九州工業大学における Microsoft Teams の全学展開

林 豊洋 [1)], 黒崎 覚 [2)], 金光 昂志 [2)]

1) 九州工業大学情報統括本部 情報基盤センター

2) 九州工業大学情報統括本部 情報基盤課

toyohiro@isc.kyutech.ac.jp

Deployment of Microsoft Teams on Kyushu Institute of Technology

Toyohiro Hayashi[1)], Satoru Kurosaki[2)], Takashi Kanemitsu[2)]

1) Information Science and Technology Center, Kyushu Institute of Technology

2) Information Infrastructure Division, Kyushu Institute of Technology

概要

本学では，電子メールに代わる効率的なコミュニケーション手段として，2022 年度より Microsoft Teams の全学展開を行った．Microsoft 365 テナントの初期設定では，全てのユーザがチーム作成権限を持つことや，ファイル共有が組織外を含め自由に行える状態にある．他の Microsoft 365 のサービス提供への影響やガバナンスの観点で懸念があると判断し，本学では適切な設定値に変更し運用を開始した．加えて，チームの作成や年次更新については電子申請に基づく承認制を採用し，統制の取れたチーム運用を実現した．

1 はじめに

九州工業大学（以下，本学）では，既存の情報システムのあり方の問題点を洗い出し，更なる最適化を目指す方針ならびに，対象のサービス更新内容や時期等をマスタープランとして定め，情報基盤の更新を行っている．

情報システムの最適化の観点では，メールシステム（電子メール）からの脱却は重点的な課題と捉えている．電子メールは時代の要求に応じて機能向上がなされてきたが，セキュリティ上の問題が絶えず生じることや，プル型のサービスであるためタイムラグが多く，細かなやり取りは電話を併用する等の運用が必要である．

メールシステムからの転換として，チャット機能・ファイル共有機能を備えたコミュニケーションツールは有力な選択肢である．本学は全学的に Microsoft 365（以下，M365）を導入しており，M365 が有するコミュニケーションツールである Microsoft Teams（以下，Teams）を学内向けの連絡手段として適用可能であるか検討した．

Teams は M365 の初期設定において，全てのユーザが自由にチームを作成でき，ファイルの共有範囲については，組織外（匿名公開）を含め自由に設定できる状態にある．初期設定での運用は他の M365 サービス提供への影響が生じる可能性やガバナンス上の懸念があると判断し，Teams を構成する M365 上のシステム設定値を調整した後に運用を開始することとした．

また，統制の取れた運用するチームには責任者を設定すること，責任者の退職等に伴う交代，チームの休眠状態を抑制するための棚卸し等が重要であることから，本学においてはチームの作成と年次更新は電子申請に基づく承認制を採用することとした．

上記の運用方針に基づき，2022 年度より Teams の全学展開を行い，2023 年 9 月現在において約 110 チームが稼働している．その運用範囲は事務（係単位）・技術部・本部内室・タスクフォース等・研究室等と多岐にわたっており，メールからの脱却が順調に進んでいる．

本稿において，本学における Teams 運用に要した M365 の設定値変更や，チーム作成・年次更新の仕組み等について詳細を述べる．

2 本学における Microsoft Teams の展開

2.1 メールシステムからの脱却

本学で稼働する情報システムは，部局やプロジェクト単位で調達がなされ，国からの指針や法律への準拠に応じて個別最適させる方針であった．対して，利用者視点での利便性等の考慮は優先度が低く，レガシーな情報システムが林立している状況であった．本学では，このような既存の情報システムのあり方の問題点

を洗い出し，更なる最適化を目指す方針（Kyutech-DX ビジョン 2023）の定義 [1] ならびに，対象のサービス更新内容や時期等をマスタープランを定義した．

情報システムの最適化の観点から，本学ではメールシステム（電子メール）からの脱却は重点的な課題と捉えている．電子メールは本学において依然として重要なコミュニケーションツールであり，全学メールサービスを用いたメール送受信数は，一日平均 7 万通程度の流量を有している．時代の要求に応じて継続的に機能向上がなされているが，根底は設計が古い情報システムであるため，セキュリティや利便性の観点で多くの課題を有する．

利用者視点で顕在化しているセキュリティ上の問題点としては，機微情報の誤送信，受信者リストの露出（BCC と TO の指定ミス），送付先ミスによる添付ファイルの流出，転送設定ミスによるドッペルゲンガードメインへの情報流出等が顕在化しており，一部は本学においても報告されている．これらの問題点に対応するセキュリティ製品は存在するが，電子メール基底の脆弱さであるため根本的な対策は困難である．

加えて，電子メールにおけるメッセージの受信は，メールサーバへ受信要求を出すプル型となるため，コミュニケーションにタイムラグが生じる．したがって，短時間での細かなメッセージのやり取りが困難であり，場合によっては電話等を併用したコミュニケーションへ発展させる必要性が生じる．

これらの問題点が，本学がメールシステムからの脱却を検討すべきと捉えている事由となる．

2.2 新たなコミュニケーションツールの検討

前述した電子メールからの脱却の手段として，本学では新たなコミュニケーションツールの導入を検討した．特に，メッセージの送受信にチャットツール，ファイルの共有にオンラインストレージを利用し，電子メールや添付ファイル運用からの転換を図るパターンが増えている．

システム構築やメンテナンスのコストを抑えるためには SaaS の活用が有力であり，具体的なシステムの候補としては，Slack + Box や，Microsoft Teams 等が考えられる．

本学は，学生・教職員・卒業生を含む全学的な電子メールサービス運用のため，2015 年度に M365 を導入していた [2]．Teams は本学が契約する M365 ライセンス（2015 年当時は A1，2020 年度より A5）に含まれる機能である [3]．追加投資なく展開できることが期待されることから，学内向けのコミュニケーションツールとしての導入に向けて検討を行った．

2.3 Teams を構成するシステム，システム設定初期値に起因する懸念点

Teams は単体のシステムではなく，M365 上のシステムの組み合わせにより構成されている．

チームを作成すると，Entra ID（チームやそのメンバー管理），SharePoint Online（メッセージ管理等），OneDrive for Business（ファイル共有），Exchange Online（電子メールとの連携）等のシステムが連携して動作し，利用者にチームの形でサービスが提供される．

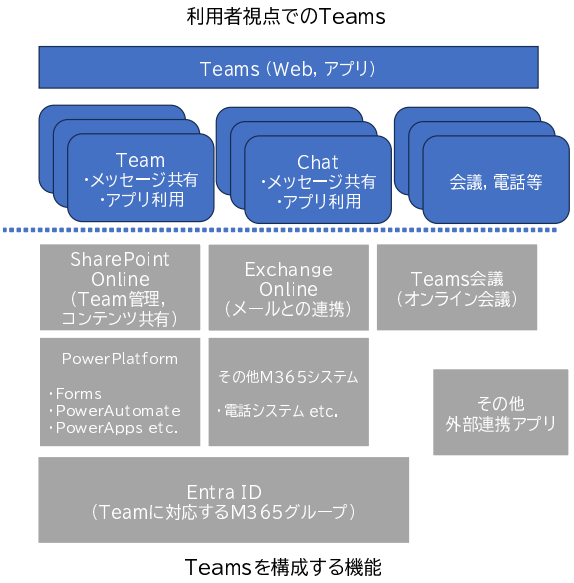

図 1　Microsoft Teams を構成するシステム

これら Teams と連携する M365 上のシステムは，Teams での利用向けに分離されている設計ではなく，M365 テナントの運用に影響が及ぶ可能性がある．加えて，M365 の各システムの設定値は初期状態では利用者にとっての自由度が高い傾向にあり，Teams の導入前に学内の運用ポリシーに合致するものであるかの判断を要する．以下にて，本学が認識する懸念点について述べる．

■チームの作成権限　Teams におけるチームの作成権限は，Entra ID 上のグループの一種である M365 グループの作成権限に依存する．本学が M365 テナントを展開した時期（2015 年 4 月）における M365 グループの作成権限の初期値は，M365 に登録されたメンバー（ゲストを除く）であった．

この当時は Teams は M365 上の正式サービスではなかったが，学生・教職員・卒業生を含む全てのユーザが自由にグループを生成できることにより，Exchange Online の配布リスト（メーリングリストに相当）の作

成を許してしまうことに大きな懸念があると判断し，グループの作成権限は管理者ロールを除き無効化していた．無効化の判断は後の Teams の正式サービス開始後，ユーザが自由にチームが作れてしまう挙動が抑制され，正しい判断であった．[*1]

■チーム名の命名規則　Teams におけるチーム名は，初期値では制約のない任意の名称が指定できる．

チーム名は，Entra ID 内の M365 グループ内の属性値にて管理され，グループの論理的な名称が M365 グループの Identity 属性値に対応する．Entra ID では，Identity 属性値はドメイン名内で一意であるため，命名規則を設けない場合，ユーザ名とチーム名が競合し，M365 上でのアカウント作成に支障が生じる．

■ゲストユーザの取扱い　Teams では，組織外のユーザをゲストとしてチームメンバーに追加することが可能である．初期値では，ゲストの追加は許可されている．

ゲスト追加により，組織外のメンバーを加えた情報交換が実現できる半面，Teams のゲストは与えられるアクセス許可範囲が広く，加えて個別にアクセス許可の制御が出来ないことが懸念となる．例として，チーム内にアップロードされたファイルの共有が可能であり，後述のファイル共有範囲の設定によっては，ファイルの情報流出を誘発する．

加えて，ゲストユーザの追加はチーム内のメンバー（ゲストを除く）であれば可能であるため，同様に情報流出のリスクが懸念される．

■ファイルの共有範囲　M365 上のオンラインストレージである Onedrive for Business は，Sharepoint Online を用いて実装されている．オンラインストレージの機能として，アップロードされたファイルの公開範囲・編集権限等の共有制御が可能であるが，初期値では制約が少ないことが問題となる．例として，初期値ではファイルアクセス用の URL を生成し，組織外ユーザが無認証でアクセスできる設定が可能である．

Teams のファイル共有は Onedrive for Business の機能を用いており，テナント上の共有設定と同一の振る舞いとなるため，チームに公開されたファイルが組織外に公開されるリスクが懸念される．加えて，本学は学生と教員が同一テナントに所属するため，慎重なアクセス設定が必要である．

上述した懸念点は，M365 の他のサービス提供に影響を及ぼすものや，チームの乱立や休眠化等の無秩序を招くものであり，M365 の設定値変更や運用を支援するシステム化が必要である．ただし，極端に自由度の低い設定とすると，コミュニケーションツールとしての機能が不足し，Teams の利用が促進されない危惧があるためバランスの良い設定値変更を実施する．

2.4　チーム提供に関するルール作成，作成手順・有効期限等の策定

本学においては Teams の提供に先立ち，チーム提供に関する最低限のルール「Microsoft Teams 利用ガイドライン」を全学方針として定めることとした．

ガイドラインには，申請可能な構成員の範囲（本学においては教職員のみを申請者とする），申請者の権限（申請したチームの所有者となり，チャネルやメンバーの追加が可能），目的外利用の禁止事項（営利的利用の禁止等），機微情報の取り扱いに関する注意事項，有効期限の導入（年度末が利用期限，更新により延長可能）等を条項として含んでいる．

■チームの作成手順　ユーザによるチームの作成権限を無効化することにより統制の取れたチームの作成が可能となる．対して，チームの作成を受け付け，内容に従って作成を進める必要があり，希望者・管理者共に負担は増大する．チームの作成に関するルールを定めることに加え，効率的にチームの作成を行うシステムが必要となる．

■チームの有効期限　部局・係向け等のチームは長期にわたる利用が見込まれる．対して，時限措置されたタスクフォース等のチームは短期利用が見込まれる．利用後のチームをそのまま存在させると，休眠化や情報流出のリスクが生まれる．また，チームの所有者が退職となり，変更となる可能性を考慮する必要がある．これらの理由より，作成したチームの有効期限を定め，棚卸し等の措置が必要となる．

3　M365 の設定値変更

■グループの作成制限　全てのユーザが自由にチームを作れる状況に制限を加えるため，Entra ID の設定を変更し，グループ作成が可能なユーザを限定化する．本学においては，グループ作成可能なユーザを追加していない（グローバル管理者は本制限によらず，グループ追加が可能となる）．

設定変更は，対象とする M365 テナントの Entra ID 上の Group.Unified 設定内の，EnableGroupCreation 属性値を False とし，GroupCreationAllowedGroupId 属性値に，グループ作成可能なユーザを管理するセキュ

[*1] グループ作成権限の初期値は，Teams の運用に限らず悪影響が懸念される．筆者らは，M365 テナントの展開後，ユーザアカウントを追加する前に無効化することを推奨する．

リティグループ等のグループ ID を指定する [4].

Listing 1　グループの作成可能範囲の限定化

```
$GroupName = "グループ作成可能セキュリティグループ名"

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id
$settingsCopy = Get-AzureADDirectorySetting -Id $settingsObjectID
$settingsCopy["EnableGroupCreation"] = $False
$settingsCopy["GroupCreationAllowedGroupId"] = $GroupName

Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy
```

■グループ作成時の命名自動付与　グループ名と通常のアカウント名との重複を防ぐため，本学においては M365 グループには名称の先頭に grp を付けることとした．管理者の運用方針として規定するのみでは操作ミスによる名称の付け忘れが想定されるため，本学においては Microsoft 365 グループに対する名前付けポリシー [5] を適用し，入力したグループ名に対して自動的に grp が付く設定としている．

なお，名前付けポリシーでは，グループ名の末尾に自動的に名称を付ける設定や，禁止用語の定義も可能である．

Listing 2　名前付けポリシーの有効化

```
Connect-AzureAD
$Setting = Get-AzureADDirectorySetting -Id (Get-AzureADDirectorySetting | where -Property DisplayName -Value "Group.Unified" -EQ).id
$Setting["PrefixSuffixNamingRequirement"] ="grp_[GroupName]"
```

本学の M365 テナントにおける Entra ID 上の Group.Unified 設定値は以下となる．グループ作成が指定したセキュリティグループメンバー以外不可であり，グループ名に grp が自動的に付与される設定値であることがわかる．

Listing 3　本学テナントにおける Group.Unified 設定値

```
$ID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id
(Get-AzureADDirectorySetting -Id $ID).values

Name                                Value
----                                -----
NewUnifiedGroupWritebackDefault     true
EnableMIPLabels                     false
CustomBlockedWordsList
EnableMSStandardBlockedWords        false
ClassificationDescriptions
DefaultClassification
PrefixSuffixNamingRequirement       grp_[GroupName]
AllowGuestsToBeGroupOwner           false
AllowGuestsToAccessGroups           True
GuestUsageGuidelinesUrl
GroupCreationAllowedGroupId         xxxx-xxxx-xxxx-xxxx-xxxx
AllowToAddGuests                    True
UsageGuidelinesUrl
ClassificationList
EnableGroupCreation                 False
```

■ゲストユーザの追加不可　ゲストユーザの取扱いは，Teams 上でゲスト追加を不可とする方法と，M365 テナントにおいて Entra ID のレベルでゲストユーザの追加を制限する方法が利用できる．

本学においては，Teams のみならず，Onedrive for business 等のファイル共有等を含めたアクセス制限を加えるためと Entra ID レベルで追加制限を付加する．Entra 管理センター上の「外部コラボレーションの設定」において，「ゲスト招待の設定」を「特定の管理者ロールに割り当てられているユーザー」以上とすることで，一般ユーザによるゲスト追加を制限できる．

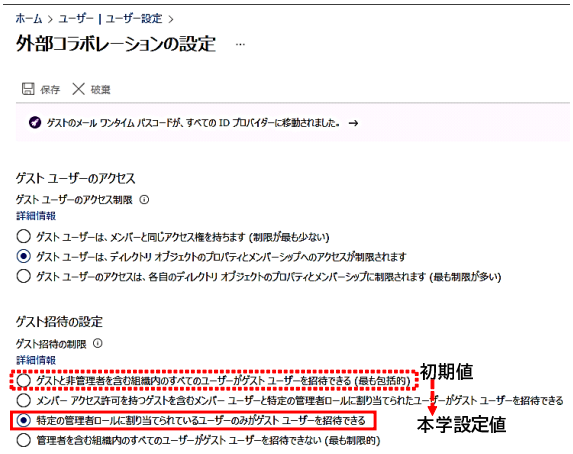

図 2　ゲストユーザの追加制限

■ファイル外部共有範囲の制限強化　SharePoint Online ならびに Onedrive for Business におけるコンテンツ共有の初期設定は「すべてのユーザ」に設定されており，サインインが必要ない URL リンクを生成できる水準となる．また，ダウンロードリンクの有効期限や確認コード（メール認証）も設定されていない．

本学においては，共有レベルを「新規および既存のゲスト」に設定し，加えて外部公開時に確認コード入力を要求するレベルに変更している．また，共有リンクの有効期限は 60 日としている．

なお，本学においては，事務職員向けとして専用の M365 テナントを別途用意しており，事務職員テナントにおいては共有レベルをテナント内ユーザのみとして，より厳しいアクセス制限を実施している．

4　チーム作成，年次更新の承認制の導入

4.1　チーム作成のオンライン申請，自動化

前述の通り，本学においては，利用者による申請に基づきチーム提供を行う方針とした．チームの利用者（=申請者）と管理者双方にとって効率的にチームの作

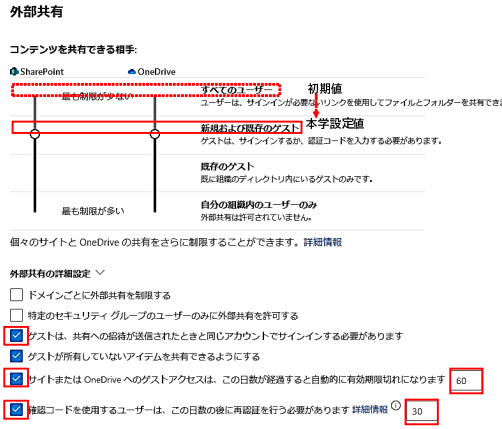

図 3　ファイル外部共有範囲の制限強化

成を行うシステムが必要となる．

本学においては，Microsoft Power Platform[6] を活用したオンライン申請・チーム作成システムを構築した．（図 4）．以下の機能群により，オンライン申請・チーム作成の自動化を実現する．

新規チーム登録手続きは，(a) チーム名や利用目的を記載するオンライン申請フォーム（Forms による利用者ユーザインタフェース），(b) 申請内容の承認，データ管理，新規チーム登録処理等のワークフロー定義（Power Automate によるワークフロー定義），(c) 申請内容，新規チーム登録結果等のデータ記憶（SharePoint Lists によるデータ管理）(d) 申請内容に基づき，PowerShell によるチーム登録処理の実施（オンプレミス側の連携処理）の機能群で構成される．

上記の手順により，Forms を用いた申請後に承認者が Teams 上で決裁処理を実行するのみで，新規チームの作成と申請者への通知が完了する．

4.2　チーム年次更新のオンライン申請

申請内容や新規チーム登録結果は SharePoint Lists に蓄積しているため，Lists を活用し，チームの年次更新の確認を実施する．年次更新システムは，申請者に承認された利用中のチームに関する情報を Lists のビュー機能により提示し，次年度の継続利用についてオンライン上で回答が収集可能な構成としている（図 5）．

5　本学における利用状況

M365 の設定値変更については，グループ作成権限の変更については 2016 年度に既に実施していたが，その他の制限付加については，2021 年度に適用を完了した．その後，手作業でチームを作成し，ゲストアクセスやファイル共有の制御が有効に機能していることを確認し，2022 年 5 月より正式にオンライン申請による Teams の展開を開始した．

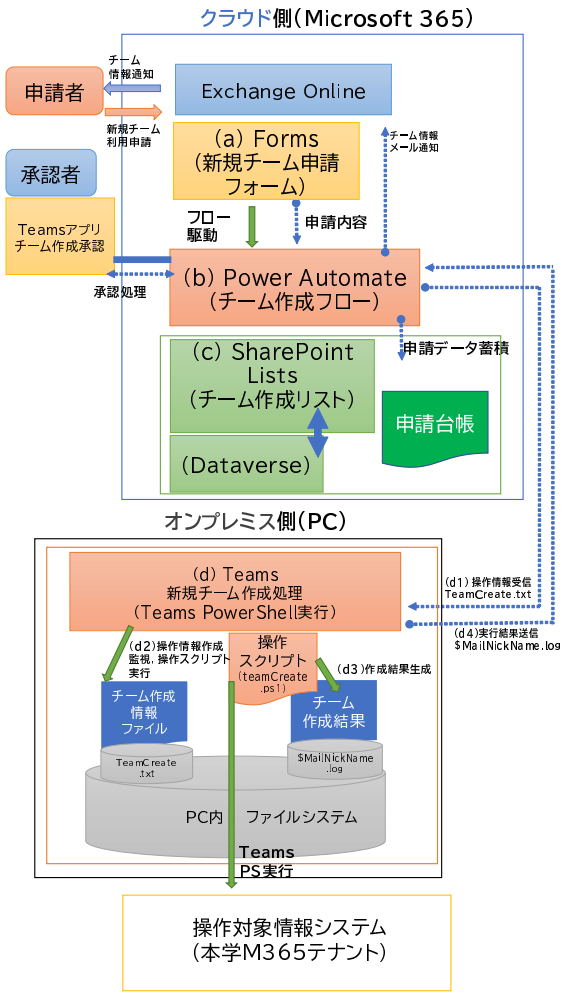

図 4　新規チームオンライン申請・作成システムの構成

開始年度である 2022 年度に，合計 78 件の新規チーム申請について承認した．2023 年度 9 月現在では約 110 チームが稼働している．申請されたチームの割合は，研究室向けが最も多く，事務（係単位）・技術部・本部内室等の長期利用が見込まれるチーム，時限付きと見込まれるタスクフォースやプロジェクトと利用範囲は多岐にわたる．電子メールからの脱却が順調に進んでいると考えられる．

年次更新については，2022 年度末である 2023 年 1 月に年次更新に関する通知を実施し，2023 年 3 月までに回答を要求した．こちらも，前述の SharePoint Lists のビューを活用したオンラインシステムにより，Excel 形式等によらない回答収集が可能であった．2022 年度申請分の 78 件のチームのうち，70 件が継続回答となった．継続しないチームの例としては，2022 年度用

図 5　チーム年次更新画面（SharePoint Lists 申請者ビュー）

の研究室向けチームと言った申請であり，年度により完全に別チームを新規に作り直す利用形態も存在することがわかった．

6　まとめ

本論文では，本学における Microsoft Teams の全学展開について，経緯や導入の際の検討事項を中心に述べた．メールに代わるコミュニケーションツールの導入検討を行う際，チャットツール・オンラインストレージ・会議ツール等を組み合わせたシステムが必要となる．M365 を導入する機関においては，必要な機能が全て包含される Teams は有力な選択肢となる．

しかし，M365 テナントの初期設定においては，ゲストユーザの取り扱いや権限，ファイル共有の権限について自由度の高い設定値が採用されており，そのままの状態での Teams 展開は懸念がある．本稿では，ガバナンスを強化した状況での Teams 展開が可能な状況とする設定値の変更について述べた．

加えて，利用者からの申請に基づくチーム作成と休眠状態を防ぐための棚卸となる年次更新の必要性ならびに，それらの自動化・オンライン化手法について述べた．本学においては，Power Platform を用いたオンライン申請と自動化，SharePoint Lists を用いた年次更新のオンライン化について実装し，利用者へ提供している．

2022 年度に Teams の正式運用開始後，既に 110 以上のチームが稼働しており，学内の連絡手段においてはメールシステムからの脱却が進みつつある．筆者らが所属する部局においてもチームを作成し，部局メンバー内の情報交換は Teams が中心となり，メールは他部局・学外との連絡手段での利用に限られる状況となっている．

今後は，教職員向けのメール通知，学内メーリングリスト，機材からアラート通知等，メールでの運用が残っている部分の Teams への転換に関する検討を進める．

参考文献

[1] 九州工業大学，Kyutech-DX ビジョン 2023，https://www.kyutech.ac.jp/information/kyutech-dxvision.html，2023.

[2] 林豊洋, 甲斐郷子, 九州工業大学における生涯メールサービスの移行，大学 ICT 推進協議会 2017 年度年次大会，2017.

[3] Microsoft, Microsoft Teams admin documentation, Microsoft Learn - Documentation, https://learn.microsoft.com/en-us/microsoftteams/.

[4] Microsoft, Manage who can create Microsoft 365 Groups, Microsoft Learn - Microsoft 365, https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-creation-of-groups，2023.

[5] Microsoft, Enforce a naming policy on Microsoft 365 groups in Azure Active Directory, Microsoft Learn - Azure, https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy，2023.

[6] Microsoft, Microsoft Power Platform documentation, Microsoft Learn - Documentation, https://learn.microsoft.com/en-us/power-platform/，2023.