東京農工大学における IDaaS を用いた新たな統合認証基盤

三島 和宏[1)], 根本 貴弘[1)], 長島 和平[1)], 石橋 みゆき[1)], 青山 茂義[1)]

1) 東京農工大学 総合情報メディアセンター

{three,nemo,nagashima,saji,aoyama}@go.tuat.ac.jp

Integrated Authentication Infrastructure with IDaaS on TUAT

Kazuhiro Mishima[1)], Takahiro Nemoto[1)], Kazuhei Nagashima[1)], Miyuki Ishibashi[1)], Shigeyoshi Aoyama[1)]

1) Information Media Center, Tokyo University of Agriculture and Technology.

概要

東京農工大学（以降、本学）では、約 5 年ごとに教育系情報システムの更新を行っている。これらのシステムを学術情報基盤システムと呼び、教育用計算機のほか、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、クラウドでの認証・ID 管理基盤である IDaaS への移行を行った。これに基づき、2021 年のシステム更新では、IDaaS と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。本稿では、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の運用開始に関連する内容についても報告する。

1 はじめに

本学の教育系情報システムは、これまでの経緯により、単なる教育用計算機のみにとどまらず、電子メールシステムや認証システムなどの基盤的システムや図書館システムなどまでを含む、非常に幅広いシステムの統合が特徴である。その概要を図 1 に示す。

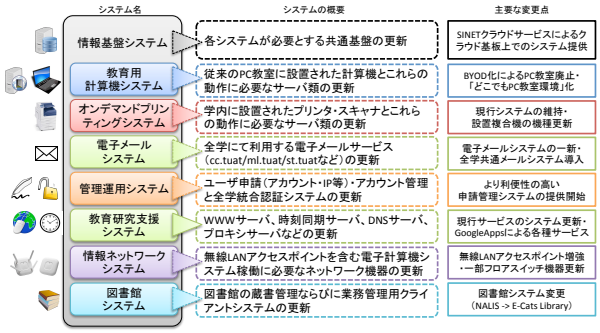

図 1 東京農工大学の教育系情報システム

これらのシステムは、およそ 5 年に 1 度のペースで更新がされており、2016 年 2 月に更新されたシステムでは「情報基盤システム」が学外のネットワークセンターに設置され、SINET5 の L2VPN サービスを経由して接続された。2021 年 10 月に現在運用されているシステムから「学術情報基盤システム」と名称を改め、各システムについても更新するとともに拡充を図った。この中でも、統合認証基盤の整備とそれに関連する多要素認証の実現が大きな軸となっており、本稿ではこの更新について詳説する。

統合認証基盤は、ユーザのアカウント情報を保持し、さまざまな情報システムの認証に用いられ、多くの大学で運用されている。統合認証基盤には、アカウントの認証を司る認証機能があり、これらと各情報システムが連携することで認証を実現している。このほか、人物に関する情報を連携させ、アカウント管理を司る ID 管理機能もある。システムによっては ID 管理は別システムにおいて運用されるケースもある。これらのシステムにより、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できる。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　東京農工大学における認証基盤周辺のシステム変遷

本学では、人物情報を管理する仕組みが複数存在する。教職員に関しては人事・給与システムが、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、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 管理運用システム“Salut”

2016年更新の教育用電子計算機システムでは、

- 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、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管理機能の具現化が必要であった。

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、実際にさまざまな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。

申請管理システムは、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、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は、図2に示すように上位システムとともに行われる。

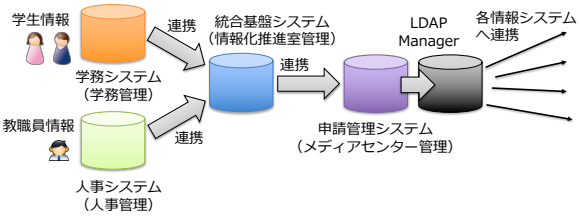

図2　学生・教職員情報の連携

また、当該の人物の属性情報に基づいて、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が可能である。下位の情報システムの連携については LDAP Manager を通じて行う。さまざまなクラウドサービスの提供に伴い、LDAP Manager のプラグインと連携のためのサーバも構築し、これらを通じて各サービスへのプロビジョニングが実施されることとなった。

3 統合認証基盤としての IDaaS の導入

2021 年に教育用電子計算機システムの更新が行われた。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の基盤はこの更新においても重要な機能として維持され、さらに新たな基盤としてクラウドをベースとした IDaaS の導入を行った[3]。実際のところ、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 を導入する検討を行っていたが、当時日本で運用するに当たって必要となるさまざまな要素が十分でなく導入には至らなかった経緯もある。

3.1 IDaaS（Identity as a Service）

IDaaS は、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 にまつわる機能をクラウド上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[4]や OpenID Connect[5]（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システムとして認証サーバ（LDAP や Active Directory などのディレクトリサーバ）を置き、オンプレミスな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一般的であった。しかし、さまざまな情報サービスのクラウド化により、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、などの機能が必要となった。

IDaaS ではこのようなクラウド時代の認証を得意とし、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。

3.2 IdaaS と人物情報連携

IDaaS では、アカウントの基礎となる人物情報を既存の情報システムと連携して管理する機能は十分ではない。このため、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。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、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し、クラウド上と必要な情報の連携が図られる。

3.3 IDaaS と申請管理システム“Salut”との統合的連携

2016 年と比較すると安定的に利用可能な IDaaS サービスが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[6]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 からの置き換えを図った。

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。

Extic は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が他の 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。ID 管理機能については、本学では ID 管理の多くの機能は申請管理システムがこの機能を担っている（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）ため、従来からの申請管理システムと Extic の組み合わせることによって IDaaS としてのメリットを享受できるようになった。

連携の概要については図 2 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 3 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 や Microsoft365 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。

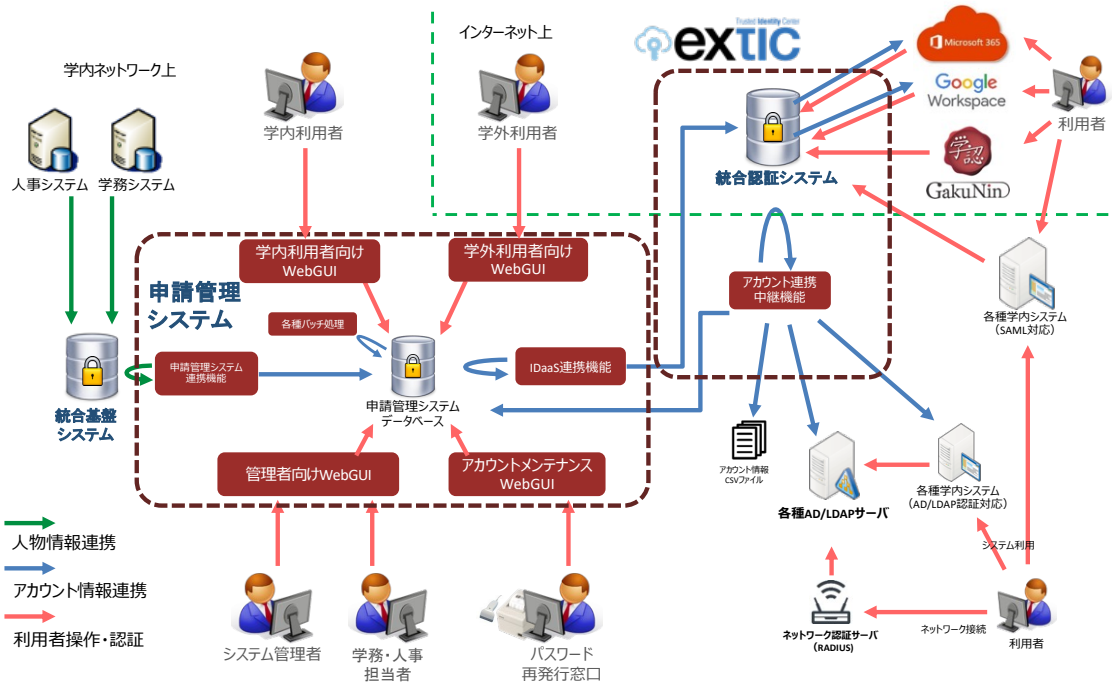

図 3　申請管理システムと Extic による情報連携と認証連携

4 IdaaS 導入における各種運用の実際

4.1 ユーザが利用する各種システムとの認証連携

(1) LDAP による認証

本学では有線 LAN ならびに無線 LAN の接続に 802.1x 認証を用いる。この際に RADIUS サーバを経由して LDAP サーバを参照している。LDAP 認証においては LDAP サーバへ連携する情報源が LDAP Manager から Extic 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。また、LDAP 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い。

(2) SAML によるフェデレーション認証

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が利用可能である。本学が利用する各サービスにおいても 2021 年のシステム更新からフェデレーション認証を採用した。また、学認 IdP についても Extic を経由する運用に変更されている。これらの認証時には図 4 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、多要素認証も求められる。図 5 に示すように、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画面で選択する。

図 4　フェデレーション認証時の認証画面

図 5　多要素認証画面（TOTP・MOTP）

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、Google Workspace、Microsoft365、Zoom、Webex、申請管理システム、moodle が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、以下のように切り替え日を分散し、問い合わせへの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。

- 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

4.3 多要素認証への対応

本学ではセキュリティ対策の一環として、多くの大学同様に、多要素認証の必須化が認証基盤の切り替えに合わせて大学の行動計画として方針が決定されていた。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を対象とした。しかし、その実施時期が、新型コロナウィルスの蔓延が始まり、学生や教職員が大学に来ることが難しくなったちょうどそのタイミングであった。多要素認証は、正しくユーザに設定を行ってもらう必要がある。これが行われない場合、多要素認証を求めるサービスへのログインができなくなってしまうため、一度実施時期については延長の決定がなされ、最終的な実施は 2021 年 12 月 15 日に行うとされ、これに合わせて取り組みがおこなれることとなった。我々も 2021 年 12 月 15 日に向けた最後の 3 ヶ月では、周知用 Web サイト・教職員ポータル・学生 Web 掲示板・説明会・ポスター（図 6 など）・各種委員会（教育委員会・運営委員会・教授会・教育研究評議会等）などを通じて、計 33 件の周知活動を展開した。

しかし、学期途中での変更で各種情報システムへのアクセスできなくなる学生が多く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、学生の多要素認証の必須化は再度延期されることとなった。周知やユーザ対応が届きやすい教職員（非常勤講師と学外者を除く）に関しては当初の予定通り必須化を行うこととした。

一部ユーザ向けの多要素認証必須化の実施日である 2021 年 12 月 15 日に向けたユーザ対応に関連した情報をまとめる。図 7 には、我々の問い合わせ用電子メールアドレスに届いたメールに含まれる関連キーワードの分析結果である。必須化の直前以外において「多要素」がキーワードになるメールはほとんど届いていない。図 8 には、ユーザの種別による設定完了数の推移を示す。この推移はキーワード分析の結果ともおおよそ合致する。実際にユーザによって設定がなされるのはどんなに事前にアナウンスをしていてもほぼ直前である。この点はユーザ対応（ユーザコミュニケーション）の現場において多く発生しうる、ユーザは土壇場になるまで動かないという事象が明確に現れたものとも言える。

5 まとめ

本稿では、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、そのシステム構成に関する概要、運用における実際について概説した。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触れている。クラウドサービスである IDaaS ではシステム構成はもちろん、運用の多くが大きく変化するイメージもあるが、実際にはオンプレミス的に運用する機器が減ったというレベルのものでもある。ただ、実際の運用においては IDaaS 自体のメンテナンスによって認証の運用に影響が出たり、ユーザが見える部分としてのカスタマイズが多くできない、など、運用的な問題も少しずつ見えてきている状況であり、本稿では取り扱いきれていない内容も多い。引き続き運用を継続し、さまざまな知見を新たに蓄積していきたい。また、多要素認証の必須化に関しても触れているが、必須化第 1 段階である 2021 年 12 月 15 日に向けたものであり、すべてのユーザが必須化された段階（2022 年 8 月 31 日）についてはまだ情報をまとめきれていない。これらの情報もまとめた上で、さらなる報告をしていきたい。

図 6　ユーザ（学生）への多要素認証必須化の告知

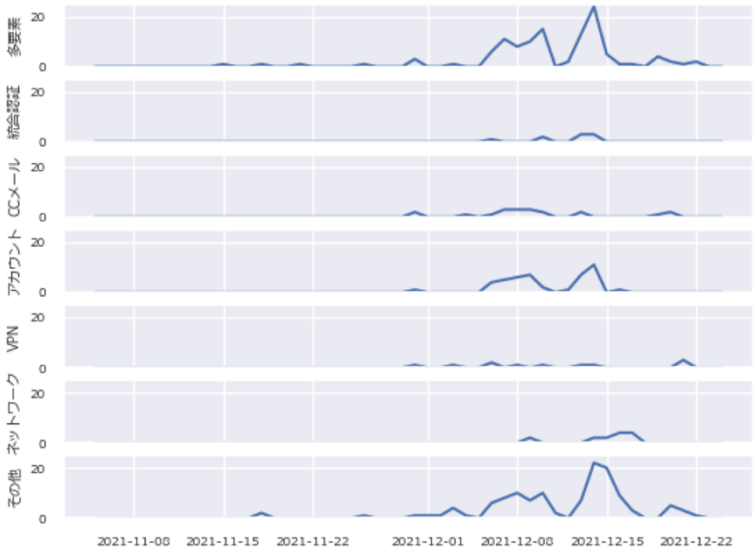

図 7　問い合わせメールでのキーワード分布

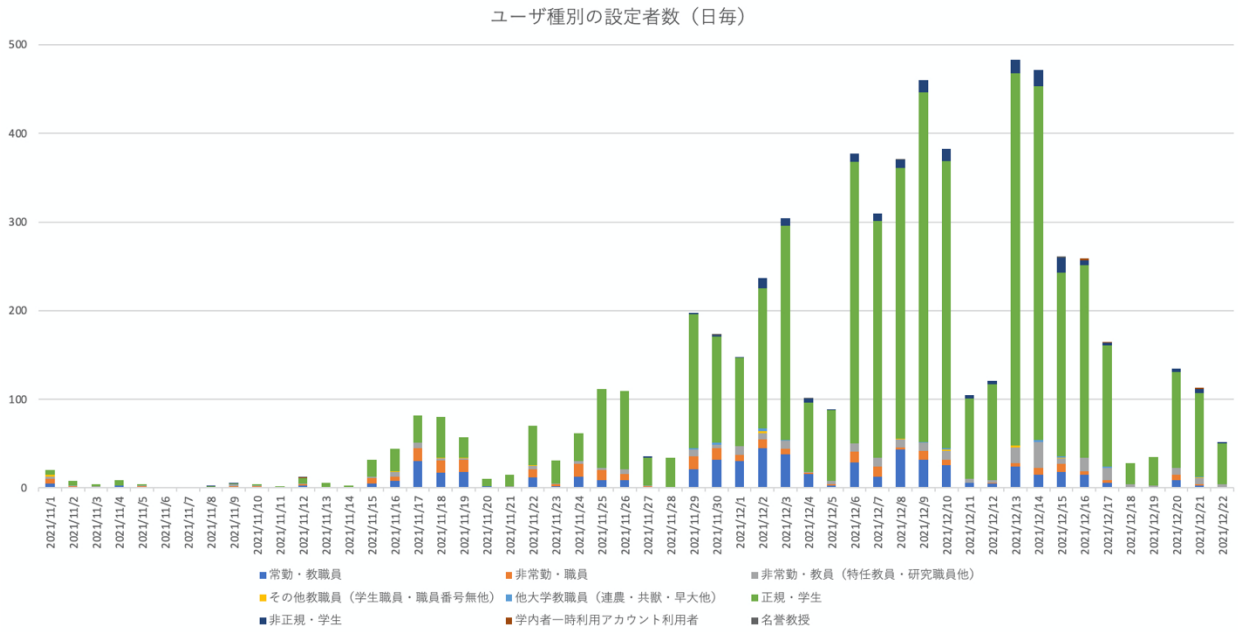

図 8　多要素認証必須化日に向けた設定完了数の推移

参考文献

[1] EXGEN NETWORKS: LDAP Manager, URL: https://www.exgen.co.jp/lm/ [web] (2022/10 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] 三島和宏, 根本貴弘, 青山茂義: 統合認証基盤としての IDaaS 導入と初期運用, IOT, [インターネットと運用技術] 2022-IOT-58(10), pp.1-6 (2022).

[4] 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)

[5] 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)

[6] EXGEN NETWORKS: Extic, URL: https://www.exgen.co.jp/extic/ [web] (2022/10 参照)