Vol.2022-IOT-58 No.10
2022/7/12

統合認証基盤としての IDaaS 導入と初期運用

三島和宏[†1]　根本貴弘[†1]　青山茂義[†1]

概要：東京農工大学（以降、本学）では、約 5 年ごとに教育系計算機システム（現：学術情報基盤システム）の更新を行っている。このシステムには、教育用計算機システムのほか、プリンティングシステム、図書館システム、さらには認証基盤システムまで含まれる幅広いものとなっている。本学の認証基盤として 2016 年更新のシステムでは認証サーバや ID 管理システムなどをプライベートクラウドでの運用に切り替えを行った。このシステムが 2021 年に更新を迎えるタイミングとなるのに合わせ、本学では新たな認証基盤のために従来のプライベートクラウドではあるがオンプレミスに類似されるシステムからクラウドでの認証・ID 管理基盤である IDaaS への移行を検討した。これに基づき、2021 年のシステム更新では、認証機能と ID 管理機能の一部として IDaaS を導入し、学内の人物情報源との統合と IDaaS でカバーできない ID 管理機能を持つ情報源システム（申請管理システム）と連携する形でシステムの運用を開始した。本システムでは、これまで本学で運用していなかったシングルサインオンや多要素認証なども運用を開始する。IDaaS と周辺システムの導入と初期段階での運用についてまとめ、これらについて報告する。

キーワード：統合認証，IDaaS，シングルサインオン（SSO），学術情報基盤システム

Implementation and Initial Operation of IDaaS as Campus-wide Integrated Authentication Infrastructure

KAZUHIRO MISHIMA[†1]　TAKAHIRO NEMOTO[†1]
SHIGEYOSHI AOYAMA[†1]

Abstract: Tokyo University of Agriculture and Technology (TUAT) replaces our educational computer system (now the Academic Information Infrastructure System) every five years. This system has a wide range of components, including not only the educational computer system, but also the printing system, library system, and even the authentication infrastructure system. The system was replaced in 2016 as the authentication infrastructure for our university, and the authentication servers and ID management system were shifted to a private cloud environment. As this system was due for renewal in 2021, we considered migrating to IDaaS, an authentication and ID management infrastructure in the cloud, from a conventional private cloud system similar to an on-premise system, for a new authentication infrastructure. Based on this, in the 2021 system renewal, IDaaS was introduced as part of the authentication and ID management functions, and the system began operating in a manner that integrates with the university's person information sources and works with the information source system (application management system), which has ID management functions not covered by IDaaS. We summarize the introduction of IDaaS and other systems and their operation in the initial stage, and report on the results of these operations.

Keywords: Integrated Authentication Infrastructure, IDaaS, SSO, Academic Information System

1. はじめに

多くの大学では、それぞれで運用する各種情報システムの認証基盤として統合認証基盤を運用している。統合認証基盤には、ID 情報を管理するための ID 管理機能とアカウントの認証を司る認証機能の 2 つの機能がある。ID 管理機能では、人物に関する情報を連携させ、必要となるアカウントの生成を行う。認証機能では、作成されたアカウントに対して認証を行うために必要な各種機能を提供する。これにより、大学における人物情報と情報システム利用アカウントについてを統合的に管理することが可能となり、学生の入退学や教職員の採用・離退職にともなったアカウントライフサイクルを実現することができる。統合認証基盤を運用し、各情報システムが統合認証基盤と連携することにより、さまざまな情報システムを共通のアカウント・ID・パスワードで利用させることも可能となるため、ユーザにとって利便性を向上させることも可能である。

2. 本学における認証基盤周辺の変遷

本学では、人物情報を管理する仕組みが複数存在する。雇用関係をもつ教職員に関しては人事・給与システムがこれを担い、教職員が新規に採用されてから退職するまでの情報を持つこととなる。学生に関しては学務システムがこれを担う。大学では、雇用関係のある教職員や正規学生のみではないため、これら以外の人物情報も管理する必要がある。本学ではこれを管理するために統合基盤システムと呼ばれる仕組みが事務情報部門にて管理されている。本稿ではこれらシステムを「上位システム」と呼ぶ。

人物情報に関連する上位システムと連携し、情報システム向けのアカウント管理を行う仕組みは 2016 年の教育用

†1 東京農工大学 総合情報メディアセンター
Information Media Center, Tokyo University of Agriculture and Technology

電子計算機システム更新において本格的に整備された。それまでは、エクスジェン・ネットワークス社製の LDAP Manager[1]を通じてネットワーク利用のための認証アカウント（LDAP アカウント）を管理するために上位システムから得た情報を元にアカウントを管理する仕組みは存在していたが、これら以外の情報システムは独立的に運用され、アカウント自体も都度の申請に基づき生成していたため、本学として統一的にアカウントを管理運用する形とはなっていなかった。

2.1 2016 年教育用電子計算機システム更新に伴うアカウント管理システムの実現と申請管理システム“Salut”

2016 年に更新をした教育用電子計算機システムでは、それまで本学が課題としていた

- アカウントの統合管理
- 情報サービスの利用管理

という 2 点についてそれまでの半自動（多くが手動）となっていた処理の自動化を図り、運用としてのコスト低減を図ることで認証に関する基盤の抜本的な刷新を図った[2]。これには、認証システムの更新と情報システムの認証統合、上位システムから得た人物情報に基づいたアカウントの生成、人物情報に基づくサービスの自動提供、利用者の希望によるサービス提供を行うための申請管理の各機能を持たせることとなった。

この更新では申請管理システム“Salut”というサービスを軸として機能の実現を図った。申請管理システムはその名前の通り元はユーザからの利用申請を受け付け、必要なサービスを有効化し、ユーザに対して当該サービスを提供する一連の処理を自動化するためのものであり、実際に教職員用メールサービス、Web ホスティングサービス、ネットワーク接続関連サービス（IP アドレス割当・MAC 認証登録等）といったサービスをユーザが自ら登録し、利用できるようにする仕組みとなっている。

申請管理システムには、上述したサービス管理機能以外に、一般的な ID 管理システムの持つ機能も有している。上位システムから人物情報の連携を受け、これに対して必要な処理を行い ID 情報の追加・変更・削除を行うことができる。この人物情報の連携に際しては、もともと、総合情報メディアセンターが管理するシステムの前段に事務情報部門が管理する統合基盤システムが存在する。しかし、ここでは情報サービスの管理に関する視点が十分ではないことから、学生に関する基礎情報は学務システム、教職員に関する基礎情報は人事システムから、統合基盤システムを経由して、メディアセンターでは申請管理システムにて人物情報の連携を受け、これに基づいてアカウント発行・削除等を行い、下位の情報システムに対して情報連携を図る。この連携については図 1 に概要を示す。また、当該の人物情報に基づいて、どのような情報サービスの利用を可能とするかの判定も行い、人に応じたサービス提供を行えるようになっている（たとえば、教員・職員・学生での提供可能サービスの違いを意識したサービス提供等）。下位の情報システムの連携については従来システムからの引き続きで LDAP Manager を通じて連携を行うようにした。この際、さまざまなクラウドサービスの提供も開始したため、これらへの連携のために LDAP Manager のプラグインと連携のためのサーバを構築し、これらを通じてクラウドサービスへのプロビジョニングも実施されることとなった。

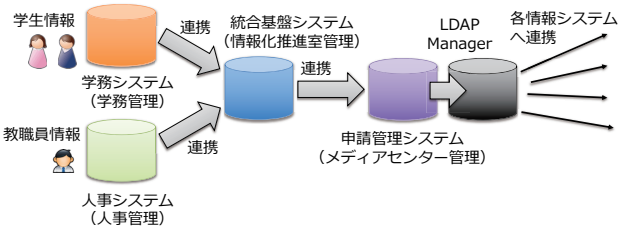

図 1　学生・教職員情報の連携

3. 2021 年学術情報基盤システム更新に合わせた統合認証基盤システムとしての IDaaS の導入

2021 年に従来の教育用電子計算機システムの更新が行われた。この際より、全体システムの名称が学術情報基盤システムと改められ、より大学としての情報基盤であることを意識したものとなった。2016 年更新において導入された申請管理システムを軸とする認証関連基盤は 2021 年更新においても重要な機能として維持された。ここでは、従来の方式での認証基盤を維持するか、新たな基盤としてクラウドをベースとした IDaaS 導入の検討が行われた。

本学では、2016 年更新に向けた検討の際に各種クラウドサービスを導入する検討を行っていたことから、認証管理・ID 管理基盤についても LDAP Manager を単純に継続するのではなく、IDaaS を導入することができないか検討を行っていた。2014 年の段階でいくつかの IDaaS を導入検討を行ったのだが、まだ日本において安心して利用できるか判断が難しかったり、価格の面において導入が困難そうであったり、といった状況があり実際の導入には至らなかった。

3.1 IDaaS

IDaaS とは、Identity as a Service の略称であり、SaaS・PaaS・IaaS などと同様にクラウド上で機能実現を図るものである。IDaaS は特に ID 機能についてをクラウドで実現するものであり、ID 管理機能、オンプレミスの認証サーバに対するプロビジョニング、クラウドに対するアカウントプロビジョニング、SAML2.0[3] や OpenID Connect[4]（OpenIDC）などのプロトコルによるフェデレーション認証機能と同様のプロトコルを利用したサービス間でのシングルサインオン機能の提供をクラウド上で展開する。

従来、認証は組織内にオンプレミスとして認証サーバ(たとえば LDAP や Active Directory などのディレクトリサーバ）を置き、オンプレミスの情報サービスがこれを参照し ID とパスワードで認証を行うということが行われるものが一般的であったが、さまざまな情報サービスのクラウド化が進むにつれて、オンプレミスの認証サーバだけでは対応が困難となり、認証情報をクラウド側へ連携させるエージェントを導入したり（Microsoft365 のクラウド ID 方式としての DirectorySync など）、フェデレーション認証機能を用いて認証連携を図ったり、などが必要となってきた。IDaaS ではこのようなクラウド時代の認証を得意とする仕組みであり、新たな認証基盤として利用が進んでいる。

主な IDaaS サービス提供事業者としては、Okta や OneLogin などが挙げられる。また、Microsoft365 のプレミアム機能として提供される Azure Active Directory も IDaaS の一種であると言える。いずれのサービスにも共通するのは、先述した ID 管理機能と認証管理機能をクラウド上で提供するものである。

3.2 IDaaS と人物情報連携

IDaaS では基礎となる人物情報を管理する機能はそこまで高機能なものではなく、すでにあるアカウント情報をディレクトリ連携によって連携させ、そこに各利用者がどのサービスが利用できるかの情報を管理者が付加する、もしくは、ある属性情報に基づき動的に判断し自動付加することで、必要となるサービスに対するプロビジョニングを行うものとなっている。このため、すでに Active Directory などのベースとなるディレクトリが整っている環境が多くの場合必要となる。IDaaS はクラウド上のサービスではあるが、このディレクトリとの連携については連携サーバやディレクトリ上に連携エージェントを導入することでクラウド上と必要な情報の連携が図られる。

このように IDaaS は人物情報のような基礎情報の管理より後段の管理が得意なシステムであるとも言える。このため、本学が必要とする上位システムからの人物情報の連携をしなければならないという点においては、IDaaS のみで必要な機能を満たすことはできない。

3.3 本学における IDaaS 導入と申請管理システムの統合的連携

2016 年と比較すると安定的に利用可能な IDaaS サービスは数多く提供されるようになった。本学ではさまざまな IDaaS サービスの中から、エクスジェン・ネットワークス社製の Extic[5]をそのサービスとして選択し、2021 年更新において統合認証基盤として導入し、これまで利用していた LDAP Manager は利用しないものとした。

Extic では、他の IDaaS サービスと同様にクラウドに対するフェデレーション認証機能、シングルサインオン機能、アカウントプロビジョニング機能、ID 管理機能を有している。また、Extic の特徴的な機能として、それ単体で Shibboleth IdP と同等の機能が利用可能であり、学認向けの Shibboleth サーバを構築運用する必要がなくなる。Shibboleth サーバは定期的なアップデート対応が必要となり、この対応が不要となるのは運用コスト低減に効果があると考えている。

しかし、アカウントプロビジョニング機能や ID 管理機能に関する部分は他の IDaaS サービスと比較すると機能が豊富であるとはいえない。しかし、ID 管理機能に関しての多くは本学では申請管理システムがこの機能を担うことが可能となっている（これまで本学では LDAP Manager の ID 管理機能の多くを利用せず、申請管理システムに必要な機能を担わせていた)。本学では、従来からの申請管理システムと Extic の組み合わせにおいて ID 管理・認証管理を実現し、認証に対しても IDaaS としてのメリットを享受する。

連携の概要については図 1 で示した LDAP Manager が Extic に置き換わった形となる。これを詳細に示し、人物情報の連携、アカウント情報の連携、各利用者との関係についてまとめたものを図 2 に示す。

申請管理システムは、上位システムである人事・給与システム、学務システム、統合基盤システムからの情報を受け、必要な情報の処理を行い、IDaaS である Extic に情報連携を行う。この際、人物情報に基づきどのサービスを誰に提供するかについてはすべて申請管理システムの持つデータベース上で情報を保持し、この管理についても申請管理システムが担う。申請管理システムからの連携を受けた Extic では、本学が利用する Google Workspace for Education や Microsoft365 Education の各サービスに対するアカウントプロビジョニング、オンプレミスの認証サーバ（LDAP・Active Directory）へのディレクトリプロビジョニング、各種学内システムに対してコマンド実行によるプロビジョニング処理などを行う。また、フェデレーション認証機能として、Google サービスと Microsoft サービスに対する SAML による認証連携、学認連携、その他学内情報システムに対する SAML による認証連携をそれぞれ行い、必要な認証処理も IdP として認証機能を担う。Extic では OpenIDC によるフェデレーション認証も可能となっているが、現時点で本学では OpenIDC に対応したシステムが存在しないため、機能は利用していない。また、Extic は FIDO によるパスワードレス認証に対応しているが、オプション機能となっており現時点では利用していない。今後、パスワードレス認証については必要性が向上してくると考えており、利用する可能性もあるとは考えている。

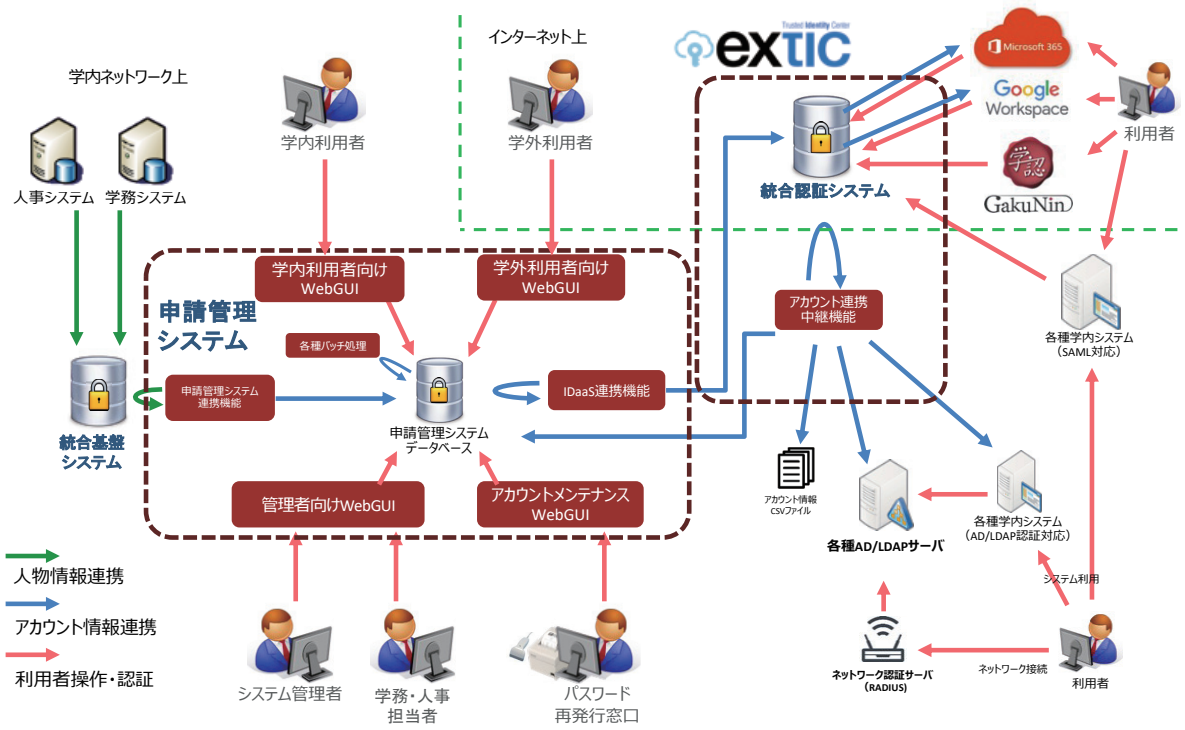

図 2　申請管理システムと Extic による情報連携と認証連携

3.4 IDaaS 導入によるクラウドサービスアカウントプロビジョニングならびにアカウントライフサイクルの改善

文献[6]にて本学のコロナ禍におけるオンライン授業のための Web 会議ツールの短期導入に関して報告した。ここでは、短期導入であるがゆえのシステム的な課題が山積していたが、2021 年更新に合わせて IDaaS による認証の統合と申請管理システムによるプロビジョニング機能により、これら課題の改善を図っている。

3.4.1 Zoom

更新以前の Zoom サービスでは、アカウントプロビジョニングは Zoom の持つ JIT プロビジョニングの機能を用いてユーザが最初に Zoom へアクセスした際に自動的にアカウントが生成される仕組みとなっていた。しかし、これではアカウントの追加のみ実施され、削除に関する処理が自動化されておらず、アカウントが存在しなくなった際に処理を考慮していないものとなっていた。今回の更新に合わせて、図 3 に示すように申請管理システムからアカウントプロビジョニングを行うようになり、人物情報の連携によってアカウントが存在しなくなった場合はアカウントの削除も含めた連携となった。ここでは Zoom の API による連携を行っている（Extic は Zoom のアカウントプロビジョニングに非対応）。また、ユーザ認証については SAML によるフェデレーション認証に対応し、Extic を通じてシングルサインオンが可能となっている。

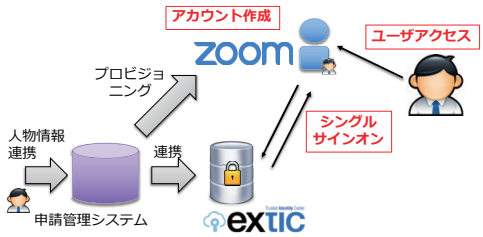

図 3　Zoom との連携

また、新規に作成されたユーザに対しては自動的に Zoom のアカウントプロビジョニングも行われるようになっている。しかし、以前からのユーザの中には本学のフェデレーション認証を行う際の ID である本学の Google サービスのメールアドレスを使って個人アカウントとして Zoom アカウントを保有しているユーザもおり、このユーザに対する混乱を避けるために、既存ユーザについてはユーザがアカウントリクエストを申請管理システムから行うとアカウントプロビジョニングを行うオプトイン方式の対応にもなっている。

3.4.2 Webex

更新以前の Webex サービスではアカウントプロビジョニングに係る機能実装がサービスインまでに準備できなかったため、Webex API を実装した Google App Script から手動でアカウントを作成するような仕組みとなっていた。今回の更新に合わせて、申請管理システム上の権限設定を変更することでアカウントプロビジョニングができるように

なった（図 4）。また、ユーザが申請管理システムを通じてアカウントリクエストができる機能も実装している。いずれも当該ユーザが存在しなくなった場合には Webex アカウントも削除される。これらは申請管理システム上に Webex の API による連携を実装している（Extic は Zoom のアカウントプロビジョニングに非対応）。

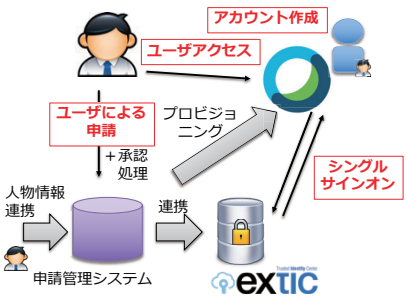

図 4　Webex との連携

3.4.3 Google Workspace（Enterprise ライセンス）

Google Workspace は、本学では Education Fundamentals を全学導入している。これに対して、有償版ライセンスである Teaching and Learning Upgrade や Education Plus などの対応も図っている。更新以前は Webex 同様手動で API を操作する Google App Script を用いていたが、更新以降は申請管理システム上にライセンスの付与を行う API 連携を実装している（図 5）。現時点ではライセンス購入を行っていないため当該機能は利用していないが、Google によるストレージポリシー変更の問題の渦中であり、今後この機能を利用する日が来る可能性が高まっていると言える。

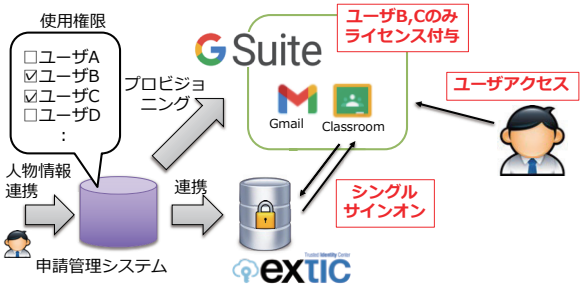

図 5　Google Workspace のライセンス連携

4.　IDaaS 導入における初期運用

4.1　ユーザ利用時の各種認証

4.1.1 キャンパスネットワーク接続（LDAP 認証）

本学では有線 LAN ならびに無線 LAN の接続に際して 802.1x 認証を導入している。この際に、RADIUS サーバを経由して LDAP サーバを認証サーバとして参照している。LDAP サーバへ連携する情報源が LDAP Manager から Extic の連携エージェントに変わったのみであり、ユーザの利用に際しては特に変更点はない。接続に際しては ID およびユーザのパスワードを要求する。

また、LDAP 認証のみで認証を行う Web サービスについても同様に特にサービス側での変更点はなく、ID およびユーザのパスワードが要求される。

4.1.2 各種クラウドサービス（SAML 認証）

各種クラウドサービスでは、SAML によるフェデレーション認証を行う。認証時には図 6 に示すような専用の認証画面が表示され、必要となる ID およびユーザのパスワードの入力が求められる。また、本学では順次多要素認証の必須化が行われており、必須化以降はこの画面のあとにワンタイムパスワードの入力が求められる。

図 6　フェデレーション認証時の認証画面

4.2　認証基盤の切替とシングルサインオン対応

認証基盤の切り替えに伴い、特にフェデレーション認証への切り替えを行うクラウドサービスでは、ユーザが認証をする際に表示される認証画面が大きく変化する。本学では、広く利用される Google Workspace、Microsoft365、Web 会議で利用される Zoom、Webex、申請管理システム自体、教職員向けメールとして利用する Google Workspace の別テナント、旧 LMS としての moodle が更新を機にフェデレーション認証へ移行した。

これらの切り替えに際しては、一定期間のアナウンス、利用者講習会を通じた周知活動を行った上で、切り替え日を分散し、問い合わせに対する対応体制の強化等を行った。特に、メールサービスと密接に関係のある Google Workspace や Microsoft365 については、従来型の認証から先進認証（OAuth2 認証）への切り替えも同時に発生することからより一層の周知が必要であった。

実際の切り替え日は以下の通りであり、切り替え後はこれらサービス間のシングルサインオンが可能となっている。

- 申請管理システム：2021 年 10 月 22 日
- Zoom：2021 年 10 月 23 日
- 教職員用 m2 メール：2021 年 10 月 25 日
- Webex：2021 年 10 月 26 日
- Microsoft365：2021 年 10 月 26 日
- Google Workspace：2021 年 10 月 27 日
- moodle：2021 年 10 月 28 日

また、学認についても旧 Shibboleth サーバから Extic へ変更となり、認証画面も図 6 に示す画面に一部学認用のオプションが追加される画面に変更となった。

4.3 多要素認証への対応

本学では総合的なセキュリティ対策の一環として、多くの大学同様に多要素認証への対応を進めている。この更新での認証基盤の切り替えに合わせて、多要素認証の必須化も計画され、実施に向けて取り組みが行われた。多要素認証を必須とするサービスとしては、Extic がカバーする範囲のすべてのフェデレーション認証、システムとして多要素認証が可能なクラウドサービスについて対象としている。

多要素認証必須化は、大学の行動計画として方針が本来決定されており、2022 年 12 月 15 日にすべてのユーザに対して実施する計画で必要な周知活動や取り組みを行ってきていた。しかし、学期途中での変更に伴い、各種情報システムへのアクセスが利用できなくなるユーザが発生するのではないかという懸念が学内委員会等で出た結果、大学としての判断として多要素認証の必須化は延期されることとなった。

しかし、すべてのユーザを安直に先延ばしにするのはセキュリティ対策として決して良いものとはいえないことから、周知やユーザ対応が届きやすいという判断で、非常勤講師ならびに学外者を除く教職員に関しては当初の予定通り必須化を実施する決定がなされた。これに基づき、当該ユーザについては Extic を通じて行われるフェデレーション認証に 2022 年 12 月 15 日から多要素認証が導入されている。

図 7　多要素認証画面（TOTP・MOTP）

多要素認証を求める画面では、TOTP をベースとしたアプリ（Google Authenticator など）を用いた認証（TOTP 認証）とメールでワンタイムパスワードを送信する認証（MOTP 認証）に対応しており、ユーザがどちらの認証にするかを認証画面で選択する形となる（図 7）。

5. まとめ

本論文では、2021 年に更新を行った学術情報基盤システムのうち、認証基盤にかかる内容について概説した。本更新に至るまでの本学の認証基盤の変遷と 2016 年更新における申請管理システムについてもまとめている。IDaaS というとクラウドサービスであり、何分にも多くのことががらっと変わってしまうのではないかという印象もあるかもしれないが、実際のところは従来の ID 管理システムであった LDAP Manager 時代と比較しても変わらない部分もある。しかしながら、当時にはなかった運用的な問題も少しずつ見えてきている状況である。すでに運用を開始し、新学期対応も含めて経過していることから、これらで見られた知見についても今後まとめていければと考えている。引き続き運用を継続し、そこでのさまざまな知見も新たに蓄積していきたい。

また、全学としての多要素認証必須化の取り組みが延期にはなったものの進んでいることから、この取り組みに置いて得られる知見も出てくると考えている。全学の認証基盤の多要素認証、その他サービスにおける多要素認証といくつかの種類はあるが、これらについても纏めていきたいと考えている。

謝辞　本学の認証基盤更新にあたっては大森浩氏をはじめとする株式会社 SRA 東北の皆様にいろいろとご対応いただきました。謹んで感謝の意を表します。

参考文献

[1]EXGEN NETWORKS: LDAP Manager, URL: https://www.exgen.co.jp/lm/ [web] (2022/06 参照)
[2]櫻田武嗣，三島和宏，石橋みゆき，萩原洋一：　管理運用システム「Salut」の概要，情報処理学会研究報告, IOT, [インターネットと運用技術] 2016-IOT-35(3), pp.1-6 (2016).
[3]S Cantor, J Kemp, R Philpott and E Maler, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0", Mar 2005. URL: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf [web] (2022/06 参照)
[4]N Sakimura, J Bradley, B de Medeiros and C Mortimore, OpenID Connect Core 1.0 incorporating errata set 1, Nov 2014. URL: http://openid.net/specs/openid-connect-core-10.html [web] (2022/06 参照)
[5]EXGEN NETWORKS: Extic, URL: https://www.exgen.co.jp/extic/ [web] (2022/06 参照)
[6]三島和宏，根本貴弘，辻澤隆彦，萩原洋一：オンライン授業展開に向けた Web 会議ツールのデプロイメント - 短期構築における理想と実際, IOT, [インターネットと運用技術] 2021-IOT-52(25), pp.1-7 (2021).