九州大学における Office 365 サービス環境の再構築

嶋吉 隆夫 [1)], 笠原 義晃 [1)], 尾花 昌浩 [2)], 藤村 直美 [1)]

1) 九州大学 情報基盤研究開発センター

2) 九州大学 情報システム部

simayosi@cc.kyushu-u.ac.jp

Restructuring of Service Infrastructure for Office 365 in Kyushu University

Takao Shimayoshi[1)], Yoshiaki Kasahara[1)], Masahiro Obana[2)], Naomi Fujimura[1)]

1) Research Institute for Information Technology, Kyushu University

2) Information Systems Department, Kyushu University

概要

九州大学では 2016 年から Office 365 を全学サービスとして正式に提供してきたが、その基盤システムやテナント運用などについて様々な課題が生じていた。そこで、基盤システムとテナントを含めて環境を新たに再構築し、2018 年 4 月から新しいサービス環境の提供を開始した。本稿では、従来の環境における課題とその解決策、さらに、新しい環境の構築過程で生じた問題とその解決方法などについて紹介する。

1 はじめに

Microsoft 社が提供する Office 365 Education はクラウドアプリケーションスイートの教育機関用エディションである。Office 365 の基本機能は教育機関に対して無償で提供されており、それには、Office Online, OneDrive for Business, Exchange Online, Skype for Business, SharePoint Online などが含まれる。本稿では Office 365 は Office 365 Education を指す。

九州大学では、2015 年から日本マイクロソフト社と結んでいる包括契約 Enrollment for Education Solutions (EES) に Office 365 ProPlus のライセンスが含まれることを受け、Office 365 の全学サービス導入について検討と評価が始められた。その後、2015 年度中に試験サービスとして提供を開始し、それを 2016 年 4 月から正式サービスとして全構成員に提供した。Office 365 の試験サービス提供以降、サービス提供のための基盤システムの管理、運用や、サービスの提供方法、内容などについて、様々な課題が明らかとなってきた。そこで検討の結果、課題を解決するため、新たなサービス環境を構築し、従来のサービス環境を廃止して移行することとした。その後、2018 年 4 月から新しい環境で正式サービスを提供している。

本稿では、九州大学における Office 365 のサービス環境を再構築した経緯と経過を紹介する。まず最初に 2 章で前提となる九州大学における構成員の識別情報について説明したのち、3 章で以前のサービス環境の構成と課題について述べる。次いで 4 章で新たに構築したサービス環境の設計について述べたのち、5 章で実装や配備、移行の方法、また、移行に際して直面した問題と解決策などについて述べる。最後に 6 章で、今後の計画と課題について述べる。

2 九州大学の構成員識別情報

九州大学では全構成員に対して、複数の情報サービスで共通して利用できる ID として SSO-KID を発行している。SSO-KID は、過去の構成員も含めて重複のない 10 桁の数字であり、個人と SSO-KID の対応が特定できないように無作為に割り振られる。全構成員の情報が格納される全学共通認証基盤の全学共通 ID 管理システムが SSO-KID を決定する。SSO-KID とパスワードの一覧は厳重に管理され、学外持出しは禁止されている。なお、全学共通 ID 管理システムでは各アカウントに対してシリアル番号である UID が付与されている。また、学生は SSO-KID 以外に、学籍番号として学生 ID を持つ。

九州大学では全構成員に対して全学基本メールサービスが提供されている。学生には “⟨学生 ID⟩@s.kyushu-u.ac.jp”、教職員には “⟨姓⟩.⟨名⟩.⟨数字⟩@m.kyushu-u.ac.jp” という全学基本メールアドレスが割り当てられる。

3　以前のサービス環境

3.1　構成

本節では、2015 年度に試験サービス、2016 年度から正式サービスとして提供していた Office 365 テナント、および、その基盤システム（以降、旧環境）[1] について説明する（図 1）。九州大学の Office 365 サービスは、教育機関向けに無償で提供される Office 365 Education (Office 365 A1) と、EES に含まれる Office 365 ProPlus のライセンスを組み合わせて使用する。Office 365 テナントを作成すると自動的に “⟨テナント名⟩.onmicrosoft.com” というドメインが割り当てられるが、一般的に組織のドメイン名をテナントに登録する。旧環境では、九州大学で以前に使用していなかったドメイン名 ms.kyushu-u.ac.jp を登録していた。

Office 365 ではユーザー識別認証サービスとして Azure Active Directory (Azure AD) が使用される。Office 365 のユーザー情報は Azure AD に格納され、ユーザーは user principal name (UPN) により識別される。旧環境では UPN として、全学基本メールアドレスのローカルパートの後に、学生、教職員によらず、@ms.kyushu-u.ac.jp を加えたものを Office 365 専用に付与していた。また、ユーザーの認証には、Azure AD を利用するクラウド認証と呼ばれる手法を用い、Office 365 専用パスワードを Azure AD に保存していた。

九州大学では構成員情報は全学共通認証基盤に格納されており、その情報を元に Azure AD にユーザー情報を設定する必要がある。その実現に、旧環境では以下の方法を用いていた。まず、オンプレミスの Active Directory（以降、オンプレ AD）を Office 365 専用に学内の仮想化基盤上に構築し、全学共通認証基盤からオンプレ AD に Office 365 のユーザー情報を登録する。全学共通認証基盤の登録内容に変更があれば、全学共通 ID 管理システムの機能により自動的にオンプレ AD の内容も変更される。次いで、オンプレ AD の内容は、Microsoft 製の Windows Azure Active Directory Sync (DirSync) を用いて Azure AD へと定期的に同期される。

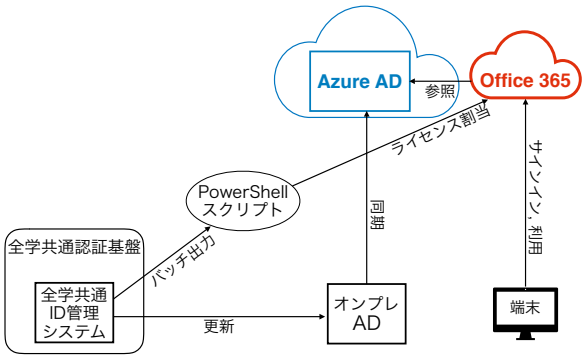

図 1　旧環境の構成

Office 365 の利用には、Azure AD へのユーザー登録だけでなく、各ユーザーにライセンスを割り当てる必要がある。旧環境では、全学共通認証基盤で追加、削除等のあった構成員の一覧を、全学共通 ID 管理システムの機能を用いて日次バッチ処理にて CSV に出力し、独自開発の PowerShell スクリプトにより処理することで、ライセンス割当、削除を行っていた。

3.2　課題

旧環境のサービス稼働後に、オンプレ AD と Azure AD との同期に使用していた DirSync は 2017 年 4 月にサポートが終了し、また、2018 年 1 月以降は DirSync からの通信を受け入れなくなることが発表された。これに対処するためには、DirSync から Azure AD Connect へと移行する必要がある。しかし、DirSync と Azure AD Connect では、ユーザー同期に必須の属性など、仕様に相違があることが判明し、全学共通認証基盤からオンプレ AD にユーザー情報を登録する部分についても変更が必要であった。

前述の通り旧環境では、Office 365 のユーザーへのライセンス割当処理に、全学共通 ID 管理システムの機能と独自開発の PowerShell スクリプトを用いていた。しかし、構成員の追加、削除における全学共通 ID 管理システムの動作が、必ずしも PowerShell スクリプト設計段階での想定通りではなかったことから、少なくない割合の新規構成員について Office 365 のライセンスが割り当てられないという不具合が発生していた。その後 PowerShell スクリプトに対して何度か対症療法的な改修が行われたものの、最後まで根本的な解決には至らなかった。なお、その設計開発は全学共通 ID 管理システムの開発元が受注していた。

九州大学では全学基本メールサービスを独自構築したシステムにより運用していることから、旧環境での Office 365 テナントではメールサービスである Exchange Online を無効にしていた。しかし、サービス提供開始後に、Skype for Business などにおいて Exchange Online を有効にしなければ一部機能に制限があることが明らかとなった。また、サービス導入時点で Office 365 の仕様や機能について十分な理解が不足していたこともあり、正式サービス開始以降に、運用部門が想定していなかった使い方を利用者が行っていることが確認できたが、後から設定を変更する

ことは既存利用者への影響から困難であった。さらに、SSO-KID とパスワードは外部に出せないことから UPN には SSO-KID 以外の文字列を用いる必要があったが、準備期間が短く十分な検討ができなかったことから、旧環境テナントでは前述の通り Office 365 専用の UPN を採用していた。しかし、その UPN は全学基本メールアドレスと混同しやすく、また、他ユーザーを指定する際などの利便性が高くなかった。これらのことから、Office 365 テナントの設計や構成について再検討が求められていた。

九州大学では、前述の通り全学基本メールサービスを独自システムで運用しているが、2019 年 1 月にそのシステムの保守期限を迎える。そのシステム更新については Office 365 サービス再構築とは独立して検討されていたが、選択肢として Exchange Online を利用する案も検討されていた。旧環境は全学基本メールサービスとは完全に独立した設計だったが、検討の結果次第で全学基本メールサービスが移行できる環境にしておくことが望ましいと考えられた。なお最終的に、全学基本メールサービスは 2018 年 12 月に Exchange Online に移行する計画が決定されている。

4　設計

4.1　要件

九州大学で全学共通 ID として発行している SSO-KID は、秘密情報ではないが他者に安易に開示するものではない。また、2 節で述べた通り、SSO-KID の一覧の学外持出しは禁止されている。つまり、クラウドサービスである Azure AD に保存されるユーザー情報には SSO-KID を登録できない。

Office 365 では、テナント内のユーザー一覧を表示する機能や、UPN や個人名、メールアドレスの一部からユーザーを検索する機能がある。しかし、学生が学生や教職員の一覧を取得可能だと問題である。また、九州大学の学生 ID は基本的に連番で付与されることから、任意の学生 ID だけから個人情報が容易に判明することには問題がある。それゆえ、学生によるユーザー一覧の取得や学生 ID から個人情報の取得ができないようにする必要がある。

Office 365 では、OneDrive for Business や Exchange Online の記憶容量はユーザーごとに確保されるが、SharePoint Online の記憶容量はテナント全体での総量が制限される。このようなテナント全体で共有する資源が、構成員による無思慮な利用によって浪費されることのないよう注意する必要がある。

4.2　構成

4.1 節で述べた要件を満たしつつ 3.2 節で述べた課題を解決するため、全学共通認証基盤から Azure AD への連携や認証のシステムを再構築し、また、テナントについても新たなテナントを作成して移行する方法を採用した。これは、旧環境の部分改修だけでは問題の抜本的解決が非常に困難であり、正式サービス開始からの期間が短ければ利用者への影響は比較的小さいと判断したことによる。本節では、九州大学における新しい Office 365 サービス環境（以下、新環境）の設計および構成について述べる（図 2）。

■テナント構成　Office 365 テナントは、学生、教職員を同じ単一のテナントに収容する。学生および教職員の一覧を学生には取得不可能にするという要件から、学生と教職員とでテナントを分割する方法についても検討を行ったが、同一テナントに収容しても要件が実現できること、テナントを分割すると構成や運用が複雑になることから、採用しなかった。

■ユーザー認証　SSO-KID とパスワードを Azure AD には保存しないという要件を満たし、かつ、Office 365 へのサインインを全学共通 ID である SSO-KID とそのパスワードで可能にすることを目的として、Office 365 のユーザー認証に Active Directory フェデレーションサービス (AD FS) を用いたフェデレーション認証と呼ばれる構成を採用する。オンプレ AD と、それを参照する AD FS サーバを構築し、オンプレ AD から Azure AD へとユーザー情報を同期させ、Azure AD への認証要求は AD FS サーバへとリダイレクトする。この構成では、Azure AD にパスワードを保存する必要がない。なお、SSO-KID を Azure AD に保存しないためには後述の方策が必要である。上記目的の実現方法として他に、Azure AD が対応している SAML を利用したシボレス認証を用いる方法も考えられたが、今回は、Microsoft 製品として提供される AD FS を用いる

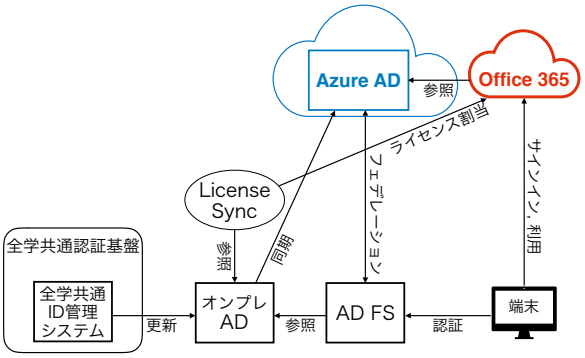

図 2　新環境の構成

方が Office 365 のサポート情報が得られやすいとの判断から、AD FS を採用した。

■サーバ構成　上記の認証方法は、以下のシステム構成により実現する。旧環境のオンプレ AD を構築していた仮想化基盤は導入時の保守期限を 2018 年度中に迎えることから、IaaS である Microsoft Azure 上にシステムを構築することとした。SINET が提供するクラウド接続サービスと Azure ExpressRoute を利用して、九州大学の内部ネットワークサブネットを Azure 上の仮想ネットワーク (VNet) として作成し、その VNet 上の仮想マシンによりシステムを構築する。それに先立ち、全学共通認証基盤が構築されている仮想化基盤の上に、全学共通 ID 管理システムと直接連携する Active Directory ドメインコントローラを準備し、AD DS を稼働させる。このオンプレ AD は今後 Office 365 以外の学内サービスによる利用も想定している。次に、上記のドメインコントローラをレプリケーションするサーバ 1 台、AD FS を稼働する冗長構成のサーバ 2 台を Azure VNet 上に配備する。これらはインターネットからのアクセスを禁止する。最後に、インターネットからのアクセスを許可する WAP サーバ 2 台を冗長構成で配備する。

■Active Directory 登録内容　全学共通認証基盤からオンプレ AD のユーザー情報に登録する内容は、他のサービスで今後利用することも考慮して検討した。Active Directory でユーザーオブジェクトの相対識別名として用いられる CN (Common-Name) 属性には、全学共通 ID 管理システムの UID を登録する。ユーザーのログオン名を表す sAMAccountName 属性には SSO-KID を、userPrincipalName 属性には SSO-KID の後に@kyushu-u.ac.jp を加えた文字列を登録する。メールアドレスを表す mail 属性には全学基本メールアドレスを、mailNickname 属性には全学基本メールアドレスのローカルパートを登録する。しかし、この状態で単純に Azure AD Connect を用いてオンプレ AD から Azure AD へと同期すると、Office 365 の UPN はオンプレ AD の userPrincipalName 属性が使われることから、UPN に SSO-KID が含まれることになる。そこで、Azure AD Connect の設定において、Office 365 の UPN にオンプレ AD の userPrincipalName 属性以外を用いる代替 ID と呼ばれる方法を採用する。全学基本メールアドレスは他者への開示が前提であるので、Office 365 の UPN として全学基本メールアドレスを用いることにし、代替 ID として mail 属性を指定する。さらに、Azure AD Connect の既定の動作では、sAMAccountName 属性は Azure AD に同期され、また、代替 ID を利用した場合、オンプレ AD の userPrincipalName 属性は Azure AD の onPremisesUserPrincipalName 属性に同期されることから、そのままでは Azure AD に全ユーザーの SSO-KID が保存されることになる。これを避けるため、上記の SSO-KID を含む属性や他の同期不要な属性について、同期規則エディターによりフィルター処理を構成することで、Azure AD に同期されないようにする。ここで、代替 ID 構成を用いる場合は、代替 ID、今回は mail 属性が変更になった場合でも、オンプレ AD と Azure AD 間でユーザーを永続的に一意対応させるために、Azure AD の sourceAnchor 属性をオンプレ AD の何らかの属性と同期する必要がある。新しい Azure AD Connect では ConsistencyGuid 機能により、ユーザーの初回同期時に自動的にオンプレ AD の ms-DS-ConsistencyGuid 属性に値を書き込み sourceAnchor 属性として使用することができる。しかし今回は、Active Directory を再構築などした場合でも継続的に Azure AD と同期できることを考え、ms-DS-ConsistencyGuid 属性に UID と固定文字列を結合した文字列をバイナリ値として登録する。

■ライセンス割当　旧環境では全学共通 ID 管理システムの機能を用いてライセンス割当、削除すべき構成員の一覧を作成していたが、この方式には様々な課題があることが明らかになっていた。そこで、全学共通 ID 管理システムからはオンプレ AD ユーザーの属性に値を設定するだけとし、別途、オンプレ AD ユーザーの属性値を元に、対応する Office 365 ユーザーにライセンスを割当、削除する構成を採用する。その実現に、サイオステクノロジー社のツール LicenseSync を利用する。全学共通 ID 管理システムから各オンプレ AD ユーザーの特定の属性に対して、ライセンス割当情報に対応するコード値とコード更新フラグを設定する。上記 LicenseSync は、一定時間ごとに AD ユーザーのコード更新フラグを確認し、更新があれば Office 365 のライセンス割当内容を変更する。

5　実装・配備・移行

5.1　移行計画

旧環境と新環境とを一定の期間に並行運用し、旧環境に保存されているコンテンツは利用者に各自で新環境へ移行してもらうこととした。新環境は 2017 年度内に稼働させて試験運用を行ったのち、2018 年 4 月から正式サービスとして提供し、旧環境は 2018 年 7 月

末でサービス提供を廃止することとした。

2018 年 1 月以降は DirSync による同期が停止するため、それ以降は全学共通認証基盤での登録内容の変更が Azure AD に反映されない。特に、新たな構成員は新環境の提供開始まで Office 365 が利用できない。そこで、新規構成員については要求に応じて手動で Office 365 アカウントを作成することとした。

5.2 新環境テナントの準備

新環境のテナントにはドメインとして、九州大学のトップドメイン名である kyushu-u.ac.jp、全学基本メールアドレスのドメイン名に利用される s.kyushu-u.ac.jp, m.kyushu-u.ac.jp を登録することとした。しかし、全学基本メールアドレスで利用しているドメイン名の登録には以下の追加作業を要した。

Microsoft 社は、教育機関が発行するメールアドレスのドメイン名が Office 365 テナントに登録されていない場合、そのメールアドレスを持つ者が自身で登録して Office 365 を利用できるセルフサインアップというサービスを提供している。セルフサインアップに用いられたドメイン名は、セルフサインアップ用に自動作成されるテナントに登録され、同じドメイン名を用いてセルフサインアップを行ったユーザーはそのテナントに登録される。s.kyushu-u.ac.jp と m.kyushu-u.ac.jp は旧環境テナントには登録していなかったことから、いずれについても既にセルフサインアップ用テナントに登録されていることが分かった。

これらのセルフサインアップ用テナントの登録ドメインから上記ドメイン名を削除する作業を以下の手順で行った。まず、s.kyushu-u.ac.jp および m.kyushu-u.ac.jp をドメイン名とするメールアドレスでセルフサインアップを行う。そのメールアドレスで Office 365 にサインインしたのち、管理画面にアクセスしてドメイン名の所有権確認の手続きを行うと、そのユーザーは当該テナントの管理者権限が得られる。ここで、ドメイン名の所有権確認には DNS の TXT レコードの変更が必要である。次いで、対象ドメイン名を削除可能にするために、全ユーザーの登録情報からそのドメイン名を削除する必要がある。セルフサインアップ用テナントについても onmicrosoft.com のサブドメインが割り当てられているので、全ユーザーの UPN について対象ドメイン名から onmicrosoft.com サブドメイン名へと変更する。ただし、この作業を実施すると、利用者はセルフサインアップしたメールアドレスで Office 365 にサインインできなくなるので、事前に登録されているメールアドレス宛にサインイン用アドレスが変更になることを連絡した。

ここまでの作業により本来は対象ドメインをテナントから削除できるはずであるが、実際にはドメインの削除に失敗した。これは、当該テナントでは全ユーザーで Exchange Online が無効であるにもかかわらず、理由は不明だが一部ユーザーに Exchange Online に関する情報が登録されており、その中に削除対象ドメイン名が含まれることが原因だと分かった。しかし、Exchange Online は有効化されていないので、どのような手段でも該当する情報は削除できない。そこで、当該ユーザーに対して一旦 Exchange Online を有効化して情報を削除したのち再度 Exchange Online を無効化することで、問題を解決した。

5.3 テナント設定

5.3.1 一般ユーザーによるユーザー情報取得の禁止

Office 365 では既定の動作として、全ユーザーの情報はグローバルアドレス一覧 (GAL) に登録され、GAL は全ユーザーが参照できる。これを回避するテナント全体の設定項目は存在しないが、個別ユーザーについて GAL への登録可否を設定できる。オンプレ AD から同期されているユーザーの場合、オンプレ AD ユーザーの msExchHideFromAddressLists 属性に False を設定すれば、そのユーザーは Office 365 テナントの GAL に登録されない。ただし、その同期には、オンプレ AD ユーザーに mailNickname 属性を設定する必要があることに注意されたい。今回、他の構成員の情報を学生が取得することを不可能にするために、全学共通 ID 管理システムから全オンプレ AD ユーザーの msExchHideFromAddressLists 属性に False を設定するようにした。

OneDrive for Business などではユーザーを検索する機能があるが、これは前述の GAL とは独立であり、既定では UPN や個人名、メールアドレスの一部からユーザーを検索できる。この状態だと、容易に全ユーザーの一覧を作成できる。SharePoint Online の設定に、メールアドレスか UPN の完全一致の場合にだけ検索可能とする SearchResolveExactEmailOrUPN 項目がある。これを True に設定することで、検索によるユーザー一覧作成を回避した。

Office 365 テナントの既定の設定では、一般ユーザーであっても Azure ポータルに接続して Azure AD にアクセスできる。これを防ぐため、Azure ポータルで条件付きアクセス機能の設定を行った。しかしこの設定だけでは、一般ユーザーが PowerShell などを用いて Azure AD に直接アクセスすれば、全ユーザー情

報を取得できる。Office 365 テナント全体設定には、一般ユーザーによる他のユーザー及びグループの情報の取得を制御する UsersPermissionToReadOtherUsersEnabled 項目がある。これを False に設定することで、一般ユーザーが Azure AD からユーザー一覧やユーザー情報を取得できないようにした。

5.3.2 一般ユーザーによるグループ作成の禁止

Office 365 には Office 365 グループという機能があり、Office 365 グループを作成すると、それに伴い、Exchange Online の共有メールボックスのメールアドレスが作成され、また、SharePoint Online のチームサイトが作成される。Office 365 テナントの既定設定では、一般ユーザーが Office 365 グループを作成できる。しかし、一般ユーザーに Office 365 グループの自由な作成を許すと、組織ドメイン名のメールアドレスが自由に作成でき、管理上の問題がある。また、SharePoint Online のチームサイトは既定では容量の上限が設定されず、テナント全体の共有資源を浪費される可能性がある。そこで、一般ユーザーによる Office 365 グループ作成を禁止する設定を行った。テナント全体でグループ作成を禁止するためには、Azure AD ディレクトリ設定の EnableGroupCreation 項目を False に設定する必要がある。なお、Office 365 テナント設定には、一般ユーザーによるセキュリティグループの作成を制御する項目もあるが、これは Office 365 グループの作成とは独立した設定である。この点について、Microsoft 社のオンライン文書では記述が不明確であるので注意を要する。

上記の設定により、一般ユーザーによる Office 365 グループの作成は禁止できる。しかし、Exchange Online や SharePoint Online には、グループ作成用インタフェースが表示されたままであり、これを操作した時点でエラーが表示される挙動を示す。これは一般の利用者にとって不親切だと考えられるので、Exchange Online と SharePonint Online において、一般ユーザーに Office 365 グループを作成させない設定を行った。ただし、これらを個別に設定するだけでは、テナント全体で Office 365 グループの作成を禁止するには不十分であり、上述の Azure AD に対する設定が必須であることに注意されたい。

5.4 サインイン手段の整備

Azure AD にてフェデレーション認証を用いて AD FS にリダイレクトされるフェデレーションドメインとして、前記 3 個のドメイン名を設定した。AD FS ではサインインに、userPrincipalName 属性値である DNS ドメイン名付きの文字列、または、“⟨NETBIOS ドメイン名⟩¥⟨sAMAccountName属性値⟩” を用いる。今回の構成では userPrincipalName 属性値には “⟨SSO-KID⟩@kyushu-u.ac.jp” が登録されている。しかし、他のサービスと同様に、利用者は SSO-KID だけを入力すれば良いようにしたい。そこで、AD FS サインイン画面のカスタマイズ機能において、SSO-KID の後に自動的に@kyushu-u.ac.jp が補完されるように JavaScript を使用した。

AD FS の認証において、Azure AD Connect で代替 ID を設定する場合には注意が必要である。Azure AD Connect のウィザードを用いて代替 ID を設定すると自動的に、Azure AD Connect で代替 ID として設定した属性の値を用いて AD FS にサインインできるように、AD FS の代替ログイン ID が構成される。今回の場合は、代替 ID に指定した mail 属性に登録される全学基本メールアドレスで AD FS にサインインできる。しかし、容易に収集できるメールアドレスを用いたサインインはセキュリティ保護の観点から不可能にしたいので、Azure AD Connect の設定後に、手動で AD FS の代替ログイン ID を無効に設定する必要があった。

フェデレーション認証を用いる場合、Office 365 のサインイン画面で@の後ろにフェデレーションドメイン名を持つ文字列を入力すると AD FS のサインイン画面にリダイレクトされる。ウェブブラウザで Office 365 にサインインする際の利用者の手間を軽減するために、Office 365 サインイン用のスマートリンクを作成した。このスマートリンクの URL にアクセスすると、最初に AD FS のサインイン画面が表示される。さらに、スマートリンクの URL は複雑であるので、スマートリンクにリダイレクトする URL https://office365.iii.kyushu-u.ac.jp/login を用意した。

試験運用中に、Skype for Business アプリケーションでのサインインは挙動が異なることが判明した。「サインイン アドレス」欄には、AD FS のサインインに用いる文字列ではなく、Office 365 の UPN を入力する必要がある。その後で表示される AD FS のサインイン画面は前述の通りである。

5.5 AD レプリケーション

今回、移行作業の最初の段階では、Azure の VNet 上に配備したオンプレ AD ドメインコントローラにおいて、レプリケーションを実施しない独立した状態で稼働させ、テスト用ユーザーを作成した状態で Azure AD と同期させて動作を確認した。次いで、全学共通 ID 管理システムと連携するオンプレ AD ドメインコン

トローラからレプリケーションさせて試験運用を行った。しかし、今回この段階で問題が発生した。

Microsoft 社は静的 NAT を含め NAT 経由での Active Directory の動作検証を行っておらず、実際に NAT 経由ではドメインコントローラのレプリケーションは動作しない。全学共通 ID 管理システムと連携するオンプレ AD ドメインコントローラは、今回 Azure 上のシステム構築を発注した業者とは別に、全学共通認証基盤の運用業者に依頼して仮想化基板上に設計構築していたが、このドメインコントローラの全通信は仮想化基盤で NAT を経由する構成となっていた。しかし、そのことを九州大学の担当者は把握できておらず、原因の特定が困難であった。

5.6 AD 同期

今回、オンプレ AD のレプリケーションを設定したのち最初の Azure AD への同期では、約 3 万弱のオブジェクトに対する処理が発生した。その際に、Azure AD が現在ビジー状態でありエラーが発生した旨を知らせる「ID 同期のエラーレポート」メールが管理者アドレス宛に計 500 通以上送信された。Microsoft サポートへの問合せに対する回答に従い経過を観察したところ、翌日には問題が解消して同期が完了した。これが Azure AD 側の一時的な問題だったのか、大量の同期を行ったことが原因だったのかは不明である。

今回の試験運用は、一部ユーザーにだけ Office 365 へのサインインを許可した状態で行ったが、ユーザーのサインイン禁止設定において問題が発生した。当初、Office 365 テナント側で個別ユーザーのサインインを禁止する操作を行ったが、その後サインインが自動的に許可されていることが判明した。一般に、オンプレ AD から Azure AD に同期された内容であっても Office 365 テナント側で行った変更は維持されるが、オンプレ AD でユーザー情報に変更があると、Azure AD 側の設定は上書きされ Office 365 テナント側で行った変更は失われる。ここで、オンプレ AD ユーザーの有効性を示す Enabled 属性が Office 365 のサインイン許可設定に同期される。今回は、試験運用中にオンプレ AD ユーザーへのライセンスコードの設定作業などを行ったことから、オンプレ AD の Enabled 属性が同期され、Office 365 のサインインが許可されたと考えられる。最終的に、オンプレ AD ユーザーの Enabled 属性を False に設定することで問題を回避したが、この手段はオンプレ AD が他のサービスでも利用されている場合には選択できない。

九州大学の構成員ではなくなった者は、一定の猶予期間を経て、全学共通認証基盤から削除され、それに伴いオンプレ AD ユーザーも削除される。オンプレ AD から削除されたユーザーは Azure AD Connect によって Azure AD から削除される。今回、年度末に非構成員となったオンプレ AD ユーザーが削除された時点で、AD 同期に問題が発生した。Azure AD Connect では、誤った削除から保護するために削除できる件数の閾値が既定で 500 に設定されており、閾値以上の削除を試みた場合にはエラーが発生し Azure AD からユーザーは削除されない。閾値の上限を解除、または、削除件数以上に設定するまで削除エラーは回復せず、削除エラーが発生している間は一切の AD 同期が行われない。今回は一時的に閾値の上限を解除することで問題を解消した。

5.7 ProPlus ライセンスの移行

九州大学の EES には Office 365 ProPlus のライセンスが含まれるが、それは構成員人数分のライセンスであるので、複数の Office 365 テナントに割り当てることはできない。それゆえ、旧環境から新環境への移行にあたり、ライセンスをテナント間で移行させる必要があった。ただし、テナント間でライセンスを移行させる場合は、ライセンス移行手続き開始後最低 30 日間は猶予状態として移行元テナントでライセンスを利用できる。

一方、利用者が移行元テナントからインストールした ProPlus については、移行元テナントに紐付いたライセンスが失効すると別テナントでライセンス認証できるのではなく、利用者自身の作業によりライセンス情報を削除する必要がある。ここで、Microsoft Office アプリケーション利用時の Office 365 へのサインインと、ライセンスが所属するテナントとは全く独立であり、アプリケーションで Office 365 からサインアウトしてもライセンス認証は解除されない。OS が Microsoft Windows の場合、インストール済みのライセンス情報を削除するには、複数手順のコマンドライン作業が必要である。これは一般の利用者には難易度が高いと判断し、Office を一旦アンインストールしてから再インストールする手順を案内した。OS が macOS の場合には、Microsoft 社が提供するライセンス認証を抹消するツールが利用できる。しかし、ライセンスの再認証には注意を要する。ウェブブラウザなどで移行元テナントなど、ライセンス認証先としたいテナントとは別のテナントにサインインしている状態で、ライセンス認証のない Office アプリケーションを起動すると、そのサインイン中のテナントを対象に自

動的にライセンス認証を行ってしまう。場合によってはウェブブラウザを終了していてもサインイン状態が維持されていると、同様の挙動を示す。

5.8 ユーザーによる移行作業

新環境の正式サービス開始前に、旧環境のサービス廃止と新環境のサービス開始について全学通知により周知を図り、また、サービス開始直後に、旧環境へのサインイン経験のある全ユーザーに対して新環境へ移行する必要がある旨をメールで案内した。その後、旧環境へのサインイン数を観察していたが想定を下回る減少数だったことから、旧環境のサインイン画面に移行案内を表示する設定を行い、また、4 月以降に旧環境を利用したユーザーに対して再度メール通知を行った。その上で、当初の予定通り 2018 年 7 月末に、旧環境テナントの全ユーザーに対しサインインを禁止する処理をおこなった。しかしながら、2018 年 8 月以降、Office 365 にサインインできなくなった、PC にインストールした Office を利用できなくなったという多数の問合せが寄せられ、また、旧環境テナントの OneDrive for Business にアクセスしたいという要望も多数寄せられた。サインイン不能や Office 使用不能の問合せに対しては新環境への移行を案内し、OneDrive for Business へのアクセス要望については個別にサインインブロックを解除する処理を行った。特に Office 365 ProPlus と OneDrive for Business については通常の利用時にはユーザーが Office 365 テナントを意識していないと考えられることから、より十分な周知期間と周知活動が必要だったと思われる。

旧環境テナントで主に利用されていたサービスは OneDrive for Business であった。前述の通り、旧環境のファイルは利用者各自で新環境に移行してもらうこととした。しかし、OneDrive for Business ではテナント間でファイルを共有できるよう設定しても、テナントをまたがったファイルのコピーはできず、テナント間で直接ファイルを移行する方法は見出せなかった。それゆえ、移行方法として、旧環境から手元に一旦ファイルをダウンロードしたのち新環境へとアップロードする方法を案内せざるを得なかった。ただし、この方法では旧環境ファイルのバージョン履歴は失われる。

5.9 効果

新環境ではユーザー認証を全学共通 ID の SSO-KID に統合したこと、簡便なサインイン手段を整備したことにより、Office 365 へのサインインの利便性は著しく向上したと考えられる。また、Office 365 の UPN を全学基本メールアドレスとしたが、ファイル共有や協調作業を行う利用者間では一般的に双方の全学基本メールアドレスを把握していると思われることから、Office 365 でユーザーを指定する際の利便性も大いに向上したと考えられる。

旧環境では、Office 365 サービス運用部門が関知していない多数の Office 365 グループが作られていた。Exchange Online は無効化していたことからメールに関する不都合は生じていなかったが、SharePoint Online のチームサイトが作成され記憶容量が消費されていた。新環境では一般ユーザーによる Office 365 グループの作成を禁止したことで、それに関する資源の消費を運用部門が管理できるようになった。

6 今後の計画と課題

九州大学では、現在独自システムで稼働している全学基本メールサービスを 2018 年 12 月に Exchange Online に移行する予定である。現時点では、新環境テナントで Exchange Online を有効にしているが、メールは現行のメールサーバに配送される状態である。今後、全学基本メールサービスの受け入れに対する準備を行う必要がある。現行の送信用 SMTP サーバでは、From フィールドに任意のアドレスが記載されたメールの送信を許可しているが、Exchange Online では Azure AD のユーザー情報に登録されたメールアドレス以外を記載したメールは送信できない。そこで、別途 SMTP サーバを学内に稼働させる予定である。

新環境テナントの現在の設定では、全ユーザーは他のユーザーの一覧を閲覧できない。しかし、教職員が教職員一覧を閲覧することには問題がなく、むしろ閲覧できる方が望ましい。これは、Exchange Online のアドレス帳ポリシー機能により GAL を分割することで実現可能であり、今後の対応課題である。

Microsoft 社は Skype for Business から Teams への移行を計画していると発表している。このことから九州大学でも Teams の利用について検討中である。しかし、Teams の活用には Office 365 グループの作成が必要である。Office 365 グループ作成の運用方法について今後検討を進める。

参考文献

[1] Yoshiaki Kasahara, Takao Shimayoshi, Masahiro Obana, and Naomi Fujimura. Our experience with introducing microsoft office 365 in kyushu university. In *Proceedings of the 2017 ACM Annual Conference on SIGUCCS*, pp. 109–112, 2017.