次世代認証連携検討作業部会議事抄録

学認に関する打ち合わせ　2020 年 12 月 24 日（木）

・認証に関する R&D を実施する体制について議論を行い、トラスト作業部会を拡充して実施することとし、委員、目的等を年度内まとめ、活動訴求等を積極的に行なうこととした。

学認に関する意見交換会　2021 年 2 月 19 日(金)

・学認は、全国の大学等と NII が連携した学術認証フェデレーションとして平成 21 年度から開始、平成 26 年 1 月 14 日より NII の事業として、学術認証運営委員会のもと安定的な　サービスとして運営されてきたが、研究開発的な活動はあまり行われてこなかった。 一方、研究データ管理やそこで必要とされる認証レベルや産学との連携、次期 HPCI における認証など、新しいトラストフレームワークが必要ではないかという意見も出てきている。このため、これらの課題や今後の目指すものについて、有志が意見交換し新作業部会を設置し課題対応するのが適切との結果を得た。

・新作業部会のミッションは、学術分野におけるオープンでセキュアな研究教育データ流通のためのトラスト技術の検討・開発、推進体制の検討および運用に向けた取り組み、その他今後のトラストフレームワークに関して必要となる事項を担当する。

学認に関する意見交換会　2021 年 3 月 11 日(木)

出席した大学、研究プロジェクト、民間それぞれの立場から、認証基盤における現状・課題の説明があった。主な課題は以下のとおり。

・学認の機関認定のハードルが高い（小規模機関の参加拡充）
・機関による IdP 運用・管理が煩雑（代理 IdP サービスのようなシステム構築）
・「機関」と「個人」の中間を規定する仕組み（各々を自在に組み合わせ・組み替えできる「プロジェクト」のような管理機能）
・利用者個人が所属機関を移動する際の仕組み
・利用者が主体的に学認を利用することの意識付けによる普及促進
・多要素認証
・安全保障問題への対応するための属性情報と属性検証
・利用者と運用者の双方にとって負担の少ない新方式の認証基盤

令和3年度第1回次世代認証連携検討作業部会　2021年4月23日(金)

1. 新しいトラストフレームワークの構造について、TrustedDBやTrustedDBを共同研究用のIdPとして運用出来ない大学に対してIDaaSを提供し連携する形態案の説明の後、以下の意見が出された。
   ・NIIのサービスは組織と契約してきたが、研究データのように利用者側の持つ情報に重きが置かれると、転職時に研究者個人が持っている情報をどう引き継ぐかという事が重要になる。
   ・IDaaSの契約主体は組織だったが、研究コミュニティが契約するモデルが出てきており、IDaaSで担う役割の差が大きくなるのが問題になりそうだ。
   ・属性保障が混乱しやすいので、TrustedDBがある機関は，認証情報・基本的な属性はTrustedDBを信用するが、プロジェクトに関わる情報はプロジェクト側が管理してはどうか。
   ・組織が本人確認する際、実在性と組織への紐づけが重要になる。

2. mAPCoreの概要及び課題、今後の計画等について説明の後、以下の意見が出された。
   ・学認参加SP（もしくはIdP）から直接グループ管理できるようAPIを整備し、外部SPからグループ管理の最低限（作成・更新・メンバー追加削除）のAPIのみを提供してメンバーに対するより細かなロールの提供を計画。
   ・mAPが、グループやプロジェクトに属していることを証明するための発行者になる。
   ・組織という枠組みと個人について、個人に注目すると、Orphan IDや複数グループに身元保証を受ける個人といった問題について、モデルが作りやすくなるのではないか。

3. UPKIのサービスについて振り返りと証明書に関わる状況の変化について説明の後、以下の意見が出された。
   ・多様性の重視によるアジリティの難化は、UPKIに限らず世の中全体の問題で、IDaaS等で統一すればアジリティは確保されるが、多様性や大学におけるR&Dどう担保するか考える必要がある。
   ・次世代認証連携基盤との関連性では、多様性の尊重とリスクコントロール、規模拡大とアジリティのバランスの検討が必要である。

   公開資料
   ・学認に関する意見交換会～IDaaS屋の意見～
   ・mAP Coreとは

令和3年度第2回次世代認証連携検討作業部会　2021年5月27日（木）

1. 国際共同研究プロジェクトの認証管理（1件）、大学の認証管理（2件）、Identity assurance、eKYCの基準の調査報告と質疑応答後、以下の意見が出された。
   ・大学では進め方に違いはあるが、IAL2相当に近い運用がなされている。
   ・継続時の利用者確認と登録時の利用者確認の区分けがあまりできていないのが問題ではないか。なお、継続的利用者確認をどうするかの追加レポートを OpenID Foundation Japanでもうすぐ出す予定である。
   ・人的な異動が発生した際の再確認をどう行なうかといったことも重要なポイントとなる。
   公開資料
   国際共同研究プロジェクトの認証管理例
   Identity Assurance と eKYC の基準について

令和3年度第3回次世代認証連携検討作業部会　2021年6月30日（水）

1. プラットフォーム側で必要なIALと属性セットについて（4件）の調査報告と質疑応答後、以下の意見が出された。
   ・研究コミュニティが持つソースを便利に使えるよう、大学や IDaaS でのアカウントが十分な信頼性を持つように認証レベルを上げてくためにIAL、AALを維持する仕組みを作っていきたい。
   ・組織が承認するというより、ある基準を満たしている組織を承認するという枠組みとすると双方に

都合が良く、そのためにはユーザの所属が常に最新のものに反映しているのが望ましい。
・グループ ID は広い範囲を想定しているので、IAL として規定するものは個々にレベル感が異なる。
・IAL2 相当の「相当」が重要だと思う。本人確認と ID 発行は余り直結しすぎると危険である。
・SP の要求する属性についてはまだ決定していないこと及び IAL2 相当といった断定しない言い方でなく、我々が日本の IAL2 を決めていかなければいけない。
・保存する研究データの重要度やソフト面からの認証で何を要求すべきなのか議論の余地がある。

2. 新認証基盤要件とトラストフレームワークプロバイダーに対する要望について説明があった後、以下の意見が出された。
・アカデミックな認証連携で企業研究者を収容する場合には線引きのハードルを上げる必要がある。
・ID 発行の定義がされると、企業だけではなく本人確認ができない大学等も IDaaS に来る。
・研究コミュニティに対し、サービスをどのように認可していくかという方向にフォーカスしていくべきで、研究コミュニティが本人確認、ID 管理、認証ポリシーで何を要求するかを考えていく必要があるが、本人確認をどうするかという部分は、研究コミュニティは外出しし、それを学認が中心となって引き受けるのではないか。
・研究コミュニティはどのような役割をすると効率的でセキュアなのか改めて議論しなければいけない。
・早期に大学の IdP で身分保証できない Orphan 研究者の ID 発行するサービスを実現し、学認でサービスできるようにしてほしい。
・IDaaS 的なものが学認にはないので、そこを学会等と一緒にやりますということができるのであれば実現の近道と感じる。

3. オープンフォーラム 2021 の認証トラック（2021 年 7 月 8 日(木)）で、「新しいトラスト ～学術分野におけるオープンでセキュアな研究データ流通のためトラスト技術～」をテーマとした後援、パネルディスカッション等の構成案について議論した。

公開資料
・新認証基盤要件とトラストフレームワークプロバイダーに対する要望

令和 3 年度第 4 回次世代認証連携検討作業部会　2021 年 7 月 26 日（月）

1. IGTF、eduGAIN、Kantara に共生や互換性の協調関係について関係者にコンタクトを取り、回答待ちである旨の報告があった。

2. AAL の滞欧について FIDO 認証について紹介があった後、以下の意見が出された。
・堅牢な認証を提供することで、研究コミュニティの提供するサービスを使えるようにすることが最終目的なので FIDO の利用等も現実的になる。

3. 学認での AAL2 以上の対応について説明があった後、以下の意見が出された。
・開発ソフトウェアの FIDO 認定について、日本は FIDO の認定を最も多く取っておりガイドラインもあるので、認定を取ってもらうのが良いと思う。

4. Kantara の基準について調査した結果について説明があった後、以下の意見が出された。
・Kantara の基準(Criteria)を基にして、大学・研究コミュニティの IAL 認証の手続きを検討していきたい。
・Kantara のプロシジャが日本に当てはまるか、当てはめるにはどうしたら良いかを議論する土台にしていきたいが、IdP を運用する大学・組織とサービスを提供する研究コミュニティの了解が得られないと混沌とするため、大学や研究コミュニティから Kantara のプロシジャについて意見を聞きたい。

公開資料
・Kantara の基準(criteria)を調査
・スマートフォンへの生体認証の搭載・FIDO 認証の摘要を通じて得られた知見を基にしたご提案
・マイナンバーカードの機能を利活用した民間 ID の認証におけるセキュリティと使い勝手の高いレベルでの両立に向けて″
・学認での AAL2 について

令和 3 年度第 5 回次世代認証連携検討作業部会　2021 年 9 月 10 日(金)

1. Microsoft における AAL2 以上の対応について、Windows11 で必須となった TPM2.0 と利用用途、Windows Hello の機能である生体認証機能、PIN 認証及び Azure AD の多要素認証について説明と質疑応答があった。

2. AAL の滞欧について FIDO 認証について紹介があった後、以下の意見が出された。
・大学側で ID パスワード認証した後にサービス側で更に認証する際、不具合が発生した場合の問い合せ先や対応工数が大きくなるといった懸念がある。

3. Kantara IAL2 の Criteria の説明及び IdP 側の指摘点として大学 2 件、研究コミュニティ 3 件が紹介された後、以下の意見が出された。
・本人確認を管理担当が行い、情報システム担当が一つのルールに従い ID 登録するのが CSP の考え方で、重要なのが ID を発行する際のエビデンスとなるが、大学が発行する身分証明証の検証ができれば強力なエビデンスとなる。
・Kantara Criteria では、作成する文書構造のテンプレートのような物はないので、日本版のテンプレートは学認が作らないといけない。・
・Kantara Criteria の訳文について、エビデンスの具体的な例示とか一般的にして大学関係者に理解しやすくし、研究コミュニティや他の IdP から解釈に関する議論が深まるようにする。
・HPCI では、現状ほぼ IAL2 の運用だが継続するわけではなく、次期認証基盤の設計・構築にあわせて HPCI での IAL 要件の整理を始める。
・GakuNin RDM での多要素認証に関するアプローチについて二段階目の認証を Gakunin RDM で行なうことは可能だが、二段階目の認証とサービスの認証が同じになる点が Kantara の基準と相反し、認証の対応コストが増えることが懸念点で慎重に検討する必要がある。
・CrP/CrPS のテンプレートの検討をきちんとする必要がある。

公開資料
・Microsoft における AAL2 以上の対応について
・Kantara の基準(criteria)を調査 (改)
・kantara IAL2 和訳資料
・GakuNin RDM の多要素認証に向けた考察

令和 3 年度第 6 回次世代認証連携検討作業部会　2021 年 10 月 15 日(金)

1. 今年度の検討目標について、「IAL、AAL、国際協力、学認での実装、新サービスの検討」の観点から検討し、作業部会の結果を外に出す目処を立て予算獲得の戦略へ繋げたいとの説明後、以下の意見が出された。
・概算要求は期間を要するので、まずは検討からプロトタイプ構築に係るような話に持っていきたい。NII では様々な事業を行っているので理解が得られれば可能ではないかと思う。

・NII 事業の枠組み拡張する形で考えてもらい、研究データやオープンサイエンスも含めた研究コミュニティがどのように利益を得るかというタマを用意やプロトタイプを構築する等、2～3 ヵ月後に少し形ができるように今年度の成果と来年度の目標を議論していきたい。
・データソサエティアライアンスから企業の認証で困っていて、個人認証だけでなく組織も認証してデータ使わせる仕組みを作りたいという悩みがある。研究だけでなくデータを利活用する産業側もターゲットに入れた方が良いと感じた。

2. 「IAL2 の新学認での運用に当たって（案)、「CrP/CrPS の例の提示（案)」についての説明があり、次のステップとして大学で運用可能か、研究コミュニティから大学は保証度が高いと認められるか、IDaaS 運用者から IDaaS ビジネスを回せるか確認するのが、次のステップになると思っているとの発言後、以下の意見が出された。
・10 月 22 日に認証研究会があるので、非公式な案として意見を聞きたいと考えている。他にもどの程度保証すれば大丈夫か意見を伺いたいと思っているのでそういう観点からも読んでもらいたい。

3. OpenID Foundation と DIF が標準化を進めている技術レイヤー、MIT 中心に Digital Credential Forum で標準化を検討しているデータフォーマットの取組紹介について説明があった。

4. eKYC の各種手法のリスク評価の手法について、IAL 評価シートを基に説明があった後、以下の意見が出された。
・eKYC を使う場面は源泉と IdP が直結していない場合で、だからこそ IDaaS という役目が出てくる。なぜ IDaaS が研究コミュニティに必要かというと企業研究者とか直結していない人の ID を収容することになるので、IdP と IAL、AAL の基準が出てきて、それを認定していただくのがありがたい。
・eKYC 評価手法を用途に応じていろいろなケースを埋めていくのが良い。
5. 人の異動に際するデータアクセスやポータビリティをサポートする仕組の実装について、Open-IDP で検討を始めているので次回報告してもらうこととした。

6. AAL に関して FIDO や Microsoft から話を伺い、オーセンティケータを提供してくれる者と大学を運用、両方を評価しないといけないので簡単にはいかないが AAL2 は必要であるといったこれまでの認識の説明後、今後どのように議論を進めていくかについて以下の意見交換があった。
・IdP 運用状況調査で質問事項を拡張して調査をしたいので、NII で議論を反映した質問項目を作って欲しい。

7. 10 月 8 日に開催された、 OpenID Foundation Japan　eKYC-WG で次世代認証連携作業部会活動状況を紹介した旨の説明があった。

公開資料
・IAL2 の新学認での運用に当たって（見解）(20210918)
・CrP/CrPS の例の提示（案）(20210918)
・DID と関連技術、その標準化動向、応用事例
・IAL 評価シート
・学術認証基盤における新トラストの創出～次世代認証連携作業検討部会の活動～

令和 3 年度第 7 回次世代認証連携検討作業部会　2021 年 11 月 12 日(金)
1. IAL2、eKYC について説明があり、eKYC のリスク評価についてはさらに拡充することとした。また、以下の意見が出された。

・NIMS 等、民間企業の研究者をサポートしなければいけない組織から見た、eKYC のリスク評価コメントや eKYC の提案があるとうれしい。
・共同研究者のコミュニティでは認証と認可の属性確認の区分けが必要で、どちらも CSP で行うことになると思う。

2. IdP 運用状況調査機微な情報を扱う SP に向けた AAL2 に関する質問項目について、11 月 15 日の週には IdP、学認情報交換 ML に対して調査を開始する旨の報告があった。次に Kantara AAL2 の基準の和訳結果について説明があり、以下の意見が出された。
・AAL は認証器の種類もたくさんあるし運用状況も違うので、AAL の調査結果を見てまとめたい。

3. 人の異動に際するデータアクセスやポータビリティをサポートする仕組について、Orthros プロジェクトでの検討状況の説明があり、以下の意見が出された。
・2 年前の Open Science Cloud で OrphanID や組織間異動で問題意識を持っていると聞いた。また、eduID が永続的な識別子を与えている。
・ID を異動した時の IAL 保証レベルを担保できるのか。欧州先行事例を素直に真似たら、現状の学認レベルのことはできても、議論している次世代の認証でやりたいことができないのではないか危惧する。
・大学が IAL2 になるのはいいと思うが、A 大学の IAL2 と B 大学の IAL2 が同じものであると紐づけるために公的個人認証のようなものが使えないと、新たな仕掛けを用意する等、大変になることを危惧している。全てに対応することができないことはわかっているが、できる範囲においては公的個人認証を使った方が効率的ではないか。
・デジタル庁で最近の学認の状況を聞かせてほしいとの話があり、うまく連携できればと思っている。また紹介があった認証プロキシでうまく紐づけと、マイナンバーカードと組み合わせた紐づけができると、NII で紐づけサービスを提供することができるのではないかという議論をしていて、今後、その辺の機能を持った Orthros を作って、先行的な取り組みに繋げられればと思っている。・今年度、基本的な認証プロキシサービスの開発を行い、産学連携の具体的なデモンストレーションとして、企業の方が Orthros 経由で GakuNin RDM にアクセスするのをオープンフォーラムで見せられるように進めているところである。

4. その他
・学認内部で参加機関に IAL2、AAL2 認定をするのは中立性の意味からどうなのかという意見を Kantara から受けたが、学認がトラストフレームワークであるという意義を失うので、死守したいと考えているとの報告があった。
・若い研究者からも情報を出してもらえるような場として合同勉強会的な場等の設置等を、今後意識する。
・.「次世代認証基盤構築のための基準策定と配備の観点からの文書評価のお願い」の公開について　学認 HP に評価依頼を公開した旨の報告があった。
・.次世代認証のフレームワークを議論するのは重要だが時間のかかる取り組みでもある。一方で議論されている仕組みを先行的に取り入れたいというニーズもあることから、賛同いただける一部の機関によるスモールスタートでパイロット的な取り組みの議論・検討を始めたいとの提案があり、サブワーキンググループを設置し、作業部会で進捗を随時報告することとした。

公開資料
・AAL2 - Kantara の基準(criteria)を調査
・KIAF-1440 SP 800-63B SAC & SoCA v4.0_和訳
・組織間異動における認証認可の課題

令和 3 年度第 8 回次世代認証連携検討作業部会　2021 年 12 月 23 日(木)

次世代認証連携における先行的取組みの検討打合せの経過報告として、新たに設置された短期取組検討サブワーキンググループの活動状況の報告があった。

1. IDaaS の AAL2 対応状況について、EXGEN NETWORKS 及び Microsoft から説明があり、以下の意見が出された。
   ・準拠する資格は学認も検討しなければいけないが、現状の技術だということがわかった。特に IDaaS で対応しており心強い。

その後、アンケート「多要素・多段階認証で利用可能な要素について」の集計途中経過について報告があり、以下の意見が出された。

・ハイエンドである認証がどうロングテールに波及していきうるのかといったビジネスモデルも早期段階である程度描けていることが重要だと感じるので、今後これらの議論が必要だと思う。
・今回のアンケートは学認以外でも、学内で使用している認証システムの多要素認証について聞いている。学認に限ってということであれば IdP の調査を別建てでやっており、そこでは多要素認証を導入している機関は一桁という結果が得られており、今回のアンケートは学認以外の多要素認証ということで、この回答が得られていると考えられる。
・アンケート結果では運用コストを問題視している結果が多いようだが、例えば Office 365 Education A1 のような無償の多要素認証が使えるので、直ぐ導入できそうな人がどのくらいいるのか知っておいた方が良い。その後これらの人達にどのように使ってもらうかというのが次のフェーズではないか。
・我々の活動のプレゼンス上げていって、これに関わることが大事だと思ってもらうことからやらないといけなくて、我々自身に問題があるという認識をもっと持った方が良い。

2. IAL のフィードバック状況について報告があり、今後の検討にあたっての考慮する点として、大学に直接雇用されていない研究者の扱いが挙げられた。

次に e シールと法人 KYC の動向について情報共有があった後、以下の意見が出された。

・会社・学会にしか所属していない者が IAL2 で身元を主張したい場合の補償として IDaaS 関係でできないかとの意図があり情報共有を依頼した。
・gBizID を利用して本人確認を行ったうえで、GakuNin RDM を利用できるといった実証評価を 2022 年のオープンフォーラムでデモンストレーションすることを目標にシステム開発を進めている。

その後、IAL 評価シートに関して前回の部会で出された意見を元に追加・修正した資料内容の説明があり、質疑応答の結果、再度議論することとなった。

公開資料

・AAL2 の新学認での運用に当たっての見解（案）（20211207）
・認証器 registry_MSAuthenticator
・e シールと法人 KYC～組織における構成員の身元確認に関連して～
・IAL 評価シート(6th_update)
・令和年月日「学認 LoA1 認定プログラム」における審査手続きについて

令和 3 年度第 9 回次世代認証連携検討作業部会　2022 年 1 月 18 日(火)

1. IAL の議論が引き続き行なわれ、始めに外部の研究者にアカウントを付与する際に KYC をどのように運用しているかについて、研究プロジェクト（2 件）から説明があった。続いて前回の議論に引き続き、IAL 評価シートについて説明があり以下の意見交換が出された。
   ・Kantara が求めている CrP/CrPS をきちんと書くことに繋がると思うが、苦労すると思うので適切に案内してあげるのが良い。

続いて OpenIDP と他の認証との認証連携に係る開発状況の紹介があり、以下の意見が出された。

・Orthros の IdP が認定対象になるかは今後考える必要がある。

続いてIALの12月末までのコメント4件について説明があり、以下の意見が出された。

・文言の曖昧さや実態に合わせた修正といったフィードバックを行い、今後、具体的な基準の策定の議論を始めていきたい。

・IALは大学なら何とかなると思うが、海外や企業の利用者を収容するためIDaaSとかOrthrosでもgBizIDの参画を依頼しなければならない。

2. AALについての議論で、認証器レジストリの運用する際の負担感に関しての検討結果に関して説明があり、以下の意見が出された。

・認証器自身の初期認定だけでなく、ライフサイクル的な視点での維持・管理が運用するうえで必要ではないか。

・IPAや大手ベンダを集めて協力を仰ぐのも必要だと思う。

・認証器レジストリの運用は面倒であることは理解しているが、短期取組検討SWGの試行で負担感を収集し報告する。

3. 学認LoA1認定プログラム」における審査手続きについて説明があり、以下の意見が出された。

・認定するアサーションの中に反映する２つの話題があるが、認定についてはKantaraのLOA1認定プログラムが走っていて、Kantara開始後に認定したことがない。今回、Kantaraに認定を求めるには結構長いネゴシエーションが必要だと思うので、学認が認定するという形で進めようと考えている。

公開資料

・IAL評価シート(6th_update、再議論)

・認証プロキシサービスOrthros

・IAL2の新学認での運用に当たって（案）(20211020)

・AAL2の新学認での運用に当たっての見解（案）(20211207)

・認証器レジストリの運用検討

・認証器registry_MSAuthenticator

・「学認LoA1認定プログラム」における審査手続きについて

令和3年度第10回次世代認証連携検討作業部会　2022年2月22日(火)

1. IALについて前回に引き続き議論が行なわれ、運用案に関して修正部分の補足説明があった後、以下の意見が出された。

・アカデミックの利用者、企業の利用者が外のIDを使えるようになったら、認可コントロールに徹していくというシナリオが正しいのかもしれない。

・MOUは学認が提供するようにしていけなくてはならない。

・提案の趣旨としては、全てに適用するものではなく段階を作ることができるのではないかということである。学認IAL2を表明する、もしくは学認IdPなので信頼しようということで適用できるSPが大部分であると思っているが、厳密に確認したいケースもあると思うのでそのような所には提案したようなことを使っていくのは良いと思う。ここから先は認可の問題で、アカウントを作ることに加えてアクセス権限をどうするかというコントロールを段階的に考えていただけると良い。

・所属確認が重要で、エビデンスとなる社員証等を学認で信用することを表明することが必要。

次に、意見募集を反映した「IAL2の新学認での運用に当たって（案)」のVer.2の修正箇所等の説明があり、slack上で検討した後公開し、IdP、SPに対し問題ない旨の確認作業を年度末から年度初めに行いたいとの発言があった。

2. AALについて、認証レジストリを運用するための検討状況について報告があり、以下の意見が出された。

・証明書の運用は大学によってバラツキが大きいので、パブリックな認証局を使う必要があるかはコスト面等の検討が必要。
・プライベート認証でもCP、CPSは書かないといけないが審査が面倒ではないか→学術機関どうしであれば、無くてもトラストフレームワークが成立するのであれば良いが、企業も含むとなるとCP、CPSを整備して示せる状態にしておくことが必要。
・AALの話題を進めた後、証明書認証の提案を議論したい。
・認証器そのものについては運用パラメタ制御まで含めると大変なので、スモールスタートで実験のできるところからお願いすることを考えたい。

公開資料
・IAL2の新学認での運用に当たって（案）(20220225)
・AAL2の新学認での運用に当たっての見解（案）(20211207)
・CrP/CrPSの例の提示（案）(20220222)
・学認における検証済み属性表現の必要性と技術仕様（案）(20220221)

令和3年度第11回次世代認証連携検討作業部会　2022年3月23日(水)
議論に先立ち、Web上で「IAL2の新学認での運用に当たって（Ver.2)」の公開をしたこと、当該文書に関して意見をいただいた大学関係者と意見交換の報告があり、認定するための基準等を文書化して機関に示すこと、作業にあたって体制整備の必要性が確認された。
続いて、SP側で「IAL2の新学認での運用に当たって（Ver.2)」について許容できるか検討した結果について基本的に問題なしとの報告があった後、以下の意見が出された。
・学認のIAL2は国際標準で認められるかに関して、Kantara、IGTFに対し、総合運用性を議論することを計画しており、学認のIAL2が国際基準と互換性があると認められるよう努力したい。
・学認のIAL2は国際基準同様、社会情勢で変化していくことを明示することが確認された。
・IAL2の認定時の基準に従って認定したものは基準の期限末まで有効とし、認定の時期によってずれは生じるが、全体としてこれを許容するということでいいのではないか。ただし、これらのルールを独自に決められるものなのか、国際的に決めごとがあり従う必要があるのかは調査する必要がある。
・Kantaraの認定期間は1年毎に更新されている。IdPフェデレーションでは、サーバ証明書のようなシビアな対応は現状求められていないが、将来的に備えた対応が必要。
・「AAL2の新学認での運用に当たって（案)」についても、公開し広く意見を求めたいとの提案があり了承された。
続いて、以下の議題について説明・議論が行なわれた。

1. Orphan IDを救済するためのエビデンスやIDaaSの運用について、共同研究サービスにおけるIDaaSモデル（企業所属研究者と共同研究を可能とするしくみ）とID保証の表現方法（ミニマム実装案）について説明があり、以下の意見が出された。
・作業部会で、このままでは日本における研究基盤が進展しないので、企業所属研究者や大学の研究者向けの共通IDaaSをサービス化して欲しい。
・研究者が異動した時に所属機関に強く関連付けられたIAL2だと、その瞬間に利用資格を失うことになるので、円滑に研究を続けるため共通IDaaSのニーズはあるのではないか。
・IAL2、AAL2はコモディティ化している背景があり、特別なことをやっているわけではないという視点で活動する。
・KYCの基準はIAL2の付属文書として分けて出したいと思っているので、ホワイトリストも含めた検討を今後もしていきたい。
2. 認証プロキシサービスOrthrosの進捗状況について説明があり、以下の意見が出された。
・どのSPに対して誰が認証できるかについて、Orthrosではどの機関のユーザかという単位で管理している。Orthros上にユーザを作る際、ユーザは自分自身で認証手段として他のアカウント

と紐付けることができる。そのうえで、どのSPに対してどういう状態のユーザをログインさせるかはSP単位で機関の管理者が設定できる。また、SP側からどのレベルならアクセスさせるか指定することもできるとの追加説明があった。

・サブワーキンググループで進めているSPとIdPの接続実験にOrthrosも繋いではどうかという意見があり検討することとした。

3. 短期取組検討サブワーキンググループにおけるタイムラインも含めた実験的な取り組みについて状況報告があった。

公開資料

・共同研究サービスにおけるIDaaSモデル(企業所属研究者との共同研究を可能とするしくみ)
・ID保証の表現方法（ミニマム実装案)
・認証プロキシサービスOrthros進捗報告(2022/03/23)
・次世代認証基盤構築のための基準策定と配備の観点からの文書再評価のお願(20220311)
・IAL2の新学認での運用に当たって（案)(20220225)

AAL（Authenticator Assurance Level）
登録済みユーザーがログインする際の認証プロセス（単要素認証or多要素認証、認証手段）の強度を示す。
Lv.1 単要素認証でOK
Lv.2 2要素認証が必要、2要素目の認証手段はソフトウェアベースのものでOK
Lv.3 2要素認証が必要、かつ2要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）

CrP/CrPS （Credential Policy Credential Practices Statement）
クレデンシャルな情報の取り扱いに係る運用方針とその実施要領）

CSP（Credential Service Provider）
NIST や KIAF の文書のモデルでは従来 IdP と呼ばれていたもので、パスワードや証明書などのクレデンシャルを利用者に発行するサービスを行うところを規制の対象としている。

eduGAIN
研究と教育のアイデンティティ連携を相互接続する国際的な連携サービス。
eKYC（electronic Know Your Customer）
サービス事業者のための、本人確認手続き

FIDO（Fast IDentity Online）
従来のパスワードに代わるとみられている認証技術のひとつ。業界標準になるとみられている。

IAL（Identity Assurance Level）
ユーザが新規登録する際に、CSP（Credential Service Provider）が行う本人確認の厳密さ、強度を示す。
Lv.1 本人確認不要、自己申告での登録でよい
Lv.2 サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
Lv.3 識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者

IDaaS（Identity as a Service）
ID管理を行うクラウドサービス

Identity assurance
属性の保証

IdP（Identify Provider）
認証システムのID管理システム。

IGTF（Interoperable Global Trust Federation）
電子インフラストラクチャおよびサイバー インフラストラクチャのプロバイダー、アイデンティティ プロバイダー、およびその他の資格のある依存当事者間の相互運用可能なグローバルな信頼関係を確立するのに役立つ共通のポリシーとガイドラインを確立するための機関

Kantara（Kantara Initiative）
「OpenID」,「SAML」（security assertion markup language),「Information Card」に係るID管理技術の相互運用を目指す業界団体。2009年6月17日に米国で設置。

mAP Core（ member Attribute Provider Core）
学認クラウドゲートウェイにおける認証システムのグループ管理機能。

NIST SP 800-63
米国立標準技術研究所(NIST)が発表した電子的認証に関するガイドライン（現在は第三版 63-3)。米国政府のセキュリティ対策利用を前提としているが、Kantara でも新規格に合わせた認証スキームを更新。

OpenID Connect
認証結果を含むユーザの ID 情報を連携するためのプロトコル

OrphanIF
学認未加入大学や企業研究者といった管理する組織、身元保証がない ID。

SP（Service Provider）
認証システムにおけるアプリケーション（サービス）側。

UPKI（University Public Key Infrastructure）
大学間連携のための全国共同電子認証基盤