

教育用パソコンにおける Microsoft 365 連携の強化

和田 智仁¹⁾

1) 鹿屋体育大学 スポーツ情報センター

wada@nifs-k.ac.jp

Strengthening Microsoft 365 Connectivity on Educational PCs

Tomohito Wada¹⁾

1) Information Technology Center for Sports Sciences, National Institute of Fitness and Sports in Kanoya

概要

従来の教育用パソコンでは管理上の理由から OneDrive アプリがインストールされていないなど Microsoft 365 の各種サービスが利用しづらい状況であった。そこでセンターシステム更改にあわせ、教室用パソコンでは Microsoft Entra Hybrid Join、貸出用のパソコンでは Microsoft Entra Join を導入した。これによって教育用パソコンから M365 の各種サービスが利用しやすくなり、授業においても OneDrive を使った作業を指示できるようになった。

1 はじめに

鹿屋体育大学では教育研究およびその他の業務での利用のため、2017 年 10 月に Microsoft 総合契約を導入した[1]。その後 2018 年 1 月には全学メールシステムをオンプレミスの Exchange Server から Exchange Online に移行し、これを契機に学内構成員における「Microsoft 職場または学校アカウント（以後、Microsoft アカウントと表記）」への認知が高まった。これ以降、Microsoft 365（以後、M365 と表記）の各種サービスも徐々に認知され、特に 2020 年のコロナ禍以降、オンデマンド授業でのビデオ配信等に Stream が、研究室やリモート会議等での資料共有に OneDrive が、各種調査には Forms が使われるようになるなど利用が広まっている。また、最近では事務系を中心に Teams の利用も始まっているなど、現在では M365 の各種サービスが大学の情報基盤として欠かせないものとなりつつある。

ただし、パソコン教室に設置された教育用パソコンにおいては、このような状況の変化に対応することなく現在に至っていた。例えば、教育用パソコンでは、電子メールや OneDrive は web ブラウザを通じて利用する必要があるなどの制約があり、M365 のサービスが利用しづらい状態にあったと言える。

そこで、2024 年 3 月にセンターシステムが更改されるタイミングで教育用パソコンにおける

M365 連携の強化を試みることにした。なお、教育用パソコンの更改に際しては、Azure Virtual Desktop 等の仮想化技術への切り替えも候補に挙がったものの、最終的にはこれまでと同様の FAT 端末が導入されている。

2 システム更改前の状況

2.1 アカウント連携について

全学メールシステム移行時の検討の結果、M365 テナントのアカウントは、学内のディレクトリサービスと自動的に連携させ運用することとなった。具体的には、Microsoft Azure AD Connect（現在の Microsoft Entra Connect）を導入し、学内認証基盤として使用しているオンプレミス Active Directory (AD) とのアカウント連携を実施することとした。これにより AD に登録されたユーザー情報が自動的に M365 へ同期され、また学内アカウント用のパスワードで M365 のサービスを利用できるようになっている。なお、2019 年 7 月には不正アクセス事案を契機に、全ての M365 アカウントの認証に多要素認証を必須とした。

2.2 演習室パソコン

これまで演習室（パソコン教室）のパソコンは、AD ドメインに参加させ、移動ユーザープロファイルとフォルダリダイレクトを用いた利用環境としていた（図 1a）。なお、個人用のデータ保存領域としては、ファイルサーバー上にユーザーあたり 5GB を割り当てている。

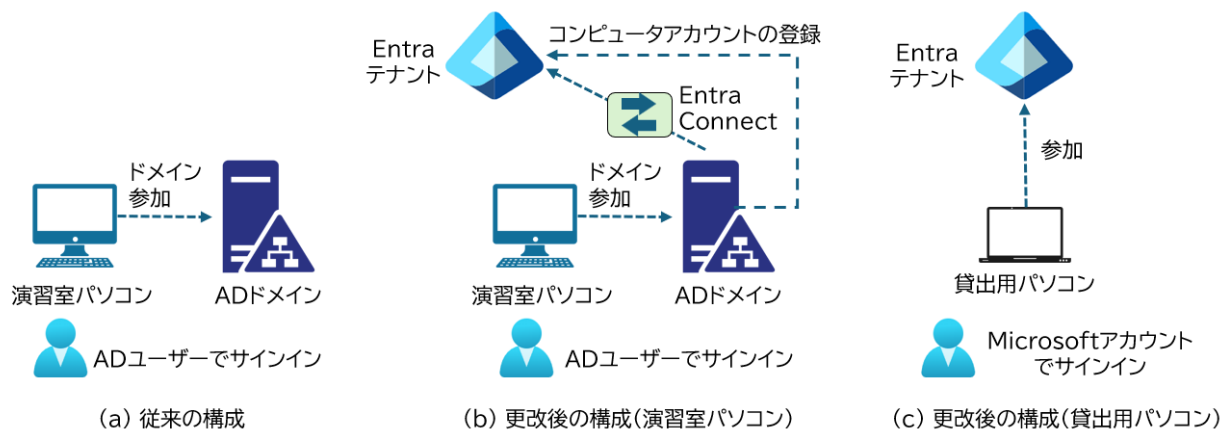


図1 構成の比較 (文献[4]の図を一部改変)

Office アプリについては、Word, Excel, PowerPoint 等についてはデスクトップアプリをインストールしていたが、Outlook, OneDrive, OneNote 等のアプリは削除していた。そのため、これらの M365 サービスを演習室パソコンから利用するには、ブラウザを使って M365 にサインインした後に、ブラウザ上で使用する必要があった。そのため、従前の演習室パソコンから OneDrive 上に保存する Word ファイルを Word デスクトップアプリで編集する、といった場合には以下の手順が必要であった。

1. ブラウザを用いて M365 にサインインする
 - (ア) メールアドレスを入力する
 - (イ) パスワードを入力する
 - (ウ) Authenticator での承認作業を行う
2. OneDrive ページにアクセスし、目的の Word ファイルをダウンロードする
3. ダウンロードしたファイルを Word で編集する
4. 編集したファイルをブラウザから OneDrive にアップロードする

演習室パソコンでの OneDrive 利用には手間がかかることから、授業では専ら学内ファイルサーバーにある個人用のデータ領域を使用するように指示していた。しかし、ファイルサーバーには自宅からアクセスできないため、授業と自宅学習との連続性が保てないという問題があった。

パソコン更改前には、上記の手順を簡略化することを目的に「シームレス SSO」を導入した。これは Microsoft Entra Connect の設定変更により実

現できるものであるが、この機能では上記手順 1 の一部が省略されるだけで利便性が大きく向上することはなかった。

2.3 貸出用パソコン

スポーツ情報センターでは、一時利用のための貸出用のパソコンも複数台管理している。貸出用パソコンは、学外など AD へのアクセスが困難な場所からの利用も想定されることからドメインには参加させていない。利用者が保存したデータ等が次の利用者に残らないようにするため、基本的には、利用者ごとにローカルアカウントを作成し、返却時にアカウントを削除している。貸与に際してアカウントの追加削除に作業が必要となる点が課題であった。

3 M365 連携の強化

3.1 Microsoft Entra Hybrid Join の導入

演習室パソコン更改にあたり従前の問題を解決すべく先行する事例の調査を行った。島田ら[2]はネットブート環境における FSLogix と Hybrid Azure AD Join による M365 クラウドサービスへの SSO 事例を報告しており、我々の環境とは異なるものの、これを参考に M365 連携の強化を行うこととした。

前述の Hybrid Azure AD Join は現在 Microsoft Entra Hybrid Join と呼ばれており、オンプレの AD ドメインに参加しているパソコンを、さらに Microsoft Entra テナントに登録する形態である[3,4]。演習室パソコンを Entra Hybrid Join とするには、アカウント連携のために使用していた Microsoft Entra Connect において、演習室パソコン

用 OU をハイブリッド参加へと構成変更するのみであった。この手順で Entra Hybrid Join されたパソコンは、これまでと同様に AD ドメインの資格情報でサインインして使用する。移動ユーザープロファイル、フォルダリダイレクトなど AD で設定したグループポリシーも有効である。このため、利用者は従前と全く同一の方法でパソコンを利用できる（図 1b）。

Entra Hybrid Join 環境では、Office デスクトップアプリや OneDrive デスクトップアプリが自動的に M365 アカウントに接続されるただし、初めて使用するパソコンあるいはログイン後 90 日を経過した場合には、MFA による認証が必要となる。

本構成を導入後、一部ユーザーでサインイン後に OneDrive アプリが起動せず、メニューからも OneDrive アプリを起動できないという症状が発生した。この症状に対しては、エクスプローラーに `odopen://launch` と入力し、強制的に OneDrive セットアップを実施することで問題を回避できた。これにより一旦セットアップが完了すれば、次回サインイン時からは問題なく OneDrive が利用できるようになるようであった。

3.2 Microsoft Entra Join の導入

貸出用パソコンは、AD ドメインに参加させることができないことから、演習室パソコンとは異なり、Microsoft Entra Join し、貸し出す運用とした（図 1c）。Microsoft Entra Join で管理者によるパソコン上での設定作業が導入時のみ必要である。Microsoft Entra Join の場合、パソコンの利用時には Microsoft アカウントを使って Windows にサインインすることになる。そのため、ユーザーが初めてサインインする際にはネットワーク接続性が要求される。ユーザー認証は Entra 上で行われ、認証に成功すると個人用の環境がパソコン上に自動的に生成されるため、事前に貸出用のアカウントをセットアップする必要はない。貸出用パソコンで OneDrive にアクセスする場合、演習室パソコンと

同様初回のみ MFA 認証が必要となるが、それ以降は OS へのサインインのみで簡便に M365 の各種サービスが利用可能である。

4 まとめ

教育用パソコンの管理手法を変更することで、それらのパソコンにおける M365 連携を強化した。これによって教育用パソコンにおいて OneDrive などの M365 サービスの利用が簡単になった。特に、演習室パソコンにおいて連携が強化されたことから、一斉授業での M365 サービス利用が可能となった。個人が所有するパソコンと演習室パソコンとの間でのデータ連携が容易になったことで、自宅での学習との連続性も確保されたと言える。

これらの導入から現在まで、特段大きな問題は確認されていない。ただし、現状では基本的な設定を実施しているのみで、細かなデバイス管理を行うには至っていない。例えば島田ら[2]はパソコンのドキュメントフォルダを OneDrive に自動リダイレクトすることで、ファイルサーバーへの保存を抑制している。教育用パソコンの運用状況を把握しつつ、今後は応用的な設定の導入を行っていきたい。

参考文献

- [1] 和田智仁, 第 4 期センターシステムおよび関連サービスについて, スポーツ情報センター広報, 8 号, pp.4-8, 2019.
- [2] 島田美月, 齋藤彰一, 松尾啓志, 丸山伸, Windows11 教育用計算機システムにおける M365 クラウドサービスへの SSO 連携について, 学術情報処理研究集会第 27 回 CACN, 2023.
- [3] Microsoft Entra ハイブリッド参加の実装を計画する, <https://learn.microsoft.com/ja-jp/entra/identity/devices/hybrid-join-plan> (2024/10/12 参照)
- [4] 竹島友理, ひと目でわかる Microsoft Entra ID, p. 279, 日経 BP, 2023.