電子メール優先配送における信頼できるMTAからのspamメール処理

山井 成良[1,a)]　ガーダ[2]　松岡 政之[2]　須藤 亨[3]　岡山 聖彦[1]　河野 圭太[1]　中村 素典[4]

概要：
重要な電子メールを遅滞なく配送できるようにするため，信頼できる送信 MTA から送られる電子メールを専用の受信 MTA で受信し，簡単なチェックのみを行うことで大量の spam メールによる輻輳や spam メールの検査に要するオーバヘッドによる遅延を軽減する，電子メール優先配送システムが提案されている．しかし，従来のシステムでは信頼できる送信 MTA から spam メールが送られてきた場合も簡単なチェックしか行えないという問題があった．そこで本稿では信頼できる送信 MTA から送られてきたメールであっても spam メールと疑われる場合には一時エラーや強制切断により一般用の受信 MTA へ再送させ，十分な検査を行う方法を提案する．

キーワード：
電子メール，迷惑メール対策，優先配送

Processing of Spam Mail Sent by Trusted MTAs on E-mail Priority Delivery System

Nariyoshi Yamai[1,a)]　Gada[2]　Masayuki Matsuoka[2]　Toru Sudo[3]　Kiyohiko Okayama[1]
Keita Kawano[1]　Motonori Nakamura[4]

Abstract:
Many email priority delivery systems, where a dedicated receiving MTA receives all messages sent from trusted sending MTAs and performs only simple anti-spam measures, have been proposed so far to reduce delivery delay due to heavy spam traffic and large overhead of anti-spam measures. However, existing systems have some problems such that the dedicated receiving MTA easily receives even spam mails sent from trusted sending MTAs only through simple anti-spam measures. In this paper, we propose a method to perform full anti-spam measures on suspicious messages sent from trusted sending MTAs, by introducing tempfailing and SMTP session abort on the dedicated receiving MTA.

Keywords: E-mail, anti-spam method, priority delivery

1. はじめに

電子メールはインターネットで最も普及しているコミュニケーション手段であり，多くの人により様々な目的に利用されている．従来の電子メールサーバの運用では，送信者から受信者へ確実に配送することが最大の目標であっ

[1] 岡山大学情報統括センター
Center for Information Technology and Management, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[2] 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[3] 岡山大学工学部
Faculty of Engineering, Okayama University
3-1-1, Tsushima-naka, Kita, Okayama 700–8530, Japan
[4] 国立情報学研究所
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda, Tokyo 101–8430, Japan
[a)] yamai@okayama-u.ac.jp

たが，現在では電子メールを遅滞無く受信者へ配送することも求められている．一方，最近蔓延している spam メールへの対策として，多くの組織では greylisting[1]，greet pause[2]，フィルタリングなどの様々な対策を適用している．しかし，これらの対策により，たとえば負荷の高い処理を行う必要がある，大きな遅延が発生する，あるいは重要なメールが迷惑メールと誤判定されるなど，通常のメール配送に支障が生じる状態が発生している [3]．

重要な電子メールを遅滞無く受信者へ配送する手段として，信頼できる送信 MTA をあらかじめホワイトリストに登録し，優先的に配送する仕組み（優先配送システム）がしばしば採用されている．その実装例として，我々はレイヤ 3 スイッチのポリシールーティング機能を用いて小規模なホワイトリストを実現し，その小規模なホワイトリストに登録する送信 MTA を動的に変更することにより，信頼できる送信 MTA の数が増加した場合でも伝送速度の劣化を抑制できる優先配送システムを提案し，その有効性を確認した [4], [5]．

従来の優先配送システムでは，信頼できる送信 MTA から送られてきた電子メールは全て正当なメールであるとみなし，無条件であるいは比較的簡単な検査を経て受信するように構成されているものが多い．ところが実際には，信頼できる送信 MTA から送られてきた電子メールであっても，ウイルス感染端末からの発信，パスワード漏洩による発信，あるいは転送設定などにより，spam メールが混在する可能性があり，簡単な検査だけで受信すると危険が生じる場合もあり得る．

そこで，本稿では我々が提案したシステムにおいて，信頼できる MTA から送られてきたメールにまず簡単な検査を行い，その結果 spam メールと疑われるメールに対して，あまり導入コストを増やすことなく本来行うべき検査を行う方法を提案する．

2. 電子メール優先配送システムと問題点

2.1 対象とする電子メール優先配送システム

本稿で想定する電子メール優先配送システムは**図 1** に示すように L3 スイッチ，優先受信 MTA，一般受信 MTA，およびコントローラから構成される．このうち，優先受信 MTA，一般受信 MTA は個別の IP アドレスとは別に共通の仮想 IP アドレスを持つ．共通の IP アドレスはメール配送に用いられ，個別の IP アドレスは L3 スイッチでパケットの中継先を指定する際に用いられる．L3 スイッチはポリシールーティング（PBR）機能を持ち，自身の持つホワイトリストに基づいてパケットの中継先を決定する．また，ホワイトリストに含まれない送信 MTA からの SYN パケットなど，ホワイトリストの更新判断に必要なパケットはコントローラに中継する．コントローラは大規模なホワイトリストを持ち，送信 MTA が優先配送の対象かどうかを判定する機能を持つ，また L3 スイッチとの間で制御用コネクションを常時確立し，L3 スイッチ内のホワイトリストに登録される送信元メールサーバを動的に変更する．

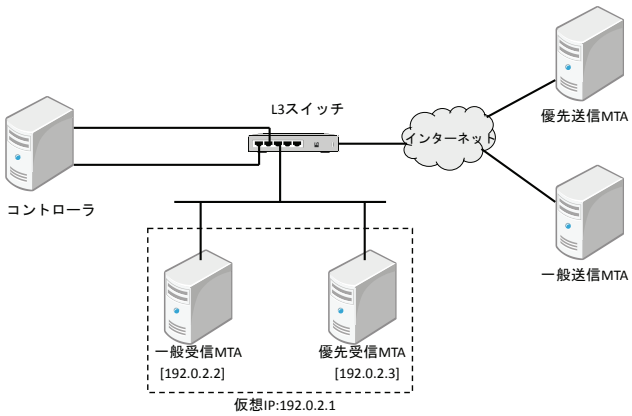

図 1 電子メール優先配送システムの構成
Fig. 1 Components of the email priority delivery system.

以下では，一般受信 MTA では greylisting，greet pause，フィルタリングなど，遅延や負荷が比較的大きい spam 対策処理 [*1] を行い，また spam 対策アプライアンス製品の導入など金銭的な運用コストが比較的高いセキュリティ対策を採用しているのに対し，優先受信 MTA では比較的簡単な spam 対策しか行っていない場合を想定する．

2.2 対象システムの問題点

前節で述べたシステムでは，信頼できる送信 MTA から送られた電子メールは必ず優先受信 MTA で処理されることになる．したがって，その電子メールの中に spam メールが含まれた場合，優先受信 MTA 上での比較的簡単な対策しか行われないため，そのまま受信者に届くことになる．

これに対して，優先受信 MTA でも一般受信 MTA と同様の spam 対策を行う方法が考えられる．しかしこの方法では，信頼できる送信 MTA から送られる電子メールの量が増加すると優先受信 MTA の負荷が増大し，優先配送すべき spam メール以外の電子メールについても配送遅延が生じることが予想される．また，たとえば一般受信 MTA に spam 対策アプライアンス製品を導入している場合，優先受信 MTA にも同じ製品を導入すると金銭的な運用コストが増加するという問題も生じる．

別の方法として，優先受信 MTA で信頼できる送信 MTA から送られた電子メールを受信した後，比較的簡単なチェックを行い，spam メールの疑いがある場合にはこれを一般受信 MTA に転送する方法が考えられる．この方法であれば優先受信 MTA では spam 対策を新たに行う必要がなくなり，金銭的な運用コストの増加を招かない．しかし，この方法でも特に信頼できる送信 MTA からサイズの大きい

[*1] 以下では特に断りのない限り spam 対策はウイルス対策を含むものとする．

電子メールが多数送られてきた場合，優先受信 MTA の負荷が増加する問題は解消できない．

3. 優先受信 MTA での spam メール処理

3.1 提案方法の概要

前章で述べたように，優先受信 MTA で一般受信 MTA と同様の spam 対策を行う方法，優先受信 MTA で信頼できる送信 MTA から送られた電子メールを受信した後に疑わしい電子メールを一般受信 MTA に転送する方法は金銭的な運用コストの増加を招いたり，優先受信 MTA の負荷を軽減できなかったりする点で問題がある．そこで，本稿では受信中にエンベロープ，ヘッダ，本文などをチェックし，疑わしいと判断した段階で一時エラーを返したり，SMTP コネクションを強制切断 [6] したりする方法を提案する．この方法ではセカンダリ MX として一般受信 MTA を指定しておき，優先受信 MTA が一時エラーを返したり強制切断したりした後に信頼できる送信 MTA がセカンダリ MX である一般受信 MTA に直ちに再送するようにする．これにより，優先受信 MTA の負荷をあまり増加させることなく早い段階で一般受信 MTA で spam メール対策を行うことが可能になる．

3.2 優先受信 MTA での spam メール判定

提案方法を実現する上で，spam メールの疑いがあるかどうかをどのような基準で判定するかが重要となる．提案方法では信頼できる送信 MTA に応じて評価基準が異なる場合を想定している．たとえば，ac.jp ドメインに属する送信 MTA を全て信頼できる送信 MTA と見なす運用が考えられるが，この運用において spam チェックを行った後に送信する MTA から送信された電子メールは spam メールの可能性が低いため優先受信 MTA でそのまま受信しても構わないのに対し，そうでない送信 MTA から送信された電子メールは spam メールの可能性が比較的高く，早目に一般受信 MTA で厳密な spam チェックを行うべきである．そこで提案方法では送信 MTA に応じて spam チェックの評価基準を個別に設定できることを前提としている．

本方法における spam チェックは，(1) エンベロープ情報受信時，(2) ヘッダ受信時，(3) 本文受信時の各時点で行うことが可能である．以下では，各時点でどのような基準に基づいて spam チェックを行えるかを述べる．

3.2.1 エンベロープ情報受信時の判定基準

SMTP コネクション確立後，DATA コマンドが送られる前に優先受信 MTA が得られる情報には，送信元 IP アドレス，エンベロープ From アドレス，エンベロープ To アドレスなどがある．これらの情報を用いると，たとえばエンベロープ From アドレスと送信元 IP アドレスを SPF（Sender Polocy Framework）[7] を用いて照合することにより転送されたメールかどうかを判別し，転送されたメールであれば MAIL コマンドに対して一時エラーを返して一般受信 MTA への再送を送信 MTA に促すことができる．

3.2.2 ヘッダ受信時の判定基準

DATA コマンドの後，優先受信 MTA が最初に受信するヘッダからは多くの情報が得られる．これらを組み合わせれば様々な判定基準を設定可能である．たとえば，ヘッダ From アドレスと送信元 IP アドレスとの照合，Content-Type ヘッダによる添付ファイルの有無（multipart/mixed であれば有と判断）や記述言語（text/plain の場合，直後の charset の値で判断）のチェック，あるいは送信側での spam チェックの有無（X-Spam-Status，X-Virus-Scanned などのヘッダの有無，あるいはこれらの値で判断）などが考えられる．

3.2.3 本文受信時の判定基準

2.2 節で述べたように，もしメッセージ全体を受信した後に spam チェックを行うのであれば優先受信 MTA の負荷を軽減することにはならない．しかし，提案方法では SMTP コネクションを途中で強制切断する機能の利用を前提としているため，本文受信中の早い段階で判定を行うことできれば優先受信 MTA の負荷を軽減につながる．本文受信時の判定の例として，添付ファイルがあるメールであっても，そのファイルが S/MIME の署名（Content-Type が application/x-pkcs7-signature であるかどうかで判断）やテキストファイル（Content-Type が text/plain かどうかで判断）のような安全なものだけであればそのまま優先受信 MTA で受信し，それ以外の種類のファイルに関する Content-Type が見つかればその時点で強制切断する方法が考えられる．

3.3 一般受信 MTA での処理

提案方法では，信頼できる送信 MTA から見ると一般受信 MTA はセカンダリ MX であるが，一般受信 MTA 自身は当該ドメインのプライマリ MX であるため，信頼できる送信 MTA から送られた電子メールを受信し，spam チェックを行った後で宛先メールボックスにメッセージを書き込む．したがって，基本的には一般受信 MTA の設定は変更する必要がない．しかし，一般受信 MTA で greylisting のような再送を求める spam 対策（tempfailing）を採用している場合には以下に示す動作により，一般受信 MTA での処理が大幅に遅れることになる．

まず，信頼できる送信 MTA から優先受信 MTA への配送が一時エラーや強制切断により失敗した場合，信頼できる送信 MTA はセカンダリ MX である一般受信 MTA に直ちに再送する．しかし，この配送に対して一般受信 MTA が一時エラーを返した場合，信頼できる送信 MTA は配送可能な MTA がこれ以上見つからないため，一定期間（RFC5321[8] では 30 分以上を推奨）待ったあと，再び優先受信 MTA への配送を試みる．この配送が再び失敗し，

一般受信 MTA へ再送を行った段階で，初めてこの配送は成功する．したがって，この配送は少なくとも信頼できる送信 MTA での再送間隔だけ遅延することになり，また優先受信 MTA は同じ電子メールに対して 2 度のチェックを行うため，その負荷も増大する．

そこで，このような動作を防止するため，一般受信 MTA では信頼できる送信 MTA をホワイトリストに登録するか，あるいは優先受信 MTA から再送かどうかを判断するのに必要な情報を取得する必要が生じる．但し，これらの対策は複数の受信 MTA を用いた tempfailing では一般的であり，実装は比較的容易である．

4. まとめ

本稿では，優先配送システムにおいて信頼できる送信 MTA から送られてきた電子メールのうち spam メールの可能性が高いものを一般受信 MTA で処理する方法を提案した．この方法では，受信中にエンベロープ情報，ヘッダ，本文をチェックし，比較的早い段階で一時エラーや強制切断により一般受信 MTA への再送を促すため，電子メールを受け取ってから一般受信 MTA に転送する方法と比べて優先受信 MTA の負荷を軽減することが可能である．

現在，一般受信 MTA への再送を促すための判定基準を検討している段階であるが，これと並行して試作システムの設計を行っている．今後の課題として，この設計に基づいて実装を行い，提案方法の有効性を検証することが挙げられる．

謝辞 本研究の一部は平成 23〜25 年度科学研究費補助金 (基盤研究 (C)，課題番号 23500122) 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] Harris, E.: The Next Step in the Spam Control War: Greylisting (online), available from <http://projects.puremagic.com/greylisting/whitepaper.html> (accessed 2013-11-18).

[2] Allman, E., Assmann, C., and Neil Shapiro, G.: Sendmail Installation and Operation Guide (online), available from <http://www.sendmail.com/pdfs/open_source/installation_and_op_guide.pdf> (accessed 2013-11-18).

[3] 飯田隆義，松竹俊和，吉田和幸：“spam 対策用 whitelist を一元管理できるメールシステムとその運用について”，情報処理学会インターネットと運用技術研究会研究報告，Vol.2010-IOT-8，No.14，pp.1–6 (2010).

[4] ガーダ，諏訪秀治，山井成良，岡山聖彦，中村素典: “レイヤ 3 スイッチを用いた大規模なホワイトリストに対応可能な電子メール優先配送システム”，情報処理学会インターネットと運用技術研究会研究報告，Vol.2012-IOT-16，No.37，pp.1–6 (2012).

[5] ガーダ，山井成良，岡山聖彦，河野圭太，中村素典：“レイヤ 3 スイッチによる動的ホワイトリストを用いた電子メール優先配送システムの評価”，情報処理学会第 75 回全国大会講演論文集，5X-8，Vol.2013，No.3，pp.377–378，2013 年 3 月．

[6] 山井成良，岡山聖彦，中村素典，清家巧，漣一平，河野圭太，宮下卓也：“SMTP セッションの強制切断による spam メール対策”，情報処理学会論文誌，Vol.50，No.3，pp.940–949，2009 年 3 月．

[7] Wong, M., Schlitt, W.: Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, RFC4408, IETF, April 2006.

[8] Klensin, J.: Simple Mail Transfer Protocol, RFC5321, IETF, October 2008.