

核融合科学研究所の電子メールサービスの Gmail と Google グループへの移行

山本孝志¹⁾, 井上望未^{1),2)}, 高山有道^{1),3)}, 井上知幸^{1),2)}, 石黒静児^{1),3),4)}

1) 核融合科学研究所 情報通信システム部

2) 核融合科学研究所 技術部

3) 核融合科学研究所 ヘリカル研究部

4) 総合研究大学院大学 物理科学研究科 核融合科学専攻

yamamoto.takashi@nifs.ac.jp

Migration process of e-mail service to Gmail and Google Groups on National Institute for Fusion Science

Takashi Yamamoto¹⁾, Nozomi Inoue^{1),2)}, Arimichi Takayama^{1),3)},
Tomoyuki Inoue^{1),2)}, Seiji Ishiguro^{1),3),4)}

1) Division of Information and Communication Systems, National Institute for Fusion Science

2) Department of Engineering Technical Services, National Institute for Fusion Science

3) Department of Helical Plasma Research, National Institute for Fusion Science

4) The Graduate University for Advanced Studies, Department of Fusion Science

概要

核融合科学研究所では電子メールサービスをオンプレミスの MailSuite で運用していたが、クラウドサービス Google G Suite for Education の導入を決めた。移行作業の期間短縮と利用者の負担軽減のため、アカウント設定やメールスプールの移行に加え、メールリングリストから Google グループへの移行における詳細設定も管理者側で行った。メールサーバの移行に伴う業務への影響を緩和させるために、運用開始の 2020 年 8 月上旬より約 1 ヶ月間において Gmail から従来の MailSuite への二重配信を行った。現在では Gmail と Google グループの運用を他の G Suite アプリと共に問題なく行っている。

1 はじめに

1.1 核融合科学研究所

大学共同利用機関法人自然科学研究機構核融合科学研究所（以下、「核融合研」）は核融合プラズマに関する学理、および、その応用の研究を目的として、国内外の大学や研究機関と共同研究を行い、世界最大の超伝導プラズマ閉じ込め実験装置「大型ヘリカル装置（LHD）」と世界トップレベルのプラズマ核融合分野専用スーパーコンピュータシステム「プラズマシミュレータ雷神」を有する。また、総合研究大学院大学の一角であるとともに、複数の大学と連携して大学院教育もあ

わせ行っている。所員は約 400 名であり管理部、技術部、ヘリカル研究部、その他の部署からなる。

1.2 メールシステム

1.2.1 MailSuite 概要

核融合研のメールサービスはこれまで代表メールサーバと呼ばれるオンプレミスのサーバ群で運用を行ってきた。核融合研設立当初の Solaris 上で構築した sendmail から、アプライアンスサーバ Mirapoint 社 M400 と M600 を経て、移行前の代表メールサーバは、仮想基盤システム上で稼働するクオリティア社（当時は DEEPSOFT 社）の MailSuite と DeepAnchor に加え、Linux 上で構築したセカンダリサーバからなるシステムで

あった。一時期は部局単位のメールサーバが存在していたが、代表メールサーバに集約している。図1に MailSuite と DeepAnchor におけるメール配送の概略を示す。MailSuite は基本的なメールサービスとメーリングリスト（以下、「ML」）機能を持ち、セキュリティ対策としてアンチウイルスとアンチスパム機能を持つ。DeepAnchor は多様なサービスを提供するが、核融合研では大容量の添付ファイル（「10MB 以上 100MB 以下」と設定）を Web のダウンロード用リンクに変換する機能を用いていた。

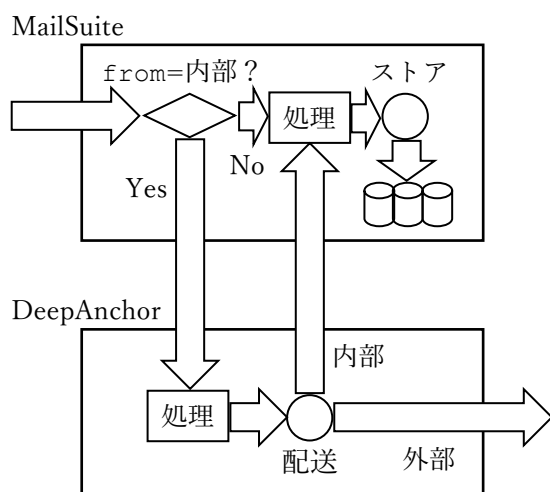


図1 代表メールシステムとメール配送

1.2.2 MailSuite のカスタマイズ機能

MailSuite の導入を検討した 2014 年は、アカウント搾取によるスパムメールの大量送信が問題となっていた。MailSuite 導入にあたりワンタイムパスワード（以下、「OTP」）による 2 段階認証が可能となるようカスタマイズを施した。E-link による名刺サイズの OTP カードを利用者へ配布して 2 段階認証を必須とした。さらに Web ログイン時だけでなく、POP、IMAP、SMTP AUTH においても、事前に Web ブラウザを通じて 2 段階認証を終えていなければ利用できないようカスタマイズを行った。この方式は非常に強力に 2019 年 7 月に利用者の錯誤によりパスワードが攻撃者に渡り、スパムメールの送信や

IMAP ログインが試みられたが、OTP 認証で防御した。

ML 機能においても、MailSuite 以前に利用していた Mailman の機能を参考にして、投稿制限とモデレート制限について、対象アドレスや除外アドレスを正規表現にて指定する機能を追加するなどのカスタマイズを行った。

これらのカスタマイズによりセキュリティと機能の両面において高レベルな電子メールサービスを提供していた[1]。

2 クラウドへの移行

2.1 オンプレミスの限界

MailSuite はセキュリティ的に満足できるものだったが、時折、送信サーバが迷惑メールの送信元と見なされ、国内外の大学や研究機関がメールを受領しないという問題があった。当初、図1に示すように、MX レコードで指定する受信サーバと送信サーバの分離が IP レピュテーションの劣化の一因と考えていたが、最近になり、セカンダリメールサーバにおけるバックスキャッターの可能性が判明した。しかしながら、対策が困難で根本的な解決に至らなかった。一方、利用者が受け取る迷惑メールも多くなり、しばしば苦情が寄せられていた。

2018 年には国内の大学にて攻撃者が搾取したアカウントを用いて被害者の個人設定を変更し、受信メールを攻撃者の元へ自動転送する事例が多発したことを受けて、核融合研のメールサービスでも緊急連絡用を除き自動転送を禁止とした。しかし、これは利便性をそこなうため、利用者からは大きな不満が出た。メールの利用頻度や重要性が高まるにつれ、メールスプールの容量制限（10GB）の拡張や、大規模な電源整備の改修が必要とされる 24 時間 365 日の運用が要請されるようになった。MailSuite の保守期限を 2020 年度末に迎えるにあたり、これらの諸条件を踏まえ、対象にクラウドサービスを含めた次期メールシ

システムの検討を 2019 年 10 月から開始した。

2.2 クラウドの選択

クラウドサービスの候補として Google G Suite for Education（以下、「G Suite」）の Gmail と Microsoft 365 for Education A3（以下、「M365」）の Exchange Online を検討した。ライセンス料金について前者は無料、後者は有料であるが、それまでに Microsoft とは Office ソフトについてサイトライセンスの契約（OVS-ES）を行っており、これを 2020 年度から M 365 に移行することが検討されていたため両者の価格面での差は考慮しなかった。一方、導入ならびに保守費用を比較した結果、MailSuite の更新案に対し、両者の優位性が明らかになった。

ML 機能については G Suite では Google グループ（以下、「グループ」）が、M365 では Exchange Online の配布リストが対応するなど機能面では差はないが、検討当時のインシデント事例や、すでに先行してクラウドを導入していた大学や研究機関の関係者へのインタビュー結果などを総合的に検討した結果、次期メールシステムとして Gmail の採用を決定した。あわせて M365 では汎用ドメイン（@nifs.jp）を扱うことになった。

3 移行準備

3.1 移行スケジュール

Gmail の運用開始時期は、例年、秋から始まる核融合研のプラズマ実験への影響を考慮して 8 月上旬と定めた。G Suite の準備は 2019 年秋より行っていたが、諸事情で作業に着手することができず、全体の見通しを得たのは 2020 年 5 月に入ってからであった。

表 1 に移行スケジュールを示す。メールシステムの移行をある時点に集中させず、利用者の都合の良いタイミングで行えるよう 1 ヶ月程の移行期間を設けた。移行期間中は新着メールを新旧両方のシステムへ配送することにより、どちらを利用しても業務に支障がないようにした。

3.2 移行方針と体制

移行作業を短期間で実施するため、移行に関する利用者への説明や問合せに要する時間を省く観点から、管理者が集中的に行うこととした。G Suite は多様なサービスを提供するが、ユーザ対応は移行の中心となる Gmail とグループの他、これに付随する Google ドライブ、カレンダー等に限定して行うこととした。

これらの移行作業の実施にあたり、情報通信システム部内に特別チームを結成し、先行導入した M365 に含まれる Microsoft Teams を用いて情報交換を行った。また、導入サポートを業者に依頼し、随時発生する問題に対する知見や、G Suite の全般的な管理方法を説明する管理者教育と、一般的な Gmail などのアプリの利用方法を説明する利用者教育の講師を依頼した。なお、データ移行やグループの設定などの実作業については導入サポートの対象外であった。

表 1 移行スケジュール

2020 年 6 月	メールスプール移行希望アンケート、管理者講習会
7 月	メールスプール移行開始 YubiKey 配布、利用者講習会
8 月上旬	Gmail 利用開始 移行期間開始（MailSuite への二重配信開始）
8 月末	移行期間終了（MailSuite への二重配信停止）
9 月上旬	2 段階認証の設定期限
12 月	名誉教授用アドレスの Gmail への移行
2021 年 3 月末	MailSuite の運用終了

4 移行作業

4.1 Education 認定とドメイン設定

2019 年 12 月の Google による G Suite for Education の利用認定と並行してドメイン設定を

行った。その際、実際に利用するドメイン (@nifs.ac.jp)をプライマリドメインに、検証用ドメインをセカンダリドメインに登録した。

4.2 アカウント

4.2.1 認証方式と初期パスワード

アカウントの管理方式は既存の MailSuite と同様のローカル認証とした。将来的に M365 と合わせて管理を行う統合認証システムを導入する予定である。初期パスワードは MailSuite の暗号化されたパスワードをそのまま Google App Script (以下、「GAS」)から Directory API で G Suite のパスワードとして設定し、初回ログイン時に変更を求めた。

4.2.2 2段階認証の設定と YubiKey の配布

MailSuite と同様に Gmail においても 2 段階認証を必須とした。2 つ目の要素としては、電話での音声案内、スマホへの SMS、認証アプリ (Google Authenticator) 等から複数選択するよう促した。また、スマホを持たない、あるいは、利用したくない利用者やバックアップ用途として、YubiKey (Yubico YubiKey 5 NFC)を調達し、利用者全員に配布した。この 2 段階認証の設定については、予定していた期間内に全員が対応を完了した。

4.3 Gmail

4.3.1 メールスプールの移行

メールスプールの移行は Google が提供する G Suite Migration for Microsoft Exchange (以下、「GSMME」)を用いて管理者側で一括して行った。アカウント数は約 400 で対象メール数は約 400 万通であった。並行処理数はデフォルトの 25 として、可用性を考慮して同一性能の 2 台の移行サーバで行った。ユーザリストをメール数でソートし、2 台に順に割当てて処理総数をそろえた (No.1 2,093,375 通、No.2 1,959,036 通)。GSMME のマニュアルには 1 通 3 秒の処理時間と記載があり、事前の実機テストでも同程度の速

度で処理されることを確認した。理想的な場合、全体の移行に要する時間は、 $4,000,000 \times 3 / (25 \times 2) = 24,000$ [秒]と 3 日 (259,200 秒) 以内に終わるが、実際には利用者単位でセッションが固定されるため、大口利用者の影響を受ける。

移行前に、大口利用者に対して不要なメールの削除依頼と IMAP の負荷を軽減するため (開始直後のフォルダ探索時にロードアベレージが 30 程度まで上昇する) MailSuite のメモリを 16MB から 24MB へ増強した。なお、事前に移行作業を自身で行う利用者を募ったが 2 名だけであった。

初回の移行状況を図 2 に示す。破線で示した急峻な右上りの集計処理部と実線のゆるやかな右下がりの移行処理部に分かれる。1 回目の実行は、意図しない Windows Update による再起動 (No.1) とネットワークタイムアウトによるコネクションの終了 (No.2) で中断した。Windows Update の一時停止とレジストリキーの調整後 [2]に再実行させた。No.1 の 7/11 近傍における未配送数が前後より多く見えるのは、誤って本来移行すべきではないフォルダ (「迷惑メール」など) を移行対象に含めてしまったためである。No.2 は理想的に 3 日間程で終了するところだったが、7/10 の再実行時に何等かの原因でリセットされた。No.1 は後半の移行速度が遅くなっている。これはフォルダ数が No.1 に偏在したためと推察される。

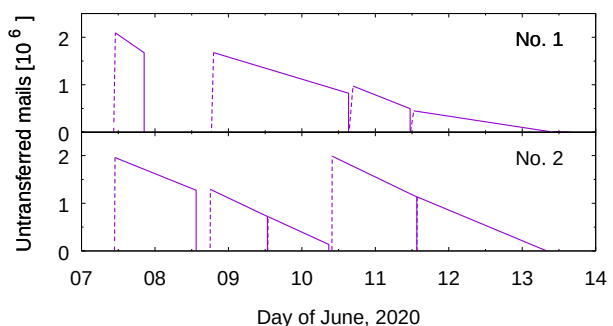


図 2 初回のメールスプール移行進捗図

以降は週に1度のペースで移行を実施し、各々1日程度で終了した。最終となる5回目は運用開始前日に行った。その回には、4.3.3節で述べるGmailからMailSuiteに転送されたメールが含まれたが、Gmailは同じメッセージIDのメールは1通しか表示しないため、利用者への影響はなかった。利用者には運用開始後に各自でGmailのスプールを確認し、不足分はMailSuiteを参照するよう通知した。

なお、GSMMEを利用するにはMailSuiteの利用者のパスワードの設定とOTP認証の回避が求められた。そのため、マスターパスワードによるアクセス許可とOTP認証の回避機能をMailSuiteに持たせるようクオリティア社に改修依頼を行った。

4.3.2 エイリアス

メールのエイリアス設定もGASを用いて行った。研究所が@nifs.ac.jpを管理ドメインとして設定する前に、個人で@nifs.ac.jpのアカウントを取得していた場合、研究所によるアカウントやエイリアスの設定と重複すると、個人のアカウント名は一時的なドメイン名に強制移行されてしまう。事前に個人アカウントを研究所が管理する組織アカウントに移行する選択肢もあるが、個人アカウント時に作成されたデータが組織の管理下におかれるため、この選択は行わなかった。個人アカウントが他の大学・研究機関や組織が管理するGoogleグループに登録されていると、重複した時点でGoogleによりメンバー名が一時的なドメイン名のアカウントに強制変更され、結果として以前の@nifs.ac.jp宛に届かなくなる事象が生じた。

4.3.3 移行期間中の二重配信

確実に運用開始日から新着メールがGmailに届くよう、その4日前にはMXレコードをMailSuiteからGmailに切替えた。1ヶ月間の移行期間中はGmailに到着した新規メールがMailSuiteにも二重配信されるようGmailの管理

者設定の転送機能を設定した。その際、Gmailに到着した全てのメールをMailSuiteに転送するとML宛のメールはGmailとMailSuiteの両方から配送されるため注意が必要である。幸い、Googleの転送設定では宛先をユーザとグループとその他に判別するオプションがあり、これを回避することができた。このような設定は事前に検証用ドメインを用いて確認した。

二重配信はGoogleも推薦する既存のMailSuiteをプライマリとしてGmailへ転送する方法があるが[3, 4]、以下の利点からGmailからMailSuiteへ転送を選択した。

- 利用者が送信したメールが迷惑メール扱いされないようにする
- 利用者に届く迷惑メールを減少させる
- 外部からのメールはGmail経由となるため、早期にGmailに移行すれば、MailSuite側に問題が発生しても影響を受けない

移行期間中、MailSuite内部で配送されるメールもGmailに転送する必要がある。これは図1のDeepAnchorの配送先をMailSuite固定からMXレコードの参照に変更することで対応した。その際の注意事項として、二重配信中は両方のシステムでアカウントとML(グループ)を作成する必要がある。利用者宛メールがMailSuiteに送付されると、そのメールは内部配信となるために、着信した時点でアカウントやMLアドレスの存在確認が行われるためである。MailSuite上のMLについてはGmailへ転送されるためメンバーを追加する必要はない。

4.3.4 メールクライアントと自動転送の制限

POPやIMAPを用いるメールクライアントはOAuth認証に対応するものに限定した。アプリパスワードによる認証方式(安全性の低いアプリ)については、Googleより推奨されていないため無効とした。

個人の自動転送についてはGmailでも原則禁止であるため、個人による設定項目から除外した。

例外として認められた設定は管理者による設定で対応しているが、MailSuite 時からその件数は大幅に減少した。

4.4 Google グループ

4.4.1 グループ概要

MailSuite における ML 機能は Google グループのメール配送機能を用いることにした。グループにはメール配送以外にも Web フォーラム機能や、Google ドライブの共有範囲の指定など幅広く利用されているため、設定には十分な注意が必要である。移行対象の ML 数は約 500 件、延べメンバー数は約 1 万 6000 人であった。なお、ML のアーカイブの移行は、利用者から要望がなかったため行わなかった。

4.4.2 グループとメンバーの設定

グループの作成とメンバーの追加は Web 管理画面より CSV ファイルによる一括設定が可能である。今回は、グループの作成は CSV ファイルで、メンバーの追加は GAS で行った。メンバーの追加を CSV ファイルで行う場合は、そのアドレスが利用者かグループかを指定する必要があるが、GAS ではその必要がなかったためである。GAS でのメンバーの追加では G Suite の 30 分の実行時間制限により途中終了したため、その度に手動で再開させた。平均 0.97 通/秒の処理速度であった。

4.4.3 詳細設定

一般的に ML の詳細設定は、管理者がグループの作成など大枠を設定した後に、各 ML 管理者が行うが、今回は管理者による一括設定を行った。

設定箇所は MailSuite の約 20 か所に対し、グループでは約 60 か所である。グループ設定の大部分は Web 管理画面から行えるが、500 件の ML の設定を手入力で行うことは非効率であるため、GAS から Directory API と Groups Settings API を用いて行った。MailSuite の ML の設定ファイルから項目毎にその情報を CSV ファイルに収集し、これらをまとめた Google スプレッドシート

から GAS を実行した。

MailSuite のカスタマイズで投稿制限やモデレート制限を正規表現が含まれたメールアドレスで指定する機能を追加していたが、一部の ML では無効な設定や矛盾した設定がされていたため、ML 管理者に問合せた後に手動にてグループのメンバーの属性を変更した。また、ML 管理者を補助する ML サブ管理者の割り当て機能も追加していたが、この情報を抽出するために、MailSuite の管理コマンドの機能追加をクオリア社に依頼した。

サブジェクトの先頭にグループ固有のテキストを挿入する機能など、グループの一部の設定項目は Web 管理画面からのみ設定可能であった。設定項目は少数だが、これらについても、自動ブラウザ操作ツール Selenium WebDriver と Python を用いて自動設定を行った[5]。

4.5 G Suite の設定

G Suite が提供するアプリケーションの多くについて Gmail の運用開始と同時に利用者へ公開した。Google ドライブにて組織外ユーザが共有されたファイルにアクセスする際には、Google アカウントによるログイン等を求めるなど、一部においてはセキュリティ維持を目的とした制限をおこなっている。

Gmail などのファイルを保管する Google Vault については、情報セキュリティ委員会の審議の結果、その保管対象を対応可能な全データと定め、運用時から有効とした。運用開始前に作成された MailSuite のメールスプールは除外した。情報セキュリティ委員会では濫用を防止するための運用ガイドラインの策定も決められた。注意点として利用者のアカウントを削除すると関連する Google Vault のデータも削除される。この回避策として利用終了のユーザを削除ではなく停止状態としているが、ライセンス数を消費するため、将来、有料版の G Suite for Education Enterprise に移行する場合は問題となりえる。

4.6 利用者への情報提供

利用者への情報提供として、利用者講習会の開催や Web サイトを通じた説明とマニュアルの配布を行った。

利用者講習会では、前半に業者による一般的な Gmail やグループなどのアプリケーションの使い方の説明、後半に核融合研の担当者による移行時の注意事項の確認が行われた。通常ならば、会議室に参集するところ、COVID-19対策のため、Google Meet によるリモート参加をメインとした。この時点では Google より COVID-19 対策として参加者数の上限緩和（100 名から 250 名）とビデオ録画機能の提供があり、これを活用した。参加者は会議室約 20 名、リモート参加約 160 名であり、参加できなかった利用者についてはオンデマンド受講を可能とした。

研究所では海外からの研究者も多数在籍するが、これらの資料は時間の制約もあり日本語版のみ提供した。

5 移行期間中の問題と今後の予定

5.1 移行期間に発生した問題

5.1.1 DeepAnchor の経路設定

MX レコードの切換えは、余裕を持たせるために、運用開始前の週末に実施した。一方、DeepAnchor の経路変更の設定漏れがあったが、切り替え直後に気が付き全体の影響はなかった。

5.1.2 SPF レコード

週明けになり、一部のサイトのメールが Gmail で受信した後に MailSuite に転送されていないことがわかった。これは、MailSuite の IP レピュテーション向上のために 2020 年 7 月より有効にしていた SPF レコードによる制限が原因であった。各サイトのメールは Gmail 経由で MailSuite に届くため、送信者アドレスが Gmail の IP アドレスとなり、SPF レコードにより指定された送信サーバと相違が生じ、fail (-a11) の指定があるサイトのメールを受信拒否していた。Gmail の送信サ

ーバを例外とすればよいが、その IP アドレスが明確ではなかったため、SPF レコードによる判定を無効とした。また、利用者に対してアナウンスを行い、運用開始前であったが休日に送信されたメールを確認する目的のため Gmail へのアクセスを可能とした。

5.1.3 転送サーバ

運用開始より 1 週間後に所内サーバから送信したメールの一部が Gmail へ転送されていないことがわかった。これは、送信者アドレスが FQDN 形式であると MailSuite は別途指定しない限り外部サーバからのメールとみなし、DeepAnchor への転送を省略するため、Gmail への転送が行われなかったことによる。当初、該当サーバ管理者へ送信者アドレスをホスト名を含まない@nifs.ac.jp 形式への変更を依頼したが、その後、中継サーバを設置し、所内からの送付先を中継サーバへ変更するよう依頼した。MailSuite の運用終了時には、中継サーバを MailSuite の IP アドレスに変更する予定である。

5.2 移行期間終了と 2 段階認証の徹底

予定通り移行期間の終了日である 8 月 31 日夕方に Gmail から MailSuite への転送を停止した。この時点でも、まだ Gmail へ未ログインやログインしたが 2 段階認証が未設定であるアカウントが残されていたため、再度依頼した結果、全員が期日前に 2 段階認証の設定を完了した。

5.3 今後の予定

5.3.1 名誉教授用ドメインの移行

核融合研では、名誉教授に対し終身利用可能なアドレス(以下、「名誉教授用アドレス」)を付与している。名誉教授用アドレスも MailSuite で稼働しており、2020 年 12 月中に Gmail への移行を開始する予定である。なお、名誉教授用アドレスの ML は運用していないため作業の省力化が見込まれるが、利用者サポートが基本的にリモートとなるため対応に大幅な負担増が予想される。

5.3.2 MailSuite の運用終了

既存の MailSuite の保守契約は 2021 年 3 月末まで有効であるため、名誉教授用アドレスの移転後もしばらくの間は所内からの参照用として運用を継続する予定である。MailSuite は仮想基盤システム上に構築されているため、運用終了後は他のサーバのリソースとして開放する。

5.3.3 中国問題への対応

核融合研でも出張者が多い中国では Gmail の利用が困難である。一般的な対策としては Google などのサービスへの接続を保証するレンタル WiFi を利用する方法があるが、無料版の Outlook on the web など他社サービスの Web メールの利用も考えられる。

6 結論

核融合研は設立当初からオンプレミスで電子メールサービスを提供していたが、検討の結果、クラウドサービスの Gmail に移行した。メールスプールの Gmail 移行については GSMME を用いることにより実施し、グループへの移行も個別に作成した GAS プログラムから Google API を利用することにより実施した。Gmail の運用開始から 1 か月間を移行期間と定め、Gmail から MailSuite への二重配信を設定した。その間に発生した問題を早期に解決し、現在は安定運用を行っている。

移行にあたり、検証用ドメインによるテストは実際の設定を確認できるため非常に有意義であった。MailSuite の導入時に、利用者認証と ML 管理について機能強化したが、そのいずれもが、Gmail の移行にあたり予想外の障壁となった。

今後も核融合研の研究活動を促進するよう、電子メールサービスに限定せず、G Suite の各種アプリの活用と M365 など他のクラウドサービスの探求と連携を進める。

参考文献

- [1] クオリティア、MailSuite 導入事例:核融合科学研究所、https://www.qualitia.co.jp/case/ms_nifs.html、(2020 年 9 月 30 日参照)。
- [2] Google、GSMME エラーコード、<https://support.google.com/a/answer/2624575>、(2020 年 9 月 30 日参照)。
- [3] Google、二重配信の設定、<https://support.google.com/a/answer/96855>、(2020 年 9 月 30 日参照)。
- [4] 宮部、戸田、南部他、京都大学教職員用メール SaaS 移行の経緯、AXIES 年次大会、TD2-2、2019。
- [5] the Selenium Project、Selenium、<https://www.selenium.dev/>、(2020 年 9 月 30 日参照)。