D6-5

日本における学術認証フェデレーション“学認”の展開

西村 健[†], 中村 素典[†], 山地 一禎[†], 大谷 誠[†], 岡部 寿男[††], 曽根原 登[†††]

[†]国立情報学研究所 学術ネットワーク研究開発センター
{takeshi,otani,motonori,yamaji}@nii.ac.jp
[††]京都大学 学術情報メディアセンター
okabe@i.kyoto-u.ac.jp
[†††]国立情報学研究所 情報社会相関研究系
sonehara@nii.ac.jp

概要：オンラインでの認証の重要性が高まる中で、大学等学術機関が提供する認証情報を各種学術サービスで利用可能にする枠組みである学術認証フェデレーション（学認）もまた重要性を増している。学認は、機関単位で契約している電子ジャーナル閲覧サービスに対する認証情報の提供を始めとして、大学を跨がる e ラーニングサービス提供や共同研究支援など様々なサービスに有効である。学認がサービス・機関にもたらすコスト削減等の効果を示す。

1 はじめに

ICT を利用した研究・教育およびその支援を目的としたサービスが急速に増加していく中、そこで必要となるオンラインでの認証もまた重要性を増している。すなわち、利用者が誰であるかを確実に識別した（=認証）上で、その利用者が利用可能なサービスやコンテンツがどれであるかを判断する（=認可）ことが、昨今の ICT を利用したサービスでは不可欠なものとなっている。これは学術サービスにおいても例外ではなく、益々数が増えてゆくサービスにおいて、各々が独自に認証・認可の機能を実装・運用することはコストの増大を招き、問題となる。

一方、学術機関の構成員にとって、研究・教育のために利用する学術サービスのそれぞれが独自の認証を要求することは、各サービスに対して独自の ID/パスワードを取得しなければならずその管理が煩雑になることを意味する。パスワードを共通にして煩雑さを避けることも考えられるが、それぞれのサービスでパスワードに使用できる文字種が異なり共通にできない場合があったり、それへの対処として共通の文字種を使用して推測が容易になってしまったり、1 つのサービスでのパスワードの漏洩が他の全てのサービスに対するリスクになったりと、セキュリティ上の問題となる。

このように、学術機関で ICT を推進していく上で課題となる認証の問題に対する解決策として、国立情報学研究所(NII)では、全国的な最先端学術情報基盤整備の一環として、学術認証フェデレーション「学認：GakuNin」の構築に取り組んでいる[1]。学認とは安全に認証情報を交換するためのフレームワークであり、かつ日本の大学等学術機関および、学術機関に限らないサービス提供者が参加する連合体である。

学認に参加する学術機関は機関の垣根を越えて認証情報を活用することができる。学認に参加するサービスは、独自に認証機能を実装しなくても、学術機関が提供する認証情報を利用することができる。つまり、従来サービスが個々に実装していた認証機能を、学術機関側に分離したととらえることができる。

また、学認に参加している学術機関の構成員は、同じく学認に参加するサービスの利用において、自分が所属する機関が提供する認証システムに対してのみ認証できれば良くなり多数の ID/パスワードの煩雑な管理から解放される。

本稿では、学認がどのようにして組織の異なるシステム間で安心・安全に認証情報を交換できるようにしているか、その取り組みについて紹介する。

2 認証の分離 ー 認証フェデレーションの構築

本稿では ICT を利用したサービスとは Web 上で実現された Web アプリケーションであるとする。

認証機能には、アカウントのライフサイクル管理として大きく以下のようなことが必要になる。

- ●パスワード登録など、特定の人に対してその人のみの秘密情報を結びつける
- ●異動などその人の情報（属性情報）が変化した場合に適切に更新する
- ●パスワードを忘れた場合の対応
- ●資格を失った場合に適切にアカウントを削除する

特に確実な認証が求められるサービスにおいてこれらを独自に実現するコストは大きく、学認では以下の仕組みを利用してこれらの機能を学術機関側に移している。ただし属性情報については、全てが学術機関に移されるわけではない。

上記のような目的を実現するプロトコルとして Security Assertion Markup Language (SAML)[2]という国際標準が策定されている。SAML では利用者を認証するシステム側を Identity Provider (IdP)、サービス提供側を Service Provider (SP)と定義して、認証情報および属性情報を IdP と SP の間で安全に送受信するためのプロトコルが定められている。このような仕組みを用いて認証情報の交換を行う組織の連合体を認証フェデレーションもしくは単にフェデレーションと呼び、InCommon[4]や SWITCHaai[5]をはじめとして世界各国で構築が進められている[6]。SAML を利用した IdP/SP の構築のために Shibboleth[7]というミドルウェアがオープンソースソフトウェアとして提供されており、機関やサービス提供者が容易に導入できるようになっている。

フェデレーションでは機関を確実に認証した上で参加承認を与えることが重要である。学認においては、書面による確認や SAML で用いられる証明書のチェックなどで実現している。また、IdP のアカウント管理の質も重要であり学認ではシステム運用基準という形で定めている。電子ジャーナル閲覧サービスのように商用サービスの提供もすでに行われており、IdP に関して一定の信頼を得ていることの証ともいえる。

3 学認による効果

この取り組みは 2008 年度の実証実験に端を発し 2010 年度から学認として本格運用を開始している。2011 年 10 月現在、学認に参加している 30 機関が認証情報を提供し、学認に参加しているサービスも 30 を数える。

学認では、参加している機関から活用事例のヒアリングを行いその内容をケーススタディという形で公開している[7]。この中でサービスのコスト削減等の効果を見ることができるのでいくつかここに引用する。

- 広島大学の事例

> 広島大学では、ネットワークの利用に際して利用者認証を実施している。そのため、学外者がネットワークを利用するにはゲスト ID が必要になるが、本学では学外者の認証に学術認証フェデレーションと連携する仕組みを導入して、ゲスト ID を不要とした。

- 佐賀大学の事例

> 従来、コンテンツを構築する場合、サービス部分に加えて認証部分もセットで開発する必要があった。しかし、今回の SSO 導入を機に認証機構部分が独立したため、今後開発する Web サービスは認証機能を実装する必要がなくなっている。そのため Web サービスの構築がより簡単になり、新たなアプローチやサービスの発見にも期待が高まっている。

このように、コスト削減だけでなくサービス・機関・利用者それぞれにメリットのあるサービス展開が学認を利用して実際に行われていることが分かる。

4 おわりに

NII が推進している学術認証フェデレーション“学認”により、ICT を利用した各種サービスのコスト削減、大学間連携を促進することが可能であることを示した。今後、認可支援によってサービスのさらなるコスト削減を目指すほか、安全性・利便性の向上を目指した様々な取り組みを行っていく予定である。

参考文献

[1] 学術認証フェデレーション：学認、http://www.gakunin.jp
[2] Security Assertion Markup Language (SAML) V2.0、http://saml.xml.org/saml-specifications
[3] Shibboleth、http://shibboleth.internet2.edu/
[4] InCommon、http://incommon.org/
[5] SWITCHaai、http://www.switch.ch/aai/
[6] REFEDS http://www.terena.org/activities/refeds/
[7] 学認活用事例集（ケーススタディ）、http://www.gakunin.jp/docs/fed/info