

LL-004

マルチホームネットワークにおける電子メールシステムの高信頼化運用手法 A Reliable Operation Method of E-mail systems on Multihomed Networks

山井 成良[†]
Nariyoshi Yamai[†]

土居 正行[‡]
Masayuki Doi[‡]

岡山 聖彦[†]
Kiyohiko Okayama[†]

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。特に、近年ではネットワークの広帯域化に伴い、添付ファイルなどを含む大容量のメッセージが頻繁に交換されるようになり、ネットワークやシステムの障害が利用者に与える影響はますます大きくなってきている。

このような障害への耐故障性を高める方法として、一般にネットワークやサーバの冗長化が知られている。このうち、ネットワーク障害への対策としては、組織ネットワークを複数のバックボーンネットワーク（以下、バックボーン）に接続するマルチホームネットワークがよく用いられている。ところが、マルチホームネットワークを導入した場合でも、従来のネットワークあるいは電子メールシステムの運用方法では、運用コストが増大したり、障害の発生箇所によってはメッセージの配送に支障をきたすことがあったりするという問題があった。

そこで本稿では、マルチホームネットワークにおいて、上記の問題を解決できるような電子メールサービス運用手法を提案する。本手法では障害の発生箇所にかかわらず電子メールが宛先に確実に配送できるバックボーンを選択し、また BGP4 (Border Gateway Protocol 4) [1] のような運用コストの高い経路制御プロトコルを必ずしも用いる必要がないという特徴を持つ。

2. 従来の電子メールシステム運用手法とその問題点

2.1 想定するネットワーク環境

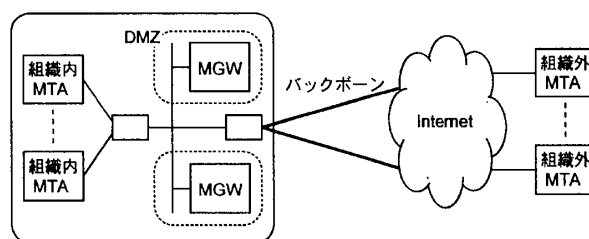
本稿では、図 1(a)(b) に示すように、対象となる組織では 1 箇所あるいは複数箇所において複数のバックボーンが接続され、マルチホームネットワークを構成しているものとする。マルチホームネットワークの運用方法としては、

- (1) 同一の組織内アドレスを各バックボーンでそのまま用い、BGP4 により経路制御を行う方法
- (2) ALG(Application Level Gateway) を導入し、組織内 IP アドレスを各バックボーンから個別に割り当てられた IP アドレスに変換する方法 [2, 3]
- (3) NAT(Network Address Translation)[4] 機能を持つ対外接続ルータを導入し、組織内 IP アドレスを各

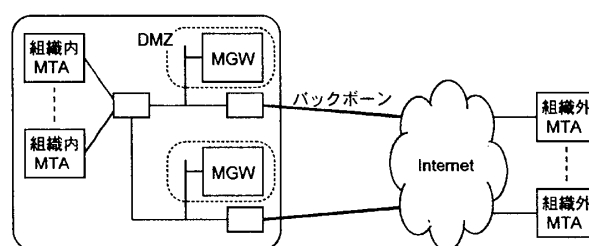
[†]岡山大学, Okayama University

[‡]株式会社 ACCESS, ACCESS Co., Ltd.

[§]国立情報学研究所, National Institute of Informatics



(a) 1 箇所ですべてのバックボーンと接続されている場合



(b) 複数箇所バックボーンと接続されている場合

図 1: 想定するネットワーク構成

バックボーンから個別に割り当てられた IP アドレスに変換する方法 [5, 6]

など、いくつかの方法が知られているが、現時点の議論ではいずれの方法でも構わない。

各バックボーンネットワークとの接続点では DMZ (De-Militarized Zone) 内にメールゲートウェイ (MGW: Mail GateWay) が導入されており、組織外から組織内および組織内から組織外への電子メールは全ていずれかのメールゲートウェイを経由して配送されるものとする。なお、メールゲートウェイは図 1(a) のように 1 箇所バックボーンに接続されている場合でも耐故障性を高めるため複数台設置されているものとする。

このような構成は組織内ネットワークのセキュリティ強化のため、また耐故障性を高めるため、多くの組織で採用されており、一般的なものである。

以下では、単純化のため、特に断りのない限り図 1(b) を対象として議論する。

2.2 従来手法の問題点

1 章で述べたように、図 1(b) のようなメールゲートウェイやバックボーンを冗長化した構成においても従来のネットワークあるいは電子メールシステムの運用方法では、様々な問題が生じる。本節では、組織外から組織内へのメッセージ配送ならびに組織内から組織外へのメッ

セージ配送のそれぞれについて従来の運用手法の問題点を示す。

2.2.1 組織外から組織内へのメッセージ配送

組織外から組織内へのメッセージ配送においては、マルチホームネットワークの運用方法にかかわらず、各メールゲートウェイをDNSサーバにMX(Mail eXchange)レコードとして登録する手法[3]がよく用いられている。この場合、組織外MTA(Mail Transfer Agent)は複数のMXレコードのうち優先度が高い順に(同じ優先度であれば無作為に)メッセージ配送を試み、正常に配送が行われた時点で動作を終了する。メールゲートウェイはメッセージを受け取ると、たとえばウイルスチェックなど所定の動作を行った後、組織内MTAに中継する。これにより、組織外MTAといくつかのメールゲートウェイとの間で通信障害が発生した場合には、通信可能なメールゲートウェイが1台でも存在すればこれを中継して組織内MTAにメッセージを配送することができる。

ところが、たとえば優先度の最も高いメールゲートウェイ(以下、これをPMG(Primary Mail Gateway)と呼ぶ)と組織内MTAとの間で通信障害が発生した場合には、従来の運用手法ではメッセージ配送に支障が生じる。すなわち、組織外MTAからPMGへの配送は正常に行われるが、PMGから組織内MTAへの配送は障害のため行われず、メッセージは障害から復旧するまでPMGに留まってしまう。この現象は特にPMGと組織内MTAが物理的に離れた場所に設置されている場合に比較的发生しやすく、メールゲートウェイの冗長化が有効でないことを意味する。

2.2.2 組織内から組織外へのメッセージ配送

組織内から組織外へのメッセージ配送においては、2.1節で述べたマルチホームネットワークの運用方法が深く関与する。

3つの運用方法のうち、(1)のBGP4により経路制御を行う方法は、ネットワーク層の範囲で経路制御が行われるため、メールゲートウェイには何ら変更を加えることなく組織外MTAと通信可能なバックボーンを選択することが可能である。しかし、この方法ではAS(Autonomous System)番号を取得した上で各バックボーンの管理者と協調して設定作業を行う必要があるなど、かなり運用コストが大きい点が問題となる。また、最近ではルータでの経路数の増加を抑制するため、小規模なネットワークについては経路情報が広告されないことがあり、その場合にはバックボーンの冗長化が有効にならない点も問題となる。

一方、(2)のALGを用いる方法として、たとえば文献[3]ではsendmail[7]におけるFallbackMXhost機能を利用する手法を紹介している。これは通常利用するメールゲートウェイでは組織外MTAにメッセージを配送できなかった場合には、そのメッセージを別のメールゲートウェイに転送し、そこから以前とは異なるバックボーンを経由して再配送するものである。ところが、この方法では、

転送先のメールゲートウェイから組織外MTAへの到達可能性を確認していないため、たとえばどのメールゲートウェイからも組織外MTA通信できない状況になった後で最初に利用したバックボーンだけが復旧した場合など、別のメールゲートウェイへの転送が必ずしも適切とは限らない場合がある。この問題点はFallbackMXhost機能を用いて全てのメールゲートウェイを循環しながら再配送を試みるようにすることで解決することは可能であるが、その場合には配送可能になるまでメッセージがメールゲートウェイ間を無駄に循環するという新たな問題が生じる。

また、(3)のNAT機能付き対外接続ルータを導入する方法では、(1)と同様にネットワーク層の範囲で経路制御が行われるため、メールゲートウェイでの設定変更は不要であり、また対外接続ルータに負荷分散機能を持たせることにより複数のバックボーンを効率よく利用することが可能になる。しかし、この方法ではこのルータに全てのバックボーンを接続する必要があるため、ネットワークの構成によってはこの方法が適用できないことがある。

以上のように、従来のネットワークあるいは電子メールシステムの運用方法では、運用コストが増大したり、適用可能なネットワーク構成に制限があったり、あるいは障害の発生箇所によってはメッセージの配送に支障をきたしたりする点が問題である。

3. 電子メールシステムの高信頼化運用手法

前節で述べたように、従来方法では組織外から組織内へのメッセージ配送および組織内から組織外へのメッセージ配送のいずれについても問題があった。そこで、本章では、いずれの方向へのメッセージ配送についても上記の問題を解決するような電子メールシステムの高信頼化運用手法を提案する。

3.1 組織外から組織内へのメッセージ配送

組織外から組織内へのメッセージ配送において従来方法で問題が生じる原因は、メールゲートウェイから組織内MTAへの配送が不確実な状態でも、そのメールゲートウェイで組織外からのメッセージ配送を正常に受け付けてしまう点にある。

そこで、本稿では、図2に示すように、組織外MTAとメールゲートウェイの間で確立されるSMTPセッション中に、宛先が判明した時点でメールゲートウェイから宛先となる組織内MTAへSMTPセッションを確立して到達性の確認を行ってからメッセージ配送を受け付ける手法(たとえば[9]参照)の利用を提案する。その際、組織内MTAへの到達性を確認できなければ、図3に示すように、メールゲートウェイは組織外MTAに一時エラーを返し、組織外MTAに次の優先度を持つメールゲートウェイへの配送を促すようにする。これにより、組織外MTAは確実に組織内MTAに配送できるメールゲートウェイを選択できるようになり、電子メールサービスの高信頼化が図れる。

なお、図2において、オーバーヘッドの低減および信頼性の更なる向上のため、メールゲートウェイ・組織内MTA間のSMTPセッションを到達性確認後も切断せずにメッ

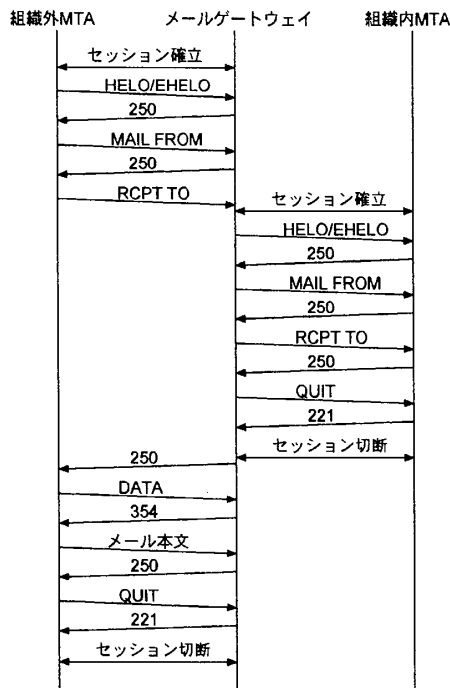


図2: 組織外から組織内へのメッセージ配送 (正常時)

セージ配送にも利用する方法が考えられる。しかし、この場合、異なる組織内MTAに属する複数の宛先が指定されると、メールゲートウェイ・組織内MTA間のSMTPセッションも複数確立して全セッションにメッセージを同時に中継する必要が生じ、また一部のSMTPセッションにおいてエラーが発生した場合の処理も複雑になるなど、全体の処理の流れがかなり複雑になるとと思われる。そのため、提案手法ではこの方法は採用しなかった。

3.2 組織内から組織外へのメッセージ配送

組織内から組織外へのメッセージ配送においても、組織外から組織内へのメッセージ配送と同様の問題が存在するため、前節で述べたように、メールゲートウェイにおいて宛先となる組織外MTAへの到達性を確認してからメッセージを受信する方法が有効である。

ところが、一般に電子メールでは複数の宛先を指定することができ、また組織内から組織外へのメッセージ配送ではこれらの宛先は異なるドメインに属することが多いと思われるため、単にSMTPセッション開始時ににおける到達性の確認だけでは不十分と思われる。すなわち、メールゲートウェイからのメッセージ配送中に一部の組織外MTAへの配送に支障が生じると、前節で述べた手法ではそれを組織内MTAが検出できず、配送可能になるまでメールゲートウェイにメッセージが留まってしまいう危険性がある。

この危険性を回避する方法として、複数の宛先が指定されている場合には1回の配送では1つの宛先しか扱わないように組織内MTAでメッセージを複製し、配送が確実に行われたかどうかをDATAコマンドの応答で判断する方法が考えられる。しかし、この方法ではメッ

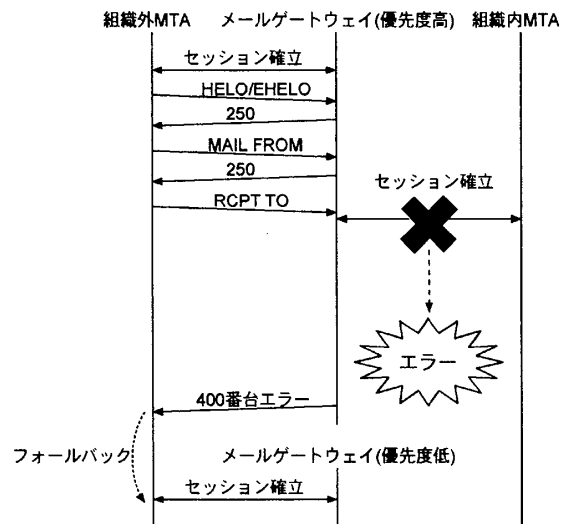


図3: 組織外から組織内へのメッセージ配送 (障害発生時)

セージの無駄な複製が行われるため、通信量の増大や遅延時間の増加などの面で好ましいとはいえない。

そこで、本稿では、組織内MTAからメールゲートウェイへのメッセージ配送プロトコルとして、従来のSMTPではなくLMTP[8]を利用する手法を提案する。LMTPは本来はローカルメール配送用のプロトコルで、SMTPとほぼ同じ過程で利用できるが、DATAコマンドに対して各宛先の配送結果を応答する点がSMTPとは異なる。例として、複数の宛先(宛先A、宛先B)が指定され、そのうち宛先Bには配送されたが宛先Aには配送されなかった場合の組織内MTA・メールゲートウェイ間の配送手順を図4に示す。この例では組織内MTAは宛先Bへの配送が行われなかったことを知りうるので、この後は別のメールゲートウェイ経由での配送を試みることができる。

なお、組織外から組織内へのメッセージ配送においても複数の宛先が指定されている場合には同様の問題が生じうるが、組織外MTAがLMTPを用いるように強制できないため、また一般に組織内ネットワークは外部ネットワークと比較すると高速かつ安定的でメッセージ配送中に組織内ネットワークの状態が変化する可能性が比較的低いと思われるため、SMTPセッション開始時の到達性のみを確認するに留めた。

本手法の他の利点としては、既存のネットワークへの導入が容易である点が挙げられる。すなわち、本手法は既存のメールゲートウェイをそのまま利用できるため、図1(a)(b)のいずれの環境でも適用可能であり、またALGを用いた方式の一種であるため、BGP4などを用いた運用コストの大きな経路制御は必要としない。

4. システムの実装と動作確認

上記の提案手法に基づき、我々は試作システムを実装した。試作システムでは、図1(a)のようなネットワーク環境を構築し、2台のメールゲートウェイを配置した。各メールゲートウェイでは、SMTPサーバとして send-

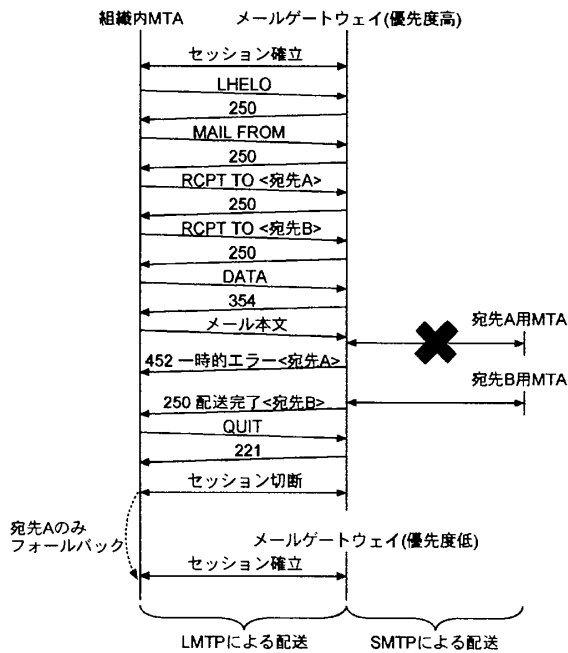


図 4: 組織内から組織外へのメッセージ配送

mailを用い、組織内MTAへの到達性を確認するためにmilter-ahead[9]を導入した。また、LMTPサーバとしてはSMTPfeed[10]を用い、組織内MTAではメールゲートウェイとの通信にLMTPを用いるようにsendmailの設定を行った。

動作確認実験としては、メールゲートウェイにおいてOS(FreeBSD)の持つフィルタリング機能(ipfw)を用いてバックボーンや組織内ネットワークに通信障害を発生させ、その場合に組織外MTAから組織内MTAへのメッセージ配送ならびに組織内MTAから組織外MTAへのメッセージ配送が正常に行われるかどうか確認した。その結果、いずれの方向のメッセージ配送においても、通信可能なメールゲートウェイを選択した場合にはそのまま配送され、また通信不可能なメールゲートウェイを選択した場合にはメールゲートウェイにより一時エラーが返されて別のメールゲートウェイを経由して配送されることを確認した。また、受信側MTAを停止させてどちらのメールゲートウェイを経由しても配送できない状況が発生させたところ、メッセージは送信側MTA内に留まり、無駄な配送が行われていないことも確認した。

以上の結果から、提案手法は3章に述べたとおり動作し、電子メールサービスの高信頼化に寄与すると言える。

5. むすび

本稿では、マルチホームネットワークにおいて電子メールサービスの信頼性を高める運用手法を提案した。本手法に基づくシステムを試作し、動作確認実験を行った結果、本手法は障害の発生箇所にかかわらず電子メールが宛先に確実に配送できるバックボーンを選択し、その有効性を確認することができた。今後の課題としては、提

案手法を実際のネットワーク環境で適用し、そ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17～19年度科学研究費補助金(基盤研究(B)、課題番号17300038)および情報通信研究機構超高速・高機能研究開発テストベッドネットワーク(プロジェクト番号JGN2-A16061)の支援を受けている。

参考文献

- [1] Rekhter, Y. and Li, T.: "A Border Gateway Protocol 4", RFC1771, IETF(1995).
- [2] 中川郁夫, 上谷一, 鍋島公章, 樋地正浩, 今野幸典: "マルチホーム環境におけるアプリケーションルーティング技術の提案", 情報処理学会分散システム運用技術研究報告, No.1998-DSM-012, pp.37-42(1998).
- [3] 野川裕記, 辰巳治之, 小林悟史, 大石憲且, 河合修吾, 秋葉澄伸: "札幌医大/NORTHにおけるマルチホーム運用の実例", Proceedings of NORTH '99 Internet Symposium, pp.72-79(1999).
- [4] Egevang, K. and Francis, P.: "The IP Network Address Translator (NAT)", RFC1631, IETF(1994).
- [5] 岡山聖彦, 山井成良, 島本裕志, 宮下卓也, 岡本卓爾: "マルチホームネットワークにおける透過的な動的トラフィック分散", 情報処理学会論文誌, Vol.41, No.12, pp.3255-3264(2000).
- [6] 岡山聖彦, 山井成良, 久保武志, 宮下卓也: "マルチホームネットワークにおけるアプリケーションプロトコルの性質を考慮した動的トラフィック分散", 情報処理学会論文誌, Vol.46, No.4, pp.1007-1016(2005).
- [7] Sendmail Inc.: "Sendmail Home", <http://www.sendmail.org/>.
- [8] Myers J.: "Local Mail Transfer Protocol", RFC2033, IETF(1996).
- [9] Howe, A.: "SnertSoft - milter-ahead/1.6 for Sendmail", <http://www.milter.info/sendmail/milter-ahead/>.
- [10] 中村素典: "電子メールの配信を高速化するSMTPfeedの設計と実装", 情報処理学会分散システム/インターネット運用技術シンポジウム'99論文集, pp.27-32(1999).