核融合研における IDaaS を用いた学認 IdP の構築

高山有道 [1),2),3)], 山本孝志 [2)]

1) 自然科学研究機構 核融合科学研究所 ヘリカル研究部
2) 自然科学研究機構 核融合科学研究所 情報通信システム部
3) 総合研究大学院大学 物理科学研究科 核融合科学専攻

takayama.arimichi@nifs.ac.jp

Deployment of GakuNin IdP based on IDaaS at NIFS

Arimichi Takayama[1),2),3)], Takashi Yamamoto[2)]

1) Department of Helical Plasma Research, National Institute for Fusion Science (NIFS), National Institutes of Natural Sciences (NINS)
2) Division of Information and Communication Systems, NIFS, NINS
3) Department of Fusion Science, Graduate University for Advanced Studies (SOKENDAI)

概要

核融合科学研究所では、Shibboleth IdP によるオンプレミスの学認 IdP からエクスジェンネットワークス社の Extic を用いた IDaaS 上の学認 IdP へ移行した。本作業は利用者側から見ると移行だが、設定・投入した情報はその多くが新規に用意したものであるため、提供側から見ると実質的には、オンプレミスでの経験を活かしつつ IDaaS 上に学認 IdP を新規構築したといえる。一連の活動の概要およびそれを通じて得られた知見を事例報告として紹介し、オンプレミスから IDaaS への移行を考えている方やこれから学認に加入し IDaaS によって学認 IdP を立ててみようと考えている方の参考に供したい。

1 はじめに

1.1 核融合科学研究所

大学共同利用機関法人自然科学研究機構核融合科学研究所 (核融合研) は核融合プラズマに関する学理、および、その応用の研究を目的として、国内外の大学や研究機関と共同研究を行っている機関である。また、総合研究大学院大学物理科学研究科を併設するとともに国内にある複数の大学の連携講座を有しており、所属学生に対する大学院教育も行っている。

内部構成員は 400 名強で、管理部、技術部、ヘリカル研究部、その他の部署に所属している。また、内部構成員のほかに国内外の大学および研究機関に所属する共同研究者が数千名存在し、各種サービスを提供している。

1.2 ユーザー認証を必要とするシステムと ID 管理

核融合研情報通信システム部で内部構成員向けに提供している主要なサービスのうち、ユーザー認証を必要とするものを表 1 に示す。

基本的に各システムごとに ID が管理され、ユーザー認証も各システムごとに行う構成となっている。システムを使用できるユーザーは当該システムに ID が登録されていることを前提としており、認可 (Authorization) の観点からは分かりやすいともいえるが、認証に必要なクレデンシャルは各システム毎に設定する必要があるためユーザーから見ると好ましい状況とは言えない。また、ユーザーの異動があった場合、システム毎に登録されている ID 情報を変更をする必要があるが、必ずしもすべてのシステムが即座に異動情報を反映できる状況にはなっていない。

これらは解決すべき課題として挙がっており段階的に取り組んでいるところであるが、これは別の機会に述べることにして、本稿では学認 IdP に焦点を絞って導入から現在までの状況を報告する。

2 学認 IdP の移行

2.1 Shibboleth IdP による学認 IdP

核融合研は 2017 年 8 月 16 日に学認運用フェデレーションへの参加が認められ、Shibboleth IdP を用いた学認 IdP を運用してきた。

学認技術ガイド[*1]など公式情報を参考に、CentOS7、Apache HTTP 2.4 Server + mod_ssl、Java 8 (OpenJDK)、Tomcat 7、Shibboleth IdP v3.1、OpenLDAP

[*1] https://www.gakunin.jp/technical

表 1　内部構成員向け主要サービス

サービス名	ID 管理・認証方法	多要素認証対応
Google Workspace[1]	Google Account	Yes
Microsoft 365	AzureAD	Yes
検疫認証システム [2]	OAuth2 (Google API)	Yes
サイボウズ	サイボウズ内蔵	No (パスワードのみ)
リモートアクセス	リモートアクセス装置内蔵	(クライアント証明書)
Eduroam	freeRADIUS + MySQL	No (パスワードのみ)
学認 (旧)	Shibboleth IdP + OpenLDAP	No (パスワードのみ)
学認 (新)	Extic	Yes

2.4 を用いて、最もシンプルな形態で構築した。

その後、Shibboleth IdP v3 系列で適宜更新を進め、Shibboleth IdP v4 への移行の際は v3 からの更新という形は取らず、CentOS7、Apache HTTP 2.4 Server + mod_ssl、Java 11 (OpenJDK)、Jetty 9.4、Shibboleth IdP v4.1、OpenLDAP 2.4 の構成で新規に構築した[*2]。

学認 IdP の導入と前後して、1.2 節で触れた課題を解決すべく ID 管理・ユーザー認証の統合化を検討しており、学認 IdP のユーザー ID 管理もその枠組みに含むことになるため、見通しがつくまでは情報通信システム部の少数の関係者のみを対象としたテスト運用と位置づけ、ユーザー情報の管理は OpenLDAP を直接たたくという形態を取っていた。

内部構成員全体への展開の上で、いかにして多要素認証へ対応するかも課題となった。2020 年の段階で、Shibboleth IdP への適用が可能かどうかは別として、内部構成員が使用可能な認証システムあるいは認証要素には Google API、Azure AD、YubiKey があった[*3]。これらを使ってなんとかできないかといろいろと試行錯誤してみたが、なかなかうまくいく解が見いだせない状況が続いていた。

また、Shibboleth IdP をオンプレミスで運用するにあたっては、各種ソフトウェアの脆弱性への対応がそれほど高くない頻度はとはいえ発生し、これが相応の負荷になっているという実感もあった。

そのような中、新型コロナウィルスの感染拡大によってテレワークが一般的となり、自宅から電子ジャーナルを閲覧したいという要望が強まってきた。

2021 年の秋、要望を実現するための手段として学認 IdP をきちんと整備すべし、という指示が研究所上層部よりなされ、予算も措置された。そこで、これまでの経験を踏まえ、オンプレミスでの運用からクラウドサービス (IDaaS) の利用に切り替えることにした。

2.2　Extic による学認 IdP への移行

前節で述べたような経緯から IDaaS を利用することになったため、まずは学認 IdP が利用できるようになることが至上命題であった。それに加えて、情報通信システム部としては、将来的に ID 管理・ユーザー認証の統合化が視野に入りうるサービスであることも要件として考慮しつつ、情報収集を進めた。

大学 ICT 推進協議会 2021 年度年次大会において、エクスジェンネットワークス社が提供する IDaaS である Extic (Exgen Trusted Identity Center) を知り、すぐに我々のニーズに適合していると直感した。

そこで、2022 年 2 月から 7 月にかけてエクスジェンネットワーク社とテレビ会議を行って課題を詰めつつ、試行環境を提供していただいて導入に向けた準備を進めた[*4]。

試行環境は学認 IdP 機能に対応していないこともあり、8 月にはライセンス数を小規模な試験に必要な数量に限定した形でエクスジェンネットワークス社と契約を結び、運用環境で学認 IdP としての動作確認を中心に構築作業を進めることにした。

■学認 IdP 開設のための事務手続き　2017 年夏より学認 IdP を運用してきており、テスト運用という位置づけとはいえ、直ちに廃止するというわけにはいかな

[*2] Shibboleth IdP v3.x からの更新としてインストールすることが推奨されていたが、この段階においてもテスト的な運用という位置づけにあり、ユーザーへの影響は僅少であることから新規構築を選択した。

[*3] 個人所有のスマートフォンは、所有率が高いとはいえ 100% ではないため代替手段を設ける必要がある。そのため、Google Workspace を導入する際に YubiKey を配布していた。

[*4] キックオフから次のステップに進むまでに半年が経過しているが、その間他の業務がいろいろ入ったため結果的にそのようになっただけであり、実働としては半月も要していない。

い面もあった。そこで、従来のものは名称を変更してユーザーの混乱を避けるようにしつつ、Extic による学認 IdP を新規設置として申請することにした。

申請は OpenIdP によるアカウントを使用し、新規 IdP 設置申請と変更申請を同時に web 申請システムから提出した。しかし、新規 IdP 設置申請には申請システムから申請したうえで、公印を押した書面を郵送する必要もある。研究所長を申請者とした申請書とするため管理部で事務処理を行う必要が生じ、手続き完了までには想定していた以上に時間を要した。

さらに、従来と同様のスコープを用いるつもりであったが、申請時に誤って entity ID に含まれるドメインをスコープとする申請としてしまった。そのため、核融合研の保有・管理するドメインではないスコープとしての申請として扱われ、エクスジェンネットワークス社の許諾書を提出する必要が生じたため、さらに余計な時間がかかってしまう事態を招いた。学認のスコープは自組織のドメイン名と一致させるのが一般的であるため、新規 IdP 設置申請が承認されたのち、直ちに正しいスコープへの変更を申請し、すぐに受理された。

なお、Extic を用いた学認 IdP の設置を申請する場合の注意点として、Extic の手順書に従ってテンプレート外メタデータを作成しアップロードする必要があることを挙げておく。

■SAML 署名および暗号化に使用する証明書　学認 IdP では SAML 署名および暗号化に使用する証明書が必要となる。Extic では UPKI 電子証明書発行サービス[*5]による証明書のみに対応している。そのため、Extic を使って学認 IdP を立てる場合、UPKI 電子証明書発行サービス利用機関であることが前提となる。核融合研は UPKI 電子証明書発行サービスの開始当初より利用機関であるため、この条件はクリアしていた。

UPKI 電子証明書の発行を依頼する場合、OpenSSL などを使用して鍵ペアおよび CSR を生成し、CSR から証明書発行申請 TSV ファイルを作成して申請するという流れになる。Extic の場合、鍵ペアおよび CSR の作成は Extic の学認 IdP 証明書新規作成機能を使用して行う必要がある。しかし、手順書をよく読まずに手元の PC で作成した鍵ペアおよび CSR を使用して UPKI 電子証明書の発行を受けてしまったため、証明書発行後すぐに失効手続きを行い、改めて Extic の学認 IdP 証明書新規作成機能を使用した正しい手順に従って UPKI 電子証明書を発行してもらうこととなってしまった。

学認 IdP で SAML 署名および暗号化に使用する証明書の主体者 DN は特に問われず、ST L、O の各項は自機関で決められた値を指定すればよい。CN は通常発行された証明書をインストールするウェブ・サーバの名前を FQDN を指定することになっている[*6]が、Extic の場合実体としてのホストが存在しない。一方、登録担当者が審査する項目の一つとして「FQDN が、サービスで申請したドメイン名を利用しており存在する FQDN であること」が挙げられている[*7]。そこで、核融合研に実在するサーバーに CNAME を付加することで実在する FQDN を生成し[*8]、その値を使用することで対処した。

■ユーザーアカウント情報の収集、加工、投入　Extic では Web ブラウザによる GUI から個別にユーザーを新規追加できるほか、CSV ファイルを用いてユーザーアカウント情報を一括して登録、変更、削除する機能が備わっている。数百人分のユーザー情報を GUI で個別に登録していくのは現実的ではないので、400 名弱のユーザー情報を CSV ファイル化して一括登録することにした。

Shibboleth IdP によるオンプレミスの学認 IdP はテスト運用の段階であったため、投入すべきユーザーアカウント情報は別途用意する必要があった。最もメンテナンスされているユーザー情報のソースとして、Google Workspace のユーザー情報として管理している Microsoft Excel ファイルがあり、この Excel ファイルの情報を加工して Extic 用の CSV ファイルを用意した。Excel ファイルから CSV ファイルへの加工には、属性値に基づく演算[*9]が必要だったため、初期投入するユーザー情報のためだけの使い捨ての Python

[*5] https://certs.nii.ac.jp/

[*6] UPKI 電子証明書発行サービス 支援システム操作手順書 2-1-1. 鍵ペア・CSR の作成

[*7] UPKI 電子証明書発行サービス サーバー証明書管理手順 1-1-4. サーバ証明書新規発行申請 TSV ファイルのアップロード

[*8] 誤ってサーバーの運用を廃止し実在しない FQDN になる危険性を回避することが目的。また、当該サーバー自身に対してもすでに UPKI 電子証明書の発行を受けていた。

[*9] 例えば、Excel ファイルでは姓名が空白文字で区切られて一つのセルに入っていたため、空白文字で姓名を分割して姓・名それぞれのカラムとして定義するとか、身分を識別するコードをもとに Affiliation 用の属性値 staff、faculty、student、member として定義するといったこと。もし姓名が空白文字で区切られていなかったらもっと面倒な処理をしないとならなかったはずで、情報のもちかたは重要な事項であることがよくわかる。

スクリプトを作成した[*10]。

Extic にはオプションとして FIDO2 認証機能が備わっている。核融合研では、当面はパスワードのみでの認証でもよいとしても、将来的にはより強固な認証方式を課すことを視野に入れている[*11]。その際の選択肢の一つとするため、Extic 導入開始時より FIDO2 認証オプションを全ユーザー分契約し、利用可能とする設定をいれた。

Extic に約 350 名分のユーザー登録用 CSV を投入してからプロビジョニングが完了するまでに要した時間は約 14 分 30 秒、一人当たり平均 2.5 秒であった。核融合研は 500 名に満たない小規模な組織であるからこの処理速度でむろん問題ないが、数千人規模の組織でも問題ない登録処理速度であろう。

■各種設定　学認 IdP として機能するには、連携する学認 SP に送出する属性を定義する必要がある。Shibboleth IdP では attribute-filter.xml および attribute-resolber.xml によってこれを行うが、Extic では GUI による管理画面で設定することができる。基本的には SP 毎に各属性の送出をオン/オフで指定する形式のため、xml を編集することと比べてずっと楽であるし誤りも生じにくくなっている。

学認サービスプロバイダー一覧 [*12] に掲載されている設定例などの情報を参考に設定すればよいが、Shibboleth IdP の場合を前提として書かれている SP も多く、まったく馴染みのない場合には少々とっつきにくいかもしれない。参考までに、本稿執筆時点で設定済みの学認 SP を表 2 に示す[*13]。

電子ジャーナルの SP の場合のように、SP の運用者 (出版社) に IdP に関する情報を伝え、SP 側で設定してもらう必要のあるケースもある。核融合研では出版社との契約は図書室が所掌しているため、出版社とのやり取りは図書室で行ってもらった。事前に IdP のエンティティ ID やスコープを尋ねられた場合の回答を図書館に伝えておくことにより、多くの出版社について (情報通信システム部が補助することなく) 図書館側のみで対応が完結できた。

以下では、個別の対応が必要となったケースや特別な設定が必要となったケースを紹介する。

いくつかの出版社では、技術担当窓口の通知が求められたため、情報通信システム部を技術担当とするよう調整した。また、Web of Science を提供している Clarivate Analytics 社の SP では送出される属性値によって認可の判断ができるようで、設定したい条件の提示を求められたが図書館では回答が困難だったため、情報通信システム部側から設定すべき条件を提示した[*14]。

AXIES Web SP では、IdP を移行し entityID が変更になったことを運営側に伝える必要があった。SP 側の設定変更がなされるまでは、移行前のオンプレミスの Shibboleth IdP が核融合研の学認 IdP として表示されていた。

学認 RDM 管理機能 SP では、管理者権限をもつユーザーの場合に eduPersonEntitlement として GakuNinRDMAdmin を含む値を送出することとされている。Extic の標準設定では、eduPersonEntitlement 属性として、well-defined な固定値 “urn:mace:dir:entitlement:common-lib-terms” [*15] 、Extic 上でユーザーごとに設定した基本属性値、拡張属性値のいずれかをマップして送出できるようになっている。標準設定で用意されている基本属性および拡張属性の中には学認 RDM 管理機能 SP での使用に適したものがなかったため、(1) eduPersonEntitlement として送出する特別な値を定義できる拡張属性を新たに追加し、(2) 学認 RDM 管理機能において管理者権限を持たせるユーザーのみに対して当該拡張属性の値として GakuNinRDMAdmin を登録し、(3) この拡張属性を学認 RDM 管理機能 SP に対して eduPersonEntitlement 属性として送出するようマップする、ことで対処した。

3　学認 IdP の移行前後で得られた知見

本稿執筆時点では、一通りの準備が完了しいよいよ数日後に本格運用に入る状態にある[*16]。そのため、幅広いユーザー層からの問い合わせ対応といったサービス運用の上で有用な知見はまだ得られていない。そこで、本章では情報通信システム部および図書室のメンバーでの試用により得られた限定的な知見を述べる。

[*10] このようなちょっとしたスキルがない場合、ユーザー登録用の CSV ファイルを準備するのは意外と面倒かもしれない。
[*11] Google Workspace や Microsoft 365 を導入する際にも、段階的に多要素認証を必須とする形態に移行した。
[*12] https://www.gakunin.jp/participants
[*13] 動作検証ができておらず、SP の運用主体との調整中のものも含んでいる。
[*14] 本稿執筆時点ではまだ問題が解決しておらず、利用可能な状態に至っていない。
[*15] https://incommon.org/community/mace-registries/registrations-in-the-urnmacedirentitlement-namespace/
[*16] 投稿期限までに本格運用に移行できることを目指していたが残念ながら間に合わなかった。

表 2　設定済みの学認 SP

サービス名	entity ID
主として情報通信システム部が使用する SP	
AXIES Website	https://axies.jp/shibboleth-sp
Eduroam JP 申請システム	https://office.eduroam.jp/shibboleth-sp
学認クラウドゲートウェイサービス	https://cg.gakunin.jp/shibboleth-sp
GakuNin RDM データ解析機能	https://jupyter.cs.rcos.nii.ac.jp/shibboleth-sp
GakuNin RDM 基本機能	https://accounts.rdm.nii.ac.jp/shibboleth-sp
GakuNin RDM 管理機能	https://admin.rdm.nii.ac.jp/shibboleth-sp
meatwiki(GakuNin mAP グループ用 Wiki)	https://meatwiki.nii.ac.jp/shibboleth-sp
出版社 (電子ジャーナル) 関係の SP	
AIP Scitation	https://scitation.aip.org/shibboleth
Annual Reviews	https://www.annualreviews.org/shibboleth
Cambridge Core	https://shibboleth.cambridge.org/shibboleth-sp
Elsevier (ScienceDirect, Scopus)	https://sdauth.sciencedirect.com/
IEEE Xplore	https://ieeexplore.ieee.org/shibboleth-sp
IOPscience	https://ticket.iop.org/shibboleth
Maruzen eBook Library	https://elib.maruzen.co.jp/shibboleth-sp
Nature Research	https://secure.nature.com/shibboleth
Oxford University Press	https://oup-sp.sams-sigma.com/shibboleth
ProQuest Ebook Central	https://sp.ebrary.com/shibboleth
SpringerLink	https://fsso.springer.com
Taylor and Francis Online	https://www.tandfonline.com/shibboleth
Taylor & Fransics eBooks	https://api.taylorandfrancis.com/
Web of Science	https://sp.tshhosting.com/shibboleth
Wiley Online Library	https://iam.atypon.com/shibboleth
World Scientific Publishing	https://www.worldscientific.com/shibboleth
その他の SP	
NINS Open Use System (NOUS)	https://nous.nins.jp/shibboleth-sp
NII FileSender	https://filesender.nii.ac.jp/shibboleth-sp

■学認 IdP を構築し稼働するまで　Shibboleth IdP を用いてオンプレミスで IdP を構築するためには、OS のインストールから始めて各種ソフトウェアをインストールし、設定するまでの最低限の作業に加え、セキュリティに十分に配慮した設定とするには相当の経験、知識が必要となる。一方、Extic ではユーザー情報の準備・投入および SP の設定をするだけで IdP として稼働させることができ、圧倒的に楽である。

少し定量的なことを述べておくと、Shibboleth IdP v3 ではじめて新規に学認 IdP を構築した際には、いろいろと試行錯誤が必要となる場面もあり、正味の作業時間として 10 日程度を費やした[*17]。一方、今回の Extic の場合、ユーザー一括登録用 CSV のための Python スクリプト作成および SP の設定を投入に要した時間は正味半日ほどであった。

学認 SP と連携させるための設定は、Shibboleth IdP では xml ファイルを編集するのに対し、Extic では GUI 管理画面上で送信する属性をオンにするだけである[*18]。要する手間も少なければ設定の誤りも発生しにくいという点で、Extic に分があるように感じる。

[*17] いろいろと経験を積んだのちに実施した Shibboleth IdP v4 での新規構築では、2 日ほどで稼働できる状態に到達した。ただし、その際には LDAP に登録するユーザー情報は IdP v3 時代に使ったものをそのまま流用したため、その時間は含んでいない。

[*18] 学認 RDM 管理機能 SP の例で述べた通り、例外もある。

■学認 IdP の維持　自前で Shibboleth IdP を構築して運用する場合、脆弱性情報が出された際などには適宜対応する必要がある。一方、Extic では運用サイド (エクスジェンネットワークス社) に任せておけばよく、対応に人員を割く必要がない点はありがたい。

Extic は数か月に一度以上の頻度で更新が行われており、仮に脆弱性が検知されたとしても長期間放棄されるようなことはなく適切に対応されるものと期待してよいだろう[*19]。

■多要素認証への対応　Shibboleth IdP によるオンプレミスでの構築では、核融合研で利用可能な認証要素を用いて多要素認証に自力で対応することは結局できなかった。Extic を導入することで自動的に多要素認証へ対応できた[*20]のは大きな効果といえる。

Extic に限った話ではないが、一口に多要素認証といってもそれを使用するための認証要素の登録方法やユーザー認証プロセスのフローはサービスごとにまちまちであり、少々ユーザーフレンドリーではないように感じる[*21]。

Extic では有償オプションとして FIDO2 認証への対応が可能であるが、利用できる OS、Web ブラウザ、FIDO2 認証器の組み合わせに制限[*22] があるほか、登録可能な FIDO2 認証器はユーザーごとに 5 つという制限もある。多数の端末を使用するようなケースでは考慮が必要になるかもしれない。

また、FIDO2 cross-platform 認証器に対し PIN の設定が必須となっている。Extic 以外の PIN 入力が必要ないサービスで利用している認証器を Extic に登録すると、当該認証器に PIN が設定されるため、Extic 以外のサービスでも PIN 入力が必要になる点には注意が必要である。

■ユーザーの命名規則　ユーザー名 (アカウント名、ユーザー ID) がサービス毎に異なっているとユーザーの混乱を招きやすく、また、統合認証化を阻害する要因ともなりうる[*23]。そこで、表 1 に掲げた各サービスでは基本的に ‘Surname.Givenname@nifs.ac.jp’ という形式の命名規則で統一させている[*24]。ただし、機器の仕様からくる制約により、リモートアクセスサービスでは、アクセス可能な領域を決めるユーザーの属性をアカウント名に含むような命名規則を例外的に採用している。

当然 Extic でも ‘Surname.Givenname@nifs.ac.jp’ という形式のユーザー名を採用しようと考えていた。しかし、Extic では eduPersonPrincipalName (ePPN) が「ユーザー名@スコープ」となる仕様であることが分かった。そこで、ePPN に ‘@nifs.ac.jp’ が二重に付されることを避けるため ‘Surname.Givenname’ を命名規則とすることにした。

ユーザー名の命名規則が他のサービスと異なる点は懸念事項であったが、実際、情報通信システム部内での試用開始早々に ‘Surname.Givenname@nifs.ac.jp’ で使用しようとして拒否されたという問い合わせが発生した[*25]。

対応策として、

1. ログイン画面のユーザー名欄に入力された値をそのまま ID とするのではなく、@以下を無視できるようにする。組織によってこの機能を必要とするかどうかは異なると思うので、管理画面で有効/無効を選択できるようにする。(ユーザー単位での制御は不要で、組織全体でのポリシーとして設定できれば十分。)
2. ログイン画面のカスタマイズ。特に表示される文言を編集できる機能。とりあえずログイン画面に、@以下をユーザー名欄に入力してはいけない旨表示できるようになるだけでも、現在の問題は軽減できるように思われる。

という機能実装の要望を 2022 年 8 月 29 日にエクスジェンネットワークス社へ提出した。その結果、9 月 18 日の更新リリースで後者の機能が実装され[*26]、最低限の対策を施せるようになった。また、前者についても「機能改善のエンハンスとして検討する」という回答をいただいており、期待しているところである。

この事例が示す通り、開発者側とのコミュニケー

[*19] ただし、Shibboleth IdP とは異なる独自に開発したシステムのようなので、独自開発部分の脆弱性がきちんと検知されるのかが不明なことは留意点として挙げられる。

[*20] Extic ではソフトウェアトークンによる TOTP、メール OTP、有償オプションとして FIDO2 パスワードレス認証に対応している。

[*21] このあたりは認証業界に標準化を望みたいところである。

[*22] Extic 仕様 - システム環境 - FIDO2 動作確認済み認証器 https://www.exgen.co.jp/extic/specs.html

[*23] 基盤となる ID を決めておいて、各サービス上の ID とマップさせればよいだけの話ではあるが、なるべく統一しておいたほうが好ましい。

[*24] 核融合研は小規模な組織であるとはいえ、姓名の組をキーとする ID では衝突が起こることは避けられず、現実にも生じている。衝突が起こった場合、2 人目以降は Givenname の直後に連番を付している。

[*25] 案内文には命名規則が他のサービスとは異なっているという点を強調して書いたつもりであるが、手順書などを読まずに試す人はそれなりの割合で存在する。

[*26] 実際には、今回の要望を出すより前にこの機能を実装することが予定されていたようである。

ションチャネルが取りやすい点も Extic のよい点であると感じている。

4　今後の課題

ここまで述べてきた通り、Extic を使用することによって、最初の目標としていた多要素認証に対応した学認 IdP は、大きな困難もなく実現できた。

次なるステップとして、Extic に備わっている

- Microsoft 365 や Google Workspace をはじめとする各種クラウドサービスへのユーザープロビジョニング機能
- オンプレミスの Active Directory、LDAP、データベース、CSV へのユーザー情報の連携機能
- SAML2.0 による SSO 機能

といった機能を活用し、統合的に ID 管理およびユーザー認証を行える環境 (いわゆる統合認証環境) の実現に向けて取り組んでいくことが今後の課題である。

5　まとめ

本稿では、Shibboleth IdP によるオンプレミスの学認 IdP からエクスジェンネットワークス社の Extic を用いた IDaaS 上の学認 IdP へ移行した事例を紹介した。

移行とは言っても、ユーザー情報は新たに用意し直したものであり、また、SP に対する設定は Shibboleth IdP で用いていた attribute-filter.xml、attribute-resolber.xml をそのまま投入したわけではなく、かつ、電子ジャーナルを中心に多数の SP を新規に追加した。そのため、実質的にはオンプレミスでの経験を活かしながら、IDaaS 上に新規構築したものといえる。

オンプレミスから IDaaS への移行を考えている方のみならず、これから学認に加入し IDaaS によって学認 IdP を立ててみようと考えている方にとって本稿が少しでも参考になれば幸いである。

謝辞

本稿で述べた一連の活動は核融合研情報通信システム部の支援のもとに実施されました。Extic を用いた学認 IdP による電子ジャーナル利用の動作検証では核融合研図書室にご協力いただきました。Extic 導入にあたり、エクスジェンネットワークス株式会社にはさまざまな助言を賜りました。ここに謝意を表します。

参考文献

[1] 山本孝志、井上望未、高山有道、井上知幸、石黒静児、「核融合科学研究所の電子メールサービスの Gmail と Google グループへの移行」、大学 ICT 推進協議会 2020 年度年次大会論文集、FB5-4、2020 年.

[2] 山本孝志、高山有道、井上知幸、中村修、「情報セキュリティ対策としての検疫認証システムの構築と評価」、学術情報処理研究 25 巻、1 号、p.9-20、2021 年.