

ISP におけるメールシステム構築事例と今後の展開

E-mail system construction examples and future development at ISPs

堀河俊介 *
Shunsuke Horikawa

赤峰康之 *
Yasuyuki Akamine

* システム基盤グループ IT ソリューション事業部 第二ソリューション部

今日の電子メールの役割は、法人のみならず一般家庭においても重要な通信手段の一つである。

その為、電子メールのやり取りを実現するメールシステムにおいては、長時間停止が許されない高い信頼性を持ったシステムが必要とされている。サービス提供者側にとっては、ウイルスやスパムといったインターネットを介して伝播する脅威からシステムを保護することはもちろんのことであり、しかも費用対効果を実現するための設計構築やシステム安定化に向けた取り組みが重要となる。

E-mail today serves as an important communication medium, not only for corporations but also for families.

Therefore, the e-mail system that supports e-mail communication must be highly reliable and free from prolonged service outage. In addition to protecting the system from internet threats such as viruses and spam, service providers must be conscious about designing and constructing a system that brings the expected results at low cost as well as stabilizing the system.

1 まえがき

某インターネットサービスプロバイダ（以降、ISP）様は、複数のケーブルテレビ局を統括するケーブルテレビ（以降、CATV）ネットワーク企業である。CATV 業界は回線のデジタル化に伴ってインターネットサービスの利用者も増加し、VoIP^{注1)}、セットトップボックス^{注2)} やビデオオンデマンド^{注3)} 等のサービス提供により会員増を目指している。

しかし、CATV 業界は総じて地域人口の制約から大幅な会員増は難しく、システム投資に関しては費用対効果を厳しく判断される。

注1) VoIP：Voice over Internet Protocol の略。インターネットやイントラネット等の TCP / IP ネットワークを使って音声データを送受信する技術。

注2) セットトップボックス：テレビに接続して様々なサービスを受けられるようにする機器の総称。

注3) ビデオオンデマンド：映像配信サービスの一つで、視聴者が要求したときに即座に映像が配信されてくるシステムのこと。

今回我々が携わることになった某 ISP 様のメールシステムも例外ではない。

本稿では、我々がこうした企業背景を考慮しつつ、メールシステムの構成提案から構築・移行にどのように取り組んだかを紹介する。

2 構築の背景と課題

2.1 構築の背景

CATV 会員数の増加やスパム増大に伴うメール流量の増加に加えて旧システムの老朽化が進み、メール送受信におけるパフォーマンスに影響が出始めた。メールは数十分の遅延が発生することもあり、メールを通信手段の一つとして頻繁に活用しているユーザーへ影響を及ぼしていた。

そのため、メール送受信の遅延等によるユーザー影響を発生させないことが顧客の第一の要望として挙げら

れた。また、今後の会員数拡大に加えてスパム等によるメール流量増加を考慮し、現状流量の 10 倍は耐えうるシステムとすることも要望として受けた。

リプレースにおいては、ハードウェア・ソフトウェア費用を最小限に抑えつつも、性能（キャパシティ）や信頼性を確保する必要がある。また、ユーザーに対して安全で安心できるサービスを提供することを目的として、スパム対策・ウイルス対策等のメールシステムとしてあるべきサービスも充実させる必要がある。

さらにはメールが通信手段の重要なツールであることからメールシステム移行時に発生するユーザー影響を極力少なくすることも重要である。

2.2 課題に対する実現方針

(1) キャパシティ確保

旧システムでは、メール流量増加によりサーバ高負荷状態が頻繁に発生することで、メール送受信の遅延が度々発生し、ユーザーへ影響を及ぼしていた。また、ユーザー影響を解消するために、メール配送を円滑にするための運用者対応も度々発生し、運用負荷も増大していた。

こうした状況を解決するためには、十分なサーバ能力（キャパシティ）を確保する必要があるが、反面ハードウェア・ソフトウェアコストを最小限に抑える必要がある。

そこで構成提案においては、まず過去の構築実績を踏まえ、流量 10 倍に対して過剰投資とならない最適なハードウェアスペックを算出し、ハードウェア選定を実施した。さらにソフトウェア選定では、商用ソフトとフリーソフトをうまく組み合わせることでコストの削減を実現した。

(2) 構築コストの低減と信頼性確保

メールボックスサーバ（メールスプール領域）の冗長化方式としては、従来 2 台のサーバでクラスタ構成とし、ストレージ専用のネットワークによってサーバとストレージ間のデータ転送を高速に行える、ストレージエリアネットワーク（以降、SAN）を採用することが多かった。

サーバのクラスタリングにおいては、クラスタソフトを使用して 2 台のサーバを運用サーバと待機サーバに分けて稼働させるため、信頼性は十分に確保できるが待機サーバは実質稼働していないためコストパフォーマンスに問題がある。さらにクラスタソフトを使用するため、そのソフトウェア費用も必要になっていた。

また SAN においては、サーバとストレージを接続するための専用のスイッチやケーブル等が必要となり、ハード費用としても高価になっていた。

そこで今回は、信頼性を確保しつつコストパフォーマンスを向上するために、メールスプール領域として SAN を利用する方式ではなく、ネットワークに直接接続して使用するネットワークストレージ（以降、NAS）を採用した。

NFS^{注4)}を利用することで、メールボックスサーバを並列に複数台設置し、全てのメールボックスサーバからユーザー毎のメールデータへのアクセスを可能とした。これにより、稼働サーバ全てをサービス機状態にすることができ、コストパフォーマンス向上を実現した。また、会員数の増加に伴う増設作業も安価にしかも迅速に対応可能とした。

さらに、負荷分散方式としてリクエストを順番に分配するラウンドロビン方式を採用することで冗長構成を確保し、クラスタソフトウェアにかかる費用を削減した。

(3) 利用サービスの充実化

ユーザーに求められることとして、まず頻発するスパムメールおよびウイルスメール等の脅威からユーザーを守ることが挙げられる。

スパムメールおよびウイルスメール等の脅威に対しては、契約ユーザー単位で提供可能な迷惑メールブロック機能とウイルスチェック機能およびユーザーが個々に設定可能なキーワードフィルター機能を提供した。

また、メール利用シーンが増加するにつれて、外出先でのメール利用ユーザーは増加傾向にあった。

そこで、外出時にも Web ブラウザや携帯電話から利用できる IMAP プロトコル対応の Web メールサービスを新たに導入し、外出先からのメール利用を実現した。

(4) ユーザー影響の無いシステム移行

メールシステムにおける旧システムから新システムへの移行においては、ユーザー情報（認証情報）の移行やメールデータの移行等が必要である。

これらのデータを移行するためには、システムを一時的に停止してメールデータにアクセスがない状態で全てのデータ移行を実施する方式が一番確実で容易であるが、システムの一時停止はメールを頻繁に利用しているユーザーへ大きな影響を及ぼしてしまう。

注4) NFS : Network File System の略。UNIX システムで利用されるファイル共有システム。

よって、移行においてはユーザー影響を発生させないためにも極力無停止で実施することが顧客要望であり課題として挙げられた。

この課題に対しては、ドメイン単位での移行やメールソフトウェア機能を十分に活用したシステム停止を伴わない方式を提案しユーザー影響のない移行を実現した。

3 システム概要

システム構成概要図を図-1に示し、ハードウェア・ソフトウェア構成を記す。

3.1 システムハードウェア構成

ハードウェア選定にあたっては、顧客要望に沿った性能を考慮しつつ過去の構築実績より選定を行った。主な使用ハードウェア構成を表-1に記す。

3.2 システムソフトウェア構成

全体的なコスト削減と機能要件充実のため商用ソフトとフリーソフトを適切に組み合わせ、低コスト/高機能なシステムを実現した。

スパム・ウイルスとメール配送の脅威になりうる箇所には、他システムにて実績があり品質・サポート面において信頼のおける商用ソフトを利用した。さらに新規導入の IMAP 対応 Web メールサーバにおいても、新規開発によるコスト面を考慮し商用版を採用した。

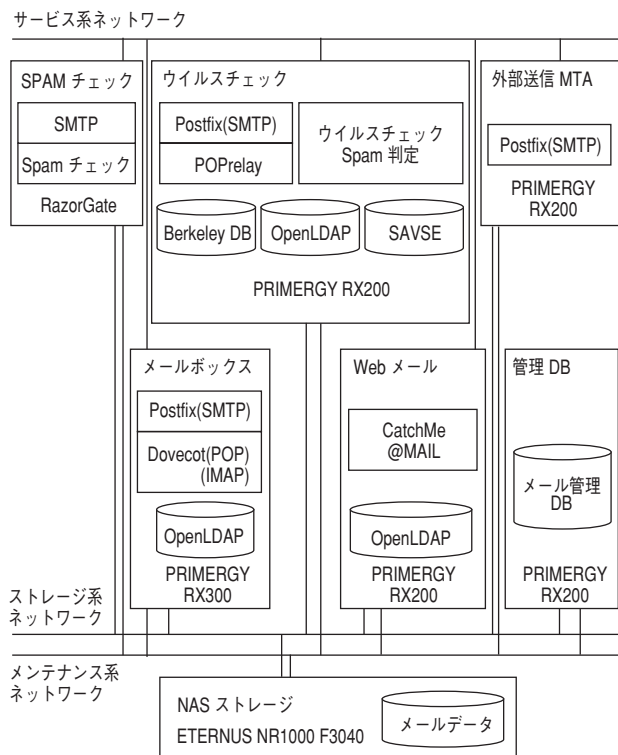
その他、SMTP^{注5)} / POP^{注6)} / IMAP^{注7)} サーバにおけるメール配送ソフトウェアやユーザー情報を格納する認証部分においては、他システムにて実績があるフリーソフトを採用し、商用版を利用した場合のライセンス費用削減（運用コスト削減）を図っている。主な使用ソフトウェア構成を表-2記す。

3.3 システムコンポーネント

(1) SPAM チェック

SPAM チェックサーバは、LDAP 連携が可能でありさらにメール配信力や大幅なスパムを検知することで定評のあった Mirapoint 社の「RazorGate^{※1)}」を採用した。

「RazorGate」は、SPAM チェック契約しているユーザーのみにライセンス費用が必要となる有益なライセンス形態方式のため、運用コストにおいても費用対効果を十分に発揮でき、また同等のサーバを複数台並べることで、拡張性の向上と導入の容易さを実現している。



●図-1 システム構成概要図●
(Fig.1-System construction diagram)

●表-1 主な使用ハードウェア一覧●

ハードウェア名 アプライアンス名	概要
PRIMERGY RX200	高性能・高信頼なラック型 (1U) 薄型 2WAY サーバ。
PRIMERGY RX300	高性能・高信頼・高拡張なラック型 (2U) 2WAY サーバ。
Mirapoint RazorGate	スパムやウイルス、マルウェア ^{※1)} 等の脅威あるメールの侵入を防ぐ、メールセキュリティアプライアンス。
ETERNUS NR1000 F3040	データの効率的な統合と活用を実現する高性能・高信頼ネットワークディスクアレイ装置。

※1 マルウェアとはコンピュータウイルス、ワーム、スパイウェア等の「悪意のこもった」ソフトウェアのことである。

注5) SMTP : Simple Mail Transfer Protocol の略。電子メールを送信するためのプロトコル。

注6) POP : Post Office Protocol の略。電子メールをサーバから受信するためのプロトコル。

注7) IMAP : Internet Message Access Protocol の略。電子メールをサーバから受信するためのプロトコル。

(2) ウイルスチェック

ウイルスチェックサーバは、ユーザーがアクセスする SMTP / POP サーバであり Symantec のアンチウイルスエンジン^{※2)}を採用している。

本システムは 1 台のサーバに電子メールサーバソフトウェア (以降、MTA) を 6 プロセス起動し、メール送信用 MTA やメール受信用 MTA を多段 MTA 構造にすることで、メールの振り分けを柔軟にこなし、以下の機能を実現している。

- 1) 契約者単位やドメイン単位のウイルスチェック
- 2) 契約者単位やドメイン単位のキーワードフィルタ一設定
- 3) ウイルス検知時通知メールのドメイン毎カスタマイズ
- 4) POP before SMTP^{注8)} / SMTP-Auth^{注9)} / POPrelay^{注10)}

また、MTA には管理の容易さを考慮し「Postfix^{※3)}」を採用した。

さらに、メール送信用 MTA やメール受信用 MTA を機能毎に分けてサーバ導入するのではなく、同一構成のサーバを複数並べるラウンドロビン方式にすることで、機能毎に発生するサーバ導入コストの削減、拡張性の向上を実現している。

(3) メールボックス

メールボックスサーバは、IMAP / POP に対応したメールボックスであり、次世代ソフトウェアである「Dovecot^{※4)}」を採用したメールシステムである。また、メール受信用の MTA にはウイルスチェックサーバ同様「Postfix」を採用した。

メールボックスサーバでは、IMAP プロトコルの利用が必須要件であったこと、メールデータ移行を考慮し旧システム側で使用しているソフトウェア (qmail) との互換性が必要であった。さらに NAS を利用したメールデータ保存に伴う NFS との互換性も考慮しなければならなかった。

よって、IMAP / POP サーバとして上記条件を満たし、様々な認証方式に対応している Dovecot を今回採用した。Dovecot は、ディスク使用容量制限機能等

注8) POP before SMTP : 電子メールの送信を行う際のユーザー認証の一つ。

注9) SMTP-Auth : メール送信に使うプロトコルである SMTP にユーザー認証機能を追加した仕様。

注10) POPrelay : POP before SMTP 機能を実装するために、POP 接続を受信しメールサーバにデータ中継を実施するプログラム。

●表-2 主な使用ソフトウェア一覧●

ソフトウェア名	概要
OS・商用ソフトウェア	
Red Hat ^{※1)} Enterprise Linux ES4	基本 Linux OS 変換機構。
三井造船 ScanMail Symantec AntiVirus Scan Engine (SAVSE)	ウイルススキャン機能を提供するために設計されたモジュール型のウイルススキャンエンジン。
CatchMe@MAIL	Web ブラウザ上で電子メールの送受信を可能にする Web メールサーバ。
主要フリーソフトウェア	
Postfix	高速さ、管理の容易さ、安全性を目指して作成されているメールサーバソフトウェア (MTA)。
Dovecot	高速で、安全で、柔軟性があり、セキュリティを第一に考えられている、オープンソースの Linux/UNIX ^{※2)} システム向けの IMAP・POP サーバ。
OpenLDAP	Lightweight Directory Access Protocol (LDAP) のフリー実装であり、ディレクトリデータベースへアクセスするためのプロトコル。
Berkeley Database	オープンソースのスタンドアロンデータベース管理ライブラリ。

※1 Red Hat は、米国その他の国で Red Hat, Inc. の登録商標若しくは商標である。

※2 UNIX は、米国およびその他の国におけるオープン・グループの登録商標である。

のオプション機能が豊富であり、今後の機能追加が期待されている。

(4) Web メール

旧メールシステムにおける Web メールは、IMAP プロトコルによる対応がされていなかった為、Web メールシステムは、いったんメールボックス上のデータを POP 受信し、別領域にデータを保持することで実現していた。その為、通常のメールスプール領域と Web メールデータ用スプール領域の二つが必要となり運用者にとって管理が複雑な状態となっていた。

よって、リプレースにおいては、管理面の容易な IMAP ベースの Web メールシステムを検討し、ユーザー情報を LDAP にて一元管理できる「CatchMe@MAIL^{※5)}」を採用した。

「CatchMe@MAIL」は、サーバライセンスタイプであるためユーザーライセンスタイプに比べ低コストでの運用が可能である。さらに、サービス対応の携帯電話および携帯情報端末 (PDA) からのメール送受信も行

うことが可能である。

「CatchMe@MAIL」のユーザー情報の管理においては、通常ノベル社の「eDirectory（商用版：LDAP ディレクトリサービス）」と連携して実施する。

しかし、今回 LDAP におけるユーザー管理においては、ウイルスチェックサーバやメールボックスサーバでも利用しているフリーソフト「OpenLDAP^{※6)}」を採用し、ライセンス費用削減を図った。フリーソフトを採用することで、構築時における導入負荷（調査等）は商用版 LDAP を利用するよりも高くなるが、ライセンス費用が不要になり運用コスト削減が図れ、トータルでのコスト削減に繋がっている。

(5) ストレージ

ストレージにおいては、メールデータ保持部分における Read / Write 性能の向上と冗長化を図るために、他社メールサービスでも運用実績があった「ETERNUS NR1000 F3040^{※7)}」を採用した。「ETERNUS NR1000 F3040」は、コントローラ部のクラスタ構成による冗長性や運用状況に応じたディスク増設による拡張性に優れている。また、本シリーズについてはトラブル発生時の迅速なサポート力に定評がある。

4 システムの特長

(1) メール送受信における特長

メール送受信経路概要図を図-2 に示し、それぞれのサーバにおける特長を記す。

1) SPAM チェックサーバ

SPAM チェックは、外部から到達するメールと内部から配送されるメールに対して、外部データベースとの連携により SPAM 有無チェックを実施する。SPAM チェックは、ウイルスチェックサーバ上に設置している LDAP と連携して契約ユーザーのみ機能する仕組みとなっている。

2) ウイルスチェックサーバ

ウイルスチェックサーバでは、サーバ内に 6 種類の MTA を実装し、受信者アドレス・送信者アドレス毎に SAVSE を経由してウイルスチェック有無を判定し、またキーワードフィルター制御も実施している。さらに、メールボックスサーバにデータを中継する POP リレー機能 (POPrelay) を実装し、POP before SMTP を実現している。6 種類の MTA は次のように分類される。

- a) SMTP-Auth / TLS ユーザー送信専用 MTA
- b) POP before SMTP ユーザー送信専用 MTA
- c) 受信者・送信者アドレス経路選択 MTA
- d) ウイルススキャン専用 MTA
- e) メールボックス経路選択 MTA
- f) 標準 MTA

3) メールボックスサーバ

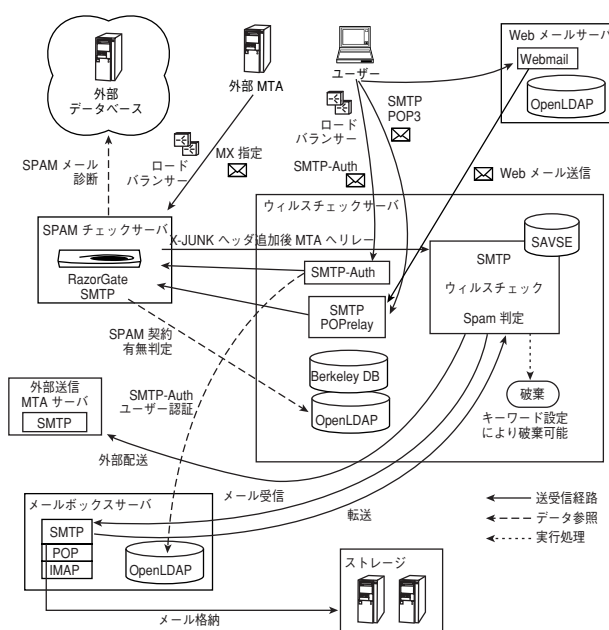
メールボックスサーバによるメール配送は、Postfix と Dovecot の連携にてメール格納処理を実施すると共にユーザー毎に設定しているメール転送処理を実現している。

(2) 冗長性の確保

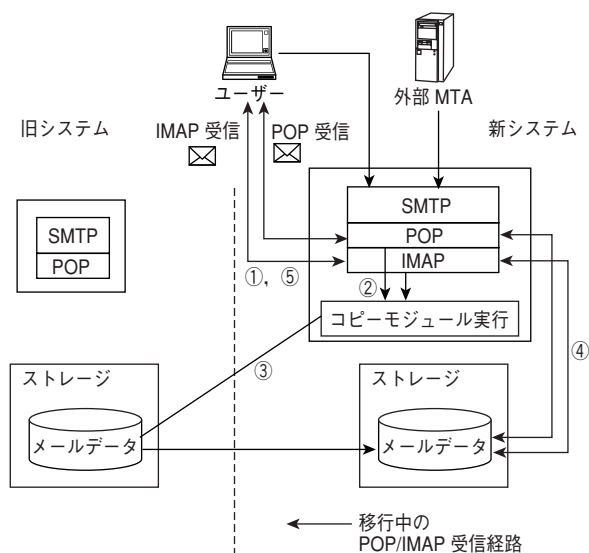
全てのサーバは冗長化しているが、同じサービスのサーバは可能な限り同一構成としている。

これにより二つのメリットをもたらしている。一つはシステムコピーによる構築期間の短縮であり、もう一つは構成が同一のためロードバランサーを用いて、負荷状況に応じて機能における分散比率を自由に変更できる点である。それにより、負荷状況に応じたサーバ増設も可能となり、余裕のあるシステム構成を実現した。

例としてウイルスチェックサーバは SMTP 機能と POPrelay 機能と LDAP 機能があり、全 8 サーバで運用している。負荷状況に応じてそれぞれを 6 : 2 や 5 : 3 のように分散比率を変えることで SMTP と POP の負荷を分けることができ、メール配送遅延や



●図-2 メール送受信経路概要図●
(Fig.2-E-mail transmission and reception path diagram)



●図-4 メールデータ移行の仕組み●
(Fig.4-E-mail data migration mechanism)

6 リプレース後の評価及び今後の展開

システム導入後、構築前に発生していたメール配送遅延は収まり、顧客クレームもゼロを継続している。またメール移行におけるメールサービス停止時間の短縮やトラブルのないスムーズな移行について、顧客から高く評価された。

今後は、メールシステムの脅威となるスパム対策において IP Reputation^{注11)} や SPF^{注12)} 等の送信者制限機能の導入を進めることで、システム全体の負荷軽減対策を図り、顧客におけるトータルコスト削減に貢献したい。

注11) IP Reputation : 送信元の IP アドレスにおける危険率を判定し、判定に応じた処理を実施するスパムメール撃墜方法。

注12) SPF : メール送信元アドレスの偽装を防止する技術。

本メールシステムで構築した内容は、某 ISP 様のような大規模メールシステムに有効だけでなく、一般中小企業ユーザーとしても十分なパフォーマンスが得られるため、小規模メールシステムとして他社展開も今後考えていきたい。

7 むすび

法人・一般家庭のメール利用シーンは、今後も様々な拡張機能を蓄えながら活発になると思われる。しかし、活発に利用される反面、メール詐欺、機密情報漏洩といった危険を含んでいる。

メールシステムの構築から運用までを担う我々としては、ユーザーが安心して利用できるメールシステムを継続提供することが重要であり、またそれに対しての費用対効果を考慮しなければならない。

当社では、今後も世の中の移り変わりに敏感に反応し、顧客の求める要望をシステムに取り込むことで、より機能性の高いシステムの提案・構築を実施していきたい。

参考文献

- 参1) RazorGate 紹介ページ
<http://www.mirapoint.co.jp/products/razorgate.php>
- 参2) Symantec アンチウイルスエンジン紹介ページ
<http://www.msr.co.jp/kikan/niservice/scanmail.html>
- 参3) Postfix 紹介ページ
<http://www.postfix-jp.info/>
- 参4) Dovecot 紹介ページ
<http://www.dovecot.org/>
- 参5) CatchMe@MAIL 紹介ページ
<http://www.canon-js.co.jp/pkg/Webmail/catchme/>
- 参6) OpenLDAP 紹介ページ
<http://www.openldap.org/>
- 参7) ETERNUS NR1000 F3040 紹介ページ
http://storage-system.fujitsu.com/jp/products/nwdiskarray/nr1000f/download/pdf/nr1000_f3040.pdf