Vol.2020-IOT-50 No.9
2020/7/10

九州大学における独自運用メールサービス集約のためのシステム開発

嶋吉 隆夫[1,a)]　笠原 義晃[1]　清家 史郎[2]　藤村 直美[1]

概要：九州大学では全構成員にクラウドメールサービスである Exchange Online を用いた全学基本メールサービスを提供しているが，歴史的経緯から，それとは独立に学部や学科，研究室などで各自のドメイン名に対する独自のメールサービスが多数運用され，メールアドレスが発行されている．しかし近年は，独自運用のメールサービスでセキュリティ上の問題が起きることが多く，また，セキュリティ対策の負担も増加している．そこで九州大学では，独自発行メールアドレスを維持しつつ，独自運用されているメールサービスを全学基本メールサービスへと集約する取り組みを進めている．本稿では，Exchange Online の配布グループ機能を用いた独自発行メールアドレスの集約方法，および，集約したメールアドレスの管理機能を提供するために構築したシステムについて述べる．

Development of a System for Consolidating Individual Email Servers in Kyushu University

Takao Shimayoshi[1,a)]　Yoshiaki Kasahara[1]　Shiro Seike[2]　Fujimura Naomi[1]

1. はじめに

九州大学情報統括本部では，2009 年より九州大学全構成員に向けて全学基本メールサービスを提供している [1], [2], [3]．2018 年 12 月には，オンプレミスメールシステムから，Microsoft が提供するクラウドサービス Office 365（現 Microsoft 365）Education に含まれるメールサービス Exchange Online へと移行し [4]，サービスを運用，提供している．全学基本メールサービスでは，構成員の登録姓名に基づき，ドメインが学生は s.kyushu-u.ac.jp，教職員は m.kyushu-u.ac.jp とする全学基本メールアドレス（以下，全学アドレス）を一律に提供している．なお，全学基本メールサービスの利用者アカウントには，全学認証基盤 [5] により管理される全学共通アカウント SSO-KID[6] を利用している．

一方，九州大学では，学部や学科などに kyushu-u.ac.jp のサブドメインを申請に応じて発行しており，歴史的経緯により，学部，学科，研究室などの数多くのサブドメイン（以下，組織ドメイン）において，独自のメールサービスが運用され，組織ドメインのメールアドレス（以下，組織アドレス）が発行されている．これらの独自運用メールサービスは，そのための経費や人員を確保することなく，教員等が業務の傍らボランティアベースでメールサーバを運用管理している場合が多い．そのような事情もあり，これらのメールサーバには，セキュリティ上の課題がある．近年は，フィッシングメールによるパスワード等の詐取，メール添付ファイルによるマルウェアの配送，標的型攻撃，ビジネスメール詐欺など，電子メールがサイバー攻撃の主要な手段として用いられており [7]，電子メールサービスの運用にはセキュリティ対策が必須であるが，それはメールサーバ管理者にとって負担となっている．また，独自運用メールサーバでは，ソフトウェアの既知の脆弱性を放置したままサーバが運用されている場合や，管理者の異動などにより管理者不在のままサーバが稼働している場合などが

[1] 九州大学情報基盤研究開発センター
Research Institute for Information Technology, Kyushu University
[2] 株式会社 Fusic 技術開発部門
Technology Development Department, Fusic Co., Ltd.
[a)] simayosi@cc.kyushu-u.ac.jp

あり，実際に，アカウント不正利用によるメール送信や，サーバへの不正アクセスなどのセキュリティ事案が頻発している．九州大学情報統括本部では，全学基本メールサービスとは別にメールホスティングサービスも提供しており，このサービスで使用しているサーバは適切にセキュリティ保守が行われている．しかし，メールアカウントの管理はホスティング利用組織側の管理者に任されており，類推可能な初期パスワードが設定されたままになっている場合や，異動や退職などにより不必要になったアカウントがメール送信可能なまま放置されている場合などがあり，ずさんなアカウント管理に起因するアカウント不正利用が多数発生している．さらに，独自発行の組織アドレスの利用者は，全学基本メールサービスと独自運用メールサービスとの少なくとも 2 個以上のメールアカウントを持つことになる．九州大学では，異なる複数のアカウントに対して同一のパスワードを使い回すことは禁じられているが，現実には複数アカウントに同一パスワードを設定している事例も多く，脆弱な独自運用メールサービスから，全学共通アカウントのパスワードが漏洩して不正利用される場合もある．

そこで，九州大学情報統括本部では，独自運用メールサービスの集約による全学的なシステム運用コストの削減とセキュリティの向上を目的に，2018 年 11 月にメールサーバ集約タスクフォースを発足させ，独自運用メールサービスを全学基本メールサービスに集約することを目指して，施策の検討，実施を進めている．本稿では，独自発行メールアドレスを Exchange Online へ集約する方法についての検討，および，そのために開発したシステムについて報告する．

2. 基本仕様の検討

2.1 独自発行メールアドレスの継続性

独自運用メールサービスの集約を考えるとき，それらが発行している組織アドレスの処置は，非常に重要な問題である．メールサービスの集約に伴い組織アドレスを全学アドレスへと集約して廃止する可能性についても検討した．しかし，メールアドレスは全世界で一意な一種の個人識別子であり，連絡先として印刷物に掲載される場合も多い．特に研究者の場合は，出版された論文に掲載されたメールアドレスは，可能な限り継続してメールが到達可能であることが求められる．また，全学アドレスは各個人に割り当てられるものであるのに対して，学部や学科の組織ドメインでは一般的に，業務上の役職や掛，窓口などに対して割り当てられた組織アドレスも存在し，これらは業務上必要である．それゆえ，既存の組織アドレスは継続してメール受信できることを前提条件として検討を進めた．

メールアドレスについては受信できることとは別に，送信メールに利用できるかについても考える必要がある．近年は，迷惑メール対策，セキュリティ対策などの必要から，メール送信時にはメッセージサブミッションサーバ (MSA)[8] により SMTP AUTH[9] を用いて送信ユーザ認証を行うことが一般的であり，認証ユーザに対して送信メールヘッダの From フィールド [10] に利用できるメールアドレスを制限するサーバも少なくない．全学基本メールサービスで利用する Exchange Online でも，From フィールドに利用できるメールアドレスには制限がある．しかし，上述のような業務グループに割り当てられた組織アドレスについては，From フィールドに利用できる必要がある．そこで，組織アドレスについては，送信メールにも利用可能とする方法を検討した．

また，独自運用メールサービスの管理者に行ったアンケートでは，多くの組織ドメインにおいて，複数のメールアドレスへと転送するメールエイリアスに加えて，組織アドレスを持つメーリングリストを運用しており，メーリングリスト機能は必要という意見が多数寄せられた．そこで，メーリングリスト機能も提供することとした．

2.2 アカウント・アドレス管理

九州大学の構成員は全員が全学アドレスを割り当てられているので，組織アドレスを利用可能な構成員は複数のメールアドレスを利用可能であり，状況に応じてメールアドレスを使い分ける必要がある．これを単純に実現するには，メールアドレスごとにアカウントを発行する方法があるが，その場合，利用者が複数アカウントを管理する必要があり，セキュリティ上の懸念がある．そこで，大学全体で各構成員に発行する全学アカウントによって組織アドレスを利用できることを検討の前提条件とした．

一方で，組織アドレスは，学生の研究室配属，教職員の着任，プロジェクト立ち上げなどに応じて発行する必要があり，また，学外者に一時的に発行する場合もある．そのような個々の場合について，全学向けメールサービスを運用する組織で全てを対応することは，運用管理コストおよび人員の観点から非常に困難である．そこで，組織アドレスについては，組織ドメイン管理者による発行，変更，削除を実現することを考えた．

3. メール集約の方法

3.1 Exchange Online の仕様

九州大学の全学基本メールサービスが利用する Exchange Online の機能および制約について説明する [11]．Exchange Online では，利用者組織全体に 1 個のテナントと呼ばれる管理単位が割り当てられる．規定でテナントに割り当てられるドメイン名のほか，複数の独自ドメイン名を登録でき，登録ドメイン名はテナントのメールアドレスに利用できる．登録ドメイン名に対して，DNS の MX レコード [12] に設定可能なメール転送エージェントの完全修飾ドメイン

名が用意される．

利用者アカウントの管理および認証には，Azure Active Directory[13]（以下，Azure AD）が用いられる．利用者アカウントはテナント全体の管理権限を持つサービス管理者だけが作成，削除できる．管理権限の対象を一部のアカウントやドメインなどに制限することはできず，サービス管理者は全ての登録ドメインの全アドレスを管理できる．

個々の利用者アカウントに複数のメールアドレスを登録できるが，それらのメールアドレス宛のメールは，利用者アカウントごとに準備される単一のメールボックスに配送される．さらに，検討段階および本稿執筆時点では，送信メールの From フィールドに利用できるメールアドレスには制限がある．基本的に，利用者アカウントに「プライマリ SMTP アドレス」として登録された 1 個のメールアドレスしか，From フィールドに利用できない．利用者アカウントに登録したプライマリ SMTP アドレス以外のメールアドレスは「セカンダリ SMTP アドレス」として扱われるが，セカンダリ SMTP アドレス宛のメールは受信できるが，送信メールの From フィールドには利用できない．

複数のメールアドレスをメンバーとして登録しメール転送できる「配布グループ」というメールアドレスを作成する機能があり，メールエイリアス機能と同等な転送アドレスを作成できる．また，利用者アカウントに対して，特定配布グループについての「SendAs 権限」を付与することで，配布グループのメールアドレスを送信メールの From フィールドに利用可能である．既定では全てのユーザーが配布グループを作成できるが，配布グループ作成の権限を一部のアカウントに限定可能である．しかし，作成権限を持つアカウントは，テナントに登録された任意のドメインに対して配布グループを作成できる．九州大学の全学基本メールサービスが利用するテナントでは，配布グループの作成権限をサービス管理者だけに制限している．なお，配布グループ機能の他に，共有メールボックスや Microsoft 365 グループという複数アカウントで共有するメールボックスを用意する機能はあるが，いわゆるメーリングリストのような，単なる転送以上にメールヘッダの追加・変更などを行うメール配信機能は提供されていない．

3.2 実現方式

前節で述べた Exchange Online の仕様を踏まえ，2 章で述べた提供機能を実現する方法について検討した．以下に，採用した基本方式について説明する（**図 1**）．

まず，集約対象の組織ドメインを Exchange Online のテナントに登録する．そして，組織アドレスそれぞれに対して，個人用，グループ用いずれの場合も，3.1 節で説明した配布グループを作成し，組織アドレスの転送先を配布グループのメンバーとして登録する．ここで，組織アドレスが個人用のアドレスである場合は，対応する全学アドレス

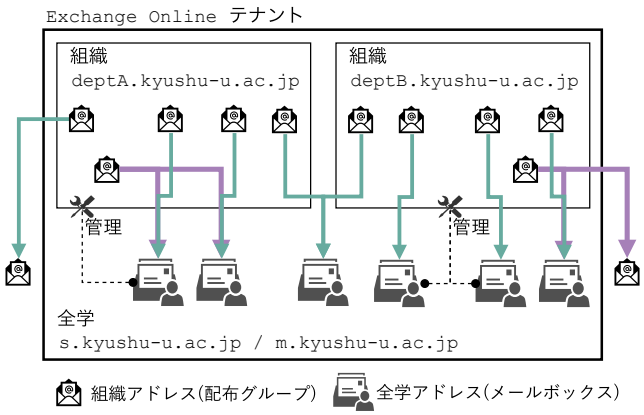

図 1 実現方式の概要

へとメールが配送されるようにメンバー登録する．これにより，組織アドレス宛のメールが全学基本メールサービスで受信できる．さらに，テナントのアカウントを持つ配布グループのメンバーには，配布グループに対する SendAs 権限をアカウントに付与する．これにより，組織アドレスを From フィールドに指定したメールが送信できる．

3.1 節で述べた通り，配布グループの作成権限を組織ドメイン管理者のアカウントに付与することは可能だが，その場合，他の組織ドメインの配布グループも作成できてしまい，問題である．そこで，組織ドメイン管理者が配布グループを作成，変更，削除できるシステムを別途開発することにした．この組織アドレス管理システムは，組織ドメイン管理者を認証して，管理対象の組織ドメインの組織アドレスに限定して配布グループの管理機能を提供し，特別に用意した配布グループ作成権限を持つアカウントを用いて代理で配布グループの管理を行う．また，各組織ドメインの 1 人以上の管理者を管理するために，Azure AD 上に各組織ドメインごとに管理者グループを作成する．

3.1 節で述べた通り，Exchange Online にはメーリングリスト機能はない．そこで，Exchange Online とは別にメーリングリストサーバを用意することにした．ただし，個々の組織ドメインのメーリングリストについて，Exchange Online からメーリングリストサーバに配送するような構成は，運用管理上の困難がある．そこで，メーリングリスト用に専用ドメインを用意し，専用ドメインのメーリングリストサーバを構築する．既存のメーリングリストを組織アドレスで継続して利用したい場合は，上記の配布グループを用いて組織アドレスから専用ドメインのアドレスに転送すればよい．

3.3 組織ドメイン移行手順

前節で述べた実現方式に従って既存の独自運用メールサービスを全学基本メールサービスへと集約するときに，組織ドメインを Exchange Online へと移行する手順を以下に説明する．ここでは，集約対象の組織ドメインを deptA.kyushu-

u.ac.jp，集約前の deptA.kyushu-u.ac.jp の MX レコードに設定されているメールサーバを mx.deptA.kyushu-u.ac.jp とする．なお，ここでの処理は PowerShell[14], [15] を用いて実行する．

3.3.1 管理者グループ作成

組織ドメインの管理権限を管理するための管理者グループを作成し，組織ドメイン管理者の全学アカウントをメンバーとして登録する．このとき，管理者グループ名は対象とする組織ドメインから一意に定まるように設定する

3.3.2 ドメイン登録

組織ドメイン deptA.kyushu-u.ac.jp を集約先の Exchange Online のテナントに登録する．このとき，組織ドメインの正当な所有者である事を DNS 設定などにより証明する確認作業が必要となる．ただし，組織ドメインの上位ドメイン（今回の例では kyushu-u.ac.jp）が予めテナントに登録してある場合は，所有権確認は不要である．

ここで，特に教育機関については多くの場合に，ドメイン登録において追加の作業が必要になる．Microsoft 365（旧 Office 365）を組織として利用していない場合に，各個人として Microsoft 365 の利用を開始することができ，これをセルフサービスサインアップと呼ぶ．その場合，セルフサービスサインアップに用いたメールアドレスのドメイン名が登録されたテナントが自動的に作成される．つまり，組織アドレスが過去にセルフサービスサインアップに用いられていた場合，対応する組織ドメインは自動生成テナントに既に登録されており，集約先テナントへのドメインの登録に失敗する．この場合，事前に自動生成テナントからドメイン登録を解除しておく必要がある [16].

3.3.3 メール中継設定

前ステップの作業を行った時点では，Exchange Online のテナントに deptA.kyushu-u.ac.jp ドメインは登録されたものの組織アドレスは存在しないため，そのテナントを用いて組織アドレス宛にメールを送信すると宛先不明のエラーとなる．そこで，前ステップ作業が完了次第速やかに，deptA.kyushu-u.ac.jp 宛のメールを既存メールサーバ mx.deptA.kyushu-u.ac.jp へ転送するように設定しなければならない．それには，先ほど登録した組織ドメインを Exchange Online で「内部の中継」に設定する．この設定により，deptA.kyushu-u.ac.jp 宛のメールは MX レコードを参照して mx.deptA.kyushu-u.ac.jp へ配送される（**図 2** A）．なお，前ステップのドメイン登録作業完了後 Exchange Online に反映されるまでに数分程度の時間が掛かる場合がある．そこで，PowerShell により登録確認と中継設定を半自動処理する．それでも，一時的な宛先不明エラーは発生しうるので，Exchange Online において，組織ドメイン deptA.kyushu-u.ac.jp 宛に送信を試みて宛先不明となったメールがないか確認するといった対応が必要である．

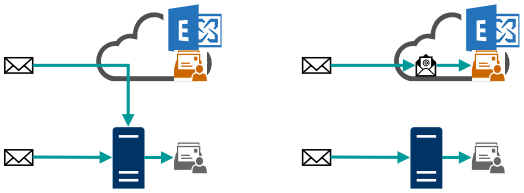

図 2 移行途中段階のメール配送フロー

3.3.4 送信コネクタ設定

組織アドレスについて逐次的な移行を実現する目的で，deptA.kyushu-u.ac.jp ドメイン宛のメールを，MX レコードの設定にかかわらず，既存サーバ mx.deptA.kyushu-u.ac.jp に配送する送信コネクタを作成する．前ステップの設定と本設定により，次ステップの MX レコードの設定切り替え以降も，組織ドメイン deptA.kyushu-u.ac.jp の Exchange Online に存在しないアドレス宛のメールは mx.deptA.kyushu-u.ac.jp へと配送される（図 2 A）．なお，Exchange Online のウェブ管理コンソールから送信コネクタを作成する場合は途中でメール配送テストが求められるが，PowerShell では必要ない．また，Exchange Online への設定変更は，本処理に限らず，Exchange Online システム全体に設定が反映されるまで 1 時間程度要することもあるので注意が必要である．

3.3.5 MX サーバ切り替え

Exchange Online が登録ドメイン deptA.kyushu-u.ac.jp に割り当てた MX レコード用の FQDN を取得し，ドメイン deptA.kyushu-u.ac.jp の MX レコードを変更する．MX レコードの変更がキャッシュ DNS サーバに浸透して以降は，組織ドメイン deptA.kyushu-u.ac.jp 宛のメールは Exchange Online に配送されることになるが，前ステップで作成した送信コネクタによって，メールは mx.deptA.kyushu-u.ac.jp へと配送される（図 2 A）．なお，ドメイン deptA.kyushu-u.ac.jp において SPF[17] が設定されていた場合は，併せて Exchange Online 用の SPF 設定を追加しておく．

3.3.6 配布グループ登録

組織アドレス用の配布グループを順次作成する．作成する配布グループの所有者として組織ドメインの管理者グループを指定する．このとき，配布グループ作成と同時に転送先アドレスをメンバーとして登録しなければならない．そうでなければ一時的なメールロストが発生する．なお，ここでの配布グループの作成は，PowerShell で行っても良いし，後述のアドレス管理システムを用いて行うこともできる．また，ある組織アドレスに対応する配布グループの転送先に設定するメールアドレスにおいて，その組織アドレス自身への転送が設定されていた場合は，配布グループ作成に先立って転送設定の解除を徹底しなければならない．特に，メッセージを保持しない転送の設定の場合は，メールロストが発生する．

組織アドレスに対応する配布グループ作成により，そのアドレス宛のメールは，送信コネクタではなく配布グループを介して配送されることになる（図 2 B）．ただし，Exchange Online に存在しない組織アドレス宛のメールは，送信コネクタを介して mx.deptA.kyushu-u.ac.jp へと配送される（図 2 A）．なお，旧メールサーバ mx.deptA.kyushu-u.ac.jp を用いてメール送信した場合は，mx.deptA.kyushu-u.ac.jp を使ったメール配送となるので注意が必要である（図 2 B）．mx.deptA.kyushu-u.ac.jp において受信メールを Exchange Online へと転送するように設定する場合は，Exchange Online 側で当該 IP アドレスからの受信コネクタを作成しておく．

3.3.7 移行終了処理

必要な組織アドレス全てについて配布グループが作成された後，Exchange Online において組織ドメイン deptA.kyushu-u.ac.jp を「内部の中継」から「権限あり」に変更し，deptA.kyushu-u.ac.jp 用に作成した送信コネクタを削除する．この作業により，Exchange Online に存在しない組織アドレスについて，Exchange Online が宛先不明として処理するようになる．さらに，送信者のなりすましへの対策のため，deptA.kyushu-u.ac.jp に対して SPF および DKIM[18] の設定を行う．DKIM 用の鍵は Exchange Online により生成される．

4. アドレス管理システムの開発

4.1 システム設計

Exchange Online に集約された組織アドレスを管理するために，組織ドメイン管理者に組織アドレス管理システムを提供する．このシステムは，利便性を考慮してウェブアプリケーションとして構築することとした．Exchange Online の仕様は利用者に断りなく変更される場合があり本システムに変更や追加が必要になる可能性があること，並びに，予算上の都合により段階的に機能拡張していく必要があることから，保全性や拡張性を考慮し，このウェブアプリケーションにはマイクロサービスアーキテクチャ [19] を採用した．全学サービス管理者の運用管理負担を考慮し，計算機や仮想機械，基盤ソフトウェアなどの保守，管理を要しないサーバレス [20] 構成として，クラウドサービスの Function as a Service (FaaS)[21]，Platform as a Service (PaaS)[22] を用いて実現する．さらに，運用にかかる費用を考慮して，システムのユーザインタフェースは，クライアントサイドで実行するシンサーバ構成とした．

本システムは主に以下の要素で構成される（**図 3**）．

組織アドレス管理ウェブサービス　RESTful ウェブサービスとして，SaaS メールサービス上の組織アドレスの管理機能を，REST API により提供する．

管理者用ウェブアプリケーション　クライアントサイドで実行され，組織ドメイン管理者に管理用ユーザインタフェースを提供する．

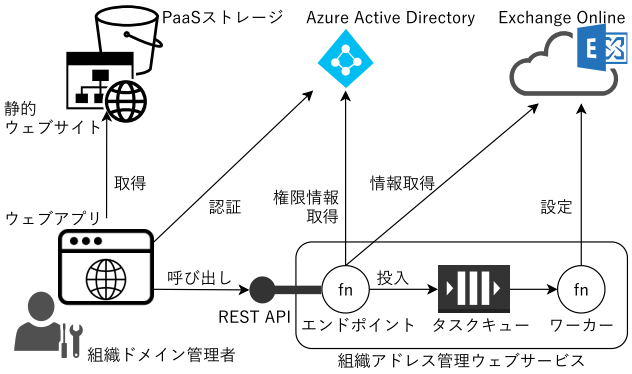

図 3　システム概略図
Fig. 3　System framework diagram.

静的ウェブサイト　PaaS 上でホスティングし，前記ウェブアプリケーションを静的コンテンツとして配信する．

4.2 組織アドレス管理ウェブサービス

組織アドレス管理ウェブサービスは，FaaS である Azure Functions[23] 上で処理を行う RESTful ウェブサービスである．組織ドメイン管理者からの処理要求に応じて，特別に用意したアカウントを用いてリモート PowerShell により，Exchange Online に対して配布グループの作成，読み取り，変更，削除の処理を実行する．

HTTP[24] を用いた REST API として，以下の機能を提供する（**表 1**）．

一覧取得　組織ドメイン管理者が管理する組織ドメインについて，配布グループに付けられた組織アドレスの一覧を応答として返す．

作成　組織アドレスと転送先（配布グループのメンバー）一覧を指定して組織アドレスを作成する．

転送先一覧取得　指定された組織アドレスの転送先一覧を応答として返す．

転送先更新　指定された組織アドレスの転送先を，指定された転送先一覧で上書き更新する．

削除　指定された組織アドレスの配布グループを削除する．

表 1 で HTTP の GET メソッドを用いる取得系エンドポイントは，実時間処理で Exchange Online からの取得結果を応答する．一方，その他のエンドポイントは，Azure Queue Storage[25] 上の非同期メッセージキューに処理要求を投入して即座に応答を返し，実際の処理はワーカースレッドによるバックグラウンド処理で行う．これは，Exchange Online における配布グループの作成やメンバー変更処理などは時間が掛かること，また，Exchange Online のリモート PowerShell 接続では最大接続数が数個に制限されており，同時に多数の REST API 呼び出しがあっても並行処理ができないことなどが理由である．バックグラウンド処理の結果は，組織ドメイン管理者宛に電子メールで送信する．

表 1　組織アドレス管理 REST API
Table 1　REST API for management of organizational addresses.

機能	HTTP メソッド	パラメタ	応答
一覧取得	GET	–	組織アドレス一覧
作成	POST	組織アドレス，転送先一覧	処理受付成否
転送先一覧取得	GET	組織アドレス	転送先一覧
転送先更新	POST	組織アドレス，転送先一覧	処理受付成否
削除	POST	組織アドレス	処理受付成否

一方，取得系の機能については，呼び出し元で継続して処理する必要があることから，実時間で結果を返すこととする．ただし，呼び出し元では処理がタイムアウトとなった際の再試行を考慮する必要がある．

4.3　管理者用アプリケーション

組織ドメイン管理者には組織アドレスを管理するためのユーザインタフェースをウェブアプリケーションとして提供する．ウェブアプリケーションは静的ウェブコンテンツとして Azure Blob Storage[26] 上でホスティングし，クライアントサイドである組織ドメイン管理者が使うウェブブラウザ上で，前節で述べた REST API の呼び出し，応答の処理，入出力などの処理を実行する．ウェブアプリケーションの処理系には HTML5[27] と ECMAScript 2015 (ES6)[28] を用いた．

4.4　認証と認可

本システムの認証および認可には，Azure AD を用いる．機密性とセキュリティを考慮して，認証と認可に関する情報は Azure AD のみに登録し，システムでは一切のアカウント情報を独自に保持せず，認証と認可は Azure AD を介して処理する．4.2 節で述べた組織アドレス管理ウェブサービスの REST API では，組織ドメイン管理者が管理権限を持つ組織ドメインに対する処理のみを受理するが，これには OAuth 2.0[29] を用いて以下の方法で行う．

OAuth 2.0 のクライアントに該当する管理者用ウェブアプリケーションは，認可サーバである Azure AD へとリダイレクトすることで組織ドメイン管理者の全学アカウントの認証を行い，Azure AD から認証コード，次いで，アクセストークンを取得する．その後，管理者用ウェブアプリケーションが，リソースサーバに該当する組織アドレス管理ウェブサービスに対して処理要求する際には，取得したアクセストークンを附して REST API エンドポイントにアクセスする．組織アドレス管理ウェブサービスは，渡されたアクセストークンにより組織ドメイン管理者を認証する．そして，アクセストークンに含まれる全学アカウントの識別名について，処理対象の組織ドメインに対応する管理者グループに所属しているかを確認し，権限のある処理要求のみを受理して実行する．管理対象の組織アドレスの

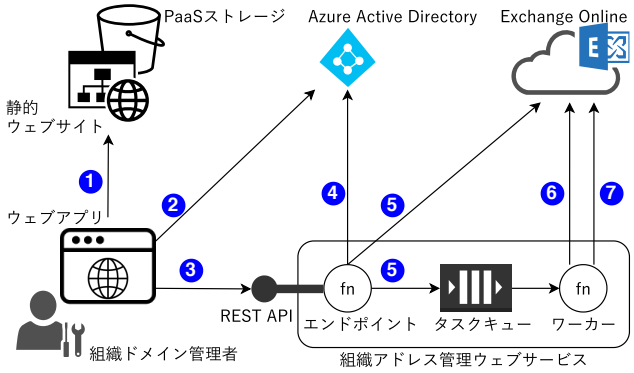

図 4　組織アドレス管理要求処理フロー

一覧は，管理者グループを介して全学アカウントが所有者となっている配布グループの一覧として取得できる．

4.5　組織アドレス管理要求処理

開発した組織アドレス管理システムにおいて，組織ドメイン管理者による組織アドレス管理の要求が処理される流れを以下にまとめる（**図 4**）．ただし，認証認可処理の詳細は省略している．

(1) 組織ドメイン管理者が，ウェブブラウザにより静的ウェブサイトにアクセスすると，認証のためにウェブブラウザを Azure AD にリダイレクトする．
(2) Azure AD は組織ドメイン管理者を認証し，認証に成功すれば，組織アドレス管理ウェブサービスのためのアクセストークンを発行する．
(3) 管理用ウェブアプリケーションは，組織ドメイン管理者による提供ユーザインタフェースの操作に応じて，組織アドレス管理ウェブサービスの REST API をアクセストークンを附して呼び出し，処理要求を送信する．
(4) 組織アドレス管理ウェブサービスは，アクセストークンにより組織ドメイン管理者を認証し，Azure AD を用いて管理権限を確認する．
(5) 組織ドメイン管理者に管理権限があれば，処理要求を受理する．取得系の処理要求のときは，Exchange Online から要求された情報を取得して，管理用ウェブアプリケーションへと応答として返す．それ以外の処理要求のときは，処理要求をタスクキューに投入し，管理用ウェブアプリケーションへと応答を返す．
(6) 組織アドレス管理ウェブサービスのワーカースレッド

は，タスクキューから処理要求を取り出し，Exchange Online に対して要求された処理を実行する．

(7) 組織アドレス管理ウェブサービスのワーカースレッドは，Exchange Online から受け取った処理結果を，Exchange Online を用いて電子メールにより組織ドメイン管理者へと送信する．

5. メーリングリストサーバ構築

メーリングリスト提供のために専用ドメイン ml.kyushu-u.ac.jp を用意し，メーリングリストサーバを構築した．本メーリングリストサーバの主なメール配送先は，Exchange Online テナントに存在するメールアドレスである．そこで，メール配送経路の最適化を考慮して，以下の構成とする．

メーリングリストサーバは Azure Virtual Machines の Linux Virtual Machines[30] を用いて構築し，Azure のパブリック IP アドレスを附与する．専用ドメイン ml.kyushu-u.ac.jp は Exchange Online に登録して MX レコードに Exchange Online を指定する．そして，Exchange Online において，ml.kyushu-u.ac.jp ドメイン宛のメールをメーリングリストサーバへと転送するように送信コネクタを作成する．ここで，セキュリティを考慮し，メーリングリストサーバで受信するメールは Exchange Online からのみに限定して受け付けるように設定する．また，メーリングリストサーバで全ての外向きメールを Exchange Online へと送信するように設定し，Exchange Online でそのための受信コネクタを作成する．なお，メーリングリストサーバソフトウェアには Mailman[31] を，メール転送エージェントには Postfix[32] を用いた．

6. おわりに

本稿で述べた集約方法を用いたテストケースとして，2019 年 11 月から 12 月にかけて，九州大学の 1 部局について独自に運用していたメールサービスを Exchange Online へと移行した．3.3 節で述べた移行手順は，そこで得られた知見を含んだものである．また，2019 年度内に，4 章で述べたシステムを構築した．ただし，管理者用アプリケーションについては，必要最低限の機能として，特定形式のファイルにより処理を行う機能だけを実装しており，ファイルはアプリケーション外で編集する必要がある．本システムは，2020 年 4 月から，上記部局の組織アドレス管理のために提供している．

当初の予定では，2020 年 4 月より全学基本メールサービス 組織利用サービスとして，独自運用メールサービス集約の受付を開始する予定であったが，昨今の状況によりサービス提供が未だ開始できていない．状況が整い次第サービス提供を開始する予定である．今後，大規模部局の移行も計画されている．また，管理者用アプリケーションの機能拡充も継続的に行っていく予定である．さらに，Exchange Online が持つ共有メールボックス機能を利用したいという要望もあり，組織アドレス管理ウェブサービスとその REST API を含めた機能追加も検討している．

謝辞 本稿で述べた集約方法やシステムの検討は，九州大学情報統括本部メールサーバ集約タスクフォースのメンバーの協力の下で行った．ここに感謝に意を表する．

本研究は JSPS 科研費 JP20K11791 の助成を受けた．

参考文献

[1] 伊東栄典，笠原義晃，藤村直美：九州大学における職員向け電子メールサービスの現状，平成 21 年度情報教育研究集会，pp. D3–4 (2009).

[2] Kasahara, Y., Ito, E. and Fujimura, N.: Introduction of New Kyushu University Primary Mail Service for Staff Members and Students, *Proceedings of the 42nd Annual ACM SIGUCCS Conference on User Services*, Association for Computing Machinery, pp. 103–106 (online), DOI: 10.1145/2661172.2662965 (2014).

[3] Kasahara, Y., Shimayoshi, T., Ito, E. and Fujimura, N.: The Past, Current, and Future of Our Email Services in Kyushu University, *Proceedings of the 2018 ACM on SIGUCCS Annual Conference*, Association for Computing Machinery, pp. 103–106 (online), DOI: 10.1145/3235715.3235737 (2018).

[4] Kasahara, Y., Shimayoshi, T., Miyaguchi, T. and Fujimura, N.: Migrate Legacy Email Services in Kyushu University to Exchange Online, *Proceedings of the 2019 ACM SIGUCCS Annual Conference*, New York, NY, USA, Association for Computing Machinery, p. 127–131 (online), DOI: 10.1145/3347709.3347817 (2019).

[5] Ito, E., Kasahara, Y. and Fujimura, N.: Implementation and Operation of the Kyushu University Authentication System, *Proceedings of the 41st Annual ACM SIGUCCS Conference on User Services*, Association for Computing Machinery, pp. 137–142 (online), DOI: 10.1145/2504776.2504788 (2013).

[6] 菅尾貴彦，戸川忠嗣，太田美和，橋倉 聡，平野広幸，伊東栄典，市川広大，先立英喜：全学共通認証基盤サービスの手続きの電子化について，第 30 回全国共同利用情報基盤センター 研究開発連合発表講演会 研究開発論文集，pp. 77–86 (2008).

[7] Verizon: 2020 Data Breach Investigations Report, Technical report (online), available from ⟨https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf⟩, Verizon Communications Inc. (2020).

[8] Gellens, R. and Klensin, J.: Message Submission for Mail, STD 72 (online), DOI: 10.17487/RFC6409, Internet Engineering Task Force (2011).

[9] Siemborski, R. and Melnikov, A.: SMTP Service Extension for Authentication, RFC 4954 (online), DOI: 10.17487/RFC4954, Internet Engineering Task Force (2007).

[10] Resnick, P.: Internet Message Format, RFC 5322 (online), DOI: 10.17487/RFC5322, Internet Engineering Task Force (2008).

[11] Microsoft: Exchange Online, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/exchange/exchange-online⟩ (accessed 2020-06-18).

[12] Mockapetris, P.: Domain names - implementation and

specification, STD 13 (online), DOI: 10.17487/RFC1035, Internet Engineering Task Force (1987).
[13] Microsoft: What is Azure Active Directory?, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis⟩ (accessed 2020-06-18).
[14] Microsoft: PowerShell Documentation, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/powershell/⟩ (accessed 2020-06-18).
[15] Microsoft: Exchange Online PowerShell, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/exchange-online-powershell⟩ (accessed 2020-06-18).
[16] 嶋吉隆夫，笠原義晃，尾花昌浩，藤村直美：九州大学における Office 365 サービス環境の再構築，大学 ICT 推進協議会 2018 年度年次大会，pp. MB2–3 (2018).
[17] Kitterman, S.: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1, RFC 7280 (online), DOI: 10.17487/RFC7208, Internet Engineering Task Force (2014).
[18] Crocker, D., Hansen, T. and Kucherawy, M.: DomainKeys Identified Mail (DKIM) Signatures, STD 76 (online), DOI: 10.17487/RFC6376, Internet Engineering Task Force (2011).
[19] Lewis, J. and Fowler, M.: Microservices, *MartinFowler.com*, (online), available from ⟨https://martinfowler.com/articles/microservices.html⟩ (2014).
[20] Roberts, M. and Chapin, J.: Differentiating Serverless, *What Is Serverless?*, O'Reilly Media, Incorporated, chapter 5 (2017).
[21] Fox, G. C., Ishakian, V., Muthusamy, V. and Slominski, A.: Status of Serverless Computing and Function-as-a-Service(FaaS) in Industry and Research, *arXiv*, No. 1708.08028 (online), DOI: 10.13140/RG.2.2.15007.87206 (2017).
[22] Mell, P. and Grance, T.: The NIST Definition of Cloud Computing, Special Publication 800-145 (online), DOI: 10.6028/NIST.SP.800-145, National Institute of Standards and Technology (2011).
[23] Microsoft: An introduction to Azure Functions, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview⟩ (accessed 2020-06-18).
[24] Fielding, R. and Reschke, J.: Hypertext transfer protocol (HTTP/1.1): Message syntax and routing, RFC 7230 (online), DOI: 10.17487/RFC7230, Internet Engineering Task Force (2014).
[25] Microsoft: What are Azure queues?, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/azure/storage/queues/storage-queues-introduction⟩ (accessed 2020-06-18).
[26] Microsoft: What is Azure Blob storage?, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-overview⟩ (accessed 2020-06-18).
[27] WHATWG: HTML Living Standard, WHATWG (Apple, Google, Mozilla, Microsoft) (online), available from ⟨https://html.spec.whatwg.org⟩ (accessed 2020-06-18).
[28] Ecma International: ECMAScript 2015 Language Specification, Standard ECMA-262 6th Edition, Ecma International (2015).
[29] Hardt, D. et al.: The OAuth 2.0 Authorization Framework, RFC 6749 (online), DOI: 10.17487/RFC6749, Internet Engineering Task Force (2012).
[30] Microsoft: Linux virtual machines in Azure, Microsoft Corporation (online), available from ⟨https://docs.microsoft.com/en-us/azure/virtual-machines/linux/overview⟩ (accessed 2020-06-18).
[31] Free Software Foundation, Inc.: Mailman - The GNU Mailing List Management System, (online), available from ⟨https://docs.mailman3.org/projects/mailman/en/latest/README.html⟩ (accessed 2020-06-18).
[32] Postfix project: The Postfix Home Page, (online), available from ⟨http://www.postfix.org⟩ (accessed 2020-06-18).