Vol.2013-CE-122 No.20
Vol.2013-CLE-11 No.20
2013/12/15

学認対応認証基盤とユーザID体系移行用CASゲートウェイの構築

永井 孝幸[1,a)]　杉谷 賢一[1]　河津 秀利[2]　中野 裕司[1]

概要：熊本大学では 2012 年度より生涯 ID である熊本大学 ID の運用を開始した．一方，学内の既存システムではユーザ ID に教職員・学生番号が用いられており，新ユーザ ID への移行をどのように実現するかが大きな課題となっていた．今回，学術認証フェデレーション対応認証基盤の構築と合わせ，Shibboleth を認証源とする CAS サーバにユーザ ID 選択機能を追加した CAS ゲートウェイを実装し，ユーザ ID 体系の移行とシングルサインオン環境を両立させるための認証基盤を構築した．本稿では構築した認証基盤の詳細について述べる．

キーワード：学術認証フェデレーション,ID 管理,CAS,Shibboleth,Grouper

Renewal of SSO infrastrcture for lifelong user account and GakuNin academic federation

Abstract: In 2012, we introduced new lifelong user account *KumadaiID* which is uniquely assigned to individuals. On the other hand, it has been a problem to support this new account in existing CAS systems where user accounts are assigned based on roles. To solve this problem, we developed a CAS gateway that enables users to select their role ID when authenticated by KumadaiID. This new lifelong account also enabled us to deploy Shibboleth IdP to join academic federation *Gakunin*. In this technical report, we describe the details of our new SSO infrastructure.

Keywords: GakuNin,academic federation,identity and access management,CAS,Shibboleth,Grouper

1. はじめに

熊本大学では 2012 年度より生涯 ID である熊本大学 ID の運用を開始した．一方，学内の既存システムではユーザ ID に教職員・学生番号が用いられており，新ユーザ ID への移行をどのように実現するかが大きな課題となっていた．熊本大学では多くのシステムが CAS 認証によるシングルサインオンを前提としており，CAS 認証に用いるユーザ ID を単純に変更するにはシステムの一斉変更が必要となるためである．

既存システムの一斉改修を避けながら新 ID による認証を導入する方法としては認証に用いる ID(ログイン ID) と各システムに回答する ID(ユーザ ID) を切り分ける方式が考えられる (図 1)．この方式では新 ID で認証を行った後，各システムへの初回アクセス時にそのシステムで利用するユーザ ID をユーザが選択できるようにすることで，既存システムに手を加えること無く新 ID でのシングルサインオン環境を実現できる．

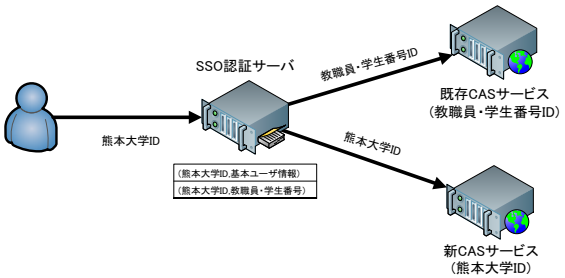

図 1　認証用ユーザ ID と利用者ユーザ ID の分離
Fig. 1　Seperation of userID from loginID

[1] 熊本大学総合情報基盤センター
Kurokami2-39-1,Kumamoto,860-8555, Japan
[2] 熊本大学情報企画ユニット
Kurokami2-39-1,Kumamoto,860-8555, Japan
[a)] tnagai@cc.kumamoto-u.ac.jp

© 2013 Information Processing Society of Japan

今回，学術認証フェデレーション対応認証基盤の構築と合わせ，Shibboleth を認証源とする CAS サーバにユーザ ID 選択機能を追加した CAS ゲートウェイを実装し，ユーザ ID 体系の移行とシングルサインオン環境を両立させるための認証基盤を構築した．本稿では構築した認証基盤の詳細について述べる．

まず今回のユーザ認証基盤整備の経緯について 2 節で述べる．次に生涯 ID 導入にあたり解決すべき課題について 3 節で述べる．続く 4 節で ID 選択機能を備えた SSO 実現方式について検討を行い，5 節で熊本大学 ID 対応ユーザディレクトリの構築結果について述べる．6 節で学認対応 Shibboleth IdP の構築方法を示し，7 節でユーザ ID 体系移行用 CAS ゲートウェイの実現方法について述べる．8 節で認証基盤の運用状況について述べ，9 節で関連事例との比較を行う．

2. ユーザ認証基盤整備の経緯

この節ではユーザ認証基盤見直しの経緯と教職員・学生番号にもとづく既存 ID の問題点を述べ，生涯 ID の導入によって認証基盤の整備が進んだ背景について説明する．

2.1 これまでの取り組み

熊本大学ではキャンパス環境の高度化及び情報セキュリティの強化を推進するため，中期計画として「情報環構想」を定め，これに沿う形でインフラの整備を行っている．「学務情報システム SOSEKI(1999 年度導入)[1]」「WebCT(2003 年度導入)」「熊本大学情報セキュリティポリシー (2003 年 2 月策定)」「CAS 認証基盤・大学ポータル (2006 年度導入)」等が主な取り組みである．

大学全体の第二期中期目標・中期計画に対応して策定された「情報環構想 2010」では情報技術の進展や大学を取り巻く社会環境の変化などを踏まえ，「熊本大学 ID（生涯サポート）の導入と熊本大学ポータルの拡充」が目標の一つとして掲げられた [2]．これは e ポートフォリオ・グループウェア・大学ポータルを始めとする生涯利用対応情報サービスの拡充を意味すると同時に，利用者情報の一元管理を含む情報セキュリティの強化も意味する．これまでに「政府統一基準対応情報セキュリティポリシーの策定 (2011 年度)」「熊本大学 ID 発行 (2011 年度〜)」「グループウェア Confluence の小規模利用 (2011 年度〜)」「学生証 IC カード化 (2012 年度)」「教職員証 IC カード化 (2013 年度)」等の取り組みを行っている．

これと並行して，総合情報基盤センターでは将来的に外部サービス利用のための認証基盤が必要になると考え，学術認証フェデレーションのテストフェデレーションへの参加 (2008 年度)，CAS サーバの GoogleApps 連携 (2010 年度) 等の取り組みを行ってきた．

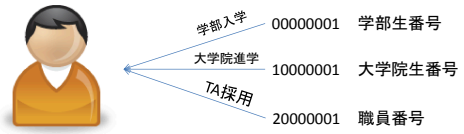

図 2 複数の教職員・学生番号アカウントを持つケース
Fig. 2 Accounts are issued for each contract

2.2 既存 ID の問題点

学生番号は学籍に対して割り当てられるため，学部を卒業して大学院に進学した場合，学部と大学院では異なった番号が割り当てられる (図 2)．このため，学生番号を認証用アカウントに用いた場合，学部生の時に利用していたシステムの情報を利用する際は学部生用アカウントでログインし，大学院生用システムを利用する時は大学院生用アカウントでログインし直す必要がある．通常，CAS では一旦ログアウトせずにユーザ ID を変更することはできないため，ログインし直すたびにユーザ名・パスワードを入力する手間が生じる．

教職員番号は雇用契約毎に割り当てられるため，大学院生が TA 等で雇用された場合は，更に TA 用の職員番号が割り当てられる．雇用に関する情報，例えば給与明細を確認する際は，改めて職員番号でログインし直す必要がある．また，少ないケースであるが学内の複数の部局で雇用された場合，それぞれの雇用契約毎に職員番号が割り当てられるため，複数の職員番号を割り当てられるケースも存在する．

大学ポータルや e ポートフォリオにおいて各利用者に対して必要な情報を集約して提示するには，このような学籍・契約単位のアカウントは不向きであり，個人を基準としてアカウントを割り当てる生涯 ID の導入が不可欠である．

2.3 生涯 ID の導入に伴う認証基盤整備の進展

熊本大学では 2008 年に学認のテストフェデレーションに参加した後，2013 年まで運用フェデレーションに参加していない．認証基盤の整備に 5 年という時間を要した背景について説明する．

Shibboleth IdP があれば認証連携そのものは問題なく行えるため，運用フェデレーションへの移行に 5 年という時間を要したのは技術的な理由では無い．Shibboleth 導入以前にシングルサインオン用の認証基盤として CAS の整備を終えていたために，二重に認証基盤にリソースを割くメリットがなかったことが一つ目の理由である．

もう一つの理由は，学内に ID 管理体制が整っていなかったことである．現在，学内の多くのシステムでは教職員・学生番号をユーザ ID に利用しており，複数身分を有する利用者はアカウントを複数保有している．これに対し，学認では利用者を一意に識別する ID(eduPersonPrincipalName, 以下 **ePPN**) をユーザ ID に用いる必要があり，既存のユーザ

© 2013 Information Processing Society of Japan

ID をそのまま用いることができなかった．更に，教員・学生などのユーザ区分属性 (eduPersonAffiliation, 以下 **ePA**) も管理する必要があるが，既存のユーザ ID では特定の桁の数字からユーザ区分が判別できるようになっていたために各利用者のユーザ区分に関する統一的なデータベースが整備されていなかった．これは技術的な問題ではなく，IdAM(Identity and Access Management) おける典型的な組織体制の問題である [3].

生涯 ID として導入された熊本大学 ID は利用者の身分に関わらず一意に割り当てられるため，学認のユーザ ID として利用可能である[*1]．更に熊本大学 ID は ID そのものからユーザ属性を推測できないように英字・数字を組み合わせたランダムな文字列が割り当てられている．このため，実運用にあたってはサービスのアクセス制御を実現するためにユーザ情報に関するデータベースを構築することが不可欠となり，名寄せをはじめとする ID 管理体制の整備が進むこととなった．

CAS と Shibboleth の両立についても，GoogleApps やアカデミッククラウドを始めとする外部サービスを利用するための認証基盤としては Shibboleth が適していること，また，CAS・Shibboleth 相互連携の技術的な目処が立ったことから Shibboleth 導入の理解が得られ，熊本大学 ID 用認証基盤と学認用認証基盤の整備を一体として進めることになった．

3. 生涯 ID 導入にあたり解決すべき課題

生涯 ID の導入は単なる ID 発行作業にとどまらず，既存システムとの連携やユーザ情報管理体制についても考慮する必要がある．本節では，生涯 ID 導入にあたり解決すべき課題について述べる．

3.1 ID 体系の移行と既存システムの連携の両立

シングルサインオン環境の整備と合わせて生涯 ID を導入する組織の場合，既存システムはそれぞれ独立した認証基盤のもとで動作していることから，中期的な計画に基づいて余裕を持って各システムのシングルサインオン対応と生涯 ID 対応を進めていくことが出来る．

一方，熊本大学のように既にシングルサインオン環境の整備が済んでいる組織において，シングルサインオン環境を保ったままユーザ ID 体系を移行することには困難を伴う．ログイン用のアカウントに熊本大学 ID を用いるように CAS サーバの設定を変更すること自体はすぐにできるが，全 CAS クライアントが熊本大学 ID に対応しなければ認証基盤として運用できない．現実には事務用・教育用など多くの CAS 対応システムが稼働しており，全ての CAS クライアントの改修を一斉に行うことは不可能である．更に，既存 ID が英数字 8 桁からなるのに対して熊本大学 ID は英数字 9 桁であるため，各種入力画面や集計ツールでの入力データ検証処理にも影響が及ぶ．

既存の CAS 認証基盤を残したまま新たに熊本大学 ID 用の CAS サーバを運用する方法が最も安全である．しかし，シングルサインオン環境が損なわれることに加え，利用者から見て熊本大学 ID を使う直接のメリットがない．

認証用ユーザ ID を熊本大学 ID に移行するには，既存の CAS 対応システムに手を加えないまま熊本大学 ID を用いた認証を実現することが不可欠であり，また，熊本大学 ID を用いるメリットがあるサービスを用意する必要がある．

3.2 ユーザ情報管理体制の構築

ユーザ ID でなくユーザ属性にもとづいたアクセス制御を行うには，ユーザ情報管理体制の構築が不可欠である．

学認の運用に必要なユーザ職種属性 (**ePA**) としては student,faculty,staff,member の区別ができればよく，基本的には各利用者の職種・学籍が把握できればよい．大学ポータルの運用にはユーザ職種属性に加えて所属学科・所属部局・履修科目等，より詳細な情報が必要となる．これらの情報については人事データベース・学務情報データベースの情報を集約することで整備が可能である．例えば金沢大学の事例では職種・雇用形態・在籍状況等にもとづいて各利用者に割り当てられたロール番号をもとに ePA 属性を設定している [4].

グループウェアについてはより複雑なグループ情報の管理が必要である．例えばグループウェア上で資料を共有する場合，「この資料は部局 A の教授職以上しか閲覧してはならない．ただし，資料登録作業のための事務員によるアクセスは許可する.」といったように職種・部局を組み合わせたグループ定義に加え，実作業上の要請から部局の枠を超えたグループを設ける必要がある．このようなグループは人事・学務データベース上の区分コードでは考慮されておらず，「情報へのアクセス制御」の観点から別途グループ管理を行う必要がある．

4. ID 選択機能を備えた SSO 実現方式の検討

生涯 ID の導入に際し，各システムへのログイン時にユーザ ID 選択機能を持たせることでシングルサインオンとユーザ ID 選択機能を両立させた事例として大阪大学の事例 [5] が挙げられる．この事例では商用の ShibbolethIdP を改修することでユーザ ID 選択機能を実現している．

今回，同様の手法を CAS 環境に適用することを検討し，Shibboleth IdP とユーザ ID 選択機能を備えた CAS ゲートウェイを組み合わせる方式を採用した．本節では CAS-Shibboleth 連携方式の実現にあたり検討した事柄について述べる．以下，IdP は Identity Provider,SP は Service Provider を表わす．

[*1] 実際には熊本大学 ID を元に作成したハッシュ値を ePPN に利用している

© 2013 Information Processing Society of Japan

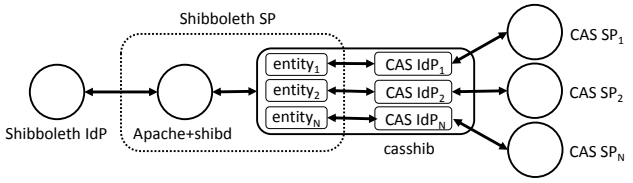

図 3 casshib のアーキテクチャ
Fig. 3 The architecture of casshib

4.1 CAS-Shibboleth 連携方式の検討

ユーザ ID 選択機能を実現するには, CAS SP 毎に異なったユーザ ID を送出する仕組みが必要となる．CAS,Shibboleth 共にオープンソースであるため原理的には際限なく独自の機能拡張が可能であるが，導入・保守のコストの面からは可能な限り既存の実装に近いことが望ましい．

CAS の認証源として Shibboleth IdP を用い，CAS SP を Shibboleth 対応させることで CAS・Shibboleth を統合したシングルサインオン環境を実現する方法として米カリフォルニア大学 Merced 校で実装された casshib[6] を用いる方法がある．casshib の基本的な仕組みは，CAS サーバを Shibboleth SP の配下に置き，shibd の送出する HTTP ヘッダからユーザ ID・ユーザ属性を取得するというものである (図 3)．

ここで, casshib では CAS サーバが (仮想的に複数の)CAS IdP として動作するよう，JA-SIG の CAS サーバ実装に対して独自の機能拡張が行われている．元々の CAS サーバ実装では全ての CAS SP に対して同一の TGC(Ticket Granting Cookie) を用いているが，casshib では CAS SP 毎に Shibboleth IdP が異なるユーザ属性を返すため SP 毎に異なった TGC を用いる[*2]．

casshib 方式の場合，Shibboleth IdP から各 SP に対して異なったユーザ属性を返すこと自体は問題なく行える．したがって，ある SP に対しては従来通り教職員・学生番号 ID を送出し，ある SP に対しては熊本大学 ID を送出するという動作を Shibboleth IdP の設定だけで実現できる．残るユーザ ID 選択機能の実装については，Shibboleth IdP に機能を追加する方法と casshib に機能を追加する方法の二通りの選択肢がある．

4.2 本学で採用した方式

Shibboleth IdP にユーザ ID 選択機能を実装する場合は認証動作そのものに手を加える必要があるため，まず商用 IdP 製品の選択肢は非常に限られたものになる．オープンソースの IdP としては，学認との相互運用を前提とすると事実上 Shibboleth と uApprove の組み合わせ [7] しか選択肢が無い．これはユーザー属性の中には個人情報に該当するものがあり，ユーザー属性の外部送信において「独立行政法人等の保有する個人情報の保護に関する法律」の「第９条（利用及び提供の制限）一」[*3]の規定を満たすために「ユーザー自身の同意を得る必要がある」ためである．

Shibboleth は機能追加・セキュリティ対応も含めて年に数回の頻度でバージョンアップが行われており，IdP 機能の根幹となる認証部分に手を入れることは避けたい．開発ロードマップによればメジャーアップデートとなる Shibboleth IdP 3.0 のリリースが 2014 年に予定されており，現行の Shibboleth IdP 2.x 系に独自の機能を実装した場合，3.x 系に移行できず認証フェデレーションの長期的な運用に支障をきたす恐れがある．また，将来 Shibboleth SP を導入することになった場合，動作保証が困難になる．

casshib にユーザ ID 選択機能を実装する場合，認証ならびにユーザ属性の取得そのものは Shibboleth IdP で行うためユーザ情報源 (LDAP,RDB 等) に直接アクセスする必要が無く，後は IdP から受け取ったどの属性値をユーザ ID として利用するかをユーザーに選択させる処理を追加するだけでよい．この場合，IdP のカスタマイズは不要なため上で述べた認証フェデレーションの運用や ShibbolethSP の動作保証の問題は生じない．

CAS サーバも機能追加・セキュリティ対応によるバージョンアップは行われているが，既存の学内システムはユーザ認証のためだけに CAS を利用しており機能追加の必要性がないことから，セキュリティ対応に伴うマイナーバージョンアップにだけ対応できればよい．

以上の検討結果から Shibboleth IdP を認証源とした CAS-Shibboleth 連携方式を採用することとし，casshib にユーザ ID 選択機能の実装を行った．開発環境では Shibboleth IdP を用い，本番環境では Shibboleth IdP+uApprove とほぼ同等の機能をもつ商用アプライアンス (ネットスプリング社製 AXIOLEIdP アプライアンス[*4]) を利用している．

5. 熊本大学 ID 対応ユーザディレクトリの構築

この節では熊本大学 ID にもとづいた認証基盤を実現するために今回構築したユーザディレクトリ (図 4) について，システム構成と情報収集体制の面から述べる．

5.1 システム構成

今回，先に 3.2 節で述べた要求を満たすため，グループ情報の管理には Internet2 プロジェクトで開発されたグループ管理用ミドルウェア Grouper[8] を用いることにした．Grouper はグループ情報を外部の LDAP に同期できるだけでなく，Web サービス API を通じた外部システム連携

[*2] SP のサービス名を service とすると，TGC は CASTGC-service という名称のクッキーに保存される．クッキーのパスも/casshib/shib/service となる．

[*3] 「本人の同意があるとき，又は本人に提供するとき」については「利用目的以外の目的のために保有個人情報を自ら利用し，又は提供することができる．」

[*4] 実装としては Shibboleth と uApprove に管理用の GUI を組み合わせたものであり，Shibboleth IdP の属性定義ファイルをほぼそのまま流用できる

© 2013 Information Processing Society of Japan

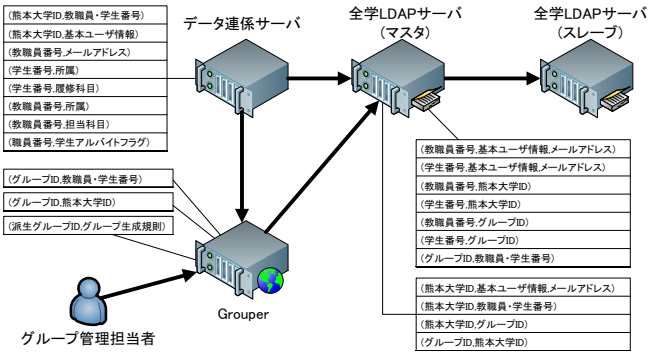

図 4 熊本大学 ID 対応ユーザディレクトリの構成
Fig. 4 System structure of new user directory system

にも対応しており，Sakai や uPortal とも組み合わせて用いられる．グループ情報の編集作業は Web 上の管理画面だけでなく，GrouperShell と呼ばれるコマンドライン環境から行うことも出来る．

Grouper は大学のように権限管理が組織内で分散した環境で利用することが想定されており，グループ定義をデータベースから一括して取り込むことができるだけでなく，定義済みグループの和集合・積集合・差集合からなる合成グループを定義できる．またグループ毎に管理担当者を割り当てることでグループ情報の管理権限を各部局に委譲することができる．

LDAP サーバーにはオープンソースの 389ds[9] を用い，マスタ・スレーブによる冗長構成とした．オープンソースの LDAP サーバーとしては OpenLDAP が広く利用されているが，管理用の GUI フロントエンドや運用に必要な技術資料が標準化されていない．389ds は管理用の GUI フロントエンドが備わっていることに加え RedHat Directory Server と互換性が有り，ReadHat の技術文書をそのまま利用できる．また，389ds には「ユーザーをグループ (groupOfUniqueNames) に対して追加・削除した際，ユーザー側の memberOf 属性の値を自動的に更新する」機能を持つ memberOf プラグインがあり，Grouper との連携にこのプラグインを利用することとした．

5.2 全学 LDAP 用アカウント原簿作成手順

全学 LDAP 用アカウント原簿は「学務情報システム SOSEKI」と「ID 管理システム」の情報を組み合わせてデータ連係サーバに集約される (図 5)．学務情報システムには教職員番号・学生番号を主キーとしたユーザ情報ならびに履修科目・担当科目情報が保存されている．ID 管理システムは熊本大学 ID のために導入したユーザ情報管理用のシステムで，各利用者に対して個人情報の閲覧・変更機能を提供するだけでなく，熊大 ID 発行のための名寄せ機能も持つ．

熊本大学では教職員・学生番号アカウントの初期パスワード管理機能を SOSEKI 上に実装しており，既存 LDAP サーバのための教職員・学生アカウント情報のリストを夜間バッチで作成している．在籍者に対して熊本大学 ID にひもづけられたアカウント原簿を作成するため，このデータを ID 管理システムに取り込み，熊本大学 ID・氏名・読み等の情報を付加した CSV ファイルを生成する．熊本大学 ID とひもづけられた教職員・学生番号 ID は LDAP アカウントの description 属性にコンマ区切りで格納する．

なお，学生のメールアドレスは SOSEKI で管理されているため，この時点で自動的に収集される．教職員のメールアドレスについても SOSEKI 上に登録されているが 5.2.2 節で後述するようにデータが不正確であるため，今回のユーザディレクトリ構築に合わせて手作業でメールアドレスの収集を行った．

以下，熊本大学 ID 発行に伴う名寄せ作業と教職員メールアドレスの収集方法について述べる．

5.2.1 名寄せ作業

熊本大学 ID は個人に対して割り当てられる ID であるため，熊本大学 ID と教職員・学生番号 ID のひもづけには名寄せ作業が必須となる [10]．

現在，名寄せ作業は新規ユーザ登録作業と合わせて月に一度の頻度で行っており，ID 管理システムにユーザ情報の CSV ファイルを取り込む際に名寄せ処理が行われる．ユーザ情報取り込みの際に「性別・生年月日が同じで，氏名 (カナ) または氏名 (英字) が同じ」データが検出されると名寄せ候補として登録処理が保留され，人手による確認を経て登録が完了する．毎月の登録作業の際，数件の名寄せ失敗が発生している．

自動名寄せに失敗したケース (同一人物であることが自動判定できなかったケース) には (1) 氏名表記の違いによるもの (2) 生年月日の誤りによるもの，(3)(稀であるが) 性別の誤りによるもの，が挙げられる．特に外国人の氏名については表記方法が統一されておらず，人事給与システムでは氏名表記にカナ小文字 (「ッ」や「ョ」など) を使っていないことから表記揺れが起きやすい．なお，名寄せを行った後で別人であることが判明したケースはこれまでに起きていない．

5.2.2 教職員メールアドレス属性の収集

学認の一部の SP にはユーザ属性としてメールアドレスを利用するものがあり，また，グループウェアの運用において各ユーザーのメールアドレスが必要となることから，教職員のメールアドレスを収集し全学 LDAP のユーザ属性として登録する作業を行った．

本学では学内の共通情報基盤としてメールアドレスを登録することについて取り決めが無く，現状では各システム内で個別に自身のメールアドレスを登録するようになっている．例えば，学内業務用の Web アプリとして「職員録システム」が整備されており，ここに自分のメールアドレスを登録できるようになっている．また，学務情報システ

© 2013 Information Processing Society of Japan

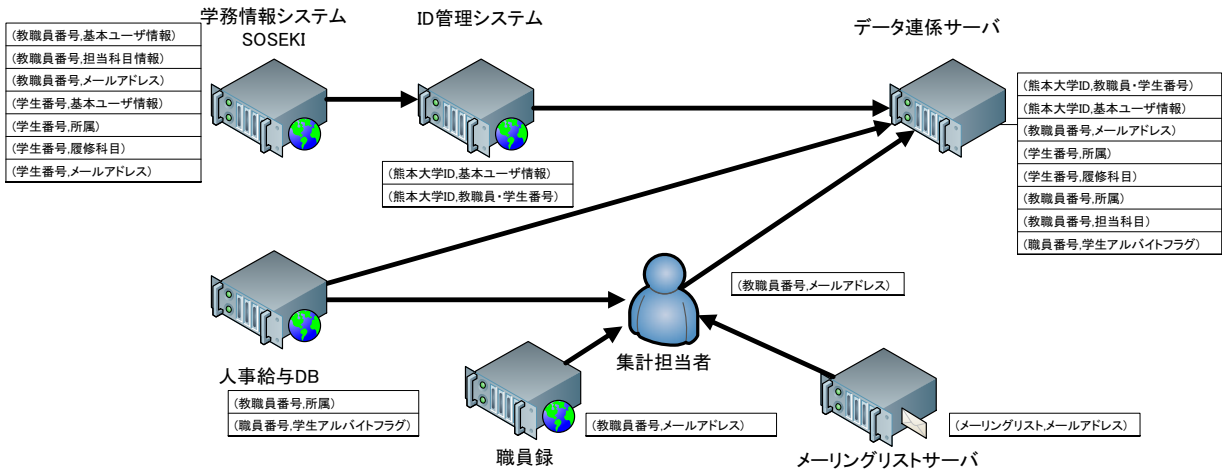

図 5 全学 LDAP 原簿データの流れ
Fig. 5 Dataflow of LDAP master data

ム「SOSEKI」にも自分のメールアドレスを登録できるようになっており，掲示情報のメール通知に利用することができる．しかしながらメールアドレスの登録・更新は義務づけられていない．

学内で利用可能な教職員メールアドレスの収集源には「全学メーリングリスト情報」「職員録情報」があったが，これらの情報は他の用途に利用することを意図したものではなかった．またどのようなメールアドレスを登録するかの規定が無いため，大学のアドレスだけでなくプロバイダのアドレスや携帯電話・Gmail のアドレスなど，個人情報に相当するメールアドレスも含まれていた．

このため，情報企画ユニットを中心として事務局内で協議を行い，全学共通 LDAP のユーザ属性としてメールアドレスを利用する承諾を得るところから作業を行った．今回収集するメールアドレスは業務に用いるものであることから，熊本大学が付与したメールアドレスである「kumamoto-u.ac.jp をドメインに持つメールアドレス」に限定し，人事データとメーリングリスト・職員録情報を付き合わせることで教職員メールアドレスの原簿を作成した．

5.3 全学 LDAP 用グループ原簿作成手順

大学ポータル・グループウェアならびに学認の運用に必要となるグループ原簿の作成手順について述べる．

全学 LDAP グループの作成に必要な原簿は人事給与 DB・学務情報 DB の情報を組み合わせて生成される (図 5)．

(1) 人事情報にもとづくグループ情報
教職員の所属部局情報については人事給与 DB の情報から教職員番号毎の所属コード一覧を生成する．この帳簿から職種・所属部局の情報が得られる．なお，熊本大学では学生アルバイトも契約上は有期雇用職員として雇用される．情報アクセス制御の観点からは一般の有期雇用職員と学生アルバイトを区別する必要があるため，有期雇用職員と学生アルバイトの区別が付くよう，学生アルバイトに該当する有期雇用職員の番号一覧を別途生成している．

(2) 学務情報にもとづくグループ情報
学生の所属部局情報は SOSEKI 上で管理されており，学生番号と所属部局コードの一覧，ならびに学生番号と履修科目コードの一覧を夜間バッチで生成する．教員の担当科目も SOSEKI 上で管理されており，教員番号と科目コードの一覧，ならびに開講科目一覧を夜間バッチで生成する．

学認用の student,faculty,staff グループはこれら基底グループの集合和からテストアカウントグループを差し引いた合成グループとして Grouper 上で定義している．なお学認運営における student グループは本学の学籍を有する者を該当者とし，faculty,staff グループについては常勤の教職員を該当者とすることで運用を開始した．その他のケースについては学内にワーキンググループを設け，継続的に検討する体制を設けている．

6. 学認対応 Shibboleth IdP の構築

学認運用フェデレーションならびに CAS ゲートウェイに対する認証源として Shibboleth IdP を構築した．熊本大学 ID での認証後，CAS ゲートウェイに対し uid 属性 (認証に用いた熊本大学 ID),description 属性 (熊本大学 ID にひもづけられた教職員・学生番号 ID),title 属性 (SP 固有の作業用アカウント) を送出する．本節ではシステム構成と IdP 構築において考慮した事柄について述べる．

6.1 システム構成と主な設定内容

学認対応 Shibboleth IdP として，Shibboleth・uApprove.jp 相当の機能を持つネットスプリング社製 AXIOLE IdP アプライアンスを導入した．アプライアンス 2 台に

© 2013 Information Processing Society of Japan

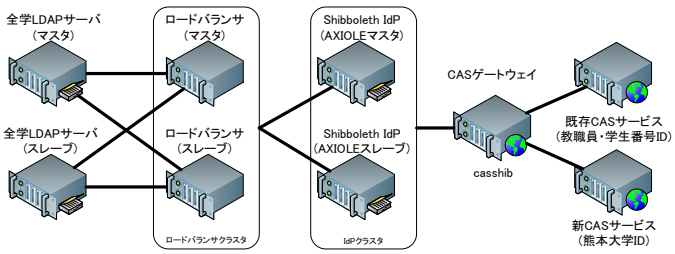

図 6 CAS ゲートウェイシステム構成
Fig. 6 System structure of CAS gateway

よる冗長構成 (マスタ・スレーブによるホットスタンバイ構成) としている．なお AXIOLE ではユーザ認証源となる LDAP サーバーを一台しか指定できない．可用性を確保するため，LDAP サーバーをソフトウェアロードバランサー (ZenLoadBalancer) の配下に置いたクラスタ構成とし，AXIOLE からは LDAP クラスタの代表 IP アドレスを参照するようにしている (図 6)．

金沢大学における Shibboleth IdP 構築事例 [4] などを参考に以下の設定を行った．

6.1.1 eduPersonPrincipalName 属性の設定

ePPN 属性の値として熊本大学 ID のハッシュ値を設定するよう，文献 [4] の **ePPN** 属性記述方法を参考に Script タグを用いて属性定義を行った．

6.1.2 eduPersonAffiliation 属性の動的な設定

ユーザの所属グループに応じて **ePA** 属性を設定するため，Script タグを用いてソースコード 1 のように属性を定義した．ユーザーが全学 LDAP において shibboleth:student, shibboleth:faculty, shibboleth:staff のどのグループに所属しているかに応じて **ePA** 属性の値が動的に設定される．

6.1.3 SP 固有の作業用アカウント属性の定義

特定のユーザーに対して SP ログイン時の選択対象ユーザ ID に SP 固有の作業用アカウントを追加するため，各 SP に応じた title 属性の定義を行っている (ソースコード 2)．この例では userA,userB,userC に対し，選択対象のユーザ ID に admin が含まれるように title 属性を定義している．なお，uid 属性にもとづいて作業用アカウントを追加するだけでなく，memberOf 属性を用いて所属グループに応じた作業用アカウントを割り当てることもできる．

6.1.4 外部 SP に対するユーザ属性の送出制限

今回構築した全学 LDAP サーバでは，在籍者・在職者のみが学認用グループに登録されるようになっている．これらのグループに登録されていないユーザーが学認フェデレーション対応の外部 SP を利用できないようにするため，学認用グループに属さないアカウントについては ePPN 属性を始めとするユーザ属性を外部 SP に送信しないように SP 毎にフィルタ設定を行った (ソースコード 3)．

6.2 卒業生・退職者に対応する熊本大学 ID アカウントの取り扱い

これまで運用してきた教職員番号アカウント・学生番号アカウントでは，熊本大学に在籍しなくなった後一定期間経過後に LDAP からアカウント情報そのものを削除していた．これに対し，生涯 ID として運用される熊本大学 ID の場合は大学に在籍しなくなった後でもアカウントは有効である．このため，卒業生・退職者についても LDAP での認証自体は行えるため，松平らの事例 [4] で指摘されているようにユーザ属性によるアクセス制限を行っていない SP との間で利用契約上の問題が生じる．

この問題の解決策として，Shibboleth IdP については SampleFilterPerSP を用いる方法が西村らによって提案されている [11]．ShibbolethIdP にフィルタ処理のためのサーブレットを追加することで，在籍しないアカウントの特定 SP に対するアクセスを禁止するというものである．

今回認証基盤に採用した AXIOLE は Shibboleth にもとづいた実装となっているが利用者側でサーブレットを追加できる作りにはなっていないため，この方法を用いることができなかった．そこで，6.1.4 節で述べたように在籍しないアカウントについては外部に ePPN 属性を始めとするユーザ属性を送信しないように属性フィルタリングを行っている．これにより SP 側のログイン処理が失敗に終わるため，SP の利用者を在籍者に制限することができる．

ただし，この実現方法は利用者から見ると「SP 側でエラーが起きた」ことになるため「自身に利用資格がないことが原因」であることが分からない．本来は IdP 側で利用資格がない旨を表示するように対応すべきであり，あくまで代用手段である．

7. ユーザ ID 体系移行用 CAS ゲートウェイの構築

本節では今回構築した CAS ゲートウェイのシステム構成，ログイン時のユーザ ID 選択機能実現方法，ならびに運用方法について述べる．

7.1 システム構成

CAS ゲートウェイ本体は shibd が稼働する Apache サーバと tomcat サーブレットコンテナから構成され，tomcat 上で casshib サーブレットが動作している．casshib は shibd によって設定された HTTP ヘッダ経由で Shibboleth IdP から uid,description,title 属性を受取り，CAS SP に対するユーザ ID 選択機能付シングルサインオン機能ならびにユーザ属性送信機能を提供する (図 6)．

7.2 casshib を用いたユーザ ID 選択機能の実現

casshib は Spring Web Flow を用いて実装されており，状態遷移フローが XML ファイルに定義されている．この

© 2013 Information Processing Society of Japan

ソースコード 1 eduPersonAffiliation 属性の定義

```
<resolver:AttributeDefinition
   xsi:type="ad:Script" id="eduPersonAffiliation" sourceAttributeID="memberOf">
    <resolver:Dependency ref="axioleExternalLdapConnector"/>
    //紙面の都合上,eduPersonAffiliation 属性の AttributeEncoder の記述を省略
    <ad:Script><![CDATA[
        importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);
        eduPersonAffiliation = new BasicAttribute("eduPersonAffiliation"); eduPersonAffiliation.getValues().add("member");
        if (typeof memberOf != "undefined" && memberOf != null ){
            count = memberOf.getValues().size(); shibPrefix = "cn=shibboleth"; shibPrefixLength = shibPrefix.length;
            facultyGroup="cn=shibboleth:faculty,ou=kugroups,dc=kumamoto-u,dc=ac,dc=jp";
            staffGroup="cn=shibboleth:staff,ou=kugroups,dc=kumamoto-u,dc=ac,dc=jp";
            studentGroup="cn=shibboleth:student,ou=kugroups,dc=kumamoto-u,dc=ac,dc=jp";
            for ( i = 0; i < count; i++ ){
                value = memberOf.getValues().get(i);
                if(value.substring(0,shibPrefixLength) != shibPrefix) continue;
                if(value == studentGroup) eduPersonAffiliation.getValues().add("student");
                else if(value == facultyGroup) {
                        eduPersonAffiliation.getValues().add("faculty"); eduPersonAffiliation.getValues().add("staff");
                } else if(value == staffGroup) eduPersonAffiliation.getValues().add("staff");
            }
        }
    ]]></ad:Script>
</resolver:AttributeDefinition>
```

ソースコード 2 SP 固有の作業用アカウント属性の定義

```
<resolver:AttributeDefinition xsi:type="ad:Mapped" id="title-confluence" sourceAttributeID="uid">
    <resolver:Dependency ref="axioleExternalLdapConnector"/>
    //紙面の都合上, title 属性の AttributeEncoder の記述を省略
    <ad:DefaultValue passThru="true"/>
    <ad:ValueMap>
        <ad:ReturnValue>$1,admin</ad:ReturnValue>
        <ad:SourceValue>(userA|userB|userC)</ad:SourceValue>
    </ad:ValueMap>
</resolver:AttributeDefinition>
```

定義を変更することで，状態遷移の条件や遷移先のサーブレットのカスタマイズを比較的容易に行うことができる．

元の casshib の実装では，shibd によって設定された REMOTE_USER の値にもとづいて credential を生成する処理が remoteAuthenticate アクションで実装されていた．ユーザ ID 選択画面に対応するサーブレットを実装し，remoteAuthenticate の状態遷移フローを変更することで図 7 のようにユーザ ID 選択機能を実装した[*5]．ここで，remoteAuthenticate 呼び出し時点で Shibboleth IdP から送出された uid 属性が REMOTE_USER に設定されているものとする．

ユーザ ID 選択画面は既存の CAS サーバのデザインを踏襲し，表示言語も切り替えられるようにしている (図 8).

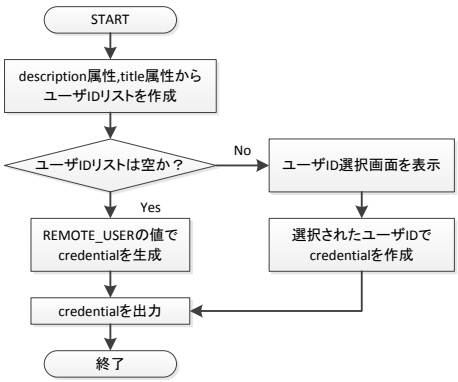

図 7 remoteAuthenticate アクションにユーザ ID 選択処理を追加
Fig. 7 flowchart of modified remoteAuthenticate action

7.3 運用方法

casshib では仮想 IdP 毎に異なったユーザ属性を保持することができ，また同じ仮想 IdP を参照する CAS SP 間ではユーザ属性を共有することができる．このことを利用し，(1) 既存 ID を必要とする CAS クライアントのための共有仮想 IdP,(2) 熊本大学 ID 対応 CAS クライアントのための共有仮想 IdP,(3) その他 CAS クライアント用の独立仮想 SP, の 3 種類の仮想 IdP を casshib 上に定義した (図 9).

(1) の共有仮想 IdP は既存 CAS クライアントに対して

[*5] 今回の実装は CAS 3.4 系の最終版を元に実装された casshib-3.4.11a をベースにしている．

© 2013 Information Processing Society of Japan

ソースコード 3 ePPA に基づいたユーザ属性の外部送出制限の例

```
<afp:AttributeFilterPolicy id="releaseAttributesToExternalSP">
  <afp:PolicyRequirementRule xsi:type="basic:AND">
    <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://serviceURI/shibboleth-sp"/>
    <basic:Rule xsi:type="basic:AttributeValueRegex" attributeID="eduPersonAffiliation" regex="student|faculty|staff"/>
  </afp:PolicyRequirementRule>
  <afp:AttributeRule attributeID="eduPersonPrincipalName">
    <afp:PermitValueRule xsi:type="basic:ANY"/>
  </afp:AttributeRule>
</afp:AttributeFilterPolicy>
```

図 8 ユーザ ID 選択画面
Fig. 8 UserID selection UI

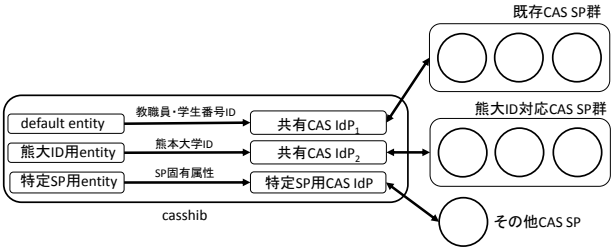

図 9 casshib の運用設定
Fig. 9 Configuration of casshib for deployment

CAS サーバの透過的な移行を可能にするためのものである．(2) の共有仮想 IdP は熊本大学 ID による認証だけを必要とし，ユーザー属性を必要としない CAS クライアントに用いる．(3) の独立仮想 IdP は認証だけでなくユーザ属性を必要とする場合，他の SP とは独立してユーザ ID を選択させたい場合，および，SP 固有のユーザアカウントを選択対象のユーザ ID に加えたい場合に用いる．

8. 運用状況

本節では熊本大学 ID, ユーザディレクトリならびに CAS ゲートウェイの運用状況について述べる．

8.1 熊本大学 ID 運用状況

学生については 1999 年度以降の在籍者，教職員については 1997 年度以降の在籍者に対して名寄せ作業を行い，熊本大学 ID の発行を終えている (2013 年 10 月末時点で 56,265 件)．熊本大学 ID そのものは学外者に対しても割り当て可能であるが，現在の運用ではまだ ID の発行を行っていない．

8.2 ユーザディレクトリ運用状況

データ連係サーバから Grouper へのデータ取り込みは定常運用に入っている．基底グループとして職種・部局に関するグループ (2013 年 10 月末時点で約 800 グループ)，学籍・学年・学科・専攻に関するグループ (2013 年 10 月末時点で 186 グループ) を取り込み，更に開講科目に関する受講生・担当教員グループ (2013 年 10 月末時点で 17140 グループ) を毎晩深夜に取り込み，LDAP に同期させている．

登録グループ数が多いことに加え，既存の教職員・学生番号 ID と熊本大学 ID の両方のグループを LDAP に保持することにしたため，稼働当初は Grouper の LDAP 同期処理に 12 時間以上かかることがあった．Grouper ならびにバックエンドデータベースの設定を見直すことで，最終的に一回の同期に要する時間を 2 時間以内に短縮した．

グループウェアでの LDAP 利用については Confluence との連携を既に行っており，教職員アカウントならびに職種・部局に関するグループを Confluence に取り組んでいる．これによりグループウェア全学運用の目処が立ったため，各業務グループ用の初期設定作業を進めているところである．

8.3 認証基盤運用状況

学認用認証基盤については部局内の動作テストを経た後，2013 年 10 月に運用フェデレーションの申請を行い，10 月末より運用フェデレーションでの稼働を開始した．CAS ゲートウェイについては試験運用段階にあり，部局内サービスでの日常利用による長期動作テストを経た後，既存 CAS サーバから切り替える予定である．

9. 関連事例との比較

9.1 CAS 対応サービスの組織間共有事例との比較

CAS 対応サービスを組織間で共有する取り組みとして，CAS サーバに独自の機能拡張を行うことでユーザ認証源となる LDAP のマルチソース化を行った福井県大学間連携プロジェクト (F レックス) の事例 [12] や，東海アカデ

© 2013 Information Processing Society of Japan

ミッククラウドの事例 [13] があるが，現在のところこれらの事例では実装が公開されていない．

今回の我々の CAS ゲートウェイの実装はオープンソースの casshib にもとづいており，Shibboleth DS との連携で CAS 対応サービスの組織間共有に対応できるだけでなく，ユーザ ID の読み替えにも対応することができる．

9.2 IdP における SP アクセス制限実装事例との比較

CAS サーバの機能を拡張し，ユーザ属性の送出と SP に対するアクセス制限を IdP 側の機能として実現した事例として，内藤・梶田らによる CAS^2 の事例が挙げられる [14]．CAS^2 では，「どのユーザがいつどこからどのように」アクセスしたかに応じて SP に対するアクセスを許可するよう，各 SP に対する ACL(Access Control List) を IdP 用の LDAP に記述することでアクセス制限を実現している．

CAS^2 は IdP 側で SP に対するアクセス制御を集中管理できる点で優れた実装であるが，CAS^2 の実装は CAS 本体に統合されておらず，2007 年以降更新されていない．このため，今後 10 年単位で認証基盤として運用することを考えると採用には慎重にならざるをえない．

Shibboleth IdP では SampleFilterPerSP プラグインを IdP に追加することで SP へのアクセス制限を実現できるが [4][11]，この手法は自由にプラグインを追加できない商用 IdP 製品には適用できない．

今回我々が構築した認証基盤では代替策として Shibboleth の標準機能である属性フィルタリングを用いて ePPN を始めとするユーザ属性の発行制御を行っており，IdP 自体の改修は不要である．また，CAS-3.4 系の casshib 実装にもとづいており，中期的な運用には支障がない．

10. まとめ

本報告では生涯 ID の導入に伴う認証基盤の再構築について述べた．ユーザー属性にもとづいた情報システムへのアクセス制御を可能とするため，人事給与システム・学務情報システムと連携したユーザディレクトリを構築し，既存の教職員・学生番号 ID と生涯 ID を紐づけたユーザー情報の配信を可能とした．

ユーザ ID 体系移行ならびに学術認証フェデレーション対応のための認証基盤として，Shibboleth 互換 IdP と CAS ゲートウェイの組み合わせによるシングルサインオン環境の構築方法を示した．ユーザ ID 選択機能を CAS ゲートウェイ上に実装することで，IdP における認証動作そのものに手を加えることなく ID 選択機能を実現している．

今回教職員メールアドレスの収集作業は人手で行っており，作業の自動化・メールアドレス登録窓口の一本化等，帳簿を最新の状態に保つための仕組み作りが残されている．最新のメールアドレスを登録しておくことがユーザー自身のメリットになることが分かるよう，各種連絡手段やグループウェアでのメール属性の活用事例を示すことが当面の課題である．

謝辞 本研究は JSPS 科研費 24501195 の助成を受けたものです．

参考文献

[1] 杉谷賢一：熊本大学学務情報システム － SOSEKI －，学術情報処理研究誌， No. 3, pp. 49–50 (1999).
[2] 熊本大学：総合情報環構想 2010, http://www.kumamoto-u.ac.jp/daigakujouhou/katudou/johokankoso.
[3] Perkins, E. L. and Allan, A.: Consider Identity and Access Management as a Process, Not a Technology, *Gartner Report*, No. G00129998 (2005).
[4] 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， No. 16, pp. 41–50 (2012).
[5] 江原康生，村尾靖子，山口文雄：大阪大学における新全学 IT 認証基盤システムの構築と移行，情報処理学会研究報告. IOT, [インターネットと運用技術]， Vol. 2011, No. 1, pp. 1–6 (2011).
[6] casshib: An extension to enable the CAS server to act as a Shibboleth service provider proxy, https://code.google.com/p/casshib/.
[7] Orawiwattanakul, T., Yamaji, K., Nakamura, M., Kataoka, T. and Sonehara, N.: User-controlled Privacy Protection with Attribute-filter Mechanism for a Federated SSO Environment Using Shibboleth, *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, pp. 243–249 (2010).
[8] Grouper: an enterprise access management system, https://spaces.internet2.edu/display/Grouper/.
[9] 389 Directory Server: The enterprise-class Open Source LDAP server for Linux, http://directory.fedoraproject.org/.
[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] 西村 健，中村素典，山地一禎，大谷 誠，岡部寿男，曽根原登：日本における学術認証フェデレーションとその役割および効果 (インターネット運用・管理, 一般)，電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ， Vol. 111, No. 375, pp. 5–8 (2012).
[12] 篭谷隆弘，西出恭生，梶田将司，山川 修：CAS マルチソース化による大学間共通認証と Web サービスへの実装，情報処理学会研究グループ報告 第 11 回 CMS 研究会，Vol. 2009-CMS-11, pp. 50–53 (2009).
[13] 梶田将司，齋藤彰一，土屋雅稔，山本大介，鈴木常彦，山口由紀子，長谷川孝博，長谷川明生，田中昌二，内田裕市，三橋一郎，太田義勝，高倉弘喜，松尾啓志：Shibboleth・CAS 連携による東海アカデミッククラウド認証基盤の構築，電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ， Vol. 111, No. 321, pp. 49–53 (2011).
[14] 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).

© 2013 Information Processing Society of Japan