

東京大学への多要素認証導入

玉造 潤史¹⁾²⁾, 竹内 朗¹⁾, 中村 誠¹⁾, 加藤 淳¹⁾, 竹内 利圭¹⁾, 本城 剛毅²⁾

1) 東京大学情報システム本部

2) 東京大学大学院理学系研究科

dics-shien.adm@gs.mail.u-tokyo.ac.jp

Introducing Multi Factor Authentication to the University of Tokyo

Junji Tamatsukuri¹⁾²⁾, Akira Takeuchi¹⁾, Makoto Nakamura¹⁾, Jun Kato¹⁾, Rika Takeuchi¹⁾, Goki Honjo²⁾

1) Division for Information and Communications Systems, the University of Tokyo.

2) Graduate School of Science, the University of Tokyo.

概要

東京大学の統合認証アカウントである UTokyo Account に対して多要素認証を導入した事例について報告する。UTokyo Account 認証基盤における多要素認証の実装と合わせて導入に必要とする各機能について示すとともに、利用者への展開の具体的な手順と成果について共有する。本施策における知見が多く的高等教育機関の IT ガバナンスの確立と IT リテラシの確保において有益であり、社会的な情勢を受け全ての機関において必須化を進める必要があることである。その確立が多要素認証導入のためだけでなく、高等教育機関において重要であることについて述べる。

1 はじめに

2020 年までの大学における情報システム整備はコロナ禍でのオンライン化に備えた準備のためのようなもので、その後の急速なオンライン活用と DX の進行とは明らかに異なっている。それまでは、大学の戦略によって進めてきた統合認証基盤整備とアカウント提供は苦難の連続で連携するサービスとの連携も一つ一つ行い、管理者と利用者に認証連携の利便性と安全性の理解を徐々に作りつつ利用を進めるものであった。ところが、オンライン授業に向けて、社会がロックアウトされていく中でも、その事前の蓄積が大学の活動を止めることなく、コミュニケーションを対面からオンラインへと切り替え、教室からクラウドサービスの活用へと切り替えを実現していった。この切り替わりはこれまで苦難の連続であった大学全体での統合認証サービスの重要性を明確にし、現状でも大学アカウントなしには業務は何も行えないような状況となった。

このような大学アカウントの重要性は安全性に対するリスクも露見させつつある状況にあ

る。大学はその特性上、直接的な雇用者である教員および教職員に加え、学生という一般企業においては顧客に分類される対象者を構成員として内包する組織である。さらに、社会連携、産学連携の観点から多くの関係者、そして名誉教授等の永続性のある関係者を大学内に受け入れることで全体として大きな活動をし、成果をあげている状況にある。これら非常に広範な構成員が利用する大学アカウントを安全に利用されている状態とし、セキュリティ維持を実現する困難度は非常に高い。ある程度のセキュリティ施策を実施しておいても組織的なセキュリティホールの残存を消すことは難しく、熊本県立大学の情報漏洩事件[2]などのセキュリティインシデントが発生していることも事実である。

東京大学では、これらの状況を踏まえて全学認証アカウントである UTokyo Account において多要素認証を導入することとした。本稿ではその準備と運用を含めて構成している。その内容の多くは他機関においても有効なものであろうと考え、その観点での記述に重点をおいて書いている。

そして、あらかじめ記載しておくが本学に

における多要素認証導入の取り組みは未だ中途であり、今後も続く取り組みであると考えている。しかし本稿を書くに至ったのは、多要素認証導入というセキュリティ対策の本当の意味は情報システム利用者のリテラシーとしてその対策が確立したときであり、それは本学のみならず、全ての高等教育機関におけるすべての構成員が、アカウント安全確保のため多要素認証を実施することが当然のこととなり、それが社会に受け入れられた状態となることによってようやく達成されるものであると考えるからである。本学においても他機関と関連する多くの非常勤講師等を介して他大学における情報リテラシー向上の困難度を認識した。単一の大学でひとつのアカウントに多くの苦勞をかけこの認識を共有することが本稿の真の目的である。

2 他大学で多要素認証導入の取り組み

2015 年頃から認証技術としての活用が始まっており、各大学では Google Workspace や Microsoft 365 サービスと合わせて提供されている多要素認証機能を活用している状況にある。当初の導入はそれぞれのサービス利用に合わせて利用されている状況にある。

大学における統合認証基盤の整備も進んでおり、現在は、大学の統合認証基盤で多要素認

証を全学的に導入することにおける技術的な問題点は解決していると考えられる。国内の認証連携サービスである学認においても高いレベルの認証要求 AAL2 を求めるサービスに応える連携体制を作っているところである。

ところが、大学構成員全体（学生・教職員の全て）に明確に多要素認証の設定を求めている高等教育機関は非常に少ない。現時点で確認できるのは広島大学、立命館大学、茨城大学[1]など一部の大学だけであり、従前から統合認証に多要素認証を取り入れていた佐賀大学、岡山大学、金沢大学などの大学が実現できているに過ぎない。多くの大学は学生に対しては多要素認証を求めることが出来ているが、特に教員に向けて必須化できていない状況にある。

このような状況は、大学という多様性を重んじる組織における IT ガバナンス確立の困難さと IT リテラシー向上実現の困難さを示していると言える。

3 UTokyo Account

UTokyo Account は本学の統合アカウントである。ID は個人ごとに割り当てられた番号（共通 ID）であり、認証レムルとして@utac.utokyo.ac.jp を付加して利用している。共通 ID は一人に一つ割り当てられ、学生・教職員それ

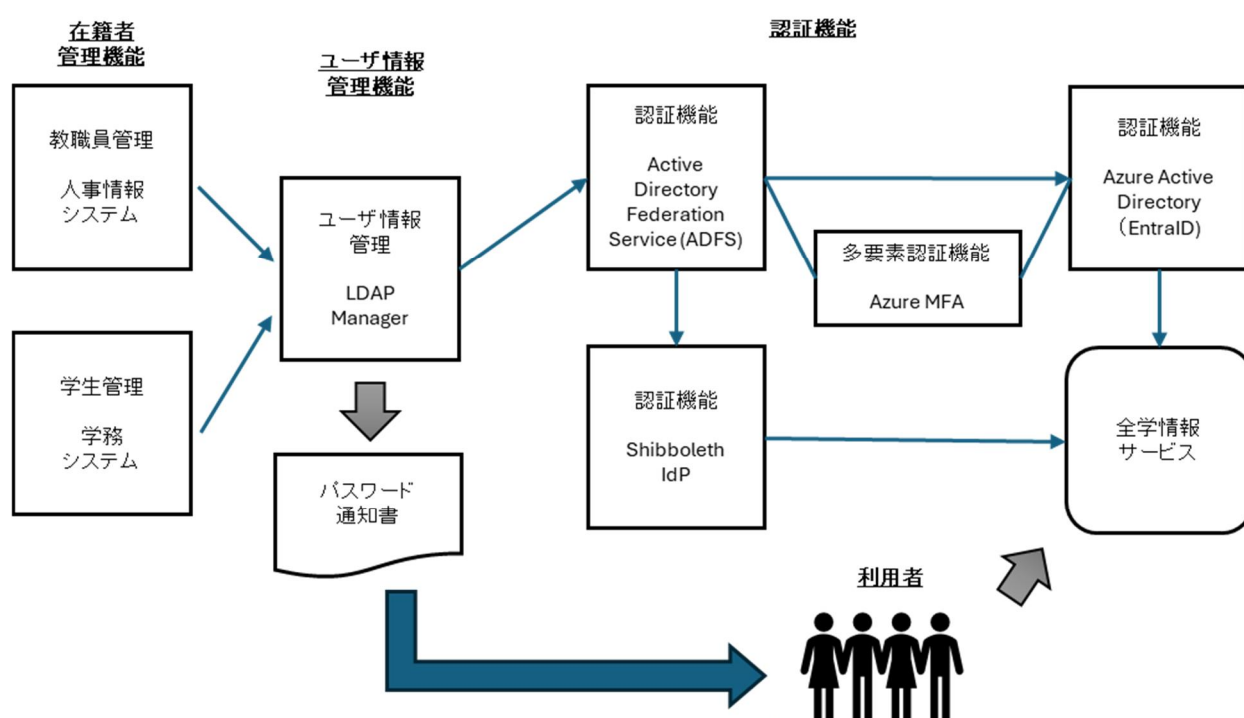


図 1 UTokyo Account 認証基盤の概要

それぞれの身分において在籍している間、全学的に提供されているシステムが関連付けられ利用できる。令和 6 年度より、共通 ID は一元化され大学に在籍している間、一つの共通 ID に関連づいたアカウントとして利用できるよう提供されている。UTokyo Account のパスワードは定期的に更新しなければならないものとなっている。(後述するが、多要素認証の導入によりパスワードの運用ポリシーも見直すこととした。)

UTokyo Account は大学に在籍する者に対して提供され、在籍者管理システムに登録されると自動的にアカウント登録がなされる。在籍手続きをする部署が UTokyo Account の部局担当者を担っており、在籍手続きの翌日以降に利用者にパスワード通知書を交付する。利用者は、初めに認証基盤が提供する利用者メニューにおいてアカウントの初期設定(パスワード更新)をしなければ利用を開始できないアカウントとして実装されている。パスワードの更新は基本的に 365 日ごとに行うこととして運用している。

UTokyo Account を用いた大学全体へのサービス提供は 2020 年春から utelecon プロジェクトのウェブサイト(情報システムの総合情報サイト@東京大学)で行われており、サポートも utelecon サイトを入り口として行われている。

4 多要素認証機構の実装

東京大学の UTokyo Account 認証基盤はユーザ情報を管理する LDAP Manager と、認証情報を管理する Microsoft 系の認証サービスと Shibboleth IdP を連携させて構成している。Microsoft 系の認証サービスはオンプレ型の Active Directory Federation Service (AD FS) とクラウドサービスの Azure Active Directory (現 Entra ID) を連携し、当初からある Shibboleth IdP を中心とした SAML 認証基盤として 2016 年から運営してきた。導入当初は、Active Directory の多要素認証はオンプレ型の MFA サーバにより実現されていたため 2016 年当初から MFA サーバがクラウド基盤上に用意していた。(管理上の利用のみでユーザへの提供には至らなかった。)

UTokyo Account は、教職員の情報は人事

(人事情報システム)より、学生は学務システム(本学の学務システムは UTAS (UTokyo Academic Affair System) と命名されている)より提供される在籍者情報に基づいて作成し、提供している。そのため、アカウントに関連した業務は、UTokyo Account 部局担当者が行っており、教職員については人事系の、学生については学務系の業務として実現されている。これはアカウントパスワードを紛失(分からなくなってしまった場合など)の再発行などに本人を確認して行う手続きの担当として実現されている。多要素認証の運用もこれらの UTokyo Account の運用状況を踏まえて実現する必要があった。

4.1 多要素認証の提供準備

2020 年以前から UTokyo Account の認証アカウントとしての利用率は非常に高い状況にあった。しかし、2020 年時点で SSO (Single Sign On) によって利用できるサービスは多くなかった。これは、当初、SSO の運用体制を効率的に運用するため、Shibboleth IdP による認証を主たる認証方法として統一的に展開していたことで、対応するサービスがそれほど多くならなかったためである。しかし、コロナ禍によりオンラインでの業務要求は高くなり、短期間で多くのサービス導入に対応する必要が生じ、認証連携をより容易でかつ安全に進める必要が出てきた。コミュニケーションを実現する Zoom、Webex、Slack 等の多くのクラウドサービスとの認証連携は既に定型化されており認証基盤の機能にビルトインされている状況にある。本学でも、従前から UTokyo Account 認証基盤で連携して利用できるようになっていた Azure Active Directory (AAD) による認証連携の活用をこれらのサービス導入に合わせて進めることとした。結果として、SSO を実現する認証基盤を柔軟に利用できるようになり、コミュニケーションサービスを中心に SSO による安全なシステム導入を実現することができた。

2021 年に入り、主たる認証サービスとして利用している AD FS サーバのバージョンアップが必要となる状況となり、その際に AAD を中心とした認証基盤へと構成を変更した。この変更により認証画面を AAD のものへと切り替え

ることを想定して準備していたが、急速に展開したオンライン化の根幹であるサインイン画面が切り替わることに對して慎重な判断があり、併せて用意した多要素認証のみを展開することとした。

多要素認証を実現する認証サービスとして Azure MFA を用い、サービスとして利用できる全ての認証方法を利用できるように構築している。導入後も Azure MFA の認証方法は徐々に拡充されており、それらについて検証しながら徐々に追加して提供している。

2024 年 10 月時点で利用できる認証方法は以下のとおりである。

- パスワードレス認証が可能な方式
 - セキュリティキー（パスキー）
 - Microsoft Authenticator
- パスワード認証と併用する方式
 - TOTP（ハードウェアトークン、認証アプリケーション（Google Authenticator））
 - 電話（SMS、音声電話：利用者に通話料金が発生しない（海外ローミング時などを除く））

現状では、FIDO2 セキュリティキーやパスキーなどのより高度な安全性をもった認証方法が利用可能であるが、特にこれらを義務付けるようなアクションは採っていない。

導入にあたっては慎重な意見も多かったため、Microsoft 認証サービスを用いた SSO と多要素認証の実証実験を 2021 年春から情報基盤センターを中心とした取り組みである「どこでもキャンパスプロジェクト」において検証した。その結果から、一般のユーザが問題なく利用できることが確認でき、提供されている認証方式をすべて提供することとした。

多要素認証の認証サービスへの適用は本学が全学的に導入している Microsoft 365 A3 ライセンスに含まれる Azure Active Directory Premium1（AADP1）を用いて行っている。AADP1 には条件付きアクセスという、サインイン時の複雑な制御を可能とする機能が含まれており、本学で利用するクラウドサービスに条件付きアクセスを用いることで、サインイン時に多要素認証を必須としたり、設定を要求した

りする制御を実現した。（5.3 節で後述するが本機能を用いてトラブルシューティングを可能としている）

5 多要素認証の運用準備

2021 年 9 月の多要素運用の提供開始に向けて、アカウント周りの説明や利用できる多要素認証方法の説明、多要素認証の認証方法が用意できない場合への対応、トラブル時の対応方法などの準備を行った。

5.1 多要素認証利用方法の準備

アカウント利用者の多要素認証設定を促すため、utelecon サイト上にアカウント初期化から多要素認証を設定するまでの一連の手順を作成した。

作成にあたっては学生サポーターの担当と協力して行い、多要素認証の設定手順の確立を多数のテストアカウントを用いて行い夏休み期間 2 か月を要して検証、実装を行った。サイトのコンテンツは 2021 年 9 月に公開したが、その後も鋭意更新している。

5.2 認証方法の準備

本学で利用する認証方法の多くは、電話機能（スマートフォンに限らず）を必要としている。本学で導入している認証方法の利用においては、利用者個人の電話を利用できることを前提としている。これは、利用者の利便性（特別に追加デバイス等を持ち歩く必要がない）を考慮のことである。個人の所有物を大学業務に利用することについての是非は議論がある点である。本学においても準備にあたって担当者レベルで議論したが、必ずしも個人の所有物のみで実現しないという方針とすることで大きな問題となっていない。

従前から、学内には携帯電話（大学の集中契約による安価な契約での通話サービス。端末は俗にガラケーと呼ばれるタイプのもの）も利用できるが、受け入れ時の契約や本人の意向により必ずしも利用できるとは限らない。そのため、多要素認証の展開にあたり、どうしても認証方法のための電話等を用意できない場合のため、TOTP によるハードウェアトークンの貸し出し体制を整備した。

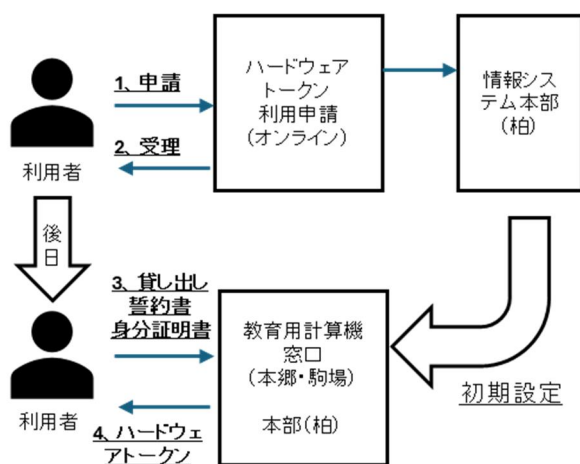


図 2 ハードウェアトークン貸し出しフロー

導入に当たっては、多要素認証がデジタル的な施策であることを踏まえ極力手続きは DX 化し、本質的に必要な本人確認のみを現場の各窓口で行って貸し出すこととして実装している。

事前に本郷・駒場・柏の各キャンパスにある情報システムを担当する部署の窓口ハードウェアトークンを用意しておき、貸与前に本部担当と窓口担当がオンラインコミュニケーションで連絡を取り合いながら初期設定を行い、窓口で本人確認を行って貸し出しを行うこととしている。(図 2)

5.3 多要素認証再設定方法の実装

多要素認証導入をした場合に生じる最も困難な問題は、利用者が多要素認証の認証手段を失った場合にサインインできないというトラブルから復旧する方法を準備することである。このような状況は、認証方法を設定したスマートフォンの機種変更や紛失、不用意な認証アプリケーションの削除などで多要素認証ができなくなる場面などで往々にして発生する。これらの状況からの復旧を困難とするのは、本人の認証方法を失っており、サインインが不可能となってしまうため、本人を機械的に確認し復旧する方法を作ることができない状況だからである。復旧に当たってはどうしても本人確認が必要であり、電子的な情報による本人確認 (eKYC: electric Known Your Customer) などの実装が必要となる。

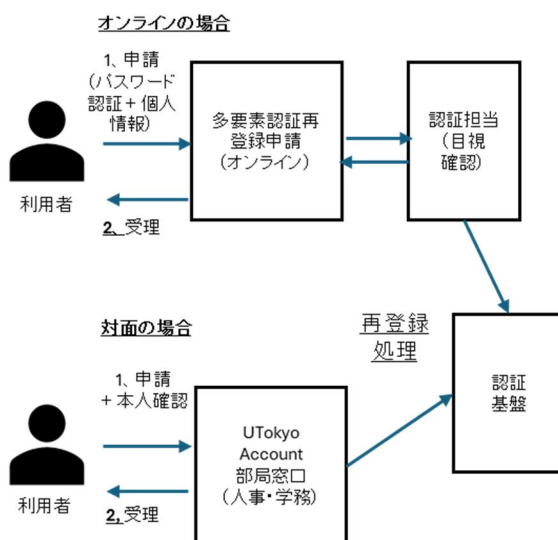


図 3 多要素認証の再登録フロー

本学では本人確認方法として、前述の条件付きアクセスを用い、パスワードによるサインインと本人しか知りえない情報を提示させることで、多要素認証の再登録を受け付けるサービスを構築した。(図 3)

利用者は、万一、本人が認証方法を失っても、このサービスを用いることでオンライン再登録でき、不可能な場合には在籍登録をした窓口において本人確認をしたうえで再登録を申請することが出来るようになっている

6 多要素認証の展開

これらの準備を行ったうえで、2021 年 9 月から多要素認証の提供を開始した。提供を開始しても大きくは広まらず、新規ユーザの初期設定時とセキュリティ対策に特に認識のあるユーザによる利用に留まる状況であった。

当然のことであるが、セキュリティ施策として追加の手順を要することになるため、適切な理解がなければ“単に不便なだけ”の機能としてみなされることが再認識された。

多要素認証の利用を広めるための取り組みを進める取り組みとして、2021 年秋から、utelecon プロジェクトが全学構成員向けに毎学期実施している説明会で利用方法と必要性を定常的なコンテンツとして提供した。また、2022 年度以降導入した新規のサービスである UTokyo VPN (全学的な VPN サービス) および UTokyo Slack において、利用時には設定と利

用を必須とした。しかし、これらの取り組みをしても、利用者は大きく伸びなかった。これは、根本的には利用者の正しい理解と利用を合わせて実現するという方針のもと、全システムに対して強制的に設定必須化を行うような「破壊的な導入」をしなかったためである。

しかし、セキュリティ施策として必要である状況は社会的な不安定さを背景により高まっている状況であった。これらを踏まえ、全構成員に対して正しい理解と利用を実現する取り組みを行うこととした。

本学の全学展開の基本方針は、「組織管理体制の上位から順に必須化をしていく」ということとした。

6.1 教職員への多要素認証の展開

教職員への全体的な多要素認証必須化は2023年7月から年末まで実施された。期間中、構成員に対して、大学として多要素認証が必要であることの説明と、部局ごとの設定状況を学内向けウェブサイト上で提供した。さらに、多要素認証を有効化したユーザの UTokyo Account のパスワード有効期限を無期限とするようパスワードポリシーを変更し、多要素認証のメリットを提示した。加えて、多要素認証の設定状況を全部局の UTokyo Account 部局担当者に提供し、未設定者に対する対応を依頼した。期間中の科所長会議（全部局の部局長が出席しなければならない学内会議）において、アナウンス及び設定状況の共有を行い、各部局の設定状況を認識して頂くことに努めた。期間中に全学のサービスに先んじて科所長会議で使用している学内独自システムである「会議資料サイト」の多要素認証化を実施し、全ての管理職が多要素認証を利用する状態とした。

一般利用者に向けては、各部局に多要素認証の設定支援の必要性を確認し、求めに応じ設定が困難な教職員に向けた対面での設定支援を実施した。この対応は障害者への対応も含め行った。また、設定方法の説明会ビデオや解説を提供し、各部局内での展開の助けとした。

結果的に設定期間の最終段階では概ね設定できた状況とすることができた。

6.2 学生への多要素認証の展開

学生への展開は、教職員への展開に続き、

2024年1月から開始した。学生への展開に合わせ、2024年3月から全学無線 LAN サービスである UTokyo Wi-Fi の2024年度アカウント発行に多要素認証（と毎年受講が必須の情報セキュリティ教育の2024年度受講）を必須とした。2023年度に発行した Wi-Fi アカウントが失効する2024年5月からは多要素認証を設定した場合のみ UTokyo Wi-Fi が利用できるようになった。

これらの施策の結果、教職員、学生とも大多数が多要素認証を設定し利用することとなった。

学生への展開は、教職員の展開と異なり、大きな問題を伴うことなく実現することができ、結果として、2024年9月より多要素認証が必須であると全体的に説明される状態となっている。

2024年3月から Shibboleth IdP のバージョンアップに伴い認証サービスを AAD へと集中化し SSO による利便性をさらに向上させた。結果として、大学全構成員に対して多要素認証の必須化を実施することができた。

2024年10月時点での認証方法の登録状況は、認証アプリ（TOTP）3.6万件、電話（SMS、音声）3.6万件、Microsoft Authenticator 3.3万件となっており、物理的な FIDO セキュリティキーの利用などは少数（200件未満）にとどまっている。セキュリティ強度の向上にはスマートフォンなどでのパスキー機能の利便性実現などより高度な認証手段の充実が待たれるところである。

7 多要素認証導入の考察

多要素認証の導入は、組織的な情報セキュリティ施策として実施するものであり、安全管理上のリスク対応である。多要素認証の一番の効果が組織的なメリットにあることは言うまでもないが、多要素認証導入の過程においては、設定を行う個人に自らにおけるメリットの理解を適切に進めることが非常に重要であることが施策実施期間中に見えてきた。

セキュリティ対策における根本的な阻害要因はオレオレ詐欺などの犯罪被害と同じく、一

般論としての理解はあっても自らが当事者となりうることの自覚につながらないことにより対策が進まないことである。

このような各個人の認識改善は一朝一夕に進まない。そのため、継続的な意識改革が必要であることが明らかになった。これらについては、今後も継続的に対応していく予定である。

高等教育機関、特に研究大学において重要なことは雇用されている教職員や正規課程の学生といった大学の主たる構成員である者以外に、関連する研究者、非常勤講師、受け入れ学生、名誉教授など大学との関わり合いが薄く、大学の組織管理構成上に明確に組み込まれていないシステム利用者の割合が多いことである。

多要素認証の導入後の状況でも、定常的な大学構成員である雇用されている教職員、正規課程の学生の設定状況は高い状況にあるが、先に述べた大学との関わりが薄い者における設定率は低い状況が顕著にある。

これらの者へのユーザサポート状況を見ると多くの場合、他に主たる所属機関があり、その機関におけるセキュリティに関する認識形成が見えてくることがある。つまり、主たる所属機関が多要素認証など個人アカウント管理の重要性を求めない限りこれらの利用者におけるセキュリティ認識を変えることは難しいということである。本学における多要素認証導入における取組は当然本学の安全性確保のためであるが、この取り組みのように世界的に普遍に必要な対策においては社会全体が同様の共通認識を持つ状況にすることが必要であることが見えてきた。

本施策の完全な完了は、他の大学等を含めた全ての高等教育機関において多要素認証が当然のこととなり、全て高等教育機関構成員が設定してある状況に至ってなされるものと言える。

謝辞

多要素認証の導入及び展開に当たっては主導的な立場で東京大学前情報基盤センター長、現在は執行役・副学長（CISO）田浦健次朗先生には共に活動していただき、多大なるご協力、

ご指導いただきました。本学前理事・副学長の太田邦史先生には多要素認証の導入方針の決断および経営層へのアクションにご支援いただきました。本施策の実施では、利用者支援とサポートの多くは本学情報システム部情報戦略課、情報支援課の皆様にご助力いただきました。特に、情報支援課教育本郷・駒場チームの皆さんにはハードウェアトークン業務を、各部局の人事・学務業務で UTokyo Account の部局での運用を担当していただいている皆様とはアカウントの提供と利用時のトラブル対応を積極的に担っていただいています。

導入と日々の運営においては学生サポーター（コモンサポーター、utelecon サポーター）の諸氏に日々のサポートを鋭意行っていただきました。

さらに、高度な認証方法の導入に当たっては駒場キャンパスにおいて本学に学生に対しセキュリティキーの提供と理解への支援を行ってくださった Yubico 社および SCSK 社と関連する皆様に感謝いたします。

参考文献

- [1] 野口宏, 大瀧保広, 山本一幸, 西原忠史, 外岡秀行, レベル分けによる多要素認証の要否の実現と認証連携の拡張、学術情報処理研究 /24 巻 1 号, 2020
https://doi.org/10.24669/jacn.24.1_78
- [2] 熊本県立大学メールアドレスの不正利用事案について、2022.12.13.
<https://www.pu-kumamoto.ac.jp/news/post-23585/>