神戸大学におけるメールサービスの Exchange Online への移行

鳩野 逸生 [1)], 伊達 弘典 [1)], 辰奥　俊宏 [2)]

1) 神戸大学 DX・情報統括本部 情報基盤センター, 2) 神戸大学 情報推進課

hatono@kobe-u.ac.jp

The mail system migration to Exchange online in Kobe University

Itsuo HATONO[1)], Hironori DATE[1)], Toshihiro TATSUOKU[2)]

1) Information Infrastracture and Digital Transformation Initiative Headquarters, Kobe University,
2) IT Promotion Devision, Kobe University

概要

神戸大学においては，2022 年 9 月に Postfix をベースとしてメールシステムから Microsoft365/Exchange Online を主として用いたシステムに移行を行った．本稿では，神戸大学におけるメールサービスの概要と移行後のシステムにおける実装について述べる．

1　はじめに

神戸大学においては，2022 年 9 月に Postfix を用いたオンプレミスのメールシステムから Microsoft365/Exchange Online[1] を用いたシステムに移行した．本稿では，移行前と移行後のメールシステムにおけるサービスの概要と，Exchange Online における実装について述べる．

2　Exchange Online への移行の背景

神戸大学のメールシステムは, 6 年のリースで契約している神戸大学教育研究用計算機システムの一部として提供されて来た. 一方，電子メールを取り巻く環境はかなり激しく変化しており, 2016 年に導入した前システムのメールサービスにおいては，迷惑メールやウイルスメールの判定を行うためのアプライアンスの機能の陳腐化や，設定の変更や運用では解決が困難な配送のトラブルが多発していた．

このような状況の下で，2022 年 9 月に更新予定のメールシステムにおいては, Microsoft365 の包括契約の範囲内で利用できる Exchange online を用いてメールシステムの再構築を行うこととしたものである．なお，神戸大学においては，Microsoft364 Education A3 と A5 セキュリティで契約している．

3　旧メールシステムにおけるサービスの概要

3.1　個人メール

- 学生ユーザ:
  - 学籍番号を用いたメールアドレスを付与.
  - メールアドレスの alias を設定可能 (1 つのみ)
  - 転送先メールアドレスを 3 つまで設定可能
- 教職員ユーザ:
  - メールアドレスを 4 つまで取得可能 (46 のドメインから選択可能)
  - すべてのメールアドレスは変更可能
  - 取得した各メールアドレスについて転送先メールアドレスを 3 つまで設定可能

3.2　メーリングリストサービス

メーリングリストソフトウェアである fml Ver.4 を利用したサービス.

- 事務用メーリングリスト
  - 事務の各係等の単位で発行 (約 300 件)
  - ユーザ管理システムにおけるユーザ属性の変更 (異動など) に同期してメーリングリストのメンバーを自動更新機能
- 一般用メーリングリスト
  - 学内教職員の申請により作成 (約 500 件)

3.3 メールサーバホスティングサービス

部局・学部等独自のメールドメインの利用を希望する場合 (15 件) に提供するサービスである．ドメインの管理者が，メールアドレスとアカウントを発行する機能を実装している．

3.4 メール中継サービス

- **発信専用:**
  メールを発信する必要がある情報システムやデバイスに必要なメールの中継機能を提供
- **送受信:**
  学内に設置されているメールサーバにおけるインターネットからのメールの送受信をメールゲートウェイを経由して中継するための機能を提供

4 更新後のメールシステムの概要

本節では，旧メールシステムにおいて実現していたメールシステムの各機能の，Exchange Online/Microsoft365 における実装および設定等をサポートするためのサーバの構成について述べる (図 1).

4.1 個人メールサービス

Microsoft365 包括契約におけるアカウント発行の制約により, 学生・教職員 1 名あたり 1 つのアカウントしか発行できないため，以下のように Exchange Online の機能を用いての実装とした．Microsoft365 のアカウントは，神戸大学教育研究用計算機システムにおける統合ユーザ管理システムにおいて，ユーザが新規に作成される場合 (学生ユーザ) あるいは，ユーザが初期設定を実施した場合 (教職員ユーザ) に作成されるが，各ユーザが利用するメールアドレスとは別に発行している[*1].

- Microsoft365 アカウント自体もメールアドレスとして機能するが，4 つまで取得可能なアドレスの中の 1 つを Microsft365 アカウントにおける primary メールアドレスとして登録する．残り 3 つ取得可能なアドレスに関しては，shared mail address を生成し，Microsoft アカウントを利用可能なアカウントとして登録することにより実現した[*2]．また，取得可能なメールアドレスのドメインと数を管理するため，メールアドレスの取得・変更・削除は，統合ユーザ管理システム上で操作するような実装となっている．
- 転送先の設定は，Exchange Online における Outlook on the web において設定することとした．
- 旧メールシステムにおいては，メール受信プロトコルとして imap/pop3 を許可していたが，Exchange Online 移行時に, imap のみに制限を行った．

4.2 メーリングリストサービス

メーリングリストサービスは，Exchange Online では同等の機能を実装することが難しいため[*3]，メーリングリストソフトウェア mailman[2] を用いて旧メーリングリストサービスと同等の機能を実装した．

メーリングリスト宛のメールは, Exchange Online で受信し，Exchange Online におけるフロールールで記述して，メールゲートウェイを経由してメーリングリストサーバへと転送している．メーリングリストサーバから発信されるメンバー向けのメールは, Exchange Online に転送されて配送される構成となっている．

4.3 メールサーバホスティングサービス

個人メールアドレスの場合と同様に, 部局・学部独自のドメインをもつメールアドレスのために Microsoft365 のアカウントを発行することができないため，shared mail address を用いた実装とした．ただし，各ドメインの管理者が各ドメインにおけるアドレスの発行を可能にするため，shared mail address の作成および利用するユーザの Microsoft アカウントを登録するための Web ブラウザで利用できる GUI を処理するためのメールサーバホスティング管理サーバを構築している．

4.4 メール中継サービス

学内外のメール発信元から送受信を受け付けるためのメールサーバを学内に構築することにより実現している．Exchange Online において，Oauth2 などの認証が行えない機器からのメールを受け付けるためには，サーバ証明書の登録が必要などの制約があるためである．

[*1] クラウド ID と呼んでいる．

[*2] Exchange Online においては，各アカウントに複数のメールアドレスを alias として登録できるが，各アカウントのメールスプールに入る前にヘッダを書き換えてしまうため，bcc: などで送信された場合，primary メールアドレスに対して送信したものか, alias として登録されたメールアドレスに送信したものか区別できなくなるため, shared mail address を用いた実装とした．

[*3] Microsoft365 の配布グループを用いるとメールの配送は実現可能であるが，従来のメーリングリストソフトウェアが持っている Subject におけるタグの追加などができないため, メーリングリスト機能は Exchange Online に移行しなかった．

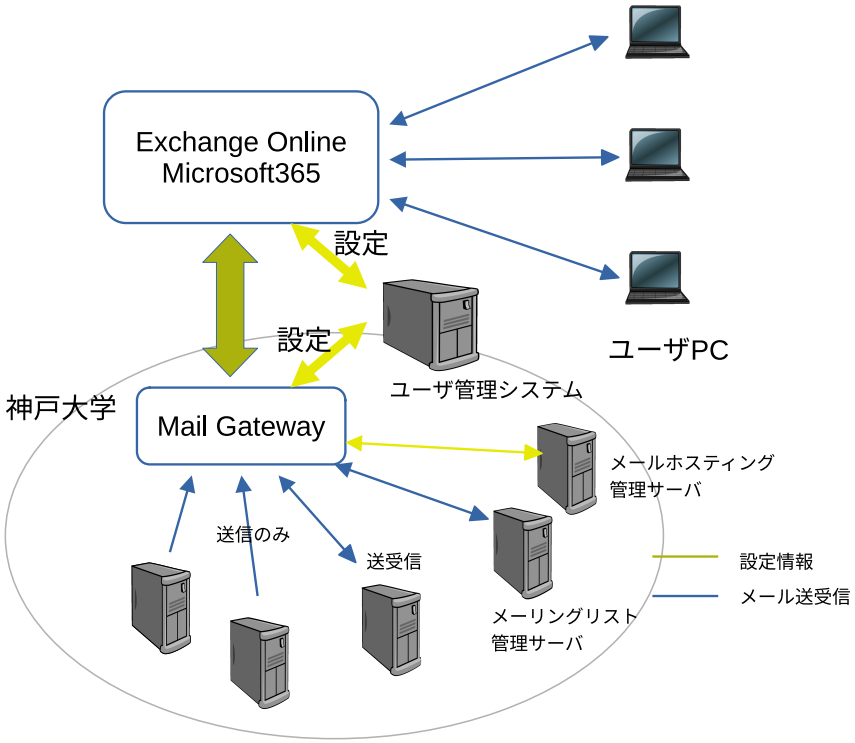

図 1　メールシステムの構成

5　旧メールシステムからの移行

旧メールシステムから Exchange Online への移行においては，移行前までに利用していたテナントとは別に移行後に利用するテナントを作成し，以下の手順で実施した．

1. 移行後に利用するテナントを新規に作成し，利用予定ドメインを Exchange Online へ登録
2. ユーザ管理システム上の情報を元にユーザのアカウントを Microsoft365 上に作成
3. 旧メールシステム上に登録されていたメールアドレスをアカウントに同期

旧システムにおけるメールスプールの移行は必要な時間を考慮して実施していない[*4]．

6　開発時の主な問題点

6.1　メールドメインの登録

本メールサービスにおいては，従来十数年に渡って利用してきたメールドメインであったことと，移行するドメインの数が 50 を超える (メーリングリスト利用分を含む) あったため，移行に際して以下の問題が発生した．

- 過去に Microsoft のサービス利用のために登録されたアカウントの一部がドメインに対する管理権限を保持していたため, Exchange Online の承認ドメインとして登録できなかった．そのため, 以前に登録されているユーザ ID(メールアドレス) の変更をお願いする必要があって相当の時間を要した[*5]．

6.2　メール送信における送信アドレスチェック

現システムの構築途中で，Exchange Online の送信においては，エンベロープ From だけでなく ヘッダー From にも設定されたメールアドレスに関して，Exchange Online 上で認証が成功しかつ発信権限が設定されていないとエラーになることが判明した．

従来のメールシステムにおいては，メーリングリストのメールアドレスをヘッダー From に設定して個人のメールアドレスが表に出ないようにしてメールの送受信を行うという運用を行ってきたが，別サーバで管理しているメーリングリストのアドレスに対して Exchange Online 上で権限設定されていないため送信エラーとなる．メーリングリストのメンバに対して

[*4] その代わり旧システムのメール受信サーバを 1 年程度保持した．

[*5] DNS の設定権限を保持している場合は，強制的に変更することは可能である．

メーリングリスト管理サーバの内にあるメンバー情報を Exchange Online 上のユーザの権限設定に反映することは現実的でないため，個人のメールアドレスと異なるメールアドレスをヘッダ From に設定したメールの発信を可能にするための送信専用サーバを設置している[*6].

6.3 メールボックスにおけるインボックスルールによる多段転送の制限

現メールシステムにおける転送は，転送設定は 1 アドレスのみで 2 つ目以降のアドレスは，はメールボックス内のインボックスルールでリダイレクトを設定することを前提としている．ところが，10 段以上のリダイレクトを設定しているユーザが存在し，旧メールシステムと同様な動作をしないことが判明した. 旧メールシステムは Postfix をベースにしており，転送の段数に制限は存在していない.

この問題に対しては，対策を行うことが難しいため，ユーザサイドに別手段で対応することを依頼している[*7].

7 移行の効果

2022 年 9 月に移行後，約 1 年間運用してきているが大きな問題はなくメールは配送されている.

7.1 情報セキュリティ対策

旧メールシステムにおいては，ウイルスメールやフィッシングメールの判定が十分に機能していなかったため，頻繁にフィシングメール上の URL をクリックしたことによる Firewall による検知が発生していたが，移行後は激減した．Exchange Online は，Microsoft365/Defender により, サイン・インのチェックが行われるとともに，メール自体のセキュリティチェックを実施したり，メール中に含まれる URL を変換してチェックするなどの処理を行う効果が出ているものと推察される.

8 課題

8.1 Exchange Online のフル機能を利用可能なソフトウェア

Exchange Online は，Web ブラウザ上で利用可のな outlook on the web 以外に，パソコン，スマートフォン, タブレット上のアプリケーションで利用可能であるが，すべての機能を利用できるのは事実上 Outlook だけである．特に，MacOS, IOS 等で利用可能な mail.app は，shared mail address の利用が困難である. また, Thunderbird 等のソフトにおいては, shared mail address を利用するためには通常以上に複雑な設定が必要であるなどの問題がある.

8.2 Defender を用いた監視

Microsoft365/Exchange Online は, Microsoft365 Defender を通して, Junk mail，virus mail の判定などのチェックを行っているが，誤判定もあり，定期的にチェックが必要である．さらに, Microsoft365/Defender の管理者コンソールは複雑であるため操作には熟練が必要である.

8.3 メーリングリスト機能

現システムにおいては，旧システムからの移行を考慮してメーリングリストサーバを別途学内に構成したが，送信者の認証が厳格化していった場合メーリングリストソフトウェアによるメールヘッダの書き換えによりメールを詐称して不正に送信されたものであると判定される確率があがって行く可能性がある．将来的には，メーリングリストの機能も, Microsoft365/Exchange Online の機能で実装することが望ましいと考えられる.

9 終わりに

本稿では，神戸大学におけるメールシステムの Microsoft365/Exchange Online への移行について述べた. 旧メールシステムでは, 各ユーザが自由にメールアドレスを設定できるなど自由度が高いサービスを提供していたが，一方でそれが Exchange Online への移行の際の困難さを上昇させてしまったことも否定はできない.

今後は，メーリングリストサービスを Microsoft365/Exchange Online の機能で実現するとともに, メールサービス自体を簡単化することによりベースとなるメールシステムを変更した場合でも移行が可能になるようにすることが必要であると考えられる.

参考文献

[1] Microsoft: Exchane Online, https://microsoft.com/ja-jp/microsoft-365/exchange/exchange-online (2023 年現在)

[2] Mailman, Mailman, the GNU Mailing List Manager, https://list.org/, (2023 年現在).

[*6] セキュリティ上の問題を軽減するため，神戸大学内からのみ発信可能としている.

[*7] 別途， teams を利用することを推奨している.