受信することが可能であり，その意味で管理コストの低減が可能になる．一方，提案方式の導入により，保存したヘッダや本文の管理などの新たな管理コストが発生する．また，通信量の増加など，運用コストもある程度の増加が見込まれる．そこで，以下では提案方式導入にともなう管理・運用コストに関して議論する．

一般に，管理・運用コストは利用者に対する利便性とトレードオフの関係にあるため，単純な比較は困難である．また，管理・運用コストはたとえばディスク容量やネットワーク帯域など，MTA の利用可能な資源量にも大きく依存する．そこで，特に断りのない限り，MTA の利用可能な資源量にある程度余裕がある状況において従来の greylisting と同程度の利便性を利用者に提供する場合を想定し，greylisting と比較した管理・運用コストの増減について考察する．なお，提案方式の導入あるいは初期設定に要するコストについては，一時的なものであるため議論しない．

4.4.1　再送判定処理の改善に関する管理・運用コスト

まず，再送判定処理の改善にともなって発生する管理・運用コストについて考察する．この場合，再送判定に用いられる 3 つ組の管理が新たな管理・運用コストとして問題となりうる．

しかし，この 3 つ組については，1 通あたりのデータ量が greylisting の場合と同程度でたかだか数百バイトであり，これを保存する期間も greylisting と同程度でよいことから，必要なデータ量も greylisting と同程度でありほとんど問題にはならない．

4.4.2　誤検出からの回復に関する管理・運用コスト

次に，再送しない MTA から配送されたメールの保存にともなって発生する管理・運用コストについて考察する．この場合，保存されるヘッダあるいは本文の管理，およびヘッダや本文の取得にともなう通信量や配送遅延時間の増加が管理・運用コストとして問題となりうる．

このうち，ヘッダあるいは本文の管理については，これらのいずれを保存する場合でも初回配送時から受信者が誤検出に気付いて回復するまでの期間（たとえば数日間）は保存しておく必要があり，保存期間が再送判定に用いられる 3 つ組と比較すると長い．また，特に本文を保存する場合には 1 通あたりのデータ量が大きくなるため比較的大きな記憶容量を必要とし，たとえばすべてのメールについて本文を保存する場合には，保存期間中に配送されるすべてのメールを保存できるだけの容量が必要になる．

しかし，従来の greylisting との比較の観点では，たとえば誤検出からの回復のために差出人アドレスや件名などヘッダに含まれる情報の一部を保存し，これを自動的に利用者に配信するだけでも従来の greylisting が提供する利便性を十分上回っているといえる．その場合，1 通あたりのデータ量はたかだか数百バイトとなるため，たとえば保存期間中に 100 万通のメールを処理する環境[⋆1]では追加で必要となる記憶容量は数百メガバイト程度であり，MTA に標準的に搭載されるディスク容量と比較するとあまり大きくなく，十分実用に耐えうる．

一方，ヘッダや本文の取得にともなう通信量や配送遅延時間については，保存期間にかかわらずつねに発生する．その増加量については再送されないメールの比率や強制切断の時期などに依存するが，たとえば 4.1 節のように再送されないメールの比率が全体の 80%である状況において本文を取得した後に強制切断を行う場合を想定すると，従来の tempfailing

⋆1 岡山大学における約 5 日分の流通量に相当する．

では全体の 20%分のメールを受信すればよいのに対して，提案方式では再送されないメールについては 1 回，再送されるメールについては 2 回通信を行うことから，全体の 120%分のメール受信が必要となる．

しかし，この場合でも tempfailing を用いずにすべてのメールを受信してからフィルタリングを行う方法と比較すると，メールの受信処理件数は 20%の増加にとどまる．また，強制切断の時期を本文取得後の代わりにヘッダ取得後に変更することにより通信量や配送遅延時間の削減が可能であることから，提案方式は通信量や配送遅延時間の観点でも実用に耐えうると思われる．

5. むすび

本研究では，従来の tempfailing の問題点である，異なる MTA からの再送への対処および誤検出時の再送されないメッセージの回復を可能にするため，SMTP セッションをヘッダあるいはメッセージ全体の受信後に強制切断する spam メール対策方式を提案した．また，提案方式に基づいて試作システムを実装して試験運用を行い，その有効性を確認した．さらに，多くのドメインからのメール配送について遅延時間が 5-way handshake と同程度に短縮できることも確認した．本方式は利用者ごとに強制切断機能の有無や切断時期を設定できる点も従来の方式には見られない特徴である．

今後の課題として，長期にわたる実運用を通じての提案手法の性能評価があげられる．また，初回配送時にメッセージを受信しながらその内容に応じて動的に動作を変更するような技法を導入することも今後検討したい．

謝辞　本研究の一部は平成 17〜19 年度科学研究費補助金（基盤研究（B），課題番号 17300038）の補助を受けている．ここに記して感謝の意を表する．

参考文献

1) The Spamhaus Project Ltd.: The Spamhaus Project–ZEN (online). available from http://www.spamhaus.org/zen/ (accessed 2008-06-10)
2) IronPort Systems, Inc.: SpamCop.net–Blocking List (bl.spamcop.net) (online). available from http://www.spamcop.net/bl.shtml (accessed 2008-06-10)
3) SORBS Publishing: SORBS (Spam and Open-Relay Blocking System) (online). available from http://www.sorbs.net/ (accessed 2008-06-10)
4) Graham, P.: Filters vs. Blacklists (online). available from http://www.paulgraham.com/falsepositives.html (accessed 2008-06-10)
5) Ramachandran, A., Dagon, D. and Feamster, N.: Can BNS-Based Blacklists Keep Up with Bots?, *Proc. 3rd Conference on E-Mail and Anti-Spam* (*CEAS 2006*), pp.55–56 (online) (2006). available from http://www.ceas.cc/2006/14.pdf
6) Harris, E.: The Next Step in the Spam Control War: Greylisting (online). available from http://projects.puremagic.com/greylisting/whitepaper.html (accessed 2008-06-10)
7) 吉田和幸：greylisting による spam メールの抑制について，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2004-DSM-35, pp.19–24 (2004).
8) 山口榮作，鈴木常彦：TCP Handshake 制御を利用した spam 対策システム，大学情報システム環境研究，No.8, pp.60–68 (2005).
9) Klensin, J.: Simple Mail Transfer Protocol, RFC 2821, IETF (2001).
10) 前野年紀：お馴染みさん方式 (online). available from http://moin.qmail.jp/_a4_aa_c6_eb_c0_f7_a4_b5_a4_f3_ca_fd_bc_b0 (accessed 2008-06-10)
11) Levine, J.R.: Experiences with Greylisting, *Proc. 2nd Conference on E-Mail and Anti-Spam* (*CEAS 2005*) (online) (2005). available from http://www.ceas.cc/papers-2005/120.pdf
12) 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，情報処理学会分散システム/インターネット運用技術研究会研究報告，No.2004-DSM-45, pp.89–94 (2007).
13) Partridge, C.: DUPLICATE MESSAGES AND SMTP, RFC 1047, IETF (1988).
14) Resnick, P.: Internet Message Format, RFC 2822, IETF (2001).
15) Levine, J., Crocker, D., Silberman, S. and Finch, T.: Bounce Address Tag Validation (BATV) (online). available from http://mipassoc.org/batv/draft-levine-smtp-batv-01.txt (accessed 2008-06-10)

(平成 20 年 6 月 10 日受付)
(平成 20 年 12 月 5 日採録)

山井　成良（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現，総合情報基盤センター）助教授を経て，平成 18 年より同教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

岡山　聖彦（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．平成 17 年同大学総合情報基盤センター助手．平成 19 年同助教．博士（工学）．インターネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

中村　素典（正会員）

平成 6 年京都大学大学院工学研究科博士後期課程単位取得退学．立命館大学理工学部助手，京都大学経済学部助教授，京都大学総合情報メディアセンター助教授，京都大学学術情報メディアセンター助教授を経て，平成 19 年より国立情報学研究所特任教授，現在に至る．博士（工学）．日本ソフトウェア科学会，電子情報通信学会各会員．コンピュータネットワーク，遠隔講義等の研究に従事．

清家　　巧（学生会員）

平成 19 年岡山大学工学部通信ネットワーク工学科卒業．現在，同大学大学院自然科学研究科（電子情報システム工学専攻）博士前期課程在学中．迷惑メール対策，分散システム運用管理等に興味を持つ．

漣　　一平（正会員）

平成 16 年岡山大学工学部通信ネットワーク工学科卒業．平成 18 年同大学大学院自然科学研究科（電子情報システム工学専攻）博士前期課程修了．同年株式会社日立製作所入社．分散システム運用管理等に興味を持つ．

河野　圭太（正会員）

平成 12 年大阪大学工学部電子情報エネルギー工学科卒業．平成 14 年同大学大学院工学研究科（情報システム工学専攻）修士課程修了．平成 16 年同大学院情報科学研究科（情報ネットワーク学専攻）博士課程修了．同年岡山大学総合情報基盤センター助手．平成 19 年同助教．モバイルネットワーク，分散システムの研究に従事．IEEE，電子情報通信学会各会員．博士（情報科学）．

宮下　卓也（正会員）

平成 3 年岡山大学工学部電気電子工学科卒業．平成 5 年同大学大学院工学研究科（電気電子工学専攻）修了．平成 8 年同大学院自然科学研究科（知能開発科学専攻）修了．平成 9 年東京農工大学ベンチャービジネスラボラトリー博士研究員．平成 10 年岡山大学総合情報処理センター助手．平成 16 年同大学総合情報基盤センター助手．平成 17 年津山工業高等専門学校情報工学科助教授．平成 19 年同准教授．ディジタル機器からの放射電磁雑音の計測・予測・抑制，分散システム，ネットワークセキュリティの研究に従事．博士（工学）．IEEE，電子情報通信学会，エレクトロニクス実装学会各会員．