"uApprove.jp"を活用した金沢大学と大学コンソーシアム間の認証連携

藤田 翔也，松平 拓也，高田 良宏，笠原 禎也
金沢大学
fujita@cie.is.t.kanazawa-u.ac.jp

概要：近年、大学教育研究機関においても組織間のサービス共有を目的とし、認証連携を行う機運が高まっている。認証連携において、認証の際に送信される情報はユーザの個人情報であるため、シングルサインオン(SSO)環境下で他機関が提供するサービス利用時は、ユーザが選択し同意した情報のみが送られるべきである。しかし、そのような機構を持つ実用構築事例はまだ十分普及していない。本研究では、”uApprove.jp”を用い、実運用システムに同機構を導入するための検証を行い、実運用に汎用的に適用できることを確認した。本稿では、検証の詳細について述べるとともに、金沢大学と大学コンソーシアム間の認証連携への導入例を提案する。

1 序論

近年、大学教育研究機関においても組織間のサービス共有を目的とする認証連携を行う機運が高まっている。認証連携の方法として、システムの認証機構の統一や一度のログインで複数の独立したサービスを利用できるシングルサインオン（Single Sign-On:以下、SSO という）が普及しつつある。

こうした背景から、国立情報学研究所（以下、NII という）を中心として、安全かつ高い利便性を備えたトラストフレームワークの構築を目的に、学術認証フェデレーション（GakuNin:以下、学認という）[1]が作られた。学認は学術 e-リソースを利用・提供する大学や機関、出版社などで構成された連合体である。学認では、SSO 機能を有するミドルウェアとして Shibboleth[2]が使用されている。また学認では、運用フェデレーションとは別に、多くの大学や機関などが新しくフェデレーションに参加し認証連携を高めるために、テストフェデレーションと呼ばれる環境も提供されている。金沢大学（以下、本学という）も、Shibboleth を導入し、運用フェデレーションに参加している。

標準仕様の Shibboleth では、各サービスが認可を行うために必要とするユーザの情報は、認証サーバから各サービスに対してユーザには見えない形で送信される。これらの情報は個人情報を含むことがあるため、ユーザに対して送信する情報を事前に提示し、ユーザが選択し承認した情報のみを送信するべきである。しかし、このような機能を持たせたシステム構築事例はまだ普及していない。

本研究では、”uApprove.jp”[3]を用いて、実運用システムに同機構を導入するための検証を行い、実運用システムへ汎用的に適用できることを示すとともに、本学と大学コンソーシアム石川（以下、UCI という）[4]の認証連携への導入例を提案する。

2 Shibboleth 認証

学認が採用する Shibboleth を用いた SSO 機能による大学間認証連携システムの概念を図 1 に示す。ユーザは所属の機関の認証サーバを通

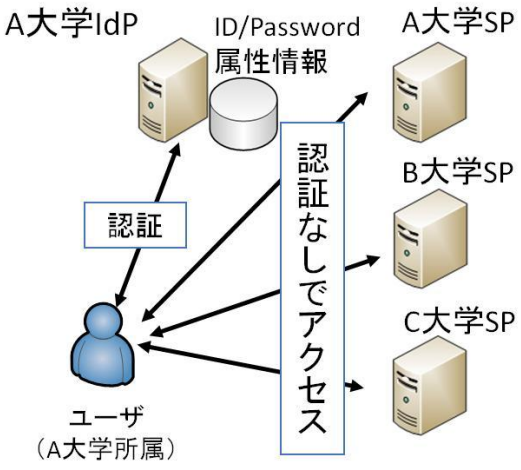

図 1 SSO システム概念図

して認証を行うことで、学認に参加するサービスサーバに対し、認証を再度行うことなくシームレスにアクセスすることができる。

Shibboleth は主に Identity Provider（以下、IdP という）、Service Provider（以下、SP という）、Discovery Service（以下、DS という）の 3 つのサーバで構成される。IdP は、大学などの組織単位で構成され、ユーザの認証を行うサーバである。また、IdP 自身はユーザの情報を持たず、LDAP などの認証基盤を参照し、特定の情報を抽出して SP へ送信する。SP は、ユーザに対して各種サービスを提供するサーバである。DS は、DS に登録されている組織の全 IdP のリストを提示し、ユーザに自分の所属する組織の IdP を選択させるサーバである。

Shibboleth の基本的な認証の流れは図 2 に示す通りである。本研究では、IdP と SP は本学に配置された仮想サーバ上に構築し、DS は NII が提供しているものを利用し、学認のテストフェデレーションで動作する環境を構築した。

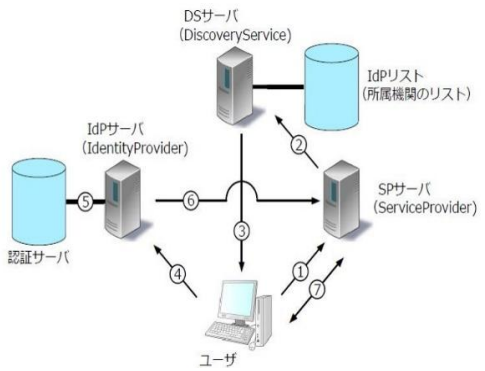

図 2 Shibboleth 認証手順

3 uApprove.jp の導入

3.1 uApprove.jp の概要

“uApprove.jp”は学認が提供する Shibboleth IdP のプラグイン機能で、SWITCH[5]で開発された”uApprove”をベースに、SP に送信する属性情報選択の機能などを加えたものである。

uApprove.jp の動作概念を図 3 に示す。図 3 を説明すると IdP が SP に対して認証済を通知すると、SP は必要な属性情報を IdP に対して要求する。このとき、IdP は SP が要求した属性情報を uApprove.jp によりユーザに提示し、ユーザにより、選択・承認された属性情報のみを SP に送信する。

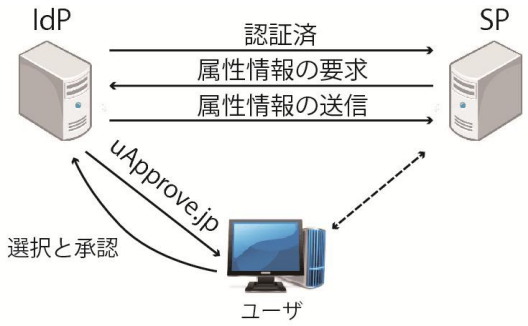

図 3 uApprove.jp の動作概念図

3.2 uApprove.jp の動作検証

本取組みではまず、uApprove.jp によりユーザの属性情報が可視化され、送出する情報は各 SP に対してユーザがそれぞれ独立に選択・承認できることを検証した。また、送付する属性情報の選択・承認は、ユーザの設定により次回以降の認証の際に省略可能とすることができ、省略設定のリセットを行うことで SP に送付する属性情報の選択・承認を再び行うことが可能であることも確認した。

動作検証した uApprove.jp の実際の画面遷移の様子を図 4 に示す。図の上部には、サービスを利用するために必須である属性情報が表示されている。図の真ん中には、サービスを利用する際のオプションとして、ユーザが送付の有無を任意に選べる属性情報が表示される。図の下部には、uApprove.jp の選択・承認手順を次回以降、省略するかどうかを選択するラジオボタンが表示される。また、属性情報にマウスポインタを合わせることで IdP からの属性情報に関する説明が表示され、属性情報の名前の最後にある”？”にマウスポインタを合わせることで、SP からのその属性情報の使用用途が表示され

る。

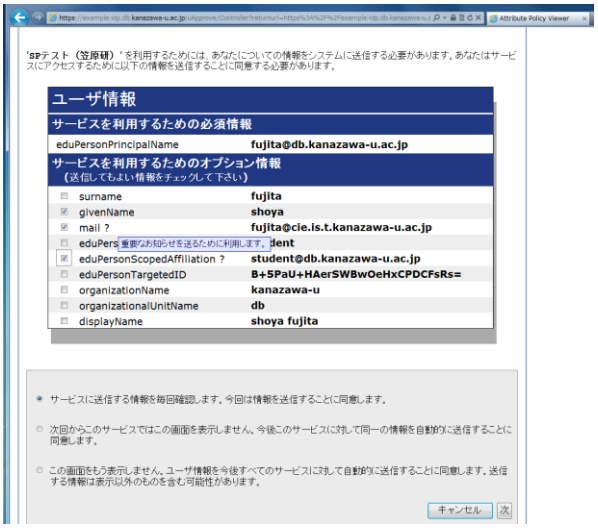

図 4 属性情報の提示と承認の画面遷移図

4 冗長化 IdP への uApprove.jp の適用

IdP は認証の要であり実運用システムへ適用するためには、冗長化は必須である。本学の IdP サーバは、Terracotta と呼ばれる Java クラスタリングソフトウェアを用いて冗長化を行っている。そのため、Terracotta により冗長化された IdP へ uApprove.jp を適用させるための方法について検討した。

uApprove.jp は必要な情報を MySQL に格納しているため、Terracotta では uApprove.jp を冗長化できない。そこで、MySQL のデータベースをマルチマスタスレーブ構成のレプリケーションとして構築することで、uApprove.jp の冗長化を行う方法を実装した。

動作検証の結果、Terracotta 及び MySQL のマルチマスタ構成によって、uApprove.jp の機能を有する IdP サーバを冗長構成で運用できることを確認した。また、負荷分散装置により各 IdP へアクセスを分散させることで、IdP サーバ 1 台への負荷を軽減することも可能である。提案する冗長化の構成は図 5 に示す通りである。

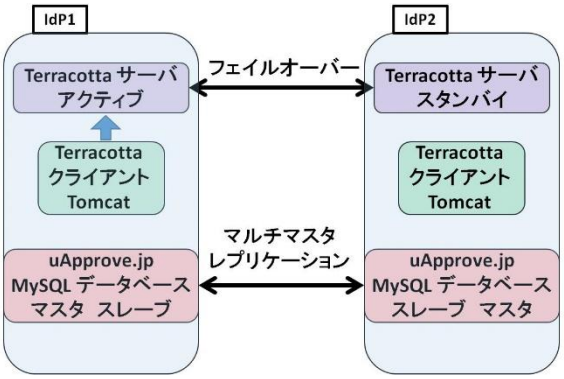

図 5 IdP 冗長化構成図

5 金沢大学と大学コンソーシアム間の認証連携

UCI は、石川県内の高等教育機関と自治体並びに関係団体で組織された連合体である。UCI の目的は、石川県内の機関が連携して、教育交流や情報発信を行うことで、それぞれの教育・活動の活性化をするとともに、その成果を地域に還元し、地域の発展に貢献することである。そのサービスの一つとして、石川県内の他大学の講義を受講できる仕組みを UCI ポータルとして提供している。本学では、UCI ポータルの運用と技術支援の中心的役割を果たしており、現在までに同サービスの Shibboleth 化を実現している。ただし、UCI ポータルは運用上の理由により、学認とは独立した環境下で運用されており各大学の学生・教職員などのユーザ認証も UCI が運用する IdP で行われている。このため、UCI ポータルが提供する各サービスを利用するには、各ユーザが自身の個人情報を UCI に届け出る必要がある。このような手続上の煩雑さから、UCI 提供のサービスは、学内サービスのようにシームレスに利用することが困難な状況にある。

このような問題を解決するため、本学の構成員が UCI ポータルを利用する際に、本学が運用する IdP サーバの認証でサービスを受けられるように整備を進めている。すでに、本学の学認用 IdP を利用した金沢大学 ID での認証までは

技術検証が進んでおり、次に本報告で検証を行った uApprove.jp の導入について検討が進んでいる。

uApprove.jp の導入により、金沢大学ユーザは、本学が発行した ID/Password を用いて認証を行えるだけでなく、上述した各種、個人情報は uApprove.jp を介して本人が承認をするだけで UCI 側に送付することが可能となる。すなわち、学内で保有する正しい個人情報を、本人の承諾を得て UCI 側に送付できるので、個人情報の登録ミスによる不整合も生じない。提案する本学と UCI の認証連携の概念を図 6 に示す。

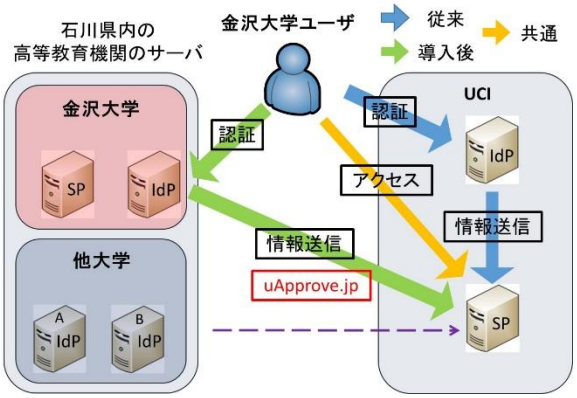

図 6 金沢大学と UCI の認証連携の概念図

図 6 を説明すると、従来では、すべてのユーザが UCI の IdP を利用し、認証を行っているが、uApprove.jp 導入後、本学の UCI ユーザは、本学の IdP により認証を行いユーザの情報が SP へ送信され、アクセスできるようになる。さらにこれを拡張して、点線で示すように、他大学のユーザも自分の所属する大学で認証を行うことができるようになれば、UCI は IdP を管理せずに済むようになり負担が軽減される。

6 結論

本研究では、SSO 環境下において、ユーザが自身の属性情報の送付に対する選択と承認機能を有する認証機構を実運用に導入するための検証を行った。”uApprove.jp”の有用性について検討するとともに、IdP サーバを冗長化し uApprove.jp を適用させることで、同機構を実運用システムへ導入可能であることを示した。

さらに、本学と UCI の認証連携の導入例を提案した。現在導入を進めており、ユーザがより利用しやすいサービスとなることが期待される。

参考文献

[1] 学術認証フェデレーション https://www.gakunin.jp (accessed 2013.10)

[2] Shibboleth, http://shibboleth.net/ (accessed 2013.10)

[3] uApprove.jp https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=13501031 (accessed 2013.10)

[4] 大学コンソーシアム石川 http://www.ucon-i.jp/ (accessed 2013.10)

[5] SWITCH, http://www.switch.ch/ (accessed 2013.10)