



「トラストフレームワーク」による

学認が連携基盤として機能するようになると、海外や商用サービスとのシームレスな連携も視野に入る。そのために不可欠となるのが、ユーザーに関する情報を事業者間で安全に流通させる「トラストフレームワーク」の構築である。トラストフレームワークは、産学でのID連携を実現することで、よりセキュアで利便性の高いオンラインサービスの基盤となる可能性を秘めている。

ユーザー認証の信頼性を保証し合う

学認を運用する際に、ポイントとなるのが認証の仕組みである。安全、かつ信頼性と利便性も高い認証基盤があってはじめて、学認の快適な利用は可能になる。それを実現するのが「トラストフレームワーク」であるという。このトラストフレームワークとはどのようなものなのか。学認におけるトラスト構築のキーパーソン、東京大学の佐藤周行准教授は次のように語る。

「簡単に言うと、オンラインサービスを利用・提供する際に、ユーザー認証の信頼性をみんなで保証し合う仕組みです。ユーザーID提供者 (IdP=Identity Provider) は、ユーザーの存在を確認し、一人ひとりにIDを提供します。そして、ユーザーの同意に基づいて、ユーザーに関する個人情報をサービス提供者 (SP=Service Provider) に安全な形で送り、オンラインサービスを受けられるようにする。そうした仕組み全体を、トラストフレームワークと言います」

ネットワーク上では、主にIDで個人を識別しているが、そのIDを本当に登録した本人が使用しているのか、確認する術はない。しかし、IDと実在の人物との対応を、信頼できる機関がきちんと保

証していれば、その問題は解消できるというわけだ。

デジタルアイデンティティ研究の第一人者である野村総合研究所の崎村夏彦上席研究員は、トラストフレームワークをこう説明する。

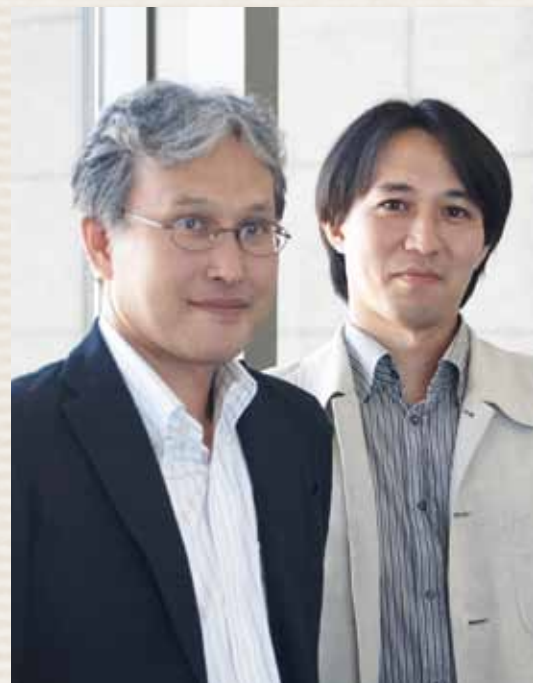
「わかりやすく言うと、食品のJAS (日本農林規格) マークもトラストフレームワークの一例です。私たちは、JASマークによって、原材料の表示が第三者機関からJASの規格に則っていると保証されていることがわかり、信頼して商品を購入しています。専門的に言えば、第三者による信用供与によって情報の非対称性を解消する、その概念をオンライン認証の世界でも実現しようというものなのです」

国を超えたサービス連携も可能に

では、トラストフレームワークの構築は、どのようなことを可能にするのだろうか。

「トラストフレームワークがきちんと構築できると、安全と利便性を両立しながら、さまざまなオンラインサービスの提供と利用が可能になります」と佐藤准教授。米国ではすでにオンライン上でのトラストフレームワークが運用され、サービスが拡充しつつあるという。米国でその仕組みを提供しているのがOpen Identity Exchange (OIX) ^{*1} という民間の非営利団体である。学認は、そのOIXから認定を受け、米国の国立衛生研究所、国立医学図書館、議会図書館などが提供するサービスに対しても、同じIDを用いたアクセスが可能となっている。

「これは学認が国際標準の信頼性を満たしていることを意味します」。OIXのボードメンバーでもある崎村氏は語る。「つまり基準さえ満たせば国を超え



佐藤 周行

東京大学
情報基盤センター
准教授
学認指定OIX LoA 1アセッサー

西村 健

国立情報学研究所
学術基盤課 学術認証推進室
特任研究員

たシームレスなサービス利用が実現できるわけです。また、それぞれのサービス提供者がそれぞれのユーザーと契約してIDを発行し、認証するという、非常に非効率的な運用の問題を解決するという点で、サービス提供側にも大きなメリットをもたらします」

ルールとツールの両輪で成り立つ

トラストフレームワークがきちんと運用されるためには、適切な運用基準 (ポリシー) を定めるとともに、その実現を支える技術が不可欠となる。その一つが「uApprove.jp」というソフトウェアである。開発に携わったNIIの西村健特任研究員は、その特徴を次のように語る。

ID連携が拓く可能性

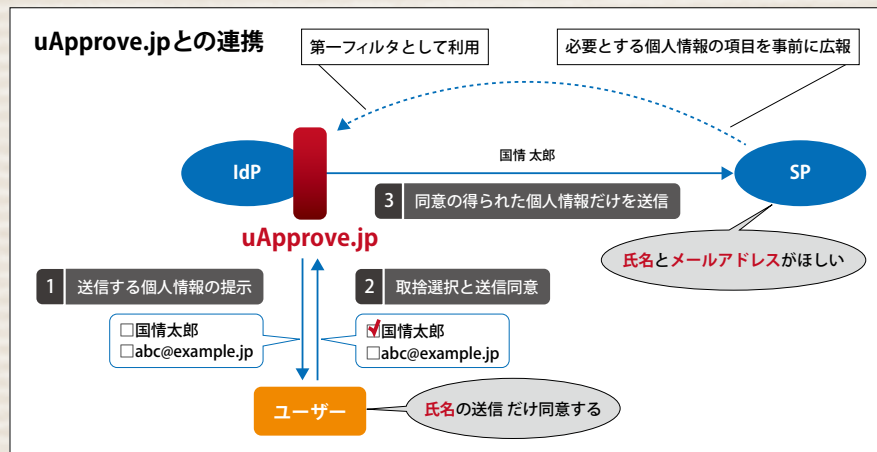


崎村 夏彦

株式会社 野村総合研究所
上席研究員
Open Identity Exchange 理事

「トラストフレームワークでは、ID発行・認証機関であるIdPが、ユーザーの有効な同意が得られた個人情報のみをSPに提供します。その機能を実現するのがuApprove.jpで、IdPが保持している個人情報のうち、SP側が必要とする項目に対してオンライン認証の際にユーザーから同意を取得し、個人情報をSP側に渡すという役割を担っています。どの情報を送るか送らないか、ユーザーが決められる機能も有します」

これについて崎村氏はこう解説する。「プライバシーに関するコンプライアンスが重要視されるようになり、各機関は様々な規則（ポリシー）を定めていますが、その実効性をuApprove.jpのようなツールを用いて保証することが重要です。このことに限らず、ID連携は、国際標準に則ったフォーマット、改ざん



IdP プラグインである uApprove.jp と連携することにより、送信が任意な属性を送信するかどうかを利用者が決めることができるようになる

や盗難から伝達中のデータを保護する技術、相手や中身が正しいか受け取る側が署名で検証する技術など、多様な技術によって成り立ちます。ルール（ポリシー）とツール（技術）、その両輪でトラストフレームワークは支えられているわけです」

産学のシームレスな ID連携で広がるサービス

適切なポリシーと先端的な情報技術によって実現されるトラストフレームワークにおいて、それ自体の信頼性の源泉となるのが、ID提供者の信頼性である。学認の場合は、ユーザーが学生や研究者であり、大学が身元を保証してIDを発行しているという点で、非常に信頼性が高いと言える。

「つまり、学認そのものがトラストフレームワークとして、大学だけでなく民間のSPにも認証の枠組みを提供する場となるのです。教育や研究だけでなく、学生の福利厚生にまで枠組みを広げることが可能になります。学認と一般的な商用サービスでは通信プロトコル^{※2}が

異なっているのですが、その間をつなぐゲートウェイ機能も開発しました。これにより、ユーザーは意識せずに学認のIDで民間SPのサービスを利用できるようになります」と佐藤准教授は期待を込める。

例えば、飛躍的に利便性が高まるのが学割サービスである。大学側がIDを保証していることにより、学生証のコピーを送るなどの面倒な手続きは必要なくなり、オンラインで簡単に学割サービスを受けることが可能になる。

学認というトラストフレームワークが産学のID連携を実現することによって、学術利用だけにとどまらず、広く社会をつなぐ基盤となる可能性が拓かれていく。セキュリティと利便性を高いレベルで両立する、未来の情報社会の姿がそこにはある。

（取材・文＝関亜希子）

※1 Open Identity Exchange (OIX)
米連邦政府向け認証フレームワークを提供する機関で、ID管理プロバイダーが連邦規格を満たすかどうか認証をする。

※2 通信プロトコル
ネットワークを介してコンピュータが通信を行ううえで、相互に決められた約束事のこと。認証に関する通信では、商用サービスの多くがOpenIDを使っているが、学認はSAMLを採用しており、認証のしくみが異なる。