マイナンバーカードを活用した全学アカウント運用

本城 剛毅 [1)], 金子 亮大 [2)], 中村 誠 [2)], 玉造 潤史 [1),2)]

1) 東京大学大学院理学系研究科
2) 東京大学情報システム本部

Campus-wide Account Management Utilizing My Number Cards

Goki Honjo [1)], Ryotai Kaneko [2)], Makoto Nakamura [2)], Junji Tamatsukuri [1),2)]

1) Graduate School of Science, the University of Tokyo.
2) Division for Information and Communications Systems, the University of Tokyo.

概要

東京大学では大学の全構成員（学生・教職員）の統合認証アカウントとして UTokyo Account を運用しているが、デジタル庁の提供するデジタル認証アプリを利用して UTokyo Account 本人確認サービスをリリースした。このサービスではマイナンバーカードによる本人確認をオンラインの機能として実現しており、UTokyo Account のパスワードをリセットする機能や多要素認証の再設定をすることができる。これによって、本人確認の精度向上や、ユーザーの処理時間の短縮が期待される。さらに、卒業・修了生など離籍後に東京大学のサービスを提供する基盤として活用する計画である。

1 はじめに

東京大学では、学内の統合認証基盤として「UTokyo Account」を運用している。このアカウントは、学務システムや LMS などの教学支援システムや学内教職員ポータルサイトへのログインに使用されているほか、全学的に利用されている各種システムにおいて、UTokyo Account による認証方式への統一が進められている。従来はシステムごとに異なる ID・パスワードを設定・管理する必要があったが、その手間が大幅に軽減された。さらに、セキュリティの観点から重要な多要素認証の導入も、UTokyo Account に一元化することで効率的に実装できるようになり、学内全体の情報セキュリティの向上にもつながっている。

UTokyo Account は、Microsoft Entra ID を基盤として構築されており、パスワード認証に加えて多要素認証を組み合わせた形で本人確認を行っている。新たに入学・入職する際には、アカウントとして ID と初期パスワードが交付され、ユーザーは初期パスワードを任意のパスワードに変更すると同時に、多要素認証の設定を行う。

多要素認証としてスマートホンにインストールされた「Microsoft Authenticator」アプリを設定した場合、ログイン時にブラウザ上で ID を入力すると Microsoft Authenticator に通知が届く。ユーザーは、ブラウザ上に表示された 2 桁の数字を Microsoft Authenticator に入力することで認証が完了する。

UTokyo Account による認証では、パスワードの入力を省略できる場面が多くなっているため、ユーザーがパスワードを忘れてしまうことがある。また、Microsoft Authenticator を利用した多要素認証はスマートホンに依存しているため、機種変更の際に旧端末を初期化してしまうと、認証ができなくなるという問題が生じる。

こうした状況に対応するため、東京大学では、パスワードの初期化や多要素認証の再設定を行う際に、対面での本人確認を実施した上で初期パスワードを再交付する方法や、特設ウェブサイトを通じて身分証明書をアップロードすることで本人確認を行う方法など、複数のリカバリー手段を用意してきた[1]。

しかし、これらの方法は、いずれも職員による目視確認を前提としているため、対応可能な時間が限られておりユーザーの問題解決まで時間を要することがあるほか、本人確認の精度にも一定の制約があった。

こうした課題を解決するため、2024 年にデジ

タル庁からリリースされた「デジタル認証アプリ」[2]に注目した。このアプリは、Android および iOS 向けのアプリで、マイナンバーカードを用いた認証や電子署名を行う際に使用される。行政手続きや民間サービスにおいて安全かつ確実な本人確認を可能にするもので、上記の問題点を技術的に大きく改善する可能性を持っていた。

アプリケーションやウェブサービスにデジタル認証アプリを使用した認証や電子署名機能を組み込みたい場合は、デジタル認証アプリサービス API[3]を呼び出すだけで簡単に実現することができる。すでに多くの行政機関や民間事業者がこの API を活用し、マイナンバーカードを使ったサービスを展開している。これにより、ユーザーはスマートホンを通じて、より便利でセキュアな手続きを行えるようになっている。

2　UTokyo Account における eKYC

UTokyo Account は全学構成員を対象としたサービス利用時の認証手段である。近年のデジタル化によりほとんどの構成員が大学活動に常時利用している状況にあり、アカウントにおけるトラブルは重大な支障を生じることとなる。

本学の UTokyo Account の大きな特徴のひとつは教職員と学生が同一のアカウントを同一の利用ポリシーで利用しているところである。前述の通りすべての構成員が多要素認証を設定してアカウントを利用している。しかし、実情として多要素認証の仕組みが完全に理解されている状況にない。そのため、認証方法として利用しているスマートホンなどを故障や機種変更等により不用意に認証手段として使えなくしてしまう利用者があとを絶たない。

このような場合、オンラインによる電子的な本人確認（eKYC）手法が確立していれば即座に再設定を提供することができる。本学の構成員管理は学務システムと人事系のシステムに分離されており、共通の本人確認に利用できる情報がなく、特に教職員には雇用関係を持たない者も多く在籍している。雇用関係を持たない者は大学が管理している個人情報も少なく、本人確認には受け入れ登録をした窓口で確認するほかない状況であった。定型的な本人確認を実現できないことはアカウント運用上の問題であった。

このような状況から eKYC の実現は運営上の課題であったが、既存の eKYC サービスは多くの場合、利用者数に応じたコストが必要で、現実的ではなかった。そのため、UTokyo Account 利用者全員（学生・教職員）が共通に保有している情報・手段を活用して eKYC を実現することが必要であり、この観点からマイナンバーカード施策の進捗を注視していた。

3　検証とシステムの実装

東京大学の情報システム本部および大学院理学系研究科の情報システムチームが共同でデジタル認証アプリを使った認証機能のシステム実装と動作検証をおこなった。その結果、学内システムに支障なく導入できることが確認されたため、UTokyo Account のパスワード初期化や多要素認証の再設定時の本人確認手段として、デジタル認証アプリを活用できるようにシステム開発を進めた。

3.1 デジタル認証アプリ

デジタル認証アプリによる認証機能を導入するには、デジタル認証アプリサービス API を呼び出すことになる。この API の技術仕様はデジタル庁の公式ウェブサイトにて公開されており、認証プロセスは OpenID Connect の認可コードフローに基づいて設計されている[3]。OpenID Connect に対応したフレームワークであれば基本的に認証機能を導入することが可能であり、開発者にとっては実装の自由度が高く、導入のハードルも比較的低い。ただし、RP（Relying Party、認証機能を組み込みたいアプリケーションやサービス）が OP（OpenID Provider、認証機能を提供するサーバー）にトークンを要求する時の認証方式として private_key_jwt 方式が採用されているため、この方式に対応したフレームワークを用いる必要がある。

認証に成功すると、PPID（Pairwise Pseudonymous Identifier、RP ごとに固有な個人識別子）とともに、API の利用申請時に指定された範囲に応じて氏名・生年月日・住所・性別といった情報（基本 4 情報と呼ばれる）を取得すること

ができる。PPID は、同じ人が認証する限りは同じ PPID が与えられるため、個人の同定に使うことができる。また、他の RP から認証した場合には別の値となるため、情報漏洩などの事故があった際の影響は限定的なものとなる。

3.2 ミドルウェアの検証

デジタル認証アプリサービスの API を呼ぶミドルウェアとして、以下の理由から mod_auth_openidc を採用した。

① このモジュールは Apache HTTP Server の拡張機能として動作するため、既存のウェブサーバー環境に容易に組み込むことができ、また設定も比較的簡単であること

② OpenID Certified™の認定を受けており[4]、OpenID Connect の仕様に準拠した動作が期待できること

③ private_key_jwt 方式による認証に対応していること

mod_auth_openidc は Apache HTTP Server の他の認証モジュールと同様に、特定の URL やディレクトリに対して OpenID Connect 認証を有効化することができる。

mod_auth_openidc の動作検証には、以下の 2 つの環境を活用した。

① OpenID Foundation が提供する OpenID Connect RP 向け Conformance Test[5]

② デジタル庁が提供するデジタル認証アプリのテスト環境[6]

Conformance Test は、mod_auth_openidc が OpenID Connect の基本仕様に準拠しているかどうかを再確認するために使用した。Conformance Test にはテストのためのプランが多く用意されているが、この中で Basic Certification Profile Relying Party Tests と Configuration Certification Profile Relying Party Tests を使用した。これらのプランの中にそれぞれ複数のシナリオが用意されていて、各シナリオで仕様通りの振る舞いをすることが確認されると、「テストに合格」となる。前者のプランは client_secret_basic 方式による認証であるが、より多くの“不適切な入力”のテストが含まれているため検証に含めた。

前者のプランはすべて合格したが、後者のプランの中で、「OP から提供される Issuer が本来のものと異なる場合に、RP がそれを検出して正しく認証を失敗するか」というシナリオのみ検証することができなかった。この点の対処については後述する。

デジタル庁のテスト環境では、主にテストカード代替機能を利用した。この機能では、通常はマイナンバーカードを用いて認証を行うところを、カードを使用せずに認証処理のテストを行うことができる。正常なレスポンスだけでなく、意図的に異常なレスポンスを返してもらうことも可能であり、異常系の挙動確認に非常に有効である。用意された異常レスポンスに対して、mod_auth_openidc はすべて正しく認証を失敗させることができた。

加えて、RP が OP から受け取るレスポンスに関して、セキュリティ強化の観点から検証すべき項目がいくつか存在する。これらの項目はデジタル庁の公式ウェブサイトに掲載されており、mod_auth_openidc がそれらに対応しているかどうかを確認するために、ソースコードの内容を確認した。現時点では、必要なセキュリティ要件を満たしていると判断している。

3.3 UTokyo Account 本人確認サービスの実装

UTokyo Account 本人確認サービスは、デジタル認証アプリで認証した際に得られる PPID と UTokyo Account を事前にひも付けておく仕組みである（図 1、図 2）。このひも付けを行っておくことで、たとえばパスワードのリセットが必

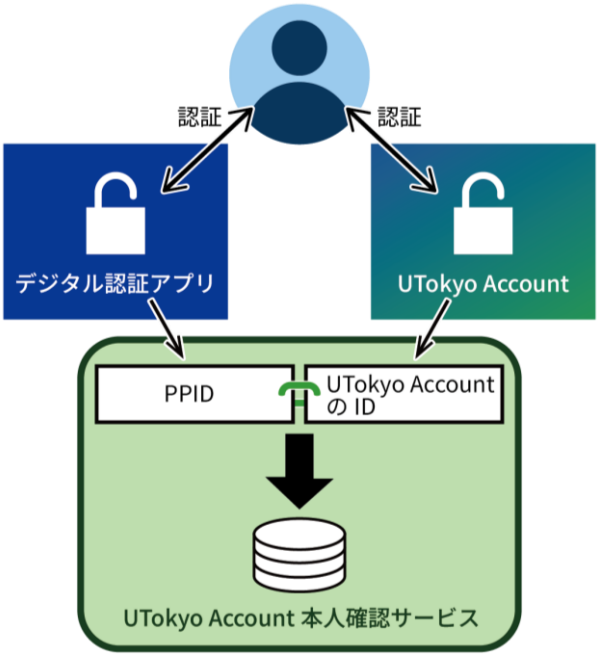

図 1：UTokyo Account 本人確認サービスのシステムイメージ図

要になった場合には、PPID から UTokyo Account を特定し、リセット処理を進めることができる。

PPID と UTokyo Account のひも付けを行う際には、当然ながら本サービス上でデジタル認証アプリと UTokyo Account の両方で認証する必要がある。本サービスでは、UTokyo Account の認証にも OpenID Connect を利用している。

mod_auth_openidc を使って複数の OP を利用する場合、OpenID Connect Discovery による自動設定は使えず、OpenID Connect Discovery で使用される URL にアクセスして取得できる設定情報を事前にダウンロードしておく必要がある。前述した OpenID Foundation の Conformance Test で検証できなかった部分についても、この設定情報をあらかじめダウンロードしておくことで対処した。

デジタル認証アプリと UTokyo Account の両方で認証が完了すると、画面上に「ひも付け」ボタンが表示される。このボタンを押すことで、PPID と UTokyo Account のひも付けが記録される。

パスワードのリセットや多要素認証の再設定を行う場合には、ユーザーはまずデジタル認証アプリで認証する。PPID に UTokyo Account がひも付けられていれば、パスワードリセットや多要素認証再設定のためのボタンが表示され、手続きを進めることができる。

3.4 パスワードリセットと多要素認証の再設定

UTokyo Account は Microsoft の Entra ID を基盤として構築されている。そのため、パスワードリセットなどの操作は Microsoft Graph API を使用して実施することができる。Graph API を使用してパスワードリセットを行った場合、次回新しいパスワードでサインインした際にはさらに別のパスワードへの変更が強制される仕組みになっている。[7]

図 2：UTokyo Account 本人確認サービス

多要素認証の再設定を行う場合には、「一時アクセスパス」[8]と呼ばれる、一度だけ多要素認証をスキップしてサインインできる特別なパスを発行する。この一時アクセスパスを使ってサインインした後、利用者は多要素認証の設定ページに誘導され、Microsoft Authenticator の再登録など多要素認証の再設定を完了できるようになっている（図 3）。

デジタル認証アプリでの認証からパスワードリセット・多要素認証の再設定まで、即時に、人手を介することなく処理を進めることができる。

4 システムの展開

サービスの提供開始は 2025 年秋の卒業・修了時期とした。秋は春よりも卒業・修了となる学生数が少なく、春に向けて十分なチューニング期間を取ることができるため開始時期として適切であるとの判断による。

システム利用情報のポータルサイトである utelecon にサービスの説明と利用開始時の事前

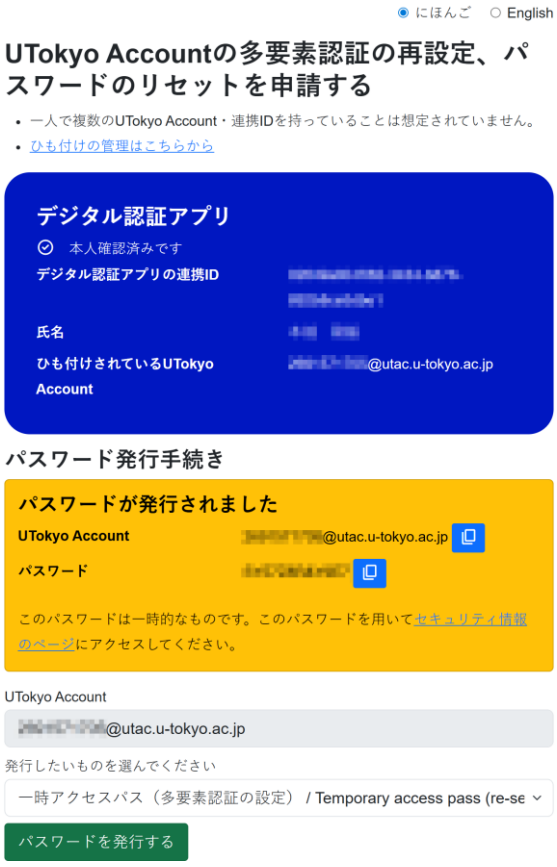

図 3：UTokyo Account 本人確認サービスで一時アクセスパスを発行した様子

連携のページ（日・英）を作成した[9]。サイト作成のため、デジタル庁からの本サービス開始前の検証情報を学生サポーターに提供し約 1 か月で精緻なサイトコンテンツが準備された。

また、毎学期、教職員向けに実施しているオンライン説明会で取り上げデモを実施した。そこで、実際の利用方法を示すとともに、設定の必要性を学内向けに提示した。

春学期で卒業・修了する学生向けには全部局の学務担当を経由して周知を行い、周知を効果的に行うため、学務担当者にとっても卒業・修了後の学生対応のために有益であることなどの説明周知を行った。

こうして提供を開始した「UTokyo Account 本人確認サービス」は、ユーザーが人手を介さずに本人確認を行える仕組みを提供するものであり、パスワードの初期化や多要素認証の再設定を迅速かつ効率的に行えるようになった。これにより、業務の省力化と処理時間の短縮、さらに学内の認証業務の質と利便性の向上が期待されている。

5　今後の展望

卒業・修了後の対応は卒業生施策においても同様に行われているため、UTokyo Account 本人確認サービスの卒業生事業における活用についても連携協議をおこなっている。今後は、本サービスと卒業生施策（卒業生アカウント）との連携を構築していく予定である。

UTokyo Account 本人確認サービスは提供を開始してまだ間もないため、想定していなかった問題が発生する可能性もある。しかし、サービスインして間もないにも関わらず、すでに、日本国外に設定された Google アカウント・Apple Account ではデジタル認証アプリをダウンロードできず、本サービスを利用できない事態が発生しており、対処を検討中である。さらにマイナンバーカードを取得した外国人に対して帰国時に返却を求めていることも判明し、留学生に対しては本機能で卒業後のサービス提供をすることが現状では困難であることが判明した。デジタル認証アプリの活用はまだ始まったばかりであり、マイナンバーカードの有効利用を進めるうえで検討していただける余地があると考えている。特に、日本の教育において国際通用性が求められていることを考えると、継続してデジタル庁へのフィードバックを行っていきたい。

マイナンバーカードを利用した本人確認機能を実装・検証して見えてきたのは、必ずしも全学的なアカウント UTokyo Account 自体と認証連携していることが必須ではないことである。現在の本学の情報システムは UTokyo Account でのみ認証して利用できるものとして展開してきた。しかし、デジタル認証アプリとマイナンバーカードを利用して提供される PPID と学内構成員情報を組み合わせることができれば、デジタル認証アプリのみで本学構成員の判別をすることが可能である。そのため、認証基盤との連携を実現しつつ、独自の認証基盤として UTokyo Account を補完するような機能を実現することができる。このような認証基盤としての活用を今後模索していきたい。

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.

[2] デジタル庁、デジタル認証アプリ、https://services.digital.go.jp/auth-and-sign/ （参照 2025 年 9 月 26 日）

[3] デジタル庁、デジタル認証アプリ　行政機関等・民間事業者向け実装ガイドライン、https://developers.digital.go.jp/documents/auth-and-sign/implement-guideline/ （参照 2025 年 9 月 26 日）

[4] OpenID Foundation、OpenID Certification – Certified Implementations、https://openid.net/certification/ （参照 2025 年 9 月 26 日）

[5] OpenID Foundation、Conformance Testing for OpenID Connect RPs、https://openid.net/certification/connect_rp_testing/ （参照 2025 年 9 月 26 日）

[6] デジタル庁、デジタル認証アプリ　テストカード代替機能、https://developers.digital.go.jp/documents/auth-and-sign/testcard_alternative/ （参照 2025 年 9 月 26 日）

[7] Microsoft、authenticationMethod: resetPassword、https://learn.microsoft.com/ja-jp/graph/api/authenticationmethod-resetpassword （参照 2025 年 9 月 26 日）

[8] Microsoft、Create temporaryAccessPassMethod、https://learn.microsoft.com/en-us/graph/api/authentication-post-temporaryaccesspassmethods （参照 2025 年 9 月 26 日）
[9] utelecon project、UTokyo Account 本人確認サービス、https://utelecon.adm.u-tokyo.ac.jp/utokyo_account/ident-myna/ （参照 2025 年 9 月 26 日）