発信者詐称 SPAM メールに対する対策手法

山井成良　　山外芳伸　　宮下卓也　　大隅淑弘

岡山大学 総合情報処理センター

{yamai,yamasoto,t_myst,oosumi}@cc.okayama-u.ac.jp

概　要

電子メールにおいて SPAM メールの蔓延は大きな問題となっている．特に，発信者アドレスを自組織のものに詐称された SPAM メールは，大量のエラーメールにより自組織のメールサーバの過負荷を招き，計算機資源やネットワーク資源を浪費する点や通常の電子メールの配送処理に影響を与える点などが問題となる．本稿ではこれらの問題点を軽減する発信者詐称 SPAM メールへの対策手法を提案する．本手法ではメールサーバを 2 台用意し，エラーメールを一方のメールサーバで集中的に処理することにより，通常のメールを処理するもう一方のメールサーバの負荷を軽減することができる．また，本手法では SPAM メールに起因するエラーメールの受信を拒否することにより計算機資源やネットワーク資源の浪費を抑えることもできる．

A Protection Method against SPAM Mails with Sender Address Spoofing

Nariyoshi Yamai, Yoshinobu Yamasoto, Takuya Miyashita, and Yoshihiro Oosumi

Computer Center, Okayama University

{yamai,yamasoto,t_myst,oosumi}@cc.okayama-u.ac.jp

Abstract

Wide spread of SPAM mails is one of the most serious problems on e-mail environment. Especially, SPAM mails with sender address spoofing should not be left alone, since they make the mail server corresponding to the spoofed address be overloaded with a great number of error mails generated by the SPAM mails, and since they waste a lot of network and computer resources. In this paper, we propose a protection method of the mail server against such SPAM mails. This method provides an additional mail server that mainly deals with the error mails to reduce the load of the original mail server. This method also provide a function that refuses error mails to these two mail servers to save the network and computer resouces.

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，多くの組織では自組織の利用者にサービスを提供するために電子メールサーバを運用している．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SPAMメール(UBE(Unsolicited Bulk E-mail) あるいはUCE(Unsolicited Commercial E-mail) とも呼ばれる) の蔓延は大きな問題になっており，その対策は重要である．

SPAMメールによる被害には，(1) 不必要なメールの受信により計算機資源，ネットワーク資源，通信費用，通信時間などを浪費する，(2)SPAMメールの中継に自組織のメールサーバが用いられることにより，当該SPAMメールの発信に関与していると疑われる，(3)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るだけでなく，エラーメールが大量に返されメールサーバが過負荷になる，などがある．このうち，(1)，(2) に対しては組織内の全てのMTA(Mail Transfer Agent) に対してopen relayを許さないようにする方法 [1]，MAPS(Mail Abuse Protection System) RBL(Realtime Black-hole List)[2] 等を用いてopen relayを許すメールサーバからは電子メールを受信しないようにする方法など，いくつかの対策手法が知られている．一方，(3) についてはSMTPの拡張[3]，authsmtpd[4]，ident-proxy[5] など，自組織の利用者が発信者アドレスを詐称しないようにする方法はいくつか提案されているが，他組織の利用者が発信者アドレスを自組織のものに詐称したSPAMメールを発信した場合の対策はこれまで知られていない．

そこで，本稿では (3) の被害に対する対応策として，エラーメールによるMTAの過負荷を軽減し，通常のメール配送にできるだけ影響を与えないようにする手法を提案する．本手法ではMTAを2台用意し，SPAMメールを一方のMTAで集中的に処理することにより，通常のメールを処理するもう一方のMTAの負荷を軽減することが可能となる．

2 発信者詐称SPAMの問題点

SPAMメールの実態は十分把握されていないが，100万以上の電子メールアドレスがCD-ROM等で販売されている現状[1]から，1度に送られるSPAMメールの宛先も同程度であると推測できる．このうちの一部のアドレスについては，宛先アドレスの誤りなどの理由によりエラーメールとして発信者に送り返される．エラーメールの発生割合についても不明であるが，仮に1%程度としても，1万通以上のエラーメールが発信者に送り返されることになる．

ところが，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，事実上全ての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，詐称アドレスと呼ぶ) として実在のアドレスが用いられると，そのアドレス宛に全てのエラーメールが短期間に集中して送られ，エラーメールの保存・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，詐称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，そのドメインに対するMTAにエラーメールが大量に送られ，このエラーメールに対するエラーの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．

MTAにおける発信者詐称SPAMメールへの対策として，当該詐称アドレス宛の電子メールの受信を拒否する方法が考えられる．しかし，この方法では詐称アドレスが実在する場合にはSPAMではない通常のメールの受信にも影響を与え，またSMTPコネクション確立後に受信するかどうかを決定するため，MTAの負荷がそれほど軽減されないことが予想される．また，別の方法として，1. で述べたMAPS RBLなどを用いてopen relayを許すMTAからのSMTPコネクションを拒否する方法が考えられる．この方法は図1のようにSPAMメールを発信するMTA(以下，SPAM発信MTAと呼ぶ) から直接送られるエラーメールに対しては有効である．しかし，図2のようにSPAMメールの発信に用いられたものとは別のMTA(以下，SPAM中継MTAと呼ぶ) からエラーメールが返される場合も多く，このようなエラーメールの受信を拒否することができない．また，この方法ではSMTPコネクションの確立後に送信側のMTAがopen relayを許すかどうかをDNSを用いて調査するため，受信側のMTA

[1] このようなCD-ROMの販売を目的としたSPAMメールが実際に流通している．

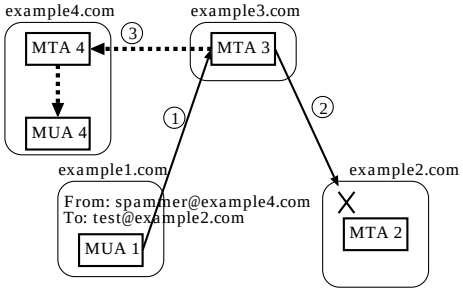

図 1: SPAM によるエラーメールの発生 (その 1)

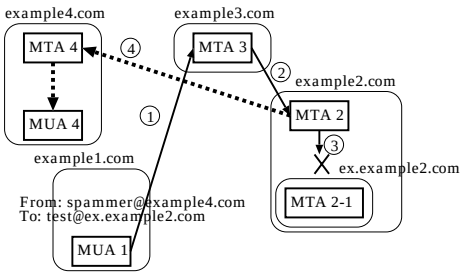

図 2: SPAM によるエラーメールの発生 (その 2)

の負荷がそれほど軽減されないことが予想される．

以上のように，上記の対策方法はいずれも MTA の負荷を軽減することは困難で，通常の電子メール配送処理に影響を与える可能性が高い．そこで，以下では MTA の負荷を軽減しながらエラーメールの処理を行う手法について考える．

3 発信者詐称 SPAM への対処

3.1 基本原理

前節で述べたように，詐称アドレスに対応する MTA では短期間に大量のエラーメールを受け取るため，MTA が過負荷となり通常のメール配送に影響を及ぼす可能性がある．このとき，MTA が 1 台しかないと，どんな方法を用いたとしても全ての処理がこの MTA に集中するため，過負荷は避けられない．

そこで，本稿では図 3 のように従来用いてきた MTA(プライマリ MTA) 以外にもう 1 台 MTA(セカンダリ MTA) を用意し，エラーメールの処理を主としてセカンダリ MTA で処理する手法を提案する．このとき，どのようにエラーメールだけをセカンダリ MTA に振り向けるかが問題となる．本手法では，ルータでのフィルタリングや DNS での MX レコードの更新によりこれを行う．

以下では，具体的な対処手法について説明する．

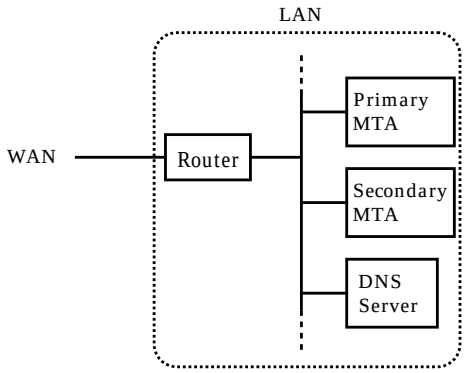

図 3: システム構成

3.2 SPAM 発信 MTA からのエラーメールの対処

2. で述べたように，エラーメールのうちの多くは SPAM 発信 MTA から直接発信される．このエラー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 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ルータで設定すればよい．これにより，図 4 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 にエラー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で拒否されるため，セカンダリ MX であるセカンダリ MTA にエラーメールを送信するようになる．

なお，SPAM 発信 MTA の IP アドレスは MTA のログから容易に取得することが可能である．

3.3 SPAM 中継 MTA からのエラーメールの対処

一般に，エラーメールを発信する SPAM 中継 MTA は数が多く，また 1 台あたりのエラーメール数は少ないことが予想される．従って，上記のようにルータでフィルタリングを行おうとすると，各 SPAM 中継 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の性能低

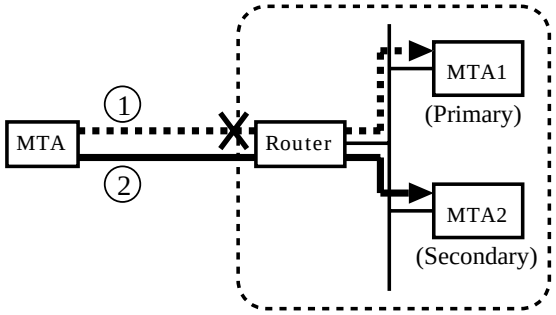

図 4: ルータで転送拒否される場合

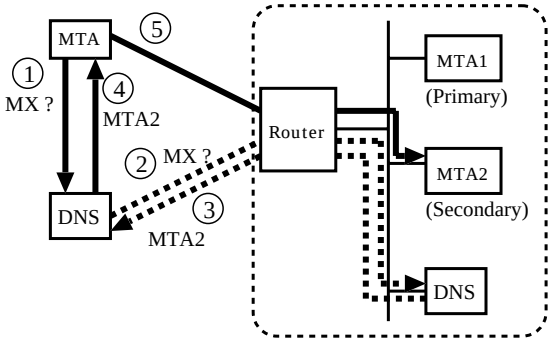

図 5: DNS にキャッシュが残っていない場合の転送例

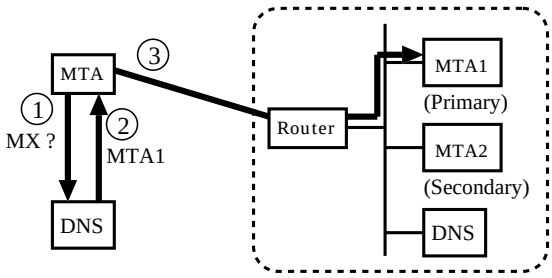

図 6: DNS にキャッシュが残っている場合の転送例

下を招くにもかかわらず，一度エラー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エラー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．

一方，このような SPAM 中継 MTA の多くは，詐称アドレスの属する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，エラーメールの送信の際に初めて DNS サーバに当該ドメインの MX レコードを問い合わせると思われる．そこで，我々はこの点に着目し，エラー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，プライマリ MX としてセカンダリ MTA を，セカンダリ MX としてプライマリ MTA を登録するようにする．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．これらの手法により，設定変更後に新たに MX レコードを問い合わせた SPAM 中継 MTA は図 5 に示すようにエラーメールをセカンダリ MTA に送信する一方で，従来から頻繁に電子メールを交換している MTA は図 6 に示すようにキャッシュされたプライマリ MX レコードに基づきプライマリ MTA に電子メールを送信するため，MTA の負荷分散を図ることができると思われる．

3.4 エラーメールの処理

次に受信したエラーメールの処理について述べる．

エラーメールが送信されてきた場合，これを受信して保存することはあまり意味がなく，計算機資源やネットワーク資源の浪費につながる．このため，エラーメール処理では早い段階でエラーメールを判別し，受信を拒否したり内容を破棄したりすべきである．但し，このとき同じ宛先に対して SPAM メールに対する苦情の電子メール (以下，苦情メールと呼ぶ) や通常の電子メール (以下，通常メールと呼ぶ) が届く可能性があるため，これらをエラーメールと区別して処理する必要がある．そこで，本手法では，発信者アドレスとして偽造されたアドレス宛に届いた電子メールを以下のような 3 段階の手順で処理する．

(1) Envelope-From が MAILER-DAEMON などエラーメール特有のアドレスで，かつ Envelope-To が SPAM の偽造されたアドレスあれば，本文を受け取る前に受信を拒否する．

(2) そうでなければ，送られたメールを一旦受け取り，ヘッダを調べる．ヘッダ中の From がエラーメール特有のアドレスであれば，その旨を記録し，メッセージを破棄する．

(3) そうでなければ，苦情メールあるいは通常メールと見なして通常の配送処理を行う．

以上の処理により，エラーメールに関する通信量を最小限に抑えることができ，MTA の負荷やディスクの使用量を軽減することが可能となる．なお，

(3) の処理において例えばSPAMメールがメッセージ中に引用されているかどうかを調べることにより苦情メールか通常メールかを区別し，苦情メールの場合には自動的に返信するような処理も可能である．

3.5 SPAM対策の開始・終了

本手法の効果を十分に発揮するには，エラーメールを大量に受け取る前に上記の対処を開始することが望ましい．これには，SPAMメールの兆候をどのようにして早期に検出できるかが問題となる．本手法の開発に際し，我々は以下のような場合にSPAMメールの兆候と見なすことを検討した．

(1) プライマリMTAにおいて特定のアドレス宛のエラーメールを特定のMTAから短時間に複数回受け取った場合．

(2) DNS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複数回あった場合．

このうち，(1) はSPAM発信MTAからのエラーメールを検出するもので，比較的確実にSPAMの兆候を検出することができる．また，ルータでのフィルタリングの対象となるMTAを特定することも可能である．一方，(2) はSPAM中継MTAからのエラーメールを検出するものであるが，DNSへの問合せは必ずしもエラーメールの送付を意味するとは限らないため，偶然にDNSへの問合せが集中して誤ってSPAMメールへの対処を開始する可能性がある．しかし，もし誤判断であっても通常はプライマリMTAだけで行うメール処理をセカンダリMTAを含めた2台のMTAで行うだけであり，何ら不都合は生じない．また，(1)，(2) ともにSPAMメールの兆候と判断する基準については，実際の運用状況に応じて調整する必要があるが，上記と同様の理由により，誤判断が増えても確実に検出できるようにすべきである．

SPAMメールの対策の終了は，詐称アドレスに対するエラー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からエラー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の両方においてエラーメールの検出を行うべきである．しかし，セカンダリMTAで受信するエラーメールの方が多いと予想され，またプライマリMTAだけでエラー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．

3.6 全体の対策手順

前節までに述べた内容をまとめると，本手法は以下のような手順で行われる．なお，一度に複数の詐称アドレスに対する対処が必要になる場合があることに留意する．

(1) 初期状態として，DNSサーバにおいてプライマリMXとしてプライマリMTAを，セカンダリMXとしてセカンダリMTAを登録しておく．このとき，これらのレコードのTTLを長く設定しておく．

(2) プライマリMTAにおいて受信ログを監視し，3.5節で示した条件を満たすエラーメールを短時間に複数回受信したかどうか調べる．また，DNSサーバにおいて問合せログを監視し，3.5節で示した条件を満たす問合せを短時間に複数回受けたかどうか調べる．もし，いずれかにおいてSPAMメールの兆候が検出されれば，次に進む．

(3) DNSサーバにおいて，プライマリMXとしてセカンダリMTAを，セカンダリMXとしてプライマリMTAを登録する．このとき，これらのレコードのTTLを短く設定する．

(4) プライマリMTAにおいてSPAMメールの兆候を検出した場合には，エラーメールの発信元とプライマリMTAとの間のSMTPコネクションを拒否するようにルータにおいてフィルタを設定する．プライマリMTA，セカンダリMTAとも詐称アドレスに関して3.4節で述べた処理を行うように設定を行う．

(5) プライマリMTAにおいて引き続き受信ログを監視し，3.5節で示した条件を満たすエラーメールを短時間に複数回受信したかどうか調べる．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においても受信ログを監視し，ルータのフィルタリングの対象となっている詐称アドレスへのエラーメールを一定期間受信しなければ，次に進む．

(6) プライマリ MTA，セカンダリ MTA において当該詐称アドレス宛のエラーメールの処理を解除する．また，ルータにおいて当該詐称アドレスに関連する MTA に対するフィルタ設定を解除する．但し，この解除は同一の MTA から別の詐称アドレスに対してエラーメールを送信していない場合に限る．もし，全てのフィルタ設定を解除した場合には次に進む．そうでなければ，(5) に進む．

(7) DNS サーバにおいて設定を初期状態に戻し，(2) に進む．

4 まとめ

本稿では発信者詐称 SPAM メールに起因する大量のエラーメールを通常の電子メールの配送にできるだけ影響を与えないで処理を行う手法を提案した．本手法では従来の MTA とは別に MTA を用意してエラーメールの多くをこの MTA で処理することにより従来の MTA の負荷を軽減する効果が期待できる．

本稿の執筆時点では，我々は前節で述べた発信者詐称 SPAM メールへの対処手法を実装したプロトタイプシステムを構築中である．本システムでは，MTA として sendmail 8.9.3[6], DNS としては BIND 8.2.3[7]，ルータとしては Cisco 1605R(IOS 11.2) を用いている．また，MTA や DNS におけるログの監視には perl で書かれたスクリプトを用い，ルータの設定変更には expect[8] を利用する予定である．

本手法では DNS における TTL の値や SPAM 対策の開始・終了における判断基準など，多くのパラメータがあり，これらは実際の運用環境に応じて決定する必要がある．しかし，本システムは SPAM 発信 MTA，SPAM 中継 MTA のそれぞれから送られるエラーメールの分布や送信タイミング，SPAM 中継 MTA における DNS キャッシュの状態など不明な点が多く，実際に発信者詐称 SPAM メールの被害に遭わない限り，これらのパラメータを調整したり，有効性を検証したりすることが困難である．そこで，プロトタイプシステム完成後にこれを公開し，他の組織の協力を得てシステムの完成度を高めていきたい．

参考文献

[1] 山井成良，大隅淑弘，林伸彦，宮下卓也，岡本卓爾: “岡山大学における電子メールのセキュリティ対策”，学術情報処理研究，No.4，pp.79–83，平成 12 年 10 月．

[2] Mail Abuse Prevention System LLC: “MAPS Realtime Blackhole List”, `http://mail-abuse.org/rbl/`, 2000.

[3] John Gardiner Myers: “SMTP Service Extension for Authentication”, RFC 2554, IETF, 1999.

[4] 石橋勇人，山井成良，安倍広多，大西克実，松浦敏雄：“メールクライアントに修正を要しない発信者詐称防止方式”，情報処理学会論文誌，Vol.41，No.11，pp.3133–3141，平成 12 年 11 月．

[5] 中西透，山井成良，安倍広多，石橋勇人，松浦敏雄，岡本卓爾：“IDENT 代理サーバによるリモートアクセスユーザ認証機構”，情報処理学会論文誌，Vol.41，No.10，pp.2907–2915，平成 12 年 10 月．

[6] Sendmail, Inc.: “Sendmail Home Page”, `http://www.sendmail.org/`.

[7] Internet Software Consortium: “Internet Software Consortium – BIND”, `http://www.isc.org/products/BIND/`, 2000.

[8] Libes, Don: *Exploring Expect*, O’Reilly & Associates, Inc. (1994)