2004－DSM－32　(14)
2004／3／29

動的に応答が変化するネームサーバー技術のメール配送エージェントへの応用

丸山 伸[1]・中村 素典[1]・岡部 寿男[1]・山井 成良[2]
1. 京都大学情報学研究科・ 2. 岡山大学総合情報処理センター
marushin@net.ist.i.kyoto-u.ac.jp　motonori@media.kyoto-u.ac.jp
okabe@media.kyoto-u.ac.jp　yamai@cc.okayama-u.ac.jp

概　要

電子メールの普及が進み利用が一般的になるにつれて、メールを遅滞なく配送することは非常に重要視されている。しかしメール転送エージェント(MTA) の負荷が増大していたり、外部から MTA に対して著しく大量のメールが送信されたりした際には、メール配送に遅延が生じるだけでなく、MTA のサービスを安定して運用することすら困難である。
そこで本研究においては、メール配送の前に行われるドメインネームサービス(DNS)への問い合わせに着目し、その応答を平常時におけるメール送受信の頻度情報等を元にメールサーバを使い分けるよう動的に変化させることで、MTA の負荷を制御できることを示す。さらにメールの受信を開始する前に送信元を識別する技術が、重要と思われるメールの遅延を小さくするだけではなく、SPAM 対策への応用の可能性についても検討する。

A Dynamic Modification on DNS Response and its Application on Mail Transfer Agent

Shin Maruyama [1], Motonori Nakamura [1], Yasuo Okabe [1], Nariyoshi Yamai [2]
1. Graduate School of Informatics, Kyoto University
2. Computer Center, Okayama University
marushin@net.ist.i.kyoto-u.ac.jp　motonori@media.kyoto-u.ac.jp
okabe@media.kyoto-u.ac.jp　yamai@cc.okayama-u.ac.jp

Abstract

Delivering e-mails without unnecessary delay is one of a very important issue as the spread of e-mail service and its use become very common. But in case that “Mail Transfer Agent (MTA)” is heavily loaded and that huge amount of mails are sent to MTA, not only the delay on mail delivery is inevitable but also managing MTA services become difficult.
In this papar, we focus on the query to the “Domain Name Service (DNS)” which usually is done just before the mail transfer. Then we propose a method of modifying the response of DNS server based on the e-mail traffic in the normal condition, and show that this method will control the load of MTA. Moreover the delay of mails which seem to be important can be shortened by detecting the sender information before starting connections which may also be utilized for the purpose of anti-SPAM.

1．はじめに

電子メールは複数のメール配送エージェント(MTA)を経由しつつ送信者の下から受信者へと配送される。従来の MTA は途中でメールを失うことなく受信者の手元へと確実に配送することが必要かつ最大の目的であった。

しかしながら電子メールの普及が進み利用が一般的になるにつれて耐障害性・冗長性といったセキュリティに関わる要求が MTA に対しても求められるようになった。特に SPAM メールやコンピュータウィルスにより発信されるメールの蔓延は大きな問題となっており、これらに対して MTA においても対策をすることが求められている。

このうち SPAM メールによる影響は

(1) 不必要なメールを受信することによる計算機資源・ネットワーク資源、そしてメール受信者の時間を浪費してしまう

(2) 自組織の端末が SPAM メールの発信や中継に関与することで、SPAM メールの発信源としての評価を受けてしまう

(3) SPAM メールの発信元アドレスとして自組織のメールアドレスが指定されてしまった場合、配送に失敗したエラーメールが自組織に返送されてくることで MTA が過負荷となり、その他のメールの受信に大きな影響が出てしまう

といった問題がある。

また、メールを大量に配信することにより感染を拡大するコンピュータウィルスが流行していることも大きな問題となっている。

このうち(1)と(2)の問題に対しては、

- メールの不正な中継を行わないように適切に設定する
- 不正な中継を行うメールサーバからの受信を拒否する方法

等が広く利用されている。近年これらに加えて MTA において組織外や組織内から受信したメールを詳細に調査することが一般的となっているため、MTA の果たすべき役割が増大し、1 通のメールあたりの処理時間や負荷が増えている。

また、(3)の問題による攻撃の頻度は低いともいえるが、ひとたび発生すると数日間に渡り数万通のメールが配送されることも珍しくなく、その被害は甚大である。

この問題に対する対策としては山井[1]による手法が知られているが、本研究においては、より柔軟にかつ動的に応答が変化する DNS サーバを用いることによるさらなる拡張を提案する。

2．DNS を利用した負荷分散

複数のサーバを利用して負荷分散を行う際には、Layer4 スイッチといったネットワーク機器で行う手法だけでなく、ドメイン・ネーム・サービスを利用して行う手法が存在する。

ドメイン･ネーム･サービス(DNS)はインターネット上のホスト名と IP アドレスとの対応を与えるために通常は利用される。DNS サーバーは DNS クライアントからホスト名を含んだ問い合わせに対して、ホスト名に対応付けられた IP アドレスを返す。この際返送する情報の有効期間を示す TTL 情報も同時に返送する。

このホスト名と IP との対応付けを動的に変更する技術は DNS ラウンドロビン方式と呼ばれ、WWW サーバの冗長化とい

った例において広く利用されている。WWW サーバのようなアプリケーションにおいてクライアントとサーバとの対応付けに制約がない場合には、この対応付けは通常はランダムに行われる。DNS サーバとして広く用いられている実装である BIND[2]を利用せず独自のサーバを作成することで、サーバとクライアントの間でのネットワーク回線の速度といったポリシーに基づき、DNS 問い合わせに対する応答を変化させる試みは、Tenbin [3] [4], DNS Balance [5], DNS Trick [6] [7] 等、これまでにも多く行われている。しかしながらこれまでは MTA に対してポリシーに基づいた負荷分散を行う必要性が認識されていなかったことから、そのような研究はほとんど行われていない。

3 DNS と MTA との連携

通常のメールであるか SPAM であるかウィルスメールであるかに関わらず、メールにはあて先となるメールアドレスが存在する。そしてそのメールをどのメールサーバに配送するべきかを知るために DNS が利用される。すなわちメールアドレスのドメイン部分に対応付けられた MX レコードが問い合わせられ、DNS サーバは対応するサーバ名と有効期間(TTL)とを返送する。この MX レコードはこれまで一般にはメールサーバを複数設置して冗長化する際に利用されてきた。

3.1 MX 問い合わせへの応答ポリシー

本研究においては、メールの発信元が MX レコードの問い合わせを行った際の応答を変化させることで、そのメールの配送先を適切なポリシーに応じて変化させることを目標とする。まず、送信側が利用するメールサーバーとネームサーバーとを調査する必要がある。そして、受信側の状況を調査し、ネームサーバの応答を変化させることとなる。

4. 全体の動作手順

もし「発信者詐称 SPAM の返送メール」が引き起こすような著しく大量のメール配送が発生したときを例に、これまでに述べた一連の技術を利用してどのような対策を行うのかを手順に従い示す。

4.1 設置されるシステムの構成

想定されるシステムの全体構成図を図 1 に示す。この図は「メールサーバ A」にメールボックスを持つ受信者を例としている。

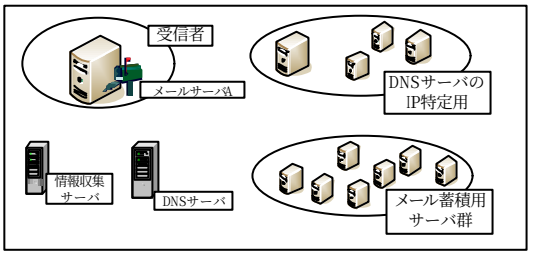

図 1: 想定されるシステム構成図

受信者のメールボックスを持つサーバ以外に「DNS サーバの IP 特定用のメールサーバ群」「一時的なメール蓄積用のサーバ群」とが必要となる。これらのサーバ群の台数は任意であるが、台数が多いほうが効率が良い。また動的に応答を変化させる DNS サーバと、クライアントの利用する DNS

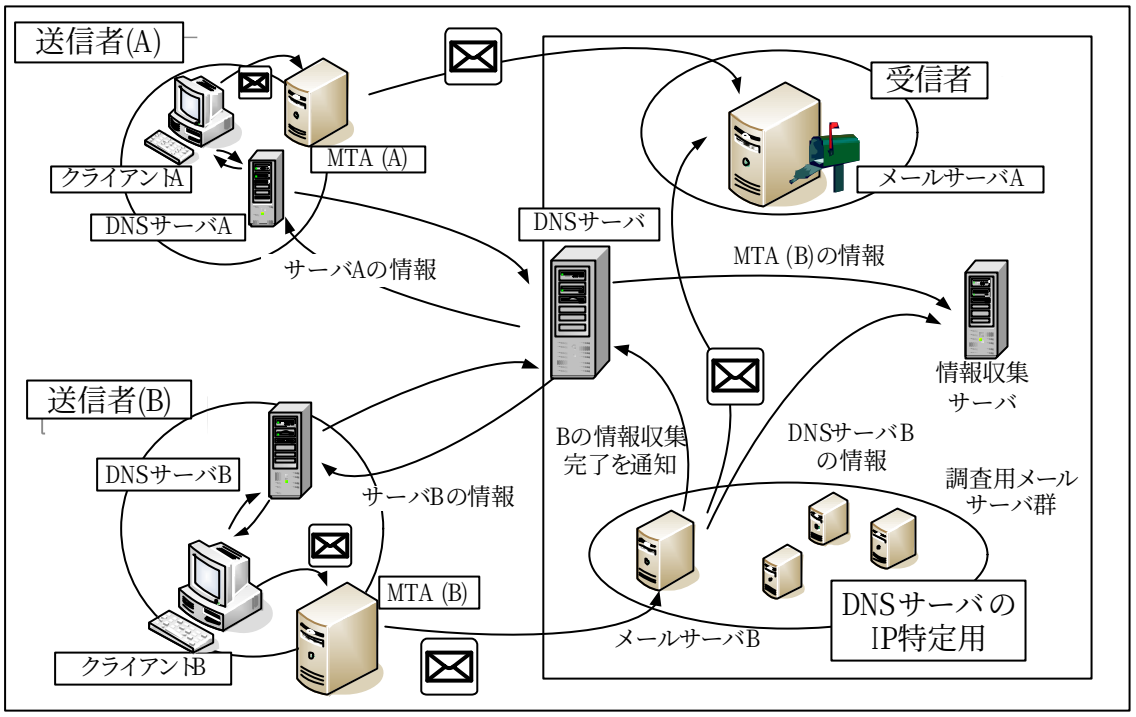

図 2　DNS サーバーの応答を操作することで、クライアントの MTA と DNS との対応付けを収集するシステム

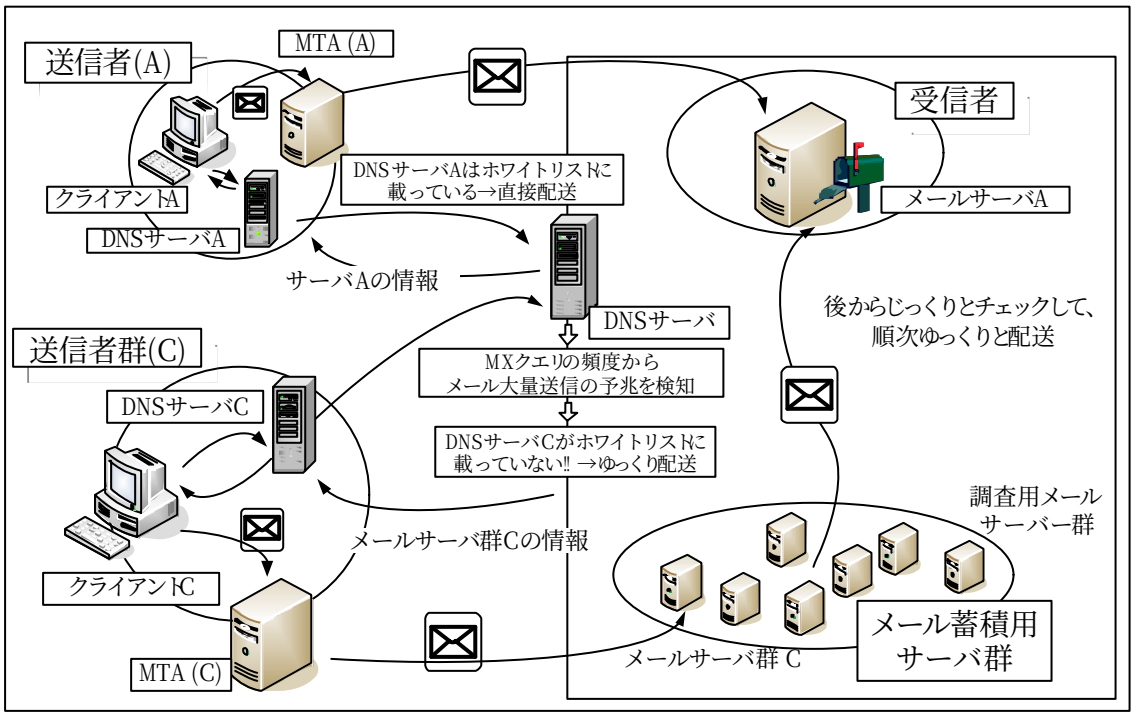

図 3 MTA の高負荷時に、DNS 問い合わせ元アドレスによっては、メールを遅延させて配送をすることで MTA のピーク負荷を下げるシステムの例

サーバ情報を収集するための情報収集サーバが存在する。

4.2 平常時に準備するべき内容

4.2.1 平常時の負荷を測定

平常時におけるメールサーバの負荷はサイト毎に大きく異なる。

まず、平常時におけるメールの送信元が利用している DNS サーバの一覧を作る作業を行う。そのために DNS サーバは次のような挙動をする。

1. DNS サーバが MX レコードの問い合わせを受けたときには、情報収集サーバに問い合わせて調査用メールサーバ群の中から空きサーバの割り当てを受ける。（ここではメールサーバ B が空いていたとする）
2. DNS サーバは比較的短い TTL をつけてメールサーバ B の情報を応答する。同時にメールサーバ B を DNS サーバ B に割り当てたことを情報収集サーバに登録する。
3. メールサーバ B はメールを受信した際に、MTA(B)の情報を情報収集サーバーに通知する。
4. 情報収集サーバは DNS サーバ B と MTA(B)の関連付けを記録した上で、TTL で指定された時間が経過した時にメールサーバ B の割り当てを解除する。

この一連の作業を繰り返すことにより DNS サーバとそれを利用する MTA との関連付けを収集することができる。この関連付けのことを以降「MX 情報問い合わせ元のホワイトリスト」と呼ぶ。

4.2 著しく大量のメール送信の検知

SPAM やウィルス、そして発信者詐称 SPAM のバウンス等により、外部から著しく大量のメールが一斉に配送されてくることがある。このような事態において DNS の応答を動的に変化させることでサーバの負荷が増大することを避けるための手順を図 3 及び以下に示す。

1. DNS サーバは MX 情報の問い合わせの頻度を常時監視し、問い合わせ回数の異常な増加を検知した際には「高負荷対応モード」に切り替える。
2. 「高負荷対応モード」においては、DNS サーバは MX 情報の問い合わせ元が、「MX 情報問い合わせ元のホワイトリスト」に含まれているかどうかを調べ、含まれている場合にはメールサーバ A の情報を応答し、含まれていない場合にはメールサーバ群 C の情報を回答する。この際の TTL は小さい値にする。
3. メールサーバ群 C の負荷が著しく高い場合には、「MX 情報問い合わせ元のホワイトリスト」に含まれていないところからの問い合わせに対して、存在しないサーバの情報を返すことも検討できる。

4.3 その他の利用法の提案

動的に応答を変化させる手法はこれまでに述べた応用例以外にも利用できる。
ある 1 つの MX レコードの問い合わせに対して著しく大量のメール配送が行われた際、それ以降同じ DNS サーバからの問い合わせがあった場合にはそれ以降に大量のメールが送信される可能性を予想し、事前に何らかの対処を行えるものと考えられる。

5. 考察

本研究においては、MX レコードの問い合わせに対して応答を動的に変更させることで、MTA への負荷を制御するシステムについて検討した。現在のところプロトタイプの実装における動作確認を行うにとどまっており、このシステムが目標とする負荷がかかった状態での検証ができていない。早急に実装を行い実証試験を行いたい。

6. 謝辞

本研究により提案されたシステムのプロトタイプ作成には tenbin を拡張して利用させていただいた。また、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) 及び、平成 15 年度「21 世紀 COE プログラム『知識社会基盤構築のための情報学拠点形成』」研究拠点形成費補助金による若手研究者研究活動経費の補助を受けている.

7. 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,

[2] Internet Software Consortium: “Internet Software Consortium – BIND”, http://www.isc.org/product/BIND/.

[3] 下川俊彦，吉田紀彦，牛島和夫，``ネームサーバを用いた柔軟な負荷分散''，インターネットコンファレンス '99，107-116

[4] T. Shimokawa, N. Yoshida, and K. Ushijima, DNS-based Mechanism for Policy-added Server Selection, SSGRR2000, 2000.

[5] 横田裕思，DNS Balance, http://openlab.ring.gr.jp/dns balance/dns balance.html.

[6] 横田裕思，DNS Trick, http://openlab.ring.gr.jp/dns balance/dns trick.html.

[7] 横田裕思，木村成伴，海老原義彦，DNS フィルタ方式によるミラーサーバ選択法の提案と実装，インターネットコンファレンス 2001 論文集, pp.121-130,