Vol.2018-CLE-25 No.9
2018/6/16

京都工芸繊維大学における利用者原簿管理基盤の強化と連携サービスの構築

永井 孝幸[1,a)]　山岡 裕美[1]　桝田 秀夫[1]

概要：京都工芸繊維大学では 2018 年 3 月に情報基盤計算機システムの更新を行い，共通サービス基盤システム・教育用計算機システム・事務システム・図書館システムを一斉に更新した．今回のシステム更新では学外関係者に対しても本学のサービスを提供できるように個人に紐付く生涯 ID を扱えるよう利用者原簿管理基盤を強化し，Shibboleth と Grouper を核とした統合認証基盤を構築した．旧システムではサービス毎の認証源に個別にアカウントを登録することでサービス利用制限を実現していたが，新システムではユーザの所属グループ属性を参照することでサービス利用を制限する方式に変更した．この方式では Grouper を用いたグループ管理と組合わせることで，新サービスの追加に対して柔軟にアクセス制御を実現することができる．本報告では利用者原簿管理を中心とした統合認証基盤の紹介と，ファイル共有・CMS・LMS 等の連携サービス構築結果について述べる．

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

Renewal of Identity and Access Management infrastructure and integrated services in Kyoto Institute of Technology

Abstract: In March 2018, Kyoto Institute of Technology renewed its computer infrastructure to update the common service infrastructure system, educational computer system, office system, and library system all at once. In this update, we implemented identity and access management infrastructure with Shibboleth and Grouper so that we can handle lifelong ID; that enables us to provide outside stakeholders with university services. To restrict available services for a user, the user account is individually registered to authentication sources for allowed services in the old system. In the new system, we moved to a new method of restricting available services by referring to the belonging group attribute of the user. When a new service is introduced, we can flexibly realize additional access control by managing the associated user group with Grouper. In this report, we introduce the integrated authentication infrastructure with unified user information database and the result of system integration for services such as file sharing, CMS, LMS and so on.

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

1. はじめに

京都工芸繊維大学では 2018 年 3 月に情報基盤計算機システムの更新を行い，共通サービス基盤システム・教育用計算機システム・事務システム・図書館システムを一斉に更新した．これまで情報科学センターの提供するシステムでは学籍・職責に紐付いたアカウント (**CIS アカウント**) を用いてきたが，今回のシステム更新では学外関係者に対しても本学のサービスを提供できるよう，個人に紐付く生涯 ID(**工繊大パーソナル ID**) を扱えるように利用者原簿管理基盤を強化し，Shibboleth と Grouper[1] を核とした統合認証基盤を構築した．旧システムではサービス毎の認証源に個別にアカウントを登録することでサービス利用制限を実現していたが，新システムではユーザの所属グループ属性を参照することで利用可能サービスを制限する方式に変更した．この方式では Grouper を用いたグループ管理と組合わせることで，新サービスの追加に対して柔軟にアク

[1] 京都工芸繊維大学情報科学センター
Matsugasaki, Sakyo-Ku, Kyoto-City, Kyoto, 606-8585, Japan
[a)] nagai@kit.ac.jp

セス制御を実現することができる．

本報告では利用者原簿管理を中心とした統合認証基盤の紹介と，ファイル共有・CMS・LMS 等の連携サービス構築結果について述べる．まず今回のシステム更新の初期検討段階で抽出した課題について 2 節で述べる．次に 3 節で生涯 ID 導入にあたり解決すべき課題について述べる．システムの仕様の検討にあたって利用した技術検証環境を 4 節で紹介する．新システムの概要を 5 節で述べ，最後に 6 節で今後の課題について述べる．

2. システム更新の課題

著者の永井は 2016 年度に京都工芸繊維大学に着任したため，前回 2014 年度の全学システム更新から現在に至るまでの経緯について詳細を把握していなかった．そこで，前回システム更新時に残されていた資料の精査と現状の把握からシステム更新における課題の抽出を行った．

2.1 全学情報インフラにおけるこれまでの取り組み

京都工芸繊維大学では全学情報インフラをサーバ系とネットワーク系に分けて更新している．サーバ系システムは 4 年おきに更新されてきており，サーバ基盤の増強に加えて利用者原簿や認証基盤の整備も順次行ってきた．

2006 年に更新した第 7 世代の全学情報システム (System7) で利用可能な学内サービスを利用者区分に応じて制限する仕組みが導入された [2]．2010 年に更新した第 8 世代の全学情報システム (System8) で統合認証基盤が導入され，各認証サーバに登録するアカウント情報を共通の利用者原簿から発行する仕組みと Shibboleth によるシングルサインオン環境が実現した．アカウントの初期状態では最低限の学内サービスのみ利用を許可し，Moodle 上の確認テストに合格した後でないと残りのサービスを利用できないように制限する仕組みもこの世代で導入している [3]．

2014 年に更新した第 9 世代の全学情報システム (System9) では情報工学教育用システム，事務システム，図書館システムとの一括調達を行う方式に変更され，仮想化基盤統一による可用性向上を実現した．人事課・学務課情報と連携してアカウントを自動的に有効化・無効化する仕組みや，サービス固有認証トークンの仕組み [4] に加え，情報共有基盤としてコンテンツ管理システム (Plone), ファイル共有システム (Proself) も導入されている．

全学ネットワークもサーバ系の更新に対応して機能強化が行われており，VPN 接続や eduroam 等のネットワーク側ユーザ認証についても共通利用者原簿上でアカウント管理を行うようになっている．2008 年にキャンパス間遠隔会議のために導入された TV 会議端末 (Polycom) も戦略的大学連携支援事業[*1],COC 事業[*2]の実施に合わせて順次整備が行われてきた．

[*1] https://www.kit.ac.jp/program/strategic/
[*2] https://www.kit.ac.jp/coc/coc_publications/

表 1 次期システム検討初期段階での System9 利用状況
Table 1 System9 usage status after initial review

導入年	サービス	システム	利用状況
199X	仮想Webホスティング	Apache	全学大規模利用
2008	TV会議	Polycom	ユースケース拡大
2010	統合認証	Shibboleth	学内利用のみ
2010	全学LMS	Moodle	全学定常利用
2012	eduroam	認証用Radius	全学定常利用
2014	サービス別認証トークン	認証用Radius	大規模展開できず
2014	ファイル共有	Proself	大規模展開できず
2014	コンテンツ管理	Plone	運用にいたらず

2.2 System9 導入結果の振返り

情報科学センターの位置づけは「基幹コンピュータシステム，学内情報ネットワークその他の情報基盤の構築，管理，運用及び保守を行うこと.」(京都工芸繊維大学情報科学センター規則第 2 条 (4)[5]) となっており，サービス部門ではなくインフラ部門として性格づけられている．しかし，提供サービス内容を決めずに基幹計算機システムを調達することは不可能である．提供すべきサービス内容については System9 の調達に先立つ 2013 年 5 月時点ですでに体系的な検討が行われている．この検討結果に基づき，認証基盤の強化と情報共有基盤の整備を行ったのが System9 導入時の意図であった．

導入時の意図がどの程度実現されたか把握するため，著者の永井が主要サービスの利用状況を確認したところ，意図通りに活用されていない部分が見受けられた (表 1)．

TV 会議システムについてはキャンパス間遠隔会議での利用だけでなく，スーパーグローバル大学創成支援事業での利用や学内イベントの中継など導入当初の想定を超えた用途で活用されており，遠隔会議ではなく映像中継サービスとしての見直しが必要な状況であった．

Shibboleth 認証については基幹システムとして一括調達したシステムについては整備が完了しているが，各部局で個別に調達したシステムについては LDAP 認証が主に利用されている状態であった．また，学認連携についてもテストフェデレーション参加から先に進んでいなかった．

共同編集に対応したコンテンツ管理システムとして導入された Plone については認証基盤との連携がうまくいかず，運用を断念した状態であった．その一方で，Apache の VirtualHost 機能を用いた仮想 Web ホスティングサービスによって大量の PukiWiki や WordPress サイトが構築され，部局や研究室の Web サイトとして活用されていた．

Proself は業務文書の保管場所や学外業者とのファイル受け渡し手段として活用されていたものの，グループ原簿と連携する機能がないためにグループ内情報共有のインフラとして使うには運用の負担が大きく，大規模展開できない状態であった．また，保存した文書に対してファイル名

での検索しかできず，必要な文書がどこにあるかは誰かに聞かなければ分からない，という状態であった．

2.3 サービス稼動状況についての考察

日々登場する最新の携帯デバイスやモバイルアプリ，クラウドサービスによって利用者の状況が刻々と変化するため，全学での活用を期待して導入したシステムが思ったほど活用されないことは当然想定される．しかし，関係者に話を聞いてみたところ以下のように依然としてニーズは健在であり拡充が必要なサービスであることが確認された．

- 海外派遣先の大学から卒業研究発表会に参加するため，発表者の映像だけでなく発表スライド・会場映像も同時に中継してほしい
- 学外の関係者と大容量ファイルを受け渡しできる仕組みを整備してほしい
- 個人情報を含むファイルをメールで配布しないで済む仕組みを整備してほしい
- 共同研究プロジェクトの学外メンバーも学内ネットワークを使いたい
- 入試の早期合格者に e-learning を受講して欲しい
- Web サイトを共同編集できる仕組みを整備してほしい
- オンラインでイベント参加申し込みを受付けられる共通の仕組みを整備して欲しい

System9 整備の方向性は間違っておらず，利用者の求める水準に追いついていない状況であると判断した．ここで注目するべきは，サービス提供に利用可能な機器・システムが導入されているにも関わらず十分なサービスを提供できていない部分である．サービス別に要因を紐解いていくと，概ね以下の要因に整理された．

- サービス容量不足 (Polycom)
- 技術的な行き詰まり (Plone)
- 機能不足 (Proself)
- 運営用システムの不足 (サービス別認証トークン)
- アカウント付与体系の限界 (Moodle)
- 利用者属性情報の不足 (Shibboleth)

2.4 全学情報システム運用において生じた制約

情報システムは運用期間を通じて少しずつ改善が加えられていくものであるが，System9 の導入から 3 年経過した 2017 年の時点でも解決が見えなかった部分がある．どのような制約が原因となっていたか主要な点について述べる．

2.4.1 実現サービスの欠損に起因する制約

サービスマネジメントの枠組みである ITIL において，サービスは (1) 利用者にとって基本的な成果を提供する**コアサービス**，(2) コアサービスの提供に必要となる**実現サービス**，(3) コアサービスに追加される**強化サービス**の 3 つに分類される．利用者が直接目にするのがコアサービスの部分であり，例えば演習室端末や電子メールが該当する．実現サービスはインフラ部分に相当し，サーバ基盤やネットワーク，認証基盤などが該当する．VPN 接続は強化サービスに該当する．

この枠組みに当てはめて考えると，System9 で利用が進んでいないシステムは実現サービスの欠損が原因と思われた．限られた予算内でシステムを調達する場合，コアサービスの整備が最優先となるが実際には実現サービスが無ければサービスは使えない．学認運用フェデレーションや認証付 CMS の運用には「グループ原簿」「利用資格原簿」を提供する「利用者原簿サービス」の整備が必要であるが，これまで明示的に検討されてこなかったサービスである．

2.4.2 ベンダー独自実装に起因する制約

System9 の利用者原簿管理システムとしてベンダー独自システム (NEC システムテクノロジー社製 SyntheUniv) が導入されていた [3]．このシステムはユーザの個人属性・アカウント属性の管理，データ連係，アカウントのプロビジョニング処理，利用者ポータルをすべて提供する統合システムである．データベース項目の定義やシステム間の連携処理, 利用者ポータルの表示項目をシステム構築時にベンダー側で作り込む方式であるため，導入後に継続的に改善を加えることは想定されていない．

利用資格管理のための項目の追加やそれに合わせた利用者ポータルの変更など，実現サービスの構築を継続的に行う仕組みがないことも大きな制約であった．

2.4.3 アカウント発行方式に起因する制約

学生に付与する CIS アカウントは入学年度の下一桁と学生番号，所属課程を組合わせた附番方式となっている．このため，原理的に 10 年毎にアカウントの重複が発生する．学部の在籍期間が最長 8 年であるため，この点は長らく問題として認識されてこなかった．

しかし Moodle の運用期間が 10 年を超えたところで問題が発生した．過去のコース情報を全て引継ながら運用してきたために Moodle 内部でログイン ID の重複が発生し，意図しないユーザがコースに登録されたり，同じログイン ID を持つ過去のユーザの情報が表示されるようになった．学生の視点から見れば CIS アカウントの寿命は 10 年で十分であるが，データの寿命の観点からは不十分である．

また，工繊大パーソナル ID 導入時は認証用 ID としての運用が十分に考慮されておらず，CIS アカウントと区別せずに LDAP 上に登録されていた．このため単純に LDAP からユーザ情報を取り込むと同一人物の CIS アカウントと工繊大パーソナル ID が全て取り込まれてしまい，データ集計に支障をきたしていた．CIS アカウントと工繊大パーソナル ID が混在しないように LDAP の再設計が必要であるが，共通利用者原簿のデータ連係設定や各システムの認証連携設定はシステム構築時点でほぼ固定されているため，修正できない状況であった．

3. 生涯 ID 導入にあたり解決すべき課題

次期システムにおいて生涯 ID に対応することは自明であったが，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 認証用利用者原簿の整備

京都工芸繊維大学では，学内での進学時に学生番号が変わっても同一のメールアドレスを使い続けられるようにすることを目的に，生涯 ID とそれを用いた生涯メールシステムを 2016 年度に導入した．導入時点では生涯 ID はメールアドレスとして利用することのみを想定しており，認証用ユーザ ID として利用することは想定されていなかった．このため，認証基盤用のアカウント原簿の構築から着手する必要がある．

3.2 利用可能サービスの認証基盤における制限方法

System9 では VPN 接続など一部のサービスについて利用者を制限する仕組みが導入されており，利用者区分 (学生, 教職員など) 毎にアカウント登録先の認証サーバを限定することでこの機能を実現している．CIS アカウントの利用者区分は大きく教職員・学生に区分され，そこから更に所属部局・課程によって細分される．

各アカウントはいずれか 1 つの区分に分類されるという大前提で構築されており，TA のように同一人物が「学生」と「職員」の複数の役割を持つ場合，利用者が複数のアカウントを使い分けることで対応している．

これに対して生涯利用可能なアカウントでは，同一人物が複数の役割を持つ場合，該当する複数の利用者区分を保持できるように利用者原簿の仕組みから見直す必要がある．また，利用者には学外利用者も含まれるために組織構造を利用者区分に当てはめるという前提が成り立たず，階層型の利用者区分も適さない．利用者を階層型に区分する代わりに，利用者の所属するグループや利用資格に応じて複数の「タグ」を付与する方式に切替える必要がある．

3.3 名寄せ作業

工繊大パーソナル ID は個人に対して割り当てられる ID であるため，工繊大パーソナル ID と CIS アカウントの紐付けには名寄せ作業が必須となる．学生の場合，学部在籍時の学生番号を SyntheUniv 上の利用者属性に持たせることで，内部進学者については名寄せ処理を自動化している．しかし，科目履修生や非正規生については別帳簿での管理が発生しており人手での確認作業が必要になる．

また，教職員については自動で名寄せを行う仕組みが整備されていない．学務課と人事労務課の間で情報共有も行っていないため，学生が本学に雇用されたケースや職員が学籍を有する場合の名寄せ作業を確実に行える場がない．

複数部局の担当者が利用者原簿を参照して名寄せ作業を行う仕組みが必要である．

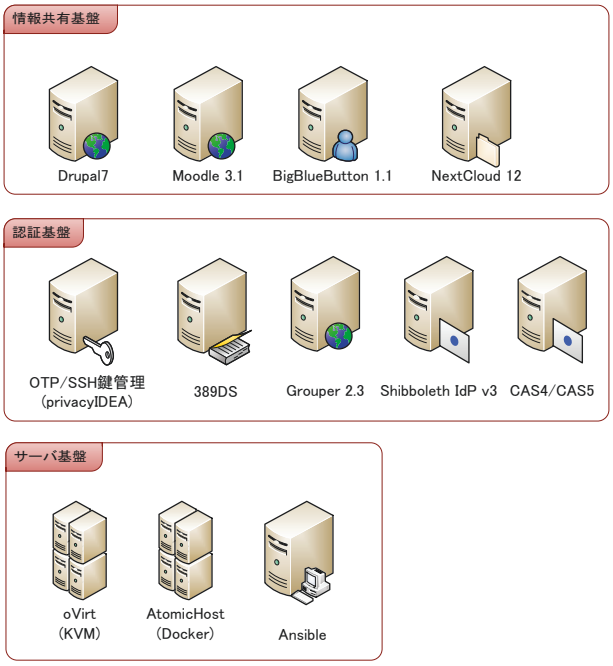

図 1 教育情報システム研究室の技術検証環境
Fig. 1 Test environment in educational technology laboratory

4. 技術検証環境の構築

合理的なシステム仕様を定めるには事前の技術検証が不可欠である．本節では学内に構築した技術検証環境について紹介する．

4.1 学習支援システム用テスト環境の構築

著者の永井が主催する教育情報システム研究室ではオンライン学習支援環境の研究開発に必要となるテスト環境としてサーバ基盤・認証基盤を独自に構築し，学習支援システムのテスト環境を構築している．具体的には仮想化基盤 (oVirt, AtomicHost, ansible), 認証基盤テスト環境 (389DS, Grouper, Shibboleth, CAS, privacyIDEA, YubiKey), 情報共有基盤 (Moodle, Nextcloud, Drupal, BigBlueButton) からなる環境である (図 1).

これは学習支援システムのテスト環境を意図したものであり，Moodle,Nextcloud 等のオンライン学習用システムにおいて利用者属性連携，グループ属性連携，シングルサインオン，LDAP 認証連携，等の技術検証を行うことができる．例えば，CAS5 サーバと privacyIDEA を連携させることで「学外から Drupal にログインする際は YubiKey による多要素認証を要求する」といった認証機構を実現できる．全学の情報システム更新とは独立の活動であるが，今

回のシステム更新においてもこのテスト環境で得られた知見を調達仕様書やシステム設計に反映している．

4.2 工繊大パーソナル ID 対応認証基盤の構築

工繊大パーソナル ID 対応認証基盤の技術試験環境を兼ね，学認運用フェデレーションに対応した認証基盤を情報科学センター内に構築した．学認用 IdP では利用者識別子 (**ePPN**) の生成に生涯 ID 相当の属性を取り扱うことが必須となるため，学認運用フェデレーションに対応できることが生涯 ID 対応の 1 つの目安となる．

ansible と oVirt/AtomicHost を組合わせることでシステム構築作業を簡略化することを目指し，GitHub で配付されている Unicon 社のコンテナイメージ[*3] をカスタマイズして Shibboleth と Grouper を組合わせる方法をとった．技術検証の結果，Shibboleth のクラスタ化は memcached ではなく hazelcast を用いて実現する方式とした．

CIS アカウントによる認証から工繊大パーソナル ID での認証に順次切替えられるようにするには，システムを運用しながらユーザ ID 体系を移行できるように計画しておく必要がある．ユーザ ID がシステム内部の識別キーやユーザインタフェースの表示内容として利用される場合，システム稼働中のユーザ ID 変更は極めて困難である．そのため，生涯 ID で提供するサービスは稼動開始時から生涯 ID を使うように構築しておく必要がある．

そこで，ユーザ認証 ID として「CIS アカウント」「工繊大パーソナル ID」のどちらで認証しても認証結果として「工繊大パーソナル ID」を返す機構を Shibboleth IdP で構築した (図 2)．CIS アカウント, 工繊大パーソナル ID のどちらも同じアカウント属性 (description 属性) に自分に紐づく工繊大パーソナル ID を持つよう LDAP を構成することで，ユーザ認証時の LDAP 検索結果から工繊大パーソナル ID を取得できるようにしている[*4]．

各連携サービスに対し，認証結果として「ログインに用いた ID」を返すか「工繊大パーソナル ID」を返すかの切替は Shibboleth IdP の標準機能 (attribute-filter) を用いて行っている．

4.3 Grouper を用いたグループ原簿の構築

Grouper はデータベースからグループ定義を読み込む機能 (grouper-loader) に加え,GUI 管理画面 (grouper-ui) でグループの共同管理を行うこともできる．Grouper 自体は特定のグループ構成を想定していないため，他大学の事例[*5] を参考にグループ構成を考える必要がある．本学ではグループを以下の 3 種類に区分して Grouper を適用した．

[*3] https://github.com/Unicon/shibboleth-idp-dockerized,https://github.com/Unicon/grouper-dockerized
[*4] 工繊大パーソナル ID の場合は自分自身に紐付けられる
[*5] `https://spaces.internet2.edu/display/Grouper/Community+Contributions`

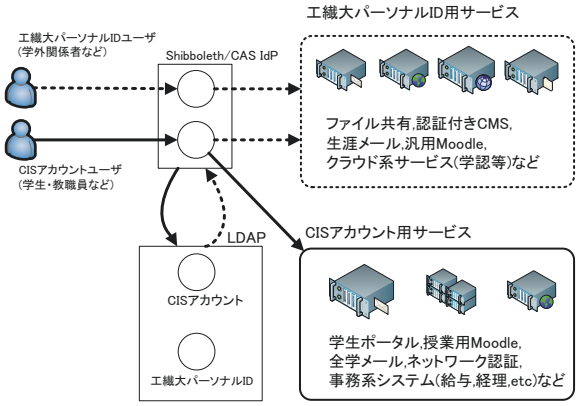

図 2 試作した認証基盤の ID 変換動作
Fig. 2 LoginID is translated inside IdP

ソースコード 1 Grouper と同期された memberOf 属性

```
# xxxxxxxx, People, cis.kit.ac.jp
dn: uid=xxxxxxxx,ou=People,dc=cis,dc=kit,dc=ac,dc=jp
memberOf: cn=kit:user:category:12,ou=Grouper,...
memberOf: cn=service:microsoft:imagine:standard:user,...
memberOf: cn=service:cis:confluence:user,ou=Grouper,...
memberOf: cn=kit:entitlement:cis:service:eduroam,...
memberOf: cn=kit:sig:cis:koho−scommittee,ou=Grouper,...
```

(1) 基本グループ
学籍情報, 職籍情報を元に所属部局，所属課程グループを自動生成
(2) 組織横断型アドホックグループ
基本グループを組合わせることで，各種会議やワーキンググループなどの組織横断型グループを手動作製
(3) サービス利用資格グループ
基本グループ・アドホックグループを組合わせることで，サービス利用条件に該当するユーザグループを作成 (電子ジャーナルなど学認 SP 用)

Grouper 上のグループ原簿を LDAP に同期させることで，グループメンバーは各 LDAP グループの member 属性，所属グループは各 LDAP アカウントの memberOf 属性に反映される (ソースコード 1)．

各連携サービスでは，LDAP 認証クエリの条件式に memberOf 属性の条件を付与したり，アクセス許可対象の指定に LDAP グループを利用することで，サービスの利用制限や情報の閲覧・編集制限を実装する．例えば，Apache では CAS 認証プラグイン mod_auth_cas から memberOf 属性を参照することで，Web サイトへのアクセスを特定グループのユーザに制限することができる (ソースコード 2)．

4.4 Talend を用いたデータ連係基盤の構築

生涯 ID に対応した認証認可基盤を実際に動作させるには，既存の各種原簿をもとにユーザ属性値の正規化,CIS アカウントと工繊大パーソナル ID の紐付け,Grouper 取り込み用グループ原簿の自動作製,CIS アカウントで定義された

ソースコード 2 Grouper 管理グループと CAS 認証の連携設定例

```
CASAttributeDelimiter |
CASValidateSAML On
CASValidateURL https://idp.cis.kit.ac.jp/idp/profile/cas/
      samlValidate
<LocationMatch /.*>
    AuthType CAS
    require cas-attribute memberOf:cn=kit:org:cis:admin,ou=
          Grouper,...
</LocationMatch>
```

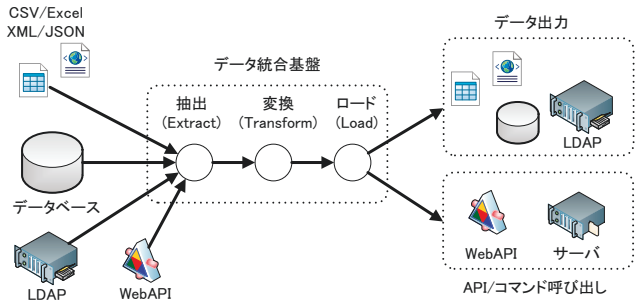

図 3 データ連係基盤 (Talend) の動作
Fig. 3 Talend is used as system integration backend

グループの工繊大パーソナル ID グループへの読み替え，等のデータ変換・集計処理や工繊大パーソナル ID 用 LDAP ディレクトリの構築を行う必要があった．

これらの処理をシェルや Python 等のスクリプト言語で実装すると属人的なツールとなり後の保守が困難になることが多い．そこで，オープンソースのデータ統合ツール Talend Open Studio を用いてデータ連係基盤を構築した (図 3)．Talend にはデータ入出力用のアダプタが豊富に用意されており，GUI エディタ上で基本処理ブロックを組合わせてデータ変換処理を記述するだけでよい[*6]．記述した処理は Java のソースコードとして出力された後に単一の Java プログラムとしてコンパイルされる．このため，開発したツールを実行するのに Talend 専用のランタイム環境を必要としない[*7]．

4.5 運用スタッフ習熟用環境の構築

上記の認証基盤を元に 2017 年 5 月に学認運用フェデレーションの参加手続きを終え，学認対応 SP との認証連携を開始した [6]．これまで VPN 接続でのみ提供していた学外からの電子ジャーナルアクセスについて学認連携が可能となったほか，人事労務課が導入するクラウドサービス型ストレスチェックシステムの認証基盤に利用することで，システム調達に先立って生涯 ID 運用に向けた利用者原簿の整備を進めた．

[*6] 自作の Java ルーチンを呼び出すこともできる
[*7] エンタープライズ版ではジョブ実行環境が用意されているが，オープンソース版では cron 等を使い自分でジョブの実行環境を作る必要がある

表 2 System10 調達システムと提供サービスの対応
Table 2 Service catalog and introduced systems in System10

サービス区分	サービス	導入システム
コアサービス	仮想Webホスティング	Apache 2.4
	LMS	Moodle 3.1
	ファイル共有	Nextcloud 12
	コンテンツ管理	Confluence 6.2
	利用者ポータル	SyntheUniv
実現サービス	利用者原簿管理	SyntheUniv
	グループ・利用資格管理	Grouper 2.3
	データ連係	SyntheUniv/Talend
	認証ディレクトリ	389DS/ActiveDirectory
	CAS/SAML認証	Shibboleth IdP 3.3
強化サービス	Web会議	BigBlueButton 1.1
	工繊大ID用LMS	Moodle 3.1
	全文検索	Solr 6.6
	サイトライセンス	Desktop Education
	学認SP連携	電子ジャーナル等

また，センター業務用に導入済みであった Confluence と JIRA のグループ管理を Grouper による管理に切替え，グループ原簿と連携したグループウェアの運用にセンターのスタッフが習熟する環境を整えた．

5. 新システム (System10) 概要

4 節で紹介した技術検証環境を用いてデータ連係基盤, 認証認可基盤に求められる要件を整理し,System9 で生じていた各種制約を緩和する方針で利用者原簿管理システム・統合認証システムの仕様を定めた[*8]．今回のシステム調達も前回 System9 の調達と同様に一般競争入札で行われ，10 月の開札から 2018 年 3 月のシステム稼働までの約 4 ヶ月で全システムの概要設計・詳細設計・移行作業を行った[*9]．

本稿に関係する利用者原簿管理・連携システム部分について新システムの概要を紹介する．調達したシステムと提供サービスの対応を ITIL フレームワークに当てはめたのが表 2 である．データ連係・利用者ポータル部分は System9 と同様に SyntheUniv であるが，5.2 節で述べるように認証認可機構はオープンソースのみで構築されている．

5.1 利用者原簿管理システム

System10 におけるアカウント情報連携は図 4 に示すように SyntheUniv を中心とした構成である．図中の白丸はベンダー独自実装による連携モジュールを表わし，Moodle 上の確認テストとの連携は構築ベンダーによる独自実装となっている．アカウント情報は学籍データベース (Dream-Campus), 職籍データベース (U-PDS) から配信される情報を元に生成され，CIS アカウント・工繊大パーソナル ID の割当てはこの時点で行われる．生成された CIS アカウン

[*8] 各システムの入札仕様は `https://www.et.cis.kit.ac.jp/system10` に掲載
[*9] センター教員はこの間，担当科目の講義や卒業研究指導等の教育業務も並行して行っている

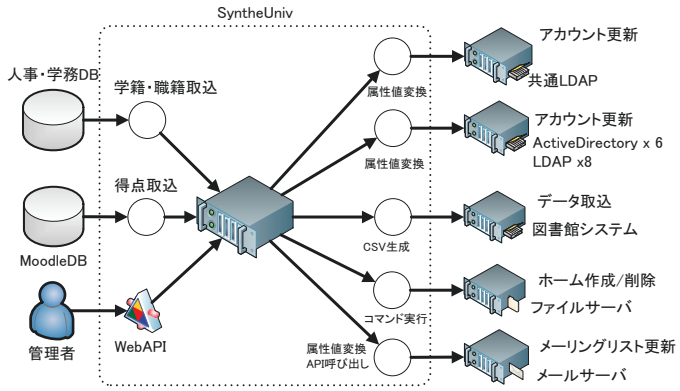

図 4 System10 におけるアカウント情報連携
Fig. 4 User data sources and accout integration in System10

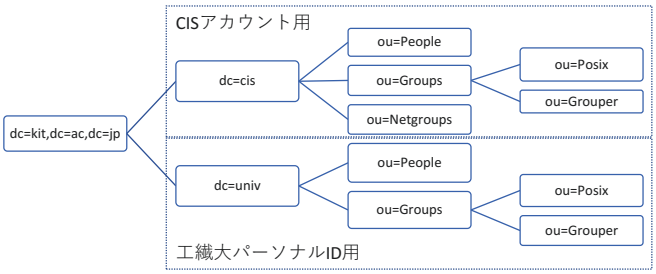

図 5 System10 認証基盤における LDAP ディレクトリ構成
Fig. 5 LDAP directory structure in System10

トは利用者区分に応じて利用が許可されたサービス用の各認証サーバに登録される．工繊大パーソナル ID アカウントは将来の認証用 ID 切替えに備えて事務局用 LDAP を除く全ての LDAP サーバに登録しているが，現時点で認証に利用しているのは共通 LDAP サーバのみである．

5.2 統合認証基盤

System10 の LDAP では，CIS アカウントと工繊大パーソナル ID を区分して扱うディレクトリ構成とした (図 5)．連携サービスは LDAP 認証設定の baseDn に CIS アカウント用ツリーを指定するか工繊大パーソナル ID 用ツリーを指定するかで，どちらのアカウントで認証を行うか切替えることができる．

認証認可基盤は技術検証環境と同様に Shibboleth と Grouper による構成となった (図 6)．SyntheUMS の配信データを中継するモジュールを開発した点を除き，オープンソースのみを用いて構築している．データ連係サーバは技術検証環境と同様に Talend を用いて本学で構築した．Grouper については一般利用者画面に表示されるユーザ属性のカスタマイズを一部独自に行っている．

5.3 工繊大パーソナル ID 対応連携サービス

CIS アカウントで利用するサービスについては System9 と System10 で大きな違いはない．本節では全関係者で利用するために工繊大パーソナル ID で構築したサービスについて紹介する．

- ファイル共有サービス (Nextcloud 12)
  user_saml プラグインを用いて SAML 認証を実現した[*10]．nextant プラグインと Solr 検索エンジンの組合わせにより全文検索機能も実現している．
- 文書共有サービス (Confluence 6.2)
  miniOrange 社の有償プラグイン”Single Sign On (SSO) for Confluence SAML” を用いて SAML 認証対応を行った．ダッシュボード画面やユーザディレクトリ画面などで個人情報 (工繊大パーソナル ID と実名の組やメールアドレス等) が表示されてしまうため，Apache フロントエンドの mod_substitute モジュールを用いて個人情報に該当する箇所を匿名化している．
- 汎用 LMS(Moodle 3.1 LTS)
  オープンソースの Web 会議システム BigBlueButton と組合わせることで，全関係者が Web カメラ映像と発表スライドを組合わせた Web 会議を行える環境を実現した．HDMI 信号を UVC 入力に変換するキャプチャデバイス[*11]と組合わせることで，外部カメラ映像や PC 画面出力の中継も可能である．また，Global Search プラグインと Solr 検索エンジンの組合わせにより全文検索機能も実現している．

6. 今後の課題

今回の認証基盤更新によりシステム内部では工繊大パーソナル ID を用いたユーザ認証が可能になったが，利用者側のユーザ認証 ID には既存の CIS アカウントを用いており，CIS アカウントに基づく既存のサービスでは利用者側でログイン用 ID を使い分ける必要がある．熊本大学で行ったように，この問題は ID 選択機能を備えたシングルサインオンサーバを構築することで原理的には解決できる [7]．SAML IdP 上での同等機能の実装が今後の課題である．

また，現在のベンダー実装ではサービス利用資格毎に個別の確認テスト合否と連携させることができない．LMS 上の確認テストと利用資格を連携させる方式として，隅谷らが文献 [8] で報告しているように LTI ツールを用いた LMS に中立な方式に切替えることが考えられる．

7. まとめ

本報告ではシステムう更新に伴う利用者原簿管理基盤の強化と連携サービスの構築結果について述べた．前システム (System9) の利用状況から学内展開が進んでいないサービスについてその要因を整理し，実現サービスの強化や生涯 ID の運用に必要な認証基盤の設計が新システムの課題であることを述べた．システム統合を実現するにはテスト

[*10] デスクトップ版クライアント，モバイル版クライアントでの SAML 認証動作も確認している
[*11] Epiphan 社製 AV.io HD や Magwell 社製 USB Capture HDMI

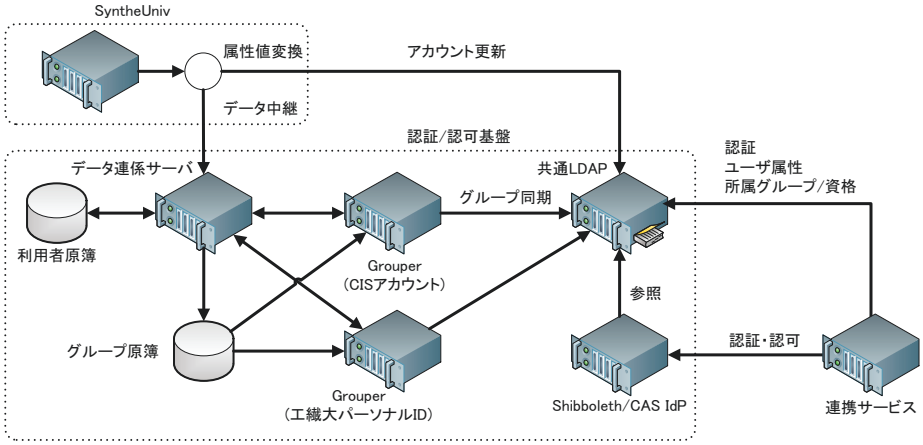

図 6 System10 認証認可基盤
Fig. 6 Identity and Access Management Infrastructure in System10

環境を用いた技術検証が不可欠であり，今回のシステム調達では仕様検討段階から学内テスト環境を使った基礎検討を行った．

予算削減が続く中でのシステム調達は，業務設計・技術サポートの部分を削ってでもまずはシステム自体を調達するということになりやすい．しかし，これは「車は買ったが整備士も運転手もいない．利用ルールも決めていない．」という状況に近い．車を適正価格で購入することと，維持管理できることと，利用ルールを整備できることは全く別の話である．それでも技術に触れること自体を目的として最新設備を調達していた時代は，これらの違いを意識しなくても大きな問題はなかった．

しかし本学の場合，多くの利用者にとって全学の情報インフラを利用する目的は最新技術に触れることではない．業務・研究・教育・学習が滞りなく進むことが目的である．現在の利用者が期待する水準は Google や Microsoft 等の大手クラウド事業者の提供するサービスの水準であるが，学内のリソースで実現可能なサービスと大手事業者が提供するサービスとの落差は極めて大きい．自前のリソースにこだわる限り，使われないシステムが積み上がるだけである．

在籍する者に対し，最新の知識・技術に触れる環境を提供することは教育研究機関としての重要な役割である．しかし，その役割を果たすために自前のリソースに執着する必要は無い．現在の一般利用者にとって，最新技術はスマートフォンと学外サービスの中にある．教育・研究・学習・業務のどれをとってももはや学内で閉じている活動はない．であるならば，利用可能な学外リソースへの円滑なアクセスを提供し，さらには大学のリソースを学外からも利用可能にすることが，全学の情報センターとしての大きな役割と考えられる．

謝辞 本研究は JSPS 科研費 15H02795 の助成を受けたものです．

参考文献

[1] Grouper: an enterprise access management system, https://spaces.internet2.edu/display/Grouper/.
[2] 桝田秀夫，平田博弘，黒江康明，柴山 潔：京都工芸繊維大学における新情報教育システムについて，PC カンファレンス，pp. 173–176 (2006).
[3] Masuda, H., Murata, K., Shibuya, Y., Wakasugi, K. and Kuroe, Y.: KIT's Campus Computer System by Virtual Machine Technology and Integrated Identity Service, *Proceedings of the 38th Annual ACM SIGUCCS Fall Conference: Navigation and Discovery*, SIGUCCS '10, New York, NY, USA, ACM, pp. 251–256 (online), DOI: 10.1145/1878335.1878398 (2010).
[4] Masuda, H., Murata, K., Shibuya, Y. and Kuroe, Y.: Distributed Campus Computer Infrastructure: Integrate Education, Research, Library and Office Activities, *Proceedings of the 42Nd Annual ACM SIGUCCS Conference on User Services*, SIGUCCS '14, New York, NY, USA, ACM, pp. 93–96 (online), DOI: 10.1145/2661172.2668055 (2014).
[5] 京都工芸繊維大学：京都工芸繊維大学情報科学センター規則, https://www.kit.ac.jp/01/prescriptions/act/frame/frame110000175.htm.
[6] 永井 孝幸, 山岡 裕美：学認始めました，京都工芸繊維大学情報科学センター広報，No. 36, pp. 10–20 (2017).
[7] 永井孝幸，杉谷賢一，河津秀利，中野裕司ほか：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，教育学習支援情報システム (CLE), 情報処理学会研究報告， Vol. 2013, No. 20, pp. 1–10 (2013).
[8] 隅谷孝洋，天野由貴，岩沢和男，渡邉英伸，西村浩二：情報セキュリティ教育と連動させたアカウント管理，学術情報処理研究， No. 21, pp. 82–88（オンライン），DOI: http://www.nipc.med.tuat.ac.jp/home/jacn/annai/jacn21st-info/JACN2017-10.pdf (2017).