金沢大学理工研究域におけるメールシステムの構築

○浜 貴幸

金沢大学 理工研究域

概要

本学では平成 20 年に改組が行われ、理学部および工学部は統合され理工学域（研究域）となった。今回この新組織において、新たにメールサービスを開始することとなり、その構築を担当した。構築するにあたり、管理者と利用者双方において簡便であることと、旧来のメールシステムにとらわれないサービスの提供を目指して、その基軸をマルチインスタンスを使った MTA と MSA の分離による設定の簡素化、ウェブインターフェイスを使ったアカウント管理、学内外を問わないシームレスなアクセスを可能とすることの 3 点に置いた。

1 設計方針

今回構築したシステムは、全くの新組織が対象であるため、過去の資産やシステムを引き継ぐ必要がなかった。そこでシステム構成については、たとえば既存のシステムをリプレースする際に、旧システムの仕様が障害となり採用しにくいような、比較的新しい方針を積極的に取り入れることとした。下記は構築にあたり検討した基本方針である。また、本システムの概要をメールの配送を中心に図 1 に示す。

- POP および POPS サービスの提供
- IMAP および IMAPS サービスの提供
- TLS (SSL) を使用した学外 MUA からの直接アクセスを可能とする
- MUA からの SMTP ポート (25/tcp) を使用したメール送信は受け付けない
- Submission と SMTPS サービスを提供
- Submission は STARTTLS を必須とする
- Submission および SMTPS は SMTP 認証を必須とする
- MTA と MSA を分離して構築する
- メールアカウントはメール専用のバーチャルアカウントとする
- すべてのメールをウィルスチェックサーバにリレーする
- ユーザ管理はウェブインターフェイス (PostfixAdmin) で行う

1.1 MTA と MSA の分離

旧来ではメールの配送サーバを構成する上で、他のサーバから配送されるメールを受け取る MTA (Message Transfer Agent)と、ユーザのメールクライアント (MUA, Mail User Agent) から送信されたメールを受け付ける MSA (Message Submission Agent) は、同じ IP アドレスの SMTP (25/tcp) サービスで提供されてきた。しかしこの形態では、オープンリレーの防止や SMTP 認証の機能を取り入れる場合、設定やトラブル時の切り分けが複雑にることが多い。さらに、スパム対策として近年 OP25B (Outbound Port 25 Blocking) を実施する ISP や LAN が増加しており、出張時などの学外 MUA からのメール送信に支障がある。

MTA と MSA を分離し、別の IP アドレスでサービスする場合、それぞれを単機能のサービスとして設定することが可能である。基本的に MTA は他の MTA から自ドメイン宛へのメールを各メールボックスに配信す

るのみ、MSA は MUA からのアクセスを認証し、預かったメールを他の MTA に転送するのみである。

本システムで採用した Postfix において、このように MTA と MSA を分離する場合、バージョン 2.6 より実装されたマルチインスタンス機能[1]を使用すると容易に設定できる。これにより、各インスタンス間で設定ファイル群を分離できるため、設定時やメンテナンス時の見通しの良さを確保できる。

1.2 学内外を問わないシームレスなアクセス

本学では、ユーザが学外のネットワークから直接アクセスできるメールシステムはあまり使われておらず、学外でのメール利用には無料のウェブメールなど第三者のサービスに転送するか、VPN を介して行われている。しかし、業務上秘匿性の高いメールを第三者のシステム上に保管することは好ましくなく、また VPN についても手続きが面倒であったり、外部の LAN への VPN 接続を禁止しているネットワークも存在しうる。

このため本システムでは、ログインパスワードや学内のメールが平文で学外の経路を通過することは好ましくないと考え、TLS (SSL) を使用したアクセスのみ、学外 MUA の直接接続を可能とした。これにより、対応する MUA を使用するユーザは、学内外を気にせずメールシステムを利用することができる。また、OP25B への対応として Submission (587/tcp) と SMTPS (465/tcp) を用意し、TLS (SSL) および SMTP 認証を必須とした。

1.3 ウェブインターフェイスを使ったアカウント管理

ユーザの追加などの管理作業は、旧学部のシステムでは、担当の事務職員がコマンドラインにて行っていた。しかしそのような環境では、操作ミスや偶発的な例外への対応困難など、いくつかのトラブルをまれに引き起こしていた。そこで本システムでは、PostfixAdmin を使用しこれらの管理作業をすべてウェブインターフェイスから行うようにした (図 2、図 3)。また、ユーザ自身によるパスワードの変更や、転送設定についても同様にウェブで行うこととした。PostfixAdmin を導入した場合、ユーザアカウントをシステムアカウントとは全く分離された、メール専用のバーチャルアカウントとすることが容易に実現できるという利点も得られる。

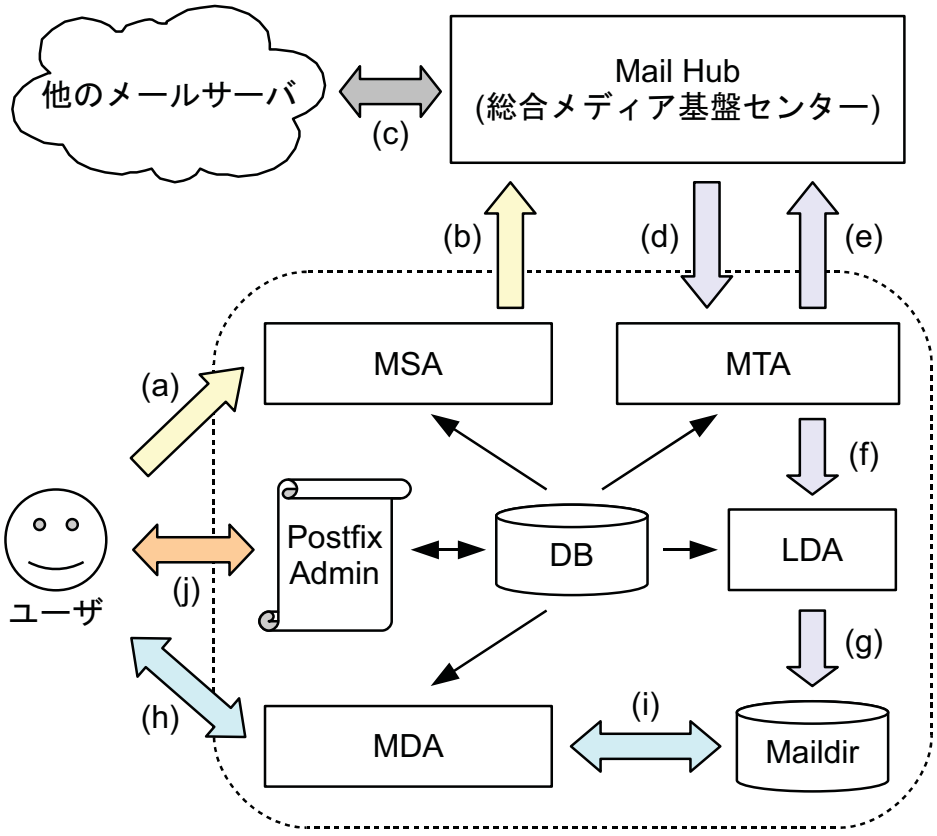

図 1. システム概要

2　システム構成

システムはサーバ機 1 台で構成した。ハードウェアについて、CPU は 4 コアのものを使用し、メモリは 8GiB 搭載した。また、HDD は 1TB のものを 2 台使用し RAID1 を設定した。表 1 に主な使用ソフトウェアを示す。

表 1. 主な使用ソフトウェア

OS	FreeBSD 7.1-RELEASE
MTA, MSA	Postfix 2.6
MDA	Dovecot 1.2
RDBMS	MySQL 5.1
HTTPd	Apache HTTP Server 2.2
アカウント管理	PostfixAdmin 2.3

3　アカウント管理

各ユーザのアカウント管理には PostfixAdmin を使用し、すべてのメールアカウントをバーチャルドメイン上のバーチャルアカウントとした。PostfixAdmin へのアクセスは HTTPS に限定し、またセキュリティーホールへの不安から、学外からのアクセスを禁止した。管理用アカウントは管理者 1 名につき 1 アカウント発行し、担当するドメインのアカウントのみ操作できるよう設定した。

アカウントの登録時や削除時には、PostfixAdmin はデータベース (DB) の情報を操作するのみである。特にアカウント削除時は、メールデータがそのまま残されるため問題となるケースが考えられる。このためアカウント削除時に実行される、メールデータも削除するなどのスクリプトを用意する必要がある。本システムでは、そのようなスクリプトで当該のメールデータを別パーティションに移動し、一定期間後に削除している。

アカウント情報を格納する DB 管理システムには MySQL を採用した。MySQL においては、パフォーマンス向上のためクエリキャッシュを使用するよう設定した。本システムのようなメールシステムでは、DB の書き換えはほとんど無く、メール配送の各局面で DB 読み出しが多く発生するため、クエリキャッシュが非常に効果的である。本システムの場合、そのキャッシュヒット率は約 96%に達する。

図 2. アカウント登録画面

図 3. アカウント一覧画面

4　メール配送

本システムではメール配送用ソフトウェアに Postfix を採用し、そのマルチインスタンス機能を用いて MSA と MTA の分離を行った。それらの機能と動作ついて、図 1 をもとに紹介する。

4.1　MSA

ユーザがメール送信を行う場合、MSA の Submission もしくは SMTPS のサービスを使用する（図 1

(a))。MSA は SMTP 認証を行い、メール送信を承認する。メールを受け取った MSA は、すべてのメールを本学のメールハブ（総合メディア基盤センター）にリレーする（図 1 (b))。メールハブではウィルスチェックが行われ、その後さらに他のメールサーバへ MX 配送される（図 1 (c))。ここで送信されたメールが本システムのドメイン宛であっても、必ずメールハブへ送られウィルスチェックされ、MTA へ返されることになる（図 1 (d))。これは MTA と MSA に別の IP アドレスを使用し、MX レコードに MTA を登録することで実現している。

また、MSA における SMTP 認証のバックエンドには、Dovecot SASL を使用した。SMTP 認証には、Cyrus SASL の使用が一般的であるが、設定が煩雑であり、DB に格納されたパスワードが Crypt 形式の場合、うまく動作させることができなかった。Dovecot SASL は設定が非常に簡単であり、対応するパスワードの保存形式が SSHA や SHA-256 など豊富に用意されている。

MSA の動作に求められる要件は RFC 4409 に示されている[2]。そこで必須とされているもののうち、SMTP エンベロープにおけるドメインがすべて FQDN (Fully Qualified Domain Name) であると保証することと、SMTP 認証が必須であることは、Postfix 2.6 においてはデフォルト設定では有効にならないので注意が必要である。また、メールヘッダの補完もデフォルトでは行われないので、MSA にて行うことが推奨される。

4.2 MTA

本システムの MTA は自ドメイン宛のメールのみ受信し、リレー動作は一切行わない。

メールハブから MTA に配送されたメール（図 1 (d)) は、まず「virtual_mailbox_domains」の設定から自ドメイン宛のものか判断され、その後「virtual_alias_maps 」の設定に従いアカウントエイリアスの解決や他ドメインへの転送が行われる（図 1 (e))。このときメールの転送時も、MSA と同様にすべてメールハブへ送信される。エイリアス解決の結果、最終的に各アカウントのメールボックスに格納される自ドメイン宛のメールは、「virtual_mailbox_maps」の設定によりアカウントが実在し有効であるか確認される。アカウントが有効であると確認されたメールは、プロセス間通信にて LDA へ送られる（図 1 (f))。

4.3 LDA

MTA にて受け取ったメールを、最終的にメールボックスへ格納（ローカル配信）するのが、LDA (Local Delivery Agent) である。メールを受け取った LDA は、DB より各アカウントのメールボックスのディレクトリ位置を取得し、メールを格納する（図 1 (g))。メールの格納には Maildir 形式を採用した。

ローカル配送は前述の MTA (Postfix) でも行えるが、本システムでは Dovecot LDA を使用した。ローカル配送に Dovecot LDA を使用する利点は次の通りである[3]。

- メールボックスのインデックスのリアルタイム更新
- Dovecot による柔軟な Quota の実現
- Quota のための maildirsize ファイルのリアルタイム更新
- Sieve のサポート

ローカル配信を MTA で行った場合、上記のインデックスや maildirsize ファイルの更新は、ユーザが MDA を介してメールボックスにアクセスした際にメールボックス全体をスキャンして行われるため、パフォーマンスの点で不利である。また、本システムのようにバーチャルアカウントの Maildir にて Quota を導入する際、通常の Postfix ではこれが実現できず、別途パッチ[4]を用意する必要がある。

5 MDA

MDA (Message Delivery Agent) には Dovecot を採用した。Dovecot は IMAP の仕様にもっとも準拠しているサーバソフトウェアの一つで、高いセキュリティとパフォーマンスが謳われている[5]。

MUA に対する MDA のサービスには POP、POPS、IMAP および IMAPS を設定した。MUA からアクセス（図 1 (h)) を受けた MDA は DB よりアカウント情報を読み込み、その後認証された当該アカウントのメールボックスとの橋渡しを行う（図 1 (j))。

6 Quota

IMAP を通じての大量アップロードや、長期間の放置、サーバにメールを残す設定などサーバのディスクスペースの圧迫を防ぐため、各アカウントのディスク使用量に上限を設ける。Quota はファイルシステムの機能ではなく、Dovecot のプラグインを使用し、各ディレクトリの maildirsize ファイル[6]を管理させることで実現できる[7]。各ユーザの制限値は DB に格納されており、Dovecot LDA はメールボックスの変化に応じて maildirsize ファイルを更新し、DB 上の制限値を参照してディスク使用量を制限する。

使用量に関するユーザへの通知は、設定した使用量を超えた場合、当該ユーザにメールを送信するよう設定した。設定は Dovecot の設定ファイルの「quota_warning」に閾値と、その超過時に実行するスクリプトを指定する。本システムでは、DB に設定された制限値と使用割合を示し、当該ユーザにディスク使用量の削減を促すメッセージを送付している。

7 メーリングリスト

7.1 学内用メーリングリスト

学内の各種業務用メーリングリストにはエイリアス機能を使用した。リストは表計算などの別ファイルで管理し、更新時にはコピーアンドペーストで上書きする運用とした。また、メーリングリスト用のドメインを個人ユーザ向けのものとは別にし、学外向けの DNS にはその MX レコードを登録しないこととした。これによりメーリングリストは学内のメールサーバを経由しなければ到達できなくなり、学外者からの投稿防止や、本来学内のみに向けた情報が、不意に学外のネットワークで流通することを抑制する効果を期待できる。

7.2 ユーザ通知用メーリングリスト

メンテナンス等でシステムを停止する場合、全ユーザに通知を行う。通知は管理者がメーリングリストと同様に特定のメールアドレスに通知文を送信する。ただし、リスト更新の手間を省くため、通知用メールアドレスのエイリアスに、すべての有効なユーザアカウントを返す SQL 文を用意し、動的にリストの生成を行う。

8 その他

8.1 TLS 設定

Postfix、Dovecot ともに TLS において使用する暗号リストは、CRYPTREC の電子政府推奨暗号リスト[8]に準拠した。Postfix では、EDH (Ephemeral Diffie-Hellman) 鍵交換を使用した暗号化を行う際、その DH パラメータにビルトインの値を使用する。この状態では、第三者によるブルートフォースアタック成功の可能性が排除できないため、独自にパラメータを設定することが推奨される[9]。

8.2 バックアップ

管理上の操作ミスに対するフェイルセーフとして、すべてのメールデータを毎日バックアップを行っている。バックアップツールは rdiff-backup を使用した。rdiff-backup は逆差分方式でバックアップ対象のコピーを行うため、直近のバックアップデータは純粋なミラーリングとなる。そのため、直近からのリカバリーが容易で扱いやすい。また DB についても、mysqldump により定期的なバックアップを行う。

8.3 ログ統計

メールの流量と使用実績の把握のため、Postfix のログの統計を管理者にメール通知している。統計処理には pflogsumm を使用し、インスタンスごとに行う。

8.4 無効アカウントの取り扱い

PostfixAdmin では、一時的にアカウントを無効にすることができる。しかし無効にした場合、PostfixAdmin のドキュメントにあるような設定のままでは、MTA からはそのアカウントが存在しないように見えるため、ユーザ不明のエラー (550 5.1.1 User Unknown) を返してしまう。この場合、ユーザが一時的に休職するなど、アカウントを残したまま使用停止にするような運用では、メールの送信者に余計な混乱を与える可能性がある。

そこで本システムでは、MTA の宛先確認の段階で、そのアカウントが存在しかつ無効に設定されている場合には、ユーザ不明とは別のエラー (550 5.2.1 Mailbox temporarily disabled) を返すようにした。ここで SMTP のレスポンスコードはメッセージの内容から 450 が適当であると思われるが、上流の MTA におけるリトライ期間内にアカウントが有効化されるケースは少ないと考え、即時に送信者へエラーメールが返されるよう 550 とした。また拡張ステータースコードについても、RFC 3463 に照らせば 4.2.1 となるが[10]、こちらも上記の理由から 5.2.1 とした。

9 まとめ

現在、各教職員には旧組織のアカウントが行き渡っているため、本システムのアカウント取得者は全体の 3 割、旧システムから移行して常用するユーザは 1 割程度に留まっている。しかし今後、旧組織の廃止に伴う旧アカウントからの移行推進や、旧システムの組み入れが予定されており、サーバ負荷やディスク使用量の増加が想定される。今回構築したシステムでは、MTA や MSA、MDA、LDA などのメールシステムにおける各機能を、それぞれ独立した単機能のサービスとして扱ったため、それぞれを別マシンに分散させてサービスするよう移行することが容易となっている。これにより、将来の規模拡大に対してある程度のスケーラビリティを担保することができた。

また、アカウント管理の業務負担軽減やユーザ設定の簡便化を PostfixAdmin の導入により実現し、TLS による安全でシームレスなアクセス手段の提供という当初の方針も達成できた。これらは現在、アカウント管理担当者や各ユーザから好評を得ており、さらに今後、アクセス手段の多様化と利便性向上のため、ウェブメールのインターフェイス導入も計画している。

参考文献

[1] http://www.postfix.org/MULTI_INSTANCE_README.html

[2] http://www.ietf.org/rfc/rfc4409.txt

[3] http://wiki.dovecot.org/LDA

[4] Postfix VDA, http://vda.sourceforge.net/

[5] http://www.dovecot.org/

[6] Maildir++, http://www.inter7.com/courierimap/README.maildirquota.html

[7] http://wiki.dovecot.org/Quota/1.1

[8] http://www.cryptrec.go.jp/list.html

[9] http://www.postfix.org/TLS_README.html#server_cipher

[10] http://www.ietf.org/rfc/rfc3463.txt