LL-002

発信者詐称spamメールに起因するエラーメール集中への対策手法

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

山井 成良 †
Nariyoshi Yamai†

繁田 展史 ‡
Nobufumi Shigeta‡

岡山 聖彦 †
Kiyohiko Okayama†

宮下 卓也 †
Takuya Miyashita†

丸山 伸 §
Shin Maruyama§

中村 素典 §
Motonori Nakamura§

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，広告等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，発生頻度は少ないが，その被害は甚大である．例えば，平成14年11月に国内のプロバイダで発生した事例では，30万通以上のspam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．このように発信者詐称spamメールは運用上極めて深刻な問題が生じるにもかかわらず，他組織の利用者が発信者アドレスを詐称してspamメールを発信すること自体を防止することは事実上不可能であり，その対策は難しい．

これに対して，我々は (4) の被害に対する対策として，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した [1]．しかし，この提案手法は基本的な対策方針を示したのみで，現実の電子メール環境に即した具体的な設計や実装は行われていない．そこで本稿では，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について，主にその設計及び実装方法を述べる．

†岡山大学, Okayama University
‡三菱電機コントロールソフトウェア（株）,
Mitsubishi Electric Control Software Corporation
§京都大学, Kyoto University

2. 発信者詐称spamメールの問題点

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．

この問題は，後述するようにspamメールの発信者とは無関係なMTAがエラーメールの配送に関係しており，同じMTAとの間で通常メールもやり取りされる可能性があるため，他のサービスにおける攻撃対策手法をそのまま利用することは困難である．たとえば，帯域制限やフィルタリングの手法は，MTAを過負荷から保護することはできるものの，通常メールの配送にも大きく影響を与えるため，適切でない．また，MTAを増設して負荷分散を行う手法はある程度の効果は見込まれるが，短時間に数十万通ものエラーメールが到着する状況では，通常メールの配送遅延が生じるのは避けられない．

3. エラーメール集中への対策手法の概要

前節で述べた問題を軽減するためには，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，通常のメールは極力プライマリMTAで受信し，エラーメールは極力セカンダリMTAで受信する方法が有効であると思われる．この方法では，2種類のメールの振分け方法が重要である．そこで，まずエラーメールの配送経路について考察する．

3.1 エラーメールの配送経路

spamメールおよびこれに起因するエラーメールの典型的な配送経路を図1，図2に示す．

まず，spam発信者は不正中継を許すMTA(spam配送MTA) を利用してspamメールの発信を行う．spam配送MTAはspamメールを受け取るとその配送を試みるが，その過程でドメイン名が無効であったり，ユーザ名

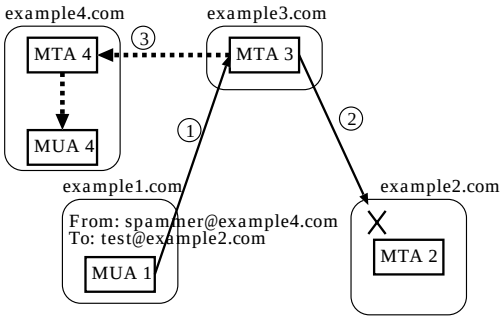

図 1: spam によるエラーメールの発生 (その 1)

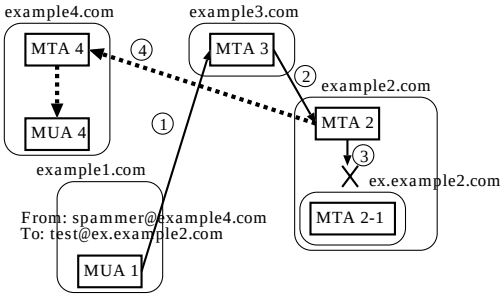

図 2: spam によるエラーメールの発生 (その 2)

が無効であったりした場合には，エラーメールが spam 配送 MTA から直ちに詐称アドレスに返送される (図 1).

一方，最近では，中継用 MTA で一旦外部からのメールを受信して，たとえば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(以下では末端 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，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メールを一旦受け取ってしまい，それを末端 MTA に配送する時点で宛先アドレスが無効であることが判明するため，エラーメールは中継用 MTA から詐称アドレスに返送される (図 2).

以上のことから，エラーメールは配送経路により 2 種類に分類できることがわかる．ひとつは図 1 のように spam 配送 MTA から直接返送されるものであり，もうひとつは図 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，前者を直接配送エラーメール，後者を中継配送エラーメールと呼ぶことにする．

3.2 直接配送エラーメールへの対策

前節で述べたように，エラーメールのうちの多くは spam 配送 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 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ルータで設定すればよい．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．

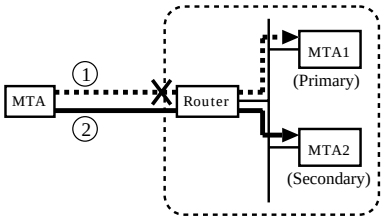

図 3: ルータでのフィルタリング

3.3 中継配送エラーメールへの対策

一般に，エラー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の性能低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，このような中継用 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 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．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中継用 MTA は図 4 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 5 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．なお，この方法では，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予め設定しておく必要があることに注意する．

3.4 対策の開始と終了

本手法の効果を十分に発揮するには，エラー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 から短時間に多数受け取った場合.

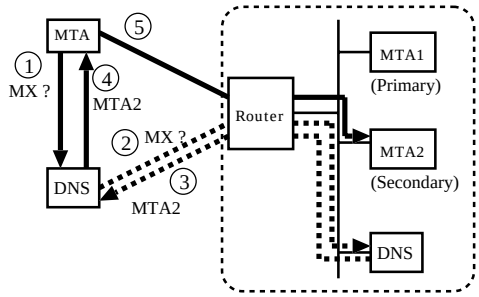

図 4: DNS にキャッシュが残っていない場合の転送例

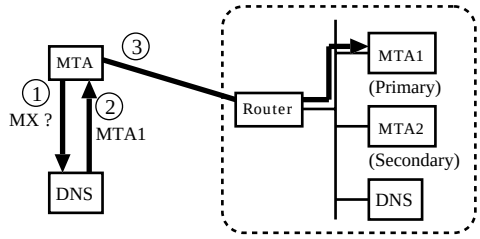

図 5: DNS にキャッシュが残っている場合の転送例

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 [2].

一方, 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.

4. エラーメール集中対策システムの設計

本節では前節で述べた方針に基づいて設計したエラー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 レコードの問合せ回数については, 対策の開始基準となる回数 (全体基準回数と呼ぶ) とは別にプライマリ DNS サーバに通報する回数 (単独基準回数と呼ぶ) を設けるようにした. すなわち, いずれか

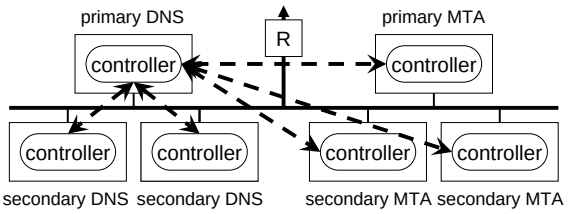

図 6: システム構成

1 つの DNS サーバが全体基準回数を超える問合せを受けた場合, ならびに複数の DNS サーバから単独基準回数を超える問合せを受け, 合計で全体基準回数を超える問合せを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, 全てのセカンダリ MTA から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 サーバから他の全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 MX レコードの問合せを基準時間内に単独基準回数以上, あるいは全体基準回数以上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エラーメールを受信したかどうか調べる. もし, いずれかにおいてエラーメール集中の兆候が検出されれば, プライマリ DNS サーバにエラーメール集中検出を通知し, 次に進む.

(3) プライマリ DNS サーバではエラー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.

(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, 全てのセカンダリ 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 において詐称アドレスを検出した場合，その詐称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 サーバでは全ての MTA に詐称アドレスを通知する．各 MTA では，詐称アドレス宛のエラーメールを拒否するように設定変更する．

(5) プライマリ MTA では引続きログを監視し，3.4 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．

- 詐称アドレス宛のエラーメールが受信されない場合はプライマリ DNS サーバにその詐称アドレスの解除通知を送信する．プライマリ DNS サーバでは全てのセカンダリ MTA から詐称アドレスの解除通知を受信すると，その詐称アドレスの解除通知を全 MTA に送信する．各 MTA ではその詐称アドレス宛のエラーメールの拒否設定を解除する．
- spam 配送 MTA からエラー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 サーバでは全てのセカンダリ MTA から同一の解除通知を受けると，ルータのフィルタリングを解除すると同時に，全てのセカンダリ 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 を監視対象から外す．
- 監視対象となるエラー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 spam 対策終了通知を送信する．プライマリ DNS サーバでは，全てのセカンダリ MTA から spam 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. 試作システムの実装と動作確認

5.1 試作システムの実装

前節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 サーバの他にセカンダリ 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．試作システムではルータは用いていないが，その代わりにプライマリ MTA において FreeBSD が持つ IP firewall 機能を用いている．

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ている．また，プライマリ DNS サーバにおける MX レコードの更新を直ちにセカンダリ 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，外部から各 DNS サーバに MX レコードの問合せを何回か行い，正しく動作するかどうか実験を行った．その際，全体基準回数は 10 分間で 4 回，単独基準回数は 10 分間で 2 回と設定した．実験の結果，いずれかの DNS サーバで全体基準回数を超えた場合および 2 つ以上の DNS サーバで単独基準回数を超え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．

次に，エラーメールを 1 つの MTA から多数発生させ，正しくエラーメールを拒否できるか実験を行った．その際，対策開始の基準としては各 MTA で 10 分間に 10 通以上のエラーメールを同一 MTA から受信した場合とした．実験の結果，エラーメール 1000 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 通のエラーメールを受信するに留まり，残りのエラーメールは全て受信拒否されていることを確認した．

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 分以上エラー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，最後のエラー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通りに動作するといえる．

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エラーメールが通常メールの配送に与える影響を軽減する手法について，その設計及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挙げられる．

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．

参考文献

[1] 山井成良，山外芳伸，宮下卓也，大隅淑弘: “発信者詐称 SPAM メールに対する対策手法”，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，2001-DSM-22-9，pp.51–56，平成 13 年 7 月．

[2] 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，平成 14 年 3 月．