学外者と共同作業するための認証基盤の拡張

中村 誠 [1)], 郡司 彩 [2)], 玉造 潤史 [1)]

1) 東京大学 情報システム本部
2) 東京大学 本部情報支援課

Extending Authentication Infrastructure for Collaboration with External Users

NAKAMURA Makoto [1)], GUNJI Aya [2)], TAMATSUKURI Junji [1)]

1) Division for Information and Communication Systems, the University of Tokyo
2) Information Systems Department, the University of Tokyo

概要

大学の学生・教職員に IT サービスとして提供している Teams，研究プラットフォームとして提供している UTokyo Azure を学外者と共同で利用するために大学の認証基盤 IdP である Entra に学外者をゲストアカウントとして登録する試行を開始した．登録申請から承認，反映を行うアプリを開発し，ゲストアカウントの機能と挙動を調査した．学外者は各自の組織アカウントあるいはメールアドレスを使用して安全かつ効率よくサービスを利用して共同作業できることが確認できた．

1 はじめに

東京大学では，メール，ファイル共有などのクラウドサービスを活用して IT サービス，情報基盤環境を構築し，学生・教職員に提供している．ここ数年はオンライン授業の柔軟な活用や在宅勤務や DX・業務改革への積極的な取り組みにより，業務や教育研究活動に IT サービスを最大限に活用する傾向が強まっている．具体的にはメールとファイル共有は Microsoft 365，Google workspace を，チャットは Slack と Teams を，会議は Zoom, Webex を活用している．

かつては学内での連絡やファイル共有の多くはメールが使われていたが，メールへのファイル添付は徐々に Google Drive，OneDrive/SharePoint に保存したファイルへのリンクを送る形に変わりつつある．周知や連絡も特に部署内や研究室などのやり取りではメールや電話から Slack，Teams や Zoom を活用することが増えている. 学外者とのやり取りもメールのみに依存せずクラウドストレージやチャットツールを利用することが増えている。なおリンクはメールの転送などで簡単に共有，拡散されうるため安全性への指摘がされることもある。

様々な IT サービスを駆使して学内外の関係者と共同作業をするようになったが，特に学外者，外部ユーザとの共有方法はサービスによってバリエーションがある．

従前の IT サービスでは学外者，外部ユーザも学生・教職員と同様に構成員として扱い，認証基盤に登録してきた．この方法では目的とするサービス以外も利用できてしまうため本来なら不要なシステム運用コストが生じたり，アカウントの適正な管理上構成員に求めているセキュリティ維持コストが過剰に生じたりしてしまい，適切な運用を実現することが困難であった．しかし，近来のクラウドサービスでは外部アカウント連携や柔軟なリソースへのアクセス管理機能などが提供されており，これらを活用することで外部ユーザとの共同作業が実現できないか検討することにした．

2 外部ユーザのサービスへの取り込み

サービスではいろいろな形で外部ユーザと共同作業をする方法が提供されており，その方法を分類する．

a. 共有リンク

Google Drive などのクラウドストレージなどでは，共有したいファイルのリンクを作成し，メールやチャットで外部ユーザに伝えることでファイルを送信したり，共同で編集したりすることができる．簡便な方法だが，リンクを知っていれば誰でもアクセス可能なこともあり，実際にアクセス

したのが誰なのか分からない場合もある点に注意が必要である．

Zoom などの会議ツールでも会議 URL を共有することで，外部ユーザと会議を実施できる．

b. 相手を指定して共有

同じくクラウドストレージなどでは，共有したい相手のメールアドレスを指定してファイルを共有することもできる．サービスによるが，メールアドレスでサインインしたり，メールアドレスに確認コードを送信するような形でユーザを確認している．

メーリングリストやアドレス帳に外部ユーザのメールアドレスを登録してメール配信する形態もこの方法の 1 つと見なせる．

c. ゲストアカウントとして登録

Slack や Teams などのチャットツールなどでは，招待したい相手のメールアドレスを指定して自テナントに参加させることができる．サービスによるが，一般的には招待したユーザがディレクトリ（名簿）に登録されることが多く，相手を指定して共有との違いである．

メールサービスでエイリアスや転送機能を利用してメールアドレスを付与することもこの方法の 1 つと見なせる．

d. 組織アカウントを使わせる

外部ユーザを学生・教職員と同じように登録し，組織アカウントを発行しサービスを使わせる．運用ルールやライセンス，組織統制などさまざまな観点で問題になりうる．

a-c の方法において，例えば Google や Apple でサインインのような外部 IdP との連携により外部ユーザをユーザを認証，識別することがある．学術機関向けサービスでも例えば GakuNin RDM では他機関 IdP や Orthros で認証された外部ユーザと共同で研究データ管理を行うことができる．

これまで共有リンクや相手を指定した共有ではなくゲストアカウントとして登録しなければ外部ユーザと共同作業できないサービスに関して，組織アカウントを使わせるという手段を取るケースが散見された．組織アカウントは学生・教職員に十分なサービスを提供するためにライセンス費用をかけて整備している．また学生・教職員に対する教育研修などにも活用されており学外者が紛れ込んでいるとそれらの業務の管理や対応コストの負担増に繋がっている．そのためサービスの特性に応じた適切な方法で外部ユーザと共同作業できることが重要である．

3　ゲストアカウントでの試行

学内での業務や研究活動においてクラウドサービスを活用して共同作業をする機会が増え活動が効率化した一方で，学外者とのやり取りが従来通りだと，情報共有の作業が二度手間になり，情報が分散して管理が煩雑になるなどの問題意識が強くなった．そこで学内での業務において活用している Teams に学外者を参加させることを検討し試行することにした．

Teams は本学の認証基盤である UTokyo Account で利用できる（図 1）．UTokyo Account は Microsoft Entra を採用しており[1]，Entra にはゲストアカウントを登録する機能があり，ゲストアカウントを Teams チームメンバとして参加させることができる．ただし誰でもゲストアカウントを招待して参加させると問題が発生する懸念があるため，招待する権限を特定のユーザに限定し，招待・参加は申請制とし承認された場合のみ登録作業を行うことにした．

UTokyo Azure も共同研究相手である学外者と共同で生成 AI モデルなどの Azure が提供する機能を活用した研究を行うため，学外者による Azure Portal の利用を検討していた．Azure Portal を利用できるのは Entra にアカウントがある必要があるため（図 1），Teams 同様にゲストアカウントを登録管理することにした．

なお Entra のアカウントの種類にはメンバーとゲストがあり，メンバーアカウントは学生/教職員の在籍者情報をもとに認証基盤の ID 管理システムが自動的に追加削除などを行っている．

4　ゲストアカウントの登録申請フロー

Teams チームへの学外者の招待申請は PowerApps で作成したツールから行う（図 2）．

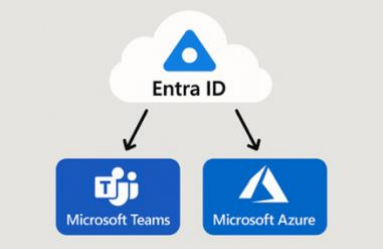

図 1 Entra と Teams, Azure の関係

図 2 Teams ゲスト登録申請アプリ

PowerApps で作成した申請は SharePoint リストに追加され，リストへの追加をトリガーとして Power Automate フローが起動される．フローでは Teams アクティブカードを用いた簡易な承認処理を実施し，承認された場合はゲストアカウント追加の API，チームグループへのメンバ追加の API などの呼び出しを行い申請結果を反映している．正常にアカウントが追加できた場合は学外ユーザと申請者に招待 URL などが記載されたメールを送信する．

チームグループへのメンバ追加は Power Automate の標準コネクタが用意されていたが，ゲストアカウント追加は標準コネクタが存在しなかった．そこでゲストアカウント追加 は Microsoft Graph API を直接呼び出すこととし， Entra にアプリ登録し，Power Automate の HTTP コネクタを用いて実装した．

PowerApps で作成した申請は運用管理担当が参加する Teams チームの SharePoint リストに保存される．標準の設定では申請者はリスト閲覧権限がないため過去の申請を確認できない．そこでリストアイテムの閲覧権限を設定する処理をフローに追加し申請者が履歴を閲覧できるようにした．

UTokyo Azure への外部ユーザの招待は Forms から申請する点は Teams チームとは異なるが，Power Automate フローの構成はほぼ同様で問題なく作成できた．

5 ゲストアカウントは何かできるのか

Entra ではゲストアカウントとして登録されたユーザはメンバー同様にディレクトリに登録される．ディレクトリに登録されたユーザはサービスによるがゲストであってもメンバーと同じようにサービスが利用できることもある．Microsoft が提供する技術情報ではゲストアカウントが Microsoft 365 などの個々のサービスの利用可否が簡潔に明示されていなかったため，ゲストアカウントは何かできるのか各サービスや機能をひとつひとつ調べることにした．

招待された学外者は所属組織が Microsoft 365 を利用している場合は自身が使用する Entra 組織アカウントでサインインする．Microsoft 365 を利用していない場合はメールアドレスに送信された確認コードを入力することで認証する．

ゲストアカウントのユーザ ID (User principal Name, UPN)は内部的には登録する際に指定したメールアドレスをルールに基づき変換した文字列となる，例えば user@example.com は user_example.com#EXT#@tenantid.onmicrosoft.com のような文字列になる．

5.1 Teams，Azure

Teams ではメンバとして登録されたチームのみにアクセスができる．チーム内でのチャットやファイルの共同編集ができる．

Azure Portal ではゲストアカウントにも RBAC（権限管理機能）で共同作成者などのロールを割り当てが可能で，権限に応じてリソースの管理ができる．なおベンダによるセキュリティ強化施作により多要素認証が求められる．また通常の URL にアクセスしてサインインする際にメールアドレスを入力してもエラーになるため，テナント ID をパラメータとして追加した URL にアクセスする必要がある．

5.2 Microsoft 365

Microsoft 365 のサービスのうち，Copilot は利用できなかった． Microsoft 365 Apps（デスクトップ版アプリ），Exchange/Outlook もライセンスが付与されていないため利用できない．

OneDrive と SharePoint も基本的には利用できないが．外部共有が有効になったサイトで，共有相手として追加されている場合は共有されたサイトやファイルのみアクセスできる．

Forms では学内者限定で共有されたフォームに回答者としてアクセスできる．ただしフォームにアクセスするためには共有 URL を入手する必要がある．また回答者のユーザ ID が UPN ではなくメールアドレスとして記録・参照されるため，Power Automate で自動処理をする際には注意が必要である．

5.3 学内サービス

学内サービスのうち，VPN，Wi-Fi アカウント申請，Slack は多要素認証の有効化と情報セキュ

リティ教育の受講が前提条件でありアクセスできない．前提条件は Entra の条件付きアクセスとアプリへのユーザ割り当て機能を用いて実現している．条件付きアクセスは，どのユーザに，どのアプリに対して，多要素認証を求めるなどどういう制御を行うかを設定する仕組みで，多様認証の認証方法を登録した後に UTokyo Acocunt 利用者メニューで利用開始したユーザに対してすべてのアプリで多要素認証を求める設定を行なっている．アプへのユーザ割り当ては，SSO 設定したアプリに割り当てたユーザのみがアプリを利用できるように制限する機能で，情報セキュリティ教育を受講したユーザが利用できるようにしている．

その他の学内サービスや業務システムの多くは利用することができない．その理由はシステム側でユーザとして未登録である，あるいは IdP が送信する属性がシステムが許容する内容ではないためである．一方で認証可否だけを参照してアクセス制御している一部のサービスはアクセスできた．

Google workspace は独自のユーザ名を採用しており，サインイン UI でユーザ名を指定できないこともありアクセスできない．

5.4 学認

学認 SP も多くは同様に利用できないが，認証可否や組織名のみを参照してアクセス制御していると考えられる一部のサービスはアクセスができた．

6 課題と今後

現時点では学外者との共同作業が終わりゲストアカウントが不要になった際に登録解除・削除を PowerApps から申請することができず，メールなどで連絡が必要である．申請履歴の閲覧が申請者に限られるため同僚や後任が申請できないことも一因であるため，履歴の閲覧権限をグループ化するなどの対応と合わせゲストアカウントの棚卸し機能を検討している．

学生・教職員が使用するメンバーアカウントのみを対象に条件付きアクセスによる多要素認証の制御を行なっているため，学外者が使用するゲストアカウントの多要素認証に関する制御ができていない．学外者も教職員と同様に多要素認証の制御をすべきであるため，登録処理と条件付きアクセスの連携を検討している．

いくつかのサービスにゲストアカウントが何らかのアクセスができることが確認されたので，必要に応じて Entra の条件付きアクセスとアプリへのユーザ割り当て機能や学認向け IdP である Shibboleth IdP の設定を調整する予定である．

UTokyo Account に関する問い合わせ窓口に，学外者がパスワード忘れや多要素認証に関して問い合わせてくることが少なくない．一部の部局・部署では学外者にサービスを提供することもあるようで，サービス利用者を在籍者として登録し UTokyo Account を使わせていることがあるようである．また学外者と連絡や共同作業を行うために学外者を在籍者として登録してしまっていることもあるようである．このような事態は大学組織としての在籍者管理として決して適切な状況とは言えないのは明らかであり，ゲストアカウントなどの認証基盤の拡張や学内サービスの設計運用の改善を行い在籍者管理の適正化に繋げていきたい．

7 関連する取り組み

デジタル庁が提供する「デジタル認証アプリ」を活用しマイナンバーカードにより UTokyo Account の利用者をオンラインで本人確認する「UTokyo Account 本人確認サービス」を開発し，9 月から運用を開始した．現在はパスワードや多要素認証の認証方法を忘れた場合や，卒業修了後のクラウドデータ救出の手続きが行える．このサービスでは UTokyo Accocunt での認証ができない場合でもデジタル認証アプリで利用者を認証しており，この方法を拡張して学外者の認証や IT サービス利用の枠組み構築を検討している．

8 まとめ

大学が導入した IT サービスを活用して学外者と共同作業を行うため，今回は大学の認証基盤である Entra のゲストアカウント機能を用いた．学外者は各自の組織アカウントあるいはメールアドレスを使用して安全かつ効率よくサービスを利用して共同作業が行えることが確認できた．

参考文献

[1] 玉造 潤史, 竹内 朗, 中村 誠, 竹内 利圭, 加藤 淳，本城 剛毅、東京大学への多要素認証導入、大学 ICT 推進協議会 2024 年度年次大会論文集、pp.11-17、2024.