

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

江原 康生^{†1} 村尾 靖子^{†2} 山口 文雄^{†2}

大阪大学では学内で運用されている様々な情報システムを統合的かつ安全に機能させる全学 IT 認証基盤システムの運用を平成 18 年 10 月から開始し、学内システムに対して SSO (シングルサインオン) による認証連携、データ連携及びログイン認証サービスを提供している。しかし既存システムは、現在の学内情勢において要求される様々な機能要件を十分に提供できない状況となり、学内システムに対する SSO 認証連携の拡大及び高度なデータ連携の推進が困難となっている。これらの要求の実現に向けて、新全学 IT 認証基盤システムの構築および移行を行い、平成 22 年 10 月より運用を開始した。本稿では当システムの概要について述べる。

Construction and Migration of Campus-wide IT Authentication Platform System in Osaka University

YASUO EBARA,^{†1} YASUKO MURAO^{†2}
and FUMIO YAMAGUCHI^{†2}

In Osaka University, the operation of a campus-wide IT authentication platform system has been started from October 2006, which provided functions to allow secure and integrative operations for various information systems operated within the campus, and contributed SSO(Single Sign-On) authentication, attribute information cooperation, and login authentication service. However, the existing system has been difficult to provide some required system functions in current campus situation. Therefore, we can't promote SSO authentication and advanced information cooperation for campus information system. In order to realize these requests, we have constructed and migrated a new campus-wide IT authentication platform system and started the system operation from October, 2010. In this paper, we describe the summary of the system.

^{†1} 大阪大学 情報基盤本部

Central Office for Information Infrastructure, Osaka University

^{†2} 大阪大学 情報推進部情報基盤課

Information and Communications Technology Services Infrastructure Division, Osaka University

1. はじめに

大阪大学では学内で運用されている様々な情報システムを PKI 認証技術のもとで統合的かつ安全に機能させる全学 IT 認証基盤システムの運用・管理を行い、SSO(シングルサインオン)による認証連携及びデータ連携、ログイン認証サービス等を提供している。しかし、平成 18 年 10 月に導入された旧システム¹⁾は、現在の学内情勢において要求される機能要件を十分に提供できない状況となってきている。

一つは学内の利用ユーザ数及び連携システムの増加に伴うシステムリソースの不足が挙げられる。例えば、年度初めの学務情報システムなどの集中利用に伴い、学内 LAN に接続された多数のクライアント端末から同時に多数の認証処理が発生する。このため、サーバの CPU 使用率等が上昇し、安定した認証連携を継続させることが非常に困難となっている。また、新たな学内システムに対する SSO 認証及びデータ連携を実現させるには、各システムの様々な要求に応じるための大規模な改修が必要とされるため、柔軟な対応が非常に困難な状況である。

さらに、本学では事務業務に関する基幹系システムとの SSO 認証及びデータ連携に向けた検討が進んでいる。しかし、学内の事務基幹系システム間で本学構成員のユーザ属性情報のコード体系は統一化されておらず、現状は手作業によるデータ連携の対応に迫られるため、業務量増大の要因となっている。システム全体の最適化を視野に入れた各システム間のデータ連携を実現させるために、ユーザ属性情報の一元管理への必要性が高まっている。

今後、学内システムに対する SSO 認証連携及びデータ連携を更に推進していく上で、上記に示すような課題が生じている。ゆえに、学内システムを統合的かつ安全に運用させるために必要とされる機能を有するシステム更新を行い、有用な認証基盤システムを構築する必要がある。本稿ではこれらの要求の実現に向けたシステム構築及び移行を行い、平成 22 年 10 月より運用を開始した新全学 IT 認証基盤システムの概要について述べる。

2. システム構成

図 1 に新全学 IT 認証基盤システムの構成図を示す。本システムは認証局システム、SSO(シングルサインオン)システム、マスターデータベースシステムから構成される。各システムはハイ・アベイラビリティなシステムとして、システム障害時においてもサービスを停止させないための対策を実施している。図 2 に新全学 IT 認証基盤システムと学内システムとの各連携状況を示す。

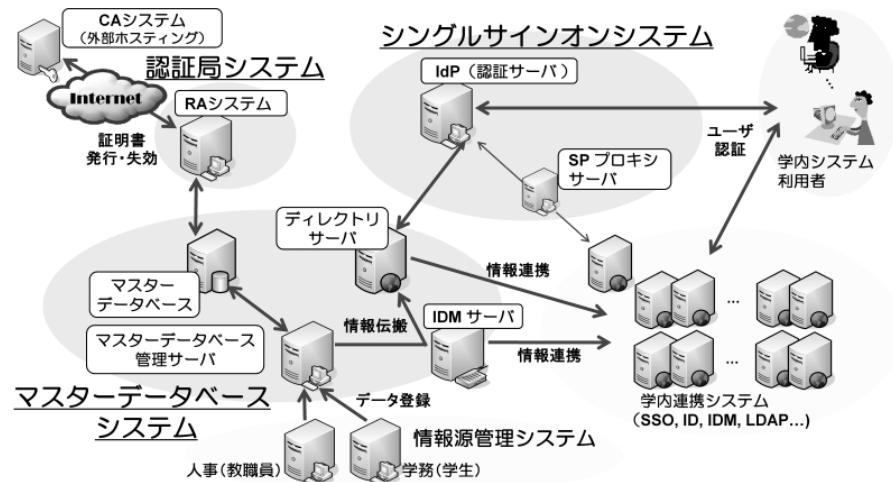


図 1 新全学 IT 認証基盤システムの構成

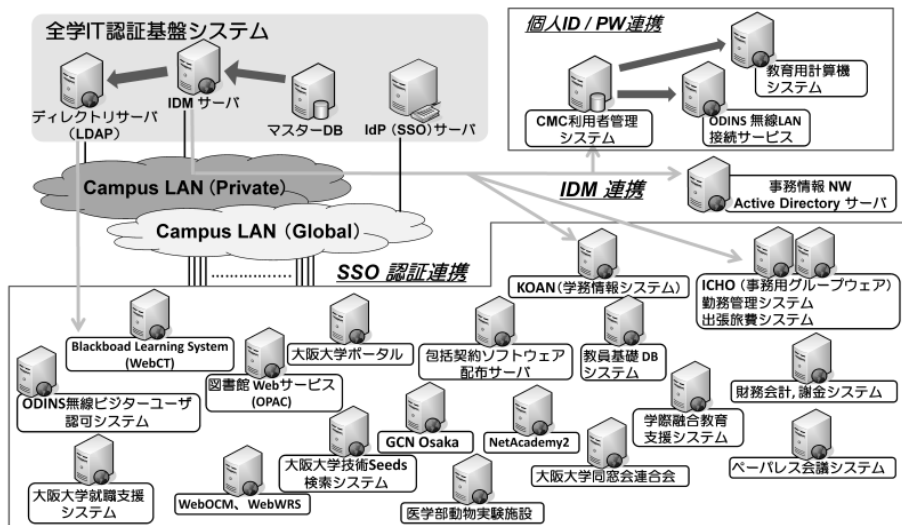


図 2 学内システムとの連携状況

平成 23 年 1 月現在、学内の 20 システムに対して SSO 連携、6 システムに対して IDM、ディレクトリサーバによるユーザ属性情報の連携を実現しており、年度内に向けてさらなるシステム連携が計画されている。特に平成 22 年度より、グループウェア (ICHO)、勤務管理、出張旅費、財務会計などの事務基幹系システムとの SSO 連携を開始しており、認証基盤システムの利用者数が拡大の一途をたどっている。

2.1 認証局システム

認証局システムでは CA システム (外部ホスティング) および RA システムを構築し、学内の各システムおよびユーザの電子証明書申請を受け付け、電子証明書および電子証明書失効リストなどの発行を行う。これらのサブシステムとして IC カードシステムを構築し、認証局システムより発行された電子証明書および鍵ペアを格納した IC カードの発行を行う機能を有している。

2.2 SSO システム

SSO システムは学内の各システムの Web アプリケーションと連携して、SSO 認証機能を提供する。本システムでは認証サーバとして、旧システムの Sun Java System Access Manager に代わり、NTT ソフトウェア (株) 製の TrustBind IdP²⁾ を導入した。TrustBind IdP サーバと SP サーバ (学内 SSO 連携システム) 間では、Liberty Alliance による OASIS-SAML2.0 に準拠した SAML 2.0 プロトコル³⁾ による SSO 認証連携を実現する。

図 3 に旧システムとの SSO 認証連携方式の比較を示す。旧システムでは SSO 連携システムの Web サーバに対して、Policy Agent というオプションモジュールをインストールすることで、Access Manager (認証サーバ) 間と独自プロトコルによる SSO 認証連携を行っていた。しかしこの方式では、クライアント (ユーザ) 端末からのアクセス数が集中する際に、Access Manager と各連携システム間の認証処理が増大し、システム負荷上昇による性能劣化を引き起こすケースが頻繁に発生していた。新システムではこの問題を改善するために、IdP 認証サーバと SP サーバ (SSO 連携システム) 間の通信において、HTTP リダイレクトを利用することで、これらのサーバ間での認証処理が発生しない仕組みを採用した。

学内の連携システム側で動作する SP サーバ機能として、オープンソースの Shibboleth SP⁴⁾ を各連携システムの Web サーバに実装を行った。Shibboleth SP の実装が困難なシステムについては、別途構築した SP Proxy サーバを用いて SSO 認証連携を行うこととした。なお、本システムにおけるクライアントと IdP サーバ間の通信はロードバランサの SSL アクセラレータ機能を用いて SSL によるデータの暗号化を行い、通信の安全性を確保する。

本システムでは SSO 認証機能に加えて、各連携システムに対する利便性の向上を目的と

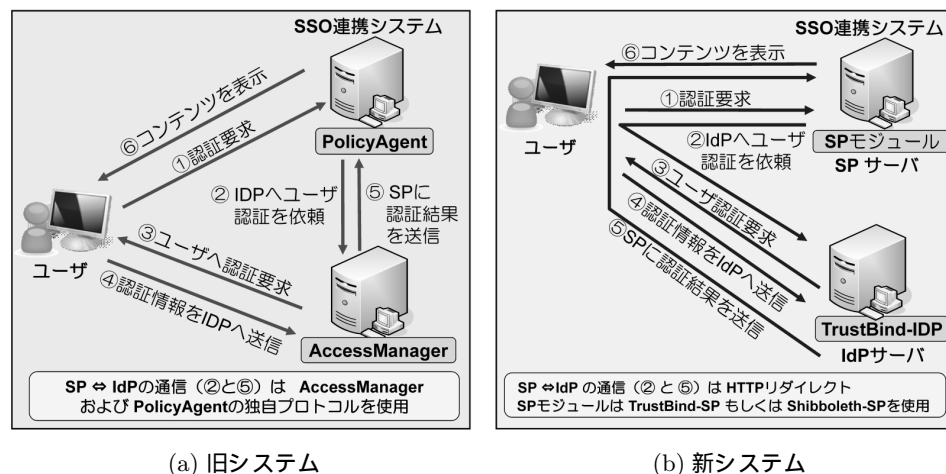


図 3 SSO 認証方式の比較

した認可機能の実現を目指している。SSO 認証・認可機能とは、ユーザに払い出された個人 ID・パスワードによる認証後にユーザの属性情報によって連携システムのアクセスや利用できるサービスを制限したり、また与えられたアクセス権限により資源へのアクセスを制御する機能である。本システムでは、SSO 認証の際に各連携システムが必要とするユーザ属性情報を指定することで、HTTP リクエストのヘッダに付加して連携システムのアプリケーションに属性情報を渡すことができる。この属性情報をアプリケーション側が活用することにより、いくつかの学内連携システムにおいて、認可機能を実現している。

2.3 マスターデータベースシステム

マスターデータベースシステムは、ユーザに関する主要な属性情報を一元管理し、学内の連携システムに効果的に参照させることで最新かつ適正な属性情報の保持を実現させることを目的として新たに導入を行った。構成として、マスターデータベース及び管理 Web サーバシステム、ユーザ属性情報を連携するための IdM (Identity Management) サーバ、ディレクトリサーバからなる。

マスターデータベース管理 Web サーバは、ユーザ属性情報の登録・編集・削除を行う機能を Web ベースの GUI で実現している。また RA システムと連携することで利用者に対する電子証明書の発行処理も行うことができる。IDM サーバは全学 IT 認証基盤システムの

ディレクトリサーバや学内連携システムに対して、個人 ID を含めた利用者の属性情報を連携する機能を提供する。IDM 機能のソフトウェアとして株式会社インテック製のパッケージ製品「結人」⁵⁾を導入した。IDM システムを使用することにより、マスターデータベースから JDBC のプロトコルで対象ユーザの属性情報を取り込み、各連携システムに対して LDAP, DCOM, JDBC 等の各種プロトコルを使用して情報連携を実現する。

3. 個人 ID 体系の再設計

全学 IT 認証基盤システムでは大阪大学個人 ID (以下、阪大個人 ID) と呼ばれる ID を、学内の利用規程に基づき、本学構成員に ID 発行を行っている。しかし旧システムでは、複数の所属や身分を持つユーザに対して、複数の阪大個人 ID の発行を行ってきた。それに該当するユーザは利用する学内連携システムの形態に応じて、阪大個人 ID を使い分けてログインする必要があり、ユーザにとって煩わしい運用形態となっていた。

この問題を解決するために、新全学 IT 認証基盤システムでは SSO 認証ログインで使用する阪大個人 ID を一つに統一し、連携システムへのログインの際には、職名、身分などのユーザ属性情報が異なる複数の ID の使い分けを可能とする新たな個人 ID 体系の再設計を行った。

新全学 IT 認証基盤システムでは、複数の阪大個人 ID を所有していたユーザに対して、SSO 認証用の ID を人物固有の属性情報 (氏名、生年月日など) が紐づく Personal ID (新阪大個人 ID) に統一する。所属部署、役職などの属性情報については Role ID という別体系の ID に紐付けることで、システム内部で 2 種類の ID を関連付けた形で管理を行う。図 4 に新旧システムにおける阪大個人 ID の管理体系を示す。

ユーザが異なる所属、身分などの属性情報を新たに持つ毎に Role ID が追加される。Personal ID は阪大個人 ID として、引き続き同じ ID の利用を可能としている。複数の Role ID を持つユーザは、その中から代表 ID を Personal ID として選択し、全学 IT 認証基盤システムの認証サーバで Personal ID とパスワードで SSO 認証後、Role ID を選択して SSO 連携システムにログインを行う方式を実現させる。

4. SSO (シングルサインオン) に伴う各種機能

4.1 利用者情報登録・変更

本システムでは新規に阪大個人 ID を発行したユーザに対して、SSO 連携システムへの初回ログイン時にパスワード、メールアドレス、内線番号を登録する機能を実装した。また

氏名	阪大個人ID	所属	職名、身分名
ユーザA	u000123a	大学院工学研究科	非常勤講師
ユーザA	u000456b	大学院人間科学研究科	准教授

(a) 旧システム

氏名	阪大個人ID (Personal ID)	Role ID	所属	職名、身分名
ユーザA	u000456b	u000123a	大学院工学研究科	非常勤講師
		u000456b	大学院人間科学研究科	准教授

(b) 新システム

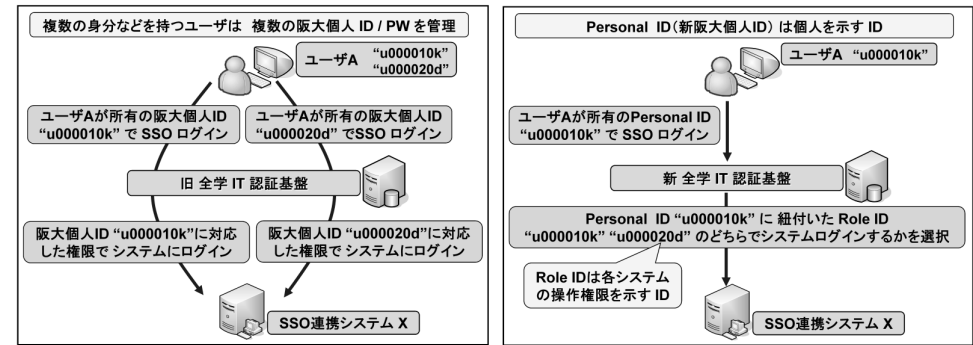
図 4 阪大個人 ID 体系の新旧比較

ユーザによる登録情報の変更も同様の処理で可能としている。この機能は旧システムのユーザによるパスワード変更機能に加えて、ユーザの連絡先の最新情報を管理することを目的として新たに導入した。ユーザがメールアドレスの登録・変更を行った際、登録されたメールアドレスの到達確認を行うため、仮登録メールをそのアドレスに送信する。そのメール本文に記載された URL へアクセスし、ユーザが確認操作を行うことで本登録が完了とする。

4.2 利用者による Role ID 選択

3. で述べた通り、新システムでは個人 ID 体系の再設計を行ったことで、ユーザの SSO 認証ログイン方式を変更している。図 5 に SSO 認証ログイン方式の新旧比較を示す。(a) の旧システムでは、複数の阪大個人 ID を管理するユーザは利用する SSO 連携システム X の形態に応じて、阪大個人 ID を使い分けてログインする必要があった。(b) の新システムでは複数の Role ID を持つユーザは、全学 IT 認証基盤システムの認証サーバで Personal ID とパスワードで SSO 認証を行った後、Role ID を選択することで、ユーザの属性に応じた SSO 連携システム X へのログインを可能としている。図 6 に SSO 認証ログイン時の基本動作の流れを示す。

図 7 に SSO 認証ログイン時における Role ID 選択画面を示す。学内の SSO 連携システムにアクセスする際には、図 7(a) の画面に示すように、最初は全学 IT 認証基盤サービスへの SSO ログイン画面が表示される。Personal ID(阪大個人 ID) とパスワードを入力して「ログイン」ボタンを押すと、(b) の画面に遷移し、ユーザが所有している全てのロール ID が表示される。この画面上で SSO 連携システムで利用したい「所属」及び「職名/身分」の



(a) 旧システム

(b) 新システム

図 5 SSO 認証ログイン方式の比較

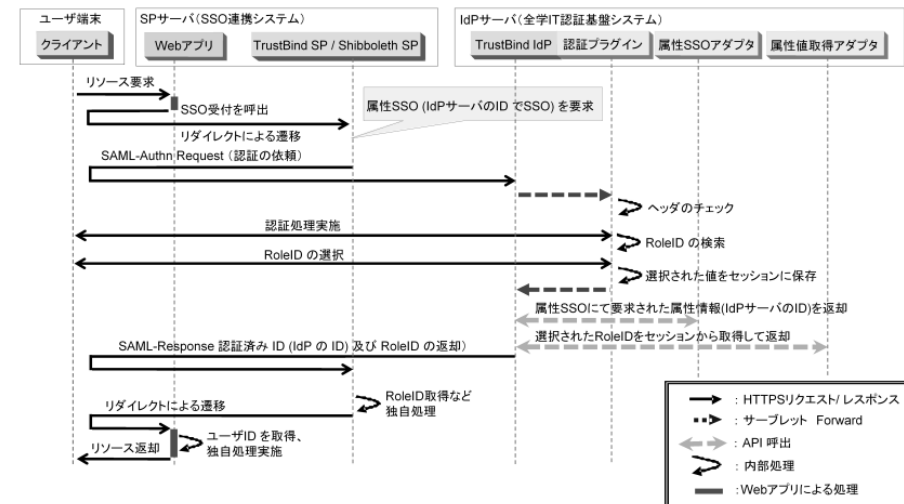
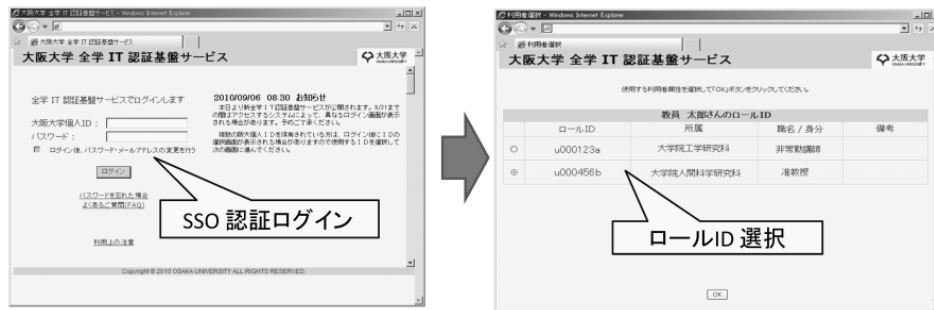


図 6 SSO 認証ログイン時の基本動作



(a)SSO 認証ログイン画面 (b) ロール ID 選択画面

図 7 SSO 認証ログイン時における Role ID 選択

Role ID を選択して「OK」ボタンを押すことでログイン処理が完了する。

4.3 入力代行設定機能

学内 SSO 連携システムで発生する教員の業務を事務系職員に代行させて入力処理などを実施したいという要求がこれまでも多くみられたが、旧システムでは本人による認証ログインしか受け付けていなかった。そのため、入力代行などを行いたい場合は教員本人の個人 ID、パスワードを他人に受け渡すなどの行為が行われており、本来の認証機能が損なわれる事態が生じている。この問題を受けて、新システムでは SSO 連携による入力代行設定機能を実装した。本機能は、学内の入力代行設定が可能な SSO 連携システムにおいて、あるユーザ（代行元）のアプリケーション操作権限を別のユーザ（代行先）に代行設定を行うことで、SSO 連携システムに代行元ユーザの環境でログインして利用することができる。

図 8 に入力代行設定画面を示す。入力代行設定は本学のグループウェア (ICHO) のワークフロー機能を用いて行う。ユーザはグループウェアにログインして、入力代行設定のメニューを選択すると図 8 の画面が表示され、設定申請を行うことができる。ユーザから申請された入力代行設定の情報はマスターデータベース上で管理される。IdP サーバは SSO 認証ログイン後にその情報を参照し、入力代行分を含め複数の Role ID を保持している利用者の場合と同様に、図 7 に示すロール ID 選択画面上に併せて選択項目として表示される。

5. マスターデータベースによるユーザ属性情報の一元管理

全学 IT 認証基盤システムでは学内の人事、学務情報システムからユーザの属性情報を情

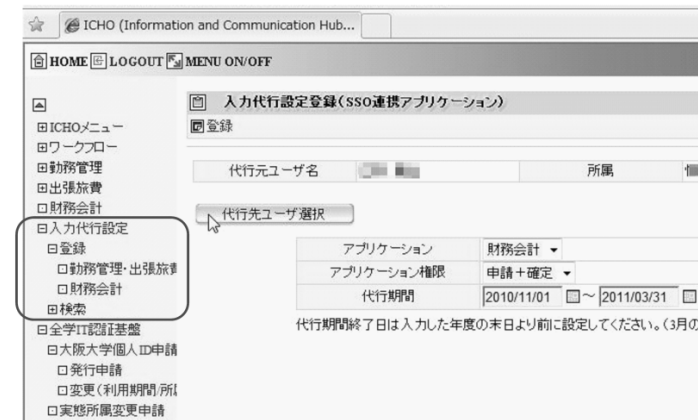


図 8 グループウェアのワークフロー機能による入力代行設定

報源として定期的に取得し、ユーザ登録、削除、更新を行っている。また、人事、学務情報システムに登録されていないが、学内システムの利用が必要な学内内部局ユーザに関しては、部局長の承認を得た上で個別申請を行い、ユーザ登録を実施している。

しかし旧システムでは、これらのユーザ属性情報が最新情報になっていないケースが多数存在していた。特にユーザの学内における所属情報に関しては人事上の所属情報をそのまま登録していたため、実際に所属する部局名と一致していないユーザが多数存在するといった問題が生じていた。その他の身分等に関する属性情報についても、現在の学内ルール等に適用できていなかったため、学内 SSO 連携システムにおける認可処理などに活用することができない問題点も指摘されていた。

このような問題点を受けて、新全学 IT 認証基盤システムではユーザに対する主要な属性情報の一元管理を行うためのマスターデータベースシステムを新たに導入した。これにより、学内連携システムが本データベースを参照することで、最新かつ適確な属性情報の管理を行い統制のとれた学内システム間連携の実現を目指す。マスターデータベースシステムでは、管理するユーザ属性情報の体系の整備、ユーザの実態に合った所属情報の整備（所属情報の区分方法、コード体系などの見直し）、認証・認可処理にも適応可能な職名、身分、分類情報の整備などを考慮してデータベースの再構築を実施した。

しかし所属情報に関しては、人事システムや職員録の情報を基にした整備では欠落情報が

多数存在していたり、学内内部局のみが把握している所属情報を取得することが非常に困難な状況もあり、これらが重要な課題として浮き彫りとなった。そこで、データベース構築時に学内の全部局に対して、現在登録されているユーザの所属情報の実態調査を行い、その回答情報を基にして旧システムのユーザ属性情報から変換作業を行い、新システムへのデータベース移行を実施した。

さらに新システムでは、常に最新のユーザの所属情報を維持管理するために、所属情報の変更申請を部局の事務担当者から行ってもらう、ユーザの実態に合った所属情報を取得する方式を採用した。図9にグループウェアのワークフロー機能による所属情報変更申請画面を示す。申請者である部局の事務担当者は所属情報を変更したいユーザについて、実態の所属情報を選択して申請を行うことで、マスターデータベース側で所属情報の変更処理が行われる。

また、グループウェアのワークフローではこれまでは紙ベースで行っていた大阪大学個人ID申請機能も提供している。この機能は全学IT認証基盤システムを利用するユーザのうち人事、学務システムに登録されていないユーザに対する個人ID発行申請を行うためである。その中でも所属、職名などの申請項目を選択方式にすることで、部局担当者からの申請情報の一元性を保つことが実現しつつある。

6. おわりに

本稿では、全学IT認証基盤システムのこれまでの運用における問題点や今後の学内システムに対するSSO認証連携及びデータ連携を更に推進していく上で必要とされる課題を受けた形でシステム構築及び移行を行い、平成22年10月より新たに運用を開始した新全学IT認証基盤システムの概要について述べた。

今後の検討課題として、学内連携システムの様々な要望に対し、柔軟な対応が可能なマスターデータベースの更なる整備、個人IDの発行方式の検討などが考えられる。特にユーザへの不要な個人IDの発行を防ぐための名寄せ問題の解決⁶⁾への取り組みも重要と考える。

また、事務基幹システムのSSO認証、データ連携の本格化に従い、業務処理の電子化への対応も急務とされる。これらに関する対応に向けて、全学共通のICカード等の導入、それを活用したPKIアプリケーション基盤の構築に向けた検討も将来的に必要と考える。

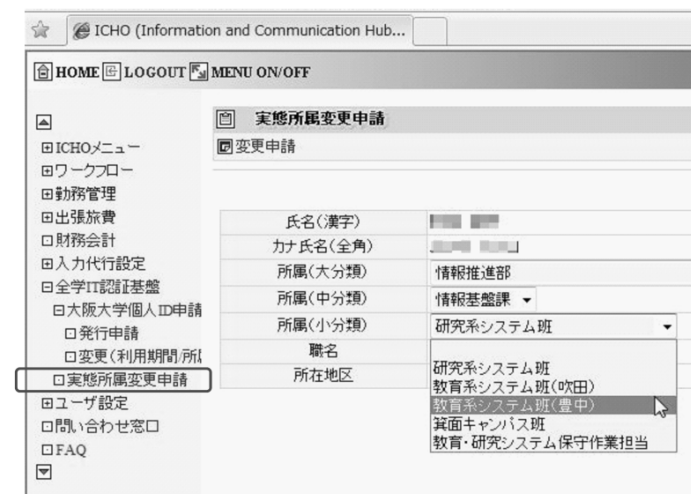


図9 グループウェアのワークフロー機能による所属情報変更申請

参考文献

- 1) 秋山 他: 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).
- 2) Web シングルサインオン TrustBind/Federation Manager, <http://www.ntts.co.jp/products/trustbind/index.html>
- 3) JapanSIG/Documents/TechTutorials <http://wiki.projectliberty.org/index.php/JapanSIG/Documents/TechTutorials>
- 4) Shibboleth <http://shibboleth.internet2.edu/>
- 5) IDM 同期システム結人, <http://www.intec.co.jp/service/network/yuito.html>
- 6) 梶田 他: 生涯利用可能な名古屋大学IDの導入に伴う名寄せ問題とその解決法, 情報処理学会研究報告, 2008-DSM-48, pp.73-78 (2008).