情報処理学会論文誌 Vol. 52 No. 2 703–713 (Feb. 2011)

大学におけるShibbolethを利用した統合認証基盤の構築

松平拓也[†1] 笠原禎也[†1] 高田良宏[†1]
東昭孝[†1] 二木恵[†1] 森祥寛[†1]

本稿では，これまで部局別に構築・運用されてきた情報システムを統合化することを目的に，統合認証基盤と各種情報サービスを一元的に利用できるポータルシステムの構築を行った．大学の構成員の多様性を考慮し，全学の情報システムに共通で利用できるIDを導入し，各システムの認証部分の共通化を行った．また，Shibbolethを用いた統合認証機構を実現し，各情報システムの利用権限については，情報システム間でユーザの属性情報を共有することにより，複数ロールを持つユーザに対しても1つのIDで，柔軟に対応できるシステムを構築した．最後に，構築した統合認証システムを金沢大学の実用システムとして実際に運用を行い，提案システムが実用レベルで十分機能することを実証した．本稿では，大学における統合認証システムの設計，構築，評価について述べ，今後の拡張についても考察する．

Integrated Authentication Infrastructure in University Based on the Shibboleth System

Takuya Matsuhira,[†1] Yoshiya Kasahara,[†1]
Yoshihiro Takata,[†1] Akitaka Higashi,[†1]
Megumi Futatsugi[†1] and Yoshihiro Mori[†1]

We constructed an infrastructure for a single-sign-on system and portal server which are applicable to the service systems in a university. Firstly we introduced a lifelong ID which is commonly used for information systems constructed in our university. Secondly we developed an authentication and authorization system using shibboleth which is an open source software package applicable for web single sign-on across or within several organizations. We improved some usages of shibboleth in order to apply it under the condition that each user has only one ID and password even though he/she has several kinds of roles. Finally we demonstrated that the proposed system can be successfully operated in Kanazawa University. In the present paper, we introduce the configuration of our proposed systems and discuss the prospects of technical solutions.

1. はじめに

インターネット技術の急速な発展にともない，多くの大学では，教育・研究・業務など様々な分野において情報システム化を進めてきた．しかし，構築した情報システムの大多数が，各部署・部局などで独自に構築・運用されてきた．必然的にこれらの情報システムは，それぞれ独自の認証機構を備え，ユーザに対して個別のIDとパスワードが発行されることとなる．そのため，大学のいたるところで情報システムが乱立し，たとえ個々の情報システムとしては機能しても，それらの公開方法や利用範囲に一貫性がなく，システム間の連携も考慮されていないのが実情である．このような環境では，ユーザは，目的の情報システムのURLを自身で管理したり，情報システムごとのIDとパスワードの対を覚えておく必要があったりと，作業効率の低下だけでなく，IDとパスワードの対をメモに残すなど，セキュリティの観点でも問題があった．また，情報システムの運用においても，情報システムごとに独自の認証機構を持つことは，人員の異動にともなう内部データ変更作業や認証機構の維持管理など，コストの増大を招いてきた．そのため，大学の情報基盤整備における次のフェーズとして，“情報化の推進”としてのICTインフラの整備にとどまらず，その上にたって行われる教育・研究・業務に必要な情報を効率良く利活用できる“より上位レベルの情報基盤整備”が重要になってきている．

このような背景のもと，我々は，全学的な視野で情報化を戦略的に整備・推進することを目的として，全学の情報システムを一元的に利用する窓口であるポータルサイトおよびユーザ認証を一元的に行う統合認証システムを構築した．全学におけるイニシアティブをとるために，全学的な情報基盤整備をミッションとする金沢大学情報戦略本部[1)]の傘下で“全学ポータルWG”という活動形態をとることでこの取り組みを実施した．

各所に分散する情報システムの一元化・融合化に必要な要素技術として，1度の認証でユーザに許可された情報システムをすべて利用可能とするシングルサインオン，およびユーザの属性情報を複数の情報システム間で安全に共有する属性共有がある．先行事例として，名古屋大学ではCentral Authentication Service[2)]を拡張したCentral Authentication and

†1 金沢大学
Kanazawa University

Authorization Service を独自に開発し，シングルサインオン環境を実現している[3),4)]．また，大阪大学では Public Key Infrastructure 技術を用いて全学 IT 認証基盤を構築している[5)]．しかし，報告事例はいずれもシンプルなシングルサインオンと最低限の属性共有の実装である．これに対し，大学で構築されている情報システムは，教育・研究・業務など，その目的が多岐にわたることから，当然，それぞれ利用できるユーザの範囲が異なり，また，システムによって運用ポリシも異なる．そのため，大学特有の複雑な所属形態にすべて適合するシステムを構築するのは容易ではない．たとえば，大学から給与が支給されるティーチングアシスタント（TA）やリサーチアシスタント（RA）として業務を担う学生や，大学職員でありながら，その大学の社会人学生でもある場合などは，それぞれの属性に応じて個々の情報システムへの認証・認可権限の設定が必要となり，多くの場合，複数の ID とパスワードを配布する結果に至る．これは，ユーザを人ではなく現在有効な職分などの属性で判断していることに起因する．これに対し，我々は，ユーザが複数の属性を持つ場合でも 1 つの ID とパスワードのみで認証・認可の制御ができる機構の実現を目指した．

一方，現在，国立情報学研究所（以下，NII と記載）が中心となり，複数の大学間での情報システムの共有，相互乗り入れの実現を目指して，UPKI プロジェクト[6)]が進められている．本プロジェクトは，個々の大学が保有する教育研究用計算機，電子コンテンツ，ネットワークなどの学術情報資源を，大学間で安全・安心に有効活用可能とするもので，今後，その必要性はますます高まると予想される．本プロジェクトの大学間認証連携には Shibboleth[7)] と呼ばれるオープンソースソフトウェアが用いられている．同プロジェクトの試みにより，大学間連携におけるシングルサインオンの環境は整備されつつある．また，佐賀大学では本プロジェクトとは別に，Opengate と呼ばれる佐賀大学内の認証システムにおいて，Shibboleth を用いてシングルサインオン環境を実現している[8)]．しかし，大学間認証連携および佐賀大学においてはシングルサインオンに関する議論が中心となっており，ユーザの属性に応じた細かな制御についてはこれからである．

我々は，これまで UPKI プロジェクトに積極的に参加し，Shibboleth に関するノウハウを蓄積してきた[9)]．そこで，先行事例や大学間連携などの現況をふまえ，Shibboleth を用いてシングルサインオンによるユーザの認証を行うと同時に，教員・職員・学生など各自の職分も識別でき，その職分に応じて利用許可されている情報システムが，再度の認証動作なしに利用可能になる統合認証システムの構築を行った．

本稿では，2 章で金沢大学（以下，本学と記載）の情報システム一元化の指針について説明し，3 章で Shibboleth の概要と問題点について議論する．続いて，4 章でその解決策について述べ，5 章で実装について述べる．6 章で構築したシステムの評価を行い，最後に成果と今後の計画について考察する．

2. 情報システム一元化の指針

本章では本学における情報システム一元化に向けた統合認証基盤構築の指針について述べる．特に「金沢大学 ID」，「ロール」，「アカンサスポータル」，「シングルサインオン対象システム」について以降順番に説明を行う．

2.1 金沢大学 ID

1 章で述べたとおり，本学では従来，情報サービスの整備は部局別・目的別に独立して行われてきたため，各情報システムが独自に ID を発行し，その認証方式も様々であった．そのため，認証システムの統一，すなわちシングルサインオンを実現するためには ID の集約を行う必要がある．

まず，学内の様々な各種システムについて，その利便性と管理効率向上を図るために，“金沢大学 ID” を導入した．金沢大学 ID は，常勤教職員・非常勤教職員，学生・研究生などを問わず，本学に関わる全構成員に対して 1 人に 1 つずつ付与する ID である．金沢大学 ID の採番方法については，金沢大学 ID の検討段階ですでに全学規模で運用を行っていた名古屋大学の名古屋大学 ID[10)] の方式を採用した．金沢大学 ID の基本的な付け方として，ランダムに与えたアルファベット 3 桁と数字 5 桁の 8 桁とし，容易に推測できないようにしている．また，転学類にともなう学籍番号変更や，卒業後に本学に就職した場合などの属性の変更によらず，同一 ID を使用できる．そして，生涯 ID として，卒業・退職後も ID を抹消されることなく，同一 ID で同窓会向けサービスなど，本学 OB としての情報サービスを受け続けることができる．

教職員番号や学籍番号のように，1 度付与されたら変更ができないものを ID とせず，金沢大学 ID に置き換えることにより，1 ユーザ 1 ID を実現できるように設計を行った．金沢大学 ID は 2 年前から，後述の教育用ポータルシステム（アカンサスポータル）で限定的に利用されていたが，全学的な情報システムの一元化および統合認証に用いる “生涯 ID” として同 ID の本格導入を決定した．なお，金沢大学 ID は 2010 年 5 月 7 日現在，44,158 件発行を行っている．

2.2 ロ　ー　ル

大学には多種多様の情報システムが存在し，それらを使用できるユーザは，システムにより様々である．たとえば，給与明細オンラインシステムは大学から給与が支給される教職員

や TA・RA が対象であり，履修登録システムは講義を受ける学生が対象となる．そのため，各情報システムは，ユーザの職分などの属性情報から，ユーザが当該システムを利用できるかどうかを判断する必要がある．そのため，我々は，ユーザの属性を “ロール” という名称で定義し，それぞれの情報システムで必要とされる区分分けを行った．学生は，在学中や既卒など 4 パターン，教員は，常勤や博士研究員など 7 パターン，職員は，常勤や派遣職員など 10 パターン，その他，一般公開講座受講生や医師など 12 パターンを設定し，予備も含め全部で 55 パターンに区分した．ユーザが複数のロールを持つ例として，本学の学部を卒業し，博士前期課程を修了した後に本学の職員になった場合は，学生（学部既卒），学生（修士既卒），職員（常勤）という 3 つのロールが与えられる．また，本学の職員に採用後に，本学の博士後期課程に社会人入学した場合は，職員（常勤）と学生（博士在学）の 2 つのロールを持つ．

このように，ロールを詳細に定義することで，情報システムがユーザの利用可否をコントロールできるように設計を行った．ただし，複数のロールを持つユーザであっても，金沢大学 ID は 1 つとなるように留意した．

2.3　アカンサスポータル

アカンサスポータルは平成 18 年度入学生からの携帯パソコンの必携化に合わせて導入された全学共通教育用の学習管理システム（LMS; Learning Management System）から出発し，毎年改良を重ね，時間割表示，成績照会，図書館サービス，メッセージ機能，コミュニケーションサイト（SNS; Social Network Service），スケジューラなど学生生活にはなくてはならない本学の教育用ポータルサイトである[11]．

本研究においても，大学全体の情報システムの一元的な窓口として，ポータルサイトが必要となるが，複数のポータルサイトを学内に立ち上げるのは本来の趣旨に反するうえ，時間的・コスト的にも無駄なため，既存のアカンサスポータルに改良を加え，同ポータルシステムの掌握範囲を教職員の教育・研究・業務・社会貢献など様々な分野へ拡張することとした．統一認証のキーはもちろん前述の金沢大学 ID である．

ただし，統合認証を用いた情報システムの一元化を実現するため，これまでアカンサスポータルと教育系の情報システム間で独自仕様の連携を行っていた部分を分離し，アカンサスポータル自身も 1 つの情報システムとして扱えるようにした．すなわち，アカンサスポータルをすべての情報システムの入り口とする一方，ユーザ認証は今回開発した統合認証システムで金沢大学 ID による認証を行うことで，ロールに応じて利用可能な情報システムをポータルから選択できるように設計した．

2.4　シングルサインオン対象システム

本節では，今回シングルサインオンの対象にしたシステムについて述べる．まず，2.3 節で説明したように，従来のアカンサスポータルと独自仕様で連携を行っていた以下の教育系システムをシングルサインオン対象システムとした．

- WebClass（ウェブクラス社の LMS）
- 教務システム
- Web シラバス
- SNS（OpenPNE[12] を用いたコミュニティーサイト）
- NALIS（NTT データ九州社の大学図書館の各種業務を支援するシステム）

次に，教育系以外の情報システムとして，以下を新規に対象とした．

- 給与明細オンラインシステム
- サイボウズ（サイボウズ株式会社のグループウェア）
- マイクロソフト配布サーバ（Windows 系 OS および Office を教職員に配布）
- ファイル共有アプリケーション（大容量ファイルを JavaApplet で共有）
- ファイル送信サービス（大容量ファイルをメールで共有）

シングルサインオンの仕組みは，1 章で紹介した Shibboleth と呼ばれるオープンソースソフトウェアを採用した．なお，Shibboleth の詳細および導入にあたって克服すべき問題点は次章で述べる．

3.　Shibboleth

本研究では，Shibboleth を用いてシングルサインオンおよび属性共有を実現した．Shibboleth を採用した理由は，Shibboleth は Apache や IIS などのミドルウェアと連携して動作するため，情報システムのアプリケーション部分の修正が最小限で済むことがある．また，属性についてはサーバ環境変数で取得可能なため，情報システム間での属性共有が行いやすいという利点もある．また，UPKI プロジェクトに代表される将来的な大学間連携を見据えていることも選定した理由として大きい．本章では，まず Shibboleth の概要を述べ，2 章で説明した情報システム一元化の達成に必要な Shibboleth の問題点を指摘する．

3.1　Shibboleth 概要

Shibboleth は，Internet2 の Middleware Architecture Committee for Education プロジェクト[13] の 1 つで，SAML2.0[14] をベースとした，異なる情報システム間でのシングルサインオンおよび属性共有を実現するオープンソースソフトウェアである．SAML とは，XML

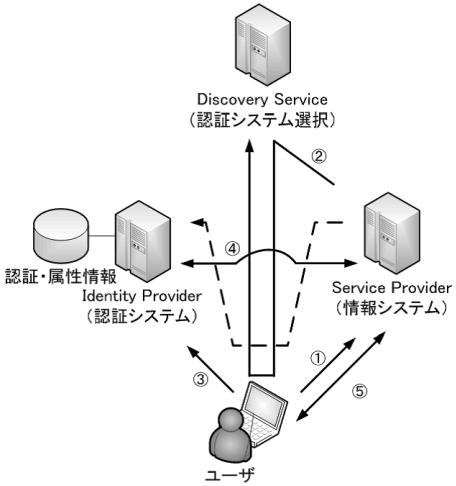

図 1　Shibboleth 動作概念図
Fig. 1　Conceptual image of Shibboleth.

を基盤にした，異なる Web サービス間での認証情報，属性情報，認可情報を交換するための標準の仕様である．Shibboleth では，Identity Provider（以下，IdP と記載），Service Provider（以下，SP と記載），Discovery Service（以下，DS と記載）の 3 つで構成される．

図 1 に Shibboleth の動作概念図を示し，それぞれの役割をあわせて述べる．ユーザは SP にアクセスを試みる（①）．SP はユーザの認証を促すために，DS にリダイレクトを行い，ユーザに IdP を選択させる（②）．DS は複数の IdP が存在する場合に，ユーザが適切な IdP を選択するための情報を提供する役割を持つ．そのため，あらかじめ SP で認証を行う IdP が決まっている場合は点線のように DS を経由せず，直接 IdP にリダイレクトする．IdP は ID/パスワード認証やクライアント証明書認証などの方法でユーザの認証を行う（③）．IdP は SP に認証結果を返し，成功の結果を受け取った場合に，SP は必要な属性を IdP に要求し，その返却値を SP のアプリケーションに渡す（④）．SP はその情報を基に，ユーザの属性に応じたサービスを提供する（⑤）．

3.2　Shibboleth 利用における問題

3.1 節の Shibboleth の概念で本学のシステム構成を考えた場合，本学統合認証サーバとして IdP を新規に構築し，2.4 節で示した各種システムを SP として動作させることで，シングルサインオンおよび属性共有の実現が可能となる．しかし，2 章で述べた指針を実現するには，以下に述べる 3 つの問題をクリアする必要がある．

（ア）複数ロールへの対応

Shibboleth では，3.1 節で説明したように，IdP から SP に対して必要な属性を渡す．ただし，複数ロールを持つユーザにも対応できるようにするには，属性の受け渡しにおいて，複数ロールに対応した属性判断ができる機能が必要である．

（イ）シングルログアウト

Shibboleth はシングルログアウトに対応していないため，共用端末などでブラウザを閉じ忘れた場合は，不正に利用される危険性がある．そのため，シングルログアウトを行う手段を考える必要がある．

（ウ）IdP の冗長化

IdP はすべての SP の認証に用いられるため，多数のユーザが日常的に使用する環境に耐える状態にするには，1 台が故障した場合でもサービスが提供できるように複数台用意し，冗長化を行う必要がある．ただし，そのためには，複数の IdP 間でセッション情報を共有する必要がある．

次章で，Shibboleth におけるこれらの問題について，我々が解決した方法について述べる．

4. 設　　計

本章では，3.2 節で述べた Shibboleth 利用における問題に対する解決方法について説明する．

4.1　複数ロールへの対応

Shibboleth では，認証のための情報および属性情報の管理を行う方法がいくつか存在するが，我々は，その中で LDAP を選択して構築を行った．LDAP には OpenLDAP [15] を選定した．その理由は，OpenLDAP はオープンソースソフトウェアであるため安価に構築できることと，Web 検索において，Shibboleth との連携に関する実績が一番多かったことがあげられる．ただし，2.2 節で述べたとおり，複数ロールを多くのユーザが持つことを前提に，LDAP の設計を行う必要がある．

LDAP のスキーマを作成するにあたり，我々は Shibboleth の属性値の返却方法に着目した．Shibboleth では，IdP が属性値を SP に対して送信し，SP のアプリケーションがサーバ環境変数として受け取る際には，セミコロン（;）で区切って 1 行の文字列として受け取

ベース(抜粋)	
金沢大学ID	abc12345
氏名	金沢　太郎
生年月日	19840101
ロール（抜粋）	
金沢大学ID	abc12345；abc12345;abc12345
ロール番号	1;1;10
個人番号	0312345678;0734567890;12345678
所属名１	工学部;工学研究科;企画部
所属名２	情報工学科;電子情報システム専攻;情報戦略課
所属名３	情報システムコース;通信ネットワーク系；情報推進係
職名	@;@;係長

図 2　複数ロールにおける属性値例
Fig. 2　An example of attribute definition for plural role.

る．そこで，すべてのロールで同じ LDAP スキーマを使用することで，ユーザはロール数分の LDAP レコードを持つことから，セミコロンでつながったそれぞれの属性値が，どのロールの属性値かをその順番から判断することとした．

前述のとおり，ロールの数はユーザによって大きく異なるので（1〜10 個程度を想定），LDAP スキーマは，各ロールで共通なデータを持つベース部分を 1 つ，ロールごとに 1 つずつ持つロール部分と分離させ，ロール部の個数を可変とし，複数ロールに対応しつつ，データの無駄な重複を防ぐ設計とした．

例として，本学工学部情報工学科情報システムコースを卒業し，本学工学研究科電子情報システム専攻通信ネットワーク系を修了し，本学に就職し，企画部情報戦略課情報推進係に所属した場合に，どのように属性値が送られるかを**図 2** に示す．このように，ベース部分は氏名や生年月日などロールで共通なものが格納されている．そして，ロール部分については，このように，セミコロンを縦に見ることで，セミコロンの各属性値がどのロールのものかをアプリケーションが容易に判断できるように環境変数として送信されてきているのが分かる．ただし，Shibboleth では，属性値が同一の値であった場合は値をマージしてしまうという特性を持っている．そこで，我々は IdP でこの動作を行っているソース部分を改変し，同一値をとる場合でも値をマージしないように修正した．さらに，Shibboleth では属性値が空白の場合は前詰めを行う部分を，値が空白のときはアットマーク（@）を属性値にセットするように改変した．このような改変を加えることで，複数ロールを持つユーザが存在する環境下でも Shibboleth で対応を行うことができるように構築を行った．

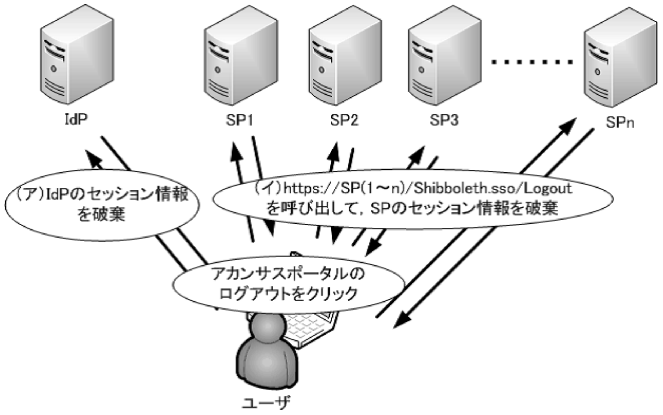

図 3　シングルログアウト概念図
Fig. 3　Conceptual image of single logout procedure.

4.2　シングルログアウト

Shibboleth を利用することで，ユーザは IdP で 1 度認証を行えば，他の情報システムにアクセスした場合でも再度認証を行う必要がなくなる．一方で，ログアウトを行った際にはすべての情報システムでログアウトを行う “シングルログアウト” の機能が必要である．しかし，SAML2.0 ではシングルログアウトの仕様が策定されているが，Shibboleth にはまだ反映されていない．そのため，我々は，すべての情報システムの窓口であるアカンサスポータルにログアウト機能を配置し，アカンサスポータルのログアウトを実行することで他のすべての SP からログアウトを行うシングルログアウト機能を構築した．

まず IdP に対してログアウト処理を行い，そのあと順番にすべての SP に対してログアウト処理を行うことでシングルログアウトを実現している．**図 3** にシングルログアウトの概念図を示すとともに，以下に IdP，SP それぞれのログアウト方法を記載する．

（ア）　IdP のログアウト方法

IdP においては，バージョン 2.1.5 ではログアウト機能は実装されていない．そこで，ユーザ側での IdP セッション管理方法を利用して，セッション情報を破棄するスクリプトを実行することで IdP のログアウトを実現した．具体的には，ユーザのブラウザ上では IdP とのセッション情報は Cookie で管理されているため，該当する Cookie と同じ変数名の Cookie を新規に生成し，その値を空にセットしてユーザのブラウザへ送信する．そうすることで，

IdP とユーザ間のセッションはリセットするため，IdP からのログアウトが完了する．

（イ） SP のログアウト方法

IdP でログアウトが完了しても，すでにログインされた SP については，セッションがタイムアウトになるまで IdP に再度問合せを行わないため，ログインが可能な状態になっている．そのため，それぞれの SP においてもログアウト処理を行う必要がある．我々は，それぞれの SP 単体でのログアウトは実装され，

https://SP サーバ名/Shibboleth.sso/Logout

にアクセスすることでユーザのブラウザとのセッションが破棄されることに着目し，上記 URL をすべての SP から呼び出すことで，全 SP からのログアウトを実現した．

（ア），（イ）の動作を一連の流れで動作するようにスクリプトに実装し，シングルログアウトを実現した．

4.3 IdP のクラスタ化

IdP はすべての SP の認証に用いられるため，認証システムの要として位置づけられる．そのため，サーバは 1 台で運用するのではなく，複数台用意し冗長化を図る必要がある．しかし，IdP は SP とのセッション情報を管理しているため，単純に負荷分散装置で管理することはできない．

そのため，Internet2 では IdP のクラスタ化を行う方法として，Terracotta[16] の使用を推奨している．Terracotta は複数の JavaVM 上で同じ Java オブジェクトを共用できるオープンソースのミドルウェアである．Terracotta を用いることで，複数の IdP 間でセッションの共有を行うことが可能になる．本学では，クライアントの IP アドレス単位でロードバランシングを行い，Terracotta でセッション情報の共有を行うように設計を行った．また，Terracotta のパフォーマンスチューニングとして，Internet2 が推奨する JavaVM メモリのセッティングを行った[17]．

負荷分散装置において，クライアント IP 単位で負荷分散を行う設定にしておくことで，IdP の冗長化を実現した．

5. 実　　装

本章では，本学における統合認証環境のシステム構成について説明するとともに，認証・認可を行うためのユーザ情報の管理について述べる．さらに，ユーザの統合認証の流れについても説明する．

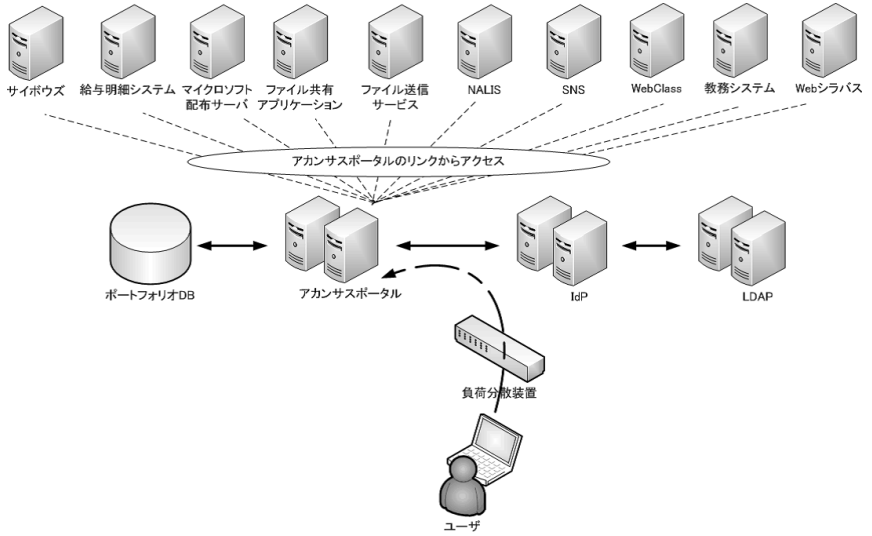

図 4　本学における統合認証システムおよびポータルシステム概要
Fig. 4　Outline of the integrated systems constructed in Kanazawa University.

5.1 全体システム構成

本学に構築したシステムの概要を**図 4** に示す．図中にあるポートフォリオ DB は，アカンサスポータルが参照するユーザデータの集まりである．アカンサスポータルサーバ（SP），IdP サーバ，LDAP サーバはそれぞれ 2 台ずつ用意し，冗長化を行うとともに，負荷分散を行っている．それぞれのサーバのスペックなど基本情報を**表 1** に示す．また，負荷分散装置には，Fujitsu 社 IPCOM BX1200LB を用い，アカンサスポータル，IdP，LDAP へのアクセスは必ず，負荷分散装置を経由するように設計し，アクセス単位はクライアント IP アドレスによるノード単位で負荷分散を行うように構築した．

2.4 節で述べたシングルサインオン対象システムは，アカンサスポータルと同様に SP として動作するように実装を行った．各 SP は，IdP から送信される複数ロール情報をセミコロンで区切り，配列に格納させることで，ユーザに対して，ロールに対応したサービスを提供できるようにした．そして図 4 に示すとおり，すべての SP へはアカンサスポータルのリンクからたどるように実装を行った．ユーザはアカンサスポータルにログインする必要があるため，シングルログアウト機構をアカンサスポータル内に配置することで，シングルログ

表 1　サーバ構成
Table 1　A list of server specification.

用途	サーバ諸元	OS	ミドルウェア
IdP	Fujitsu PRIMERGY BX620 CPU: Xeon X5570 (2.93GHz/8MB)×2 Memory: 8GB HDD: 300GB(2.5inch SAS 10000rpm (RAID1))	Red Hat Enterprise Linux 5.4(x64)	ShibbolethIdP2.1.5 Apache2.2.3 Jdk1.6.0update17 Tomcat6.0.20 Ant1.7.0 Terracotta3.1.1
SP (ポータル)	Fujitsu PRIMERGY BX620 CPU: Xeon X5570 (2.93GHz/8MB)×2 Memory: 8GB HDD: 300GB(2.5inch SAS 10000rpm (RAID1))	Red Hat Enterprise Linux 5.4(x64)	ShibbolethSP2.3.1 Apache2.2.14
LDAP	Fujitsu PRIMERGY BX620 CPU: Xeon X5570 (2.93GHz/8MB)×2 Memory: 8GB HDD: 147GB(2.5inch SAS 10000rpm (RAID1))	Red Hat Enterprise Linux 5.4(x64)	OpenLDAP2.4.19

アウトの問題を解決した．また，IdP においては，Terracotta を用いて 2 台の IdP 間でセッション共有を行い，負荷分散装置経由でアクセスすることで IdP クラスタ化を実現した．

5.2　ユーザ情報の管理

本節では，ユーザにおける認証情報および属性情報の LDAP への反映方法について述べる．教職員および学生に関する情報は，人事システムおよび教務システムから取得を行う．人事システムおよび教務システムから取得した情報は，アカンサスポータルを経由して SOAP（Simple Object Access Protocol）通信により LDAP に反映される．アカンサスポータルでは，新規に取得した情報とすでに LDAP に登録されている情報の比較を行う．LDAP に存在しないユーザは「新規」，両方に情報が存在し情報に差異が見られるユーザは「変更」，新規データ内に情報が存在しないユーザは「退職」となる．なお，「退職」になっても，ロールが変更になるだけで，ユーザ情報の削除は行わない．また，派遣職員や共同研究会社社員など人事システムおよび教務システムのどちらにもユーザ情報が存在しない場合は，アカンサスポータルに配置したユーザ管理画面で登録および変更を行う．

5.3　統合認証の流れ

ユーザは，アカンサスポータルにアクセスすると，IdP にリダイレクトされ，**図 5** に示す統合認証画面において認証を行う．認証に成功したのち，アカンサスポータルには，IdP からユーザの基本情報およびロール情報が送信され，その情報を基に自分が与えられたロール

図 5　認証画面
Fig. 5　Authentication page.

でログインを行う．ユーザは，自分が現在所属しているロールを選択することが可能で，アカンサスポータルは，ユーザが選択したロールに応じて利用可能な情報システムを提示する．そしてユーザは，アカンサスポータルを経由して利用したい情報システムにアクセスするという手順をとる．ユーザはアカンサスポータルから他の情報システムにアクセスを行っているように感じるが，アカンサスポータルもその他の情報システムと同様に，Shibboleth SP として構築を行っているため，実際は Shibboleth によるシングルサインオンを行っていることになる．すなわち，ユーザが直接各情報システムにアクセスをした場合も，認証前であれば統合認証画面が表示され，1 度でも認証された後であれば直接その SP のサービスを受けられることになる．SP では，IdP から送信されてきた属性情報を基に，ユーザの利用制限を行う．ユーザが複数のロールを持っていた場合は，アプリケーションサイドでセミコロンを分割し，属性値を確認するように構築を行っている．4.1 節で説明したように LDAP スキーマを設計したことにより，アプリケーションサイドでの作業は最小限にとどまる工夫がなされている．

このように，ユーザは情報システムへの窓口がアカンサスポータルで統一化されるとともに，金沢大学 ID で 1 度認証を行えば，傘下のサービスが一元的に利用できる環境が実現した．

6. 評　　価

本章では，5 章で説明した本学における統合認証環境の運用実績について述べる．

5 章で述べた統合認証環境は平成 22 年 3 月 22 日から本格稼働を開始した．**図 6** に平成 22 年 4 月 1 日から 4 月 30 日の 1 カ月間の IdP での認証数の推移を示す．4 月は学生の履修登録や，全入学生対象の情報処理基礎の講義があり，アカンサスポータルを経由しての LMS の利用が多いため，1 年で最もアクセスが集中する月である．7 日の入学宣誓式の日に各学類によるオリエンテーションがあり，その際にアカンサスポータルの説明があったため，認証数が 5,100 回とアクセス数が前後の日よりも多い．また，12 日の前期授業開始から認証数が増加して推移しているのが分かる．そして，IdP での認証は 21 日の 148,320 回が 4 月の最大値である．アカンサスポータルを経由して，WebClass を多くの講義で利用していたことに起因している．このように，圧倒的に認証数の多い 21 日においても，認証処理ができないなどの問題は発生しなかった．次に，4 月 21 日の IdP の認証数とそれにともなう CPU 負荷率およびメモリ使用率を**図 7** に示す．図から，15 時ごろから大量のアクセスが発生しているのが分かる．これは，情報処理基礎で，181 名の学生が同時に講義を受講しているのと同時に，複数の学類でもアカンサスポータル経由で WebClass を用いた講義を行っていたためと考えられる．認証数の増加にともない，メモリの使用率が大きく増加しているのが見て取れる．一方で，CPU については 2〜3%程度しか使用していない．すなわち，IdP においては認証数とメモリについては相関があり，認証数の増加にともない，メモリの使用率は増加する．しかし，CPU においては認証数が増加しても負荷にはほとんど影響を及ぼさない．そして，これだけの認証数があってもメモリは 20%以上の余力があり，CPU にもほとんど負荷がかかっていないことから，IdP の動作には問題ないことを確認することができた．

21 日のアカンサスポータルサーバにおいて，IdP サーバと同様に認証が成功した数とそのときの CPU 負荷率およびメモリ使用率をグラフにしたものを**図 8** に示す．このように，アカンサスポータルサーバにおいてはメモリ，CPU ともに認証数が増減してもほとんど変化していないことが分かる．そのため，SP においてもリソースに負荷を与えることなく運用できていることを確認できた．

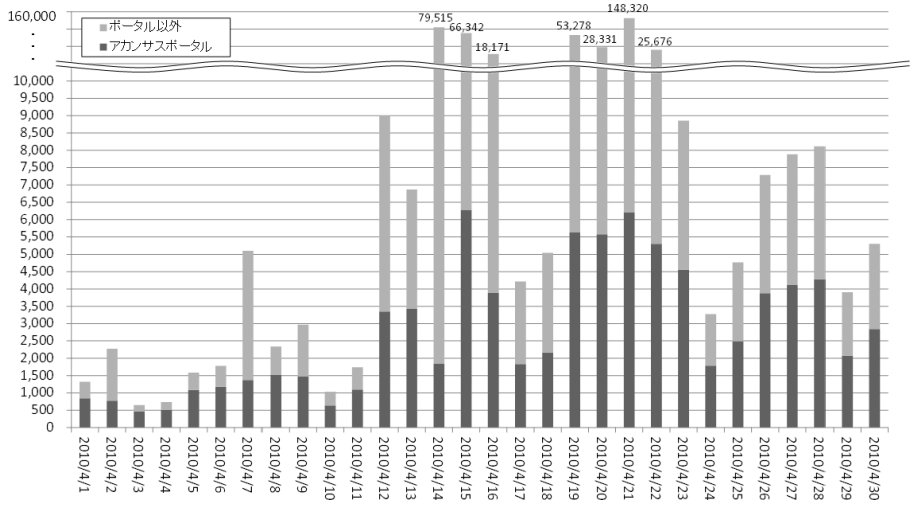

図 6　IdP における認証数の推移（2010/4/1〜2010/4/30）
Fig. 6　Number of authentication executed at IdP (April 1, 2010~April 30, 2010).

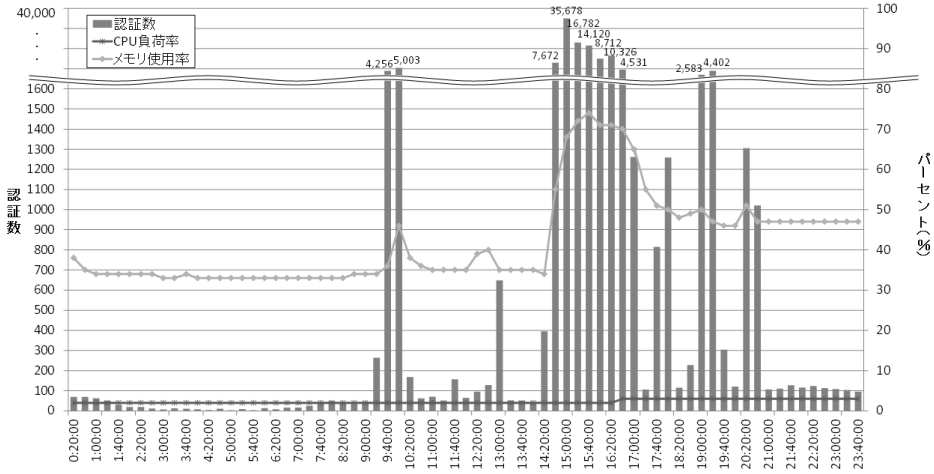

図 7　IdP サーバにおける認証数と CPU 負荷率およびメモリ使用率（2010/4/21）
Fig. 7　Number of logins, CPU loads and memory consumption at IdP on April 21, 2010.

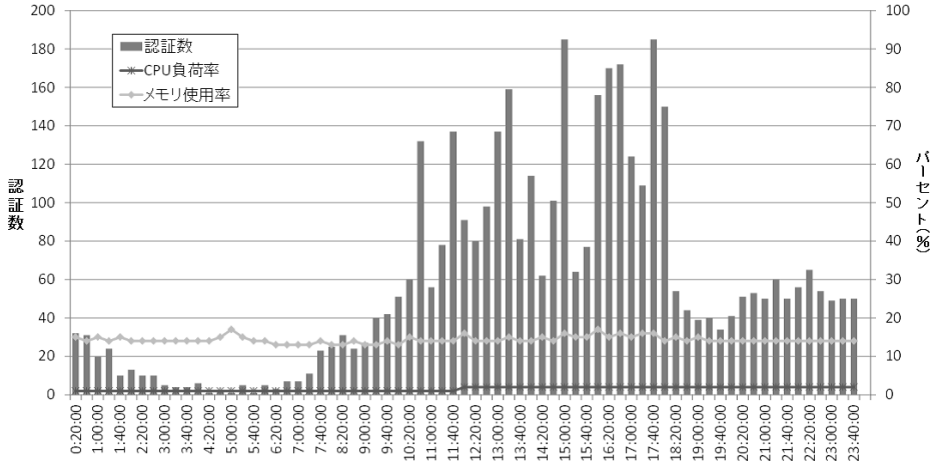

図 8　アカンサスポータルにおける IdP 認証数と CPU 負荷率およびメモリ使用率（2010/4/21）
Fig. 8　Number of logins, CPU loads and memory consumption at portal server on April 21, 2010.

7. ま と め

7.1 成　　果

本稿では，我々が行った本学における統合認証システムの設計，実装，システム評価について述べた．本システムにより実現した項目は以下のとおりである．

- Shibboleth を導入することにより，これまでは独立していた各種情報システムにおける認証機構の一元化を実現した．
- 金沢大学 ID という生涯 ID を導入するとともに，LDAP スキーマの設計に配慮し，Shibboleth IdP の属性情報の送信形式を利用することにより，複数ロールに対応できる仕組みを実現した．これにより，各情報システムはロールに応じたサービスを提供できるようになった．
- Shibboleth では未実装のシングルログアウトを実装したことで，セキュリティを向上させることができた．
- Terracotta を用いることで IdP のクラスタ化を実現し，信頼性の高い認証機構を構築した．
- 構築したシステムの評価を行うことで，実運用にも十分耐えうるシステムであることを実証した．
- 大学特有の複雑な所属形態にも対応し，将来的に大学間連携にも活用できる統合認証基盤環境を構築できた．

本学のように Shibboleth を研究的な側面で利用するのではなく，教育と業務に拡大し，日常的に利用されている情報システムに適用している点が，これまで報告されているものと大きく異なる．そのため，本学の取り組みはこれから Shibboleth を導入する様々な組織においても十分転用可能なレベルに達しているといえる．また，これから情報システムの一元化を検討している大学関係者の一助となることを期待している．

7.2 今後の計画

今後，本学統合認証システムの発展において以下の計画を考えている．

- GakuNin との連携

  NII が中心となって大学間連携を推進しており，平成 21 年度からは電子ジャーナルや一部の NII のサービスが GakuNin と呼称される大学間認証連携基盤を利用し，シングルサインオン環境で利用できるようになってきている．本学も平成 20 年度に NII が行ったシングルサインオン実証実験への参加をきっかけに，本学独自のサービスである「ファイル送信サービス」および「非文献コンテンツ公開サービス」を提供し，積極的に活動に参加を行っている．しかし，現在は GakuNin で本学が認証を行う IdP は，今回構築した統合認証システムのものとは別のサーバを構築し，運用を行っている．理由としては，金沢大学 ID は半永久的に有効であり，GakuNin で提供している大学在籍者に提供するサービスと十分整合がとれていないことがあげられる．そのため現在は，3.1 節で触れた DS を構築して学内 SP 用 IdP と学外 SP 用 IdP をユーザに選択させるとともに，GakuNin 用の LDAP サーバを構築し，学外 SP 用 IdP に参照させる必要がある．この問題を解決するために，本稿で扱ったロールによる認可制御を GakuNin でも活かせる仕掛けの実現が必要といえる．
- 携帯電話への対応

  アカンサスポータルや WebClass などは携帯電話からのログインを許可している．しかし，Shibboleth では認証に Cookie を用いているが，一部の携帯電話では Cookie を使用することができない．そのため，今後 Shibboleth のソースを一部改修し，Cookie を用いない方法で Shibboleth 認証を行えるようにすることを検討している．今後は携帯電話を使ったアクセスは増えると考えられるため，対応することは非常に重要である．
- SP の冗長化について

今回，WebClass のアクセスが多い原因として，3 台構成で DNS ロードバランスを行っていることがある．そのため，SP をクラスタ化することで，IdP における認証数を大幅に削減できることが予想される．SP のクラスタ化に関しては，Shibboleth の SP 機能を用いることで実現可能であり，テスト環境においては正常に動作し，IdP での認証数が大幅に減っていることを確認している．しかし，現在は Shibboleth SP デーモンの冗長化は行われておらず，Shibboleth SP デーモンを起動しているサーバに障害が発生した場合は，結局サービスを継続することができなくなる．そのため，できるだけ早急に Shibboleth SP デーモンの冗長化を実現することが望まれる．Shibboleth SP デーモンの冗長化に成功したのち，本番環境に適用することを考えている．

- 名寄せの対応

  職員となった後に社会人学生になった場合や，学部を卒業してから職員になった場合などは，最初はそれぞれ異なる金沢大学 ID がロールごとに割り当てられる．その後に，アカンサスポータルの名寄せ管理画面から，金沢大学 ID をどちらかに寄せる処理を行う必要がある．今後は，名寄せ処理の完全自動化について検討を行う予定である．

- ユーザ情報の自動反映

  5.2 節で述べたとおり，統合認証基盤で利用するユーザ情報は人事システムおよび教務システムから取得している．現在は教務システムとはアカンサスポータルを通じて連携を行い，変更があった場合に自動で即時反映が可能である．しかし，人事システムはデータの更新は手動で月 1 回となっている．そのため，今後はシステムの運用部署である総務部人事課とアカンサスポータルとの自動連携に向けた協議を進めていく予定である．

- IdP および SP サーバの仮想化

  IdP および SP については，CPU の負荷がほとんどなく，メモリの使用率もまだ余裕があることが分かった．そのため，今後 IdP や SP を追加していく際には，サーバを仮想化し，リソースの節約を行うことが望まれる．

これらの機能を実現することにより，さらに大規模で，柔軟性に富んだ統合認証システムへと発展していくことができると考えている．

参 考 文 献

1) 金沢大学情報戦略本部．http://www.imc.kanazawa-u.ac.jp/info/publication/kouhou2008.pdf (accessed 2010.8)
2) Central Authentication Service. http://www.jasig.org/cas (accessed 2010.8)
3) 内藤久資，梶田将司，小尻智子，平野　靖，間瀬健二：大学における統一認証基盤としての CAS とその拡張，情報処理学会論文誌，Vol.47, No.4, pp.1127–1135 (2006).
4) 梶田将司，内藤久資，小尻智子，平野　靖，間瀬健二：CAS によるセキュアな全学認証基盤の構築，情報処理学会研究報告，Vol.2005, No.39, pp.35–40 (2005).
5) 秋山豊和，寺西裕一，岡村真吾，坂根栄作，長谷川剛ほか：大阪大学における全学 IT 認証基盤の構築，情報処理学会論文誌，Vol.49, No.3, pp.1249–1264 (2008).
6) UPKI イニシアティブ．https://upki-portal.nii.ac.jp/ (accessed 2010.8)
7) Shibboleth. http://shibboleth.internet2.edu/ (accessed 2010.8)
8) 大谷　誠，江藤博文，渡辺健次，只木進一，渡辺義明：シングルサインオンに対応したネットワーク利用者認証システムの開発，情報処理学会論文誌，Vol.51, No.3, pp.1031–1039 (2010).
9) 松平拓也，笠原禎也，高田良宏，井町智彦：UPKI 認証連携基盤に基づく安全なデータ共有システム構築の試み，学術情報処理研究，No.13, pp.84–90 (2009).
10) 太田芳博，梶田将司，田島嘉則，田島尚徳，平野　靖，内藤久資，間瀬健二：大学における生涯 ID のための名寄せ手法，情報処理学会論文誌，Vol.51, No.3, pp.965–973 (2010).
11) 松本豊司，鈴木恒雄，佐藤正英，堀井祐介，井町智彦：e-Learning の全学展開を考慮した情報処理基礎教育システムの構築，教育システム情報学会誌，Vol.25, No.1, pp.87–99 (2008).
12) OpenPNE. http://www.openpne.jp/ (accessed 2010.8)
13) MACE. http://middleware.internet2.edu/MACE/ (accessed 2010.8)
14) SAML2.0. http://www.oasis-open.org/specs/index.php (accessed 2010.8)
15) OpenLDAP. http://www.openldap.org/ (accessed 2010.8)
16) Terracotta. http://www.terracotta.org/ (accessed 2010.8)
17) Shibboleth 2 Documentation. https://spaces.internet2.edu/display/SHIB2/IdPClusterIssues (accessed 2010.8)

(平成 22 年 5 月 18 日受付)
(平成 22 年 11 月 5 日採録)

松平　拓也（学生会員）

平成 16 年信州大学工学部情報工学科卒業．平成 16 年 4 月金沢大学総合メディア基盤センター技術職員に着任．平成 18 年信州大学大学院工学研究科博士前期課程情報工学専攻修了．修士（工学）．平成 19 年より金沢大学大学院自然科学研究科博士後期課程電子情報科学専攻在学中．専門は多様な公開ポリシに対応した分散型データ公開手法に関する研究・開発．電子情報通信学会会員．

笠原　禎也（正会員）

平成元年京都大学工学部電気工学第二学科卒業．平成 3 年同大学大学院修士課程修了．平成 4 年同大学院博士課程中退，京都大学工学部助手に着任．平成 7 年同大学大学院工学研究科助手．平成 10 年同大学院情報学研究科助手．平成 14 年金沢大学工学部准教授，平成 15 年同大学総合メディア基盤センター准教授，同大学院自然科学研究科兼任．平成 21 年より同センター教授．専門は科学データベースからの知識発見・情報処理法，科学衛星搭載波動受信器における機上インテリジェント信号処理および衛星搭載ソフトウェア受信器開発，宇宙空間中の波動の伝搬機構およびプラズマ波動・粒子相互作用の研究．平成 8 年 3 月博士（工学）（京都大学）取得．電子情報通信学会，地球電磁気・地球惑星圏学会，米国地球物理学会連合各会員．

高田　良宏（正会員）

2010 年金沢大学大学院自然科学研究科博士後期課程電子情報科学専攻修了．博士（工学）．現在，金沢大学総合メディア基盤センター助教，専門分野は，データベース，e-Learning．データベースシステムの研究・開発に従事．情報知識学会，電子情報通信学会，コンピュータ利用協議会各会員．

東　　昭孝

平成 19 年金沢大学大学教育開発・支援センター職員．平成 20 年同センター特任助教．平成 22 年 4 月より同大学総合メディア基盤センター特任助教．大学に導入されている学習システムや業務支援システムの運用に関する調査，ポータルの開発・運営・管理の担当，ならびに認証システム開発に従事．

二木　　恵

平成 20 年金沢大学 FD・ICT 教育推進室専任職員．平成 21 年 4 月より金沢大学総合メディア基盤センター専任職員．ポータルシステムおよび認証システムの開発に従事．

森　　祥寛

平成 11 年金沢大学理学部卒業．平成 13 年同大学大学院自然科学研究科数物科学専攻博士課程前期修了．平成 16 年同大学院自然科学研究科物質構造科学専攻博士課程後期修了後，研究生を経た後，同年 10 月金沢大学総合メディア基盤センター教務補佐員採用．平成 19 年同大学学生部学務課教務第一係に着任．平成 21 年同大学総合メディア基盤センター助教．専門は理論物理学（素粒子物理学）．教育に ICT を活用する方法論，特に e ラーニング用教材作成と SNS 等のコミュニティの教育活用について研究．日本教育工学会，教育システム情報学会各会員．