

CA2109

動向レビュー

次世代認証連携が拓く次世代学術基盤

国立情報学研究所 トラスト・デジタルID 基盤研究
開発センター

1. 学認の構築とその性格—長い前書き

1.1 認証連携と学認の構築

インターネットの世界で認証連携とは、「利用者が所属機関（利用者は機関からアカウントを与えられているという前提が必要）で認証した結果を、信頼関係に基づいて他機関のサービスが受け入れ、シングルサインオン（SSO）や属性連携を実現する仕組み」のことを言う。日本における大学等研究機関（以下「機関」）のアカウントを使って認証連携を実現したのが「学認」⁽¹⁾である。2010年に正式に運用が始まり、今では参加機関数400超⁽²⁾、全国の大学数の約半数を数えるまでにいった。

もちろん、2010年当時ではSSOの普及も進んでおらず、対象となるサービスの数も限定されており、理解のための環境の整備もこれからという感じだったが、現在はSSOの利便性が広く認識されるようになった。これについては、機関内での学習管理システム（Learning Management System：LMS）や学務システムを含む多様なサービスをSSOで利用可能な環境が整備されたことが大きい。さらに、近年、自機関の外にあるサービスが広く公開されるようになったことも大きい。公開されたサービスには、電子ジャーナルなどの学術系サービスに加えて、福利厚生系のサービスも増えてきた。これらをサポートするための基盤として、学認は育ってきた。

認証連携の仕組みは、世界的に見ても国を単位として構築が始まった。当初は利用者にアピールするサービスが電子ジャーナル程度しかなかったものの、それから順調に成長し、現在カバーするサービスの種類と数の多さは、認証連携が広く普及したことの証明になっている。

認証連携がその価値を発揮するのは、機関外にあるサービスを機関内のアカウントで利用する時である。日本に限らず、世界的に見ても高性能計算（High Performance Computing：HPC）の計算資源やデータ基盤がSaaS（Software as a Service）の形で利用者に提供されることが一般的になっている。それらの大規模なリソースの共用は、チームを組んで大規模に研究を展開する現代の研究形態では鍵となるものである。従来、高価なリソースは、提供者側が、利用者の審査やアカウント発行などの利用者管理を行っていた。一

つの機関内にリソースが設置される場合でも、他機関の利用者を受け入れる運用形式が取られてきた。ここでは、予算の管理から他機関の利用者を含むアカウントの管理までをリソース提供側で行うことで、認証認可に関わる運用管理を行ってきた。ここに「所属機関内のアカウントで他機関のリソースを」という考えが押し寄せてきたとき、運用管理体制の組み直しが大変な作業を要することは容易に想像できる。日本では（スーパー）コンピュータが共同利用リソースの代表的なものとされているが、最近ではSPRING8（大型放射光施設）などの大型実験施設、全国で20～30か所あるとされる大型電子顕微鏡の施設などを含めて、国内の機関等が共同で利用する全国の施設や拠点（2026年現在で全国に88か所⁽³⁾）の整備が進められてきた。

1.2 トラストフレームワークと認証強度

共同利用されるリソースの利用者の管理は、以前から大きな問題であった。利用希望者の利用資格をどう判定するかという問題に、従前は利用希望者の所属する機関の確認と裏書によってこれに替えていた。学認を運用するときの基本的な考え方もこれに近い。すなわち、一つの機関から発行されたアカウントで他機関のリソースへアクセスするときは、アカウントが機関から正当に発行されたことと、そのアカウントを使った機関内でのアクセス情報が十分信頼できることをアカウント側は主張し、リソース提供側がそれを信頼することが成立してはじめてアクセスが許されるようになる。アカウントを運用管理する機関と、リソースを提供する機関がこの認証強度についての信頼関係を表明した上で、機関内アカウントで機関外のリソース利用を許す枠組を「トラストフレームワーク」と言い、21世紀初めから考え方の整備が進められてきた。

そうはいつても、提供するリソースが高価なもの、または安全保障上厳しい管理を要求するものである場合には、認可は容易ではない。自然、利用者管理とログイン管理を含めたすべての運用管理要件を抱え込み、機関が提供するアカウントでのログインは信頼しないということになった。技術的には、当時一般的だったパスワードを使った認証に対する攻撃のリスクが無視できないことが明らかになっていったことに加え、そもそも、管理の外にいる者が「私は認証されました」という結果を持ってきても、それが高価なリソース利用を許可するに値するとは心理的に納得しがたい。リソースの提供側に立てば、この判断はやむを得ないところもある。しかし、研究者としては、この判断によって、HPCや医療情報のデータベースへのアクセスに専用アカウントの発行という手間がかかるのは不満だろう。この意味での信頼関係の醸成はなかなか進まず、

トラストフレームワークとしての学認は、オンラインでの高価なリソースや機微情報の利用拡大には足踏みが続けてきた。

2. 学認の現代化としての次世代認証連携

2.1 学認を取り巻く環境の変化

そうこうしている間に、インターネット上で様々なリソースを提供する流れが加速した。世の中の多くの、誤解を恐れずに言えばほぼすべてのコンテンツがインターネットを通して入手可能になったと考えられて久しい。インターネットの性能向上とともに、認証のセキュリティ向上も、この流れに拍車をかけた。スマートフォンの多要素認証アプリである Google Authenticator のサービス開始が 2010 年、Microsoft Authenticator のそれが 2015 年であるが、これらによって、スマートフォンが認証の強度を高める装置として完全に定着した。それまでは認証強化のためには、カードリーダーを含む新たなデバイスを用意することが必要だったが、その軛から一気に解放された。また、ブラウザやパスワードマネージャを用いて長くて複雑なパスワードを管理できるようになった結果、認証への信頼が増し、コンテンツビジネスは急速に成長した。

機関内部においても、認証基盤の運用を委託する事業者がスマートフォン等を利用した強い認証を提供す

るようになった。今や、機関内環境でスマートフォンを利用した強化された認証を採用する機関が増えつつある。

2.2 学認の現代化としての次世代認証基盤の構築

この流れは、認証強度の不十分さが理由で進まなかった、学認を通じた高価なリソースへのアクセスに再び光を当てた。技術的な解決の可能性が見いだされたところで、学認は「次世代認証連携基盤」の名の下、機関認証基盤と、高価なリソース利用のためのシステム、プロトコル整備を本格的に目指すこととなった。

つまり「次世代認証連携基盤」の整備は、インターネット上の学術リソースへのセキュアなアクセスを可能とし、現代的な研究方法への適合を目指す、認証基盤の現代化の動きであり、2020 年代の学認の活動の大きな部分を占めている。図は次世代認証連携のスコープを示すものである。以後、この中の認証強度に関係するものを説明する。

3. 次世代認証連携基盤の配備の実際

3.1 認証強度の IAL と AAL による表現

学術リソースにセキュアにアクセス可能とするには、まず、リソース提供側の納得を得なければならぬ。学認は、認証強度のリスク評価にまず取り組ん



図 現在の次世代認証連携のスコープ (国立情報学研究所 トラスト・デジタル ID 基盤研究開発センター作成)

※ IHV モデル：デジタルに検証可能な証明書 (VC) の流通を発行者 (Issuer)、所持者 (Holder)、検証者 (サービス提供者) (Verifier) 間で行うデータモデル

だ。2010年代からこのリスク評価の評価軸は整理されつつあった。具体的には Identity Proofing（本人の身元確認。本人が実在した上で当該機関に所属していること）、Authentication（アカウントを持っている本人自身が認証を行っていること）、Federation（認証情報が発行側（身元情報提供者）と利用側（サービス提供者）の間で信頼されていること）の3つであり、技術や運用によって信頼度にレベルをつけるものであった（3つの保証レベル（Assurance Level）を、それぞれ IAL（身元確認）、AAL（認証強度）、FAL（連携信頼）と言う）。当時から、抽象的な基準（REFEDS Assurance Framework：RAF⁽⁴⁾）から具体的な基準（NIST SP800-63⁽⁵⁾）まで、いくつかのものが提案されていた。内実としては、認証基盤を運用する者の間で漠然と合意が取れているものであった。そこで、米国立標準技術研究所（NIST）の基準を参考にして、日本の機関運営の実情に合わせて検討を行った。

まず、日本の機関内でのアカウントの運用のされ方を検証、評価した。特に IAL について以下の検証結果を得た。

1. 日本の学術機関のアカウント運用は安定しており、十分信頼できる。特に学生と教職員のアカウントの運用管理については、世界的に高い信頼性を主張できるレベルである。ここで各機関が従来の運用管理方針を大きく変える必要はないと評価された。
2. 一方、学術機関に特有なものとして、機関外の研究者を受け入れて行う共同研究がある。共同研究を行う国内外の他の学術機関や産業界の人材に対してアカウントを提供することも一般的に行われているため、この運用は、正しく統制することが求められる。

学認では、関連する規程文書を策定し、実施可能性に関する実証実験を行った。特に「IDaaS や共同利用機関の管理するアカウントが IAL2 を満たすためのガイドライン」⁽⁶⁾は、日本の実情に応じて、高い認証レベルを実現するために、ID の管理・認証を行う外部サービス（Identity as a Service：IDaaS）の技術を利用するときのガイドラインであり、リソース提供側が自ら利用者を管理する場合のレベル感を規定したものである。ここでは外部研究者を受け入れるための身元確認の方法として、マイナンバーカードを含む、社会的に通用する様々な身分証の利用と、その検証方法に言及している。

ここで規準策定の当初から視野に入っていた IDaaS について言及したい。認証基盤の運用にかかるコストをどう手当てするかは、以前から大きな問題であった。以前は、セキュリティ上の観点等から、信頼されるデー

タベースとの接続すらも大きな交渉事であったが、認証基盤の重要性が認識されるようになると、接続が必須であり、関係するセキュリティ等のコストも必要であるとの理解が得られるようになった。学認開始当初から（実は世界的にも）標準的な認証・認可オープンソースソフトウェアであった Shibboleth⁽⁷⁾を使った自前での運用から、IDaaS を採用してコスト、構築時間、さらには運用技術を外出する形に舵を切るのは当然であった。今後、高信頼性を持つ認証器（多要素認証に用いる技術）の運用が一般化し、運用コストを Shibboleth で賄うのが難しくなるにつれて、IDaaS の運用が一般的になると考えられる。学認は、IDaaS の採用を前提とした認証基盤の運用統制を図る予定である。

次に問題になるのは、AAL のレベルで本人を認証する技術である。単一のパスワード認証では信頼されにくいという現状を打破するには、複数の方法で確度を上げる多要素認証が求められた。技術的に見ても、顔認証技術の採用やパスワードレス認証を行うパスワードの出現など、技術の進歩は急であるが、前述ののとおり、スマートフォンの普及により技術を採用する際のハードルが下がり、合理的なコストで準備できる環境が整った。認証器の採用には、リスク評価が必要である。学認は、急速に進歩する技術に対応し、各機関の採用の便宜を図るため、認証器の統一したリスク評価の枠組を構築し、結果を公開した。これが「認証器レジストリ」⁽⁸⁾であり、Japan FIDO Alliance⁽⁹⁾等の知見の導入により、早期の立ち上げに成功した。

3.2 IAL2/AAL2 運用のための方策

このように、機関内部で高いレベルで認証されたという情報は、一定のプロトコルで機関外のリソース提供者に対して届けなければならない。学認は、当初からこの情報流通のために関連するプロトコルを策定しており、その技術レベル（FAL）に気を配っている。海外でも同様のプロトコルが定められており、運用が開始されたら、国際相互運用性のための交渉が必要になることを意識している。本来、IDaaS は、機関内、または IDaaS 提供事業者内での情報流通のみに気を配ればよく、機関をまたいだ情報流通に配慮されることがままあった。幸い、機関内での情報を機関外で流通させるための代理サーバ（プロキシ）が成熟した技術としてさまざまな事業者から提供されている。次世代認証基盤での IDaaS の運用では、自前で機関外のリソースへのアクセスのための情報流通を可能にする解の他に、プロキシを通して機関外リソースを利用する形態が一般的になることを予想している。

4. 提供属性の整備とさらなる展開

4.1 流通させる属性の再検討

認証が IAL、AAL の観点から強化されるようになると、次に問題になるのは、リソース提供の判断に用いる本人属性の提供である。認証基盤から得られる認証情報の確度が上がると、付随して送出される属性も同様な認証強度を持っていると考えてよい。例えば、一定の研究科に所属している、身分が教員であるといった情報はリソース提供判断にあたっての重要な情報である。学認は、サービス開始時から、プライバシー上の考慮から最小限の認証情報の提供にとどめる方針で運用されてきた。ところが、認証強度が上がれば、認証連携を通じた共同研究の実現が視野に入ることになり、名前や身分等の情報の流通が強く求められるようになる。実際、研究のために交換する本人属性セットとして、世界的には R&S (Research and Scholarship)⁽¹⁰⁾ が定められており、こうした国際相互運用性への対応が求められている。

4.2 共同研究等のサポート

共同研究推進の観点に立つと、機関を越えた研究プロジェクトをどう支援するかにも解が求められる。ここでは、①機関を越えたプロジェクトに関する属性の管理とともに、②プロジェクト参加メンバーの所属する機関が認証基盤を用意していない場合のセーフティネットの整備が必要である。プロジェクトが国内外の参加者からなる大きなグループによって運営されるときサポートのために、既存のシステム (国立情報学研究所運用のもので言えば、①はグループ管理システム mAP (member Attribute Provider)、②は認証プロキシサービス Orthros⁽¹¹⁾) を強化することにより、国外からの認証連携基盤を収容するような国際連携を見据えた対応を計画している。

実は、大学等では、本人に関係する情報を属性の形で保有しており、それを証明書の形で外部に出すことが本来業務の一部として行われている。証明書は、学生証等の身分証、在学証明等の資格証、成績証明等の事項記述証明を含む。高い認証強度で本人がこれら証明書の発行を要求することに応じて、証明書をオンラインで発行することは、大学デジタルトランスフォーメーション (DX) を加速するものとして重要な位置を占めている。次世代認証基盤は、この要請にも応えるものである。

5. 次世代認証基盤が拓く次世代学術基盤

次世代認証基盤の整備は、認証情報のレベルの改善により、高価な情報へのアクセスを可能にする仕組みの枠を超え、改善された認証情報を利用してどのよ

うに研究、特にプロジェクトをベースにした国際共同研究をサポートするかに軸足を移している。さらに、認証基盤から送出される認証レベルの高い情報を用いて、大学 DX のために各種証明書をオンラインで流通させる仕組の構築も視野に入ることになった。ここには、次世代認証基盤の設計と構築に際しての思想が反映されている。本稿では、その大枠を提示した。今後、国際共同研究や大学 DX の展開の基盤となることを期待している。

- (1) 学認.
<https://www.gakunin.jp/>, (参照 2026-07-23).
- (2) “IdP・SP 一覧”. 学認.
<https://www.gakunin.jp/participants>, (参照 2026-07-23).
- (3) “共同利用・共同研究拠点 (Joint Usage / Research Center)”. 文部科学省.
https://www.mext.go.jp/a_menu/kyoten/, (参照 2026-07-23).
- (4) “REFEDS Assurance Framework”. REFEDS.
<https://refeds.org/assurance>, (accessed 2026-07-23).
- (5) Grassi, Paul A.; Garcia, Michael E.; Fenton, James L. Digital Identity Guidelines. 2017, (NIST Special Publication, 800-63-3).
<https://doi.org/10.6028/NIST.SP.800-63-3>, (accessed 2026-07-23).
- (6) 佐藤周行. IDaaS や共同利用機関の管理するアカウントが IAL2 を満たすためのガイドライン (案). 2022, 7p.
<https://www.gakunin.jp/sites/default/files/2022-07/IDaaS%E3%82%84%E5%85%B1%E5%90%8C%E5%88%A9%E7%94%A8%E6%A9%9F%E9%96%A2%E3%81%AE%E7%AE%A1%E7%90%86%E3%81%99%E3%82%8B%E3%82%A2%E3%82%AB%E3%82%A6%E3%83%B3%E3%83%88%E3%81%8C%81%82%E3%82%92%E6%BA%80%E3%81%9F%E3%81%99%E3%81%9F%E3%82%81%E3%81%AE%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3%E3%83%88%E6%A1%88%EF%BC%89.pdf>, (参照 2026-07-23).
- (7) 野田英明, 吉田幸苗, 井上敏宏, 片岡真, 阿藤品治夫. Shibboleth 認証で変わる学術情報アクセス. カレントアウェアネス. 2011, (307), CA1736, p. 4-7.
<https://doi.org/10.11501/3050825>, (参照 2026-07-23).
- (8) “認証器レジストリとは”. 学認 AAL2 認証器レジストリ.
<https://level2.gakunin.jp/about/>, (参照 2026-07-23).
- (9) FIDO Alliance.
<https://fidoalliance.org/?lang=ja>, (参照 2026-07-23).
- (10) Harris, N. REFEDS Research and Scholarship Entity Category. ver.1.3, Zenodo, 2016.
<https://doi.org/10.5281/zenodo.6832218>, (accessed 2026-07-23).
- (11) 西村健. 新学認における NII の取り組み: Orthros × mAP Core., 2023, 45p.
<https://www.gakunin.jp/sites/default/files/2023-06/%E6%96%B0%E5%AD%A6%E8%AA%8D%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8B%E3%81%AE%E5%8F%96%E3%82%8A%E7%B5%84%E3%81%BF%EF%BC%9A%OrthrosC3%97mAPCore.pdf>, (参照 2026-07-23).

[受理: 2026-08-07]

Center for Trust and Digital Identity Research and Development, National Institute of Informatics
Building the Future Academic Infrastructure through Next-Generation Identity Federation (参照)