

福岡学園における Microsoft 365 導入と利活用

亀井 愛¹⁾, 藤村 直美¹⁾

1) 福岡学園 福岡歯科大学

kamei@fdcnet.ac.jp

Report on Introduction and Utilization of Microsoft 365 at Fukuoka Gakuen

Ai Kamei¹⁾, Naomi Fujimura¹⁾

1) Fukuoka Dental College, Fukuoka Gakuen

概要

福岡学園では Microsoft 365 における Exchange メールの利用等を目的として、2022 年度に Microsoft 365 を導入した。その後、Microsoft 365 のサービスである OneDrive や SharePoint・ファイル保護機能等を全学的に利用している。本稿では、Microsoft 365 導入における認証方法、ネットワーク設計変更点、メールの移行手順やセキュリティ・作成したアドレスブックポリシー・学生への一斉メール用の動的配布グループ・デバイスからのメール送信実現方法、Teams のグループ作成申請や SharePoint での規程集システム構築などの事例を報告する。

1 はじめに

本学のような小規模大学では、ネットワークや情報システムの運用を担当するのは、情報系職員のみで教員が直接関与しないことが多く、情報環境の将来構想の策定やそれに向けての意思決定が容易ではない。そうした状況において、2022 年度から情報担当の顧問が採用され、大学の情報環境の将来像を検討し、Microsoft 365 (以下 M365 という) の導入を前倒しして、M365 を活用した情報環境整備を開始した。ここでは M365 の導入を中心に、情報環境整備の問題点や成果を報告する。

2 M365 の導入

2.1 認証

本学では従来から全学共通認証として Microsoft の Active Directory (以下 AD という) を構成し、学内の様々なシステムは Kerberos や LDAPS で認証していた。M365 導入にあたっては、オンプレ AD の認証情報を利用することとし、具体的には Azure AD (現 Microsoft Entra ID) に Azure AD Connect (現 Microsoft Entra Connect) [1]を用いて同期することにした。本学では M365 が初めての全学的なクラウド利用となるため、確実にセキュリティを担保し、安心して利用してもらうため多要素認証を必須とした。

2.2 ネットワーク

ネットワークの学外接続は、プロキシと FireWall を経由し、SINET と 1Gbps (ダークファイバー) で接続していた。また、プロキシを経由せず FireWall から直接学外へ抜ける通信は drop する設計にしている。

M365 はセッションを多く確立すること、クラウド上にあることから学外へのトラフィックが増加することを見込んだ。第一に、プロキシがボトルネックになることを防止するため、M365 の通信についてはプロキシを経由することなく FireWall を直接通過するよう PAC ファイルを定義した。

一方、FireWall に M365 の通信許可ルールを IP ベースで設定することは、不可能と考えた。FireWall は Fortinet 社の Fortigate を利用していたが、IP ベースのルールではなく、ISDB (Internet Service Database) [2]を利用することで、自動で更新されるデータベースにより M365 の通信許可のルールを実現できた (図 1)。

さらに M365 導入翌年にタイミングよく FireWall を更新する予定があったため、将来を見越して、トラフィック増加に耐えられるよう学外接続を 1Gbps から 10Gbps に増速した。

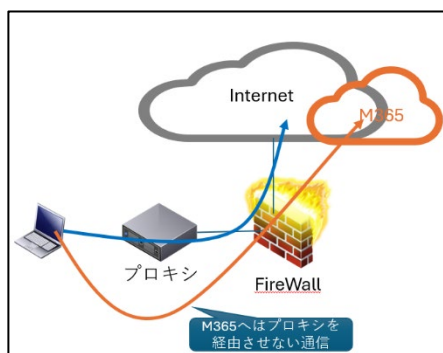


図 1 M365 への通信

3 Exchange(メール)

3.1 メールの導入

従来、福岡学園にける教職員用メールサーバ環境は、LinuxOS によりオンプレミスで構築していた。メールの送受信について、基本利用は学内のみとし、学外からの送受信はできず、どうしても学外での利用が必要な場合は、SSL-VPN を介するという運用方針としていた。

2023 年度にメールサーバのハードウェア保守期限切れが控えていたため、M365 の導入を視野に入れ、2020 年度から実際にテナントを作成し、メール環境の検証をしていた。メールに関するセキュリティの保守的な考え方が続く中、教員による学外からのメール利用の強い希望と情報顧問着任を契機とし、2022 年度に M365 の本格導入を決定し、まずは教職員に展開、次年度の 2023 年度に学生に M365 のメールの利用を展開した。

3.2 メールアドレスのドメインと移行

全く異なるメールシステムを導入するに際して、新しいメールシステムへ円滑に移行するため、従前使用していたメールアドレスをそのまま使うのではなく、一定期間、新旧のメールアドレスを並行運用することとし、メールアドレス用のサブドメイン名を変更することにした。

教職員：college.fdcnet.ac.jp → fdcnet.ac.jp

学生：student.fdcnet.ac.jp → edu.fdcnet.ac.jp

旧アドレスは、当該サーバの保守が切れるまで猶予 1 年間使用できることとし、その後は廃止することとした。移行期間中は旧メールアドレスにきたメールは M365 の新メールアドレスに転送し、利用者は M365 のメールアドレスのみ受信すればよい状況にした。旧メールサーバ停止については、

当初は旧メールアドレスから送信禁止、次に旧メールサーバからの受信禁止、旧メールからの転送停止（サーバ電源断）と段階を踏むことで、大きな混乱もなく新しいメールアドレスに移行できた。

3.3 SPF/DKIM/DMARC

SPF (Sender Policy Framework)については、カスタムドメインに追加する過程で DNS に TXT レコードの追加が必須であるため、特段意識せずとも備わる。しかし、DKIM (Domain Keys Identified Mail) や DMARC (Domain-based Message Authentication, Reporting, and Conformance)はそうではないため、意識して実施する必要がある、DKIM 設定は M365 管理画面からドメインの DKIM キーの作成、DNS に C レコードの追加、DMARC の設定は DNS に TXT レコードの追加を実施した。最近、Google のポリシー変更に伴ってこれは必須の作業となった。

3.4 メールのセキュリティ

M365 導入前からの課題として、メールの添付ファイルは、送信後に取り消しが困難であり、宛先間違いや、ファイル添付誤りによる情報流出を考えると、廃止したい機能である。個人情報等が入った添付ファイルを PPAP (パスワード付き添付ファイルをメールで送信し、後から別メールでパスワードを送信する) で送信する方法も面倒なだけで、セキュリティ上の効果はない。

M365 導入を契機に、添付ファイルの誤送信防止対応や実質無意味な PPAP の利用を禁止したいと強く考えていた。しかしながら、全ての送受信メールで添付ファイルを禁止にすると業務に支障が出ることから、添付ファイル付きのメールの受信は制限なし、送信時の添付ファイルの大きさを 10MB 以内に制限し、かつパスワード付き添付ファイルの送信を禁止した。原則としてメールの添付ファイルの代わりに OneDrive によるファイル受け渡しに誘導することとした。送信時の PPAP は Exchange メールフロールール[3]に作成することで禁止とした (図 2)。

メールの転送も転送先のサーバのセキュリティレベルに依存し、必ずしも安全とは限らないことから、学外でメールを送受信できるようになったことを踏まえ、迷惑メール対策の送信ポリシーと、役割ベースのアクセス制御設定により自動転送を禁止した。そのため利用者は必ず M365 のメールサーバから直接メールを読まないといけない。

図 2 PPAP 送信禁止ルール

3.5 アドレスブックポリシーと動的配布グループ

アドレスブックポリシー[4](以下ABPという)について、学生用に1つ、教職員用に2つ作成した。学生用のABPには学生のみアドレスリスト、教職員のABPのうち、学生と連絡を取る教職員は教職員と学生のアドレスリスト、その他は教職員のみアドレスリストのセットとした。なお、アドレスブックポリシーやアドレスリストの作成は管理画面からは行えないため、PowerShellによりNew-AddressBookPolicy コマンド等を使用し作成した。

また、学生への連絡は学年単位で行うことが多いため、動的配布グループ[5]を作成した。ADのDepartment属性に学年をセットし、その属性をもとに動的配布グループのルールを設定した。これによって学年単位でのメール送信が容易になった。

3.6 デバイスからのメール

複合機でスキャンしたデータや、各種システムからの自動メール送信に対応する必要があった。ここで問題となったのが、まず多要素認証である。これについては、条件付きアクセスで例外的にパスワード認証のみ(ただし、限定したメールアドレスかつ本学所有のグローバルIPアドレスからの発信のみ)とすることとした。

次に問題となったのはシステムによっては、条件により送信元メールアドレスを使い分けているという運用である。具体的には、例えば、すでに運

用していた広報用Webサーバの問い合わせのフォームでは、問い合わせを受けたことを知らせるメールを問い合わせ者(学外)に送信するが、問い合わせに対応する部署のアドレスをそれぞれ送信元に指定するという仕様で動作していた。

このWebサーバはメールアドレスの認証情報が1つしかセットできないCMSを利用していた。1つ目の解決策として候補に挙がったのは、直接送信である。直接送信はExchangeサーバのTCP25番ポートに直接送信する方法で、テナント内のアドレスにのみに送信できる方法である、しかしこれではテナント外(学外者)へは送信できない。

次に上がった解決方法として、M365のSMTPリレーを使用して、メールを送信するコネクタを設定する方法である(図3)。この設定でExchangeTCP25番ポートに認証なしでメールを送信し、さらに学外者のメールアドレスにも送信可能となった[6]。

図 3 SMTP リレーの送信コネクタ

4 Teams の利用

Teamsはデフォルトの設定で使用すると、自由にグループが作成できたり、Third Party アプリを使用できたりと無法地帯になることが懸念された。また、少ないスタッフでM365の導入・運用を行うため、初めはスモールスタートし、徐々に展開して行きたいと考えた。そのため、導入年はTeamsのグループ作成の受付を見合わせた。

M365導入前は、遠隔会議や遠隔授業のために、

Zoom の契約を行っていたが、Zoom の契約更新のタイミングで Teams を使いたいとの要望もあり、導入の翌年からグループの作成を許可することにした。グループは勝手に作成できるのではなく、申請制（教職員のみ可）とすることにし、その申請は Forms で受け付けた。

5 SharePoint

5.1 会議資料配布

本学ではいくつかの会議で資料をメールで電子配布し、iPad（学校貸与）で見るという方法を取っていた。この iPad が非常に古く M365 を利用できない（認証すらできない）ことが判明し、代替手段を模索した。検討の結果、学校貸与の iPad は使用しない、今後は教職員が持つ端末（PC、タブレット等）を利用する、電子資料配布は SharePoint のドキュメントライブラリを利用することとした。

運用方法としては、会議毎に SharePoint のサイトを作るのではなく、会議の事務を担当する事務課ごとにサイトを開設した。そして、会議体毎にドキュメントライブラリを作成し、アクセス権を付与する方法をとった。

SharePoint のグループ単位のアクセス権限は、サイトが作成された際にデフォルトで用意されているグループであるサイト所有者・メンバー・閲覧者と、細やかな設定ができるカスタマイズ可能なグループ[7]で実施できる。サイトを管理する事務課の課員は、サイト内の会議体すべての資料の編集を実施するため、デフォルトにあるグループのサイトのメンバーとして登録した。会議参加者については、カスタマイズで作成したグループに所属させ、当該ドキュメントライブラリのみを閲覧可能とする権限設定にした。これらの設定により、サイトを管理する事務課員は会議体すべての資料を編集することができ、会議参加者は参加する会議体のドキュメントライブラリのみ閲覧でき、参加していない会議体の資料にはアクセスできない環境を作成した。

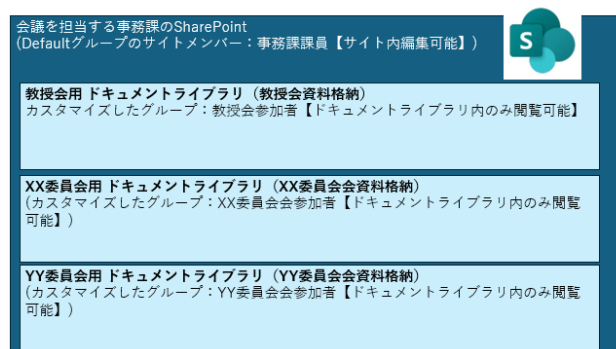


図 4 会議資料配布用 SharePoint のアクセス権

5.2 諸規程集

SharePoint を活用して既存の事務文書管理システムを置き換えた。これまで本学の諸規程集システムは、規程を全文検索でき、一覧からも辿れるというシステムで、従前では Windows サーバにオープンソースの全文検索サーバ Fess[8]を配置していた。これを SharePoint のドキュメントライブラリに置き換えた。ドキュメントライブラリはファイルを置くだけで全文検索が実現できる。

諸規程集には、現行の規程と旧規程について掲載しているが、旧規程は全文検索結果に出してほしくないという要望があったため、旧規程用に別にドキュメントライブラリを作成し、ドキュメントライブラリの設定で「このドキュメントライブラリのアイテムを検索結果に表示する」を「いいえ」にすることで、検索結果に表示されないようにした。

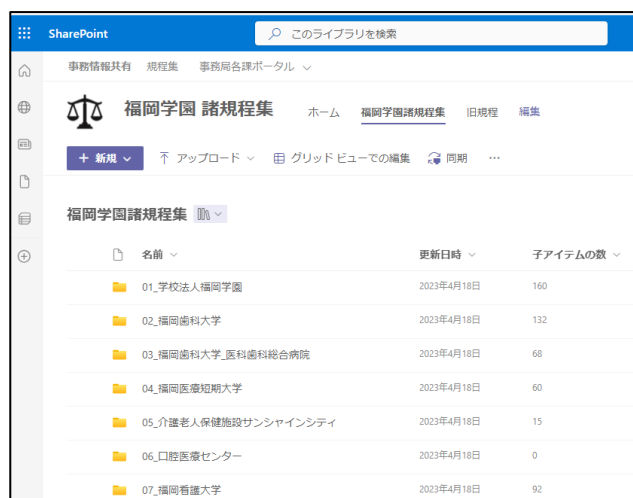


図 5 福岡学園 諸規程集

6 その他の機能

6.1 暗号化（Azure Information Protection）

M365 導入以前より、情報流出対策として、またマイナンバー取り扱いの対応として事務局で作成するファイルを暗号化していた。教員は暗号化ソフトを導入していなかったため、暗号化したファイルを誤って教員に渡し、ファイルが開けないというトラブルも起きていた。

M365 導入により、Azure Information Protect(以下 AIP という)を利用したファイル暗号化（保護）を実施することにした。AIP は、ラベルをテナントで定義し、そのラベルをだれが利用できるかの設定ができる。あまり複雑にすると利用者が抵抗を感じ使用しないことが予想されたため、1 つだけラベルを作成し、教職員のみ使用できるようにした。その結果、ファイルを容易に暗号化でき、本学の ID を持つ教職員であれば誰でも参照できる。一方でファイルが万が一外部に流出しても、内容が漏洩することはない。

6.2 Outlook 予定表の利用（学園スケジュールの周知）

これまで国立情報学研究所が提供する CMS NetCommons2 を利用して学園全体の予定を管理・周知していたが、すでにメンテナンスが終了しており、別の情報サービスに乗り換えを行う必要があった。M365 の導入に合わせて、学園内で周知すべき教授会や入試のスケジュールについては、Outlook の予定表を利用することにした。学園スケジュール用に 1 つアカウントを作成し、予定表の共有設定で、予定を入力する事務職員に「編集が可能」な権限を、予定を閲覧する教職員に「すべての詳細を閲覧可能」な権限を付与することで実現した。

6.3 Office の活用

M365 の導入に伴って、Office (Word, Excel, PowerPoint 等)を教職員と学生が追加の費用負担なしに利用できるようになった。教職員が Office を整備する経費を節約できるだけでなく、学生は在学中の経済的な負担を軽減でき、大学の魅力を向上できる。大学において、BYOD (Bring Your Own Device)を活用した教育を推進する上で、大きな利点になっている。

7 導入効果

メールを学外から送受信できることで教職員ともに利便性が上がったとの感想を多くもらった。また、今まではパソコンでの利用が多かったが、各自のスマートフォンで簡単な設定でメールを送受信できるようになったため、学内で机を離れたときにメールを見ることができ機動力と利便性が上がった。

学生は在学期間中 Office が無料になり、経済的負担が減った。OneDrive でどこからでもファイルを安全にアクセス可能となり、学外での簡単な確認作業が容易にできるようになった。

予期せずによかったこととして、オンプレ AD は学内のシステムの認証しかできていなかったが、Microsoft Entra ID を使えるようになったので、クラウドサービスで全学共通認証として使えるようになり、今年度から導入した電子教科書の認証に使用できた。さらに、多要素認証も利用可能になり、セキュリティレベルを上げることができた。

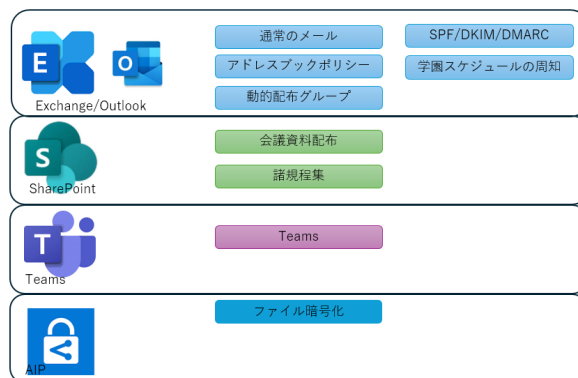


図 6 Microsoft 365 の利活用概要

8 今後の展望

導入して 2 年経過し、色々な場面で M365 が利用されている。特にメールを学外から送受信できることは喜ばれている。それまでは VPN を利用する、あるいは他のメールアドレスに転送し、そこから（本学とは異なるアドレスで）本学の業務に関連するメールを送受信するなどの問題があったが、これらの問題は解消した。

現状で学内の利用者の声を聴くと、メールをはじめとして、まだまだサービスを上手に使えていなかったり、便利なサービスを知らない職員が多いようである。教職員の ICT スキルを改善するため、SD (Staff Development)を実施し、便利な機能を

紹介し、自発的に活用してもらえようとする予定である。

事務局から DX を進めたいという要望も上がっているため、Power Automate 等を使った事務 DX 勉強会を実施し、身近な作業を自動化することで、ルーチンワークでも楽しく行えるようにする勉強会を行っている。

さらに、セキュリティを考慮して、VPN の設備を 2024 年度一杯で廃止する予定で、学外からの利用を規制し、VPN 経由でしか利用できなかったサービス、例えばオンラインジャーナルを学外から利用可能にするために、Microsoft Entra ID を認証データベースとした学認構築についても準備中である。

9 参考文献

- [1] Microsoft 社: Microsoft Entra Connect とは,
<https://learn.microsoft.com/ja-jp/entra/identity/hybrid/connect/whatis-azure-ad-connect> (2024-09-02 参照)
- [2] Fortinet 社 : Microsoft 365 のネットワークセキュリティ
<https://www.fortinet.com/jp/solutions/industries/office365-network-security> (2024-09-02 参照)
- [3] Microsoft 社: Exchange Online のメールフロールールを管理する - メールフロールールの作成,
<https://learn.microsoft.com/ja-jp/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules#create-a-mail-flow-rule> (2024-09-02 参照)
- [4] Microsoft 社: Exchange Online のアドレス帳ポリシー
<https://learn.microsoft.com/ja-jp/exchange/address-books/address-book-policies/address-book-policies> (2024-09-02 参照)
- [5] Microsoft 社: 動的配布グループを管理する
<https://learn.microsoft.com/ja-jp/exchange/recipients/dynamic-distribution-groups/dynamic-distribution-groups?view=exchserver-2019> (2024-09-02 参照)
- [6] Microsoft 社: Microsoft 365 または Office 365 を使用して電子メールを送信するように多機能デバイスまたはアプリケーションを設定する方法
<https://learn.microsoft.com/ja-jp/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365> (2024-09-02 参照)
- [7] Microsoft 社: アクセス許可レベルおよびグループを決定する (SharePoint Server)

<https://learn.microsoft.com/ja-jp/sharepoint/sites/determine-permission-levels-and-groups-in-sharepoint-server#determine-whether-you-need-custom-permission-levels-or-groups> (2024-09-02 参照)

- [8] コードリブズ社: 全文検索サーバー Fess
<https://fess.codelibs.org/ja/> (2024-09-02 参照)