発信者詐称 spam メールに起因するバウンスメール集中への対策方法

山井成良[†1] 岡山聖彦[†1] 宮下卓也[†2]
繁田展史[†3] 丸山伸[†4] 中村素典[†5]

spam メールの蔓延は電子メールにおいて深刻な問題となっている．特に，宛先不明により送り返されるバウンスメールの，詐称発信者に対応する特定の MTA（Mail Transfer Agent）への集中は，ネットワーク資源や計算機資源を大量に消費し，また MTA の過負荷により通常の電子メール（通常メール）の配送に遅延が生じる点で非常に深刻な問題である．そこで，本稿では中小規模の組織を対象としたバウンスメール集中への対策方法を提案する．本方法では，中小規模の組織ではバウンスメールの大部分が普段は電子メールをやりとりしていない MTA から送られる点に着目し，主にバウンスメールを処理する MTA を追加して通常メールとは分離して処理を行う．これにより，通常メールを処理する MTA は負荷が軽減され，通常メールの配送遅延を抑えることが可能になる．実際の事例におけるアクセス記録を分析した結果，本方法はバウンスメールと通常メールを十分高い精度で分離し，通常メールを処理する MTA を効果的にバウンスメール集中から保護できることが確認された．

A Protection Method against Massive Bounce Mails Caused by Sender Spoofed Spam Mails

Nariyoshi Yamai,[†1] Kiyohiko Okayama,[†1] Takuya Miyashita,[†2]
Nobufumi Shigeta,[†3] Shin Maruyama[†4]
and Motonori Nakamura[†5]

Wide spread of spam mails is a serious problem on e-mail environment. Particularly, spam mails with a spoofed sender address is very serious, since they make the MTA (Mail Transfer Agent) corresponding to the spoofed address be overloaded with massive bounce mails generated by the non-deliverable spam mails, and since they waste a lot of network and computer resources. In this paper, we propose a protection method of the MTA against such massive bounce mails, which is suitable for relatively small sites. This method introduces additional mail servers that mainly deal with the bounce mails, considering that the most MTAs sending back bounce mails are likely to have never sent any mails to the target domain recently. This causes the load of the original mail server to be reduced. According to the analysis of the access logs in the the practical example we have experienced, we confirm that the proposed method can fairly separate massive bounce mails from normal mails and can effectively protect the original MTA against massive bounce mails.

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 メールによる被害には，(1) 一般の利用者は，受信した大量の電子メールの中から少数の非 spam メールを選別するために時間を浪費し，場合によっては非 spam メールを誤って削除する危険性がある，(2) 不必要なメールの受信により計算機資源やネットワーク資源を浪費する，(3) spam メールの中継に自組織の MTA（Mail Transfer Agent）が用いられることにより，当該 spam メール

†1 岡山大学総合情報基盤センター
Information Technology Center, Okayama University
†2 津山工業高等専門学校
Tsuyama National College of Technogoly
†3 三菱電機コントロールソフトウェア株式会社
Mitsubishi Electric Control Software Corporation
†4 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University
†5 京都大学学術情報メディアセンター
Academic Center for Computing and Media Studies, Kyoto University

の発信に関与していると疑われる，(4) spam メールの発信者アドレスを自組織のものに詐称されることにより，当該 spam メールの発信に関与していると疑われ，また宛先不明を通知するエラーメール（バウンスメール）の大量発生により MTA が過負荷になる，などがある．

このうち，(4) については，“Joe job” とも呼ばれる事実上のサービス不能（DoS: Denial of Service）攻撃であり，発生頻度は少ないが，その被害は甚大である．たとえば，2002 年 11 月に国内のプロバイダで発生した事例[1] では，30 万通以上のバウンスメールが宛先不明のため詐称された発信元の MTA に送られ，負荷の集中により最大 15 時間の配送遅延が生じ，また復旧までに約 2 日半を要したという被害が発生している．また，2003 年 10 月には米国で少なくとも 3 つのドメインが Joe job の対象となり，多数のバウンスメールを受け取るという事例が発生している[2]．

上記 (4) の問題に対して，これまでにいくつかの対策方法が発表されている[3)~9)]．しかし，従来の対策方法はいずれもバウンスメール発信による通信量を抑制したり，あるいはバウンスメール受信によるディスク使用量を軽減したりすることを主眼としており，通常の電子メール（以下，通常メール）の配送遅延を軽減する効果は期待できない．また，MTA の負荷を軽減する方法としては，MTA の多重化による負荷分散が考えられる．しかし，単純な負荷分散ではすべての MTA に等しく負荷がかかるため，多数のバウンスメールが一度に発生すると，十分な数の MTA を設置しているような大規模な組織でない限り，すべての MTA の過負荷により通常メールの配送に遅延が生じる危険性がある．このように，バウンスメールによるサービス不能攻撃への従来の対策は，いずれも通常メールの配送遅延を避けられない点で問題がある．

そこで本稿では，中小規模の組織を対象とし，通常メールの配送遅延の軽減を目的とした対策方法を提案する．この方法では，中小規模の組織ではバウンスメールの大部分が普段は電子メールをやりとりしていない MTA から送られる点に着目し，バウンスメールと通常メールを異なる MTA で分離して処理を行う．これにより，通常メールを処理する MTA は負荷が軽減され，通常メールの配送遅延を抑えることが可能になる．

2. 従来の対策方法とその問題点

現状の電子メールの仕組みでは発信者アドレスの詐称が容易であるため，事実上すべての spam メールでは発信者を特定されないように発信者アドレスが詐称されている．このとき，詐称された発信者アドレス（以下，被害アドレスと呼ぶ）として実在のアドレスが用いられると，そのアドレス宛にすべてのバウンスメールが短期間に集中して送られ，バウンスメールの保存・記録にディスクを大量に使用するだけでなく，過負荷による MTA の停止や spam ではない通常メールの配送遅延が発生するなどの問題が生じる．また，被害アドレスが実在しないものであっても，ドメイン名の部分が実在すれば，そのドメイン（以下，被害ドメインと呼ぶ）に対する MTA（以下，被害 MTA と呼ぶ）にバウンスメールが大量に送られ，このバウンスメールに対する配送不能通知が管理者に送られる点を除き，上記の場合と同様の問題が生じる．

この問題に対して，これまでにいくつかの対策が発表されている[3)~9)]．これらは，バウンスメールの発信側での対策と受信側での対策に大別できる．

バウンスメール発信側での対策として，Frei ら[3] はバウンスメールによるサービス不能攻撃の影響を分析し，たとえば，バウンスメールの発生を抑えるため宛先不明メールの受信を拒否する，あるいはバウンスメールによる通信量を抑えるために元の電子メールの本文を含めない，などの方法を推奨している．また，現在普及しつつある SPF（Sender Policy Framework）[4]，SenderID [5]，DomainKeys [6]，IIM（Identified Internet Mail）[7] などの発信者認証技術を用いれば，宛先不明メールの受信時に発信者詐称を検出してバウンスメールの発信を抑制することが可能となる．これらの対策を MTA に導入すると，その MTA ではバウンスメールの発生や通信量を抑える効果が得られるが，これらの対策が広範囲に普及しているとはいえない現状では，その効果は限定的であり，バウンスメールによるサービス不能攻撃を防止する効果までは期待できない．

一方，バウンスメール受信側での対策として，postfix ではエラーとなった元のメール中に含まれるヘッダを調べ，たとえば Received ヘッダや From ヘッダ中に詐称の痕跡が残されていれば受信を拒否する方法を利用できる[8]．また，同様の方法として，BATV（Bounce Address Tag Validation）[9] では，エンベロープ From アドレスのローカルパート（@より左側の部分）を書き換えることによりバウンスメールが正当なものかどうかを判断できるようにし，バウンスメールの受信時には宛先アドレスが正当なものでなければ受信を拒否することが可能である．これらの方法はいずれも，実在する被害アドレス宛に送られたバウ

ンスメールをメールボックスに格納しないことを目的としており，ディスクの使用量を削減する効果が期待できる．しかし，これらの対策ではバウンスメールの受信後あるいは受信中にバウンスメールの正当性を識別する必要があるため，1 通あたりの処理時間が増加する点が問題となる．すなわち，大量のバウンスメールが MTA に到着した場合には MTA がますます過負荷になり，通常メールの配送がさらに遅れる危険性がある．

バウンスメール受信側での別の対策として，DNS ラウンドロビンなどの技法を用いて MTA を多重化し，MTA 間で負荷分散を図る方法が考えられる．しかし，単純な負荷分散ではすべての MTA に等しく負荷がかかるため，多数のバウンスメールが一度に発生すると，被害ドメインに十分な数の MTA を設置していない限り，すべての MTA が過負荷になってしまい通常メールの配送に遅延が生じる危険性がある．実際，文献 1) の事例では 4 台の MTA を用意したにもかかわらず，すべての MTA が過負荷になり，通常メールの配送に遅延を生じる結果となった．

以上のように，バウンスメールによるサービス不能攻撃への従来の対策は，いずれも限定的な効果しか期待できず，通常メールの配送に遅延が生ずる点が問題である．

3. バウンスメール集中への対策手法の概要

前章で述べた問題を軽減するため，我々は従来の MTA（プライマリ MTA）とは別の MTA（セカンダリ MTA）を設置し，通常メールは極力プライマリ MTA で受信し，バウンスメールは極力セカンダリ MTA で受信する方法を提案する．この方法では，2 種類のメールの振り分け方法が重要である．そこで，まずバウンスメールの配送経路について考察する．

3.1 バウンスメールの配送経路

spam メールおよびこれに起因するバウンスメールの典型的な配送経路を**図 1**，**図 2** に示す．

まず，図 1 に示すように，spam 発信者は不正中継を許す MTA（spam 配送 MTA，originating MTA）を利用して spam メールの発信を行う（図 1 (1)）．spam 配送 MTA は spam メールを受け取るとその配送を試みる（同 (2)）が，その過程でドメイン名が無効であったり，ユーザ名が無効であったりした場合（同 (3)）には，バウンスメールが spam 配送 MTA からただちに被害 MTA（victim MTA）に返送される（同 (4)）．

一方，最近では，中継用 MTA（relay MTA）でいったん外部からの電子メールを受信して，たとえば電子メール中のウィルスの有無を確認した後にドメイン内部の別の MTA（以下，末端 MTA と呼ぶ）に配送するようにしているドメインも多い．その場合には，図 2 に示すように，spam 配送 MTA が spam 発信者から spam メールを受け取る（図 2 (1)）と，spam 配送 MTA は中継用 MTA への配送を試みる．ところが，中継用 MTA 自身は宛先アドレスのドメイン名だけを見て中継の可否を決定するため，@以降のドメイン部分が正しければその電子メールをいったん受け取ってしまう（同 (2)）．その後，中継用 MTA はその電子メールを末端 MTA に配送しようとする（同 (3)）が，その時点で宛先アドレスが無効であることが判明する（同 (4)）ため，バウンスメールは中継用 MTA から被害アドレスに返送される（同 (5)）．

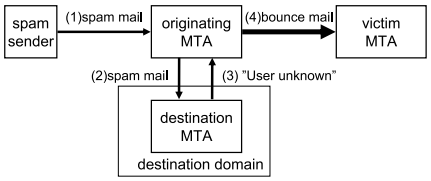


図 1 バウンスメールの配送経路（直接配送）
Fig. 1 Delivery of bounce mails (direct delivery).

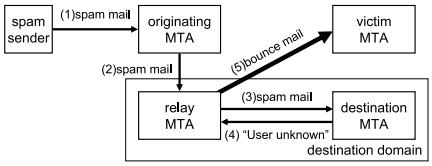


図 2 バウンスメールの配送経路（中継配送）
Fig. 2 Delivery of bounce mails (redirected delivery).

以上のことから，バウンスメールは配送経路により 2 種類に分類できることが分かる．1 つは図 1 のように spam 配送 MTA から直接返送されるものであり，もう 1 つは図 2 のように中継用 MTA から返送されるものである．以下では，前者を直接配送バウンスメール，後者を中継配送バウンスメールと呼ぶことにする．

3.2 直接配送バウンスメールへの対策

前節で述べたように，直接配送バウンスメールは 1 つの spam 配送 MTA から被害ドメイン宛に多数発信されることが予想される．このバウンスメールをセカンダリ MTA で受信するためには，当該ドメインのセカンダリ MX として DNS にセカンダリ MTA を登録しておき，spam 発信 MTA の IP アドレスをいずれかの MTA のログから取得すると，spam 配送 MTA からプライマリ MTA への SMTP コネクションを拒否するように経路上のいずれかのルータ，レイヤ 3 スイッチあるいはプライマリ MTA 自身（以下，ルータ

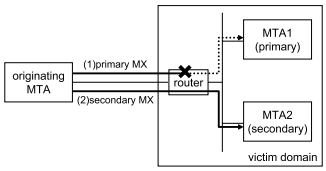


図 3 直接配送バウンスメールの配送
Fig. 3 Delivery of direct bounce mails.

などと表す）の IP フィルタリング機能を用いて設定すればよい．これにより，**図 3** に示すように spam 発信 MTA はまずプライマリ MX であるプライマリ MTA にバウンスメールを送信しようとするが，コネクションの確立をルータなどで拒否されるため，セカンダリ MX であるセカンダリ MTA にバウンスメールを送信するようになる．

なお，この手法ではルータなどにおいてフィルタリングの対象となる IP アドレスを自由に追加・削除できる機能が必要となる．この機能は，Cisco 社製品など一部のルータやレイヤ 3 スイッチでは実装されていないが，たとえば ACL（Access Control List）の設定内容をいったん消去してから再設定したり，複数の ACL を交互に書き換えて適用したりすることにより，若干オーバヘッドは増加するものの同等の機能を実現することができる．一方，プライマリ MTA では，多くの OS が対象を自由に追加・削除できるようなフィルタリング機能を有しているため，問題とはならないと思われる．

また，プライマリ MTA では，たとえば FreeBSD の IP firewall など，TCP コネクションを確立する前にフィルタリングを行う機能を用いる必要がある．これは，

- TCP コネクション確立後に受信を拒否する場合には，一般にユーザプロセス起動後にフィルタリング処理が行われ，プライマリ MTA の負荷が軽減されなくなるため，
- たとえば qmail [10] などプライマリ MTA が TCP コネクション確立後に受信を拒否してもセカンダリ MTA への配送を試みないプログラムが普及しているため，

の 2 つの理由に基づく．

3.3 中継配送バウンスメールへの対策

一般に，バウンスメールを発信する中継用 MTA は数が多く，また 1 台あたりのバウンスメール数は少ないことが予想される．したがって，上記のようにルータなどでフィルタリングを行おうとすると，各中継用 MTA に対して個別のフィルタ設定を行う必要があるため，フィルタ数の増加によりルータなどの性能低下を招くにもかかわらず，一度バウンスメールを受信してからその発信元に対するフィルタを設定しても同一の発信元からのバウンスメールの送信が少ないため，実際に有効であるか疑問である．

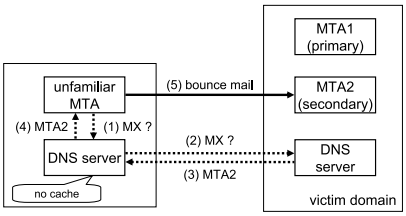


図 4 中継配送バウンスメールの配送
Fig. 4 Delivery of redirected bounce mails.

一方，被害ドメインが中小規模であれば，このような中継用 MTA の多くは，被害ドメインとの間で通常は電子メールの交換を行っておらず（以下，このような MTA を非親交 MTA（unfamiliar MTA）と呼ぶ），バウンスメールの送信の際に初めて DNS サーバに被害ドメインの MX レコードを問い合わせるものと思われる．そこで，我々はこの点に着目し，バウンスメールの受信を検出した時点で DNS の MX レコードを書き換える．具体的には，プライマリ MX のレコードを削除し，セカンダリ MTA がプライマリ MX として登録されるようにする．また，これらの MX レコードに対するキャッシュの有効期限（TTL）を通常は長めに設定しておき，MX レコード書き換え時には短く設定するようにする．その結果，設定変更後は電子メールは以下の手順により配送される．

非親交 MTA が被害ドメインにバウンスメールを送ろうとすると，**図 4** に示すように非親交 MTA はまず身近な DNS サーバに被害ドメインの MX レコードを問い合わせる（図 4 (1)）．すると，この DNS サーバではキャッシュ中に被害ドメインの MX レコードが存在しないため，被害ドメインの DNS サーバにこれを問い合わせる（同 (2)）．被害ドメインの DNS サーバでは設定変更後はセカンダリ MTA がプライマリ MX として登録されているため，これを問合せ元の DNS サーバに応答し（同 (3)），非親交 MTA は身近な DNS サーバからの応答（同 (4)）に基づきセカンダリ MTA にバウンスメールを配送する（同 (5)）．

一方，**図 5** に示すように，普段から頻繁に被害ドメインとの間で電子メールを交換している MTA（以下，親交 MTA（familiar MTA）と呼ぶ）が電子メールを配送しようとすると，同様に MTA はまず身近な DNS サーバに被害ドメインの MX レコードを問い合わせる（図 5 (1)）．ところが，この DNS サーバには

キャッシュ中に MX レコードが存在している可能性が高く，その場合には設定変更前の値であるプライマリ MTA が返される（同 (2)）ため，親交 MTA はプライマリ MTA に電子メールを配送する（同 (3)）．

このような動作により，中継配送バウンスメールの多くはセカンダリ MTA に配送される一方で，通常の電子メールは主としてプライマリ MTA に配送されるため，MTA の負荷分散を図ることができる．

なお，セカンダリ MTA では，攻撃を受けている間は被害アドレス宛（被害アドレスのローカルパートがランダムに選ばれている場合には被害ドメイン宛のすべて）のバウンスメール（MAIL-FROM アドレスが空あるいはそのローカルパートが MAILER-DAEMON であるような電子メール）の受信を拒否するように設定すれば，セカンダリ MTA の負荷を軽減できる．ただし，その代わりに，対策方法の動作中に被害ドメインの利用者が宛先不明の電子メールを偶然送信した場合に返される正当なバウンスメールまでも受信拒否する危険性が生じる．また，セカンダリ MTA が通常メールを受信した場合にこれをプライマリ MTA に転送できるようにあらかじめ設定しておく．

3.4 対策の開始と終了

本方法の効果を十分に発揮するには，バウンスメール集中の兆候を早期に検出することが重要である．これについては，

(1) プライマリ MTA においてバウンスメールを短時間に多数受け取った場合，
(2) DNS サーバに対して特定のドメインに対する MX レコードの問合せが短時間に多数あった場合，

の各場合を兆候の検出と見なす方法が有効である[11]．ただし，MX レコードの代わりに全（ANY）レコードを問い合わせる MTA も存在することから，以下では MX レコードと全レコードの両者（以下，MX/ANY レコードと表す）に対する問合せを考慮するものとする．

一方，対策の終了は，被害アドレスに対するバウンスメールが一定期間検出されなくなった時点で行う．本手法ではプライマリ MX としてプライマリ MTA がキャッシュされている spam 中継 MTA からバウンスメールが送られる可能性があるため，本来であればプライマリ MTA，セカンダリ MTA の両方においてバウンスメールの検出を行うべきである．しかし，セカンダリ MTA で受信するバウンスメールの方が多いと予想され，またプライマリ MTA だけでバウンスメールを受信する状態では本手法の効果が発揮されないため，セカンダリ MTA だけで終了を判断すれば十分であると思われる．

4. バウンスメール集中対策システムの設計

本章では前章で述べた方針に基づいて設計したバウンスメール集中対策システムについて述べる．

4.1 システム構成

一般に DNS サーバやセカンダリ MTA は複数台設置されることがあるため，これらが連携して動作する必要がある．特に，対策の開始や終了は 1 台のサーバで判定するのではなく，システム全体として判定するようにする必要がある．

そこで，本システムでは**図 6** に示すようにプライマリ DNS サーバが中心となって他のサーバを制御するようにした．その際，MX/ANY レコードの問合せ回数については，多少の誤差を許容しても少ない通信量で集計を行えるようにするため，対策の開始基準となる回数（以下，開始基準回数と呼ぶ）とは別にプライマリ DNS サーバに通報する回数（以下，通報基準回数と呼ぶ）を設けるようにした．すなわち，各セカンダリ DNS サーバは通報基準回数の問合せを基準時間内に受けるたびに問合せの回数とその受信期間をプライマリ DNS サーバに通知し，プライマリ DNS サーバが自身での問合せ件数を含めて合計で開始基準回数の問合せを基準時間内に受けたと判断できる場合に対策を開始するようにした．

また，対策の終了判定は，すべてのセカンダリ MTA からバウンスメールが一定期間検出されなくなった時

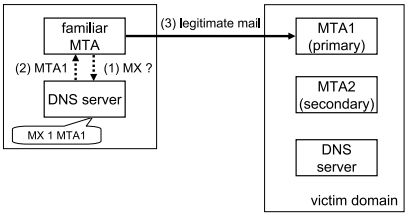


図 5 通常メールの配送
Fig. 5 Delivery of legitimate mails.

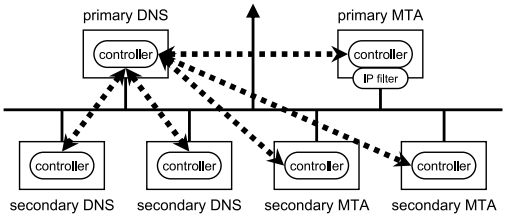


図 6 試作システムの構成
Fig. 6 Configuration of the prototype system.

点で行うようにした．この構成により，新たにセカンダリ DNS サーバやセカンダリ MTA を追加する場合にも，これらとプライマリ DNS サーバとの間で新たに通信を行うようにすればよく，他のサーバは変更する必要がないという利点も有する．

4.2 全体の手順

これまで述べた内容をまとめると，対策手法は以下のような手順で動作する．

(1) 初期状態として，プライマリ MTA およびセカンダリ MTA をそれぞれプライマリ MX，セカンダリ MX として全 DNS サーバに登録しておく．このとき，これらのレコードの TTL を長く設定しておく．また，プライマリ DNS サーバから他のすべてのサーバ上の対策プログラムとコネクションを確立しておく．

(2) 各 DNS サーバで問合せログを監視し，特定のドメインに対する通報基準回数の MX/ANY レコード問合せを基準時間内に受けたかどうか調べる．また，各 MTA においてログを監視し，3.4 節で示した条件を満たすバウンスメールを受信したかどうか調べる．もし，いずれかにおいてバウンスメール集中の兆候が検出されれば，プライマリ DNS サーバにバウンスメール集中検出を通知し，次に進む．

(3) プライマリ DNS サーバではバウンスメール集中検出メッセージを受信すると，プライマリ MX レコードを削除する．このとき，このレコードの TTL を短く設定する．プライマリ MX レコードの削除はただちに各セカンダリ DNS サーバに伝えられる．また，これにともない，各セカンダリ DNS サーバは問合せログの監視を休止する．

(4) いずれかの MTA で spam 配送 MTA を特定した場合，その MTA の IP アドレスをプライマリ DNS サーバに通知する．プライマリ DNS サーバはルータなどにおいて spam 配信 MTA からプライマリ MTA への SMTP コネクションを拒否するフィルタリングを設定すると同時に，すべてのセカンダリ MTA に対して spam 配信 MTA の IP アドレスを通知する．各セカンダリ MTA では通知された MTA からの受信をこれ以降監視するようにする．また，いずれかの MTA において被害アドレスを検出した場合，その被害アドレスをプライマリ DNS サーバに通知する．プライマリ DNS サーバではすべての MTA に詐称アドレスを通知する．各 MTA では，被害アドレス宛のバウンスメールの受信を拒否するように設定変更する．

(5) プライマリ MTA では引き続きログを監視し，3.4 節で示した条件を満たすバウンスメールを短時間に複数回受信したかを調べる．もし，このような受信があれば (4) に進む．また，セカンダリ MTA ではログを監視し，以下の処理を行う．

- 被害アドレス宛のバウンスメールが受信されない場合はプライマリ DNS サーバにその被害アドレスの解除通知を送信する．プライマリ DNS サーバではすべてのセカンダリ MTA から被害アドレスの解除通知を受信すると，その被害アドレスの解除通知を全 MTA に送信する．各 MTA ではその被害アドレス宛のバウンスメールの受信拒否設定を解除する．
- spam 配送 MTA からバウンスメールが受信されない場合はプライマリ DNS サーバに当該 MTA のフィルタリング解除通知を送信する．プライマリ DNS サーバではすべてのセカンダリ MTA から同一の解除通知を受けると，ルータなどのフィルタリングを解除すると同時に，すべてのセカンダリ MTA に当該 MTA の監視解除通知を送信する．各セカンダリ MTA では当該 MTA を監視対象から除外する．
- 監視対象となるバウンスメールが一定期間受信されない場合，プライマリ DNS サーバにバウンスメール対策終了通知を送信する．プライマリ DNS サーバでは，すべてのセカンダリ MTA からバウンスメール対策終了通知を受信した場合，(6) に進む．

(6) DNS サーバにおける MX レコードの設定を初期状態に戻し，(2) に進む．

5. 提案方法の実装と評価

5.1 試作システムの実装

前章で述べた設計に基づき，試作システムの実装を行った．試作システムではプライマリ MTA，プライマリ DNS サーバのほかにセカンダリ MTA，セカンダリ DNS サーバを各 2 台用意した．各計算機の OS には FreeBSD（4.5 および 4.9）を用いた．試作システムでは IP フィルタリング機能として，プライマリ MTA が持つ FreeBSD の IP firewall を用いた．

各 DNS サーバでは BIND9.2.2 を用い，MX レコードの更新には標準装備の動的更新機能を用いた．その際，TSIG 署名付き更新機能を用いることにより，外部からの更新を防ぐように設定した．また，プライマ

リ DNS サーバにおける MX レコードの更新をただちにセカンダリ DNS サーバに反映させるため，DNS NOTIFY 機能を利用した．一方，各 MTA では sendmail 8.12.9 を用いた．各 DNS サーバや各 MTA におけるログの監視や制御には perl を用いた自作プログラムを用いた．

5.2 動作確認

次に試作システムの動作確認について述べる．

試作システムの動作確認には，本来であれば発信者詐称 spam メールを実際に発信することが望ましいが，この方法は倫理上問題がある．そこで実際のネットワークと切り離した実験環境を構築し，その環境でシミュレーション実験を行った．

まず，DNS サーバへの MX/ANY レコードの問合せ回数に基づく対策開始動作が正しく実行されるかどうかを確認するため，外部から各 DNS サーバに MX レコードを何回か問い合わせる実験を行った．その際，文献 11) の結果に基づき，開始基準回数は 10 分間で 4 回，通報基準回数は 10 分間で 2 回と設定した．実験の結果，いずれかの DNS サーバが開始基準回数の MX レコード問合せを受けた場合および 2 つ以上の DNS サーバで通報基準回数の MX レコード問合せを受けた場合のいずれの場合にも試作システムはこれを正しく検出し，DNS サーバにおいてプライマリ MTA に関する MX レコードが削除されていることを確認した．また，中継配送バウンスメールに対する対策が有効かどうかを確認するため，この状態で外部の DNS サーバのキャッシュをいったん無効化し，これを参照する外部の MTA を用意して試作システムに対してバウンスメールの配送を試みた．その結果，すべてのバウンスメールはセカンダリ MTA に配送されることを確認した．

次に，プライマリ MTA におけるバウンスメールの受信数に基づく対策開始動作が正しく実行されるかどうか，ならびに直接配送バウンスメールに対する対策が有効かどうかを確認するため，プライマリ MTA に関する MX レコードが存在する状態でバウンスメールを 1 台の外部 MTA から多数発生させて試作システムに配送する実験を行った．その際，対策開始の基準としては，文献 11) の結果に基づき，各 MTA で 10 分間に 10 通以上のバウンスメールを同一 MTA から受信した場合とした．実験の結果，バウンスメール 1,000 通を送信したところ，プライマリ MTA で 10 通，2 台のセカンダリ MTA では各 4 通のバウンスメールを受信するにとどまり，残りのバウンスメールはまずプライマリ MTA でフィルタリングされ，その後セカンダリ MTA で受信拒否されたことを確認した．

表 1 被害ドメインに関する攻撃期間中の電子メールおよび MX/ANY レコード問合せに関する統計
Table 1 Statistics of mails and MX/ANY queried of the victim domain during the attack.

全メール数	73,320
バウンスメール数	68,578
その他の宛先不明メール数	4,435
全メールに対する送信 MTA 数	22,276
同一 MTA からの最大メール数	2,996
MX/ANY レコード問合せ件数	30,119
MX/ANY レコード問合せ元数	21,636
MX レコード有効期限	7 日間

最後に，対策終了状態を正しく判定できるか実験を行った．10 分以上バウンスメールを受信しなかった場合には初期状態に復旧するように設定したところ，最後のバウンスメールを受信拒否してから 10 分経過後に初期状態に戻ることが確認された．

以上の結果から，試作システムは実験した範囲では期待どおりに動作するといえる．

5.3 有効性の検証

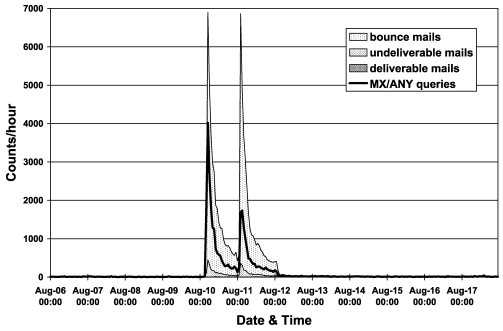
次に試作システムの有効性を検証する．

前節と同様に，試作システムの有効性の検証を行うためには，本来であれば発信者詐称 spam メールを実際に発信することが望ましいが，この方法は倫理上問題があるため困難である．そこで，我々は長期間にわたって我々のドメインに対する攻撃を待ち続けた．その結果，2004 年 8 月 10 日午前 4 時 33 分から 8 月 12 日午前 3 時 38 分☆にかけて岡山大学のあるサブドメインに対して 6 万 8 千通以上のバウンスメールによる攻撃を受けた．

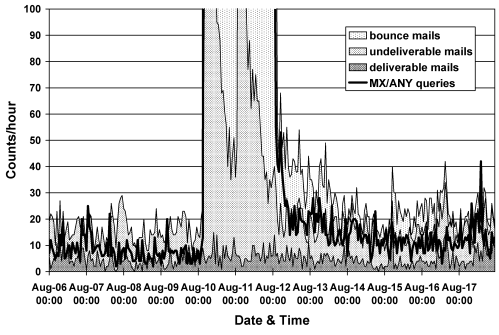
残念ながら，攻撃を受けた期間には試作システムを被害ドメインには導入していなかったため，代わりの方法として岡山大学全体のメールゲートウェイ（2 台）および DNS サーバ（4 台）に残されていた 2004 年 8 月 6 日午前 0 時から 2004 年 8 月 17 日午後 12 時までのログを解析した．

被害ドメインに関する攻撃期間中の電子メールおよび MX/ANY レコード問合せに関する統計を**表 1** に示す．また，被害ドメイン宛の 1 時間あたりのバウンスメール（発信者アドレスが空であるものに限る）数（bounce mails），バウンスメール以外の宛先不明メール（以下，宛先不明メール）数（undeliverable mails），バウンスメール以外の正規の受信者宛の電子メール（以下，配送可能メール）数（deliverable mails）を積上げ面グラフとして**図 7** に示す．この図には被害ドメ

☆ この期間の特定は 5.4 節で述べる方法に基づく．



(a) 全体図
(a) overall view



(b) 拡大図
(b) magnified view

図 7 1 時間あたりの電子メール受信数および MX/ANY レコード問合せ件数
Fig. 7 The numbers per hour of mails and MX/ANY queries.

インに対する 1 時間あたりの MX/ANY レコード問合せ件数も折れ線グラフとして示してある．この図より，被害ドメインは 2 回に分けて攻撃を受けたことが分かる．どちらの回においてもバウンスメール数が増加すれば MX/ANY レコード問合せ件数も増加することから，我々が想定したとおり，バウンスメールを送信した多くの MTA が MX レコードのキャッシュを持っていないことが分かる．なお，宛先不明メール数もバウンスメールの増加に合わせて増加していることに注意する．このうちの大部分は，この攻撃では被害アドレスのローカルパートがランダムであったため，spam メール受信側で動作する spam 対策システム☆や自動返信システム☆☆が返送した電子メールが宛先不明となったものである．

次に，我々はログを基に，試作システムが導入されていたと仮定した場合における提案方法の有効性を解析した．その結果を以下に示す．なお，上記のようにバウンスメールの増加にともなって宛先不明メールも増加し，被害ドメインの MTA に悪影響を及ぼすことから，以下の解析ではバウンスメールと宛先不明メール（以下，両者をあわせて攻撃メールと呼ぶ）を対象に解析を行った．

まず，バウンスメール 68,578 通と宛先不明メール 4,435 通をあわせた計 73,013 通の攻撃メールのうち，攻撃開始以前に何らかの電子メール（おそらく spam メールと思われる）の配送を受けた MTA から発信されたものが 195 通（0.3%）確認された．これらの MTA は攻撃メール配送時にも MX レコードをキャッシュに持っていたと推定されるため，これらの 195 通はプライマリ MTA に配送されるものと思われる．残りの攻撃メールについては，MX レコードの有効期限全体にわたるログを確認できないが，表 1 の送信 MTA 数と MX/ANY レコード問合せ元数がほぼ等しいことから，そのほとんどについては送信 MTA が MX レコードのキャッシュを持たないと推定される．これにより，たとえ攻撃の兆候を検出するまでの時間差を考慮したとしても，ほとんどの攻撃メールがセカンダリ MTA に配送されるものと思われる．

なお，表 1 で示されている 2,996 通など，同一 MTA から多数配送されたバウンスメールについては直接配送バウンスメールの疑いがある．しかし，ログ解析だけでは MX/ANY レコードの問合せ元と MTA との対応が不明確であるため，プライマリ MTA へのフィルタリングが必要であったか，それともプライマリ MX レコードの削除だけで十分だったかは検証できなかった．

次に，配送可能メールから spam メールと思われるものを除いたもの（以下，通常メール）191 通のうち，攻撃開始以前に発信が確認できなかった MTA から送られてきたものおよび攻撃開始以降に MX/ANY レコードの問合せが確認された MTA から送られてきたものは合計で 29 通（15%）あった．これらの電子メールは攻撃開始後に MX/ANY レコードの問合せがあったと推定されるため，セカンダリ MTA に配送されたと思われる．そのうちの大部分は偶然 MX レコードのキャッシュが無効化されたもので，また残りについては，おそらく MX レコードのキャッシュを定期的（1 日に 1 回）に無効化しているものと思われることがログ解析により判明している．この値は MX レコードの有効期限の調整やホワイト DNS サーバリスト[12] の導入により改善できるものと思われる．

以上の分析結果から，提案方法は攻撃メールと通常

☆ ここでは発信者が実在していることを確認するため，再送を促すメッセージを自動返信するものを指す．
☆☆ ここでは電子メールを受信すると自動的に発信者に留守や転送先を通知するようなシステムを指す．

メールを十分高い精度で分離し，プライマリ MTA を効果的にバウンスメールを含む攻撃メールによるサービス不能攻撃から保護できるといえる．

5.4 各種パラメータに関する考察

文献 11) では 40 通程度の宛先不明メールを自ら送信した場合のバウンスメールの受信頻度と DNS サーバにおける MX/ANY レコードの問合せ頻度を調査したが，この調査は実際の攻撃とは大きく異なるため，これだけでは不十分である．そこで，今回の攻撃事例のログに基づき，対策の開始・終了基準など各種パラメータについて考察する．

まず，対策の終了基準を考察するため，2 台の MTA におけるバウンスメールの受信間隔を解析した．その際，終了基準となるバウンスメール無検出時間を目安として 10 分に設定し，この設定が妥当であるかどうかを検証した．その結果，1 台目の MTA のログでは 8 月 12 日午前 3 時 24 分頃，2 台目の MTA のログでは 8 月 12 日午前 3 時 38 分頃，さらに 1 台しかセカンダリ MTA がなかった場合を想定して 2 台の MTA のログを統合したものについても 8 月 12 日午前 3 時 38 分頃にそれぞれ初めてバウンスメール無検出時間が 10 分を超えたことが確認された．この時刻は図 7 における攻撃終了時刻とよく一致することから，上記の 10 分は対策の終了基準として妥当と思われる．

次に，対策の開始基準を考察するため，3.4 節で述べたようにプライマリ MTA におけるバウンスメールの受信頻度と DNS サーバにおける MX/ANY レコードの問合せ頻度をログを用いて解析した．このうち後者については 4 台の DNS サーバのうち 2 台のみドメイン登録におけるネームサーバとして登録していたため，この 2 台のログのみを解析の対象とした．

攻撃開始時（8 月 10 日午前 4 時 33 分頃）におけるバウンスメール受信累積数と MX/ANY レコード問合せ累積件数を**図 8** に示す．この図より，プライマリ MTA は最初のバウンスメール受信時刻からの 1 分間で 5 通以上のバウンスメールを受信し，また各 DNS サーバは最初の MX/ANY レコード問合せ受信時刻からの 1 分間でともに 10 回以上の MX/ANY レコードの問合せを受信したことが分かる．したがって，プライマリ MTA で 1 分以内に 5 通のバウンスメールを受信したとき，また DNS サーバでは通報基準回数として 1 分以内に 10 回，起動基準回数としては 1 分以内に 20 回の問合せがあったときが対策開始基準の候補として考えられる．

一方，対策開始基準の設定では，攻撃の兆候を誤検出しないこと，ならびにできるだけ早期に攻撃の兆候を検出できることの両方が同時に求められる．そこで，上記の対策終了基準を満たした後のバウンスメール受信数および MX/ANY レコード問合せ件数を調査した．その結果，バウンスメールについては最も集中している部分で 5 秒間で 7 通の受信があり，上記の 1 分以内に 5 通では誤検出を起こすことが判明したため，受信回数を増加させて 2 分以内に 10 通を受信したときとするのが今回の事例では妥当と思われる．また，MX/ANY レコードについては，2 台の DNS サーバの合計で 1 分間に最大 5 件の問合せしかないことが判明したため，早期に検出できるように通報基準回数として 1 分以内に 5 回，起動基準回数としては 1 分以内に 10 回の問合せがあったときとするのが妥当と思われる．

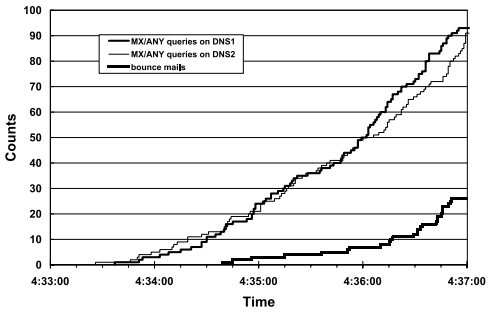


図 8 攻撃開始時におけるバウンスメール受信累積数および MX/ANY レコード問合せ累積件数
Fig. 8 The cumulative bounce mails and MX/ANY queries at the start of the attack.

ただし，上記の開始・終了基準は今回の事例のみから得られた結果であり，たとえばメーリングリストを運用するなど普段から多量の電子メールを発信しているような環境には必ずしも妥当であるとは限らないことに注意が必要である．

6. ま と め

本稿では，発信者詐称 spam メールに起因して大量に発生するバウンスメールによるサービス不能攻撃に対して，バウンスメールと通常の電子メールを分離して処理することにより通常の電子メールの配送に与える影響を軽減する方法を提案し，その設計および実装方法を述べた．また，シミュレーション実験により，試作システムが正しく動作することを確認し，実際の事例を分析して提案方法の有効性を確認した．今後の課題としては，実際のネットワークでの運用を通して有効性を検証し，また他の環境での事例を収集して対策の開始・終了基準など各種パラメータの調整を行うことがあげられる．

謝辞 本研究の一部は平成 15〜16 年度科学研究費補助金（基盤研究（C)(2)，課題番号 15500039）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) 柴沼 均：大量迷惑メールで障害，毎日新聞縮刷版，635，毎日新聞社，2002 年 11 月 7 日朝刊 26 面 (2002).
2) McWilliams, B.: Wired News: Time-Travel Spammer Strikes Back (2003). http://www.wired.com/news/technology/0,1282,61026,00.html
3) Frei, S., Silvestri, I. and Ollmann, G.: Mail Non-Delivery Notice Attacks (2004). http://www.techzoom.net/mailbomb
4) Wong, M. and Schlitt, W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-MAIL, version 1, Internet-Draft: draft-schlitt-spf-classic-02, IETF, work in progress (2005).
5) Lyon, J. and Wong, M.: Sender ID: Authenticating E-Mail, Internet-Draft: draft-lyon-senderid-core-01, IETF, work in progress (2005).
6) Delany, M.E.: Domain-based Email Authentication Using Public-KeysAdvertised in the DNS (DomainKeys), Internet-Draft: draft-delany-domainkeys-base-02, IETF, work in progress (2005).
7) Fenton, J. and Thomas, M.: Identified Internet Mail, Internet-Draft: draft-fenton-identified-mail-02, IETF, work in progress (2005).
8) Postfix Backscatter Howto. http://www.postfix.org/BACKSCATTER_README.html
9) Levine, J., Crocker, D., Silberman, S. and Finch, T.: Bounce Address Tag Validation (BATV) (2004). http://mipassoc.org/batv/draft-levine-mass-batv-00.txt
10) Levine, J.: *qmail*, O'Reilly (2004).
11) 田中 清，山井成良，岡山聖彦，宮下卓也，中村素典，丸山 伸：発信者詐称 SPAM メールによるサービス不能攻撃の早期検出手法，情報処理学会第 64 回全国大会講演論文集，2H-2 (2002).
12) 丸山 伸，中村素典，岡部寿男，山井成良，岡山聖彦，宮下卓也：動的に応答を変える DNS を利用した電子メール受信の優先制御，情報処理学会論文誌，Vol.47, No.4, pp.1021–1030 (2006).

(平成 17 年 7 月 8 日受付)
(平成 18 年 2 月 1 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を経て，現在岡山大学総合情報基盤センター助教授．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．博士（工学）．インタ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．

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．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．

繁田　展史

平成 14 年岡山大学工学部情報工学科卒業．平成 16 年同大学大学院自然科学研究科博士前期課程修了．同年三菱電機コントロールソフトウェア株式会社入社．広域分散システム，高速ネットワーク等に興味を持つ．

丸山　　伸（学生会員）

平成 10 年京都大学大学院理学研究科地球惑星科学専攻博士後期課程研究指導認定退学．平成 10 年京都大学学術情報メディアセンター教務技官，平成 11 年同助手として，教育用計算機システムの運用管理および設計に従事．平成 15 年京都大学大学院情報学研究科博士後期課程入学，同在学中．教育用計算機システムの運用技術，大規模システムの構築技術，電子メールの配送におけるセキュリティ向上技術等に興味を持つ．有限会社シー・オー・コンヴ取締役．

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を経て，平成 14 年より京都大学学術情報メディアセンター助教授，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．