政府関係機関事業紹介

学認が実現するオンラインサービスへのログインの進化形

国立情報学研究所　学術認証推進室

1．はじめに

前回の「UPKI電子証明書発行サービス」につづき、「学認」をご説明いたします。学認は、大学・研究機関等学術機関が運用する認証基盤を通じて機関外の商用のものを含めた各種オンラインサービスにログインするための仕組みです。いわゆるシングルサインオン（SSO）と呼ばれたりもしますが、SSOで利用者の利便性を向上させつつ安全性も向上させることができます。

2．シングルサインオン（SSO）とは

Google、MicrosoftなどのIT企業が一社でメールサービスやファイルストレージなど数多くのオンラインサービスを提供している例は少なくありません。この場合裏側の技術はともかく、サービスや機能ごとにパスワードを要求するのはユーザー体験として望ましくなく、パスワードの要求を少なくする努力が行われています。これが利用者視点でのシングルサインオン（Single Sign-On, SSO）と言えます。つまり利用者から見れば一度ID・パスワードを入力して本人であることを確認しているのだから同じブラウザ・環境を利用している限り同じ利用者であることは明白なので、別サービスへ遷移したとしても再度パスワードを要求しないということです。

特に同一事業者が各種サービスを提供する場合は、SSOは正常な進化の形であり、すでにそれが一般的になっているとも言えます。このSSOに慣れた利用者から見ればサービスが異なるとはいえそれぞれのサービスでログインが強制されるのは時代遅れと映るかもしれません。

では事業者をまたがったSSOは実現されるでしょうか？多くの人が他社のアカウントを指定してログインできるようにしているサービスを見たことがあるでしょう。しかし例えば一般のGoogleアカウントでそのままMicrosoft提供のOffice 365を利用できるようになるとは考えにくく、事業者主導のID管理・SSOではこの点で限界があると言えます。

技術的な話をしますと、SSO実現のため認証結果を受け渡すことを目的とする認証連携技術として主なものでSAML（サムル,Security Assertion Markup Language）およびOpenID Connectがあげられます。他にも表面的にSSOを実現する技術はありますが、上述のような認証連携技術を用いるのが安全でありメンテナンス性や汎用性など長期的に見て最も有利です。

3．SSOの先を行くフェデレーション

我々はSSOの一歩先を考えています。まず、ID・パスワードを管理するという役割を各大学・研究機関等が担うものとし、追加の役割を与えます。２節で示したグローバルなID管理ではどうしても小回りがきかず利用者が本当に必要とするサービスにSSOできないということになります。逆にどんなサービスでもSSOの対象とすると問題のあるサービスに利用者を誘導することになります。言い換えれば利用者に寄り添うよりきめ細やかなサポートが必要と考えます。

つまり、機関が責任を持ってSSOの範囲を定め後述の属性の管理も含めてこれをコントロールすることで、利用者である構成員が不用意にポリシーに抵触するサービスを利用しない、個人情報を提供しないよう制御します。

利用者保護と表裏一体として、限定したサービスを利用するよう誘導することでサービス利用のガバナンスを強化することができます。

この機関の役割をSAML用語でIdP（Identity Provider）と呼びます。一方IdPと連携し提供されるサービス全体、もしくは狭義にIdPと連携する部分をSAML用語でSP（Service Provider）と呼びます。

次に、利用者に関する情報である属性を扱います。例えば○○大学の構成員であることがサービス利用の条件である場合、学生であることが学割サービスを受ける条件である場合、など、所属機関であれば自然に保持している属性を必要な範囲

でサービスに受け渡すことで、サービス提供の可否の判断に役立てることができます。これはSSOよりさらに踏み込んだ連携と言えます。

フェデレーションは、乱暴な言い方をすればSSOの概念に加えてID管理を組織単位とし、利用者に属性を付与したものであると言えます。正確にはこれに規程（ポリシー）を加えそれを遵守するIdPおよびSPの連合体なのですが、詳しい説明は[1]に委ねます。

前述の通りSSOの範囲を定めるのはIdPの役割であるため、フェデレーションに参加しているSPであるというのは一つの判断基準ではありますが、最終的に各SPとSSOする、認証連携するかどうかの判断はIdPが行います。逆に、フェデレーションに参加していなくても機関として有用なSP、特に学内で提供されているSPのようなものがあれば、IdPの判断で連携対象として追加することが可能です。

ここで「それぞれの機関が利用サービスに制限を加えさらに独自のものを追加するなら利用者は把握が困難になるのではないか」と思われた方がいるかもしれません。ご安心ください、そのための仕組みをご用意しております。本誌2017年度No.４で紹介した「クラウドゲートウェイサービス」（現在のサービス名は学認クラウドゲートウェイサービス）をご参照ください。

４．日本におけるフェデレーション「学認」とインターフェデレーション「eduGAIN」

日本において学術向けのオンラインサービスを対象とした認証フェデレーション、すなわち利用する機関と提供する機関・事業者から構成された連合体が「学認」です。全国の大学・研究機関等学術機関とNIIが連携して、2009年に構築開始、2010年に「学認」という名称（当時は愛称）が与えられました。そして2014年にNIIの１事業となり現在に至ります。学認には2019年６月末時点で223の学術機関、商用／海外含め161のサービスが参加しています。

「日本で」と前置きしたように日本以外の国や地域でも学認と同様の学術認証フェデレーションが構築されています。さらにeduGAIN[3]という、インターフェデレーションの枠組みも存在します。eduGAINはフェデレーションを越えたIdPとSPの認証連携を可能にします。

５．学認に参加するメリット

表面的には、学認に参加しているサービスにSSOできるようになることがメリットです。これにはID管理の集約に伴うコスト削減や共通の安全な認証連携技術を用いることによる連携コストの削減、セキュリティ向上などが含まれます。ただし、有償サービスは個別に契約が必要であることにご注意ください。主に電子ジャーナルサイトは有償ですが、ｅラーニング、共同研究支援、学割サービス、就職情報サービスなど、すでに利用可能となっているサービスは多岐にわたり今後も増える見込みです。学認に参加しているサービスについて詳しくは[2]をご参照ください。さらに、学認に参加した上でeduGAINに参加していただければ、世界中の何千ものサービスにログインすることが可能になります。

もちろん、３節であげたフェデレーションのメリットを享受できます。さらに、近年増加しているSAML対応のクラウドサービスと独自に認証連携する道が開けます。

一方で、何らかのSAML実装、IdPを用意しなければ参加できないということがデメリットと言えるかもしれません。しかし近年はすぐに使えるアプライアンス製品やIdP機能を含めた認証基盤を運用含めお任せできるクラウドサービスIDaaS（アイダース）など、選択肢が広がっております。詳しくは事務局までご相談ください。

６．おわりに

本稿で紹介した「学認」へ参加いただくことで学認参加サービスとの連携・当該サービスへのログインが容易になることはもちろん、認証情報および属性情報を集中管理することでコスト集約・機関内情報基盤のセキュリティ水準の底上げ・サービス利用のガバナンス向上・利用者保護への足がかりにもなります。もし関心をお持ちいただけたら、ご質問ご相談などお気軽に学認事務局 gakunin-office@nii.ac.jp までご連絡ください。

参考文献および関連URL

[1] 西村健，中村素典，山地一禎，佐藤周行，大谷誠，岡部寿男，曽根原登，“多様なポリシーを反映可能な認証フェデレーション機構の実現，”電子情報通信学会論文誌 vol. J96-D no. 6 pp. 1400-1412，2013.
[2] 学認，IdP・SP一覧，https://www.gakunin.jp/participants/
[3] 学認，eduGAINに参加する，https://www.gakunin.jp/join/eduGAIN/