2005－DSM－39（6）
2005／10／14

大学向け業務アプリケーション利用権限集中管理方式の提案

Proposal of Centralized Use Policy Management System of Business Applications in University

尾川　正美*1*2，敷田　幹文*2

Masami OGAWA*1*2, Mikifumi SHIKIDA*2

あらまし　近年，大学では業務の効率化，学生・教職員へのサービス向上を目指して多くのビジネスアプリケーションが導入されている．しかし，その利用者管理，権限管理は個別のアプリケーション毎に行われており，個人情報保護やＴＣＯ削減の両面から問題となっている．我々は，代表的な業務処理システムを調査・分析し，個人認証と業務処理権限認証を統合的に実施するシステムの枠組みを検討した．これにより，個人情報を事務用 NET（ネットワーク）内に隠蔽して安全性を向上させると共に大学内業務の SSO(Single Sign On) が実現できる見通しができた．

キーワード：ＳＳＯ，ＬＤＡＰ，統合認証，個人情報保護，ＳＯＡ

Abstract：In recent years, most universities prepared many business applications for not only student and employee services but also effective office work. In real products, the user authentication services are provided by each application systems. Now, some problems are pointed out such as severe private information management, a large quantity of TCO (Total Cost of Ownership) and so on. We investigated and analyze each domain's business schema and operation's schema for each role of work. Then we have found the needs to manage separately and to connect virtually both personal information and business role. Also we designed integrated authentication and business role management system. I believe this will lead us both safety management of private information and university systems SSO (Single Sign On) solution.

Keywords：SSO, LDAP, Integrated Authentication, Private Information Management, SOA

1. 背景

近年，大学は社会情勢の変化を受けて，経営の効率化，学生・教職員・父兄などの関係者へのサービス向上を目指して，基幹業務の強化や新たなサービスを導入して来ている．これらのサービスは学内だけでなく学外からも利用できる様にWebサービスとして提供されるのが一般的である．

これらのアプリケーションは個々の業務部門の要求に基づいて設計・開発・運用されてきた背景から，大学の全体システムとしての整合性に対する配慮に欠け，重複した情報を保有した形態となっている．特に，その利用者管理システムを個別に実現している事は個人情報が大学システム内に複数存在する事であり，漏洩の危険を増大させ，情報最新性の維持を困難にしている．

また，多くのサービスが提供されるに連れて，一度の Login で全てのアプリケーションを横断的に利用できる SSO(Single Sign On)に対する要求が高まって来た．

*1 富士通株式会社　Fujitsu ltd
*2 北陸先端科学技術大学院大学　Japan Advanced Institute of Science and Technology

我々は，富士通が提供している代表的な大学向けアプリケーションパッケージをモデルに，個人認証と業務権限認証の実態を分析・整理し，統合的に実施する方策を検討した．

統合的な認証基盤の構築事例として，LDAP (Lightweight Directory Access Protocol) [1]を用いた事例や Role の概念を用いる方式 [2][3]が報告されているが，業務処理権限との関係を含めた詳細な議論や分析はなされて居なかった．

今回，我々は大学関連アプリケーションを総合システムとして捉えた SOA(Service Oriented Architecture) [4] 方式での再構築を推進する一環として検討を開始した．

2. 大学向け業務アプリケーションの現状分析と課題

ここでは，我々が大学向けに提供している代表的な業務処理パッケージについて，個人認証や業務権限認証がどの様に管理されているか分析を行った．また，当社システムに限定されず，業務遂行要件として一般的に共通である運用条件などを整理した．

2.1 図書館システム(ILIS/WAVE) [5]

本システムは図書・雑誌の購入から配架，情報検索，貸し出し返却など一連のサービスを提供するものである．システムの利用者は，管理系は図書館職員，利用系は教職員，学生ならびに地域住民など多岐に渡るという特徴がある．

学内の利用者に関する基本情報は年度始めに学籍システムや職員人事システムなどから入手されるが，一般的に独自の ID 管理体系を有している．外部の LDAP や NIS の認証機能を利用する事もできるが，特別な利用者が存在するので ID の追加・削除権限を持つ事が条件となる．

一般に管理系システムは図書館内 NET（ネットワーク）もしくは事務用 NET に接続されているが，OPAC（蔵書検索）などのサービス系は教育・研究 NET に接続されており，別々の認証システムが動作する．

ILIS では職務名と職務権限を自由に定義でき，それに応じた権限認証を行う．大学によっては係共通の ID で何人かが業務を遂行しているケースも有り，業務遂行責任に対する考え方が曖昧なケースも有る．

2.2 学生管理，成績管理等基幹システム(Campusmate) [6]

本システムは学生に関する基幹業務であり，学生サービス拡張ニーズの広がりに対応して逐次新たなサブシステムを追加リリースしている．現在は，①志願者・候補者　②NET 出願　③入試　④学生（学籍，保護者，保証人その他）⑤教務（履修，成績，時間割その他）　⑥学費　⑦就職　⑧校友会　⑨学生カルテ　⑩ポータル（各種連絡，日常業務窓口）　⑪各種サービス（教室予約，シラバス，　各種申請・アンケートなど）等の機能を提供している．

システムの利用者は各サービス提供元事務職員と教員及び学生だが，一部のサービスは卒業生，保護者などにも開放される方向にある．

利用権限は業務処理上の個別機能およびデータとの対応関係が複雑なため ID 単位に機能利用許諾を DB 管理している．サブシステムは組織構造に合わせた機能集合として命名している．

学生に関してはサービスの性格からあらゆる情報を保有しており，個人情報保護の観点から最も注意を要するが，運用の容易性を重視する

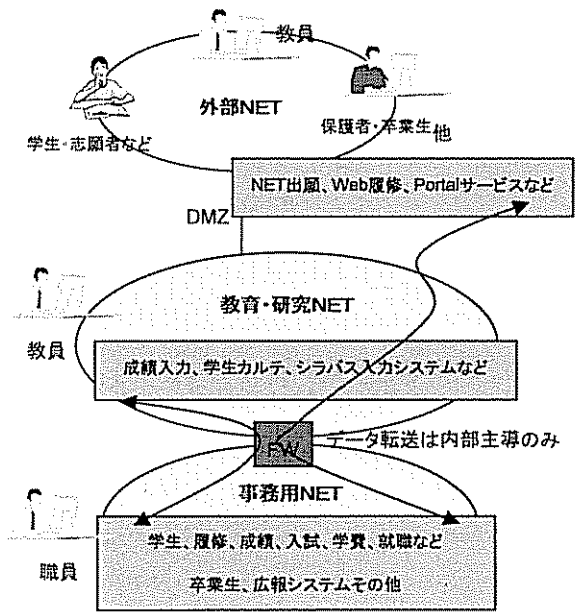

図１．サービスと認証の配置

という顧客要請から個人情報の暗号化は一般的に行っていない.

また，学生には入学以前から卒業後まで一貫して対応する為に，学籍番号とは別の生涯IDに相当する内部管理番号を個人対応に付与しており，教職員にも同様の体系を適用している.

サーバの配置は図書館システムと同様に図1に示す様にセキュリティに配慮し，利用者の所在に合わせて機能を配置し，そこで必要な認証を行って居る．利用者管理情報はそこでの必要最小限に止めて保有しており，DBアクセスは全て記録している.

2.3 e-Learning(Campusmate/Course Navig) [7]

所謂 CMS(Course Management System)，或いはLMS(Learning Management System)機能を有し，教材作成支援，情報共有サービスなどを含む総合的教育支援システムを目指している．e-Learningの為に最適化しており，教育コースを構造的に管理する機能やテスト機能，クラス内で議論できる機能などが有り，履修，成績処理で教務システムと連携する.

利用者は教員（TAを含む），学生（生涯教育，聴講生を含む）が利用する．また、クラスで議論する空間を持つことなどから，一般に学籍番号をベースにしたID体系を採用するのが通例だが，外部の聴講生などを扱う事から，固有の利用者管理システムを内蔵している.

サーバは通常，外部ＮＥＴからもアクセス可能な教育研究ＮＥＴに配置される。

2.4 財務会計（Glovia/Campus) [8]

法人としての予算管理，収入・支出管理，財務管理，資産管理などを行う.

利用者は主として経理，管財，会計担当の事務職員が中心であるが，物品購入などのサービスは全教職員が利用する.

部門，プロジェクトなどの予算枠毎に責任と権限を規定する必要が有り，個人ID毎に利用できるサブシステムと詳細機能範囲を定義できる．物品請求は教育研究NETからも利用でき，職務毎（申請者，承認者，部局職員，スーパなど）に権限規定と代行者設定ができる.

2.5 人事給与(ICMPS)

教職員の採用から昇給・昇格，異動，退職などの人事情報を管理し，給与計算機能や関連システムへの教職員情報提供を一元管理する.

主な利用者は，人事・総務部門の職員であるが，人事総合サービスの機能を提供する場合には，各個人からの人事異動情報の申請や個人情報（給与支給明細含む）の照会，職員育成計画の登録，業績や目標管理の申請・評価入力を行うため，全教職員がその利用対象となる.

取り扱う個人情報が多く，利用者も多岐にわたるため高いレベルでセキュリティ対応している．使用許諾データ及び業務の関係を利用者毎にＤＢ管理しておりLDAPベースの認証基盤にも対応可能となっている.

機密データについては，SecureBox(フォルダ単位などでの自動暗号化複合化機能)による暗号化を行うとともに，表形式データへのデータ抽出や給与明細表の PDF 化とファイルダウンロード時の暗号化対応も実施している.

2.6 ワークフロー(MyOFFICE) [9]

人事諸届け，就業関係，旅費精算，総務購買などの日常的な事務処理サービスシステムである．内部的に人事給与システムと連携できる．本システムは未だ多くの大学に導入されてはいないが注目はされつつある.

利用者は全ての教職員であり，教育研究 NET，事務用 NET の双方にサーバを設置する必要が有る．人事給与システムと同様だが，ICカードや生体認証を使った厳しい本人確認処理が必要で，アクセス記録も必須である.

利用権限は申請者，承認者という関係については，個別申請に対する権限を動的に個人に対して指定可能である他に管理職としての権限定義，代行設定などが行える.

3. ID管理体系の整理とSSO要求

一般的に，ID体系が全学的に統一されない最大の理由は組織が縦割りで，全体を統制する機能が弱い事だと言われる．個別事由を調整して全学的な調整を行っていくCIO的な職務の設置が今後は不可欠になっていくと考える.

3.1 ID体系の相互関係と全学共通IDの可能性に関する考察

教職員の ID と基本情報は人事システムで最初に作られ，学生の ID と基本情報は学生管理基幹システムで創成される性格を有する．現状，これらのシステムから必要な情報を抽出して，関係システムに配布している．この事は，この２つのシステムで作成される ID を全学的に共同利用できる可能性を示している．

現状，ID 体系は個別業務管理部門が独自の判断で設計しているが，汎用的で充分な大きさの ID 空間が提供されれば，共通化を妨げる要因は見当たらない．

それぞれの業務システムは他のシステムを利用する事が無い例外的な利用者，作業者などの為に限定的な固有 ID を追加できる柔軟性を求めて居る．この ID は全学的に配布されたとしても，その権限管理が正常に機能すれば実害は無く，これも全学共通 ID 体系の阻害要因では無い．

3.2 SSO 要求

日常の業務遂行が IT を活用して進められる範囲が拡大して行くに連れて，業務の切り換え時点で必要となる認証は煩雑なものと感じられて来る．

先に掲げた特徴的な業務だけでも，表１下段に示す様に特定の利用者毎に SSO に対する要求が発生し得る．

職員は自らが担当する業務システムと共通サービスであるワークフローと図書システムを利用するので，その範囲でのSSOが期待される．

教員はほぼ全てのシステムに何らかの関係を持つので，SSOが実現された場合のメリットが大きい事が判る．

しかし，実現に向けては生体認証など本人認証の強化，無応答時間監視などのなりすまし防止策を同時に施す必要が有る．

4. 利用権限集中管理方式

個人認証基盤として用いるディレクトリィシステムは，実質的な標準として多くの製品で対応されているLDAPをベースに考える事とした．LDAPは内部に持つ情報の柔軟性が有り,設計の

表１．業務毎の ID，権限管理と SSO 要求の関係

	図書館	基幹業務	e-Learning	財務会計	人事給与	ワークフロー
利用者	・図書館職員 ・学生 ・教員	・各事務部門職員 ・教員 ・学生とその親族 ・卒業生	・教員 ・補助教員 ・学生／聴講生 ・管理職員	・教員 ・会計関連職員	・幹部教員 ・幹部職員 ・人事関連職員	・全ての職員 ・全ての教員
内部管理IDと外部IDとの関係	独自ID体系だが，外部認証連携可能	学生を生涯管理すべく，内部ID番号付与．受験番号，学籍番号その他をリンク．教職員も内部番号を付与し，教職員コードと対応付け．	独自の認証だが，一般には学籍番号，教員コードを利用	独自の管理番号を個人に付与，職員コードと1：1対応させる．部門コードを合わせて設定し，アクセス範囲を規定．	独自の認証だが，一般的には教員・職員コードを利用	教職員IDで管理外部認証との連携可能．
業務権限との関係	職務名を自由に定義でき，職務名毎に利用できる機能一覧を定義．	個人(内部個人ID単位)に利用できるサブシステム＋機能を定義．	教員，TA，学生と課目(コース)の関係を定義。立場毎に機能範囲，権限規定．	個人ID毎に利用できるサブシステム，詳細機能範囲を定義． 物品調達では職務(申請者，承認者，部局職員，部局承認者，スーパ権限)毎に権限規定．代行者設定可．	個人(内部個人ID単位)に利用できる機能を定義するとともに，部門単位にセキュリティを設定(利用権限の無い部門の情報参照を抑止)。	職務階層構造を定義できる．承認者は動的に設定可．代行者設定可能．
保有個人情報	氏名、連絡先、貸し出し履歴。	学生に関して可能な限り全て．住所，氏名，資格，賞罰，経歴，保護者住所・氏名，保証人住所・氏名，健康管理，課外活動，奨学金，履修履歴，成績　その他 教員からは，資格(教務主任，就職担当など)，課外活動との関係，生活指導などの関係でアクセス制限．	所属，氏名，連絡先，履修・成績情報．	給与・旅費・謝金等の振込み先としての、氏名，口座情報．支払金額，個人研究内容．旅程等	人事情報(所属，氏名，生年月日，年齢，住所，採用，勤務，資格，職位，等級，職務履歴，業績，研修，目標管理，家族，通勤等)，給与情報(現職位，昇給，本給，手当，給与支給，控除，組合等，勤怠等)	人事情報，出張履歴など．
SSO要求						
学生	○	○	○			
教員	○	○	○	○	○	○
職員 図書	○					○
会計	○			○		○
人事	○				○	○
学生	○	○				○
教務	○	○	○			○

自由度が高いが，セキュリティ面，性能面での課題が指摘されており，これらの面はシステム設計上で配慮する必要が有る．

また，Webサービスのセキュア認証とSSOの基盤としてはやはり，実質的な標準となりつつあるSOAP[10]とKerberos[11]を利用する事で既存ブラウザでの一般的な利用を可能にする．

4.1 システムの構成

2 章での分析と 3 章で述べた ID 体系に対する考察から，本人認証時点で詳細な業務処理権限をディレクトリィで保持する事は，運用を考えた場合現実的でなく，サブシステム単位での利用権限認証に留めるべきである．詳細な権限は業務システムが審査する事とし，そこへのアクセス権限を初期の認証で検証し許可する構造を採用した．

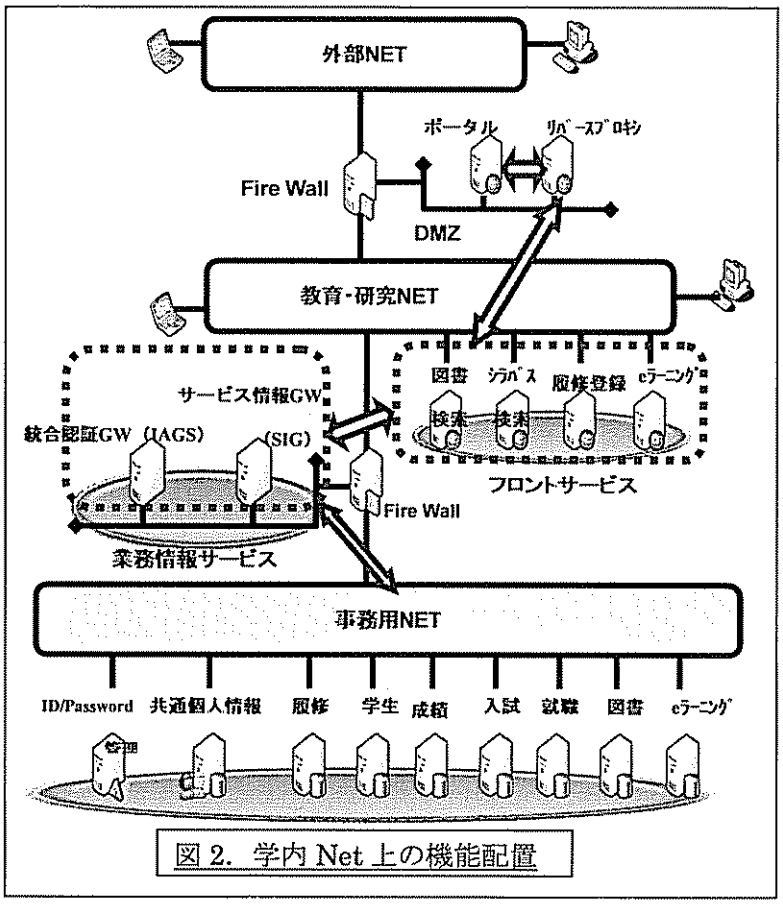

図 2. 学内 Net 上の機能配置

本人確認と業務認証を総合的に実施する IAG (Integrated Authentication Gateway) 経由で LDAP へアクセス，個人詳細情報へのアクセス制御を行う SIG (Service Information Gateway) 経由で詳細業務権限認証を実施する．全体の機能配置を図 2 に示す．ID/Password 管理は LDAP ディレクトリィを用いる．以下に本システムの特徴的なスキーマとして定義するオブジェクトクラスを説明する．

① 個人 ID/Password を属性として定義するオブジェクトクラスで，他に生涯 ID，個人名などの属性を持つ．

② 社会的な立場，役割を属性として定義するオブジェクトクラス

③ サービス機能と利用を許可された個人を属性として定義するオブジェクトクラス．

外部からのアクセスは全て DMZ 上のポータル経由で AIG に接続して本人認証を行った後，ポータルサービス経由の通信のみ許可される．

個人情報を扱う業務処理サービスは事務 NET に接続されている各種サーバで実施され，ここへのアクセスは FW(Fire Wall)経由でアプリケーションレイヤの接続制御を併用する事で強固なセキュリティを確保する．

4.2 処理の流れ

処理の流れを図 3 および以下に示す

①ポータルサービスに対してログイン要求送信

②ログイン要求はIAGを経由して認証サービスに送信され、正しくログイン処理がされるとTGS(Ticket Granting Server)からTGT(Ticket Granting Ticket)が発行される

③TGTと共に利用可能な業務が初期メニューとしてブラウザに渡され表示される

④メニューから業務を選択すると TGT がブラウザから業務サービスに送信される

⑤業務サービスは TGT の正当性を IAG 経由でチェック

⑥TGT の正当性がチェックされると SIG を経由して個人情報や詳細な業務権限を取得

⑦業務サービスで詳細な業務処理上のアクセス

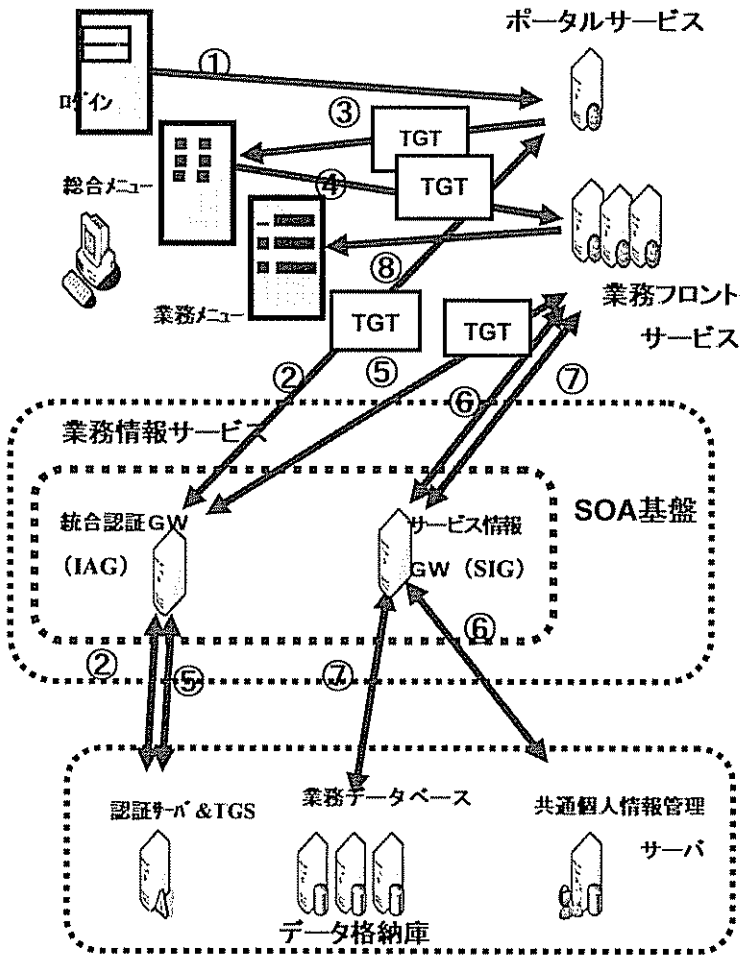

図 3. Login からサービス利用の流れ

権限をチェック

⑧業務処理の詳細メニューが表示され，個人の権限範囲での業務遂行を開始

個人情報は業務横断で利用できる構造に再設計して共通化し，専用サービスとして管理する方向で一元化を目指す．

5. まとめと今後の課題

本論文では大学で利用される複数の業務処理 Web アプリケーションでの ID ならびに利用権限管理とその認証システムの実現方法について現状の問題点と解決策を運用面，技術面含めて分析し設計した．

これにより，学内の本人認証システムの統合とセキュリティ強化，事務を含めた全学 NET の構築を安全に行える方式が確立できた．

大学システムの高度化とサービスの安価かつ短納期実現を目指して，今後は SOA の概念に沿って全ての業務を包含した大学システムのモデル化を推進していく．それにより，様々な業務の段階的な構築の容易性や既存ツールのサービス化による再利用促進が実現できると信ずる．それらの共通基盤として個人情報管理システムを具体化していきたい．

参考文献

(1) LDAP：Lightweight Directory Access Protocol(v3), RFC2251(Dec. 1997)

(2)能城他："異機種環境におけるディレクトリィサービスを用いたユーザ管理機構システムの提案", Technical Report of IEICE, IN2002-196, IA2002-52 (2003-02), pp.31-34

(3) 梶田他："CAS によるセキュアな全学認証基盤の構築", IPSJ SIG Technical Report, 2005-DSM-37, pp.35-40 (2005)

(4) SOA：Service-Oriented Architecture, http://www-306.ibm.com/software/info/openenvironment/soa/

(5) ILIS/WAVE： http://software.fujitsu.com/jp/ilis_univ/wave/index.html

(6) Campusmate：http://software.fujitsu.com/jp/campusmate/intro.html

(7) Campusmate/CourseNavig：http://software.fujitsu.com/jp/campusmate/coursenavig/intro.html

(8)Glovia/Campus：http://glovia.fujitsu.com/jp/topics/03feb/030225t2.html

(9) MyOFFICE：http://glovia.fujitsu.com/jp/products/myoffice/index.html

(10) SOAP：http://www.w3.org/2000/xp/Group/

(11) Kerberos：The Kerberos Network Authentication Service(V5), RFC1510(Sep.1993)