金沢大学における統合認証基盤の現状と課題

松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 藤田 翔也

金沢大学

takusng@kenroku.kanazawa-u.ac.jp

概要：金沢大学では Shibboleth を用いた統合認証基盤を構築し，生涯 ID である金沢大学 ID でのシングルサインオン環境を実現している．本学の統合認証基盤では，学内の情報サービス群だけではなく，学術認証フェデレーション（学認）や大学コンソーシアム石川（UCI）で提供されている学外の情報サービス群も利用可能な設計としている．本稿では，本学における統合認証基盤の現状について説明し，今後の課題について考察する．

1 はじめに

金沢大学（以下，本学という）では，これまで各部署・部局が独立して構築・運用していた情報システムの融合化の一環として，金沢大学統合認証基盤（Kanazawa University Single Sign On（以下，KU-SSO という））を構築し，平成 22 年 3 月から本格稼働を開始した[1]．KU-SSO のミドルウェアとして Shibboleth[2]を採用し，一度の認証でユーザに許可された情報システムを全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情報システム間で安全に共有する仕組みを提供している．

本学に限らず，他大学においても学内の統合認証基盤として Shibboleth を採用する事例が増えてきた[3][4][5]．その背景として，学術認証フェデレーション[6]（以下，学認という）の存在が大きい．学認とは，国立情報学研究所（以下，NII という）が中心となって進めている，学術サービスを利用する機関，学術サービスを提供する機関・出版社等から構成された連合体を指す．各機関は学認に参加することで，相互に認証連携を行うことが可能となる．本学は，平成 20 年度に NII が中心となって実施した「UPKI 認証連携基盤によるシングルサインオン実証実験[7]」から学認に積極的に参画しており，そこで積み重ねてきたノウハウを KU-SSO に反映した．さらに本学では，学内および学認環境の間をシームレスに接続できるように，どちらの環境下でも生涯 ID である金沢大学 ID で利用可能な設計とした[8]．

また，本学は石川県内の高等教育機関で組織する大学コンソーシアム石川[9]（以下，UCI という）に加盟している．UCI の目的は，石川県内の機関が連携して教育交流・情報発信・調査研究等を行うことで，それぞれの教育・活動を活性化するとともにその成果を地域社会に還元し，地域の発展に貢献することである．本学は UCI において中心的な役割を担っており，これまでに UCI サービスの Shibboleth 化を進めてきた．但し，UCI は運用上の理由により，学認とは独立した環境にある．現在，我々は本学の UCI ユーザが KU-SSO の認証で UCI のサービスを利用できるように整備を進めているところである．

このように KU-SSO は，学内の認証から組織間の認証連携まで非常に重要な役割を担っている．我々は KU-SSO の最終形態として，ユーザが学内外などサービスの提供場所に依存することなくシームレスにアクセスできる環境の実現を目指し，日々改良を続けているところである．

本稿では，本学における統合認証基盤の現状について説明するとともに，今後の課題について考察を行う．

2 Shibboleth

本章では，本学の統合認証基盤を説明するにあたり，本学の統合認証基盤として採用している Shibboleth の概要について述べる．

2.1 Shibboleth 概要

Shibboleth は SAML2.0 [10]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．Shibboleth は 3 つのシステムから構成される．

- Identity Provider (IdP)
  - ユーザを認証する．
  - ユーザ属性情報を SP に送信する．
- Service Provider (SP)
  - ユーザの認証を IdP に要求する．
  - ユーザの属性を IdP から受信し，アプリケーションに渡す．
- Discovery Service (DS)
  - 複数の IdP が存在する場合に，ユーザが適当な IdP を決定するための情報を提供する．

2.2 Shibboleth 動作

図 1 に Shibboleth の動作概念図を示す. ユーザは利用したい SP にアクセスを行う（①）．SP はユーザに認証を促すため, DS にリダイレクトを行い，ユーザに IdP を選択させる（②）．あらかじめ SP で認証を行う IdP が決まっている場合は②の作業は省略される．ユーザは IdP で認証を行う（③）．IdP は SP に対して認証結果を返し，認証に成功した場合は，SP は IdP に対して必要な属性を要求し，その返却値を SP に送付する（④）．SP はその属性値を利用し, ユーザの属性に応じてサービスを提供する（⑤）．

3 KU-SSO

本章では，まず KU-SSO の概要について説明し，学内環境および学認環境の現状について説明する．

3.1 KU-SSO 概要

本学の KU-SSO 環境を図 2 に示す. 本学のユーザは，学内の SP を利用したい場合は学内用 IdP で認証を行う．また，学認の SP を利用したい場合は学認用 IdP で認証を行う. ただし, 学内用 IdP および学認用 IdP はそれぞれ同一の LDAP を参照

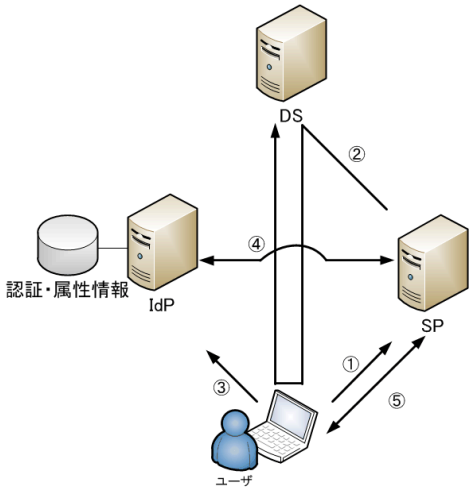

図 1　Shibboleth 動作概念図

することで, どちらの IdP も後述する金沢大学 ID で認証可能としている．また，UCI に関しても，環境を Shibboleth 化するとともに, 学認用 IdP を利用した金沢大学 ID での認証までは実装済みである．ただし，UCI 環境については，ユーザ属性情報の送付など，双方の細かいインターフェースの調整がいまも進行中で，現在のところ本運用には至っていない. そのため, 現状では, 認証は UCI の事務局が管理している IdP で行っている. 現在, 我々はこの問題を解決し，学認用 IdP で認証できるように整備を進めている[11].

3.1.1 金沢大学 ID

金沢大学 ID は，KU-SSO での認証に用いる生涯 ID である．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 つずつ付与される．ID の採番方法は，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，他人の ID を容易に推測できないようにした．また，転学類に伴う学籍番号変更や，卒業後に本学に就職した場合などの場合においても，同一 ID を使用でき，卒業・退職後も ID を抹消されず，“1 ユーザ 1ID”を実現した．なお，金沢大学 ID の発行件数は 61048 件である（2013/10/25 現在）.

3.1.2 ロール

SP には，教育・研究・業務に関する様々なものがあり，それらを使用できるユーザは，SP の利用目的によってそれぞれ異なる．そのため，各 SP

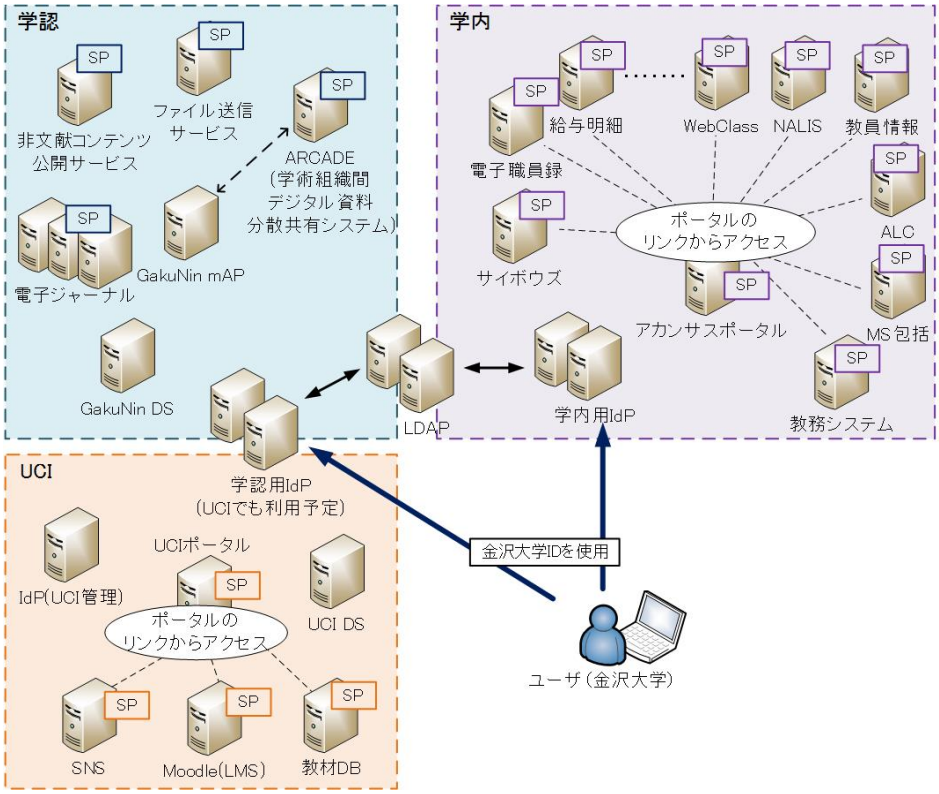

図 2　KU-SSO 概念図（2013/10/25 現在）

が，ユーザの職分等の属性情報から，当該 SP を利用できる権限があるかどうかを判断できるように，ユーザの属性を“ロール”という名称で定義し，区分分けを行っている．表 1 にロールの一覧を示す．また，ユーザが複数のロールを持つことも想定している．たとえば，本学の学部を卒業後に本学の職員（学務系以外）になった場合は，学生（既卒），職員（常勤学務系以外）という 2 つのロールが付与される．但し，複数ロールを持つユーザであっても，金沢大学 ID は 1 つである．

3.2 学内環境

本節では KU-SSO における学内環境の現状について説明する．

3.2.1 学内 SP 対応状況

学内環境においては，2013/10/25 現在，28 の情報システムを SP 化している．SP 化しているシステムの一覧は以下の通りである（企業名が記載されているものは，当該企業のパッケージ品を SP 化したものである）．

- アカンサスポータル
- WebClass（LMS：株式会社ウェブクラス）
- 学内 Web（教職員・学生向け情報の閲覧）

表 1　ロール一覧

区分	ロール名
学生	入学前
	在学
	既卒
	退学
教員	常勤
	教諭
	研究員
	非常勤講師
	名誉教授
	医員
	TA
	RA
	退職・転出
	その他（学外教員等）
職員	常勤学務係
	常勤学務係以外
	非常勤学務係
	非常勤学務係以外
	非職員学務係・秘書含
	非職員学務係以外・秘書
	教務補佐員
	退職
その他	管理者
	管理者（システム別）
	学外学生（公開講座）
	ゲスト
	学外学生修了（公開講座）
	委託業者等（共同研究）
	家族等

- 教務システム（履修登録，成績入力・照会等：SCSK 株式会社）
- 電子職員録（教職員の連絡先等の閲覧）
- サイボウズガルーン 3（サイボウズ株式会社）
- 予算執行支援システム（財務会計サブシステム：富士通株式会社）
- 給与明細等オンラインシステム（給与支給明細閲覧，源泉徴収関係届出等：人材開発株式会社）
- 駐車許可証交付システム（駐車許可証発行の申請）
- プロジェクト管理システム（Redmine[12]を使用した進捗管理）
- 統合アカウント管理システム（ネットワーク（Wi-Fi）接続用 ID 管理）
- NALIS（図書業務管理：株式会社 NTT データ九州）
- アカウント管理システム（金沢大学 ID 管理，パスワード変更・再発行等）
- ファイル送信サービス（サイズの大きなファイルをダウンロード）
- ALC NetAcademy2（英語教材：株式会社アルク教育社）
- SNS（OpenPNE[13]のコミュニティサイト）
- Microsoft 包括ライセンス（Microsoft ソフトウェアダウンロード）
- 教員情報データベース（教員実績入力，閲覧，評価）
- 会議資料管理システム（会議資料をアップロードし，主に iPad で閲覧）
- Web シラバス（シラバス情報入力，閲覧）
- 教材データベース（NetCommons2[14]を使用した教材共有）
- ファイル共有アプリケーション（Java Applet 上でのファイル共有）
- 留学生ネット（留学生用交流サイト）
- 事務局用アカウント管理システム（事務職員向けサービス用情報管理）
- ソフトウェアダウンロード（ウィルス対策ソフト等のダウンロード）
- 施設管理システム（施設の情報入力，閲覧：株式会社サイバーブルー）
- アカンサスライブ（Adobe Flash Media Server[15]によるキャンパス天気状況の動画配信）
- 中期目標・中期計画進捗管理システム

このように，教育・研究・業務など，多岐にわたるシステムを Shibboleth SP 化し，シングルサインオン環境を実現している．

3.2.2 学内環境利用状況

本節では，KU-SSO における学内環境の利用状況について説明する．

まずは，学内用 IdP の利用状況について述べる．2013/4 における学内用 IdP の認証数の日別推移を図 3 に示す．4 月は全入学生対象の情報処理基礎の講義や学生の履修登録，さらにはアカンサスポータルを経由しての LMS の利用があるため，一年のうちで IdP での認証が多く行われる月である．平日は軒並み 1 万件を越えるアクセスがあり，多い日では一日あたり 2 万件近くを記録する日もある．また，図 4 に時間別推移を示す．このように講義や業務が始まる 8 時以降から認証数が急増し，講義や業務が終わる 18 時頃まで非常に多くの認証が行われる．そして，18 時以降もコンスタントに認証が行われていることが分かる．

次に，学内用 SP 群の利用状況について述べる．2013/4 における学内 SP の認証状況を図 5 に示す．アカンサスポータル，WebClass，教務システムの教育系システムが多くの割合を占めていることがわかる．一方で，学内 Web，電子職員録，サイボウズ等の業務系システムも一定の割合を占めている．KU-SSO 利用対象者における教職員の割合は学生に比べると少ないことを考慮すると，教職員の KU-SSO 利用数も十分多いことが推測できる．また，駐車許可証交付システムが上位に来ているが，これは 4 月が学生の駐車許可申請時期であることから一時的なものであると考えられる．

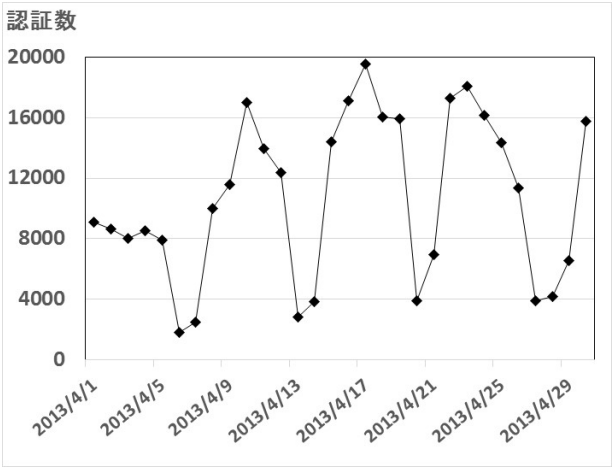

図 3　学内用 IdP 認証数の日別推移(2013/4)

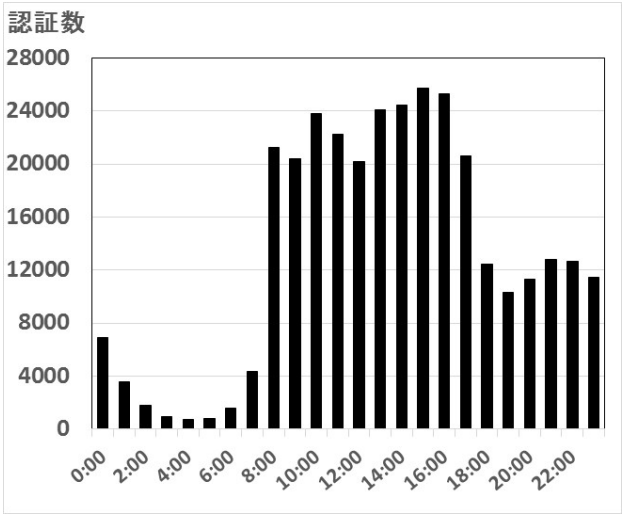

図 4　学内用 IdP 認証数の時間別推移(2013/4)

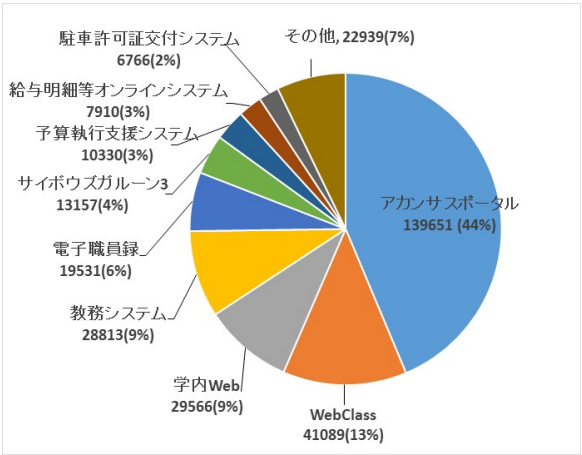

図 5　学内 SP 認証状況(2013/4)

3.3 学認環境

本節では KU-SSO における学認環境の現状について説明する．学認環境においても金沢大学 ID を利用可能にするためには，KU-SSO を「学術認証フェデレーション システム運用基準（以下，運用基準という） Ver1.2[16]」に適合させる必要がある．そこで我々は，学認の利用を「在籍する教職員・学生」に限定させることでこの運用基準をクリアした．具体的には，NII が提供している FPSP プラグイン[17]を本学の学認用 IdP に組み込み，表 1 に示すロールの中で，在籍する教職員・学生のロールを持つユーザだけ学認サービスへのアクセスを許可している．該当するロールは，表 1 における色つきのロール，すなわち学生（在学），教員（常勤，教諭，研究員，医員），職員（常勤学務係，常勤学務係以外，非常勤学務係，非常勤学務係以外，教務補佐員）である．それ以外のロールが割り当てられているユーザには認証後，IdP によりアクセス拒否画面を提示し，学認の SP を利用できないようにしている．

また，本学では 2013/10/25 現在，3 つの SP を学認で提供している．提供しているサービスは，「ファイル送信サービス[18]」，「金沢大学データリポジトリ[19]」，および「学術組織間デジタル資料分散共有システム（以下，ARCADE という）[20]」である．以下にそれぞれのサービスの概要について説明する．

- ファイル送信サービス

ファイル送信サービスは，メールでは添付できない大容量のファイルを相手に送信したい場合に，ファイルの転送を行う SP である．このようなサービスを行う上で問題となるのはユーザの管理であり，学認を利用することで，本学でユーザを管理することなく，ユーザの身元を確認できる．

- 金沢大学データリポジトリ

金沢大学データリポジトリは，DSpace[21]で構築した，大学で生産された実験観測データなどを特定の組織やグループに限定して公開を行うことを目的とした SP である．現在，科学観測衛星「あけぼの」による地球周辺の電波観測データのスペクトル画像を PNG 化したものを，学認で認証が成功したユーザだけに公開している．

- ARCADE

ARCADE は組織を超えたユーザ同士でファイ

ルを共有するソフトウェアである．図 6 に ARCADE の利用モデル例を示す．利用者は，NII が提供する GakuNin mAP[22]を利用して共通するグループを作成することで，異なる機関に所属するユーザ同士でも ARCADE を利用してグループ領域にあるファイルの閲覧やアップロード・ダウンロードが可能となる．

4 KU-SSO の課題

3 章では，KU-SSO の概要と現状について説明した．本章では KU-SSO における課題について考察する．現在，我々は以下の 4 つの課題について検討を行っている．

- UCI 環境の KU-SSO 対応

本学のユーザが UCI のサービスを利用する場合，現状では UCI 事務局が管理する IdP においてユーザの追加が必要になる．そこで，KU-SSO を利用することで，UCI 事務局のユーザ登録にかかる負担の軽減および本学のユーザの利便性向上が期待できる．しかしながら，UCI のサービスは学外の扱いであり，ユーザの同意なしに UCI サービスに対してユーザ属性情報を送付することは，個人情報保護の観点から望ましくない．そこで，我々は NII が提供している uApprove.jp[23]を利用し解決を図ることとした．uApprove.jp を利用することで，ユーザ属性情報送付の判断をユーザに委ねることができる．そのため，UCI 環境で必要となる，所属，学生番号，氏名などのユーザ属性情報を送付する旨をユーザに提示し，同意を得るように実装を進めているところである．

- IdP クラスタ方式の再検討

IdP は KU-SSO の要であり，クラスタ化は必須項目である．現在，本学の IdP は Terracotta[24]を用いてクラスタ化を実現している．Terracotta は，もともと Shibboleth が推奨していたクラスタ方式であるが，最近は情報が更新されていないために将来的な不安が残る．そのため，NII が提供している IdP の冗長化方法[25]を参考にしながら，本学に最適なクラスタ方式を検討しているところである．

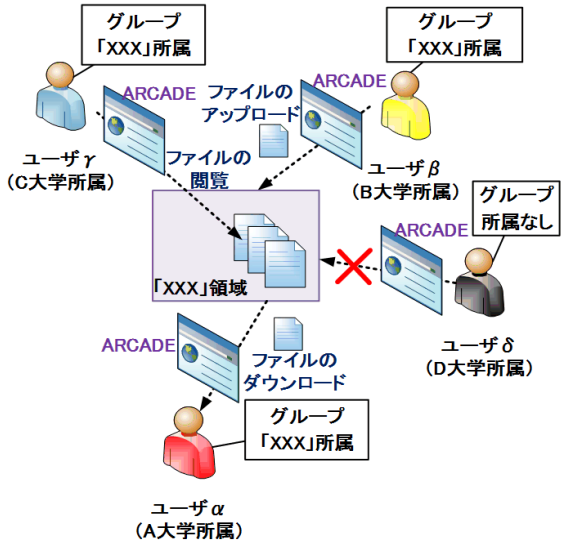

図 6　ARCADE 利用モデル例

- 多要素認証の導入

現在，学内環境の SP 群においては，学内からは全てアクセス可能であるが，学外からのアクセスを許可していない SP が存在する．これらの SP に対して学外からアクセスするためには VPN を利用する必要がある．しかし，本学の VPN は，今日広く普及している iOS や Android を搭載した端末で利用できなかったり，VPN との相性により SP が提供するサービスが上手く動作しなかったりという問題がある．その結果，本学に通うことが物理的に不可能な社会人学生や，出張先からのアクセス需要が高い教員に対して不便を強いてしまっている．これらの SP が VPN を必要とする理由として，現在の本学の認証方式が ID/PW だけで運用されていることが大きい．そのため，学外からのアクセス時において多要素認証を導入し，セキュリティレベルを向上することで，当該 SP が VPN を利用することなしにアクセスできる環境に移行できると考え，現在検討を進めている．

- IdP サーバの一元化

現在のところ，学内および学認それぞれの環境をまたぐ際には，認証画面を表示することで環境が異なるということをユーザに示し，注意喚起を促している．しかし，将来的にはどちらもシームレスに利用できる環境を構築することが，ユーザの利便性向上とシステム管理負荷低減の双方の観点から望ましい．ただし，現在は KU-SSO 環境に

おいてはシングルログアウトを実現しているが，GakuNin 環境では実現できていない．そのため，両環境におけるシングルログアウトを実現できる機構を考案する必要があると考えている．

5 おわりに

本稿では，本学の統合認証基盤である KU-SSO の現状について説明を行い，今後の課題について考察を行った．学内環境においては，これまでに多くの学内サービスの SP 化を進めてきたことで，学内情報システムの融合化が達成できていると考えている．また，学認環境においても，本学から積極的に SP を提供し，ユーザの利便性を向上させるとともに，学認の普及の一助となることも期待している．

今後は 4 章で考察した課題の解決を中心として，KU-SSO 環境をさらに発展させていきたいと考えている．

謝辞

本研究は科研費若手研究 B （25750080），基盤研究 C（23501140）の助成を受けたものである．

参考文献

[1] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, 森 祥寛, “大学における Shibboleth を利用した統合認証基盤の構築”, 情報処理学会論文誌, Vol.52 No.2, pp.703-713, (2011)

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

[3] 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)

[4] 河野圭太, 藤原 崇起, 大隅 淑弘, 岡山 聖彦, 山井成良, 稗田隆, “岡山大学における生涯 ID を実現する統合認証システムの構築”, 学術情報処理研究, No15, pp.171-175, (2011)

[5] 学認活用事例集（ケーススタディ）, http://www.gakunin.jp/info/ (accessed 2013.10)

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

[7] 平成 20 年シングルサインオン実証実験報告書, http://www.gakunin.jp/index.php?action=pages_view_main&active_action=repository_view_main_item_snippet&index_id=40&page_no=1&list_view_num=20&sort_order=7&page_id=85&block_id=227 (accessed 2013.10)

[8] 松平 拓也, 笠原 禎也, 高田 良宏, 東 昭孝, 二木 恵, “学認との融合化を視野に入れた金沢大学統合認証基盤の構築と運用”, 学術情報処理研究, No13, pp.41-50, (2012)

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

[10] SAML2.0, https://www.oasis-open.org/standards#samlv2.0 (accessed 2013.10)

[11] 藤田 翔也, 松平 拓也, 高田 良宏, 笠原 禎也, “"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”, 大学 ICT 推進協議会 2013 年度年次大会論文集, 印刷中, (2013)

[12] Redmine, http://redmine.jp/ (accessed 2013.10)

[13] OpenPNE, http://www.openpne.jp/ (accessed 2013.10)

[14] NetCommons, http://www.netcommons.org/ (accessed 2013.10)

[15] Adobe Flash Media Server, http://help.adobe.com/ja_JP/flashmediaserver/techoverview/index.html (accessed 2013.10)

[16] 学術認証フェデレーション システム運用基準 (Ver.1.2), http://www.gakunin.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=36&item_no=1&page_id=85&block_id=227 (accessed 2013.10)

[17] FPSP プラグイン, https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=12158554 (accessed 2013.10)

[18] ファイル送信サービス, https://sp1.db.kanazawa-u.ac.jp/sendfile/ (accessed 2013.10)

[19] 金沢大学データリポジトリ, https://sp2.db.kanazawa-u.ac.jp/dspace/ (accessed 2013.10)
[20] ARCADE, https://arcade.cis.kanazawa-u.ac.jp/ (accessed 2013.10)
[21] DSpace, http://www.dspace.org/ (accessed 2013.10)
[22] GakuNin mAP, https://map.gakunin.nii.ac.jp/map/ (accessed 2013.10)
[23] uApprove.jp, https://meatwiki.nii.ac.jp/confluence/pages/viewpage.action?pageId=13501031 (accessed 2013.10)
[24] Terracotta, http://terracotta.org/ (accessed 2013.10)
[25] 認証基盤の冗長化 技術編, http://www.gakunin.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=207&item_no=1&page_id=85&block_id=227 (accessed 2013.10)