

オンプレミスのメール転送サービスから Microsoft 365 を使った メールサービスへの切り替えの試み

宇田川 暢¹⁾

東海国立大学機構 情報環境部 情報システム運用課

udagawa@nagoya-u.jp

An attempt to migration from on-premise email forwarding service to email service using Microsoft 365

UDAGAWA Mitsuru

Information System Operations Division, Tokai National Higher Education and Research System

概要

名古屋大学で提供してきたメール転送サービスのサービス終了を機に、新たなメールサービスを提供することとなった。その際、利用者に対して不便を強いないことや、運用負荷を減らすことに重点を置いてサービス提供方法について検討をおこなった。

1 はじめに

1.1 メール転送サービスの提供

名古屋大学では 2004 年から「メールエイリアスサービス」としてメール転送サービスを行ってきた[1]。これは、汎用 JP ドメインの nagoya-u.jp をメールドメインとして、利用者から希望アドレスの申請を受け付け、指定された別のメールアドレスに転送するサービスである。また、同アドレスを送信元としてメール送信が可能な送信サービスも提供しており、これらのサービスの利用には、いわゆる生涯 ID である名古屋大学 ID（以下、名大 ID）を認証に利用していた。これにより、メールエイリアスサービスは在籍中のみならず、離籍後も継続して利用可能なメールアドレスとして提供されてきた。

1.2 メールエイリアスサービスの問題

情報セキュリティの確保を目的として、近年求められるようになってきた多要素認証の導入の要請や、送信ドメイン認証への未対応による転送メールの受け取り拒否といった問題が発生するようになり、サービス改善の要望や問い合わせ対応に苦慮する事態となってきた。

メールエイリアスサービスで利用してきた Postfix[2]により構築された SMTP サーバでは実運用に耐えうる多要素認証の導入は不可能であり、また、送信ドメイン認証の問題については、不特

定多数のメールサービスへの転送を前提としたメール転送サービス側では、効果的な対応手段は存在していない。

1.3 送信ドメイン認証とメール転送

送信ドメイン認証は基本的に 2 種類の方法で導入される。一つはそのドメインのメールアドレスでのメール送信元となるメールサーバ等の IP アドレスを DNS の TXT レコードに記載しておく SPF (Sender Policy Framework) である。この SPF の評価対象となる送信元 IP アドレスは直前に中継されたメールサーバのものになる。そのため、例えばある組織（組織 A）の SPF レコードに組織 A が管理する IP アドレスが全て記載されているとしても、別の組織（組織 B）のネットワークからメールが送信され、組織 A にあるサーバを中継する場合は、そのメールアドレスの SPF レコードに組織 A の IP アドレスが含まれていることは通常は無い。したがって、転送メールを受け取ったメールサーバは、メールドメインの SPF レコードに記載されていない IP アドレスから受け取ったメールについて SPF によるチェックに失敗することになる。

もう一つは、メール送信時にメールの本文と From アドレス等に対して秘密鍵を用いてデジタル署名を行い、受信者が DNS レコードに記載された公開鍵を用いて署名の検証を行うことで、改竄されていないことを確認する DKIM (DomainKeys Identified Mail) となる。DKIM については転送時に

本文や署名対象となっているメールヘッダの変更が無ければ、DKIM のチェックに影響はない。言い換えると一般的にメーリングリストの運用で行われるような、メールサブジェクトの書き換えを行った場合は、検証に失敗して改竄とみなされる。

また、送信ドメイン認証には DMARC や ARC も存在するが、SPF および DKIM を導入したうえでの対応となることから、本稿では言及しないものとする。

2 後継サービス

2.1 後継サービスの検討と検証

メールエイリアスサービスの今後について検討した結果、前述の問題からメールエイリアスサービスの存続は困難であると判断したため、後継サービスを立ち上げることとなった。

問題を解消するためにはメール転送サービスではなく、メールボックスを持つ一般的なメールサービスが適当と考えられたため、Microsoft 365 を利用したメールサービスの実現可能性について検証を行った。

2.2 Exchange Online for Alumni ライセンス

Microsoft 社の提供する Microsoft 365（以下、M365）サービスの中に、「Exchange Online for Alumni」がある。これは教育機関であることが確認された M365 テナントにおいて、無償で利用可能なメールサービス専用ライセンスである。

しかしながら、同ライセンスは卒業生や退職者のみ利用可能なライセンスとして設定されており、在籍中の学生・教職員が利用することはライセンス違反となってしまうことが、Microsoft 社への問い合わせで判明した。これについては、教育機関の M365 テナントで無償利用可能な「Office 365 A1」に含まれる「Exchange Online Plan1」のライセンスを併用することで対応可能と判断した。ただし、Office 365 A1 ライセンスは在籍者のみ利用可能なライセンスとなっているため、利用者の属性に応じて Office 365 A1 と Exchange Online for Alumni とを使い分けを行う必要がある。

2.3 ハイブリッド構成によるメール中継

メールエイリアスサービスの利用者の大半が離籍者であることから、一度にすべての利用者を既存サービスから M365 で提供されるメールサービスの Exchange Online（以下、ExO）に切り替えることは非現実的であると判断し、既存サービスとの同時稼働について検証を行った。

ExO ではハイブリッド構成として、オンプレミスのメールサーバと同時に稼働させることが可能であるため、この点について問題となることはなかった。ハイブリッド構成では DNS の MX レコードには M365 を指定しておき、M365 テナントに存在しないメールアドレスについては、オンプレミス側に転送するという動作になる。

なお、本件ではメール転送サーバとメール送信サーバが異なるサーバであったため問題にはならなかったが、Postfix ではローカル配送が優先されるため、送信サーバから同メールドメインを持つ M365 に対してメール送信できない。その場合は transport_maps 機能を利用し、M365 に存在するメールアドレスについては MX に対して配送するように設定する必要がある。

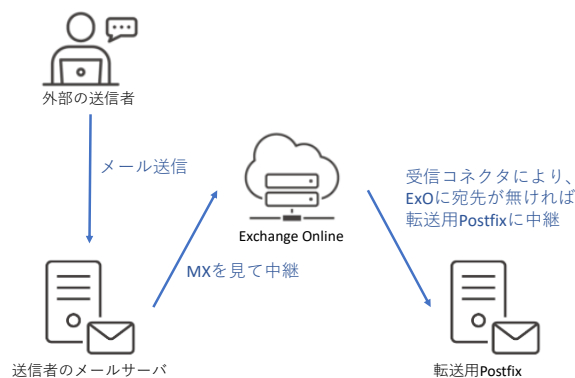


図1 ハイブリッド構成概略

ハイブリッド構成を利用することで、メールサービスを中断すること無く、ExO 側にアカウントを作成した利用者から順次メールを切り替えることが可能であると分かった。

先行事例とした嶋吉ほか[3]による九州大学の報告では、このドメイン登録と受信コネクタで工夫が必要だったとあるが、検証では「ドメイン登録」、「受信コネクタ作成」、「MX レコード変更」の順で作業を行うことで期待通りの動作となった。

2.4 アカウント管理

メールエイリアスサービスの利用者は検証時点で4,000人強であり、また、今後利用者が増え続けることが予想されるため、後継サービスでは、メールなどで既存サービスからの切替や新規申請受付を行い、手作業による Entra ID へのアカウント登録やExO管理センターでの変更などは行わないようにする必要があった。Microsoft Graph と呼ばれる REST API が用意されており、これを利用したアカウントの自動作成が可能であることを確

認した。ただし、転送先アドレスの設定などは Microsoft Graph では対応しておらず、一部の処理は PowerShell により行う必要があった[4]ため、まずは PowerShell を利用しなくても済むようなサービス設計とすることとした。

2.5 ライセンス割り当て

前述のとおり、利用者により異なる ExO ライセンスの割り当てを行う必要がある。Microsoft Graph でライセンスの割り当てを各アカウントに対して行うことが可能だが、ライセンス割り当てを行った後に不要な SKU を無効にする処理を行う必要があり、複雑な管理を行う必要があることが調査の中で分かった。SKU は M365 の各ライセンスに含まれる個別のソフトウェアを指し、例えば Office 365 A1 では「Exchange Online Plan 1」、「Teams」、「Share Point Plan 1」、「Forms Plan2」などが含まれていて、ライセンス割り当てを行うとその中に含まれる全ての SKU が有効となる。

そのため、アカウント個別にライセンス割り当てを行わず、あらかじめ「Exchange Online for Alumni」、「Office 365 A1 for Faculty」、「Office 365 A1 for Student」が割り当てられたセキュリティグループを作成し、アカウント作成時に該当するグループに追加することとした。

2.6 パスワードリセット／多要素認証の削除

また、後継サービスを提供するにあたって、パスワード忘れ等への対応のためのサポートコスト低減が必須であると考えた。筆者は直接の担当ではないが、東海国立大学機構および名古屋大学で提供している認証サービスにおいて、パスワード忘れによるパスワードリセットや、スマートフォンの故障や買い替えによる多要素認証の再登録への対応依頼が問い合わせの多くを占めている。

この問題に対して、ユーザ自身によるパスワードリセットおよび多要素認証の削除が可能になる機能の実装について検証を行った結果、こちらも Microsoft Graph を利用して実現することが可能であることが分かった。

2.7 検証結果

以上を踏まえ、M365 を利用することでメールエイリアスサービスの後継となるメールサービスの提供を実現することが可能であるとの判断に至った。

3 サービス設計

メールエイリアスサービスの後継となるメールサービスについて、以降は「nagoya-u.jp メール」と呼称する。

nagoya-u.jp メールを実現するためのサービスについては以下のように設計した。

3.1 学内メールサービスとの棲み分け

学内には在籍者に対して付与される「機構メール」アドレスが存在している。これは東海国立大学機構（以下、機構）の学生および教職員に対し、全員に付与されている。しかし、機構メールは離籍して一定期間後に使用不能となってしまう。これに対して、nagoya-u.jp メールは離籍後も永続的に利用可能なサービスとして提供する予定としている。

一方、情報セキュリティの観点で言えば、nagoya-u.jp メールに保存されているメールは離籍後もそのまま保持されることになる。教職員が退職した後、機構に関する機密情報が持ち出されることのリスク、および、離籍後にメール漏洩のインシデント対応が発生した場合の対応を考慮して、nagoya-u.jp メールを機構の業務に利用しないよう求める項目を利用規約に取り入れることとした。また、機構メールから nagoya-u.jp メールへのメール転送も禁止としている。なお、この制限は在籍中の教職員のみ対象となり、学生は対象としていない。

メールエイリアスサービスがそうであったが、nagoya-u.jp メールは主に教員が異動や退職後にも名古屋大学のドメイン名を冠した個人用メールアドレスを利用し続けることができるサービスということをセールスポイントとしている。そもそものメールサービス環境自体が異なるのかもしれないが、他大学で一般的に提供されているアルムナイメールが学生を対象としていることと異なっている。

また、利用する M365 テナントは東海国立大学機構で全学的に利用しているテナントではなく、nagoya-u.jp メール専用のテナントを作成して利用することとなった。

3.2 ウェブシステムによるアカウント管理

先述の通り、運用負荷を減らすために可能な限り利用者対応を自動化することを目的とするため、自然にウェブシステムを利用したセルフサービスとした。nagoya-u.jp メールへの申請や管理を目的

としたシステムを「nagoya-u.jp メール申請システム」と呼称する。

4 nagoya-u.jp メール申請システム

nagoya-u.jp メール申請システムは、オンプレミスのサーバにいわゆる LAMP 環境で構築されており、現時点で以下の機能を持っている。

4.1 申請機能

新たに nagoya-u.jp メールの利用を希望する際は、名古屋大学 ID を利用した認証システムである「多要素認証 CAS」[5]で認証後、一問一答のウィザード形式で申請を行うことができる。現在は名古屋大学では「機構アカウント」による認証が利用されているが、離籍者からの申請も可能なように暫定的にこのようにしている。

まずは利用規約への同意を求める画面が表示され、利用希望者は申請を開始する前に、利用規約に同意する必要がある。

希望するメールアドレスを入力する。希望メールアドレスが重複チェックや NG ワードチェックで問題ないと判断された場合、次のステップに進む。NG ワードにはシステムや大学運営上意味がありそうなキーワードがリスト化されており、完全一致でチェック結果が NG となる。

続いて連絡先メールアドレスの入力を求められる。この連絡先メールアドレスは申請の承認結果の通知のほか、パスワードリセットなどに利用される。本システムにおいて、連絡先メールアドレス等の入力時は、入力されたメールアドレスに確認用コードとして数桁の数字が送信される。この数字を指定時間内に入力することで、メールアドレスの所有者であることの確認と、メールアドレスが入力間違いでないことのチェックをしている。

連絡先メールアドレスの入力が完了したのち、申請内容の確認画面が表示され、ここで申請を確定すると申請内容が本システムに保存される。申請者の氏名や所属（在籍中の場合）といった情報は、LDAP サーバから自動的に取得されたものが申請内容に含めて保存される。

管理者は申請完了通知メールを受けとった後、申請内容を確認し、申請内容に問題がなければ承認を行う。申請が承認された場合、Entra ID へのアカウント作成と利用者の属性を元に適切な ExO 用のライセンスが割り当てられたセキュリティグループへの追加が行われる。

承認結果は申請者にメール通知されるが、このメールには初期パスワードは記載されず、後述のパスワードリセットを案内される。

4.2 代理申請機能

名古屋大学 ID 導入前の離籍者や自身の名古屋大学 ID とパスワードを忘れてしまった離籍者の場合は、前掲の方法で申請を行うことができないため、身分証による本人確認と、在籍履歴の確認のための書類による申請となる。

管理者は申請内容を確認したのち、代理申請機能によって、本人に代わって申請を行ったのちに承認を行う。

4.3 メールエイリアスサービスからの移行機能

メールエイリアスサービスの利用者は、2つの方法でそれまでのメールアドレスを引き継いで利用することができる。

1つは前述の多要素認証 CAS による認証で、こちらは主に在籍者を対象としている。認証結果から LDAP でメールエイリアスアドレスを取得し、当該メールアドレスを nagoya-u.jp メールとして利用できるように設定する。

もう1つは指定したメールエイリアスサービスのメールアドレス宛に確認コードを送信、到達を確認することで、認証を行っている。本システム上で総当たりでメールアドレスを入力されることによる迷惑行為を防ぐため、メールエイリアスアドレスとその転送先メールアドレスの両者の入力を求め、一致した場合にのみ確認コードを送信するようにしている。

どちらかの方法で認証したのち、申請時と同様に利用規約への同意を求め、移行手続きを進める。

移行手続きでは連絡先メールアドレスの入力は任意となっており、また、既存の転送先メールアドレスを nagoya-u.jp メールでも引き続き転送先として引き継ぐことができるようになっている。ここでは転送しないようにすることも可能であり、別の転送先メールアドレスを指定することも可能となっている。

最後に確認画面が表示されたのち、移行手続きを開始することになるが、申請とは異なりただちに移行処理が行われ、処理完了後に初期パスワードがウェブブラウザの画面に表示される。

移行完了後は本機能を利用できないようになる。

4.4 パスワードリセット機能

利用者は自分の nagoya-u.jp メールアドレスと連絡先メールアドレスの組み合わせを専用フォーム

に入力することで、パスワードリセットを行うことができるようになっている。

移行機能と同じように、ここでもメールアドレスの組み合わせが一致している場合のみ、確認コードが送信される。また、迷惑行為を防ぐため、確認コードの再送信は 24 時間以上経過している必要がある。

パスワードリセット時には新たに生成されたパスワードが上書きされるが、生成するパスワードはメモをしたりタイプしたりした際に間違えにくいよう、複数のキーワードを利用したパスフレーズ形式で生成される。

パスワードリセットとともに多要素認証の初期化も行われ、当該メールアドレスに紐づけられた多要素認証の設定がすべて削除される。処理完了後は新しいパスワードがウェブブラウザの画面上に表示される。

パスワードリセット後、利用者は次回ログイン時にパスワード変更と多要素認証の登録を求められる。

4.5 連絡先メールアドレス変更機能

主に利用者の都合により、登録されている連絡先メールアドレスを変更する必要がある場合、nagoya-u.jp メールアカウントでログインすることで、連絡先メールアドレスを変更することができるようになっている。

本機能については、Entra ID にエンタープライズアプリケーションとして登録し、OpenID Connect で認証を利用することで実現している。

4.6 表示名変更機能

Exchange プロトコルを利用するメールアプリ（Outlook や Apple Mail など）を利用している場合、メールの差出人欄を変更することができない仕様となっている。これについては通常は Entra ID で設定されている値を管理者が変更する必要があるが、都度対応しなくても済むよう、

この機能は Microsoft Graph を利用して実装している。

4.7 所属グループ変更機能

利用者の在籍状態が変更となった場合、アカウントに対して割り当てている M365 のライセンスを変更する必要がある。そのため、LDAP サーバを利用して在籍状態のチェックを行い、在籍状態が変更になった場合は参加させるべきグループを変更するような処理を定期的に行えるようにした。

また、グループ変更時に ExO のライセンスが割り当てられていないタイミングが存在しないよう、参加させるべきグループに追加で登録し、2 つのグループに所属している状態にしておいて、別のタイミングで不要となったグループから削除している。

5 専用ウェブサイトの作成

nagoya-u.jp メールの利用者が問い合わせ時に混乱しないようにすることや、問い合わせ対応負荷を減らすために FAQ などを掲載した本サービス専用のウェブサイトを作成し、メールドメインと同じ <https://nagoya-u.jp/> で公開した。

また、本ウェブサイトは nagoya-u.jp メール利用者からのメールを受け取った相手側に対して、本メールサービスは名古屋大学が公式に提供しているメールサービスであること、および、利用者が名古屋大学の在籍者であるとは限らないことを対外的に明示する機能を持っている。

6 サービス切り替え

nagoya-u.jp メール申請システムの作成後、メールエイリアスサービスから nagoya-u.jp メールへのサービス切り替えを行った。

6.1 ハイブリッド構成の構築

検証でも述べた通り、既存のメールエイリアス利用者に対してメールを転送し続けながら、nagoya-u.jp メールへの移行完了者および新規利用者のメール受信を実現するため、ハイブリッド構成の設定を行った。これについては以下の手順で実現することが可能であった。

1. M365 テナントへのカスタムドメイン追加
2. 受信コネクタの設定
3. MX レコードの変更

まず、nagoya-u.jp メール用 M365 に nagoya-u.jp ドメインをカスタムドメインとして追加した。これにより、nagoya-u.jp をメールドメインとして利用できるようになり、nagoya-u.jp 宛てのメールについてのコネクタを設定することができるようになった。

次に受信コネクタの設定を行った。M365 に届いたメールは、同テナント内に宛先メールアドレスが存在する場合はそこに配送されるが、テナント内に無いメールアドレスについては、受信コネクタで次の中継先となるサーバを指定することがで

きるようになっている。よって、nagoya-u.jp メールのテナント内に宛先メールアドレスが存在しない場合は、現行のメールエイリアスサービスの転送用メールサーバを中継先として指定する設定を追加した。

最後に MX レコードを ExO で指定されたものに変更することで、それまでメールエイリアスサービスの転送用メールサーバに届いていたメールは M365 を経由することになり、サービス停止することなく nagoya-u.jp メール導入の準備を行うことが可能となる。

メールエイリアスサービスの利用者は名古屋大学の在籍者または離籍者となるため問題ないが、無償で提供される ExO ライセンスの対象とならない利用者が受信コネクタでの中継先サーバに存在している場合、その利用者数だけ別途有償の Exchange Online Protection または ExO のライセンスが必要になる。

6.2 内部テスト

nagoya-u.jp メールの構想に関係する教職員を対象に、内部テストを行った。その結果、文言修正などのほかに以下の要望に対応することとなった。

6.2.1 移行時の転送先の引継ぎ

移行した利用者が今までどおり転送のみを利用したい場合、わざわざウェブメールにログインして設定を行う必要があり手間であることと、移行すれば今まで通り転送されると利用者が考えていた場合に、メールが届かないと問い合わせがくるであろうと指摘があった。

当初は Microsoft Graph での対応が不可能なためスコープ外としていたが、システム構築中の検証で PowerShell コマンドを利用した設定を行うことが可能となったことから、メールエイリアスサービスでの転送先アドレスの引継ぎ機能を追加で実装した。

ただし、Entra ID へのアカウント作成と ExO のメールボックス作成完了のタイミングについて、場合によって数十秒から 10 分程度とかなりの時間差があることが発覚した。そのため、30 秒のスリープを入れながら最大 15 回の転送先設定を試みる仕様としている。ごくまれにはあるがこの時間内に完了しない可能性があるため、その場合は転送先の設定処理を打ち切って、移行処理完了画面に転送先の設定に失敗した旨を表示するようにしている。

6.2.2 移行時のメールでの認証

当初は移行する際に多要素 CAS での認証を必須としていたが、離籍者がパスワードを覚えていない可能性が高いとの指摘を受け、問い合わせ対応の負荷軽減のために前述のメール認証機能を追加で実装した。ただし、実装コストの都合により、移行開始受付からおよそ一ヶ月遅れでの機能追加となった。

6.3 メールエイリアスサービスの新規申請停止

メールエイリアスサービスの終了と nagoya-u.jp メールが後継サービスとなることを明確にするため、次項の移行受付開始の直前にメールエイリアスサービスの新規利用の受付を停止した。

6.4 メールエイリアスサービスの移行受付開始

nagoya-u.jp メールの開始後には多数の問い合わせが集中することが想定されたため、負荷分散を目的として、まずは既存のメールエイリアスサービスの利用者の移行対応のみを行い、後に新規利用の受付を行うこととした。また、問い合わせ対応の中で FAQ の充実を行った。

6.5 新規利用申請の受付開始

移行手続きの問い合わせが落ち着いてきた頃に新規利用申請の受付を開始した。

7 現在の利用状況

2024 年 9 月末の時点で、nagoya-u.jp メールの利用者数を表 1 として示す。

図 2 は移行受付を開始した 2023 年 11 月 6 日以降の週当たりの利用者数増加を積み上げ棒グラフで、累積の利用者を折れ線グラフで表している。移行について 3 つのピークがみられるが、左から順に「受付開始」、「メール認証での受付開始」、「メールエイリアスサービス終了直前」となっており、それぞれ数日前に対象者に対してアナウンスのメールを送信している。

また、新規申請受付開始は 2024 年 2 月 5 日からとなった。

表 1 nagoya-u.jp メール利用者集計

グループ	新規	移行	小計
学生	98	76	174
教職員	275	724	999
離籍者	46	675	721
小計	419	1,475	1,894

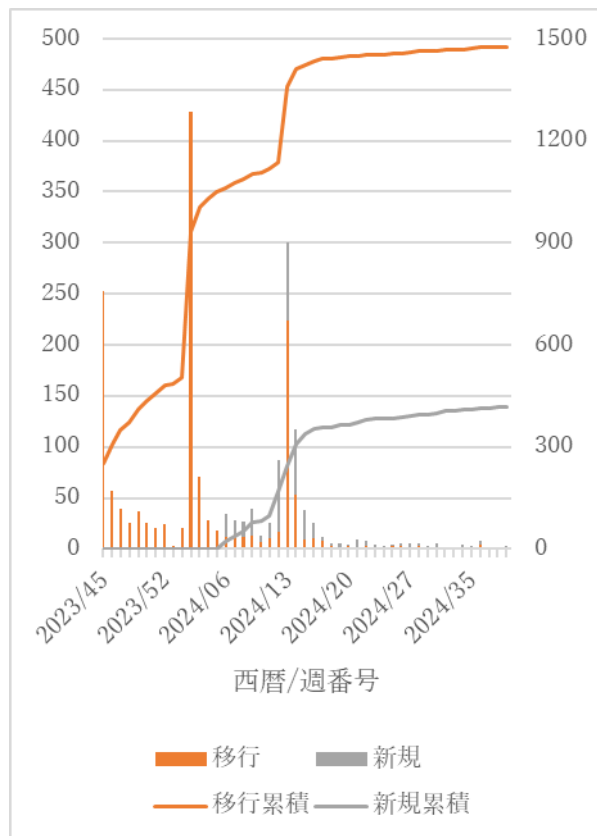


図 2 nagoya-u.jp メール利用者数推移

離籍者について学生または教職員のどちらであったかの内訳は不明であるが、在籍者に限って言えば教職員の利用者が多くなっている。

8 さいごに

nagoya-u.jp メールは名古屋大学の在籍者及び離籍者に向けたいわゆる生涯メールサービスであるが、将来にわたって長期的なサービス提供が可能かどうかについて Microsoft 社の意向に寄るところが大きい。

例えば九州工業大学では 2012 年から Yahoo!メール Academic Edition を利用して生涯メールサービスを提供していたが、数年後に Yahoo!社によるサービス提供終了のため、Microsoft Office 365（現在の M365）に乗り換えすることになり [6]、2024 年 12 月末をもって全てのサービスを終了することとなっている [7]。

サービスの提供にあたって当初予測することができなかった様々な問題が発生することが予想されるが、できる限り長期に渡って nagoya-u.jp メールを提供しつづけたと考えている。

最後に、nagoya-u.jpメールのサービス検討について長期間にわたって協力いただいた「メールの

在り方 WG」の皆様、および、サービスの検討にあたり複数回に渡って問い合わせに対応いただいた Microsoft 株式会社様に深くお礼申し上げたい。

参考文献

- [1] 梶田将司、メールエイリアス実験サービスについて、名古屋大学情報連携基盤センターニュース 3 巻、3 号、177-178、2005 年。
- [2] The Postfix Home Page、<https://www.postfix.org/>、2024 年 10 月 20 日 閲覧。
- [3] 嶋吉隆夫、笠原義晃、清家史郎、藤村直美、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、情報処理学会研究報告 50 巻、9 号、1-8、2020 年。
- [4] Exchange Online PowerShell、<https://learn.microsoft.com/en-us/powershell/exchange/exchange-online-powershell?view=exchange-ps>、2024 年 10 月 20 日 閲覧。
- [5] 嶋田創、柘植朗、後藤明史、名古屋大学 ID の多要素認証への移行と得られた知見、情報処理学会研究報告 60 巻、9 号、1-8、2023 年。
- [6] 林豊洋、生涯メールサービスに対する Microsoft Office 365 の導入 -Yahoo!メール Academic Edition からの移行-、九州工業大学情報科学センター広報、第 28 号、83-95、2016 年。
- [7] 卒業・修了生向け九工大メールサービスの提供終了のお知らせ（2024 年 9 月）、https://www.kyutech.ac.jp/media/001/202409/20240909_kyutechmail.pdf、2024 年 10 月 20 日 閲覧。