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

丸山 伸[†1] 中村素典[†2] 岡部寿男[†2]
山井成良[†3] 岡山聖彦[†3] 宮下卓也[†4]

電子メールが広く利用されるようになるにつれて，メールを遅延なく即時に配送することが求められている．しかし，メール配送エージェント（MTA）に大量のメールが送りつけられて負荷がかかったときには，メールの配送に遅延が生じるだけでなく，MTA の運用の継続すら困難な事態となってしまう．このような高負荷時においても特定のメールを優先的に配送する技術が求められている．本論文では，メールが配送される直前に行われるネームサーバ（DNS）に対する問合せに着目し，DNS 問合せのソースアドレスに基づいて信頼できる発信者からのメールを他のメールから分離し，遅延なく優先して配送する手法を提案する．まず DNS の問合せに対してその応答として毎回異なる回答を送り，回答したサーバにメールが送られてくるのを待つ手順を繰り返すことで，DNS 問合せ元の IP アドレスとメールの発信者との対応表を作成する．次に優先して配送するべきメールの基準に基づき，優先して配送するべき DNS 問合せ元の一覧「White DNS Server List」を抽出する．この表に基づいてメールの配送先を振り分けることで，大量のメールが配送されてくる際にも信頼できる発信者からのメールを他のメールとは独立したサーバで取り扱うことができ，遅延を引き起こすことなく配送できる．そのためのシステム構築方法を示すとともに，実験により有効性を確認した．

Priority Control in Receiving E-mails by Giving a Separate Response to Each DNS Query

Shin Maruyama,[†1] Motonori Nakamura,[†2] Yasuo Okabe,[†2]
Nariyoshi Yamai,[†3] Kiyohiko Okayama[†3]
and Takuya Miyashita[†4]

Delivering e-mails without unnecessary delay is one of the very important issues as the spread of e-mail service and its use become very common. But in case that a “Mail Transfer Agent (MTA)” is heavily loaded by huge amount of mails sent to the MTA, not only the delay on mail delivery is inevitable but also managing the MTA service becomes difficult. Thus, a delivery method that treats legitimate mails with priority is requested. In this paper, we focus on the query to the “Domain Name Service (DNS)” which is usually processed just before the mail transfer, and propose a new delivery method which separates legitimate mails from others according to the source IP address of the DNS query. That is, employing a crafted DNS server which responds to each DNS query with separate IP address, and wait for incoming mails at each address, we get a correspondence table between a DNS query and the incoming mail. And we also show that we can lead legitimate mails to the separated mail servers by dynamically changing the DNS response based on this table, and deliver them with short delay even in the case that others servers are loaded by many other mails.

1. はじめに

近年，電子メールは多くの人により様々な目的に利用されるようになり，社会的に重要なインフラと認識されるようになっている．特に，緊急にかついっせいに配送されるべき「緊急情報」や「安否情報」等にも電子メールが利用されるようになり，メールに対する要求は「確実に相手のもとへと到達する」ことから「遅延なく即座に到達する」ことへと変化している．

一方，電子メールはインターネットで利用される数

†1 京都大学大学院情報学研究科
Graduate School of Informatics, Kyoto University
†2 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
†3 岡山大学総合情報基盤センター
Information Technology Center, Okayama University
†4 津山工業高等専門学校
Tsuyama National College of Technology

あるアプリケーションの中でも様々な問題のあるものとしても認識されている．特に，spam やウィルスの送出するメールの蔓延は，大量のメールによりサーバに負荷を引き起こすだけでなく，場合によってはサーバの処理能力を超えて機能停止に追い込んだりサーバ周辺のネットワークの帯域を消費し尽くしたりすることもあり，いずれもメールの配送に遅延を引き起こす．このような直接的な影響以外にも，spam やウィルス対策の処理による遅延も無視できない．

大部分が不当なメールが大量に配送されてくる状況においてメールの配送に生じる遅延を軽減する手法としては，(1) サーバの負荷分散法，(2) DNS ブラックリスト法[1] 等が利用されることが多い．しかし，これらの手法では配送されてくるメールの数がそれほど多くないうちは有効ともいえるが，メールの数が膨大となったときには効果が薄れる．さらにはこれらの手法はいずれも spam メール等の不当なメールとその他のメールとを同列に扱うため，不当なメールの影響でメールの配送に遅延が生じる問題に対する根本的な対策とはなっていない．

そこで本論文では，メールの配送前に行われる DNS 問合せに着目し，DNS の問合せ元に応じて応答を変えるように機能を持たせた DNS サーバを利用することで，優先するべきメールとそれ以外のメールとを異なるメールサーバで処理する手法を提案する．

まず，DNS 問合せに対して毎回異なるホストを示す応答を返し，そのホストに送られてくるメールとの対応付けを得ることにより，(DNS サーバ, メールサーバ, ドメイン名) の対応付け「DNS サーバエントリ」を得る．次に，受信する各メールに対してこの手順を繰り返すことにより，DNS サーバエントリのリスト「DNS サーバリスト」が作られる．

その後，優先して配送するべき送信者からの MX レコードの問合せに対して応答を変えるために，DNS サーバリストから優先して配送するべきメールの発信者のエントリを抽出し「White DNS Server List」として保持することで，優先して配送するべきメールとその他のメールとの配送先を振り分けることができる☆．

この手法によりメールを振り分けることで，spam やウィルス等の影響で大量のメールが送られてきた際においても，優先する必要のないメールにはウィルスや spam の判定に十分な時間をかけつつ，優先するべきメールには遅延を生じることなく配送できる．

以下，2 章では従来の対策とその問題点をまとめ，3 章で本手法の詳細を述べる．4 章では本手法の実装と評価を行ったうえで，5 章で結論を述べる．

2. 従来の研究

電子メールを利用するうえで spam やウィルスメールの存在は古くから問題とされており，様々な対策手法が提案されている[2),3)]．特に spam 等によるメールの大量発信を防ぐために，発信者認証技術[4)] や Outbound Port25 Blocking[5)] といった手法が提案されているが，いずれもまだ普及には至っていない[6)]．

spam やウィルス等の影響により不当なメールの集中が引き起こされた際には，サーバの負荷があがり，必然的にその他のメールにも遅延が生じることになる．この遅延を短縮するためにサーバの負荷を下げるための手法としては，これまでに主に次のような方法が利用されてきた．

(1) 負荷分散法：レイヤ 4 スイッチや DNS ラウンドロビンを利用して負荷分散を行う．
(2) DNS ブラックリスト法：発信者が spam 送信を行おうとしているかどうかを，送信者の IP アドレスを元に DNS を利用して判定する手法（以下，DNS BL 法とする）．

負荷分散法は，MX レコード問合せに対して DNS ラウンドロビン技術を用いたり，レイヤ 4 スイッチを用いたりすることで，到着するメールを複数のサーバに分散させる手法である．到着するメールは各サーバに平均的に分散されたり，場合によってはサーバの処理能力に応じて分散されたりする．

しかし，どのようにメールを分散するにせよ，それぞれのサーバは割り当てられたメールのすべてを受信することになり，CPU やハードディスク，ネットワークといったリソースを消費することとなる．いいかえると，負荷分散法では，サーバの数を増やすことでメール集中の影響を小さくすることはできるが，依然として到着するメールに比例した負荷を各サーバは受けることとなる．それゆえに，負荷分散法ではサーバの負荷が高くなった際に優先して配送したいメールの配送遅延を減らすことはできない．

次の「DNS BL 法」は，メール送信者が spam を送信しようとしているかどうかを，送信者の IP アドレスにより判定する方法である．もし，送信者の IP アドレスが DNS ブラックリストと呼ばれるデータベースにより「黒（spam 送信者）」として登録されていた場合にはメールの受信を拒否する手法である．

☆ 多くのメールクライアントは手近の DNS サーバを経由して DNS 問合せをすることが多いので，ここでは便宜的に DNS Server List として扱うことにする．

この手法を利用することで MTA はメールの本文を受信することなく拒絶することができるので，負荷分散法を用いる場合に比べて負荷を下げることができると期待される．

しかしながら，この方法を用いたとしても，

- 「spam 送信者である」と判定された発信者が，不要なメールを送ろうと何度も接続を繰り返す可能性がある，
- 同時にサーバに接続されるコネクションの数が増えることで，サーバのリソースが消費し尽くされる危険性がある，

といった問題点があるため，この「DNS BL 法」をサーバの負荷を避ける最善の方法とすることはできない．

ここに述べた以外に，発信者を詐称して送信された spam メールが大量のエラーメール☆となってメール集中を引き起こすことが知られている[7)~9)]（「バックスキャッタ攻撃」とも呼ばれる）．この種のメール集中に対する対策手法として，山井らによる研究[10),11)]があるが，この手法は DNS のキャッシュ機構を活用してメール集中を避けようとするものであるため，ウィルスや spam といった繰り返しメールを送信する発信者に対する対策には使えない．

3. 提 案 手 法

前章で述べたように，メールサーバが高負荷になっている状況において，優先するべきメールを遅延なく配送するためには，サーバにメールが配送された後の対処だけでは対応できない．そこで我々はメールが送信されるよりも前に行われる MX レコードの問合せに着目し，平常時に「DNS 問合せ元の IP アドレスとメールの発信者との対応表」をあらかじめ作成しておくことで，メールの配送時にはこの表を利用して優先するべきメールをその他のメールから分離し，非常時においても低遅延で配送する手法を提案する．

3.1 提案手法の概要

メールが優先するべきものであるか否かにかかわらず，一般にメール送信前には MX レコードの問合せが行われる（**図 1**）．通常，MX レコードの問合せ元とメールの送信元とは必ずしも同じサーバとはいえないため，両者を対応付けることには困難があるが，この対応を得ることができれば，DNS の問合せ元からメールの送信者を予測することができ，優先するべき

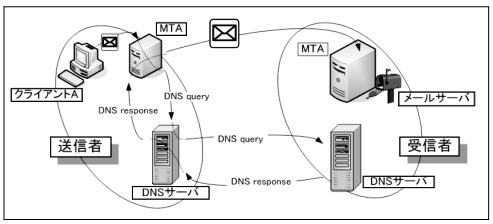

図 1 DNS 問合せとメール送信
Fig. 1 DNS query and mail transfer.

メールの分離に利用することができる．

そこで我々はこれまでに，DNS の問合せを受けるごとに，MX の応答に毎回異なるメールサーバのホスト名を返したうえでメールサーバを監視することで，MX レコードの DNS 問合せのソース IP アドレスとその後にメールサーバに配送されるメールとを対応付け，(DNS サーバ, メールサーバ, ドメイン名) の組合せ「DNS サーバエントリ」を得る手法を提案した[12)]．

この手法により受信するメールのそれぞれに対して繰り返し適用することで，DNS サーバエントリのリスト「DNS サーバリスト」を作成する．

このリストの各エントリとそのエントリを作る元となったメールに基づき，以降のメールを優先配送すべきかどうか判断する．こうして得られた優先配送すべきエントリのリストを「White DNS Server List」と名付け，後に，優先配送すべきメールをそれ以外と区別するために利用する．すなわち，「White DNS Server List」に含まれるサイトからの DNS 問合せには優先受信メールサーバの情報を返すことで，メール配送のコネクションが張られるよりも前に優先して配送するべきメールをその他のものから分離して，「優先受信メールサーバ」へと誘導することができる．

「優先受信メールサーバ」は優先して配送するべきメールのみを扱うためその負荷は低いレベルに保たれることになり，遅延を生じることなくメールを配送できることになる．

3.2 White DNS Server List

この手法を利用するうえでは，どのようにして「White DNS Server List」を作成するかという点が問題となる．単純な方法としては，受信したメールのそれぞれについて優先配送したいメールかどうかを判断しつつ，該当するメール送信者のサイトの管理者にどの IP アドレスから DNS 問合せが行われるかを尋ねることができるが，この手法は手間がかかるだけでなく非効率的である．それゆえ以下の節において，「(DNS サーバ, メールサーバ, ドメイン名) の対応付けのリスト」を自動的に取得し，そこから優先配送するべきエ

☆ 日本の靖国神社のサイトにおける事例では，ピーク時には 1 秒あたり 15,000 通以上のメールが観測された．

ントリを抽出することで，「White DNS Server List」を作成する手順を提案する．

3.2.1 DNS 問合せとメール送信者の自動対応付け

本章では，DNS 問合せ元とメール送信者とを自動的に対応付けて，(DNS サーバ, メールサーバ, ドメイン名) のリスト「DNS サーバリスト」を得る手順の詳細を述べる．

まず，DNS 問合せとそれに対応するメールサーバとの対応付けをするために用いる，1 台ないしは複数台の「調査用メールサーバ」を設置する．調査用メールサーバが複数の IP アドレスを並行して利用することで，対応付けの調査を効率良く進めることができるようになるが，少なくとも 1 つの IP アドレスがあればよい．また，必ずしも複数台利用する必要はなく 1 台のサーバに複数の IP アドレスがある設定でも本手法を適用できる．

次に DNS 問合せ元の IP アドレスにより応答を変化させることができる「特殊な DNS サーバ」を設置する．

そして，通常のメールを受けるための「通常受信メールサーバ」と，優先して配送されるべきメールを受信するためのメールサーバ「優先受信メールサーバ」とを設置する．通常受信メールサーバにメールが集中し，ネットワークが混雑する可能性を考慮し，優先受信メールサーバは通常受信メールサーバとは異なるネットワークに配置することが好ましい．

「優先受信メールサーバ」と「通常受信メールサーバ」は，それぞれ所定のウィルスチェックや spam チェック等を行ったあと，そのメールを「最終受信メールサーバ」に転送する．

それぞれの「調査用メールサーバ」は，以下のいずれかの状態をとる：

Released どの DNS 問合せにも割り当てられていない状態

Assigned ある特定の DNS 問合せに割り当てられ，メールが届くのを待っている状態

Waiting 少なくとも 1 通のメールが届いたあと，DNS 応答の TTL の時間が経過し，その後しばらくの緩衝となる時間が過ぎるのを待っている状態

Assigned の状態でメールを受け取ることなく TTL の時間が経過した場合にも Waiting の状態へと移行する．Waiting の状態で緩衝時間も経過すると，Released の状態に戻る．これらの状態推移については，この後で詳細に述べる．

調査用メールサーバと DNS サーバは，以下の要領で相互に連携して動作する．

(1) DNS サーバに MX レコードの問合せが来るのを待つ．

(2) DNS サーバに問合せを受けたときには，問合せ元が「White DNS Server List」に含まれているかどうかを確認し，含まれている場合には「優先受信メールサーバ」の情報を回答する．

(3) 「Released」の状態にある「調査用メールサーバ」のうち 1 台を選択し割り当てる．Released の状態の「調査用メールサーバ」が 1 台もないときには「通常受信メールサーバ」の情報を返し，調査を終了する．この際，送信者がメールを送信してくるまでの時間に相当する程度に短かい TTL で情報を返す．

(4) 割り当てられた「調査用メールサーバ」の状態を Assigned に変更する．

(5) 割り当てられた「調査用メールサーバ」の情報を，DNS 応答として返す．その際の TTL（有効期間）は比較的短かいものとすることが好ましい．

(6) 割り当てられた「調査用メールサーバ」にメールが送られてくるのを待つ．

(7) メールを受信した際に，DNS 問合せの情報と受信したメールに関する情報とを関連付けて「DNS サーバエントリ」として記録したうえで，メールは「通常受信メールサーバ」に転送する．その後，「調査用メールサーバ」の状態を Waiting に変更する．

(8) 「調査用メールサーバは所定の緩衝時間の間待機したあと，状態を Released に変更し初期状態に戻る．

メールが送られてくる際に，この手順を繰り返して適用することで，「DNS サーバエントリ」のリストを得る．このリストのことを「DNS サーバリスト」と呼ぶ．

3.2.2 「White DNS Server List」の作成

前項までの手順により，DNS 問合せとメール本文との対応が得られている．この対応付けから，「優先配送したいメールを送ってくると考えられる組織」からメールが送られてくる際の DNS 問合せ元の一覧を抽出するためには，前項で得られた「DNS サーバリスト」に対して何らかの基準を与える必要がある．

この抽出基準の例をあげると，次のようなものである：

- メールの Envelope やヘッダに含まれるメールアドレス
- DNS 問合せ元の IP アドレス

- ユーザが指定したメールアドレスや IP アドレスから送られてくるメール
- spam 判定の手法により spam ではないと判断されたメール

上記のような機械的に判断できる基準ではなく，利用者自身により手動にて基準を与えることもできる．すなわち，どのような選択基準を与えた場合においても，上述の「DNS サーバリスト」から利用者の与える基準に沿うメールを送信した DNS サーバエントリを抽出することができる．これを今後「White DNS Server List」と呼び，メールの振り分けに利用することにする．

3.3 White DNS Server List を用いたメール振り分け

まず，「優先受信メールサーバ」に対して「White DNS Server List」に登録された MTA 以外から IP アドレスを直に指定することでメールが送られてくることがないように，ファイアウォール（FW）においてフィルタを行う．

そのうえで，MX レコードの問合せがあった際に，問合せ元が「White DNS Server List」に含まれているかどうかを確認する．含まれている場合には，その問合せに対しては「優先受信メールサーバ」の情報を回答し，含まれていないときには「通常受信メールサーバ」の情報を回答するように DNS サーバを設定する．

ここで「優先受信メールサーバ」の情報を返す際には，その情報と同時に大きな Preference 値（低い優先度）で「通常受信メールサーバ」の情報を渡しておく．このようにすることで，いったん「White DNS Server List」に登録された送信者がウィルスに感染した等の理由により多数のメールを送ってくる状態となったことを「優先受信メールサーバ」で検出したときには，その送信者からのメールが「優先受信メールサーバ」に届くことがないようファイアウォール（FW）でフィルタをすることで，メールは Preference 値の大きな「通常受信メールサーバ」へと送られるようにできる．

この一連の設定により，優先して配送したいメールは「優先受信メールサーバ」に配送され，その他のメールは「通常受信メールサーバ」に配送されるようになる．

次に「優先受信メールサーバ」は，メールを受信するとそれを「最終受信メールサーバ」へと遅滞なく転送する．一方，「通常受信メールサーバ」は，最終的にはメールを「最終受信メールサーバ」に転送することになるが，一度に大量に転送して負荷をかけることのないように転送速度を制限する．「通常受信メールサーバ」に著しく大量のメールが送られて運用に支障をきたす際には受信を制限や停止する．

また，「通常受信メールサーバ」では，spam 対策の有効な手法とされている「おなじみさん方式」[13),14)]や「分散協調型フィルタ方式」[15),16)]のような，メール配送に遅延を生じる spam チェック方式を利用することができる．

3.4 高負荷時の挙動

前節までに，「“White DNS Server List” を作成する作業」と「“White DNS Server List” に基づいて配送する作業」との手順を述べたが，“White DNS Server List” の作成作業は常時行う必要はない．

特に高負荷時には “White DNS Server List” を作成する作業は中断し，すでに作成済みの “White DNS Server List” を用いて優先受信する作業のみを行うことで，このシステムに対する負荷の上昇は DNS サーバと通常受信メールサーバに限定され，優先受信メールサーバに送られてくるメールは遅滞なく配送される．

また，優先受信メールサーバに向けて多量のメールが配送されようとする場合には，(1) “White DNS Server List” に登録されていない多数のメールサーバからいっせいに配信される場合，(2) “White DNS Server List” に登録されているサーバがウィルスに感染し多数のメールを送信してくるようになった場合，の 2 つが考えられる．

前者の場合には，優先受信メールサーバの上流にあるファイアウォールで流入が防止されるため，優先受信メールサーバの負荷をあげることはない．

後者の場合でも，優先受信メールサーバに対して同一の MTA から大量のメールの流入があることを検知した際には，ファイアウォールにおいてフィルタして，通常受信メールサーバの負荷を低く保つ．また，優先受信メールサーバへと通過させるべき送信者の IP アドレスが増えると，ファイアウォールのルールが同じく増えることが懸念されるが，これには優先受信メールサーバとファイアウォールをそれぞれ複数台に増やすことで対応できる．

なお，ファイアウォールにおいて受信を拒否しても，いずれの場合においてもすべてのメールは優先度の低い MX である通常受信サーバへと転送されることとなるため，メールが失われることはない．

3.5 DNS や MTA を共有する送信者への対応

このシステムでは MTA から送られてくるメールを優先受信メールサーバに配送しようとするかどうかを，DNS の問合せ元のみで判断するため，もし多数

の MTA が同一の DNS サーバを利用している場合には問題が生じる．

この場合，これらの MTA のうち 1 つが “White DNS Server List” に登録されると，他のすべての MTA からのメールも優先受信メールサーバに配送されようとする．しかし，“White DNS Server List” に登録されていない MTA からのメールは，優先受信メールサーバの上流にあるファイアウォールを通過することができないため，メールは優先度の低い MX である通常受信メールサーバに配送されることになる．

逆に，1 つの MTA が複数の DNS を利用している場合において，その MTA から送信されてくるメールを優先受信するためには，その MTA が利用する DNS サーバのそれぞれが個別に “DNS サーバエントリ” として登録されている必要がある．しかし，一般にシステムが高負荷となり優先配送を必要とする時間帯は全体から見ると一部分であるため，通常時より定常的にメールの送受信を行っている送信者が利用する DNS サーバエントリは順次登録されていることが期待される．

4. 提案手法の実装と評価

提案手法の有効性を確認するために，前章で述べたシステムを構築し，自動的に「White DNS Server List」を生成できることとそれを用いて優先して配送したいメールを分離する実験を行った．

4.1 機器構成

試験環境は FreeBSD5.3 が動作している 6 台の PC とファイアウォールで構成されている（**図 2**）．

PC1 は「最終メールサーバ」で，最終的にすべてのメールを受信し蓄積することになるサーバである．このサーバはインターネットから直接アクセスできない場所に設置する．

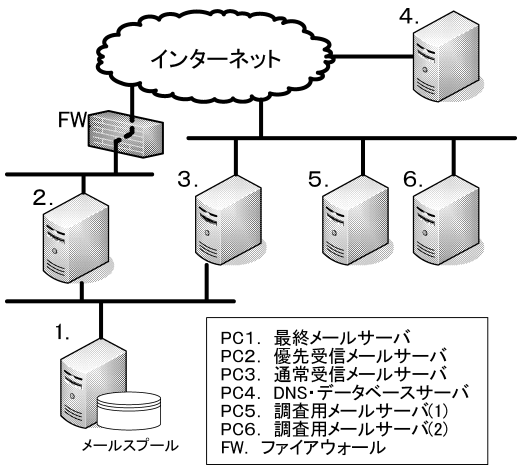

図 2 システム構成の概要
Fig. 2 Overview of the system.

PC2 は「優先受信メールサーバ」であり，優先して受信するべきメールはこのサーバが受信する．このサーバはインターネットとの接続部分にファイアウォールを設置することで，あらかじめ許可されたメールサーバからの接続のみが認めるように制限される．限定されたメールのみがこのサーバを通過するように制御が行われるため，負荷があがることはない．

PC3 は「通常受信メールサーバ」で，優先受信する必要のないメールはこのサーバが受信する．PC1 への転送速度は制限する．

PC4 は DNS とデータベースサーバである．詳細については後に述べる．

PC5 および PC6 は「調査用メールサーバ (1) および (2)」である．これらのサーバはインターネット側にそれぞれ 64 個ずつの IP アドレスを持つように “ifconfig alias” を利用して設定されたため，あわせて 128 個の MTA が「White DNS Server List」を作るために利用される．受け取ったメールは PC3 に渡す．

4.2 DNS と MTA

DNS サーバとしては，動的に応答を変える機能を有する Tenbin [17] を利用する．Tenbin は Ruby スクリプト言語[18] で記述されており，本実験において必要な細かい調整をするのに適している．

メール送信側の負荷が大きいときでも，単純にメールを送る処理は数秒程度の時間で完了するものと考え，MX レコード問合せの応答における TTL（有効期間）は 60 秒とした．また，TTL が切れたあとにメールが送られてくる可能性を考慮して，TTL が切れたあと 10 分間は，同じ MTA を再指定しないようにした．

MTA は Sendmail [19] を採用した．メールを受信したときに “Sendmail::Milter” [20),21)] を介して thread 機能を持つ perl を呼び出し，必要な情報をデータベースに記録するように実装した．

データベースは PostgreSQL [22] を利用した．

また，3.2.2 項で述べたとおり，各メールを優先して配送するかどうかの判断基準が必要となる．この試験においては，「特定のドメインから送られてくるメールを優先して配送する」という基準を採用することにした．

4.3 評価と考察

構築したシステムをインターネット環境で運用し，「DNS サーバエントリ」および「DNS サーバリスト」が提案手法により得られることを確認した．また，試

験的にいくつかのメールを送付することで，正しい情報が取得されていることも確認した（**表 1**）．

このデータから上述の「優先配送するかどうか」の判断基準に基づき，優先して配送するべきメールを送ってきたサイトの DNS 問合せ元の情報を一覧にして「White DNS Server List」を作成した．このリストに載っているアドレスからの DNS 問合せに対して構築されたシステムは「優先配送メールサーバ」の情報を返していることを確認した．

しかしながら，今回の実験期間においてはメールが集中してサーバが過負荷になるようなことはなかったため，実環境でのこの種のテストは行えなかった．そこで，今後もこの試験システムを稼働させつづけ，またより大きなサイトでの動作試験を行うことで，このシステムの有効性を確認できるものと思われる．

1 週間にわたる調査期間中に 1,788 通のメールを受信した．1,788 通のメールに対して，DNS の問合せ元 IP は 89 アドレス，メールの送信元 IP は 106 アドレスであった．これらのメールの優先配送にあたっては 144 の “DNS サーバエントリ” が参照され，うち 21 エントリ，530 通が優先配送の対象とするべきメールと判定され，それらはすべて優先受信サーバへと配送された．

一般にメールを受信する頻度には偏りがあるが，同時に利用された調査用メールサーバは最大 3 台であった．この調査においては調査用メールサーバは 128 個の IP アドレスを利用したが，この数は数個程度と少なくても問題とはならないと思われる．また，もしメール受信数が増えて調査用の IP アドレスを利用し尽くした場合でも，調査が一時的に止まるだけでシステムの挙動には影響しない．

まず，DNS サーバとメールサーバの IP アドレスが，どの程度離れた IP アドレスであるかを調査した．

メールサーバと DNS サーバとが同一の IP アドレスのものは 21 対ありそこから 424 通のメールを受信した．これらの送信元は，

表 1 自動的に取得された DNS サーバエントリの例
Table 1 Examples of the acquired DNS server entry.

DNS query source IP address	MTA IP address	domain part of e-mail from address
210.224.163.5	ns.ikefu.jp [210.224.163.5]	@ikefu.jp
133.69.65.100	c66-33.ibcast.net [133.69.66.33]	@marushin.gr.jp
130.54.12.1	smtp2.mbox.m... [130.54.12.66]	@staff.mbox.m...

- 大規模なメーリングリストサーバ
- NAT 機能を持つファイアウォールと思われるもの

と思われるもので，今回の観測においてはこれらから送られてくるメールにはウィルスメールや spam は含まれていなかった．これはウィルスや spam 配信に利用されている端末は，メールはそれ自身で配送しようとするが，DNS 問合せは近隣のネームサーバを利用しているからではないかと推測している．

次に DNS サーバとメールサーバの IP アドレスの距離を観測した．ここでは subnet のネットマスクが 24 bit であると仮定して，同一の subnet から送られてきているものと，それ以外のものとを数えると**表 2** のようになった．この結果，DNS サーバとメールサーバとは必ずしも近い IP アドレスにあるわけではなく，IP アドレスの近さで DNS サーバとメールサーバの対応関係を与えることは容易ではないことが分かった．

次に，DNS の問合せが行われてからメールの送信までにどの程度の時間間隔があるのかを調査したところ，最短 0.376 秒，最長 440 秒であった（**図 3**）．また，約 80%の場合においてメールを送信する 10 秒前以内に DNS の問合せが行われていた．同様に，98.8%が 60 秒以内に，99.7%が 120 秒以内に DNS 問合せを行っていた．60 秒以上の間隔が空くのは，大規模なメーリングリストの場合やメールマガジン等からの配送の場合であった．この調査結果から今回の試験環境で，DNS サーバの回答における TTL と調査用サー

表 2 DNS と MTA の距離別の分布
Table 2 Distribution of the distance of DNS and MTA.

	受信メール数	(DNS, MTA) 対の数
全体	1,788	144
同一の IP	424	21
同一の subnet	434	34
その他	930	89

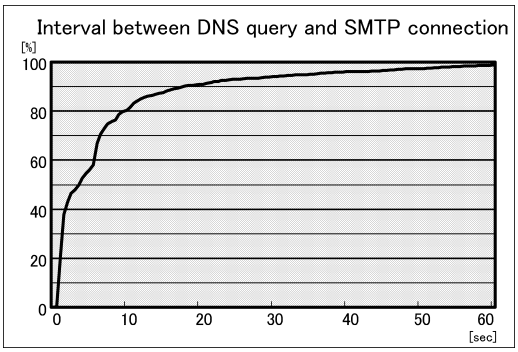

図 3 DNS 問合せからメール送信までの時間分布
Fig. 3 Interval between DNS query and SMTP connection.

バを再利用するまでの時間をそれぞれ 60 秒，600 秒と設定した点には大きな問題はないことが分かった．しかしながら，より大規模なメーリングリストからのメールを受信する場合や，DNS 問合せの結果を長時間キャッシュするような MTA が存在する可能性を考えると，TTL の主旨を考えるともう少し長く調整をする方が好ましい．

しかし，逆に TTL を長くすると「調査用メールサーバ」が Assigned の状態の間に 2 通以上のメールを受信して，その調査から得られる情報の信頼性に検討が必要となる可能性が高くなる．通常想定されるケースとして，送信者が 1 回の DNS 問合せの回答を利用して 2 通以上のメールを送信する場合であるが，これは別段問題とはならない．それに対して，過去に問合せた DNS 情報の TTL 情報（有効期限）の期限を越えてアプリケーションが長時間 DNS 問合せの回答を保持してメールを送信してくる場合があり，これは間違った対応付けを取得してしまう原因となる．対策として TTL の値を小さくすることでこの問題が生じる可能性を下げることはできるが，TTL を小さくしても確実に重複を回避することはできない．

そこで，TTL の値は大きすぎないように調整するとともに，Assigned の状態の間に 2 通以上のメールを受信した場合には，

(1) ヘッダ等の情報により同一の発信者や同一の MTA からのものと認められる場合には通常どおり受信する☆，
(2) 別の MTA からのメールの場合には，先のメールから収集した情報を無効とする，

といった対応が必要となると考えられる．これらのうち，(1) の現象は，同一の MTA が複数のメールを次々と配送する場合に生じるものであるため，そのときに得られた情報を DNS サーバエントリとして利用することには問題はない．逆に，(2) のような現象は「調査用メールサーバの IP アドレスを決めうちでメールを送信してくる MTA が存在した場合」や，「DNS の TTL 情報を無視したりアプリケーションでキャッシュしたりする MTA が存在した場合」に発生するため，このような場合に得られた DNS サーバエントリの情報は不確かなものである可能性が高いため破棄することがよいと思われる．なお，この場合においても「DNS サーバエントリ」の情報を取得できないことにはなるが，受信したメールが失われることはない．

☆ 別の MTA から届いた場合においても，同一の発信者からのものであることを確認できるのであれば，両方の MTA の情報を登録してもよい．

5. 結　　論

本論文において我々は，MX レコードの DNS 問合せ元の IP アドレスに応じて応答を動的に変化させることで，spam やウィルス等の影響により大量のメールが送られてくる状況においても，メールの送信者により配送先を変化させ，優先的に配送したいメールに遅延を生じることなくで配送するシステムを提案した．

具体的には，MX レコードの DNS 問合せと送られてくるメールとを対応付ける手法に着目し，DNS サーバの応答を動的に変えることでこの対応表を自動的に生成する．次にこの対応表に対して何らかの基準を与えることで，優先して受信するべき対応の一覧「White DNS Server List」を生成し，DNS 問合せの段階でその後に送られてくるメールを優先して配送するべきかどうかを判断する手順を示した．

そして得られた「White DNS Server List」を利用して優先して配送するべきメールは独立したサーバを経由するように DNS サーバの応答を変化させることで，それらのメールを優先して低遅延で配送する手順を提案し，実験を通してこの手法の有効性を確認した．

優先配送しなくてもよいメールには分散協調型等の遅延を生じる spam フィルタ等を適用するといった実用的な試験を行いつつ，より大規模な環境で運用し高負荷時における挙動を確認することが今後の課題である．

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) Spamcop: SpamCop.net. http://www.spamcop.net/bl.shtml
2) I-005c: E-Mail Spamming countermeasures Detection and prevention of E-Mail spamming (1997). http://www.ciac.org/ciac/bulletins/i-005c.shtml
3) Manager's Guide to Coping with Spam, The Open Group Messaging Forum (July 2003). http://www.opengroup.org/messaging/spam/July_2003/Coping_with_Spam997.pdf
4) Gellens, R. and Klensin, J.: Message Submission (Dec. 1998). http://www.faqs.org/rfcs/rfc2476.html
5) http://www.postcastserver.com/help/Port_25_Blocking.aspx
6) Watson, B.: Beyond Identity: Addressing Problems that Persist in an Electronic Mail

System with Reliable Sender Identication, CEAC (2004). http://www.ceas.cc/papers-2004/140.pdf
7) Incident at Japanese shrine (Sep. 2004). http://www.yasukuni.or.jp/new/osirase.htm
8) Mail Non-Delivery Attack, Alert Number: AL04-005, Public Safety and Emergency Preparedness Canada (PSEPC) (Apr. 2004). http://www.ocipep-bpiepc.gc.ca/opsprods/alerts/2004/AL04-005_e.asp
9) Frei, S., Silvestri, I. and Ollmann, G.: Mail Non-Delivery Notice Attacks (Apr. 2004). http://www.techzoom.net/mailbomb
10) Yamai, N., Okayama, K., Miyashita, T., Maruyama, S. and Nakamura, M.: A Protection Method against SPAM Mails with Sender Address Spoofing, *SAINT2005* (2005).
11) 山井成良，岡山聖彦，宮下卓也，繁田展史，丸山伸，中村素典：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，情報処理学会論文誌，Vol.47, No.4, pp.1010–1020 (2006).
12) Maruyama, S., Nakamura, M., Okabe, Y. and Yamai N.: A Dynamic Modification on DNS Response and its Application on Mail Transfer Agent, IPSJ SIG Technical Report, 2004-DSM-32-14, pp.79–84 (2004).
13) 鈴木常彦，後藤邦夫，山口榮作，石川雅彦：MTA による spam 対策の実践報告，情報処理学会研究報告，IPSJ SIG Technical Report, Vol.2004, No.77, 2004-DSM-034 (2004).
14) 前野年紀：「お馴染さん」方式. http://spam.qmail.jp/onazimi/
15) Rhyolite Software: Distributed Checksum Clearinghouse (2004). http://www.rhyolite.com/anti-spam/dcc/
16) 漣 一平，山井成良，岡山聖彦，宮下卓也，丸山伸，中村素典：遅延評価による分散協調型 spam フィルタの検出率向上，2003-CSEC-024 (Mar. 2004).
17) Shimokawa, T., Yoshida, N. and Ushijima, K.: DNS-based Mechanism for Policy-added Server Selection, *SSGRR2000* (2000).
18) Ruby Home Page. http://www.ruby-lang.org/en/
19) Sendmail, Inc.: Sendmail Home Page. http://www.sendmail.org/
20) Milter Home Page. http://www.milter.org/
21) Sendmail::Milter Home Page: http://sendmail-milter.sourceforge.net/
22) PostgreSQL Global Development Group: PostgreSQL Home Page. http://www.postgresql.org/

(平成 17 年 7 月 13 日受付)
(平成 18 年 2 月 1 日採録)

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 年京都大学総合情報メディアセンター教務技官，平成 11 年京都大学学術情報メディアセンター助手として，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．

岡部 寿男（正会員）

昭和 63 年京都大学大学院工学研究科情報工学専攻修士課程修了．同大学工学部助手，大型計算機センター助教授等を経て，平成 14 年より京都大学学術情報メディアセンター教授．博士（工学）．並列・分散アルゴリズム，インターネットワーキング等の研究に従事．電子情報通信学会，システム制御情報学会，日本ソフトウェア科学会，IEEE，ACM，EATCS 各会員．

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．